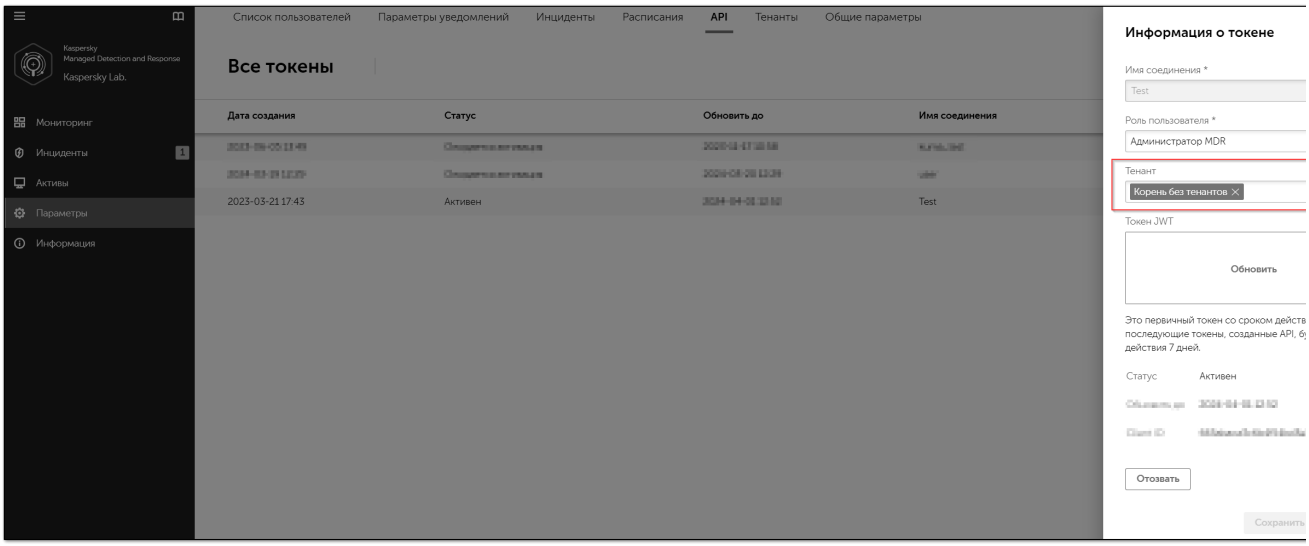
Интеграция с Kaspersky MDR

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

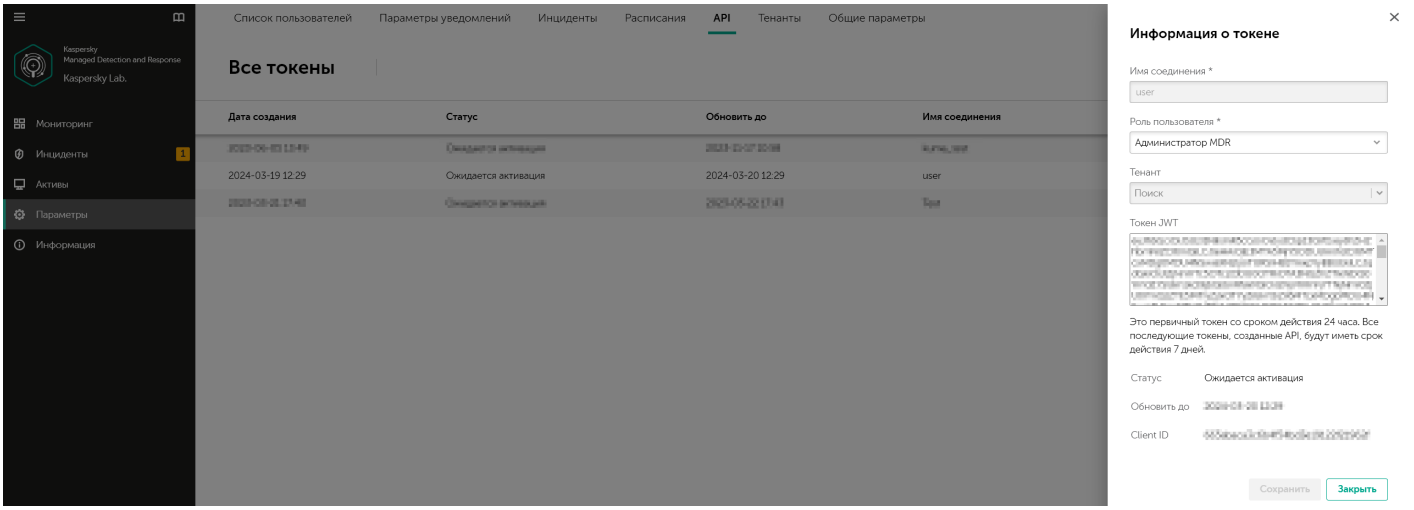
Предварительные требования

- На пограничном МСЭ создайте правило доступа к **mdr.kaspersky.com** по порту **TCP/443** (https://mdr.kaspersky.com)
- В KUMA добавьте пользователя с ролью Администратор и доступом к API (права **POST /events)**
- В консоли MDR сгенерируйте токен для доступа к API:
    - Перейдите в **Settings -> API**
    - Нажмите **Add** и укажите **Connection Name** (данное имя будет использоваться, как имя пользователя при создании инцидентов/комментариев/вложений и т.д., так как токен доступа не привязан к конкретному пользователю)
    - Укажите **Role**, чтобы определить права доступа для токена
    - Укажите **Tenant** при необходимости

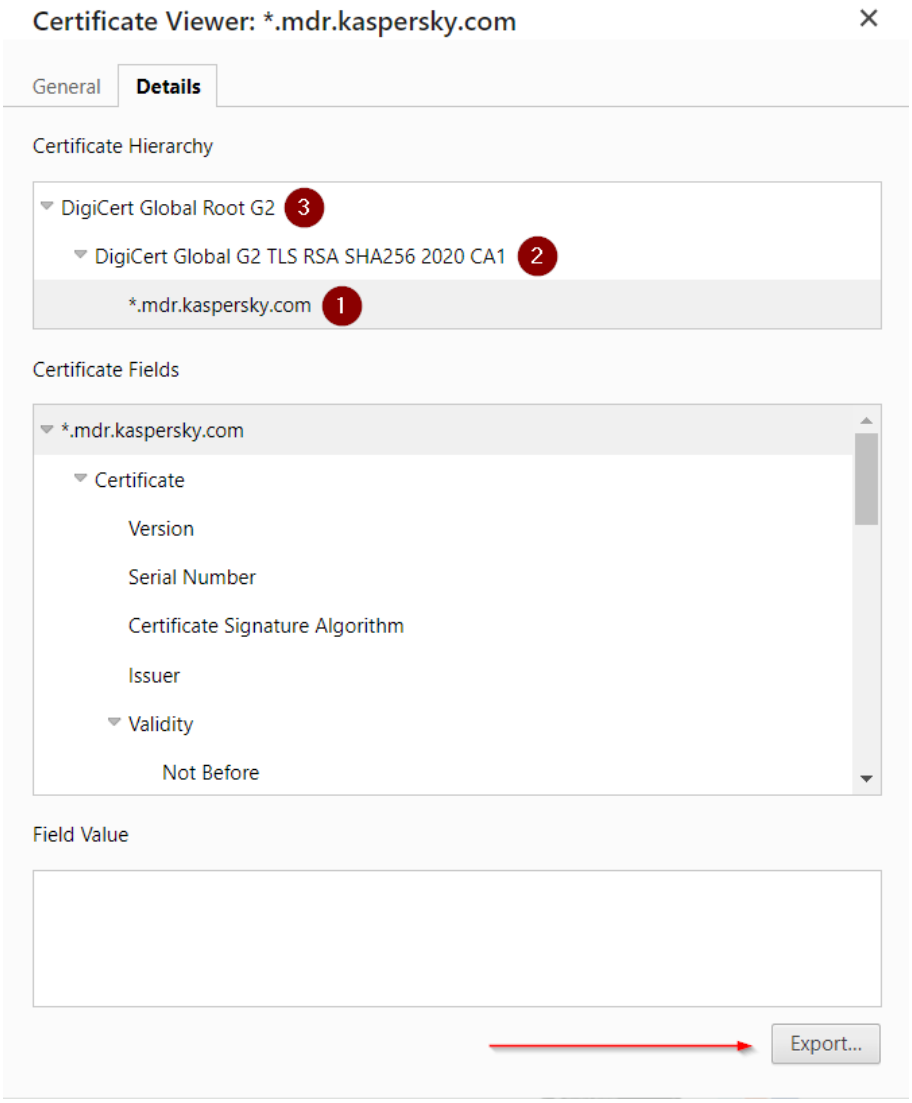
> Если для создаваемых в консоли MDR инцидентов в поле "Тенант" отсутствует значение, добавьте значение "**Корень без тенанта**", чтобы скрипт при подключении обнаружил данные инциденты



- Нажмите **Generate**
- После завершения процесса генерации будут получены:
  - **JWT Token** - он же **refresh_token**, который требуется активировать, чтобы получить новую пару **refresh_token** и **access_token**
  - **ClientID** - ID-клиента для подключения к API (требуется указывать при каждом запросе к API MDR)



- Загрузите архив **kuma_mdr_integration.tar.gz** со скриптом отсюда - **https://box.kaspersky.com/f/11a58e42f63e4cef8741/**
- Загрузите актуальную цепочку сертификатов для консоли mdr.kaspersky.com в формате pem. После загрузки файлов выполните объединение сертификатов в один файл **mdr.pem** (см. скриншот ниже).


Certificate Viewer: *.mdr.kaspersky.com
General
Details
Certificate Hierarchy
DigiCert Global Root G2
3
DigiCert Global G2 TLS RSA SHA256 2020 CA1
2
*.mdr.kaspersky.com
1
Certificate Fields
*.mdr.kaspersky.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
Export...

```
-----BEGIN CERTIFICATE-----
MIIHujCCBqKgAwIBAgIQCfd78crUhJ1lnoXdEuPT9TANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMTA3MDUwMDAwMDBa
Fw0yMjA3MjAyMzU5NTlaMFcxCzAJBgNVBAYTAlJVMQ8wDQYDVQQHEwZNb3Njb3cx
GTAXBgNVBAoTEEFPIEthc3BlcnNreSBMYWIxHDAaBgNVBAMMEyoubWRyLmthc3Bl
cnNreS5jb20wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDcunj7B+v7
Ywv8eQeSlt10Yr4fR8PDr8cmW1hBuB/BjtLITcaO6DnB4qucZueEchF88cZSKeXV
211iWItOFU/6hzm0+RdxqePFX+/B1j9mlrmNVAtXWXwPIUa+bC5fJ2uYmqWDkQK6
5R4yEM6sg+671/cePUJqLQBAT/5QvVj2uCLvUushhEkxWpqETXLswVDdY1tcqSnP
n191nbQk4TivWPoNDI5zPIcFHfr4mUFysMCETSZc7i7a2ZcHV0qLQLQa9m9c+OzN
Yax8PFTOn2ltvYxhVXYam6amU9hYzitJg/wS9nI+FgkEDvn/wHmNeB9/0nZzwNZx
IVPaz1fwPk1cQAti0vd93+Vw8jCBV6wX7LlMPF1EGB+UTjgX4bnzo6kzrvr3IMZe
Y98UK48CS8SHT/gt8gIduf+RcxJaPFJ0rNQ7Z0fzWukGs19/BxIfo6THM9jfwC/D
+q/SpYUtGtdD3DUw6kGVM8tsVP5aIvI5Yt/yIhstHxLIKbfYM45fj5hLHeN8AtVj
RGV0iCXqB+kCrpetl3uMS0su/PsG4JNZNdzgLCa7N3XCBto3iLA3gSxep05wRVA1
63wmadIPTx7QgvDstIToZVfxchleIbifCJ/0LuXE3edhC7e/ANvnsPyFo6dYEUeV
4yULT2zuosuCRgJjCaCN06PsV4Ntt2pcSQIDAQABo4IDiDCCA4QwHwYDVR0jBBgw
FoAUt2ui6qiqhIx56rTaD5iyxZV2ufQwHQYDVR0OBBYEFN/FZS5dTDcvvOSwWCS1
ZoDZQLXnMDEGA1UdEQQqMCiCEyoubWRyLmthc3BlcnNreS5jb22CEW1kci5rYXNw
ZXJza3kuY29tMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYI
KwYBBQUHAwIwgY8GA1UdHwSBhzCBhDBAoD6gPIY6aHR0cDovL2NybDMuZGlnaWNl
cnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBMS0xLmNybDBAoD6gPIY6
aHR0cDovL2NybDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAy
MENBMS0xLmNybDA+BgNVHSAENzA1MDMGBmeBDAECAjApMCcGCCsGAQUFBwIBFhto
dHRwOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwfwYIKwYBBQUHAQEEczBxMCQGCCsG
AQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5jb20wSQYIKwYBBQUHMAKGPWh0
dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRMU1JTQVNIQTI1NjIw
MjBDQTEtMS5jcnQwDAYDVR0TAQH/BAIwADCCAX0GCisGAQQB1nkCBAIEggFtBIIB
aQFnAHUARqVV63X6kSAwtaKJafTzfREsQXS+/Um4havy/HD+bUcAAAF6dhwGcgAA
BAMARjBEAiBvkP0ksqgsQtTkjrtT7Zf+VjltRLqvb5/k+prilZ21rAIgKlO/CWIV
kSxZ1YS4OqJFYt7f/cVzochPtAspDUXXz/AAdQBRo7D1/QF5nFZtuDd4jwykeswb
J8v3nohCmg3+1IsF5QAAAXp2HAaoAAAEAwBGMEQCIFf5B07TdaJtpj63WtS2nzF4
Y6JCKHX55Wzfgb+UAuHHAiBSMJ+Uu5i5RGe28BJ8pbRJmYnRfe6317f+OZhg1LjH
eQB3AEHIyrHfIkZKEMahOglCh15OMYsbA+vrS8do8JBilgb2AAABenYcBoEAAAQD
AEgwRgIhAMjnJKTPeq/oQ6RGz7N1dgVFhMbUXOoPD3BdtiZdspSXAiEA7H4lySGM
XuVdw38QJjBkk/rScAMtT3nCyURxh3/ao6YwDQYJKoZIhvcNAQELBQADggEBAGyi
zDK8GnkfWVriNouzGZK2t9zei2N8acBoUDDIFWsdW3/D+nOA+VC+FYdLmf3fTUR1
50d8xTbHw9Vh0bSFfozk/zurCUsFs+IFxU3kDgUWZEJgvvRSsLbGh/0RIaj+TZDB
YWoQmG2l9QyowUngSDGZrmmPj0X0FlCIU/idH4SHPKotOTbx3s6eijbzaReHLrie
jKE+hwZlQRlnRyugwR4++p4qwxbXATx24lW9uf8zZV8RkT2gmS9Qj4kPS/sLWTv3
oBJN6vOUCt7j3BdLFEoXaMdyQxJZLjmcJrDqTorkjMSW1AxckT3XzkggXTlXG3uC
Ovew/C3aBoxtuA6Oevk=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEvjCCA6agAwIBAgIQBtjZBNVYQ0b2ii+nVCJ+xDANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0yMTA0MTQwMDAwMDBaFw0zMTA0MTMyMzU5NTlaME8xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERpZ2lDZXJ0IFRMUyBS
U0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6a
qXodgojlEVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddn
g9/n00tnTCJRpt8OmRDtV1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuW
raKImxW8oHzf6VGo1bDtN+I2tIJLYrVJmuzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGB
Afr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkDKa77SU+kFbnO8lwZV21r
eacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBgjCCAX4wEgYDVR0TAQH/BAgwBgEB
/wIBADAdBgNVHQ4EFgQUt2ui6qiqhIx56rTaD5iyxZV2ufQwHwYDVR0jBBgwFoAU
A95QNVbRTLtm8KPiGxvDl7I90VUwDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQG
CCsGAQUFBwMBBggrBgEFBQcDAjB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGG
GGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2Nh
```

Описание интеграции

Описанная в данной статье интеграция с Kaspersky Managed Detection and Response позволяет автоматически импортировать инциденты из консоли MDR в KUMA.

Настройка

- Скопируйте архив **kuma_mdr_integration.tar.gz** на сервер (в случае распределенной инсталяции на сервер Core) и распакуйте его в папку **/opt** с помощью следующей команды:

```
sudo tar -xf kuma_mdr_integration.tar.gz -C /opt
```

- Перейдите в папку **/opt/mdr/conf** и отредактируйте файл **config.yml**:
  - В секции **General settings** укажите **актуальный путь до папок (по умолчанию, указан /opt/mdr/*)**, а также **client_id**
  - В секции **Modules settings** -> **kuma** укажите:
    - api_url (FQDN/IP:порт API-интерфейса KUMA)
    - username (ранее созданный пользователь с доступом к API)
    - password (пароль ранее созданного пользователя с доступом к API)
    - tenantId (тенант, в котором будут создаваться инциденты)

> TenantID можно получить из события аудита KUMA

  - В секции **Modules settings** -> **logging** также укажите **актуальный путь до папки со скриптом (по умолчанию, указан /opt/mdr/log)**
- Перейдите в папку **/opt/mdr/conf** и добавьте в файл **.refresh_token** ранее сгенерированный токен для доступа к API MDR

> После добавления токена в файл **.refresh_token** проверьте, что в конце файла отсутствует символ новой строки \n , из-за которого попытка аутентификации будет неуспешной. См. команды ниже:

```
# проверяем наличие символа новой строки
wc -l /opt/mdr/conf/.refresh_token
# если вывод "1 .refresh_token", то удаляем символ
perl -p -i -e 'chomp if eof' /opt/mdr/conf/.refresh_token
# проверяем, что символ новой строки успешно удален
wc -l /opt/mdr/conf/.refresh_token
```

```
# должен быть вывод "0 .refresh_token"
```

- Перейдите в папку **/opt/mdr/conf** и в файле **.last_check** укажите время, начиная с которого необходимо начать собирать инциденты. Для теста можно указать время до появления последнего инцидента. Формат в милисекундах, то есть должно быть 13 цифр (пример, 1672520400000)
- Замените существующий файл **/opt/mdr/conf/mdr.pem** на актуальный (см. этап "Предварительные требования")
- Запустите скрипт **main.py** с помощью команды:

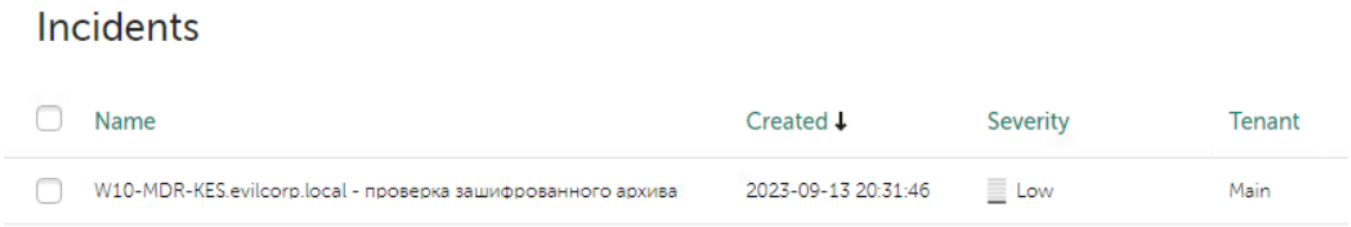
```
python3 ./main.py
```

> Если при запуске скрипта появляются сообщения об отсутствии необходимых пакетов - выполните их установку

- Если после запуска скрипта в консоли отсутствую ошибки (кроме предупреждений о невалидном сертификате), значит интеграция работает корректно.

> Лог работы скрипта пишется в /opt/mdr/log/app.log

- Убедитесь, что выполнен импорт инцидентов, созданных в консоли MDR начиная с момента времени, указанного в файле **.last_check**



- Остановите выполнение скритпа **main.py**
- Запустите скрипт **main.py** в фоновом режиме с помощью команды:

```
nohup python3 /opt/mdr/main.py &
```

- Настройте автоматический запуск скрипта после перезагрузки сервера:

```
sudo crontab -e
@reboot sleep 300 && python3 /opt/mdr/main.py & # sleep в 5 минут добавлен, чтобы сервис kuma-core успел стартовать
```

Revision #20
Created 26 February 2024 14:04:55 by Dmitry Borisov
Updated 3 February 2025 07:59:53 by Koala