Платформа Радар

Описание публичного API

Версия 3.5.4

ООО Пангео Радар

Содержание

API для внешних потребителей

API для внешних потребителей используется для интеграции внешних потребителей с **Платформой Радар** на программном уровне.

Для авторизации в методах используется ключ API, который можно получить в настройках кластера **Платформы Радар**.
Для вызова методов вам понадобится значение ***global_api_key***.

Особености работы с API через провайдера мультиарендности Karaken

Платформа Радар, начиная с версии 3.2.0, позволяет выбирать инстанс, к которому должен обращаться метод API. Если инстанс в методе API не указан, то обращение идет к основному инстансу.

MASTER_KARAKEN_HOST - это основная точка входа для обработки запросов, для обращений API используются порты 9000 и 9009.

Получение списка подключенных инстансов

Тип метода: GET

Метод

`https://<MASTER_KARAKEN_HOST>:9000/karaken/instance/list`

Заголовки (headers):

`PgrApiKey: api_key_string`

`Content-Type: application/json`

Входные параметры: отсутствуют

Выходные параметры:

Параметр	Описание
id	Идентификатор инстанса
name	Наименование инстанса
url	URL инстанса с номером используемого порта
sort_order	Порядок сортировки

Пример ответа:

```
[
    {
        "id": "38c62166-0a5e-f51a-d583-6de7c200ef8a",
        "name": "172.30.254.70",
        "url": "https://172.30.254.70:9000",
        "sort_order": 0
    },
    {
        "id": "38c62166-0a5e-f51a-d583-6de7c200ef9a",
        "name": "172.30.254.70 (2)",
        "url": "https://172.30.254.70:9000",
        "sort_order": 0
    }
]
```

Выполнение запросов к подчиненным инстансам

Для выполнения запроса к подчиненному инстансу необходимо в заголовке, помимо APIKey, передать идентификатор требуемого инстанса. В этом случае метод будет обработан указанным инстансом.

Например, если сделать запрос к получению списка инцидентов с указанием идентификатора инстанса из спсика инстансов в заголовке `PgrSelectedInstance: <string>`:

```
GET https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/incidents?
page=1&per_page=1&order=id%20DESC

Headers:
PgrApiKey: api_key_string
PgrSelectedInstance: 38c62166-0a5e-f51a-d583-6de7c200ef9a
Content-Type: application/json
```

то будет получен ответ:

```
[
    {
        "objects": [
            {
```

```
                "id": "c017287c-7e30-42c2-bcfd-d62e5e9d71b5",
                "description": "..."
            },
            {
                "id": "c017287c-7e30-42c2-bcfd-d62e5e9d71b6",
                "description": "..."
            }
        ],
        "total": 2
    }
]
```

Как видно из ответа, компонент Karaken возвращает массив объектов, содержащих в себе детали запроса в подчиненный инстанс. Указание конкретного инстанса приводит к ограничению количества
элементов массива к одному конкретно указанному инстансу.

Если же не указать заголовок `PgrSelectedInstance`, то ответ будет содержать в себе все подмножество подключенных инстансов.

В таком режиме не рекомендуется использовать фильтрацию или пагинацию, т.к. данные среди всех инстансов могут не совпадать. При этом, при указании конкретного инстанса с помощью заголовка
`PgrSelectedInstance` возможно осуществлять все API операции через мастер сервер со всеми подчиненными инстансами. Разница будет лишь в том, что формат ответа будет отличаться от прямого
взаимодействия, а само тело ответа будет находиться в ключе`data` внутри элемента массива запрашиваемого инстанса.

Использование стандартных фильтров

Многие описанные ниже методы поддерживают стандартные фильтры - возможность отфильтровать возвращаемые данные по выходному параметру по условиям:

- **like**. Позволяет отфильтровать по вхождению в параметре. Пример:

  `?id=like,31549173`

  Будут найдены все идентификаторы, содержащие `31549173`

- **gt**. Позволяет отфильтровать по значению параметра, больше указанного значения. Пример:

  `?created_at=gt,2020-01-01`

  Будут отобраны записи, созданные после `2020-01-01`

- **lt**. Позволяет отфильтровать по значению параметра, меньше указанного значения. Пример:

  `?created_at=lt,2020-01-01`

  Будут отобраны записи, созданные до `2020-01-01`

- **in**. Позволяет отфильтровать по вхождению параметра в список значений. Пример:

  `?id=in,31549173-fa4c-4a5c-a9e1-1107dbb8a48d,31549173-fa4c-4a5c-a9e1-1107dbb8a49d`

  Будут отобраны идентификаторы, входящие в указанный список.

- **notin**. Позволяет отфильтровать по исключению вхождения параметра в список значений. Пример:

`?id=notin,31549173-fa4c-4a5c-a9e1-1107dbb8a48d,31549173-fa4c-4a5c-a9e1-1107dbb8a49d`

Будут отобраны идентификаторы, не входящие в указанный список.

- **eq**. Позволяет задать точное соответствие параметра значению. Пример:

  `?id=eq,31549173-fa4c-4a5c-a9e1-1107dbb8a48d`

  Будет найден идентификатор с указанным значением.

- **noteq**. Позволяет задать исключение точного соответствия параметра значению. Пример:

  `?id=noteq,31549173-fa4c-4a5c-a9e1-1107dbb8a48d`

  Будут найдены идентификаторы кроме идентификатора с указанным значением.

- **isnull**. Позволяет отфильтровать по пустому значению параметра. Пример:

  `?fileid=isnull`

  Будут отобраны записи с пустыми идентификаторами файлов.

- **isnotnull**. Позволяет отфильтровать по непустому значению параметра. Пример:

  `?fileid=isnotnull`

  Будут отобраны записи с непустыми идентификаторами файлов.

Для некоторых методов необходимо указывать имя параметра с именем сущности через точку. Например `?finding.created_at=gt,2020-01-01`

Также в query строке запроса можно указать дополнительные параметры: page (номер страниц), per_page (количество строк в странице) для пагинации, order для сортировки,
search для поиска по нескольким полям сущности.

Описание методов API

Инциденты

Получение списка типов инцидентов

Тип метода: GET

Метод
`https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/findings`

Заголовки (headers):
`PgrApiKey: api_key_string`
`PgrSelectedInstance: string`
`Content-Type: application/json`

Входные параметры:

Поддерживаются стандартные фильтры

Выходные параметры и пример ответа:

```
{
  "objects": [
    {
      "title": "MS-WIN-Изменение политики аудита",
```

```
      "description": "На одном или нескольких узлах обнаружены изменения политики аудита. Это событие может указывать на несанкционированную деятельность злоумышленника. Поэтому к нему следует отнестись с большим вниманием: подобные действия могут понизить уровень безопасности в компании. Групповая политика – это функция семейства операционных систем Microsoft Windows NT, которая обеспечивает управление рабочей средой учетных записей пользователей и компьютеров. Групповая политика обеспечивает централизованные управление и настройку операционных систем, приложений и пользовательских параметров в среде Active Directory. Набор конфигураций групповой политики называется объектом групповой политики (Group Policy Object, GPO). Версия групповой политики, называемая локальной групповой политикой (LGPO или LocalGPO), позволяет управлять объектами групповой политики без использования Active Directory на автономных компьютерах. ",
      "risk_impact": "Незапланированное изменение правила политики аудита неавторизованным пользователем представляет большой риск. В худшем случае ИТ-система может оказаться уязвимой к различным атакам злоумышленников и вредоносного ПО. Воспользовавшись этой уязвимостью, злоумышленники могут получить полный контроль над ИТ-системой и возможность красть, изменять и удалять данные или устанавливать программы-вымогатели без ведома владельцев системы. \r\n \r\nh2. Ссылки \r\n \r\nhttps://docs.microsoft.com/en-us/windows/desktop/srvnodes/group-policy \r\nhttps://www.varonis.com/blog/group-policy/ ",
      "solution": "* Убедитесь, что действие запланировал и выполнил авторизованный пользователь, используя установленные процессы и процедуры управления изменениями. \r\n* Рассмотрите возможность отслеживания изменений и обновлений рабочих систем с помощью системы управления изменениями (например, системы отслеживания). Сопоставляйте такие события с утвержденными/ авторизованными изменениями. \r\n* Измените права на защищенный доступ к журналам событий соответствующим образом. Это можно сделать локально или через групповую политику.",
      "created_at": "2023-04-10T13:08:01.29391Z",
      "updated_at": "2023-04-10T13:08:01.29391Z",
      "id": "31549173-fa4c-4a5c-a9e1-1107dbb8a48d",
      "display_id": 67,
      "mitigation": "Профилактика вредоносной деятельности эффективнее, чем исправление ее последствий. Далее приведен список основных рекомендаций по повышению безопасности ваших систем: \r\n \r\n* Если настройки аудита были изменены, верните их в исходное состояние. \r\n* Если известен идентификатор входа в систему, используйте его для сопоставления с другими связанными событиями (например, идентификатор события 4624). \r\n* Убедитесь, что только доверенные сотрудники могут изменять настройки рабочих систем и что все такие изменения авторизуются и регистрируются системой управления изменениями. \r\n* Если внесенное изменение является несанкционированным, клиент должен выяснить причину его внесения и потенциальную степень его влияния на систему. ",
      "synopsis": "Обнаружены изменения политики аудита. ",
      "local": false,
      "type": "policy_violation",
      "identifier": {
        "maxpatrol": {},
        "nessus": {},
        "redcheck": {}
      },
      "comment": "",
      "fallback_raw_risklevel": 0,
      "new_version": false,
      "client_note": "",
```

```
      "internal_note": "",
      "cpes": [],
      "category_id": "",
      "customer_created": false,
      "software_compliance": false,
      "itsm_last_synced_at": null,
      "updated_by": "",
      "created_by_customer": "",
      "edited_by": "",
      "front_link": "http://172.30.254.75/rmc/incidents/types/show/31549173-fa4c-
4a5c-a9e1-1107dbb8a48d"
    }
  ],
  "total": 1
}
```


Получение списка инцидентов

Тип метода: GET

Метод

`https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/incidents?page=1&per_page=1&order=id%20DESC`

Заголовки (headers):

`PgrApiKey: api_key_string`

`PgrSelectedInstance: string`

`Content-Type: application/json`

Входные параметры:

Поддерживаются стандартные фильтры

Выходные параметры и пример ответа:

```
{
    // массив инцидентов
    "objects": [
        {
            // идентификатор инцидента
            "id": "00000000-0000-0000-0000-000000000004b",
            // ОПИСАНИЕ УГРОЗЫ
            "description": "Модуль аналитики киберугроз обнаружил попытку
установить связь с
            использованием подозрительного сертификата TLS. Злоумышленники могут
использовать
            сертификаты с истекшим сроком действия или ненадежные сертификаты
для своих целей.
            Протокол защиты транспортного уровня (Transport Layer Security) TLS
обеспечивает
            шифрование соединения между сервером и клиентами. В соответствии со
стандартом PCI,
            «для обеспечения соответствия требованиям стандарта защиты данных
PCI (PCI DSS) в
            отношении безопасности платежных данных следует до 30 июня 2018 года
прекратить
```

использование протокола SSL и ранней версии протокола TLS и внедрить усовершенствованный протокол шифрования TLS версии 1.1 или выше (настоятельно рекомендуется использовать TLS v1.2)». ",
// ПОСЛЕДСТВИЯ РЕАЛИЗОВАННОЙ УГРОЗЫ
"risk_impact": "Связь с использованием вредоносных сертификатов TLS является подозрительной и может оказать негативное влияние на корпоративную сеть. В случае успеха злоумышленника наиболее опасными являются следующие риски: \r\n \r\n* Раскрытие информации: Уязвимость, которая может привести к раскрытию учетных данных жертвы. В результате киберпреступник может получить действительные учетные данные, а с их помощью – доступ к конфиденциальной информации. \r\n* Повышение привилегий: Злоумышленник, успешно воспользовавшийся этой уязвимостью, может запустить произвольный код от имени администратора. В этом случае он также получает возможность устанавливать программы, просматривать, изменять и удалять данные, создавать новые учетные записи с полными правами пользователя. \r\n* Удаленное выполнение кода: Эта уязвимость позволяет злоумышленнику получить доступ к чужому вычислительному устройству и вносить изменения, независимо от географического расположения этого устройства. \r\n* Распространение вредоносного контента или спама, а также перенаправление доменов на страницы с вредоносным контентом и выдача себя за владельцев учетных записей с целью распространения фальшивого контента или вредоносных ссылок. \r\n* Сбор учетных данных для продажи третьим сторонам. \r\n \r\nh2. Ссылки \r\n\r\nhttps://www.greenhousedata.com/blog/how-secure-is-https-tls-ssl-increasingly•used-to-transmit-malware \r\nhttp://www.certificate-transparency.org/what-is-ct \r\nhttps://www.csoonline.com/article/3212965/why-ssl-tls-attacks-are-on-the-rise.html \r\nhttps://www.pcisecuritystandards.org/document_library ",
// РЕКОМЕНДАЦИИ ПО УСТРАНЕНИЮ УГРОЗЫ
"solution": "* Немедленно заблокируйте трафик, направленный на целевой узел. \r\n* Проверьте узел на предмет взлома. \r\n* Проанализируйте, является ли такое поведение признаком действий злоумышленников. \r\n* Просканируйте узел с помощью антивирусной программы на предмет наличия угроз и устраните их в случае выявления. \r\n* Установите корневой центр сертификации на все подключаемые к узлу клиенты. Для этого используйте групповые политики Windows: 1) Откройте соответствующий объект

```
            групповой политики (GPO) 2) В дереве консоли выберите узел
«Доверенные корневые центры
            сертификации»: имя объекта политики/конфигурация компьютера/
настройки Windows/настройки
            безопасности/политики открытого ключа/доверенные корневые центры
сертификации 3)
            Выберите пункт «Все задачи» в меню «Действие» и нажмите на кнопку
[Импорт...] для
            добавления корневого сертификата.",
            // РЕКОМЕНДАЦИИ ПО УМЕНЬШЕНИЮ РИСКА
            "mitigation": "* Отключите узел-источник от сети. \r\n* Используйте
только
            сертификаты, подписанные доверенным центром сертификации. \r\n*
Проверяйте брандмауэр и
            групповые политики. ",
            // Статус инцидента
            "status": "new",
            // Уровень значимости инцидента
            "risklevel": 7,
            // идентификатор актива связанного с инцидентом
            "service_asset_id": "00000000-0000-0000-0000-000000000153",
            // дата создания инцидента
            "created_at": "2021-10-21T07:04:35.717156Z",
            // дата обновления инцидента
            "updated_at": "2021-10-21T07:04:36.969609Z",
            // идентификатор типа инцидента
            "finding_id": "5000ed94-823b-4b28-bf05-2aeade5632ac",
            // результаты анализа инцидента
            "analysis_output": "",
            // Краткое описаниа инцидента
            "synopsis": "Обнаружена попытка установить связь с использованием
подозрительного сертификата TLS.",
            // Наименование инцидента
            "title": "Обнаружена попытка установить связь с использованием
подозрительного сертификата TLS",
            // Уровень риска инцидента
            "risk": "medium",
            // Дата принятия инцидента
            "acknowledged_at": null,
            // Скоринговое число инцидента
            "immediate_action_score": 0.71502495,
            // Период реакции на инцидент
            "throughput_period": "normal",
            // Дата изменения периода реакции на инцидент
            "throughput_period_change": "2021-10-21T07:04:36.261123Z",
            // идентификатор правила корреляции
            "logmule_identifier": "",
            // Идентификатор последнегое происшествия
            "last_occurrence_id": "00000000-0000-0000-0000-000000000128",
            // Назначено на пользователя (идентификатор)
            "user_id": "",
            // Дата изменения инцидента
            "updated_by": "93adf94b-0f93-45d1-8b3c-a15a38399d49",
            // Назначено на группу пользователей (идентификатор)
            "group_id": "eedb34c7-9c94-4226-8504-ecc1ea3ab46d",
```

```
            // Инцидент принят пользователем (идентификатор)
            "acknowledged_by": "",
            // Инцидент изменен пользователем (идентификатор)
            "edited_by": "",
            // Наименование актива связанного с инцидентом
            "service_asset_name": "127.0.0.1",
            // Наличие актива связанного с инцидентом
            "service_asset_active": true,
            // Кол-во происшествий
            "occurrence_count": 5,
            // Логин назначенного пользователя
            "user_short_name": "",
            // Наименование группы назначенных пользователей
            "group_name": "users",
            // Человеко-читаемый идентификатор типа инцидента
            "finding_display_id": 53,
            // кол-во переоткрытий инцидента
            "reopened_count": 0,
            // тип сообытия
            "event_type": "logmule_result",
            // тип инцидента
            "finding_type": "network_anomaly",
            // айпи адресс последнего происшествия
            "last_occurrence_ip": "127.0.0.1",
            // Дата последней смены статуса инцидента
            "last_status_change": "2021-10-21T07:04:35.983333Z",
            // Дата проведения сканирования
            "last_scan": null,
            // Дата последнего происшествия
            "last_occurrence": "2021-10-21T07:04:33.255Z",
            // Уязвимость эксплуатируется удаленно?
            "remote_exploitable": false,
            // Сетевая видимость актива
            "service_asset_network_exposure": 3,
            // Отображаемое имя инцидента
            "display_title": "Обнаружена попытка установить связь с
использованием подозрительного сертификата TLS",
            // Время реакции на инцидент
            "customer_retention_time": 0,
            // известен с даты
            "visible_since": null,
            // известен в кол-ве дней
            "visible_since_in_days": 0,
            // Пользователь последний изменивший статус инцидента
            "last_customer_status_change": null,
            // Объект актива связанного с инцидентом
            "service_asset": {
                "id": "00000000-0000-0000-0000-000000000153",
                "type": "Host",
                "name": "127.0.0.1",
                "description": "",
                "coordinates": "--- [] ",
                "active": true,
                "scan_id": "",
                "value": 3,
```

```
                "client_note": "",
                "internal_note": "",
                "location": "",
                "network_exposure": 3,
                "responsible_person": "",
                "technical_specialist": "",
                "responsible_group_id": "eedb34c7-9c94-4226-8504-ecc1ea3ab46d",
                "edited_by": ""
            },
            // Происшествия связанные с инцидентом
            "occurrences": [
                {
                    // идентификатор происшествия
                    "id": "c17e0980-89e5-4cce-8e89-9ee678747c7b",
                    // тип события
                    "event_type": "logmule_result", // manual_source
                    // ip хоста вызвавшего происшествие
                    "ip": "127.0.0.1",
                    // порт хоста вызвавшего происшествие
                    "port": 0,
                    // мак адрес хоста вызвавшего происшествие
                    "mac": "",
                    // начало проишествия
                    "start_occurrence": "2021-09-10T10:33:30Z",
                    // окончание проишествия
                    "end_occurrence": "2021-09-10T10:33:30Z",
                    // идентификатор инцидента связанного с проишествием
                    "service_asset_finding_id": "00000000-0000-0000-0000-
000000000004b",
                    // дата создания проишествия
                    "created_at": "2021-09-10T10:43:49.150985Z",
                    // дата изменения проишествия
                    "updated_at": "2021-09-10T10:43:49.150985Z",
                    // FQDN хоста вызвавшего происшествие
                    "fqdn": "WINSRV02.demo.local",
                    "logmule_result": {
                        // идентификатор результата сработки правила
                        "id": "48d1c174-6d3e-4859-85bd-70da6a5e3aff",
                        // идентификатор правила корреляции
                        "rule_id": "f1a5609b-bb13-4f8f-948b-92147b617f78",
                        // Дата создания сработки
                        "created_at": "2021-09-15T09:21:59.44004Z",
                        // Дата изменения сработки
                        "updated_at": "2021-09-15T09:21:59.44004Z",
                        // результат анализа сработки правила
                        "analysis_output": "Зафиксирована неуспешная попытка
аутентификации с узла \"\" (\"\") с IP-адресом 192.168.200.2 под УЗ с истекшим
сроком действия пароля \"akuchelev\".",
                        // событие вызвавшее сработку правила корреляции
                        "event": {
                            // логлайны вызвавшие сработку
                            "@loglines": {
                                "1Os": [
                                    {
                                        "@__data_class__": [
```

```
                                        "logmule.logline",
                                        "Logline"
                                    ],
                                    "@timestamp": "2021-09-
15T12:22:30.798416+00:00",
                                    "action": "authenticate",
                                    "epoch": 1631708550.798416,
                                    "event": {
                                        "auth": {
                                            "key": {
                                                "length": 0
                                            },
                                            "method": {
                                                "description": "A user or
computer logged on to this computer from the network - 3",
                                                "id": "3"
                                            },
                                            "protocol": {
                                                "name": "NTLM",
                                                "version": "-"
                                            }
                                        },
                                        "category": "host_authentication",
                                        "description": "An account failed to
log on.",
                                        "logsource": {
                                            "application": "os",
                                            "host": "172.19.0.2",
                                            "input": "file-input",
                                            "name": "Microsoft Windows",
                                            "product": "windows",
                                            "subsystem": "authentication",
                                            "vendor": "microsoft"
                                        },
                                        "severity": 6.0,
                                        "subcategory":
"host_authentication_failed",
                                        "timestamp": "2021-09-
15T12:22:30.7984162Z",
                                        "uuid":
"AAAAAGFBuzOrp+C7hegeVZv+G96QLMhg",
                                        "worker": {
                                            "host": "c96a88b69f66",
                                            "internal": false,
                                            "ip": "172.19.0.2"
                                        }
                                    },
                                    "initiator": {
                                        "host": {
                                            "fqdn": [],
                                            "hostname": [],
                                            "internal": false,
                                            "ip": [
                                                "192.168.200.2"
                                            ]
```

```
                                        },
                                        "socket": {
                                            "port": 3466
                                        },
                                        "user": {
                                            "domain": "-",
                                            "id": "S-1-0-0",
                                            "name": "-"
                                        }
                                    },
                                    "observer": {
                                        "event": {
                                            "id": "4625",
                                            "type": "security"
                                        },
                                        "host": {
                                            "fqdn": [
                                                "v-demo-dc01.demo.local"
                                            ],
                                            "hostname": [],
                                            "internal": false,
                                            "ip": []
                                        }
                                    },
                                    "outcome": {
                                        "description": "unknown -
0xC0000071",
                                        "name": "failure",
                                        "original": "0xC0000071"
                                    },
                                    "reportchain": {
                                        "collector": {
                                            "host": {
                                                "fqdn": [],
                                                "hostname": [
                                                    "v-stand-09"
                                                ],
                                                "internal": false,
                                                "ip": []
                                            },
                                            "timestamp": "2021-09-
13T01:39:46.393963+03:00"
                                        },
                                        "relay": {
                                            "host": {
                                                "fqdn": [],
                                                "hostname": [],
                                                "internal": false,
                                                "ip": [
                                                    "172.30.254.106"
                                                ]
                                            }
                                        }
                                    },
```

```
                                        "routing_key":
"#.microsoft.windows.os.authentication.#",
                                        "target": {
                                            "auth": {
                                                "process": {
                                                    "name": "NtLmSsp"
                                                }
                                            },
                                            "host": {
                                                "fqdn": [
                                                    "v-demo-dc01.demo.local"
                                                ],
                                                "hostname": [],
                                                "internal": false,
                                                "ip": []
                                            },
                                            "process": {
                                                "path": {
                                                    "original": "-"
                                                }
                                            },
                                            "user": {
                                                "domain": "DEMO",
                                                "id": "S-1-0-0",
                                                "name": "akuchelev"
                                            }
                                        }
                                    },
                                    {
                                        "@__data_class__": [
                                            "logmule.logline",
                                            "Logline"
                                        ],
                                        "@timestamp": "2021-09-
15T12:22:35.798416+00:00",
                                        "action": "authenticate",
                                        "epoch": 1631708555.798416,
                                        "event": {
                                            "auth": {
                                                "key": {
                                                    "length": 0
                                                },
                                                "method": {
                                                    "description": "A user or
computer logged on to this computer from the network - 3",
                                                    "id": "3"
                                                },
                                                "protocol": {
                                                    "name": "NTLM",
                                                    "version": "-"
                                                }
                                            },
                                            "category": "host_authentication",
                                            "description": "An account failed to
log on.",
```

```
                                        "logsource": {
                                            "application": "os",
                                            "host": "172.19.0.2",
                                            "input": "file-input",
                                            "name": "Microsoft Windows",
                                            "product": "windows",
                                            "subsystem": "authentication",
                                            "vendor": "microsoft"
                                        },
                                        "severity": 6.0,
                                        "subcategory":
"host_authentication_failed",
                                        "timestamp": "2021-09-
15T12:22:35.7984162Z",
                                        "uuid":
"AAAAAGFBuzMFtX1RDhFsHdyljRn8svp2",
                                        "worker": {
                                            "host": "c96a88b69f66",
                                            "internal": false,
                                            "ip": "172.19.0.2"
                                        }
                                    },
                                    "initiator": {
                                        "host": {
                                            "fqdn": [],
                                            "hostname": [],
                                            "internal": false,
                                            "ip": [
                                                "192.168.200.2"
                                            ]
                                        },
                                        "socket": {
                                            "port": 3466
                                        },
                                        "user": {
                                            "domain": "-",
                                            "id": "S-1-0-0",
                                            "name": "-"
                                        }
                                    },
                                    "observer": {
                                        "event": {
                                            "id": "4625",
                                            "type": "security"
                                        },
                                        "host": {
                                            "fqdn": [
                                                "v-demo-dc01.demo.local"
                                            ],
                                            "hostname": [],
                                            "internal": false,
                                            "ip": []
                                        }
                                    },
                                    "outcome": {
```

```
                                        "description": "unknown -
0xC0000071",
                                        "name": "failure",
                                        "original": "0xC0000071"
                                    },
                                    "reportchain": {
                                        "collector": {
                                            "host": {
                                                "fqdn": [],
                                                "hostname": [
                                                    "v-stand-09"
                                                ],
                                                "internal": false,
                                                "ip": []
                                            },
                                            "timestamp": "2021-09-
13T01:39:46.393963+03:00"
                                        },
                                        "relay": {
                                            "host": {
                                                "fqdn": [],
                                                "hostname": [],
                                                "internal": false,
                                                "ip": [
                                                    "172.30.254.106"
                                                ]
                                            }
                                        }
                                    },
                                    "routing_key":
"#.microsoft.windows.os.authentication.#",
                                    "target": {
                                        "auth": {
                                            "process": {
                                                "name": "NtLmSsp"
                                            }
                                        },
                                        "host": {
                                            "fqdn": [
                                                "v-demo-dc01.demo.local"
                                            ],
                                            "hostname": [],
                                            "internal": false,
                                            "ip": []
                                        },
                                        "process": {
                                            "path": {
                                                "original": "-"
                                            }
                                        },
                                        "user": {
                                            "domain": "DEMO",
                                            "id": "S-1-0-0",
                                            "name": "akuchelev"
                                        }
```

```
                                    }
                                }
                            ]
                        },
                        "@over": [
                            "initiator.host.ip",
                            "initiator.host.fqdn",
                            "initiator.host.hostname",
                            "target.user.name"
                        ],
                        "@routing_key":
"#.microsoft.windows.os.authentication.#",
                        // дата события
                        "@timestamp": "2021-09-15T12:22:30+00:00",
                        "@values": {
                            "10s": 2
                        },
                        "@window_list": [
                            "10s"
                        ],
                        "end_event_time": 1631708555,
                        "initiator": {
                            "host": {
                                "fqdn": [],
                                "hostname": [],
                                "ip": [
                                    "192.168.200.2"
                                ]
                            }
                        },
                        "start_event_time": 1631708550,
                        "target": {
                            "user": {
                                "name": "***"
                            }
                        }
                    },
                    "acknowledged": false,
                    "risklevel": 4,
                    "occurred_at": "2021-09-15T12:22:30Z",
                    "occurrence_id": "c17e0980-89e5-4cce-8e89-9ee678747c7b",
                    "error": "",
                    "service_asset_id": "00000000-0000-0000-0000-
000000000153",
                    "asset_info": {
                        "ip": "192.168.200.2",
                        "hostname": "",
                        "fqdn": "",
                        "mac": ""
                    },
                    "incident_identifier": "***"
                }
            }
        ],
        // ссылка на инцидент
```

```
            "front_link": "http://127.0.0.1:8080/rmc/incidents/show/00000000-
0000-0000-0000-00000000004b"
        }
    ],
    // общий счетчик кол-во инцидентов в ответе
    "total": 4
}
```

Обновление статуса инцидентов

Тип метода: PUT

Метод

`https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/incidents/update/status`

Заголовки (headers):
`PgrApiKey: api_key_string`

`PgrSelectedInstance: string`

`Content-Type: application/json`

Входные параметры:

Параметр	Описание
id	Идентификатор инцидента
status	Статус инцидента

status =

- new: "Новый"
- assigned_customer: "Назначен"
- working_customer: "В работе"
- feedback_required: "Запрошена информация"
- verify_close: "Ожидает проверки"
- risk_accepted: "Риск принят"
- closed: "Закрыт"
- invalid: "Недействительный"

Пример вызова:

```
{
    "id": "00000000-0000-0000-0000-00000000004b", //string
    "status": "new" //string
}
```

Выходные параметры: Отсутствуют

Обновление уровня рисков инцидентов

Тип метода: PUT

Метод

`https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/incidents/update/critical`

Заголовки (headers):
`PgrApiKey: api_key_string`
`PgrSelectedInstance: string`
`Content-Type: application/json`

Входные параметры:

Параметр	Описание
id	Идентификатор инцидента
risklevel	Уровень риска - число с запятой от 0.0 до 10.0

Пример вызова:

```
{
    "id": "00000000-0000-0000-0000-00000000004b", //string
    "risklevel": 4.1
}
```

Выходные параметры: Отсутствуют

Активы

Получение списка активов

Тип метода: GET

Метод
`https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/serviceAssets`

Заголовки (headers):
`PgrApiKey: api_key_string`
`PgrSelectedInstance: string`
`Content-Type: application/json`

Входные параметры:

Поддерживаются стандартные фильтры

Выходные параметры и пример ответа:

```
{
  "objects": [
    {
      "id": "e2ad28ad-7249-4e71-b724-8617d44a39d9",
      "type": "Host",
      "name": "192.168.15.15",
      "description": "",
      "coordinates": "--- [] ",
      "active": true,
      "scan_id": "",
      "value": 3,
      "client_note": "",
      "internal_note": "",
```

```
      "location": "",
      "network_exposure": 3,
      "responsible_person": "",
      "technical_specialist": "",
      "responsible_group_id": "",
      "edited_by": "",
      "risk": "none",
      "network_interfaces": [
        {
          "id": "2dccfb43-f30a-4389-a6cf-94691b7b0a4a",
          "name": "192.168.15.15",
          "ip": "192.168.15.15",
          "mac": "",
          "fqdn": [],
          "os": "",
          "service_asset_id": "e2ad28ad-7249-4e71-b724-8617d44a39d9",
          "edited_by": ""
        }
      ],
      "all_open_count": 1,
      "front_link": "http://172.30.254.75/rmc/service_assets/show/e2ad28ad-7249-
4e71-b724-8617d44a39d9"
    }
  ],
  "total": 1
}
```


Получение перечня групп активов

Тип метода: GET

Метод

`https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/serviceAssetGroups`

Заголовки (headers):

`PgrApiKey: api_key_string`

`PgrSelectedInstance: string`

`Content-Type: application/json`

Входные параметры:

Поддерживаются стандартные фильтры

Выходные параметры и пример ответа:


```
{
  "objects": [
    {
      "id": "929941bd-9037-4059-b5be-568d1029e62b",
      "name": "Филиал 17",
      "network_ranges": [],
      "domain": "",
      "itsm_synced": false,
      "created_at": "2023-04-10T14:39:45.400048Z",
      "updated_at": "2023-04-10T14:39:45.400048Z",
      "regex": "",
```

```
      "subject_id": "",
      "object_id": "",
      "is_kii": false,
      "is_fincert": false,
      "responsible_person": "",
      "technical_specialist": "",
      "system_id": "",
      "responsible_group_id": "",
      "edited_by": "",
      "service_assets": [
        {
          "id": "e2ad28ad-7249-4e71-b724-8617d44a39d9",
          "type": "Host",
          "name": "192.168.15.15",
          "description": "",
          "coordinates": "--- [] ",
          "active": true,
          "scan_id": "",
          "value": 3,
          "client_note": "",
          "internal_note": "",
          "location": "",
          "network_exposure": 3,
          "responsible_person": "",
          "technical_specialist": "",
          "responsible_group_id": "",
          "edited_by": "",
          "network_interfaces": [
            {
              "id": "2dccfb43-f30a-4389-a6cf-94691b7b0a4a",
              "name": "192.168.15.15",
              "ip": "192.168.15.15",
              "mac": "",
              "fqdn": [],
              "os": "",
              "service_asset_id": "e2ad28ad-7249-4e71-b724-8617d44a39d9",
              "edited_by": ""
            }
          ]
        }
      ]
    }
  ],
  "total": 1
}
```


Пользователи

Получение списка пользователей

Тип метода: GET

Метод

`https://<MASTER_KARAKEN_HOST>:9000/cruddy/public/api/v1/users`

Заголовки (headers):

`PgrApiKey: api_key_string`

`PgrSelectedInstance: string`

`Content-Type: application/json`

Входные параметры:

Поддерживаются стандартные фильтры

Выходные параметры и пример ответа:


```
{
    "objects":[
        {
            "id":"93adf94b-0f93-45d1-8b3c-a15a38399d49",
            "email":"",
            "first_name":"",
            "last_name":"",
            "username":"admin"
        }
    ],
    "total":1
}
```