Триггеры в плейбуках

> Конструктор jq для OSMP: https://koalapower.github.io/jq_builder/

> 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/273327.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 триггеров 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.

Т.к. описание триггера плейбуков отличается для Алертов и Инцидентов данная статья разделена на две соответствующие части.

Алерты

Свойства алерта

Ниже приведены примеры триггеров для алертов, по их базовым свойствам

1. Имя алерта начинается с `Test`

```
.Name | startswith("Test")
```

2. Имя алерта `Test`

```
.Name == "Test"
```

3. Тактика `TA0003`

```
[.MITRETactics[] | .ID == " TA0003"] | any
```

4. Техника `T1098`

```
[.MITRETechniques[] | .ID == " T1098"] | any
```

5. Уровень важности алерта высокий (`high`). Возможные значения: `low`, `medium`, `high`, `critical`.

```
.Severity =="high"
```

6. Статус алерта - новый (`new`). Возможные значения: `new`, `inProgress`, `inIncident`, `closed`.

```
.Status == "new"
```

Правила корреляции

Ниже приведены примеры триггеров для алертов, по свойствам правил корреляции

1. Правило начинается с `Test`

```
[.Rules[] | .Name | startswith("Test")] | any
```

2. Название правила `Test`

```
[.Rules[] | .Name=="Test"] | any
```

3. Название правила содержит `Test`

```
[.Rules[] | .Name | contains("Test")] | any
```

3. Правило соответствует регулярному выражению `^R\d{3}.+` (характерно для коробочного контента)

```
[.Rules[]| .Name | test("R\\d{3}.+") ] | any
```

4. Уровень важности правила - критический (`critical`). Возможные значения: `low`, `medium`, `high`, `critical`.

```
[.Rules[] | .Severity == "critical"] | any
```

5. Алерт относится к КИИ (содержит КИИ активы)

```
.IsCII
```

Активы

В разделе приведены примеры триггеров для активов, связанных с алертами. Т.к. в SMP активы объединяют в себе устройства и пользователей, раздел разделен на две соответствующие части.

Устройства

1. Имя устройства `TEST-PC`

```
[.Assets[] | select(.Type == "host") | .Name=="TEST-PC"] | any
```

2. ID устройства `00000000-0000-0000-0000-000000000000`

```
[.Assets[] | select(.Type == "host") | .ID=="00000000-0000-0000-0000-000000000000"] | any
```

3. По категории критичности актива

3.1 Актив относится к КИИ

```
[.Assets[] | select(.Type == "host") | .CIICategory == "CII"] | any
```

3.2 Актив не относится к КИИ

```
[.Assets[] | select(.Type == "host") | .CIICategory == "notCII"] | any
```

Пользователи

1. Имя учетной записи `test`

```
[.Assets[] | select(.Type == "user") | .Name=="test"] | any
```

2. ID учетной записи (внутренний ID в платформе) `00000000-0000-0000-0000-000000000000`

```
[.Assets[] | select(.Type == "user") | .ID=="00000000-0000-0000-0000-000000000000"] | any
```

Наблюдаемые объекты

В разделе приведены примеры триггеров для наблюдаемых объектов, связанных с алертами.

> Наблюдаемые объекты - это индикаторы, в т.ч. хэши, ip-адреса, url, домены, имена пользователей и т.п., которые автоматически извлекаются из базовых и корреляционных событий по внутренней логике SMP и добавляются в карточку алерта/ицидента в соответствующий раздел.

1. Домен `DEMO.LAB`

```
[.Observables[] | select(.Type == "domain") | .Value=="DEMO.LAB"] | any
```

2. URL `https://abc.demo.lab`

```
[.Observables[] | select(.Type == "url") | .Value=="https://abc.demo.lab"] | any
```

3. Хэш

3.1 MD5 хэш `00000000000000000000000000000000`

```
[.Observables[] | select(.Type == "md5") | .Value=="00000000000000000000000000000000"] | any
```

3.2 SHA256 хэш `0000000000000000000000000000000000000000000000000000000000000000`

```
[.Observables[] | select(.Type == "sha256") |
.Value=="0000000000000000000000000000000000000000000000000000000000000000"] | any
```

4. IP-адрес

4.1 IP-адрес равен `192.168.100.100`

```
[.Observables[] | select(.Type == "ip") | .Value=="192.168.100.100"] | any
```

4.2 IP-адрес находится в подсети `192.168.100.0/24` (грубый пример)

```
[.Observables[] | select(.Type == "ip") | .Value | (test("^192\\.168\\.100\\.")] | any
```

> В jq нет встроенной функции проверки адреса в подсети, поэтому предлагается использовать обходные пути через регулярные выражения или contains.

5. Имя пользователя `Alice`

```
[.Observables[] | select(.Type == "userName") | .Value=="Alice"] | any
```

6. Устройство

6.1 Имя устройства `abc.demo.lab`

```
[.Observables[] | select(.Type == "hostName") | .Value=="abc.demo.lab"] | any
```

6.1 Домен устройства `demo.lab` (грубый пример)

```
[.Observables[] | select(.Type == "hostName") | .Value | endswith(".demo.lab")] | any
```

События

Помимо прочего, в триггерах можно обращаться к базовым и корреляционным событиям и извлекать для проверки их них любую информацию. В виду большого числа вариантов ниже будет приведено лишь несколько примеров такого использования.

1. По SID пользователя из базового события в поле `SourceUserID` равный `S-1-5-18`

```
[.OriginalEvents[] | .BaseEvents[] | .SourceUserID == "S-1-5-18"] | any
```

2. По домену из базового события в поле `SourceNtDomain` равный `DEMO.LAB`

```
[.OriginalEvents[] | .BaseEvents[] .SourceNtDomain=="DEMO.LAB" ] | any
```

Инциденты

Свойства инцидента

Ниже приведены примеры триггеров для инцидентов, по их базовым свойствам

1. Имя инцидента начинается с `Test`

```
  .Name | startswith("Test")
```

2. Имя инцидента `Test`

```
  .Name == "Test"
```

3. Тактика `TA0003`

```
[ .Alerts[] | .MITRETactics[] | .ID == " TA0003"] | any
```

4. Техника `T1098`

```
[ .Alerts[] | .MITRETechniques[] | .ID == " T1098" ] | any
```

5. Уровень важности инцидента высокий (`high`). Возможные значения: `low`, `medium`, `high`, `critical`.

```
.Severity =="high"
```

6. Уровень приоритета инцидента высокий (`high`). Возможные значения: `low`, `medium`, `high`, `critical`.

```
.Priority =="high"
```

7. Статус инциденнта - открыт (`open`). Возможные значения: `open`, `inProgress`, `hold`, `closed`.

```
.Status == "open"
```

8. Имя рабочего процесса инцидента `standard`.

```
.WorkflowName == "standard"
```

9. Инцидент относится к КИИ (содержит КИИ активы)

```
.IsCII
```

Правила корреляции

Ниже приведены примеры триггеров для инцидентов, по свойствам правил корреляции

1. Правило начинается с `Test`

```
[ .Alerts[] | .Rules[] | .Name | startswith("Test")] | any
```

2. Название правила `Test`

```
[ .Alerts[] | .Rules[] | .Name=="Test"] | any
```

3. Название правила содержит `Test`

```
[ .Alerts[] | .Rules[] | .Name | contains("Test")] | any
```

3. Правило соответствует регулярному выражению `^R\d{3}.+` (характерно для коробочного контента)

```
[ .Alerts[] | .Rules[]| .Name | test("R\\d{3}.+") ] | any
```

4. Уровень важности правила - критический (`critical`). Возможные значения: `low`, `medium`, `high`, `critical`.

```
[ .Alerts[] | .Rules[] | .Severity == "critical"] | any
```

Активы

В разделе приведены примеры триггеров для активов, связанных с инцидентами. Т.к. в SMP активы объединяют в себе устройства и пользователей, раздел разделен на две соответствующие части.

Устройства

1. Имя устройства `TEST-PC`

```
[ .Alerts[] | .Assets[] | select(.Type == "host") | .Name=="TEST-PC"] | any
```

2. ID устройства `00000000-0000-0000-0000-000000000000`

```
[ .Alerts[] | .Assets[] | select(.Type == "host") | .ID=="00000000-0000-0000-0000-
000000000000"] | any
```

3. По категории критичности актива

3.1 Актив относится к КИИ

```
[ .Alerts[] | .Assets[] | select(.Type == "host") | .CIICategory == "CII"] | any
```

3.2 Актив не относится к КИИ

```
[ .Alerts[] | .Assets[] | select(.Type == "host") | .CIICategory == "notCII"] | any
```

Пользователи

1. Имя учетной записи `test`

```
[ .Alerts[] | .Assets[] | select(.Type == "user") | .Name=="test"] | any
```

2. ID учетной записи (внутренний ID в платформе) `00000000-0000-0000-0000-000000000000`

```
[ .Alerts[] | .Assets[] | select(.Type == "user") | .ID=="00000000-0000-0000-0000-
000000000000"] | any
```

Наблюдаемые объекты

В разделе приведены примеры триггеров для наблюдаемых объектов, связанных с инцидентами.

> Наблюдаемые объекты - это индикаторы, в т.ч. хэши, ip-адреса, url, домены, имена пользователей и т.п., которые автоматически извлекаются из базовых и корреляционных событий по внутренней логике SMP и добавляются в карточку алерта/ицидента в соответствующий раздел.

1. Домен `DEMO.LAB`

```
[ .Alerts[] | .Observables[] | select(.Type == "domain") | .Value=="DEMO.LAB"] | any
```

2. URL `https://abc.demo.lab`

```
[ .Alerts[] | .Observables[] | select(.Type == "url") | .Value=="https://abc.demo.lab"] | any
```

3. Хэш

3.1 MD5 хэш `00000000000000000000000000000000`

```
[ .Alerts[] | .Observables[] | select(.Type == "md5") |
.Value=="00000000000000000000000000000000"] | any
```

3.2 SHA256 хэш `0000000000000000000000000000000000000000000000000000000000000000`

```
[ .Alerts[] | .Observables[] | select(.Type == "sha256") |
.Value=="0000000000000000000000000000000000000000000000000000000000000000"] | any
```

4. IP-адрес

4.1 IP-адрес равен `192.168.100.100`

```
[ .Alerts[] | .Observables[] | select(.Type == "ip") | .Value=="192.168.100.100"] | any
```

4.2 IP-адрес находится в подсети `192.168.100.0/24` (грубый пример)

```
[ .Alerts[] | .Observables[] | select(.Type == "ip") | .Value | test("^192\\.168\\.100\\.")] | any
```

> В jq нет встроенной функции проверки адреса в подсети, поэтому предлагается использовать обходные пути через регулярные выражения или contains.

5. Имя пользователя `Alice`

```
[ .Alerts[] | .Observables[] | select(.Type == "userName") | .Value=="Alice"] | any
```

6. Устройство

6.1 Имя устройства `abc.demo.lab`

```
[ .Alerts[] | .Observables[] | select(.Type == "hostName") | .Value=="abc.demo.lab"] | any
```

6.1 Домен устройства `demo.lab` (грубый пример)

```
[ .Alerts[] | .Observables[] | select(.Type == "hostName") | .Value | endswith(".demo.lab")] | any
```

События

Помимо прочего, в триггерах можно обращаться к базовым и корреляционным событиям и извлекать для проверки их них любую информацию. В виду большого числа вариантов ниже будет приведено лишь несколько примеров такого использования.

1. По SID пользователя из базового события в поле `SourceUserID` равный `S-1-5-18`

```
[ .Alerts[] | .OriginalEvents[] | .BaseEvents[] | .SourceUserID == "S-1-5-18"] | any
```

2. По домену из базового события в поле `SourceNtDomain` равный `DEMO.LAB`

```
[ .Alerts[] | .OriginalEvents[] | .BaseEvents[] .SourceNtDomain=="DEMO.LAB" ] | any
```

Объединение условий

Приведенные выше условия можно объединять между собой используя различные логические операторы, такие как or, and, not.

Например, выражение для "Имя инцидента начинается с `Test`, статус инцидента - открыт (`open`) и инцидент не относится к КИИ

```
( .Name | startswith("Test")) and (.Status == "open") and (.IsCII | not)
```

В примерах с массивами выше часто встречается условие с `any`, которое означает "совпадение как минимум одного объекта", если для условия требуется совпадение всех объектов, то условие следует заменить на `all`.

Например, для инцидента, у которого все связанные правила корреляции имеют важность критические

```
[ .Alerts[] | .Rules[] | .Severity == "critical"] | all
```

Также для сравнения не с одним, но с массивом значений можно использовать оператор `IN`.

Например, триггер по нескольким именам хостов

```
[ .Alerts[] | .Assets[] | select(.Type == "host") | .Name | IN("TEST-PC1", "TEST-PC2", "ADMIN-PC")] | any
```

Заключение

Данная статья содержит базовый набор выражений, которые пригодятся при описании триггеров 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).

Полезные ссылки

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 #8
Created 2025-12-01 09:38:55 UTC by Koala
Updated 2026-10-05 08:13:10 UTC by Koala