

Tenable and Splunk Integration

August 17, 2016 (Revision 1)

Table of Contents

Introduction	3
Recommended Configurations	
SecurityCenter + Splunk	
SecurityCenter Continuous View™ + Splunk (SecurityCenter + LCE + PVS + Splunk)	
Optional Configuration	
Passive Vulnerability Scanner Only (Standalone) + Splunk	
SecurityCenter	4
Integration Requirements	
Integration Configuration	5
Splunk Add-on for Tenable Configuration	5
Nessus	
Integration Requirements	
Integration Configuration	
Splunk Add-on for Tenable Configuration	
Passive Vulnerability Scanner	15
Integration Requirements	15
Integration Configuration	15
Tenable PVS Configuration	15
Splunk Configuration	
Log Correlation Engine	21
Integration Requirements	21
Integration Configuration	21
Tenable LCE Splunk Client Configuration	21
Splunk Configuration	23
Tenable LCE Syslog Forwarding	26
About Tenable Network Security	

Introduction

Tenable[™] and Splunk have a history of collaboration and interaction between our enterprise security solutions. Many customers want Tenable vulnerability and continuous monitoring data shared with their Splunk environment.

This document describes how to deploy integrations between Tenable Nessus[®], SecurityCenter[™], Passive Vulnerability Scanner[™] (PVS[™]), and Log Correlation Engine[™] (LCE[®]) and Splunk solutions, specifically Splunk Enterprise, and covers multiple methods of integration; we have worked to provide flexibility to support many different configurations. Please email any comments and suggestions about this document or its instructions to support@tenable.com.

Tenable Solution	Integration Type	Owner	Description
SecurityCenter	Vulnerability Metrics	Splunk	Splunk receives vulnerability data collected by SecurityCenter
Nessus	Nessus Host Scans, Nessus Plugins	Splunk	Splunk receives vulnerability data collected by Nessus, Splunk collects Nessus plugin information from the Tenable Knowledgebase
PVS	Passive Syslog Collection	Tenable	Real-time vulnerability and event data is sent from PVS to Splunk via syslog
LCE	Syslog Forwarding (bi-directional)	Tenable	LCE server collects data from Splunk, or log and event data collected by a LCE Client is sent to Splunk

Recommended Configurations

SecurityCenter + Splunk

SecurityCenter API \rightarrow Splunk Connector \rightarrow Splunk DB

How it works: SecurityCenter collects vulnerability data. The Splunk connector then connects to the SecurityCenter API to extract the vulnerability data and insert it into the Splunk DB.

Why: Fast and easy export of your Tenable vulnerability data to Splunk allows your correlation of vulnerabilities with the events in the Splunk console.

SecurityCenter Continuous View[™] + Splunk (SecurityCenter + LCE + PVS + Splunk)

SecurityCenter API \rightarrow Splunk Connector \rightarrow Splunk DB

Event Traffic (syslog) \rightarrow LCE (forward) \rightarrow Splunk DB (syslog)

How it works: SecurityCenter collects vulnerability data. The Splunk connector connects to the SecurityCenter API to extract vulnerability data and insert the data into the Splunk DB. By forwarding event traffic to LCE first, rich vulnerability and threat data can be correlated with all the SecurityCenter vulnerability sensor data.

Why: Fast and easy export of your Tenable vulnerability data to Splunk allows your correlation of vulnerabilities with the events in the Splunk console. Using LCE's Syslog Forwarding and Event Rules features, it can send all, or selected, logs to Splunk Enterprise for storage. This can result in a significant reduction in the cost of Splunk storage costs.

Optional Configuration

SecurityCenter API \rightarrow Splunk Connector \rightarrow Splunk DB

Event Traffic (syslog) \rightarrow Splunk DB (forward) \rightarrow LCE

How it works: SecurityCenter collects vulnerability data. The Splunk connector connects to the SecurityCenter API to extract the vulnerability data and insert it into the Splunk DB. The Tenable LCE Splunk Client forwards data that Splunk collects to the LCE server. Once the data reaches the LCE server, the data is reviewed and normalized so it can be queried in SecurityCenter.

Why: In addition to having Splunk collect events, the LCE Client for Splunk (available on the Tenable Support Portal) allows you to extract event data for correlation with all SecurityCenter vulnerability sensor data, allowing a better view of vulnerabilities and their impact from the SecurityCenter console. Check out the many SecurityCenter dashboards for some ideas of the pre-built event data that can be reported: https://www.tenable.com/sc-dashboards.

Passive Vulnerability Scanner Only (Standalone) + Splunk

PVS (syslog) \rightarrow Splunk PVS Connector \rightarrow Splunk DB

How it works: PVS collects vulnerability data. The Splunk PVS connector connects to PVS to extract the vulnerability data and insert it into the Splunk DB.

Why: PVS performs the completely passive collection of vulnerability data (via TAP/Mirror/SPAN). This data and device discovery provides tremendous insight into the applications and systems on your network, which is extremely important to incident response teams as deep knowledge about unmanaged systems are automatically imported to Splunk.

SecurityCenter

SecurityCenter consolidates and evaluates vulnerability data across an organization, prioritizing security risks and providing a clear view of the organization's security posture. With SecurityCenter's pre-built, highly customizable dashboards and reports, and the industry's only Assurance Report Cards (ARCs), users can visualize, measure, and analyze the effectiveness of their security program. The Splunk Add-on for Tenable allows Splunk users to collect SecurityCenter data, which is then indexed for further analysis.

This section assumes that the user has working knowledge of SecurityCenter and Splunk.

Integration Requirements

The following are required in order to integrate SecurityCenter with Splunk:

- SecurityCenter 5.3.1 or 5.3.2
- Splunk 6.x or higher

Integration Configuration

Splunk Add-on for Tenable Configuration

The Splunk Add-on for Tenable is available for download at https://splunkbase.splunk.com/app/1710/ (login required).

From Splunk, click the Manage Apps "gear" icon, located in the upper-left side of the screen.

piunk>		Administrator 🗸 🛛 Messages 🗸	Settings V Activity V Help V Find	
pps 🌣	Forwarders: Deployment 🛛 😫		Explore Splunk Enterprise	^
Search & Reporting	Forwarders by Status Split by Status Total: \$result.count\$			
		Waiting for data		

Select "Install app from file".

splunk> Apps ~				Adn	ninistrator 🗸 Messa	ges 🗸 🦷 Settings 🗸	Activity V Help V Find	
Apps								
								٩
Browse more apps	pp from file Create app							
Showing 1-15 of 15 items	Û						Results per page 25	~
Showing 1-15 of 15 items	Folder name ÷	Version 🕈	Update checking \$	Visible \$	Sharing ‡	Status ≑	Results per page 25	~
Showing 1-15 of 15 items	Folder name +	Version 🕈	Update checking ÷ Yes	Visible \$	Sharing ÷ App Permissions	Status ÷ Disabled Enable	Results per page 25	~
Showing 1-15 of 15 items Name ÷ SplunkForwarder SplunkForwarder	Folder name ÷ SplunkForwarder SplunkLightForwarder	Version ÷	Update checking \$ Yes Yes	Visible ¢ No No	Sharing ÷ App Permissions App Permissions	Status ≎ Disabled Enable Disabled Enable	Results per page 25	~
Showing 1-15 of 15 items Name SplunkForwarder SplunkLightForwarder Log Event Alert Action	Folder name ÷ SplunkForwarder SplunkLightForwarder alert_Jogevent	Version ¢ 6.4.2	Update checking Yes Yes Yes	Visible ≎ No No No	Sharing ÷ App Permissions App Permissions App Permissions	Status ◆ Disabled Enable Disabled Enable Enabled Disable	Results per page 25 Actions Edit properties View objects	~
Showing 1-15 of 15 items Name SplunkForwarder SplunkLightForwarder Log Event Alert Action Webhook Alert Action	Folder name = SplunkForwarder SplunkLightForwarder alert_Jogevent alert_webhook	Version \$	Update checking • Yes Yes Yes Yes	Visible ÷ No No No No	Sharing ÷ App Permissions App Permissions App Permissions App Permissions	Status Disabled Enable Disabled Enable Enabled Disable Enabled Disable	Results per page 25 Actions	

Click "Browse".

splunk > Apps ~		Administrator 🗸	Messages 🗸	Settings \vee	Activity 🗸	Help \sim	Find	
Upload app Apps » Upload app								
	Upload an app If you have a .spl or targz app file to install, you can upload it using this fo	orm.						
_	You can replace an existing app via the Splunk CLI. 😭 Learn more. File Browse No file selected.							
	Upgrade app. Checking this will overwrite the app if it already exists	s.						
	Cancel		_	Upload	_	_	_	

Select the downloaded Splunk Add-on for Tenable file, and click "Upload".

splunk> Apps ~	Administrator v Messages v Settings v Activity v Help v Find
Upload app Apps » Upload app	
	Upload an app If you have a .spl or .tar.gz app file to install, you can upload it using this form. You can replace an existing app via the Splunk CLI. 😭 Learn more.
	File Browse splunk-add-on-for-nessus_500.tgz Upgrade app. Checking this will overwrite the app if it already exists.
	Cancel

When Splunk has completed processing, it will require a restart. After restarting and logging back into Splunk, navigate back to "Managing Apps", as described in the first step. You will now see a "Splunk Add-on for Tenable" listed under "Apps". Click the "Launch app" link under "Actions" to the right of the app name.

nns									
hha									
									٩
Browse more apps	app from file Create app								
showing 1-16 of 16 items									Results per page 25 🗸
Name ‡	Folder name ‡	Version ‡	Update \$ checking	Visible ‡	Sharing ‡	Status ‡	Actions		
Name 🕈 SplunkForwarder	Folder name +	Version \$	Update checking Yes	Visible \$	Sharing ¢	Status ÷ Disabled Enable	Actions		
Name © SplunkForwarder SplunkLightForwarder	Folder name \$ SplunkForwarder SplunkLightForwarder	Version ‡	Update checking Yes Yes	Visible ¢ No No	Sharing ÷ App Permissions App Permissions	Status ÷ Disabled Enable Disabled Enable	Actions		
Name \$ SplunkForwarder SplunkLightForwarder Splunk Add-on for Tenable	Folder name \$ SplunkForwarder SplunkLightForwarder Splunk_TA_nessus	Version \$	Update checking Yes Yes Yes	Visible * No No Yes	Sharing App Permissions App Permissions Global Permissions	Status Clisabled Enable Disabled Enable Enabled Disabled	Actions	properties View object	ts 12 View details on SplunkApps
Name SplunkForwarder SplunkLightForwarder Splunk Add-on for Tenable Log Event Alert Action	Folder name = SplunkForwarder SplunkLightForwarder Splunk_TA_nessus alert_logevent	Version ¢ 5.0.0 6.4.2	Update checking Yes Yes Yes Yes	Visible * No No Yes No	Sharing Carries Sharing App Permissions App Permissions Global Permissions App Permissions	Status Constant Status Constant Status Constant Status Constant Status S	Actions	properties View object	ts 년 View details on SplunkApps
Name SplunkForwarder SplunkLightForwarder Splunk Add-on for Tenable Log Event Alert Action Webhook Alert Action	Folder name * SplunkForwarder SplunkLightForwarder Splunk_TA_nessus alert_Jogevent alert_webhook	Version ¢ 5.0.0 6.4.2 6.4.2	Update checking Yes Yes Yes Yes Yes	Visible ¢ No Yes No No	Sharing App Permissions App Permissions Global Permissions App Permissions App Permissions App Permissions	Status \$ Disabled Enable Disabled Enable Enabled Disable Enabled Disable Enabled Disable	Actions	properties View object iew objects iew objects	s 년 View details on SplunkApps

Click the "Configuration" tab at the top of the screen then the "Add SecurityCenter Server" button to the right of the screen.

Inputs Configuration	Search	Splunk Add-on for Tenable
Configuration		
Configure your Security Cente	r server, proxy and logging level.	
Security Center Server	Proxy Logging	
		Add Security Center Server
D Security Center Servers	filter	Add Security Center Serve

A window is displayed where users can uniquely name the SecurityCenter server, as well as input the URL and login credentials for SecurityCenter. Complete the fields and click "**Add**".

Name*	Remote SecurityCenter Server	
	Enter a unique name for each security center server.	
URL*	http://172.16.1.118	
	For example, https://10.10.10.10:443	
Username*	techanalyst	
Password*		

From the "Inputs" screen, select "Create New Input" and click "SecurityCenter".

splun	k> App: Splunk Add-on for T	enable 🗸		Administrator 🗸	Messages 🗸	Settings 🗸	Activity 🗸	Help 🗸	Find
Inputs	Configuration Search							Splun	k Add-on for Tenable
Inpu	ts								Create New Input
Create da	ata inputs to collect data from Te	enable.						- 6	Security Center
0 Inputs	Service : All ~		filter						Nessus
i Nam	ne ^	Service 0	Interval 0	Index 0		Status 0		Act	ions

A window is displayed where users can name the SecurityCenter input, and utilize the "Server" parameter to select the SecurityCenter server that was previously set up in the Configurations tab.

Name*	Perimeter SecurityCenter	
	Enter a unique name for each security center input.	
Server*	SC5.3.2	Ŧ
Metrics*	Vulnerability	Ŧ
Start Time	2016-08-01T09:00:00+0800	
	The add-on starts collecting data with a date later than this UTC time. The ago.	e default time is 30 days
Interval*	60	
	Time interval of input in seconds.	
Index*	default	*

7

Enter or select values for the remaining parameters (from the Splunk documentation):

- Metrics: Select Vulnerabilities to collect vulnerability data discovered on SecurityCenter. The source type for this data is automatically set to tenable:sc:vuln
- Start Time: The add-on starts collecting data with a date later than this time. The default is 30 days before the configuration. The format is "YYYY-DD-MMThh:mm:ssTZD", e.g., 2016-08-01T09:00:00+0800 stands for fetching data from 2016-08-01 09:00:00 in UTC+8 time zone.
- Interval: The number of seconds to wait before the Splunk platform runs the command again. The default is 60.
- Index: The index in which to store SecurityCenter data.

Click "Add" to finalize the "Inputs" configuration.

The SSL certificate from the SecurityCenter server must be copied to the Splunk server for full communication to occur between SecurityCenter and Splunk. Refer to Splunk's documentation under "Check the warning messages of Tenable SecurityCenter" at:

http://docs.splunk.com/Documentation/AddOns/released/Nessus/ConfigureModularInput2

From the main Splunk screen, click "Search & Reporting" (or "Search" from the Splunk Add-on for Tenable screen).

splunk>		Administrator V Messages V Settings V Activity V Help V Find
Apps 🌣	Forwarders: Deployment 🙋 🔹	Explore Splunk Enterprise
Search & Reporting	Forwarders by Status Split by Status	
Splunk Add-on for Tenable	Total: 0	

If configured correctly, the "What to Search" portion of the screen has populated with your SecurityCenter data. You can then click "**Data Summary**" for detailed information.

ter search here				All time ~ Q
o Event Sampling V				💡 Smart Mode 🕯
How to Search	What to Search			
If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.	1,967 Events INDEXED	9 months ago EARLIEST EVENT	21 hours ago LATEST EVENT	
Documentation (2) Tutorial (2)	Data Summary	-		
Cooreb History				

Click the "Sources" tab for access to the SecurityCenter scan data.

arch Pivot Reports Ale	Data Summary				×	Se	arch & Reporting
Search	Hosts (1) Sources (1)	Sourcetypes (1)					All time × Q
No Event Sampling V	filter						Smart Mode ~
	Source 0	al	Count 0	Last Update 0			
	scan_result_id:1	al 🗸	4,158	7/28/16 12:17:24.000 PM			
How to Search						J	
If you aren't familiar with searching more, checkout one of the following	g in Splunk, or want to learn Ig resources.	4,158 Events INDEXED		5 days ago EARLIEST EVENT	5 days ago LATEST EVENT		
Documentation 12 Tutoria	112	Data Summa	ry				
Search History							

If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

Nessus

Tenable Nessus prevents network attacks by identifying the vulnerabilities and configuration issues that hackers use to penetrate your network. The Splunk Add-on for Tenable allows a Splunk software administrator to collect Tenable vulnerability scan data from Nessus and SecurityCenter via the REST API. The add-on supports Nessus 6.x, as well as 5.x for backwards compatibility.

This section assumes that the user has working knowledge of Nessus and Splunk, and a working instance of Splunk Enterprise. For information on obtaining and installing Splunk Enterprise, please refer to the Splunk Enterprise Installation Manual.

Integration Requirements

The following are required in order to integrate Tenable Nessus with Splunk:

- Nessus 6.x or 5.x
- Splunk Add-on for Tenable
- Splunk 6.x or higher

Integration Configuration

Splunk Add-on for Tenable Configuration

The Splunk Add-on for Tenable is available for download at http://splunkbase.splunk.com/app/1710 (login required).

From Splunk, click on the Manage Apps "gear" icon, located in the upper-left side of the screen.

splunk>	Administrator V Messages V Settings V Activity V Help V Find
Apps 🌣	Forwarders: Deployment 🙋 🌣
Search & Reporting	Forwarders by Status Split by Status Totel: \$result.count\$
	Waiting for data

Select "Install app from file".

splunk> Apps ~				Admi	inistrator 🗸 Messa	iges ∽ Settings ∽	Activity \sim	Help \sim	Find	
Apps										
										٩
Browse more apps Install a	pp from file Create app									
Showing 1-15 of 15 items	Û							I	Results per page	25 ~
Showing 1-15 of 15 items	Folder name \$	Version ‡	Update checking \$	Visible 🕈	Sharing \$	Status ≑	Actions	I	Results per page	25 🗸
Showing 1-15 of 15 items Name ÷ SplunkForwarder	Folder name +	Version \$	Update checking \$	Visible ≎ No	Sharing \$ App Permissions	Status ÷ Disabled Enable	Actions	1	Results per page	25 🗸
Showing 1-15 of 15 items Name SplunkForwarder SplunkLightForwarder	Folder name ÷ SplunkForwarder SplunkLightForwarder	Version ÷	Update checking + Yes Yes	Visible ≎ No No	Sharing ÷ App Permissions App Permissions	Status ÷ Disabled Enable Disabled Enable	Actions		Results per page	25 🗸
Showing 1-15 of 15 items Name SplunkForwarder SplunkLightForwarder Log Event Alert Action	Folder name ÷ SplunkForwarder SplunkLightForwarder alert_Jogevent	Version \$	Update checking + Yes Yes Yes	Visible ≎ No No No	Sharing ÷ App Permissions App Permissions App Permissions	Status ÷ Disabled Enable Disabled Enable Enabled Disable	Actions Edit proper	ties View ol	Results per page	e 25 v
Showing 1-15 of 15 items Name SplunkForwarder SplunkLightForwarder Log Event Alert Action Webhook Alert Action	Folder name ÷ SplunkForwarder SplunkLightForwarder alert_Jogevent alert_webhook	Version \$	Update checking Yes Yes Yes Yes	Visible \$ No No No No No	Sharing ÷ App Permissions App Permissions App Permissions App Permissions	Status ≎ Disabled Enable Disabled Enable Enabled Disable Enabled Disable	Actions Edit propert Edit propert	ties View ol	Results per page	25 🗸

Click "Browse".

plunk > Apps ~	Administrator v Messages v Settings v Activity v Help v Find
	Upload an app
	If you have a .spl or .tar.gz app file to install, you can upload it using this form.
	You can replace an existing app via the Splunk CLI. 🖆 Learn more.
	File
	Browse No file selected.
	Upgrade app. Checking this will overwrite the app if it already exists.
	Cancel

Select the downloaded Splunk Add-on for Tenable file, and click "Upload".

DIUNK> Apps ~	Administrator v Messages v Settings v Activity v Help v Find
pload app	
льг» орюад арр	
	Upload an app
	If you have a spl or .tar.gz app file to install, you can upload it using this form.
	You can replace an existing app via the Splunk CLI. 😭 Learn more.
	File
	Browse splunk-add-on-for-nessus_500.tgz
	Upgrade app. Checking this will overwrite the app if it already exists.
	Cancel

When Splunk has completed processing, it will require a restart. After restarting and logging back into Splunk, navigate back to "Managing Apps", as described in the first step. You will now see a "Splunk Add-on for Tenable" listed under "Apps". Click the "Launch app" link under "Actions" to the right of the app name.

splunk'> Apps ~					Admin	istrator 🗸 Messa	iges v Settings v Activity v Help v Find
Apps							
							٩
Browse more apps Install	app from file Create app						
Showing 1-16 of 16 items							Results per page 25 🗸
Name \$	Folder name 🕈	Version \$	Update \$	Visible \$	Sharing \$	Status +	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	_
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	Ĵ,
Splunk Add-on for Tenable	Splunk_TA_nessus	5.0.0	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects 🗷 View details on SplunkApps
Log Event Alert Action	alert_logevent	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects

From the "Inputs" screen, select "Create New Input" and click "Nessus".

Spiurik > App. Spiurik Add-on for renable	e 🌱		Administrator V	Messages \sim	Settings 🗸	Activity 🗸	Help 🗸	Find
nputs Configuration Search							Splun	k Add-on for Tenable
Inputs Create data inputs to collect data from Tenable D Inputs Service : All ~	2.	filter						Create New Input ~
Name ^ Serv	vice 0	Interval 🗧	Index 0		Status 🗘		Ac	tions

Fill in the required information and change the Nessus Metrics drop-down to "Nessus Host Scans".

inputs configuration Search		Add Nessus Input		×	
Inputs			Enter a unique name for each nessus input.	^	Create New Input
Freate data inputs to collect data from Te	enable.	Nessus Metrics*	Nessus Host Scans		create New input V
Inputs Service : All ~			Select Nessus Host Scans to collect vulnerabilities discovered on hosts. Select Nessus Plugins to collect plugin information from Tenable Knowledgebase.		
Name ^	Service 0	Nessus Server URL*	https://127.0.0.1:8834	- 11	Actions
Server	Nessus		For example, https://10.10.10.10:8834		Action ~
		Access Key*	••••••	- 11	
			Nessus Access Key generated in the Nessus server.	- 11	
		Secret Key*	,	- 11	
			Nessus Secret Key generated in the Nessus server.	- 11	
		Start Date*	1999/01/01	- 11	
			The add-on starts collecting data with a date later than this UTC time. Default is '1999/01/01'. For	- 11	
			Nessus Host Scans, this value refers to the host scaned date. For Nessus Plugins, this value refers to the last modification date.	- 1	
		Batch Size*	100000	- 1	
			The batch size of events collected during each interval. Default is 100000. 0 means unlimited. Must be 0, or greater than or equal to 1000.	v	
		Cancel		Add	
				_	

The Access Key and Secret Key required from Nessus are located in Nessus under "User Profile" > "API Keys".

Log in to Nessus, and click the down arrow on the right side of the menu bar beside the user name. Next, select "User Profile".

Scans		Upload		User Profile	
				Help & Support	
• New Scan	Scans / My Scans			What's New	
				Sign Out 🛛 📲	
Ay Scans	Name	Schedule	Last Modif	iea 🔺	
irash	discovery	Monthly on day 29 at 2:30 PM	O 12:36 PM	1	-
II Scans	Host Security Sanity Check	On Demand	🗲 April 8		×
Jew Folder	Malware scan	On Demand	10/23/15)	- ×

Click "API Keys".

User Profile		
Back	User Profile / Account Settings	
Account Settings	Username	
Change Password	User Type System Administrator	
Plugin Rules		
API Keys	Save Cancel	

Generate the API keys, and then copy and paste the Access Key and Secret Key from the screen to the Access Key and Secret Key fields of the "Add Nessus Input" screen in Splunk.



In Splunk, click "Add" to complete the action.

sp	App: Splunk Add-on for Te	enable 🗸		Administrator 🗸 🛛 🕅	Messages 🗸	Settings 🗸	Activity 🗸	Help 🗸 🛛 Find	
Inp	uts Configuration Search							Splunk Add-on for	Tenable
In Cre	IPUTS ate data inputs to collect data from Te	nable.						Create New Ir	iput V
2 Ir	nputs Service : All ~		filter						
i	Name ^	Service 0	Interval 0	Index 0		Status 0		Actions	
>	Nessus Host Scans	Nessus	86400	default		Enabled		Action ~	

From the main Splunk screen, click "Search & Reporting" (or "Search" from the Splunk Add-on for Tenable screen).

splunk>		Administrator V Messages V Settings V Activity V Help V Find
Apps 🔹	Forwarders: Deployment 🛛 🔹	Explore Splunk Enterprise
Search & Reporting	Forwarders by Status Split by Status	
Splunk Add-on for Tenable	Total: 0	

If configured correctly, the "What to Search" portion of the screen has populated with your Nessus data. You can then click "**Data Summary**" for detailed information.

arch Pivot Reports Alerts Dashboards				Search & Reporting
Search				
nter search here				All time ~ Q
o No Event Sampling ∽				P Smart Mode ∽
How to Search	What to Search			
If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.	1,967 Events INDEXED	9 months ago EARLIEST EVENT	21 hours ago LATEST EVENT	
Documentation L2 Tutorial L2	Data Summary	•		
Search History				
> Expand your search history.				

Click the "Sources" tab for access to the Nessus scan data.

reh Divet Deports Aler					_	Coorob & Doportin
Search	Data Summary Hosts (1) Sources (3,121) Sourcetypes (1)			>	<	Search & Reportin
nter search here Jo Event Sampling V	(filter)	< Prev	1 2 3	4 5 6 7 8 9 ··· Next>		All time ~ Q
	Source 0	at	Count 0	Last Update 🗅	^	
	https://127.0.0.1:8834/scans/11/hosts/10	al 🗸	18	7/28/16 12:55:30.000 PM		
How to Search	https://127.0.0.1:8834/scans/11/hosts/101	al 🗸	4	7/28/16 12:55:30.000 PM		
If you aren't familiar with searching	https://127.0.0.1:8834/scans/11/hosts/11	al 🗸	6	7/28/16 12:55:30.000 PM		
more, checkout one of the following	https://127.0.0.1:8834/scans/11/hosts/12	al 🗸	18	7/28/16 12:55:30.000 PM		
	https://127.0.0.1:8834/scans/11/hosts/14080	al 🗸	17	7/28/16 12:55:36.000 PM		
Documentation 🖄 Tutorial	https://127.0.0.1:8834/scans/11/hosts/152	al 🗸	3	7/28/16 12:55:30.000 PM		
	https://127.0.0.1:8834/scans/11/hosts/153	al 🗸	3	7/28/16 12:55:30.000 PM		
Search History	https://127.0.0.1:8834/scans/11/hosts/154	al 🗸	5	7/28/16 12:55:31.000 PM		
Search History	https://127.0.0.1:8834/scans/11/hosts/158	al 🗸	5	7/28/16 12:55:31.000 PM		
Expand your search history.	https://127.0.0.1:8834/scans/11/hosts/159	al 🗸	8	7/28/16 12:55:31.000 PM		

If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

Passive Vulnerability Scanner

Tenable PVS eliminates network blind spots by continuously monitoring network traffic in real time to discover active assets, identify cloud applications, and detect anomalous activity. The PVS app for Splunk is able to process tens of terabytes of data per day and find security-relevant information through comprehensive analysis. In order to uncover threats carried on mobile, virtual, and cloud devices, Splunk requires reliable data to analyze. The vulnerability and device discovery power of PVS used with the comprehensive analysis of Splunk provides network and security information for effective threat intelligence.

This section assumes that the user has working knowledge of Tenable PVS and Splunk. To download the Tenable Network Security PVS App for Splunk, see: https://splunkbase.splunk.com/app/1844/.

Integration Requirements

The following are required in order to integrate Tenable PVS with Splunk:

- Tenable Passive Vulnerability Scanner, Version 4.x or higher (including 5.x). To obtain a PVS evaluation, see: http://www.tenable.com/products/passive-vulnerability-scanner/evaluate.
- Splunk 6.x and higher.

Integration Configuration

Tenable PVS Configuration

From the PVS UI, navigate to "Configuration".



🛠 PVS Settings	PVS Settings			
Feed Settings				
Cloud Settings	Setting Type	Monitoring	<u> </u>	
Web Proxy Settings	Monitored Network Interf	Monitoring	^	
Chart Settings		PVS Proxy PVS Web Server		
🖌 Email Settings		Plugins		
/> Plugin Settings		Realtime Events Reports		
Nessus Scanner Settings	Monitored Netwo Addresses and Rar	Session Analysis		

In the "Realtime Syslog Server List", click "**Add**" to enter the IP address and UDP port of the Splunk server and then click "**Add**" to finalize the addition.

Settings		
🕂 Add Sy	log Item	×
Real	172.28.36.205	
Port	514	
Format Type	 Standard CEF 	
Vulr Protocol	● UDP◎ TCP	
Add Can	9	

Select "Syslog" in the "Setting Type" drop-down menu.

Click "**Update**" to complete the process.

PVS Settings	PVS Settings	
Feed Settings		
Cloud Settings	Setting Type Syslog	
Web Proxy Settings	Realtime Syslog Server List 172.28.36.205:514	Add
Chart Settings		Edit
Email Settings		Remove
Plugin Settings	Vulnerability Syslog Server	Add
Nessus Scanner Settings	List	Edit
		Remove
		×

The IP address and UDP port must be entered in the format of "IP:PORT" (e.g., 10.1.1.10:514).

Splunk Configuration

Download the Tenable Network Security PVS App for Splunk from https://splunkbase.splunk.com/app/1844/. Log in to Splunk and click the gear icon next to "Apps".

splunk> Apps 🌣	Explore Splunk Enterprise	Adminis	rator ∨ Messages ∨ Settings ∨ ,	Activity - Help - Find - X
Search & Reporting				
+	Product Tours New to Splunk? Take a tour to help you on your way.	Add Data Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.	Explore Data Explore data and define how Hunk parses that data	Splunk Apps 2 Apps and add-ons extend the capabilities of Splunk Enterprise.
				Close

On the "Apps" screen, click "Install app from file", browse to the Tenable Network Security PVS App for Splunk .tgz file, and click "Upload".

Jpioad an app	
f you have a .spl or .tar.gz app file to install, you can upload it using this form.	
′ou can replace an existing app via the Splunk CLI. 📑 Learn more.	
ïle	
Browse tenable-network-security-pvs-app-for-splunk_102.tgz	
Upgrade app. Checking this will overwrite the app if it already exists.	
Cancel	Upload

The app is now listed and enabled.

Browse more apps Install ap	p from file Create app						
Showing 1-17 of 17 items							Results per page 25 💌
Name ≑	Folder name 🕈	Version ‡	Update ‡ checking	Visible ‡	Shering ‡	Status ‡	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Log Event Alert Action	alert_logevent	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	6.4.2	Yes	No	App Permissions	Enabled	Edit properties View objects
framework	framework		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	
introspection_generator_addon	introspection_generator_addon	6.4.2	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
Tenable Network Security PVS	pvs	1.0.2	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects 🖾 View details on SplunkApps
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	6.4.2	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects 🖪 View details on SplunkApps

In the Splunk UI, navigate to "Settings" > "Data" > "Data Inputs". To the right of "UDP", click "Add new".

splunk> Apps ~	Administrator 🗸	Messages 🗸	Settings 🗸	Activity \sim	Help \sim
Data inputs					
Local inputs					
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and re	ceiving between two	Splunk instanc	es, go to Forwa	arding and rec	eiving.
Туре			Inputs		Actions
Files & directories			5		Add new
Index a local file or monitor an entire directory.					
HTTP Event Collector			0		Add new
Receive data over HTTP or HTTPS.					
тср			0		Add new
Listen on a TCP port for incoming data, e.g. syslog.					
UDP			1		Add new
Listen on a UDP port for incoming data, e.g. syslog.					
			2		Add new
Scripts					

Under "Select Source", select "UDP" and enter "514" for the port. Click "Next".

	Administrator 🗸	Messages 🗸 Settings 🗸 A	Activity 🗸
w Done Next>			
Configure this instance to listen on syslog). Learn More 🖪	any TCP or UDP port to capture	data sent over the network (such a	as
	TCP	UDP	
Port? 5	14 ample: 514		
Source name override? o	ptional st:port		
Only accept connection from?	ptional ample: 10.1.2.3, !badhost.splunk.com, *.c	splunk.com	
	w Done Next>	Administrator V W Done (Next) Configure this instance to listen on any TCP or UDP port to capture syslog). Learn More [3 TCP Port? 514 Example: 514 Source name override? optional host:port Only accept connection from? optional example: 10.1.2.3, !badhost splunk.com, *:	Administrator Messages Settings J W Done Image: Next >> Image

In the "**Input Settings**" screen, click the drop-down for "**Select Source Type**". Under "**Operating System**", select "**syslog**". If not already selected, choose "**Tenable Network Security PVS**" next to "App Context", and select "**IP**" next to "Method".

splunk> Apps ~		Administrator 🗸 🗌	Messages 🗸 Settings 🗸 Activity 🗸 Help 🗸 🛛 Find
Add Data	< Revi	filter	
Select Source Input Settings Review Done		Application	
		Database	
Input Settings		Email	
optionally set additional input parameters for this data input as follows:		Miscellaneous	
Courses have		Network & Security	
Source type The course type is and of the default fields that Splunk acciencits all		Operating System	linux_messages_syslog Format found within the Linux log file
incoming data. It tells Splunk what kind of data you've got, so that		Structured	/var/log/messages
Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.		Web	linux_secure Format for the /var/log/secure file
		Select Source Type 🗸	containing all security related messages on a Linux machine
App context			syslog Output produced by many syslog
Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts	Арр Со	ntext Tenable Network Security PVS \	daemons, as described in RFG3164 by the IETF
improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More [2]			windows_snare_syslog Output produced by the Snare syslog server on Windows
Host			
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More 13	Metl	nod? IP DNS Custo	

Click "Review" to review all changes, and then "Submit" to finalize the configuration.

Select "**Apps**" and "**Tenable Network Security PVS**" in the upper-left corner of the screen to display your initial PVS Dashboard.



If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

Log Correlation Engine

Tenable LCE unifies vulnerability collection and event analysis data through Tenable SecurityCenter, which provides easyto-use dashboards to display multiple data points in a centralized view. Organizations that choose to send Splunk logs to the LCE have a unique advantage in that Splunk data is normalized by LCE and can be included for automatic anomaly detection, asset discovery, and additional vulnerability information, including botnet and malware detection.

The Tenable LCE Splunk Client forwards data that Splunk collects to the LCE server. Once the data reaches the LCE server, the data is reviewed and normalized so it can be queried in SecurityCenter.

Tenable LCE also has the ability to forward any log it receives to one or more syslog servers, including Splunk. Using LCE's Syslog Forwarding and Event Rules features, it can send all, or selected, logs to Splunk Enterprise. Once the logs are received in Splunk, the data can be filtered and queried to produce meaningful dashboards and reports for a more complete view of the enterprise.

This section assumes that the user has working knowledge of Tenable LCE and Splunk, and a working instance of Splunk Enterprise. For information on obtaining and installing Splunk Enterprise, please refer to the Splunk Enterprise Installation Manual.

Integration Requirements

The following are required in order to integrate Tenable LCE with Splunk:

- Log Correlation Engine version 4.8 and higher
- Log Correlation Engine Splunk Client version 4.6 and higher
- Splunk 6.x and higher

Integration Configuration

To configure Splunk Enterprise to forward logs to Tenable LCE, follow the steps in the "Tenable LCE Splunk Client Configuration" and "Splunk Configuration" sections.

For detailed steps on configuring syslog forwarding from Tenable LCE to Splunk Enterprise, see the "Tenable LCE Syslog Forwarding" section.

Tenable LCE Splunk Client Configuration

The LCE Splunk Client is available for download from the Tenable Support Portal at https://support.tenable.com (login required). Log in and navigate to the "Downloads > Log Correlation Engine" section and download the "Log Correlation Engine Splunk Client".

Once downloaded, copy the LCE Splunk Client to the host it will be installed on. The LCE Client can be installed directly onto a Splunk server. For LCE Splunk Client installation tips, refer to the LCE 4.8 User Guide.

After the LCE Splunk Client is installed, log in to the system it is installed on to begin the configuration.



All shell commands need to be executed by a user with root privileges.

To configure the LCE Splunk client, execute the "set-server-ip.sh" script (as shown below). Once prompted, enter the LCE server IP address or hostname and LCE server port (default is 31300). Once the information is updated, the LCE Splunk Client daemon is restarted.

```
# /opt/lce_splunk/set-server-ip.sh
Enter the new desired LCE server IP or host name.
>>
192.168.22.11
Enter the new desired LCE server port [31300].
>>
31300
Updating LCE Server IP from 203.0.113.1 to 192.168.22.11...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Splunk Client daemon [
OK ]
Starting LCE Splunk Client daemon [
OK ]
```

Optionally, you can execute the "set-server-ip.sh" script (as shown below) with the LCE server IP address or hostname and LCE server port as arguments. Once the information is updated, the LCE Splunk Client daemon is restarted.



If you encounter any issues with LCE Client installation or configuration, or have any feature requests for this integration, contact Tenable Support.

Splunk Configuration

After the LCE Splunk Client is installed and configured, the Splunk Indexer has to be configured in order to send data from Splunk to the LCE Splunk Client. That data is then sent from the LCE Splunk Client to the LCE server, where it is normalized before being forwarded on to SecurityCenter.

To begin the Splunk configuration, log in to Splunk Web (http://<IP address or hostname>:8000) as a user with administrator privileges. Once logged in, click "**Settings**" in the top menu bar and select "**Forwarding and receiving**".

splunk>	/app/launcher/home		Administrator	✓ Messages ✓ Settings ✓ Acti	খা চার্ট wity প Help প Find
Apps 🄹 📏 Search & Reporting	Explore Splunk Enterprise		Add Data	KNOWLEDGE Searches, reports, and alerts Data models Event types Tags Fields	DATA Data inputs Forwarding and receiving Indexes Report acceleration summaries
	Product Tours New to Splunk? Take a tour to help you on your way.	Add D Add or forward o Enterprise. Afterward field	Explore Data	Lookups User interface Alert actions Advanced search All configurations Styres Server settings Server settings	Virtual indexes Source types Source types DISTRIBUTED ENVIRONMENT Indexer clustering Forwarder management Distributed search
			Distributed Management Console	Licensing	Access controls
		հվա			

Click "Add new" under the "Configure forwarding" action.

→ C 172.26.37.23:8000/en-US/manager/launcher/forwardreceive	
splunk> Apps ~	Administrator \vee Messages \vee Settings \vee Activity \vee
Forwarding and receiving	
Forward data	
Set up forwarding between two or more Splunk instances.	
	Actions
Forwarding defaults	
Configure forwarding	Add new
Receive data	
Configure this instance to receive data forwarded from other instances.	
	Actions
Configure receiving	Add new

In the "**Host**" box, enter the IP address or hostname and port (default 9800) of the LCE Splunk Client host. Click "**Save**" to finalize the settings.

→ C [] 172.26.37.23:8000/	en-US/manager/launcher/data/outputs/tcp/server/_new?action=edit			9		
splunk> Apps ~		Administrator 🗸	Messages 🗸	Settings ~	Activity ~	Help ~
Add new						
orwarding and receiving	» Forward data » Add new					
	Enter host:port to forward data to. Data will be auto load balanced to each host:port.					
	Host *					
	172.26.37.23:9800					
	Set as host:port or IP:port. You must also enable receiving on this host.					
	Cancel				Si	ave
-			-	-	_	

Once saved, the LCE Splunk Client will be listed in the "Host" list. Verify that the "Status" is set to "Enabled".

Administrator ∨ Messages ∨ Settings ∨	Activity ~ Help
Status ≑	Actions
Enabled Disable	Clone Delete
	Status ÷ Enabled Disable

To finalize the Splunk configuration, log in to the Splunk Indexer as a root user. Once logged in, edit the "outputs.conf" file and add the lines below in bold.



The default location of the outputs.conf file is /opt/splunk/etc/system/local/outputs.conf.

```
[tcpout]
defaultGroup = default
disabled = 0
indexAndForward = 1
[tcpout-server://LCE_IP_OR_Hostname:9800]
[tcpout:default]
disabled = 0
server = LCE_IP_OR_Hostname:9800
sendCookedData = false
```

Save the file, and then restart the Splunk services. Once the services restart, Splunk data is now able to be forwarded to the LCE Splunk Client.

To complete the setup, log in to the web interface of the LCE server previously configured to communicate with the LCE Splunk Client. Once logged in to the LCE server, the following steps will need to be performed:

- Authorize the LCE Splunk Client
- Configure the LCE Splunk Client Policy
- Assign the Policy to the LCE Splunk Client

For detailed instruction on how to perform these steps and finalize the configuration, please refer to the LCE 4.8 User Guide.

Tenable LCE Syslog Forwarding

To configure syslog forwarding from LCE to Splunk, log in to LCE's web interface and navigate to "Configuration".

Health and Stat	tus			
U Service Status	Service	Status	Last Started	Version
Feed	Log Engine	ОК	2016 Aug 04 11:11:00	4.8.0
	Query Interface	ОК	2016 Aug 04 11:10:56	4.8.0
Statistics	Log Indexer	ОК	2016 Aug 04 11:10:53	4.8.0
Data Sansors	Vulnerability Reporter	ОК	2016 Aug 04 11:11:00	4.8.0
	Statistics Engine	ОК	2016 Aug 04 11:11:05	4.8.0
Alerts 8	TASL Engine	OK	2016 Aug 04 11:11:01	4.8.0

Click "Advanced" in the left-hand menu.

🖌 System Configu	uration		
Basic	Server Address		An IPv4 address, i.e. 203.0.113.0 By default LCE listens on all addresses.
O IDS	LCE Client Port	31300	[1-65535] Usually 31300
Load Balancing	UDP Syslog Port	514	[1-65535] Usually 514
	TCP Syslog Port	601	[1-65535] Usually 601
Advanced	Encrypted TCP Syslog Listen Port	6514	[1-65535] Usually 6514
Control	SNMP Port	162	[1-65535] Usually 162
Feed Settings	Include Networks		A series of IPv4/CIDR filters: 203.0.0.0/16 192.0.2.0/24 A single IP address:

Scroll down until you reach the "Data Forwarding" section and enter the IP address or hostname of the Splunk server, the port number, and the format flag (e.g., 172.26.37.23:601,2 as shown in the screenshot below) in the "Syslog Forwarding TCP" section. The format flag can be set as 0 (include LCE header text), 1 (exclude LCE header text), or 2 (CEF format).

Tenable recommends using format flag "2", which sends the logs to Splunk in the Common Event Format (CEF), and prevents having to create new parsing rules. To use this format, download the "Splunk CEFUtils Add-on" from SplunkBase (login required) and install it on your Splunk Enterprise instance. Installation and configuration instructions are included on the download page.

🗲 System Configur	ration				
	Data Forwarding				
 Storage IDS Load Balancing 	Syslog Forwarding	203.0.111.50:514,1		LCE will Each line (IP or ho The defa The form 0 - inclu 1 - exclu 2 - CEF f	forward all events to these UDP servers. e should be: istname}[port,format_flag] ult port is 514. nat flag may be: de LCE header text de LCE header text format, version 0
Advanced	Syslog Forwarding TCP	172.26.37.23:601,2	1	LCE will Each line	forward all events to these TCP servers. • should be:
Control			-	{IP or ho The defa The form	stname}[port,format_flag,ASCII delimiter] ult port is 601. nat flag may be:
Feed Settings				0 - inclu 1 - exclu 2 - CEF f	de LCE header text ide LCE header text format, version 0

After entering the Splunk server information, scroll to the bottom of the window and click "Update" to save changes.

Note: While Splunk Enterprise can be configured to accept syslog data on any TCP or UDP port, Splunk recommends using TCP. The default TCP port is 610, but can be changed to a different port that suits your environment. Please refer to the "<u>Getting Data In</u>" document by Splunk for more details.

LCE can also be configured to send only selected events to Splunk through the use of "Event Rules". "Event Rules" are located in the "Advanced" section of the "Configuration" menu.

In the example below, the "Event Rule" is set to filter on the sensor name "TASL". Once the rule is applied, LCE will only send those related events to Splunk.

🗲 System Configu	uration		
Basic	TASL Parameters		Advanced TASL parameters can be entered nere.
Generation Storage	Event Rules		
O IDS	Event Rules	Name: <u>tasl_only_rule</u> +Sensors: <u>TASL</u>	Event rules can be used to enable alerts for specific conditions or ignore events that meet some criteria.
Load Balancing		<u>CEF</u> : 192.168.111.221: -port 514	
Advanced	Debugging		
Control	Write Unnormalized Logs	0	Deprecated - users are encouraged to instead enable "Store Unnormalized Logs" above. If non-zero, this is the number of
Feed Settings			unnormalized logs to write to the rolling notmatched.txt file in the database directory.
	Save All Logs File	/fully/qualified/filename.txt	Deprecated - this should be enabled temporarily for debugging

For more detailed instructions on creating "Event Rules", refer to the LCE 4.8 User Guide.

If you encounter any issues with Splunk installation or configuration, or have any feature requests for this integration, contact Splunk Support.

About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.