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

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/help/XDR/1.4/ru-RU/270357.htm

В SMP в плейбуках для описания триггеров, правил сегментации и агрегации, а также для фильтров в действиях плейбуков используется язык jq. В этой статье приведены выражения на языке jq, которые будут полезны при создании действий плейбуков.

> Для тренировки в написании выражений на jq можно воспользоваться специальными платформами, например такой: https://www.devtoolsdaily.com/jq_playground/. Также, по опыту, LLM помощники хороши справляются с этой задачей.

В зависимости от выбранного типа действия в плейбуке потребуется задать выражение, которое извлечет из алерта/инцидента активы (пользователи и устройства), хэш, PID или путь к файлу, IP-адрес и наблюдаемые объекты любых типов. По этой причине вместо создания готовых плейбуков было принято решение опубликовать примеры таких выражений, которые могут быть использованы сразу в большом количестве плейбуков и покрывать множество кейсов.

Также от объекта над которым выполняются действия - Алерт, Инцидент, Выбранные объекты - зависит jq-запрос. Поэтому запросы ниже разделены на три соответствующие группы.

??????

В разделе приведены примеры фильтров для раличных типов действий, выполняемых над Алертом.

??????

Ниже приведены примеры jq-выражений для извлечения активов. Выражение в общем смысле должно возвращать массив ID активов.

??????????

1. Имя устройства `TEST`

```
[ alert.Assets[] | select(.Name == "TEST") | .ID]
```

2. Тип актива - устройство (host)

```
[ alert.Assets[] | select(.Type == "host") | .ID]
```

3. Тип актива - устройство (host) и имеет признаки атакующего (IsAttacker)

```
[ alert.Assets[] | select(.Type == "host" and .IsAttacker) | .ID]
```

Тип актива - устройство (host) и имеет признаки жертвы (IsVictim)

```
[ alert.Assets[] | select(.Type == "host" and .IsVictim) | .ID]
```

> Признак "атакующего" и признак "жертвы" настраиваются в правиле корреляции путем обогащения поля AttackerHostID и VictimHostID соответственно. В данные поля могут быть записаны значения из Device/Source/DestinationAssetID.

???????????

Имя пользователя `Alice`

```
[ alert.Assets[] | select(.Name == "Alice") | .ID]
```

Тип актива - пользователь (user)

```
[ alert.Assets[] | select(.Type == "user") | .ID]
```

Тип актива - пользователь (user) и имеет признаки атакующего (IsAttacker)

```
[ alert.Assets[] | select(.Type == "user" and .IsAttacker) | .ID]
```

Тип актива - пользователь и имеет признаки жертвы (IsVictim)

```
[ alert.Assets[] | select(.Type == "user" and .IsVictim) | .ID]
```

> Признак "атакующего" и признак "жертвы" настраиваются в правиле корреляции путем обогащения поля AttackerUserID и VictimUserID соответственно. В данные поля могут быть записаны значения из Source/DestinationAccountID.

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

Ниже приведены примеры jq-выражений для извлечения наблюдаемых объектов. Выражение в общем смысле должно возвращать массив значений наблюдаемых объектов.

1. Хэши

1.1 MD5

```
[ alert.Observables[] | select(.Type == "md5") | .Value ]
```

1.2 SHA256

```
[ alert.Observables[] | select(.Type == "sha256") | .Value ]
```

2. IP-адреса

```
[ alert.Observables[] | select(.Type == "ip") | .Value ]
```

3. URL

```
[ alert.Observables[] | select(.Type == "url") | .Value ]
```

4. Все объекты (например, для действия по обогащению)

```
[ alert.Observables[] | .Value ]
```

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

Для действий также может быть полезна информация из событий, например, путь к файлу.

```
[ alert.OriginalEvents[] | .BaseEvents[] | select(.DeviceEventClassID == "4688") |
.DestinationProcessName ]
```

?????????

В разделе приведены примеры фильтров для раличных типов действий, выполняемых над Инцидентом.

??????

Ниже приведены примеры jq-выражений для извлечения активов. Выражение в общем смысле должно возвращать массив ID активов.

??????????

1. Имя устройства `TEST`

```
[ incident.Alerts[] | .Assets[] | select(.Name == "TEST") | .ID]
```

2. Тип актива - устройство (host)

```
[ incident.Alerts[] | .Assets[] | select(.Type == "host") | .ID]
```

3. Тип актива - устройство (host) и имеет признаки атакующего (IsAttacker)

```
[ incident.Alerts[] | .Assets[] | select(.Type == "host" and .IsAttacker) | .ID]
```

Тип актива - устройство (host) и имеет признаки жертвы (IsVictim)

```
[ incident.Alerts[] | .Assets[] | select(.Type == "host" and .IsVictim) | .ID]
```

> Признак "атакующего" и признак "жертвы" настраиваются в правиле корреляции путем обогащения поля AttackerHostID и VictimHostID соответственно. В данные поля могут быть записаны значения из Device/Source/DestinationAssetID.

???????????

Имя пользователя `Alice`

```
[ incident.Alerts[] | .Assets[] | select(.Name == "Alice") | .ID]
```

Тип актива - пользователь (user)

```
[ incident.Alerts[] | .Assets[] | select(.Type == "user") | .ID]
```

Тип актива - пользователь (user) и имеет признаки атакующего (IsAttacker)

```
[ incident.Alerts[] | .Assets[] | select(.Type == "user" and .IsAttacker) | .ID]
```

Тип актива - пользователь и имеет признаки жертвы (IsVictim)

```
[ incident.Alerts[] | .Assets[] | select(.Type == "user" and .IsVictim) | .ID]
```

> Признак "атакующего" и признак "жертвы" настраиваются в правиле корреляции путем обогащения поля AttackerUserID и VictimUserID соответственно. В данные поля

могут быть записаны значения из Source/DestinationAccountID.

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

Ниже приведены примеры jq-выражений для извлечения наблюдаемых объектов. Выражение в общем смысле должно возвращать массив значений наблюдаемых объектов.

1. Хэши

1.1 MD5

```
[ incident.Alerts[] | .Observables[] | select(.Type == "md5") | .Value ]
```

1.2 SHA256

```
[ incident.Alerts[] | .Observables[] | select(.Type == "sha256") | .Value ]
```

2. IP-адреса

```
[ incident.Alerts[] | .Observables[] | select(.Type == "ip") | .Value ]
```

3. URL

```
[ incident.Alerts[] | .Observables[] | select(.Type == "url") | .Value ]
```

4. Все объекты (например, для действия по обогащению)

```
[ incident.Alerts[] | .Observables[] | .Value ]
```

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

Для действий также может быть полезна информация из событий, например, путь к файлу.

```
[ incident.Alerts[] | .OriginalEvents[] | .BaseEvents[] | select(.DeviceEventClassID ==
"4688") | .DestinationProcessName ]
```

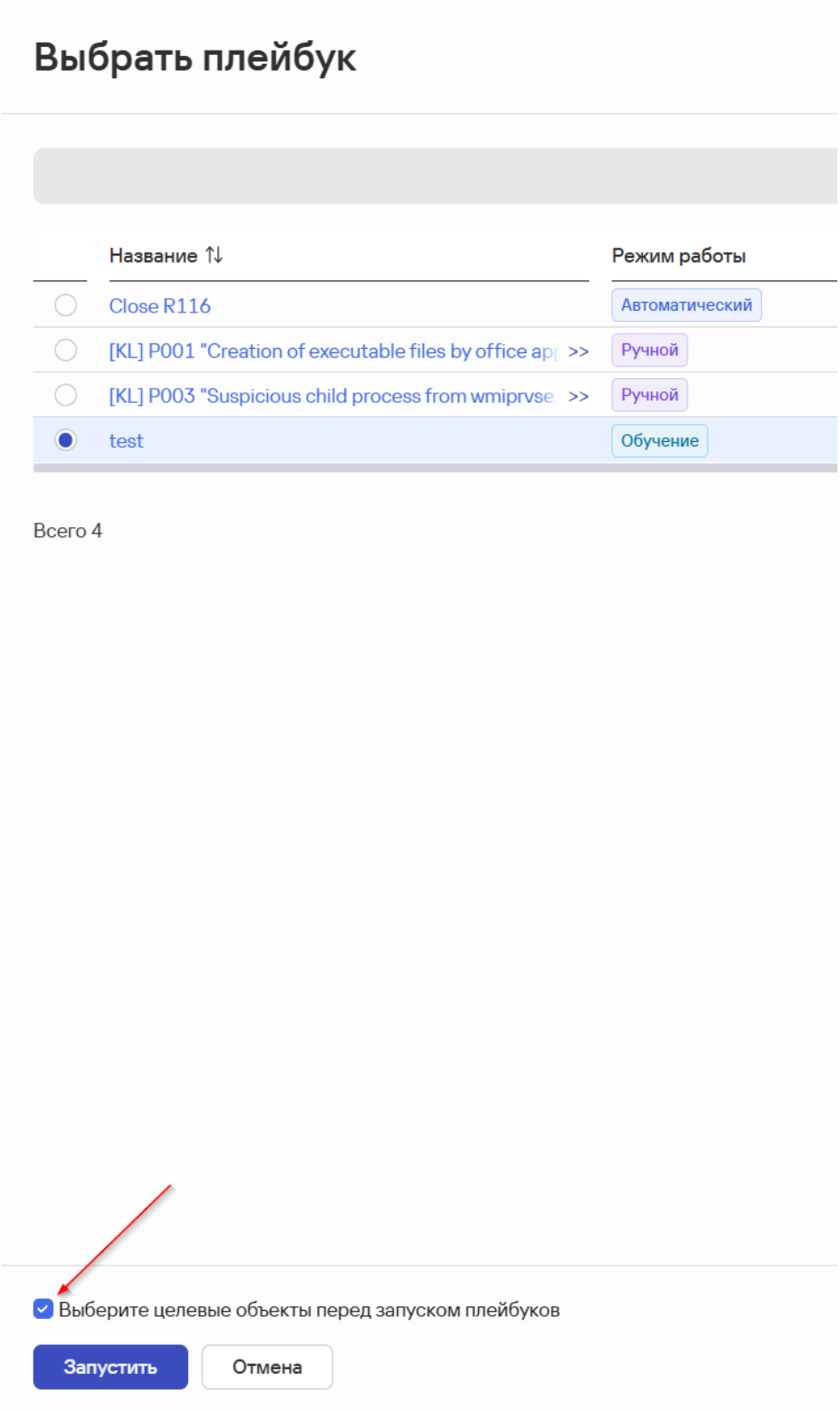
????????? ???????

Помимо возможности автоматического выбора активов и индикаторов для реагирования, их можно также задавать вручную при реагировании. В таком случае синтаксис будет отличаться от используемого в Алертах и Инцидентах при автоматическом выборе, но при

этом будет одинаков независимо от места применения плейбука.

Выбор объектов для запуска плейбуков

Выбор объектов для запуска доступен при ручном запуске плейбука. Для этого надо поставить галочку у соответствующей настройки перед запуском плейбука.



Т.к. объекты перед запуском выбирают вручную, то тонкая дополнительная фильтрация лишена смысла. Ниже будут приведены примеры для для указания активов и наблюдаемых объектов, разделенных только по их типам.

??????

Ниже приведены примеры jq-выражений для извлечения активов. Выражение в общем смысле должно возвращать массив ID активов.

??????????

```
[ .input.assets[] | select(.Type=="host") | .ID ]
```

???????????

```
[ .input.assets[] | select(.Type=="user") | .ID ]
```

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

Ниже приведены примеры jq-выражений для извлечения наблюдаемых объектов. Выражение в общем смысле должно возвращать массив значений наблюдаемых объектов.

1. Хэши

1.1 MD5

```
[ .input.observables[] | select(.Type == "md5") | .Value ]
```

1.2 SHA256

```
[ .input.observables[] | select(.Type == "sha256") | .Value ]
```

2. IP-адреса

```
[ .input.observables[] | select(.Type == "ip") | .Value ]
```

3. URL

```
[ .input.observables[] | select(.Type == "url") | .Value ]
```

??????????

Данная статья содержит базовый набор выражений, которые пригодятся при описании действий плейбуков. Если у вас есть замечания или предложения по содержимому статьи, а также собственные идеи для выражений - пишите в наш телеграм-канал (ссылка и инструкция на главной странице).

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

Модель данных алерта - https://support.kaspersky.com/help/XDR/1.4/ru-RU/269125.htm

Модель данных инцидента - https://support.kaspersky.com/help/XDR/1.4/ru-RU/269168.htm

---

Revision #4
Created 2025-12-01 13:08:50 UTC by Koala
Updated 2025-12-04 11:03:16 UTC by Koala