Hunting for Evil:
Security Monitoring with Cisco Stealthwatch

LTRSEC-8421

Speakers:

Peter Johnson & Brian Ford
Technical Marketing Engineers | Security Business Group

Learning Objectives

Cisco Stealthwatch collects and analyzes network data to deliver comprehensive visibility and protection for even the largest and most dynamic networks. Stealthwatch analyzes industry standard NetFlow data from Cisco and other vendors Routers, Switches, Firewalls, and other network devices to detect advanced and persistent security threats such as internally spreading malware, data leakage, botnet command and control traffic and network reconnaissance.

As a key component to combat the stealthiest, sophisticated cyber-attacks by providing visibility into the most complex network threats by analyzing traffic patterns in the interior (LAN and borders) of the network. The Cisco Identity Services Engine (ISE) solution supplements Stealthwatch NetFlow based behavioral threat detection data with contextual information such as user identity, user authorization level, device-type, and posture. Together Stealthwatch and Cisco ISE present network security analysts with a view integrating NetFlow data and contextual information enabling the security analyst to detect and discern the potential severity of threats in a timely, efficient, and cost-effective manner.

This lab is designed to familiarize you with the use of the Cisco Stealthwatch solution. You will be interacting with a previously configured and deployed solution in a simulated enterprise environment.

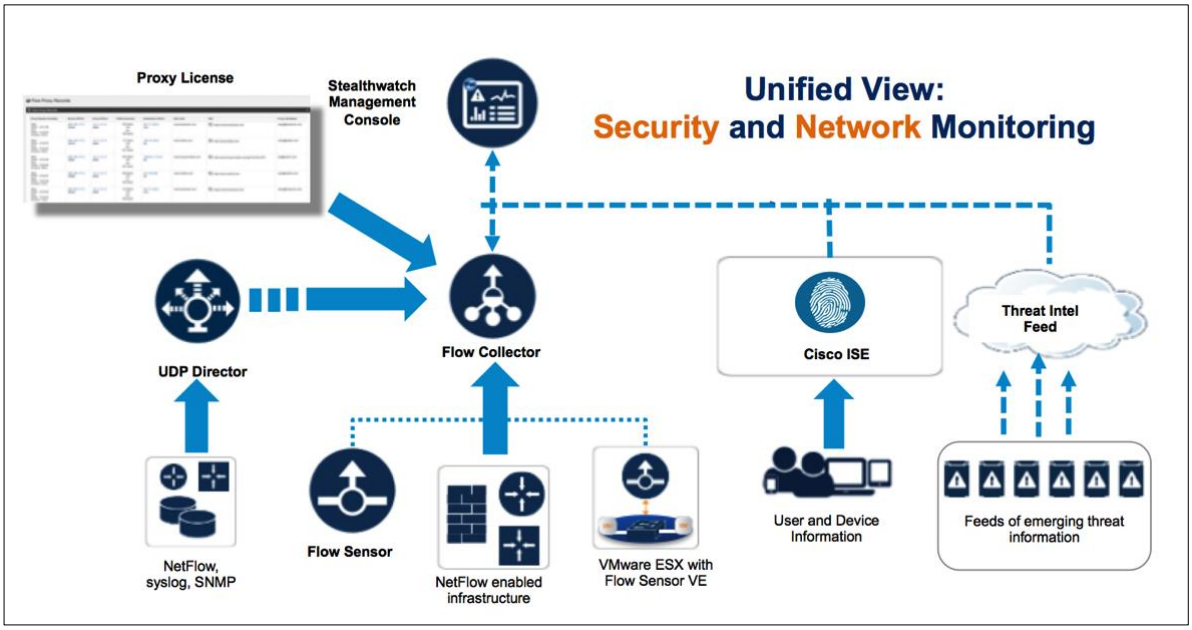
Stealthwatch components include:

• Stealthwatch Management Console

• Flow Collector

• Flow Sensor

• UDP Director



There are 15 different exercises in this lab.

Exercises 1 through 5 will familiarize users with the Stealthwatch product and the Web and Swing client interfaces.

- The Web Client (WebUI), which can be viewed as a snapshot of the overall network security posture/view that allows you to dig in deeper for context around events.
- Advanced Operational Console (Swing Client) Full customizable console UI for product installation and setup, advanced investigation, drill down, and data visualization.

Exercises 6 through 15 cover a wide range of uses cases and scenarios around the kinds of use cases and usage of the Stealthwatch product. Users will be investigating alarms and events taking place on the simulated network environment.

At the end of each exercise there will be questions relating to the activity. Please take a moment and answer these questions to the best of your knowledge. The questions will be reviewed at the end of the lab session.

This lab uses the GOLD Lab facilities to allow users to connect to and use a live deployment of Stealthwatch. The GOLD Lab is available within the Cisco Corporate network.

In order to use Stealthwatch in the GOLD Lab users will use RDP (Remote Desktop Protocol) to connect to a Windows PC in the GOLD Lab. From that Windows PC user will use both a web browser (Internet Explorer or Firefox) and the Stealthwatch Java (Swing) client.

Note: The Stealthwatch Swing client is a Java application. This client doesn't run in a web browser and as such there is no 'Java in a web browser' security concern.

Exercises

This guide includes the following exercises:

- Exercise 1: The WebUI
- Exercise 2: The Swing Client UI
- Exercise 3: Inspecting Host Group setup
- Exercise 4: Performing a flow query
- Exercise 5: Using documents
- Exercise 6: Confirming the configuration of a policy
- Exercise 7: Investigating an alarm
- Exercise 8: Worm Propagation Investigation
- Exercise 9: Insider Threat Detection
- Exercise 10: Identifying a DDoS Attack
- Exercise 11: Building an audit trail

Product Overview: Stealthwatch

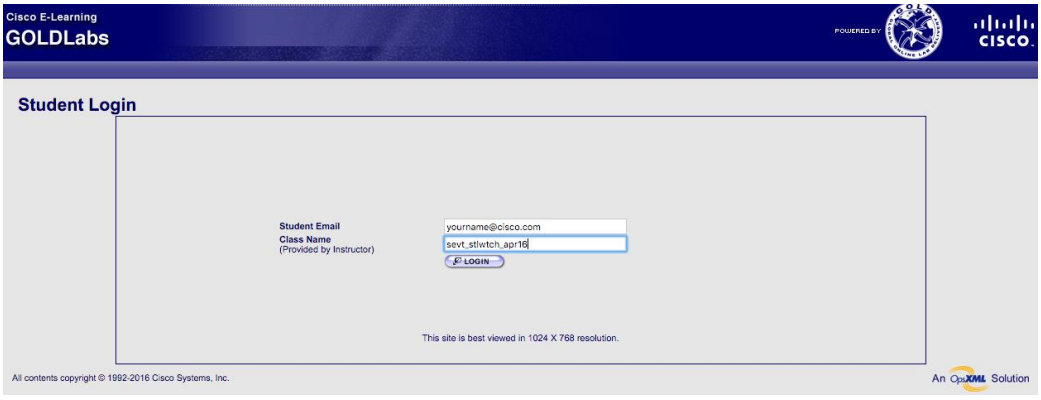
In these exercises, you act as the administrator of an existing Stealthwatch Cyber Threat Defense Solution deployment at ACME Corporation. The deployment has been pre-configured and is operational the day you arrive on site. Take a moment to familiarize yourself with the topology below before accessing the environment. Please ask your instructor any and all questions you may have about the product without hesitation.

Lab Topology and Access

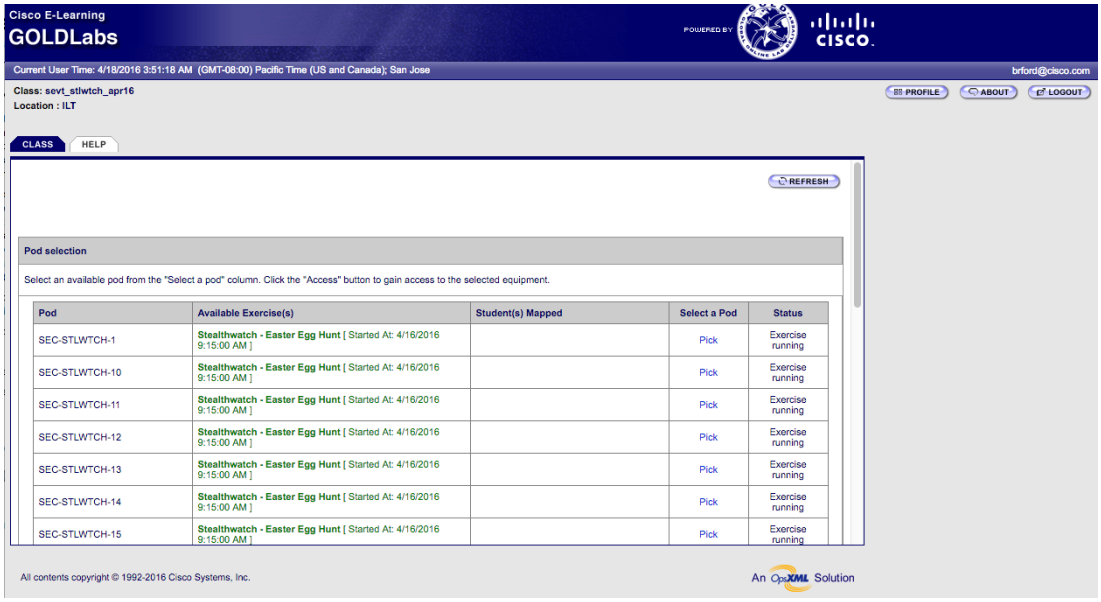
Each student has a dedicated, remotely accessible workstation from which the exercises will be conducted.

Using your web browser enter the URL:

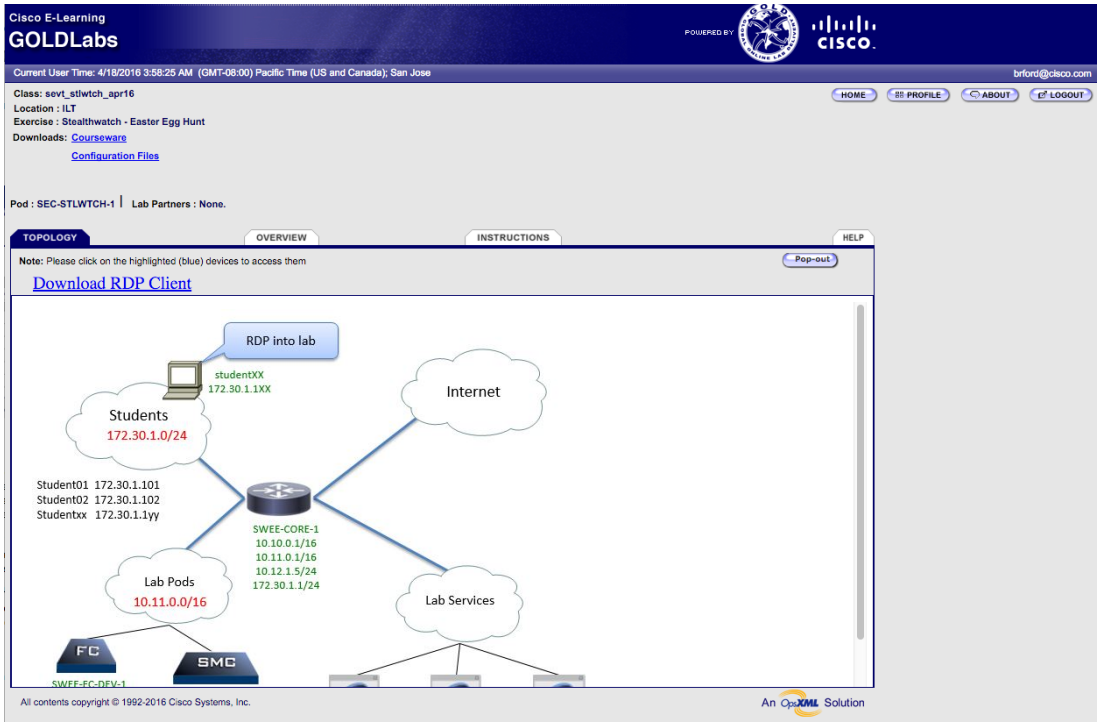
https://labops-out.cisco.com/labops/ilt



In the fields displayed enter your Cisco Email User ID for Student Email and the class name.



From the menu 'Pick' or select an available lab pod.



Details of how to access this workstation, as well as the other systems that will be used in the course of these exercises, are displayed on-screen at the end of the introductory presentation.

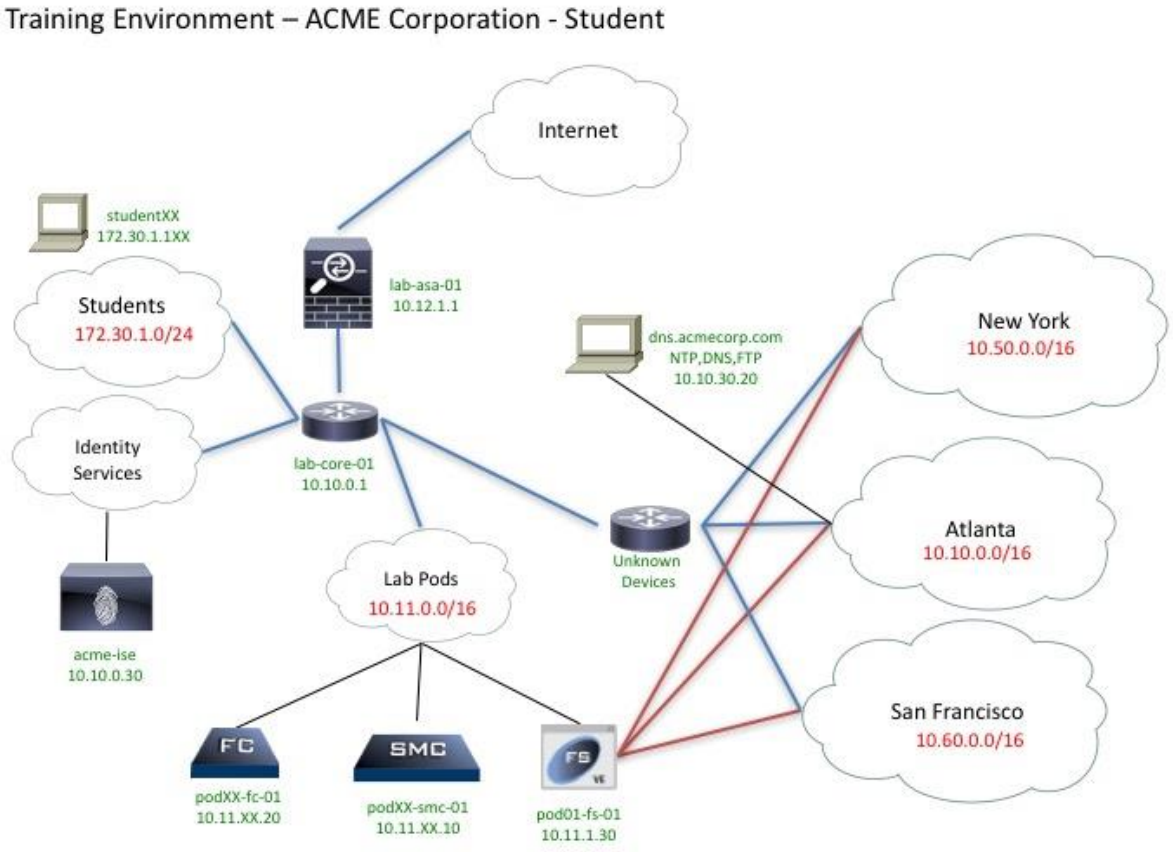
To connect to your workstation, perform the following tasks:

1. Using a Remote Desktop Protocol (RDP) client, connect to your assigned workstation using the IP address and port number shown on the information screen.
2. Log in using the credentials shown in the Student workstation box on the information screen.
3. You should now be connected to a Windows desktop system; from which you will perform the rest of the exercises in this guide.

NOTE: It is important that you connect only to your assigned workstation, so that you will not conflict with other students in the class when performing the exercises.

Lab Topology

This is the topology used for this lab.



Accounts and Passwords

The table that follows lists the accounts and passwords used in this lab.

Access To	Account (username/password)
Stealthwatch SMC	analyst/3aster3gg

Exercise 1: The WebUI

Exercise Description

Now that you are connected to the environment, the next step is to access the interface of the Stealthwatch Management Console (SMC). Please note that while you will be logging in as an administrator, the Stealthwatch systems are shared resources, used by other students and classes.

Exercise Objective

Understand the layout and tools available on the Stealthwatch WebUI dashboard.

Exercise Steps

Step 1 Using your web browser, connect via HTTPS to the Stealthwatch SMC shown on your Student Information Sheet.

Step 2 If a Certificate Error page is displayed, click on "continue to this website."

Step 3 Log in to your Stealthwatch Management Console using the credentials listed in the beginning of this document.

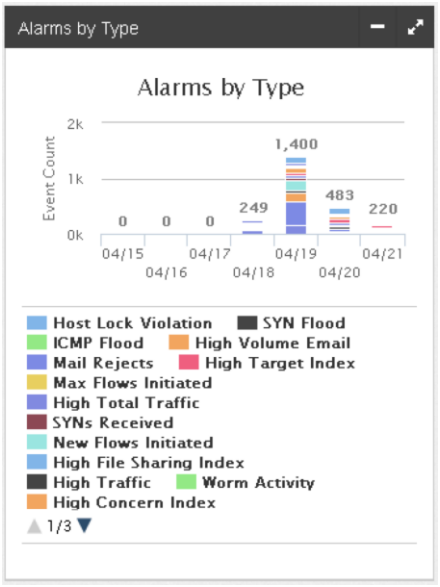
Step 4 Upon logging on, you will be presented with the SMC's WebUI Dashboard. Make note of the following information provided front and center about your network environment:

Step 5 Along the top, **Alarm Categories** with the current number of active alarms.

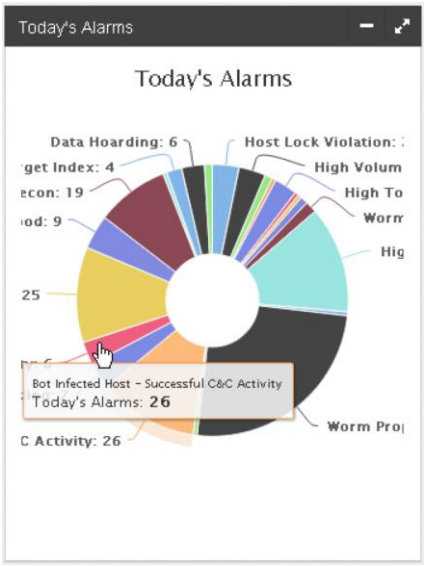
Clicking on a number will display details around the associated alarm type:

a. **Concern Index –** summarizes unusual behavior that could be malware
b. **Data Hoarding** – users/hosts observed moving large amounts of data
c. **Exfiltration** – users/hosts sending data outside of the network
d. **Recon** and **Exploitation** around a targeted attack
e. **Command and Control (C&C)** – botnet communication activity detected in the network
f. **DDoS Source** - alerts for an internal host potentially involved in DDoS activity)
g. **DDoS Target** - alerts for internal hosts potentially being targeted by DDoS acvitiy
h. **Policy Violation** -alarms triggered off of policies and custom events defined by the Stealthwatch system's administrator
i. **Anomaly** - Other anomalous detected behavior.

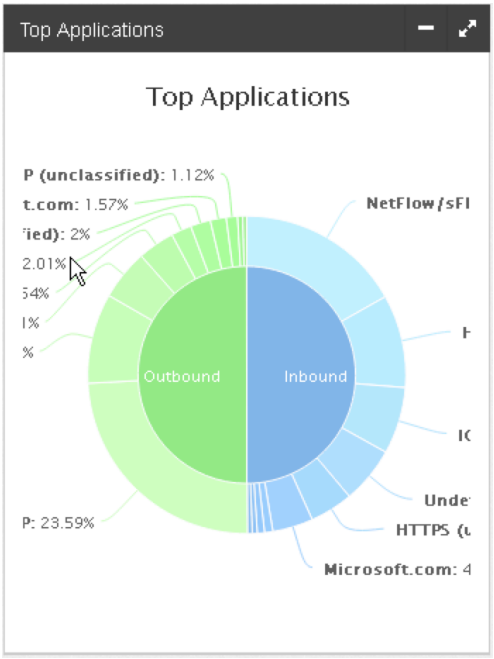
Step 6 **Alarms by Type**: A bar graph depicting the past week's alarm trends, broken down by day and alarm types. You can click on any of the Alarm types in the various presented days' bar graph to see the correlating alarm details for that day. You can click the arrows in the upper right corner of the box to expand the chart to fill the screen for easier reading.



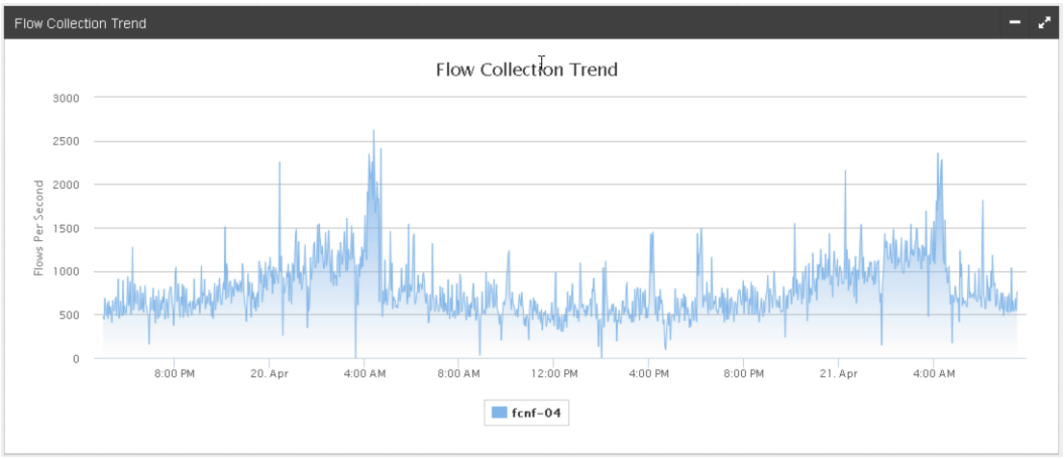
Step 7 **Today's Alarms:** This pie chart provides an overview of all alarms that have occurred in the present day. You can click on any of the Alarm types in the chart to see the correlating alarm details for the day. You can click the arrows in the upper right corner of the box to expand the chart to fill the screen for easier reading.



Step 8 **Top Applications:** This pie chart shows the top inbound and outbound application traffic types seen across your network.



Step 9 **Flow Collection Trend**: This chart shows the ebbs and flows of collected NetFlow activity from the past 48 hours.



Step 10 Along the left side of the WebUI, there are a number of options available allowing you to drill down into additional information about your enterprise. Clicking the [+] beside each will cause a list to drop down, with options you can select.

a. Under **Network**:

i. **Host** – This view displays all observed hosts on your network, as well as the alarms associated with them.

ii. **User** – This view displays all observed users on your network, as well as the alarms associated with them.

b. Under **Flows**:

i. **Flow Search** – Brings up the Flow analysis screen, which allows you do construct and execute queries into Stealthwatch's collected NetFlow database.

ii. **Host Search** – Brings up the Host Search screen which allows you to quickly query for information on an observed host, providing data on when it was first and last seen on the network, how much data transfer it was involved in, and other information, such as the peers it communicated with most.

iii. **Saved Queries** – A list of saved Flow searches that can be defined by Stealthwatch users to quickly query commonly searched for parameters.

iv. **Saved Results** – Once a query has been completed from the Flow Search interface, it can be saved and will appear on this screen.

c. Under **Tools** (not all options may be available here if you are not on an admin account):

i. **Settings** – Allows the Stealthwatch administrator to access a number of integration options, as well as install system updates.

ii. **Network Classification** – This currently locates hosts engaged in scanning activity not in the Scanners Host Group, or without a scanners policy applied.

iii. **Custom Events** – Brings up the Custom Security Events screen, which allows you to define custom alerts that will appear as alarms, based upon criteria.

iv. **Custom Applications** – Allows a Stealthwatch administrator to configure custom application definitions, based on observed attributes on the network.

v. **Job Management** – A list of Saved and Ongoing flow queries executed on the SMC.

Step 11 Feel free to investigate the features of the WebUI Dashboard. We will be covering many facets of it in the coming exercises.

Step 12 When you are done, click **Dashboard** in the left to return to the main **Dashboard** page.

QUESTIONS:

1. What three ways can be used to quickly get information around host(s) engaged in data hoarding activity?
2. What two ways can you access information about Hosts on your network?

Exercise 2: The Swing Client

Exercise Description

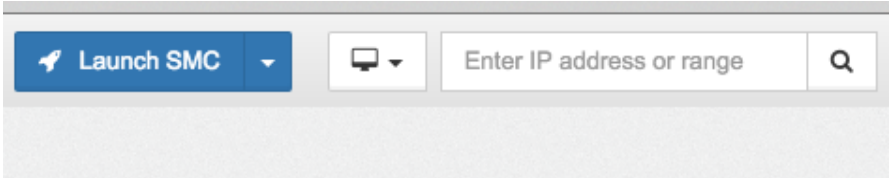
The Stealthwatch Management Console (SMC) provides a comprehensive, graphical view of the entire security infrastructure of your organization. All of the information gathered from NetFlow, ISE and NBAR-capable routers is combined into a single view.

Exercise Objective

Understand the layout and tools immediately available on the Stealthwatch Swing Client.

Exercise Steps

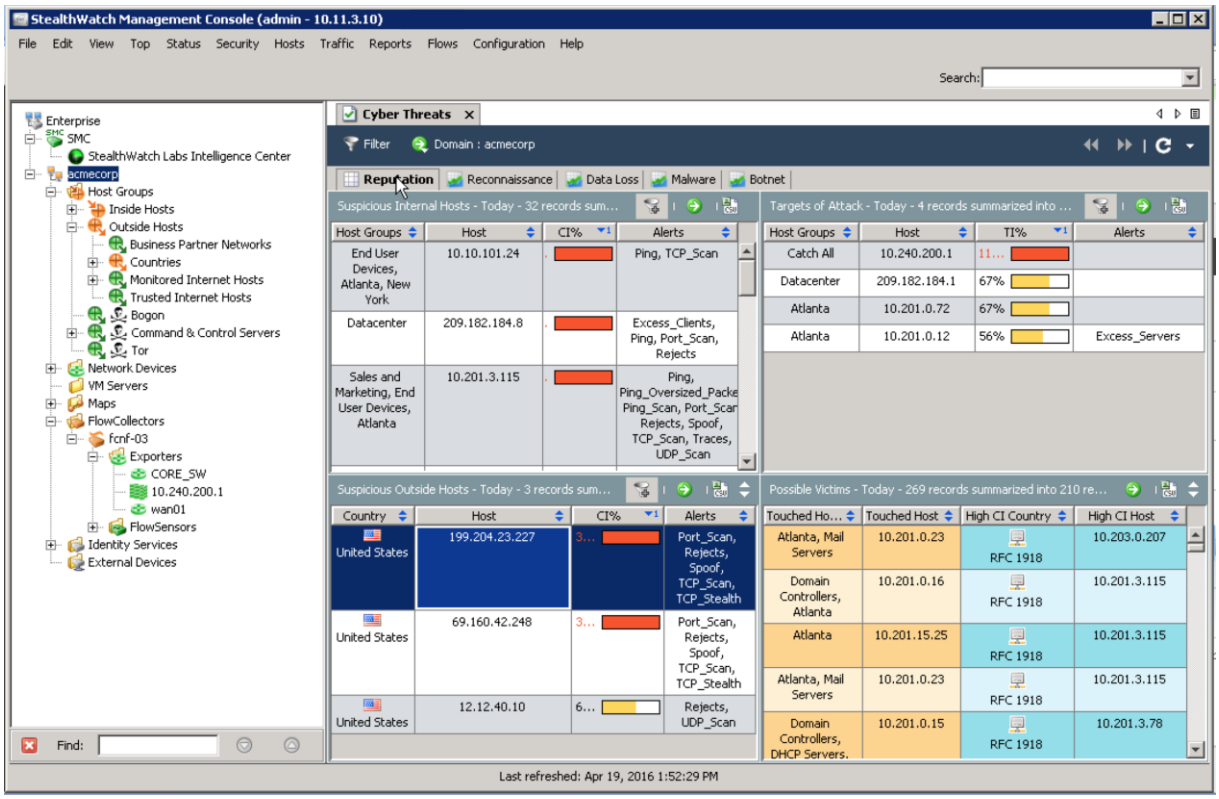
Step 1 From your workstation, launch the **Stealthwatch Management Console** Swing Client by clicking the **Launch SMC** button on the WebUI.



Step 2 Accept and continue through any security warnings.

Step 3 When prompted, login as **analyst/3aster3gg**.

Step 4 When you've successfully authenticated, you will be presented with the Stealthwatch Swing Client.



Step 5 The list of items in the left navigation pane of the Swing Client interface is often called the **Enterprise tree**. This tree displays the structure of your monitored network.

a. Click the plus and minus signs in the Enterprise Tree to investigate the branches of the **acmecorp** tree. The enterprise tree includes:

i. **Host Groups**—contains logical groupings of IP Address blocks.

ii. **Network Devices**—contains exporters, firewalls, and other network devices reporting to the system. If the exporter is a firewall or other flow-blocking device, the appropriate icon is displayed.

iii. **VM Servers**—contains VM servers (that is, ESXi hosts) being monitored by FlowSensor VEs. Each VM server folder contains the virtual machines (VMs) that exist on it, grouped according to their Resource Pool.

iv. **Maps**—contains relational flow maps, a graphical view of the status of multiple Host Groups, and any communications between them.

v. **Flow Collectors**—contains all the Stealthwatch FlowCollectors associated with the domain.

vi. **Identity Services**—contains devices that identify user information, such as Cisco ISE, associated with the domain. The Cisco ISE devices exist within a cluster, represented by a folder.

vii. **External Devices**—contains all the external devices, such as Snort test devices, that are associated with the domain.

NOTE: The color of the highest level of an item indicates the highest alarm level for any of the branches under that item. For example, if any of the branches under the Inside Hosts branch (located under Host Groups) are orange, the Inside Host level displays orange. This serves as a visual indicator that the branch has an alarm within its hierarchy.

Severity Level	Associated Color
Critical	Red
Major	Orange
Minor	Yellow
Trivial	Blue
Informational	Light Blue
No Alarm Exists	Green

Severity Levels

Step 6 Under the domain branch of the Enterprise Tree are the Host Groups. A Host Group is logical grouping of IP Address blocks. The Host Group structure is a hierarchical structure divided into two primary buckets – Inside and Outside. Host Groups are central to traffic and behavior monitoring. Behavior monitoring is performed for each host and Host Group, and is compared against the baseline behavior for that group.

a. Click the plus sign on the **Host Groups** heading.

b. Click the plus signs in the **Inside Hosts** and **Outside Hosts** groups to view how these hosts are organized.

c. By default, the Inside Hosts folder contains a folder named **Catch All**, which contains the large IP ranges that correspond to the target network. You cannot rename, move or delete the Catch All folder. The Catch All Host Group properties can be edited to define which IP ranges to add to this folder.

NOTE: You can hover the cursor over various elements in the SMC client interface to display summary information about the element.

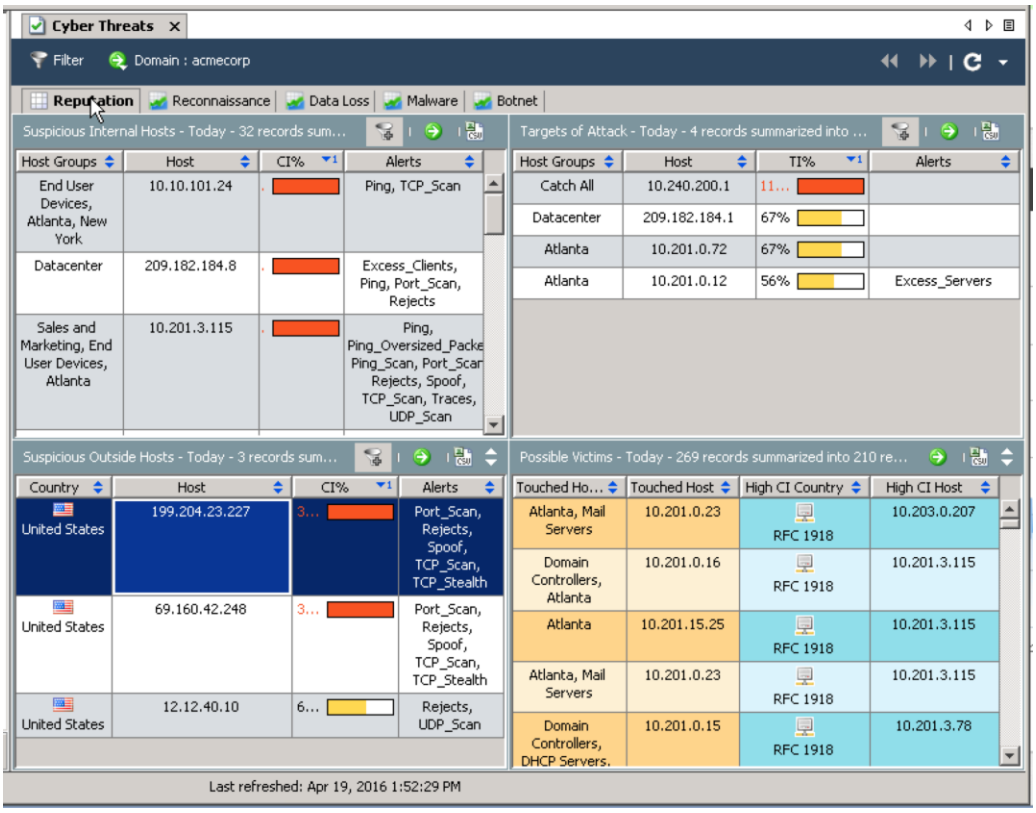
---

d. Expand the tree to view **Host Groups > Inside Hosts > Business Units > Engineering**.
e. Right-click the Engineering group and select **Configuration > Host Group Properties**.
f. The Edit Host Group window opens and displays hosts with IP addresses within the defined network ranges.
g. Click **Close** to return to the SMC interface.

Step 7 To the right of the Enterprise Tree is a tabbed interface that displays **Dashboards and Documents**. The SMC displays tables and charts, with system data displayed as documents in the center of the SMC GUI. The active document is the document you are currently viewing.

a. Active documents refresh automatically, while Inactive documents do not.
b. Users should manage the number of documents that are open, as they do not time out or close automatically.

Step 8 By default, when you login to the Swing Client the **Cyber Threats** Dashboard will be displayed in the document window.



Step 9 The Cyber Threats Dashboard is designed to track the following:

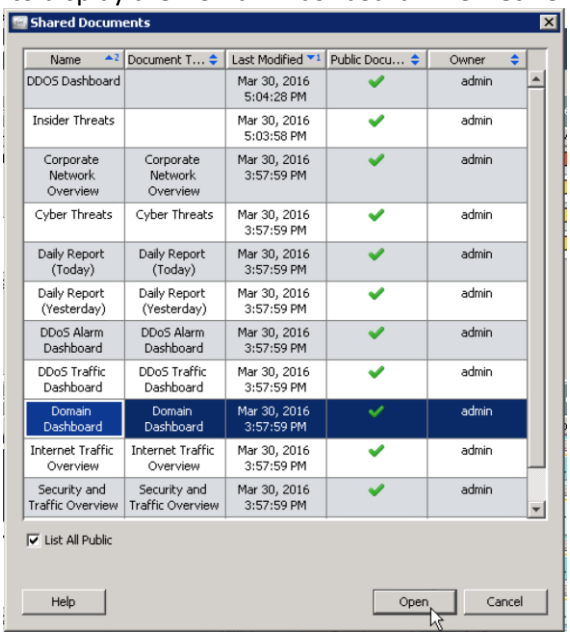
a. **Reputation** - High-level information about suspicious internal and external hosts.
b. **Reconnaissance** – probing of the network to uncover attack vectors that can be leveraged for customized attacks.
c. **Data Loss** – the export of sensitive information back to an attacker, generally via command-and-control communications.
d. **Malware** – the spread of malware across hosts on the internal network to gather security reconnaissance information, steal data or create backdoors for infiltrating a network.
e. **Botnet** – command and control communications between attackers and compromised hosts within the network.

Step 10 The Domain Dashboard provides a high-level view of potential threat activity on your network.

a. Highlight the **acmecorp** domain in the Enterprise tree.

b. From the menu options, select **File > Open**, and select the **Domain Dashboard** from the **Shared Documents** listing. Make sure that **List All Public** is checked.

c. Click **Open** to display the **Domain Dashboard**. The **Network Map** tab displays.



d. Select the **Summary** tab.

NOTE: The High Concern Inside Hosts table on the Summary tab is set to filter the results to show only high concern hosts. If the table is empty, no high concern hosts exist in the network at this time. Uncheck the filter to see hosts that are not exhibiting high concern behaviors.

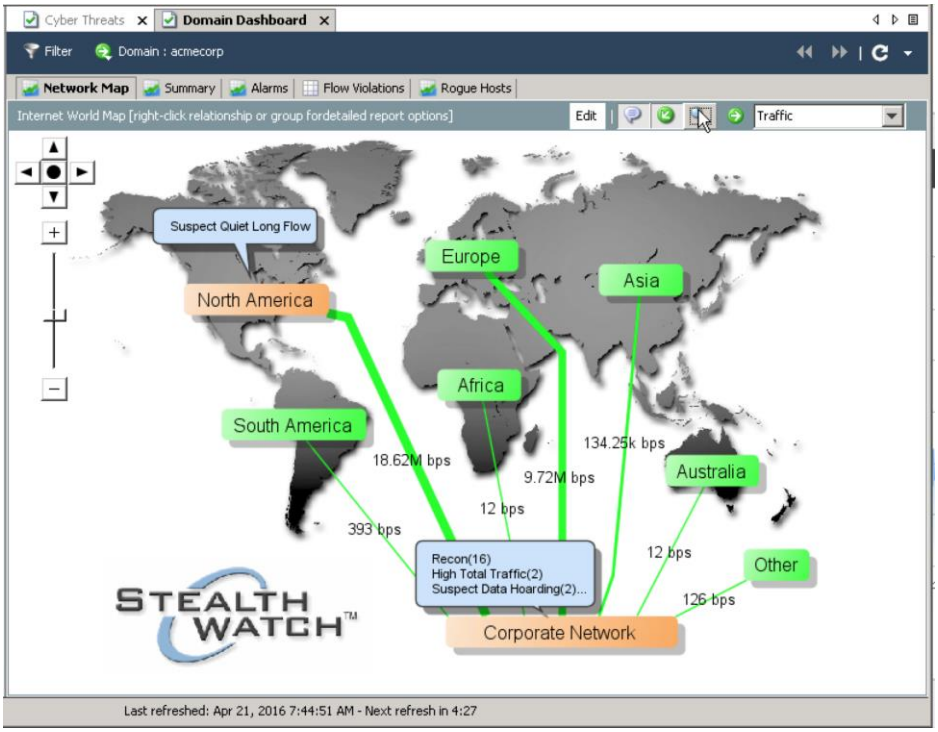
---

   i. The panels here provide an overview of Hosts exhibiting the most signs of concern and alarms, possibly requiring investigation. Traffic patterns for the last 24 hours are presented visually to reference for any anomalous activity.

e. Select the **Alarms** tab.
   i. All current active alarms, as well as alarm trends for the last week, are presented here.

f. Select the **Flow Violations** tab.
   i. All currently defined Host Locking rules are displayed and detailed here, as well as the number of times the rule has been violated today.

g. Select the **Rogue Hosts** tab.
   i. This tab shows all observed internal hosts not currently assigned to a Host group.



Step 11 You will very likely have accumulated a large number of open tabs in your SMC display. As a quick way to clean up, press ctrl + shift + W to close all open tabs at once. Then select **Status > Dashboards > Cyber Threats Dashboard** to return to the original state at the beginning of the exercise.

QUESTIONS:

1. Where can you find a library of preconfigured dashboards for visualizing your collected netflow data?
2. What does a light blue alarm color mean?

Exercise 3: Inspecting Host Group setup

Exercise Description

Host Groups are an important part of the way Stealthwatch organizes information and classifies traffic and behavior patterns. The deployment has been pre-configured with Host Groups to reflect the IP Address space of ACME Corporation, including both built-in Host Groups as well as customer-defined Host Groups for this deployment.

Exercise Objective

The goal of this exercise is the get an overview on the existing Host Group configuration and to know how to classify host and groups. Classifying hosts and Host Groups allows easier and enhanced monitoring and policy assignment.

Exercise Steps

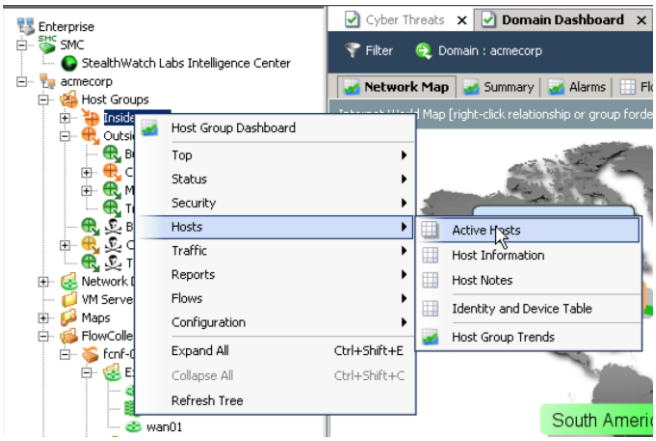
Step 1 This exercise takes place in the Swing Client. Make sure you have it in the foreground.

Step 2 Review built-in Host Groups

a. From the Enterprise tree Expand the plus sign next to the **acmecorp** domain

b. Expand the plus sign next to Host Groups, as a result the two default Host Groups displays, **Inside**, **Outside**

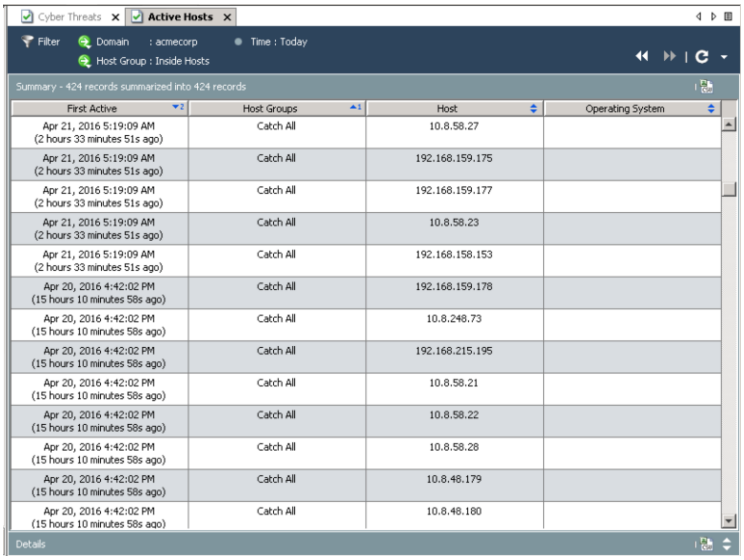
c. Right click on **Inside Hosts** and Select **Hosts > Active Hosts.** As result the Active hosts document displays listing all active hosts classified as inside.



d. Click the **Host Group** column header to sort by **Host Group** classification. Notice that a lot of IPs belong to the **Catch All** Host Group.

i. **Catch All** Host Group is configured by default to include all private IP ranges (RFC 1918) as its members

ii. It's recommended that you include all the public IP ranges that are assigned to the enterprise under the catch all group



Step 3 Review **Catch All** Host Group

a. Right-click on the **Catch All** Host Group and select **Configuration> Host Group Properties**

b. The edit Host Group dialog will display, notice the configured private IP ranges under **Ranges**

c. Click **Close** to exit

Step 4 Using the **Search** field:

a. Type the IP address of SMC in your lab in the **search field** that is top right corner of the Swing Client GUI then click **Enter**

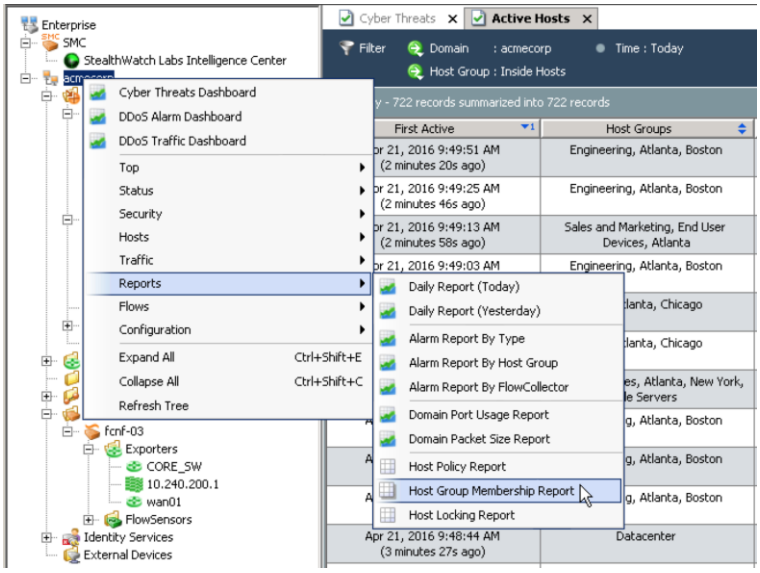
b. The search result window will appear with the **SMC IP** in the list

c. Right-click on the entry for your SMC IP Address in the results window and select **Configuration > Manage Host Groups**. Note the Host Group that your SMC belongs to.

d. Close the Host Groups window and repeat the process for the IP address of your student desktop system. Is it in the same group(s) as the SMC?

Step 5 Using Host Group Membership Report

a. Right click on the **acmecorp** domain select **Reports > Host Group Membership Report.**



b. The **Host Group Membership Report Opens**

c. The report view can be customized

i. Right click on any column Header. This will allow you to check and uncheck report options to display or hide columns (**Note**: this is valid for all reports in Stealthwatch)

d. Click on the Column header to sort ascending or descending the results in the fields> (**Note**: this is valid for all reports in Stealthwatch)

e. Examine the results. How many inside and outside Host Groups are defined.

f. Right-click the **By Function** Host Group under **Inside Hosts** and select Expand All. Notice that not all of the Host Groups shown in the enterprise tree also appear in the **Host Group Membership Report tab**.

g. When you are done with the exercise, clean up by closing the Host Group Membership Report tab, then right-click **By Function** in the enterprise tree and select **Collapse All** to reduce visual clutter.

QUESTIONS:

1. What does the Catch All Host Group contain by default?
2. Can you produce host membership reports for Host Groups defined deeper inside the Enterprise tree?

Exercise 4: Performing Flow Queries

Exercise Description

For this exercise, we want to demonstrate how to search for specific devices on the network. Let's look at a simple exercise that will allow us to use the flow data to determine this information.

Exercise Objective

Learn how to craft flow queries in both the Swing Client and WebUI.

Exercise Steps

Step 1 Let's first get acquainted with the basics of the Flow Table and how to access this document. This part of the exercise takes place in the Swing Client. Make sure you have it in the foreground.

NOTE: It is important to remember that while it is certainly possible to access large amounts of flow data at a time, this is usually not an efficient starting point; best practice is to start with higher level data, and then focus in on only the relevant flows.

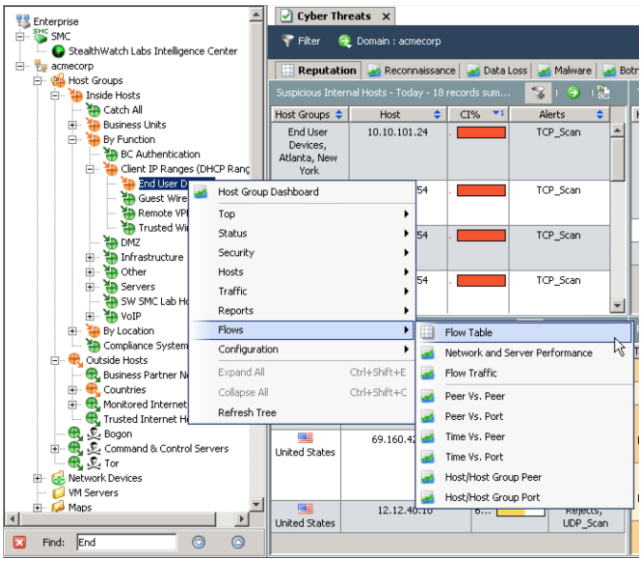
Step 2 Click on **acmecorp** in the enterprise tree.

Step 3 In the **Find** field on the bottom of the enterprise tree pane, type **End** and press **Enter**.

NOTE: The **Search** field in the upper right corner searches through actual flow data; the **Find** field searches for named objects in the enterprise tree.

Step 4 Your search should return the **Inside Hosts > By Function > Client IP Ranges (DHCP Range) > End User Devices** Host Group.

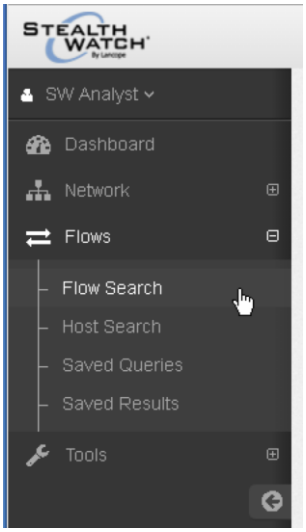
Step 5 Right-click the **End User Devices** Host Group and select **Flows > Flow Table**. How many records are returned?



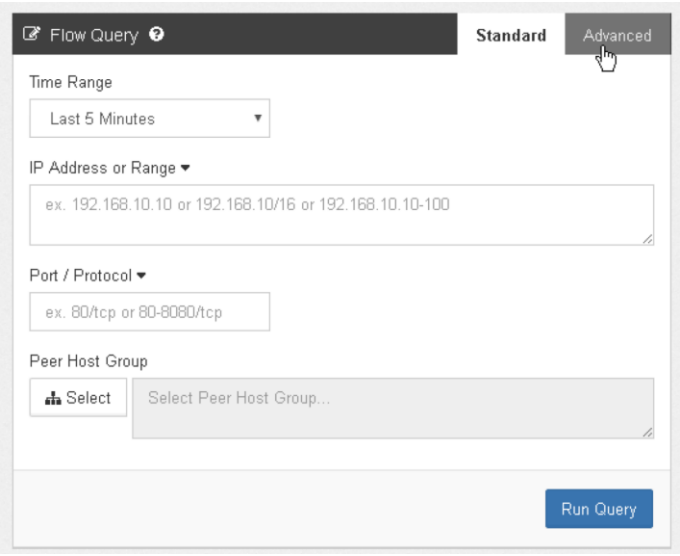
Step 6 Close all of the Flow Table Documents in your SMC to clean up after this part of the exercise.

Step 7 The second part of this exercise takes place in the SMC WebUI. Minimize the Swing Client so the web browser with the Dashboard visible is in front.

Step 8 Select **Flows > Flow Search** on left navigation panel.



Step 9 Select **Advanced** search tab



Step 10 Set the following filters:

a. **Range**: 5 minutes

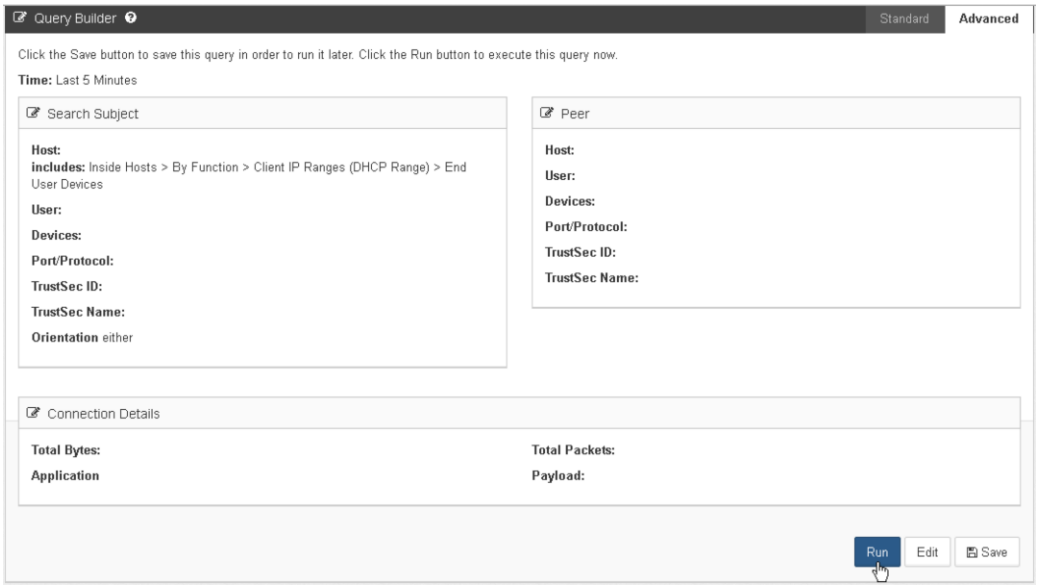
b. **Search Subject**:

i. For Host, select **Inside Hosts > By Function > Client IP Ranges (DHCP Range) > End User Devices**.

ii. Leave the rest of the settings alone, but make note of the options available to you for fine tuning a query.

Step 11 Click **Review Query** at the bottom of the screen.

Step 12 Review your query settings, and click **Run** when ready.



Step 13 How many records are returned?

NOTE: The results returned here may vary from what was seen in the Swing Client, due to time of execution.

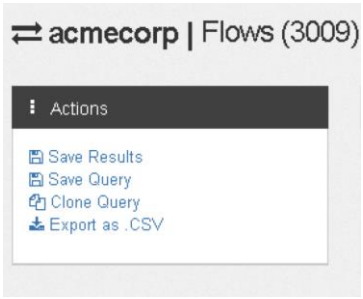
Step 14 Note the options available in the **Actions** panel when the query has completed:

a. **Save Results** – Saves the current results of the executed queries for later review. Saved results can be accessed from **Flows > Saved Results** in the left navigation panel.

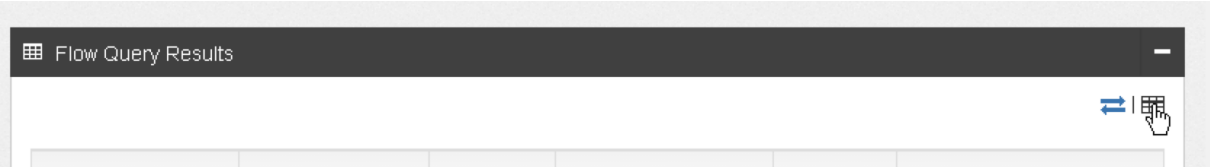
b. **Save Query** – Saves the current query parameters for use later. Saved queries can be accessed from **Flows > Saved Queries** in the left navigation panel.

c. **Clone Query** – Starts a new flow query with the parameters of the current one copied into the options.

d. **Export as .CSV** – Exports the current results into a .csv formatted file that can be downloaded to your local machine for external usage and analysis.



Step 15 In the top right corner of the Flow Query results panel, note the grid icon. Click it to switch to **Tabular** view.

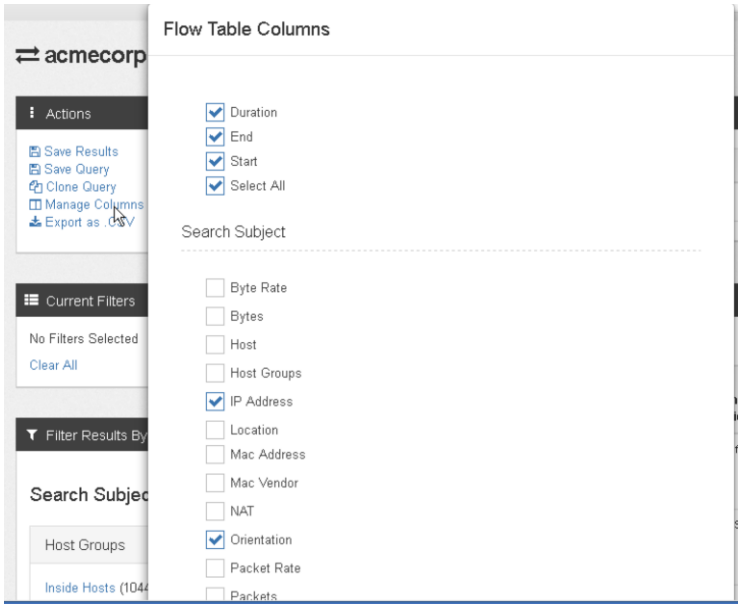


Step 16 In the **Actions** panel, note that you have a new option available: **Manage Columns**. Click it.

Step 17 Make note of the various other columns of information you can add to your Flow query results, giving you additional context around the activity.

a. To add additional columns of information, mark the check box beside the data attribute. You can add and remove to tailor the displayed results to your needs.

b. For now, click **Cancel**.



Step 18 Make note of the options available to you along the left side of the Flow Query Results table to refine your results.

Step 19 Click the **Dashboard** link on left navigation panel to return to the WebUI's dashboard screen. You are done with this exercise.

QUESTIONS:

1. How many different device host IPs are associated with the user **Ethel**?
2. What are any three additional columns of information available to you in the **WebUI**'s Flow query results?

Exercise 5: Using Documents

Exercise Description

Stealthwatch can display flows and statistical information in numerous ways. Documents are opened and displayed on the right panel whenever a query or a report is requested such as Flow queries and Top reports. In addition to the documents that are opened when the Swing Client launches, the SMC has a large number of other documents and dashboards predefined. This exercise examines a few of them that may be of interest to many customers.

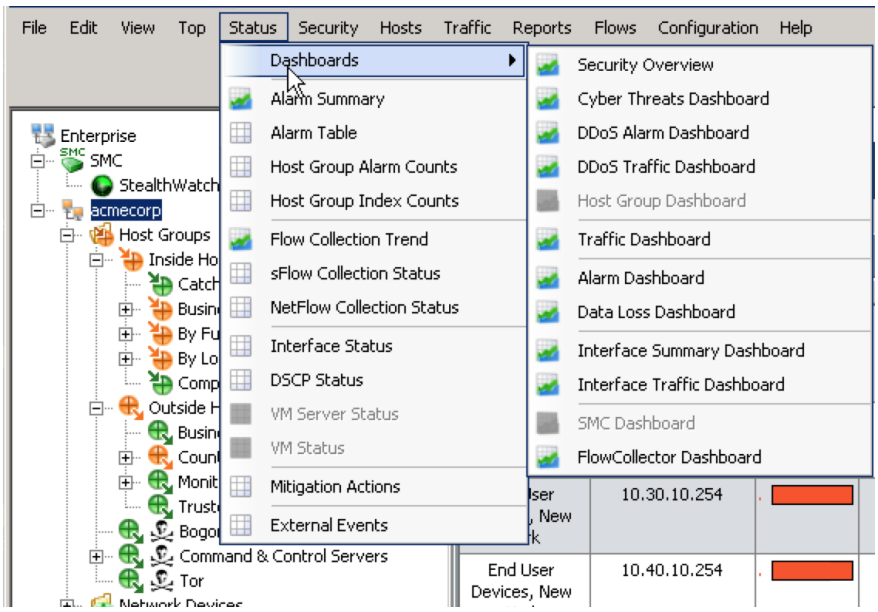
Exercise Objective

Understand documents and their use for troubleshooting and investigation.

Exercise Steps

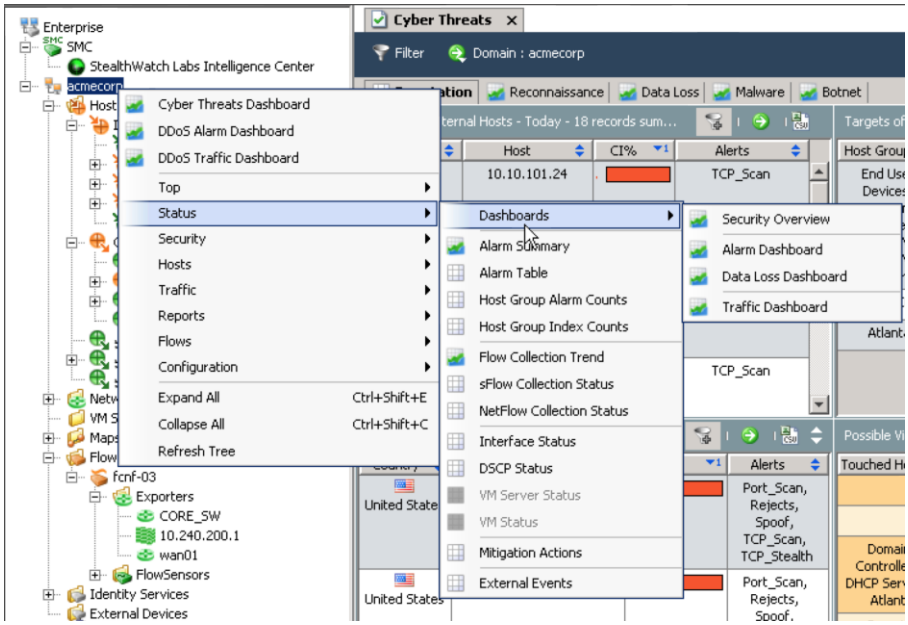
Step 1 This exercise takes place in the Swing Client. Make sure you have it in the foreground.

Step 2 To display the dashboard options available to you on your SMC, click **Status** from the top menu bar, and then **Dashboards** to see a list of available dashboards.



Step 3 Notice that the list of available dashboards and documents changes, depending on what is selected in the enterprise tree on the left. For example:

a. Select, and then right-click **acmecorp** in the enterprise tree, then **Status > Dashboards**.



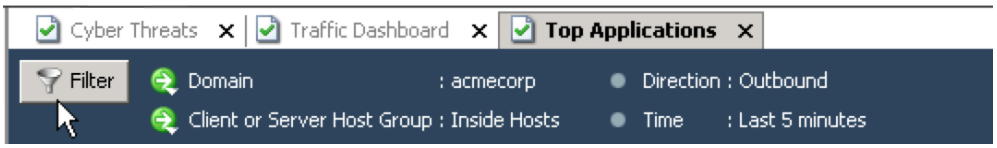
b. Select, and then right-click **SMC** in the enterprise tree, then **Status > Dashboards**.

C. Which items are available in both cases? Which in only one?

Step 4 Click **Status > Dashboards > Traffic Dashboard** in the menu bar to see a display of current traffic initiated by inside and outside hosts. Select **Help > Help** to access context- sensitive help for this dashboard. After reading about the dashboard contents, switch back to the Stealthwatch Management Console window.

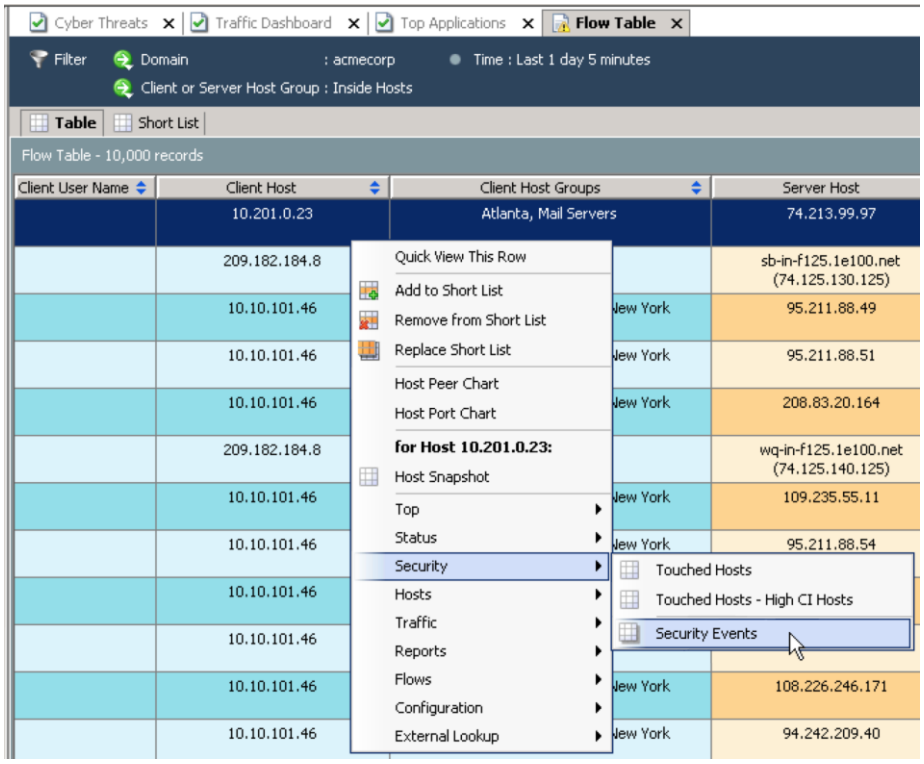
Step 5 Documents and dashboards can also be displayed directly from various levels of the enterprise tree hierarchy. For example, right-click the **acmecorp** domain and select **Top > Applications > Outbound**. Notice the filter conditions displayed in the dark blue banner bar at the top of the document. Which Host Group is selected? What is the time range of the displayed information? Which applications are shown at the top?

Step 6 Click the **Filter** icon in the banner bar. Select **Date/Time** and change the values from their current 0 days, 0 hours, 5 minutes to 1 day, 0 hours, 0 minutes, and click **OK**. Did the top applications change?



Step 7 Right-click the top application in the list and select **Flows > Flow Table**. This shows the actual flows that make up the traffic shown in the top applications document.

Step 8 Pick an interesting-looking IP address (server or client) from the list, right-click that field, and select **Security > Security Events**. This displays Concern Index (CI) events associated with that one IP address. Notice in the banner bar that the filter now is set to select only the IP address you have chosen.



Step 9 Feel free to explore other documents, hosts, and other information elements as time allows.

a. The **DDOS Alarm** and **DDOS Traffic Dashboards** highlight that relevant activity in your environment.

b. You can also explore additional documents, similarly to how you accessed the Domain Dashboard in the previous exercise, by clicking **File > Open** on the top menu, selecting a Shared Document, and clicking **Open**.

Step 10 At the conclusion of the exercise, you will very likely have accumulated a large number of open tabs in your SMC display. As a quick way to clean up, press ctrl + shift + W to close all open tabs at once. Then select **Status > Dashboards > Cyber Threats Dashboard** to return to the original state at the beginning of the exercise.

QUESTIONS:

1. What dashboards are immediately available via right-click for **acmecorp**?

Exercise 6: Confirming the parameters of a rule/policy

Exercise Description

By default, in normal Stealthwatch operation new IPs are assigned to the "Catch All" Host Group. The administrator will then assign these IPs to the appropriate Host Group. Hosts detected on the network are assigned a host policy based on the group they are assigned to. If the host does not have a specific policy assigned to it or to the Host Group it belongs to, the host will inherit the default inside or outside policy.

Host locking allows the establishment of rules for the data flows between hosts and/or Host Groups. Host locking helps in auditing security policies and in improving compliance.

Exercise Objective

Understand Host Policy and verify compliance using Host Locking.

Exercise Steps

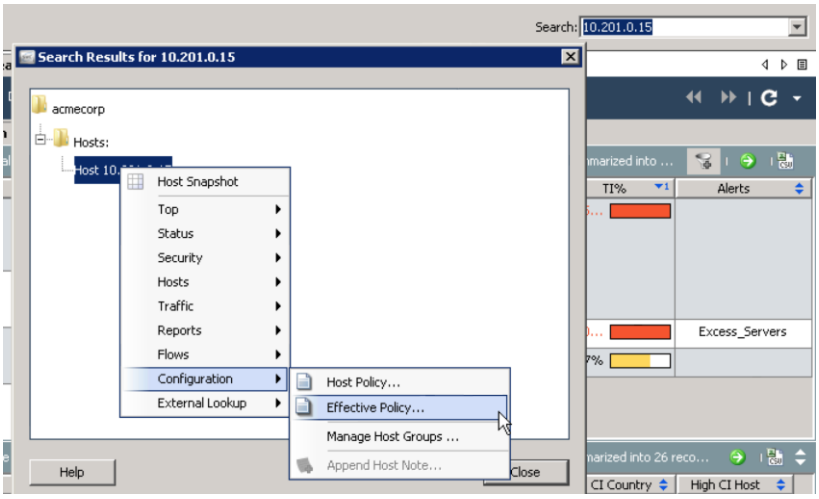
Step 1 This exercise takes place in the Swing Client. Make sure you have it in the foreground.

Step 2 View the effective **host policy** of a host:

a. In the upper right corner search field type the IP 10.201.0.15.

b. The search dialog box appears with the IP 10.201.0.15 under the Hosts list.

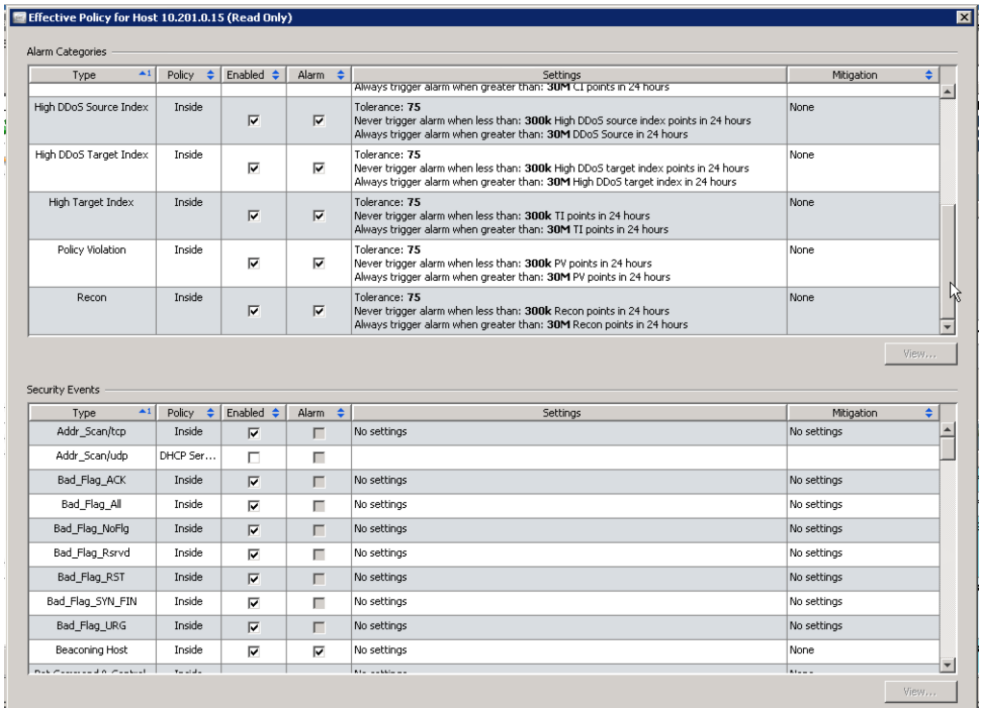
c. Right click on the IP and choose **Configuration > Effective policy**



d. The effective Policy window will display.

e. Note the **Alarm Categories** section and the **Security Events** section

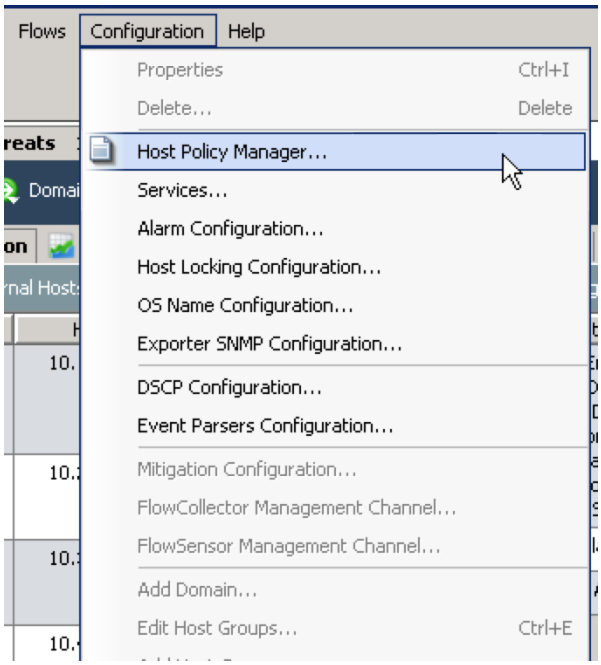
f. What are the **Alarms categories** and **Security events** that are affecting this host?



Step 3 Close the **Effective Policy** window.

Step 4 View the built in **Host Policies:**

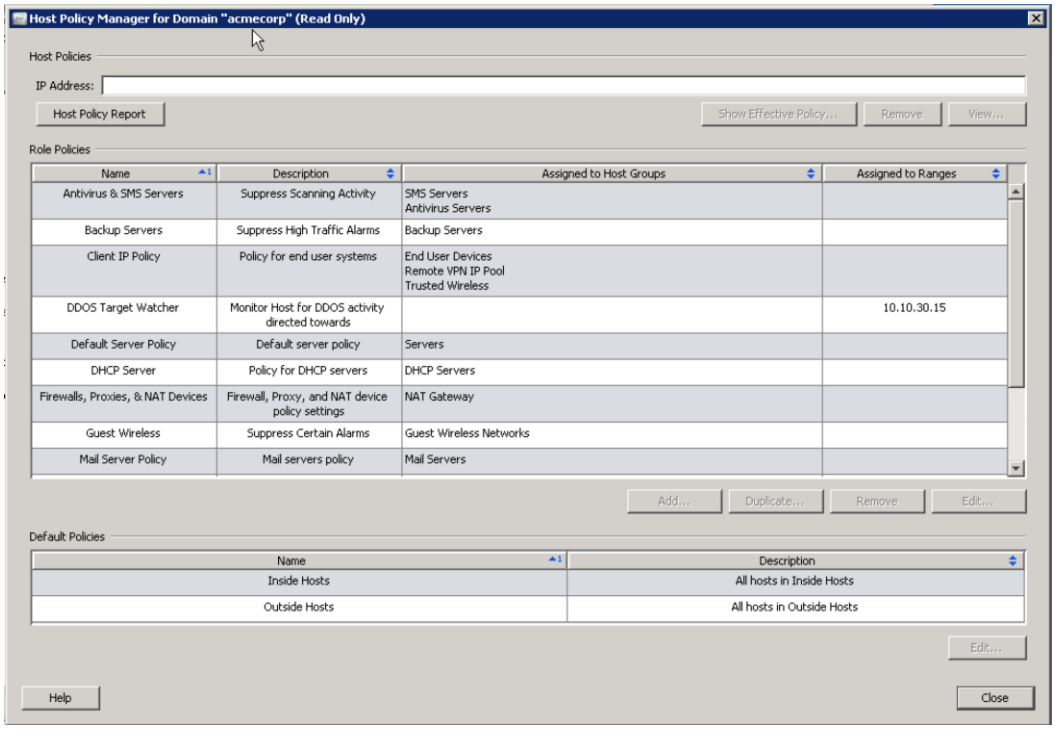
a. From the top menu choose **Configuration** > **Host Policy Manager.**



b. The **Host Policy Manager** displays. Note the Role Policies section.

c. How many **Host Groups** have Role Policies assigned to them?

d. How many default policies exist?

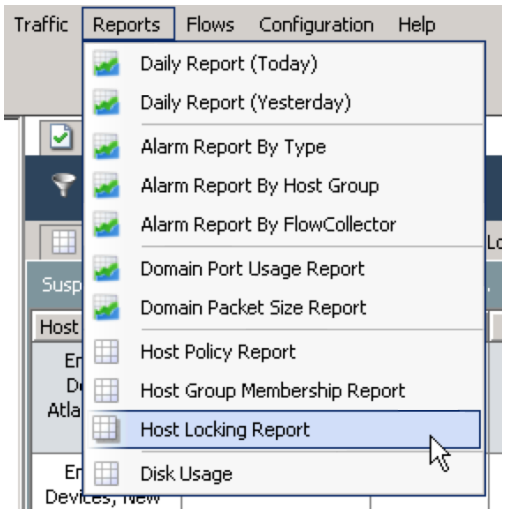


e. Double-click one of the default polices, the **Edit default Policy** displays, note the Alarms Categories and Security events that are manageable by this policy.

f. How many Alarm Categories are disabled?

Step 5 View **Host Locking Report**:

a. From the top menu select **Reports > Host Locking Report.**



b. The **Host locking report** displays showing all of the host locking rules on the system and indicates which of those rules have been violated and how many times

c. Double click on the **Violation** count.

d. The **Alarm** table will be display filtered to show only the alarms for that particular rule violation

e. What are the different sources of violations? What are the targeted destinations?

Step 6 Close the open windows to return to the main Swing Client. You are done with this exercise.

QUESTIONS:

1. What are the Data Exfiltration alarm settings for host **10.201.3.84**?
2. How many times have the host locking rules been violated?

Exercise 7: Investigating an Alarm

Exercise Description

Stealthwatch leverages a number of behavior and policy based algorithms to alarm it's users about observed behavior on the network. A very common alarm for Stealthwatch users to investigate are hosts with High CI (Concern Index) values. We will now perform this task and attempt to determine if it is normal behavior and also if it can be corrected.

Exercise Objective

In this exercise, your goal is to learn how to investigate an alarm in Stealthwatch, as well as export the relevant data for submission to IT.

Exercise Steps

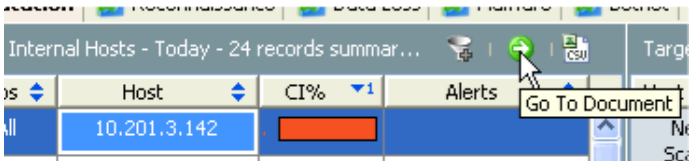
Step 1 This part of the exercise takes place in the Swing Client. Make sure you have it in the foreground.

Step 2 If necessary, reopen the Cyber Threats Dashboard from the **Status > Dashboards** menu and view the **Reputation** tab in the dashboard.

Step 3 In the upper left quadrant, observe the **Suspicious Internal Hosts** list of inside hosts with a high CI value.

NOTE: If space is too tight to allow full display of the CI% column, you can see the values by hovering the mouse pointer over each bar.

Step 4 For a better view of these high CI hosts, use the green **Go To Document** control to open a new **Concern Index** document tab.



Step 5 In the resulting table, pay close attention to the top host in the list. Right-click the row for that host and select **Status > Alarm Table** to see the alarms associated with the high CI host. What is the cause of the high CI value in this case?

Step 6 Right-click a row in the Alarm Table and **select Quick View This Row** to see more details. What additional information about the activity is available? How long did the flow last? What other host was involved?

Step 7 Switch back to the **Concern Index** document and pick one of the rows related to scanning (e.g., TCP_Scan) events. Right-click the row and select **Security > Security Events**.

Step 8 Which port(s) and network ranges are being scanned? Switch to the **Summary of Target Hosts** tab. Does it appear that the hosts being scanned are targeted, or evenly distributed?

Step 9 Switch back to the **Table** tab in the **Security Events** document and examine the **Security Events** column information. Is any port being targeted that is of particularly high security interest?

Step 10 Right-click one of the rows and select **Quick View This Row**. Notice the hit count. Is this a stealthy scan? Close the Quick View window after examining the data.

Step 11 Right-click a **host IP** in one of the rows and select **Host Snapshot** to see details of the host that is performing the scan.

Step 12 Select the **Exporter Interfaces** tab of the Host Snapshot document. Which NetFlow source(s) do you see?

Step 13 Switch to the **Identity, DHCP & Host Notes** tab. Examine the information that is provided by the Cisco ISE integration. What can you tell about the user and device?

Step 14 Switch to the **Security** tab. Has this scanning host "touched" another host? (Note: If nothing shows up for today, try changing the Filter expression to include yesterday.) Recall that "touched" means that the scanning host has made a connection to the touched host and exchanged data.

Step 15 In the **Touch Information** section of the **Security** tab, right-click the **! Yes** field in either the **Has Touched Another** or **Has Been Touched** column, and select either **Touched Hosts** or **Hosts Touched By,** depending what is available. How many other hosts has this scanning host touched?

Step 16 To print the host snapshot to a file and forward to your IT Security department to investigate and remediate this machine. In the main menu bar, select **File > Print to File**, name the file **malware-host.pdf** and save the host snapshot to your **Desktop** folder.

Step 17 As a last step in this exercise, return to the **Cyber Threats** dashboard, right-click the tab, and select Close Others to clean up the interface a bit. Switch to the **Reconnaissance** tab of the **Cyber Threats** dashboard and examine the **Top Scans from Outside** panel in the lower right corner. Are we reporting external scans? If so, from where? What do they appear to be looking for?

Step 18 After you have completed your investigations, close any remaining open documents except for the Cyber Threats dashboard.

Step 19 The second part of this exercise takes place in the SMC WebUI. Minimize the Swing Client so the web browser with the Dashboard visible is in front.

Step 20 We will investigate a high CI alarm, using the information available in the WebUI.

Step 21 Along the top row of active alarms is **Concern Index**:

a. If there is a number present in the alarm's box, click it.

b. If there is a "**0**" in the alarm's box (e.g.- no current active alarms), enlarge the **Today's Alarms** panel and click on either the pie slice or text for **High Concern Index**.

Step 22 A page with an alarm table will open, displaying all source hosts currently engaging in what appears to be suspicious activity.

Step 23 In the **Details** column there is a brief summary of the amount of observed activity, versus the threshold required to trigger the alarm. Click on this text for any host.

Step 24 The **Security Event Details** page will load, displaying the relevant information for the security events that triggered the alarm, including source IP, target IP, the concern index score for the event and the type of event.

Step 25 Review the security events around the alarm. What sort of behavior is the host engaged in? Does any of the activity appear to be targeting specific ports of interest?

Step 26 Click the host's IP address in the **Source Host** field. This will open the **Host Report** for the host.

Step 27 Look at the **Alarms by Type (last 7 days)** panel. Has this host been involved in any other suspicious behavior over the course of the past week?

Step 28 Click on the bar for an alarm represented in the **Alarms by Type (last 7 days)** to get additional details around the activity.

Step 29 Click the **Dashboard** link on left navigation panel to return to the WebUI's dashboard screen. You are done with this exercise.

QUESTIONS:

1. In step 17, we asked "Are we reporting external scans? If so, from where?" What was the top external scanner host's IP?

Exercise 8: Worm Propagation Investigation

Exercise Description

There is a Worm Tracker document in the Swing Client that can help you determine and visualize systems that are exhibiting Worm-like activity. We are going to examine this now.

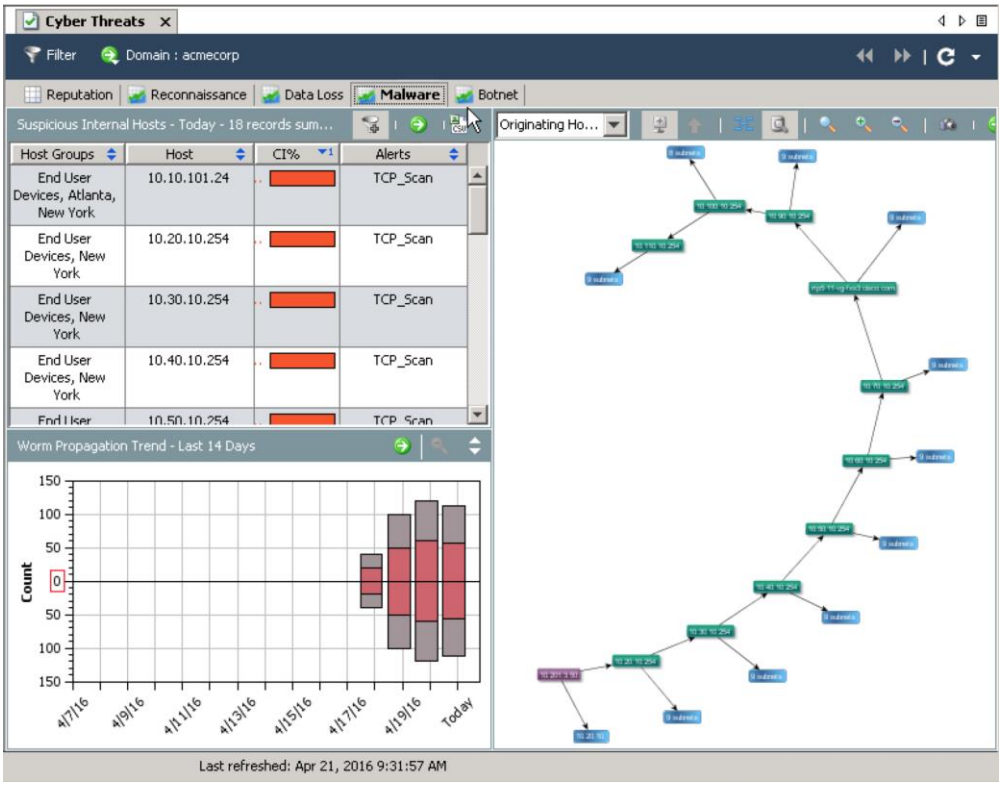
Exercise Objective

In this exercise, your goal is to inspect Stealthwatch's visualization of a worm propagating across your network for information regarding the spread.

Exercise Steps

Step 1 Return to the Swing Client Stealthwatch Management Console (SMC) interface.

Step 2 If necessary, reopen the **Cyber Threats Dashboard** from the **Status > Dashboards** menu and view the **Malware** tab in the dashboard.



Step 3 Hover over some of the items in the **Worm Propagation Trend** graph. Is there an observable trend over time? Where does the majority of the activity appear to be located?

Step 4 Notice the graphical representation of malware spread in the **Worm Tracker** display on the right side of the window. The items shown may be too small to easily identify; click on the **Turn On Magnifier** icon and move your mouse pointer across the graph. Click the icon again to turn off the magnifier.

Step 5 Move your mouse pointer over a **purple** rectangle, representing a primary source of infection in the network. Notice the pop-up display with more information about the host's activity.

Step 6 Right-click on the purple rectangle, and select **Host Snapshot**. View the information in the **Identity, DHCP & Host Notes** tab, and consider how this would be useful for incident response.

Step 7 Examine the **Security Events** tab. What kind of scans and other behavior do you see from this host?

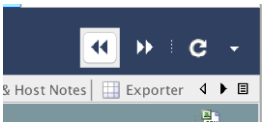
Step 8 Examine **Touch Information** in the **Security** tab.

a. Has the host been touched?

b. Has it touched others? Bring up the **Host Snapshot** for one of the **green** rectangles in the original screen (secondary infections) and compare the **Touch Information**.

Step 9 Right-click the **Yes** in the **Has Touched Another** column and select **Hosts Touched By**.

NOTE: If the Has Touched Another column does not show "Yes", click on the View Earlier Data button in the filter for the tab.



Step 10 Are all of the hosts listed in **Touched Hosts** also present as green rectangles in the original worm tracker display? Why?

Step 11 Close any open tabs except the Cyber Threats dashboard to clean up at the end of this exercise.

QUESTIONS:

1. What is the IP address of the last host in the malware spread chain?
2. How many subnets did it scan?

Exercise 9: Insider Threat Detection

Exercise Description

When activity on the network deviates from established norms, and when hosts on the network behave in ways that they normally wouldn't or shouldn't this can be a sign of attack. In addition to attacks designed to disrupt activities across a network, more and more often attacks are being executed in order to gain access to information stored on the target network with the intent to steal it. This could be credit card information, personnel records, social security numbers, classified documents, etc.

Exercise Objective

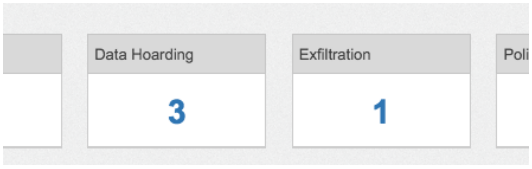
Explore Stealthwatch's ability to identify insider threats in the network.

Exercise Steps

Step 1 The first part of this exercise takes place in the SMC WebUI. Minimize the Swing Client so the web browser with the WebUI **Dashboard** visible is in front.

Step 2 The alarm categories showcased along the top of the Dashboard prominently include two concerned with insider threat detection: **Data Hoarding** (user stealing data) and **Exfiltration** (user sending data out).

Step 3 From the Dashboard, you can drill into either of these alarms independently by clicking on the number beneath to see what alarms are currently active. The WebUI can also be used to provide insight into all of the host activity observed across the network and which hosts are triggering alarms in multiple categories.

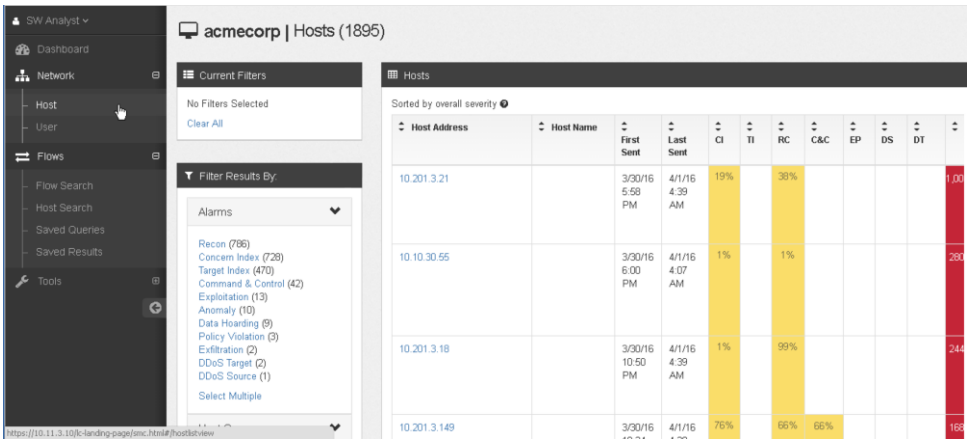


Step 4 Click **Network > Host** on the left navigation panel.

Step 5 The host list screen will appear. The list has columns displaying the IP address and host name. In addition, there are columns corresponding to the alarm categories displayed on the **Dashboard**.

NOTE: You may need to scroll the table to the horizontally to view all the columns.

Step 6 Mouse-over the column headers to display the alarm names and descriptions.



Step 7 By default, the list is sorted by alarm category severity, so the hosts with the worst alarms are at the top of the list. The order is based on the aggregate (combination) of alarm categories for each host.

Step 8 To change the sort order, click an arrow in any column heading.

NOTE: To restore the default sort, click **Sorted by overall severity** at the top of the table.

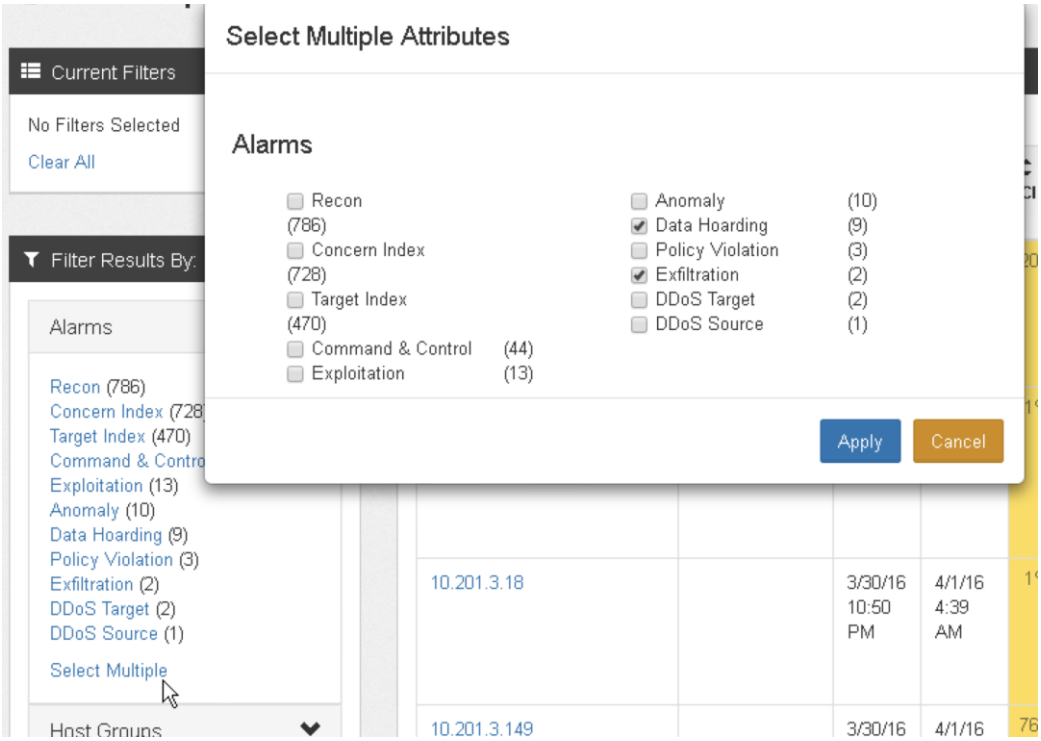
Step 9 Along the left side of the page are options to filter this list, allowing you to focus your attention on more specific hosts.

Step 10 For this exercise, we want to concentrate on Data Hoarding and Exfiltration activity. Highlight these hosts by either:

a. On the **Filter Results By** panel, under **Alarms**:

i. Click **Select Multiple**.

ii. Check the boxes for **Data Hoarding** and **Exfiltration**.



iii. Click **Apply**.

Step 11 Note the hosts triggering these alarms. Notice how the host classified as a terminal sever has a lot of **Data Hoarding/Exfiltration** events. This probably indicates suspicious behavior.

Step 12 Click on the host **10.201.0.23**.

Step 13 The **Host Report** page for **10.201.0.23** opens.

Step 14 The Host Report summarizes an extensive array of data around a host's observed activities on your network. Providing information about other alarm categories the host has been involved in, Host Summary, User Logged in, Traffic Flow to other groups both inside and outside.

Step 15 Feel free to explore any of the other hosts triggering alarms back on the host list screen.

Step 16 When you are done, click the **Dashboard** link on left navigation panel to return to the WebUI's dashboard screen.

Step 17 The second part of this exercise takes place in the Swing Client. Return to your Stealthwatch Management Console (SMC) interface.

Step 18 If necessary, reopen the **Cyber Threats Dashboard** from the **Status > Dashboards** menu and view the **Data Loss** tab in the dashboard.

Step 19 Choose a current or recent instance of suspected data loss in the **Top Data Loss Hosts** or **Data Loss Trend by Group** displays.

Step 20 **Right-click** the event and select **Alarm Table**. What is triggering the alarms? Is there a consistent theme in the source of the events?

Step 21 **Right-click** on some of the alarms and select **Flows > Associated Flow Table**. What destinations are seen for the suspected data leakage?

Step 22 **Right-click** on the destination of the data export and select **Host Snapshot** for the destination. What additional information do you find under the **Identification**, **Alarms**, **Security**, and **Security Events** tabs?

Step 23 Close any open tabs except the Cyber Threats dashboard to clean up at the end of this exercise.

QUESTIONS:

1. Often, user activity can result in Stealthwatch creating multiple alarms for the same event. What other alarms might Stealthwatch generate for data hoarding and exfiltration alarms?

Exercise 10: Identifying a DDoS Attack

Exercise Description

Stealthwatch aggregates observed network activity and performs behavioral and policy driven analytics against what it sees in order to surface problematic activities. While we don't position our self as a DDOS solution, we're going to leverage our analytical capabilities to identify a DDoS attack against an internal host using the WebUI.

Exercise Objective

To see how Stealthwatch can identify a DDoS attack, using the WebUI.

Exercise Steps

Step 1 This exercise takes place in the SMC WebUI. Minimize the Swing Client so the web browser with the WebUI **Dashboard** visible is in front.

Step 2 Two of the alarm types displayed on the Dashboard concern DDoS activities:

a. **DDoS Target**: Hosts in your network that are on the receiving end of a DDoS attack.

b. **DDoS Source**: Hosts in your network engaged in DDoS like activity.

Step 3 We will look into DDoS target hosts in our network. Click on the number below the alarm to navigate into the **Alarm Dashboard**.

NOTE: If the number is 0 for **DDoS Target**, navigate to the **Network > Host** list and sort the DT (DDoS Target) column to find a host hit as a DDoS target over the course of the day.

Click on the **% number** in the **DT** column for that host to bring up the **Alarm Dashboard**.

Step 4 Within the **DDoS Target Alarm Dashboard** make note of the following:

a. **Application Traffic** pane: This shows the last two hours of network activity for the host(s) involved in the DDoS attack. If the attack is active, large increases in traffic would be visible here. Note, you can click and drag on the chart to zoom into areas for a closer look at the activity.

b. **Summary of Targets:** If the alarm is active, a list of all hosts affected by the DDoS attack would be displayed here as a pie chart, indicating the comparative severity of the attack on each.

c. **Alarms:** Displays the time the attack started against the host(s), and what part(s) of the network the target belongs to.

Step 5 In the **Alarms** panel, click the **Details** cell text for for more information about the activity against the target.

Step 6 Within the **Security Event Details**, make note of the types of security events triggering along with timestamps of the behavioral change.

Step 7 Click the **Target Host's IP** to navigate to the **Host Report**.

Step 8 Within the Host Report for make note of:

a. Alarm categories that have triggered for this host (DDoS Target)

b. **Host Summary** to learn about the host.

c. **Traffic by Peer** to visualize the heavy traffic coming in.

d. **Alarms by Type** to review current and past security events that have triggered against this host.

e. **Application traffic**, to see current and trends of traffic for this host.

Step 9 Click the **Dashboard** link on left navigation panel to return to the WebUI's dashboard screen. You are done with this exercise.

QUESTIONS:

1. What kind of DDOS traffic is the host being attacked with?
2. What country is the DDOS attack traffic coming from?

Exercise 11: Building an audit trail

Exercise Description

Using the WebUI Dashboard, you can look into alarms such as Data Hoarding (user collecting data, potentially from several sources) and Data Exfiltration (user sending data out to one or multiple sources on the Internet). This could be indicative of several possible scenarios:

- Disgruntled employee
- Person about to leave the company
- Person abusing privileged credentials
- Person stealing and selling trade secrets
- Compromised user credentials

Once a potential insider threat has been identified, you can build an audit trail around their activities.

Exercise Objective

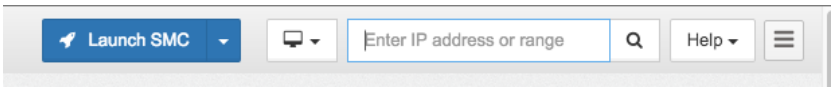
In this exercise, your goal is to build an audit trail around a suspect host's activity.

Lab Exercise Steps

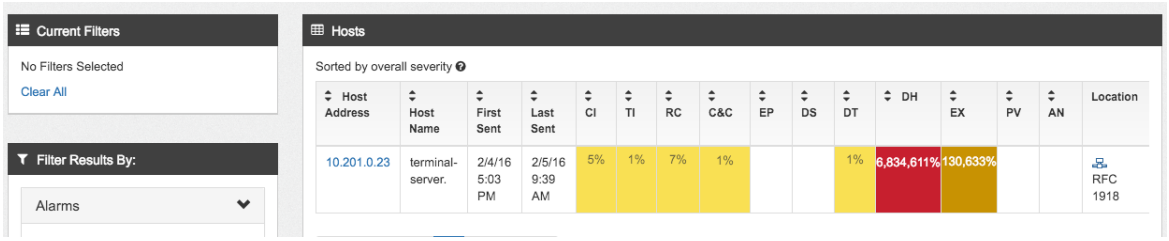
Step 1 This exercise takes place in the SMC WebUI. Minimize the Swing Client so the web browser with the Dashboard visible is in front.

Step 2 Since we previously looked at host **10.201.0.23** as a suspect host, we will examine it in more detail.

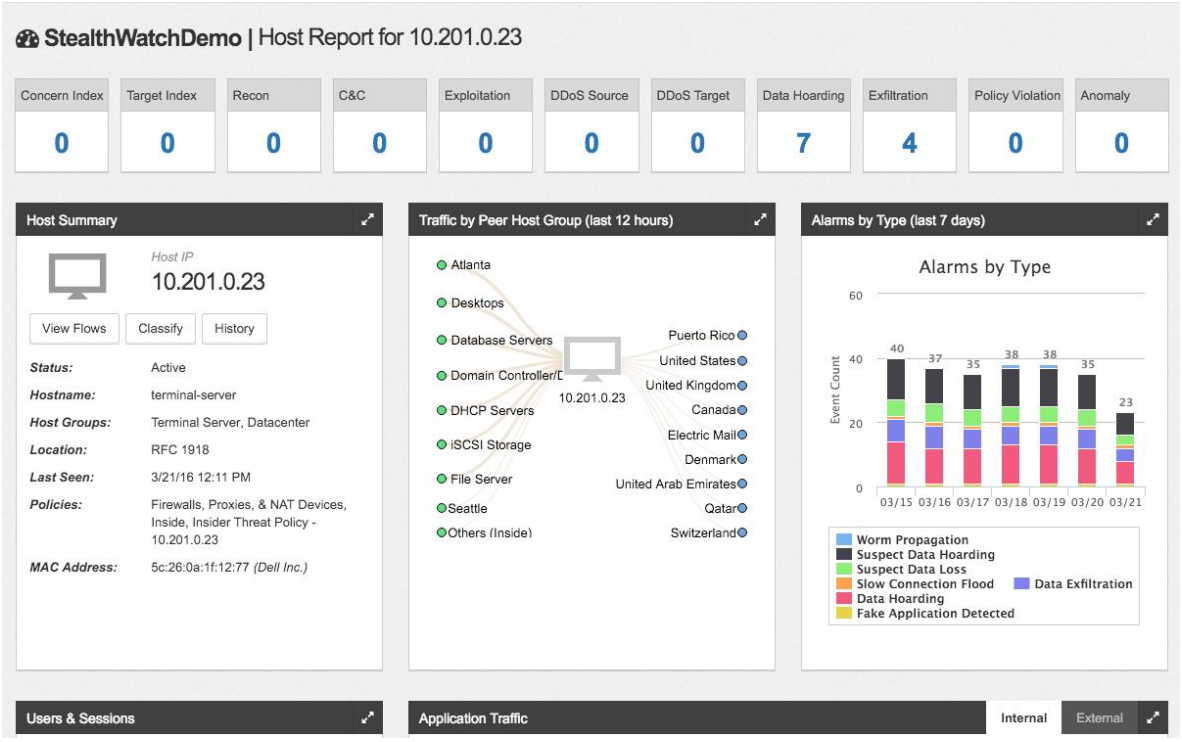
Step 3 In this example, enter the **10.201.0.23** address into the search field on the top of the Dashboard.



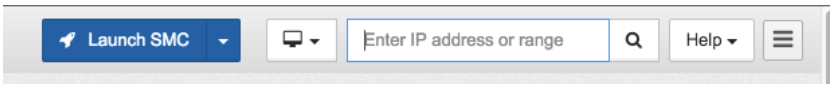
Step 4 In the Hosts Address column on the Hosts list, click the suspect host's IP address.



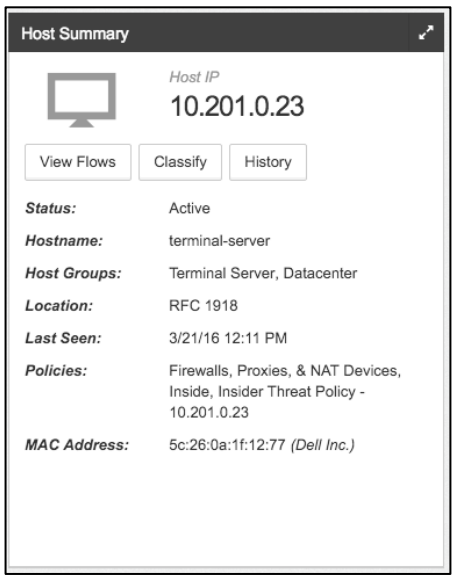
Step 5 Here we see all the summary data provided within the Host report. Along the top of this screen are the alarms related to the host you are investigating. This functions similarly to the alarm list on the front page of the Dashboard, except it displays the details of each occurrence of the alarm for the current host.



NOTE: If you follow any links that take you away from the host you are investigating, you can return to the Host report by searching for it again in the field on top of the screen.



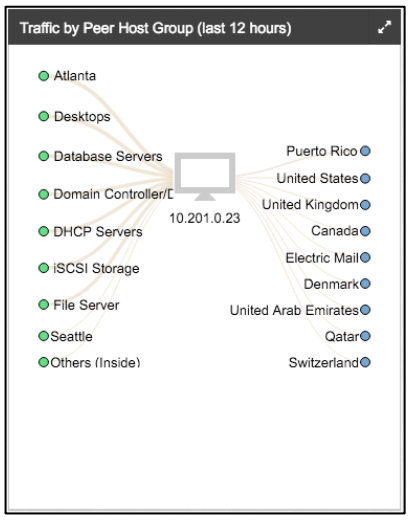
Step 6 The **Host Summary** window provides host name, location, when it was last seen, the policies that are applied, and the Host Group.



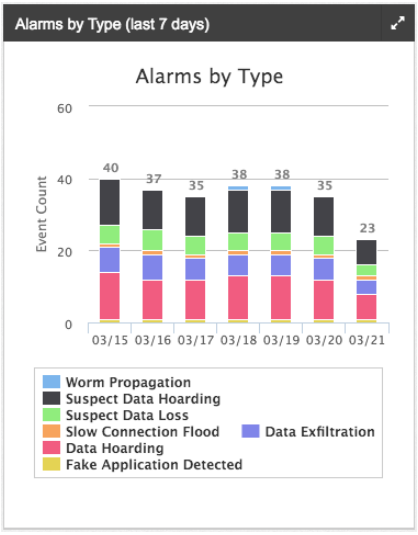
Step 7 We also see **Traffic by Peer Host Group**. This will indicate where this host has been retrieving and sending traffic. In this window we can tell by the thickness of the lines which Host Group peers have had the most data transferred with the host.

Step 8 Clicking on a listed Peer Host Group will take you to the **Flow Query** screen and allow you to review all communication that has occurred between the host and peers within the

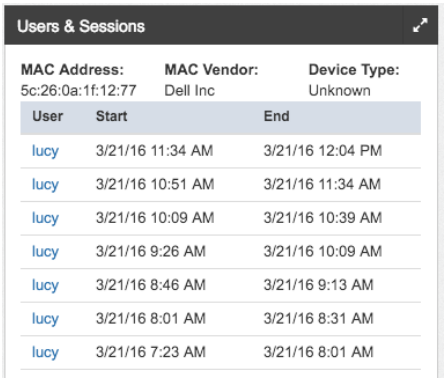
group for the last 12 hours. This amount of time searched and other variables can be modified as needed. Feel free to explore the activity the host has been engaged in.



Step 9 **Alarms by Type** displays all of the alarms associated to the host that have occurred over the past week.

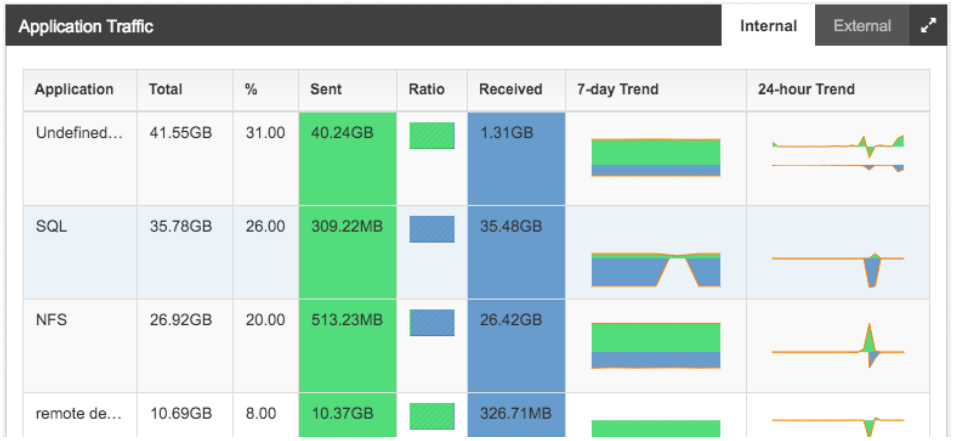


Step 10 In the **Users and Sessions** panel you can see what user has logged in while this alarm was triggered, through information provided via integration with ISE or Active Directory.

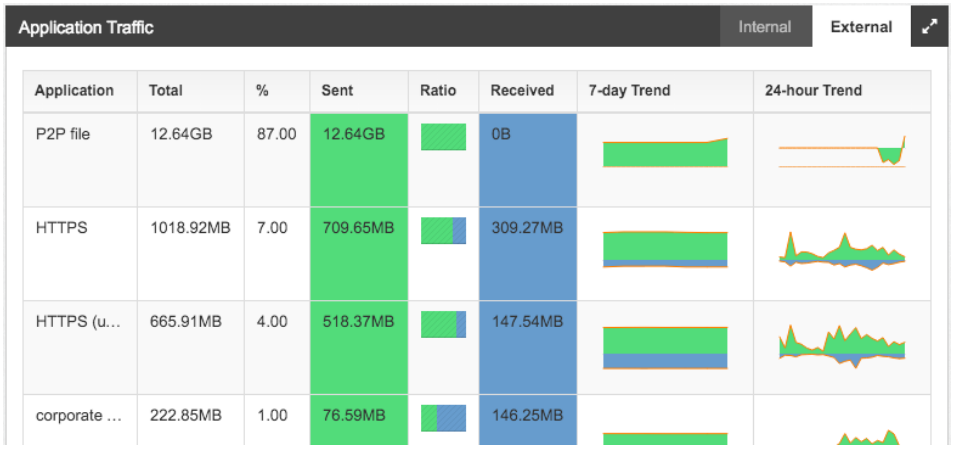


Step 11 The **Application Traffic** panel shows:

a. Initially, application traffic to other **Internal** hosts is displayed. The highest amounts of traffic attributed to the host, in addition to the identified application responsible.



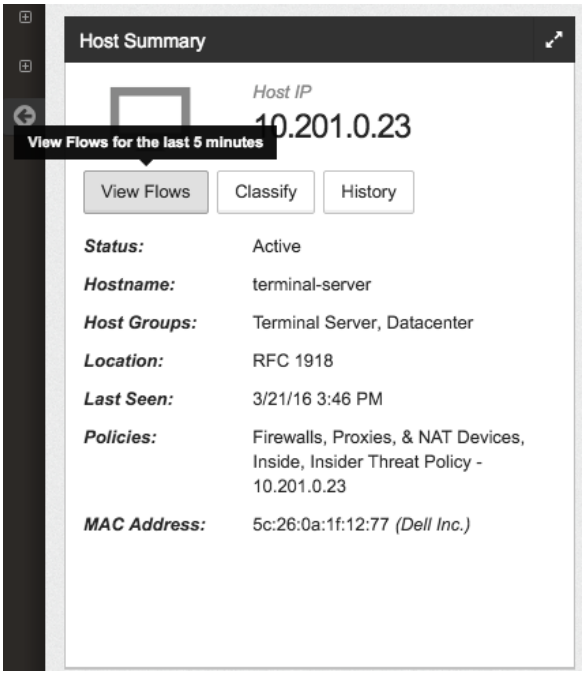
b. Click **External** on the Application Traffic Window for a summary of the highest amounts of traffic attributed to the host going outside of your network, in addition to the identified application responsible.



c. The **Application Traffic** panel covers **7 day** and **24 hour** trends. You can mouse over the mini-charts in each column for additional information. In addition, you can click in the box for a given application's 7 day or 24-hour trend to perform a flow query on the observed traffic for the selected period.

Step 12 Make note of the large amount of internal data transfer, and the large amount of data being externally. Also make note of the other application traffic being leveraged by the host, as well as the type and amount of each.

Step 13 Back in the **Host Summary** panel, click **View Flows** to get more information and quickly answer further questions about the host's recent activity. By default, the query searches for all activity in the last 5 minutes.



Step 14 To ensure some activity is displayed, you will want to run the query with a longer span of time in the **Range** field. Change that setting to 8 hours.

a. Click **Review Query** to verify your settings.

b. Click **Run** to execute the query.

Step 15 The **Flow Query Results** panel shows all the communication this host has been engaged in, both internal and external. Review the types and amount of activity observed.

Step 16 When you are done, click the IP address of the host you are investigating in the **Search Subject** column to return to the **Host Report**.

Step 17 By using the Web UI, we have been able to gather all the necessary information to help determine the appropriate actions to take for the event.

QUESTIONS:

1. What method and to what country was this host most likely exfiltrating their stolen data?
2. What Host Group did one of their primary targets belong to?

Additional Resources

You can find other useful information related to the topics covered in this lab at the following URLs :

- www.cisco.com/go/stealthwatch