KASPERSKY

How to integrate Kaspersky Threat Data Feeds with FortiSIEM

Document version: 1.0

Dear User,

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

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof incur civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document, and graphic images related to it, may be used for informational, non-commercial, and personal purposes only.

Kaspersky Lab reserves the right to amend this document without additional notification.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document to which rights are held by third parties, or for any potential harms associated with use of the document.

Document revision date: 06.05.2019

© 2019 AO Kaspersky Lab. All Rights Reserved.

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

Contents

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).

How to integrate Kaspersky CyberTrace with FortiSIEM

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

► *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 20).

In this chapter

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, add the following elements to the `Configuration > InputSetting > RegExps > Source id="default"` element:

```
<Device type="CONTEXT">[^\|]*\|([^\|]*\|[^\|]*)\|</Device>
<DeviceIp type="CONTEXT"
concatenate="#1">dvc\=(\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})(?:$|\s|\,)</Devi
ceIp>
<UserName type="CONTEXT">user\=(.*?)(?:$|\s|\,)</UserName>
<DeviceAction type="CONTEXT">act=(.*?)(?:$|\s|\,)</DeviceAction>
```

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

```
<![CDATA[Kaspersky Lab|Kaspersky
CyberTrace|1.0|1|4|alert=%Alert%;msg=%RecordContext%]]>
```

> If you are using Kaspersky CyberTrace Web for specifying this value, omit `<![CDATA[` in the beginning and `]]>` in the end of the value.

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

```
<![CDATA[Kaspersky Lab|Kaspersky
CyberTrace|1.0|2|8|reason=%Category%;detected=%MatchedIndicator%;act=%De
viceAction%;dst=%RE_IP%;src=%SRC_IP%;md5=%RE_MD5%;sha1=%RE_SHA1%;sha2=%R
E_SHA256%;request=%RE_URL%;dvc=%DeviceIp%;sourceServiceName=%Device%;sus
er=%UserName%;msg=%RecordContext%]]>
```

> If you are using Kaspersky CyberTrace Web for specifying this value, omit `<![CDATA[` in the beginning and `]]>` in the end of the value.

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. In the `Configuration > NormalizingRules` element, specify the following rule:

```
<Replace input="&lt;" output="&#10;&lt;" />
```

You can also create this rule by using Kaspersky CyberTrace Web as follows:

Figure 1. Normalizing rule for FortiSIEM events

9. 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.

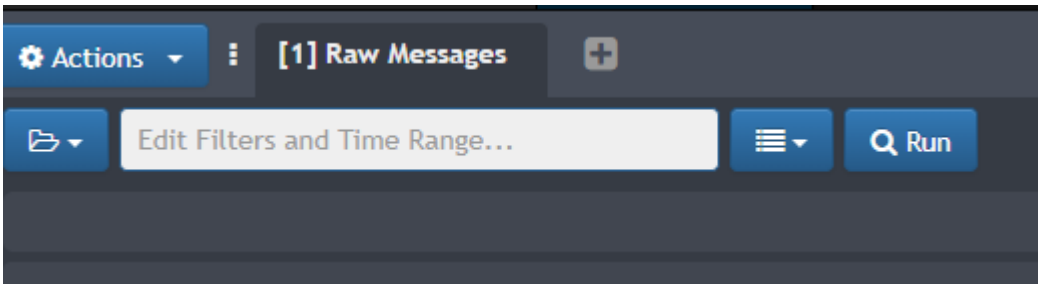


Figure 2. Selecting FortiSIEM events

The **Filters** form appears which allows you to 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 (for example, last 10 minutes), or specify that events are to be displayed in real time.

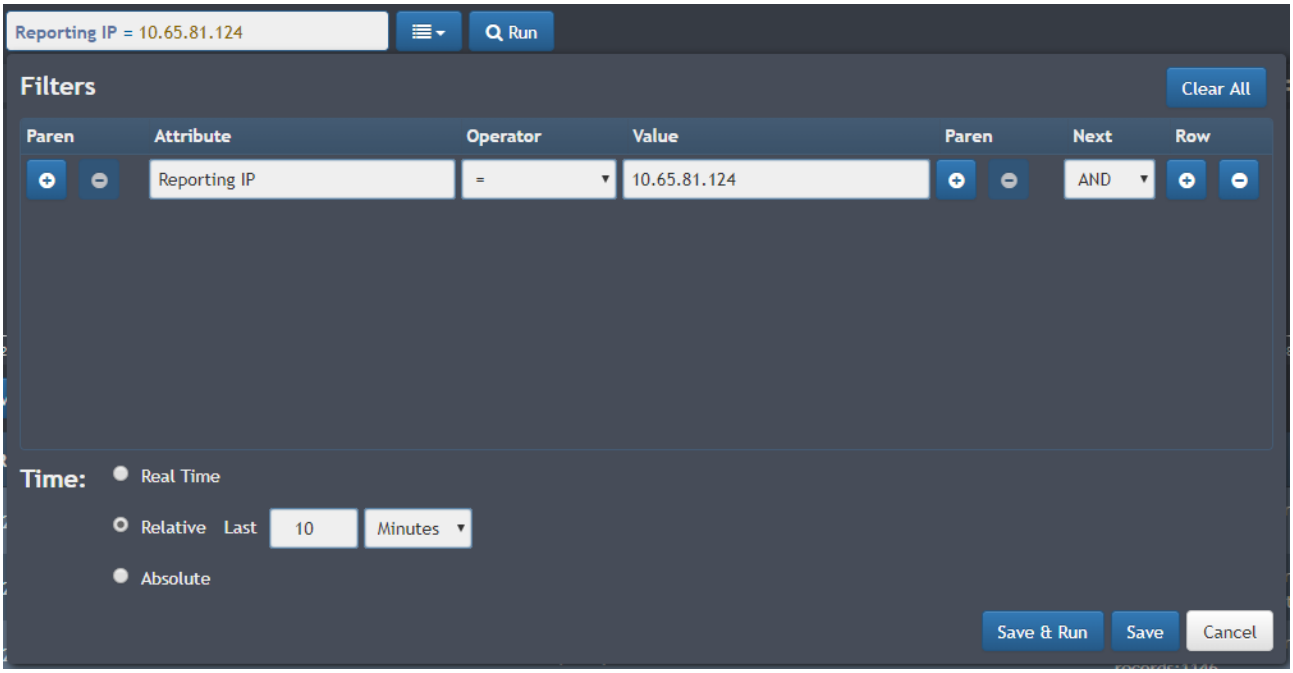


Figure 3. Setting the filter for FortiSIEM events

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.

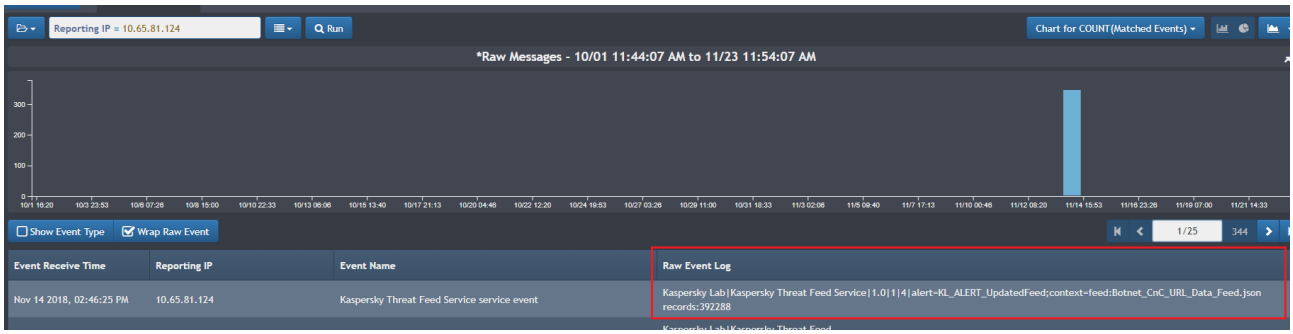


Figure 4. FortiSIEM events displayed

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 you use must have administrator rights.

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

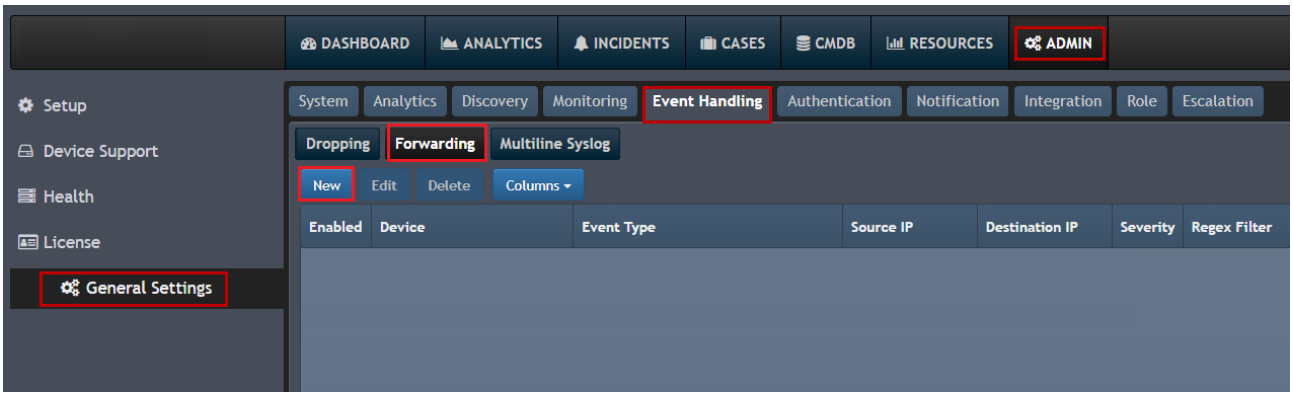


Figure 5. Creating a new forwarding rule

   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.

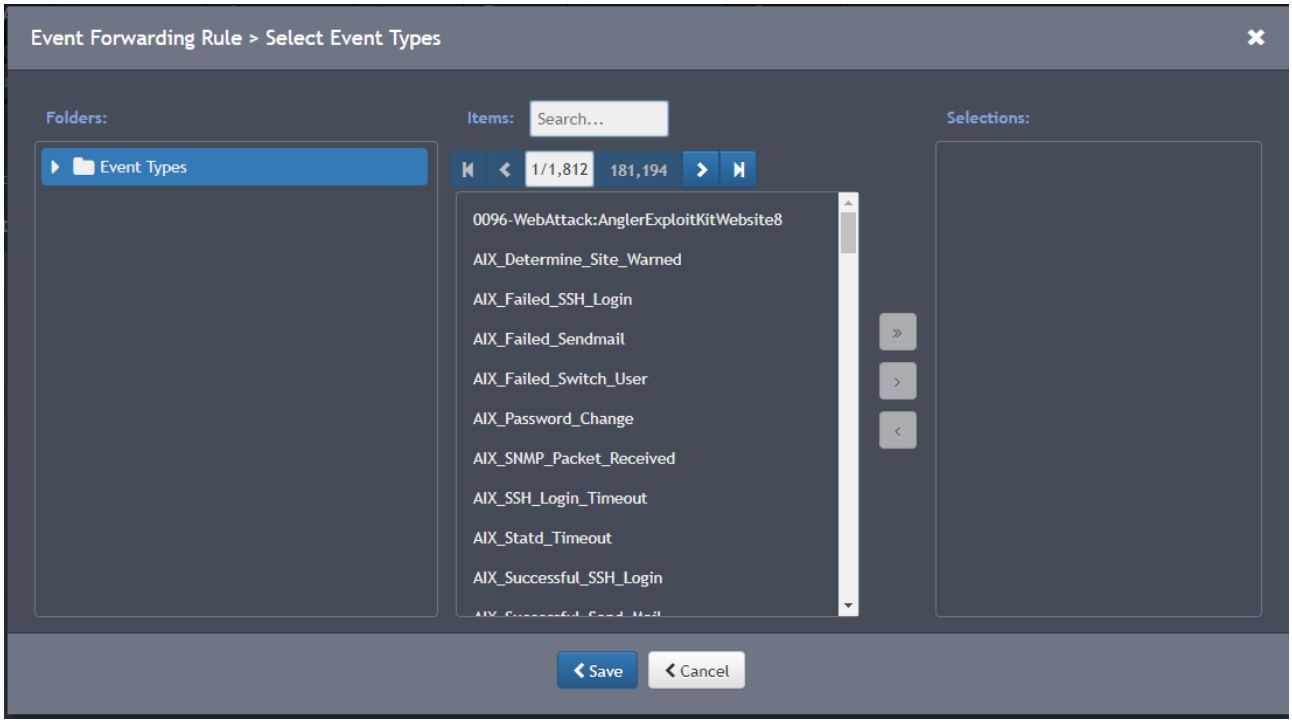


Figure 6. Selecting event types

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.

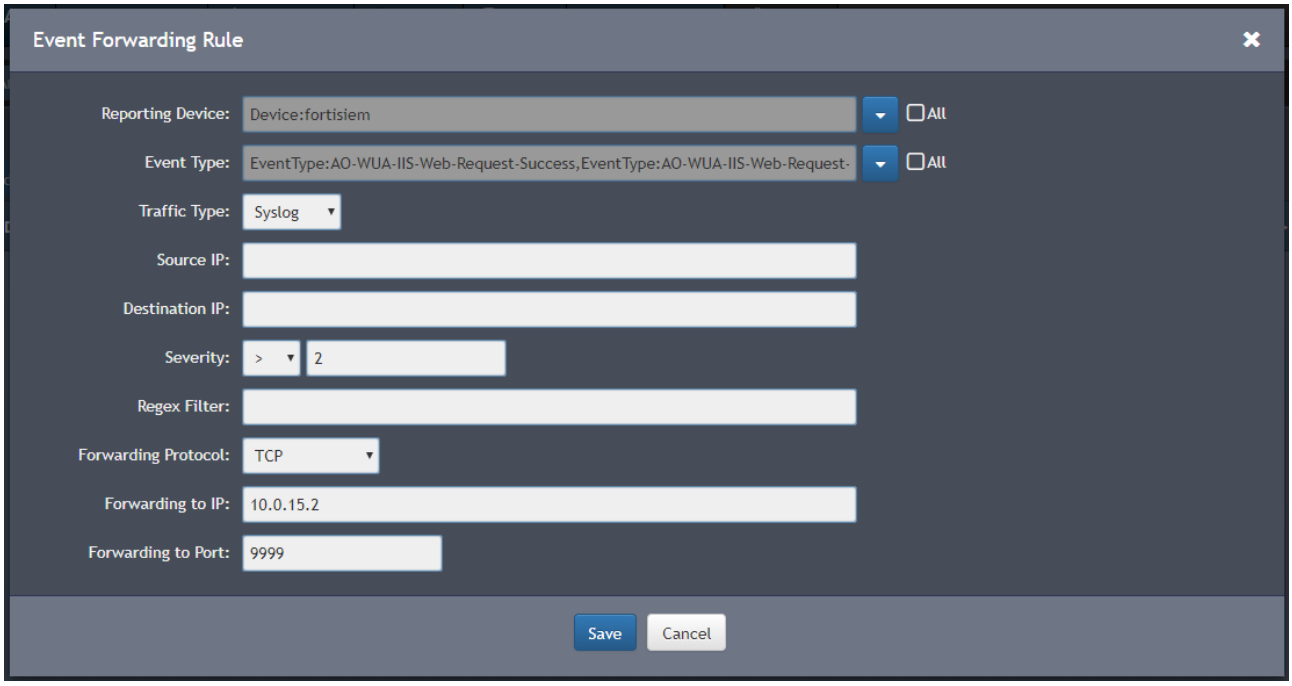


Figure 7. Event Forwarding Rule window

4. Click **Save**.

Receiving events from Kaspersky CyberTrace in FortiSIEM

This section describes how to configure Kaspersky CyberTrace and FortiSIEM so that FortiSIEM will receive events from Kaspersky CyberTrace.

► *To receive events from Kaspersky CyberTrace in FortiSIEM:*

1. Add Kaspersky CyberTrace to FortiSIEM as an event source (see section "Adding Kaspersky CyberTrace as an event source" on page 12).
2. In FortiSIEM, add the `Device IP Address` field and the `Detected indicator` field (see section "Adding fields in FortiSIEM" on page 13).
3. In FortiSIEM, add rules for parsing events from Kaspersky CyberTrace (see section "Adding rules for parsing events from Kaspersky CyberTrace" on page 14).
4. Optionally, in FortiSIEM add descriptions of events from Kaspersky CyberTrace (see section "Adding descriptions of events" on page 17).

In this section

Adding Kaspersky CyberTrace as an event source

This section describes how to add Kaspersky CyberTrace as an event source in FortiSIEM.

► *To add Kaspersky CyberTrace as an event source:*

1. Open the FortiSIEM web console.
2. Select **Admin** > **Device Support** > **Device/App**.
3. Click **New**.

   The **Device/Application Type Definition** window opens.
4. Specify the following information:
   - In the **Category** field, select **Application**.
   - In the **Vendor** field, specify **Kaspersky**.
   - In the **Model** field, specify **CyberTrace**.
   - In the **Version** field, specify **ANY**.
   - In the **Device/App Group** field, select **Applications > Infrastructure App** item.
   - Do not change the **Biz Service Group** field.

- Clear any selected items from the drop-down list of the **Access Protocol** field.

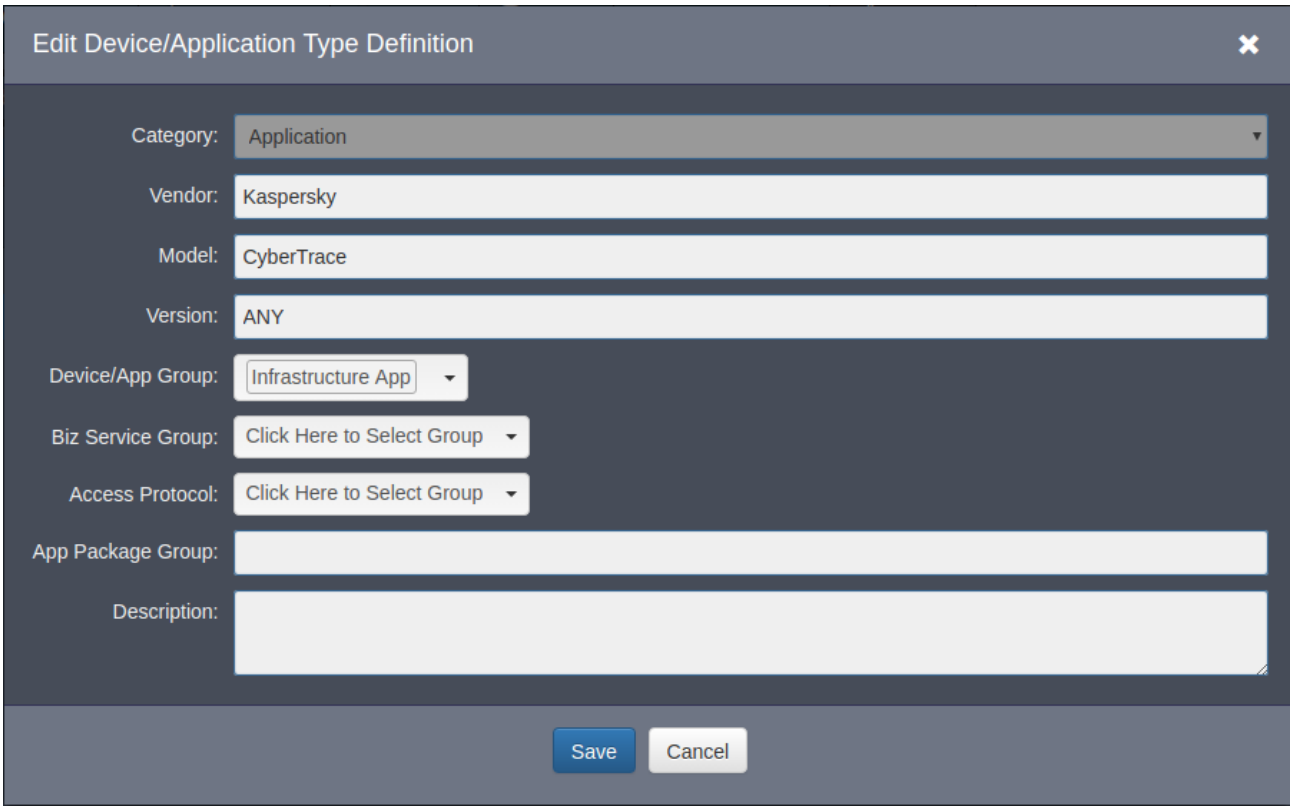


Figure 8. Editing a device/app type definition

5. Click **Save**.

   A new item appears in the list of supported devices and applications.

6. Click **Apply**.

For more information about supporting devices and applications, visit http://help.fortinet.com/fsiem/5-1-1/Online-Help/HTML5_Help/Working_with_Devices_and_Applications.htm.

Adding fields in FortiSIEM

By default, a detection event sent by Kaspersky CyberTrace contains the IP address of the device that sent the original event and a field for the detected indicator. However, FortiSIEM does not contain fields for storing this IP address and indicator. This section describes how to add a field for storing values that you need in FortiSIEM.

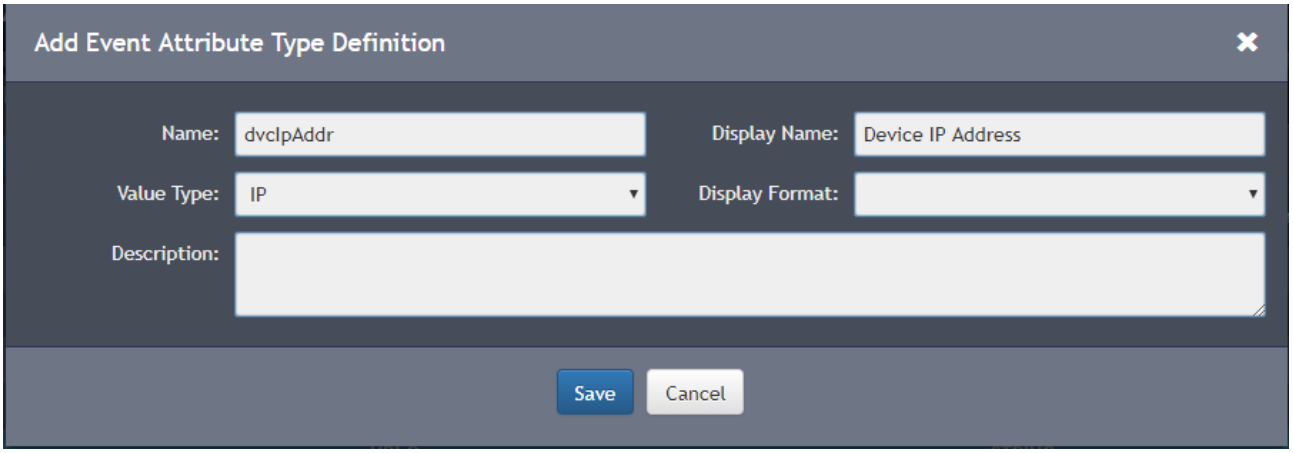
► *To add a field for storing an IP address and detected indicator in FortiSIEM:*

1. On the FortiSIEM web console, select **Admin** > **Device Support** > **Event Attribute**.
2. Click **New**.

   The **Add Event Attribute Type Definition** window opens.

3. Specify the following information:
   - In the **Name** field, specify **dvcIpAddr**.

- In the **Display Name** field, specify **Device IP Address**.
- In the **Value Type** field, select **IP**.
- Fill in the rest of the fields as you wish.



4. Click **Save**.
5. Click **New**.
6. In the **Add Event Attribute Type Definition** window that opens, specify the following information:
   - In the **Name** field, specify **detectedIndicator**.
   - In the **Display Name** field, specify **Detected indicator**.
   - In the **Value Type** field, select **String**.
   - Fill in the rest of the fields as you wish.
7. Click **Save**.
8. Click **Apply**.

For more information about adding a new field in FortiSIEM, visit http://help.fortinet.com/fsiem/5-1-1/Online-Help/HTML5_Help/Working_with_Event_Attributes.htm.

Adding rules for parsing events from Kaspersky CyberTrace

This section describes how to add rules in FortiSIEM for parsing events that arrive from Kaspersky CyberTrace.

► *To add rules in FortiSIEM for parsing events:*

1. On the FortiSIEM web console, select **Admin** > **Device Support** > **Parser**.
2. Select the parser after which you want to add a new one and click **New**.

   The **Event Parser Definition** window opens.
3. Specify the following values:
   - In the **Name** field, specify **CyberTrace_Event**.
   - In the **Device Type** field, select **Kaspersky CyberTrace**.
   - In the **Test Event** field, specify the following value:

```
Kaspersky Lab|Kaspersky
CyberTrace|1.0|2|8|reason=KL_DETECTION_TEST_EVENT;detected=%MatchedIndic
ator%;act=test_msg;dst=8.8.8.8;src=10.0.15.56;md5=AAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA;sha1=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;sha2=AAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;request=http://tes
t.test;dvc=127.0.0.5;sourceServiceName=TEST_DEVICE;suser=test_user;msg=t
here_is_some_context:true and_more:true
Kaspersky Lab|Kaspersky
CyberTrace|1.0|1|4|alert=KL_TEST_ALERT;msg=there_is_some_context:true
and_more:true
```

- In the **Parser XML** field, specify the following value:

```
<eventFormatRecognizer>
  <![CDATA[Kaspersky\sLab\|Kaspersky\sCyberTrace]]>
</eventFormatRecognizer>
 <patternDefinitions>
 <pattern name="patVbar" ><![CDATA[[^|]*]]></pattern>
 <pattern name="patStrQuote" ><![CDATA[[^" \\]+]]></pattern>
 </patternDefinitions>
 <parsingInstructions>
 <collectFieldsByRegex src="$_rawmsg" >
 <regex>
<![CDATA[<:patVbar>\|<:patVbar>\|<_ver:patVbar>\|<_event:patVbar>\|<even
tSeverity:patVbar>\|<_body:gPatMesgBody>]]>
 </regex>
 </collectFieldsByRegex>
 <choose>
 <when test='$_event = "2"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace detection
event</setEventAttribute>
 </when>
 <when test='$_event = "1"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace service
event</setEventAttribute>
 </when>
 </choose>
 <collectFieldsByKeyValuePair kvsep="=" sep=";" src="$_body" >
 <attrKeyMap attr="alertName" key="alert" />
 <attrKeyMap attr="threatCategory" key="reason" />
 <attrKeyMap attr="detectedIndicator" key="detected" />
 <attrKeyMap attr="srcAction" key="act" />
 <attrKeyMap attr="destIpAddr" key="dst" />
 <attrKeyMap attr="srcIpAddr" key="src" />
 <attrKeyMap attr="hashMD5" key="md5" />
 <attrKeyMap attr="hashSHA1" key="sha1" />
 <attrKeyMap attr="hashSHA2" key="sha2" />
 <attrKeyMap attr="uriQuery" key="request" />
 <attrKeyMap attr="dvcIpAddr" key="dvc" />
 <attrKeyMap attr="serviceName" key="sourceServiceName" />
```

```
<attrKeyMap attr="user" key="suser" />
<attrKeyMap attr="msg" key="msg" />
</collectFieldsByKeyValuePair>
</parsingInstructions>
```

If you add new regular expressions and change the format of detection events in the kl_feed_service.conf configuration file, specify the new format of detection events in the **Test Event** field. Also, in the **Parser XML** field, in the `collectFieldsByKeyValuePair` element, add the correspondence rules between fields that are in the events from Kaspersky CyberTrace and FortiSIEM fields in which the values of the former fields must be stored. The correspondence rules must have the following format: `<attrKeyMap attr="%FortiSIEM_field%" key="%Kaspersky_CyberTrace_field%" />`.

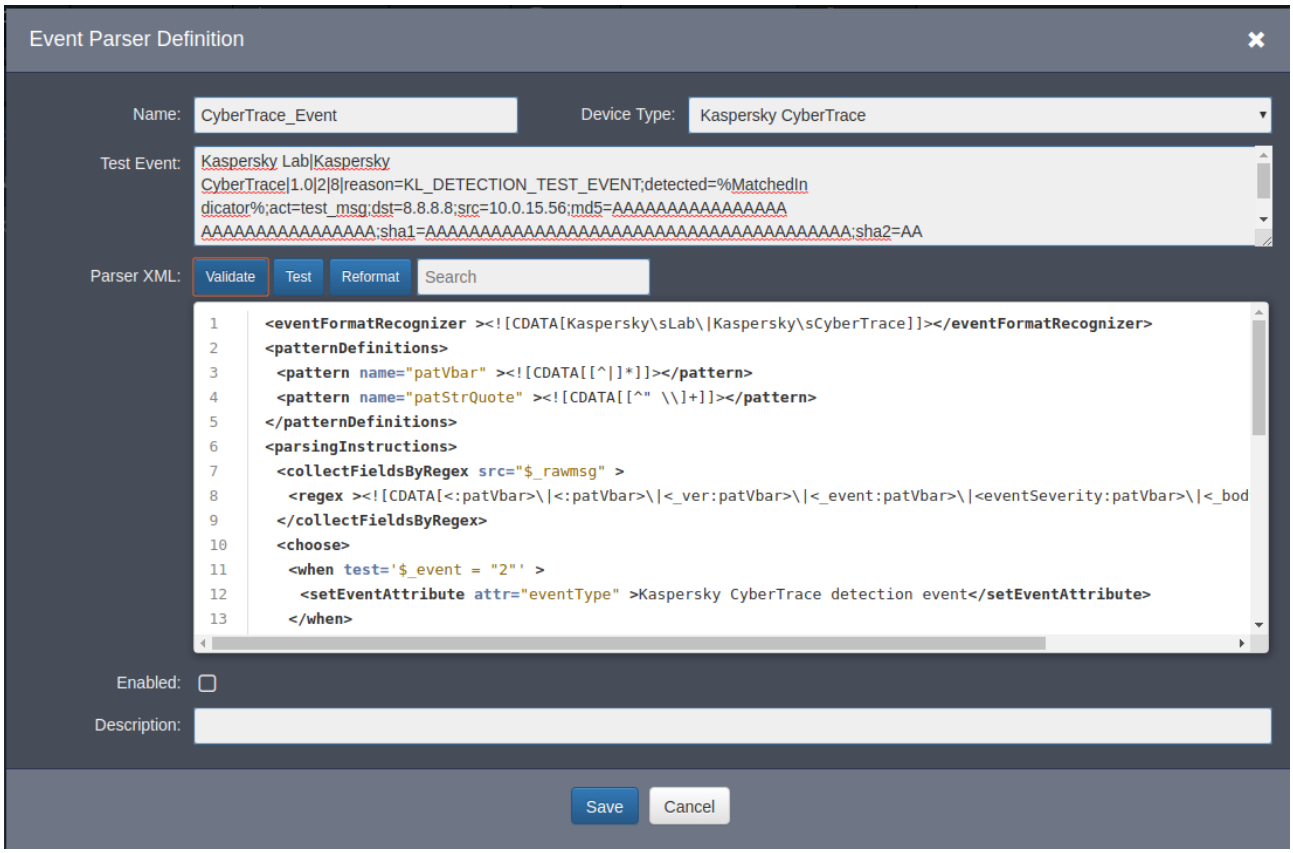


Figure 9. Editing a parser definition

4. Click the **Reformat** button.
5. Click the **Validate** button to validate the XML data in the **Parser XML** field.

   A message tells you whether the validation passed or failed.
6. Click the **Test** button.

   A window for testing the entered data opens.
7. In the **Test Event Parser** window, click the **Test** button.

   If error messages appear in the **Errors** column:

a. Contact your technical account manager (TAM) to reconcile the contents of the **Test Event** field and the contents of the **Parser XML** field.

b. Click **Back** and specify the correct data in the **Test Event** field and in the **Parser XML** field.

c. Test the data again.

8. Click **Back**.
9. In the **Event Parser Definition** window, select the **Enabled** check box.
10. Click **Save**.
11. In the **Admin** > **Device Support** > **Parser** section, click **Apply**, and in the message box that opens click **Yes** to agree to the changes.

For more information about event parsers, visit http://help.fortinet.com/fsiem/5-1-1/Online-Help/HTML5_Help/Configuring_parsers.htm.

Adding descriptions of events

This section explains how to add descriptions to detection events and service events that are sent by Kaspersky CyberTrace.

► *To add descriptions to events from Kaspersky CyberTrace:*

1. On the FortiSIEM web console, select **Admin** > **Device Support** > **Event** > **New**.

   The **Event Definition** window opens.
2. Specify the following data:
   - In the **Name** field, specify **PH_DEV_MON_CUST_CYBERTRACE_DETECTION_EVENT**.
   - In the **Device Type** field, select **Kaspersky CyberTrace**.
   - In the **Event Type Group** field, select **Security**.
   - In the **Severity** field, select **8-MEDIUM**.
   - In the **Description** field, specify **Detection events from Kaspersky CyberTrace**.
3. Click **Save**.
4. Select **Admin > Device Support > Event > New**.
5. In the **Event Definition** window that opens, specify the following data:
   - In the **Name** field, specify **PH_DEV_MON_CUST_CYBERTRACE_SERVICE_EVENT**.
   - In the **Device Type** field, select **Kaspersky CyberTrace**.
   - In the **Event Type Group** field, select **Info**.
   - In the **Severity** field, select **4-LOW**.
   - In the **Description** field, specify **Service events from Kaspersky CyberTrace**.
6. Click **Save**.
7. In the **Admin** > **Device Support** > **Event** section, click **Apply**, and in the message box that opens click **Yes** to agree to the changes.

Displaying actionable fields

This section describes how to display an actionable field in events that FortiSIEM receives from Kaspersky CyberTrace. The `threat_score` field is used as an example.

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.

First, you edit the kl_feed_service.conf configuration file to make the `threat_score` field actionable in Kaspersky CyberTrace. Second, you edit the parsing rules in FortiSIEM to display events from Kaspersky CyberTrace correctly.

Editing the kl_feed_service.conf configuration file

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

1. 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.
2. In the `Configuration > OutputSettings > EventFormat` element, specify the following value:

```
<![CDATA[Kaspersky Lab|Kaspersky
CyberTrace|1.0|2|8|reason=%Category%;detected=%MatchedIndicator%;act=%De
viceAction%;dst=%RE_IP%;src=%SRC_IP%;md5=%RE_MD5%;sha1=%RE_SHA1%;sha2=%R
E_SHA256%;request=%RE_URL%;dvc=%DeviceIp%;sourceServiceName=%Device%;sus
er=%UserName%;%ActionableFields%msg=%RecordContext%]]>
```

3. In the `Configuration > OutputSettings > ActionableFieldContextFormat` element, specify the following value:

```
%ParamName%=%ParamValue%;
```

4. To element `<Feed filename="IP_Reputation_Data_Feed.json" enabled="true" type="default">`, add the following data:

```
<ActionableFields>
    <ActionableField name="threat_score" output_name="kl_threat_score"/>
</ActionableFields>
```

5. Save the kl_feed_service.conf file.
6. Restart Feed Service (a component 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)

You can reconfigure and restart Feed Service by using Kaspersky CyberTrace Web.

Editing parsing rules for events from Kaspersky CyberTrace

► *To edit in FortiSIEM the rules for parsing events from Kaspersky CyberTrace:*

1. On the FortiSIEM web console, select **Admin** > **Device Support** > **Parser**.
2. Open the **CyberTrace_Event** item in the list of parsers.

   The **Event Parser Definition** window opens containing the data of the `CyberTrace_Event` parser.
3. Change the data as follows:
   - In the **Test Event** field, specify the following value:

```
Kaspersky Lab|Kaspersky
CyberTrace|1.0|2|8|reason=KL_DETECTION_TEST_EVENT;detected=%MatchedIndic
ator%;act=test_msg;dst=8.8.8.8;src=10.0.15.56;md5=AAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA;sha1=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;sha2=AAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;request=http://tes
t.test;dvc=127.0.0.5;sourceServiceName=TEST_DEVICE;suser=test_user;kl_th
reat_score=100;msg=there_is_some_context:true and_more:true
Kaspersky Lab|Kaspersky
CyberTrace|1.0|1|4|alert=KL_TEST_ALERT;msg=there_is_some_context:true
and_more:true
```

   - In the **Parser XML** field, specify the following value:

```
<eventFormatRecognizer>
  <![CDATA[Kaspersky\sLab\|Kaspersky\sCyberTrace]]>
</eventFormatRecognizer>
 <patternDefinitions>
 <pattern name="patVbar" ><![CDATA[[^|]*]]></pattern>
 <pattern name="patStrQuote" ><![CDATA[[^" \\]+]]></pattern>
 </patternDefinitions>
 <parsingInstructions>
 <collectFieldsByRegex src="$_rawmsg" >
 <regex>
<![CDATA[<:patVbar>\|<:patVbar>\|<_ver:patVbar>\|<_event:patVbar>\|<even
tSeverity:patVbar>\|<_body:gPatMesgBody>]]>
 </regex>
 </collectFieldsByRegex>
 <choose>
 <when test='$_event = "2"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace detection
event</setEventAttribute>
 </when>
 <when test='$_event = "1"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace service
event</setEventAttribute>
 </when>
 </choose>
 <collectFieldsByKeyValuePair kvsep="=" sep=";" src="$_body" >
 <attrKeyMap attr="alertName" key="alert" />
 <attrKeyMap attr="threatCategory" key="reason" />
```

```
<attrKeyMap attr="detectedIndicator" key="detected" />
<attrKeyMap attr="srcAction" key="act" />
<attrKeyMap attr="destIpAddr" key="dst" />
<attrKeyMap attr="srcIpAddr" key="src" />
<attrKeyMap attr="hashMD5" key="md5" />
<attrKeyMap attr="hashSHA1" key="sha1" />
<attrKeyMap attr="hashSHA2" key="sha2" />
<attrKeyMap attr="uriQuery" key="request" />
<attrKeyMap attr="dvcIpAddr" key="dvc" />
<attrKeyMap attr="serviceName" key="sourceServiceName" />
<attrKeyMap attr="user" key="suser" />
<attrKeyMap attr="msg" key="msg" />
<attrKeyMap attr="threatScore" key="kl_threat_score" />
</collectFieldsByKeyValuePair>
</parsingInstructions>
```

4. Click **Reformat**.
5. Click **Validate** to validate the XML data in the **Parser XML** field.
6. Click **Test**.

   A window for testing the entered data opens.
7. In the **Test Event Parser** window, click **Test**.

   If the test result window contains error messages:

   a. Contact your technical account manager (TAM) to reconcile the contents of the **Test Event** field and the contents of the **Parser XML** field.

   b. Click **Back** and specify the correct data in the **Test Event** field and in the **Parser XML** field.

   c. Test the data again.
8. Click **Back**.
9. In the **Event Parser Definition** window, select the **Enabled** check box.
10. Click **Save**.
11. In the **Admin** > **Device Support** > **Parser** section, click **Apply**, and in the message box that opens click **Yes** to agree to the changes.

    Now events from Kaspersky CyberTrace are displayed correctly in FortiSIEM.

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.

► *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.

AO Kaspersky Lab

Kaspersky Lab 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 Lab 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 Lab is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky Lab 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 Lab 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 Lab products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky Lab 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 Lab applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. 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 Lab 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 Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky Lab'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 Lab website:	https://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab's web community:	https://community.kaspersky.com

Trademark notices

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

FortiSIEM is a either 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.