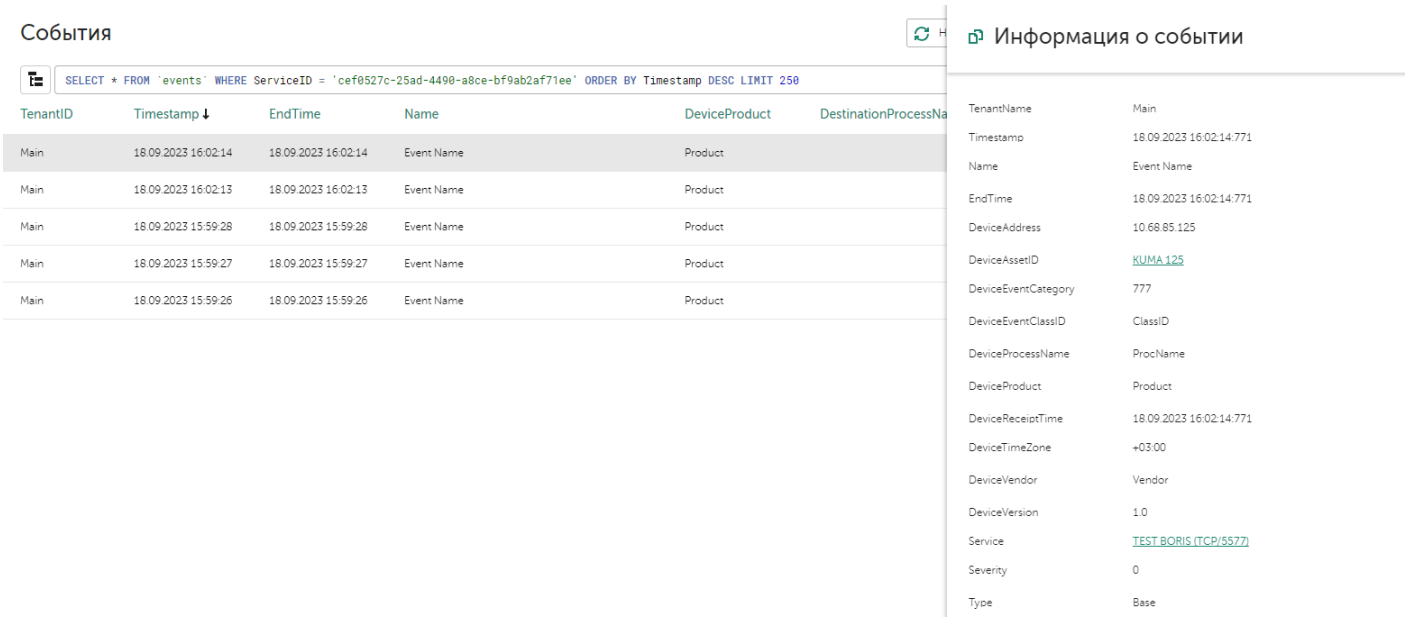
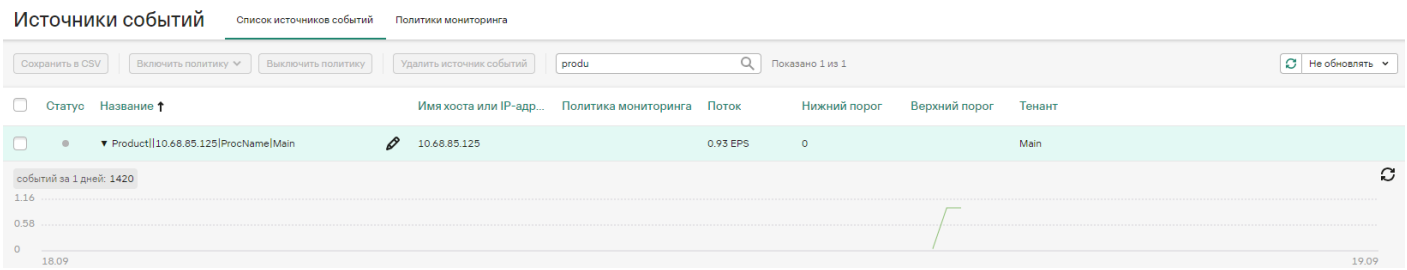
????????? ????????????
?????????? ? ???????

В рамках данной статьи настроим политику мониторинга определенного источника с взведением алерта при срабатывании политики.

На системы приходят следующие события:



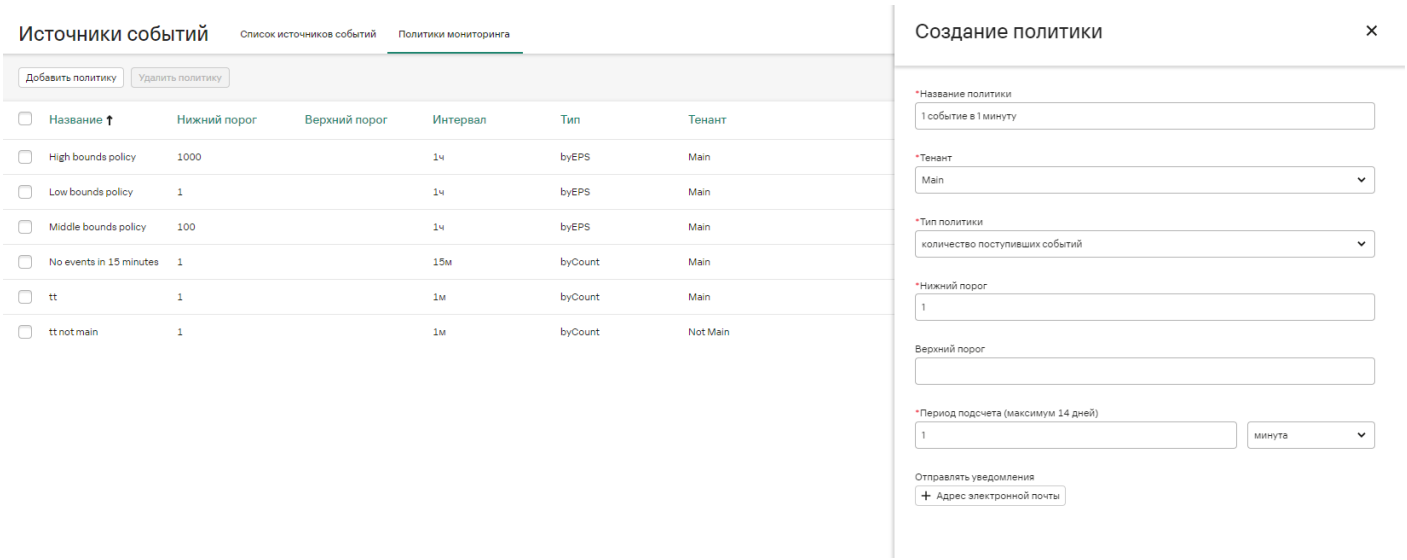
Имеем следующий источник событий (перейдите (в меню слева) на вкладку **Состояние источников**):



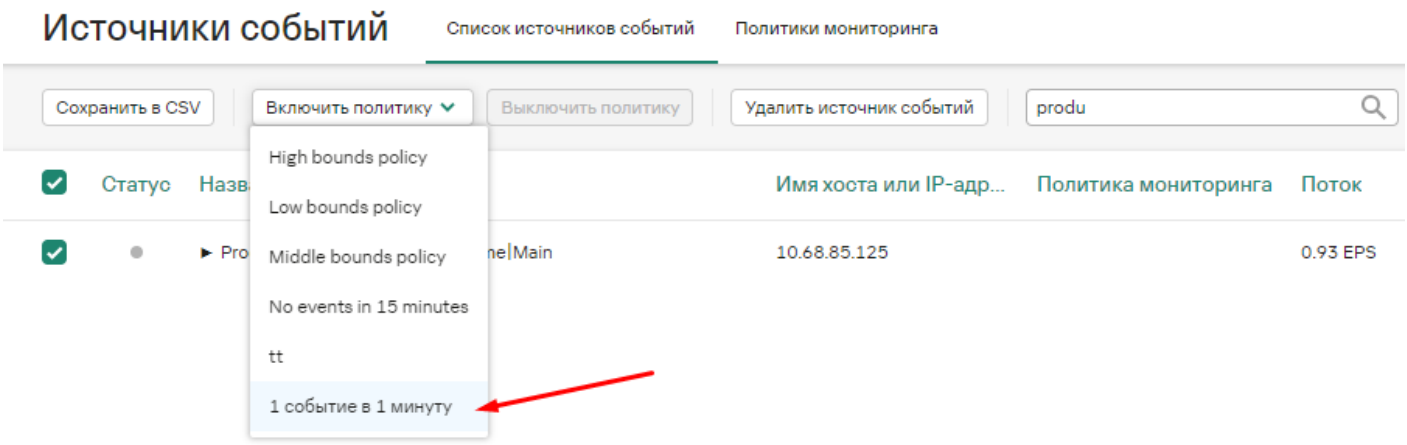
Собятия на этом источнике поступают с потоком 1 EPS.

> Создание источников событий происходит один раз в минуту с именем следующего формата после парсинга: "DeviceProduct|DeviceHostname|DeviceAddress|DeviceProcessName".

Настроим политику мониторинга для этого источника: хотя бы 1 событие в течение 1 минуты. Перейдите на вкладку **Политики мониторинга** и наша политика будет выглядеть следующим образом:

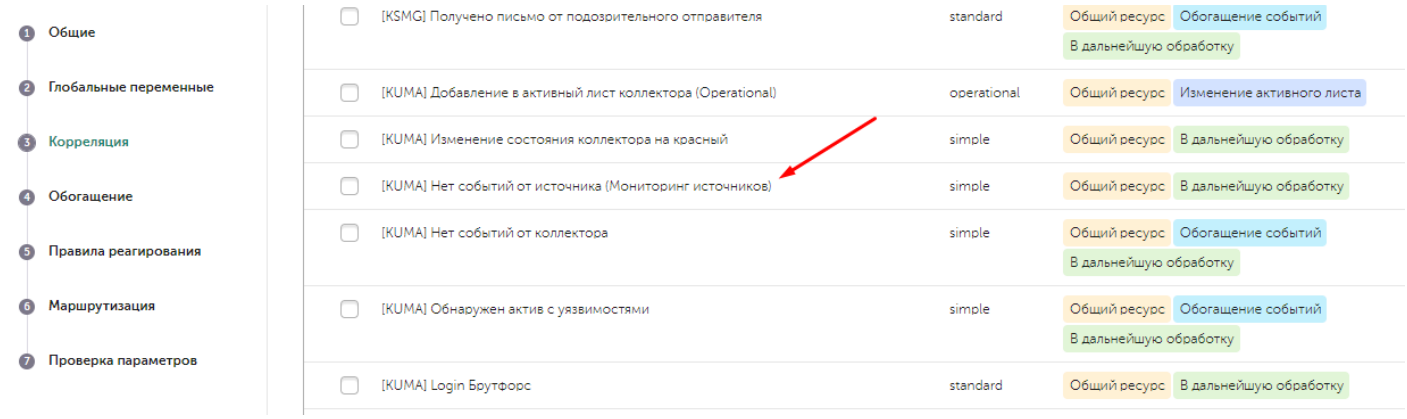


Также можно настроить электронную почту для уведомлений в случае срабатывания политики. Затем необходимо нажать на кнопку **Добавить**. Затем необзодимо перейти снова на вкладку **Список источников событий**, выделить источник и закрепить ранее созданную политику:

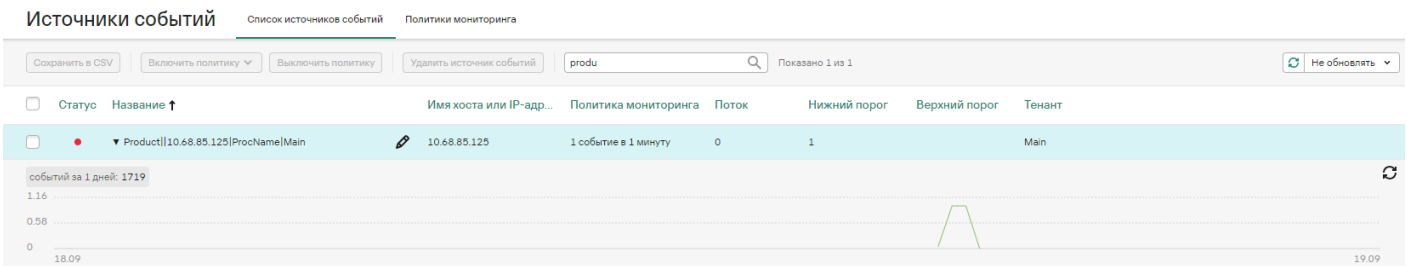


Флажок статуса источника после добавления станет зеленым (означает - соответствие политике).

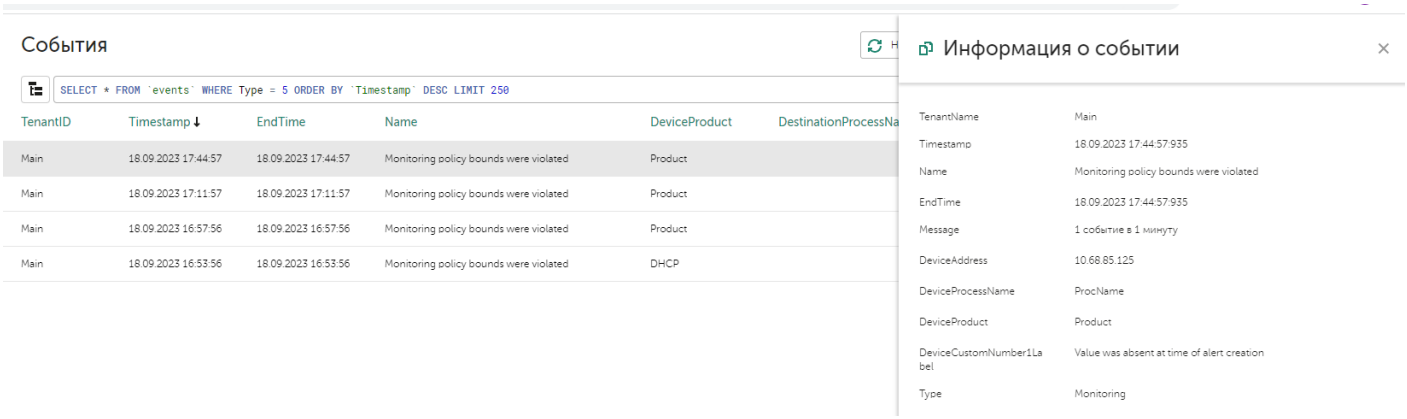
Убедимся, что правило корреляции мониторинга источников (в стоставе Pre-Sales-Pack) добавлено в коррелятор:



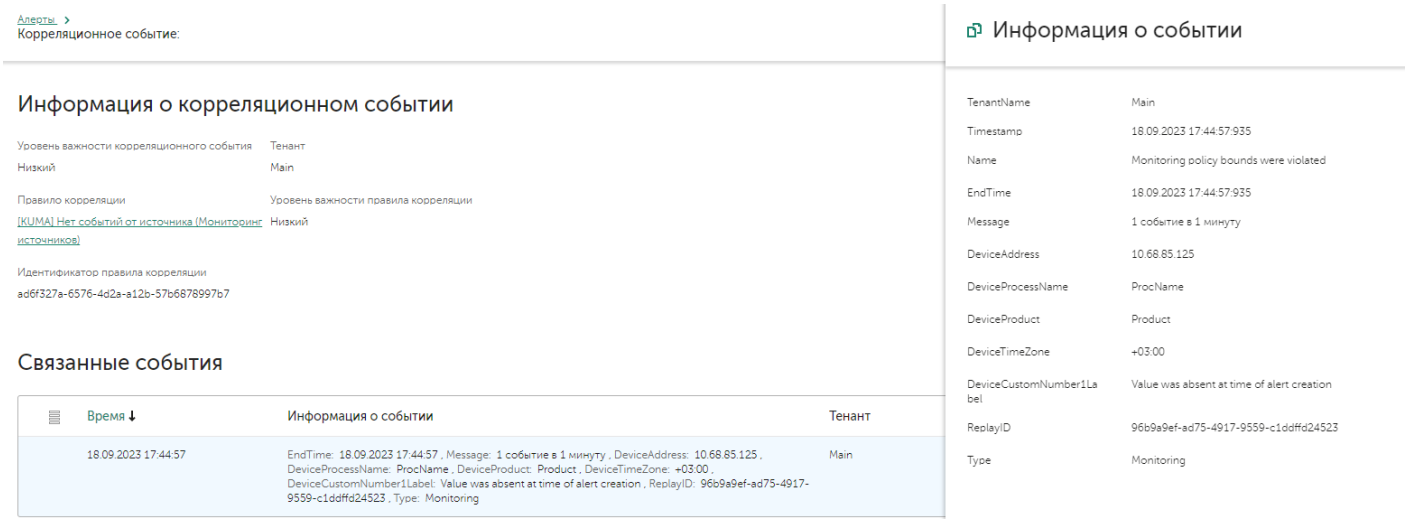
Отключаем подачу событий и получаем следующее:



В событиях:



Алерт:



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