Revised: September 9, 2025

Integrate Cisco Cyber Vision with Splunk

Visualize Cisco Cyber Vision data with Splunk

Cisco Cyber Vision extends Security Operation Centers to the OT domain. This extension helps you unify security across IT and OT, which protects your enterprise network more effectively. Splunk is Cisco's tool for consolidating event logs across both IT and OT. It is also a leader in the SIEM market.

Cisco solutions such as Cyber Vision, Secure Equipment Access, Secure Firewalls, and Identity Services Engine can share data with Splunk. Non-Cisco products can also integrate and share data. Splunk provides a unified view across all domains. It can also correlate events to better detect advanced threats.

Splunk's Security Orchestration, Automation and Response (SOAR) engine lets you build sophisticated automation to remediate threats. Integrate Cyber Vision with Splunk for real-time views of large data sets to better detect and respond to threats and vulnerabilities.

Benefits

Real-time monitoring of data at scale

Splunk excels at processing and analyzing large volumes of data in real time. When integrated with Cyber Vision, you can view OT and IT security, event, and syslog data instantly.

Custom dashboards

The Cyber Vision application on Splunk offers custom dashboards to focus on specific Cyber Vision data such as operational summaries, security insights, and syslog overviews.

Seamless integration with Cisco solutions

Splunk supports out-of-the-box integration with many Cisco solutions. This capability reduces setup complexity and allows you to work with data in a manner that suits your requirements.

Cyber Vision apps in Splunk

To enable data transfer between Cyber Vision and Splunk, you must install and configure two apps in your Splunk Enterprise portal.

You must first install and configure the Cisco Cyber Vision Splunk Add-On. Next, install the Cisco Cyber Vision Splunk App.

Cisco Cyber Vision Splunk Add-On

The Cyber Vision Splunk Add-On app allows Splunk to receive data from Cisco Cyber Vision using Cisco Cyber Vision RESTful APIs. With this app, Splunk:

- Receives data related to devices, vulnerabilities, activities, and events from Cyber Vision.
- Transforms the received data into a format that can be leveraged by the Cyber Vision Splunk App. The data can also be used with other Splunk products such as Asset and Risk Intelligence and Enterprise Security.

Cisco Cyber Vision Splunk App

The Cisco Cyber Vision Splunk App delivers three custom dashboards that allow you to focus on data that matters most to your organizational role and typical requirements.

Dashboard name	Use the dashboard to view
Operational Summary	Operational events, asset summaries, top protocols used, and top talkers identified.
Security Insights	Asset security events and vulnerabilities.
Syslog Overview	Syslog security and operational events.

Prerequisites

Licensing requirements

System	Minimum license required
Cisco Cyber Vision	Advantage
Splunk	Ingest license Data volumes for your network determine the Splunk Ingest license you need.

System requirements

System	Minimum supported version
Cisco Cyber Vision	5.1.0
Splunk	9.1.x

Port requirements

If your deployment includes firewalls, you must configure certain port accesses. Define the ports in relevant configurations for both Splunk and Cyber Vision Center systems.

Port	Communication requirement
TCP 443	API communications between Splunk and Cyber Vision Center, initiated by Splunk.
TCP, TCP+TLS, or UDP. **No recommended port number.**	Syslog communications from Cyber Vision Center to Splunk.

Getting started

For instructions on installing Splunk Enterprise on Linux, macOS or Windows systems, see the official Splunk documentation.

Set up HTTPS access

After you install Splunk Enterprise, the first login typically uses an HTTP URL. At first login, enable HTTPS for Splunk Web by carrying out these steps:

Step 1 In your Splunk Enterprise portal, go to **Settings** > **System** > **Server settings**.

Step 2 In the **Splunk Web** area, in the **Enable SSL (HTTPS) in Splunk Web** field, click **Yes**.

Install Cyber Vision apps

Step 1 From the Splunk Enterprise main menu, choose **Apps**.

Step 2 Click **Find more apps**.

Step 3 In the search field, enter **Cisco Cyber Vision**.

Step 4 To download the Cisco Cyber Vision Splunk App and Cisco Cyber Vision Splunk Add-On apps, click **Install** on the relevant selections.

Step 5 For each app, follow the instructions displayed on the screen. You must validate your Splunk credentials and complete the installations.

The **Apps** left pane displays the apps when the installations are successful.

Configure data share between Cyber Vision and Splunk

Connecting Cyber Vision center and Splunk involves multiple steps:

- Generate an API token in Cyber Vision Center.
- Configure a certificate verification method for the Cyber Vision and Splunk connection.
- Add an account to Cisco Cyber Vision Splunk Add-On
- Add input methods for the account.

Generate an API token in Cyber Vision Center

Step 1 In Cyber Vision Center, choose **Admin** > **API** > **Token**.

Step 2 To create an API token:

a) Enter a name for the token.
b) Click the **Status** button to enabled state.
c) (Optional) Set an expiry date for the token.
d) Click **Create**.

Step 3 In the **Token**, click the copy to clipboard icon for the newly added API token to view or copy the token.

(Optional) Disable certificate verification for app

You can choose to connect Cyber Vision Center with Splunk without a certificate validation step. This method is recommended for non-production environments such as test or proof-of-concept networks.

Disable certificate verification requirement using the Splunk command line tool.

Splunk stores installed apps in the /opt/splunk/etc/apps directory.

To edit the necessary files, you need sudo or root access to the directory.

Step 1 Using the Splunk CLI tool, access Cisco Cyber Vision app files.

Example:

```
root@splunk:~# cd /opt/splunk/etc/apps/TA-cisco_cybervision/bin/
```

Step 2 Edit the Cyber Vision Utils Python file

Example:

```
root@splunk:/opt/splunk/etc/apps/TA-cisco_cybervision/bin# vi TA_cisco_cybervision_utils.py
```

Step 3 Change `VERIFY_SSL = True` to `VERIFY_SSL = False`.

Step 4 Save the changes to the Python file, then exit the directory.

(Optional) Use Self-Signed Certificates from Cyber Vision Center

Step 1 In a web browser, enter **https://<*Center IP address*>.ca.pem**

Step 2 Copy the contents of the certificate for use in the Splunk account creation task.

Add Account to Cisco Cyber Vision Splunk Add-On

In this task, you must choose a certificate verification method.

- If you don't want to use certificate verification, refer to (Optional) Disable certificate verification for app, on page 3.
- To use a self-signed certificate, refer to (Optional) Use Self-Signed Certificates from Cyber Vision Center, on page 4.
- To use a CA-signed certificate, generate a signed certificate from a certificate authority of your choice. CA-signed certificates are typically the most secure option, and are recommended for most production networks.

Step 1 From the **Apps** menu, choose **Cisco Cyber Vision Splunk Add-On**.

Step 2 Select **Configuration**.

Step 3 Click **Add**.

Step 4 To add an account:

a) Enter a unique name for the account.
b) Enter the Cyber Vision Center FQDN.
c) Enter the API token you generated in the Generate an API token in Cyber Vision Center task.
d) To use certificate verification, check the **Use Custom CA Certificate** check box.
e) In the **Custom CA certificate** text field, enter the contents of the Center's self-signed or CA-signed certificate.
f) Click **Add**.

The Cyber Vision Center is listed in the **Account** section of the **Configuration** page.

If you encounter certificate verification errors, check if DNS server resolution is configured accurately in Splunk.

Add inputs to Splunk

Add input types to Splunk to specify the data to import from Cisco Cyber Vision. You can configure these input types:

- Cyber Vision Events
- Cyber Vision Devices
- Cyber Vision Flows
- Cyber Vision Activities
- Cyber Vision Vulnerabilities

Repeat this task for each input type you want to configure.

Step 1 From the **Apps** menu, choose **Cisco Cyber Vision Splunk Add-On**.

Step 2 Select **Inputs**.

Step 3 From the **Create New Input** drop-down list, choose the input type you want to configure and enter the following details:

a) Enter a name for the input type.

b) Enter an interval in seconds for input retrieval.

Start with a long interval that spans several hours. Update the interval value when deployment activity changes or when your requirements change.

c) Enter an index value to specify a repository location. The Splunk Search feature uses the index value for efficient search and retrieval.

d) In the **Global Account** field, choose the Center from which to gather inputs.

e) Enter a start date. The start date only applies to the first time information is retrieved from the connected Cyber Vision Center.

For subsequent data pulls, the start date is not used. Only new data from the configured interval is retrieved.

Add syslog data source in Splunk

Step 1 From the Splunk main menu, choose **Settings** > **Data** > **Data inputs**.

Step 2 From the **Local inputs** section, select the protocol you want to use, and click **Add new**.

Step 3 Enter a port number. You must use the same port number in the syslog configurations in Splunk and in Cisco Cyber Vision Center.

Step 4 Click **Next** at the top of the page.

Step 5 Configure the input settings:

a) From the **Source type** drop-down list, choose **cisco:cybervision:syslog**.

b) From the **App context** drop-down list, choose **Cisco Cyber Vision Splunk Add-On**.

c) In the **Host** field, choose **IP**.

d) In the **Index** field, choose **Default**.

e) Click **Review**.

Step 6 To add the data input method, click **Submit**.

(Optional) Define Syslog port using Splunk CLI

If you prefer to configure the syslog port for Splunk using CLI, carry out the steps of this task. Alternatively, use the **Port** field in the Add syslog data source in Splunk, on page 5 task to define the syslog port.

Step 1 Log into the Splunk command line tool.

Step 2 Access the inputs configuration file. An example of a typical inputs file path is `<splunk-home>/etc/system/local/inputs.conf`.

Step 3 Add the port configuration details to the configuration file. Here is an example of a TCP+TLS port configuration.

Example

```
[tcp-ssl:6514]
disabled = false
serverCert = /opt/splunk/etc/certs/<cert-file-name>.pem
sslRootCAPath = /opt/splunk/etc/certs/ca.pem
sslPassword = <passphrase of the private key generated above>
```

Add syslog configuration in Cyber Vision Center

Step 1 From the Cyber Vision Center main menu, choose **Admin** > **System**.

Step 2 In the **Syslog Configuration** area, click **Configure**.

Step 3 In the **Protocol** and **Port** fields, enter the same values that you used in the Splunk syslog configuration.

Step 4 In the **Host** field, enter the address of the Splunk instance to connect to.

Step 5 Select a CEF syslog format to apply.

Step 6 Click **Save Configuration**.

Cyber Vision dashboards and source APIs

If the Cisco Cyber Vision Splunk Add-On app is configured correctly, it retrieves inputs from connected Cyber Vision centers. The gathered data is displayed in three dashboards in Cisco Cyber Vision App for Splunk.

To view the dashboards, from the **Apps** menu, choose **Cisco Cyber Vision App for Splunk**.

Table 1: Dashboard elements and the APIs that fetch the required data

Dashboard	Dashboard element	Input used (API)
Operational Summary	Events Distribution By Severity Over Time	Events
	Events By Severity	Events
	Severity - * By Type	Events
	Events Of Type - *	Events
	Devices Details	Devices
	Top 10 Protocols	Activities
	Top 10 Talkers	Flows
Security Insights	Events Distribution By Severity Over Time	Events
	Events By Severity	Events
	Top 10 Vulnerabilities	Devices

Dashboard	Dashboard element	Input used (API)
Syslog Overview	All	Syslog

Using Splunk search app

The Splunk search app allows you to search for particular data, save reports, and create custom dashboards. For information on how to effectively use the search app, see the official Splunk documentation.

Figure 1: Example of a data search in Splunk