kaspersky

CyberTrace, Cribl, Splunk integration

Data Feeds Integration Guidelines

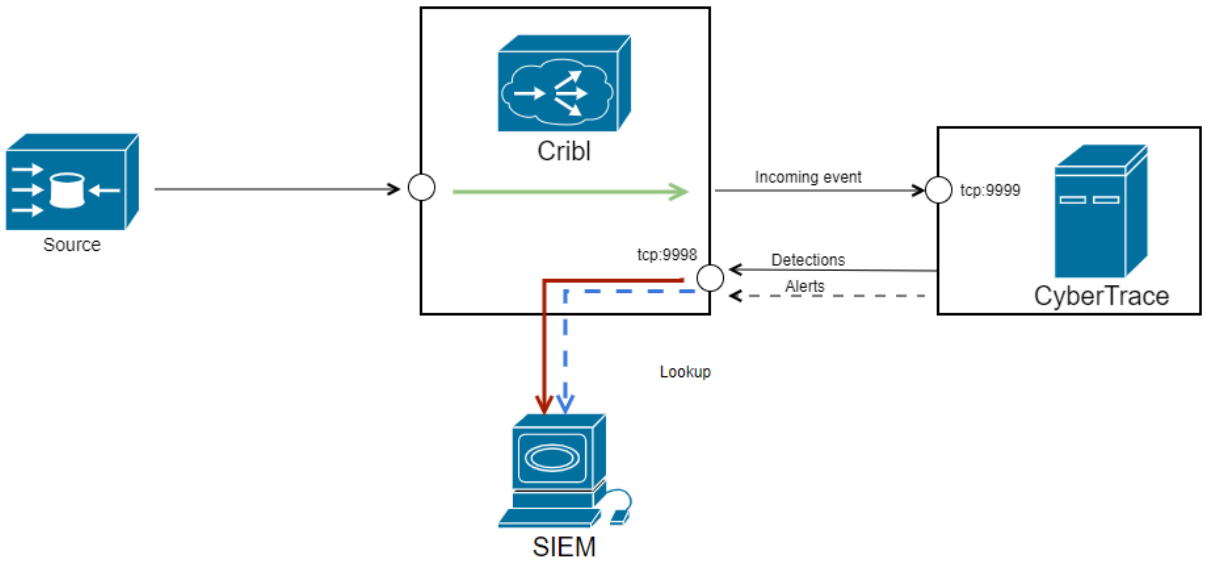
11.04.2022

kaspersky

Kaspersky CyberTrace, Cribl, Splunk

Integration guidelines

The guidelines describe steps necessary to implement the scheme outlined in the picture below. The scheme assumes only one instance of CyberTrace, the document does not touch the performance topic, nor the distributed integration schemes. The guide includes the following stages.



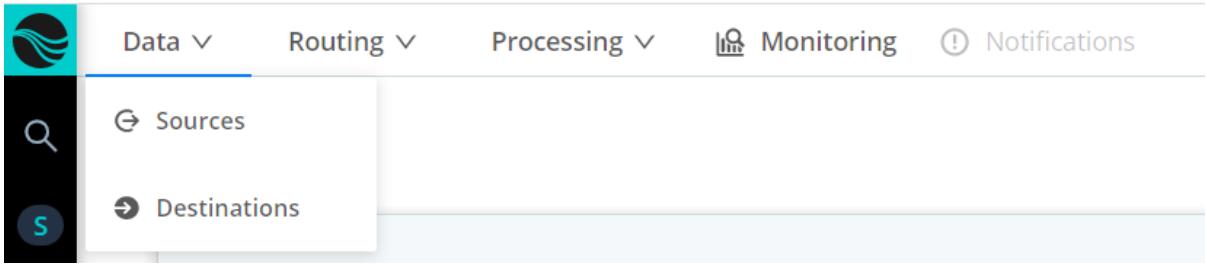
1. The logs are being forwarded to CyberTrace via Cribl, y CyberTrace sends the detections via Cribl as well

kaspersky

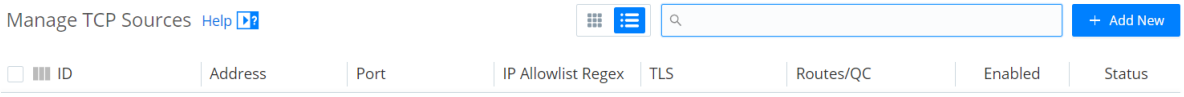
1. Adding the log_scanner Source in Cribl

Add a new data source to accept events from the CyberTrace *log_scanner* utility.

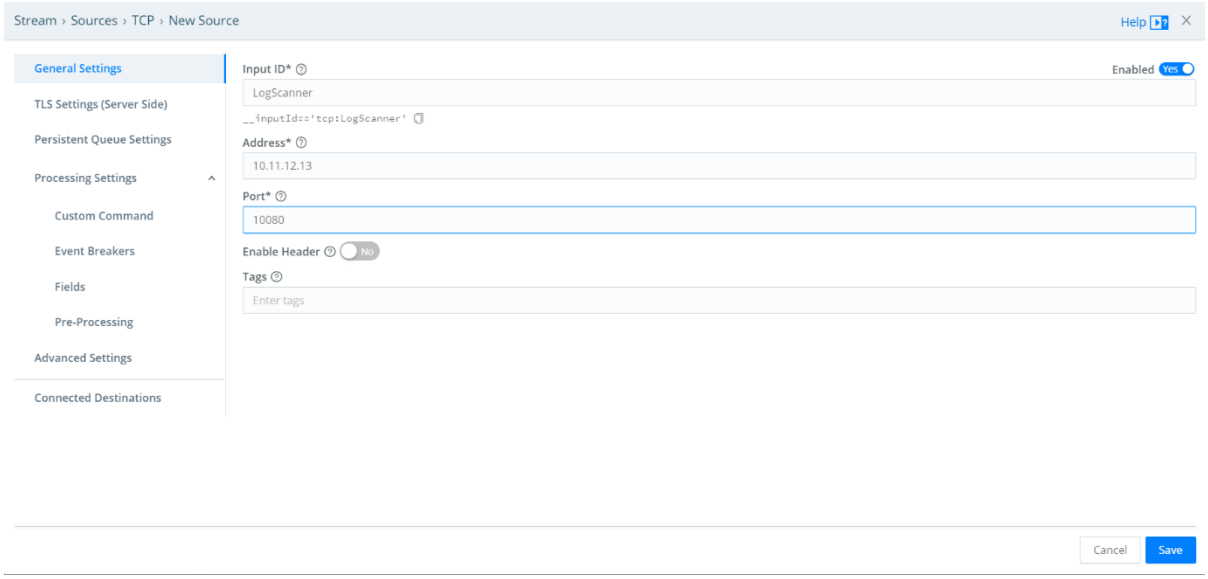
1. In the Cribl UI go to menu **Data** and choose **Sources**



2. In the types list choose **TCP** and press "**+ Add new**"



3. In the **Input ID** field specify "LogScanner"
4. In the **Address** field specify the IP address of the interface which is going to accept CyberTrace log_scanner events
5. In the **Port** field specify an available port (e.g. 10080) which is going to be receiving the CyberTrace events



6. Press **Save**. The source will appear in the list of sources under the name of "LogScanner"

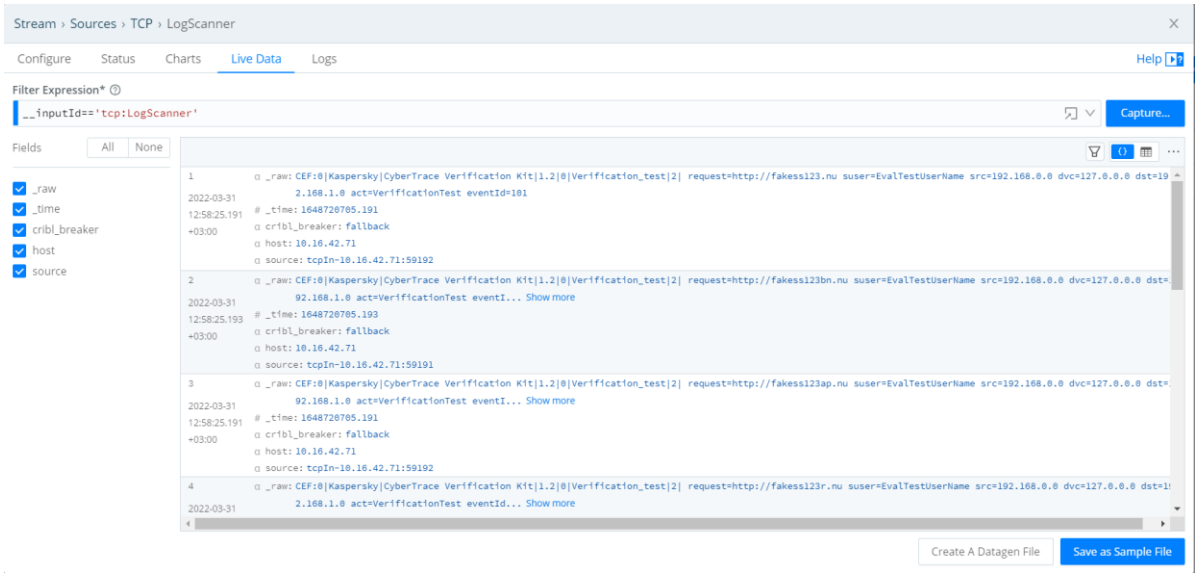
Verifying the settings:

1. On the CyberTrace machine, go to the `%service_dir%/log_scanner` directory and send the events from the verification file to Cribl. In order to do that:
   a. In file `log_scanner.conf` in the ***Connection*** element specify the values of IP and port specified in the Cribl settings earlier. Please find more information about the config file `log_scanner.conf` in the documentation: https://support.kaspersky.com/CyberTrace/1.0/en-US/171646.htm
   b. Send the events from file `%service_dir%/verification/kl_verification_test_cef.txt` to Cribl:

```
./log_scanner -p ../verification/kl_verification_test_cef.txt
```

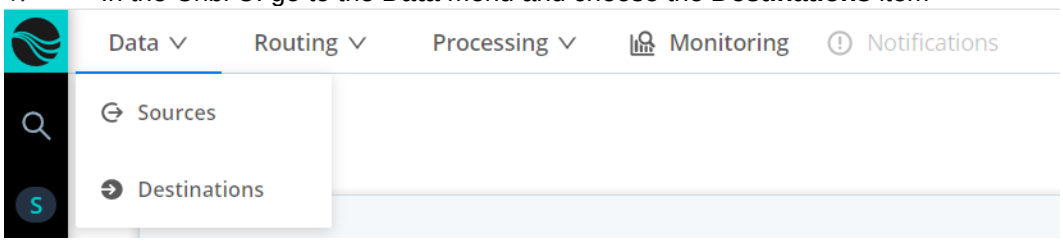
c. Please find more information about Log Scanner usage in the documentation: https://support.kaspersky.com/CyberTrace/1.0/en-US/171643.htm

2. In the **Data Sources** page in Cribl among the **TCP** sources choose item named "LogScanner" from the list of available sources, go to the **Live Data** tab
3. If necessary send the verification events again (please refer to the step above)
4. Ten events from the verification file `kl_verification_test_cef.txt` are going to appear in the **Live Data** tab

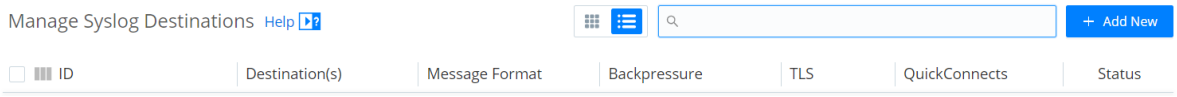


2. Adding the CyberTrace Destination in Cribl

1. In the Cribl UI go to the **Data** menu and choose the **Destinations** item

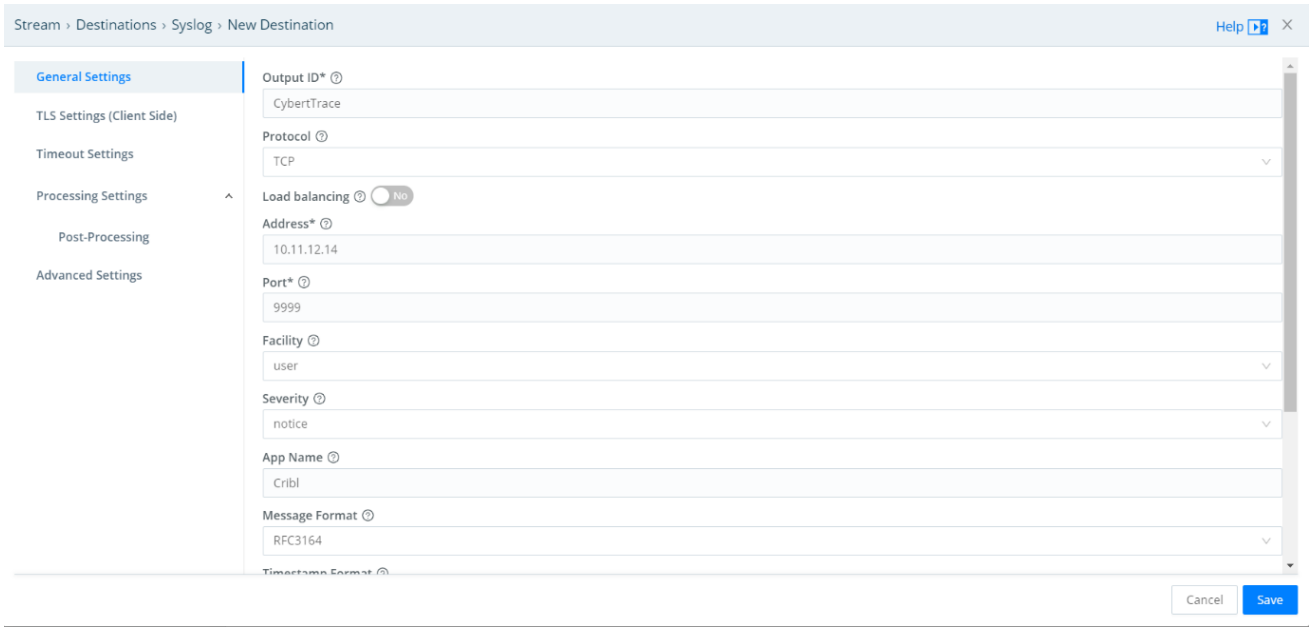


2. Choose type **Syslog** and press the "**+ Add new**" button



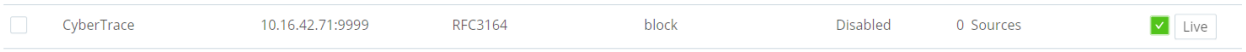
3. In the **Output ID** field specify the "CyberTrace" value
4. In the **Protocol** field choose TCP
5. In the **Address** field choose the IP address of the CyberTrace host

6. In the **Port** field specify port 9999 – the port where CyberTrace receives the events (how to configure CyberTrace please see below)



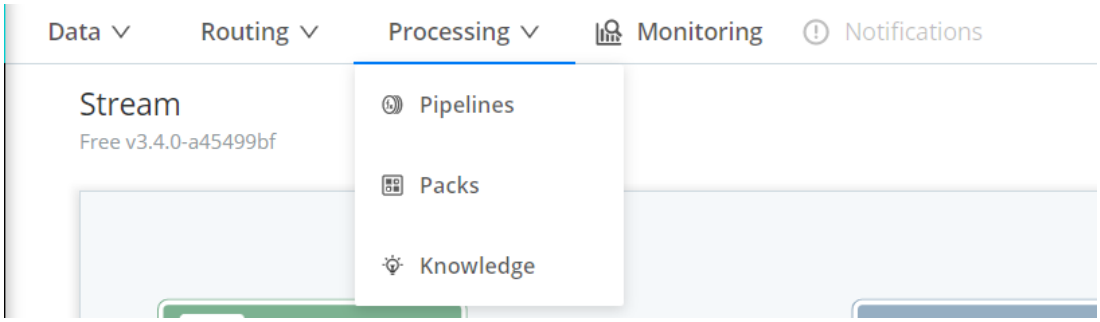
7. Leave the other fields with the default values **Save**.

The new Destination will appear in the list under the name of "CyberTrace" and, assuming everything is configured correctly, the "Status" column will contain a green checkbox

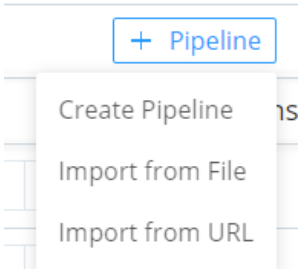


3. Creating the Pipeline in Cribl for sending the source event to CyberTrace

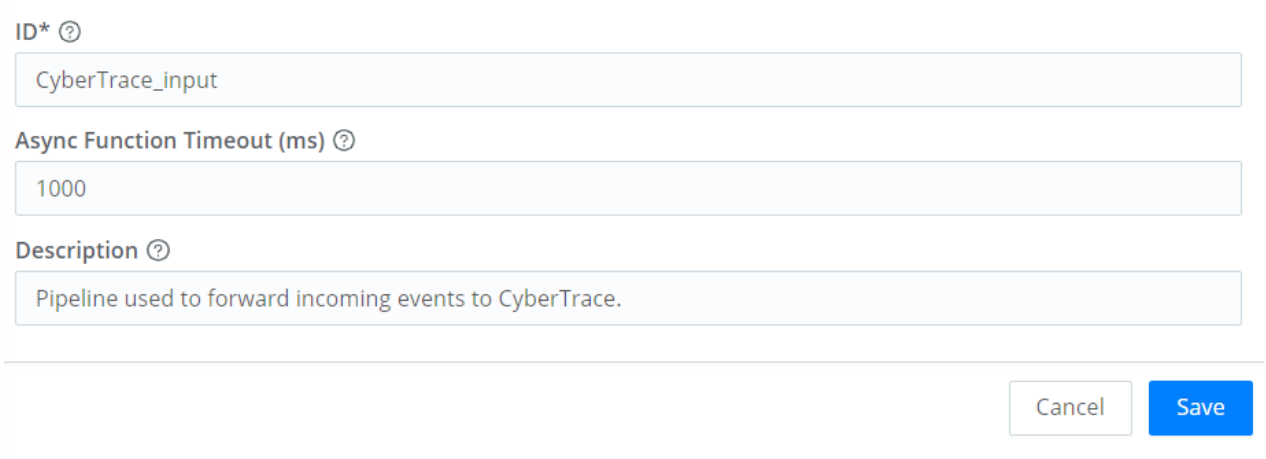
1. In the Cribl UI go to the **Processing** menu and choose the **Pipelines** item



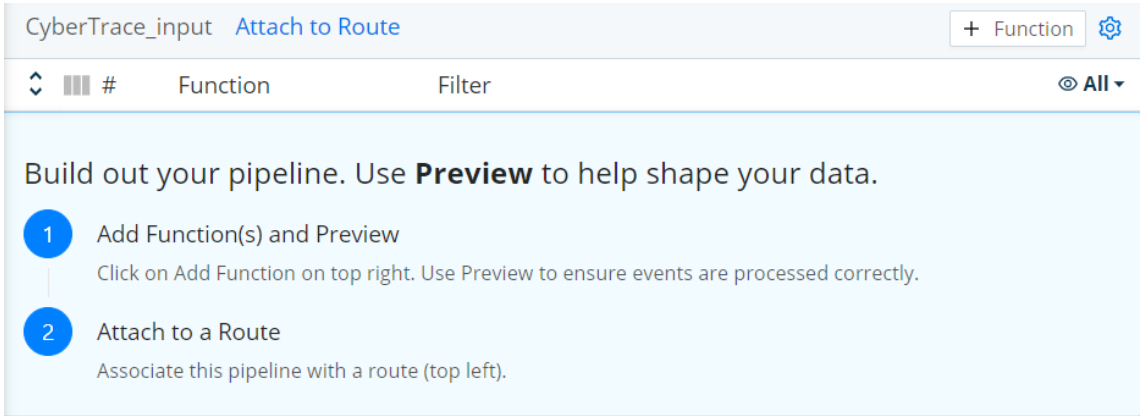
2. Press the "**+ Pipeline**" button and in the list choose the "**Create Pipeline**" item



3. In the **ID** field specify the "CyberTrace_input" value
4. Optionally, fill the Description field



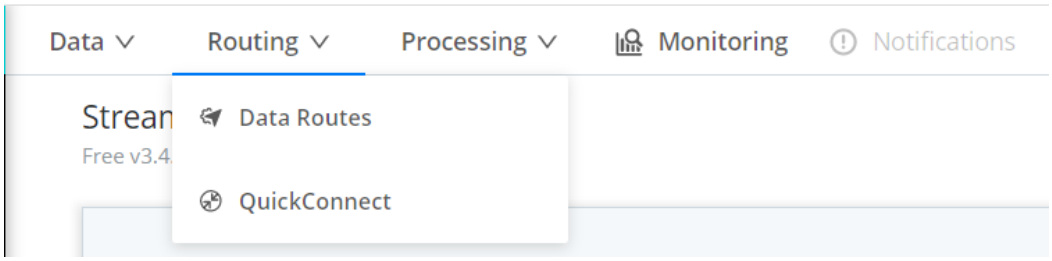
5. Press **Save**. The screen will show the recommendation of adding functions and attaching the pipeline to a Route.



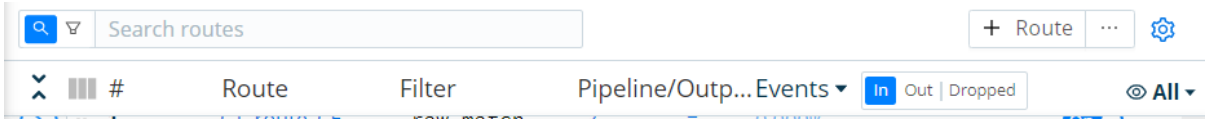
This guide does not cover adding functions in the existing pipeline as it assumed the source event to be forwarded to CyberTrace as is.

4. Creating a Route in Cribl, forwarding the source event to CyberTrace

1. In the Cribl UI go to the **Routing** menu and choose item **Data Routes** or choose the **Attach to Route** item in the pipeline window "CyberTrace_input" (please refer to the sections of adding the pipeline above)



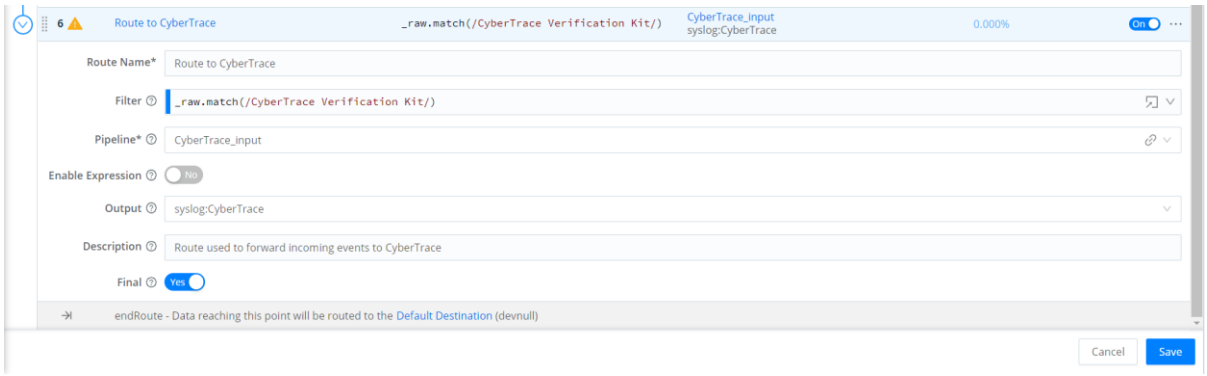
2. In the window which opened press the "**+ Route**" button



3. In the **Route Name** field please specify the "Route to CyberTrace" value
4. In the **Filter** field specify the following string:

```
_raw.match(/CyberTrace Verification Kit/)
```

5. An incoming event will be attached to the route "Route to CyberTrace" based on it containing a substring "CyberTrace Verification Kit".
6. In the **Pipeline** field specify the "CyberTrace_input" pipeline
7. Leave the "No" value in the **Enable Expression** field
8. In the **Output** field please choose destination named "syslog:CyberTrace" created earlier
9. Optionally, add a **Description**
10. Leave the "Yes" value in the **Final** field if the goal is to send the events to CyberTrace only



11. Press **Save**
12. Drag'n'drop the newly created route to a position where the other routes located above won't prevent forwarding of Log Scanner events to the "Route to CyberTrace" route
13. Press **Save** at the end of the window

5. Adding the CyberTrace Source in Cribl

Add the new data source to accept the events (detections and alerts) from CyberTrace.
This should be done in the same way as in section "Adding the log_scanner Source in Cribl".
Set the name of the source to "CyberTrace", and the port where Cribl is going to accept the CyberTrace events, please set to 9998.

kaspersky

6. Configuring CyberTrace

1. When you install CyberTrace, specify SIEM = "Splunk".
2. In the CyberTrace UI on the **Settings > Service** page in the "Service listens on" section specify the IP address and port where CyberTrace is going to accept incoming events.

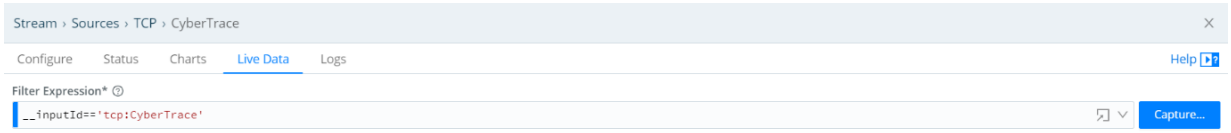
   Those settings must coincide with destination parameters added in Cribl in section "Adding the CyberTrace destination in Cribl".

3. In the same page in section "Service sends events to" specify the IP address and port of the host where Cribl is going to expect events from CyberTrace.

   Those settings should coincide with the source added in Cribl in "Adding the Source of CyberTrace in Cribl".

7. Intermediate verification test

1. In the Cribl UI go to menu **Data** and choose the **Sources** item
2. Choose the "CyberTrace" source from the list of TCP sources and go to tab **Live Data**
3. Press the **Capture** button

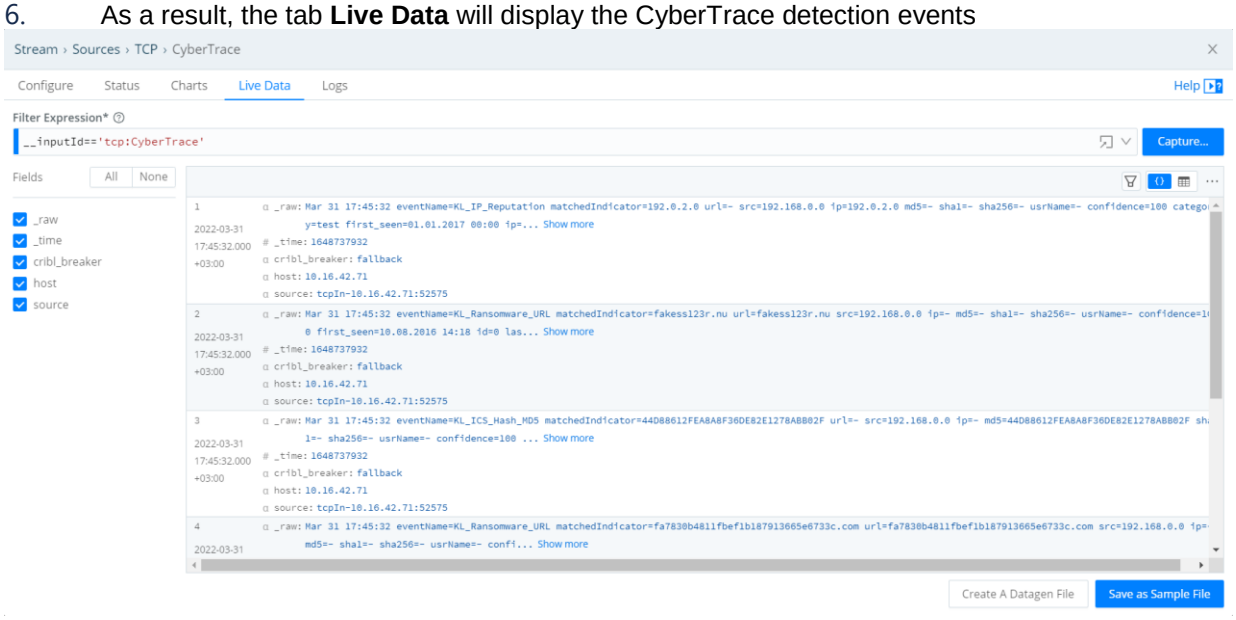


4. While Cribl is accepting the events from the CyberTrace source, it is necessary to send the verification events from file `kl_verification_test_cef.txt` on the CyberTrace node via *log_scanner* (located in `%service_dir%/log_scanner`) to Cribl:

```
./log_scanner -p ../verification/kl_verification_test_cef.txt
```

5. Please find more information about log_scanner usage in the CyberTrace online documentation: https://support.kaspersky.com/CyberTrace/1.0/en-US/171643.htm

6. As a result, the tab **Live Data** will display the CyberTrace detection events



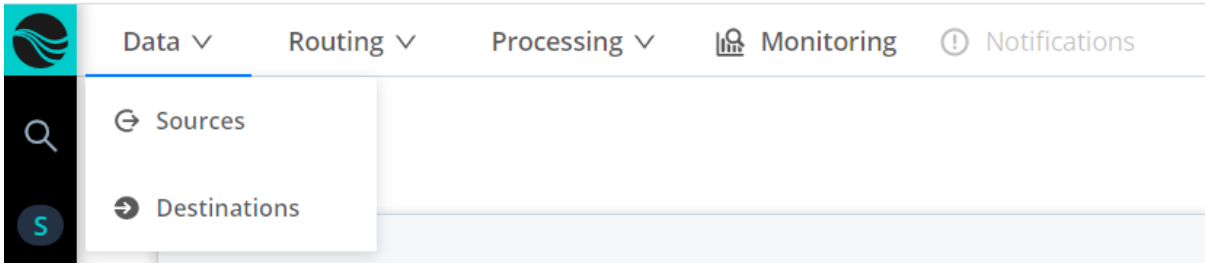
8. Configuring the delivery of CyberTrace detections and alerts from Cribl to Splunk

The steps of configuring the events forwarding from Cribl to the SIEM should involve:

- Adding the SIEM destination;
- Adding the pipeline (one or two – if the detections and alerts should be processed in a different way) to process the events before passing to the SIEM;
- Adding the route and attaching it to the pipeline from the step above.

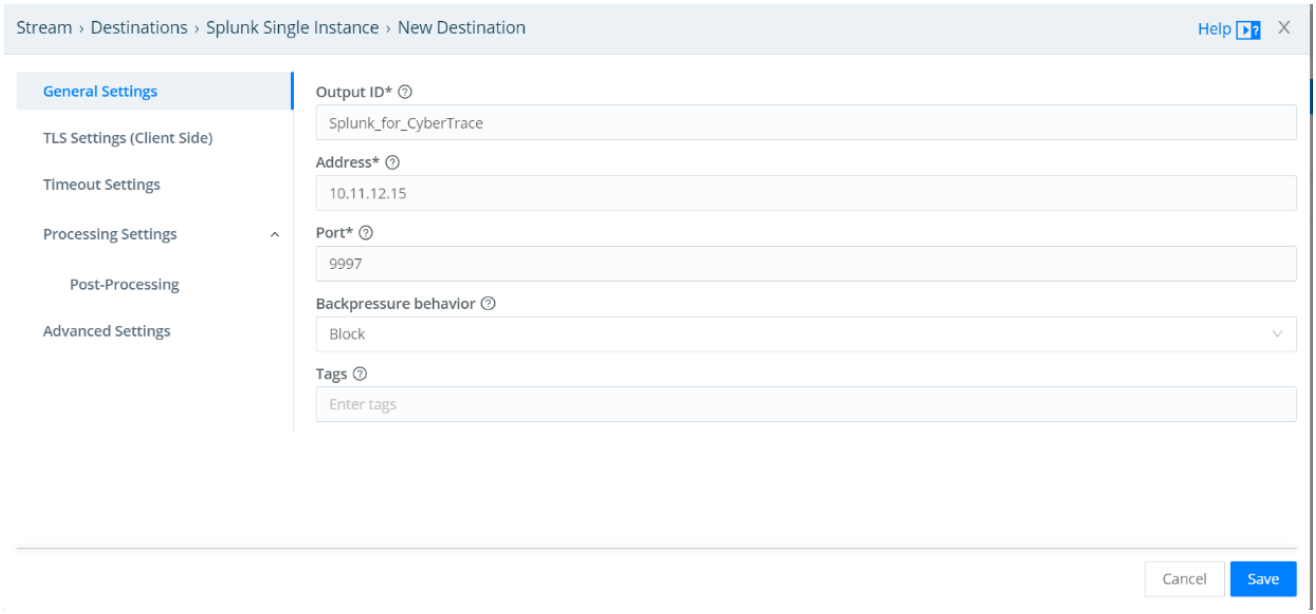
Adding Destination Splunk in Cribl

1. In the Cribl UI go to menu **Data** and choose the **Destinations** item



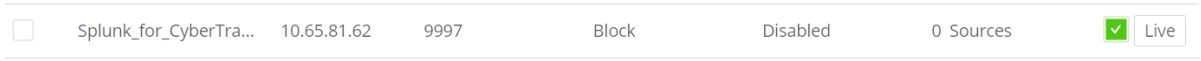
2. Choose type **Splunk (Splunk Instance)** and press the "**+ Add new**" button

3. In the **Output ID** field specify "Splunk_for_CyberTrace"
4. In the **Address** field specify the IP address of the host running Splunk Enterprise Indexer
5. In the **Port** field specify the port where Splunk accepts events for the index (by default this is port 9997)



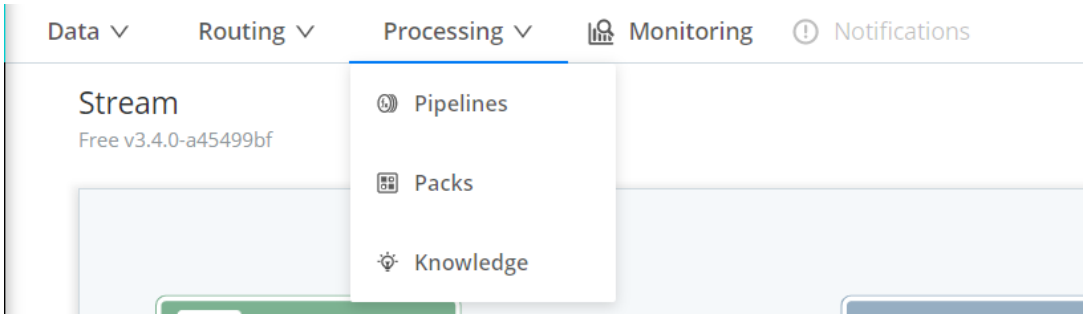
6. Leave all the remaining fields with the default values and press **Save**.

The new Destination Will appear in the list named "Splunk_for_CyberTrace" and a green checkbox should appear in the Status column, assuming everything was set correctly

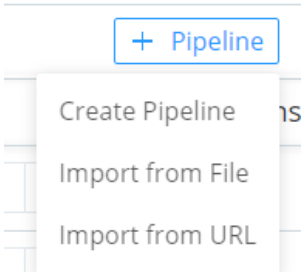


Creating a Pipeline in Cribl, forwarding the CyberTrace detection event

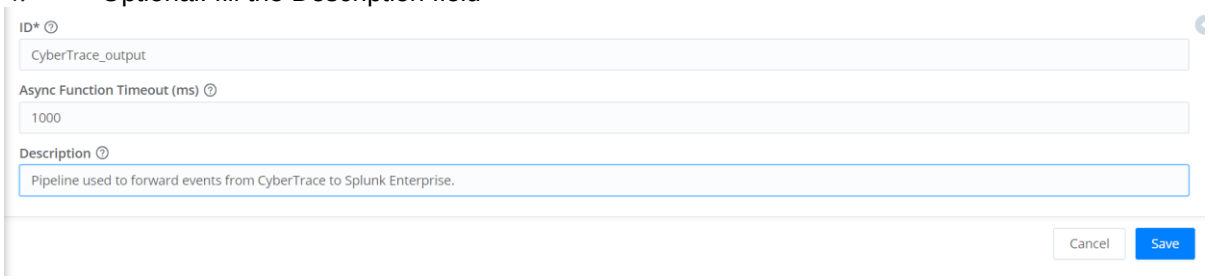
1. In the Cribl UI go to menu **Processing** and choose the **Pipelines** item



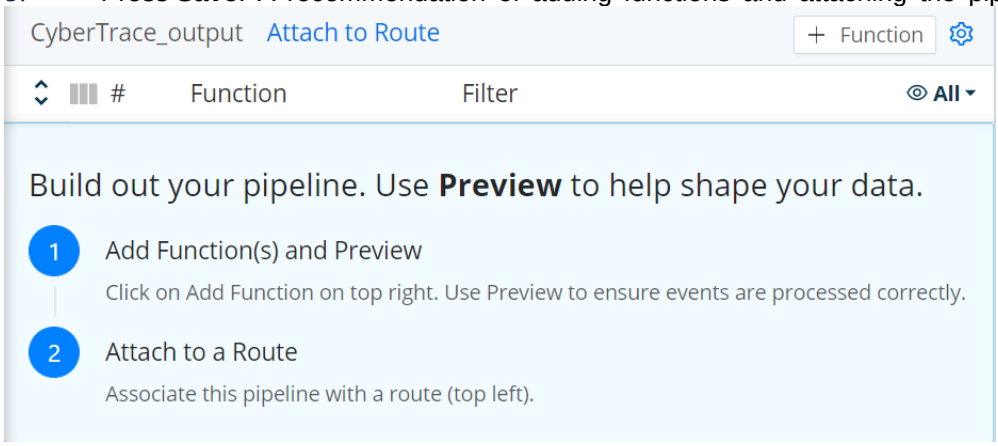
2. Press the "+ Pipeline" button and choose "Create Pipeline" in the list



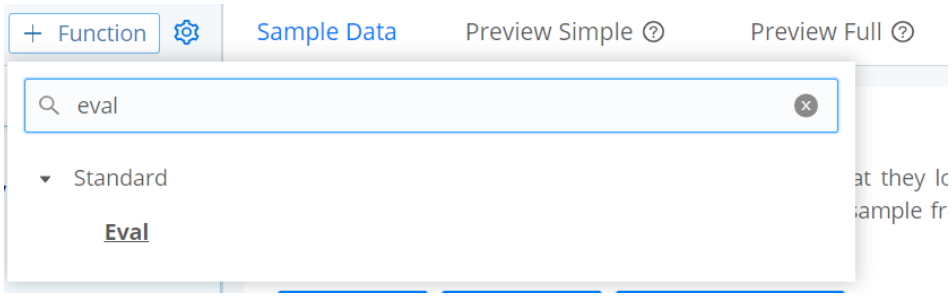
3. In the **ID** field specify "CyberTrace_output"
4. Optional: fill the Description field



5. Press **Save**. A recommendation of adding functions and attaching the pipeline to Route will be shown.



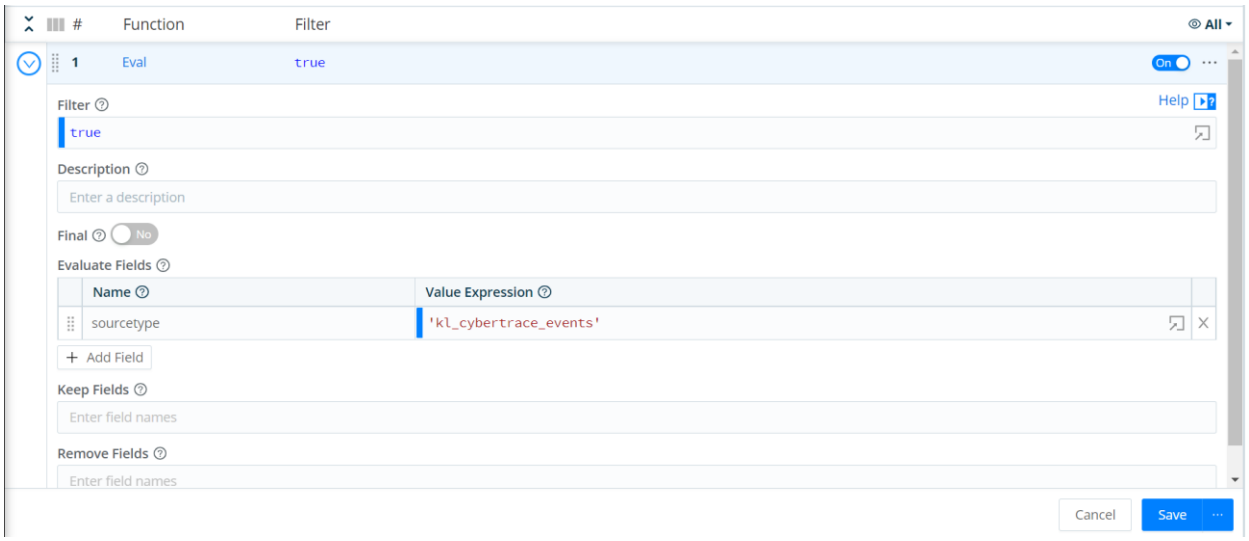
6. Press button "**+ Function**" and find the **eval** function in the list



The eval function configuration will be shown.

7. In the **Filter** field leave value "true"
8. In the **Description** field optionally specify the function description, e.g. "Function used to add sourcetype field to CyberTrace events."
9. In the **Final** field leave the default value "No"

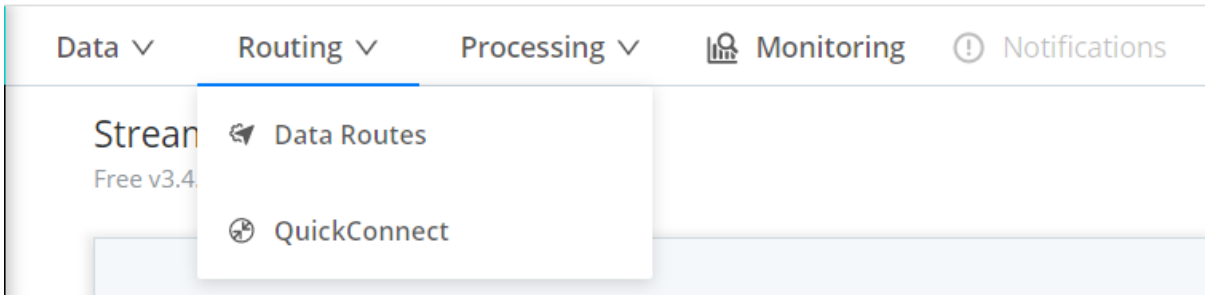
10. Press button “**+ Add Field**” and fill the newly appeared fields:
Name = sourcetype,
Value Expression = 'kl_cybertrace_events' (including the quote symbols)



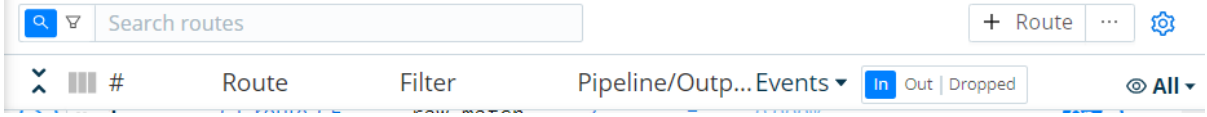
11. Leave the remaining fields as-is and press **Save**
As a result of this configuration, the CyberTrace event will get a field *sourcetype* with the 'kl_cybertrace_event' value. This field is used in the CyberTrace Search Head App for Splunk, therefore without this function the CyberTrace events won’t be displayed in the app.

Creating the Route in Cribl for sending the source event to CyberTrace

1. In the Cribl UI go to menu **Routing** and choose the **Data Routes** item or choose item **Attach to Route** in the window of pipeline "CyberTrace_output" (please refer to the sections of adding a pipeline above)



2. In the window that opened press button “**+ Route**”

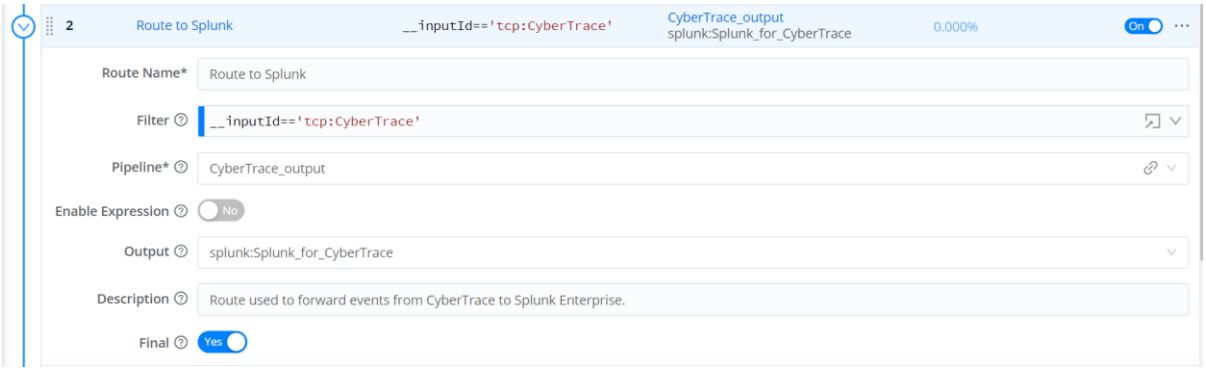


3. In the **Route Name** field please specify the value "Route to Splunk"
4. In the **Filter** field specify the following string:

```
__inputId=='tcp:CyberTrace'
```

5. All incoming events from the "CyberTrace" source will automatically be linked to route "Route to Splunk”.

6. In the **Pipeline** field specify the "CyberTrace_output" pipeline
7. Leave value "No" in the **Enable Expression** field
8. In the **Output** field choose the destination named "splunk:Splunk_for_CyberTrace", created earlier
9. Optionally fill **Description**
10. Leave the "Yes" value in the **Final** field



11. Press **Save**
12. Drag'n'drop the created route onto a position where the routes above do not prevent the CyberTrace log_scanner events getting into the route "Route to CyberTrace", but below the route named "Route to CyberTrace".

Press **Save** at the bottom of the page.

9. Setting up Splunk

1. Install the Kaspersky CyberTrace application for Splunk Enterprise Search Head App, in accordance with the guide: https://support.kaspersky.com/CyberTrace/1.0/en-US/167077.htm
More information about the application is available here: https://support.kaspersky.com/CyberTrace/1.0/en-US/169256.htm
2. Configure the Search Head App according to the guide: https://support.kaspersky.com/CyberTrace/1.0/en-US/167080.htm
3. (Optional) Configure the lookup script according to the guide: https://support.kaspersky.com/CyberTrace/1.0/en-US/167081.htm

10. The final verification test

After Cribl was integrated with the SIEM (please refer to "Configuring the forwarding of detections and alerts from Cribl to SIEM") please log onto the CyberTrace node and, using *log_scanner* (from `%service_dir%/log_scanner`), send the events from file `kl_verification_test_cef.txt` to Cribl:

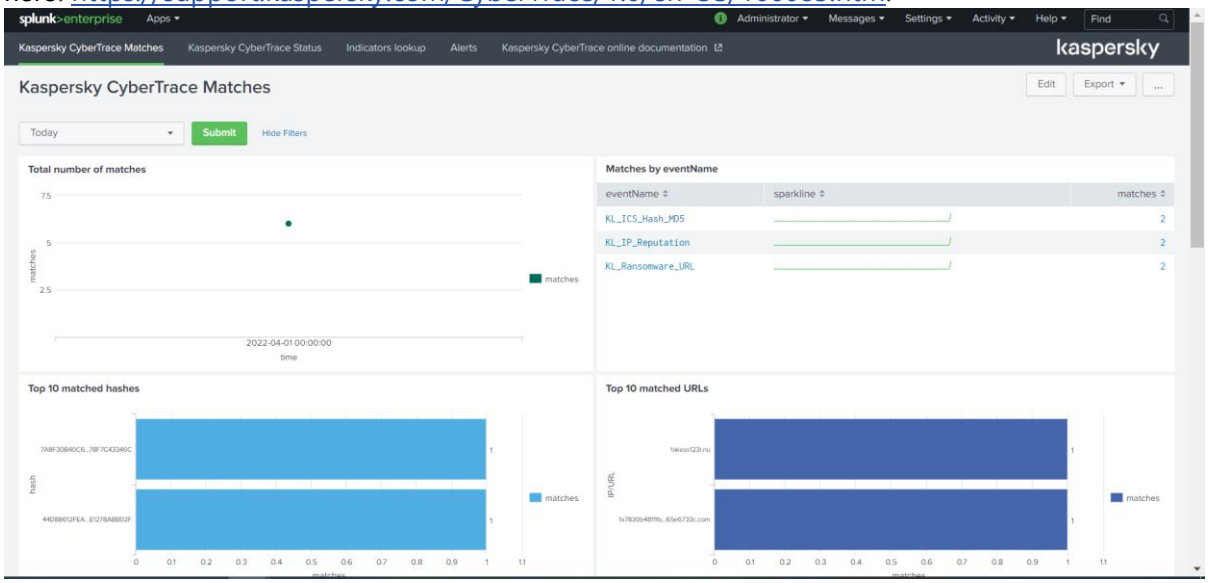
```
./log_scanner -p ../verification/kl_verification_test_cef.txt
```

Please find more information about the *log_scanner* usage here: https://support.kaspersky.com/CyberTrace/1.0/en-US/171643.htm

As a result of the verification test, the detection events should appear in the SIEM. The number of the detections depends on the list of feeds used in CyberTrace.

In the Splunk Enterprise UI open Kaspersky CyberTrace App and go to the **Kaspersky CyberTrace Matches** tab.

As a result of the verification test on the page with the dashboards you should be able to see the information about the detected indicators from file `kl_verification_test_cef.txt`. The number of detections depends on the list of feeds active in CyberTrace, more information is available here: https://support.kaspersky.com/CyberTrace/1.0/en-US/166083.htm.



Information about the CyberTrace alerts will be displayed in the "Kaspersky CyberTrace Status" tab (more information about the alerts available here: https://support.kaspersky.com/CyberTrace/1.0/en-US/198337.htm).

www.kaspersky.com/
www.securelist.com