CyberTrace, Cribl, Splunk integration

Data Feeds Integration Guidelines

11.04.2022

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. Adding the CyberTrace log_scanner source in Cribl
- 2. Adding the CyberTrace Destination in Cribl
- 3. Creating the Pipeline in Cribl for sending the source event
- 4. Creating a Route in Cribl, forwarding the source event to CyberTrace
- 5. Configuring CyberTrace
- 6. Adding the CyberTrace Source in Cribl
- 7. Intermediate verification test
- 8. Configuring the forwarding of CyberTrace detections and alerts from Cribl to Splunk
- 9. Setting up Splunk
- 10. The final verification test



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

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 U	l go to menu Dat a	a and choose Sour	ces		
	Data 🗸	Routing \vee	Processing \vee	🔝 Monitoring	() Notifica	tions
Q	⊖ Sources					
S	Destinat	ons				
2.	In the types li	st choose TCP a	nd press " + Add ne	w "		
Manage	TCP Sources Help	?		λ.		+ Add New
. III ID	Addr	ess Port	IP Allowlist Regex TLS	Routes/QC	Enabled	Status

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

Stream > Sources > TCP > New Sou	irce	Help 📭 🗙
General Settings	Input ID* 💿	Enabled Yes 🔵
TLS Settings (Server Side)	LogScanner	
Persistent Queue Settings	Address* ③	
Processing Settings	10.11.12.13	
Custom Command	Port* (0) 10080	
Event Breakers	Enable Header (2) (196)	
Fields	Tags 💿	
Pre-Processing		
Advanced Settings		
Connected Destinations		
		Cancel Save

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

Verifying the settings:

On the CyberTrace machine, go to the %service dir%/log scanner directory and send the events 1. from the verification file to Cribl. In order to do that:

In file log scanner.conf in the Connection element specify the values of IP and port specified in the a. 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: <u>https://support.kaspersky.com/CyberTrace/1.0/en-US/171643.htm</u>

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



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

Manage Syslog Destinations Help 📭		Е	٩			+ Add New	
ID	Destination(s)	Message Format	Bac	ckpressure	TLS	QuickConnects	Status

- 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)

Stream > Destinations > Syslog > Ne	w Destination	Help 🕨	? ×
General Settings	Output ID* 💮		^
TLS Settings (Client Side)	CybertTrace		
Timeout Settings	Protocol ③ TCP		~
Processing Settings	Load balancing ③ 🔵 🔊		
Post-Processing	Address* ①		-1
Advanced Settings	10.11.12.14 Port* ①		-1
	9999		
	Facility ①		_
	user Severity @		<u> </u>
	notice		~
	App Name ③		
	Message Format (2)		
	RFC3164		~
	Timestame Format 🗇	Cancel	▼ Save

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

CyberTrace	10.16.42.71:9999	RFC3164	block	Disabled	0 Sources	Live

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

Data ∨ Routing ∨	Processing ∨	🔝 Monitoring	 Notifications
Stream Free v3.4.0-a45499bf	Pipelines		
	Packs		
	🌣 Knowledge		

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

ID* ⑦		
CyberTrace_input		
Async Function Timeout (ms) ③		
1000		
Description ⑦		
Pipeline used to forward incoming events to CyberTrace.		
	Cancel	Save

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

CyberTrace_input Attach to Route	+ Function 🕸
Image: # Function Filter	⊚ All ▼
Build out your pipeline. Use Preview to help shape your data.	
1 Add Function(s) and Preview Click on Add Function on top right. Use Preview to ensure events are processed correctly	у.
2 Attach to a Route Associate this pipeline with a route (top left).	

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

२ ४ ऽ(arch routes			+	Route … 🔯
X Ⅲ #	Route	Filter	Pipeline/Outp Events 🕶	In Out Dropped	⊚ All ▼

- 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

6 A Route to 0	CyberTrace	_raw.match(/CyberTrace Verification Kit/)	CyberTrace_input syslog:CyberTrace	0.000%	On ···
Route Name*	Route to CyberTrace				
Filter 🗇	_raw.match(/CyberTrace Verificatio	on Kit/)			万 ~
Pipeline* 🗇	CyberTrace_input				0 v
Enable Expression ⑦	No				
Output 🕐	syslog:CyberTrace				v
Description ⑦	Route used to forward incoming events to 0	CyberTrace			
Final 🗇	Yes				
→ endRoute	- Data reaching this point will be routed to th	e Default Destination (devnull)			
					Cancel Save

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.

6. Configuring CyberTrace

- 1. When you install CyberTrace, specify SIEM = "Splunk".
- 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 <code>%service_dir%/log_scanner</code>) 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: <u>https://support.kaspersky.com/CyberTrace/1.0/en-US/171643.htm</u>

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

Stream > Sources > TCP > CyberTrace X							
Configure Status Ch	iharts Live Data Logs	Help 💽?					
Filter Expression* ③	er Expression* ⑦						
inputId=='tcp:CyberTrace' □							
Fields All None		8					
✓ _raw ✓ _time ✓ cribl_breaker ✓ host	1 a _raw: Nar 31 17:45:32 eventName=KL_IP_Reputation matchedIndicator=192.0.2.0 url=- src=192.168.0.0 1p=192.0.2.0 md5=- shal=- sha 2022:03:1 y=test first_seen=01.01.2017 00:00 1p= Show more 17:45:32:00 a cribL_breaker: fallback 03:00 a cribL_breaker: fallback 0 source: tcp1:0-10.16.21.7:52575	1256=- usrName=- confidence=100 catego +					
source	2 a _raw: Nar 31 17:45:32 eventName=KL_Ransomware_URL matchedIndicator=fakess123r.nu url=fakess123r.nu url=fakess123	ihal≃- sha250≕- usrName≃- confidence=1					
	3 a _raw: Mar 31 17:45:32 eventName=KL_ICS_Hash_MD5 matchedIndfcator=44088612FEA8A8F360E82E1278A8882F url=- src=192.168.0.0 1p=- md 2022.03.1 1=- sha256=- usrName=- confidence=100 Show more 17:45:32.00	15-44088612FEA8A8F360E82E1278A8882F sh					
	4 0_rww:har ii irisiz eventumerk_kaniommare_ukt matchedIndicitor#fa23064811fbef1b1879136566733c.com url=fa283664811fbef1b18 2022.03.31 md5== shale= sha256== usrkame== confi Show more 4	8791300560733c.com src=192.168.8.0 1p= •					
	Create	e A Datagen File Save as Sample File					

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





- 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)



Stream > Destinations > Splunk Single Instance > New Destination			
General Settings	Output ID* ③		
TLS Settings (Client Side)	Splunk_for_CyberTrace		
Timeout Settings	Address* ⑦ 10.11.12.15		
Processing Settings	∧ Port* ⑦		
Post-Processing	9997 Backpressure behavior ⑦		
Advanced Settings	Block	~	
	Tags 🗇		
	Enter tags		
		Cancel Save	

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

		Splunk_for_CyberTra	10.65.81.62	9997	Block	Disabled	0 Sources	Live
--	--	---------------------	-------------	------	-------	----------	-----------	------

Creating a Pipeline in Cribl, forwarding the CyberTrace detection event

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

Data \lor Routing \vee	Processing V 🔒 Monitoring ① Notifications
Stream Free v3.4.0-a45499bf	9 Pipelines
	III Packs
	诊 Knowledge

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



3. In the ID field specify "CyberTrace_output"

 Optional: fill the Description field 	
ID* ③	(
CyberTrace_output	
Async Function Timeout (ms) 💿	
1000	
Description ⑦	
Pipeline used to forward events from CyberTrace to Splunk Enterprise.	
	Cancel Save

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



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"

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

# Function	Filter	© All
1 Eval	true	On O
Filter ⑦		Help 📭?
true		2
Description ⑦		
Enter a description		
Final @ No		
Evaluate Fields ⑦		
Name ⑦	Value Expression ⑦	
sourcetype	'kl_cybertrace_events'	× R
+ Add Field		
Keep Fields ⑦		
Keep Fields ⑦ Enter field names		
Keep Fields ⑦ Enter field names Remove Fields ⑦		

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)

	Data ∨	Routing \vee	Processing V	Monitor	ing !	Notificat	tions
	Strean Free v3.4.	😭 Data Route	S				
		🛞 QuickConn	ect				
2.	In the wir	ndow that opened	press button " + R o	oute"			
٩	☑ Search rou	utes				+ Route ··	·· 🕸
×	##	Route Fi	ilter Pipel	ine/Outp Events 🔻	In Out Drop	ped	⊚ All -

- 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

\diamond	2 Route to	Splunk	inputId=='tcp:CyberTrace'	CyberTrace_output splunk:Splunk_for_CyberTrace	0.000%	On ••••
	Route Name	Route to Splunk				
	Filter 🤅)inputId=='tcp:Cyber	Trace'			\square \land
	Pipeline*	CyberTrace_output				I v
	Enable Expression ⑦ 🔵 №					
	Output 🔇	splunk:Splunk_for_CyberTr	ace			V
	Description @					
	Final 🤅) Yes				

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: <u>https://support.kaspersky.com/CyberTrace/1.0/en-US/167077.htm</u>

More information about the application is available here: <u>https://support.kaspersky.com/CyberTrace/1.0/en-US/169256.htm</u>

2. Configure the Search Head App according to the guide: <u>https://support.kaspersky.com/CyberTrace/1.0/en-US/167080.htm</u>

3. (Optional) Configure the lookup script according to the guide: <u>https://support.kaspersky.com/CyberTrace/1.0/en-US/167081.htm</u>

10. The final verification test

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

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

Pleasefindmoreinformationaboutthelog_scannerusagehere: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: <u>https://support.kaspersky.com/CyberTrace/1.0/en-US/166083.htm</u>.

punk>enterprise Apps •			aministrator • Messages •	Settings • Activity	Help Find
aspersky CyberTrace Matches Kaspersky CyberTrace Status Indicators lookup Alerts Ka	aspersky CyberTra	ce online documentation			kaspersky
aspersky CyberTrace Matches					Edit Export •
Today					
Total number of matches		Matches by eventName			
75		eventName =	sparkline *		matche
		KL_ICS_Hash_MD5		1	
5		KL_IP_Reputation			
25	matches	KL_Ransomware_URL			
2022-04-0100:00:00 time					
Fop 10 matched hashes		Top 10 matched URLs			
Эмягодоноса. Элерсединос 440984074А. Коллинанори 1	matches	188251231 ги 197			a matchi
0 01 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1	11	0	01 0.2 0.3 0.4 0	0.5 0.6 0.7 0.8	0.9 1 1.1

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

kaspersky

www.kaspersky.com/ www.securelist.com