Guide Cisco public

cisco
The bridge to possible

Cisco Catalyst SD-WAN Splunk Integration

User guide

Contents

Introduction

Cisco SD-WAN and ZBFW

A software-defined wide area network
(SD-WAN) is a virtualized service that connects and extends enterprise networks over large geographical distances. Cisco SD-WAN provides unparalleled visibility across WAN, optimal connectivity for end users, and the most comprehensive security platform to harden the network.
The Cisco Zone-Based Firewall is the successor of the Classic IOS firewall or CBAC (Context-Based Access Control). It primarily deals with the security "zones". We can assign router interfaces to various security zones and control the traffic between them. The firewall dynamically inspects traffic passing through zones.

Cisco SD-WAN Splunk Integration

Cisco SD-WAN Splunk Integration will have 2 components:

- Cisco SD-WAN Add-on for Splunk
- Cisco SD-WAN App for Splunk

Cisco SD-WAN Add-on for Splunk

Add-ons are used for data optimization and collection processes. Cisco SD-WAN Add-on for Splunk collects different types of Cisco logs Data and Netflow Data and stores them into Splunk indexes.

Cisco SD-WAN App for Splunk

The Cisco SD-WAN App will present dashboards for different types of Cisco Logs and NetFlow Data. The app is used for visualization, analysis, and representation. The dashboard will use the data collected by the Add-on.

Contents

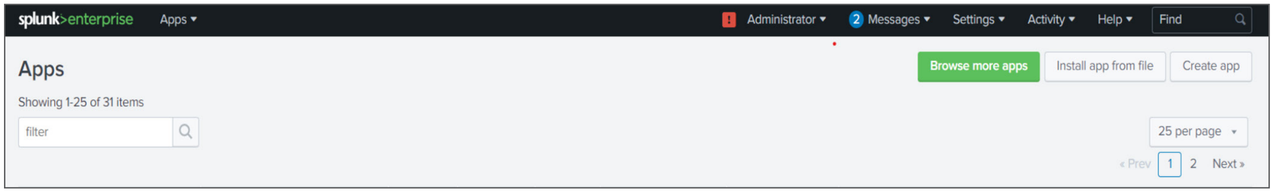
Pre-Requisites

- Install Splunk App for Stream and Splunk Add-on for Stream Forwarders in the Splunk instance to collect the NetFlow (v9) data.
- Make sure that the receiver UDP port (Ex. 4739) is open and bypass the firewall traffic.

Installation and configuration of Cisco SD-WAN

The Add-on and App can be installed in two different ways:

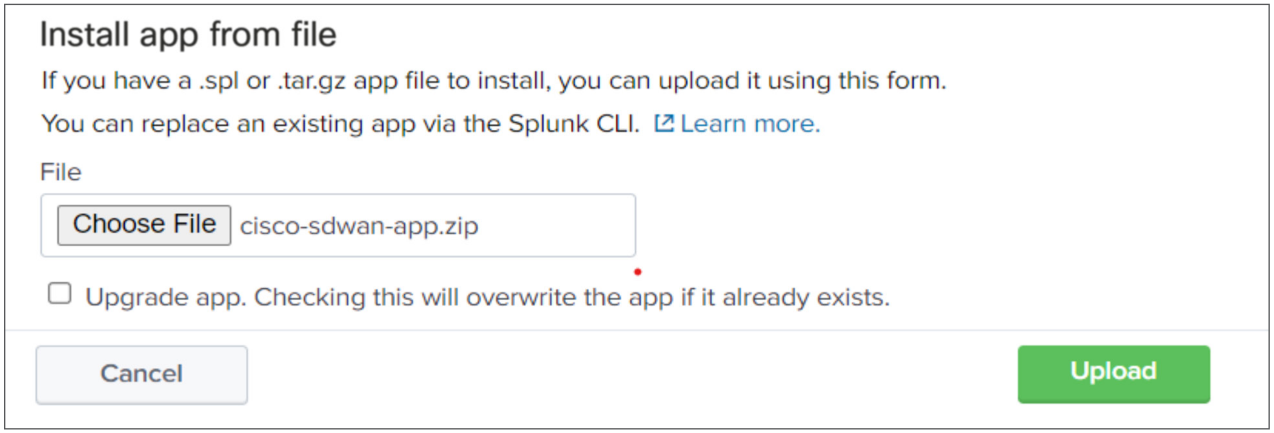
- Through the Splunk user interface from **Apps > Manage Apps > Install the app from file**. Upload the downloaded file.



Apps

Showing 1-25 of 31 items

- By extracting the compressed file (<>-xx-x.x.x-x.tar.gz) into the $SPLUNK_HOME$/etc/apps folder.



Install app from file

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

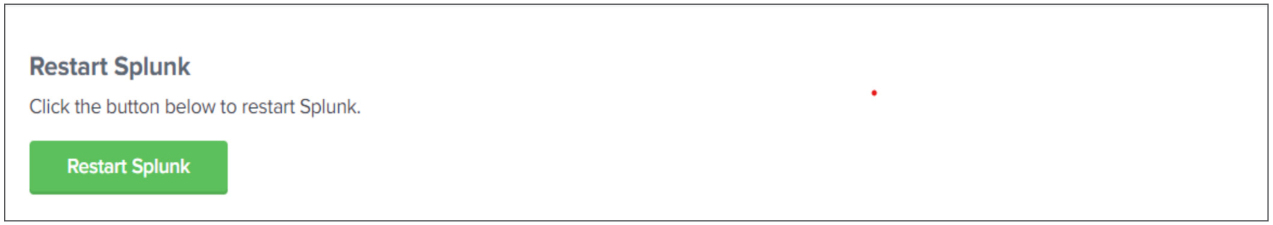
You can replace an existing app via the Splunk CLI. Learn more.

File: cisco-sdwan-app.zip

□ Upgrade app. Checking this will overwrite the app if it already exists.

Contents

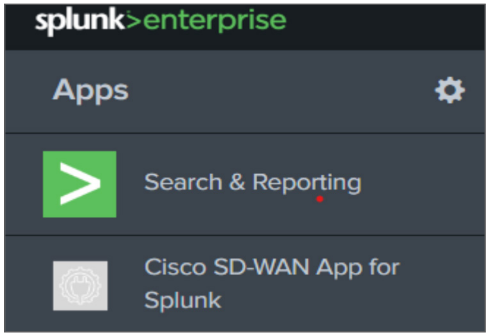
- **Note:** Splunk restart is required after App and Add-on installation.



Restart Splunk

Click the button below to restart Splunk.

- Once you log in under Splunk, click on **Cisco SD-WAN App For Splunk** on the left side of the screen.



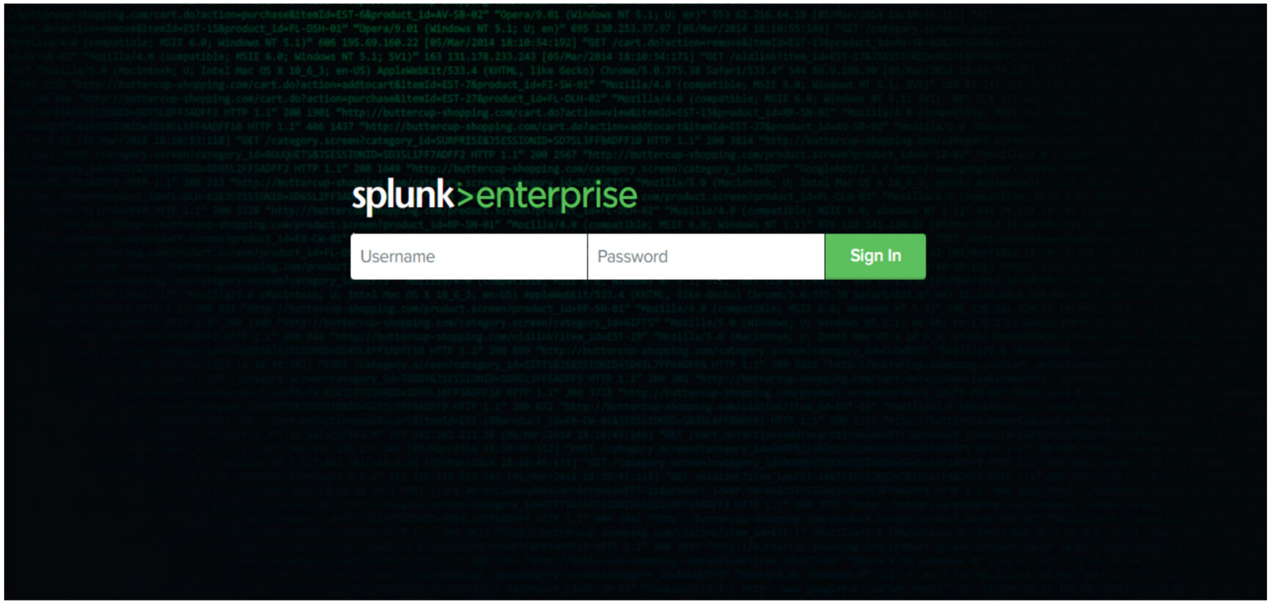
Add-on configuration

Configure Inputs on Splunk for Syslog Data:

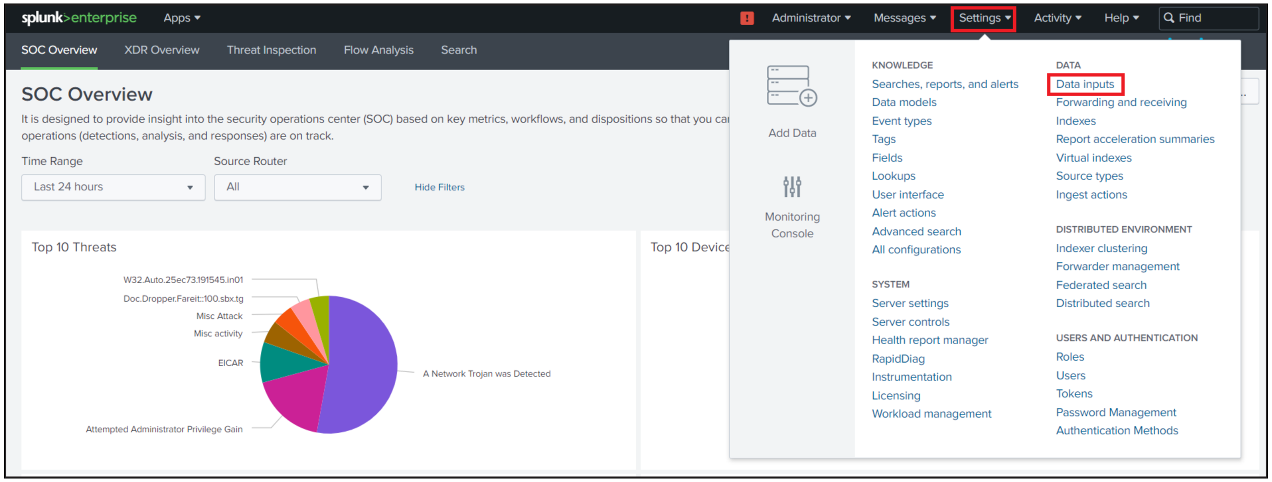
The “Cisco SD-WAN Add-on for Splunk” manages inputs through TCP/UDP inputs provided by Splunk. To configure inputs:

Contents

1. Login to Splunk WEB UI.



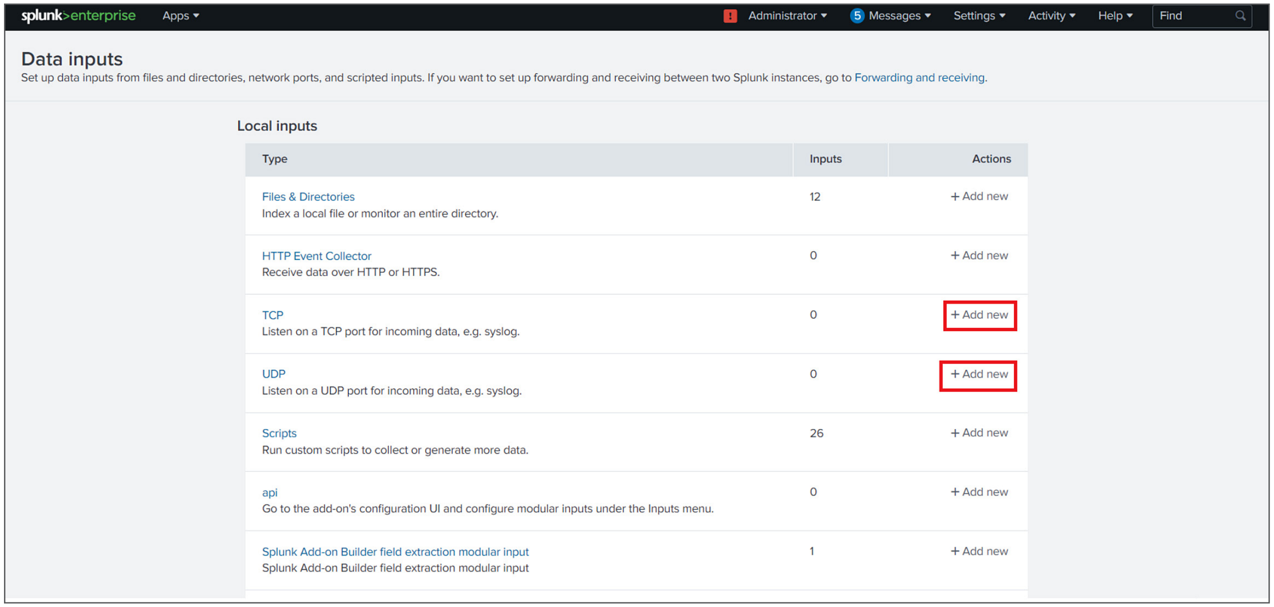
2. Navigate to Settings > Data inputs.



It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you ca operations (detections, analysis, and responses) are on track.

Contents

3. Choose TCP or UDP and click New.



Data inputs

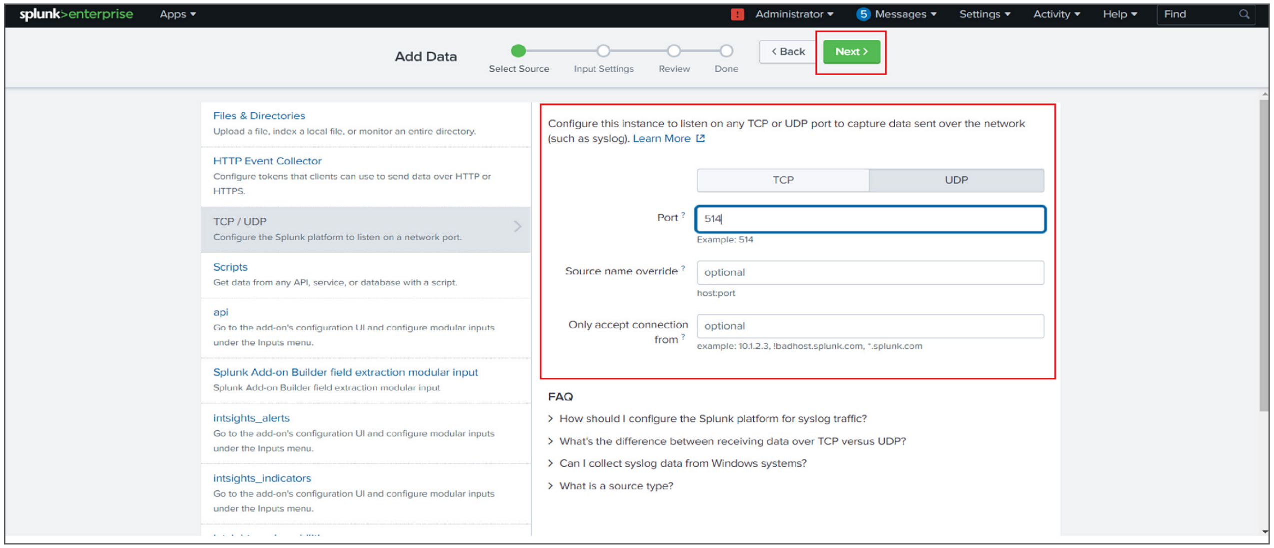
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Local inputs

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	12	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Scripts Run custom scripts to collect or generate more data.	26	+ Add new
api Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.	0	+ Add new
Splunk Add-on Builder field extraction modular input Splunk Add-on Builder field extraction modular input	1	+ Add new

4. In the left pane, click TCP/UDP to add an input.
5. Click the TCP or UDP button to choose between a TCP or UDP input.
6. In the Port field, enter a port number on which you are forwarding the logs from Cisco SD-WAN.
7. In the Source name override field, enter a new source name to override the default source value, if necessary.
8. Click Next to continue to the Input Settings page.

Contents



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

api
Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.

Splunk Add-on Builder field extraction modular input
Splunk Add-on Builder field extraction modular input

intsights_alerts
Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.

intsights_indicators
Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

TCP | UDP

Port ? 514
Example: 514

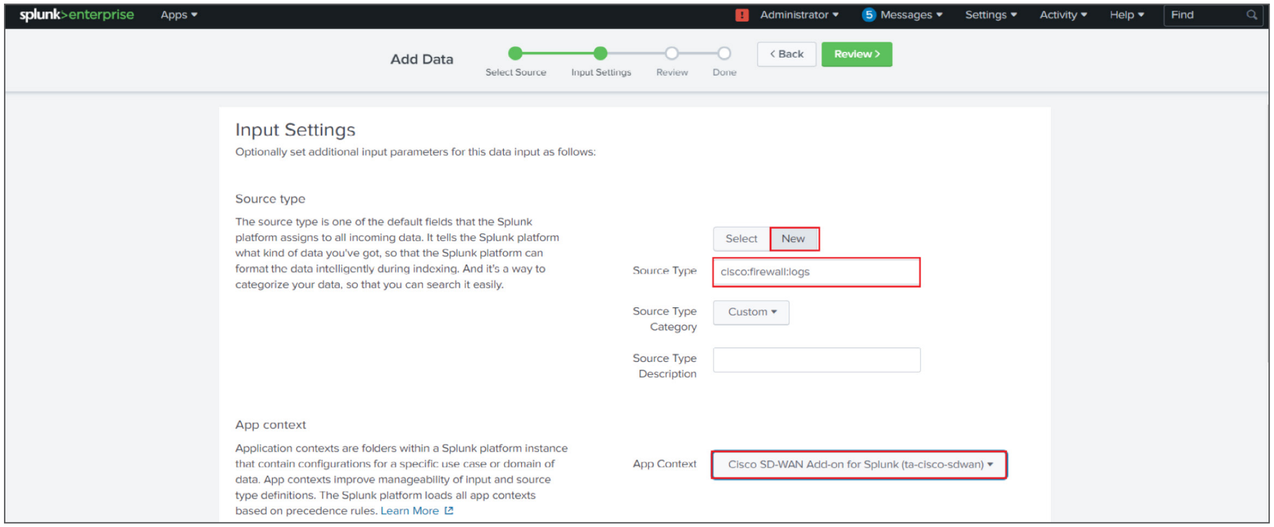
Source name override ? optional
host:port

Only accept connection from ? optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

FAQ
- › How should I configure the Splunk platform for syslog traffic?
- › What's the difference between receiving data over TCP versus UDP?
- › Can I collect syslog data from Windows systems?
- › What is a source type?

9. Set the sourcetype as cisco:firewall:logs.

10. Set App context to Cisco SD-WAN Add-on.



Input Settings
Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select | New

Source Type: cisco:firewall:logs

Source Type Category: Custom ▾

Source Type Description:

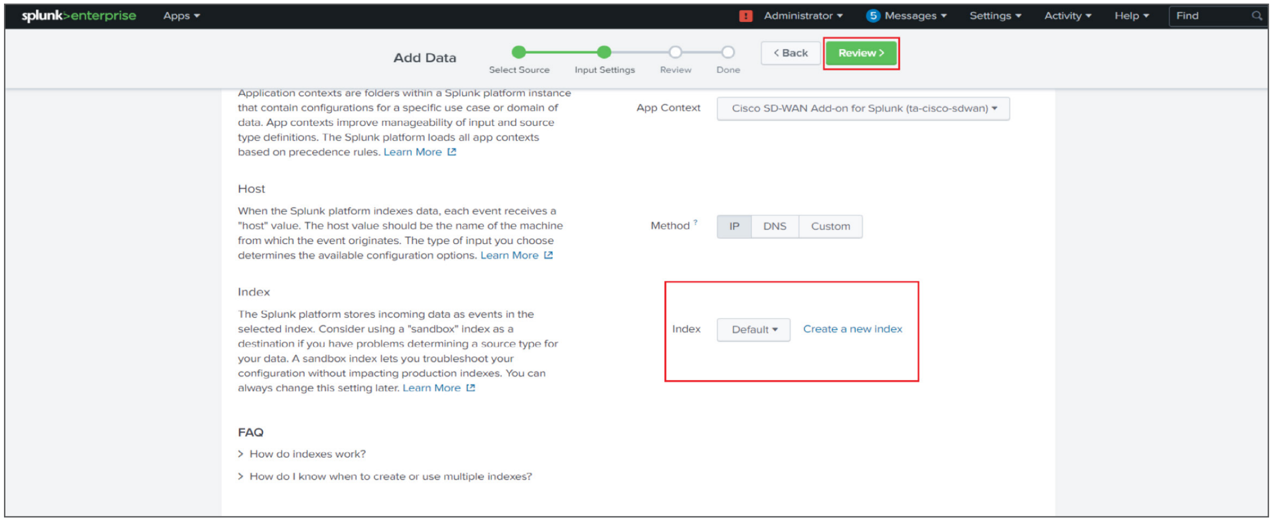
App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Cisco SD-WAN Add-on for Splunk (ta-cisco-sdwan) ▾

Contents

11. Set the Index that Splunk Enterprise should send data to for this input.

12. Click Review.



Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Cisco SD-WAN Add-on for Splunk (ta-cisco-sdwan)

Host

When the Splunk platform 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

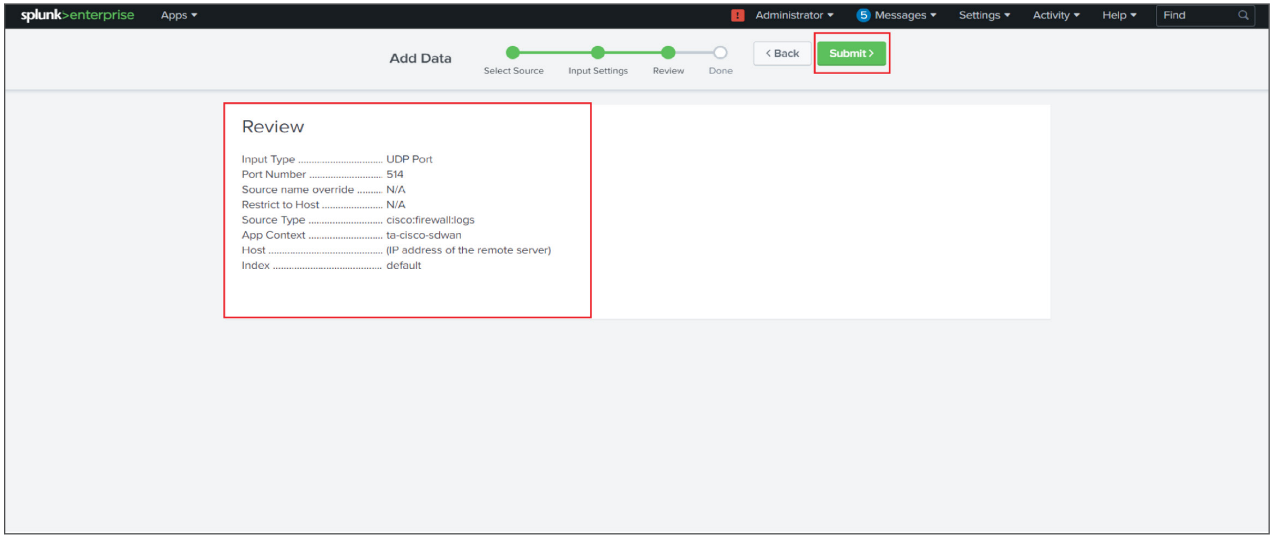
Method: IP | DNS | Custom

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default | Create a new index

13. Click Submit once you have ensured that everything is correct.



Review

```
Input Type ............................ UDP Port
Port Number .......................... 514
Source name override ......... N/A
Restrict to Host ..................... N/A
Source Type ........................... cisco:firewall:logs
App Context ........................... ta-cisco-sdwan
Host ........................................ (IP address of the remote server)
Index ....................................... default
```

Once the input is configured, execute the following query to see if Syslog events are being received.

index=<configured_index> sourcetype=”cisco:sdwan”

Configure inputs on Splunk for NetFlow data

Steps to follow:

1. Once the “Splunk App for Stream” & “Splunk Add-on for Stream Forwarders” is installed in the desired Splunk Instance.
2. Open “Splunk App for Stream” > Click on “Configuration” > Click on “Configure Streams”
3. In the “Search” filter search for the keyword “netflow”.
4. For “netflow” stream > Goto “Action” > “Edit”
5. Update the “Mode” to “Enabled” & select the desired index, by default “main” will be selected.
6. Click on Save.
7. SSH into the Destination VM example VM: x.x.x.x (should be replaced with the VM in which data is been collected)
8. Goto Location: $SPLUNK_HOME/etc/apps/Splunk_TA_stream/local

Contents

9. Create a “streamfwd.conf” in the “local” folder Sample format of ‘streamfwd.conf’ as below:

```
[streamfwd]
netflowReceiver.<N>.ip = <ip_address>
netflowReceiver.<N>.port = <port_number>
netflowReceiver.<N>.decoder = <flow_protocol>
```

Below is an example file for the ip x.x.x.x and port 4739:

```
[streamfwd]
netflowReceiver.0.ip = x.x.x.x
netflowReceiver.0.port = 4739
netflowReceiver.0.decoder = netflow
```

10. Save the changes.

11. All the NetFlow events will get ingested in the Destination VM: x.x.x.x (should be replaced with the VM in which data is been collected)

12. Verify the ingestion of events by using the following query from the “Destination VM: x.x.x.x” (should be replaced with the VM in which data is been collected)

    - index=”<desired index name>” sourcetype=”stream*”

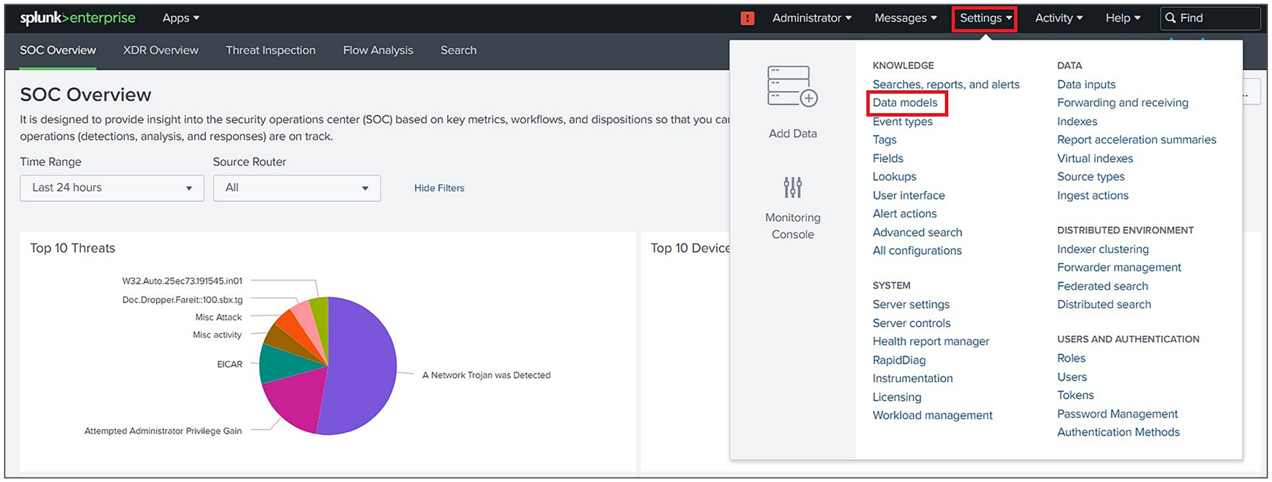
Note: Refer to the documentation for setting up a new NetFlow stream.

Contents

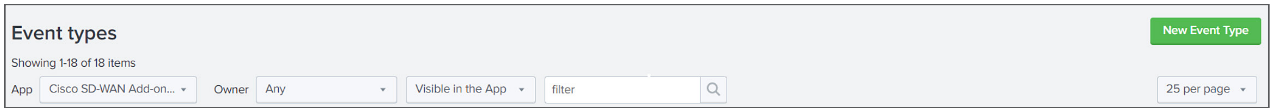
Configure Event Types on Splunk Search Head Instance

To use the CIM mapped fields, a user first needs to configure the event type to provide the index in which the data is being collected. To configure event type:

- Navigate to Settings > Event types.



- Select "Cisco SD-WAN Add-on for Splunk" from the App dropdown.

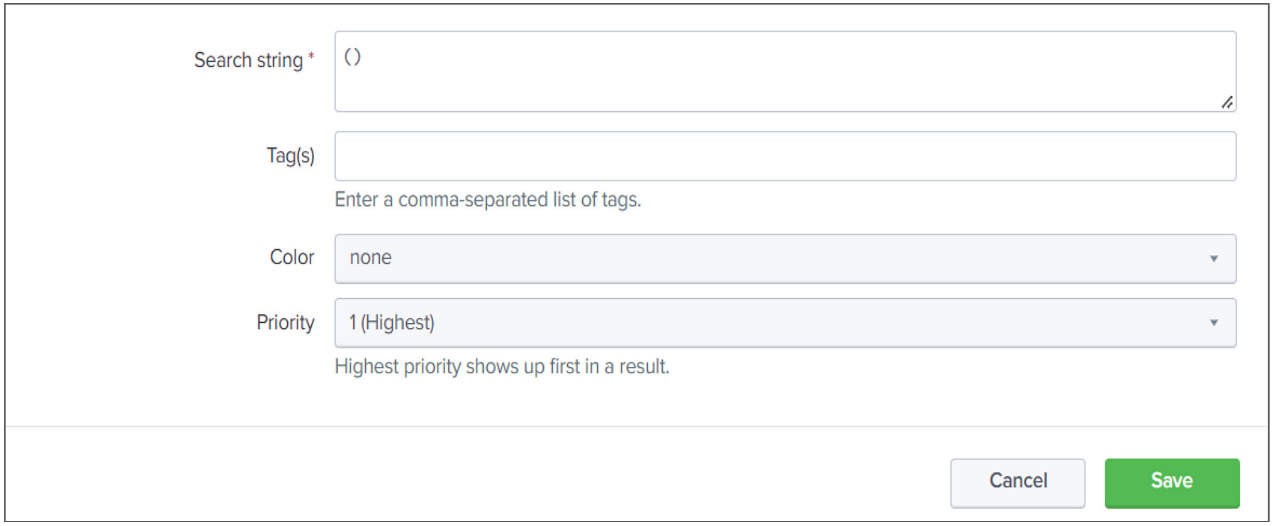

Event types

Showing 1-18 of 18 items

App: Cisco SD-WAN Add-on... Owner: Any Visible in the App filter 25 per page

- Click on "cisco_sdwan_index".

- Update "()" with "index=<your_configured_index>" in the existing definition to use your configured index.



Search string * ()

Tag(s)

Enter a comma-separated list of tags.

Color none

Priority 1 (Highest)

Highest priority shows up first in a result.

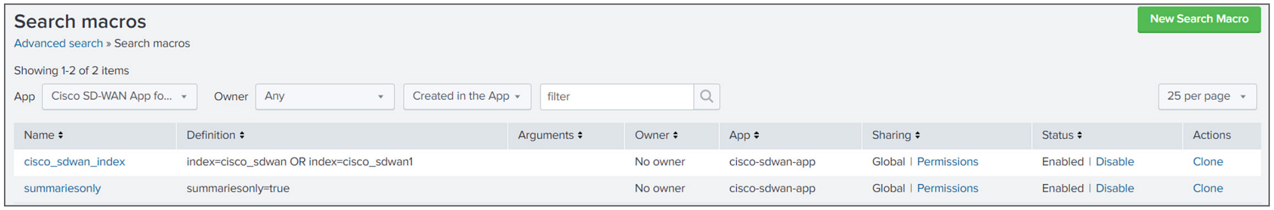
- Click Save.

Data searching

Macros

- Cisco_sdwan_index
  - If you are using a custom index in Add-on for data collection then kindly update the "cisco_ sdwan_index" macro in the app.
- Summariesonly:
  - If you want to visualize only accelerated data then change this macro to "summariesonly=true", the Default value of the macro is "summariesonly=false"
- nataddress_regular:
  - Definition for the extracted NAT addresses to convert them to ipv4 addresses.
- nataddress_datamodel:
  - Definition for the extracted NAT addresses to convert them to ipv4 addresses in datamodel.

Contents



Search macros

Advanced search » Search macros

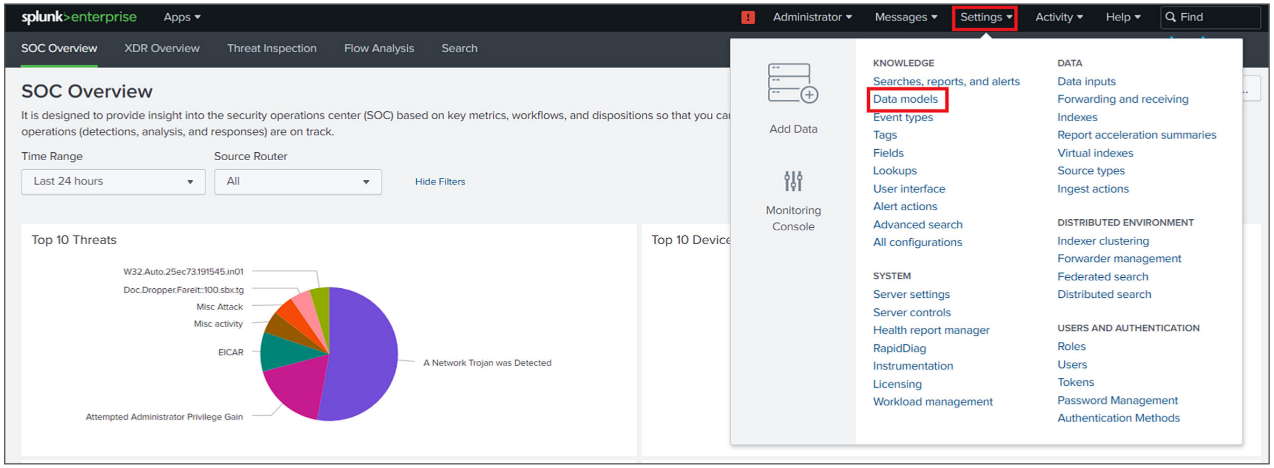
Showing 1-2 of 2 items

App: Cisco SD-WAN App fo... Owner: Any Created in the App filter 25 per page New Search Macro

Name	Definition	Arguments	Owner	App	Sharing	Status	Actions
cisco_sdwan_index	index=cisco_sdwan OR index=cisco_sdwan1		No owner	cisco-sdwan-app	Global | Permissions	Enabled | Disable	Clone
summariesonly	summariesonly=true		No owner	cisco-sdwan-app	Global | Permissions	Enabled | Disable	Clone

Data model

- The Cisco SD-WAN Splunk Application consists of two data models, “Cisco SDWAN” for syslog data and “Cisco SDWAN Netflow” for NetFlow data:
  - Cisco_SDWAN - Maps Syslog data based on different log types.
  - Cisco_SDWAN_NETFLOW - Maps NetFlow data from Cisco SDWAN.
- The acceleration for the data model is disabled by default.
- As all the dashboards are populated using data model queries and real-time search doesn’t work with the data model, all the real-time search filters are disabled.
- If you want to improve the performance of dashboards, you just need to enable the acceleration of the data model. Please follow the below steps:
  - On the Splunk menu bar, click Settings -> Data models.



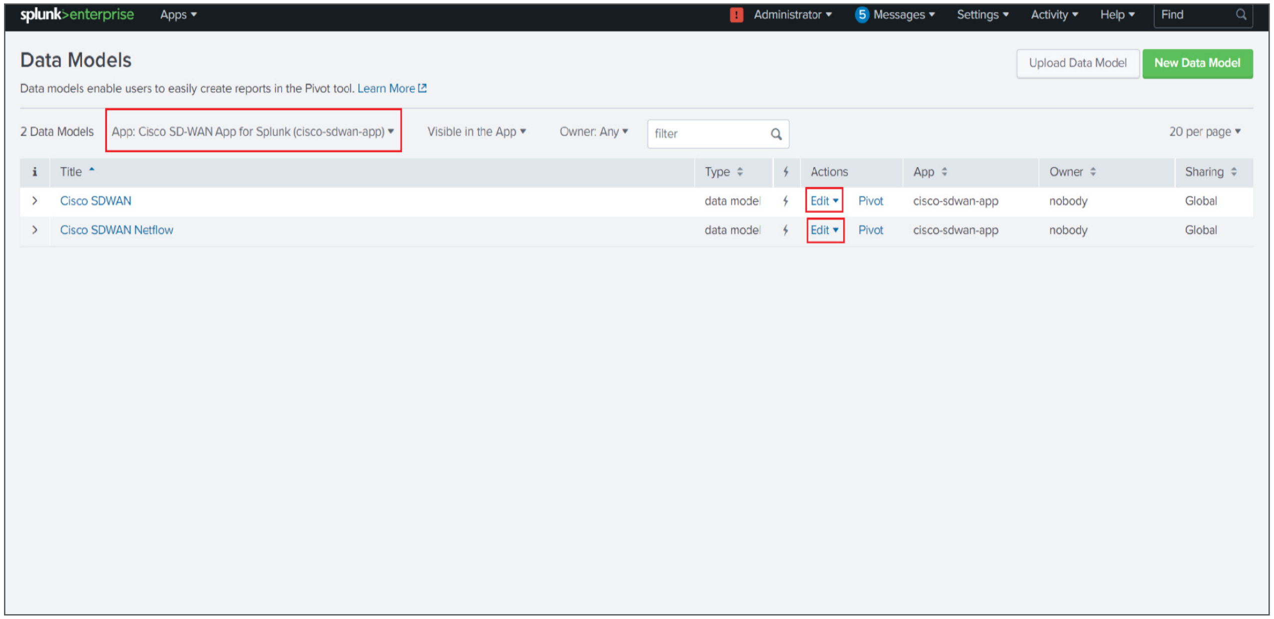
SOC Overview

It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you ca operations (detections, analysis, and responses) are on track.

Time Range: Last 24 hours
Source Router: All

Contents

- Select “Cisco SDWAN App for Splunk” in the “App” context dropdown.
- In the “Actions” column, click on Edit and click Edit Acceleration for the “Cisco SDWAN” Data model. This will display the pop-up menu for Edit Acceleration.



Data Models

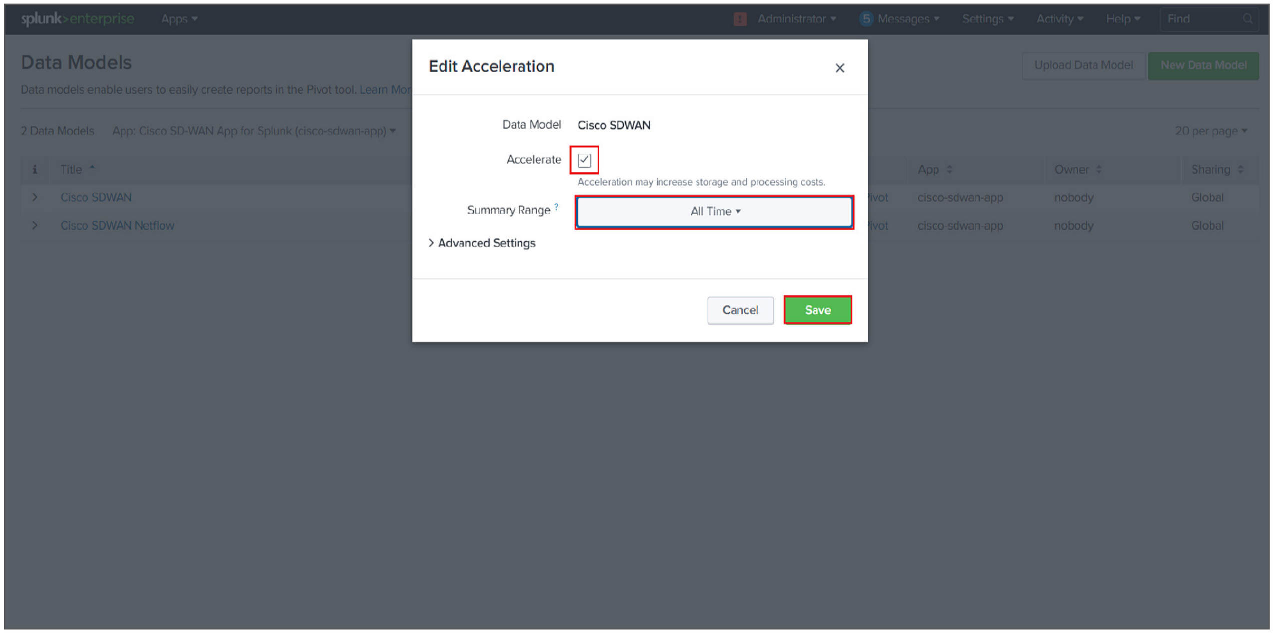
Data models enable users to easily create reports in the Pivot tool. Learn More

2 Data Models | App: Cisco SD-WAN App for Splunk (cisco-sdwan-app) ▾ | Visible in the App ▾ | Owner: Any ▾ | filter | 20 per page ▾

i	Title	Type	⚡	Actions		App	Owner	Sharing
>	Cisco SDWAN	data model	⚡	Edit ▾	Pivot	cisco-sdwan-app	nobody	Global
>	Cisco SDWAN Netflow	data model	⚡	Edit ▾	Pivot	cisco-sdwan-app	nobody	Global

- Check or uncheck Accelerate checkbox to “Enable” or “Disable” data model acceleration respectively.
- If acceleration is enabled, select the summary range to specify the acceleration period. The recommended acceleration period is 7 days. The acceleration period can be changed as per user convenience.
- To save acceleration changes click on the Save button.

Contents



Data Models

Data models enable users to easily create reports in the Pivot tool. Learn Mor

2 Data Models App: Cisco SD-WAN App for Splunk (cisco-sdwan-app)

i	Title		App	Owner	Sharing
>	Cisco SDWAN	ivot	cisco-sdwan-app	nobody	Global
>	Cisco SDWAN Netflow	ivot	cisco-sdwan-app	nobody	Global

Edit Acceleration

Data Model Cisco SDWAN

Accelerate ☑

Acceleration may increase storage and processing costs.

Summary Range ? All Time

- Follow the Similar Steps to Enable/Disable Acceleration Cisco_SDWAN_Netflow Data model

- Warning: The accelerated data models help in improving the performance of the dashboard but it increases the disk usage on the Indexer.

Dashboards

SOC dashboard

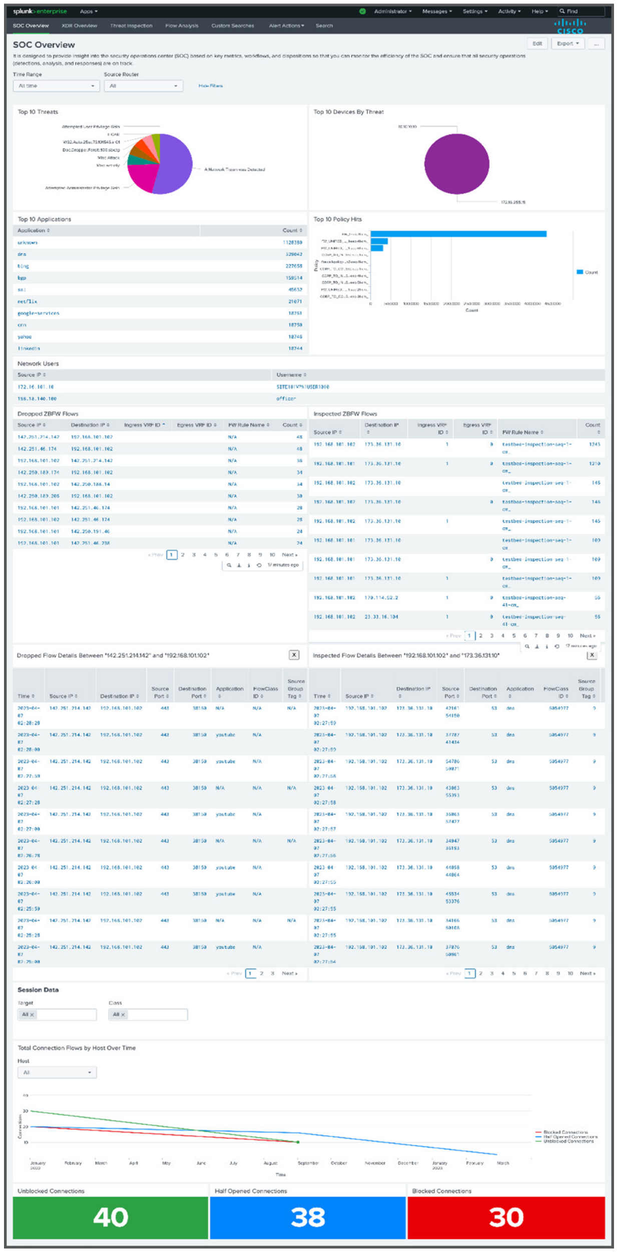
Description

It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you can monitor the efficiency of the SOC and ensure that all security operations (detections, analysis, and responses) are on track.

The dashboard will consist of the below-mentioned panels

Contents

Screenshot



SOC Overview

It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you can monitor the efficiency of the SOC and ensure that all security operations (detections, analysis, and responses) are on track.

Time Range: All time ▾

Source Router: All ▾

Top 10 Threats

Top 10 Devices By Threat

Top 10 Applications

Application ⇕	Count ⇕
unknown	1128380
dns	329042
bing	227658
bgp	159514
ssl	45632
netflix	21071
google-services	18751
cnn	18750
yahoo	18746
linkedin	18744

Top 10 Policy Hits

Network Users

Source IP ⇕	Username ⇕
172.16.101.10	SITE101VPN1USER1010
156.18.140.100	officer

Dropped ZBFW Flows

Source IP ⇕	Destination IP ⇕	Ingress VRF ID ⌃	Egress VRF ID ⇕	FW Rule Name ⇕	Count ⇕
142.251.214.142	192.168.101.102			N/A	48
142.251.46.174	192.168.101.102			N/A	48
192.168.101.102	142.251.214.142			N/A	36
142.250.189.174	192.168.101.102			N/A	34
192.168.101.102	142.250.188.14			N/A	34
142.250.189.206	192.168.101.102			N/A	30
192.168.101.101	142.251.46.174			N/A	28
192.168.101.102	142.251.46.174			N/A	28
192.168.101.101	142.250.191.46			N/A	24
192.168.101.101	142.251.46.238			N/A	24

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

17 minutes ago

Inspected ZBFW Flows

Source IP ⇕	Destination IP ⇕	Ingress VRF ID ⇕	Egress VRF ID ⇕	FW Rule Name ⇕	Count ⇕
192.168.101.102	173.36.131.10	1	0	testbed-inspection-seq-1-cm_	1243
192.168.101.101	173.36.131.10	1	0	testbed-inspection-seq-1-cm_	1210
192.168.101.102	173.36.131.10			testbed-inspection-seq-1-cm_	145
192.168.101.102	173.36.131.10		0	testbed-inspection-seq-1-cm_	145
192.168.101.102	173.36.131.10	1		testbed-inspection-seq-1-cm_	145
192.168.101.101	173.36.131.10			testbed-inspection-seq-1-cm_	109
192.168.101.101	173.36.131.10		0	testbed-inspection-seq-1-cm_	109
192.168.101.101	173.36.131.10	1		testbed-inspection-seq-1-cm_	109
192.168.101.102	170.114.52.2	1	0	testbed-inspection-seq-41-cm_	55
192.168.101.102	23.33.16.104	1	0	testbed-inspection-seq-41-cm_	55

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

17 minutes ago

Dropped Flow Details Between "142.251.214.142" and "192.168.101.102"

Time ⇕	Source IP ⇕	Destination IP ⇕	Source Port ⇕	Destination Port ⇕	Application ⇕	FlowClass ID ⇕	Source Group Tag ⇕
2023-04-07 02:28:28	142.251.214.142	192.168.101.102	443	38158	N/A	N/A	N/A
2023-04-07 02:28:00	142.251.214.142	192.168.101.102	443	38158	youtube	N/A	
2023-04-07 02:27:59	142.251.214.142	192.168.101.102	443	38158	youtube	N/A	
2023-04-07 02:27:28	142.251.214.142	192.168.101.102	443	38158	N/A	N/A	N/A
2023-04-07 02:27:00	142.251.214.142	192.168.101.102	443	38158	youtube	N/A	
2023-04-07 02:26:28	142.251.214.142	192.168.101.102	443	38158	N/A	N/A	N/A
2023-04-07 02:26:00	142.251.214.142	192.168.101.102	443	38158	youtube	N/A	
2023-04-07 02:25:59	142.251.214.142	192.168.101.102	443	38158	youtube	N/A	
2023-04-07 02:25:28	142.251.214.142	192.168.101.102	443	38158	N/A	N/A	N/A
2023-04-07 02:25:00	142.251.214.142	192.168.101.102	443	38158	youtube	N/A	

« Prev 1 2 3 Next »

Inspected Flow Details Between "192.168.101.102" and "173.36.131.10"

Time ⇕	Source IP ⇕	Destination IP ⇕	Source Port ⇕	Destination Port ⇕	Application ⇕	FlowClass ID ⇕	Source Group Tag ⇕
2023-04-07 02:27:59	192.168.101.102	173.36.131.10	42161 54150	53	dns	5054977	9
2023-04-07 02:27:59	192.168.101.102	173.36.131.10	37787 41434	53	dns	5054977	9
2023-04-07 02:27:58	192.168.101.102	173.36.131.10	54786 59871	53	dns	5054977	9
2023-04-07 02:27:58	192.168.101.102	173.36.131.10	43863 55393	53	dns	5054977	9
2023-04-07 02:27:57	192.168.101.102	173.36.131.10	36863 57427	53	dns	5054977	9
2023-04-07 02:27:56	192.168.101.102	173.36.131.10	34947 36153	53	dns	5054977	9
2023-04-07 02:27:55	192.168.101.102	173.36.131.10	44858 44864	53	dns	5054977	9
2023-04-07 02:27:55	192.168.101.102	173.36.131.10	45534 53376	53	dns	5054977	9
2023-04-07 02:27:55	192.168.101.102	173.36.131.10	34166 50168	53	dns	5054977	9
2023-04-07 02:27:54	192.168.101.102	173.36.131.10	37876 50961	53	dns	5054977	9

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Session Data

Target: All ×

Class: All ×

Total Connection Flows by Host Over Time

Host: All ▾

Unblocked Connections	Half Opened Connections	Blocked Connections
40	38	30

Panels

The Dashboard should have the below panels:

1. Top 10 Threats
   - **Description:** This panel displays a Pie chart for Top 10 Threats
   - **Chart Type:** Pie Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** Inline Threat Details Panel
   - **Sourcetype:** cisco:sdwan:utd:logs

2. Threat Detail for a Particular Threat
   - **Description:** This panel displays a details for particular threat
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:utd:logs

3. Top 10 Devices by Threat
   - **Description:** This panel displays a Pie chart Top 10 Devices by threat
   - **Chart Type:** Pie Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
   - **Drilldown (on click):** Inline Device Details Panel
   - **Sourcetype:** cisco:sdwan:utd:logs

4. Device details for a particular device
   - **Description:** This panel displays a details for particular Device
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Source IP, Source Port, Destination IP, Destination Port
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:utd:logs

5. Top 10 Applications
   - **Description:** This panel displays the top 10 applications with their count
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** Inline Application Detail Panel
   - **Sourcetype:** stream:netflow

6. Application Details for a Particular Application
   - **Description:** This panel displays a details for particular Application
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Source IP, Source Port, Destination IP, Destination Port, Input Snmpidx, Output Snmpidx
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** stream:netflow

7. Top 10 Policy Hits
   - **Description:** This panel displays the top 10 Policy Hits with their count
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker,Source Router
   - **Drilldown (on click):** Inline Policy Details Panel
   - **Sourcetype:** stream:netflow

8. Policy Details for a Particular Policy
   - **Description:** This panel displays a details for particular Policy
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Action, Source IP, Source Port, Destination IP, Destination Port, Input Snmpidx, Output Snmpidx
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** stream:netflow

9. Total Connection Flows by Host Over Time
   - **Description:** This panel displays a timechart for the top All connections
   - **Chart Type:** Line Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router, Host, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:host:tcp:alert:on

10. Unblocked connections
    - **Description:** This panel displays a single value count of a total number of unblocked connection
    - **Chart Type:** Single Value
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To panel unblocked connections by hosts
    - **Sourcetype:** cisco:sdwan:unblock:host

11. Unblocked connections by unblocked hosts
    - **Description:** This panel displays a table of unblocked connections by unblocked hosts with their count
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To raw events for selected unblocked host
    - **Sourcetype:** cisco:sdwan:unblock:host

12. Half opened connections
    - **Description:** This panel displays a single value count of a total number of half opened connection
    - **Chart Type:** Single Value
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To Half opened connections by half opened hosts panel
    - **Sourcetype:** cisco:sdwan:host:tcp:alert:on

13. Half Opened Connections by half opened hosts
    - **Description:** This panel displays a table of half opened connections by half opened hosts with their count
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To raw events for selected half opened host
    - **Sourcetype:** cisco:sdwan:host:tcp:alert:on

14. Blocked Connections
    - **Description:** This panel displays a single value count of a total number of blocked connections
    - **Chart Type:** Single Value
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To raw events
    - **Sourcetype:** cisco:sdwan:block:host

15. Blocked Connections by blocked hosts
    - **Description:** This panel displays a table of blocked connections by blocked hosts with their count
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To raw events for selected blocked host
    - **Sourcetype:** cisco:sdwan:host:tcp:alert:on

16. Dropped ZBFW Flows
    - **Description:** This panel displays a table of dropped ZBFW flows between source ip and destination ip with their total count
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** Panel for dropped flow details between source ip and destination ip
    - **Sourcetype:** stream:netflow

17. Dropped ZBFW Flows between Source IP and Destination IP
    - **Description:** This panel displays a table of all the dropped ZBFW flows between source ip and destination ip
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To raw event
    - **Sourcetype:** stream:netflow

18. Inspected ZBFW Flows
    - **Description:** This panel displays a table of inspected ZBFW flows between source ip and destination ip with their total count
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** Panel for inspected flow details between source ip and destination ip
    - **Sourcetype:** stream:netflow

19. Inspected ZBFW Flows between Source IP and Destination IP
    - **Description:** This panel displays a table of all the inspected ZBFW flows between source ip and destination ip
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
    - **Drilldown (on click):** To raw event
    - **Sourcetype:** stream:netflow

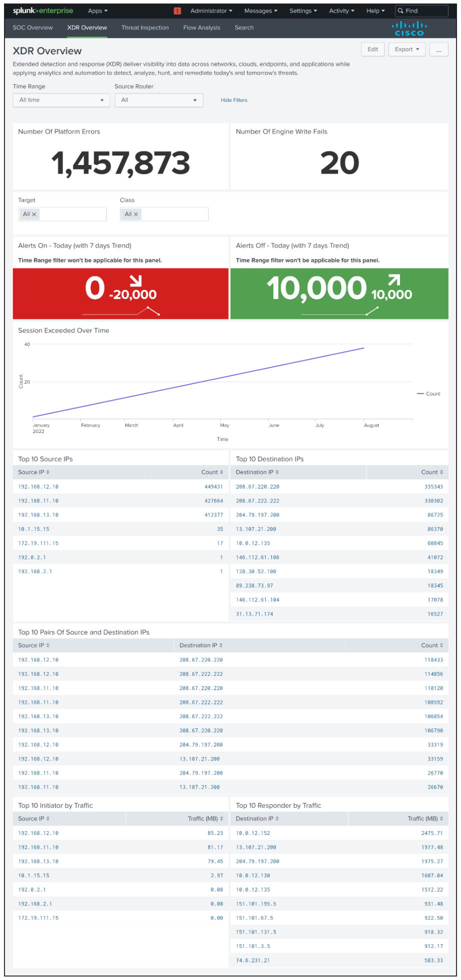
Contents

XDR Dashboard

Description

Extended detection and response (XDR) delivers visibility into data across networks, clouds, endpoints, and applications while applying analytics and automation to detect, analyze, hunt, and remediate today’s and tomorrow’s threats.

Screenshot



XDR Overview

Extended detection and response (XDR) deliver visibility into data across networks, clouds, endpoints, and applications while applying analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats.

Time Range: All time

Source Router: All

Number Of Platform Errors: 1,457,873

Number Of Engine Write Fails: 20

Target: All

Class: All

Alerts On - Today (with 7 days Trend)

Time Range filter won't be applicable for this panel.

0 -20,000

Alerts Off - Today (with 7 days Trend)

Time Range filter won't be applicable for this panel.

10,000 10,000

Top 10 Source IPs

Source IP	Count
192.168.12.10	449431
192.168.11.10	427664
192.168.13.10	412377
10.1.15.15	35
172.19.111.15	17
192.0.2.1	1
192.168.2.1	1

Top 10 Destination IPs

Destination IP	Count
208.67.220.220	335343
208.67.222.222	330302
204.79.197.200	86725
13.107.21.200	86370
10.0.12.135	60845
146.112.61.106	41072
128.30.52.100	18349
89.238.73.97	18345
146.112.61.104	17078
31.13.71.174	16527

Top 10 Pairs Of Source and Destination IPs

Source IP	Destination IP	Count
192.168.12.10	208.67.220.220	118433
192.168.12.10	208.67.222.222	114856
192.168.11.10	208.67.220.220	110120
192.168.11.10	208.67.222.222	108592
192.168.13.10	208.67.222.222	106854
192.168.13.10	208.67.220.220	106790
192.168.12.10	204.79.197.200	33319
192.168.12.10	13.107.21.200	33159
192.168.11.10	204.79.197.200	26770
192.168.11.10	13.107.21.200	26670

Top 10 Initiator by Traffic

Source IP	Traffic (MB)
192.168.12.10	85.23
192.168.11.10	81.17
192.168.13.10	79.45
10.1.15.15	2.97
192.0.2.1	0.08
192.168.2.1	0.08
172.19.111.15	0.00

Top 10 Responder by Traffic

Destination IP	Traffic (MB)
10.0.12.152	2475.71
13.107.21.200	1977.48
204.79.197.200	1975.27
10.0.12.130	1607.04
10.0.12.135	1512.22
151.101.195.5	931.48
151.101.67.5	922.50
151.101.131.5	918.32
151.101.3.5	912.17
74.6.231.21	583.33

Contents

Panels

The Dashboard should have the below panels:

1. Number Of Platform Errors
   - **Description:** This panel displays a single value count of a total number of platform errors
   - **Chart Type:** Single Value
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:smart:lic:platform:error

2. Number Of Engine Write Fails
   - **Description:** This panel displays a single value count of a total number of engine write fail
   - **Chart Type:** Single Valued
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:dmi:cli:engine:write:fail

3. Alerts On - Today (with 7 days Trend)
   - **Description:** This panel displays a single value count of a total number of Alert on in last 24 hours with last month trend
   - **Chart Type:** Single Value
   - **Chart Filter:** Use Time Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:alert:on

4. Alerts Off - Today (with 7 days Trend)
   - **Description:** This panel displays a single value count of a total number of Alert off in last 24 hours with last month trend
   - **Chart Type:** Single Value
   - **Chart Filter:** Use Time Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:alert:off

5. Session Exceeded Over Time
   - **Description:** This panel displays a timechart for the count of session exceeded in 1d span
   - **Chart Type:** Line Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:sessions:maximum

6. Top 10 Source IPs
   - **Description:** This panel displays a tabular view of top 10 Source IP and no. of requests
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:session:audit:trail:start

7. Top 10 Destination IPs
   - **Description:** This panel displays a tabular view of top 10 Destination IP and no. of requests
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:session:audit:trail:start

8. Top 10 Pairs Of Source and Destination IPs
   - **Description:** This panel displays a tabular view of top 10 Source IP and Destination IP combination and no. of requests
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:session:audit:trail:start

9. Top 10 Initiator by Traffic
   - **Description:** This panel displays a tabular view of top 10 Source IP and its traffic
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:session:audit:trail

10. Top 10 Responder by Traffic
   - **Description:** This panel displays a tabular view of top 10 Destination IP and its traffic
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker, Source Router, Target, Class
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:session:audit:trail

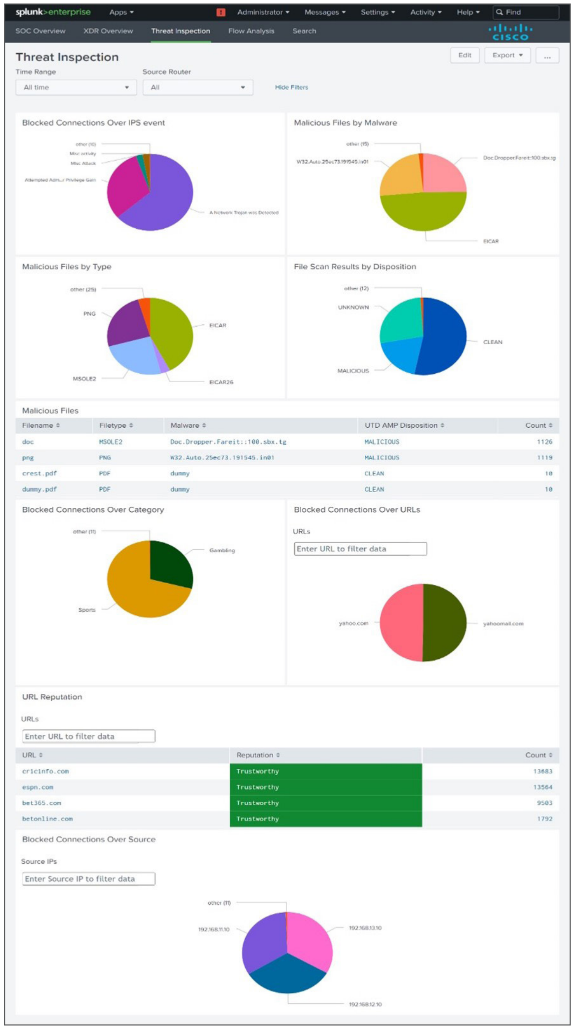
Contents

Threat Inspection dashboard

Description

Provide tactical guidance and insights to detect, investigate and respond to the latest threats.

Screenshot



Threat Inspection

Time Range: All time

Source Router: All

Malicious Files

Filename	Filetype	Malware	UTD AMP Disposition	Count
doc	MSOLE2	Doc.Dropper.Fareit::100.sbx.tg	MALICIOUS	1126
png	PNG	W32.Auto.25ec73.191545.in01	MALICIOUS	1119
crest.pdf	PDF	dummy	CLEAN	10
dummy.pdf	PDF	dummy	CLEAN	10

URLs: Enter URL to filter data

URL Reputation

URLs: Enter URL to filter data

URL	Reputation	Count
cricinfo.com	Trustworthy	13683
espn.com	Trustworthy	13564
bet365.com	Trustworthy	9503
betonline.com	Trustworthy	1792

Source IPs: Enter Source IP to filter data

Contents

Panels

The Dashboard should have the below panels:

1. Blocked Connections Over IPS Event
   - **Description:** This panel displays pie chart for blocked calls by classification
   - **Chart Type:** Pie Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** Inline Classification Details Panel
   - **Sourcetype:** cisco:sdwan:utd:logs

2. Classification Details for a Particular IPS
   - **Description:** This panel displays a details for particular IPS
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:utd:logs

3. Malicious Files by Malware
   - **Description:** This panel displays pie chart for Malicious files by malware
   - **Chart Type:** Pie Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** Inline Malware Detail Panel
   - **Sourcetype:** cisco:sdwan:utd:logs

4. Malware Details for Particular Malware
   - **Description:** This panel displays a details for particular Filetype
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:utd:log

5. Malicious Files by Type
   - **Description:** This panel displays pie chart for Malicious files by type
   - **Chart Type:** Pie Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** Inline Filetype Detail Panel
   - **Sourcetype:** cisco:sdwan:utd:logs

6. Filetype Detail for a Particular filetype
   - **Description:** This panel displays a details for particular Filetype
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:utd:logs

7. File Scan Results by Disposition
   - **Description:** This panel displays pie chart for Malicious files by disposition
   - **Chart Type:** Pie Chart
   - **Chart Filter:** Shared Time Range Picker, Source Router
   - **Drilldown (on click):** Inline UTD Amp Disposition Details Panel
   - **Sourcetype:** cisco:sdwan:utd:logs

8. UTD Amp Disposition Details for a Particular Malware
   - **Description:** This panel displays a details for particular Filetype
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** cisco:sdwan:utd:logs

9. Malicious Files
   - **Description:** This panel displays table of Malicious files by Filename, Filetype, Malware, UTD AMP Disposition
   - **Chart Type:** Tabular view

- **Chart Filter:** Shared Time Range Picker, Source Router
- **Drilldown (on click):** To raw events
- **Sourcetype:** cisco:sdwan:utd:logs

10. Blocked Connections over category
    - **Description:** This panel displays pie chart for blocked calls by category
    - **Chart Type:** Pie Chart
    - **Chart Filter:** Shared Time Range Picker, Source Router
    - **Drilldown (on click):** Inline Url Details for Category Panel
    - **Sourcetype:** cisco:sdwan:utd:logs

11. URL Details for Category for a Particular Category
    - **Description:** This panel displays a details for url details with its Reputation for particular category
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router
    - **Drilldown (on click):** Inline url detail panel
    - **Sourcetype:** cisco:sdwan:utd:logs

12. URL Details for a Particular URL
    - **Description:** This panel displays a details for particular url
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
    - **Drilldown (on click):** To raw events
    - **Sourcetype:** cisco:sdwan:utd:logs

13. Blocked Connections over URLs
    - **Description:** This panel displays the blocked calls by urls with their count
    - **Chart Type:** Pie chart
    - **Chart Filter:** Shared Time Range Picker, Source Router, URL
    - **Drilldown (on click):** Inline Url Details Panel
    - **Sourcetype:** cisco:sdwan:utd:logs

Contents

14. URL Details for a Particular URL
    - **Description:** This panel displays a details for particular url
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
    - **Drilldown (on click):** To raw events
    - **Sourcetype:** cisco:sdwan:utd:logs

15. URL Reputation
    - **Description:** This panel displays the table of the worst reputed urls with their reputation
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, URL
    - **Drilldown (on click):** To raw events
    - **Sourcetype:** cisco:sdwan:utd:logs

16. Blocked Connections over source
    - **Description:** This panel displays the table of the blocked calls by source with their count
    - **Chart Type:** Pie chart
    - **Chart Filter:** Shared Time Range Picker, Source Router, Source IP
    - **Drilldown (on click):** Inline Source Details Panel
    - **Sourcetype:** cisco:sdwan:utd:logs

17. Source Details for a Particular Source
    - **Description:** This panel displays a details for particular source
    - **Chart Type:** Tabular view
    - **Chart Filter:** Shared Time Range Picker, Source Router, Device IP, Device Name, Action, Source IP, Source Port, Destination IP, Destination Port
    - **Drilldown (on click):** To raw events
    - **Sourcetype:** cisco:sdwan:utd:logs

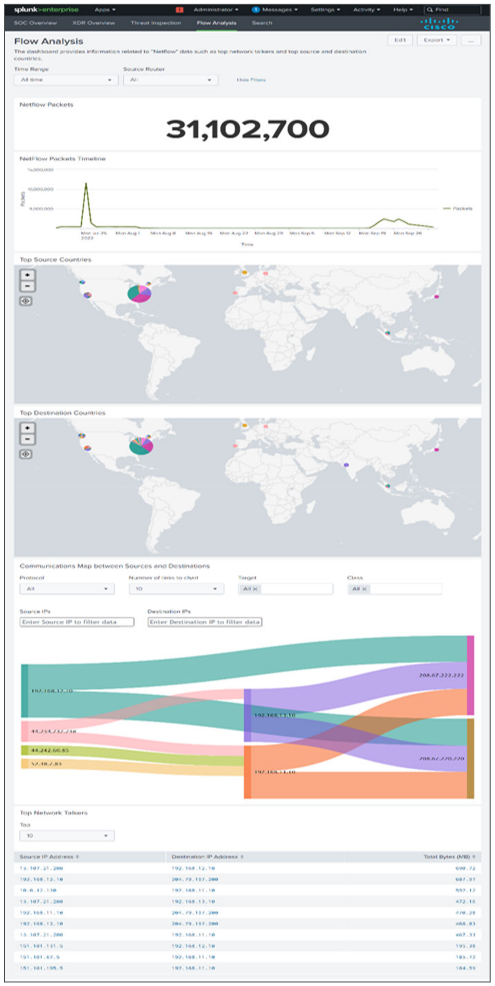
Contents

Flow Analysis

Description

The dashboard provides information related to “Netflow” data such as top network talkers and top source and destination countries.

Screenshot



Flow Analysis

The dashboard provides information related to "Netflow" data such as top network talkers and top source and destination countries.

Time Range: All time

Source Router: All

Netflow Packets

31,102,700

NetFlow Packets Timeline

Top Source Countries

Top Destination Countries

Communications Map between Sources and Destinations

Protocol: All

Number of links to chart: 10

Target: All

Class: All

Source IPs: Enter Source IP to filter data

Destination IPs: Enter Destination IP to filter data

Top Network Talkers

Top: 10

Source IP Address	Destination IP Address	Total Bytes (MB)
13.107.21.200	192.168.12.10	690.72
192.168.12.10	204.79.197.200	687.97
10.0.12.130	192.168.11.10	552.12
13.107.21.200	192.168.13.10	472.16
192.168.11.10	204.79.197.200	470.28
192.168.13.10	204.79.197.200	468.83
13.107.21.200	192.168.11.10	467.33
151.101.131.5	192.168.12.10	195.38
151.101.67.5	192.168.11.10	185.72
151.101.195.5	192.168.11.10	184.55

Panels

The Dashboard should have the below panels:

1. Netflow Packets
   - **Description:** This panel displays a single value count of a total number of connection
   - **Chart Type:** Single Valued
   - **Chart Filter:** Shared Time Range Picker
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** stream:netflow
2. NetFlow Packets Timeline
   - **Description:** This panel displays the line chart netflow records packet
   - **Chart Type:** Line Chart
   - **Chart Filter:** Shared Time Range Picker
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** stream:netflow
3. Top Source Countries
   - **Description:** This panel displays the top source countries
   - **Chart Type:** Geographical Map
   - **Chart Filter:** Shared Time Range Picker
   - **Drilldown (on click):** N/A
   - **Sourcetype:** stream:netflow
4. Top Destination Countries
   - **Description:** This panel displays the top destination countries
   - **Chart Type:** Geographical Map
   - **Chart Filter:** Shared Time Range Picker
   - **Drilldown (on click):** N/A
   - **Sourcetype:** stream:netflow

Contents

5. Communications Map Between Sources and Destinations
   - **Description:** This panel displays a sankey diagram to visualize packet transfer from source to destination based on protocol
   - **Chart Type:** Sankey Diagram
   - **Chart Filter:** Shared Time Range Picker, Source Router, Protocol, Number Of Links To Chart, Target, Class, Source IPs, Destination IPs
   - **Drilldown (on click):** N/A
   - **Sourcetype:** cisco:sdwan:log:summary

6. Top Network Talkers
   - **Description:** This panel displays the top network talkers
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** stream:netflow

7. Top 10 Application
   - **Description:** This panel displays the top 10 applications with their count
   - **Chart Type:** Tabular View
   - **Chart Filter:** Shared Time Range Picker,Source Router
   - **Drilldown (on click):** Inline Application Detail Panel
   - **Sourcetype:** stream:netflow

8. Application Details for a Particular Application
   - **Description:** This panel displays a details for particular Application
   - **Chart Type:** Tabular view
   - **Chart Filter:** Shared Time Range Picker, Source Router, Source IP, Source Port, Destination IP, Destination Port, Input Snmpidx, Output Snmpidx
   - **Drilldown (on click):** To raw events
   - **Sourcetype:** stream:netflow

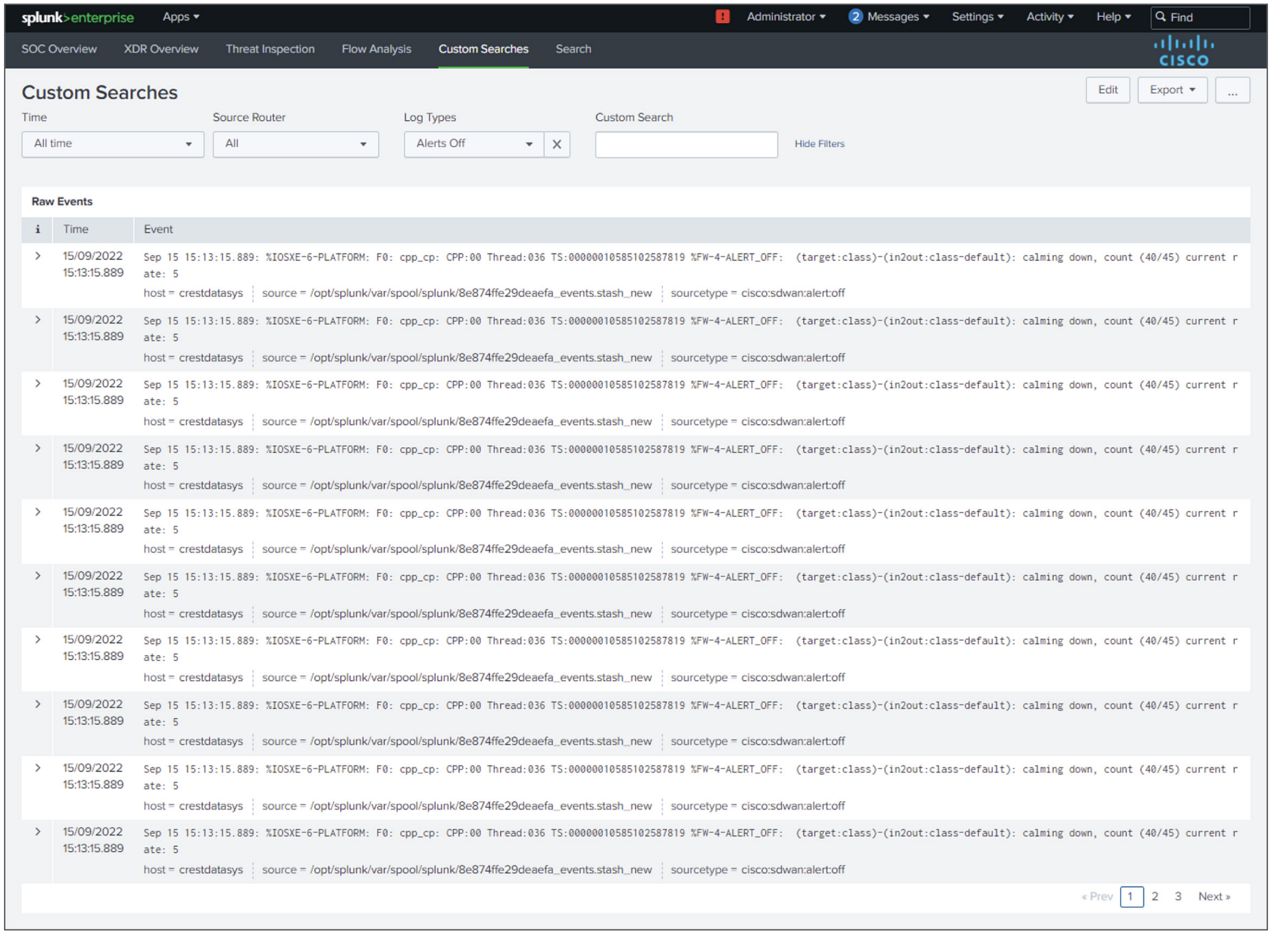
Contents

Custom Searches

Description

The dashboard provides predefined event types that helps in searching data based on its categories.

Screenshot



Custom Searches

Time: All time

Source Router: All

Log Types: Alerts Off

Custom Search:

Raw Events

i	Time	Event
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current rate: 5 host = crestdatasys ┊ source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new ┊ sourcetype = cisco:sdwan:alert:off

Contents

Panels

The Dashboard contains panel having raw events for the selected filters (i.e. Time, Source Router, Log Types, Custom Search).

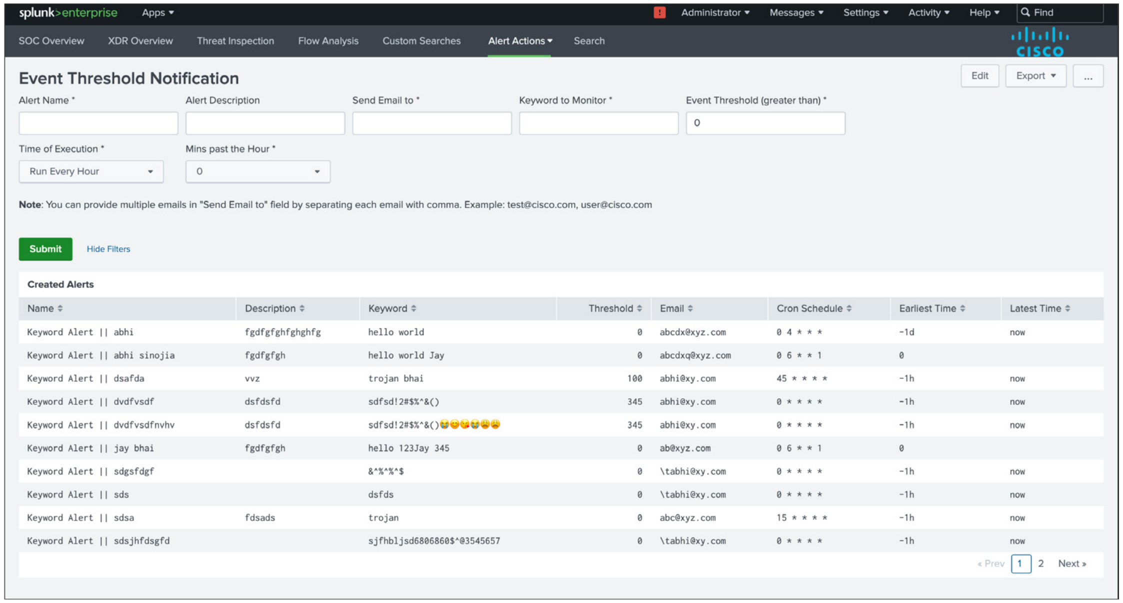
Time: Select the time range within which you are looking for data.
Source Router: Select the appropriate host.
Log Types: Select the types of the logs that you are looking for.
Custom Search: Search the keywords which are part of the raw events.

Event Threshold Notification

Description

The dashboard provides the user the ability to create Splunk alerts based on the “Keywords” and can set the threshold and the schedule as per the requirements.

Screenshot



Event Threshold Notification

Alert Name *

Alert Description

Send Email to *

Keyword to Monitor *

Event Threshold (greater than) * 0

Time of Execution * Run Every Hour

Mins past the Hour * 0

Note: You can provide multiple emails in "Send Email to" field by separating each email with comma. Example: test@cisco.com, user@cisco.com

Created Alerts

Name	Description	Keyword	Threshold	Email	Cron Schedule	Earliest Time	Latest Time
Keyword Alert || abhi	fgdfgfghfghghfg	hello world	0	abcdx@xyz.com	0 4 * * *	-1d	now
Keyword Alert || abhi sinojia	fgdfgfgh	hello world Jay	0	abcdxq@xyz.com	0 6 * * 1	0	
Keyword Alert || dsafda	vvz	trojan bhai	100	abhi@xy.com	45 * * * *	-1h	now
Keyword Alert || dvdfvsdf	dsfdsfd	sdfsd!2#$%^&()	345	abhi@xy.com	0 * * * *	-1h	now
Keyword Alert || dvdfvsdfnvhv	dsfdsfd	sdfsd!2#$%^&()😭😊😘😭😩😩	345	abhi@xy.com	0 * * * *	-1h	now
Keyword Alert || jay bhai	fgdfgfgh	hello 123Jay 345	0	ab@xyz.com	0 6 * * 1	0	
Keyword Alert || sdgsfdgf		&^%^%^$	0	\tabhi@xy.com	0 * * * *	-1h	now
Keyword Alert || sds		dsfds	0	\tabhi@xy.com	0 * * * *	-1h	now
Keyword Alert || sdsa	fdsads	trojan	0	abc@xyz.com	15 * * * *	-1h	now
Keyword Alert || sdsjhfdsgfd		sjfhbljsd6806860$^@3545657	0	\tabhi@xy.com	0 * * * *	-1h	now

« Prev 1 2 Next »

Panels

The Dashboard contains a panel that gives details about the alerts that are created by the user.

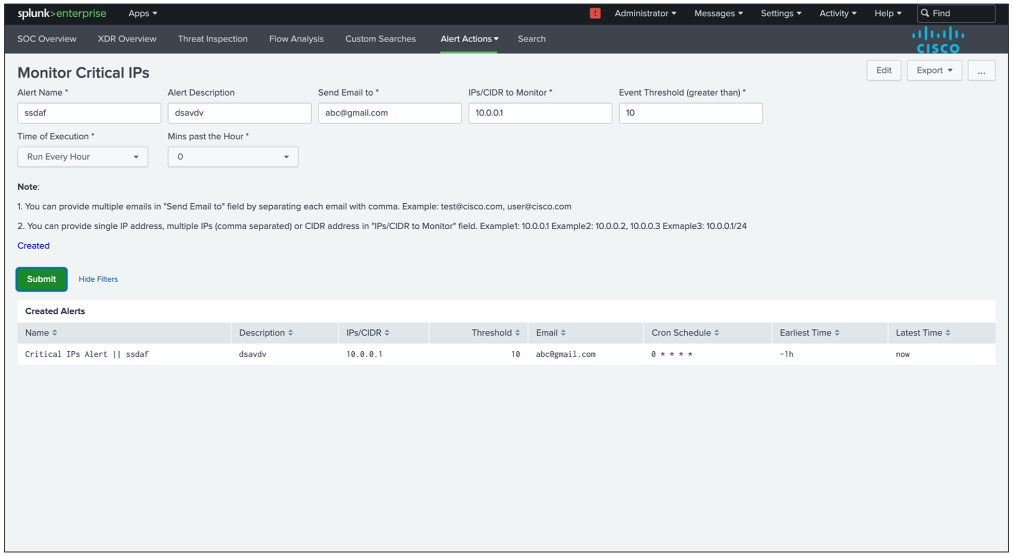
Name: Name of the alert.
Description: Description for the respective alert.
Keyword: Keyword for which the alert is created.
Threshold: Threshold count for the keyword.
Email: Email of user to send the alert to.
Cron Schedule: Cron at which the alert is executed.
Earliest Time: Earliest time for the data to be considered.
Latest Time: Latest time for the data to be considered.

Monitor Critical IPs

Description

The dashboard provides the user the ability to create Splunk alerts based on the “IPs/CIDR” and can set the threshold and the schedule as per the requirements.

Screenshot



Monitor Critical IPs

Alert Name *: ssdaf
Alert Description: dsavdv
Send Email to *: abc@gmail.com
IPs/CIDR to Monitor *: 10.0.0.1
Event Threshold (greater than) *: 10
Time of Execution *: Run Every Hour
Mins past the Hour *: 0

Note:

1. You can provide multiple emails in "Send Email to" field by separating each email with comma. Example: test@cisco.com, user@cisco.com

2. You can provide single IP address, multiple IPs (comma separated) or CIDR address in "IPs/CIDR to Monitor" field. Example1: 10.0.0.1 Example2: 10.0.0.2, 10.0.0.3 Exmaple3: 10.0.0.1/24

Created

Created Alerts

Name	Description	IPs/CIDR	Threshold	Email	Cron Schedule	Earliest Time	Latest Time
Critical IPs Alert || ssdaf	dsavdv	10.0.0.1	10	abc@gmail.com	0 * * * *	-1h	now

Panels

The Dashboard contains a panel that gives details about the alerts that are created by the user.

Name: Name of the alert.
Description: Description for the respective alert.
IPs/CIDR: IPs/CIDR for which the alert is created.
Threshold: Threshold count for the IPs/CIDR.
Email: Email of user to send the alert to.
Cron Schedule: Cron at which the alert is executed.
Earliest Time: Earliest time for the data to be considered.
Latest Time: Latest time for the data to be considered.

Uninstalling Cisco SD-WAN App and Add-on for Splunk

Disabling the App and Add-on

To disable the App and Add-on, you must be logged into Splunk as an Administrator and follow the steps below.

- Click the App name in the title bar, and then click Manage Apps.
- In the search box, type the name of the app, and then click Search. In the Status column, next to both the App and Add-on, click Disable

Uninstalling the App and Add-on

Follow the below instructions based on your environment.

Uninstall from a standalone environment

1. Disable the App and Add-on from the Splunk user interface as detailed above.
2. Log into the Splunk machine from the backend and delete the App and Add-on folders. The app and its directory are typically located in $SPLUNK_HOME/etc/apps/cisco-sdwan-app, and add-on and its directory are typically located in $SPLUNK_HOME/etc/apps/ta-sdwan-app.

Contents

3. Verify that no local configuration files related to Cisco SDWAN App/Add-on are available in the $SPLUNK_HOME/etc/system and $SPLUNK_HOME/etc/users folders. If the local folder is present, remove it as well.

4. Restart Splunk.

Uninstall from a distributed or clustered environment (To be Checked)

In a cluster or distributed environment, the Cisco SD-WAN App is installed on all the Search Heads and the Cisco SD-WAN Add-on is installed on Search Heads and Forwarders.

The steps to uninstall the App and Add-on are the same as for Standalone.

1. To perform any installation or uninstallation step on all the search nodes of a distributed environment, use a deployer manager.

2. From the deployer machine, go to $SPLUNK_HOME$/etc/shcluster/apps and remove the App and Add-on folders and execute cluster bundle command. Refer

Troubleshooting

Cisco SD-WAN Add-on for Splunk

- To check the fields extracted for Syslog data by the Cisco SDWAN Add-on for Splunk:
  - index=<your_index_name> sourcetype=”cisco:sdwan*” in Splunk in verbose mode.
  - “cisco:firewall:logs” must be selected as sourcetype while configuring the Syslog input.
- To check the fields extracted for Netflow data by the Cisco SDWAN Add-on for Splunk:
  - index=<your_index_name> sourcetype=”stream*” in Splunk in verbose mode.

Contents

Cisco SD-WAN App for Splunk

- If dashboards are not getting populated or found data discrepancy between the panel search result and drilldown search result:
  - Check whether you have correctly configured the index in the cisco_sdwan_index macro.
  - Also, you can verify if the data is there in the index by running the search query:
    - index=”<your_index_name>”
  - Try expanding Time Range.
- If in SOC Dashboard “Top 10 Applications” Panel is not getting populated run the savesearch as per the given steps:
  - Go to Settings -> Searches, reports, and alerts
  - Select “Cisco SD-WAN for Splunk” in the “App” context dropdown and “All” in the “Owner” dropdown.
  - Run the “cisco_sdwan_netflow” savedsearch with “All time” time range.
- If in SOC Dashboard “Top 10 Policy Hits” Panel is not getting populated run the savesearch as per the given steps:
  - Go to Settings -> Searches, reports, and alerts
  - Select “Cisco SD-WAN for Splunk” in the “App” context dropdown and “All” in the “Owner” dropdown.
  - Run the “cisco_sdwan_action” and “cisco_sdwan_policy” savedsearches with “All time” time range.