Платформа Радар

API для внешних сервисов

Версия 4.2.0

ООО «Пангео Радар»

Оглавление

1. Общие сведения

В **Платформу Радар** можно обращаться из сторонних решений посредством публичного API, которое работает по протоколу HTTPS и предоставляет набор методов запрос/ответ.

Базовый пример запроса для удаленного обращения:

```
<Тип метода, например POST>

https://<MASTER_KARAKEN_HOST>:9000/<сервис>/<версия API>/<ресурс>/<endpoint>

PgrApiKey: <global_api_key>
Content-Type: application/json
PgrSelectedInstance: <идентификатор инстанса>

{
    <Тело запроса>
}
```

Где:

- <MASTER_KARAKEN_HOST> – это основная точка входа для обработки запросов;
- <port> – порт для обращения. По умолчанию: 9000;
- <сервис> – наименование сервиса (компонента), к которому выполняется запрос;
- <версия API> – версия API по которой выполняется запрос;
- <название ресурса> – название ресурса, к которому выполняется обращение. Например, service_asset_findings (Инциденты);
- <endpoint> – конечная точка указанного ресурса;
- <PgrApiKey> – авторизация с помощью ключа API, который можно получить в разделе **Администрирование → Кластер →** вкладка **API ключи →** параметр global_api_key. Пользователь, с помощью чьего ключа выполняется API-запрос, должен иметь права на выполнение такого типа запросов. Указывается в заголовке запроса;
- <PgrSelectedInstance> – идентификатор инстанса к которому будет выполнено обращение. Указывается в заголовке запроса. Идентификатор инстанса можно скопировать по соответствующей кнопке в разделе **Администрирование → Кластер →** вкладка **Управление мультиарендностью**.

Примечание *В документации все примеры приведены для локальных запросов, которое допускает обращение по протоколу HTTP. При удаленном обращении должен использоваться* ***только*** *протокол HTTPS и соответствующий порт.*

При описании моделей данных используются следующие обозначения:

- основная модель;
- модель второго уровня: объект или массив, входящий в основную модель;
- модель третьего уровня: объект или массив, входящий в модель второго уровня;
- модель четвертого уровня: объект или массив, входящий в модель третьего уровня.

2. Инциденты ИБ

2.1 Инциденты

2.1.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	service_asset_findings
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	Ресурс service_asset_findings отвечает за управление инцидентами информационной безопасности.

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/service_asset_findings/create	Создание инцидента
PUT	/service_asset_findings/update	Обновление информации об инциденте
POST	/service_asset_findings/search	Поиск инцидентов
GET	/service_asset_findings/{id}	Получение инцидента по ID
DELETE	/service_asset_findings/{id}	Удаление инцидента
POST	/service_asset_findings/group	Группировка инцидентов
POST	/service_asset_findings/mass_delete	Удаление списка инцидентов

Тип	Метод	Описание
DELETE	/service_asset_findings/all	Удаление всех инцидентов
GET	/service_asset_findings/_meta	Получение свойств инцидентов и действий пользователей
GET	/sevice_asset_findings/by_event_uuid	Поиск инцидентов, связанных с конкретным событием
POST	/service_asset_findings/add_events	Добавление связи событий с инцидентом через правило корреляции
POST	/service_asset_findings/close_for_occurrences	Закрытие инцидентов по ID происшествий
POST	/service_asset_findings/bulk_create_with_vulnerabilities	Создание/обновление инцидентов из уязвимостей
POST	/service_asset_finding/mass_change_status	Массовое изменение статуса инцидентов
POST	/service_asset_finding/mass_assign_to_user	Массовое изменение пользователя инцидентов

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
500	Ошибка сервера

Модели объектов:

Название	Описание
ServiceAssetFinding	Модель данных ресурса service_asset_findings

2.1.2 Модель ресурса «Инциденты»

Модель данных ServiceAssetFinding:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор инцидента
created_at	string time	Required	Дата создания в формате: date-time
updated_at	string time	Required	Дата изменения в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента

Параметр	Тип данных	Обязательность	Описание
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace; - delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе

Параметр	Тип данных	Обязательность	Описание
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов
service_asset_name	string	Required	Название актива, на котором обнаружен инцидент
service_asset_active	boolean	Required	Флаг активности актива
occurrence_count	integer	Required	Количество происшествий
user_short_name	string	Optional	Короткое имя пользователя
group_name	string	Optional	Наименование группы, в которую добавлен инцидент
finding_display_id	integer	Required	Идентификатор типа инцидента
reopened_count	integer	Optional	Количество переоткрытий
event_type	string	Optional	Тип связанных событий на основе привязанного правила
finding_type	string	Required	Тип инцидента
ports	Array<integer>	Required	Порты на которых найдена уязвимость
last_occurrence_id	string uuid		Идентификатор последнего происшествия в формате uuid
service_asset_value	integer	Required	Значимость актива
tag_titles	Array<string>		Набор тэгов
last_status_change	string time	Optional	Дата последнего изменения статуса в формате: date-time

Параметр	Тип данных	Обязательность	Описание
last_scan	string time	Optional	Дата последнего выполненного сканирования актива в формате: date-time
authenticated	boolean	Optional	Флаг проводилось ли сканирование актива с использованием сканера
last_occurrence	string time	Optional	Дата последнего происшествия в формате: date-time
remote_exploitable	boolean	Optional	Флаг эксплуатируема ли уязвимость удаленно
service_asset_network_exposure	integer	Required	Сетевая доступность актива. Тип сетевой видимости актива может принимать следующие значения: - 1 – актив напрямую подключен к сети Интернет; - 2 – актив располагается в демилитаризованной зоне (DMZ); - 3 – актив подключен к сети Интернет через Proxy-сервер; - 4 – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы; - 5 – актив не подключен к сети.
finding_category	string	Required	Категория типа инцидента
display_title	string	Optional	Заголовок
customer_retention_time	integer	Optional	Продолжительность работы клиента
visible_since	string time	Optional	Дата, с которой инцидент виден пользователям в формате date-time
visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
last_customer_status_change	string time	Optional	Дата последнего изменения статуса пользователем в формате: date-time
finding_title	string	Required	Заголовок инцидента
incident_group_title	string	Optional	Название группы инцидентов
custom_values	object	Optional	Связанные поля, заполненные вручную или при сработке правила
trace_id	string uuid	Optional	Идентификатор действия для аудита жизненного цикла сущности в формате uuid
service_asset	object<ServiceAsset>	Optional	Актив
finding	object	Optional	Тип инцидента
last_occurrence_entity	object<Occurrence>	Optional	Последнее происшествие
user	object	Optional	Пользователь
group	object	Optional	Группа пользователей
incident_group	object<IncidentGroup>	Optional	Группа инцидентов

Параметр	Тип данных	Обязательность	Описание
occurrences	Array<Occurrence>	Optional	Массив связанных происшествий
custom_field_values	Array<CustomFieldValue>	Optional	Массив значений дополнительных полей
comments	Array<object>	Optional	Комментарии пользователей
documents	Array<object>	Optional	Документы
messages	Array<Message>	Optional	Связанные сообщения пользователей
service_asset_finding_status_changes	Array<ServiceAssetFindingStatusChange >	Optional	Связанные операции по изменению статуса инцидента
service_asset_groups	Array<ServiceAssetGroup>	Optional	Связанные группы активов
_relations	object<relations>	Optional	Словарь, описывающий связанные модели через идентификаторы

Модель данных ServiceAsset:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор актива
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
type	string	Required	Тип актива
name	string	Required	Название актива
description	string	Optional	Описание актива
coordinates	string	Optional	Координаты актива (не используется)
active	boolean	Optional	Флаг активности
scan_id	string	Optional	ID сканера активов (не используется)
value	integer	Optional	Значимость актива. В платформе значимость актива может принимать следующие значения: - 1 – ключевой; - 2 – важный; - 3 – некритичный; - 4 – распределенный;

Параметр	Тип данных	Обязательность	Описание
			- 5 – тестовый.
client_note	string	Optional	Клиентские заметки (не используется)
internal_note	string	Optional	Внутренние заметки (не используется)
location	string	Required	Расположение актива
network_exposure	integer	Optional	Сетевая доступность актива. Тип сетевой видимости актива может принимать следующие значения: - 1 – актив напрямую подключен к сети Интернет; - 2 – актив располагается в демилитаризованной зоне (DMZ); - 3 – актив подключен к сети Интернет через Proxy-сервер; - 4 – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы; - 5 – актив не подключен к сети.
responsible_person	string	Optional	Ответственное лицо
technical_specialist	string	Optional	Технический специалист
responsible_group_id	string	Optional	ID группы ответственных
edited_by	string	Optional	Кем изменён (не используется)

Модель данных Occurrence:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор происшествия
created_at	string time	Required	Дата создания происшествия: date-time
updated_at	string time	Required	Дата изменения происшествия: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
event_type	string	Required	Тип происшествия. Допустимые значения: - manual_source - logmule_go_result - software_compliance_source - vulnerability - watchdog_result
ip	string	Required	IP-адрес актива
mac	string	Required	MAC-адрес актива

Параметр	Тип данных	Обязательность	Описание
start_occurrence	string	Required	Время первого изменения статуса в клиентской системе
end_occurrence	string	Required	Время последнего изменения статуса в клиентской системе
service_asset_finding_status_change_id	string	Required	Идентификатор операции смены статуса инцидента
service_asset_finding_id	string	Required	Идентификатор инцидента
fqdn	string	Required	FQDN актива
incident_identifier	string	Required	Идентификатор инцидента во внешней системе
fincert_sync_status	number	Required	Состояние синхронизации с внешней системой
fincert_id	string	Required	Идентификатор внешней системы
sopka_sync_status	number	Required	Состояние синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)
sopka_id	string	Required	Идентификатор внешней системы реагирования на компьютерные инциденты (CERT)
fincert_sync_result	string	Required	Результат синхронизации с внешней системой
sopka_sync_result	string	Required	Результат синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)
id	string	Required	Идентификатор происшествия
created_at	string time	Required	Дата создания происшествив: date-time
updated_at	string time	Required	Дата изменения происшествия: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
event_type	string	Required	Тип происшествия. Допустимые значения: - manual_source - logmule_go_result - software_compliance_source - vulnerability - watchdog_result
ip	string	Required	IP-адрес актива
mac	string	Required	MAC-адрес актива
start_occurrence	string	Required	Время первого изменения статуса в клиентской системе
end_occurrence	string	Required	Время последнего изменения статуса в клиентской системе
service_asset_finding_status_change_id	string	Required	Идентификатор операции смены статуса инцидента

Параметр	Тип данных	Обязательность	Описание
service_asset_finding_id	string	Required	Идентификатор инцидента
fqdn	string	Required	FQDN актива
incident_identifier	string	Required	Идентификатор инцидента во внешней системе
fincert_sync_status	number	Required	Состояние синхронизации с внешней системой
fincert_id	string	Required	Идентификатор внешней системы
sopka_sync_status	number	Required	Состояние синхронизации с внешней системой реагирования на компьютерные инциденты
sopka_id	string	Required	Идентификатор внешней системы реагирования на компьютерные инциденты
fincert_sync_result	string	Required	Результат синхронизации с внешней системой
sopka_sync_result	string	Required	Результат синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)

IncidentGroup:

Параметр	Тип данных	Обязательность	Описание
title	string	Required	Название группы инцидентов
description	string	Optional	Расширенное описание группы инцидентов
user_id	string	Optional	Идентификатор назначенного пользователя
group_id	string	Optional	Идентификатор назначенной группы пользователей

Модель данных CustomFieldValue:

Параметр	Тип данных	Обязательность	Описание
custom_field_id	string	Optional	Идентификатор значения дополнительного поля
service_asset_finding_id	string	Optional	Идентификатор инцидента, в которое добавлено дополнительное поле
string_value	string	Optional	Значение дополнительного поля с типом данных "строка"
integer_value	integer	Optional	Значение дополнительного поля с типом данных "целое число"

Параметр	Тип данных	Обязательность	Описание
float_value	number	Optional	Значение дополнительного поля с типом данных "число с плавающей запятой"
date_value	date	Optional	Значение дополнительного поля с типом данных "дата"
json_value	string	Optional	Значение дополнительного поля с типом данных "JSON"
boolean_value	boolean	Optional	Значение дополнительного поля с типом данных "логический"

Модель данных Message:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор сообщения пользователя
created_at	string	Required	Дата создания в формате `date-time`
updated_at	string	Required	Дата изменения в формате `date-time`
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
subject	string	Optional	Тема (Предмет) сообщения
body	string	Optional	Тело сообщения
service_asset_id	string	Optional	Идентификатор связанного актива
service_asset_finding_id	string	Optional	Идентификатор связанного инцидента
service_asset_finding_status_change_id	string	Optional	Идентификатор связанного изменения статуса инцидента
automated	boolean	Optional	Флаг автоматического создания
finding_id	string	Optional	Идентификатор связанного типа инцидента
itsm_sync_status	string	Optional	Статус синхронизации с внешними системами. Допустимые значения: - not_synced - scheduled - aborted - synced - waiting_confirmation
itsm_last_synced_at	string	Optional	Время синхронизации с внешними системами
itsm_sync_error	string	Optional	Описание ошибки синхронизации

Параметр	Тип данных	Обязательность	Описание
sender_id	string	Optional	Идентификатор пользователя инициировавшего синхронизацию

ServiceAssetFindingStatusChange:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор операции смены статуса инцидиента
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
service_asset_finding_id	string	Required	Идентификатор инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
revisit_at	string	Optional	Возвращен ли статус
itsm_sync_status	string	Optional	Статус синхронизации с внешними системами. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
itsm_last_synced_at	string	Optional	Время синхронизации с внешними системами в формате date-time
itsm_sync_error	string	Optional	Описание ошибки синхронизации
user_id	string	Required	Идентификатор пользователя

Модель данных ServiceAssetGroup:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы активов
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
name	string	Required	Название группы активов
network_ranges	Array<string>	Optional	Список подсетей
domain	string	Optional	Домен
itsm_synced	boolean	Optional	Признак синхронизации с системой управления ИТ-услугами
regex	string	Optional	Регулярное выражение
subject_id	string	Optional	Идентификатор субъекта
object_id	string	Optional	Идентификатор объекта
is_kii	boolean	Optional	Признак принадлежности к объектам критической инфраструктуры
is_fincert	boolean	Optional	Признак вхождения в систему информационного обмена между участниками финансового рынка
responsible_person	string	Optional	Имя ответственного пользователя
technical_specialist	string	Optional	Технический специалист
system_id	string	Optional	Идентификатор системы
responsible_group_id	string	Optional	Идентификатор ответственной группы
edited_by	string	Optional	Идентификатор пользователя, внесшего изменения

Relations:

Параметр	Тип данных	Обязательность	Описание
occurrences	Array<string>	Optional	Идентификаторы происшествий
custom_field_values	Array<string>	Optional	Идентификаторы значений дополнительных полей

Параметр	Тип данных	Обязательность	Описание
comments	Array<string>	Optional	Идентификаторы комментариев
documents	Array<string>	Optional	Связанные документы
messages	Array<string>	Optional	Связанные сообщения пользователей
service_asset_finding_status_changes	Array<string>	Optional	Связанные операции по изменению статуса инцидента
service_asset_groups	Array<string>	Optional	Идентификаторы групп инцидентов

2.1.3 Создание инцидента

Запрос:

Тип	Метод
POST	/service_asset_findings/create

Описание:

При выполнении запроса будет создан инцидент с заданными параметрами.

Параметры заголовка:

Pgr-User-ID: ID пользователя (uuid).

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_findings/create
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace;

Параметр	Тип данных	Обязательность	Описание
			- delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную

Параметр	Тип данных	Обязательность	Описание
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов

Пример тела запроса:


```
{
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "mitigation": "string",
  "status": "assigned_customer",
  "risklevel": 0,
  "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
  "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
  "analysis_output": "string",
  "synopsis": "string",
  "title": "string",
  "risk": "none",
  "acknowledged_at": "2023-12-20T00:00:01.652259Z",
  "alert_type": "automatic",
  "client_note": "string",
  "internal_note": "string",
  "external": false,
  "immediate_action_score": 0,
  "throughput_period": "grace",
  "throughput_period_change": "2023-12-20T00:00:01.652259Z",
  "customer_created": false,
  "c_visible_since": "2023-12-20T00:00:01.652259Z",
  "c_visible_since_in_days": 0,
  "c_reopened_count": 0,
  "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
  "logmule_identifier": "string",
  "c_remote_exploitable": true,
  "c_occurrence_count": 0,
  "c_customer_retention_time": 0,
  "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "itsm_sync_status": "scheduled",
  "external_id": "string",
  "itsm_sync_error": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
  "reopened_at": "2023-12-20T00:00:01.652259Z",
  "display_id": 0
}
```

Успешный ответ:

Статус код: 201 - успешное создание инцидента.

Формат: JSON.

Тело ответа: «Модель ресурса «Инциденты»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "mitigation": "string",
  "status": "assigned_customer",
  "risklevel": 0,
  "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
  "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
  "analysis_output": "string",
  "synopsis": "string",
  "title": "string",
  "risk": "none",
  "acknowledged_at": "2023-12-20T00:00:01.652259Z",
  "alert_type": "automatic",
  "client_note": "string",
  "internal_note": "string",
  "external": false,
  "immediate_action_score": 0,
  "throughput_period": "grace",
  "throughput_period_change": "2023-12-20T00:00:01.652259Z",
  "customer_created": false,
  "c_visible_since": "2023-12-20T00:00:01.652259Z",
  "c_visible_since_in_days": 0,
  "c_reopened_count": 0,
  "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
  "logmule_identifier": "string",
  "c_remote_exploitable": true,
  "c_occurrence_count": 0,
  "c_customer_retention_time": 0,
  "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "itsm_sync_status": "scheduled",
  "external_id": "string",
  "itsm_sync_error": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
  "reopened_at": "2023-12-20T00:00:01.652259Z",
  "display_id": 0,
```

```
"service_asset_name": "string",
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
},
"finding": {},
"last_occurrence_entity": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
```

```
    "end_occurrence": "2023-12-20T00:00:01.652259Z",
    "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-ee5963306be7",
    "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
    "fqdn": "string",
    "incident_identifier": "string",
    "fincert_sync_status": 10,
    "fincert_id": "",
    "sopka_sync_status": 10,
    "sopka_id": "",
    "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
    "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
  },
  "user": {},
  "group": {},
  "incident_group": {
    "title": "string",
    "description": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
  },
  "occurrences": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "uuid",
      "event_type": "manual_source",
      "ip": "string",
      "mac": "string",
      "port": 0,
      "start_occurrence": "2023-12-20T00:00:01.652259Z",
      "end_occurrence": "2023-12-20T00:00:01.652259Z",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "fqdn": "string",
      "incident_identifier": "string",
      "fincert_sync_status": 10,
      "fincert_id": "",
      "sopka_sync_status": 10,
      "sopka_id": "",
      "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
      "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
    }
  ],
  "custom_field_values": [
    {
      "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "string_value": "string",
      "integer_value": 0,
      "float_value": 0,
      "date_value": "2023-12-20T00:00:01.652259Z",
      "json_value": {},
      "boolean_value": true
    }
  ],
  "comments": [
    {}
  ],
  "documents": [
    {}
  ],
  "messages": [
```

```
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "uuid",
      "subject": "string",
      "body": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "automated": true,
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
    }
  ],
  "service_asset_finding_status_changes": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "uuid",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "status": "string",
      "revisit_at": "string",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
    }
  ],
  "service_asset_groups": [
    {
      "title": "string",
      "description": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
    }
  ],
  "_relations": {
    "occurrences": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "custom_field_values": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "comments": [
      "string"
    ],
    "documents": [
      "string"
    ],
    "messages": [
      "string"
    ],
    "service_asset_finding_status_changes": [
      "string"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
```

```
  }
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при создании объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.4 Обновление инцидента

Запрос:

Тип	Метод
PUT	/service_asset_findings/update

Описание:

При выполнении запроса будет обновлена информация об инциденте в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля модели, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в объекте _relations отсутствуют зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются;
- Зависимости игнорируются в теле запроса;
- Зависимости в ответе всегда null.

Пример запроса:

PUT

`http://127.0.0.1/cruddy/v2/service_asset_findings/update`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор инцидента
created_at	string time	Required	Дата создания в формате: date-time
updated_at	string time	Required	Дата изменения в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят

Параметр	Тип данных	Обязательность	Описание
			- verify_close - ожидает проверки; - working_customer - в работе.
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace; - delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем

Параметр	Тип данных	Обязательность	Описание
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов
_relations	object<relations>	Optional	Словарь, описывающий связанные модели через идентификаторы

Модель object<relations>:

Параметр	Тип данных	Обязательность	Описание
occurrences	Array<string>	Optional	Идентификаторы происшествий

Параметр	Тип данных	Обязательность	Описание
custom_field_values	Array<string>	Optional	Идентификаторы значений дополнительных полей
comments	Array<string>	Optional	Идентификаторы комментариев
documents	Array<string>	Optional	Связанные документы
messages	Array<string>	Optional	Связанные сообщения пользователей
service_asset_finding_status_changes	Array<string>	Optional	Связанные операции по изменению статуса инцидента
service_asset_groups	Array<string>	Optional	Идентификаторы групп инцидентов

Пример тела запроса:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "mitigation": "string",
  "status": "assigned_customer",
  "risklevel": 0,
  "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
  "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
  "analysis_output": "string",
  "synopsis": "string",
  "title": "string",
  "risk": "none",
  "acknowledged_at": "2023-12-20T00:00:01.652259Z",
  "alert_type": "automatic",
  "client_note": "string",
  "internal_note": "string",
  "external": false,
  "immediate_action_score": 0,
  "throughput_period": "grace",
  "throughput_period_change": "2023-12-20T00:00:01.652259Z",
  "customer_created": false,
  "c_visible_since": "2023-12-20T00:00:01.652259Z",
  "c_visible_since_in_days": 0,
  "c_reopened_count": 0,
  "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
  "logmule_identifier": "string",
  "c_remote_exploitable": true,
  "c_occurrence_count": 0,
  "c_customer_retention_time": 0,
  "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "itsm_sync_status": "scheduled",
  "external_id": "string",
  "itsm_sync_error": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
```

```
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
  "reopened_at": "2023-12-20T00:00:01.652259Z",
  "display_id": 0,
  "_relations": {
    "occurrences": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "custom_field_values": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "comments": [
      "string"
    ],
    "documents": [
      "string"
    ],
    "messages": [
      "string"
    ],
    "service_asset_finding_status_changes": [
      "string"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
```


Успешный ответ:

Статус код: 200 - успешное обновление информации об инциденте.

Формат: JSON.

Тело ответа: «Модель ресурса «Инциденты»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "mitigation": "string",
  "status": "assigned_customer",
  "risklevel": 0,
  "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
  "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
  "analysis_output": "string",
  "synopsis": "string",
```

```
  "title": "string",
  "risk": "none",
  "acknowledged_at": "2023-12-20T00:00:01.652259Z",
  "alert_type": "automatic",
  "client_note": "string",
  "internal_note": "string",
  "external": false,
  "immediate_action_score": 0,
  "throughput_period": "grace",
  "throughput_period_change": "2023-12-20T00:00:01.652259Z",
  "customer_created": false,
  "c_visible_since": "2023-12-20T00:00:01.652259Z",
  "c_visible_since_in_days": 0,
  "c_reopened_count": 0,
  "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
  "logmule_identifier": "string",
  "c_remote_exploitable": true,
  "c_occurrence_count": 0,
  "c_customer_retention_time": 0,
  "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "itsm_sync_status": "scheduled",
  "external_id": "string",
  "itsm_sync_error": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
  "reopened_at": "2023-12-20T00:00:01.652259Z",
  "display_id": 0,
  "_relations": {
    "occurrences": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "custom_field_values": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "comments": [
      "string"
    ],
    "documents": [
      "string"
    ],
    "messages": [
      "string"
    ],
    "service_asset_finding_status_changes": [
      "string"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.5 Поиск инцидентов

Запрос:

Тип	Метод
POST	/service_asset_findings/search

Описание:

При выполнении запроса будут возвращены найденные инциденты с учётом заданных фильтров.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/service_asset_findings/search`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений - substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят связанность с моделью по идентификатору если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null

Параметр	Тип данных	Обязательность	Описание
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "virtual_search": {
    "value": "string",
    "strict": false
  },
  "relations": [
```

```
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array<ServiceAssetFinding>	Список найденных инцидентов
total	integer	Количество найденных инцидентов

Пример ответа:


```
{
  "items": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "analysis_output": "string",
      "synopsis": "string",
      "title": "string",
      "risk": "none",
      "acknowledged_at": "2023-12-20T00:00:01.652259Z",
      "alert_type": "automatic",
      "client_note": "string",
      "internal_note": "string",
      "external": false,
      "immediate_action_score": 0,
      "throughput_period": "grace",
      "throughput_period_change": "2023-12-20T00:00:01.652259Z",
      "customer_created": false,
```

```
"c_visible_since": "2023-12-20T00:00:01.652259Z",
"c_visible_since_in_days": 0,
"c_reopened_count": 0,
"c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"logmule_identifier": "string",
"c_remote_exploitable": true,
"c_occurrence_count": 0,
"c_customer_retention_time": 0,
"last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
"itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
"itsm_sync_status": "scheduled",
"external_id": "string",
"itsm_sync_error": "string",
"user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
"updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
"group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
"acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
"created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
"edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
"incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
"reopened_at": "2023-12-20T00:00:01.652259Z",
"display_id": 0,
"service_asset_name": "string",
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
```

```
        "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
        "value": 3,
        "client_note": "string",
        "internal_note": "string",
        "location": "string",
        "network_exposure": 3,
        "responsible_person": "string",
        "technical_specialist": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      },
      "finding": {},
      "last_occurrence_entity": {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "trace_id": "uuid",
        "event_type": "manual_source",
        "ip": "string",
        "mac": "string",
        "port": 0,
        "start_occurrence": "2023-12-20T00:00:01.652259Z",
        "end_occurrence": "2023-12-20T00:00:01.652259Z",
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "fqdn": "string",
        "incident_identifier": "string",
        "fincert_sync_status": 10,
        "fincert_id": "",
        "sopka_sync_status": 10,
        "sopka_id": "",
        "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
        "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
      },
      "user": {},
      "group": {},
      "incident_group": {
        "title": "string",
        "description": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
      },
      "occurrences": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "trace_id": "uuid",
          "event_type": "manual_source",
          "ip": "string",
          "mac": "string",
          "port": 0,
          "start_occurrence": "2023-12-20T00:00:01.652259Z",
          "end_occurrence": "2023-12-20T00:00:01.652259Z",
          "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "fqdn": "string",
          "incident_identifier": "string",
          "fincert_sync_status": 10,
          "fincert_id": "",
          "sopka_sync_status": 10,
          "sopka_id": "",
```

```
        "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
        "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
      }
    ],
    "custom_field_values": [
      {
        "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "string_value": "string",
        "integer_value": 0,
        "float_value": 0,
        "date_value": "2023-12-20T00:00:01.652259Z",
        "json_value": {},
        "boolean_value": true
      }
    ],
    "comments": [
      {}
    ],
    "documents": [
      {}
    ],
    "messages": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "trace_id": "uuid",
        "subject": "string",
        "body": "string",
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "automated": true,
        "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
        "itsm_sync_status": "not_synced",
        "itsm_last_synced_at": "string",
        "itsm_sync_error": "string",
        "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
      }
    ],
    "service_asset_finding_status_changes": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "trace_id": "uuid",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "status": "string",
        "revisit_at": "string",
        "itsm_sync_status": "not_synced",
        "itsm_last_synced_at": "string",
        "itsm_sync_error": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
      }
    ],
    "service_asset_groups": [
      {
        "title": "string",
        "description": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
      }
```

```
      ],
      "_relations": {
        "occurrences": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "custom_field_values": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "comments": [
          "string"
        ],
        "documents": [
          "string"
        ],
        "messages": [
          "string"
        ],
        "service_asset_finding_status_changes": [
          "string"
        ],
        "service_asset_groups": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "total": 1
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.6 Получение инцидента по ID

Запрос:

Тип	Метод
GET	/service_asset_findings/{id}

Описание:

При выполнении запроса будет возвращен инцидент с соответствующим ID.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/service_asset_findings/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор инцидента

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Инциденты»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
```

```
"description": "string",
"risk_impact": "string",
"solution": "string",
"mitigation": "string",
"status": "assigned_customer",
"risklevel": 0,
"service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
"finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
"analysis_output": "string",
"synopsis": "string",
"title": "string",
"risk": "none",
"acknowledged_at": "2023-12-20T00:00:01.652259Z",
"alert_type": "automatic",
"client_note": "string",
"internal_note": "string",
"external": false,
"immediate_action_score": 0,
"throughput_period": "grace",
"throughput_period_change": "2023-12-20T00:00:01.652259Z",
"customer_created": false,
"c_visible_since": "2023-12-20T00:00:01.652259Z",
"c_visible_since_in_days": 0,
"c_reopened_count": 0,
"c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"logmule_identifier": "string",
"c_remote_exploitable": true,
"c_occurrence_count": 0,
"c_customer_retention_time": 0,
"last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
"itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
"itsm_sync_status": "scheduled",
"external_id": "string",
"itsm_sync_error": "string",
"user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
"updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
"group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
"acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
"created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
"edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
"incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
"reopened_at": "2023-12-20T00:00:01.652259Z",
"display_id": 0,
"service_asset_name": "string",
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
```

```
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
},
"finding": {},
"last_occurrence_entity": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
  "end_occurrence": "2023-12-20T00:00:01.652259Z",
  "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-ee5963306be7",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "fqdn": "string",
  "incident_identifier": "string",
  "fincert_sync_status": 10,
  "fincert_id": "",
  "sopka_sync_status": 10,
  "sopka_id": "",
  "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
  "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
},
"user": {},
"group": {},
"incident_group": {
  "title": "string",
  "description": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
},
"occurrences": [
```

```
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "uuid",
      "event_type": "manual_source",
      "ip": "string",
      "mac": "string",
      "port": 0,
      "start_occurrence": "2023-12-20T00:00:01.652259Z",
      "end_occurrence": "2023-12-20T00:00:01.652259Z",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "fqdn": "string",
      "incident_identifier": "string",
      "fincert_sync_status": 10,
      "fincert_id": "",
      "sopka_sync_status": 10,
      "sopka_id": "",
      "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
      "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
    }
  ],
  "custom_field_values": [
    {
      "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "string_value": "string",
      "integer_value": 0,
      "float_value": 0,
      "date_value": "2023-12-20T00:00:01.652259Z",
      "json_value": {},
      "boolean_value": true
    }
  ],
  "comments": [
    {}
  ],
  "documents": [
    {}
  ],
  "messages": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "uuid",
      "subject": "string",
      "body": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "automated": true,
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
    }
  ],
  "service_asset_finding_status_changes": [
    {
```

```
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "uuid",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "status": "string",
      "revisit_at": "string",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
    }
  ],
  "service_asset_groups": [
    {
      "title": "string",
      "description": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
    }
  ],
  "_relations": {
    "occurrences": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "custom_field_values": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "comments": [
      "string"
    ],
    "documents": [
      "string"
    ],
    "messages": [
      "string"
    ],
    "service_asset_finding_status_changes": [
      "string"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.7 Удаление инцидента

Запрос:

Тип	Метод
DELETE	/service_asset_findings/{id}

Описание:

При выполнении запроса будет удален инцидент с соответствующим ID.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/service_asset_findings/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор инцидента

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
error	string	Текст ошибки
error_code	array	Код ошибки. Допустимые значения: - 11002 - общая ошибка удаления; - 11003 - запрос не затронул ни одной сущности; - 11004 - удаляемый объект не найден; - 11011 - удаление невозможно из-за наличия блокирующих связей
relations	object RelationErrors	Объект, содержащий информацию о связанных моделях, блокирующих удаление
relations{dynamic_relation_name}	Array<object>	Поле объекта описывает название связи и может отличаться в зависимости от конкретной модели и существующих у нее связей
{dynamic_relation_name}/id	string	Идентификатор модели, блокирующей удаление
{dynamic_relation_name}/name	string	Название или описание модели если оно у нее есть

Пример ответа:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.8 Группировка инцидентов

Запрос:

Тип	Метод
POST	/service_asset_findings/group

Описание:

При выполнении запроса инциденты будут сгруппированы по заданному полю.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/service_asset_findings/group`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки инцидентов

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.9 Массовое удаление инцидентов

Запрос:

Тип	Метод
POST	/service_asset_findings/mass_delete

Описание:

При выполнении запроса будут удалены инциденты с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_findings/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности; - 11011 - удаление невозможно из-за наличия связанных данных.

Пример ответа:

```
{
  "results": [
    {
      "id": "string",
      "error_code": 11001
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.10 Удаление всех инцидентов

Запрос:

Тип	Метод
DELETE	/service_asset_findings/all

Описание:

При выполнении запроса из базы данных будут удалены все инциденты.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/service_asset_findings/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.11 Получение свойств инцидентов и действий пользователей

Запрос:

Тип	Метод
GET	/service_asset_findings/_meta

Описание:

При выполнении запроса будут возвращены свойства инцидентов и список действий пользователей над ними.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/service_asset_findings/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:


```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
```

```
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.12 Добавление связи события с инцидентом

Запрос:

Тип	Метод
POST	/service_asset_findings/add_events

Описание:

При выполнении запроса будет создана связь события с инцидентом через правило корреляции.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_findings/add_events
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
incident_id	string uuid	Required	Идентификатор инцидента в формате uuid
logmule_rule_id	string uuid	Required	Идентификатор правила корреляции в формате uuid
event_ids	Array<string>	Required	Список идентификаторов событий

Пример тела запроса:

```
{
  "incident_id": "2f811c5b-b888-4fb3-aac5-3c6a4b05df32",
  "logmule_rule_id": "7ab24f6b-16c5-4921-b571-0ae76a048bb4",
  "event_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
results	object	Результат добавления события в инциденте
results{event_id}	string uuid	Идентификатор события в формате uuid
results{error_code}	number	0 - отсутствие ошибки, событие добавлено к инциденту; 12001 - ошибка создания результата сработки с инцидентом; 12002 - событие не найдено; 12003 - поле @timestamp не найдено в событии; 12004 - поле @timestamp имеет неправильный тип; 12005 - ошибка парсинга поля @timestamp 12006 - инцидент не найден; 12007 - ошибка прикрепления сработки к инциденту 12008 - ошибка кодирования события в JSON 12009 - событие уже добавлено к инциденту

Пример ответа:


```
{
  "results": {
    "event_id": "a7a26ff2-e851-45b6-9634-d595f45458b7",
    "error_code": 0
  }
}
```


2.1.13 Поиск инцидентов по событию

Запрос:

Тип	Метод
GET	/sevice_asset_findings/by_event_uuid

Описание:

При выполнении запроса будет выполнен поиск инцидентов, связанных с указанным событием.

Параметры строки запроса:

Параметр	Тип данных	Обязательность	Описание
uuid	string	Required	Идентификатор события

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/sevice_asset_findings/by_event_uuid?uuid=a7a26ff2-e851-45b6-9634-d595f45458b7
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
objects	Array<ServiceAssetFinding>	Массив моделей полученных инцидентов (см. раздел «Модель ресурса «Инциденты»»)
total	number	Общее количество связанных инцидентов

Пример ответа:


```
{
  "objects": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "analysis_output": "string",
      "synopsis": "string",
      "title": "string",
      "risk": "none",
      "acknowledged_at": "2023-12-20T00:00:01.652259Z",
      "alert_type": "automatic",
      "client_note": "string",
      "internal_note": "string",
      "external": false,
      "immediate_action_score": 0,
      "throughput_period": "grace",
      "throughput_period_change": "2023-12-20T00:00:01.652259Z",
      "customer_created": false,
      "c_visible_since": "2023-12-20T00:00:01.652259Z",
      "c_visible_since_in_days": 0,
      "c_reopened_count": 0,
      "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "logmule_identifier": "string",
      "c_remote_exploitable": true,
      "c_occurrence_count": 0,
      "c_customer_retention_time": 0,
      "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "itsm_sync_status": "scheduled",
      "external_id": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
```

```
"created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
"edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
"incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
"reopened_at": "2023-12-20T00:00:01.652259Z",
"display_id": 0,
"service_asset_name": "string",
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
},
"finding": {},
"last_occurrence_entity": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
```

```
        "event_type": "manual_source",
        "ip": "string",
        "mac": "string",
        "port": 0,
        "start_occurrence": "2023-12-20T00:00:01.652259Z",
        "end_occurrence": "2023-12-20T00:00:01.652259Z",
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "fqdn": "string",
        "incident_identifier": "string",
        "fincert_sync_status": 10,
        "fincert_id": "",
        "sopka_sync_status": 10,
        "sopka_id": "",
        "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
        "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
      },
      "user": {},
      "group": {},
      "incident_group": {
        "title": "string",
        "description": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
      },
      "occurrences": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "trace_id": "uuid",
          "event_type": "manual_source",
          "ip": "string",
          "mac": "string",
          "port": 0,
          "start_occurrence": "2023-12-20T00:00:01.652259Z",
          "end_occurrence": "2023-12-20T00:00:01.652259Z",
          "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "fqdn": "string",
          "incident_identifier": "string",
          "fincert_sync_status": 10,
          "fincert_id": "",
          "sopka_sync_status": 10,
          "sopka_id": "",
          "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
          "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
        }
      ],
      "custom_field_values": [
        {
          "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "string_value": "string",
          "integer_value": 0,
          "float_value": 0,
          "date_value": "2023-12-20T00:00:01.652259Z",
          "json_value": {},
          "boolean_value": true
        }
      ],
      "comments": [
```

```
      {}
    ],
    "documents": [
      {}
    ],
    "messages": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "trace_id": "uuid",
        "subject": "string",
        "body": "string",
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "automated": true,
        "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
        "itsm_sync_status": "not_synced",
        "itsm_last_synced_at": "string",
        "itsm_sync_error": "string",
        "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
      }
    ],
    "service_asset_finding_status_changes": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "trace_id": "uuid",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "status": "string",
        "revisit_at": "string",
        "itsm_sync_status": "not_synced",
        "itsm_last_synced_at": "string",
        "itsm_sync_error": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
      }
    ],
    "service_asset_groups": [
      {
        "title": "string",
        "description": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
      }
    ],
    "_relations": {
      "occurrences": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "custom_field_values": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "comments": [
        "string"
      ],
      "documents": [
        "string"
      ],
      "messages": [
        "string"
      ],
```

```
        "service_asset_finding_status_changes": [
          "string"
        ],
        "service_asset_groups": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "total": 0
}
```


Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.1.14 Закрытие инцидентов по ID происшествий

Запрос:

Тип	Метод
POST	/service_asset_findings/close_for_occurrences

Описание:

При выполнении запроса инцидентам, выбранным по occurrence_id, будет присвоен статус closed.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/service_asset_findings/close_for_occurrences`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
occurrence_ids	Array<string>	Required	Список идентификаторов происшествий для поиска и закрытия инцидентов
user_id	string	Required	Идентификатор пользователя

Пример тела запроса:

```
{
  "occurrence_ids": [
    "0cd06fe9-9a7c-45d2-89e5-201e0d1c84e1",
    "f1b8a921-fee8-4bbd-bc3c-c4a7ea998303"
  ],
  "user_id": "128064b6-c95a-45b5-a0ee-94360df67274"
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов закрытия инцидентов
results{occurrence_id}	string	Идентификатор происшествия
results{service_asset_finding_id}	string	Идентификатор инцидента
results{error_code}	integer	Код ошибки: - 0 - нет ошибок; - 11003: происшествие с заданным ID не найдено; - 1406: ошибка при чтении инцидента; - 1407: ошибка изменения инцидента; - 12012: недопустимый формат ID.

Пример ответа:

```
{
```

```
  "results": [
    {
      "occurrence_id": "0cd06fe9-9a7c-45d2-89e5-201e0d1c84e1",
      "service_asset_finding_id": "0239abe3-4080-4ab7-a1c1-92de0194638b",
      "error_code": 0
    }
  ]
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request Empty occurrence_id	Неверный тип параметра запроса, либо отсутствует обязательный параметр Не заданы ID происшествий
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.1.15 Создание/обновление инцидентов из уязвимостей

Запрос:

Тип	Метод
POST	/service_asset_findings/bulk_create_with_vulnerabilities

Описание:

При выполнении запроса будет создан/обновлен инцидент на основе обнаруженной уязвимости по следующей логике:

- Из уязвимости извлекаются данные актива.
- Выполняется поиск по активу и типу инцидент:
  - если инцидент находится, то он будет обновлен;
  - иначе создается новый инцидент.
- Для этого инцидента создаётся происшествие (occurrence) с event_type: vulnerability.
- Если вместо идентификатора типа инцидента указано will_be_created, для данной уязвимости будет создан новый тип инцидента.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/service_asset_findings/bulk_create_with_vulnerabilities`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
vulnerability_finding_ids	object>	Required	Словарь, содержащий ID уязвимостей и ID типов инцидентов:
user_id	string	Required	Идентификатор пользователя, присваивается в updated_by инцидентов и новых типов инцидентов. Также определяет значение поля customer_created новых инцидентов: - если администратор: false; - иначе true.

Пример тела запроса:

```
{
  "vulnerability_finding_ids": {
    "96a0b522-1327-4b33-9b26-e1d75f6a6774": "4552a850-9a2f-4840-9d8a-0960aee9232c",
    "a91736d0-a536-4440-b651-6e18ce6bbd45": "5b545017-ade0-4fa1-a36b-98ede079df0f"
  },
  "user_id": "128064b6-c95a-45b5-a0ee-94360df67274"
}
```

Успешный ответ:

Статус код: 200 – успешное создание/обновление инцидентов и типов.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
_	Array<ServiceAssetFinding>	Список созданных/обновленных инцидентов

Пример ответа:


```
{
  "_": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "analysis_output": "string",
      "synopsis": "string",
      "title": "string",
      "risk": "none",
      "acknowledged_at": "2023-12-20T00:00:01.652259Z",
      "alert_type": "automatic",
      "client_note": "string",
      "internal_note": "string",
      "external": false,
      "immediate_action_score": 0,
      "throughput_period": "grace",
      "throughput_period_change": "2023-12-20T00:00:01.652259Z",
      "customer_created": false,
      "c_visible_since": "2023-12-20T00:00:01.652259Z",
      "c_visible_since_in_days": 0,
      "c_reopened_count": 0,
      "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "logmule_identifier": "string",
      "c_remote_exploitable": true,
      "c_occurrence_count": 0,
      "c_customer_retention_time": 0,
      "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "itsm_sync_status": "scheduled",
      "external_id": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
      "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
      "reopened_at": "2023-12-20T00:00:01.652259Z",
      "display_id": 0,
      "service_asset_name": "string",
```

```
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
},
"finding": {},
"last_occurrence_entity": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
  "end_occurrence": "2023-12-20T00:00:01.652259Z",
```

```
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "fqdn": "string",
        "incident_identifier": "string",
        "fincert_sync_status": 10,
        "fincert_id": "",
        "sopka_sync_status": 10,
        "sopka_id": "",
        "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
        "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
      },
      "user": {},
      "group": {},
      "incident_group": {
        "title": "string",
        "description": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
      },
      "occurrences": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "trace_id": "uuid",
          "event_type": "manual_source",
          "ip": "string",
          "mac": "string",
          "port": 0,
          "start_occurrence": "2023-12-20T00:00:01.652259Z",
          "end_occurrence": "2023-12-20T00:00:01.652259Z",
          "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "fqdn": "string",
          "incident_identifier": "string",
          "fincert_sync_status": 10,
          "fincert_id": "",
          "sopka_sync_status": 10,
          "sopka_id": "",
          "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
          "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
        }
      ],
      "custom_field_values": [
        {
          "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "string_value": "string",
          "integer_value": 0,
          "float_value": 0,
          "date_value": "2023-12-20T00:00:01.652259Z",
          "json_value": {},
          "boolean_value": true
        }
      ],
      "comments": [
        {}
      ],
      "documents": [
        {}
      ],
      "messages": [
```

```
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "trace_id": "uuid",
          "subject": "string",
          "body": "string",
          "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
          "automated": true,
          "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
          "itsm_sync_status": "not_synced",
          "itsm_last_synced_at": "string",
          "itsm_sync_error": "string",
          "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
        }
      ],
      "service_asset_finding_status_changes": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "trace_id": "uuid",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "status": "string",
          "revisit_at": "string",
          "itsm_sync_status": "not_synced",
          "itsm_last_synced_at": "string",
          "itsm_sync_error": "string",
          "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
        }
      ],
      "service_asset_groups": [
        {
          "title": "string",
          "description": "string",
          "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
          "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
        }
      ],
      "_relations": {
        "occurrences": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "custom_field_values": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "comments": [
          "string"
        ],
        "documents": [
          "string"
        ],
        "messages": [
          "string"
        ],
        "service_asset_finding_status_changes": [
          "string"
        ],
        "service_asset_groups": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
```

```
      }
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	1.Bad Request 2. empty vulnerability_finding_ids 3. empty vulnerability ID should be uuid format 4. vulnerability ID is empty 5. finding ID should be uuid format or will_be_created 6. finding ID is empty	1. Неверный тип параметра запроса, либо отсутствует обязательный параметр 2. Не заданы ID уязвимостей и типов инцидентов 3. Недопустимый формат ID уязвимости 4. ID уязвимости не может быть пустой строкой 5. Недопустимое значение ID типа инцидента, должен быть uuid или will_be_created 6. ID типа инцидента не может быть пустой строкой
404	Not Found	Редактируемый объект не найден в БД
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.16 Массовое изменение статуса инцидентов

Запрос:

Тип	Метод
POST	/service_asset_finding/mass_change_status

Описание:

При выполнении запроса будет обновлен статус инцидента.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_finding/mass_change_status
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Массив идентификаторов инцидентов
status	string	Optional	Новый статус инцидентов

Пример тела запроса:

```
{
  "ids": [
    "7bc42fd2-057c-4117-b367-8528bec75c80",
    "8baf5d9f-7ca8-45cf-956a-14aa2f5833f2"
  ],
  "status": "string"
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Массив результатов обновления статуса
results**{id}**	string	Идентификатор инцидента
results**{error_code}**	integer	Код ошибки: - 0 - нет ошибок; - 11003 - объект с заданным ID не найдено; - 11001 - при работе с БД возникла ошибка нарушения целостности, - 11002 - прочие ошибки БД.

Пример ответа:

```
{
  "results": [
    {
      "id": "7bc42fd2-057c-4117-b367-8528bec75c80",
      "error_code": 0
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	ids are empty status is empty Bad Request	Массив ID инцидентов не задан Статус не задан Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.17 Массовое изменение пользователя инцидентов

Запрос:

Тип	Метод
POST	/service_asset_finding/mass_assign_to_user

Описание:

При выполнении запроса будет изменен пользователь, ответственный за обработку инцидента (поле user_id).

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_finding/mass_assign_to_user
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Массив идентификаторов инцидентов
user_id	string	Optional	Идентификатор нового пользователя. Если новое значение user_id не задано, присвоит ""

Пример тела запроса:

```
{
  "ids": [
    "7bc42fd2-057c-4117-b367-8528bec75c80",
    "8baf5d9f-7ca8-45cf-956a-14aa2f5833f2"
  ],
  "user_id": "a147c6cf-4980-457c-8f46-2835e76cf2eb"
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Массив результатов обновления пользователей
results**{id}**	string	Идентификатор инцидента
results**{error_code}**	integer	Код ошибки: - 0 - нет ошибок; - 11003 - объект с заданным ID не найдено; - 11002 - прочие ошибки БД.

Пример ответа:

```
{
  "results": [
    {
      "id": "7bc42fd2-057c-4117-b367-8528bec75c80",
      "error_code": 0
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Пользователь не найден в БД
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 404:


```
{
  "error": "Not Found",
  "error_code": 404
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.1.18 Массовое изменение группы пользователей инцидентов

Запрос:

Тип	Метод
POST	/service_asset_finding/mass_assign_to_group

Описание:

При выполнении запроса будет изменена группа пользователей, ответственный за обработку инцидента (поле group_id).

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_finding/mass_assign_to_group
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов
group_id	string	Optional	Идентификатор новой группы пользователей

Пример тела запроса:

```
{
  "ids": [
    "7bc42fd2-057c-4117-b367-8528bec75c80",
    "8baf5d9f-7ca8-45cf-956a-14aa2f5833f2"
  ],
  "group_id": "bc9e0ada-07bb-4fa0-a8b1-0e972ca8fd3f"
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Массив результатов обновления группы пользователей
results{id}	string	Идентификатор происшествия
results{error_code}	integer	Код ошибки: - 0 - нет ошибок; - 11003 - объект с заданным ID не найдено; - 11002 - прочие ошибки БД.

Пример ответа:


```
{
  "results": [
    {
      "id": "7bc42fd2-057c-4117-b367-8528bec75c80",
      "error_code": 0
    }
  ]
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Группа не найдена в БД
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2 Типы инцидентов

2.2.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	findings
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	Ресурс findings отвечает за управление типами инцидентов. Типы инцидентов содержат сведения об угрозах, на основе которых создаются инциденты. В платформе каждый инцидент всегда принадлежит к определенному типу инцидента.

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/findings/create	Создание типа инцидента
PUT	/findings/update	Обновление информации о типе инцидента
POST	/findings/search	Поиск типов инцидентов
GET	/findings/{id}	Получение типа инцидента по ID
DELETE	/findings/{id}	Удаление типа инцидента
POST	/findings/group	Группировка типов инцидентов
POST	/findings/mass_delete	Массовое удаление типов инцидентов
DELETE	/findings/all	Удаление всех типов инцидентов
GET	/findings/_meta	Получение свойств типов инцидентов и действий пользователей

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
409	Попытка присвоить объекту существующее уникальное значение атрибута
422	Другие ошибки удаления
500	Ошибка сервера

Модели объектов:

Название	Описание
Finding	Модель данных ресурса findings

2.2.2 Модель ресурса «Типы инцидентов»

Модель данных Finding:

Параметр	Тип данных	Обязательность	Описание
title	string	Required	Наименование типа инцидента
description	string	Required	Общее описание типа инцидента
risk_impact	string	Required	Описание влияния инцидента на уровень риска
solution	string	Required	Рекомендации по устранению инцидента
display_id	number	Required	Идентификатор отображения инцидента, автоматически инкрементируется при добавлении новых
mitigation	string	Required	Описание профилактики данного типа инцидента

Параметр	Тип данных	Обязательность	Описание
synopsis	string	Required	Краткое описание сути инцидентов данного типа
local	boolean	Required	Флаг локальности типа инцидента
type	string	Required	Типов уязвимости, к которому принадлежит тип инцидента. Допустимые значения: network_anomaly: сетевая аномалия - актив проявляет сетевую активность, которую проявлять не должен; policy_violation: нарушение политики - это наступление условий, нарушающих политику безопасности эксплуатации актива (задуманную службой безопасности); vulnerability: уязвимость - у злоумышленника есть возможность получить контроль (полный или частичный) над активом.
identifier	object	Optional	Объект, хранящий связанные идентификаторы уязвимостей сторонних сканеров
comment	string	Optional	Комментарий пользователя
fallback_raw_risklevel	number	Required	Цифровое обозначение уровня риска. Допустимые значения от 0 до 10.
new_version	boolean	Required	Допустимые значения: true, false. Значение по умолчанию: true.
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутренние заметки
cpes	Array<string>		
category_id	string uuid	Required	Идентификатор категории типов инцидентов в формате uuid
customer_created	boolean	Required	Флаг характеризующий тип инцидента как созданный клиентом
software_compliance	boolean	Required	Флаг соответствия программного обеспечения
itsm_last_synced_at	string time	Required	Время последнего изменения статуса в системе
updated_by	string uuid	Required	Идентификатор пользователя обновившего информацию о типе инцидента в формате uuid
created_by_customer	string uuid	Required	Идентификатор пользователя создавшего тип инцидента в формате uuid
edited_by	string uuid	Required	Идентификатор пользователя (в формате uuid) изменившего тип инцидента
is_system	boolean	Required	Флаг помечающий тип инцидента как системный (приходит вместе с эксперт паком)
category	object	Required	Категория типа инцидента
service_asset_findings	Array<ServiceAssetFindingNoRelations>	Required	Связанные инциденты

Параметр	Тип данных	Обязательность	Описание
rules	Array<Rule>	Required	Связанные правила
messages	Array<Message>	Optional	Сообщения, связанные с типом инцидента
id	string uuid	Required	Идентификатор
created_at	string time	Required	Дата создания в формате: date-time
updated_at	string time	Required	Дата изменения в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
_relations	object<relations>	Optional	Словарь, описывающий связанные модели через идентификаторы

Модель данных ServiceAssetFindingNoRelations:

Параметр	Тип данных	Обязательность	Описание
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа

Параметр	Тип данных	Обязательность	Описание
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace; - delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему

Параметр	Тип данных	Обязательность	Описание
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов

Модель данных Rule:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор правила
created_at	string time	Required	Дата создания правила в формате: date-time
updated_at	string time	Required	Дата изменения правила в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название правила
frontend_data	Array<FrontendData>	Optional	Данные визуального конструктора правила

Параметр	Тип данных	Обязательность	Описание
test_data	Array<object>	Optional	Список событий для тестирования правила (логлайны)
settings	Array<SettingRule>	Required	Список настроек правила
active	boolean	Required	Флаг активности правила
reload	boolean	Required	Флаг перезагрузки правила после обновления
finding_id	string	Required	Идентификатор инцидента
description	string	Required	Описание правила
lua	string	Required	Код правила в формате Lua
is_retro	boolean	Required	Флаг: используется ли правило для ретроспективной корреляции
is_system	boolean	Required	Флаг: системное ли правило
stats	object	Optional	Статистика сработок и ошибок правила
stats{result_count}	integer	Optional	Количество срабатываний правила
stats{error_count}	integer	Optional	Количество ошибок правила
is_error	integer	Required	Количество ошибок
running_at	string time	Required	Дата и время запуска в формате date-time
logmule_go_filters	Array<LogmuleGoFilters>	Required	Фильтры потока событий
logmule_go_modules	Array<LogmuleGoModules>	Required	Макросы
finding	Array<RuleFinding>	Required	Связанный тип инцидента
logmule_go_results	Array<LogmuleGoResults>	Required	Результат сработки правила корреляции
rule_sets	Array<RuleSets>	Optional	Набор правил
service_asset_findings	Array<ServiceAssetFinding>	Optional	Список инцидентов («Модель ресурса «Инциденты»»)
value_storesë	Array<ValueStores>	Optional	Табличные списки

Модель данных Rule_Array<FrontendData>:

Параметр	Тип данных	Обязательность	Описание
alert	Object<Alert>	Required	Щаблон алерта
grouper	Object<Grouper>	Required	Шаблон группера
actions	Array<Actions>	Required	Действия, по результатам сработки правила
conditions	Array<Conditions>	Required	Конструктор условий. Объекты в массиве могут отличаться в зависимости от типа условия: 1. Сравнение (“CompareCondition”). Структура меняется в зависимости от источника данных. - LoglineGetExpression - значение из события; - TableGetExpression, TableCountExpression или TableDefinitionExpression - значение из табличного списка; - ConstExpression - ручной ввод значения 2. Логическое выражение (“LogicalCondition”)
version	integer	Required	Версия схемы конструктора правил

Модель данных Rule_Array<FrontendData>_Object<Alert>:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	ID шаблона алерта
trace_id	string	Optional	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название шаблона алерта
create_incident	boolean	Required	Флаг: создавать ли инцидент в результате сработки правила
assign_to_customer	boolean	Required	Флаг: назначить ли инцидент пользователю
risk_level	number	Required	Уровень риска. Допустимые значения от 0 до 10.
asset_ip	string	Required	IP-адрес актива
asset_hostname	string	Required	Hostname актива
asset_fqdn	string	Required	FQDN актива
asset_mac	string	Required	MAC-адрес актива
first_and_last_logs	boolean	Required	Флаг: записывать ли в журнал первое и последнее событие
trim_logs	integer	Required	Количество событий для записи в журнал
template	string	Required	Описание шаблона

Модель данных Rule_Array<FrontendData>_Object<Grouper>:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	ID шаблона группера
trace_id	string	Optional	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название шаблона группера
grouped_by	Array<string>	Required	Поля для группировки
aggregated_by	Array<string>	Required	Поля для агрегации
grouped_time_field	string	Required	Время события (название поля)
grouped_time_type	string	Required	Формат времени, одно из: “RFC3339Nano”, “RFC3339”, “ANSIC”, “UnixDate”, “RubyDate”, “RFC822”, “RFC822Z”, “RFC850”, “RFC850”, “RFC1123”, “RFC1123Z”, “Stamp”, “StampMilli”, “StampMicro”, “StampNano”, “UnixMilli”, “UnixMicro”
detection_windows	integer	Required	Период группировки
detection_windows_unit	string	Required	Единица измерения периода группировки. Допустимые значения: - ms - s - m - h
aggregate_count	integer	Required	Порог количества событий для срабатывания
aggregate_unique	boolean	Required	Флаг: активировать ли только уникальные события.

Модель данных Rule_Array<FrontendData>_Array<Actions>:

Параметр	Тип данных	Обязательность	Описание
TTL	string	Optional	Время жизни события (логлайна) в минутах
key	object	Optional	Ключ для действия
key**{default}**	object	Required	Объект ключа по умолчанию
key{default}**/type**	string	Optional	Тип ключа. Допустимые значения: - ”type” == “value” - Значение - ”type” == “field” - Поле события

Параметр	Тип данных	Обязательность	Описание
key{default}/**value**	string	Optional	Значение ключа
type	string	Optional	Тип действия. Допустимые значения: - ”type” == “store-set” - Установка значения в табличном списке; - ”type” == “store-remove” - Удаление записи в табличном списке; - ”type” == “store-truncate” - Очистка табличного списка.
store	string	Optional	Табличный список, над которым совершается действие
value	string	Optional	Значение
column	string	Optional	Колонка

Модель данных Rule_Array<FrontendData>_Array<Conditions>:

Любой из:

- Сравнение;
- Логическое выражение.

Сравнение:

Параметр	Тип данных	Обязательность	Описание
type	string	Required	Тип условия
id	string	Required	Идентификатор условия
parentId	string	Optional	Идентификатор родительского условия
negation	boolean	Required	Флаг: включить ли для функции сравнения отрицание
compareFn	string	Optional	Функция сравнения. Допустимые значения:eq, streq, exist, in, substr, search, gt, gte, lt, lte, in_sub, in_pref, in_suf, pref, suf, table_search, table_check_ip, between
expressions	Array<Expressions>	Required	Выражение. Массив может содержать разную структуру объекта, в зависимости от источника данных: - LoglineGetExpression - значение из события - TableGetExpression, TableCountExpression или TableDefinitionExpression - значение из табличного списка - ConstExpression - ручной ввод значения

Сравнение_Array<Expressions>:

Один из:

- LoglineGetExpression
- TableGetExpression
- TableCountExpression
- TableDefinitionExpression
- ConstExpression

LoglineGetExpression:

Параметр	Тип данных	Обязательность	Описание
type	string	Required	Тип выражения
value	string	Required	Значение

TableGetExpression:

Параметр	Тип данных	Обязательность	Описание
type	string	Required	Тип выражения
store	string	Required	Источник данных (табличный список)
column	string	Required	Колонка
key	object	Required	Ключ
key**{type}**	string	Required	Тип ключа. Допустимые значения: logline-get, const-string
key**{value}**	string	Required	Значение ключа

TableCountExpression:

Параметр	Тип данных	Обязательность	Описание
type	string	Required	Тип выражения
store	string	Required	Источник данных (табличный список)

TableDefinitionExpression:

Параметр	Тип данных	Обязательность	Описание
type	string	Required	Тип выражения
store	string	Required	Источник данных (табличный список)
column	string	Required	Колонка

ConstExpression:

Параметр	Тип данных	Обязательность	Описание
type	string	Required	Тип выражения. Допустимые значения:const-string, const-integer, const-double, const-boolean, const-ip, const-cidr, const-date, const-null, const-string-array
value	string	Required	Значение. Параметр “value” принимает значения разных типов, в зависимости от значения “type”: - “type” == “const-string” => “value” == “string" - "type” == “const-integer” => “value” == “string" - "type” == “const-double” => “value” == “string" - "type” == “const-boolean” => “value” == “boolean" - "type” == “const-ip” => “value” == “string" - "type” == “const-cidr” => “value” == “string" - "type” == “const-date” => “value” == “string" - "type” == “const-null” => “value” == “null" - "type” == “const-string-array” => “value” == “array of strings”

Логическое выражение:

Параметр	Тип данных	Обязательность	Описание
type	string	Required	Тип условия
id	string	Required	Идентификатор условия
parentId	string	Optional	Идентификатор родительского условия
negation	boolean	Required	Флаг: включить ли для функции сравнения отрицание
operator	string	Required	Оператор. Допустимые значения: and, or

Модель данных Rule_Array<SettingRule>:

Параметр	Тип данных	Обязательность	Описание
function_metrics	boolean	Optional	Флаг: собирать ли дополнительные метрики
is_constructor	boolean	Optional	Флаг: создано ли правило с помощью визуального конструктора
max_alerts	integer	Optional	Максимальное количество сработок
max_alerts_per_second	integer	Optional	Максимальное количество сработок в секунду
max_rule_memory_mb	integer	Optional	Ограничение памяти (Мб)

Модель данных Rule_Array<LogmuleGoFilters>:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор фильтра
created_at	string time	Required	Дата создания в формате uuid
updated_at	string time	Required	Дата изменения в формате uuid
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название фильтра
config	Array<Config>	Required	Список фильтров по полям
logmule_go_rules	Array<object>	Optional	Список правил, использующих данный фильтр
stat	Array<Stats>	Optional	Статистика потока по данному фильтру
_relations	object	Optional	Словарь, описывающий связанные модели через идентификаторы
_relations{logmule_go_rules}	Array<string>	Optional	Список идентификаторов связанных правил
id	string	Required	Идентификатор фильтра
created_at	string time	Required	Дата создания в формате uuid
updated_at	string time	Required	Дата изменения в формате uuid
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита

Параметр	Тип данных	Обязательность	Описание
name	string	Required	Название фильтра
config	Array<Config>	Required	Список фильтров по полям
logmule_go_rules	Array<object>	Optional	Список правил, использующих данный фильтр

Модель данных Rule_Array<LogmuleGoFilters>_Array<Config>:

Параметр	Тип данных	Обязательность	Описание
compareFn	string	Required	Функция сравнения. Допустимые значения:equal, substr, exist, intersection
expressions	object	Required	Выражения использующиеся в функции сравнения. >= 1 знаков
expressions**{type}**	string	Required	Тип выражения. Допустимые значения: logline-get, const-string, const-null, const-string-array
expressions**{value}**	object	Required	Значение
type	string	Required	Тип условия. Допустимые значения: compare-condition
parentId	string	Optional	Идентификатор родительского элемента
ignore_case	boolean	Optional	Флаг: игнорировать ли регистр при сравнении строковых данных
negation	boolean	Optional	Флаг: выполнять ли инверсию по результатам сравнения

Модель данных Rule_Array<LogmuleGoFilters>_Array<Stats>:

Параметр	Тип данных	Обязательность	Описание
hit_count	integer	Optional	
hit_eps	integer	Optional	
check_count	integer	Optional	
check_eps	integer	Optional	
check_time	integer	Optional	

Модель данных Rule_Array<LogmuleGoModules>:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор макроса
created_at	string time	Required	Дата создания макроса в формате: date-time
updated_at	string time	Required	Дата изменения макроса в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название макроса
content	string	Required	Код макроса
is_system	boolean	Required	Флаг: является ли макрос системным
logmule_go_rules	Array<object>	Optional	Список правил, использующих данный макрос
rules	Array<object>	Optional	Список объектов связанных правил (загружается всегда через GetByID или по запросу через GenericSearch)
_relations	object	Optional	Словарь, описывающий связанные модели через идентификаторы
_relations**{rules}**	Array<string>	Optional	Список идентификаторов связанных правил

Модель данных Rule_Array<RuleFinding>:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор сработки правила
created_at	string time	Required	Дата создания сработки в формате: date-time
updated_at	string time	Required	Дата изменения сработки в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита

Модель данных Rule_Array<LogmuleGoResults>:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор результата сработки парвила
created_at	string time	Required	Дата создания результата сработки в формате: date-time
updated_at	string time	Required	Дата изменения результата сработки в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
rule_id	string	Required	Идентификатор правила
analysis_output	string	Required	Результат анализа
event	object	Required	Событие строкой
compressed_event	string array	Required	Событие одной строкой в формате byte array
risklevel	number float	Required	Уровень риска в формате float
occurred_at	string time	Required	Дата и время происшествия в формате: date-time
occurrence_id	string	Required	Идентификатор происшествия
error	string	Required	Ошибка
service_asset_id	string	Required	Идентификатор актива
asset_info	object<asset>	Required	Данные актива
incident_identifier	string	Required	Идентификатор инцидента
metadata	string map	Required	Метаданные в формате map
logmule_go_rule	object	Required	Правило, по которому произошла сработка
occurrence	object	Required	Происшествие
service_asset	object	Required	Актив, на котором произошла сработка

Модель данных Rule_Array<LogmuleGoResults>_ object<asset>:

Параметр	Тип данных	Обязательность	Описание
ip	string	Required	IP-адрес актива
hostname	string	Required	Хостнейм актива
fqdn	string	Required	FQDN актива
mac	string	Required	MAC-адрес актива

Модель данных Rule_Array<RuleSets>:

Параметр	Тип данных	Обязательность	Описание
id	string uuid	Optional	Идентификатор набора правил
created_at	string time	Optional	Дата создания набора правил в формате: date-time
updated_at	string time	Optional	Дата изменения набора правил в формате: date-time
trace_id	string	Optional	Идентификатор трассировки действия пользователя для аудита
name	string	Optional	Название набора правил
create_service_asset_findings	boolean	Optional	Флаг: создавать ли инцидент по результатам сработки набора правил
rule	object	Optional	Правила входящие в набор
service_asset_groups	object	Optional	Связанные группы активов

Модель данных Rule_Array<ValueStores>:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор хранилища (RVS, табличный список)
created_at	string time	Required	Дата создания табличного списка в формате: date-time
updated_at	string time	Required	Дата изменения табличного списка в формате: date-time

Параметр	Тип данных	Обязатель ность	Описание
name	string	Required	Название табличного списка
description	string	Required	Описание табличного списка
values_scheme	string	Required	Схема значений хранилища (Json как строка)
is_large	boolean	Required	Флаг: используется ли хранилище под большой объем данных
mask_values	boolean	Required	Флаг маскировать ли значения в пользовательском интерфейсе (значения не будут показываться пользователю)
type	string	Required	Тип БД хранилища (на данный момент поддерживается только postgresql - “pg”)
version	integer	Required	Версия хранилища (автоматически увеличивается при изменениях в БД)
source	string	Required	Имя сервера БД, путь к файлу или папке (Не используется. По умолчанию - пустое)
scheme	string	Required	Схема БД
db_name	string	Required	Имя БД
user	string	Required	Имя пользователя БД (Не используется. По умолчанию - пустое)
password	string	Required	Пароль пользователя БД (Не используется. По умолчанию - пустое)
store_count	integer	Required	Количество записей в хранилище
content	object	Required	Контент. По умолчанию - null.
tollerId	string	Optional	Идентификатор трассировки

Модель данных Message:

Параметр	Тип данных	Обязатель ность	Описание
id	string	Required	Идентификатор сообщения пользователя
created_at	string	Required	Дата создания в формате `date-time`
updated_at	string	Required	Дата изменения в формате `date-time`
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
subject	string	Optional	Тема (Предмет) сообщения

Параметр	Тип данных	Обязательность	Описание
body	string	Optional	Тело сообщения
service_asset_id	string	Optional	Идентификатор связанного актива
service_asset_finding_id	string	Optional	Идентификатор связанного инцидента
service_asset_finding_status_change_id	string	Optional	Идентификатор связанного изменения статуса инцидента
automated	boolean	Optional	Флаг автоматического создания
finding_id	string	Optional	Идентификатор связанного типа инцидента
itsm_sync_status	string	Optional	Статус синхронизации с внешними системами. Допустимые значения: - not_synced - scheduled - aborted - synced - waiting_confirmation
itsm_last_synced_at	string	Optional	Время синхронизации с внешними системами
itsm_sync_error	string	Optional	Описание ошибки синхронизации
sender_id	string	Optional	Идентификатор пользователя, инициировавшего синхронизацию

Модель данных Relations:

Параметр	Тип данных	Обязательность	Описание
service_asset_findings	Array<string>		Массив идентификаторов инцидентов, связанных с типом инцидента
rules	Array<string>		Массив идентификаторов правил, связанных с типом инцидента
messages	Array<string>		Массив идентификаторов сообщений, связанных с типом инцидента

2.2.3 Создание типа инцидента

Запрос:

Тип	Метод
POST	/findings/create

Описание:

При выполнении запроса будет создан тип инцидента с заданными параметрами.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/findings/create`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
title	string	Required	Наименование типа инцидента
description	string	Required	Общее описание типа инцидента
risk_impact	string	Required	Описание влияния инцидента на уровень риска
solution	string	Required	Рекомендации по устранению инцидента
display_id	number	Required	Идентификатор отображения инцидента, автоматически инкрементируется при добавлении новых
mitigation	string	Required	Описание профилактики данного типа инцидента
synopsis	string	Required	Краткое описание сути инцидентов данного типа
local	boolean	Required	Флаг локальности типа инцидента
type	string	Required	Типов уязвимости, к которому принадлежит тип инцидента. Допустимые значения: network_anomaly: сетевая аномалия - актив проявляет сетевую активность, которую проявлять не должен; policy_violation: нарушение политики - это наступление условий, нарушающих политику безопасности эксплуатации актива (задуманную службой безопасности); vulnerability: уязвимость - у злоумышленника есть возможность получить контроль (полный или частичный) над активом.
identifier	object	Optional	Объект, хранящий связанные идентификаторы уязвимостей сторонних сканеров
comment	string	Optional	Комментарий пользователя
fallback_raw_risklevel	number	Required	Цифровое обозначение уровня риска. Допустимые значения от 0 до 10.
new_version	boolean	Required	Допустимые значения: true, false. Значение по умолчанию: true.

Параметр	Тип данных	Обязательность	Описание
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутренние заметки
cpes	Array<string>		
category_id	string uuid	Required	Идентификатор категории типов инцидентов в формате uuid
customer_created	boolean	Required	Флаг характеризующий тип инцидента как созданный клиентом
software_compliance	boolean	Required	Флаг соответствия программного обеспечения
itsm_last_synced_at	string time	Required	Время последнего изменения статуса в системе
updated_by	string uuid	Required	Идентификатор пользователя обновившего информацию о типе инцидента в формате uuid
created_by_customer	string uuid	Required	Идентификатор пользователя создавшего тип инцидента в формате uuid
edited_by	string uuid	Required	Идентификатор пользователя (в формате uuid) изменившего тип инцидента
is_system	boolean	Required	Флаг помечающий тип инцидента как системный (приходит вместе с эксперт паком)

Пример тела запроса:


```
{
  "title": "string",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "display_id": 0,
  "mitigation": "string",
  "synopsis": "string",
  "local": true,
  "type": "network_anomaly",
  "identifier": {},
  "comment": "string",
  "fallback_raw_risklevel": 10,
  "new_version": true,
  "client_note": "string",
  "internal_note": "string",
  "cpes": [
    "string"
  ],
  "category_id": "8de4c9fd-61a4-4c0b-bf88-0ed3a0fe3fa2",
  "customer_created": true,
  "software_compliance": true,
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
```

```
  "is_system": true
}
```


Успешный ответ:

Статус код: 201 – успешное создание типа инцидента.

Формат: JSON.

Тело ответа: «Модель ресурса «Типы инцидентов»».

Пример ответа:


```
{
  "title": "string",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "display_id": 0,
  "mitigation": "string",
  "synopsis": "string",
  "local": true,
  "type": "network_anomaly",
  "identifier": {},
  "comment": "string",
  "fallback_raw_risklevel": 10,
  "new_version": true,
  "client_note": "string",
  "internal_note": "string",
  "cpes": [
    "string"
  ],
  "category_id": "8de4c9fd-61a4-4c0b-bf88-0ed3a0fe3fa2",
  "customer_created": true,
  "software_compliance": true,
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "is_system": true,
  "category": {},
  "service_asset_findings": [
    {
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "analysis_output": "string",
      "synopsis": "string",
      "title": "string",
      "risk": "none",
      "acknowledged_at": "2023-12-20T00:00:01.652259Z",
      "alert_type": "automatic",
```

```
      "client_note": "string",
      "internal_note": "string",
      "external": false,
      "immediate_action_score": 0,
      "throughput_period": "grace",
      "throughput_period_change": "2023-12-20T00:00:01.652259Z",
      "customer_created": false,
      "c_visible_since": "2023-12-20T00:00:01.652259Z",
      "c_visible_since_in_days": 0,
      "c_reopened_count": 0,
      "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "logmule_identifier": "string",
      "c_remote_exploitable": true,
      "c_occurrence_count": 0,
      "c_customer_retention_time": 0,
      "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "itsm_sync_status": "scheduled",
      "external_id": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
      "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
      "reopened_at": "2023-12-20T00:00:01.652259Z",
      "display_id": 0
    }
  ],
  "rules": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "frontend_data": {
        "alert": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "create_incident": true,
          "assign_to_customer": true,
          "risk_level": 5.35,
          "asset_ip": "string",
          "asset_hostname": "string",
          "asset_fqdn": "string",
          "asset_mac": "string",
          "first_and_last_logs": false,
          "trim_logs": 1,
          "template": "string",
          "mitre": ""
        },
        "grouper": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "grouped_by": [
            "string"
          ],
          "aggregated_by": [
            "string"
          ],
```

```
    "grouped_time_field": "string",
    "grouped_time_type": "2023-12-20T00:00:01.652259Z",
    "detection_windows": 5,
    "detection_windows_unit": "ms",
    "aggregate_count": 1,
    "aggregate_unique": true
  },
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
  "max_rule_memory_mb": 1
},
"active": true,
"reload": true,
"finding_id": "uuid",
"description": "string",
"lua": "string",
"is_retro": false,
"is_system": true,
"stats": {
  "result_count": 1,
  "error_count": 0
},
"is_error": 0,
"running_at": "2023-12-20T00:00:01.652259Z",
"logmule_go_filters": [
  {
```

```
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "name": "string",
      "config": [
        {
          "compareFn": "equal",
          "expressions": [
            {
              "type": "logline-get",
              "value": {}
            }
          ],
          "type": "compare-condition",
          "parentId": "string",
          "ignore_case": true,
          "negation": true
        }
      ],
      "logmule_go_rules": null,
      "stats": {
        "hit_count": 0,
        "hit_eps": 0,
        "check_count": 0,
        "check_eps": 0,
        "check_time": 0
      },
      "_relations": {
        "logmule_go_rules": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "logmule_go_modules": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "content": "string",
      "is_system": true,
      "logmule_go_rules": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "name": "string",
          "frontend_data": {
            "alert": {
              "id": "uuid",
              "trace_id": "uuid",
              "name": "string",
              "create_incident": true,
              "assign_to_customer": true,
              "risk_level": 5.35,
              "asset_ip": "string",
              "asset_hostname": "string",
              "asset_fqdn": "string",
              "asset_mac": "string",
              "first_and_last_logs": false,
              "trim_logs": 1,
              "template": "string",
              "mitre": ""
            },
            "grouper": {
```

```
    "id": "uuid",
    "trace_id": "uuid",
    "name": "string",
    "grouped_by": [
      "string"
    ],
    "aggregated_by": [
      "string"
    ],
    "grouped_time_field": "string",
    "grouped_time_type": "2023-12-20T00:00:01.652259Z",
    "detection_windows": 5,
    "detection_windows_unit": "ms",
    "aggregate_count": 1,
    "aggregate_unique": true
  },
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
  "max_rule_memory_mb": 1
},
"active": true,
"reload": true,
"finding_id": "uuid",
"description": "string",
"lua": "string",
"is_retro": false,
```

```
        "is_system": true,
        "stats": {
          "result_count": 1,
          "error_count": 0
        },
        "is_error": 0,
        "running_at": "2023-12-20T00:00:01.652259Z"
      }
    ],
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"finding": {
  "id": "uuid",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid"
},
"logmule_go_results": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "rule_id": "uuid",
    "analysis_output": "string",
    "event": {},
    "compressed_event": "string",
    "risklevel": 5.35,
    "occurred_at": "2023-12-20T00:00:01.652259Z",
    "occurrence_id": "uuid",
    "error": "string",
    "service_asset_id": "uuid",
    "asset_info": {
      "ip": "string",
      "hostname": "string",
      "fqdn": "string",
      "mac": "string"
    },
    "incident_identifier": "string",
    "metadata": "{\"key\": \"value\"}",
    "logmule_go_rule": null,
    "occurrence": null,
    "service_asset": null,
    "service_asset_groups": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "network_ranges": [],
        "domain": "string",
        "itsm_synced": false,
        "regex": "string",
        "subject_id": "string",
        "object_id": "string",
        "is_kii": false,
        "is_fincert": false,
        "responsible_person": "string",
        "technical_specialist": "string",
        "system_id": "string",
```

```
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      }
    ],
    "_relations": {}
  }
],
"rule_sets": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "Набор 1",
    "create_service_asset_findings": false,
    "rule": null,
    "service_asset_groups": null
  }
],
"service_asset_findings": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
```

```
"reopened_at": "2023-12-20T00:00:01.652259Z",
"display_id": 0,
"service_asset_name": "string",
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
},
"finding": {},
"last_occurrence_entity": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
```

```
            "start_occurrence": "2023-12-20T00:00:01.652259Z",
            "end_occurrence": "2023-12-20T00:00:01.652259Z",
            "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
            "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
            "fqdn": "string",
            "incident_identifier": "string",
            "fincert_sync_status": 10,
            "fincert_id": "",
            "sopka_sync_status": 10,
            "sopka_id": "",
            "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
            "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
          },
          "user": {},
          "group": {},
          "incident_group": {
            "title": "string",
            "description": "string",
            "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
            "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
          },
          "occurrences": [
            {
              "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
              "created_at": "2023-12-20T00:00:01.652259Z",
              "updated_at": "2023-12-20T00:00:01.652259Z",
              "event_type": "manual_source",
              "ip": "string",
              "mac": "string",
              "port": 0,
              "start_occurrence": "2023-12-20T00:00:01.652259Z",
              "end_occurrence": "2023-12-20T00:00:01.652259Z",
              "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "fqdn": "string",
              "incident_identifier": "string",
              "fincert_sync_status": 10,
              "fincert_id": "",
              "sopka_sync_status": 10,
              "sopka_id": "",
              "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
              "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
            }
          ],
          "custom_field_values": [
            {
              "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "string_value": "string",
              "integer_value": 0,
              "float_value": 0,
              "date_value": "2023-12-20T00:00:01.652259Z",
              "json_value": {},
              "boolean_value": true
            }
          ],
          "comments": [
            {}
          ],
          "documents": [
            {}
          ],
```

```
          "messages": [
            {
              "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
              "created_at": "2023-12-20T00:00:01.652259Z",
              "updated_at": "2023-12-20T00:00:01.652259Z",
              "subject": "string",
              "body": "string",
              "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
              "automated": true,
              "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
              "itsm_sync_status": "not_synced",
              "itsm_last_synced_at": "string",
              "itsm_sync_error": "string",
              "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
            }
          ],
          "service_asset_finding_status_changes": [
            {
              "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
              "created_at": "2023-12-20T00:00:01.652259Z",
              "updated_at": "2023-12-20T00:00:01.652259Z",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "status": "string",
              "revisit_at": "string",
              "itsm_sync_status": "not_synced",
              "itsm_last_synced_at": "string",
              "itsm_sync_error": "string",
              "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
            }
          ],
          "service_asset_groups": [
            {
              "title": "string",
              "description": "string",
              "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
              "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
            }
          ],
          "_relations": {
            "occurrences": [
              "497f6eca-6276-4993-bfeb-53cbbbba6f08"
            ],
            "custom_field_values": [
              "497f6eca-6276-4993-bfeb-53cbbbba6f08"
            ],
            "comments": [
              "string"
            ],
            "documents": [
              "string"
            ],
            "messages": [
              "string"
            ],
            "service_asset_finding_status_changes": [
              "string"
            ],
            "service_asset_groups": [
              "497f6eca-6276-4993-bfeb-53cbbbba6f08"
            ]
          }
```

```
  }
],
"value_stores": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "name": "uuid",
    "description": "string",
    "values_scheme": [
      {
        "name": "field",
        "type": "int",
        "is_key": false
      }
    ],
    "is_large": true,
    "mask_values": true,
    "type": "pg",
    "version": 1,
    "source": "",
    "scheme": "vstore",
    "db_name": "vs_111dfca1defc11faa11dc11f1d11fd11",
    "user": "",
    "password": "",
    "store_count": 10,
    "content": null,
    "tollerId": "string",
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    },
    "logmule_go_rules": {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "frontend_data": {
        "alert": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "create_incident": true,
          "assign_to_customer": true,
          "risk_level": 5.35,
          "asset_ip": "string",
          "asset_hostname": "string",
          "asset_fqdn": "string",
          "asset_mac": "string",
          "first_and_last_logs": false,
          "trim_logs": 1,
          "template": "string",
          "mitre": ""
        },
        "grouper": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "grouped_by": [
            "string"
          ],
          "aggregated_by": [
            "string"
          ],
          "grouped_time_field": "string",
```

```
        "grouped_time_type": "2023-12-20T00:00:01.652259Z",
        "detection_windows": 5,
        "detection_windows_unit": "ms",
        "aggregate_count": 1,
        "aggregate_unique": true
      },
      "actions": [
        {
          "TTL": "string",
          "key": {
            "_default": {
              "type": "value",
              "value": "string"
            }
          },
          "type": "store-set",
          "store": "string",
          "value": "string",
          "column": "string"
        }
      ],
      "conditions": [
        {
          "type": "compare-condition",
          "id": "uuid",
          "parentId": null,
          "negation": false,
          "compareFn": "eq",
          "expressions": [
            {
              "type": "logline-get",
              "value": "string"
            }
          ]
        }
      ],
      "version": 2
    },
    "test_data": [
      {}
    ],
    "settings": {
      "function_metrics": false,
      "is_constructor": false,
      "max_alerts": 1,
      "max_alerts_per_second": 1,
      "max_rule_memory_mb": 1
    },
    "active": true,
    "reload": true,
    "finding_id": "uuid",
    "description": "string",
    "lua": "string",
    "is_retro": false,
    "is_system": true,
    "stats": {
      "result_count": 1,
      "error_count": 0
    },
    "is_error": 0,
    "running_at": "2023-12-20T00:00:01.652259Z"
  }
 }
],
```

```
      "_relations": {
        "logmule_go_filters": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "logmule_go_modules": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "logmule_go_results": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "rule_sets": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "service_asset_findings": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "value_stores": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "messages": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "subject": "string",
      "body": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "automated": true,
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
    }
  ],
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "_relations": {
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rules": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при создании объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.4 Обновление типа инцидента

Запрос:

Тип	Метод
PUT	/findings/update

Описание:

При выполнении запроса будет обновлена информация о типе инцидента в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля модели, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в объекте _relations отсутствуют зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются;
- Зависимости игнорируются в теле запроса;
- Зависимости в ответе всегда null.

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "logmule_go_rules": [] // - очистит все связи с правилами
    // "logmule_go_rules": ["uuid1", "uuid2"] // - создаст связь с 2 правилами
    // "logmule_go_rules": ["uuid1"] // - оставит связь только с первым правилом
  }
}
```

Изменен в версии: 3.7.3

Пример запроса:

PUT

`http://127.0.0.1/cruddy/v2/findings/update`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
title	string	Required	Наименование типа инцидента
description	string	Required	Общее описание типа инцидента
risk_impact	string	Required	Описание влияния инцидента на уровень риска
solution	string	Required	Рекомендации по устранению инцидента
display_id	number	Required	Идентификатор отображения инцидента, автоматически инкрементируется при добавлении новых
mitigation	string	Required	Описание профилактики данного типа инцидента
synopsis	string	Required	Краткое описание сути инцидентов данного типа

Параметр	Тип данных	Обязательность	Описание
local	boolean	Required	Флаг локальности типа инцидента
type	string	Required	Типов уязвимости, к которому принадлежит тип инцидента. Допустимые значения: network_anomaly: сетевая аномалия - актив проявляет сетевую активность, которую проявлять не должен; policy_violation: нарушение политики - это наступление условий, нарушающих политику безопасности эксплуатации актива (задуманную службой безопасности); vulnerability: уязвимость - у злоумышленника есть возможность получить контроль (полный или частичный) над активом.
identifier	object	Optional	Объект, хранящий связанные идентификаторы уязвимостей сторонних сканеров
comment	string	Optional	Комментарий пользователя
fallback_raw_risklevel	number	Required	Цифровое обозначение уровня риска. Допустимые значения от 0 до 10.
new_version	boolean	Required	Допустимые значения: true, false. Значение по умолчанию: true.
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутренние заметки
cpes	Array<string>		
category_id	string uuid	Required	Идентификатор категории типов инцидентов в формате uuid
customer_created	boolean	Required	Флаг характеризующий тип инцидента как созданный клиентом
software_compliance	boolean	Required	Флаг соответствия программного обеспечения
itsm_last_synced_at	string time	Required	Время последнего изменения статуса в системе
updated_by	string uuid	Required	Идентификатор пользователя обновившего информацию о типе инцидента в формате uuid
created_by_customer	string uuid	Required	Идентификатор пользователя создавшего тип инцидента в формате uuid
edited_by	string uuid	Required	Идентификатор пользователя (в формате uuid) изменившего тип инцидента
is_system	boolean	Required	Флаг помечающий тип инцидента как системный (приходит вместе с эксперт паком)
id	string uuid	Required	Идентификатор
created_at	string time	Required	Дата создания в формате: date-time
updated_at	string time	Required	Дата изменения в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита

Параметр	Тип данных	Обязательность	Описание
_relations	object<relations>	Optional	Словарь, описывающий связанные модели через идентификаторы

Модель данных Relations:

Параметр	Тип данных	Обязательность	Описание
service_asset_findings	Array<string>		Массив идентификаторов инцидентов, связанных с типом инцидента
rules	Array<string>		Массив идентификаторов правил, связанных с типом инцидента
messages	Array<string>		Массив идентификаторов сообщений, связанных с типом инцидента

Пример тела запроса:


```
{
  "title": "string",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "display_id": 0,
  "mitigation": "string",
  "synopsis": "string",
  "local": true,
  "type": "network_anomaly",
  "identifier": {},
  "comment": "string",
  "fallback_raw_risklevel": 10,
  "new_version": true,
  "client_note": "string",
  "internal_note": "string",
  "cpes": [
    "string"
  ],
  "category_id": "8de4c9fd-61a4-4c0b-bf88-0ed3a0fe3fa2",
  "customer_created": true,
  "software_compliance": true,
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "is_system": true,
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "_relations": {
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rules": [
```

```
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Успешный ответ:

Статус код: 200 - успешное обновление информации о типе инцидента.

Формат: JSON.

Тело ответа: «Модель ресурса «Типы инцидентов»».

Пример ответа:


```
{
  "title": "string",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "display_id": 0,
  "mitigation": "string",
  "synopsis": "string",
  "local": true,
  "type": "network_anomaly",
  "identifier": {},
  "comment": "string",
  "fallback_raw_risklevel": 10,
  "new_version": true,
  "client_note": "string",
  "internal_note": "string",
  "cpes": [
    "string"
  ],
  "category_id": "8de4c9fd-61a4-4c0b-bf88-0ed3a0fe3fa2",
  "customer_created": true,
  "software_compliance": true,
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "is_system": true,
  "category": {},
  "service_asset_findings": [
    {
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
```

```
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  }
],
"rules": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "string",
    "frontend_data": {
      "alert": {
        "id": "uuid",
        "trace_id": "uuid",
        "name": "string",
        "create_incident": true,
        "assign_to_customer": true,
        "risk_level": 5.35,
        "asset_ip": "string",
        "asset_hostname": "string",
        "asset_fqdn": "string",
        "asset_mac": "string",
        "first_and_last_logs": false,
        "trim_logs": 1,
        "template": "string",
        "mitre": ""
      },
      "grouper": {
        "id": "uuid",
        "trace_id": "uuid",
        "name": "string",
```

```
      "grouped_by": [
        "string"
      ],
      "aggregated_by": [
        "string"
      ],
      "grouped_time_field": "string",
      "grouped_time_type": "2023-12-20T00:00:01.652259Z",
      "detection_windows": 5,
      "detection_windows_unit": "ms",
      "aggregate_count": 1,
      "aggregate_unique": true
    },
    "actions": [
      {
        "TTL": "string",
        "key": {
          "_default": {
            "type": "value",
            "value": "string"
          }
        },
        "type": "store-set",
        "store": "string",
        "value": "string",
        "column": "string"
      }
    ],
    "conditions": [
      {
        "type": "compare-condition",
        "id": "uuid",
        "parentId": null,
        "negation": false,
        "compareFn": "eq",
        "expressions": [
          {
            "type": "logline-get",
            "value": "string"
          }
        ]
      }
    ],
    "version": 2
  },
  "test_data": [
    {}
  ],
  "settings": {
    "function_metrics": false,
    "is_constructor": false,
    "max_alerts": 1,
    "max_alerts_per_second": 1,
    "max_rule_memory_mb": 1
  },
  "active": true,
  "reload": true,
  "finding_id": "uuid",
  "description": "string",
  "lua": "string",
  "is_retro": false,
  "is_system": true,
  "stats": {
    "result_count": 1,
```

```
    "error_count": 0
  },
  "is_error": 0,
  "running_at": "2023-12-20T00:00:01.652259Z",
  "logmule_go_filters": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "name": "string",
      "config": [
        {
          "compareFn": "equal",
          "expressions": [
            {
              "type": "logline-get",
              "value": {}
            }
          ],
          "type": "compare-condition",
          "parentId": "string",
          "ignore_case": true,
          "negation": true
        }
      ],
      "logmule_go_rules": null,
      "stats": {
        "hit_count": 0,
        "hit_eps": 0,
        "check_count": 0,
        "check_eps": 0,
        "check_time": 0
      },
      "_relations": {
        "logmule_go_rules": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "logmule_go_modules": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "content": "string",
      "is_system": true,
      "logmule_go_rules": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "name": "string",
          "frontend_data": {
            "alert": {
              "id": "uuid",
              "trace_id": "uuid",
              "name": "string",
              "create_incident": true,
              "assign_to_customer": true,
              "risk_level": 5.35,
              "asset_ip": "string",
              "asset_hostname": "string",
              "asset_fqdn": "string",
              "asset_mac": "string",
```

```
    "first_and_last_logs": false,
    "trim_logs": 1,
    "template": "string",
    "mitre": ""
  },
  "grouper": {
    "id": "uuid",
    "trace_id": "uuid",
    "name": "string",
    "grouped_by": [
      "string"
    ],
    "aggregated_by": [
      "string"
    ],
    "grouped_time_field": "string",
    "grouped_time_type": "2023-12-20T00:00:01.652259Z",
    "detection_windows": 5,
    "detection_windows_unit": "ms",
    "aggregate_count": 1,
    "aggregate_unique": true
  },
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
  "max_rule_memory_mb": 1
},
```

```
        "active": true,
        "reload": true,
        "finding_id": "uuid",
        "description": "string",
        "lua": "string",
        "is_retro": false,
        "is_system": true,
        "stats": {
          "result_count": 1,
          "error_count": 0
        },
        "is_error": 0,
        "running_at": "2023-12-20T00:00:01.652259Z"
      }
    ],
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"finding": {
  "id": "uuid",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid"
},
"logmule_go_results": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "rule_id": "uuid",
    "analysis_output": "string",
    "event": {},
    "compressed_event": "string",
    "risklevel": 5.35,
    "occurred_at": "2023-12-20T00:00:01.652259Z",
    "occurrence_id": "uuid",
    "error": "string",
    "service_asset_id": "uuid",
    "asset_info": {
      "ip": "string",
      "hostname": "string",
      "fqdn": "string",
      "mac": "string"
    },
    "incident_identifier": "string",
    "metadata": "{\"key\": \"value\"}",
    "logmule_go_rule": null,
    "occurrence": null,
    "service_asset": null,
    "service_asset_groups": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "network_ranges": [],
        "domain": "string",
        "itsm_synced": false,
        "regex": "string",
        "subject_id": "string",
```

```
        "object_id": "string",
        "is_kii": false,
        "is_fincert": false,
        "responsible_person": "string",
        "technical_specialist": "string",
        "system_id": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      }
    ],
    "_relations": {}
  }
],
"rule_sets": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "Набор 1",
    "create_service_asset_findings": false,
    "rule": null,
    "service_asset_groups": null
  }
],
"service_asset_findings": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
```

```
"updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
"group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
"acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
"created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
"edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
"incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
"reopened_at": "2023-12-20T00:00:01.652259Z",
"display_id": 0,
"service_asset_name": "string",
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
},
"finding": {},
"last_occurrence_entity": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
```

```
            "created_at": "2023-12-20T00:00:01.652259Z",
            "updated_at": "2023-12-20T00:00:01.652259Z",
            "event_type": "manual_source",
            "ip": "string",
            "mac": "string",
            "port": 0,
            "start_occurrence": "2023-12-20T00:00:01.652259Z",
            "end_occurrence": "2023-12-20T00:00:01.652259Z",
            "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
            "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
            "fqdn": "string",
            "incident_identifier": "string",
            "fincert_sync_status": 10,
            "fincert_id": "",
            "sopka_sync_status": 10,
            "sopka_id": "",
            "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
            "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
          },
          "user": {},
          "group": {},
          "incident_group": {
            "title": "string",
            "description": "string",
            "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
            "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
          },
          "occurrences": [
            {
              "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
              "created_at": "2023-12-20T00:00:01.652259Z",
              "updated_at": "2023-12-20T00:00:01.652259Z",
              "event_type": "manual_source",
              "ip": "string",
              "mac": "string",
              "port": 0,
              "start_occurrence": "2023-12-20T00:00:01.652259Z",
              "end_occurrence": "2023-12-20T00:00:01.652259Z",
              "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "fqdn": "string",
              "incident_identifier": "string",
              "fincert_sync_status": 10,
              "fincert_id": "",
              "sopka_sync_status": 10,
              "sopka_id": "",
              "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
              "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
            }
          ],
          "custom_field_values": [
            {
              "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "string_value": "string",
              "integer_value": 0,
              "float_value": 0,
              "date_value": "2023-12-20T00:00:01.652259Z",
              "json_value": {},
              "boolean_value": true
            }
          ],
```

```
            "comments": [
              {}
            ],
            "documents": [
              {}
            ],
            "messages": [
              {
                "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
                "created_at": "2023-12-20T00:00:01.652259Z",
                "updated_at": "2023-12-20T00:00:01.652259Z",
                "subject": "string",
                "body": "string",
                "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
                "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
                "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
                "automated": true,
                "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
                "itsm_sync_status": "not_synced",
                "itsm_last_synced_at": "string",
                "itsm_sync_error": "string",
                "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
              }
            ],
            "service_asset_finding_status_changes": [
              {
                "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
                "created_at": "2023-12-20T00:00:01.652259Z",
                "updated_at": "2023-12-20T00:00:01.652259Z",
                "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
                "status": "string",
                "revisit_at": "string",
                "itsm_sync_status": "not_synced",
                "itsm_last_synced_at": "string",
                "itsm_sync_error": "string",
                "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
              }
            ],
            "service_asset_groups": [
              {
                "title": "string",
                "description": "string",
                "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
                "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
              }
            ],
            "_relations": {
              "occurrences": [
                "497f6eca-6276-4993-bfeb-53cbbbba6f08"
              ],
              "custom_field_values": [
                "497f6eca-6276-4993-bfeb-53cbbbba6f08"
              ],
              "comments": [
                "string"
              ],
              "documents": [
                "string"
              ],
              "messages": [
                "string"
              ],
              "service_asset_finding_status_changes": [
```

```
        "string"
      ],
      "service_asset_groups": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"value_stores": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "name": "uuid",
    "description": "string",
    "values_scheme": [
      {
        "name": "field",
        "type": "int",
        "is_key": false
      }
    ],
    "is_large": true,
    "mask_values": true,
    "type": "pg",
    "version": 1,
    "source": "",
    "scheme": "vstore",
    "db_name": "vs_111dfca1defc11faa11dc11f1d11fd11",
    "user": "",
    "password": "",
    "store_count": 10,
    "content": null,
    "tollerId": "string",
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    },
    "logmule_go_rules": {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "frontend_data": {
        "alert": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "create_incident": true,
          "assign_to_customer": true,
          "risk_level": 5.35,
          "asset_ip": "string",
          "asset_hostname": "string",
          "asset_fqdn": "string",
          "asset_mac": "string",
          "first_and_last_logs": false,
          "trim_logs": 1,
          "template": "string",
          "mitre": ""
        },
        "grouper": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "grouped_by": [
```

```
      "string"
    ],
    "aggregated_by": [
      "string"
    ],
    "grouped_time_field": "string",
    "grouped_time_type": "2023-12-20T00:00:01.652259Z",
    "detection_windows": 5,
    "detection_windows_unit": "ms",
    "aggregate_count": 1,
    "aggregate_unique": true
  },
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
  "max_rule_memory_mb": 1
},
"active": true,
"reload": true,
"finding_id": "uuid",
"description": "string",
"lua": "string",
"is_retro": false,
"is_system": true,
"stats": {
  "result_count": 1,
  "error_count": 0
```

```
            },
            "is_error": 0,
            "running_at": "2023-12-20T00:00:01.652259Z"
          }
        }
      ],
      "_relations": {
        "logmule_go_filters": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "logmule_go_modules": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "logmule_go_results": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "rule_sets": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "service_asset_findings": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "value_stores": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "messages": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "subject": "string",
      "body": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "automated": true,
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
    }
  ],
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "_relations": {
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rules": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
409	name_already_used	Попытка присвоить объекту существующее уникальное значение атрибута
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 409:

```
{
  "error": "Bad Request",
  "error_code": 409,
  "extra": {
    "fields": [
      "name"
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.5 Поиск типов инцидентов

Запрос:

Тип	Метод
POST	/findings/search

Описание:

При выполнении запроса будут возвращены найденные типы инцидентов с учётом заданных фильтров.

По умолчанию в объекты не загружаются связанные модели по типам связи many2many и has-many, для включения загрузки их нужно указывать в поле relations объекта запроса.

Есть возможность расширить ответ информацией об идентификаторах связанных сущностей, возвращаемых в поле _relations, для этого необходимо и одноименном поле запроса передать список связанных моделей.

Поле _relations запроса расширяет поле relations для связей кроме один-к-одному, т.е. сущности, указанные в последнем поле, появятся в ответе в поле _relations в любом случае.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_findings/search
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска

Параметр	Тип данных	Обязательность	Описание
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений - substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят связанность с моделью по идентификатору если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "virtual_search": {
    "value": "string",
    "strict": false
  },
  "relations": [
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array <Finding>	Список найденных типов инцидентов

Параметр	Тип данных	Описание
total	integer	Количество найденных типов инцидентов

Пример ответа:


```
{
  "items": [
    {
      "title": "string",
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "display_id": 0,
      "mitigation": "string",
      "synopsis": "string",
      "local": true,
      "type": "network_anomaly",
      "identifier": {},
      "comment": "string",
      "fallback_raw_risklevel": 10,
      "new_version": true,
      "client_note": "string",
      "internal_note": "string",
      "cpes": [
        "string"
      ],
      "category_id": "8de4c9fd-61a4-4c0b-bf88-0ed3a0fe3fa2",
      "customer_created": true,
      "software_compliance": true,
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "is_system": true,
      "category": {},
      "service_asset_findings": [
        {
          "description": "string",
          "risk_impact": "string",
          "solution": "string",
          "mitigation": "string",
          "status": "assigned_customer",
          "risklevel": 0,
          "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
          "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
          "analysis_output": "string",
          "synopsis": "string",
          "title": "string",
          "risk": "none",
          "acknowledged_at": "2023-12-20T00:00:01.652259Z",
          "alert_type": "automatic",
          "client_note": "string",
          "internal_note": "string",
          "external": false,
          "immediate_action_score": 0,
          "throughput_period": "grace",
          "throughput_period_change": "2023-12-20T00:00:01.652259Z",
          "customer_created": false,
```

```
      "c_visible_since": "2023-12-20T00:00:01.652259Z",
      "c_visible_since_in_days": 0,
      "c_reopened_count": 0,
      "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "logmule_identifier": "string",
      "c_remote_exploitable": true,
      "c_occurrence_count": 0,
      "c_customer_retention_time": 0,
      "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "itsm_sync_status": "scheduled",
      "external_id": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
      "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
      "reopened_at": "2023-12-20T00:00:01.652259Z",
      "display_id": 0
    }
  ],
  "rules": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "frontend_data": {
        "alert": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "create_incident": true,
          "assign_to_customer": true,
          "risk_level": 5.35,
          "asset_ip": "string",
          "asset_hostname": "string",
          "asset_fqdn": "string",
          "asset_mac": "string",
          "first_and_last_logs": false,
          "trim_logs": 1,
          "template": "string",
          "mitre": ""
        },
        "grouper": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "grouped_by": [
            "string"
          ],
          "aggregated_by": [
            "string"
          ],
          "grouped_time_field": "string",
          "grouped_time_type": "2023-12-20T00:00:01.652259Z",
          "detection_windows": 5,
          "detection_windows_unit": "ms",
          "aggregate_count": 1,
          "aggregate_unique": true
        },
```

```
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
  "max_rule_memory_mb": 1
},
"active": true,
"reload": true,
"finding_id": "uuid",
"description": "string",
"lua": "string",
"is_retro": false,
"is_system": true,
"stats": {
  "result_count": 1,
  "error_count": 0
},
"is_error": 0,
"running_at": "2023-12-20T00:00:01.652259Z",
"logmule_go_filters": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "name": "string",
    "config": [
      {
        "compareFn": "equal",
        "expressions": [
          {
```

```
            "type": "logline-get",
            "value": {}
          }
        ],
        "type": "compare-condition",
        "parentId": "string",
        "ignore_case": true,
        "negation": true
      }
    ],
    "logmule_go_rules": null,
    "stats": {
      "hit_count": 0,
      "hit_eps": 0,
      "check_count": 0,
      "check_eps": 0,
      "check_time": 0
    },
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"logmule_go_modules": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "string",
    "content": "string",
    "is_system": true,
    "logmule_go_rules": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "frontend_data": {
          "alert": {
            "id": "uuid",
            "trace_id": "uuid",
            "name": "string",
            "create_incident": true,
            "assign_to_customer": true,
            "risk_level": 5.35,
            "asset_ip": "string",
            "asset_hostname": "string",
            "asset_fqdn": "string",
            "asset_mac": "string",
            "first_and_last_logs": false,
            "trim_logs": 1,
            "template": "string",
            "mitre": ""
          },
          "grouper": {
            "id": "uuid",
            "trace_id": "uuid",
            "name": "string",
            "grouped_by": [
              "string"
            ],
            "aggregated_by": [
```

```
      "string"
    ],
    "grouped_time_field": "string",
    "grouped_time_type": "2023-12-20T00:00:01.652259Z",
    "detection_windows": 5,
    "detection_windows_unit": "ms",
    "aggregate_count": 1,
    "aggregate_unique": true
  },
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
  "max_rule_memory_mb": 1
},
"active": true,
"reload": true,
"finding_id": "uuid",
"description": "string",
"lua": "string",
"is_retro": false,
"is_system": true,
"stats": {
  "result_count": 1,
  "error_count": 0
},
"is_error": 0,
"running_at": "2023-12-20T00:00:01.652259Z"
```

```
      }
    ],
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"finding": {
  "id": "uuid",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid"
},
"logmule_go_results": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "rule_id": "uuid",
    "analysis_output": "string",
    "event": {},
    "compressed_event": "string",
    "risklevel": 5.35,
    "occurred_at": "2023-12-20T00:00:01.652259Z",
    "occurrence_id": "uuid",
    "error": "string",
    "service_asset_id": "uuid",
    "asset_info": {
      "ip": "string",
      "hostname": "string",
      "fqdn": "string",
      "mac": "string"
    },
    "incident_identifier": "string",
    "metadata": "{\"key\": \"value\"}",
    "logmule_go_rule": null,
    "occurrence": null,
    "service_asset": null,
    "service_asset_groups": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "network_ranges": [],
        "domain": "string",
        "itsm_synced": false,
        "regex": "string",
        "subject_id": "string",
        "object_id": "string",
        "is_kii": false,
        "is_fincert": false,
        "responsible_person": "string",
        "technical_specialist": "string",
        "system_id": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      }
    ],
    "_relations": {}
  }
],
```

```
"rule_sets": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "Набор 1",
    "create_service_asset_findings": false,
    "rule": null,
    "service_asset_groups": null
  }
],
"service_asset_findings": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0,
    "service_asset_name": "string",
    "service_asset_active": true,
    "occurrence_count": 0,
    "user_short_name": "string",
    "group_name": "string",
```

```
      "finding_display_id": 0,
      "reopened_count": 0,
      "event_type": "string",
      "finding_type": "string",
      "ports": [
        0
      ],
      "last_occurrence_ip": "string",
      "service_asset_value": 0,
      "tag_titles": [
        "string"
      ],
      "last_status_change": "2023-12-20T00:00:01.652259Z",
      "last_scan": "2023-12-20T00:00:01.652259Z",
      "authenticated": true,
      "last_occurrence": "2023-12-20T00:00:01.652259Z",
      "remote_exploitable": true,
      "service_asset_network_exposure": 0,
      "finding_category": "string",
      "display_title": "string",
      "customer_retention_time": 0,
      "visible_since": "2023-12-20T00:00:01.652259Z",
      "visible_since_in_days": 0,
      "last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "finding_title": "string",
      "incident_group_title": "string",
      "custom_values": {},
      "trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
      "service_asset": {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "type": "Host",
        "name": "Актив",
        "description": "Описание актива",
        "coordinates": "--- []",
        "active": true,
        "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
        "value": 3,
        "client_note": "string",
        "internal_note": "string",
        "location": "string",
        "network_exposure": 3,
        "responsible_person": "string",
        "technical_specialist": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      },
      "finding": {},
      "last_occurrence_entity": {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "event_type": "manual_source",
        "ip": "string",
        "mac": "string",
        "port": 0,
        "start_occurrence": "2023-12-20T00:00:01.652259Z",
        "end_occurrence": "2023-12-20T00:00:01.652259Z",
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "fqdn": "string",
        "incident_identifier": "string",
```

```
    "fincert_sync_status": 10,
    "fincert_id": "",
    "sopka_sync_status": 10,
    "sopka_id": "",
    "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
    "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
  },
  "user": {},
  "group": {},
  "incident_group": {
    "title": "string",
    "description": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
  },
  "occurrences": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "event_type": "manual_source",
      "ip": "string",
      "mac": "string",
      "port": 0,
      "start_occurrence": "2023-12-20T00:00:01.652259Z",
      "end_occurrence": "2023-12-20T00:00:01.652259Z",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "fqdn": "string",
      "incident_identifier": "string",
      "fincert_sync_status": 10,
      "fincert_id": "",
      "sopka_sync_status": 10,
      "sopka_id": "",
      "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
      "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
    }
  ],
  "custom_field_values": [
    {
      "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "string_value": "string",
      "integer_value": 0,
      "float_value": 0,
      "date_value": "2023-12-20T00:00:01.652259Z",
      "json_value": {},
      "boolean_value": true
    }
  ],
  "comments": [
    {}
  ],
  "documents": [
    {}
  ],
  "messages": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "subject": "string",
      "body": "string",
```

```
                "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
                "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
                "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
                "automated": true,
                "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
                "itsm_sync_status": "not_synced",
                "itsm_last_synced_at": "string",
                "itsm_sync_error": "string",
                "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
              }
            ],
            "service_asset_finding_status_changes": [
              {
                "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
                "created_at": "2023-12-20T00:00:01.652259Z",
                "updated_at": "2023-12-20T00:00:01.652259Z",
                "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
                "status": "string",
                "revisit_at": "string",
                "itsm_sync_status": "not_synced",
                "itsm_last_synced_at": "string",
                "itsm_sync_error": "string",
                "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
              }
            ],
            "service_asset_groups": [
              {
                "title": "string",
                "description": "string",
                "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
                "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
              }
            ],
            "_relations": {
              "occurrences": [
                "497f6eca-6276-4993-bfeb-53cbbbba6f08"
              ],
              "custom_field_values": [
                "497f6eca-6276-4993-bfeb-53cbbbba6f08"
              ],
              "comments": [
                "string"
              ],
              "documents": [
                "string"
              ],
              "messages": [
                "string"
              ],
              "service_asset_finding_status_changes": [
                "string"
              ],
              "service_asset_groups": [
                "497f6eca-6276-4993-bfeb-53cbbbba6f08"
              ]
            }
          }
        ],
        "value_stores": [
          {
            "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
            "name": "uuid",
            "description": "string",
```

```
"values_scheme": [
  {
    "name": "field",
    "type": "int",
    "is_key": false
  }
],
"is_large": true,
"mask_values": true,
"type": "pg",
"version": 1,
"source": "",
"scheme": "vstore",
"db_name": "vs_111dfca1defc11faa11dc11f1d11fd11",
"user": "",
"password": "",
"store_count": 10,
"content": null,
"tollerId": "string",
"_relations": {
  "logmule_go_rules": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ]
},
"logmule_go_rules": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "name": "string",
  "frontend_data": {
    "alert": {
      "id": "uuid",
      "trace_id": "uuid",
      "name": "string",
      "create_incident": true,
      "assign_to_customer": true,
      "risk_level": 5.35,
      "asset_ip": "string",
      "asset_hostname": "string",
      "asset_fqdn": "string",
      "asset_mac": "string",
      "first_and_last_logs": false,
      "trim_logs": 1,
      "template": "string",
      "mitre": ""
    },
    "grouper": {
      "id": "uuid",
      "trace_id": "uuid",
      "name": "string",
      "grouped_by": [
        "string"
      ],
      "aggregated_by": [
        "string"
      ],
      "grouped_time_field": "string",
      "grouped_time_type": "2023-12-20T00:00:01.652259Z",
      "detection_windows": 5,
      "detection_windows_unit": "ms",
      "aggregate_count": 1,
      "aggregate_unique": true
    },
    "actions": [
```

```
            {
              "TTL": "string",
              "key": {
                "_default": {
                  "type": "value",
                  "value": "string"
                }
              },
              "type": "store-set",
              "store": "string",
              "value": "string",
              "column": "string"
            }
          ],
          "conditions": [
            {
              "type": "compare-condition",
              "id": "uuid",
              "parentId": null,
              "negation": false,
              "compareFn": "eq",
              "expressions": [
                {
                  "type": "logline-get",
                  "value": "string"
                }
              ]
            }
          ],
          "version": 2
        },
        "test_data": [
          {}
        ],
        "settings": {
          "function_metrics": false,
          "is_constructor": false,
          "max_alerts": 1,
          "max_alerts_per_second": 1,
          "max_rule_memory_mb": 1
        },
        "active": true,
        "reload": true,
        "finding_id": "uuid",
        "description": "string",
        "lua": "string",
        "is_retro": false,
        "is_system": true,
        "stats": {
          "result_count": 1,
          "error_count": 0
        },
        "is_error": 0,
        "running_at": "2023-12-20T00:00:01.652259Z"
      }
    }
  ],
  "_relations": {
    "logmule_go_filters": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "logmule_go_modules": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
```

```
            "logmule_go_results": [
              "497f6eca-6276-4993-bfeb-53cbbbba6f08"
            ],
            "rule_sets": [
              "497f6eca-6276-4993-bfeb-53cbbbba6f08"
            ],
            "service_asset_findings": [
              "497f6eca-6276-4993-bfeb-53cbbbba6f08"
            ],
            "value_stores": [
              "497f6eca-6276-4993-bfeb-53cbbbba6f08"
            ]
          }
        }
      ],
      "messages": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "created_at": "2023-12-20T00:00:01.652259Z",
          "updated_at": "2023-12-20T00:00:01.652259Z",
          "subject": "string",
          "body": "string",
          "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
          "automated": true,
          "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
          "itsm_sync_status": "not_synced",
          "itsm_last_synced_at": "string",
          "itsm_sync_error": "string",
          "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
        }
      ],
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "_relations": {
        "service_asset_findings": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "rules": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "messages": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "total": 1
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр

Код	Ответ	Описание
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.6 Получение типа инцидента по ID

Запрос:

Тип	Метод
GET	/findings/{id}

Описание:

При выполнении запроса будет возвращен тип инцидента с соответствующим ID.

Если не указан параметр relations то подгружаются все связи объекта. Если параметр указан, но не имеет значений - связи не подгружаются. Если параметр указан и содержит значения (поля модели хранящие связанные сущности) то они будут заполнены в ответе.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/findings/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор типа инцидента

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Типы инцидентов»».

Пример ответа:


```
{
  "title": "string",
  "description": "string",
  "risk_impact": "string",
  "solution": "string",
  "display_id": 0,
  "mitigation": "string",
  "synopsis": "string",
  "local": true,
  "type": "network_anomaly",
  "identifier": {},
  "comment": "string",
  "fallback_raw_risklevel": 10,
  "new_version": true,
  "client_note": "string",
  "internal_note": "string",
  "cpes": [
    "string"
  ],
  "category_id": "8de4c9fd-61a4-4c0b-bf88-0ed3a0fe3fa2",
  "customer_created": true,
  "software_compliance": true,
  "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
  "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
  "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "is_system": true,
  "category": {},
  "service_asset_findings": [
    {
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
```

```
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  }
],
"rules": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "string",
    "frontend_data": {
      "alert": {
        "id": "uuid",
        "trace_id": "uuid",
        "name": "string",
        "create_incident": true,
        "assign_to_customer": true,
        "risk_level": 5.35,
        "asset_ip": "string",
        "asset_hostname": "string",
        "asset_fqdn": "string",
        "asset_mac": "string",
        "first_and_last_logs": false,
        "trim_logs": 1,
        "template": "string",
        "mitre": ""
      },
      "grouper": {
        "id": "uuid",
```

```
      "trace_id": "uuid",
      "name": "string",
      "grouped_by": [
        "string"
      ],
      "aggregated_by": [
        "string"
      ],
      "grouped_time_field": "string",
      "grouped_time_type": "2023-12-20T00:00:01.652259Z",
      "detection_windows": 5,
      "detection_windows_unit": "ms",
      "aggregate_count": 1,
      "aggregate_unique": true
    },
    "actions": [
      {
        "TTL": "string",
        "key": {
          "_default": {
            "type": "value",
            "value": "string"
          }
        },
        "type": "store-set",
        "store": "string",
        "value": "string",
        "column": "string"
      }
    ],
    "conditions": [
      {
        "type": "compare-condition",
        "id": "uuid",
        "parentId": null,
        "negation": false,
        "compareFn": "eq",
        "expressions": [
          {
            "type": "logline-get",
            "value": "string"
          }
        ]
      }
    ],
    "version": 2
  },
  "test_data": [
    {}
  ],
  "settings": {
    "function_metrics": false,
    "is_constructor": false,
    "max_alerts": 1,
    "max_alerts_per_second": 1,
    "max_rule_memory_mb": 1
  },
  "active": true,
  "reload": true,
  "finding_id": "uuid",
  "description": "string",
  "lua": "string",
  "is_retro": false,
  "is_system": true,
```

```
"stats": {
  "result_count": 1,
  "error_count": 0
},
"is_error": 0,
"running_at": "2023-12-20T00:00:01.652259Z",
"logmule_go_filters": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "name": "string",
    "config": [
      {
        "compareFn": "equal",
        "expressions": [
          {
            "type": "logline-get",
            "value": {}
          }
        ],
        "type": "compare-condition",
        "parentId": "string",
        "ignore_case": true,
        "negation": true
      }
    ],
    "logmule_go_rules": null,
    "stats": {
      "hit_count": 0,
      "hit_eps": 0,
      "check_count": 0,
      "check_eps": 0,
      "check_time": 0
    },
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"logmule_go_modules": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "string",
    "content": "string",
    "is_system": true,
    "logmule_go_rules": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "frontend_data": {
          "alert": {
            "id": "uuid",
            "trace_id": "uuid",
            "name": "string",
            "create_incident": true,
            "assign_to_customer": true,
            "risk_level": 5.35,
            "asset_ip": "string",
            "asset_hostname": "string",
```

```
    "asset_fqdn": "string",
    "asset_mac": "string",
    "first_and_last_logs": false,
    "trim_logs": 1,
    "template": "string",
    "mitre": ""
  },
  "grouper": {
    "id": "uuid",
    "trace_id": "uuid",
    "name": "string",
    "grouped_by": [
      "string"
    ],
    "aggregated_by": [
      "string"
    ],
    "grouped_time_field": "string",
    "grouped_time_type": "2023-12-20T00:00:01.652259Z",
    "detection_windows": 5,
    "detection_windows_unit": "ms",
    "aggregate_count": 1,
    "aggregate_unique": true
  },
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
```

```
          "max_rule_memory_mb": 1
        },
        "active": true,
        "reload": true,
        "finding_id": "uuid",
        "description": "string",
        "lua": "string",
        "is_retro": false,
        "is_system": true,
        "stats": {
          "result_count": 1,
          "error_count": 0
        },
        "is_error": 0,
        "running_at": "2023-12-20T00:00:01.652259Z"
      }
    ],
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"finding": {
  "id": "uuid",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid"
},
"logmule_go_results": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "rule_id": "uuid",
    "analysis_output": "string",
    "event": {},
    "compressed_event": "string",
    "risklevel": 5.35,
    "occurred_at": "2023-12-20T00:00:01.652259Z",
    "occurrence_id": "uuid",
    "error": "string",
    "service_asset_id": "uuid",
    "asset_info": {
      "ip": "string",
      "hostname": "string",
      "fqdn": "string",
      "mac": "string"
    },
    "incident_identifier": "string",
    "metadata": "{\"key\": \"value\"}",
    "logmule_go_rule": null,
    "occurrence": null,
    "service_asset": null,
    "service_asset_groups": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "network_ranges": [],
        "domain": "string",
        "itsm_synced": false,
```

```
        "regex": "string",
        "subject_id": "string",
        "object_id": "string",
        "is_kii": false,
        "is_fincert": false,
        "responsible_person": "string",
        "technical_specialist": "string",
        "system_id": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      }
    ],
    "_relations": {}
  }
],
"rule_sets": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "Набор 1",
    "create_service_asset_findings": false,
    "rule": null,
    "service_asset_groups": null
  }
],
"service_asset_findings": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
```

```
"itsm_sync_error": "string",
"user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
"updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
"group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
"acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
"created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
"edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
"incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
"reopened_at": "2023-12-20T00:00:01.652259Z",
"display_id": 0,
"service_asset_name": "string",
"service_asset_active": true,
"occurrence_count": 0,
"user_short_name": "string",
"group_name": "string",
"finding_display_id": 0,
"reopened_count": 0,
"event_type": "string",
"finding_type": "string",
"ports": [
  0
],
"last_occurrence_ip": "string",
"service_asset_value": 0,
"tag_titles": [
  "string"
],
"last_status_change": "2023-12-20T00:00:01.652259Z",
"last_scan": "2023-12-20T00:00:01.652259Z",
"authenticated": true,
"last_occurrence": "2023-12-20T00:00:01.652259Z",
"remote_exploitable": true,
"service_asset_network_exposure": 0,
"finding_category": "string",
"display_title": "string",
"customer_retention_time": 0,
"visible_since": "2023-12-20T00:00:01.652259Z",
"visible_since_in_days": 0,
"last_customer_status_change": "2023-12-20T00:00:01.652259Z",
"finding_title": "string",
"incident_group_title": "string",
"custom_values": {},
"trace_id": "df570c03-5a03-4cea-8df0-c162d05127ac",
"service_asset": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
},
"finding": {},
```

```
          "last_occurrence_entity": {
            "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
            "created_at": "2023-12-20T00:00:01.652259Z",
            "updated_at": "2023-12-20T00:00:01.652259Z",
            "event_type": "manual_source",
            "ip": "string",
            "mac": "string",
            "port": 0,
            "start_occurrence": "2023-12-20T00:00:01.652259Z",
            "end_occurrence": "2023-12-20T00:00:01.652259Z",
            "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
            "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
            "fqdn": "string",
            "incident_identifier": "string",
            "fincert_sync_status": 10,
            "fincert_id": "",
            "sopka_sync_status": 10,
            "sopka_id": "",
            "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
            "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
          },
          "user": {},
          "group": {},
          "incident_group": {
            "title": "string",
            "description": "string",
            "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
            "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
          },
          "occurrences": [
            {
              "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
              "created_at": "2023-12-20T00:00:01.652259Z",
              "updated_at": "2023-12-20T00:00:01.652259Z",
              "event_type": "manual_source",
              "ip": "string",
              "mac": "string",
              "port": 0,
              "start_occurrence": "2023-12-20T00:00:01.652259Z",
              "end_occurrence": "2023-12-20T00:00:01.652259Z",
              "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "fqdn": "string",
              "incident_identifier": "string",
              "fincert_sync_status": 10,
              "fincert_id": "",
              "sopka_sync_status": 10,
              "sopka_id": "",
              "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
              "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
            }
          ],
          "custom_field_values": [
            {
              "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
              "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
              "string_value": "string",
              "integer_value": 0,
              "float_value": 0,
              "date_value": "2023-12-20T00:00:01.652259Z",
              "json_value": {},
              "boolean_value": true
```

```
      }
    ],
    "comments": [
      {}
    ],
    "documents": [
      {}
    ],
    "messages": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "subject": "string",
        "body": "string",
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "automated": true,
        "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
        "itsm_sync_status": "not_synced",
        "itsm_last_synced_at": "string",
        "itsm_sync_error": "string",
        "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
      }
    ],
    "service_asset_finding_status_changes": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "status": "string",
        "revisit_at": "string",
        "itsm_sync_status": "not_synced",
        "itsm_last_synced_at": "string",
        "itsm_sync_error": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
      }
    ],
    "service_asset_groups": [
      {
        "title": "string",
        "description": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
      }
    ],
    "_relations": {
      "occurrences": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "custom_field_values": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "comments": [
        "string"
      ],
      "documents": [
        "string"
      ],
      "messages": [
        "string"
```

```
      ],
      "service_asset_finding_status_changes": [
        "string"
      ],
      "service_asset_groups": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"value_stores": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "name": "uuid",
    "description": "string",
    "values_scheme": [
      {
        "name": "field",
        "type": "int",
        "is_key": false
      }
    ],
    "is_large": true,
    "mask_values": true,
    "type": "pg",
    "version": 1,
    "source": "",
    "scheme": "vstore",
    "db_name": "vs_111dfca1defc11faa11dc11f1d11fd11",
    "user": "",
    "password": "",
    "store_count": 10,
    "content": null,
    "tollerId": "string",
    "_relations": {
      "logmule_go_rules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    },
    "logmule_go_rules": {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "frontend_data": {
        "alert": {
          "id": "uuid",
          "trace_id": "uuid",
          "name": "string",
          "create_incident": true,
          "assign_to_customer": true,
          "risk_level": 5.35,
          "asset_ip": "string",
          "asset_hostname": "string",
          "asset_fqdn": "string",
          "asset_mac": "string",
          "first_and_last_logs": false,
          "trim_logs": 1,
          "template": "string",
          "mitre": ""
        },
        "grouper": {
          "id": "uuid",
          "trace_id": "uuid",
```

```
    "name": "string",
    "grouped_by": [
      "string"
    ],
    "aggregated_by": [
      "string"
    ],
    "grouped_time_field": "string",
    "grouped_time_type": "2023-12-20T00:00:01.652259Z",
    "detection_windows": 5,
    "detection_windows_unit": "ms",
    "aggregate_count": 1,
    "aggregate_unique": true
  },
  "actions": [
    {
      "TTL": "string",
      "key": {
        "_default": {
          "type": "value",
          "value": "string"
        }
      },
      "type": "store-set",
      "store": "string",
      "value": "string",
      "column": "string"
    }
  ],
  "conditions": [
    {
      "type": "compare-condition",
      "id": "uuid",
      "parentId": null,
      "negation": false,
      "compareFn": "eq",
      "expressions": [
        {
          "type": "logline-get",
          "value": "string"
        }
      ]
    }
  ],
  "version": 2
},
"test_data": [
  {}
],
"settings": {
  "function_metrics": false,
  "is_constructor": false,
  "max_alerts": 1,
  "max_alerts_per_second": 1,
  "max_rule_memory_mb": 1
},
"active": true,
"reload": true,
"finding_id": "uuid",
"description": "string",
"lua": "string",
"is_retro": false,
"is_system": true,
"stats": {
```

```
            "result_count": 1,
            "error_count": 0
          },
          "is_error": 0,
          "running_at": "2023-12-20T00:00:01.652259Z"
        }
      }
    ],
    "_relations": {
      "logmule_go_filters": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "logmule_go_modules": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "logmule_go_results": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "rule_sets": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "service_asset_findings": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "value_stores": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  }
],
"messages": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "subject": "string",
    "body": "string",
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
    "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
    "automated": true,
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "itsm_sync_status": "not_synced",
    "itsm_last_synced_at": "string",
    "itsm_sync_error": "string",
    "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
  }
],
"id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
"created_at": "2023-12-20T00:00:01.652259Z",
"updated_at": "2023-12-20T00:00:01.652259Z",
"_relations": {
  "service_asset_findings": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "rules": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "messages": [
```

```
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.7 Удаление типа инцидента

Запрос:

Тип	Метод
DELETE	/findings/{id}

Описание:

При выполнении запроса будет удален тип инцидента с соответствующим ID.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/findings/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор типа инцидента

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
422	11002 11003 11004 11011	Общая ошибка удаления Запрос не затронул ни одной сущности Удаляемая модель не найдена Удаление невозможно из-за наличия блокирующих связей
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 422:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.8 Группировка типов инцидентов

Запрос:

Тип	Метод
POST	/findings/group

Описание:

При выполнении запроса типы инцидентов будут сгруппированы по заданному полю.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/findings/group`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки типов инцидентов

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.9 Массовое удаление типов инцидентов

Запрос:

Тип	Метод
POST	/findings/mass_delete

Описание:

При выполнении запроса будут удалены типы инцидентов с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/findings/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности.

Пример ответа:

```
{
  "results": [
    {
      "id": "string",
      "error_code": 11001
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.10 Удаление всех типов инцидентов

Запрос:

Тип	Метод
DELETE	/findings/all

Описание:

При выполнении запроса из базы данных будут удалены все типы инцидентов.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/findings/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
422	11001 11012 11003	Ошибка связанных данных (зависимости) Ошибка некорректно настроенных связей (отсутствие on cascade и пр.) Запрос на изменение не затронул ни одной строки
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 422:

```
{
  "error_code": "11001 // ошибка связанных данных (зависимости)",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.2.11 Получение свойств типов инцидента и действий пользователей

Запрос:

Тип	Метод
GET	/findings/_meta

Описание:

При выполнении запроса будут возвращены свойства типов инцидентов и список действий пользователей над ними.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/findings/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:

```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
}
```


Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3 Группы инцидентов

2.3.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	incident_groups
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	Ресурс incident_groups отвечает за управление группами инцидентов. Группы инцидентов предназначены для упрощения исследования инцидентов сотрудниками. Схожие инциденты помещают в группы, а их затем назначают пользователям.

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/incident_groups/create	Создание группы инцидентов
PUT	/incident_groups/update	Обновление информации о группе инцидентов
POST	/incident_groups/search	Поиск групп инцидентов
GET	/incident_groups/{id}	Получение группы инцидентов по ID
DELETE	/incident_groups/{id}	Удаление группы инцидентов
POST	/incident_groups/group	Группировка групп инцидентов
POST	/incident_groups/mass_delete	Массовое удаление групп инцидентов
DELETE	/incident_groups/all	Удаление всех групп инцидентов
POST	/incident_groups/{id}/action	Действие над группой инцидентов по ID

Тип	Метод	Описание
GET	/incident_groups/_meta	Получение свойств групп инцидентов и действий пользователей

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
409	Попытка присвоить объекту существующее уникальное значение атрибута
422	Другие ошибки удаления
500	Ошибка сервера

Модели объектов:

Название	Описание
IncidentGroup	Модель данных ресурса incident_groups

2.3.2 Модель ресурса «Группы инцидентов»

Модель данных IncidentGroup:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы инцидентов
created_at	string time	Required	Дата создания группы инцидентов в формате: date-time
updated_at	string time	Required	Дата изменения группы инцидентов в формате: date-time

Параметр	Тип данных	Обязательность	Описание
title	string	Required	Название группы инцидентов
description	string	Required	Расширенное описание группы инцидентов
user_id	string	Required	Идентификатор пользователя, на которого назначена группа инцидентов
group_id	string	Required	Идентификатор группы пользователей, на которую назначена группа инцидентов
incidents_count	number	Required	Количество инцидентов, входящих в группу
service_asset_findings	Array<ServiceAssetFinding>	Required	Список инцидентов, входящих в группу
user	object	Required	Объект, описывающий связанного пользователя
group	object	Required	Объект, описывающий связанную группу пользователей
service_asset_findings	Array<string>	Required	Список идентификаторов инцидентов, входящих в группу
id	string	Required	Идентификатор группы инцидентов
created_at	string time	Required	Дата создания группы инцидентов в формате: date-time

Модель данных ServiceAssetFindingNoRelations:

Параметр	Тип данных	Обязательность	Описание
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.

Параметр	Тип данных	Обязательность	Описание
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace; - delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.

Параметр	Тип данных	Обязательность	Описание
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов

2.3.3 Создание группы инцидентов

Запрос:

Тип	Метод
POST	/incident_groups/create

Описание:

При выполнении запроса будет создана группа инцидентов с заданными параметрами.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/incident_groups/create`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
title	string	Required	Название группы инцидентов
description	string	Required	Расширенное описание группы инцидентов
user_id	string	Required	Идентификатор пользователя, на которого назначена группа инцидентов
group_id	string	Required	Идентификатор группы пользователей, на которую назначена группа инцидентов

Пример тела запроса:

```
{
  "title": "string",
  "description": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f"
}
```

Успешный ответ:

Статус код: 201 – успешное создание группы инцидентов.

Формат: JSON.

Тело ответа: «Модель ресурса «Группы инцидентов»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "title": "string",
  "description": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "incidents_count": 0,
  "service_asset_findings": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "user": {},
  "group": {}
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
409	name_already_used	Попытка создать объект с существующим уникальным атрибутом
500	Internal Server Error	Другие ошибки при создании объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 409:


```
{
  "error": "Bad Request",
  "error_code": 409,
  "extra": {
    "fields": [
      "name"
    ]
  }
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3.4 Обновление группы инцидентов

Запрос:

Тип	Метод
PUT	/incident_groups/update

Описание:

При выполнении запроса будет обновлена информация о группе инцидентов в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля модели, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в объекте _relations отсутствуют зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются;
- Зависимости игнорируются в теле запроса;
- Зависимости в ответе всегда null.

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "logmule_go_rules": [] // - очистит все связи с правилами
    // "logmule_go_rules": ["uuid1", "uuid2"] // - создаст связь с 2 правилами
    // "logmule_go_rules": ["uuid1"] // - оставит связь только с первым правилом
  }
}
```

Пример запроса:

PUT

`http://127.0.0.1/cruddy/v2/incident_groups/update`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы инцидентов
created_at	string time	Required	Дата создания группы инцидентов в формате: date-time
updated_at	string time	Required	Дата изменения группы инцидентов в формате: date-time
title	string	Required	Название группы инцидентов
description	string	Required	Расширенное описание группы инцидентов
user_id	string	Required	Идентификатор пользователя, на которого назначена группа инцидентов
group_id	string	Required	Идентификатор группы пользователей, на которую назначена группа инцидентов
_relations	object	Required	Словарь, описывающий связанные модели через идентификаторы
_relations**{service_asset_findings}**	Array<string>	Required	Список идентификаторов инцидентов, входящих в группу

Пример тела запроса:

```
{
  "title": "string",
  "description": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "trace_id": "uuid",
  "_relations": {
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```

Успешный ответ:

Статус код: 200 - успешное обновление информации о группе инцидентов.

Формат: JSON.

Тело ответа: «Модель ресурса «Группы инцидентов»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "title": "string",
  "description": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "incidents_count": 0,
  "service_asset_findings": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "user": {},
  "group": {}
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
409	name_already_used	Попытка присвоить объекту существующее уникальное значение атрибута
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 409:

```
{
  "error": "Bad Request",
  "error_code": 409,
  "extra": {
    "fields": [
      "name"
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3.5 Поиск группы инцидентов

Запрос:

Тип	Метод
POST	/incident_groups/search

Описание:

При выполнении запроса будут возвращены найденные группы инцидентов с учётом заданных фильтров.

По умолчанию в объекты не загружаются связанные модели по типам связи many2many и has-many, для включения загрузки их нужно указывать в поле relations объекта запроса.

Связи _relations загружаются всегда и отражают текущее состояние связей модели.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/incident_groups/search`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений - substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят связанность с моделью по идентификатору

Параметр	Тип данных	Обязательность	Описание
			если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "virtual_search": {
```

```
    "value": "string",
    "strict": false
  },
  "relations": [
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array<IncidentGroups>	Список найденных групп инцидентов
total	integer	Количество найденных групп инцидентов

Пример ответа:

```
{
  "items": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "title": "string",
      "description": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "incidents_count": 0,
      "service_asset_findings": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "user": {},
      "group": {}
    }
  ],
  "total": 1
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3.6 Получение группы инцидентов по ID

Запрос:

Тип	Метод
GET	/incident_groups/{id}

Описание:

При выполнении запроса будет возвращена группа инцидентов с соответствующим ID.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/incident_groups/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор группы инцидентов

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Группы инцидентов»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "title": "string",
  "description": "string",
  "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
  "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
  "incidents_count": 0,
  "service_asset_findings": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "user": {},
  "group": {}
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
```

```
  "error": "Bad Request",
  "error_code": 400
}
```


Код 404:


```
{
  "error": "Not Found",
  "error_code": 404
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.3.7 Удаление группы инцидентов

Запрос:

Тип	Метод
DELETE	/incident_groups/{id}

Описание:

При выполнении запроса будет удалена группа инцидентов с соответствующим ID.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/incident_groups/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор группы инцидентов

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
422	11002 11003 11004 11011	Общая ошибка удаления Запрос не затронул ни одной сущности Удаляемая модель не найдена Удаление невозможно из-за наличия блокирующих связей
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 422:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
```

```
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3.8 Группировка групп инцидентов

Запрос:

Тип	Метод
POST	/incident_groups/group

Описание:

При выполнении запроса группы инцидентов будут сгруппированы по заданному полю.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/incident_groups/group
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки групп инцидентов

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3.9 Массовое удаление групп инцидентов

Запрос:

Тип	Метод
POST	/incident_groups/mass_delete

Описание:

При выполнении запроса будут удалены группы инцидентов с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/incident_groups/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности.

Пример ответа:

```
{
  "results": [
    {
      "id": "string",
      "error_code": 11001
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3.10 Удаление всех групп инцидентов

Запрос:

Тип	Метод
DELETE	/incident_groups/all

Описание:

При выполнении запроса из базы данных будут удалены все группы инцидентов.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/incident_groups/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
422	11001 11012 11003	Ошибка связанных данных (зависимости) Ошибка некорректно настроенных связей (отсутствие on cascade и пр.) Запрос на изменение не затронул ни одной строки
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 422:

```
{
  "error_code": "11001 // ошибка связанных данных (зависимости)",
  "relations": {
    "dynamic_relation_name": [
      {
```

```
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.3.11 Действие над группой инцидентов по ID

Запрос:

Тип	Метод
POST	/incident_groups/{id}/action

Описание:

При выполнении запроса будет выполнено действие над группой инцидентов с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/incident_groups/{id}/action
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор группы инцидентов

Header параметры запроса:

Параметр	Описание
restriction	Тип ограничения для действия

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
action	string	Required	Действие над группой инцидентов. Допустимые значения: - add_incidents - добавить инциденты в группу; - remove_incidents - удалить инциденты из группы; - close_incidents - закрыть выбранные инциденты, состоящие в группе; - delete_incidents - удалить выбранные инциденты, входящие в группу; - close_all_incidents - закрыть все инциденты, входящие в группу; - delete_all_incidents - удалить все инциденты, входящие в группу
ids	Array<string>	Required	Список ID объектов, над которыми совершается действие

Пример тела запроса:

```
{
  "action": "string",
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа. Состав ответа определяется непосредственно в сервисе, который реализует данный метод.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр

Код	Ответ	Описание
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.3.12 Получение свойств групп инцидентов и действий пользователей

Запрос:

Тип	Метод
GET	/incident_groups/_meta

Описание:

При выполнении запроса будут возвращены свойства групп инцидентов и список действий пользователей над ними

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/incident_groups/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:


```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
```

```
}
```

Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.4 Происшествия

2.4.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	occurrences
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	Ресурс occurrences отвечает за управление происшествиями.

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/occurrences/create	Создание происшествия
PUT	/domain/update	Обновление информации о происшествии
POST	/occurrences/search	Поиск происшествий
GET	/occurrences/{id}	Получение происшествия по ID
DELETE	/occurrences/{id}	Удаление происшествия
POST	/occurrences/group	Группировка происшествий
POST	/occurrences/mass_delete	Массовое удаление происшествий
DELETE	/occurrences/all	Удаление всех происшествий
GET	/domain/_meta	Получение свойств происшествий и действий пользователей

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
422	Другие ошибки удаления
500	Ошибка сервера

Модели объектов:

Название	Описание
Occurrence	Модель данных ресурса occurrences

2.4.2 Модель ресурса «Происшествия»

Модель данных Occurrence:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор происшествия
created_at	string	Required	Дата создания происшествия в формате: date-time
updated_at	string	Required	Дата изменения происшествия в формате: date-time
event_type	string	Required	Тип происшествия. Допустимые значения: - manual_source - logmule_go_result - software_compliance_source - vulnerability - watchdog_result

Параметр	Тип данных	Обязательность	Описание
ip	string	Required	IP-адрес актива
mac	string	Required	MAC-адрес актива
port	integer	Required	Порт
start_occurrence	string	Required	Время первого изменения статуса в клиентской системе
end_occurrence	string	Required	Время последнего изменения статуса в клиентской системе
service_asset_finding_status_change_id	string	Required	Идентификатор операции смены статуса инцидента
service_asset_finding_id	string	Required	Идентификатор инцидента
fqdn	string	Required	FQDN актива
incident_identifier	string	Required	Идентификатор инцидента во внешней системе
fincert_sync_status	number	Required	Состояние синхронизации с внешней системой
fincert_id	string	Required	Идентификатор внешней системы
sopka_sync_status	number	Required	Состояние синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)
sopka_id	string	Required	Идентификатор внешней системы реагирования на компьютерные инциденты (CERT)
fincert_sync_result	string	Required	Результат синхронизации с внешней системой
sopka_sync_result	string	Required	Результат синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)
service_asset_finding	Array<ServiceAssetFindingNoRelations>	Required	Инцидент
service_asset_finding_status_change	object<ServiceAssetFindingStatusChange>	Required	Смена статуса инцидента
vulnerabilities	Array<Vulnerability>	Required	Уязвимости
logmule_go_results	Array<LogmuleGoResults>	Required	Результат работы правила корреляции (см. «**Ошибка! Источник ссылки не найден.**»)
_relations	object	Required	Словарь, описывающий связанные модели через идентификаторы
_relations**{logmule_go_results}**	Array<string>	Required	Результаты работы правил корреляции
_relations**{vulnerabilities}**	Array<string>	Required	Связанные уязвимости

Модель данных ServiceAssetFindingNoRelations:

Параметр	Тип данных	Обязательность	Описание
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент

Параметр	Тип данных	Обязательность	Описание
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace; - delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент

Параметр	Тип данных	Обязательность	Описание
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов

ServiceAssetFindingStatusChange

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор операции смены статуса инцидента
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
service_asset_finding_id	string	Required	Идентификатор инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
revisit_at	string	Optional	Возвращен ли статус
itsm_sync_status	string	Optional	Статус синхронизации с внешними системами. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
itsm_last_synced_at	string	Optional	Время синхронизации с внешними системами в формате date-time

Параметр	Тип данных	Обязательность	Описание
itsm_sync_error	string	Optional	Описание ошибки синхронизации
user_id	string	Required	Идентификатор пользователя

Модель данных Vulnerability

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор
created_at	string	Required	Дата создания в формате: date-time
updated_at	string	Required	Дата изменения в формате: date-time
plugin_id	integer	Optional	ID плагина
plugin_name	string	Optional	Название плагина
description	string	Optional	Описание уязвимости
severity	integer	Optional	Важность
additional_data	Array<object>	Optional	Дополнительные данные в формате map<string,string>
protocol	string	Optional	Тип протокола (tcp, udp и пр.). “-1”, если не определён
port	integer	Optional	Порт
occurrence_id	string	Optional	ID происшествия в формате uuid
synopsis	string	Optional	Краткое описание
vulnerability_host_id	string	Optional	ID хоста уязвимости
exploitable	boolean/null	Optional	Флаг возможности использования
plugin_output	string	Optional	Результат работы плагина, зависит от типа отчета (сканирования)
solution	string	Optional	Алгоритм устранения уязвимости
compare_port	integer	Optional	При создании из результата сканирования, совпадает с полем port
compare_protocol	string	Optional	При создании из результата сканирования, совпадает с полем protocol

Параметр	Тип данных	Обязательность	Описание
service_asset_id	string	Optional	ID актива
vulnerability_scan_id	string	Optional	ID результата сканирования (отчёта)
external	boolean	Optional	Флаг внешней уязвимости
remote_exploitable	boolean	Optional	Флаг возможности удалённого использования
cvss_vector	string	Optional	Вектор метрик оценки по CVSS
cvss_temporal_vector	string	Optional	Вектор временных метрик оценки по CVSS
cvss_base_score	number	Optional	Оценка уязвимости по CVSS
cvss_temporal_score	number	Optional	Временная оценка уязвимости по CVSS
risk_factor	string	Optional	Текстовая степень важности (none, low, medium и т.д.)
plugin_modification_date	string	Optional	Дата изменения плагина (не связано с изменениями в БД, заполняется из результата сканирования) в формате: date-time
publication_date	string	Optional	Дата публикации в формате: date-time

2.4.3 Создание объекта происшествия

Запрос:

Тип	Метод
POST	/occurrences/create

Описание:

При выполнении запроса будет создан объект происшествия с заданными параметрами.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/occurrences/create
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
event_type	string	Required	Тип происшествия. Допустимые значения: - manual_source - logmule_go_result - software_compliance_source - vulnerability - watchdog_result
ip	string	Required	IP-адрес актива
mac	string	Required	MAC-адрес актива
port	integer	Required	Порт
start_occurrence	string	Required	Время первого изменения статуса в клиентской системе
end_occurrence	string	Required	Время последнего изменения статуса в клиентской системе
service_asset_finding_status_change_id	string	Required	Идентификатор операции смены статуса инцидента
service_asset_finding_id	string	Required	Идентификатор инцидента
fqdn	string	Required	FQDN актива
incident_identifier	string	Required	Идентификатор инцидента во внешней системе
fincert_sync_status	number	Required	Состояние синхронизации с внешней системой
fincert_id	string	Required	Идентификатор внешней системы
sopka_sync_status	number	Required	Состояние синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)
sopka_id	string	Required	Идентификатор внешней системы реагирования на компьютерные инциденты (CERT)
fincert_sync_result	string	Required	Результат синхронизации с внешней системой
sopka_sync_result	string	Required	Результат синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)

Пример тела запроса:

```
{
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
  "end_occurrence": "2023-12-20T00:00:01.652259Z",
```

```
  "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-ee5963306be7",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "fqdn": "string",
  "incident_identifier": "string",
  "fincert_sync_status": 10,
  "fincert_id": "",
  "sopka_sync_status": 10,
  "sopka_id": "",
  "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
  "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9"
}
```


Успешный ответ:

Статус код: 201 – успешное создание объекта происшествия.

Формат: JSON.

Тело ответа: «Модель ресурса «Происшествия»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
  "end_occurrence": "2023-12-20T00:00:01.652259Z",
  "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-ee5963306be7",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "fqdn": "string",
  "incident_identifier": "string",
  "fincert_sync_status": 10,
  "fincert_id": "",
  "sopka_sync_status": 10,
  "sopka_id": "",
  "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
  "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9",
  "service_asset_finding": {
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
```

```
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  },
  "service_asset_finding_status_change": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
    "status": "string",
    "revisit_at": "string",
    "itsm_sync_status": "not_synced",
    "itsm_last_synced_at": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
  },
  "vulnerabilities": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
      "plugin_name": "string",
      "description": "string",
      "severity": 0,
      "additional_data": {},
      "protocol": "string",
      "port": 0,
      "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
      "synopsis": "string",
      "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
      "exploitable": true,
      "plugin_output": "string",
      "solution": "string",
      "compare_port": -1,
      "compare_protocol": "",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
```

```
    "external": false,
    "remote_exploitable": false,
    "cvss_vector": "string",
    "cvss_temporal_vector": "string",
    "cvss_base_score": 0,
    "cvss_temporal_score": 0,
    "risk_factor": "string",
    "plugin_modification_date": "string",
    "publication_date": "string"
  }
],
"logmule_go_result": {
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "rule_id": "uuid",
  "analysis_output": "string",
  "event": {},
  "compressed_event": "string",
  "risklevel": 5.35,
  "occurred_at": "2023-12-20T00:00:01.652259Z",
  "occurrence_id": "uuid",
  "error": "string",
  "service_asset_id": "uuid",
  "asset_info": {
    "ip": "string",
    "hostname": "string",
    "fqdn": "string",
    "mac": "string"
  },
  "incident_identifier": "string",
  "metadata": "{\"key\": \"value\"}",
  "logmule_go_rule": null,
  "occurrence": null,
  "service_asset": null,
  "service_asset_groups": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "network_ranges": [],
      "domain": "string",
      "itsm_synced": false,
      "regex": "string",
      "subject_id": "string",
      "object_id": "string",
      "is_kii": false,
      "is_fincert": false,
      "responsible_person": "string",
      "technical_specialist": "string",
      "system_id": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
    }
  ],
  "_relations": {}
},
"_relations": {
  "logmule_go_results": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "vulnerabilities": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
```

```
    ]
  }
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при создании объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.4.4 Обновление объекта происшествия

Запрос:

Тип	Метод
PUT	/domain/update

Описание:

При выполнении запроса будет обновлена информация о группе инцидентов в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля модели, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в объекте _relations отсутствуют зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются;
- Зависимости игнорируются в теле запроса;
- Зависимости в ответе всегда null.

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "logmule_go_rules": [] // - очистит все связи с правилами
    // "logmule_go_rules": ["uuid1", "uuid2"] // - создаст связь с 2 правилами
    // "logmule_go_rules": ["uuid1"] // - оставит связь только с первым правилом
  }
}
```

Пример запроса:

PUT

`http://127.0.0.1/cruddy/v2/domain/update`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор происшествия
created_at	string	Required	Дата создания происшествия в формате: date-time
updated_at	string	Required	Дата изменения происшествия в формате: date-time
event_type	string	Required	Тип происшествия. Допустимые значения: - manual_source - logmule_go_result - software_compliance_source - vulnerability - watchdog_result
ip	string	Required	IP-адрес актива
mac	string	Required	MAC-адрес актива

Параметр	Тип данных	Обязательность	Описание
port	integer	Required	Порт
start_occurrence	string	Required	Время первого изменения статуса в клиентской системе
end_occurrence	string	Required	Время последнего изменения статуса в клиентской системе
service_asset_finding_status_change_id	string	Required	Идентификатор операции смены статуса инцидента
service_asset_finding_id	string	Required	Идентификатор инцидента
fqdn	string	Required	FQDN актива
incident_identifier	string	Required	Идентификатор инцидента во внешней системе
fincert_sync_status	number	Required	Состояние синхронизации с внешней системой
fincert_id	string	Required	Идентификатор внешней системы
sopka_sync_status	number	Required	Состояние синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)
sopka_id	string	Required	Идентификатор внешней системы реагирования на компьютерные инциденты (CERT)
fincert_sync_result	string	Required	Результат синхронизации с внешней системой
sopka_sync_result	string	Required	Результат синхронизации с внешней системой реагирования на компьютерные инциденты (CERT)
_relations	object	Required	Словарь, описывающий связанные модели через идентификаторы
_relations**{logmule_go_results}**	Array<string>	Required	Результаты работы правил корреляции
_relations**{vulnerabilities}**	Array<string>	Required	Связанные уязвимости

Пример тела запроса:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
  "end_occurrence": "2023-12-20T00:00:01.652259Z",
  "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-ee5963306be7",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "fqdn": "string",
  "incident_identifier": "string",
```

```
  "fincert_sync_status": 10,
  "fincert_id": "",
  "sopka_sync_status": 10,
  "sopka_id": "",
  "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
  "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9",
  "_relations": {
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Успешный ответ:

Статус код: 200 - успешное обновление информации о происшествии.

Формат: JSON.

Тело ответа: «Модель ресурса «Происшествия»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
  "end_occurrence": "2023-12-20T00:00:01.652259Z",
  "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-ee5963306be7",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "fqdn": "string",
  "incident_identifier": "string",
  "fincert_sync_status": 10,
  "fincert_id": "",
  "sopka_sync_status": 10,
  "sopka_id": "",
  "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
  "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9",
  "service_asset_finding": {
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
```

```
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  },
  "service_asset_finding_status_change": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
    "status": "string",
    "revisit_at": "string",
    "itsm_sync_status": "not_synced",
    "itsm_last_synced_at": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
  },
  "vulnerabilities": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
      "plugin_name": "string",
      "description": "string",
      "severity": 0,
      "additional_data": {},
      "protocol": "string",
      "port": 0,
      "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
      "synopsis": "string",
      "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
      "exploitable": true,
```

```
      "plugin_output": "string",
      "solution": "string",
      "compare_port": -1,
      "compare_protocol": "",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "external": false,
      "remote_exploitable": false,
      "cvss_vector": "string",
      "cvss_temporal_vector": "string",
      "cvss_base_score": 0,
      "cvss_temporal_score": 0,
      "risk_factor": "string",
      "plugin_modification_date": "string",
      "publication_date": "string"
    }
  ],
  "logmule_go_result": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "rule_id": "uuid",
    "analysis_output": "string",
    "event": {},
    "compressed_event": "string",
    "risklevel": 5.35,
    "occurred_at": "2023-12-20T00:00:01.652259Z",
    "occurrence_id": "uuid",
    "error": "string",
    "service_asset_id": "uuid",
    "asset_info": {
      "ip": "string",
      "hostname": "string",
      "fqdn": "string",
      "mac": "string"
    },
    "incident_identifier": "string",
    "metadata": "{\"key\": \"value\"}",
    "logmule_go_rule": null,
    "occurrence": null,
    "service_asset": null,
    "service_asset_groups": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "network_ranges": [],
        "domain": "string",
        "itsm_synced": false,
        "regex": "string",
        "subject_id": "string",
        "object_id": "string",
        "is_kii": false,
        "is_fincert": false,
        "responsible_person": "string",
        "technical_specialist": "string",
        "system_id": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      }
    ],
    "_relations": {}
  },
```

```
  "_relations": {
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 404:


```
{
  "error": "Not Found",
  "error_code": 404
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.4.5 Поиск происшествий

Запрос:

Тип	Метод
POST	/occurrences/search

Описание:

При выполнении запроса будут возвращены найденные происшествия с учётом заданных фильтров.

По умолчанию в объекты не загружаются связанные модели по типам связи many2many и has-many, для включения загрузки их нужно указывать в поле relations объекта запроса.

Есть возможность расширить ответ информацией об идентификаторах связанных сущностей, возвращаемых в поле _relations, для этого необходимо и одноименном поле запроса передать список связанных моделей.

Поле _relations запроса расширяет поле relations для связей кроме один-к-одному, т.е. сущности, указанные в последнем поле, появятся в ответе в поле _relations в любом случае.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/occurrences/search
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений - substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят связанность с моделью по идентификатору если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
```

```
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "virtual_search": {
    "value": "string",
    "strict": false
  },
  "relations": [
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array<Occurrence>	Список найденных происшествий
total	integer	Количество найденных происшествий

Пример ответа:

```
{
  "items": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "event_type": "manual_source",
```

```
      "ip": "string",
      "mac": "string",
      "port": 0,
      "start_occurrence": "2023-12-20T00:00:01.652259Z",
      "end_occurrence": "2023-12-20T00:00:01.652259Z",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "fqdn": "string",
      "incident_identifier": "string",
      "fincert_sync_status": 10,
      "fincert_id": "",
      "sopka_sync_status": 10,
      "sopka_id": "",
      "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
      "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9",
      "service_asset_finding": {
        "description": "string",
        "risk_impact": "string",
        "solution": "string",
        "mitigation": "string",
        "status": "assigned_customer",
        "risklevel": 0,
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
        "analysis_output": "string",
        "synopsis": "string",
        "title": "string",
        "risk": "none",
        "acknowledged_at": "2023-12-20T00:00:01.652259Z",
        "alert_type": "automatic",
        "client_note": "string",
        "internal_note": "string",
        "external": false,
        "immediate_action_score": 0,
        "throughput_period": "grace",
        "throughput_period_change": "2023-12-20T00:00:01.652259Z",
        "customer_created": false,
        "c_visible_since": "2023-12-20T00:00:01.652259Z",
        "c_visible_since_in_days": 0,
        "c_reopened_count": 0,
        "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
        "logmule_identifier": "string",
        "c_remote_exploitable": true,
        "c_occurrence_count": 0,
        "c_customer_retention_time": 0,
        "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
        "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
        "itsm_sync_status": "scheduled",
        "external_id": "string",
        "itsm_sync_error": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
        "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
        "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
        "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
        "reopened_at": "2023-12-20T00:00:01.652259Z",
        "display_id": 0
      },
      "service_asset_finding_status_change": {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
```

```
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
    "status": "string",
    "revisit_at": "string",
    "itsm_sync_status": "not_synced",
    "itsm_last_synced_at": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
  },
  "vulnerabilities": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
      "plugin_name": "string",
      "description": "string",
      "severity": 0,
      "additional_data": {},
      "protocol": "string",
      "port": 0,
      "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
      "synopsis": "string",
      "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
      "exploitable": true,
      "plugin_output": "string",
      "solution": "string",
      "compare_port": -1,
      "compare_protocol": "",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "external": false,
      "remote_exploitable": false,
      "cvss_vector": "string",
      "cvss_temporal_vector": "string",
      "cvss_base_score": 0,
      "cvss_temporal_score": 0,
      "risk_factor": "string",
      "plugin_modification_date": "string",
      "publication_date": "string"
    }
  ],
  "logmule_go_result": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "rule_id": "uuid",
    "analysis_output": "string",
    "event": {},
    "compressed_event": "string",
    "risklevel": 5.35,
    "occurred_at": "2023-12-20T00:00:01.652259Z",
    "occurrence_id": "uuid",
    "error": "string",
    "service_asset_id": "uuid",
    "asset_info": {
      "ip": "string",
      "hostname": "string",
      "fqdn": "string",
      "mac": "string"
    },
    "incident_identifier": "string",
    "metadata": "{\"key\": \"value\"}",
    "logmule_go_rule": null,
```

```
        "occurrence": null,
        "service_asset": null,
        "service_asset_groups": [
          {
            "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
            "created_at": "2023-12-20T00:00:01.652259Z",
            "updated_at": "2023-12-20T00:00:01.652259Z",
            "name": "string",
            "network_ranges": [],
            "domain": "string",
            "itsm_synced": false,
            "regex": "string",
            "subject_id": "string",
            "object_id": "string",
            "is_kii": false,
            "is_fincert": false,
            "responsible_person": "string",
            "technical_specialist": "string",
            "system_id": "string",
            "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
            "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
          }
        ],
        "_relations": {}
      },
      "_relations": {
        "logmule_go_results": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "vulnerabilities": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "total": 1
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.4.6 Получение происшествия по ID

Запрос:

Тип	Метод
GET	/occurrences/{id}

Описание:

При выполнении запроса будет возвращено происшествие с соответствующим ID.

Если не указан параметр relations, то подгружаются все связи объекта. Если параметр указан, но не имеет значений - связи не подгружаются. Если параметр указан и содержит значения (поля модели хранящие связанные сущности), то они будут заполнены в ответе.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/occurrences/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор происшествия

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Происшествия»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "event_type": "manual_source",
  "ip": "string",
  "mac": "string",
  "port": 0,
  "start_occurrence": "2023-12-20T00:00:01.652259Z",
  "end_occurrence": "2023-12-20T00:00:01.652259Z",
  "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-ee5963306be7",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "fqdn": "string",
  "incident_identifier": "string",
  "fincert_sync_status": 10,
  "fincert_id": "",
  "sopka_sync_status": 10,
  "sopka_id": "",
  "fincert_sync_result": "7325f612-d464-4395-bb86-c83b3b6893fb",
  "sopka_sync_result": "d91aad7a-d9ad-4941-bf19-b94f42afada9",
  "service_asset_finding": {
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
```

```
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  },
  "service_asset_finding_status_change": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
    "status": "string",
    "revisit_at": "string",
    "itsm_sync_status": "not_synced",
    "itsm_last_synced_at": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5"
  },
  "vulnerabilities": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
      "plugin_name": "string",
      "description": "string",
      "severity": 0,
      "additional_data": {},
      "protocol": "string",
      "port": 0,
      "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
      "synopsis": "string",
      "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
      "exploitable": true,
      "plugin_output": "string",
      "solution": "string",
      "compare_port": -1,
      "compare_protocol": "",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "external": false,
      "remote_exploitable": false,
      "cvss_vector": "string",
      "cvss_temporal_vector": "string",
      "cvss_base_score": 0,
      "cvss_temporal_score": 0,
      "risk_factor": "string",
      "plugin_modification_date": "string",
      "publication_date": "string"
    }
  ],
  "logmule_go_result": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "rule_id": "uuid",
    "analysis_output": "string",
    "event": {},
    "compressed_event": "string",
    "risklevel": 5.35,
    "occurred_at": "2023-12-20T00:00:01.652259Z",
```

```
    "occurrence_id": "uuid",
    "error": "string",
    "service_asset_id": "uuid",
    "asset_info": {
      "ip": "string",
      "hostname": "string",
      "fqdn": "string",
      "mac": "string"
    },
    "incident_identifier": "string",
    "metadata": "{\"key\": \"value\"}",
    "logmule_go_rule": null,
    "occurrence": null,
    "service_asset": null,
    "service_asset_groups": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "network_ranges": [],
        "domain": "string",
        "itsm_synced": false,
        "regex": "string",
        "subject_id": "string",
        "object_id": "string",
        "is_kii": false,
        "is_fincert": false,
        "responsible_person": "string",
        "technical_specialist": "string",
        "system_id": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      }
    ],
    "_relations": {}
  },
  "_relations": {
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.4.7 Удаление объекта происшествия

Запрос:

Тип	Метод
DELETE	/occurrences/{id}

Описание:

При выполнении запроса будет удален объект происшествия с соответствующим ID.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/occurrences/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор происшествия

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
422	11002 11003 11004 11011	Общая ошибка удаления Запрос не затронул ни одной сущности Удаляемая модель не найдена Удаление невозможно из-за наличия блокирующих связей
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404

}
```

Код 422:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.4.8 Группировка происшествий

Запрос:

Тип	Метод
POST	/occurrences/group

Описание:

При выполнении запроса происшествия будут сгруппированы по заданному полю.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/occurrences/group
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки происшествий

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.4.9 Массовое удаление происшествий

Запрос:

Тип	Метод
POST	/occurrences/mass_delete

Описание:

При выполнении запроса будут удалены происшествия с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/occurrences/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности.

Пример ответа:

```
{
  "results": [
    {
      "id": "string",
      "error_code": 11001
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.4.10 Удаление всех происшествий

Запрос:

Тип	Метод
DELETE	/occurrences/all

Описание:

При выполнении запроса из базы данных будут удалены все происшествия.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/occurrences/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
422	11001 11012 11003	Ошибка связанных данных (зависимости) Ошибка некорректно настроенных связей (отсутствие on cascade и пр.) Запрос на изменение не затронул ни одной строки
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 422:

```
{
  "error_code": "11001 // ошибка связанных данных (зависимости)",
  "relations": {
    "dynamic_relation_name": [
      {
```

```
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.4.11 Получение свойств происшествий и действий пользователей

Запрос:

Тип	Метод
GET	/domain/_meta

Описание:

При выполнении запроса будут возвращены свойства полей происшествия и список действий пользователей над ними в интерфейсе платформы.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/domain/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса

Параметр	Тип данных	Описание
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:


```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5 Дополнительные поля

2.5.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	custom_fields
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	Ресурс custom_fields отвечает за управление дополнительными полями, которые можно добавлять к инцидентам информационной безопасности

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/custom_fields/create	Создание дополнительного поля
PUT	/custom_fields/update	Обновление информации о дополнительном поле
POST	/custom_fields/search	Поиск дополнительных полей
GET	/custom_fields/{id}	Получение объекта по ID
DELETE	/custom_fields/{id}	Удаление объекта
POST	/custom_fields/group	Группировка объектов по заданному полю
POST	/custom_fields/mass_delete	Удаление объектов по списку ID
DELETE	/custom_fields/all	Удаление всех объектов в таблице БД
GET	/custom_fields/_meta	Получение свойств полей в UI и кастомных действий

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
409	Попытка создать объект с существующим уникальным атрибутом
422	Другие ошибки удаления
500	Ошибка сервера

Модели объектов:

Название	Описание
CustomFields	Модель данных ресурса custom_fields

2.5.2 Модель ресурса «Дополнительные поля»

Модель данных CustomField

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор дополнительного поля
created_at	string	Required	Дата создания
updated_at	string	Required	Дата изменения
field_key	string	Required	Уникальный ключ поля
title	string	Required	Наименование дополнительного поля

Параметр	Тип данных	Обязательность	Описание
field_type	string	Required	Тип данных, указываемый в дополнительном поле, например: - boolean; - json; - string; - integer; - double; - date.
order_direction	integer	Required	Порядок отображения дополнительного поля в карточке инцидента
custom_field_values	array_of<object>	Optional	Значения дополнительного поля
_relations	object	Optional	Словарь, описывающий связанные модели через идентификаторы: отношение значений дополнительного поля (ключ) к идентификатору дополнительного поля (значение)
_relations{custom_field_values}	Array<string>	Optional	Список идентификаторов связанных значений дополнительного поля

Модель данных CustomFieldValues

Параметр	Тип данных	Обязательность	Описание
custom_field_id	string	Optional	Идентификатор значения дополнительного поля
service_asset_finding_id	string	Optional	Идентификатор инцидента, в которое добавлено дополнительное поле
string_value	string	Optional	Значение дополнительного поля с типом данных "строка"
integer_value	integer	Optional	Значение дополнительного поля с типом данных "целое число"
float_value	number	Optional	Значение дополнительного поля с типом данных "число с плавающей запятой"
date_value	date	Optional	Значение дополнительного поля с типом данных "дата"
json_value	string	Optional	Значение дополнительного поля с типом данных "JSON"
boolean_value	boolean	Optional	Значение дополнительного поля с типом данных "логический"

2.5.3 Создание дополнительного поля

Запрос:

Тип	Метод
POST	/custom_fields/create

Описание:

При выполнении запроса будет создано дополнительное поле с заданными параметрами.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/custom_fields/create`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
field_key	string	Required	Уникальный ключ поля
title	string	Required	Наименование дополнительного поля
field_type	string	Required	Тип данных, указываемый в дополнительном поле
order_direction	integer	Required	Порядок отображения дополнительного поля в карточке инцидента

Пример тела запроса:

```
{
"field_key": "string",
"title": "string",
"field_type": "string",
"order_direction": 0
}
```

Успешный ответ:

Статус код: 201 – успешное создание дополнительного поля.

Формат: JSON.

Тело ответа: «Модель ресурса «Дополнительные поля»».

Пример ответа:

```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
```

```
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "field_key": "string",
  "title": "string",
  "field_type": "string",
  "order_direction": 0,
  "custom_field_values": [
    {
      "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "string_value": "string",
      "integer_value": 0,
      "float_value": 0,
      "date_value": "2023-12-20T00:00:01.652259Z",
      "json_value": {},
      "boolean_value": true
    }
  ],
  "_relations": {
    "custom_field_values": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
409	name_already_used	Попытка присвоить объекту существующее уникальное значение атрибута
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 409:


```
{
  "error": "Bad Request",
  "error_code": 409,
  "extra": {
    "fields": [
      "name"
    ]
  }
}
```


Код 500:


```
{
```

```
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.4 Обновление дополнительного поля

Запрос:

Тип	Метод
PUT	/custom_fields/update

Описание:

При выполнении запроса будет обновлена информация о дополнительном поле в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля модели, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в объекте _relations отсутствуют зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются;
- Зависимости игнорируются в теле запроса;
- Зависимости в ответе всегда null.

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "logmule_go_rules": [] // - очистит все связи с правилами
    // "logmule_go_rules": ["uuid1", "uuid2"] // - создаст связь с 2 правилами
    // "logmule_go_rules": ["uuid1"] // - оставит связь только с первым правилом
  }
}
```

Пример запроса:

PUT

`http://127.0.0.1/cruddy/v2/custom_fields/update`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор дополнительного поля
created_at	string	Required	Дата создания
updated_at	string	Required	Дата изменения
field_key	string	Required	Уникальный ключ поля
title	string	Required	Наименование дополнительного поля
field_type	string	Required	Тип данных, указываемый в дополнительном поле, например: - boolean; - json; - string; - integer; - double; - date.
order_direction	integer	Required	Порядок отображения дополнительного поля в карточке инцидента

Пример тела запроса:

```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "field_key": "string",
  "title": "string",
  "field_type": "string",
  "order_direction": 0
}
```

Успешный ответ:

Статус код: 200 - успешное обновление информации о дополнительном поле.

Формат: JSON.

Тело ответа: «Модель ресурса «Дополнительные поля»».

Пример ответа:


```
{
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "field_key": "string",
  "title": "string",
  "field_type": "string",
  "order_direction": 0,
  "custom_field_values": [
    {
      "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "string_value": "string",
      "integer_value": 0,
      "float_value": 0,
      "date_value": "2023-12-20T00:00:01.652259Z",
      "json_value": {},
      "boolean_value": true
    }
  ],
  "_relations": {
    "custom_field_values": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
409	name_already_used	Попытка присвоить объекту существующее уникальное значение атрибута
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
```

```
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 409:

```
{
  "error": "Bad Request",
  "error_code": 409,
  "extra": {
    "fields": [
      "name"
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.5 Поиск дополнительных полей

Запрос:

Тип	Метод
POST	/custom_fields/search

Описание:

При выполнении запроса будут возвращены найденные объекты с учётом заданных фильтров.

По умолчанию в объекты не загружаются связанные модели по типам связи many2many и has-many, для включения загрузки их нужно указывать в поле relations объекта запроса.

Связи _relations загружаются всегда и отражают текущее состояние связей модели.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/custom_fields/search
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений - substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят связанность с моделью по идентификатору если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "virtual_search": {
    "value": "string",
    "strict": false
  },
  "relations": [
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
```

```
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array <CustomField>	Список найденных дополнительных полей
total	integer	Количество найденных дополнительных полей

Пример ответа:


```
{
  "items": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "field_key": "string",
      "title": "string",
      "field_type": "string",
      "order_direction": 0,
      "custom_field_values": [
        {
          "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
          "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
          "string_value": "string",
          "integer_value": 0,
          "float_value": 0,
          "date_value": "2023-12-20T00:00:01.652259Z",
          "json_value": {},
          "boolean_value": true
        }
      ],
      "_relations": {
        "custom_field_values": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      }
    }
  ],
  "total": 1
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.6 Получение дополнительного поля по ID

Запрос:

Тип	Метод
GET	/custom_fields/{id}

Описание:

При выполнении запроса будет возвращено дополнительное поле с соответствующим ID.

Если не указан параметр relations, то подгружаются все связи объекта. Если параметр указан, но не имеет значений - связи не подгружаются. Если параметр указан и содержит значения (поля модели хранящие связанные сущности), то они будут заполнены в ответе.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/custom_fields/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор дополнительного поля

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Дополнительные поля»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "field_key": "string",
  "title": "string",
  "field_type": "string",
  "order_direction": 0,
  "custom_field_values": [
    {
      "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "string_value": "string",
      "integer_value": 0,
      "float_value": 0,
      "date_value": "2023-12-20T00:00:01.652259Z",
      "json_value": {},
      "boolean_value": true
    }
  ],
  "_relations": {
    "custom_field_values": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.7 Удаление дополнительного поля

Запрос:

Тип	Метод
DELETE	/custom_fields/{id}

Описание:

При выполнении запроса будет удален объект происшествия с соответствующим ID.

Пример запроса:

DELETE

`http://127.0.0.1/cruddy/v2/custom_fields/{id}`

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор дополнительного поля

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
422	11002 11003 11004 11011	Общая ошибка удаления Запрос не затронул ни одной сущности Удаляемая модель не найдена Удаление невозможно из-за наличия блокирующих связей
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 422:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.8 Группировка дополнительных полей

Запрос:

Тип	Метод
POST	/custom_fields/group

Описание:

При выполнении запроса дополнительные поля будут сгруппированы по заданному полю.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/custom_fields/group
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки объектов

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.9 Массовое удаление дополнительных полей

Запрос:

Тип	Метод
POST	/custom_fields/mass_delete

Описание:

При выполнении запроса будут удалены дополнительные поля с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/custom_fields/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности.

Пример ответа:

```
{
  "results": [
    {
      "id": "string",
      "error_code": 11001
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
```

```
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.10 Удаление всех дополнительных полей

Запрос:

Тип	Метод
DELETE	/custom_fields/all

Описание:

При выполнении запроса из базы данных будут удалены все дополнительные поля.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/custom_fields/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
422	11001 11012 11003	Ошибка связанных данных (зависимости) Ошибка некорректно настроенных связей (отсутствие on cascade и пр.) Запрос на изменение не затронул ни одной строки
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 422:

```
{
```

```
  "error_code": "11001 // ошибка связанных данных (зависимости)",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.5.11 Получение свойств полей и списка действий пользователей

Запрос:

Тип	Метод
GET	/custom_fields/_meta

Описание:

При выполнении запроса будут возвращены свойства дополнительных полей и список действий пользователей над ними.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/custom_fields/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:


```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
}
```


Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.6 Значения дополнительных полей

2.6.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	custom_fields_values
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	Ресурс custom_fields_values отвечает за управление значениями, которые указываются в дополнительных полях инцидента.

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/custom_field_values/create	Создание значения дополнительного поля
PUT	/custom_field_values/update	Обновление информации о значении дополнительного поля
POST	/custom_field_values/search	Поиск значений дополнительных полей
GET	/custom_field_values/{id}	Получение значения дополнительного поля
DELETE	/custom_field_values/{id}	Удаление значения дополнительного поля
POST	/custom_field_values/group	Группировка значений дополнительного поля
POST	/custom_field_values/mass_delete	Массовое удаление значений дополнительного поля
DELETE	/custom_field_values/all	Удаление всех значений дополнительного поля
GET	/custom_field_values/_meta	Получение свойств полей и списка действий пользователя в интерфейсе

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
422	Другие ошибки удаления
500	Ошибка сервера

Модели объектов:

Название	Описание
CustomFieldValue	Модель данных ресурса custom_fields_values

2.6.2 Модель ресурса «Значения дополнительных полей»

Модель данных CustomFieldValue:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор значения дополнительного поля
created_at	string	Required	Дата создания
updated_at	string	Required	Дата изменения
custom_field_id	string	Optional	Идентификатор значения дополнительного поля
service_asset_finding_id	string	Optional	Идентификатор инцидента, в которое добавлено дополнительное поле
string_value	string	Optional	Значение дополнительного поля с типом данных "строка"

Параметр	Тип данных	Обязательность	Описание
integer_value	integer	Optional	Значение дополнительного поля с типом данных "целое число"
float_value	number	Optional	Значение дополнительного поля с типом данных "число с плавающей запятой"
date_value	date	Optional	Значение дополнительного поля с типом данных "дата"
json_value	string	Optional	Значение дополнительного поля с типом данных "JSON"
boolean_value	boolean	Optional	Значение дополнительного поля с типом данных "логический"
custom_field	array_of<object>	Required	Параметры дополнительного поля
service_asset_finding	array_of<object>	Required	Параметры инцидента

Модель данных CustomField

Параметр	Тип данных	Обязательность	Описание
field_key	string	Required	Уникальный ключ поля
title	string	Required	Наименование дополнительного поля
field_type	string	Required	Тип данных, указываемый в дополнительном поле, например: - boolean; - json; - string; - integer; - double; - date.
order_direction	integer	Required	Порядок отображения дополнительного поля в карточке инцидента

Модель данных ServiceAssetFinding

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор инцидента
created_at	string time	Required	Дата создания в формате: date-time
updated_at	string time	Required	Дата изменения в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита

Параметр	Тип данных	Обязательность	Описание
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace;

Параметр	Тип данных	Обязательность	Описание
			- delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную

Параметр	Тип данных	Обязательность	Описание
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов

2.6.3 Создание значения дополнительного поля

Запрос:

Тип	Метод
POST	/custom_field_values/create

Описание:

При выполнении запроса будет создано значение дополнительного поля с заданными параметрами для выбранного дополнительного поля.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/custom_field_values/create
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
custom_field_id	string	Optional	Идентификатор значения дополнительного поля
service_asset_finding_id	string	Optional	Идентификатор инцидента, в которое добавлено дополнительное поле
string_value	string	Optional	Значение дополнительного поля с типом данных "строка"
integer_value	integer	Optional	Значение дополнительного поля с типом данных "целое число"
float_value	number	Optional	Значение дополнительного поля с типом данных "число с плавающей запятой"
date_value	date	Optional	Значение дополнительного поля с типом данных "дата"

Параметр	Тип данных	Обязательность	Описание
json_value	string	Optional	Значение дополнительного поля с типом данных "JSON"
boolean_value	boolean	Optional	Значение дополнительного поля с типом данных "логический"

Пример тела запроса:

```
{
  "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "string_value": "string",
  "integer_value": 0,
  "float_value": 0,
  "date_value": "2023-12-20T00:00:01.652259Z",
  "json_value": {},
  "boolean_value": true
}
```

Успешный ответ:

Статус код: 201 – успешное создание значения дополнительного поля.

Формат: JSON.

Тело ответа: «Модель ресурса «Значения дополнительных полей»».

Пример ответа:

```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "string_value": "string",
  "integer_value": 0,
  "float_value": 0,
  "date_value": "2023-12-20T00:00:01.652259Z",
  "json_value": {},
  "boolean_value": true,
  "custom_field": {
    "field_key": "string",
    "title": "string",
    "field_type": "string",
    "order_direction": 0
  },
  "service_asset_finding": {
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
```

```
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.6.4 Обновление значения дополнительного поля

Запрос:

Тип	Метод
PUT	/custom_field_values/update

Описание:

При выполнении запроса будет обновлена информация о значении дополнительного поля в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля модели, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в объекте _relations отсутствуют зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются;
- Зависимости игнорируются в теле запроса;
- Зависимости в ответе всегда null.

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "logmule_go_rules": [] // - очистит все связи с правилами
    // "logmule_go_rules": ["uuid1", "uuid2"] // - создаст связь с 2 правилами
    // "logmule_go_rules": ["uuid1"] // - оставит связь только с первым правилом
  }
}
```

Пример запроса:

PUT

`http://127.0.0.1/cruddy/v2/custom_field_values/update`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор значения дополнительного поля
created_at	string	Required	Дата создания
updated_at	string	Required	Дата изменения
custom_field_id	string	Optional	Идентификатор значения дополнительного поля
service_asset_finding_id	string	Optional	Идентификатор инцидента, в которое добавлено дополнительное поле
string_value	string	Optional	Значение дополнительного поля с типом данных "строка"
integer_value	integer	Optional	Значение дополнительного поля с типом данных "целое число"
float_value	number	Optional	Значение дополнительного поля с типом данных "число с плавающей запятой"
date_value	date	Optional	Значение дополнительного поля с типом данных "дата"
json_value	string	Optional	Значение дополнительного поля с типом данных "JSON"
boolean_value	boolean	Optional	Значение дополнительного поля с типом данных "логический"

Пример тела запроса:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "string_value": "string",
  "integer_value": 0,
  "float_value": 0,
  "date_value": "2023-12-20T00:00:01.652259Z",
  "json_value": {},
  "boolean_value": true
}
```

Успешный ответ:

Статус код: 200 - успешное обновление информации о значении дополнительного поля.

Формат: JSON.

Тело ответа: «Модель ресурса «Значения дополнительных полей»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "string_value": "string",
  "integer_value": 0,
  "float_value": 0,
  "date_value": "2023-12-20T00:00:01.652259Z",
  "json_value": {},
  "boolean_value": true,
  "custom_field": {
    "field_key": "string",
    "title": "string",
    "field_type": "string",
    "order_direction": 0
  },
  "service_asset_finding": {
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
```

```
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 404:


```
{
  "error": "Not Found",
  "error_code": 404
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.6.5 Поиск значений дополнительных полей

Запрос:

Тип	Метод
POST	/custom_field_values/search

Описание:

При выполнении запроса будут возвращены найденные объекты с учётом заданных фильтров.

По умолчанию в объекты не загружаются связанные модели по типам связи many2many и has-many, для включения загрузки их нужно указывать в поле relations объекта запроса.

Есть возможность расширить ответ информацией об идентификаторах связанных сущностей, возвращаемых в поле _relations, для этого необходимо и одноименном поле запроса передать список связанных моделей.

Поле _relations запроса расширяет поле relations для связей кроме один-к-одному, т.е. сущности, указанные в последнем поле, появятся в ответе в поле _relations в любом случае.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/custom_field_values/search
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов

Параметр	Тип данных	Обязательность	Описание
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений - substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят связанность с моделью по идентификатору если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
```

```
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "virtual_search": {
    "value": "string",
    "strict": false
  },
  "relations": [
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array <CustomFieldValue>	Список найденных значений дополнительных полей
total	integer	Количество найденных значений дополнительных полей

Пример ответа:


```
{
  "items": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "string_value": "string",
      "integer_value": 0,
      "float_value": 0,
      "date_value": "2023-12-20T00:00:01.652259Z",
      "json_value": {},
      "boolean_value": true,
      "custom_field": {
        "field_key": "string",
        "title": "string",
        "field_type": "string",
        "order_direction": 0
      },
      "service_asset_finding": {
        "description": "string",
        "risk_impact": "string",
        "solution": "string",
        "mitigation": "string",
        "status": "assigned_customer",
        "risklevel": 0,
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
        "analysis_output": "string",
        "synopsis": "string",
        "title": "string",
        "risk": "none",
        "acknowledged_at": "2023-12-20T00:00:01.652259Z",
        "alert_type": "automatic",
        "client_note": "string",
        "internal_note": "string",
        "external": false,
        "immediate_action_score": 0,
        "throughput_period": "grace",
        "throughput_period_change": "2023-12-20T00:00:01.652259Z",
        "customer_created": false,
        "c_visible_since": "2023-12-20T00:00:01.652259Z",
        "c_visible_since_in_days": 0,
        "c_reopened_count": 0,
        "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
        "logmule_identifier": "string",
        "c_remote_exploitable": true,
        "c_occurrence_count": 0,
        "c_customer_retention_time": 0,
        "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
        "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
        "itsm_sync_status": "scheduled",
        "external_id": "string",
        "itsm_sync_error": "string",
        "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
        "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
        "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
        "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
        "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
```

```
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
        "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
        "reopened_at": "2023-12-20T00:00:01.652259Z",
        "display_id": 0
      }
    }
  ],
  "total": 1
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```


2.6.6 Получение значения дополнительного поля по ID

Запрос:

Тип	Метод
GET	/custom_field_values/{id}

Описание:

При выполнении запроса будет возвращено значение дополнительного поля с соответствующим ID.

Пример запроса:

GET

`http://127.0.0.1/cruddy/v2/custom_field_values/{id}`

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор значения дополнительного поля

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Значения дополнительных полей»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "custom_field_id": "a0fa4fc5-cabd-4219-9751-6d126c809065",
  "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
  "string_value": "string",
  "integer_value": 0,
  "float_value": 0,
  "date_value": "2023-12-20T00:00:01.652259Z",
  "json_value": {},
  "boolean_value": true,
  "custom_field": {
    "field_key": "string",
    "title": "string",
    "field_type": "string",
    "order_direction": 0
  },
  "service_asset_finding": {
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
```

```
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  }
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.6.7 Удаление значения дополнительного поля

Запрос:

Тип	Метод
DELETE	/custom_field_values/{id}

Описание:

При выполнении запроса будет удалено значение дополнительного поля с соответствующим ID.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/custom_field_values/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор значения дополнительного поля

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
422	11002 11003 11004 11011	Общая ошибка удаления Запрос не затронул ни одной сущности Удаляемая модель не найдена Удаление невозможно из-за наличия блокирующих связей
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 422:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.6.8 Группировка значений дополнительных полей

Запрос:

Тип	Метод
POST	/custom_field_values/group

Описание:

При выполнении запроса значения дополнительного поля будут сгруппированы по заданному полю.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/custom_field_values/group
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки объектов

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.6.9 Массовое удаление значений дополнительного поля

Запрос:

Тип	Метод
POST	/custom_field_values/mass_delete

Описание:

При выполнении запроса будут удалены дополнительные поля с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/custom_field_values/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам

Параметр	Тип данных	Описание
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности.

Пример ответа:

```
{
  "results": [
    {
      "id": "string",
      "error_code": 11001
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.6.10 Удаление всех значений дополнительного поля

Запрос:

Тип	Метод
DELETE	/custom_field_values/all

Описание:

При выполнении запроса из базы данных будут удалены все значения всех дополнительных полей.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/custom_field_values/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
422	11001 11012 11003	Ошибка связанных данных (зависимости) Ошибка некорректно настроенных связей (отсутствие on cascade и пр.) Запрос на изменение не затронул ни одной строки
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 422:

```
{
  "error_code": "11001 // ошибка связанных данных (зависимости)",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
```

```
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

2.6.11 Получение свойств значений дополнительных полей и действий пользователей

Запрос:

Тип	Метод
GET	/custom_field_values/_meta

Описание:

При выполнении запроса будут возвращены свойства значений дополнительных полей и список действий пользователей над ними.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/custom_field_values/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса

Параметр	Тип данных	Описание
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:

```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3. Активы

3.1 Активы

3.1.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	service_assets
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	Ресурс service_assets отвечает за управление информацией об активах.

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/service_assets/create	Создание актива
PUT	/service_assets/update	Обновление актива
POST	/service_assets/search	Поиск активов
GET	/service_assets/{id}	Получение актива по ID
DELETE	/service_assets/{id}	Удаление актива
POST	/service_assets/group	Группировка активов
POST	/service_assets/mass_delete	Массовое удаление активов

Тип	Метод	Описание
DELETE	/service_assets/all	Удаление всех активов
GET	/service_assets/_meta	Получение свойств полей активов и действий пользователей
POST	/service_assets/merge	Скомпоновать несколько активов в один

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
409	Попытка создать объект с существующим уникальным атрибутом
422	Другие ошибки удаления
500	Ошибка сервера

Модели объектов:

Название	Описание
ServiceAssets	Модель данных ресурса service_assets

3.1.2 Модель ресурса «Активы»

Модель данных ServiceAsset

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор актива

Параметр	Тип данных	Обязательность	Описание
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
type	string	Required	Тип актива
name	string	Required	Название актива
description	string	Optional	Описание актива
coordinates	string	Optional	Координаты актива (не используется)
active	boolean	Optional	Флаг активности
scan_id	string	Optional	ID сканера активов (не используется)
value	integer	Optional	Значимость актива. В платформе значимость актива может принимать следующие значения: - 1 – ключевой; - 2 – важный; - 3 – некритичный; - 4 – распределенный; - 5 – тестовый.
client_note	string	Optional	Клиентские заметки (не используется)
internal_note	string	Optional	Внутренние заметки (не используется)
location	string	Required	Расположение актива
network_exposure	integer	Optional	Сетевая доступность актива. Тип сетевой видимости актива может принимать следующие значения: - 1 – актив напрямую подключен к сети Интернет; - 2 – актив располагается в демилитаризованной зоне (DMZ); - 3 – актив подключен к сети Интернет через Proxy-сервер; - 4 – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы; - 5 – актив не подключен к сети.
responsible_person	string	Optional	Ответственное лицо
technical_specialist	string	Optional	Технический специалист
responsible_group_id	string	Optional	ID группы ответственных
edited_by	string	Optional	Кем изменён (не используется)
hardware_informations	Array<HardwareInformation>	Optional	Связанная информация по аппаратному обеспечению

Параметр	Тип данных	Обязательность	Описание
logmule_go_results	Array<LogmuleGoResult>	Optional	Связанные результаты сработки
messages	Array<Message>	Optional	Связанные сообщения пользователей
network_interfaces	Array<Network_interfaces>	Optional	Связанные сетевые интерфейсы
service_asset_findings	Array<Service_asset_finding>	Optional	Связанные инциденты
service_asset_groups	Array<Service_asset_group>	Optional	Связанные группы активов
software	Array<Software>	Optional	Связанное ПО
vulnerabilities	Array<Vulnerability>	Optional	Связанные уязвимости
vulnerability_hosts	Array<Vulnerability_host>	Optional	Связанные уязвимые хосты
responsible_group	object<ResponsibleGroup>	Optional	Группа ответственных пользователей
_relations	object<relations>	Optional	Словарь идентификаторов связанных объектов
is_local	boolean	Optional	Флаг, является ли актив локальным
risk	string	Optional	Словесное описание критичности риска (вычисляется по связанным инцидентам). Доступные значения: - none - low - medium - high
risklevel	number	Optional	Числовое выражение критичности риска (вычисляется по связанным инцидентам)
mac_ip	object<mac_ip>	Optional	Список объектов, описывающих IP и MAC связанных сетевых интерфейсов
os_list	Array<string>	Optional	Список ОС, установленных на связанных сетевых интерфейсах
responsible_group_name	string	Optional	Название группы ответственных пользователей
closed_count	number	Optional	Кол-во закрытых инцидентов
risk_accepted_count	number	Optional	Кол-во инцидентов со статусом “Риск принят”
all_open_count	number	Optional	Кол-во открытых инцидентов
last_scan	string	Optional	Дата и время последнего сканирования актива в формате date-time
authenticated	boolean	Optional	Признак использования аутентификации при сканировании
authentication_info	object	Optional	Объект, содержащий метаинформацию об аутентификации при сканировании

Параметр	Тип данных	Обязательность	Описание
network_interface_ids	Array<string>	Optional	Список идентификаторов связанных сетевых интерфейсов

Модель данных Hardware_Information

Параметр	Тип данных	Обязательность	Описание
hardware_type	string	Optional	Тип аппаратного обеспечения
name	string	Optional	Наименование аппаратного обеспечение
manufacturer	string	Optional	Производитель
serial_number	string	Optional	Серийный номер
additional_info	string	Optional	Дополнительные сведения
is_old	boolean	Optional	Флаг, устаревшая ли информация о состоянии аппаратного обеспечения

Модель данных LogmuleGoResult

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор результата сработки парвила
created_at	string time	Required	Дата создания результата сработки в формате: date-time
updated_at	string time	Required	Дата изменения результата сработки в формате: date-time
rule_id	string	Required	Идентификатор правила
analysis_output	string	Required	Результат анализа
event	object	Required	Событие строкой
compressed_event	string array	Required	Событие одной строкой в формате byte array
risklevel	number float	Required	Уровень риска в формате float
occurred_at	string time	Required	Дата и время происшествия в формате: date-time
occurrence_id	string	Required	Идентификатор происшествия

Параметр	Тип данных	Обязательность	Описание
error	string	Required	Ошибка
service_asset_id	string	Required	Идентификатор актива
asset_info	object<asset>	Required	Данные актива
incident_identifier	string	Required	Идентификатор инцидента
metadata	string map	Required	Метаданные в формате map

LogmuleGoResultsAsset

Параметр	Тип данных	Обязательность	Описание
ip	string	Required	IP-адрес актива
hostname	string	Required	Хостнейм актива
fqdn	string	Required	FQDN актива
mac	string	Required	MAC-адрес актива

Модель данных Message

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор сообщения пользователя
created_at	string	Required	Дата создания в формате `date-time`
updated_at	string	Required	Дата изменения в формате `date-time`
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
subject	string	Optional	Тема (Предмет) сообщения
body	string	Optional	Тело сообщения
service_asset_id	string	Optional	Идентификатор связанного актива
service_asset_finding_id	string	Optional	Идентификатор связанного инцидента

Параметр	Тип данных	Обязательность	Описание
service_asset_finding_status_change_id	string	Optional	Идентификатор связанного изменения статуса инцидента
automated	boolean	Optional	Флаг автоматического создания
finding_id	string	Optional	Идентификатор связанного типа инцидента
itsm_sync_status	string	Optional	Статус синхронизации с внешними системами. Допустимые значения: - not_synced - scheduled - aborted - synced - waiting_confirmation
itsm_last_synced_at	string	Optional	Время синхронизации с внешними системами
itsm_sync_error	string	Optional	Описание ошибки синхронизации
sender_id	string	Optional	Идентификатор пользователя, инициировавшего синхронизацию

Модель данных Network_Interface

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор сетевого интерфейса
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
name	string	Required	Название сетевого интерфейса
ip	string	Optional	IP адрес сетевого интерфейса
mac	string	Optional	MAC адрес сетевого интерфейса
fqdn	string	Optional	FQDN
os	string	Optional	Операционная система
service_asset_id	string	Optional	Идентификатор связанного актива
edited_by	string	Optional	Идентификатор пользователя внесшего изменения
service_asset_name	string	Optional	Название связанного актива

Параметр	Тип данных	Обязательность	Описание
service_asset_location	string	Optional	Локация связанного актива
service_asset_value	integer	Optional	Значение связанного актива
service_asset_network_exposure	integer	Optional	Коэффициент сетевой видимости связанного актива
service_asset_group_names	Array<string>	Optional	Список названий связанных групп активов
has_service_asset	boolean	Optional	Флаг, является ли активом

Модель данных ServiceAssetFinding

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор инцидента
created_at	string time	Required	Дата создания в формате: date-time
updated_at	string time	Required	Дата изменения в формате: date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
description	string	Required	Подробное описание инцидента
risk_impact	string	Required	Описание последствий, которые могут возникнуть, если угроза была реализована
solution	string	Required	Рекомендации по устранению инцидента
mitigation	integer	Required	Описание профилактики данного типа инцидента
status	string	Required	Состояние инцидента в зависимости от того какая с ним работа была проведена оператором. Допустимые значения: - assigned_customer - назначен; - closed - закрыт; - feedback_required - запрошена информация; - invalid - недействительный; - new - новый; - risk_accepted - риск принят - verify_close - ожидает проверки; - working_customer - в работе.
risklevel	number	Required	Уровень риска. Допустимые значения от "0" до "10"
service_asset_id	string	Required	Идентификатор актива, на котором обнаружен инцидент
finding_id	string	Required	Идентификатор типа инцидента

Параметр	Тип данных	Обязательность	Описание
analysis_output	string	Required	Результат анализа. Заполняемое поле в правиле корреляции. Например: на активе {{ .event.IP}} произошло…
synopsis	string	Required	Краткое описание сути инцидентов данного типа
title	string	Required	Название инцидента
risk	string	Required	Описание уровня риска инцидента. Допустимые значения: - none; - low; - medium; - high.
acknowledged_at	string	Required	Дата выявления / обнаружения инцидента
alert_type	string	Required	Политика поведения платформы над инцидентом при "сработке" правила корреляции
client_note	string	Optional	Заметки клиента
internal_note	string	Optional	Внутреннее примечание
external	boolean	Required	Эксплуатируема ли удаленно уязвимость, на основе которой создан инцидент
immediate_action_score	number	Required	Срочность инцидента. Результат перемножения уровня риска, которое было присвоено по результату сработки правила корреляции и “значимости актива”. при этом значимость актива из 2х параметров. Значимость и сетевая видимость.
throughput_period	string	Required	Статус инцидент в логике оповещений операторов о задержке в обработке. Допустимые значения: - grace; - delay; - unacceptable.
throughput_period_change	string	Required	Время изменения поля **throughput_period**
customer_created	boolean	Optional	Флаг, что создан пользователем, а не автоматически
c_visible_since	string	Optional	Дата и время с которой инцидент виден пользователям
c_visible_since_in_days	integer	Optional	Количество дней, в течение которых инцидент виден пользователям
c_reopened_count	integer	Optional	Количество повторных открытий инцидента
c_last_customer_status_change	string	Optional	Дата и время последнего изменения статуса инцидента пользователем
logmule_identifier	string	Optional	Идентификатор, который можно задать в правиле (текстовое), а потом использовать для фильтрации.
c_remote_exploitable	boolean	Required	Возможность удаленного использования
c_occurrence_count	integer	Required	Количество происшествий в инциденте
c_customer_retention_time	integer	Required	Количество времени удержания клиента

Параметр	Тип данных	Обязательность	Описание
last_occurrence_id	string	Required	Идентификатор последнего происшествия
itsm_last_synced_at	string format: date-time	Optional	Время последнего изменения статуса происшествия, который был отправлен в стороннюю систему
itsm_sync_status	string	Optional	Статус происшествия, отправленного в стороннюю систему. Допустимые значения: - scheduled; - aborted; - synced; - not_synced; - waiting_confirmation
external_id	string	Optional	Идентификатор инцидента во внешней клиентской системе
itsm_sync_error	string	Optional	Ошибка синхронизации с внешней клиентской системой
user_id	string	Optional	Идентификатор пользователя, назначенного на инцидент
updated_by	string	Optional	Идентификатор пользователя, который последний обновил инцидент
group_id	string	Optional	Группа пользователей, назначенных на инцидент
acknowledged_by	string	Optional	Идентификатор пользователя, который подтвердил инцидент
created_by_customer	string	Optional	Идентификатор пользователя, который вручную создал инцидент
edited_by	string	Optional	Идентификатор пользователя, который последний отредактировал инцидент, созданный вручную
incident_group_id	string	Optional	Идентификатор группы инцидентов, в которую входит инцидент
reopened_at	string	Optional	Время, когда данный инцидент был открыт заново
display_id	integer	Required	Идентификатор инцидента, созданный по алгоритму, который регулирует последовательность присвоения идентификаторов

Модель данных ServiceAssetGroup

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы активов
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
name	string	Required	Название группы активов

Параметр	Тип данных	Обязательность	Описание
network_ranges	Array<string>	Optional	Список подсетей
domain	string	Optional	Домен
itsm_synced	boolean	Optional	Признак синхронизации с системой управления ИТ-услугами
regex	string	Optional	Регулярное выражение
subject_id	string	Optional	Идентификатор субъекта
object_id	string	Optional	Идентификатор объекта
is_kii	boolean	Optional	Признак принадлежности к объектам критической инфраструктуры
is_fincert	boolean	Optional	Признак вхождения в систему информационного обмена между участниками финансового рынка
responsible_person	string	Optional	Имя ответственного пользователя
technical_specialist	string	Optional	Технический специалист
system_id	string	Optional	Идентификатор системы
responsible_group_id	string	Optional	Идентификатор ответственной группы
edited_by	string	Optional	Идентификатор пользователя, внесшего изменения

Модель данных Software

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор
created_at	string	Required	Дата создания
updated_at	string	Required	Дата изменения
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название
raw_output_line	string	Optional	Необработанная строка данных (уникальное значение)
version	string	Optional	Версия

Параметр	Тип данных	Обязательность	Описание
release	string	Optional	Релиз При создании из результата сканирования, совпадает с version. При сканировании ПО, не заполняется.
os	string	Optional	Операционная система
display_name	string	Optional	Название клиента (отображается в деталях инцидента)
description	string	Optional	Описание
software_group_id	string	Optional	ID группы ПО
tsvector	string	Optional	readonly Используется для оптимизации поиска, заполняется автоматически (при создании и изменении объекта) из полей raw_output_line, name, version, release.

Модель данных Vulnerability

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор
created_at	string	Required	Дата создания в формате: date-time
updated_at	string	Required	Дата изменения в формате: date-time
plugin_id	integer	Optional	ID плагина
plugin_name	string	Optional	Название плагина
description	string	Optional	Описание уязвимости
severity	integer	Optional	Важность
additional_data	Array<object>	Optional	Дополнительные данные в формате map<string,string>
protocol	string	Optional	Тип протокола (tcp, udp и пр.). “-1”, если не определён
port	integer	Optional	Порт
occurrence_id	string	Optional	ID происшествия в формате uuid
synopsis	string	Optional	Краткое описание
vulnerability_host_id	string	Optional	ID хоста уязвимости

Параметр	Тип данных	Обязательность	Описание
exploitable	boolean/null	Optional	Флаг возможности использования
plugin_output	string	Optional	Результат работы плагина, зависит от типа отчета (сканирования)
solution	string	Optional	Алгоритм устранения уязвимости
compare_port	integer	Optional	При создании из результата сканирования, совпадает с полем port
compare_protocol	string	Optional	При создании из результата сканирования, совпадает с полем protocol
service_asset_id	string	Optional	ID актива
vulnerability_scan_id	string	Optional	ID результата сканирования (отчёта)
external	boolean	Optional	Флаг внешней уязвимости
remote_exploitable	boolean	Optional	Флаг возможности удалённого использования
cvss_vector	string	Optional	Вектор метрик оценки по CVSS
cvss_temporal_vector	string	Optional	Вектор временных метрик оценки по CVSS
cvss_base_score	number	Optional	Оценка уязвимости по CVSS
cvss_temporal_score	number	Optional	Временная оценка уязвимости по CVSS
risk_factor	string	Optional	Текстовая степень важности (none, low, medium и т.д.)
plugin_modification_date	string	Optional	Дата изменения плагина (не связано с изменениями в БД, заполняется из результата сканирования) в формате: date-time
publication_date	string	Optional	Дата публикации в формате: date-time

Модель данных VulnerabilityHost

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор
created_at	string	Required	Дата создания в формате: date-time
updated_at	string	Required	Дата изменения в формате: date-time
ip	string	Optional	IP-адрес

Параметр	Тип данных	Обязательность	Описание
mac	string	Optional	MAC-адрес
fqdn	string	Optional	Доменное имя
properties	string	Optional	Дополнительные свойства (не используется)
scan_begin	null / string	Optional	Начало сканирования в формате: date-time
scan_end	null / string	Optional	Окончание сканирования в формате: date-time
service_asset_id	string	Optional	Идентификатор актива
vulnerability_scan_id	string	Optional	Идентификатор результата сканирования
os	string	Optional	Операционная система
authenticated	boolean	Optional	Флаг аутентификации
scan_error	string	Optional	Ошибка при сканировании
name	string	Required	Название
authentication_info	object	Optional	Информация для аутентификации (не используется) Словарь (ключ-значение) - ключ: string - значение: любой тип

Модель данных ResponsibleGroup

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы ответственных пользователей
name	string	Required	Название группы
parent_group	string	Required	Название родительской группы
realm_id	string	Required	Идентификатор области
email	string	Required	Почта
phone_number	string	Required	Телефон
leader_id	string	Required	Идентификатор руководителя группы
accept_risk	boolean	Required	Флаг автоматического принятия риска

Параметр	Тип данных	Обязательность	Описание
visible_scan_schedules	boolean	Required	Флаг видимости расписания сканирования
stop_scans	boolean	Required	Флаг прекращения сканирования
edited_by	string	Required	Идентификатор пользователя, изменившего информацию о группе
user_ids	Array<string>	Required	Список ID пользователей в группе

Модель данных _relations

Параметр	Тип данных	Обязательность	Описание
hardware_informations	Array<string>	Optional	Список связанных идентификаторов моделей информации об аппаратном обеспечении
logmule_go_results	Array<string>	Optional	Список связанных идентификаторов моделей сработок
messages	Array<string>	Optional	Список связанных идентификаторов моделей сообщений пользователей
network_interfaces	Array<string>	Optional	Список связанных идентификаторов моделей сетевых интерфейсов
service_asset_findings	Array<string>	Optional	Список связанных идентификаторов моделей инцидентов
service_asset_groups	Array<string>	Optional	Список связанных идентификаторов моделей групп активов
software	Array<string>	Optional	Список связанных идентификаторов моделей ПО
vulnerabilities	Array<string>	Optional	Список связанных идентификаторов моделей уязвимостей
vulnerability_hosts	Array<string>	Optional	Список связанных идентификаторов моделей хостов уязвимостей

Модель данных mac_ip

Параметр	Тип данных	Обязательность	Описание
ip	string	Optional	IP адрес
mac	string	Optional	MAC адрес
service_asset_id	string	Optional	Идентификатор связанного актива

3.1.3 Создание актива

Запрос:

Тип	Метод
POST	/service_assets_create

Описание:

При выполнении запроса будет создан актив.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится актив связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в активе _relations отсутствуют зависимости не обновляются
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию
- Если поле зависимости указано и в значении пустой список, то все связи удаляются

Например, следующий запрос:

```
{
  "name": "Test",
  ...
  "_relations": {
    "service_asset_groups": [] // - очистит все связи с группами активов
    // "service_asset_groups": ["uuid1", "uuid2"] // - создаст связь с 2 группами
активов
    // "service_asset_groups": ["uuid1"] // - оставит связь только с первой группой
активов
  }
}
```

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_assets/create
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
type	string	Required	Тип актива
name	string	Required	Название актива
description	string	Optional	Описание актива
coordinates	string	Optional	Координаты актива (не используется)
active	boolean	Optional	Флаг активности
scan_id	string	Optional	ID сканера активов (не используется)
value	integer	Optional	Значимость актива. В платформе значимость актива может принимать следующие значения: - 1 – ключевой; - 2 – важный; - 3 – некритичный; - 4 – распределенный; - 5 – тестовый.
client_note	string	Optional	Клиентские заметки (не используется)
internal_note	string	Optional	Внутренние заметки (не используется)
location	string	Required	Расположение актива
network_exposure	integer	Optional	Сетевая доступность актива. Тип сетевой видимости актива может принимать следующие значения: - 1 – актив напрямую подключен к сети Интернет; - 2 – актив располагается в демилитаризованной зоне (DMZ); - 3 – актив подключен к сети Интернет через Proxy-сервер; - 4 – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы; - 5 – актив не подключен к сети.
responsible_person	string	Optional	Ответственное лицо
technical_specialist	string	Optional	Технический специалист
responsible_group_id	string	Optional	ID группы ответственных
edited_by	string	Optional	Кем изменён (не используется)
_relations	object<relations>	Optional	Словарь идентификаторов связанных объектов

Модель данных _relations

Параметр	Тип данных	Обязательность	Описание
hardware_informations	Array<string>	Optional	Список связанных идентификаторов моделей информации об аппаратном обеспечении
logmule_go_results	Array<string>	Optional	Список связанных идентификаторов моделей сработок
messages	Array<string>	Optional	Список связанных идентификаторов моделей сообщений пользователей
network_interfaces	Array<string>	Optional	Список связанных идентификаторов моделей сетевых интерфейсов
service_asset_findings	Array<string>	Optional	Список связанных идентификаторов моделей инцидентов
service_asset_groups	Array<string>	Optional	Список связанных идентификаторов моделей групп активов
software	Array<string>	Optional	Список связанных идентификаторов моделей ПО
vulnerabilities	Array<string>	Optional	Список связанных идентификаторов моделей уязвимостей
vulnerability_hosts	Array<string>	Optional	Список связанных идентификаторов моделей хостов уязвимостей

Пример тела запроса:


```
{
  "trace_id": "uuid",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "_relations": {
    "hardware_informations": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "network_interfaces": [
```

```
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerability_hosts": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Успешный ответ:

Статус код: 201 – успешное создание актива.

Формат: JSON.

Тело ответа: «Модель ресурса «Активы»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "hardware_informations": [
    {
      "hardware_type": "string",
      "name": "string",
      "manufacturer": "string",
      "serial_number": "string",
      "additional_info": "string",
```

```
      "is_old": false
    }
  ],
  "logmule_go_results": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "rule_id": "uuid",
      "analysis_output": "string",
      "event": {},
      "compressed_event": "string",
      "risklevel": 5.35,
      "occurred_at": "2023-12-20T00:00:01.652259Z",
      "occurrence_id": "uuid",
      "error": "string",
      "service_asset_id": "uuid",
      "asset_info": {
        "ip": "string",
        "hostname": "string",
        "fqdn": "string",
        "mac": "string"
      },
      "incident_identifier": "string",
      "metadata": "{\"key\": \"value\"}"
    }
  ],
  "messages": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "subject": "string",
      "body": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "automated": true,
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
    }
  ],
  "network_interfaces": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "ip": "string",
      "mac": "string",
      "fqdn": "string",
      "os": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "service_asset_name": "string",
      "service_asset_location": "string",
      "service_asset_value": 0,
      "service_asset_network_exposure": 0,
      "service_asset_group_names": [
        "string"
```

```
    ],
    "has_service_asset": true
  }
],
"service_asset_findings": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "description": "string",
    "risk_impact": "string",
    "solution": "string",
    "mitigation": "string",
    "status": "assigned_customer",
    "risklevel": 0,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
    "analysis_output": "string",
    "synopsis": "string",
    "title": "string",
    "risk": "none",
    "acknowledged_at": "2023-12-20T00:00:01.652259Z",
    "alert_type": "automatic",
    "client_note": "string",
    "internal_note": "string",
    "external": false,
    "immediate_action_score": 0,
    "throughput_period": "grace",
    "throughput_period_change": "2023-12-20T00:00:01.652259Z",
    "customer_created": false,
    "c_visible_since": "2023-12-20T00:00:01.652259Z",
    "c_visible_since_in_days": 0,
    "c_reopened_count": 0,
    "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
    "logmule_identifier": "string",
    "c_remote_exploitable": true,
    "c_occurrence_count": 0,
    "c_customer_retention_time": 0,
    "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
    "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
    "itsm_sync_status": "scheduled",
    "external_id": "string",
    "itsm_sync_error": "string",
    "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
    "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
    "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
    "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
    "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
    "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
    "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
    "reopened_at": "2023-12-20T00:00:01.652259Z",
    "display_id": 0
  }
],
"service_asset_groups": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "name": "string",
    "network_ranges": [],
    "domain": "string",
    "itsm_synced": false,
    "regex": "string",
```

```
      "subject_id": "string",
      "object_id": "string",
      "is_kii": false,
      "is_fincert": false,
      "responsible_person": "string",
      "technical_specialist": "string",
      "system_id": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
    }
  ],
  "software": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "raw_output_line": "string",
      "version": "string",
      "release": "string",
      "os": "string",
      "display_name": "",
      "description": "string",
      "software_group_id": "d7939ec9-4754-44e2-b522-27172eae4658",
      "tsvector": "'17':4,12 '17.5.2.1':8,16,17 'driver':3,11 'for':5,13
'microsoft':1,9 'odbc':2,10 'server':7,15 'sql':6,14"
    }
  ],
  "vulnerabilities": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
      "plugin_name": "string",
      "description": "string",
      "severity": 0,
      "additional_data": {},
      "protocol": "string",
      "port": 0,
      "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
      "synopsis": "string",
      "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
      "exploitable": true,
      "plugin_output": "string",
      "solution": "string",
      "compare_port": -1,
      "compare_protocol": "",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "external": false,
      "remote_exploitable": false,
      "cvss_vector": "string",
      "cvss_temporal_vector": "string",
      "cvss_base_score": 0,
      "cvss_temporal_score": 0,
      "risk_factor": "string",
      "plugin_modification_date": "string",
      "publication_date": "string"
    }
  ],
  "vulnerability_hosts": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
```

```
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "ip": "192.168.0.1",
      "mac": "string",
      "fqdn": "string",
      "properties": "string",
      "scan_begin": null,
      "scan_end": null,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "os": "string",
      "authenticated": true,
      "scan_error": "string",
      "name": "string",
      "authentication_info": {
        "key1": {
          "nestedKey": "nestedValue"
        },
        "key2": [
          "listItem1",
          "listItem2"
        ],
        "key3": 42,
        "key4": null
      }
    }
  ],
  "responsible_group": {
    "id": "uuid",
    "name": "string",
    "parent_group": "string",
    "realm_id": "string",
    "email": "string",
    "phone_number": "string",
    "leader_id": "string",
    "accept_risk": true,
    "visible_scan_schedules": true,
    "stop_scans": true,
    "edited_by": "string",
    "user_ids": [
      "uuid"
    ]
  },
  "_relations": {
    "hardware_informations": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "network_interfaces": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
```

```
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerability_hosts": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  },
  "is_local": true,
  "risk": "low",
  "risklevel": 1.2,
  "mac_ip": {
    "ip": "127.0.0.1",
    "mac": "FF:FF:FF:FF:FF:FF",
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e"
  },
  "os_list": [
    [
      "macOs",
      "windows"
    ]
  ],
  "responsible_group_name": "Admins",
  "closed_count": 5,
  "risk_accepted_count": 4,
  "all_open_count": 3,
  "last_scan": "2023-12-20T00:00:01.652259Z",
  "authenticated": false,
  "authentication_info": {},
  "network_interface_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ]
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
409	name_already_used	Попытка присвоить объекту существующее уникальное значение атрибута
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 409:


```
{
  "error": "Bad Request",
  "error_code": 409,
```

```
  "extra": {
    "fields": [
      "name"
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.4 Обновление актива

Запрос:

Тип	Метод
PUT	/service_assets/update

Описание:

При выполнении запроса будет обновлена информация об активе в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

В поле _relations в качестве ключей могут быть указаны названия полей моделей, которые ссылаются на другие модели. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью.

Управление работает следующим образом:

- Если поля в активе _relations отсутствуют, то зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются.

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "service_asset_groups": [] // - очистит все связи с группами активов
```

```
    // "service_asset_groups": ["uuid1", "uuid2"] // - создаст связь с 2 группами
активов
    // "service_asset_groups": ["uuid1"] // - оставит связь только с первой группой
активов
  }
}
```

Пример запроса:

PUT

```
http://127.0.0.1/cruddy/v2/service_assets/update
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
id	string	Required	Идентификатор актива
type	string	Required	Тип актива
name	string	Required	Название актива
description	string	Optional	Описание актива
coordinates	string	Optional	Координаты актива (не используется)
active	boolean	Optional	Флаг активности
scan_id	string	Optional	ID сканера активов (не используется)
value	integer	Optional	Значимость актива. В платформе значимость актива может принимать следующие значения: - 1 – ключевой; - 2 – важный; - 3 – некритичный; - 4 – распределенный; - 5 – тестовый.
client_note	string	Optional	Клиентские заметки (не используется)
internal_note	string	Optional	Внутренние заметки (не используется)
location	string	Required	Расположение актива
network_exposure	integer	Optional	Сетевая доступность актива. Тип сетевой видимости актива может принимать следующие значения: - 1 – актив напрямую подключен к сети Интернет; - 2 – актив располагается в демилитаризованной зоне (DMZ);

Параметр	Тип данных	Обязательность	Описание
			- 3 – актив подключен к сети Интернет через Proxy-сервер; - 4 – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы; - 5 – актив не подключен к сети.
responsible_person	string	Optional	Ответственное лицо
technical_specialist	string	Optional	Технический специалист
responsible_group_id	string	Optional	ID группы ответственных
edited_by	string	Optional	Кем изменён (не используется)
_relations	object<relations>	Optional	Словарь идентификаторов связанных объектов

Модель данных _relations

Параметр	Тип данных	Обязательность	Описание
hardware_informations	Array<string>	Optional	Список связанных идентификаторов моделей информации об аппаратном обеспечении
logmule_go_results	Array<string>	Optional	Список связанных идентификаторов моделей сработок
messages	Array<string>	Optional	Список связанных идентификаторов моделей сообщений пользователей
network_interfaces	Array<string>	Optional	Список связанных идентификаторов моделей сетевых интерфейсов
service_asset_findings	Array<string>	Optional	Список связанных идентификаторов моделей инцидентов
service_asset_groups	Array<string>	Optional	Список связанных идентификаторов моделей групп активов
software	Array<string>	Optional	Список связанных идентификаторов моделей ПО
vulnerabilities	Array<string>	Optional	Список связанных идентификаторов моделей уязвимостей
vulnerability_hosts	Array<string>	Optional	Список связанных идентификаторов моделей хостов уязвимостей

Пример тела запроса:


```
{
  "trace_id": "uuid",
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "type": "Host",
  "name": "Актив",
```

```
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "_relations": {
    "hardware_informations": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "network_interfaces": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerability_hosts": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Успешный ответ:

Статус код: 200 - успешное обновление информации об активе.

Формат: JSON.

Тело ответа: «Модель ресурса «Активы»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
```

```
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "hardware_informations": [
    {
      "hardware_type": "string",
      "name": "string",
      "manufacturer": "string",
      "serial_number": "string",
      "additional_info": "string",
      "is_old": false
    }
  ],
  "logmule_go_results": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "rule_id": "uuid",
      "analysis_output": "string",
      "event": {},
      "compressed_event": "string",
      "risklevel": 5.35,
      "occurred_at": "2023-12-20T00:00:01.652259Z",
      "occurrence_id": "uuid",
      "error": "string",
      "service_asset_id": "uuid",
      "asset_info": {
        "ip": "string",
        "hostname": "string",
        "fqdn": "string",
        "mac": "string"
      },
      "incident_identifier": "string",
      "metadata": "{\"key\": \"value\"}"
    }
  ],
  "messages": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "subject": "string",
      "body": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "automated": true,
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "itsm_sync_status": "not_synced",
```

```
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
    }
  ],
  "network_interfaces": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "ip": "string",
      "mac": "string",
      "fqdn": "string",
      "os": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "service_asset_name": "string",
      "service_asset_location": "string",
      "service_asset_value": 0,
      "service_asset_network_exposure": 0,
      "service_asset_group_names": [
        "string"
      ],
      "has_service_asset": true
    }
  ],
  "service_asset_findings": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "analysis_output": "string",
      "synopsis": "string",
      "title": "string",
      "risk": "none",
      "acknowledged_at": "2023-12-20T00:00:01.652259Z",
      "alert_type": "automatic",
      "client_note": "string",
      "internal_note": "string",
      "external": false,
      "immediate_action_score": 0,
      "throughput_period": "grace",
      "throughput_period_change": "2023-12-20T00:00:01.652259Z",
      "customer_created": false,
      "c_visible_since": "2023-12-20T00:00:01.652259Z",
      "c_visible_since_in_days": 0,
      "c_reopened_count": 0,
      "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "logmule_identifier": "string",
      "c_remote_exploitable": true,
      "c_occurrence_count": 0,
      "c_customer_retention_time": 0,
      "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "itsm_sync_status": "scheduled",
```

```
      "external_id": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
      "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
      "reopened_at": "2023-12-20T00:00:01.652259Z",
      "display_id": 0
    }
  ],
  "service_asset_groups": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "network_ranges": [],
      "domain": "string",
      "itsm_synced": false,
      "regex": "string",
      "subject_id": "string",
      "object_id": "string",
      "is_kii": false,
      "is_fincert": false,
      "responsible_person": "string",
      "technical_specialist": "string",
      "system_id": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
    }
  ],
  "software": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "raw_output_line": "string",
      "version": "string",
      "release": "string",
      "os": "string",
      "display_name": "",
      "description": "string",
      "software_group_id": "d7939ec9-4754-44e2-b522-27172eae4658",
      "tsvector": "'17':4,12 '17.5.2.1':8,16,17 'driver':3,11 'for':5,13
'microsoft':1,9 'odbc':2,10 'server':7,15 'sql':6,14"
    }
  ],
  "vulnerabilities": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
      "plugin_name": "string",
      "description": "string",
      "severity": 0,
      "additional_data": {},
      "protocol": "string",
      "port": 0,
      "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
```

```
      "synopsis": "string",
      "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
      "exploitable": true,
      "plugin_output": "string",
      "solution": "string",
      "compare_port": -1,
      "compare_protocol": "",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "external": false,
      "remote_exploitable": false,
      "cvss_vector": "string",
      "cvss_temporal_vector": "string",
      "cvss_base_score": 0,
      "cvss_temporal_score": 0,
      "risk_factor": "string",
      "plugin_modification_date": "string",
      "publication_date": "string"
    }
  ],
  "vulnerability_hosts": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "ip": "192.168.0.1",
      "mac": "string",
      "fqdn": "string",
      "properties": "string",
      "scan_begin": null,
      "scan_end": null,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "os": "string",
      "authenticated": true,
      "scan_error": "string",
      "name": "string",
      "authentication_info": {
        "key1": {
          "nestedKey": "nestedValue"
        },
        "key2": [
          "listItem1",
          "listItem2"
        ],
        "key3": 42,
        "key4": null
      }
    }
  ],
  "responsible_group": {
    "id": "uuid",
    "name": "string",
    "parent_group": "string",
    "realm_id": "string",
    "email": "string",
    "phone_number": "string",
    "leader_id": "string",
    "accept_risk": true,
    "visible_scan_schedules": true,
    "stop_scans": true,
    "edited_by": "string",
    "user_ids": [
      "uuid"
```

```
    ]
  },
  "_relations": {
    "hardware_informations": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "network_interfaces": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerability_hosts": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  },
  "is_local": true,
  "risk": "low",
  "risklevel": 1.2,
  "mac_ip": {
    "ip": "127.0.0.1",
    "mac": "FF:FF:FF:FF:FF:FF",
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e"
  },
  "os_list": [
    [
      "macOs",
      "windows"
    ]
  ],
  "responsible_group_name": "Admins",
  "closed_count": 5,
  "risk_accepted_count": 4,
  "all_open_count": 3,
  "last_scan": "2023-12-20T00:00:01.652259Z",
  "authenticated": false,
  "authentication_info": {},
  "network_interface_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.5 Поиск активов

Запрос:

Тип	Метод
POST	/service_assets/search

Описание:

При выполнении запроса будут возвращены найденные объекты с учётом заданных фильтров.

По умолчанию в объекты не загружаются связанные модели по типам связи many2many и has-many, для включения загрузки их нужно указывать в поле relations объекта запроса.

Связи _relations загружаются всегда и отражают текущее состояние связей модели.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/rule_sets/search
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений - substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят

Параметр	Тип данных	Обязательность	Описание
			связанность с моделью по идентификатору если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
```

```
  "virtual_search": {
    "value": "string",
    "strict": false
  },
  "relations": [
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array<ServiceAsset>	Список найденных активов
total	integer	Количество найденных значений дополнительных полей

Пример ответа:

```
{
  "items": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "type": "Host",
      "name": "Актив",
      "description": "Описание актива",
      "coordinates": "--- []",
      "active": true,
      "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
      "value": 3,
      "client_note": "string",
      "internal_note": "string",
      "location": "string",
      "network_exposure": 3,
      "responsible_person": "string",
      "technical_specialist": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "hardware_informations": [
        {
```

```
        "hardware_type": "string",
        "name": "string",
        "manufacturer": "string",
        "serial_number": "string",
        "additional_info": "string",
        "is_old": false
      }
    ],
    "logmule_go_results": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "rule_id": "uuid",
        "analysis_output": "string",
        "event": {},
        "compressed_event": "string",
        "risklevel": 5.35,
        "occurred_at": "2023-12-20T00:00:01.652259Z",
        "occurrence_id": "uuid",
        "error": "string",
        "service_asset_id": "uuid",
        "asset_info": {
          "ip": "string",
          "hostname": "string",
          "fqdn": "string",
          "mac": "string"
        },
        "incident_identifier": "string",
        "metadata": "{\"key\": \"value\"}"
      }
    ],
    "messages": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "subject": "string",
        "body": "string",
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
        "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
        "automated": true,
        "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
        "itsm_sync_status": "not_synced",
        "itsm_last_synced_at": "string",
        "itsm_sync_error": "string",
        "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
      }
    ],
    "network_interfaces": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "ip": "string",
        "mac": "string",
        "fqdn": "string",
        "os": "string",
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
        "service_asset_name": "string",
```

```
      "service_asset_location": "string",
      "service_asset_value": 0,
      "service_asset_network_exposure": 0,
      "service_asset_group_names": [
        "string"
      ],
      "has_service_asset": true
    }
  ],
  "service_asset_findings": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "analysis_output": "string",
      "synopsis": "string",
      "title": "string",
      "risk": "none",
      "acknowledged_at": "2023-12-20T00:00:01.652259Z",
      "alert_type": "automatic",
      "client_note": "string",
      "internal_note": "string",
      "external": false,
      "immediate_action_score": 0,
      "throughput_period": "grace",
      "throughput_period_change": "2023-12-20T00:00:01.652259Z",
      "customer_created": false,
      "c_visible_since": "2023-12-20T00:00:01.652259Z",
      "c_visible_since_in_days": 0,
      "c_reopened_count": 0,
      "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "logmule_identifier": "string",
      "c_remote_exploitable": true,
      "c_occurrence_count": 0,
      "c_customer_retention_time": 0,
      "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "itsm_sync_status": "scheduled",
      "external_id": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
      "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
      "reopened_at": "2023-12-20T00:00:01.652259Z",
      "display_id": 0
    }
  ],
  "service_asset_groups": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
```

```
        "name": "string",
        "network_ranges": [],
        "domain": "string",
        "itsm_synced": false,
        "regex": "string",
        "subject_id": "string",
        "object_id": "string",
        "is_kii": false,
        "is_fincert": false,
        "responsible_person": "string",
        "technical_specialist": "string",
        "system_id": "string",
        "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
        "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
      }
    ],
    "software": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "name": "string",
        "raw_output_line": "string",
        "version": "string",
        "release": "string",
        "os": "string",
        "display_name": "",
        "description": "string",
        "software_group_id": "d7939ec9-4754-44e2-b522-27172eae4658",
        "tsvector": "'17':4,12 '17.5.2.1':8,16,17 'driver':3,11 'for':5,13
'microsoft':1,9 'odbc':2,10 'server':7,15 'sql':6,14"
      }
    ],
    "vulnerabilities": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "created_at": "2023-12-20T00:00:01.652259Z",
        "updated_at": "2023-12-20T00:00:01.652259Z",
        "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
        "plugin_name": "string",
        "description": "string",
        "severity": 0,
        "additional_data": {},
        "protocol": "string",
        "port": 0,
        "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
        "synopsis": "string",
        "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
        "exploitable": true,
        "plugin_output": "string",
        "solution": "string",
        "compare_port": -1,
        "compare_protocol": "",
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
        "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
        "external": false,
        "remote_exploitable": false,
        "cvss_vector": "string",
        "cvss_temporal_vector": "string",
        "cvss_base_score": 0,
        "cvss_temporal_score": 0,
        "risk_factor": "string",
        "plugin_modification_date": "string",
        "publication_date": "string"
```

```
  }
],
"vulnerability_hosts": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "ip": "192.168.0.1",
    "mac": "string",
    "fqdn": "string",
    "properties": "string",
    "scan_begin": null,
    "scan_end": null,
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
    "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
    "os": "string",
    "authenticated": true,
    "scan_error": "string",
    "name": "string",
    "authentication_info": {
      "key1": {
        "nestedKey": "nestedValue"
      },
      "key2": [
        "listItem1",
        "listItem2"
      ],
      "key3": 42,
      "key4": null
    }
  }
],
"responsible_group": {
  "id": "uuid",
  "name": "string",
  "parent_group": "string",
  "realm_id": "string",
  "email": "string",
  "phone_number": "string",
  "leader_id": "string",
  "accept_risk": true,
  "visible_scan_schedules": true,
  "stop_scans": true,
  "edited_by": "string",
  "user_ids": [
    "uuid"
  ]
},
"_relations": {
  "hardware_informations": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "logmule_go_results": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "messages": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "network_interfaces": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "service_asset_findings": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
```

```
        "service_asset_groups": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "software": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "vulnerabilities": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "vulnerability_hosts": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ]
      },
      "is_local": true,
      "risk": "low",
      "risklevel": 1.2,
      "mac_ip": {
        "ip": "127.0.0.1",
        "mac": "FF:FF:FF:FF:FF:FF",
        "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e"
      },
      "os_list": [
        [
          "macOs",
          "windows"
        ]
      ],
      "responsible_group_name": "Admins",
      "closed_count": 5,
      "risk_accepted_count": 4,
      "all_open_count": 3,
      "last_scan": "2023-12-20T00:00:01.652259Z",
      "authenticated": false,
      "authentication_info": {},
      "network_interface_ids": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ]
    }
  ],
  "total": 1
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.6 Получение актива по ID

Запрос:

Тип	Метод
GET	/service_assets/{id}

Описание:

При выполнении запроса будет возвращен актив с соответствующим ID.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/service_assets/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор актива

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Активы»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "type": "Host",
  "name": "Актив",
  "description": "Описание актива",
  "coordinates": "--- []",
  "active": true,
  "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
  "value": 3,
  "client_note": "string",
  "internal_note": "string",
  "location": "string",
  "network_exposure": 3,
  "responsible_person": "string",
  "technical_specialist": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "hardware_informations": [
    {
      "hardware_type": "string",
      "name": "string",
      "manufacturer": "string",
      "serial_number": "string",
      "additional_info": "string",
      "is_old": false
    }
  ],
  "logmule_go_results": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "rule_id": "uuid",
      "analysis_output": "string",
      "event": {},
      "compressed_event": "string",
      "risklevel": 5.35,
      "occurred_at": "2023-12-20T00:00:01.652259Z",
      "occurrence_id": "uuid",
      "error": "string",
      "service_asset_id": "uuid",
      "asset_info": {
        "ip": "string",
        "hostname": "string",
        "fqdn": "string",
        "mac": "string"
      },
      "incident_identifier": "string",
      "metadata": "{\"key\": \"value\"}"
    }
  ],
  "messages": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "subject": "string",
      "body": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
```

```
      "service_asset_finding_id": "08a5c673-3c5c-48ab-bf6c-f2ee47d8df88",
      "service_asset_finding_status_change_id": "8d6bf02f-aab2-4fbc-ab53-
ee5963306be7",
      "automated": true,
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "itsm_sync_status": "not_synced",
      "itsm_last_synced_at": "string",
      "itsm_sync_error": "string",
      "sender_id": "3194e023-c19f-4a42-9172-9e18d68e3a3a"
    }
  ],
  "network_interfaces": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "ip": "string",
      "mac": "string",
      "fqdn": "string",
      "os": "string",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "service_asset_name": "string",
      "service_asset_location": "string",
      "service_asset_value": 0,
      "service_asset_network_exposure": 0,
      "service_asset_group_names": [
        "string"
      ],
      "has_service_asset": true
    }
  ],
  "service_asset_findings": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "description": "string",
      "risk_impact": "string",
      "solution": "string",
      "mitigation": "string",
      "status": "assigned_customer",
      "risklevel": 0,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "finding_id": "feebf65a-2eaa-4fae-aab2-772450efdffe",
      "analysis_output": "string",
      "synopsis": "string",
      "title": "string",
      "risk": "none",
      "acknowledged_at": "2023-12-20T00:00:01.652259Z",
      "alert_type": "automatic",
      "client_note": "string",
      "internal_note": "string",
      "external": false,
      "immediate_action_score": 0,
      "throughput_period": "grace",
      "throughput_period_change": "2023-12-20T00:00:01.652259Z",
      "customer_created": false,
      "c_visible_since": "2023-12-20T00:00:01.652259Z",
      "c_visible_since_in_days": 0,
      "c_reopened_count": 0,
      "c_last_customer_status_change": "2023-12-20T00:00:01.652259Z",
      "logmule_identifier": "string",
```

```
      "c_remote_exploitable": true,
      "c_occurrence_count": 0,
      "c_customer_retention_time": 0,
      "last_occurrence_id": "92c2542a-a9bb-4370-b835-20b1c9ac1fe9",
      "itsm_last_synced_at": "2023-12-20T00:00:01.652259Z",
      "itsm_sync_status": "scheduled",
      "external_id": "string",
      "itsm_sync_error": "string",
      "user_id": "a169451c-8525-4352-b8ca-070dd449a1a5",
      "updated_by": "deea00dc-b6b6-4412-a483-26ac61e1f6fe",
      "group_id": "306db4e0-7449-4501-b76f-075576fe2d8f",
      "acknowledged_by": "57e93f65-9db5-4b3c-8761-f3edd8ac8276",
      "created_by_customer": "d299b51b-03f1-4b72-b793-1fb027d05389",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
      "incident_group_id": "5ce55b8d-2342-4286-bf58-bfe807f8c05c",
      "reopened_at": "2023-12-20T00:00:01.652259Z",
      "display_id": 0
    }
  ],
  "service_asset_groups": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "network_ranges": [],
      "domain": "string",
      "itsm_synced": false,
      "regex": "string",
      "subject_id": "string",
      "object_id": "string",
      "is_kii": false,
      "is_fincert": false,
      "responsible_person": "string",
      "technical_specialist": "string",
      "system_id": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
    }
  ],
  "software": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "raw_output_line": "string",
      "version": "string",
      "release": "string",
      "os": "string",
      "display_name": "",
      "description": "string",
      "software_group_id": "d7939ec9-4754-44e2-b522-27172eae4658",
      "tsvector": "'17':4,12 '17.5.2.1':8,16,17 'driver':3,11 'for':5,13
'microsoft':1,9 'odbc':2,10 'server':7,15 'sql':6,14"
    }
  ],
  "vulnerabilities": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "plugin_id": "8b176ba5-fa8e-458e-94ad-85d1ae8f3be0",
      "plugin_name": "string",
```

```
      "description": "string",
      "severity": 0,
      "additional_data": {},
      "protocol": "string",
      "port": 0,
      "occurrence_id": "8508ee33-23a1-4a06-ae02-1eb167405e7b",
      "synopsis": "string",
      "vulnerability_host_id": "f7091c30-f117-455e-9531-6af6bb5ece68",
      "exploitable": true,
      "plugin_output": "string",
      "solution": "string",
      "compare_port": -1,
      "compare_protocol": "",
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "external": false,
      "remote_exploitable": false,
      "cvss_vector": "string",
      "cvss_temporal_vector": "string",
      "cvss_base_score": 0,
      "cvss_temporal_score": 0,
      "risk_factor": "string",
      "plugin_modification_date": "string",
      "publication_date": "string"
    }
  ],
  "vulnerability_hosts": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "ip": "192.168.0.1",
      "mac": "string",
      "fqdn": "string",
      "properties": "string",
      "scan_begin": null,
      "scan_end": null,
      "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e",
      "vulnerability_scan_id": "b72752e1-e814-4606-9275-f2ac9ca468b7",
      "os": "string",
      "authenticated": true,
      "scan_error": "string",
      "name": "string",
      "authentication_info": {
        "key1": {
          "nestedKey": "nestedValue"
        },
        "key2": [
          "listItem1",
          "listItem2"
        ],
        "key3": 42,
        "key4": null
      }
    }
  ],
  "responsible_group": {
    "id": "uuid",
    "name": "string",
    "parent_group": "string",
    "realm_id": "string",
    "email": "string",
    "phone_number": "string",
    "leader_id": "string",
```

```
    "accept_risk": true,
    "visible_scan_schedules": true,
    "stop_scans": true,
    "edited_by": "string",
    "user_ids": [
      "uuid"
    ]
  },
  "_relations": {
    "hardware_informations": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "logmule_go_results": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "messages": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "network_interfaces": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_findings": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_asset_groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerabilities": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "vulnerability_hosts": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  },
  "is_local": true,
  "risk": "low",
  "risklevel": 1.2,
  "mac_ip": {
    "ip": "127.0.0.1",
    "mac": "FF:FF:FF:FF:FF:FF",
    "service_asset_id": "09122f07-8b1e-48dc-96fd-379806f6c51e"
  },
  "os_list": [
    [
      "macOs",
      "windows"
    ]
  ],
  "responsible_group_name": "Admins",
  "closed_count": 5,
  "risk_accepted_count": 4,
  "all_open_count": 3,
  "last_scan": "2023-12-20T00:00:01.652259Z",
  "authenticated": false,
  "authentication_info": {},
  "network_interface_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.7 Удаление актива

Запрос:

Тип	Метод
DELETE	/service_assets/{id}

Описание:

При выполнении запроса будет удален актив с соответствующим ID.

Пример запроса:

DELETE

`http://127.0.0.1/cruddy/v2/service_assets/{id}`

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор актива

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
422	11002 11003 11011	Общая ошибка удаления Запрос не затронул ни одной сущности Удаление невозможно из-за наличия блокирующих связей
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 422:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.8 Группировка активов по заданному полю

Запрос:

Тип	Метод
POST	/service_assets/group

Описание:

При выполнении запроса активы будут сгруппированы по заданному полю.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_assets/group
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки объектов

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.9 Массовое удаление активов

Запрос:

Тип	Метод
POST	/service_assets/mass_delete

Описание:

При выполнении запроса будут удалены активы с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_assets/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 0 - отсутствие ошибки - успешное удаление; - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности.

Пример ответа:


```
{
  "results": [
    {
      "id": "string",
      "error_code": 0
    }
  ]
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 500:


```
{
```

```
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.10 Удаление всех активов

Запрос:

Тип	Метод
DELETE	/service_assets/all

Описание:

При выполнении запроса из базы данных будут удалены все активы.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/service_assets/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.11 Получение свойств полей активов и действий пользователей

Запрос:

Тип	Метод
GET	/service_assets/_meta

Описание:

При выполнении запроса будут возвращены свойства полей активов и список действий пользователей над ними.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/service_assets/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.

Параметр	Тип данных	Описание
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:


```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
}
```


Другие возможные ответы:

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:


```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.1.12 Скомпоновать несколько активов в один

Запрос:

Тип	Метод
POST	/service_assets/merge

Описание:

При выполнении запроса указанные активы будут объединены в один. При этом будет создан новый актив и удалены старые активы.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_assets/merge
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
asset_ids	Array<string>	Required	Список идентификаторов активов которые необходимо объединить. Нельзя указывать меньше двух активов

Пример тела запроса:

```
{
  "asset_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    "497f6eca-6276-4993-bfeb-53cbbbba6f09"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
finalAssetId	string	Идентификатор результирующего актива

Пример ответа:

```
{
  "finalAssetId": "946a1fa6-183e-4eb5-801d-a995b897fe27"
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2 Группы активов

3.2.1 Обзор

Основные характеристики:

Характеристика	Значение
Наименование	service_asset_groups
Компоненты	Cruddy
Появился в версии	3.7.0
Доступен в версиях	3.7.0 и выше
Авторизация по токену	**Security scheme type:** http **Bearer format:** JWT
Авторизация по APIkey	**Security scheme type:** apiKey **Header parameter name:** PgrApiKey
Версия API	v2
Описание	service_asset_groups отвечает за управление информацией о группах активов.

Список методов для работы с ресурсом:

Тип	Метод	Описание
POST	/service_asset_groups/create	Создание группы активов
PUT	/service_asset_groups/update	Обновление группы активов
POST	/service_asset_groups	Поиск группы активов
GET	/service_asset_groups/{id}	Получение группы активов по ID
DELETE	/service_asset_groups/{id}	Удаление группы активов
POST	/service_asset_groups/group	Группировка групп активов
POST	/service_asset_groups/mass_delete	Массовое удаление групп активов
DELETE	/service_asset_groups/all	Удаление всех групп активов
GET	/service_asset_groups/_meta	Получение свойств полей групп активов и действий пользователей

Ответы методов:

Статус код	Описание
200	Успех
201	Успешное создание объекта
204	Успешный ответ. Пустое тело ответа
400	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Ресурс не найден
409	Попытка создать объект с существующим уникальным атрибутом
422	Другие ошибки удаления
500	Ошибка сервера

Модели объектов:

Название	Описание
ServiceAssetGroup	Модель данных ресурса service_asset_groups

3.2.2 Модель ресурса «Группы активов»

Модель данных ServiceAssetGroup

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы активов
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
name	string	Required	Название группы активов
network_ranges	Array<string>	Optional	Список подсетей

Параметр	Тип данных	Обязательность	Описание
domain	string	Optional	Домен
itsm_synced	boolean	Optional	Признак синхронизации с системой управления ИТ-услугами
regex	string	Optional	Регулярное выражение
subject_id	string	Optional	Идентификатор субъекта
object_id	string	Optional	Идентификатор объекта
is_kii	boolean	Optional	Признак принадлежности к объектам критической инфраструктуры
is_fincert	boolean	Optional	Признак вхождения в систему информационного обмена между участниками финансового рынка
responsible_person	string	Optional	Имя ответственного пользователя
technical_specialist	string	Optional	Технический специалист
system_id	string	Optional	Идентификатор системы
responsible_group_id	string	Optional	Идентификатор ответственной группы
edited_by	string	Optional	Идентификатор пользователя, внесшего изменения
software_compliance_checks	Array<SoftwareComplianceCheck>	Optional	Связанные проверки соотвествия ПО
responsible_group	object<Responsible_Group>	Optional	Ответственная группа пользователей
groups	Array<Group>	Optional	Связанные группы пользователей
service_assets	Array<ServiceAsset>	Optional	Связанные активы
rule_sets	Array<RuleSet>	Optional	Связанные наборы правил
_relations	object<relations>	Optional	Словарь идентификаторов связанных объектов
service_asset_ids	Array<string>	Optional	Идентификаторы связанных активов
service_asset_ids_count	integer	Optional	Количество связанных активов
responsible_group_name	string	Optional	Название группы ответственных пользователей
group_ids	Array<string>	Optional	Идентификаторы связанных групп пользователей
rule_set_ids	Array<string>	Optional	Идентификаторы связанных наборов правил

Параметр	Тип данных	Обязательность	Описание
user_groups	Array<object>	Optional	Связанные группы пользователей
user_groups**{id}**	string	Optional	Идентификатор группы
user_groups**{name}**	string	Optional	Наименование группы
performed_at	string	Optional	Время выполнения сравнения ПО

Модель SoftwareComplianceCheck

Параметр	Тип данных	Обязательность	Описание
service_asset_group_id	string	Required	Идентификатор группы активов
compliant	boolean	Required	Флаг соответствия
id	string	Required	Идентификатор проверки соответствия ПО
created_at	string	Required	Дата создания
updated_at	string	Required	Дата изменения

Модель данных ResponsibleGroup

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы ответственных пользователей
name	string	Required	Название группы
parent_group	string	Required	Название родительской группы
realm_id	string	Required	Идентификатор области
email	string	Required	Почта
phone_number	string	Required	Телефон
leader_id	string	Required	Идентификатор руководителя группы
accept_risk	boolean	Required	Флаг автоматического принятия риска

Параметр	Тип данных	Обязательность	Описание
visible_scan_schedules	boolean	Required	Флаг видимости расписания сканирования
stop_scans	boolean	Required	Флаг прекращения сканирования
edited_by	string	Required	Идентификатор пользователя, изменившего информацию о группе
user_ids	Array<string>	Required	Список ID пользователей в группе

Модель данных Group

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы ответственных пользователей
name	string	Required	Название группы
parent_group	string	Required	Название родительской группы
realm_id	string	Required	Идентификатор области
email	string	Required	Почта
phone_number	string	Required	Телефон
leader_id	string	Required	Идентификатор руководителя группы
accept_risk	boolean	Required	Флаг автоматического принятия риска
visible_scan_schedules	boolean	Required	Флаг видимости расписания сканирования
stop_scans	boolean	Required	Флаг прекращения сканирования
edited_by	string	Required	Идентификатор пользователя, изменившего информацию о группе
user_ids	Array<string>	Required	Список ID пользователей в группе

Модель данных ServiceAsset

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор актива

Параметр	Тип данных	Обязательность	Описание
created_at	string	Required	Дата создания в формате date-time
updated_at	string	Required	Дата изменения в формате date-time
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
type	string	Required	Тип актива
name	string	Required	Название актива
description	string	Optional	Описание актива
coordinates	string	Optional	Координаты актива (не используется)
active	boolean	Optional	Флаг активности
scan_id	string	Optional	ID сканера активов (не используется)
value	integer	Optional	Значимость актива. В платформе значимость актива может принимать следующие значения: - 1 – ключевой; - 2 – важный; - 3 – некритичный; - 4 – распределенный; - 5 – тестовый.
client_note	string	Optional	Клиентские заметки (не используется)
internal_note	string	Optional	Внутренние заметки (не используется)
location	string	Required	Расположение актива
network_exposure	integer	Optional	Сетевая доступность актива. Тип сетевой видимости актива может принимать следующие значения: - 1 – актив напрямую подключен к сети Интернет; - 2 – актив располагается в демилитаризованной зоне (DMZ); - 3 – актив подключен к сети Интернет через Proxy-сервер; - 4 – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы; - 5 – актив не подключен к сети.
responsible_person	string	Optional	Ответственное лицо
technical_specialist	string	Optional	Технический специалист
responsible_group_id	string	Optional	ID группы ответственных
edited_by	string	Optional	Кем изменён (не используется)

Модель данных RuleSet

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор
created_at	string	Required	Дата создания
updated_at	string	Required	Дата изменения
name	string	Required	Название набора правил соответствия ПО. Уникальное
create_service_asset_findings	boolean	Optional	Флаг создания инцидентов

Модель данных _relations

Параметр	Тип данных	Обязательность	Описание
groups	Array<string>	Optional	Идентификаторы связанных групп пользователей
rule_sets	Array<string>	Optional	Идентификаторы связанных наборов правил
service_assets	Array<string>	Optional	Идентификаторы связанных активов
software_compliance_checks	Array<string>	Optional	Идентификаторы связанных проверок соответствия ПО

3.2.3 Создание группы активов

Запрос:

Тип	Метод
POST	/service_assets_create

Описание:

При выполнении запроса будет создана группа активов.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

Ключами в поле _relations могут быть названия полей моделей, ссылающиеся на другие. Например, если у модели связь с моделью правил корреляции и в нем хранится актив связанного правила, то это поле можно использовать при управлении данной связью

Управление работает следующим образом:

- Если поля в активе _relations отсутствуют зависимости не обновляются
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию
- Если поле зависимости указано и в значении пустой список, то все связи удаляются

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "service_assets": [] // - очистит все связи с активами
    // "service_assets": ["uuid1", "uuid2"] // - создаст связь с 2 активами
    // "service_assets": ["uuid1"] // - оставит связь только с первым активом
  }
}
```

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/service_asset_groups/create`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название группы активов
network_ranges	Array<string>	Optional	Список подсетей
domain	string	Optional	Домен
itsm_synced	boolean	Optional	Признак синхронизации с системой управления ИТ-услугами
regex	string	Optional	Регулярное выражение
subject_id	string	Optional	Идентификатор субъекта
object_id	string	Optional	Идентификатор объекта
is_kii	boolean	Optional	Признак принадлежности к объектам критической инфраструктуры

Параметр	Тип данных	Обязательность	Описание
is_fincert	boolean	Optional	Признак вхождения в систему информационного обмена между участниками финансового рынка
responsible_person	string	Optional	Имя ответственного пользователя
technical_specialist	string	Optional	Технический специалист
system_id	string	Optional	Идентификатор системы
responsible_group_id	string	Optional	Идентификатор ответственной группы
edited_by	string	Optional	Идентификатор пользователя, внесшего изменения
_relations	object<relations>	Optional	Словарь идентификаторов связанных объектов

Модель данных _relations

Параметр	Тип данных	Обязательность	Описание
groups	Array<string>	Optional	Идентификаторы связанных групп пользователей
rule_sets	Array<string>	Optional	Идентификаторы связанных наборов правил
service_assets	Array<string>	Optional	Идентификаторы связанных активов
software_compliance_checks	Array<string>	Optional	Идентификаторы связанных проверок соответствия ПО

Пример тела запроса:


```
{
  "trace_id": "uuid",
  "name": "string",
  "network_ranges": [],
  "domain": "string",
  "itsm_synced": false,
  "regex": "string",
  "subject_id": "string",
  "object_id": "string",
  "is_kii": false,
  "is_fincert": false,
  "responsible_person": "string",
  "technical_specialist": "string",
  "system_id": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "_relations": {
    "groups": [
```

```
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rule_sets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_assets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software_compliance_checks": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  }
}
```


Успешный ответ:

Статус код: 201 – успешное создание группы активов.

Формат: JSON.

Тело ответа: «Модель ресурса «Группы активов»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "name": "string",
  "network_ranges": [],
  "domain": "string",
  "itsm_synced": false,
  "regex": "string",
  "subject_id": "string",
  "object_id": "string",
  "is_kii": false,
  "is_fincert": false,
  "responsible_person": "string",
  "technical_specialist": "string",
  "system_id": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "software_compliance_checks": [
    {
      "service_asset_group_id": "89c15508-7cc6-40d3-94c1-0f63c26cac7d",
      "compliant": true,
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z"
    }
  ],
  "responsible_group": {
    "id": "uuid",
    "name": "string",
    "parent_group": "string",
    "realm_id": "string",
    "email": "string",
```

```
    "phone_number": "string",
    "leader_id": "string",
    "accept_risk": true,
    "visible_scan_schedules": true,
    "stop_scans": true,
    "edited_by": "string",
    "user_ids": [
      "uuid"
    ]
  },
  "groups": [
    {
      "id": "uuid",
      "name": "string",
      "parent_group": "string",
      "realm_id": "string",
      "email": "string",
      "phone_number": "string",
      "leader_id": "string",
      "accept_risk": true,
      "visible_scan_schedules": true,
      "stop_scans": true,
      "edited_by": "string",
      "user_ids": [
        "uuid"
      ]
    }
  ],
  "service_assets": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "type": "Host",
      "name": "Актив",
      "description": "Описание актива",
      "coordinates": "--- []",
      "active": true,
      "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
      "value": 3,
      "client_note": "string",
      "internal_note": "string",
      "location": "string",
      "network_exposure": 3,
      "responsible_person": "string",
      "technical_specialist": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
    }
  ],
  "rule_sets": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "New rule set",
      "create_service_asset_findings": false
    }
  ],
  "_relations": {
    "groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rule_sets": [
```

```
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_assets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software_compliance_checks": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  },
  "service_asset_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "service_asset_ids_count": 0,
  "responsible_group_name": "string",
  "group_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "rule_set_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "user_groups": [
    {
      "id": "uuid",
      "name": "Test group"
    }
  ],
  "performed_at": "string"
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
409	name_already_used	Попытка присвоить объекту существующее уникальное значение атрибута
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:


```
{
  "error": "Bad Request",
  "error_code": 400
}
```


Код 409:


```
{
  "error": "Bad Request",
  "error_code": 409,
  "extra": {
    "fields": [
      "name"
```

```
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.4 Обновление группы активов

Запрос:

Тип	Метод
PUT	/service_asset_groups/update

Описание:

При выполнении запроса будет обновлена информация о группе активов в соответствии с заданными параметрами.

Работает по принципу частичного обновления, т.е. будут обновлены только те поля, которые были переданы в запросе.

Позволяет также управлять связями многие ко многим с другими моделями через поле _relations.

В поле _relations в качестве ключей могут быть указаны названия полей моделей, которые ссылаются на другие модели. Например, если у модели связь с моделью правил корреляции и в нем хранится объект связанного правила, то это поле можно использовать при управлении данной связью.

Управление работает следующим образом:

- Если поля в активе _relations отсутствуют, то зависимости не обновляются;
- Если поле зависимости указано и в значении не пустой список идентификаторов, то связи модели приводятся к описанному состоянию;
- Если поле зависимости указано и в значении пустой список, то все связи удаляются.

Например, следующий запрос:

```
{
  "id": "uuid",
  ...
  "_relations": {
    "service_assets": [] // - очистит все связи с активами
    // "service_assets": ["uuid1", "uuid2"] // - создаст связь с 2 активами
    // "service_assets": ["uuid1"] // - оставит связь только с первым активом
  }
}
```

Пример запроса:

PUT

`http://127.0.0.1/cruddy/v2/service_asset_groups/update`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
id	string	Required	Идентификатор группы активов
trace_id	string	Required	Идентификатор трассировки действия пользователя для аудита
name	string	Required	Название группы активов
network_ranges	Array<string>	Optional	Список подсетей
domain	string	Optional	Домен
itsm_synced	boolean	Optional	Признак синхронизации с системой управления ИТ-услугами
regex	string	Optional	Регулярное выражение
subject_id	string	Optional	Идентификатор субъекта
object_id	string	Optional	Идентификатор объекта
is_kii	boolean	Optional	Признак принадлежности к объектам критической инфраструктуры
is_fincert	boolean	Optional	Признак вхождения в систему информационного обмена между участниками финансового рынка
responsible_person	string	Optional	Имя ответственного пользователя
technical_specialist	string	Optional	Технический специалист
system_id	string	Optional	Идентификатор системы
responsible_group_id	string	Optional	Идентификатор ответственной группы
edited_by	string	Optional	Идентификатор пользователя, внесшего изменения
_relations	object<relations>	Optional	Словарь идентификаторов связанных объектов

Модель данных _relations

Параметр	Тип данных	Обязательность	Описание
groups	Array<string>	Optional	Идентификаторы связанных групп пользователей
rule_sets	Array<string>	Optional	Идентификаторы связанных наборов правил
service_assets	Array<string>	Optional	Идентификаторы связанных активов
software_compliance_checks	Array<string>	Optional	Идентификаторы связанных проверок соответствия ПО

Пример тела запроса:


```
{
  "id": "uuid",
  "trace_id": "uuid",
  "name": "string",
  "network_ranges": [],
  "domain": "string",
  "itsm_synced": false,
  "regex": "string",
  "subject_id": "string",
  "object_id": "string",
  "is_kii": false,
  "is_fincert": false,
  "responsible_person": "string",
  "technical_specialist": "string",
  "system_id": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "_relations": {
    "groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rule_sets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_assets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software_compliance_checks": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  },
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08"
}
```


Успешный ответ:

Статус код: 200 - успешное обновление информации о группе активов.

Формат: JSON.

Тело ответа: «Модель ресурса «Группы активов»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "name": "string",
  "network_ranges": [],
  "domain": "string",
  "itsm_synced": false,
  "regex": "string",
  "subject_id": "string",
  "object_id": "string",
  "is_kii": false,
  "is_fincert": false,
  "responsible_person": "string",
  "technical_specialist": "string",
  "system_id": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "software_compliance_checks": [
    {
      "service_asset_group_id": "89c15508-7cc6-40d3-94c1-0f63c26cac7d",
      "compliant": true,
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z"
    }
  ],
  "responsible_group": {
    "id": "uuid",
    "name": "string",
    "parent_group": "string",
    "realm_id": "string",
    "email": "string",
    "phone_number": "string",
    "leader_id": "string",
    "accept_risk": true,
    "visible_scan_schedules": true,
    "stop_scans": true,
    "edited_by": "string",
    "user_ids": [
      "uuid"
    ]
  },
  "groups": [
    {
      "id": "uuid",
      "name": "string",
      "parent_group": "string",
      "realm_id": "string",
      "email": "string",
      "phone_number": "string",
      "leader_id": "string",
      "accept_risk": true,
      "visible_scan_schedules": true,
      "stop_scans": true,
      "edited_by": "string",
```

```
      "user_ids": [
        "uuid"
      ]
    }
  ],
  "service_assets": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "type": "Host",
      "name": "Актив",
      "description": "Описание актива",
      "coordinates": "--- []",
      "active": true,
      "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
      "value": 3,
      "client_note": "string",
      "internal_note": "string",
      "location": "string",
      "network_exposure": 3,
      "responsible_person": "string",
      "technical_specialist": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
    }
  ],
  "rule_sets": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "New rule set",
      "create_service_asset_findings": false
    }
  ],
  "_relations": {
    "groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rule_sets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_assets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software_compliance_checks": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  },
  "service_asset_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "service_asset_ids_count": 0,
  "responsible_group_name": "string",
  "group_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "rule_set_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "user_groups": [
    {
      "id": "uuid",
```

```
      "name": "Test group"
    }
  ],
  "performed_at": "string"
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Редактируемый объект не найден в БД
500	Internal Server Error	Другие ошибки при обновлении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.5 Поиск групп активов

Запрос:

Тип	Метод
POST	/service_asset_groups/search

Описание:

При выполнении запроса будут возвращены найденные объекты с учётом заданных фильтров.

По умолчанию в объекты не загружаются связанные модели по типам связи many2many и has-many, для включения загрузки их нужно указывать в поле relations объекта запроса.

Связи _relations загружаются всегда и отражают текущее состояние связей модели.

Пример запроса:

POST

`http://127.0.0.1/cruddy/v2/rule_sets/search`

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
include_fields	Array<string>	Required	Список полей для выборки. Если модель содержит поля, не указанные в запросе, они будут отсутствовать в ответе
exclude_fields	Array<string>	Required	Список полей для удаления из выборки. Если модель содержит поля, указанные в запросе, они будут отсутствовать в ответе
filters	Array<filters>	Required	Список фильтров по полям модели
ordering	Array<ordering>	Required	Настройки сортировки
virtual_search	object<virtual_search>	Required	Поле для поиска по подстроке по всем строковым полям модели и настройка строгого поиска
relations	Array<string>	Required	Список связей для выборки. Список доступных связей отображается в ответе запроса на получение метаданных - “/_meta”
limit	integer	Required	Лимит выдачи найденных объектов
offset	integer	Required	Отступ от начала результата поиска в базе
_relations	Array<string>	Optional	Перечисление связанных сущностей, идентификаторы которых нужно вернуть в ответе в поле _relations

Array of filters:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Название поля модели
value	object	Required	Значение для фильтрации
filter_type	string	Required	В зависимости от этого значения определяется допустимые значения в поле value. Допустимые значения: - equal -> строка|число, проверяет равенство значений

Параметр	Тип данных	Обязательность	Описание
			- substr -> строка, проверяет вхождение подстроки - intersection -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный массив - range -> массив (тип элемента зависит от типа поля), проверяет вхождение значения поля в переданный диапазон - related -> строка или массив строк (uuid), проверят связанность с моделью по идентификатору если value: [], проверяет наличие или отсутствие связанных сущностей - exists -> значение отсутствует, проверяется равенство колонки с null
negation	boolean	Optional	Флаг использования отрицания при проверке фильтра

Array of ordering:

Параметр	Тип данных	Обязательность	Описание
field	string	Required	Поле модели, выбранное для сортировки
direction	string	Required	Направление сортировки. Допустимые значения: - asc - desc

Object VirtualSearch:

Параметр	Тип данных	Обязательность	Описание
value	string	Required	Значение, выбранное для поиска
strict	boolean	Required	Опция, включающая строгий поиск. Возможные значения: - true - строгий поиск включена; - false - строгий поиск выключен.

Пример тела запроса:

```
{
  "include_fields": [
    "string"
  ],
  "exclude_fields": [
    "string"
  ],
  "filters": [
    {
      "field": "string",
      "value": [
        "name",
        [
          "value1",
          "value2"
        ]
      ],
      "filter_type": "equal",
      "negation": false
    }
  ],
```

```
  "ordering": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "virtual_search": {
    "value": "string",
    "strict": false
  },
  "relations": [
    "service_asset_findings",
    "logmule_go_rules",
    "user"
  ],
  "limit": 20,
  "offset": 0,
  "_relations": [
    "string"
  ]
}
```


Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array<ServiceAssetGroup>	Список найденных групп активов
total	integer	Количество найденных значений дополнительных полей

Пример ответа:


```
{
  "items": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "string",
      "network_ranges": [],
      "domain": "string",
      "itsm_synced": false,
      "regex": "string",
      "subject_id": "string",
      "object_id": "string",
      "is_kii": false,
      "is_fincert": false,
      "responsible_person": "string",
      "technical_specialist": "string",
```

```
"system_id": "string",
"responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
"edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
"software_compliance_checks": [
  {
    "service_asset_group_id": "89c15508-7cc6-40d3-94c1-0f63c26cac7d",
    "compliant": true,
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z"
  }
],
"responsible_group": {
  "id": "uuid",
  "name": "string",
  "parent_group": "string",
  "realm_id": "string",
  "email": "string",
  "phone_number": "string",
  "leader_id": "string",
  "accept_risk": true,
  "visible_scan_schedules": true,
  "stop_scans": true,
  "edited_by": "string",
  "user_ids": [
    "uuid"
  ]
},
"groups": [
  {
    "id": "uuid",
    "name": "string",
    "parent_group": "string",
    "realm_id": "string",
    "email": "string",
    "phone_number": "string",
    "leader_id": "string",
    "accept_risk": true,
    "visible_scan_schedules": true,
    "stop_scans": true,
    "edited_by": "string",
    "user_ids": [
      "uuid"
    ]
  }
],
"service_assets": [
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "created_at": "2023-12-20T00:00:01.652259Z",
    "updated_at": "2023-12-20T00:00:01.652259Z",
    "type": "Host",
    "name": "Актив",
    "description": "Описание актива",
    "coordinates": "--- []",
    "active": true,
    "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
    "value": 3,
    "client_note": "string",
    "internal_note": "string",
    "location": "string",
    "network_exposure": 3,
    "responsible_person": "string",
    "technical_specialist": "string",
```

```
            "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
            "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
          }
        ],
        "rule_sets": [
          {
            "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
            "created_at": "2023-12-20T00:00:01.652259Z",
            "updated_at": "2023-12-20T00:00:01.652259Z",
            "name": "New rule set",
            "create_service_asset_findings": false
          }
        ],
        "_relations": {
          "groups": [
            "497f6eca-6276-4993-bfeb-53cbbbba6f08"
          ],
          "rule_sets": [
            "497f6eca-6276-4993-bfeb-53cbbbba6f08"
          ],
          "service_assets": [
            "497f6eca-6276-4993-bfeb-53cbbbba6f08"
          ],
          "software_compliance_checks": [
            "497f6eca-6276-4993-bfeb-53cbbbba6f08"
          ]
        },
        "service_asset_ids": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "service_asset_ids_count": 0,
        "responsible_group_name": "string",
        "group_ids": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "rule_set_ids": [
          "497f6eca-6276-4993-bfeb-53cbbbba6f08"
        ],
        "user_groups": [
          {
            "id": "uuid",
            "name": "Test group"
          }
        ],
        "performed_at": "string"
      }
    ],
    "total": 1
}
```


Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при поиске объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.6 Получение группы активов по ID

Запрос:

Тип	Метод
GET	/service_asset_groups/{id}

Описание:

При выполнении запроса будет возвращена группа активов с соответствующим ID.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/service_asset_groups/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор группы активов

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа: «Модель ресурса «Группы активов»».

Пример ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "created_at": "2023-12-20T00:00:01.652259Z",
  "updated_at": "2023-12-20T00:00:01.652259Z",
  "name": "string",
  "network_ranges": [],
  "domain": "string",
  "itsm_synced": false,
  "regex": "string",
  "subject_id": "string",
  "object_id": "string",
  "is_kii": false,
  "is_fincert": false,
  "responsible_person": "string",
  "technical_specialist": "string",
  "system_id": "string",
  "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
  "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c",
  "software_compliance_checks": [
    {
      "service_asset_group_id": "89c15508-7cc6-40d3-94c1-0f63c26cac7d",
      "compliant": true,
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z"
    }
  ],
  "responsible_group": {
    "id": "uuid",
    "name": "string",
    "parent_group": "string",
    "realm_id": "string",
    "email": "string",
    "phone_number": "string",
    "leader_id": "string",
    "accept_risk": true,
    "visible_scan_schedules": true,
    "stop_scans": true,
    "edited_by": "string",
    "user_ids": [
      "uuid"
    ]
  },
  "groups": [
    {
      "id": "uuid",
      "name": "string",
      "parent_group": "string",
      "realm_id": "string",
      "email": "string",
      "phone_number": "string",
      "leader_id": "string",
      "accept_risk": true,
      "visible_scan_schedules": true,
```

```
      "stop_scans": true,
      "edited_by": "string",
      "user_ids": [
        "uuid"
      ]
    }
  ],
  "service_assets": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "type": "Host",
      "name": "Актив",
      "description": "Описание актива",
      "coordinates": "--- []",
      "active": true,
      "scan_id": "9a59f0f5-5572-476d-a7fc-c960ef43a5af",
      "value": 3,
      "client_note": "string",
      "internal_note": "string",
      "location": "string",
      "network_exposure": 3,
      "responsible_person": "string",
      "technical_specialist": "string",
      "responsible_group_id": "2d40d7ca-3218-4132-89ef-42e29379a567",
      "edited_by": "9501acb5-3be0-4719-a60e-dfa79624666c"
    }
  ],
  "rule_sets": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "created_at": "2023-12-20T00:00:01.652259Z",
      "updated_at": "2023-12-20T00:00:01.652259Z",
      "name": "New rule set",
      "create_service_asset_findings": false
    }
  ],
  "_relations": {
    "groups": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "rule_sets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "service_assets": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "software_compliance_checks": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
  },
  "service_asset_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "service_asset_ids_count": 0,
  "responsible_group_name": "string",
  "group_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "rule_set_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "user_groups": [
```

```
    {
      "id": "uuid",
      "name": "Test group"
    }
  ],
  "performed_at": "string"
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
500	Internal Server Error	Другие ошибки при получении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.7 Удаление группы активов

Запрос:

Тип	Метод
DELETE	/service_asset_groups/{id}

Описание:

При выполнении запроса будет удалена группа активов с соответствующим ID.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/service_asset_groups/{id}
```

Path параметры запроса:

Параметр	Описание
{id}	Идентификатор группы активов

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
404	Not Found	Объект не найден в БД
422	11002 11003 11011	Общая ошибка удаления Запрос не затронул ни одной сущности Удаление невозможно из-за наличия блокирующих связей
500	Internal Server Error	Другие ошибки при удалении объекта

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
```

```
  "error": "Bad Request",
  "error_code": 400
}
```

Код 404:

```
{
  "error": "Not Found",
  "error_code": 404
}
```

Код 422:

```
{
  "error": "string",
  "error_code": "11002 // общая ошибка удаления",
  "relations": {
    "dynamic_relation_name": [
      {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string"
      }
    ]
  }
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.8 Группировка групп активов по заданному полю

Запрос:

Тип	Метод
POST	/service_asset_groups/group

Описание:

При выполнении запроса группы активов будут сгруппированы по заданному полю.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_groups/group
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
group_field	string	Required	Поле для группировки объектов

Пример тела запроса:

```
{
  "group_field": "string"
}
```

Успешный ответ:

Статус код: 200 – успешный ответ.

Формат: JSON.

Параметры ответа:

Параметр	Тип данных	Описание
items	Array	Список объектов, сгруппированных по полю
items**{value}**	string	Значение поля
items**{count}**	integer	Количество повторений

Пример ответа:

```
{
  "items": [
    {
      "value": "string",
      "count": 1
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Ошибка маппинга поля группировки с моделью группируемых объектов, другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса*.

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.9 Массовое удаление групп активов

Запрос:

Тип	Метод
POST	/service_asset_groups/mass_delete

Описание:

При выполнении запроса будут удалены группы активов с соответствующими ID.

Пример запроса:

POST

```
http://127.0.0.1/cruddy/v2/service_asset_groups/mass_delete
```

Тело запроса:

Параметр	Тип данных	Обязательность	Описание
ids	Array<string>	Required	Список ID удаляемых объектов

Пример тела запроса:

```
{
  "ids": [
    "string"
  ]
}
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
results	Array<object>	Список результатов по удаляемым объектам
results**{id}**	string	Уникальный идентификатор объекта
results**{error_code}**	integer	Код ошибки удаления. Допустимые значения: - 0 - отсутствие ошибки - успешное удаление; - 11001 - ошибка связанных данных (зависимостей) - 11002 - общая ошибка удаления (выполнения запроса в БД); - 11003 - запрос не затронул ни одной сущности.

Пример ответа:

```
{
  "results": [
    {
      "id": "string",
      "error_code": 0
    }
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание
400	Bad Request	Неверный тип параметра запроса, либо отсутствует обязательный параметр
500	Internal Server Error	Другие ошибки при удалении объектов

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 400:

```
{
  "error": "Bad Request",
  "error_code": 400
}
```

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.10 Удаление всех групп активов

Запрос:

Тип	Метод
DELETE	/service_asset_groups/all

Описание:

При выполнении запроса из базы данных будут удалены все группы активов.

Пример запроса:

DELETE

```
http://127.0.0.1/cruddy/v2/service_asset_groups/all
```

Успешный ответ:

Статус код: 204 – запрос успешно обработан.

Формат: пустое тело ответа.

Другие возможные ответы:

Код	Ответ	Описание

Код	Ответ	Описание
500	Internal Server Error	Другие ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```

3.2.11 Получение свойств полей групп активов и действий пользователей

Запрос:

Тип	Метод
GET	/service_asset_groups/_meta

Описание:

При выполнении запроса будут возвращены свойства полей групп активов и список действий пользователей над ними.

Пример запроса:

GET

```
http://127.0.0.1/cruddy/v2/service_asset_groups/_meta
```

Успешный ответ:

Статус код: 200 – запрос успешно обработан.

Формат: JSON.

Тело ответа:

Параметр	Тип данных	Описание
fields	Array	Список полей для пользовательского интерфейса
fields**{name}**	string	Название поля
fields**{type}**	string	Тип данных, поддерживаемый полем. Например: - string; - date; - boolean.
fields**{filters}**	Array<string>	Список фильтров. Допустимые значения: - equal; - substr; - intersection; - range.
actions	Array<string>	Список массовых действий
instance_actions	Array	Список действий над отдельными объектами
instance_actions**{action}**	string	Название действия
instance_actions**{params}**	object	Параметры, определяющие действие
relations	Array<string>	Список связей

Пример ответа:

```
{
  "fields": [
    {
      "name": "string",
      "type": "boolean",
      "filters": [
        "equal"
      ]
    }
  ],
  "actions": [
    "string"
  ],
  "instance_actions": [
    {
      "action": "string",
      "params": {}
    }
  ],
  "relations": [
    "string"
  ]
}
```

Другие возможные ответы:

Код	Ответ	Описание

Код	Ответ	Описание
500	Internal Server Error	Ошибки сервера

Примечание: *Текст ошибки не фиксированный, может изменяться в зависимости от фактического ответа получателя запроса.*

Код 500:

```
{
  "error": "Internal Server Error",
  "error_code": 500
}
```