

- 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):

Информация о событии

TenantName	Main
Timestamp	05.09.2023 17:23:50:583
EndTime	05.09.2023 17:23:50:583
DeviceAddress	10.68.85.2
DeviceAssetID	Устройство 002
DeviceReceiptTime	05.09.2023 17:23:50:583
DeviceTimeZone	+03:00
SourceAddress	10.68.85.125
SourceAssetID	KUMA 125
DestinationHostName	kafka.services.external.dyn.kata.sales.lab
DestinationProcessName	DNS
DeviceCustomField1	

???????? ?????????????? ?????????????? ?? ??????????

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 #13

Created 2023-09-05 14:20:13 UTC by Boris RZR

Updated 2026-05-18 10:57:43 UTC by Koala