

InfoSec App Hands-On Workshop

Lab Guide

Overview

This lab guide contains the hands-on exercises for the InfoSec App Hands-On workshop. Before proceeding with these exercises, please ensure that you have a copy of the workshop slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: <https://splk.it/Infosec-Attendee>

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the [Splunk Show portal](#) and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one [here](#) before proceeding with the rest of the workshop.



Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. <https://show.splunk.com/event/<eventID>>) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

Overview	1
Exercise 1 – Set Up the InfoSec App	3
Description	3
Steps	3
Exercise 2 – Investigating with InfoSec App Dashboards	9
Description	9
Steps	9
Exercise 3 – Malware Investigation and Alerts	12
Description	12
Steps	12
Exercise 4 – User Behavior Investigation	16
Description	16
Steps	16
Exercise 5 – Customize the InfoSec App	19
Description	19
Steps	19
Exercise 6 – Adding Security Content: New Use Case	25
Description	25
Steps	25
Exercise 7 – Adding Security Content: New Dashboard	30
Description	30
Steps	30
Summary	36

Exercise 1 – Set Up the InfoSec App

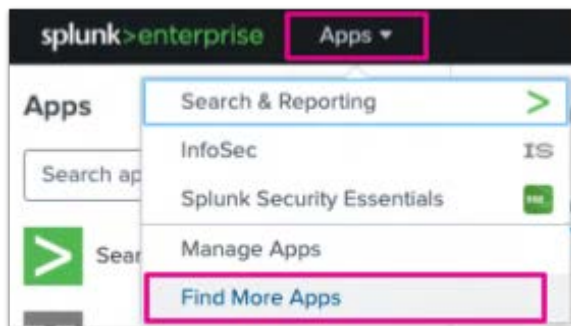
Description

Our first task is to install the Splunk Add-on for AWS and finish setting up the InfoSec App for Splunk, ensuring that the dashboards are populating correctly.

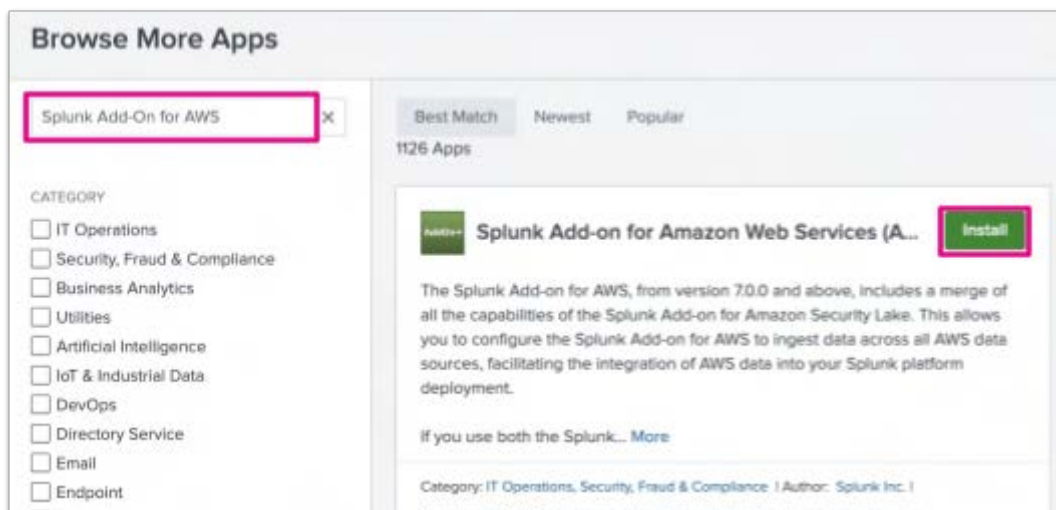
Steps

Install the Splunk Add-on for AWS

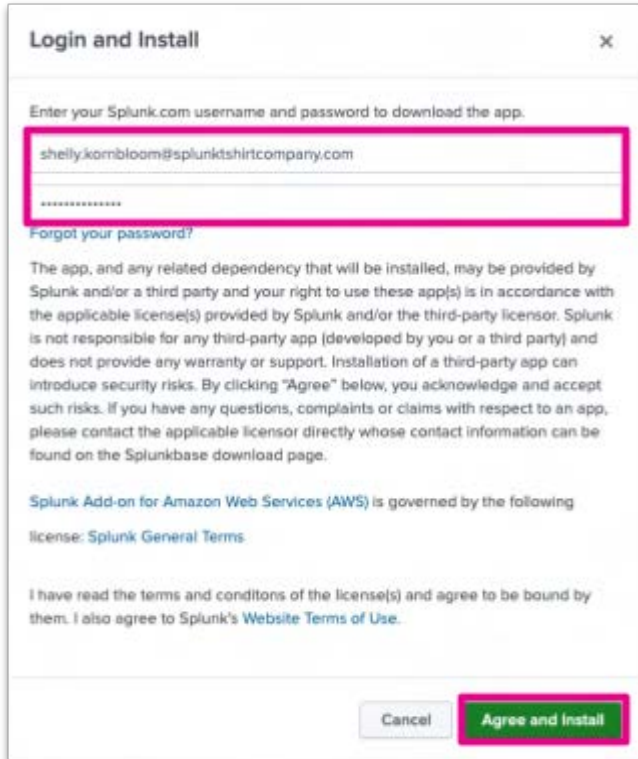
1. Log into your Splunk environment using the credentials from Splunk Show (<https://show.splunk.com>)
2. In the top menu bar click on **Apps > Find More Apps**.



3. Search for "Splunk Add-on for AWS". Find the **Splunk Add-on for Amazon Web Services (AWS)** search results and click on **Install**.



4. Enter your splunk.com credentials when prompted and click on **Agree and Install**.



5. In the top menu bar navigate to **Apps > Manage Apps** and check that the Splunk Add-on for AWS is listed.

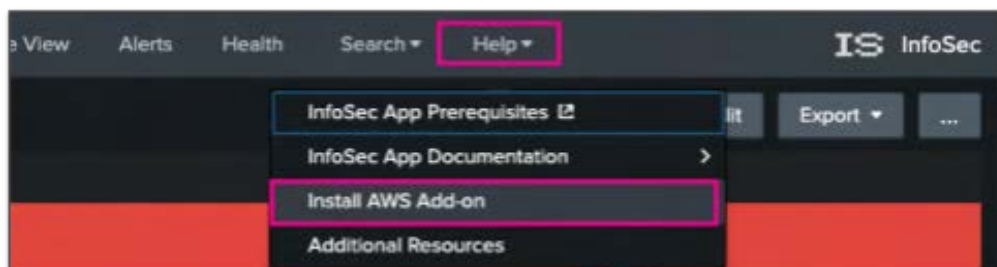
Alternative Installation Method

****You only need to follow these steps if you were unable to install the add-on from Splunkbase****

If you have any issues installing the add-on from Splunkbase using the above steps, we've provided an alternative installation method just for this workshop.

Steps

1. Open the InfoSec app and on the menu bar click on **Help > Install AWS Add-on**

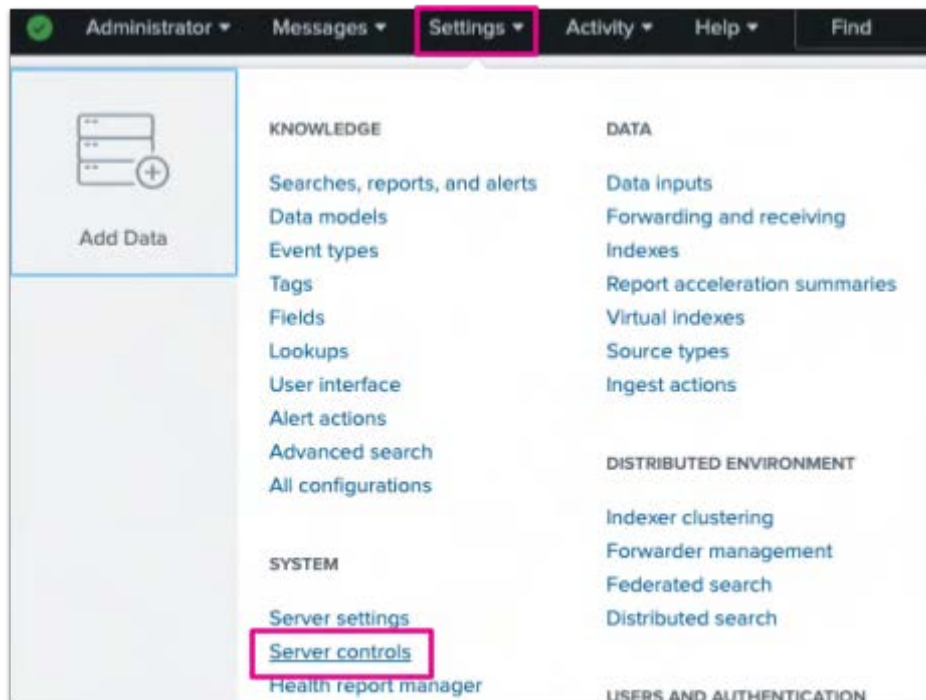


2. Check the '**Install Splunk Add-on for AWS**' checkbox.



This will run a script in the background to install the add-on for you - again, this is a custom workaround to help in this workshop and is not natively part of the InfoSec App for Splunk.

3. In the top right corner of the screen click on **Settings** > **Server controls**.



Click on **Restart Splunk**. If prompted for confirmation by your web browser, click on **OK** to continue.



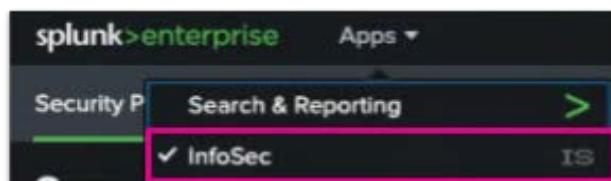
The reboot process should take no longer than a few minutes. When it has finished you will see the Splunk login screen again. When you do, **log back in to Splunk**.

4. In the top menu bar navigate to **Apps** > **Manage Apps** and check that the Splunk Add-on for AWS is listed.

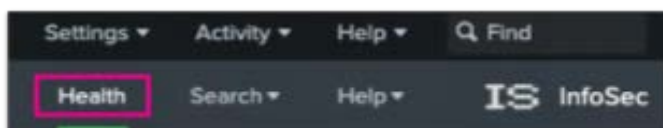
Check the Health of the InfoSec App for Splunk

Now that we've installed the AWS add-on, let's check the overall health of the InfoSec app.

6. Open the **InfoSec App for Splunk** by clicking on **Apps > InfoSec**.



7. Click on the **Health** dashboard from the menu.



8. The first two rows of panels on the Health dashboard provide an overview of the data in your Splunk environment.

Using the Health dashboard, identify the following information:

Q. How many events are feeding each of the data models?

Q. Which data models are accelerated and which (if any) are not accelerated?

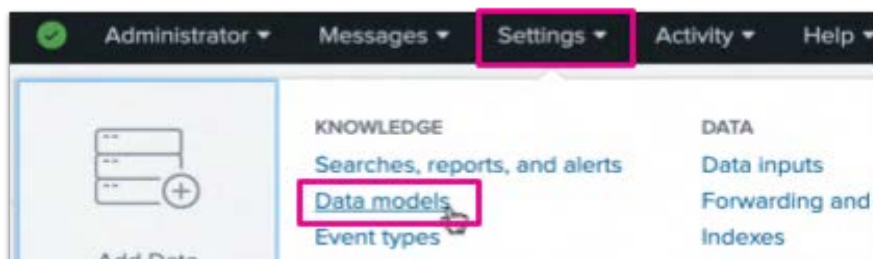
Q. What installed add-ons are being used by the InfoSec app?

You should notice that the Authentication (also referred to as “CIM_Authentication”) data model does not contain any events (see the “Data Models Used by InfoSec App: Events in 24 Hours” and “Data Models Used by InfoSec App: Details in 24 Hours” panels) and also is not currently accelerated (it’s not listed under the “Data Model Acceleration Status” panel.)

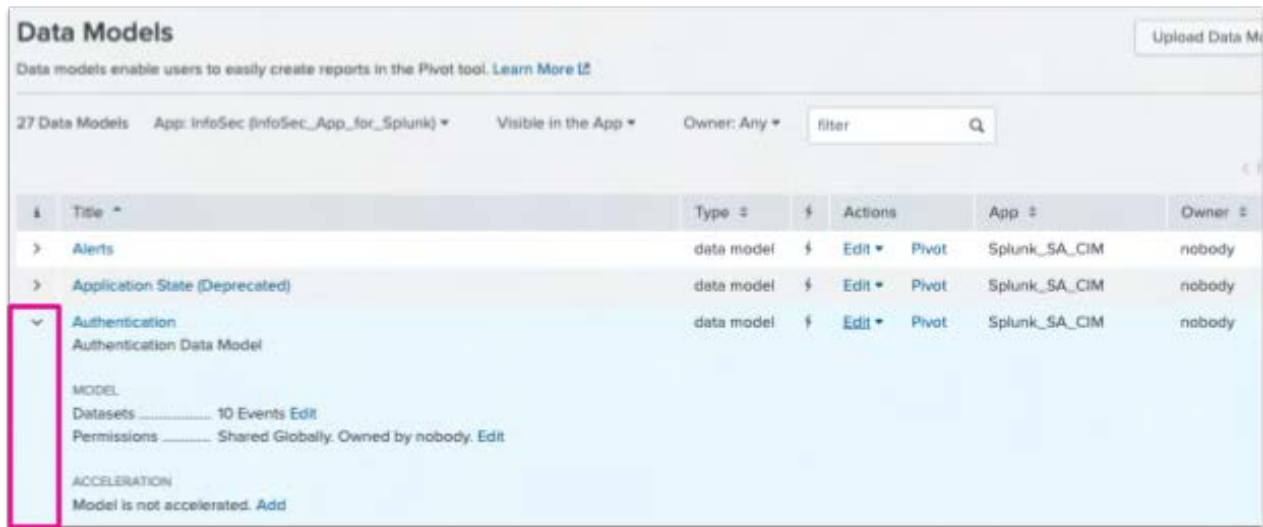
Let’s fix that...

Accelerate the Authentication Data Model

9. In the top right corner of the screen click on **Settings > Data models**.



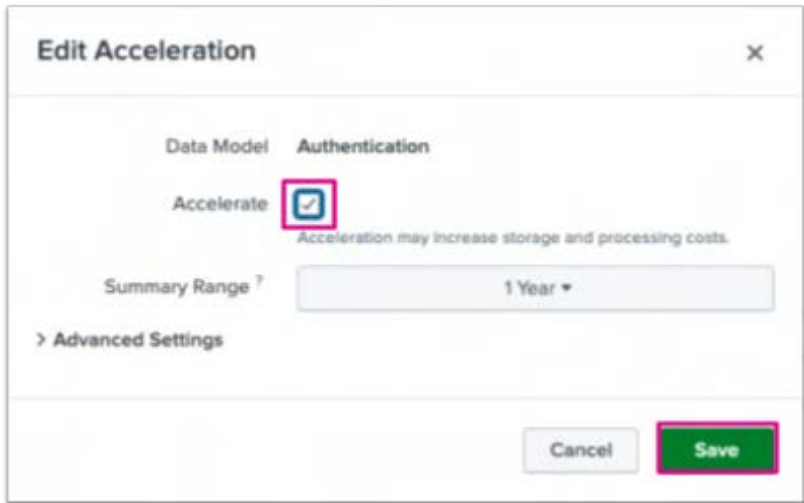
10. Identify the **Authentication** data model. Click on the arrow to expand this section to view more information about this data model.



11. Notice that under the **ACCELERATION** section it says “Model is not accelerated”. Click on **Add**.



12. On the **Edit Acceleration** dialog box, check the **Accelerate** checkbox and click on **Save**. (Leave all other settings unchanged.)



13. Splunk will now start to build the data model accelerations for this data model. Return to the InfoSec app **Health** dashboard and track the progress of the accelerations under the **Data Model Acceleration Status** panel.

When the acceleration status reaches 100% any warnings at the top of the dashboard should disappear.

Alerts **Health** Search ▾ Help ▾ IS InfoSec

Edit Export ▾ ...

Data Model Acceleration Status

All accelerated data models and their status

data_model ↕	complete ↕
CIM_Authentication	100 %
CIM_Change	100 %
CIM_Email	100 %
CIM_Endpoint	100 %
CIM_Endpoint.Filesystem	100 %
CIM_Endpoint.Processes	100 %
CIM_Endpoint.Registry	100 %
CIM_Endpoint.Services	100 %
CIM_Intrusion_Detection	100 %

Note: The acceleration process may take up to 10 min to reach 100% and increases in steps, so don't be worried if it stays at "0%" for some time.

Exercise 2 – Investigating with InfoSec App Dashboards

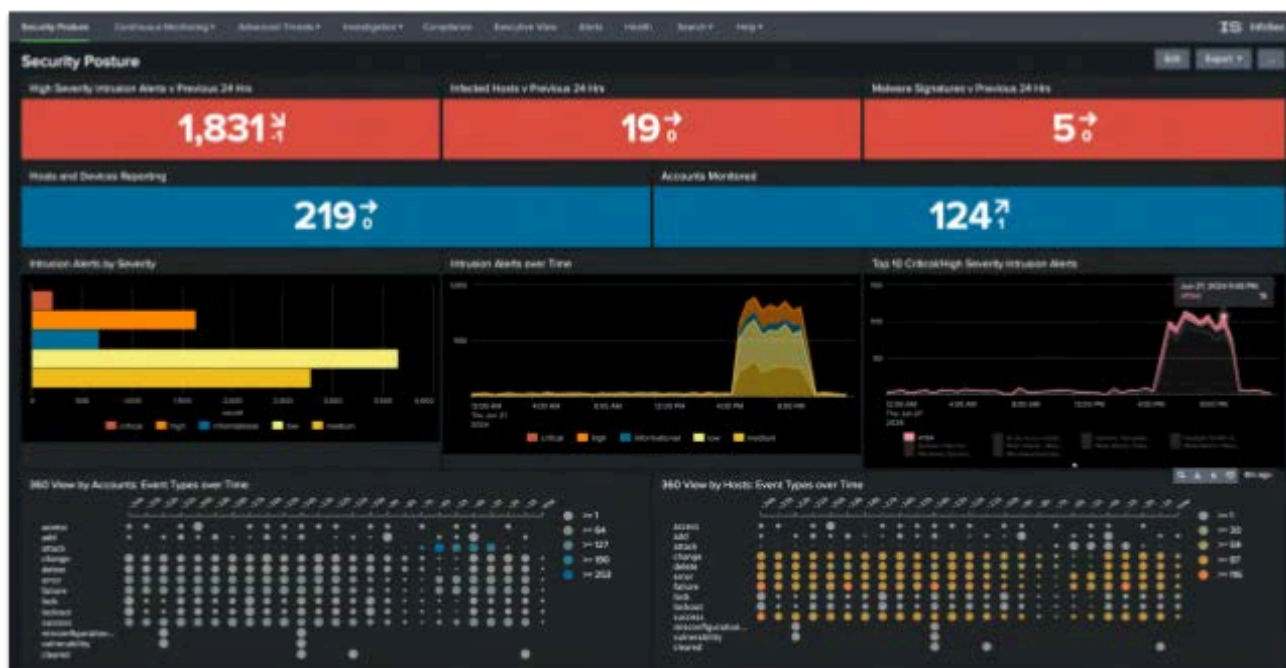
Description

Now the InfoSec app setup is complete, we're ready to start investigating.

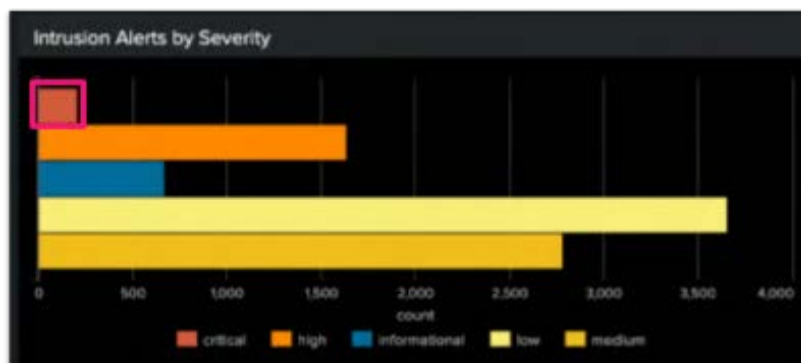
This exercise demonstrates how to use the InfoSec app dashboards to investigate critical security events and gain insights.

Steps

1. Open the **InfoSec** app's **Security Posture** dashboard. This dashboard provides a high level view to monitor the security in your Splunk environment.

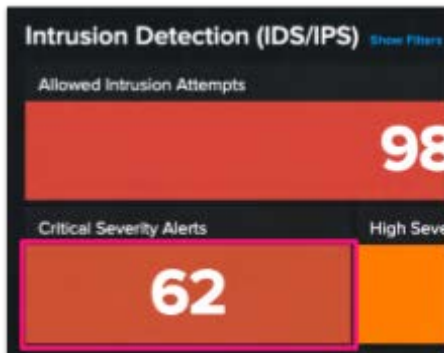


2. Investigate intrusion alerts by clicking on any of the bars on the **Intrusion Alerts by Severity** chart.



This will take you to the **Intrusion Detection (IDS/IPS)** dashboard where you will see more detailed information about intrusion events.

3. Filter the dashboard by critical alerts by clicking on the **Critical Severity Alerts** panel.



4. Identify the top 3 intrusion signatures by sorting the **count** column from highest to lowest (click on the **count** column header on the **Intrusion Signatures** panel).

Optionally click on any of the signature names to view the raw event.

The screenshot shows the 'Intrusion Signatures' table. The table has three columns: 'signature #', 'severity #', and 'count #'. The 'count #' column is highlighted with a red box. The table lists several intrusion signatures, all with a severity of 'critical'. The top three signatures by count are:

signature #	severity #	count #
'Application and Device Control is ready'	critical	3
'C:\Program Files (x86)\uplunktshirtcompany.com\Product\12.1.4.5\Bin64\yyyyy.exe'	critical	1
ACS-1.1 Block access to autorun.inf	critical	4
ACS-1.1 Block access to autorun.inf - Caller MD5=xxxxx86c5d511fdca327445d21aeb1	critical	18
ACS-1.1 Block access to autorun.inf - Caller MD5=xxxxx8578ba0ddetaf5ea8f7f97a83c	critical	1
ACS-1.1 Block access to autorun.inf - Caller MD5=xxxxx81435663fc6c873e39beb17be1	critical	1
Adobe Flash Player Remote Code Execution Vulnerability	critical	2

5. Now let's see what malware is being detected. In the menu bar navigate to **Continuous Monitoring > Malware**.

Using this dashboard, identify the following information:

- What malware has been detected in the last 24 hours?
- What are the top 3 malware types?



Exercise 3 – Malware Investigation and Alerts

Description

Now that we've taken a quick look at a few of the dashboards included in the InfoSec App for Splunk, we're ready to dive further into our investigations.

The IT team has asked us to find malware-infected files and set up an alert for future detections.

Steps

Find Malware-Infected Files

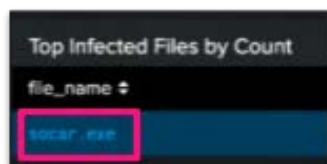
1. Using the InfoSec app's **Malware** dashboard (**Continuous Monitoring > Malware**), identify the **top malware-infected files**.



file_name	count
socar.exe	61
The Characters Myth No Anyone Can Reason The Art and Science of .log	17
SSSSS Start and Change.exe	12
about877	8
Policy22	4
msackdown.exe	4
down.exe	4
msackdown.exe	4
msackdown.exe	4
policy.exe	4
recharger 3.0 .log	4

We can see that **socar.exe** is the top infected file.

2. Click on the file name (“**socar.exe**”) to drill down into the search results where we can view more detail about these events.



From the search results and the fields displayed on the left of the search page, answer the following questions:

- Which host(s) are infected with this malware?
- What are the file paths of socar.exe on the infected host(s)?

Now that you know where the infected files are, you can inform the IT team so they remediate this issue.

Create an Alert

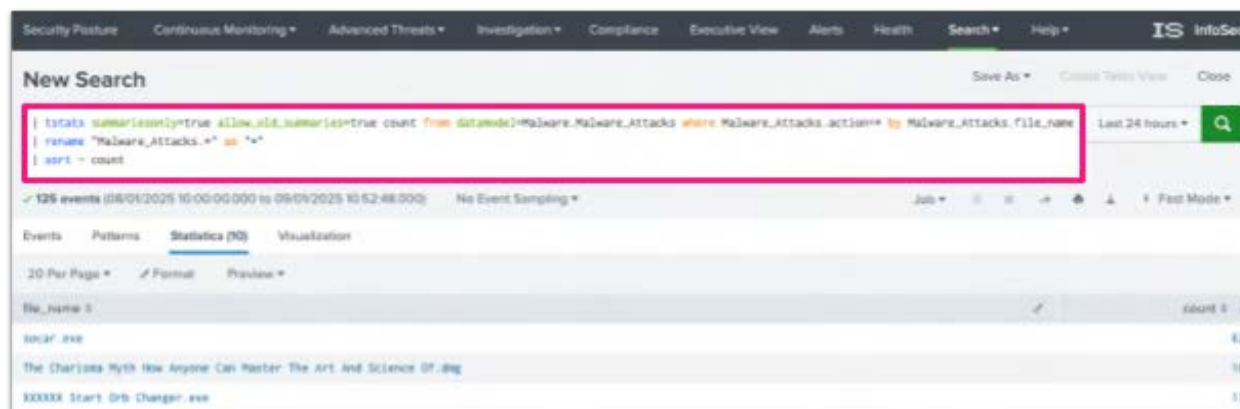
Now let's create an alert to inform the team if this infection is seen again in future.

1. Return to the **Malware** dashboard (**Continuous Monitoring > Malware**) and click on the search (🔍) button beneath the **Top Infected Files by Count** table.



file_name	count
socar.exe	61
The Charisma Myth How Anyone Can Master The Art And Science Of .log	37
XXXXXX Start Orb Changer.exe	12
idm01677	8
Policy022	4
assidknewactive.exe	4
dsungamreactive.exe	4
meackerethreactive.exe	4
pdfkey.exe	4
resharper.3.x.kaygen.exe	4

2. We can now see the full search that creates this table.



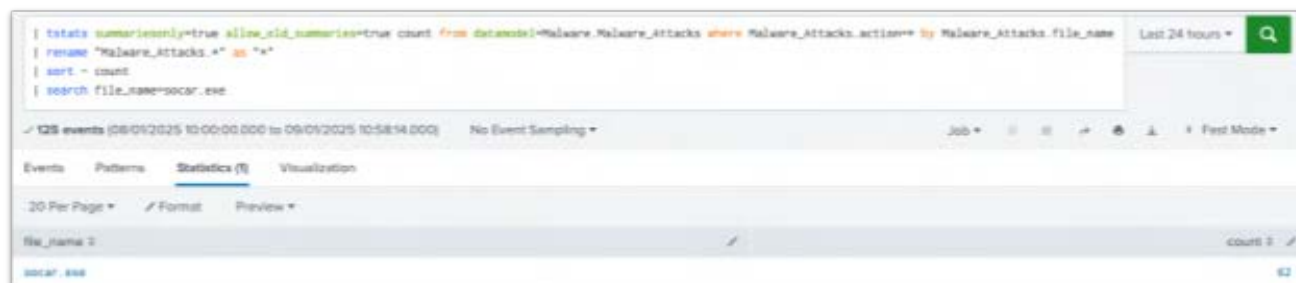
```
| tstats summariesonly=true allow_old_summaries=true count from datamodel=Malware.Malware_Attacks where Malware_Attacks.action=* by Malware_Attacks.file_name  
| rename 'Malware_Attacks.*' as '*'  
| sort - count
```

file_name	count
socar.exe	61
The Charisma Myth How Anyone Can Master The Art And Science Of .log	37
XXXXXX Start Orb Changer.exe	12

In this scenario we want to create an alert specifically for when the **socar.exe** file is detected. To do that, add the following filter to the end of the search:

```
| search file_name=socar.exe
```

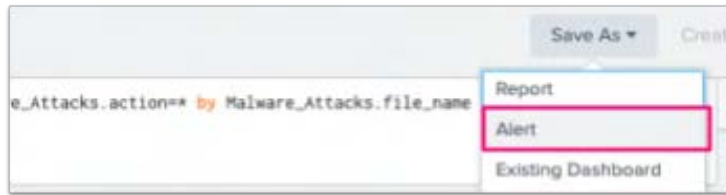
3. Now re-run your search and check that you only see that file in the table.



```
| tstats summariesonly=true allow_old_summaries=true count from datamodel=Malware.Malware_Attacks where Malware_Attacks.action=* by Malware_Attacks.file_name  
| rename 'Malware_Attacks.*' as '*'  
| sort - count  
| search file_name=socar.exe
```

file_name	count
socar.exe	61

4. To create an alert, above the search box click on **Save As > Alert**.



5. Create an alert that runs every hour, to be triggered when **socar.exe** is detected (i.e. if the number of results returned by this search is greater than “0”).

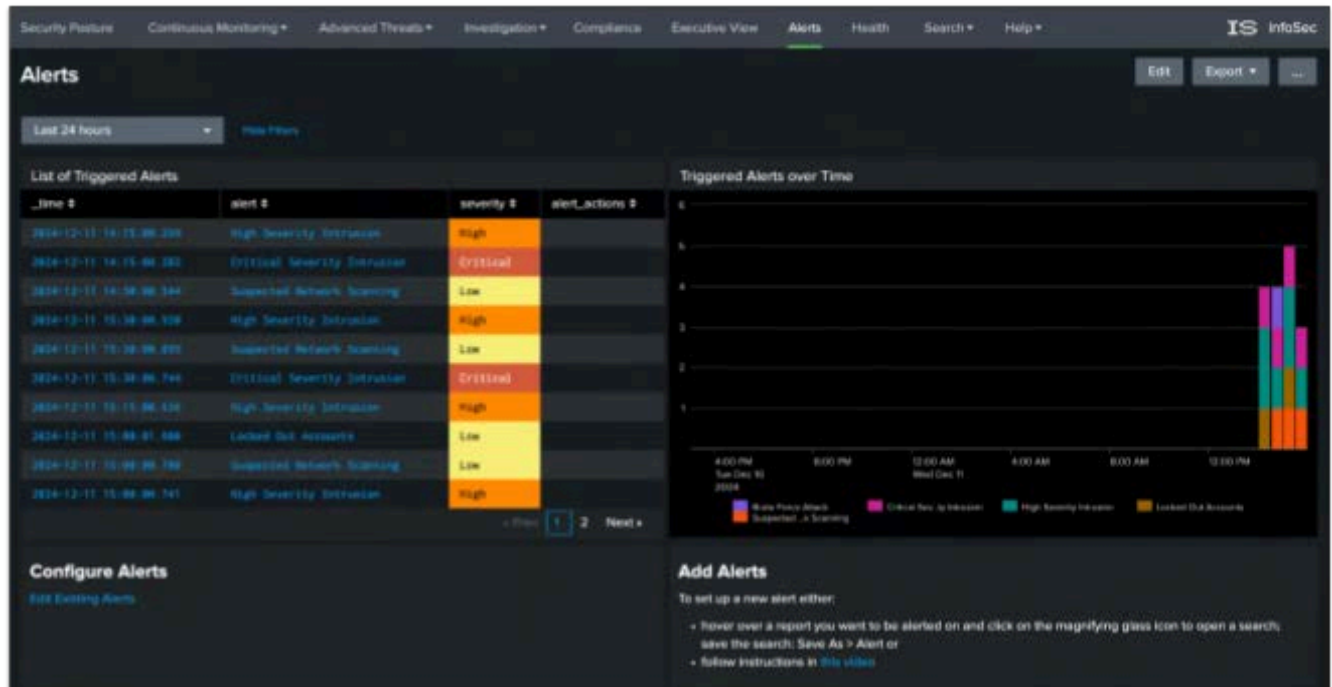
A screenshot of the 'Save As Alert' configuration dialog in Splunk. The dialog has a title bar with 'Save As Alert' and a close button. It is divided into several sections: 'Settings', 'Trigger Conditions', and 'Throttle'. In the 'Settings' section, the 'Title' is 'Infected "socar.exe" detected', the 'Description' is 'Optional', 'Permissions' are set to 'Private', 'Alert type' is 'Scheduled', and the frequency is 'Run every hour'. In the 'Trigger Conditions' section, the 'Trigger alert when' is set to 'Number of Results', which is 'is greater than' '0'. The 'Trigger' is set to 'Once'. There is a 'Throttle' checkbox which is unchecked. The 'Expires' field is set to '24' hours.

6. Under the **Trigger Actions** section click on **+ Add Actions** and select **Add to Triggered Alerts**. This means any alerts created will be added to the Triggered Alerts list within Splunk.

Leave the Severity as **Medium** and click on **Save**.

A screenshot of the 'Trigger Actions' section in Splunk. It shows a '+ Add Actions' button. Below it, there is a list of actions. The first action is 'Add to Triggered Alerts', which has a bell icon. To the right of this action is a 'Remove' button. Below the action list, there is a 'Severity' dropdown menu set to 'Medium'.

When your alert triggers it will be displayed on the InfoSec app's Alerts dashboard.



Exercise 4 – User Behavior Investigation

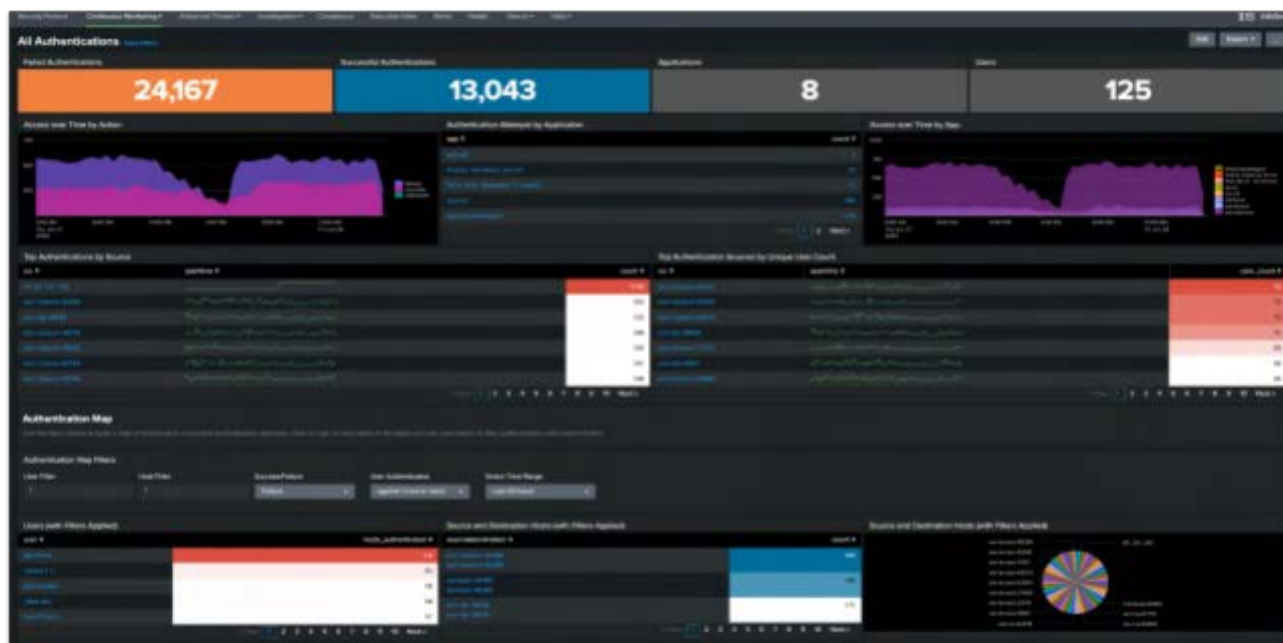
Description

Analyzing user behaviors helps detect unauthorized access and account modifications, addressing potential insider threats.

In this exercise we will look for any sudden access changes, unauthorized role modifications, or unusual activity.

Steps

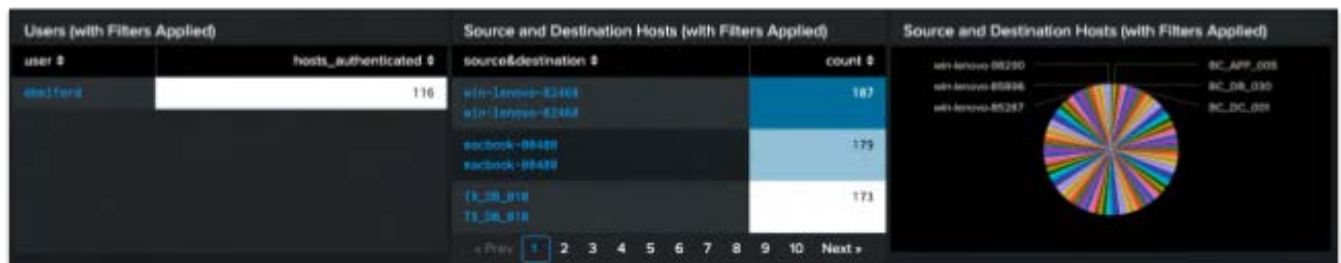
1. In the InfoSec app, browse to **Continuous Monitoring > All Authentications**. This dashboard shows us all authentication actions taken in our environment.



2. Scroll down to the **Users (with Filters Applied)** table. This shows us the number of times each user authenticated against any of the hosts/systems in our environment. Notice that **ebelford** has authenticated against an unusually high number of hosts compared to the other users.

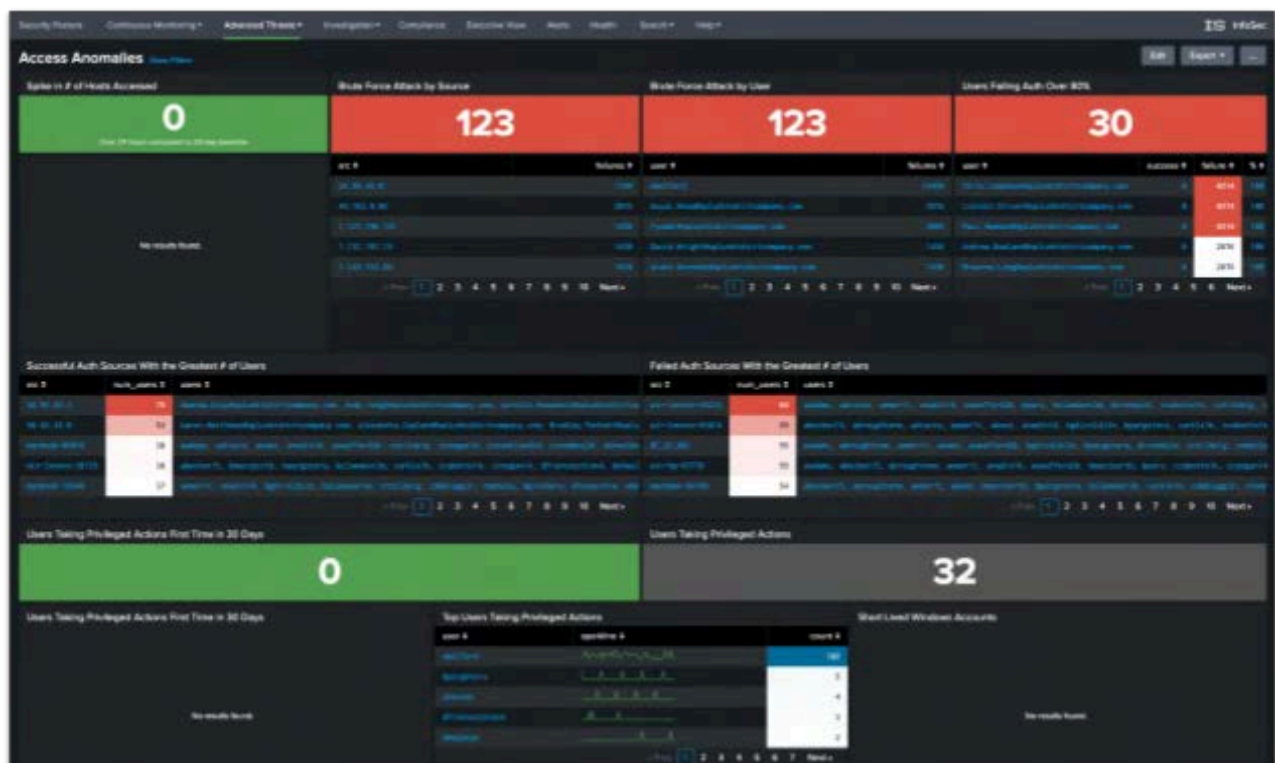
Users (with Filters Applied)	
user #	hosts_authenticated #
ebelford	116
vsewallis	63
ghincowef	58
jowarday	58
heillierl	57

- Optionally click on the **ebelford** user to filter the panels in that section by just that user. You will be able to see the sources and destinations that they authenticated against.

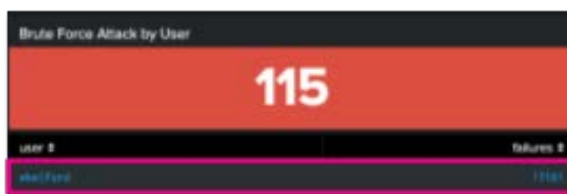


Let's now look in a bit more detail at access anomalies to see what else we can find.

4. Browse to **Advanced Threats > Access Anomalies** and identify the following information:
- Which users had the most login failures?
 - Which users are performing the most privileged actions?



Notice that **ebelford** has both a high number of failed logins (see **Brute Force Attack by User**) and also is taking a large number of privileged actions (see **Top Users Taking Privileged Actions**). Click on the name “**ebelford**” in either of those tables to navigate to the **User Investigation** dashboard.



5. Review the account changes made by **ebelford** shown on this dashboard - is there anything suspicious or anomalous? (Hint: Pay attention to the **Account Changes** chart.)



From the insights we've gathered it's clear that the **ebelford** account has been behaving strangely and is carrying out actions out of line with other accounts. At this point we now have enough information to work with the IT team to lock the user account and force a password reset and work to reverse any malicious changes that were made.

Exercise 5 – Customize the InfoSec App

Description

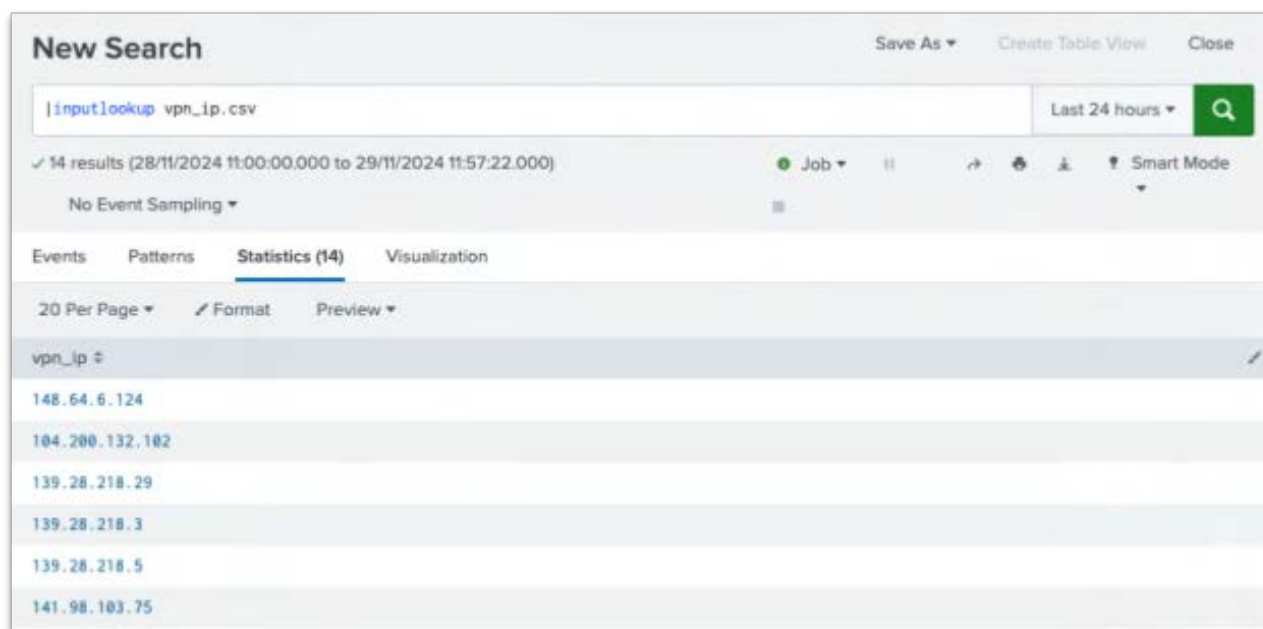
The InfoSec app contains some great out of the box views for common use security cases, but we can tailor the content to ensure it's as relevant as possible to the university's needs.

The university's IT team wants to exclude known VPN IP addresses from the **Geographically Improbable Access** search to remove false positives that can result when users connect to the university's systems using a VPN. They have uploaded a lookup file (**vpn_ip.csv**) containing those IPs, which we can use to tailor our content.

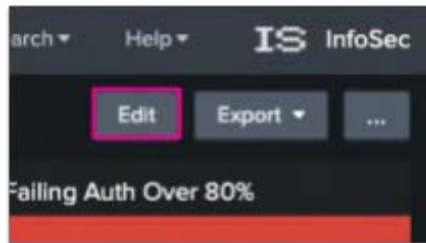
Steps

1. In the InfoSec app go to **Search > Search** and check the contents **vpn_ip.csv** lookup file by running the following search:

```
| inputlookup vpn_ip.csv
```



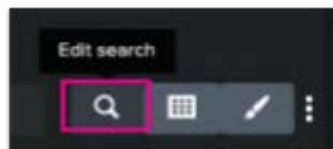
2. Navigate to **Advanced Threats > Access Anomalies** and switch to **Edit** mode.



3. Scroll down to the **Geographically Improbable Access** table. Notice that we see src IP addresses from India as well as Australia. The India IPs are from our VPN provider and need to be filtered out.

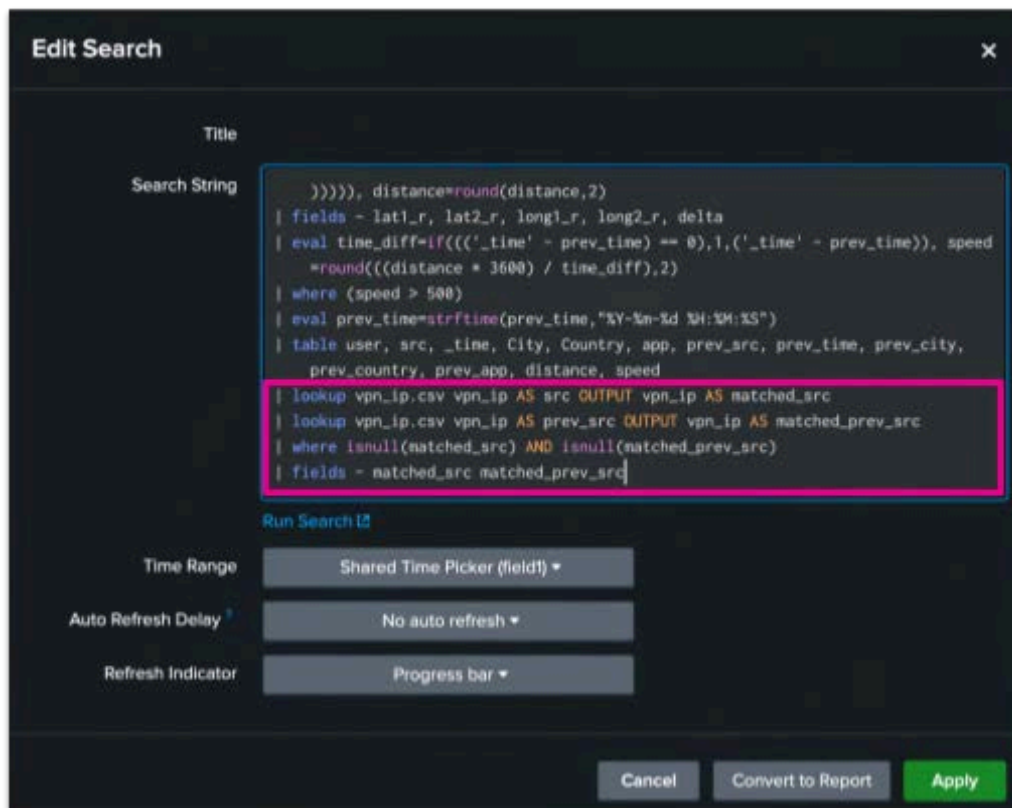
user	src	_time	City	Country	app	prev_src
Varsha.Mahadevan@splunkshirtcompany.com	58.96.43.0	2024-09-19 12:00:01	North Sydney	Australia	AzureActiveDirectory	148.64.6.124
mickey.perre@splunkshirtcompany.com	58.96.43.3	2024-09-19 12:00:01	North Sydney	Australia	AzureActiveDirectory	220.253.98.44
shaun.stuart@splunkshirtcompany.com	58.96.43.0	2024-09-19 12:00:01	North Sydney	Australia	AzureActiveDirectory	1.132.107.15
Varsha.Mahadevan@splunkshirtcompany.com	148.64.6.124	2024-09-19 12:01:01	Mumbai	India	AzureActiveDirectory	58.96.43.0
Varsha.Mahadevan@splunkshirtcompany.com	58.96.43.0	2024-09-19 12:01:01	North Sydney	Australia	AzureActiveDirectory	148.64.6.124

4. Click the magnifying glass icon above this table to edit the search.



5. In the **Search String** box, add the following SPL at the end of the search:

```
| lookup vpn_ip.csv vpn_ip AS src OUTPUT vpn_ip AS matched_src
| lookup vpn_ip.csv vpn_ip AS prev_src OUTPUT vpn_ip AS matched_prev_src
| where isnull(matched_src) AND isnull(matched_prev_src)
| fields - matched_src matched_prev_src
```



This search will lookup the IP addresses in our search results against our lookup file of the university's known IP addresses, and only return results that are NOT in those IP ranges.

SPL Line-by-Line Explanation:

```
| lookup vpn_ip.csv vpn_ip AS src OUTPUT vpn_ip AS matched_src
```

- ↳ Match the field “**vpn_ip**” in the lookup file with the field “**src**” from our data. Where there is a matched value it outputs a new field called “**matched_src**”, with the value of the IP address that was matched.

```
| lookup vpn_ip.csv vpn_ip AS prev_src OUTPUT vpn_ip AS matched_prev_src
```

- ↳ Repeat the exact same step but with the **prev_src** field, outputting a new field called “**matched_prev_src**”.

```
| where isnull(matched_src) AND isnull(matched_prev_src)
```

- ↳ Applies a filter to only show events **where** the “**matched_src**” and “**matched_prev_src**” fields are both empty, meaning if the IP address was in the lookup file and in the logs, they were “marked” as

“matched” and they won’t be shown in the final table (thus, not reported as geographically improbable access).

```
| fields - matched_src matched_prev_src
```

- ↳ Removes the fields that we don’t want to show because they were just temporary fields to help us with filtering the IP addresses.

6. Click on **Apply** to save the search.

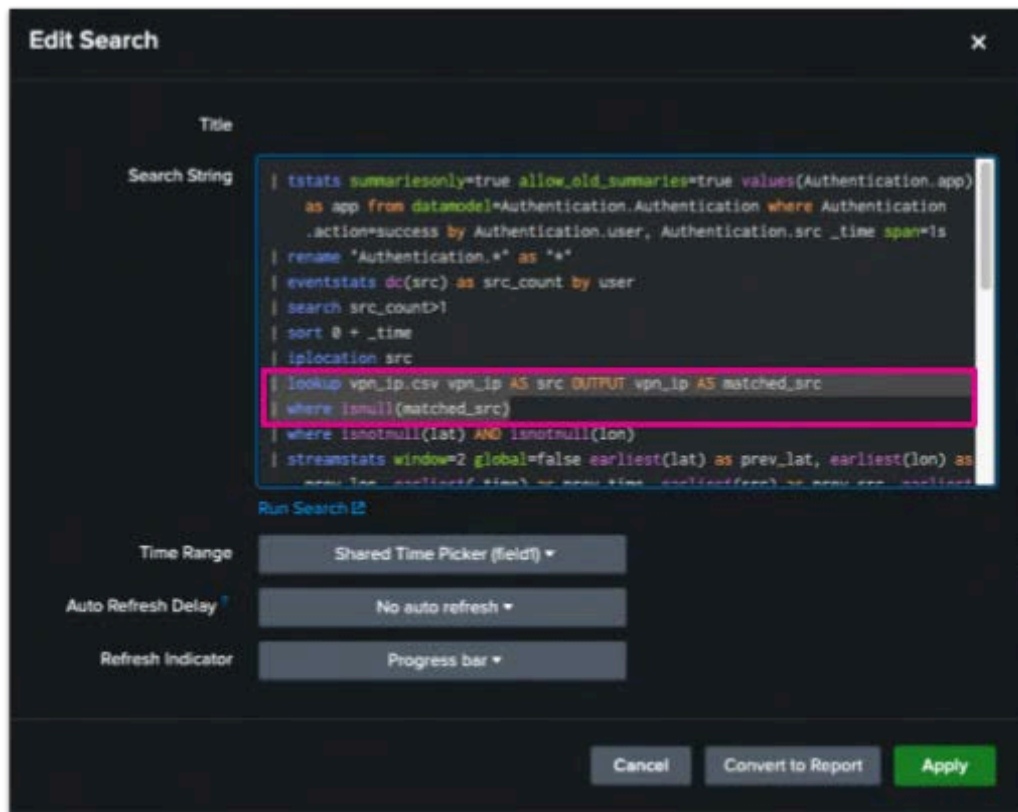
Notice now that the table updates and we only see events from **Australia** as we have filtered out our **India** IP addresses using our modified search.

user	src	_time	City	Country	app	prev_src	prev_time	prev_city	prev_country
Widney_jamie@lunaticcircuscompany.com	58.58.43.1	2024-10-24 00:23:01	North Sydney	Australia	AccountActiveDirectory	238.233.58.44	2024-10-24 00:23:01	Woolloomooloo	Australia
shaun.stuart@lunaticcircuscompany.com	58.58.43.8	2024-10-24 00:23:01	North Sydney	Australia	AccountActiveDirectory	1.132.180.15	2024-10-24 00:23:01	Woolloomooloo	Australia
Widney_jamie@lunaticcircuscompany.com	238.233.58.44	2024-10-24 00:24:01	Woolloomooloo	Australia	AccountActiveDirectory	58.58.43.1	2024-10-24 00:23:01	North Sydney	Australia
Widney_jamie@lunaticcircuscompany.com	58.58.43.1	2024-10-24 00:24:01	North Sydney	Australia	AccountActiveDirectory	238.233.58.44	2024-10-24 00:24:01	Woolloomooloo	Australia
shaun.stuart@lunaticcircuscompany.com	1.132.180.15	2024-10-24 00:24:01	Woolloomooloo	Australia	AccountActiveDirectory	58.58.43.8	2024-10-24 00:23:01	North Sydney	Australia

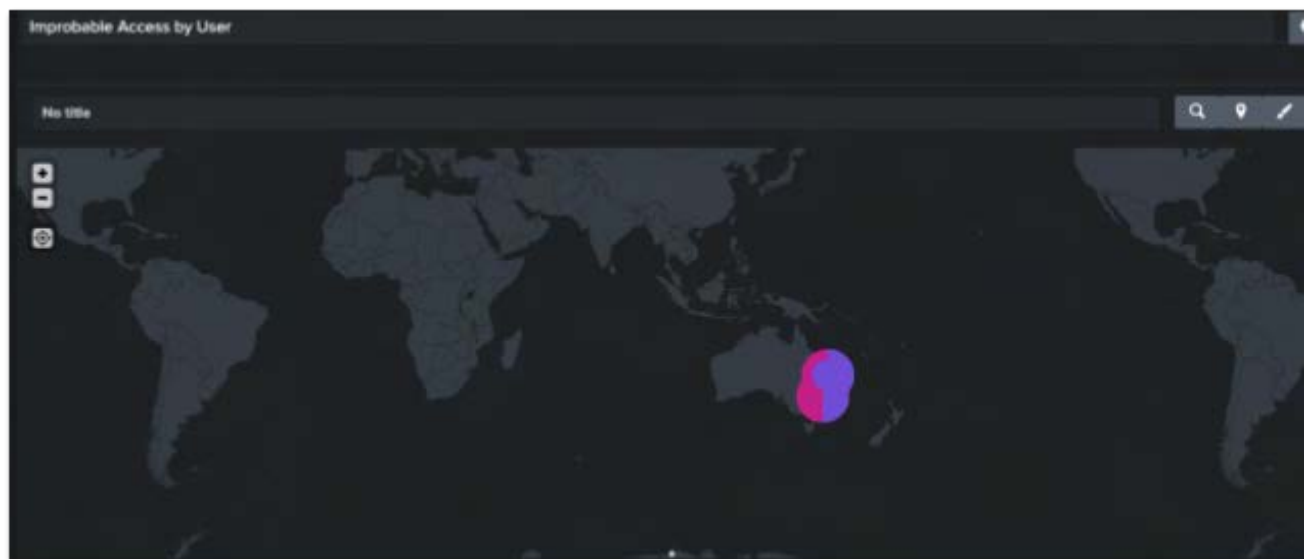
7. We now need to customize the **Improbable Access by User** map visualization beneath this table to also filter out our known IP addresses.

Click the magnifying glass icon above the map to edit the search and add these two lines under the iplocation line:

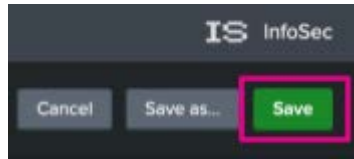
```
| lookup vpn_ip.csv vpn_ip AS src OUTPUT vpn_ip AS matched_src  
| where isnull(matched_src)
```

8. Click on **Apply** to save the search. Verify that you no longer see India IP addresses highlighted on the map.



9. **Save** your dashboard.



Exercise 6 – Adding Security Content: New Use Case

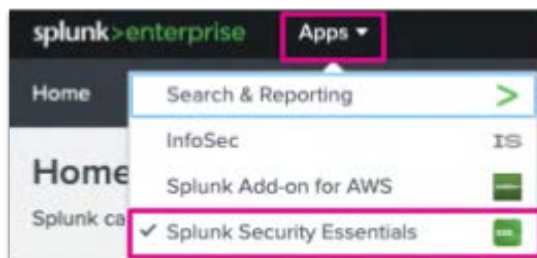
Description

The free Splunk Security Essentials app provides a great way to find and add new security use cases. Doing so helps you to enhance the InfoSec app's capabilities and address emerging security needs.

The Security team wants a new dashboard panel to show recurring infections on any of the hosts in the Buttercup State University environment.

Steps

1. Navigate to **Apps > Splunk Security Essentials**.



2. On the menu click on **Content > Security Content**.



3. In the search field type "Recurring Infection on Host" and click on the **Recurring Infection on Host** use case in the results.

Search

Recurring Infection on Host

☒ Hide Low Scoring Matches

Search

Examples

Recurring Infection on Host

Looks for the same malware occurring multiple times on the same host.

Featured

Execution Initial Access

Drive-by Compromise

User Execution Phishing

Delivery None

- On the **Recurring Infection on Host** use case page, scroll down and click on **Live Data**. Review the search **query** and click the search button to run the search.

View

Demo Data **Live Data** Accelerated Data

Prerequisites

Check Status Open in Search Resolution (if needed)

Must have Symantec AV data ☒ Open in Search For simplicity, this search is written specifically for Symantec AV data, but it can be easily modified for other sources.

Enter a search

```
index= sourcetype=symantec:* earliest=-360
| state count range=time || TimeRange by Risk_Name, Computer_Name
| where TimeRange>1800
| eval TimeRange_In_Hours = round(TimeRange/3600, 2), TimeRange_In_Days = round(TimeRange/3600/24, 2)
```

✓ 373 events (22/09/2024 12:17:44.000 to 22/10/2024 12:17:45.387)

Last 24 hours

Job 11 16 Smart Mode

- Scroll down to the **Raw Data Preview** section and verify that you see results.

Raw Data Preview

(Click Select New Values above to find outliers.)

Risk_Name	Computer_Name	count	TimeRange	TimeRange_In_Days	TimeRange_In_Hours
Backdoor.Jaggyer	boxster	9	173357	2.81	68.15
Backdoor.Jaggyer	continental	18	195863	3.26	54.19
Backdoor.Jaggyer	Frontier	9	173357	2.81	68.15
Backdoor.Jaggyer	rabbit	9	173357	2.81	68.15
Backdoor.Jaggyer	gryphon	9	173357	2.81	68.15
Backdoor.Jaggyer	salon	9	173357	2.81	68.15
Backdoor.Jaggyer	Thunderbolt	9	173357	2.81	68.15
SQMR.Neurstic.125	acclaim	9	173357	2.81	68.15
SQMR.Neurstic.125	boxster	18	173465	2.81	68.18
SQMR.Neurstic.125	continental	9	173357	2.81	68.15

1 2 3 4 5 6 Next

- Copy the search query to your clipboard (**CTRL+C** on Windows, **CMD+C** on Mac) and navigate to the InfoSec app.

7. Open the InfoSec app's **Search** view (**Search > Search**) and paste in the SPL you copied to your clipboard. Optionally run the search to verify that it copied/pasted correctly.

Risk_Name	Computer_Name	count	TimeRange	TimeRange_In_Days	TimeRange_In_Hours
Backdoor.Joggver	boxster	9	173357	2.01	48.15
Backdoor.Joggver	continental	10	195083	2.25	54.19
Backdoor.Joggver	frontier	9	173357	2.01	48.15
Backdoor.Joggver	rabbit	9	173357	2.01	48.15

8. Edit the search to create a table that only includes the “**Risk_Name**”, “**Computer_Name**” and “**count**” fields. To do this, add the following line to the end of the search:

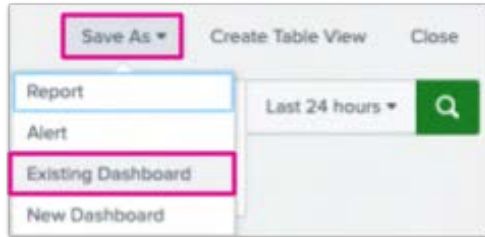
```
| table Risk_Name, Computer_Name, count
```

9. Re-run the search to verify that you only see the specified fields/columns in the table.

Risk_Name	Computer_Name	count
Trojan.Gen.2	bravada	2
Trojan.Gen.2	optima	2

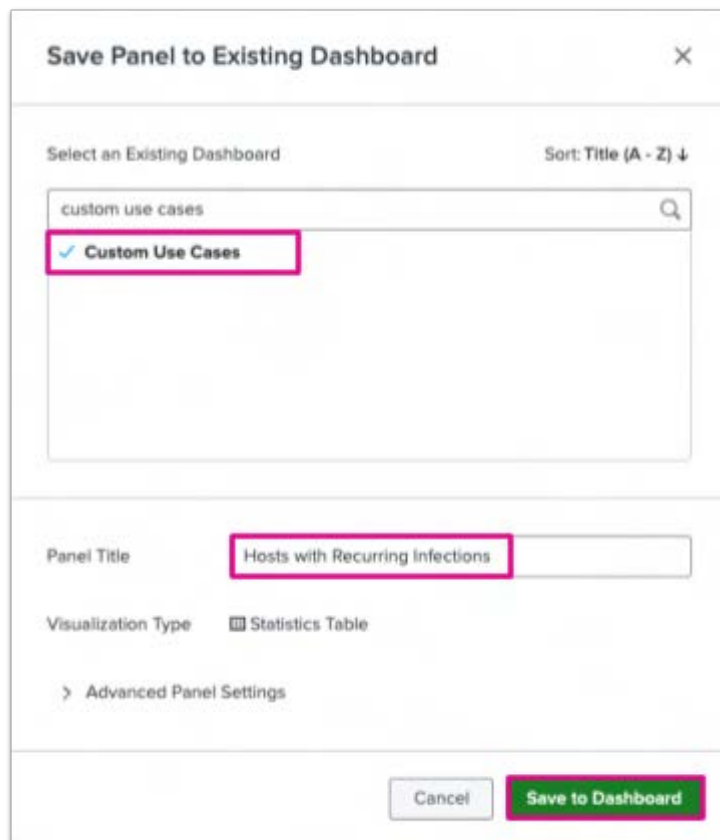
10. We now need to add this to a dashboard within the InfoSec app. For this exercise we will use the **Custom Use Cases** dashboard, which is provided out of the box as a place for custom searches such as this.

Click on **Save As > Existing Dashboard**.



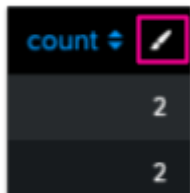
11. Search for and select the **Custom Use Cases** dashboard.


Give your panel a title, such as “**Hosts with Recurring Infections**” and click on **Save to Dashboard**.



12. On the popup click **View Dashboard**. (If you already closed that prompt, navigate to the dashboard at **Advanced Threats > Custom Use Cases**).

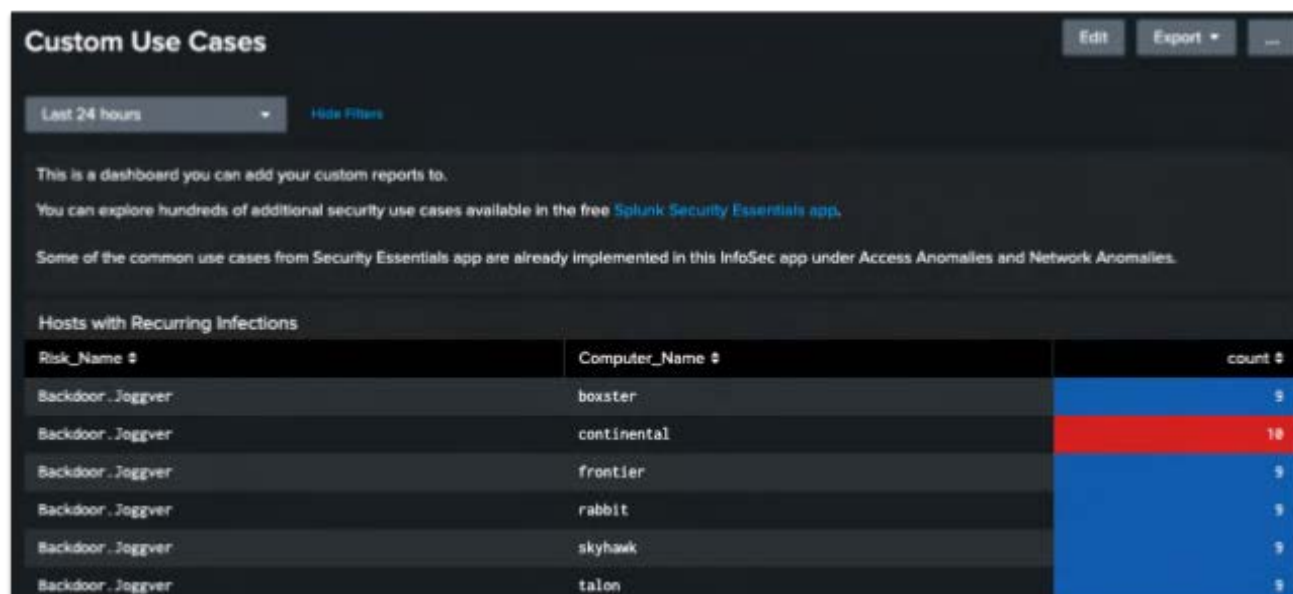
13. To help make the table easier to reach, add some colour by putting the dashboard into **Edit** mode and clicking on the edit (✎) icon for the **count** column.



14. Edit the color ranges as shown so a count of **10 or greater** will be red 



Make sure you **save** your dashboard when you're finished!



Risk_Name	Computer_Name	count
Backdoor.Joggver	boxster	9
Backdoor.Joggver	continental	10
Backdoor.Joggver	frontier	9
Backdoor.Joggver	rabbit	9
Backdoor.Joggver	skyhawk	9
Backdoor.Joggver	talon	9

Exercise 7 – Adding Security Content: New Dashboard

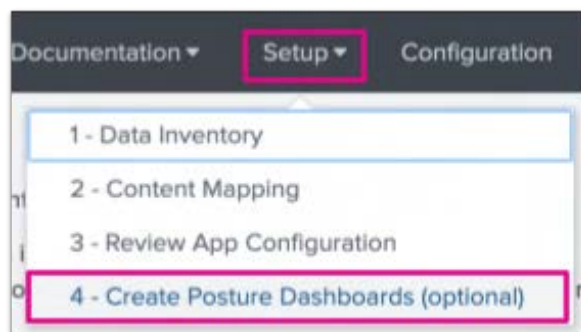
Description

The Security team has asked us to create a new custom dashboard showing network security insights, to help strengthen their continuous monitoring and network security.

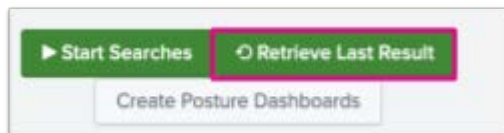
For this exercise we will use Splunk Security Essentials, which has a useful feature to help with creating new custom dashboards.

Steps

1. Open the Splunk Security Essentials app and in the menu bar navigate to **Setup > 4 - Create Posture Dashboards**.



2. Since we've already run this report for you, click on **Retrieve Last Result** to populate the report.



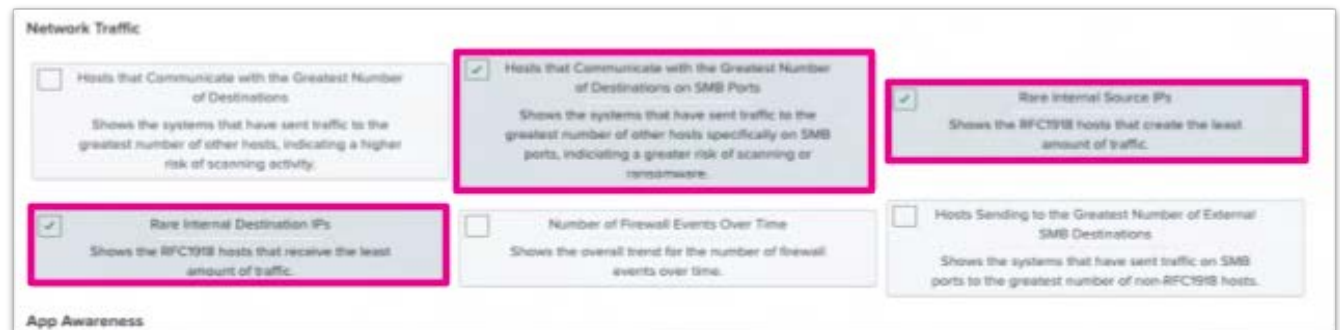
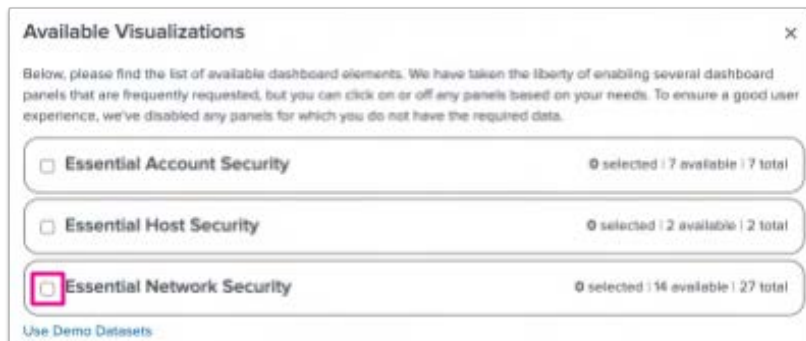
Note: If the 'Retrieve Last Results' button is not present or is greyed out, please refresh the page.

3. Click on **Create Posture Dashboards**.

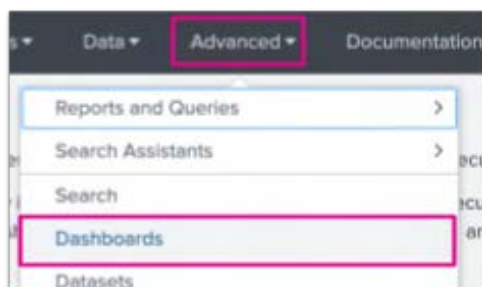


4. On the **Available Visualizations** popup, select **Essential Network Security** and ensure only the following detections are selected:

- **Rare Internal Destination IPs**
- **Rare Internal Source IPs**
- **Hosts communicating with the most destinations on SMB ports**



5. Your dashboard has now been created! Locate the new dashboard by navigating (still within Splunk Security Essentials) to **Advanced > Dashboards**.



You should see the new **Essential Network Security** dashboard listed.



- Optionally open the dashboard and verify that it contains the use cases you selected.

Essential Network Security Edit Export ...

Last 7 days Hide Filters

Network Traffic

Hosts that Communicate with the Greatest Number of Destinations on SMB Ports		Rare Internal Source IPs		Rare Internal Destination IPs	
All_Traffic.src_ip	count	All_Traffic.src_ip	count	All_Traffic.dest_ip	count
66.1.1.7	3	10.154.1.71	0	10.154.1.88	0
66.1.1.10	2	10.154.10.169	0	10.154.10.203	0
66.1.1.2	2	10.154.127.222	0	10.154.10.247	0
10.154.10.24	1	10.154.13.30	0	10.154.10.77	0
10.154.10.26	1	10.154.13.93	0	10.154.114.20	0
10.154.10.29	1	10.154.14.21	0	10.154.122.120	0
10.154.10.31	1	10.154.15.16	0	10.154.135.14	0
66.1.1.4	1	10.154.15.8	0	10.154.252.92	0
66.1.1.5	1	10.154.210.135	0	10.154.0.203	0
66.1.1.6	1	10.154.217.70	0	10.66.28.45	0

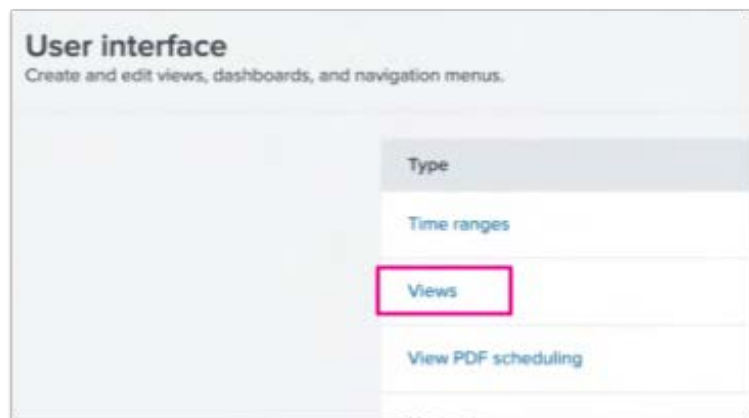
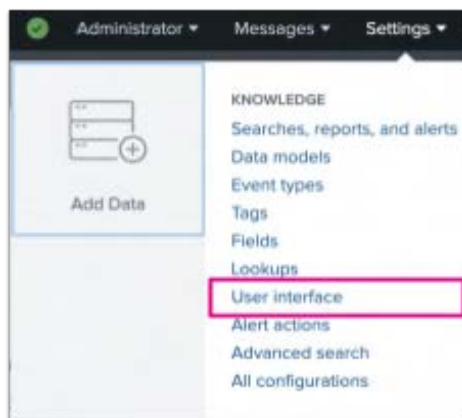
Shows the systems that have sent traffic to the greatest number of other hosts specifically on SMB ports, indicating a greater risk of scanning or ransomware.

Shows the RFC1918 hosts that create the least amount of traffic.

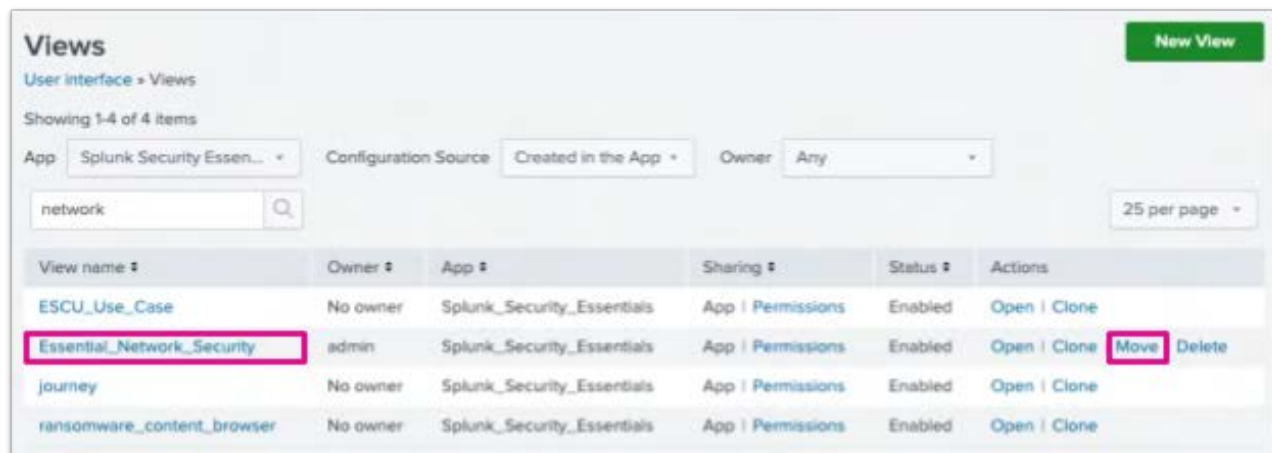
Shows the RFC1918 hosts that receive the least amount of traffic.

Now let's move the dashboard to the InfoSec app so it's alongside the rest of our security dashboards.

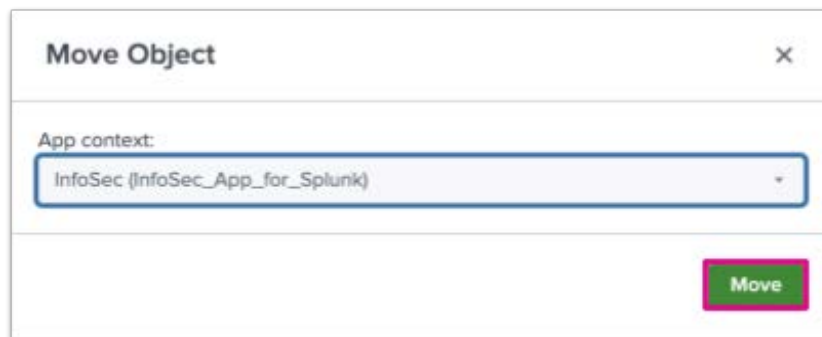
- In the top right corner of the screen go to **Settings** > **User interface**. On the **User interface** page click on **Views**.



8. Locate the **Essential_Network_Security** view (i.e. our dashboard) in the list and under the **Actions** column click on **Move**.



9. On the **Move Object** popup, select the InfoSec app and click **Move**.

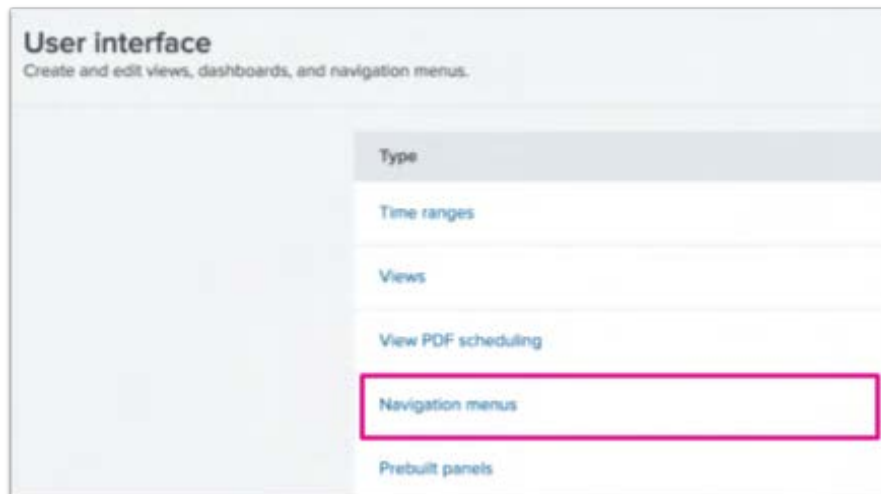


10. Your dashboard has now been moved to the InfoSec app! Verify this by opening the **InfoSec** app and navigating to **Search > Dashboards** and locating the dashboard in the list.

> Endpoints	Edit	nobody	InfoSec_App_for_Spl..
> Error Details	Edit	nobody	Splunk_TA_aws
> Essential Network Security	Edit	admin	InfoSec_App_for_Spl..
> Executive View	Edit	nobody	InfoSec_App_for_Spl..
> Firewalls	Edit	nobody	InfoSec_App_for_Spl..

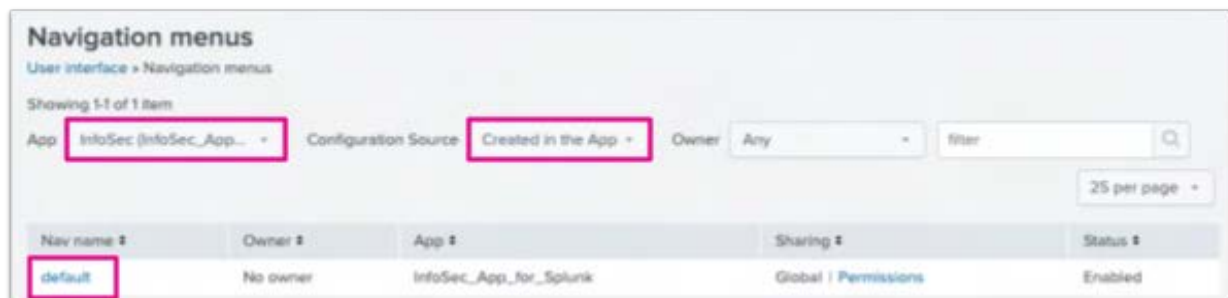
Our final step will be to add this dashboard to the dropdown menus within the InfoSec app. Add the dashboard to the navigation menu. This will help users to find this new dashboard and the insights it contains.

11. In the top right corner of the screen go to **Settings > User interface** and click on **Navigation menus**.



12. Ensure the **App** context is set to “**InfoSec (InfoSec_App_for_Splunk)**” and **Configuration Source** is set to “**Created in the App**”.

Click on the **default** navigation menu for the **InfoSec_App_for_Splunk**.



Here we can edit the XML of the navigation menus for this app.

13. Let's add our new dashboard under the **Continuous Monitoring** dropdown. To do this, locate the `<view name="malware">` line and add the following new line beneath it (note that the view name is case sensitive):

```
<view name="Essential_Network_Security"/>
```



Click on **Save**.

14. Now return to the **InfoSec** app and click on the **Continuous Monitoring** dropdown in the menu. You should now see your new dashboard listed!



A screenshot of the 'Essential Network Security' dashboard in the InfoSec app. The dashboard has a top navigation bar with links like 'Security Posture', 'Continuous Monitoring', 'Advanced Threats', etc. Below the navigation bar, there's a section titled 'Network Traffic'. It contains three tables. The first table, 'Hosts that Communicate with the Greatest Number of Destinations on SMB Ports', lists internal IP addresses and their counts. The second table, 'Rare Internal Source IPs', lists IP addresses and their counts. The third table, 'Rare Internal Destination IPs', lists IP addresses and their counts. Each table has a 'Page 1' indicator and a 'Next' button. Below each table is a brief description of what the data represents.

Summary

Congratulations on completing the hands-on exercises in today's workshop! By completing these exercises, you have helped Buttercup State University to customize the InfoSec App for Splunk to meet its specific needs, allowing them to enhance their security posture, and detect and respond to security threats more effectively.