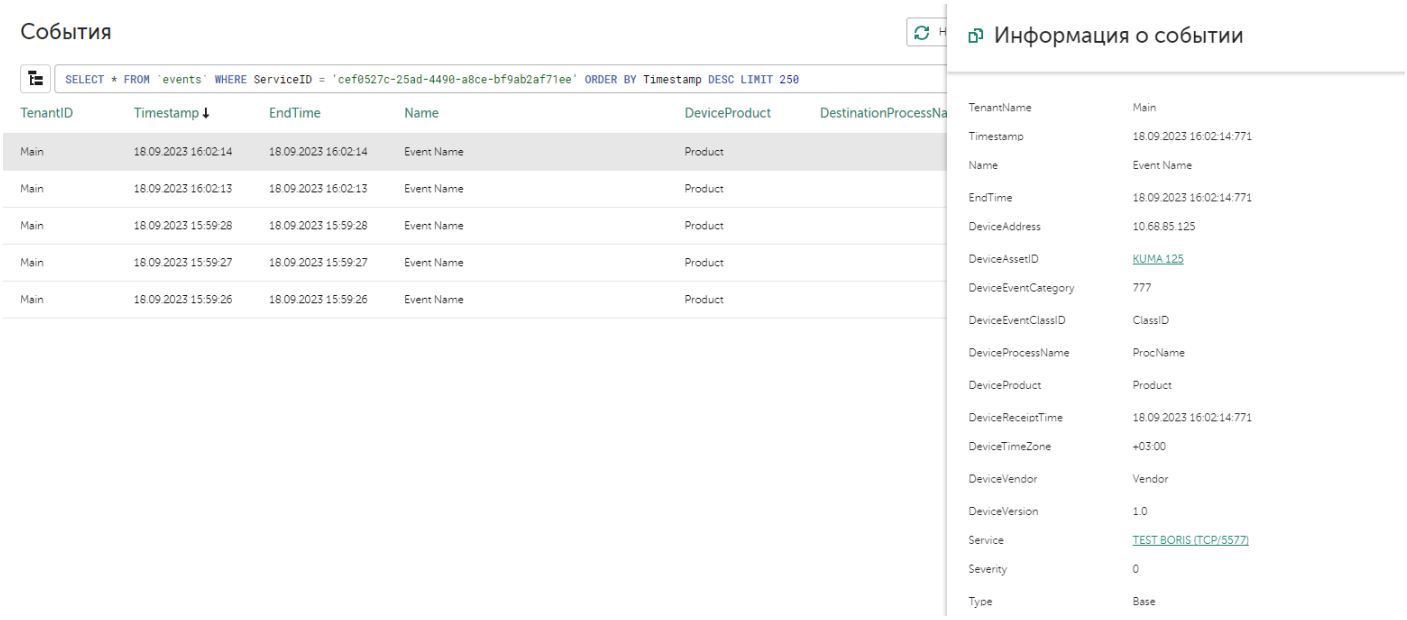
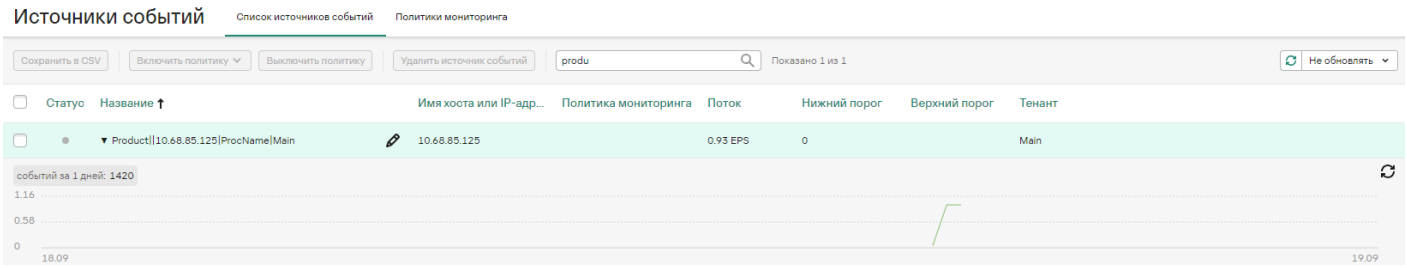
Настройка мониторинга источников с алертом

? ?????? ?????? ?????? ???????? ???????? ??????????? ????????????? ????????? ? ?????????? ?????? ??? ???????????? ????????.

?? ??????? ???????? ????????? ???????:



????? ????????? ???????? ??????? (????????? (? ???? ?????) ?? ??????? **Состояние источников**):

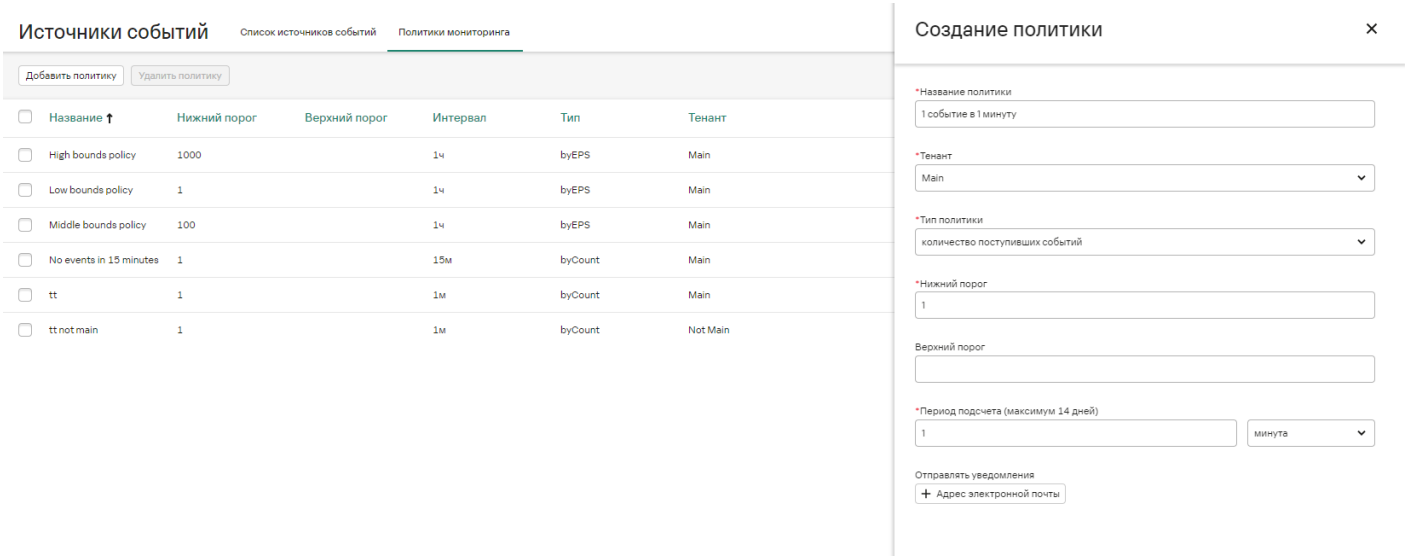


??????? ?? ???? ????????? ????????? ? ??????? 1 EPS.

> ???????? ?????????? ??????? ?????????? ???? ??? ? ?????? ? ?????? ?????????? ??????? ????? ????????: "DeviceProduct|DeviceHostname|DeviceAddress|DeviceProcessName".

???????? ???????? ??????????? ??? ????? ?????????: ???? ?? 1 ??????? ? ??????? 1 ??????. ????????? ?? ??????? **Политики мониторинга** ? ???? ???????? ????? ????????? ?????????

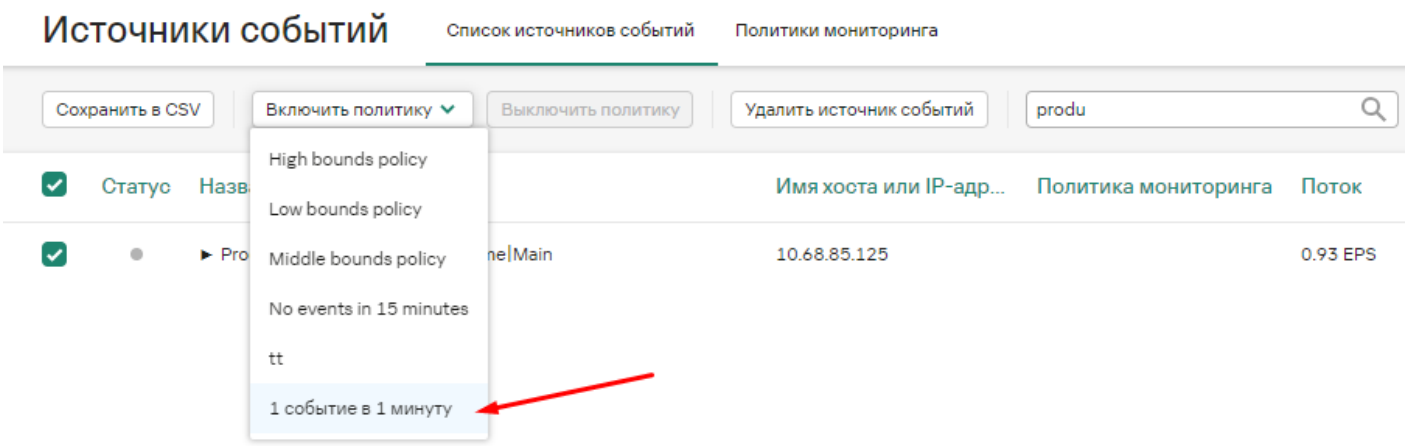
???????:



????? ????? ????????? ??????????? ????? ??? ??????????? ? ?????? ???????????? ????????.

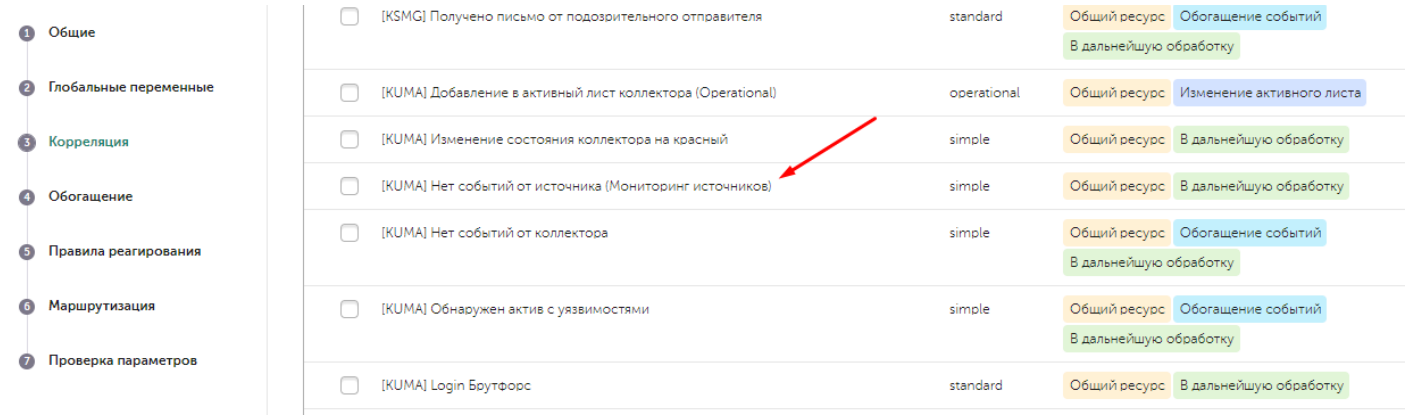
????? ?????????? ?????? ?? ?????? **Добавить**. ????? ?????????? ??????? ????? ?? ???????

Список источников событий, ???????? ???????? ? ????????? ????? ????????? ????????:

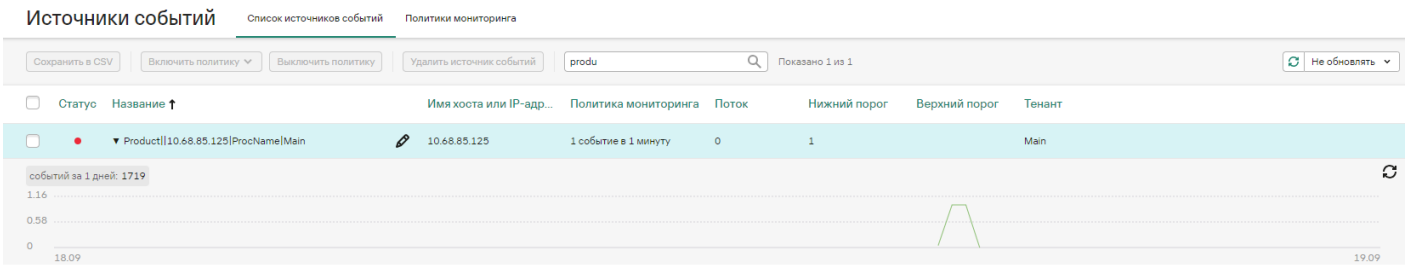


?????? ??????? ????????? ????? ?????????? ?????? ??????? (???????? - ???????????? ????????).

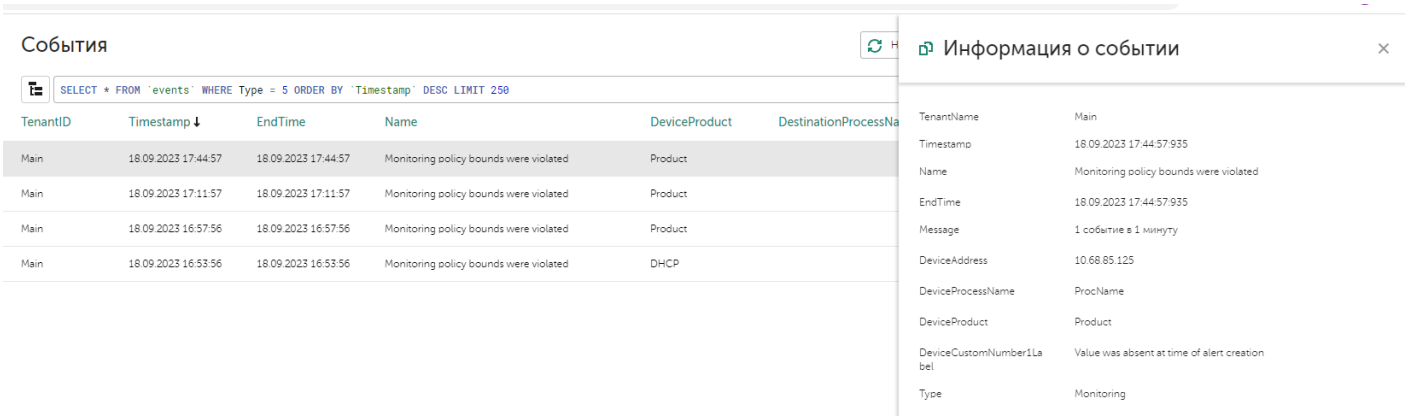
????????, ??? ??????? ?????????? ??????????? ?????????? (? ???????? Pre-Sales-Pack) ????????? ? ??????????:


1 Общие
2 Глобальные переменные
3 Корреляция
4 Обогащение
5 Правила реагирования
6 Маршрутизация
7 Проверка параметров
[KSMG] Получено письмо от подозрительного отправителя
standard
Общий ресурс
Обогащение событий
В дальнейшую обработку
[KUMA] Добавление в активный лист коллектора (Operational)
operational
Общий ресурс
Изменение активного листа
[KUMA] Изменение состояния коллектора на красный
simple
Общий ресурс
В дальнейшую обработку
[KUMA] Нет событий от источника (Мониторинг источников)
simple
Общий ресурс
В дальнейшую обработку
[KUMA] Нет событий от коллектора
simple
Общий ресурс
Обогащение событий
В дальнейшую обработку
[KUMA] Обнаружен актив с уязвимостями
simple
Общий ресурс
Обогащение событий
В дальнейшую обработку
[KUMA] Login Брутфорс
standard
Общий ресурс
В дальнейшую обработку

????????? ?????? ??????? ? ???????? ?????????:


Источники событий
Список источников событий
Политики мониторинга
Сохранить в CSV
Включить политику
Выключить политику
Удалить источник событий
produ
Показано 1 из 1
Не обновлять
Статус
Название
Имя хоста или IP-адр...
Политика мониторинга
Поток
Нижний порог
Верхний порог
Тенант
Product||10.68.85.125|ProcName|Main
10.68.85.125
1 событие в 1 минуту
0
1
Main
событий за 1 дней: 1719
1.16
0.58
0
18.09
19.09

? ????????:


События
SELECT * FROM `events` WHERE Type = 5 ORDER BY `Timestamp` DESC LIMIT 250
TenantID
Timestamp
EndTime
Name
DeviceProduct
DestinationProcessNa
Main
18.09.2023 17:44:57
18.09.2023 17:44:57
Monitoring policy bounds were violated
Product
Main
18.09.2023 17:11:57
18.09.2023 17:11:57
Monitoring policy bounds were violated
Product
Main
18.09.2023 16:57:56
18.09.2023 16:57:56
Monitoring policy bounds were violated
Product
Main
18.09.2023 16:53:56
18.09.2023 16:53:56
Monitoring policy bounds were violated
DHCP
Информация о событии
TenantName
Main
Timestamp
18.09.2023 17:44:57.935
Name
Monitoring policy bounds were violated
EndTime
18.09.2023 17:44:57.935
Message
1 событие в 1 минуту
DeviceAddress
10.68.85.125
DeviceProcessName
ProcName
DeviceProduct
Product
DeviceCustomNumber1Label
Value was absent at time of alert creation
Type
Monitoring

?????:



Revision #5
Created 2023-09-18 13:00:45 UTC by Boris Rzr
Updated 2024-10-03 07:58:41 UTC by Boris Rzr