Обогащение событий информацией об Активах

Активы могут попасть в KUMA следующими способами:

- От KSC (FQDN, IP, MAC, Имя ассета (в KSC, Владелец [Principal name], Информация об уязвимостях, Информация об установленном ПО, Информация о hardware)
- От KICS
- От Vulnerability Scanner: Из коробки: MP8 Scanner, RedCheck. Через новые PreSalesPack скрипты: Nessus, OWASP ZAP;
- От CMDB выгрузка в виде CSV, затем скриптом через API добавление в KUMA (скрипт в **PreSalesPack**);
- Вручную

Коллекторы KUMA с периодически получают списки ассетов (активов) от ядра KUMA и хранят их памяти в виде таблиц, позволяющих определить AssetID по **IP адресу и/или FQDN**.

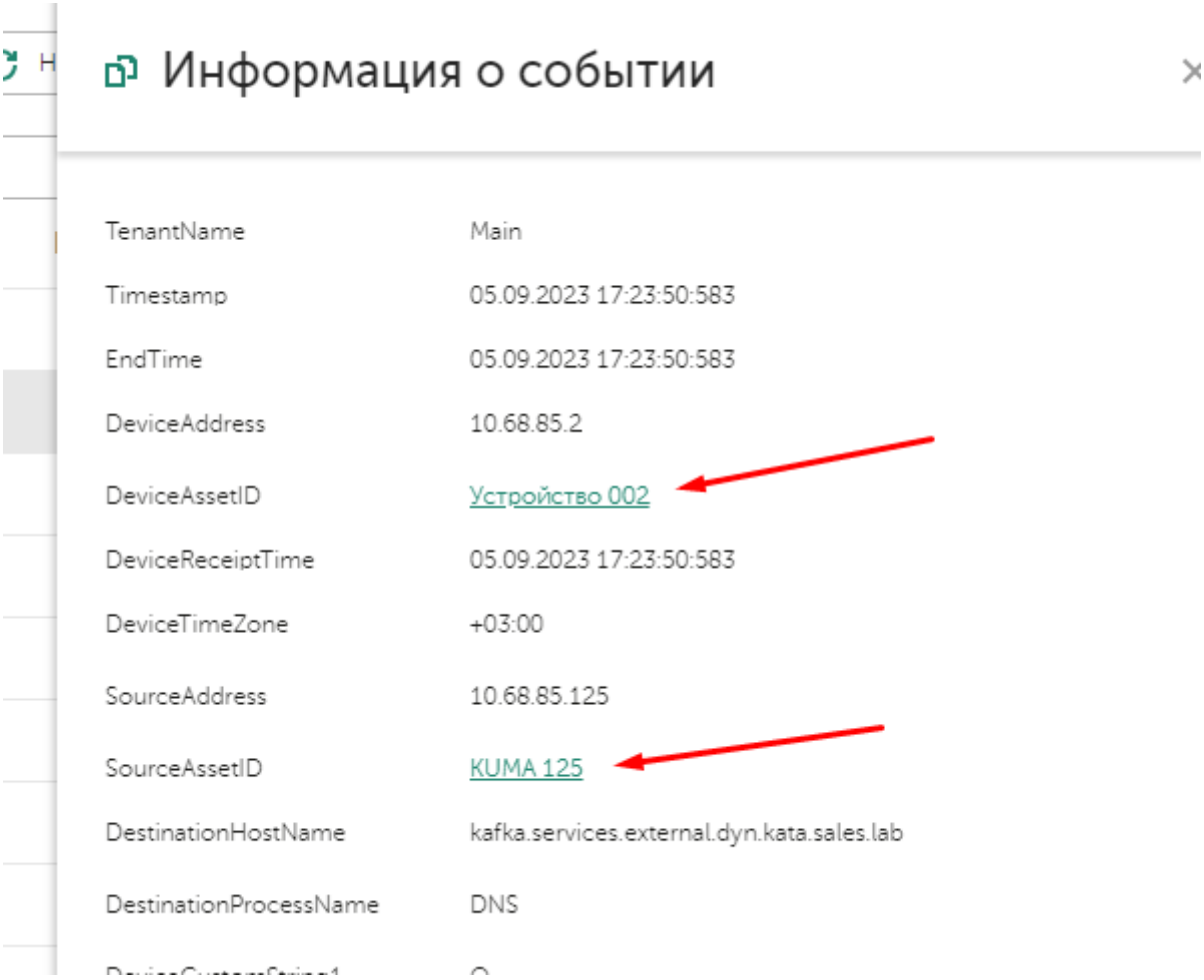
> У ассета может быть указан массив значений IP и/или FQDN. Обогащение проверяет все IP ассета и/или FQDN.

При поступлении события в коллектор, коллектор выполняет:

- нормализацию данных в поля события KUMA;
- если в событии содержится информация о SourceAddress, Destination Address, DeviceAddress, SourceHostName, DestinationHostName, DeviceHostName коллектор выполняет поиск IP - AssetID и/или FQDN - AssetID;
- если информация об ассете найдена, AssetID проставляется в соответствующее поле нормализованного события;
- В общем случае, в нормализованное событие могут быть проставлены 3 типа AssetID: SourceAssetID, DestinationAssetID, DeviceAssetID.

После чего события, обогащенные информацией об ассетах направляются в коррелятор и/или хранилище.

Пример обогащенного события (при нажатии открывается карточка актива):



Правила обогащения информацией об активах

Информация в событии	Информация в карточке актива	Будет ли обогащение
IP	IP + FQDN	Да
FQDN	IP + FQDN	Да
IP + FQDN	IP + FQDN	Да
IP	IP	Да
FQDN	IP	Нет
IP + FQDN	IP	Нет
IP	FQDN	Нет
FQDN	FQDN	Да
IP + FQDN	FQDN	Да

Revision #8
Created 5 September 2023 14:20:13 by Boris Rzr
Updated 7 July 2024 08:06:07 by Koala