



Cisco Catalyst SD-WAN Splunk Integration

User guide





Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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.



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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.

splunk>enterprise Apps •	1 Administrator -	2 Messages	 Settings ▼ 	Activity -	Help 🔻	Find	Q,
Apps			Browse more ap	ps Insta	ll app from file	Create a	pp
Showing 1-25 of 31 items							
filter Q					« Prev	25 per page	▼ xt »

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					
Choose File cisco-sdwan-app.zip					
Upgrade app. Checking this will overwrite the app if it already exists.					
Cancel	Upload				



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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

Restart Splunk

Click the button below to restart Splunk.

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:



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

1. Login to Splunk WEB UI.



2. Navigate to Settings > Data inputs.

splunk>enterprise Apps ▼	I	I Administrator 🔻	Messages	Activity - Help - Q Find
SOC Overview XDR Overview Threat Inspection Flow Analysis Search SOC Overview Threat Inspection Flow Analysis Search It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and operations (detections, analysis, and response) are on track. Time Range Source Router Last 24 hours All Hide Filters	dispositions so that you car	Add Data	KNOWLEDGE Searches, reports, and alerts Data models Event types Tags Fields Lookups User interface Alert actions	Data Data inputs Forwarding and receiving Indexes Report acceleration summaries Virtual indexes Source types Ingest actions
Top 10 Threats W32.Auto.25ec73391545.in01 Doc.DropperFarett:100.bit.10 Misc.Attack Misc.actively BICAR Attempted Administrator Phyllege Gain	Top 10 Device	Console	Advanced search All configurations SYSTEM Server controls Health report manager RapidDiag Instrumentation Licensing Workload management	DISTRIBUTED ENVIRONMENT Indexer clustering Forwarder management Federated search Distributed search USERS AND AUTHENTICATION Roles Users Tokens Password Management Authentication Methods



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

3. Choose TCP or UDP and click New.

splunk>enterprise Apps -		! Administrator 🔻	互 Messages ▼	Settings 🕶	Activity -	Help 🔻	Find	Q
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.				
L	ocal inputs							
	Туре	Input	S	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.



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

splunk >enterprise Apps	× Add Data	Administrator Solution Administrator Solution Administrator Adminiterator Administrator Administrator
	Files & Directories Select So Uplead a file, index a local file, or monitor an entire directory. HTTP Event Collector Configure tokems that clients can use to send data over HTTP or HTTPs. TCP / UDP Configure the Splank platform to listen on a network port. Scripts Get data from any API, service, or database with a script. Scripts	rce Input Settings Review Done Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as sysiog). Learn More 12 TCP UDP Port 7 Still Example: 514 Source name override 7 optional Instance Ins
	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	Only accept connection optional from 7 example: 10.1.2.3, tbadhost splunk.com, *.splunk.com
	Splank Add-on Bulder field extraction modular input intsights_atlerts Go to the add-onk configuration UI and configure modular inputs under the leputs menu.	FAQ How should I configure the Splunk platform for syslog traffic? What's the difference between receiving data over TCP versus UDP? Conclude use for data for Madeuro e staree?
	Intsights_indicators Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.	Can't Currect system duala noni remotovo systems: What is a source type?

- 9. Set the sourcetype as cisco:firewall:logs.
- 10. Set App context to Cisco SD-WAN Add-on.

splunk ≻enterprise Apps ▼	1 Administrator • 🕒 Messages • Settings • Activity • Help • Find Q
	Add Data C C Back Review >
	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 what kind of data you've gots of that Byblunk platform can format the data incliligently during indexing. And it's a way to categorize your data, so that you can search it easily. Source Type Custom * Category Custom * Description Source Type
	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 12



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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

12. Click Review.

splunk>enterprise Apps -	🚹 Administrator 🕶 🐻 Messages 💌 Settings 👻 Activity 👻 Help 👻 Find 🔍
	Add Data C C C C C C C C C C C C C C C C C C
	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 12
	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 12
	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 12
	FAQ > How do Indexes work? > How do I know when to create or use multiple indexes?

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

splunk >enterprise Apps ▼	Add Data Select Source	Input Settings Review	Image: Administrator → O Cone	5 Messages ▼ Settings ▼	Activity ▼ Help ▼	Find Q
	Input Type UDP Port Port Number 54 Source name override N/A Restrict to Host N/A Source Type Ciscoffrevalt/logs App Context IP address of the remote server) Index default	,				

Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

Once the input is configured, execute the following query to see if Syslog events are being received. index=<configured_index> sourcetype="cisco:sdwan"

.........

The bridge to possible

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. (should be replaced with the VM in which data is been collected)
- 8. Goto Location: \$SPLUNK_HOME/etc/apps/Splunk_TA_stream/local



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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." (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.



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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			New Event Type
Showing 1-18 of 18 items			
App Cisco SD-WAN Add-on Owner Any	Visible in the App filter	Q	25 per page 👻

• Click on "cisco_sdwan_index".



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

 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.
	Cancel Save

· 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.

Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

Search macros Advanced search » Search macro	os					New	Search Macro
Showing 1-2 of 2 Items App Cisco SD-WAN App fo * Owner Any * Created in the App * filter Q 25 per page *							
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.

splunk>enterprise Apps •	8	Administrator 🕶	Messages 🗸 Sett	ings 🕶	Activity -	Help 🔻	Q, Find	
SOC Overview XDR Overview Threat Inspection Flow Analysis Search SOC Overview It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so the operations (detections, analysis, and responses) are no track.	at you car	Add Data	KNOWLEDGE Searches, reports, an Data models Event types	d alerts	DATA Data in Forward Indexes	puts ding and rec	ceiving	
Time Range Source Router Last 24 hours All Hide Filters		dið Igi Monitoring Console	Fields Lookups User interface Alert actions Advanced search		Virtual Source Ingest a	types actions	DNMENT	
Top 10 Threats Top 1 W32 Auto 25ec73191545 ino1 Doc DropperFaret:100.3bx1g Misc Attack Misc activity EICAR A Network Trojan was Detected	0 Device		All configurations SYSTEM Server settings Server controls Health report manage RapidDiag Instrumentation Licensing Workload management	er ent	Indexer Forwar Federa Distribu USERS J Roles Users Tokens Passwo Authen	clustering der manage ted search ited search AND AUTHEN ord Manager tication Met	ment TICATION nent hods	



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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.

splur	k >enter	orise Apps •				! Adı	ministr	rator 🔻 🏼 N	lessages 🔹 Settings 💌	Activity • Help •	Find Q
Data r	a Mod	els ble users to easily create reports in the Pivot tool. Learn Mo	vre 12							Upload Data Model	New Data Model
2 Data	Models	App: Cisco SD-WAN App for Splunk (cisco-sdwan-app) 💌	Visible in the App ${\color{red} {\bf v}}$	Owner: Any 🔻	filter		٩				20 per page 🔻
i	Title 📍					Type 🗘	4	Actions	App ‡	Owner ‡	Sharing 🗘
>	Cisco SD	WAN				data model	4	Edit - Pivo	t cisco-sdwan-app	nobody	Global
>	Cisco SD	WAN Netflow				data model	4	Edit 🔻 Pivo	t 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.



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting



- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

splunko ent	verprise Acco	• Threat Inspect							0	Administrati	ar • Messa	945 F	Setings =	Activity = 14	میں - م	<u>l</u> u
SOC OV	verview													D.	CISC R Deport	•
it is designed (detections, a	to provide insight in nalysis, and respons	to the security operates and the security operation of the security operation is a security of the security operation operation of the security operation operatio	tons center ()	IOC) based or	key metrics, w	rosdiawa, ara	d clapealt or	n so that you	can rapeit	or the efficiency	of the SOC er	d ernun	that all security	operations		
Time Range		Source Router														
ALCEN		14		-												
Top 10 The	reats							Top 10 De	vices By	Threat						
	Attempted User I	I Old														
	DecDroppe For	0.0541.44														
		Net whether	•	4.8	knoch Tuperman	Dutacted										
	Anomprie Arministratio											_				
												1		173.85.165.16		
Top 10 Apr	plications						C	Top 10 Po	ācy Hirs							
where a	Ψ.						1128389	10,0400	10,1-11,0-1							
de s							329642	Courter (n an an an an							
tap							159514	2 000, 10.0	2.321.52.54 5.5.485.66							Count
861							456.52	CORP., TO, C	1							
google-ser	viers						21671			0 x0000	DODO NASO	200,000	Court Court	350100 40100	0 453200	
om							18759									
11/Media							18745									
Network L	lsers															
Source IP 0 172,16,161	.16						Alernetice 0	/5081010								
155.18.140	.100						fficer									
Dropped 2	20PW Flows	a P a langer a	APP 10 *	toress were en	6 para	Nore -	Court	Inspected	ZOFW F	lows Dest safee. P	(pasar-	00	Doress viae			Count
142,251,25	4.142 152.168.	161.162			N/A		41	Source IP 1		-		iD o	10 1	Fit Dule Noree		0
142.251.46	174 152.168.	101.102			N/A		45	-12.162.10				1	•	ce.	erran-sag-1-	1245
142.259.18	9.174 192.168.	101.102			N/A		и	192, 168, 16	0.10	73.36.131.10		1		Cestber-inspe ce,	etter-see-1-	1219
152.168.10	1.102 142.258.	128.14			N/A		14 12	192, 168, 16	11.142	173.36.131.10				Cestber Juspe ce.	cline seg 1-	145
192.168.10	1.101 142.251.	00.174			N/A		28	117.168.10	11.112	173.26.121.10				tastbas-sape	ction-mq+l+	145
152,168,10	0.102 142.251.	06.174			N/A		25	192.168.18	1.162	173.36.131.10		1		textbec-impe	ction-ang-1-	145
112.164.18	0.161 142.251	64. 728			N/A		24	152, 168, 10	1.10	173.35.131.10				testbet-impe	ction-seg-1-	169
			<1787	2 3 4	5 6 7 I	8 9 10 1 O Vet	Next >	192, 168, 16	n. 101	173.36.121.10				testher impe	ction and 1-	169
								192 168 10	11.101	173.36.131.10		1		tastbas-sage	etian-sag-1-	109
								192, 168, 10	1.162	179.114.52.2		1		testbee-inspe	ction-sea-	55
								192.168.10	1.142	23.33.16.134		1		Al-on, Lestber-Jospe	ctionning	55
													1 2 3	41-01_	8 9 10	Next+
Dropped P	Pow Details Betw	ten *142.251.214.14	2" and "192:	168.101.102*			X	Inspected	Flow De	talis Between	192.168.101	02° and	173.36.131.10	9.4	i 0 7=	X
Tere 4		0	Source	Destruction	Application	ForGass	Seurce Group	Total A		De	stinution IP	Source	Destination	Application	FlowCass	Seurce Group
2023-04-	140.251.214.142	192.145.101.102	-441	381.68	N/3	N/A	N/A	2823-84-	192,168	. 101. 102 12	. 36. 131. 38	42161	53	des	6854977	
62 26 29								92:27:59								_
87 82:28:00					yactan			#2 #2:27:00				43434				
2022-04-	142.251.214.142	192.168.101.102	442	38159	yastube	N/3.		2823-84+	192,158	. 191 . 192 17.	. 36, 131, 18	54786	53	des	5954977	
82.22.58	141 251 214 141	102 148 141 142	40	34153	8/2	NO	19/4	92.27.5A	132 158	101 102 17	AL 111 18	43843	9		5054177	
#7 #2:27:25								97 92:27:58				55393				
2023-04-	142.251.214.142	192,168,101,102	441	38158	yactube	N/A		2823-84- 97	192,158	191.192 12	. 36, 131, 18	35863	53	des	0054977	
#2-27-00 2022-04-	142.251.214.142	192.168.101.102	442	38158	N/3.	N/3.	IN/A	82(27)57	192,158	.191.192 12	. 26. 121. 18	24947	53	dea	5054977	
87 87: 26: 25								82 82127155				36193				
2823-84 87	142.251.214.142	192,168,101,102	442	38159	yostate	N/2.		2823 84 97	192, 198	. 191 . 192 17	. 96, 131, 18	44058	53	des	5954977	2
82.20.00	142.251.214.142	102.165.101.102	40	381.59	yostube	N/A		2823-84+	192,158	. 101 . 102 17	. 36. 131. 18	45534	53	des	5854377	,
67 62:25:59								92:27:55				53376				
2023-04+ 02 02-20-24	140.251.214.142	112,165,101,102	441	38154	N/A	N/A	N/A	7823-84+ 92 92-22-54	197, 198	191,192 12	1.36,131,18	54166 59168	53	des	5954977	
2822-64-	142.251.214.142	192.168.101.102	40	38158	yastate	N/A		2823-84-	192,198	. 101. 102 12.	. 26, 121, 18	37876	53	des	5854977	
87.75.98						-		80127.54				54961	-			
Sealer .	Data				4 PR0V	2 8	readily a						1 2 3	• 5 8 7	6 9 10	reitit s
Target		Cass														
AI ×		Al ×														
Host	rection Hows by I	nust Over Time														
Al																
9122				_											Biochael Conne	1016
0							-					_		-	 Unblacked Car 	netters
28.49	Nanay	Noci Apri	May	10%	1.15	Aug.st.	bas	enter ocui	60	Nevenber Di	orter Ja	1997 23	Privay 1	Gr13		
Labler	f Connection:				Half Ona	n Connection	1994				Rinder	0000-7				
Uniciticities	. comections		_		Han Opener	- cennectic	a0	_			endexed	.omfett	v- 3		_	
		40					3	8					-	30		



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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.

OC Overview XOR Overview Threat Inspection Flow	Analysis	Search	cisco
KDR Overview Intended detection and response (XDR) deliver visibility into data as	cross networ	cs, clouds, endpoints, and applications while	Edt Export •
pplying analytics and automation to detect, analyze, hunt, and rem	ecliste today	s and tomorrow's threats.	
ime Range Source Router			
Alline •	но	- HERE	
Number Of Platform Errors 1 457 873		Number Of Engine Write Fails	•
1,437,873		20	·
Target Class			
×IA			
Alerts On - Today (with 7 days Trend)		Alerts Off - Today (with 7 days Trend)	
Time Range filter won't be applicable for this panel.		Time Range filter won't be applicable for t	this panel.
O -20,000		10,00	0 10,000
40		_	_
τ.	_		
8**			- c
January Petraary March April 2022	May	Jane July	August
	Time		
Top 10 Source IPs		Top 10 Destination IPs	
Source IP =	Count =	Destination IP #	Cor
192.168.12.10	449431	288.67.228.228	33
192.168.11.10	427654	246.67.222.222	33
10.1.10.10	36	13, 197, 21, 284	
172.19.111.15	17	10.0.12.135	
192.0.2.1			
192.168.2.1		146.112.61.126	
		146.112.01.106 128.30.52.100	4
	1	146.112.01.186 128.30.52.180 89.230.73.97	
	1	146.112.01.106 128.30.52.100 89.228.73.07 146.112.61.104	4 1 1
	1	146.112.01.186 128.30.52.188 86.238.73.37 146.112.61.184 31.13.71.174	
Top 10 Pairs Of Source and Destination IPs	1	146, 112, 01, 186 128, 30, 52, 180 88, 228, 73, 67 146, 112, 61, 184 31, 13, 71, 174	, , , , , , , , , , , , , , , , , , ,
Top 10 Pairs Of Source and Destination IPs Source IP 1 Destin	1 nation IP 0	146,112,61,186 128,28,22,180 88,228,73,37 146,112,61,184 31,13,71,174	a T T T T
Top 10 Pairs Of Source and Destination IPs Source IP 1 Destin 192, 161, 12, 19 201, 42	1 nation IP 0 7, 220, 220	146,112,31,388 138,30,30,180 89,220,71,87 146,112,31,384 31,13,77,174	4 1 1 1 1 1 1 1 1
Top 10 Pairs Of Source and Destination IPs Source P 1 Death 10 10 10 10 10 2014.5 192, 164, 12, 10 2014.5	1 netion IP 0 7.222.222	146,112,31,188 178,30,32,189 86,328,72,37 186,112,31,186 31,13,77,174	4 1 1 1 1 1 1 1 1 1 1
Top 10 Parks Of Source and Destination IPs Source 9: 9: 044, 12, 19: 294, 42 192, 144, 12, 19: 294, 42 192, 144, 11, 19: 294, 44 192, 144, 11, 19: 294, 44	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	146,112,41,186 178,32,62,186 82,829,73,97 146,112,41,184 31,13,77,174	4 1 1 1 1 1 1 1 1 1 1 1 1
Top 10 Pins Of Source and Destination (P) Outlin 50xes # 3 Outlin 10: 141, 12 241, 42 10: 241, 12, 10 241, 42 10: 241, 12, 10 241, 42 10: 241, 12, 10 241, 42 10: 241, 11, 10 241, 42 10: 241, 12, 10 241, 42	1 ation IP 0 7.220.220 7.220.220 7.222.222 7.222.222	146,112,41,180 178,10,63,180 82,282,73,27 146,112,41,184 31,13,71,174	ے میں
Top 10 Pars of Savure and Destination IPs Savari # 1 Deam 100:146.17.0 244.6 100:146.17.0 244.6 100:146.17.0 244.6 100:146.17.0 244.6 100:146.17.0 244.6 100:146.17.0 244.6 100:146.17.0 244.6	1 aution IP 0 7.220.220 7.222.222 7.222.222 7.222.222 7.222.223 7.222.223	146, 112, 43, 106 (123, 36, 23, 23, 24) (36, 30, 36, 24) (36, 112, 24), 104 (36, 112, 24), 104 (37, 112, 24), 104	
Top 10 Pars Of Source and Destination IP Outs Source IF J Outs 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244. 10: 14: 13: 14 244.	1 aution #* 0 7, 220, 220 7, 222, 222 7, 222, 223 7, 222, 223 7, 222, 223 7, 220, 220 9, 197, 200	146,1124,139 126,232,232 146,112,245 146,112,245 146,112,245 146,112,245 146,112,245 146,112,245 146,112,245 146,112,14514,145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145145 146,145	د می ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱
Top 10 Pain Of Sauce and Destination (IP) Data Sauce of 1 Data 10: 140: 0.19 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44 10: 140: 1.0 20: 44	1 aution #* 0 7.220.220 7.222.222 7.220.220 7.222.222 7.220.220 9.197.200 9.197.200	146.112.415.106 1136.106.2010.112 146.112.415.104 146.112.415.104 31.01.01.017.174	د د د د د د د د د د د د د د د د د د د
Top 10 Pars Of Source and Destination (PK Source # F Data 101, 141, 13 Data 102, 141, 14 Data	1 aution № 0 7.220.220 7.220.220 7.220.220 7.220.220 7.220.220 9.197.200 9.197.200 9.197.200	144, 174, 174, 174 184, 194, 194, 194 184, 174, 274, 194 194, 174, 274, 194 194, 174, 194	د من المراجع ال المراجع المراجع ا المراجع المراجع ا المراجع المراجع
Tay 10 Pairs Of Sacres and Destination (W - Sacres W - Sacres W - 10 101 Adv 11 0 204 Adv 11 102 Adv 11 0 204 Adv 11	1 ation #* 0 7.220.220 7.220.220 7.220.220 7.220.220 7.220.220 9.197.200 9.197.200 9.197.200 9.197.200 9.197.200	44.112.4134 2013.402.448 2013.202.448 2013.202.414 2013.202.414 2013.202.415 2013.2	
Top 10 Parts of Saurce and Destination IV Saurce IV Dears 100:144.7.1.0 Dears 100:145.7.1.0 Dears	1 aution #* 0 7. 220, 220 7. 222, 222 7. 222, 222 7. 222, 222 9. 197, 200 9. 197, 200 9. 197, 200 9. 197, 200 9. 197, 200	14.112.1196 123.193.194 142.112.113 144.112.01.114 145.112.01.114 145.112.01.114	4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Top 10 Pars Of Source and Destination (FW) Destination (FW) Source # F Destination (FW) Destination (FW) 101, 101, 101 Destination (FW) Destination (FW) 102, 104, 104, 101 Destination (FW) Destination (FW) 102, 104, 104, 104 Destination (FW) Destination (FW) 104, 104, 104, 104, 104, 104, 104, 104,	1 aution #* 0 7. 220, 220 7. 222, 222 7. 222, 222 7. 222, 222 9. 197, 200 9.	14, 11, 24, 11, 104 154, 112, 114 144, 112, 24, 114 144, 112, 24, 114 15, 13, 11, 134 15, 13, 11, 134 Top 10 Responder by Traffic Destination P I	
Top 10 Pars Of Saurce and Destination (IV Dear Saura IV Dear 102:144:0.7.0 204:14 102:144:0.7.0 204:14 102:144:0.7.0 204:14 102:144:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14 102:145:0.7.0 204:14	1 attion IP 0 7, 220, 220 7, 222, 222 7, 222, 222 7, 222, 222 7, 222, 223 7, 222, 223 7, 222, 223 9, 197, 200 9, 197, 200 1, 2	14.11.2.1.194 13.102.14 14.102.14.14 14.102.11.14 14.102.11.14 14.102.11.14 14.102.11.14 15.102.11.14 15.102.11 15.102.11 15.102.11 15.102.11 15.102.11	4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Top 10 Parsy Of Source and Destination UN Data Store # 4 Data 100, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 102, 144, 73, 10 204, 44 103, 144, 73, 10 204, 44 104, 104, 104 204, 44 104, 104, 104 204, 44 104, 104, 104 204, 44 104, 104, 104 204, 44	attion 8° 0 7,220,220 7,222,222 7,222,222 7,222,222 7,222,222	144.112.1196 128.193.2196 149.219.112.11 149.112.01144 149.112.01144 149.112.01144 149.112.01144 Порто D Responder by Turtite Destination IF 4 149.12.112 13.112.1128	
Top SD Pain Of Source and Description Data Source P 1 Data 100 140 7.0 1 244 4 100 140 7.0 1 244 4 100 140 7.0 1 244 4 100 140 7.0 1 244 4 100 140 7.0 1 244 4 100 140 7.0 1 244 4 100 140 7.0 1 244 4 100 140 7.0 1 244 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 100 140 7.0 1 101 4 101 140 7.0 1 101 4 101 140 7.0 1 101 4 101 140 7.0 1 101 4 101 140 7.0 1 101 4	1 auton IP 0 2, 20, 20, 20, 20, 20, 20, 20, 20, 20, 2	на. 11.2.1.104 12.3.1.9.7.46 13.2.9.7.47 14.2.9.7.47 15.3.7.1.74 17.3.7.1.74 17.3.7.1.74 17.3.7.1.74 17.3.7.1.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.7.74 19.3.777 19.3.777 19.3.777 19.3.777 19.3.777 19.3.777 19.3.777 19.3.777 19.3.777 19.3.777 19.3.777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.7777 19.3.77777 19.3.77777 19.3.77777 19.3.77777 19.3.	
Top 50 Pars Of Source and Destination TV- Source #1 Deam 501 All 2, 10 Deam 502 All 2, 10 Deam 503 All 2, 10 Deam 504 All 2, 10 Deam	1 atton IP 0 7, 220, 220 7, 200, 200 8, 197, 200 8,	14.11.21.194 13.19.3.194 14.11.21.41.14 14.11.21.41.14 14.11.21.41.14 14.11.21.41.14 14.11.21.41.14 14.11.21.41 14.11.21.41 14.11.21.41 14.11.21.14 14.11.14 14.14	
Top 30 Pairs Of Source and Destination (Feb Value) Database (Feb Val	* atton \$* 0 7, 220, 220 7, 210, 200 7, 200	 На. 112.10.104 На. 112.104 На. 202.104 На. 202.104 На. 112.101 На.	
Top 10 Part Of Source and Destination W Store # 0 Deam 100 144 0, 0 Dea	1 1 1 1 1 1 1 1 1 1 1 1 1 1	14. 11. 24. 194 23. 24. 25. 24 24. 24. 25. 24 24. 12. 26. 144 24. 15. 26. 144 25. 15. 15. 15. 15. 15. 15. 15. 15. 15. 1	
Top 30 Pairs Of Slocce and Destination (Weights) Destination (Weights) Destination (Weights) Status 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 20 (Weights) 100 (Weights)<	1 1 1 1 1 1 1 1 1 1 1 1 1 1	 Ha 11.2.1.194 Ha 11.2.1.194 Ha 12.2.1.9.2.1.49 Ha 20.2.1.9.1.41 	
Top 50 Paris Of Sources and Description Data States # 5 Data 100 144 0.20 204 04 100 144 0.20 204 04 100 144 0.20 204 04 100 144 0.20 204 04 100 144 0.20 204 04 100 144 0.20 204 04 100 144 0.20 204 04 100 144 0.20 204 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 100 144 0.20 104 04 101 145 04 104 04 101 145 04 104 04 101 145 04 104 04 101 145 04 104 04 <td>1 1 1 1 1 1 1 1 1 1 1 1 1 1</td> <td> Ha, 11, 24, 104 Ha, 13, 24, 35, 24 Ha, 13, 24, 34 Ha, 14, 34<</td> <td></td>	1 1 1 1 1 1 1 1 1 1 1 1 1 1	 Ha, 11, 24, 104 Ha, 13, 24, 35, 24 Ha, 13, 24, 34 Ha, 14, 34<	



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

Threat Inspection dashboard

Description

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





Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

Flow Analysis

Description

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





Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

- 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



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

Custom Searches

Description

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

splunk	c>enterprise	Apps 🕶	II Administrator ▼ 2 Messages ▼ Settings ▼ Activity ▼ Help ▼ Q Find
SOC O	verview XI	R Overview Threat Inspection Flow Analysis Custom Searches Search	ւլիսիս cisco
Cust	tom Sear	Source Router Log Types Custom Search	Edit Export •
All tin	ne	Ali Ali Ali Ali	Hide Filters
Raw B	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 T5:00000010585102587819 %Fr ate: 5	-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current r
	15/00/2022	nost = crestdatasys source = /opuspiunk/vai/spool/spiunk/868/4ffe29deaeta_events.stasn_new source	ype = cisco.sdwan.aiert.on
	15:13:15.889	Sep Is 15:13:15:889: XL05XE-6-PLATFORM: F0: CPD_CP: LPP:00 Infread:056 IS:0000001058510258/819 XF1 ate: 5 host = crestdatasys source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new source	-4-ALEXI_UFF: (target:class)-(inzout:class-default): calming down, count (40/45) current r yppe = ciscosdwankalertoff
>	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 %F1 ate: 5 host= crestdatasus source = /ont/snlunk/kar/cnon/isnlunk/Re874ffp20deaefa events stash_new source	-4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current r
>	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 %Fi ate: 5	ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current r
>	15/09/2022 15:13:15.889	nost = crestalatasys	<pre>ype = ciscussiverilaterion -4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current r here = ciscussiverilaterioff</pre>
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 T5:00000010585102587819 %Fi ate: 5	ype Cuccanonananancon -4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current r
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 T5:00000010585102587819 %Plate: 5 best = crestdatasus = course = /ont/snlunk/kar/cnon/isnlunk/Re824ffo20daada events stash_new = source	<pre></pre>
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 T5:00000010585102587819 %F1 ate: 5 host = crestdatasys source = /opt/splunk/var/spco//splunk/8e074ffc29deaefa_events.stash_new source	y -4-ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current r ype = cisco:sdwan:alertoff
>	15/09/2022 15:13:15.889	Sep 15 15:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 T5:00000010585102587819 %F0 ate: 5 hot= crestdatasys source = /ont/snlunk/var/cnon/isnlunk/8e874ffe29deaefa events stash new source	
>	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 %F1 ate: 5	<pre>ALERT_OFF: (target:class)-(in2out:class-default): calming down, count (40/45) current r</pre>
		host = crestdatasys source = /opt/splunk/var/spool/splunk/8e874ffe29deaefa_events.stash_new source	ype = ciscosdwan:alert.off « Prev 1 2 3 Next »



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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.

splunk>enterprise Apps •				Administrator •	Messages Settings	 Activity < Help 	Q Find
		vsis Custom Searches Alert	Actions - Search				ahaha
Event Threshold Net	ification					Edit	Evport x
Event Inresnoid Not	Alart Description	Cond Empil to *	Kouward to Mapitar*	Event Threshold	(greater then) *	Lui	
Alert Name	Alert Description	Send Email to	Keyword to Monitor	Event Threshold	(greater than)		
Time of Execution *	Mins past the Hour *						
Run Every Hour 👻	0 *						
Note: You can provide multiple emai	ils in "Send Email to" field by separatir	ng each email with comma. Example: te	est@cisco.com, user@cisco.com	1			
Submit Hide Filters							
Created Alerts							
Name ‡	Description ¢	Keyword \$	Threshold \$	Email ¢	Cron Schedule \$	Earliest Time ‡	Latest Time ‡
Keyword Alert abhi	fgdfgfghfghghfg	hello world	0	abcdx@xyz.com	04***	-1d	now
Keyword Alert abhi sinojia	fgdfgfgh	hello world Jay	0	abcdxq@xyz.com	06**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	06**1	0	
Keyword Alert sdgsfdgf		8^%^%^\$	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	8 * * * *	-1h	now
				-		<	Prev 1 2 Next »



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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.

splunk>enterprise Apps •				L 1	Administrator 👻 Messag	ges 🔹 Settings 👻 🗚	Activity • Help • Q Find
	Threat Inspection Flow Analy		Alert Actions - Se				սիսիս
							CISCO
Monitor Critical IPs							Edit Export •
Alert Name *	Alert Description	Send Email to *	IPs/CIDR to Mo	nitor *	Event Threshold (greater t	han) *	
ssdaf	dsavdv	abc@gmail.com	10.0.0.1		10		
Time of Execution *	Mins past the Hour *						
Run Every Hour *	0 -						
Net							
Note:	Manual Pressiliant Redaktor and	ale annull with a more firmanale.					
1. You can provide multiple emails in	Send Email to field by separating ea	ich email with comma. Example:	test@cisco.com, user@	PCISCO.com			
 z. rou can provide single IP address 	, multiple IPs (comma separated) or C	IDR address in "IPS/CIDR to Moni	itor field. Example1: 10	10.0.1 Example2: 10.0.0	.2, 10.0.0.3 Exmaple3: 10.0	0.1/24	
Created							
Submit Hide Filters							
Created Alerts							
Name ¢	Description ¢	IPs/CIDR ©	Threshold ¢	Email ¢	Cron Schedule ¢	Earliest Tim	ne © Latest Time ©
Critical IPs Alert ssdaf	dsavdv	10.0.0.1	10	abc@gmail.com	0 * * * *	-1h	now



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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.



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

 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. <u>Refer</u>

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.



Introduction

Pre-Requisites

Installation and configuration of Cisco SD-WAN

Configure inputs on Splunk for NetFlow data

Configure Event Types on Splunk Search Head Instance

Data searching

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

Troubleshooting

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.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) C07-3406706-01 07/23