

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

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

На системы приходят следующие события:

События

```
SELECT * FROM `events` WHERE ServiceID = 'cef0527c-25ad-4490-a0ce-bf9ab2af71ee' ORDER BY Timestamp DESC LIMIT 250
```

| TenantID | Timestamp ↓ | EndTime | Name | DeviceProduct | DestinationProcessName |
|----------|---------------------|---------------------|------------|---------------|------------------------|
| Main | 18.09.2023 16:02:14 | 18.09.2023 16:02:14 | Event Name | Product | |
| Main | 18.09.2023 16:02:13 | 18.09.2023 16:02:13 | Event Name | Product | |
| Main | 18.09.2023 15:59:28 | 18.09.2023 15:59:28 | Event Name | Product | |
| Main | 18.09.2023 15:59:27 | 18.09.2023 15:59:27 | Event Name | Product | |
| Main | 18.09.2023 15:59:26 | 18.09.2023 15:59:26 | Event Name | Product | |

Информация о событии

| | |
|---------------------|---------------------------------------|
| TenantName | Main |
| Timestamp | 18.09.2023 16:02:14:771 |
| Name | Event Name |
| EndTime | 18.09.2023 16:02:14:771 |
| DeviceAddress | 10.68.85.125 |
| DeviceAssetID | KUMA.125 |
| DeviceEventCategory | 777 |
| DeviceEventClassID | ClassID |
| DeviceProcessName | ProcName |
| DeviceProduct | Product |
| DeviceReceiptTime | 18.09.2023 16:02:14:771 |
| DeviceTimeZone | +03:00 |
| DeviceVendor | Vendor |
| DeviceVersion | 1.0 |
| Service | TEST BORIS (TCP/5577) |
| Severity | 0 |
| Type | Base |

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

Источники событий

Список источников событий | Политики мониторинга

Сохранить в CSV | Включить политику | Выключить политику | Удалить источник событий | | Показано 1 из 1 | Не обновлять

| Статус | Название ↑ | Имя хоста или IP-адр... | Политика мониторинга | Поток | Нижний порог | Верхний порог | Тенант |
|--------------------------|------------------------------------|-------------------------|----------------------|----------|--------------|---------------|--------|
| <input type="checkbox"/> | Product 10.68.85.125 ProcName Main | 10.68.85.125 | | 0.93 EPS | 0 | | Main |

событий за 1 день: 1420

События 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:

The screenshot shows the 'Источники событий' (Event Sources) interface. On the left, there is a table of monitoring policies. On the right, a 'Создание политики' (Create Policy) dialog box is open, showing the configuration for a new policy.

| Имя | Нижний порог | Верхний порог | Интервал | Тип | Тенант |
|-------------------------|--------------|---------------|----------|---------|----------|
| High bounds policy | 1000 | | 1ч | byEPS | Main |
| Low bounds policy | 1 | | 1ч | byEPS | Main |
| Middle bounds policy | 100 | | 1ч | byEPS | Main |
| No events in 15 minutes | 1 | | 15м | byCount | Main |
| tt | 1 | | 1м | byCount | Main |
| tt not main | 1 | | 1м | byCount | Not Main |

The 'Создание политики' dialog box contains the following fields:

- *Название политики: 1 событие в 1 минуту
- *Тенант: Main
- *Тип политики: количество поступивших событий
- *Нижний порог: 1
- Верхний порог: (empty)
- *Период подсчета (максимум 14 дней): 1, минута
- Отправлять уведомления: + Адрес электронной почты

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

The screenshot shows the 'Источники событий' (Event Sources) interface. A dropdown menu is open over the 'High bounds policy' row, showing a list of available monitoring policies. A red arrow points to the '1 событие в 1 минуту' option.

| Статус | Название | Имя хоста или IP-адрес | Политика мониторинга | Поток |
|--------|-------------------------|------------------------|----------------------|-------|
| ✓ | High bounds policy | | | |
| ✓ | Low bounds policy | | | |
| ✓ | Middle bounds policy | 10.68.85.125 | 0.93 EPS | |
| ✓ | No events in 15 minutes | | | |
| ✓ | tt | | | |
| ✓ | 1 событие в 1 минуту | | | |

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

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

- 1 Общие
- 2 Глобальные переменные
- 3 Корреляция
- 4 Обогащение
- 5 Правила реагирования
- 6 Маршрутизация
- 7 Проверка параметров

| | | | | |
|--------------------------|--|-------------|--|--|
| <input type="checkbox"/> | [KSMG] Получено письмо от подозрительного отправителя | standard | Общий ресурс В дальнейшую обработку | Обогащение событий |
| <input type="checkbox"/> | [KUMA] Добавление в активный лист коллектора (Operational) | operational | Общий ресурс | Изменение активного листа |
| <input type="checkbox"/> | [KUMA] Изменение состояния коллектора на красный | simple | Общий ресурс | В дальнейшую обработку |
| <input type="checkbox"/> | [KUMA] Нет событий от источника (Мониторинг источников) | simple | Общий ресурс | В дальнейшую обработку |
| <input type="checkbox"/> | [KUMA] Нет событий от коллектора | simple | Общий ресурс | Обогащение событий В дальнейшую обработку |
| <input type="checkbox"/> | [KUMA] Обнаружен актив с уязвимостями | simple | Общий ресурс | Обогащение событий В дальнейшую обработку |
| <input type="checkbox"/> | [KUMA] Login Брутфорс | standard | Общий ресурс | В дальнейшую обработку |

Отключаем подачу событий и получаем следующее:

Источники событий | Список источников событий | Политики мониторинга

Сохранить в CSV | Включить политику | Выключить политику | Удалить источник событий | | Показано 1 из 1 |

| <input type="checkbox"/> | Статус | Название ↑ | Имя хоста или IP-адр... | Политика мониторинга | Поток | Нижний порог | Верхний порог | Тенант |
|--------------------------|------------------------------------|------------------------------------|-------------------------|----------------------|-------|--------------|---------------|--------|
| <input type="checkbox"/> | ● | Product[10.68.85.125]ProcName/Main | 10.68.85.125 | 1 событие в 1 минуту | 0 | 1 | | Main |

событий за 1 день: 1719

В событиях:

События | | |

`SELECT * FROM `events` WHERE Type = 5 ORDER BY `Timestamp` DESC LIMIT 250`

| TenantID | Timestamp ↓ | EndTime | Name | DeviceProduct | DestinationProcessName |
|----------|---------------------|---------------------|--|---------------|------------------------|
| 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 |
| DeviceCustomNumberLabel | Value was absent at time of alert creation |
| Type | Monitoring |

Алерт:

[Алерты](#) >
Корреляционное событие:

Информация о корреляционном событии

Уровень важности корреляционного события: **Низкий** | Тенант: **Main**

Правило корреляции: **[KUMA] Нет событий от источника (Мониторинг источников)** | Уровень важности правила корреляции: **Низкий**

Идентификатор правила корреляции: `adb6327a-6576-4d2a-a12b-57b6878997b7`

Связанные события

| Время ↓ | Информация о событии | Тенант |
|---------------------|--|--------|
| 18.09.2023 17:44:57 | EndTime: 18.09.2023 17:44:57, Message: 1 событие в 1 минуту, DeviceAddress: 10.68.85.125, DeviceProcessName: ProcName, DeviceProduct: Product, DeviceTimeZone: +03:00, DeviceCustomNumberLabel: Value was absent at time of alert creation, ReplayID: 96b9a9ef-ad75-4917-9559-c1ddf24523, Type: Monitoring | Main |

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 |
| DeviceTimeZone | +03:00 |
| DeviceCustomNumberLabel | Value was absent at time of alert creation |
| ReplayID | 96b9a9ef-ad75-4917-9559-c1ddf24523 |
| 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