kaspersky

How to integrate Kaspersky Threat Data Feeds with FortiSIEM

Product version: 1.1

kaspersky

Dear User,

Thank you for choosing Kaspersky as your security software provider. We hope that this document will help you to use our product.

Document revision date: 24/03/2020

https://www.kaspersky.com
https://help.kaspersky.com
https://support.kaspersky.com

About Kaspersky (https://www.kaspersky.com/about/company)

kaspersky

Contents

About this document 4
How to integrate Kaspersky CyberTrace with FortiSIEM 5
Configuring Kaspersky CyberTrace for integration with FortiSIEM 5
Configuring event forwarding from FortiSIEM 9
Receiving events from Kaspersky CyberTrace in FortiSIEM 11
Displaying actionable fields 12
Looking up events received from Kaspersky CyberTrace in FortiSIEM 13
AO Kaspersky Lab 14
Trademark notices 15

kaspersky

About this document

This document contains instructions for integrating Kaspersky Threat Data Feeds with such security information and event management (SIEM) software as FortiSIEM™.

We recommend that you integrate Kaspersky Threat Data Feeds with FortiSIEM using Kaspersky CyberTrace because Kaspersky CyberTrace offers the following features:

- Automatic high-performance matching of incoming logs and events with Kaspersky Threat Data Feeds, OSINT feeds, or any other custom feeds in the most popular formats (JSON, STIX, XML, CSV). Demo feeds from Kaspersky and OSINT are available out of the box.
- Internalized process of parsing and matching incoming data significantly reduces SIEM solution load. Kaspersky CyberTrace parses incoming logs and events, matches the resulting data to feeds, and generates its own alerts on threat detection. Consequently, a SIEM solution has to process less data.
- Generates feed usage statistics for measuring the effectiveness of feeds.
- In-depth threat investigation through on-demand lookup of indicators (hashes, IP addresses, domains, URLs). Bulk scanning of logs and files is also supported.
- Universal approach to integration of threat matching capabilities with SIEM solutions and other security controls. SIEM connectors for a wide range of SIEM solutions can be used to visualize and manage data about threat detections.
- IoC and related context are efficiently stored in RAM for rapid access and filtering.
- Kaspersky CyberTrace Web, a web user interface for Kaspersky CyberTrace, provides data visualization, on-demand IoC lookup functionality, and access to Kaspersky CyberTrace configuration. Kaspersky CyberTrace Web also supports the management of feeds, log parsing rules, black lists and white lists, and event sources.
- Command-line interface for Windows and Linux® platforms.
- Advanced filtering for feeds and log events. Feeds can be converted and filtered based on a broad set of criteria such as time, popularity, geographical location, and threat type. Log events can be filtered based on custom conditions.
- DMZ integration support. The computer on which event data is matched against feeds can be located in DMZ and isolated from the Internet.
- In standalone mode, where Kaspersky CyberTrace is not integrated with a SIEM solution, Kaspersky CyberTrace receives logs from various sources such as networking devices and parses these logs according to defined regular expressions.
- Export lookup results that match feeds to CSV format for integration with other systems (firewalls, network and host IDS, custom tools).
- Exposes obfuscation techniques used by some threats to hide malicious activities in logs.

Use Kaspersky CyberTrace for Log Scanner (https://support.kaspersky.com/13858) for integration with FortiSIEM.

The application contains a certificate for the demo version of Kaspersky Threat Data Feeds. To obtain a certificate for the commercial version of Kaspersky Threat Data Feeds, contact the Kaspersky CyberSecurity Service team (intelligence@kaspersky.com).

kaspersky

How to integrate Kaspersky CyberTrace with FortiSIEM

This section describes the steps you take to integrate Kaspersky CyberTrace with FortiSIEM.

Integration instructions provided in this document apply to FortiSIEM version 5.2.

► *To integrate Kaspersky CyberTrace with FortiSIEM:*

1. Configure Kaspersky CyberTrace for integration with FortiSIEM (see section "Configuring Kaspersky CyberTrace for integration with FortiSIEM" on page 5).
2. Configure forwarding events from FortiSIEM to Kaspersky CyberTrace (see section "Configuring event forwarding from FortiSIEM" on page 9).
3. Configure sending events from Kaspersky CyberTrace and receiving them in FortiSIEM (see section "Receiving events from Kaspersky CyberTrace in FortiSIEM" on page 11).

After this, you can browse events, received from Kaspersky CyberTrace, in FortiSIEM (see section "Looking up events received from Kaspersky CyberTrace in FortiSIEM" on page 13).

In this chapter

Configuring Kaspersky CyberTrace for integration with FortiSIEM 5
Configuring event forwarding from FortiSIEM 9
Receiving events from Kaspersky CyberTrace in FortiSIEM 11
Displaying actionable fields 12
Looking up events received from Kaspersky CyberTrace in FortiSIEM 13

Configuring Kaspersky CyberTrace for integration with FortiSIEM

This section describes how to configure Kaspersky CyberTrace for integration with FortiSIEM.

► *To configure Kaspersky CyberTrace for integration with FortiSIEM:*

1. Install Kaspersky CyberTrace as described at https://click.kaspersky.com/?hl=en-US&link=online_help&pid=CyberTrace&version=1.0&helpid=162489.
   - In Linux®, Kaspersky CyberTrace is installed to the `/opt/kaspersky/ktfs` directory.
   - For the Windows® installation, the installation directory is hereinafter referred to as `%CyberTrace_installDir%`.
2. Open the kl_feed_service.conf configuration file for edit.

- In Linux, the kl_feed_service.conf file is located in the `/opt/kaspersky/ktfs/etc` directory.
- In Windows, the kl_feed_service.conf file is located in the `%CyberTrace_installDir%\bin` directory.

> You can also configure Kaspersky CyberTrace and specify the settings described in this section by using Kaspersky CyberTrace Web.

3. Make sure that the `Configuration > InputSettings > ConnectionString` element contains the IP address of the computer on which Kaspersky CyberTrace will operate, and an unoccupied port (for example, `9999`). The IP address and port must be specified in the format `%IP_address%:%port%` (for example, `10.43.11.15:9999`).
4. In the kl_feed_service.conf file, set the following elements to the `Configuration > InputSetting > RegExps > Source id="default"` element:

```
<RE_HASH type="HASH" extract="all">([\da-fA-F]{32,64})</RE_HASH>

<RE_IP type="IP"
extract="first">dst\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:$|\s)</RE_I
P>

<SRC_IP type="IP"
extract="first">src\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:$|\s)</SRC_
IP>

<RE_URL type="URL"
extract="all"><![CDATA[(?:\:\/\/)((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00
a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-\x{ffff}0-9]*)(?:\.(?:[a-z\x{00a1}-\x
{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{fff
f}\-0-9]{2,}+)))(?:\.*:\d{2,5})?+(?:\.*\/[^\s\"\<\>]*+)?+)]]></RE_URL>

<Device type="CONTEXT"
extract="first">[^\|]*\|[^\|]*\|([^\|]*)\|</Device>

<Product type="CONTEXT"
extract="first">[^\|]*\|[^\|]*\|([^\|]*)\|</Product>

<Id type="CONTEXT" extract="first">eventId\=(\d+)(?:$|\s)</Id>

<DeviceIp type="CONTEXT"
extract="first">dvc\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:$|\s)</Devi
ceIp>

<UserName type="CONTEXT" extract="first">suser\=(.*?)(?:$|\s)</UserName>
```

5. In the `Configuration > OutputSettings > AlertFormat` element, specify the following value:

```
CEF:0|Kaspersky|CyberTrace|3.1|1|CyberTrace Service Event|4|
reason=%Alert% msg=%RecordContext%
```

6. In the `Configuration > OutputSettings > EventFormat` element, specify the following value:

```
CEF:0|Kaspersky|CyberTrace|3.1|2|CyberTrace Detection
Event|8|reason=%Category% dst=%RE_IP% src=%SRC_IP% dvc=%DeviceIp%
fileHash=%RE_HASH% request=%RE_URL% sourceServiceName=%Device%
sproc=%Product% suser=%UserName% externalId=%Id% %ActionableFields%
```

```
cs5Label=MatchedIndicator cs5=%MatchedIndicator% msg=%RecordContext%
```

7. In the `Configuration > OutputSettings > ConnectionString` element, specify the IP address of the FortiSIEM installation to which Kaspersky CyberTrace will send detection events, and port `514`.

   Specify the IP address and port in the format `%IP_address%:%port%` (for example, `10.43.11.43:514`).

8. Make sure that the `Configuration > OutputSettings > ActionableFieldContextFormat` element contains the following value:

   ```
   <![CDATA[%ParamName%=%ParamValue% ]]>
   ```

9. Make sure that the `Configuration > OutputSettings > RecordFieldContextFormat` element contains the following value:

   ```
   <![CDATA[%ParamName%:%ParamValue% ]]>
   ```

10. Make sure that the value of the `enabled` attribute of the `Configuration > OutputSettings > FinishedEventFormat` element is `false`.

    In the `InputSettings > EventDelimiter` element, specify the following rule:

    ```
    <![CDATA[[^\=](\<\d+\>)]]>
    ```

11. In the Feeds element, replace all occurrences of `RE_SHA1`, `RE_MD5` and `RE_SHA256` with `RE_HASH`.
12. Restart Feed Service, which is one of the modules of Kaspersky CyberTrace, by running the following command:
    - `/opt/kaspersky/ktfs/etc/init.d/kl_feed_service restart` (in Linux)
    - `%CyberTrace_installDir%\bin\kl_control.bat restart` (in Windows)

Viewing the format of forwarded events in FortiSIEM

The procedure above assumes that universal regular expressions are used for extracting IP addresses, URLs, and hashes from events sent from FortiSIEM. You may have to change these and other regular expressions depending on the format of the events. For example, you may have to do this for extracting from an event the user name or other data that will later be inserted in a detection event and sent to FortiSIEM. Before editing the existing regular expressions or adding new ones you have to analyze the original events arrived in Kaspersky CyberTrace.

You can also browse these events in Kaspersky CyberTrace Web as described at https://click.kaspersky.com/?hl=en-US&link=online_help&pid=CyberTrace&version=1.0&helpid=162489. After you configure the event forwarding in FortiSIEM, in Kaspersky CyberTrace Web select the **Settings** tab and then the **Matching** tab, and in the **Event parsing rules** section you will see the events that arrive in Kaspersky CyberTrace.

► *To view the format of events in FortiSIEM:*

1. On the FortiSIEM web console, select the **Analytics** tab.

2. Click inside the **Edit Filters and Time Range** text field.

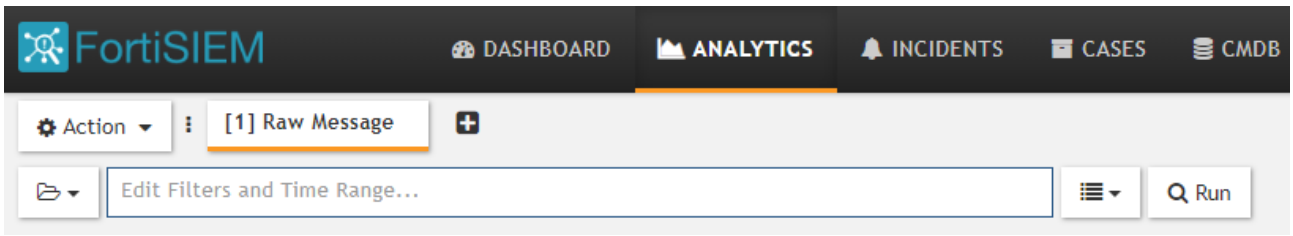

Figure 1. Selecting FortiSIEM events

The **Filters** form appears in which you can set a filter and time range for events.

3. Specify the filter for desired events.

   For example, you can specify the IP address of the device from which the events arrive in FortiSIEM (the `Reporting IP` attribute). Also, in the **Time** settings group you can specify the time range for the events (such as **Last 10 minutes**), or specify that events are to be displayed in real time. See the figure below.

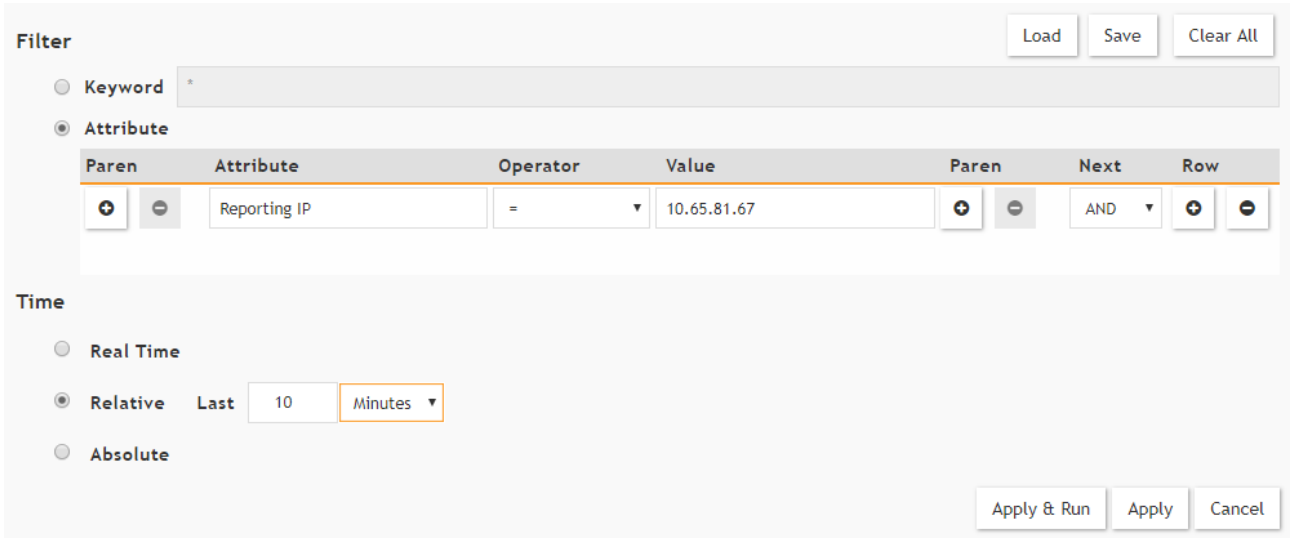

Figure 2. Setting the filter for FortiSIEM events

4. Click the **Save & Run** button.

   The **Raw Event Log** column contains events in the same format in which they are forwarded from FortiSIEM to CyberTrace.

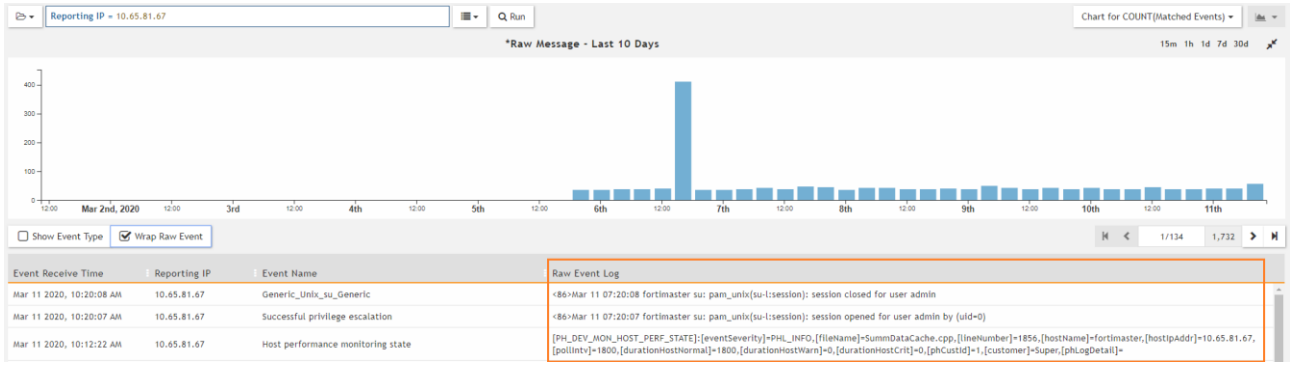

Figure 3. FortiSIEM events displayed

For more information about requesting events on the **Analytics** tab, visit http://help.fortinet.com/fsiem/5-1-1/Online-Help/HTML5_Help/Viewing_real_time_search_results.htm.

Configuring event forwarding from FortiSIEM

This section describes how to configure event forwarding from FortiSIEM to Kaspersky CyberTrace.

► *To configure event forwarding from FortiSIEM to CyberTrace:*

1. Open the FortiSIEM web console.

   The FortiSIEM account that you use must have administrator rights.

2. Select **Admin** > **Settings** > **Event Handling** > **Forwarding**.

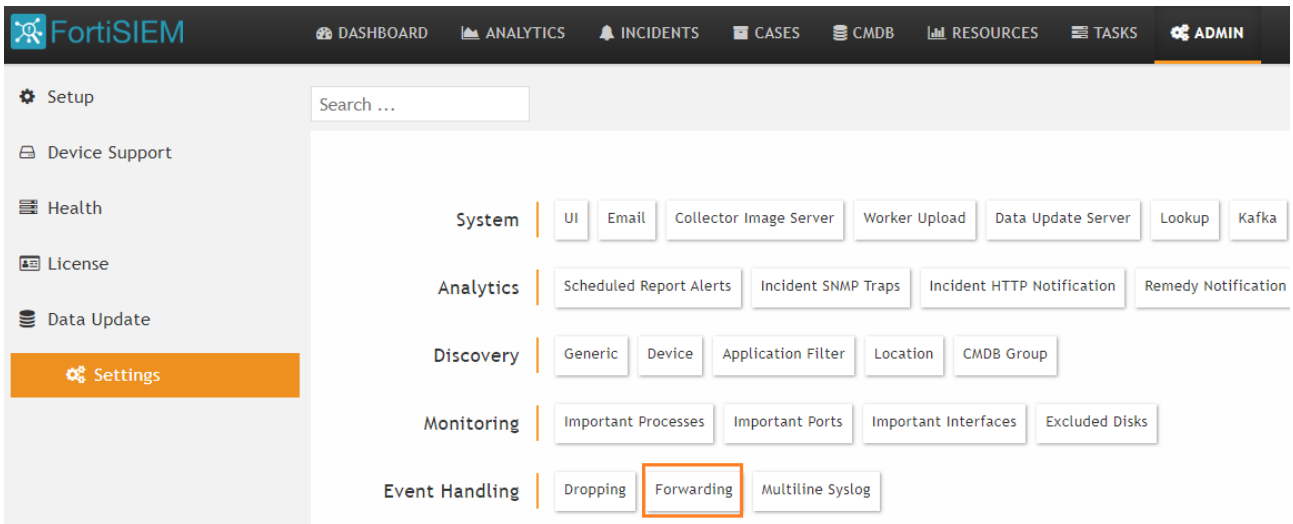

Figure 4. Creating a new forwarding rule

   The **Event Forwarding Rule** window opens.

3. Specify the event forwarding settings:

   - In the **Reporting Device** field, specify the devices from which the events must be forwarded to Kaspersky CyberTrace. You can select **All** to indicate that events from every device must be forwarded to Kaspersky CyberTrace.

     - For more choices, click the down arrow to open the **Event Dropping Rule > Select Reporting Devices** window, and make selections in the **Folders**, **Items**, and **Selections** panes.

     The **Reporting Device** field must not be empty.

   - In the **Event type** field, specify the types of events that must be forwarded to Kaspersky CyberTrace. You can select **All** to indicate that events of every type must be forwarded to Kaspersky CyberTrace.

- For more choices, click the down arrow to open the **Event Forwarding Rule > Select Event Types** window, and make selections in the **Folders**, **Items**, and **Selections** panes.

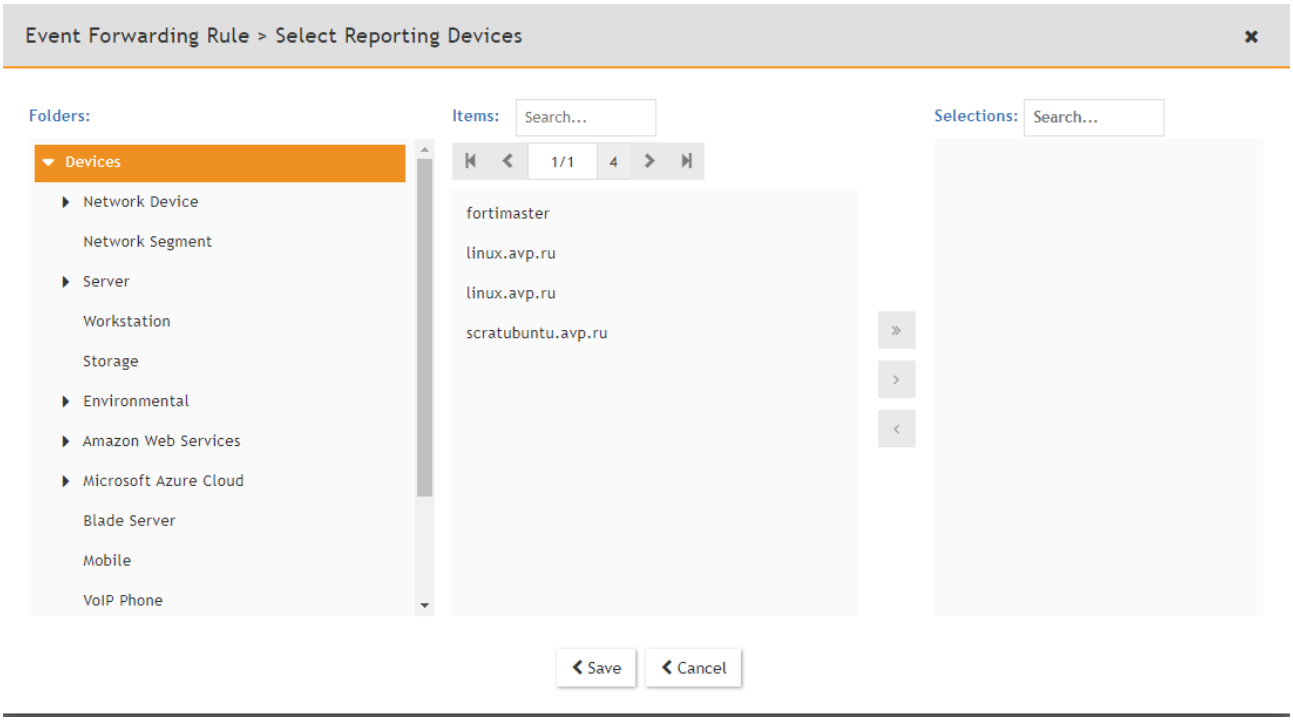

Figure 5. Selecting event types

The **Event type** field must not be empty.

- In the **Traffic Type** field, select **Syslog**.
- In the **Source IP** field, you can specify the value that must be present in all the forwarded events in the corresponding field.
- In the **Destination IP** field, you can specify the value that must be present in all the forwarded events in the corresponding field.
- In the **Severity** fields, you can specify the desired severity of events.
- In the **Regex Filter** field, you can specify the regular expression to which must forwarded events match.
- In the **Forwarding Protocol** field, select **TCP**.
- In the **Forwarding to IP** field, specify the IP address of the computer on which Kaspersky CyberTrace runs.

  This IP address is specified in the `InputSettings > ConnectionString` element of the kl_feed_service.conf configuration file (see section "Configuring Kaspersky CyberTrace for integration with FortiSIEM" on page 5).
- In the **Forwarding to Port** field, specify the port of the computer on which Kaspersky CyberTrace runs.

  This port is specified in the `InputSettings > ConnectionString` element of the kl_feed_service.conf configuration file.

- In the **Format** field, select **CEF**.

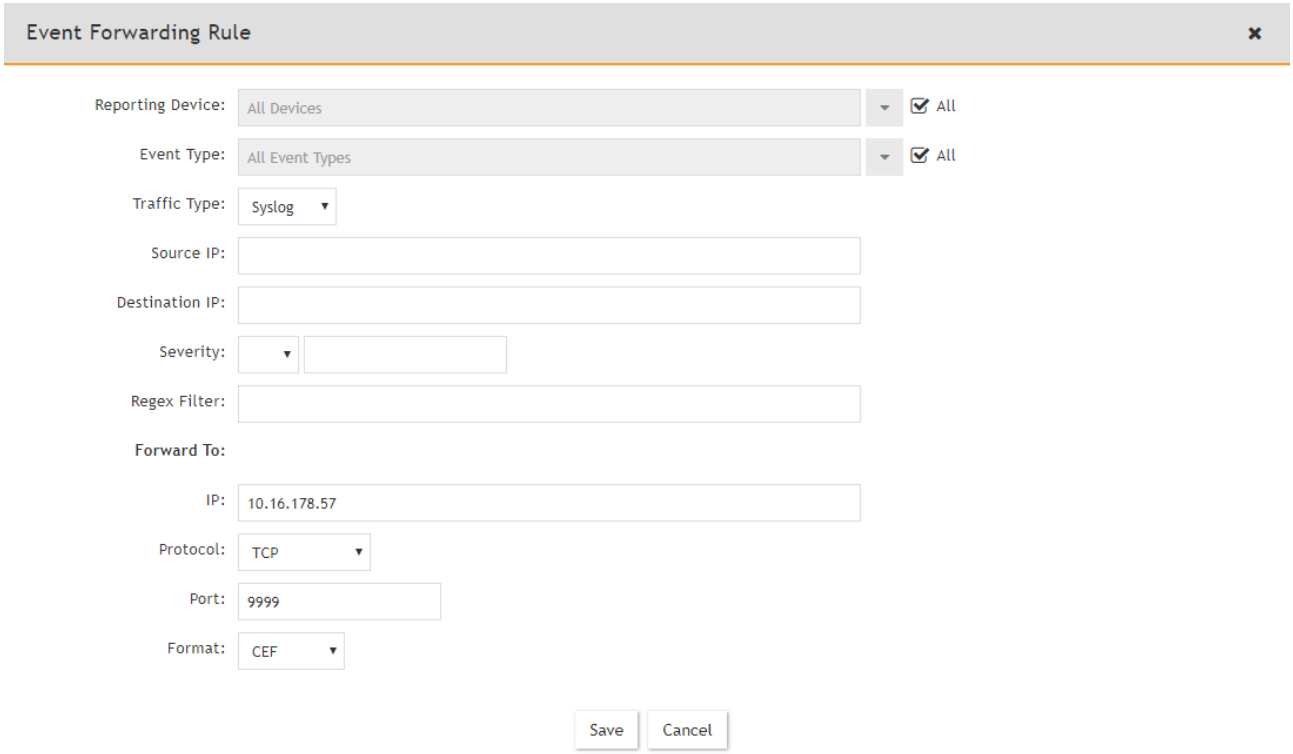

Figure 6. Event Forwarding Rule window

4. Click **Save**.

   The **Event Forwarding Rule** window closes and the **Forwarding** window displays the new event forwarding rule.

5. In the Forwarding window, select **Enable** for the new event forwarding rule.

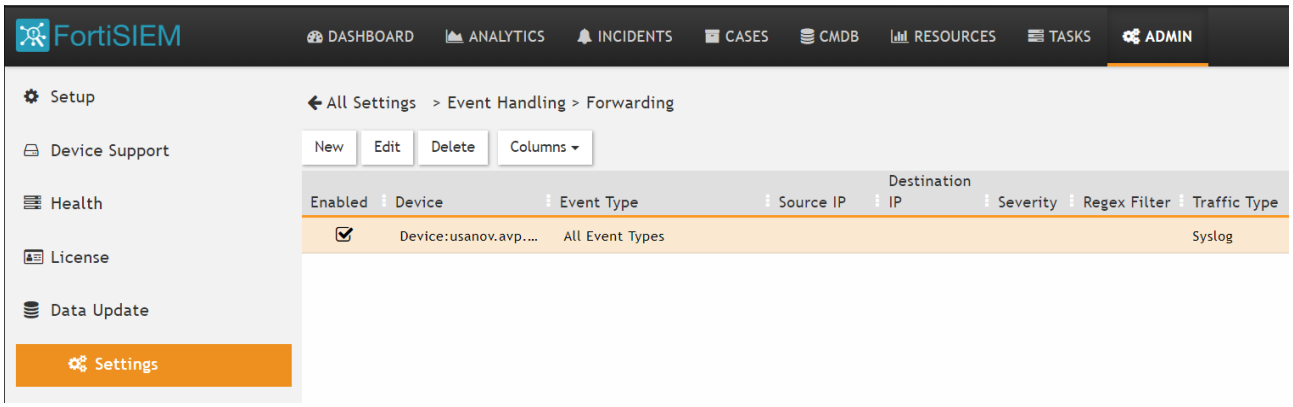

Figure 7. Event Forwarding Rule window

Receiving events from Kaspersky CyberTrace in FortiSIEM

Kaspersky CyberTrace sends events to FortiSIEM in CEF format. FortiSIEM can automatically parse events in this format.

kaspersky

Displaying actionable fields

This section describes how to display an actionable field in events that FortiSIEM receives from Kaspersky CyberTrace.

You can insert some fields into outgoing events separately from the context of feed records. You can name these fields in the outgoing events as you like. These fields are referred to as *actionable*; they are listed in the `ActionableFields` element of a feed description in the kl_feed_service.conf configuration file.

The `threat_score` field is used as an example. To display this actionable field, add it by using Kaspersky CyberTrace Web.

When FortiSIEM receives an event with this field, the field will be displayed automatically.

Adding an actionable field by using the web interface

► *To make the `threat_score` field actionable in Kaspersky CyberTrace:*

1. Open Kaspersky CyberTrace Web in your browser.
2. Select the **Settings > Feeds** tab.
3. In the **Filtering rules for feeds** section, make sure that the **Kaspersky feeds** tab is selected.
4. Expand the IP Reputation Data Feed in the list.
5. Locate the **Actionable fields** section and click the **Add new field** button to add a new actionable field.
6. In the **Field name** text box, specify the name of a field in the original feed, `threat_score`.
7. In the **Output** text box specify a name of an unused CEF field. This field will hold the value of the actionable field in the outgoing events. For example, you can use the `cs3` value.
8. Scroll down the the **Feeds** tabbed page and click the **Save** button.

Looking up events received from Kaspersky CyberTrace in FortiSIEM

This section describes how to browse, in FortiSIEM, only those events that are received from Kaspersky CyberTrace.

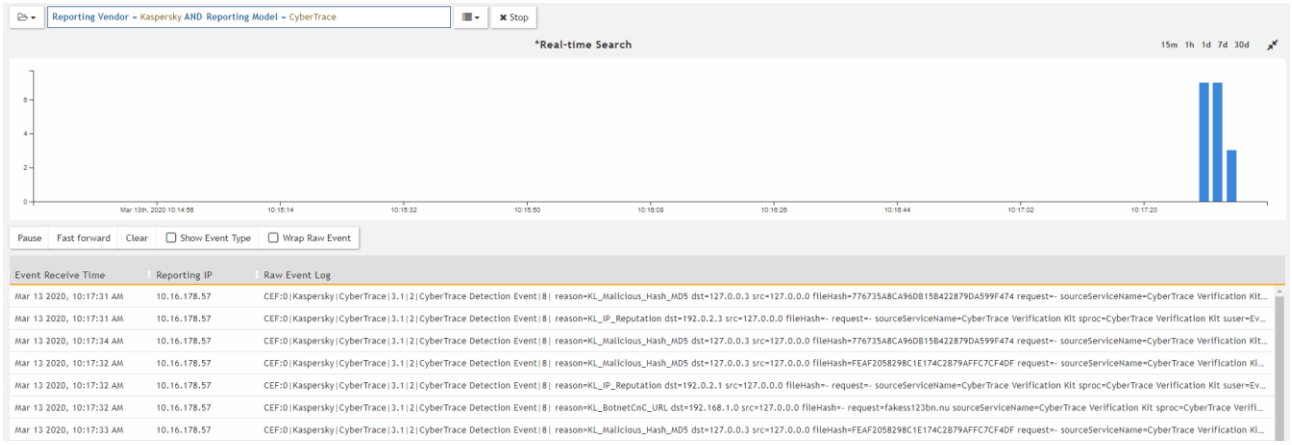

Figure 8. Browsing events received from Kaspersky CyberTrace

► *To browse, in FortiSIEM, events received from Kaspersky CyberTrace:*

1. On the FortiSIEM web console, select the **Analytics** tab.
2. Click inside the **Edit Filter and Time Range** field.

   The **Filters** form appears which allows you to set a filter and time range for events.
3. Specify the following filter:
   - **Attribute**: `Reporting Vendor`
   - **Operator**: `=`
   - **Value**: `Kaspersky`
4. Click the plus sign (**+**) in the **Row** column.
5. In the new row specify another filter
   - **Attribute**: `Reporting Model`
   - **Operator**: `=`
   - **Value**: `CyberTrace`
6. In the **Time** settings group, specify the period during which the desired events arrived to FortiSIEM.
7. Click **Save & Run**.

   The **Analysis** tab now contains only those events from Kaspersky CyberTrace that arrived during the selected period.

kaspersky

AO Kaspersky Lab

Kaspersky is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

Products. Kaspersky products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include their signatures in databases used by Kaspersky applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky. It is no coincidence that many other developers use the Kaspersky Anti-Virus engine in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky website:	https://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Community:	https://community.kaspersky.com

kaspersky

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

FortiSIEM is either a registered trademark or trademark of Fortinet Corporation in the United States and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.