

GeoIP-обогащение (Геоданными)

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

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/KUMA/3.2/ru-RU/233257.htm>

Скачанная и конвертированная база (IP2Location) -
<https://box.kaspersky.com/f/b961a874400a4a0ab66b/>

Российская база (требуется регистрация) - <https://geoip.noc.gov.ru/>

Скачивание БД

IP2Location

Чтобы скачать базы необходимо зарегистрироваться. После регистрации и входа на сайт переходим по ссылке: <https://lite.ip2location.com/database-download>
И выбираем нужную нам БД (есть для ipv4 и ipv6) и скачиваем.

Product Name	IPv4 Database ⓘ	IPv6 Database ⓘ
DB1.LITE IP-COUNTRY		
DB3.LITE IP-COUNTRY-REGION-CITY		
DB5.LITE IP-COUNTRY-REGION-CITY-LATITUDE-LONGITUDE		
DB9.LITE IP-COUNTRY-REGION-CITY-LATITUDE-LONGITUDE-ZIPCODE		
DB11.LITE IP-COUNTRY-REGION-CITY-LATITUDE-LONGITUDE-ZIPCODE-TIMEZONE		

MAXMIND

Скачивание БД также доступно после регистрации. Также при регистрации проверяется соответствие выбранной страны и ip, с которого вы регистрируетесь. При этом при выборе страны отсутствует Россия. Возможно проблему можно решить через VPN.

Конвертация БД

Перед импортом базы ее необходимо конвертировать в формат, понятный KUMA. Для конвертации данных используется скрипт. Актуальный скрипт и команды запуска тут:

<https://support.kaspersky.com/help/KUMA/2.1/ru-RU/233259.htm>

В простейшем случае команда запуска выглядит так:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out geoip_ip2location.csv
```

После запуска нужно подождать 20-30 сек и в случае успешной конвертации получим файл CSV:

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dronov_d\Desktop\GEO>python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out geoip_ip2location.csv
Successfully done.

```

Загрузка БД в KUMA

Загрузка БД (предварительно сконвертированной скриптом!) осуществляется по пути:
Settings - Common - GeoIP settings - Import from file

Kaspersky Unified Monitoring and Analysis Platform

Selected tenants: 1

Dashboard

Alerts

Incidents

Events

Assets

Reports

Resources

Task manager

Settings

Source status

Metrics

Administrator

Users

Tenants

Domain authorization

Threat intelligence

Kaspersky Threat Lookup

Kaspersky CyberTrace

Integrations

Kaspersky Security Center

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Endpoint Detection and Response

LDAP server

IRP / SOAR

RuCERT

Other

Alerts

License

Incidents

Asset audit

Hierarchy

Common

Common

GeoIP settings

Import from file Export

SMTP server settings

Disabled

*Host

*Port

Secret +

Alias for KUMA Core server ?

*From

Disable monitoring notifications

* Monitoring notifications interval

Save

После добавления БД необходимо перезапустить все сервисы, где настроено обогащение по GeoIP (при выполнении тестов было достаточно выполнить reload, а не restart)

GeoIP settings

After uploading geodata you must restart services with 'geographic data' enrichment rules.

Import from file Export

При импорте нового файла с данными GeoIP ранее добавленные данные перезапишутся (с созданием события аудита). Поэтому если нужно внести незначительные изменения для кастомизации сопоставления рекомендуется скачать текущую БД из интерфейса KUMA, после чего внести туда изменения и подгрузить обратно.

TenantName	Main
Timestamp	2022-07-25 13:07:03 :485
EndTime	2022-07-25 13:07:03 :485
DeviceAction	new geobase imported
DeviceHostName	kuma-2-0.sales.lab
DeviceProduct	KUMA
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
SourceAddress	10.16.51.33
SourcePort	63488
SourceUserID	f01d4d6e-f5fd-844f-ae1a-af96e335d358
SourceUserName	dronov@sales.lab
DeviceCustomString5	61877019-0c82-4757-a6f2-d20faeccb694
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Main
DeviceCustomString6Label	tenant name
EventOutcome	succeeded
Type	Audit

Обогащение GeoIP

- В разделе **Ресурсы - Правила Обогащения** создаем новое правило
- В поле Source kind выбираем geographic data
- В поле Mapping geographic data to event fields выбираем поле события KUMA, в котором присутствует нужный для обогащения ip-адрес
- Здесь же выбираем Geodata attribute и соответствующее поле события KUMA Event field to write to
- Для GeoIP добавлены новые поля событий, но можно использовать любые

Create enrichment rule

*Name	<input type="text" value="GeoIP"/>
*Tenant	<input type="text" value="Main"/>
*Source kind	<input type="text" value="geographic data"/>
*Mapping geographic data to event fields	<input type="text" value="DeviceCustomIPv6Address1"/> ?
	<input type="text" value="Country"/> <input type="text" value="SourceCountry"/> ×
	<input type="text" value="Region"/> <input type="text" value="SourceRegion"/> ×
	<input type="text" value="City"/> <input type="text" value="SourceCity"/> ×
	<input type="text" value="Longitude"/> <input type="text" value="SourceLongitude"/> ×
	<input type="text" value="Latitude"/> <input type="text" value="SourceLatitude"/> ×
	<input type="button" value="+ Add geodata attribute"/>
	<input type="button" value="+ Add event field with IP address"/>
Debug	<input type="text"/>
Description	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">Description</div>

Save

Сопоставление по умолчанию доступно, если в качестве источника IP выбрано одно из полей событий SourceAddress, DestinationAddress и DeviceAddress.

При выборе других полей в качестве источника сопоставление по умолчанию не доступно.

*Mapping geographic data to event fields

SourceAddress ?

Geodata attribute Event field to write to

+ Add geodata attribute Apply default mapping

*Mapping geographic data to event fields

SourceAddress ?

Country SourceCountry ✗

Region SourceRegion ✗

City SourceCity ✗

Longitude SourceLongitude ✗

Latitude SourceLatitude ✗

+ Add geodata attribute Apply default mapping

Далее нужно созданное правило выше закрепить в коллекторе в части обогащения. Пример того, как выглядит обогащенное событие:

SourceAddress	8.8.8.8
<u>SourceCity</u>	<u>Mountain View</u>
<u>SourceCountry</u>	<u>United States of America</u>
<u>SourceLatitude</u>	<u>37.40599</u>
<u>SourceLongitude</u>	<u>-122.078514</u>
SourcePort	49048
SourceProcessName	Advapi
<u>SourceRegion</u>	<u>California</u>

Формат файла CSV:

```
Network,Country,Region,City,Latitude,Longitude
10.0.0.0/8,Russia,Moscow,Butovo,,
192.168.0.0/16,Russia,SPB,Zelenograd,,
```

Revision #10

Created 11 August 2023 14:43:47 by Boris RZR

Updated 5 November 2024 10:25:55 by Boris RZR