

# Table of Contents

Detecting SSH bruteforce attacks using triggers in QoE ..... 3

*System trigger for detecting SSH bruteforce attacks* ..... 3



# Detecting SSH bruteforce attacks using triggers in QoE

[Triggers](#) are used to search data in QoE Stor by specified parameters. When a trigger fires, one of the following actions can occur:

- notification in GUI
- HTTP action
- email delivery

Required SSG DPI options:

- [Statistics gathering and analysis on protocols and directions](#)
- [Subscriber notifications](#)

Required additional modules:

- [DPIUI2 \(GUI - Graphical User Interface\)](#)
- [Implementation and administration](#)

## System trigger for detecting SSH bruteforce attacks

The trigger for detecting SSH bruteforce attacks (name — "ssh bruteforce") is a system trigger and is available in "QoE analytics" → "Triggers and notifications" (disabled by default).

### General trigger information

| Common                              |                   |                     |                                   |
|-------------------------------------|-------------------|---------------------|-----------------------------------|
| Trigger name *                      | Severity          | Trigger             |                                   |
| ssh bruteforce                      | Hight             | ▼                   | <input type="checkbox"/> Disabled |
| Days of the week *                  | Check frequency * | Number of positives |                                   |
| Mon, Tue, Wed, Thu, Fri, Sat, Sun ▼ | 10 minutes        | ▼ 0                 |                                   |
| Start date                          | End date          | Start time          | End time                          |
| 12/01/2024                          | 12/31/2099        | 00:00               | 23:55                             |

- Trigger name: "ssh bruteforce";
- Days of week — all;
- Check frequency — 10 minutes;
- Trigger activation frequency — 0;
- Start/end dates and times can be set if needed.



Every day, a check will be performed every 10 minutes according to the conditions described below.

## Queries

| Queries                                |            |                |   |                  |                  |   |
|--|------------|----------------|---|------------------|------------------|---|
| +                                      |            |                |   |                  |                  |   |
|  | Query name | Report         |   | Period from      | Period to        |   |
| <input checked="" type="checkbox"/> On | A          | Ssh bruteforce | ▽ | now - 30 minutes | now - 20 minutes | 🗑 |

For this trigger a non-editable query is preset with the following parameters:

- Table to scan: Raw full netflow → Tables → Attacks detection → Ssh bruteforce;
- Period from: now - 30 minutes
- Period to: now - 20 minutes

## Conditions

| Conditions                             |      |            |          |            |                 |          |       |
|--|------|------------|----------|------------|-----------------|----------|-------|
| +                                      |      |            |          |            |                 |          |       |
|  | Bind | Query name | Function | Combinator | Serie           | Operator | Value |
| <input checked="" type="checkbox"/> On | AND  | A          | avg      |            | Session lifetir | <=       | 20    |
| <input checked="" type="checkbox"/> On | AND  | A          | max      |            | Sessions per    | >=       | 1500  |

- Add two "+" fields
- Link - AND
- Function - avg
- Series in field 1 - session lifetime to subscriber <= 20 (ms)
- Series in field 2 - number of sessions per subscriber >= 1500



We set the trigger conditions: average duration of SSH sessions to a subscriber is less than 20 ms and the number of SSH sessions for the subscriber is greater than 1500 for the analyzed period.

## Error handling



- In "If no errors" — no data

- In "If error or timeout" — save last state



With this configuration, if there are no errors, no data is saved; if errors occur, information about suspicious activity is saved.

## Actions

### E-mail action



- Click the "</>" icon to auto-fill the form
- In the "To" field — specify the email address
- With this setup, when the trigger fires an email with the notification details (ID, trigger name, status, link to the report — saved state) will be sent to the specified address

### Notification



- Click "</>" to auto-fill the form
- Select notification type — "Warning"
- This will create a notification in the SSG system

You can get a link to the report via the notifications menu

Select the notification Choose — "Details"

Follow the report link — the report will open in a new browser window.

### HTTP action



Click "</>" to auto-fill the form. Choose the method most suitable for your ticket system and enter the URL.



Keep in mind — the numeric thresholds for sessions, incoming packets, etc., are given as averaged examples. Fine-tune thresholds based on your network specifics.