Splunk SIEM Integration Guide

The Nile Service Block (NSB) integrates with Splunk Technology's dat searching product, Splunk, via Splunk's HTTP Event Collector (HEC), export NSB security events – audit logs and user device events – to Splunk for log analysis and archiving by the customer.

Overview

The Nile Service Block (NSB) integrates with Splunk Technology's data searching product, Splunk, via Splunk's *HTTP Event Collector* (HEC), to export NSB security events – audit logs and user device events – to Splunk for log analysis and archiving by the customer.

Prerequisites

- Cloud Splunk instance, or an on-premises Splunk instance, with access from Nile cloud.
- Administrative log in to Spunk instance.
- Administrative log in to Nile Portal.

Limitations:

- Nile Service Block supports only signed SSL certificates, or HTTP access with no SSL. Selfsigned HTTPS certificates are not acceptable.
- Nile does not support the Splunk Cloud's free trial offer. That trial offer uses SSL with a selfsigned certificate. There is no option to disable self-signed certificates on Splunk Cloud's free trial, or for Nile to accept self-signed certificates.

Splunk Configuration:

Create Splunk HTTP Event Collector

• Log in to Splunk instance as an administrator.

\leftarrow	\rightarrow	С	A Not Secure	20.232.17.62:8000/en-US/account/login?return_to=%2Fen-US%2F
--------------	---------------	---	--------------	---



- Navigate to Settings
- Select **Data inputs** from the DATA section.

	i Administrator 🔻	Messages 🔻 Settings 🔻	Activity - Help - Find a
ard	Administrator •	Messages • Settings • KNOWLEDGE Searches, reports, and alerts Data models Event types Tags Tags Fields Lookups User interface Alert actions Advanced search All configurations Server settings Server controls Health report manager RapidDiag Instrumentation Licensing	Activity Help Find Activity Activity Activity Activity Help Find Activity Ac
			Authentication Methods

• Click on the + Add new link to create a new HTTP event collector (HEC).

splunk>enterprise Apps -		6	Administrator 🔻	Message
Data inputs Set up data inputs from files and directories, network ports, and sc	ripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwardin	g and receiving.		
L	ocal inputs			
	Туре	Inputs		Actions
	Files & Directorles Index a local file or monitor an entire directory.	11	+ A	dd new
	HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ A	dd new
	TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ A	dd new

- Type a descriptive name for the collector in this example, we will use "nile_test". Keep all other values at their default value ("optional").
- Click the **Next** button

splunk>enterprise Apps -		🛕 Administrator 🔻 Me	ssages 🔻
	Add Data Select Sou	urce Input Settings Review Done	
	Files & Directories Upload a file, index a local file, or monitor an entire directory.	Configure a new token for receiving data over HTTP. Learn More 12	
	HTTP Event Collector $>$ Configure tokens that clients can use to send data over HTTP or HTTPS.	Name nile_test	
	TCP / UDP Configure the Splunk platform to listen on a network port.	Description ? optional	
	Scripts Get data from any API, service, or database with a script.	Output Group (optional) None 🕶	
	Systemd Journald Input for Splunk This is the input that gets data from journald (systemd's logging component) into Splunk.	Enable indexer	
	Splunk Secure Gateway Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets	FAQ → What is the HTTP Event Collector?	
	Splunk Secure Gateway Mobile Alerts TTL Cleans up storage of old mobile alerts	 How do I set up the HTTP Event Collector? How do I view and configure the tokens that I can use to send data to the HTTP Event Collector? 	t

• Keep the **Source Type** as Automatic;

Keep the index as "main".

NOTE: HEC data will be stored at by default in the main index; you can create a specific index by clicking on the **Create a new index**. This can be changed at any time. This example uses the main index; in production, use a sandbox index first then change the setting later.

• Click the **Review** button

							A	Administrator 🔻	Messages 🔻
	Add Data	Select Source	Input Settings	Review	—O Done	< Back	Review >		
Input Setting Optionally set additio	JS nal input parameters for	this data input as	s follows:						
Source type The source type is on platform assigns to al what kind of data you format the data intelli categorize your data,	ne of the default fields th I incoming data. It tells t I've got, so that the Splu gently during indexing. so that you can search	at the Splunk he Splunk platforn nk platform can And it's a way to it easily.	m		Auto	omatic	Select New	'	
Index The Splunk platform s selected index. Consi destination if you hav your data. A sandbox configuration without always change this se	stores incoming data as ider using a "sandbox" ir re problems determining index lets you troubles! impacting production in etting later. Learn More	events in the ndex as a a source type fo noot your idexes. You can	r						
Select Allowed Indexes	Available add item(s) and bistory and bist	d all > Selected ☐ main	item(s)« remove	all Select inc	dexes that cl	ients will be	able to select from	ι.	
Default Index	∎ main ▼ Create	a new index							

- Verify the HTTP Event Collector configuration.Click the **Submit** button

splunk>enterprise Apps •	i) Administrator ▼ Messages ▼
	Add Data Select Source Input Settings Review Done
	Input Type Token Name nile_test Source name override N/A Description N/A Enable indexer acknowledg No Output Group Output Group N/A Allowed indexes main
	Default index main Source Type

• Copy the contents of Token Value, and save it in a text file for later use in the Nile Portal settings.

(Example here is "55344676-48db-4a9a-a522-23b95C".)

• Click the Start Searching button

~	Token has been created successfully. Configure your inputs by going to Settings > Data Inputs									
	Token Value	5534467	76-48db-4a9a-a522-23b95C							
	Start Searc	hing	Search your data now or see examples and tutorials. 🛽							
	Add More I	Data	Add more data inputs now or see examples and tutorials.							
Download Apps			Apps help you do more with your data. Learn more. 🛽							
	Build Dashb	oards	Visualize your searches. Learn more. 🛽							

 Enter a search string; in this example, source="http:nile_test" (index="main")



Configure the Splunk HTTP Event Collector

After creating the HTTP Event Collector, enable the Collector, and configure the URL port and SSL options.

- From the Data section, click the **Data inputs** link
- Click on HTTP Event Collector link.

splunk>enterprise Apps -			Administrator •	Messages 🔻 Settings 🔻	Activity Help Find Q
Data inputs Set up data inputs from files and directories, network ports, and sc	ripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to For	warding and rec			DATA
L	.ocal inputs		Add Data	Data models Event types	Forwarding and receiving Indexes
	Туре	Inputs		Tags Fields	Report acceleration summaries
	Files & Directories Index a local file or monitor an entire directory.	11		Lookups User interface	Source types
	HTTP Event Collector Receive data over HTTP or HTTPS	1	Explore Data	Alert actions Advanced search All configurations	DISTRIBUTED ENVIRONMENT
	тср	0	ŶĮŶ	SYSTEM	Forwarder management Data Fabric Federated search
	Listen on a TCP port for incoming data, e.g. syslog.		Console	Server settings	Distributed search

• In the HTTP Event Collector page, click on **Global Settings** button

splunk>enterprise App	s 🔻			Administrator •	Messages 🔻	Settings 🔻	Activity 🔻	Help 🔻	Find Q
HTTP Event Collect Data Inputs > HTTP Event Collect	tor						GI	obal Setting	New Token
1 Tokens	App: All 🔻 filter	۹. ۵							20 per page 🔻
Name [*]		Actions	Token Value 🗘	Source Type \$		Index	÷	Status	\$
nile_test		Edit Disable Delete	55344676-48db-4a9a-a522-23b950110761			main		Enable	ed

- Enter these values into the form
 All Tokens: click on Enabled
 Enable SSL: check (HTTPS) or uncheck (HTTP) the checkbox
 HTTP Port Number: 8088 (default).
 Keep all other settings in their default value.
- Click the **Save** button

Edit Global Settings	j.		×
All Tokens	Enabled	Disabled	
Default Source Type	Select Source Type -		
Default Index	Default 🔻		
Default Output Group	None 🔻		
Use Deployment Server			
Enable SSL	for HTTPS		
HTTP Port Number ?	8088		
		Cancel	Save

This example shows that SSL is disabled, and the port number is the default value.

icon

NOTE

Important Note: The SSL and Port Number setting is a global setting, and will affect all HTTP Event Collectors.

Nile Portal Configurations:

Add Splunk collector to Nile Portal

- Login to Nile portal https://u1.nile-global.cloud/ using an admin account
- Navigate to (Settings button) ? Global Settings tab ? Integration subtab

n														
::		DHCP							Global settings					
며											Identity	Integrations		
8														
▲														
0														
				U										
C		,	Subscribe to	o Alerts ar	nd Even	ts								

- Click on ?; a new popup window will open
- Click on **Splunk**

Splunk	Contemporation Logic Monitor	(A) Web Hook	E mail
			CANCEL

• Fill out Splunk information:

Token: Copy and paste the token saved when creating the Splunk HEC URL: Enter Splunk cloud URL plus HTTP port number from Splunk HEC global settings (example: https://<customer_id>.splunlkcloud.com:8088 as in our settings we have 8088 as HTTP port number) • Click the Next button

Add Splunk (SIEM)	×
Name* default	
URL http://20.232.17.62:8088	
	NEVE

Select, by clicking on the checkboxes, if Audit, User Device Events, and/or Alerts need to be sent to Splunk

A	dd Splunk (SIEM)		×
	Audit		
	User Device Events		
	Alerts		
		BACK 54	AVE

• Click the **Save** button to save the settings. Click on **Splunk**, then click on ?, to test the connection

n							
::	Service areas	DHCP	Authentication	Segments	Wireless	Access Management	A
ᄃ							
▲	default	t (splunk)	TUS:-0				
0							
	URL						
c	http://20.232.17.62	:8088 ·					
	Subscription	s					
	Alerts audit						

n							
	Service areas	DHCP	Authentication	Segments	Wireless	Access Management	A
ᄃ							
	dofaul	t (coluple)					
▲	Tested	lon:- STAT	rus: - 🎧			/ • 🗠	
0			Ŭ			Test	
	URL http://20.232.17.62	2:8088 •					
C	Subscription	s					
	Alerts audi	t)					
n							
::	Service areas	DHCP	Authentication	Segments	Wireless	Access Management	Å
ᄃ							
	defau	lt (coluple)					
▲	Test	on: - STA	TUS: -(j)				
0			Ŭ				
	URL http://20.232.17.6	2:8088 •					
C	Subscription	าร					
	Alerts	it					

 If the test is successful, the collector status will change to UP (Green). if it fails it will show up as DOWN (red)



• To modify Splunk URL or Token, click on (pen); to delete Splunk integration, click on (trash)

Verify Nile Events under Splunk Search and Report:

- Login to Splunk instance as administrator.
- In the top menu, click on Search element Use the HEC name as a source, the index name for the specific index, and the filter for searching for specific data.For this example, the HEC name is "nile_test", the index name is "main", and the filter is: source="http:nile_test" (index="main")

Search Analytics Datasets F	Reports Alerts Dashboards
New Search	
source="http:nile_test" [dindex="mai	n" , topic"audit")
✓ 9 events (3/29/22 4:00:00.000 PM to 3	/30/22 4:32:40.000 PM) No Event Sampling *
Events (9) Patterns Statistics	Visualization
Format Timeline - Zoom Out Mar 29, 2022 4:00 PM	+ Zoom to Selection × Deselect
	1 day 1 hour
	List 👻 🖌 Format 20 Per Page 👻
< Hide Fields :≡ All Fields	i Time Event
SELECTED FIELDS a host 1 a source 1 a splunk_server 1 INTERESTING FIELDS a action 3 a additionalDetails.newValue.instance 1 # additionalDetails.newValue.lastTest 1 a additionalDetails.newValue.settings.c heckCertificate 1 a additionalDetails.newValue.settings.u ris() 2 a additionalDetails.newValue.type 1 a additionalDetails.newValue.type 1 a additionalDetails.oldValue.instance 1	<pre>> 3/30/22 { [-] 4:15:37.000 PM action: Test additionalDetails: ([+] } agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.83 Safari/537.36 auditDescription: Tested SIEM 'default' entity: SIEM errorMessage: null id: b5140666-97C8-4e41-bb54-ad5d677ee86e sourceIP: time: 1648656937000 tonic: audit user: i Show as raw text host = 20.232.1762:8088 _ source = http:nile_test _ splunk_server = VMTest</pre>

Use a topic name to display only audits or user device events

Examples: source="http:nile_test" (index="main", topic"audit") source="http:nile_test" (index="main", topic"userdeviceevents")