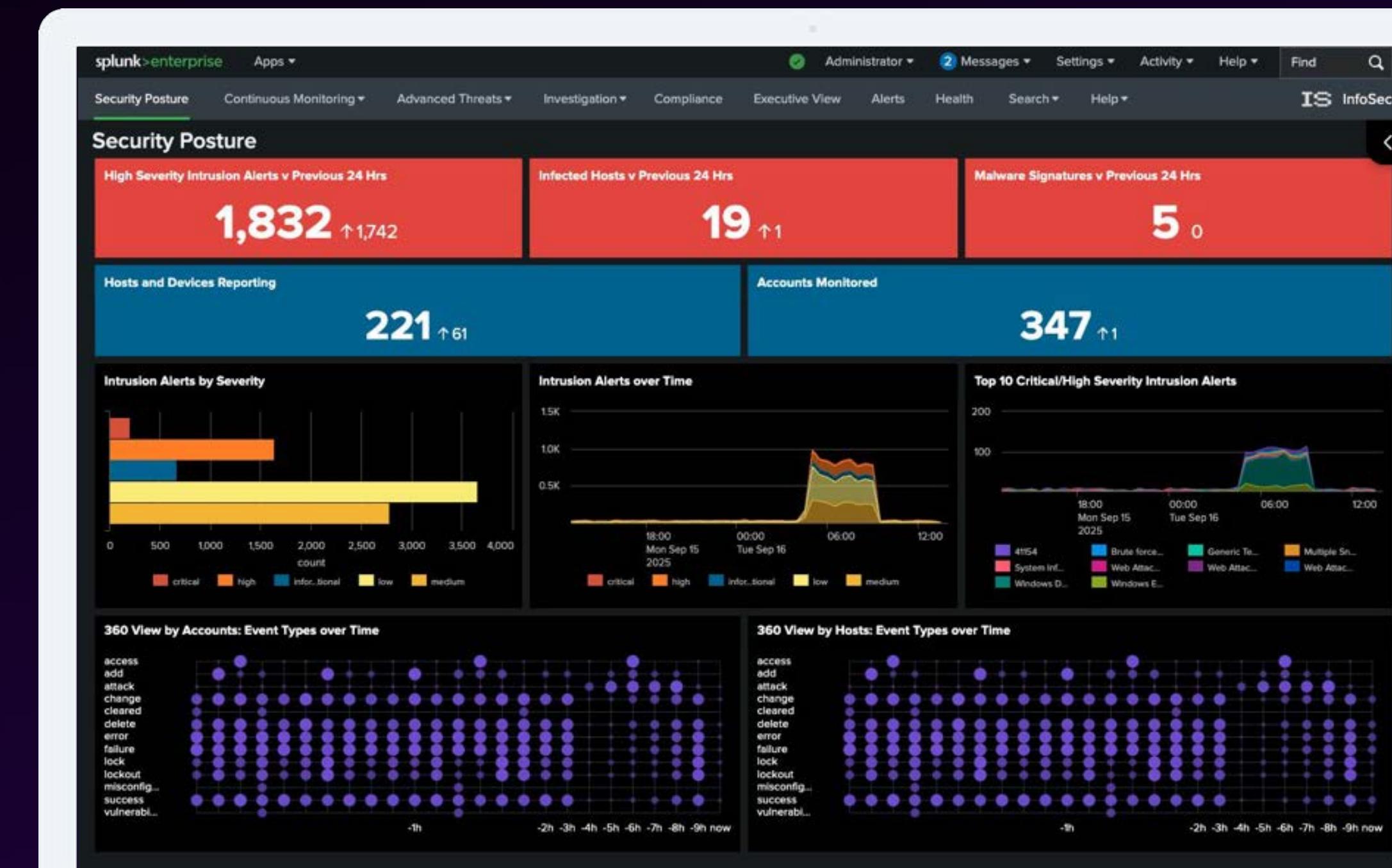


InfoSec App for Splunk

Hands-On Workshop



Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as "expects," "anticipates," "targets," "goals," "projects," "intends," "plans," "believes," "momentum," "seeks," "estimates," "continues," "endeavors," "strives," "may," variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the "Risk Factors" section of Cisco's most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the "Risk Factors" section of Splunk's most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk's website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

Target Audience



Role:

- ✓ Admins or Security Analysts

Experience (Should meet at least one of these):

- ✓ Some basic Splunk knowledge or hands-on experience
- ✓ Or you have attended a hands-on Splunk workshop, e.g. Splunk4Rookies

Please introduce yourself!

- Name
- Company/organization
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



Workshop Agenda



- Splunk security overview
- Data fundamentals
- InfoSec App for Splunk: setup and configuration
- Hands-on investigation
- Customizing the Infosec app
- Introduction to Splunk Security Essentials
- Combining InfoSec App for Splunk with Splunk Security Essentials
- Splunk Resources and next steps



REGISTRATION

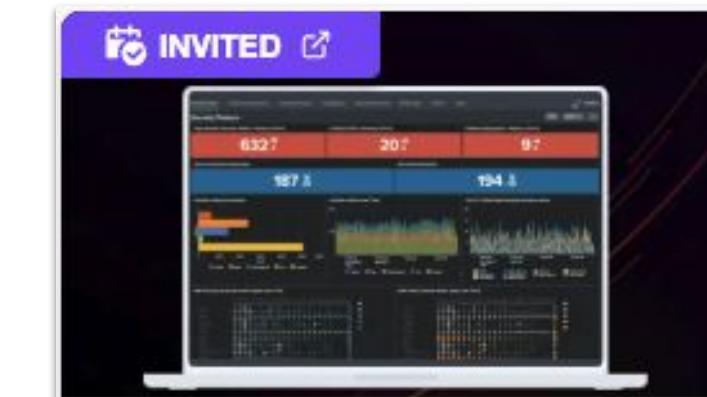
5 MINS

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:
<https://show.splunk.com/event/<eventID>
3. Download the hands-on lab guide:
<https://splk.it/Infosec-Lab-Guide>
Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
<https://splk.it/Infosec-Attendee>

Goal



SECURITY

InfoSec App Hands-on

⌚ 08/10 10:43 - 08/10 17:42

💻 Enterprise

📅 InfoSec App Hands-on

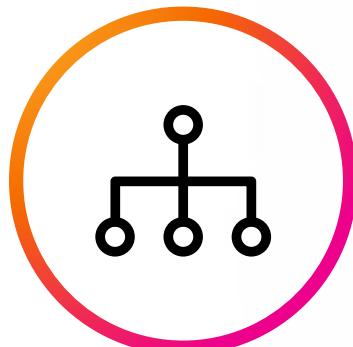
▶ AVAILABLE

Actions ▾

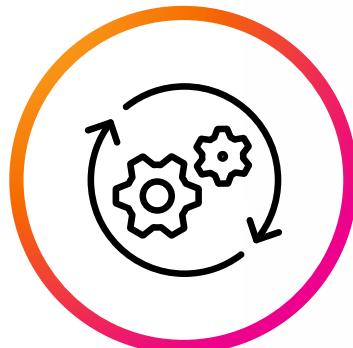
👤 + Enroll event

Enroll in today's event

Today, It's Hard to be Resilient



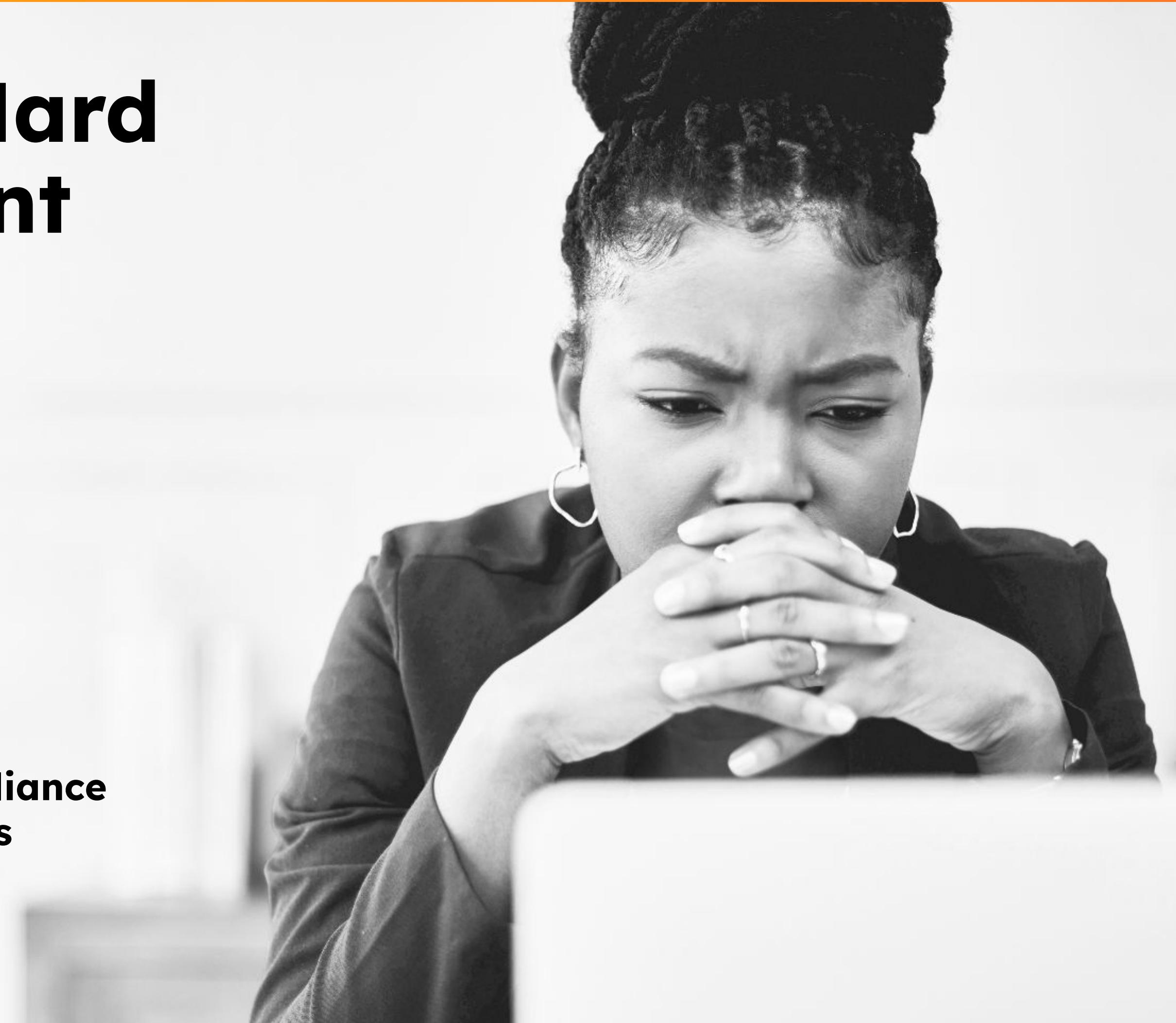
**Complex
Environments**



**Siloed tools
and teams**



**Evolving compliance
and regulations**



Splunk delivers unparalleled digital resilience.

Providing **end-to-end visibility** and insights across your entire digital footprint

Powering the **SOC of the future** with unified threat detection investigation and response, enhanced with network insights

Delivering **observability for the entire enterprise** to prevent unplanned downtime across all environments

Unified by a flexible platform that provides enterprise scale data management

Build digital resilience with Splunk.

Splunk brings SecOps, ITOps and engineering together to...



Prevent major
issues



Remediate
faster



Adapt quickly

The path to greater digital resilience.

Security SecOps

Foundational Visibility

See across environments

Search, monitor and investigate for real-time security monitoring

FREE

Splunk Security Essentials

FREE

InfoSec App for Splunk

PAID

Enterprise Security (SIEM)

FREE

Machine Learning Toolkit

PAID

Security Orchestration, Automation & Response (SOAR)

PAID

Attack Analyzer

PAID

User Behavior Analytics (UBA)

Guided Insights

Detect threats and issues with context

Reduce noise, detect more threats and identify risk with AI/ML powered detections

Proactive Response

Get ahead of issues

Accelerate incident investigations and response using automation

Unified Workflows

Collaborate seamlessly

Maximize SOC efficiency with integrated threat detection, investigation and response

Accelerated by Splunk AI

InfoSec App for Splunk Overview

Free Security app on Splunkbase

- Works on Splunk Enterprise and Splunk Cloud
- Uses standard Splunk functionality
- Requires CIM-compliant data
- Install on search head/cluster only
- 25 out-of-the-box dashboards which group many more panels
 - Security Posture
 - Compliance
 - Access Anomalies
 - Network Anomalies

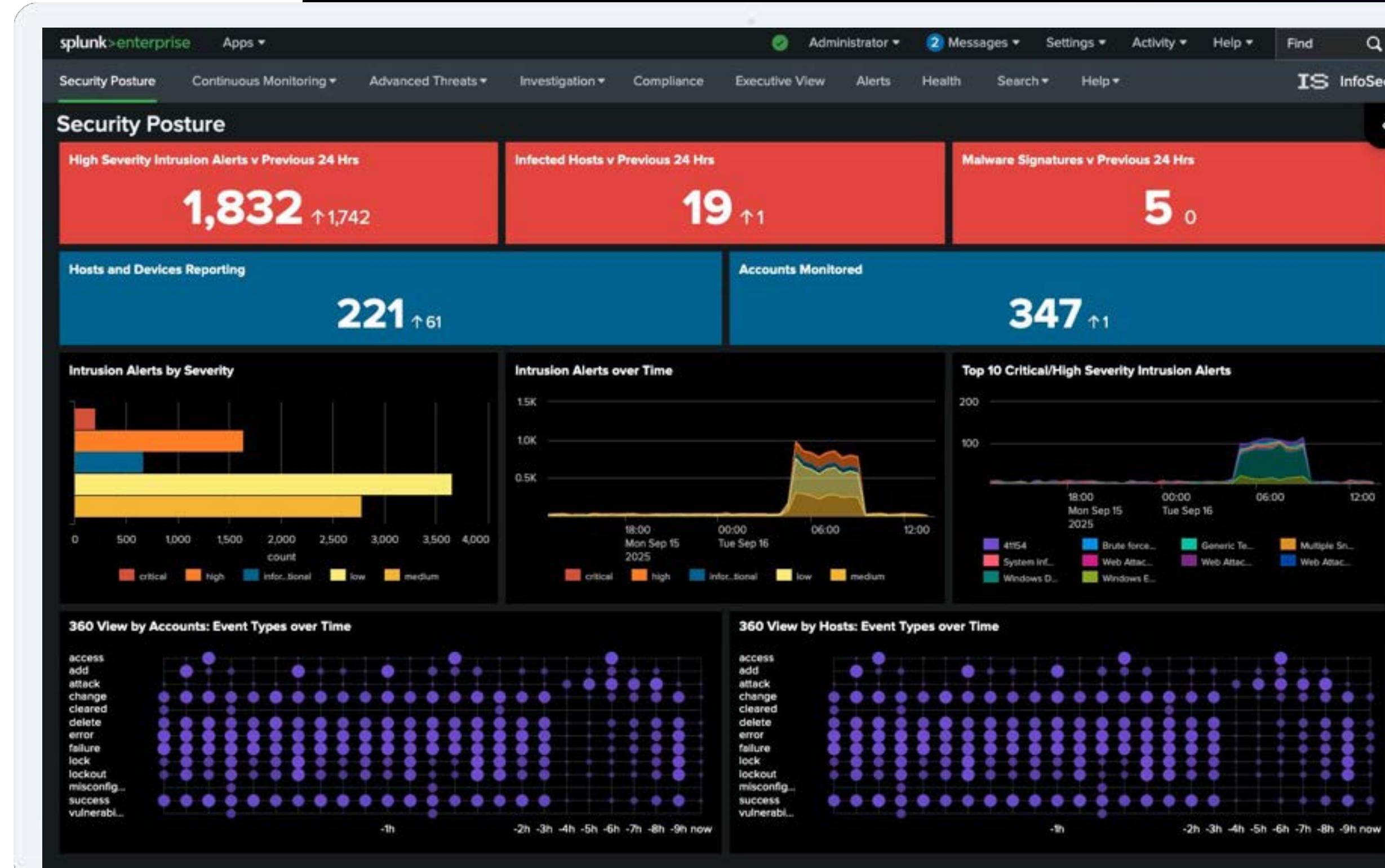
The screenshot shows the InfoSec App for Splunk page on Splunkbase. At the top, there's a navigation bar with 'splunkbase' logo, 'Collections', 'Apps', a search bar ('Find an app'), 'Submit an App', and 'Log In'. Below the header, the app's logo ('IS') and title ('InfoSec App for Splunk') are displayed. A brief description follows: 'InfoSec app for Splunk is your starter security pack. InfoSec app is designed to address the most common security use cases, including continuous monitoring and security investigations. InfoSec app also includes a number of advanced threat detection use cases. All of the components of...' and 'Built by Splunk Inc.' Below this, there's a 'Login to Download' button and a row of four screenshots showing different dashboard panels. Further down, there are sections for 'Latest Version 1.7.0' (released June 28, 2021), 'Compatibility' (Splunk Enterprise, Splunk Cloud, Platform Version: 9.2, 9.1, 9.0, 8.2, 8.1, 8.0, 7.3, 7.2, CIM Version: 5.X, 4.X, 3.X), 'Rating' (5 stars from 14 reviews), 'Support' (Splunk Supported App, Learn more), and 'Ranking' (#44 in Security, Fraud & Compliance).

Learn more: <https://docs.splunk.com/Documentation/InfoSec>

InfoSec App for Splunk design principles

Easy to use and modify with a minimal knowledge of Splunk

- Simple - no SPL knowledge required
- Out of the box content for common security use cases
- Leverages selected security content from Splunk Security Essentials (SSE)



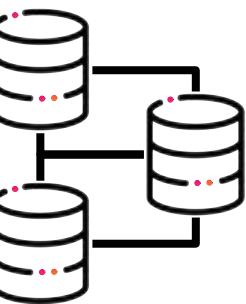
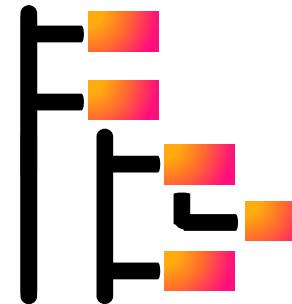
What are Data Models?

A data model is a search-time mapping of data into a hierarchical structure

- Structured, hierarchical mapping of semantic knowledge of a collection of datasets.
- A collection of objects
 - That have constraints and attributes
 - Where child objects inherit those constraints and attributes
 - Outlines the details necessary to enable searches of a dataset information



Splunk's Common Information Model (CIM)



Preconfigured data models

Contains a collection of preconfigured data models that you can apply to your data at search time

Normalize your data

Helps you to normalize your data to match a common standard

Use common field names for equivalent events from different sources or vendors

E.g. Use "src_ip" instead of

- "sourceIPAddress" in AWS data, and
- "callerIp" in GCP data

Utilizes tags

User-defined labels that group events, hosts, or other objects for easier identification, organization, and searching

E.g. Create a "critical_error" tag for events that contain "error" and "high severity". Then you can simply search for "tag=critical_error"

Learn More about Splunk Add-ons and the Common Information Model:

<https://docs.splunk.com/Documentation/AddOns/released/Overview/Add-onsandCIM>

How do you ensure your data is CIM compliant?

Tags!

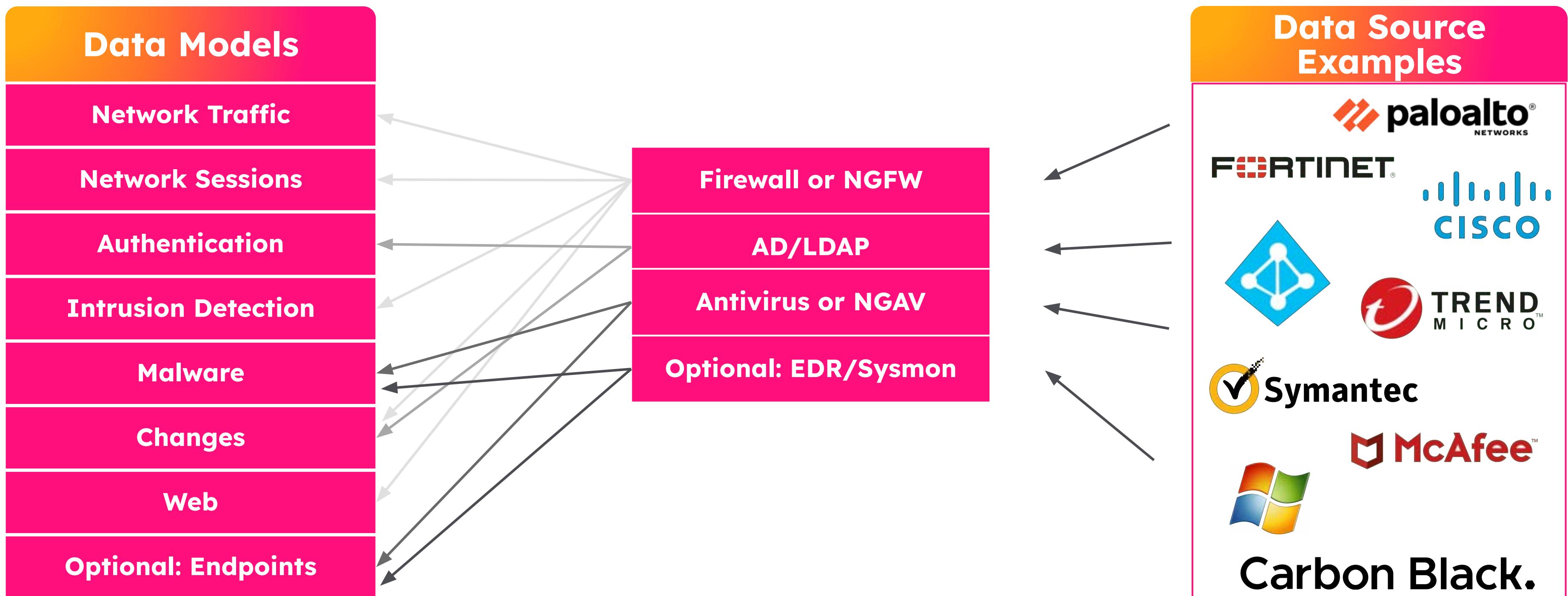
- The CIM employs the use of tags to identify data to different data models
- Ensure your data is tagged properly
 - Example: Check the tags field

The screenshot shows a histogram of tag values. The x-axis represents the tag values, and the y-axis represents the count of events. The top three values are authentication, os, and security, each with a count of 34,245 and a percentage of 100%.

Tag Value	Count	%
authentication	34,245	100%
os	34,245	100%
security	34,245	100%



InfoSec App Data Sources



Splunk **Common Information Model** allows using
many other data sources in the InfoSec App

InfoSec App Implementation

High level overview

- 1. Send AD, FW, AV data to Splunk using CIM-compliant add-ons**
- 2. Install required add-ons from Splunkbase (CIM Add-On, Force Directed Visualization, Lookup File Editor)**
- 3. Enable Data Model Acceleration via UI (Authentication, Change, Intrusion Detection, Malware, Network Sessions, Network Traffic, Endpoint, Web)**
- 4. Install InfoSec App from Splunkbase, no initial configuration required**
(Steps 2–4 take approximately 5 mins to complete)

Name	Folder name	Version
InfoSec	InfoSec_App_for_Splunk	1.7.0
Slack Alerts	slack_alerts	2.3.0
Search & Reporting	search	9.2.1
Sankey Diagram	sankey_diagram_app	1.4.0 Update to 1.6.0
Punchcard	punchcard_app	1.5.0
Home	launcher	
Force Directed Visualisation App for Splunk	force_directed_viz	3.1.0
Splunk Common Information Model	Splunk_SA_CIM	5.3.2

Today's Scenario

Your Company

- Buttercup State University is a close-knit community college home to approximately 2,500 students.
- Security hasn't been a top priority but recent cyber attacks on other universities have brought it into focus.
- Buttercup State University has recently invested in Splunk to help address any potential threats or breaches swiftly.

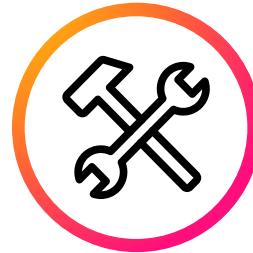
Your Role

- You are one of the Security Analysts at Buttercup State University and are also fairly new to Splunk.
- The IT team have installed Splunk, forwarded data from a variety of sources and also installed some apps, including the InfoSec App for Splunk.
- They've now tasked you with finishing the setup and providing some specific security insights for IT management...

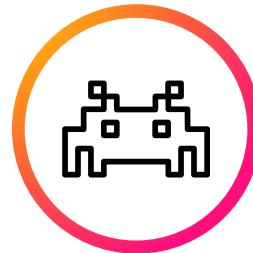


**BUTTERCUP STATE
UNIVERSITY**

What Has the University Asked For?



IT team: Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly



Malware: Find Malware-infected files and setup an alert for future detections



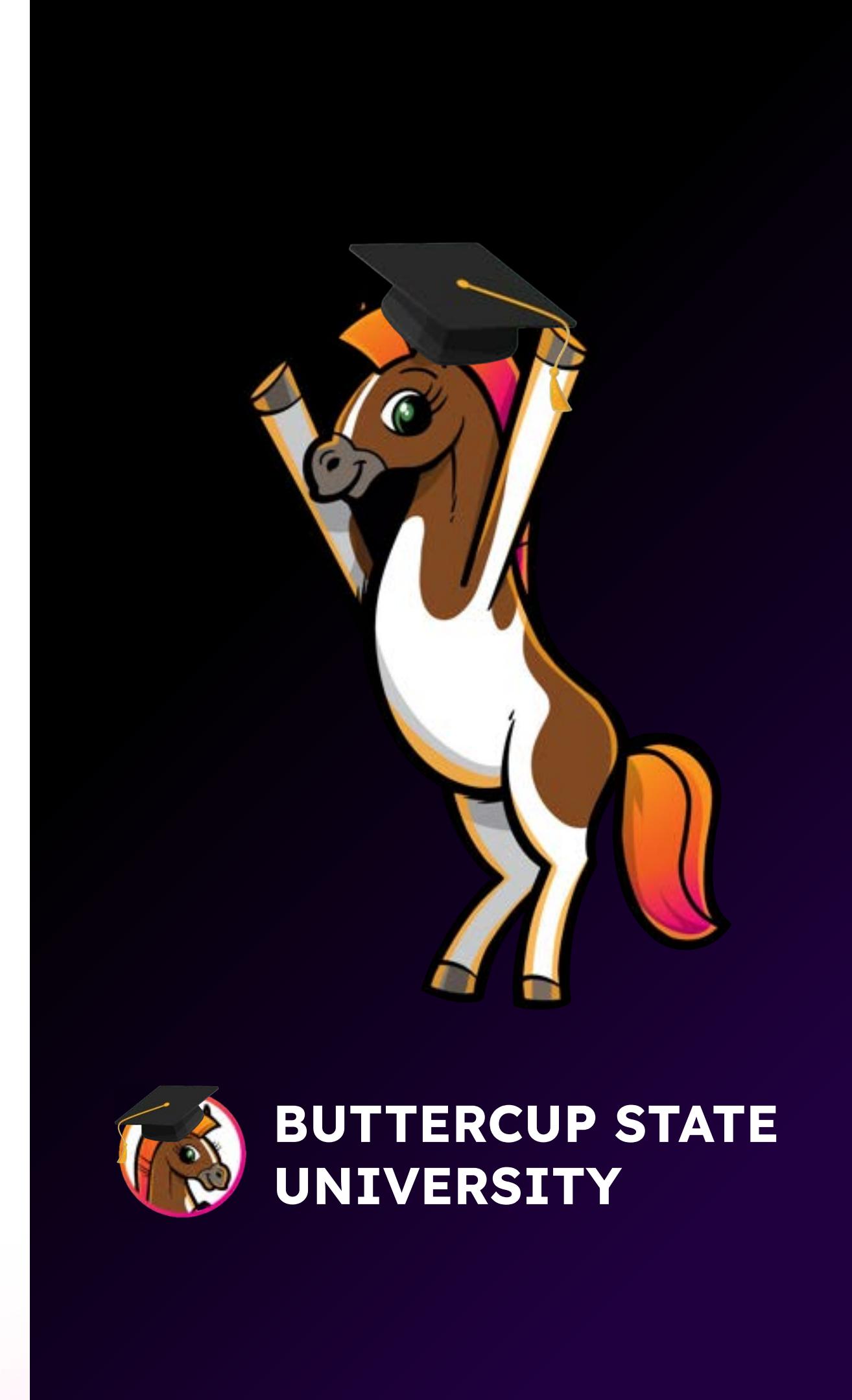
User behavior: Look for sudden access changes, unauthorized role modifications, or unusual activity



Customize the InfoSec App: Look for ways to customize the content for Buttercup State University



Add additional security content: Review the content in Splunk Security Essentials and add any new use cases you think might be valuable



Set Up the InfoSec App

Install the Splunk Add-on for AWS and finish setting up the InfoSec App for Splunk

Tasks

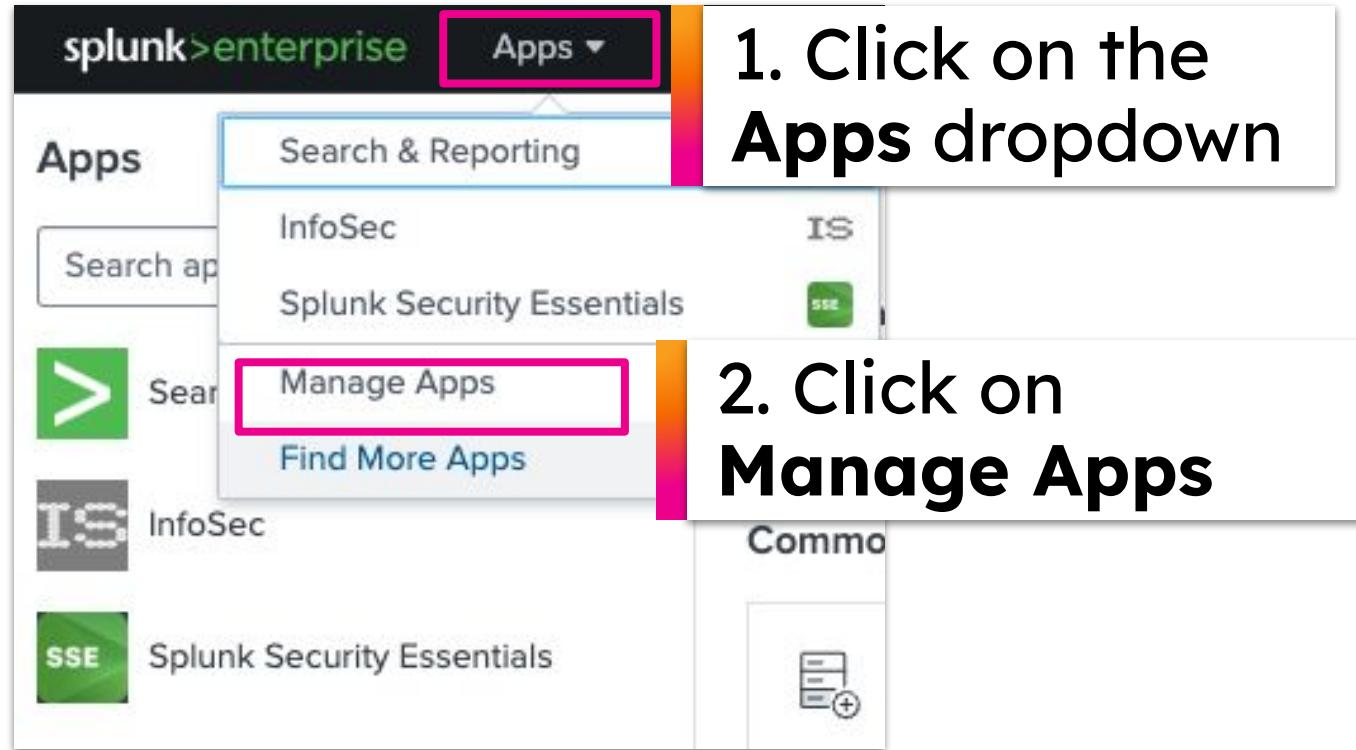
1. Install the Splunk Add-on for AWS
2. Confirm the health of the InfoSec App for Splunk
3. Accelerate data models

**Lab Exercise
#1**



Check Which Add-ons are Installed

Via Splunk Web



The screenshot shows the 'Manage Apps' page with the title 'Apps' and a subtitle 'Showing 1-25 of 46 items'. A search bar with 'filter' and a magnifying glass icon is present. The table has columns for Name, Folder name, Version, Update checking, Visible, Sharing, and Status. The data is as follows:

Name	Folder name	Version	Update checking	Visible	Sharing	Status
InfoSec App Demo	InfoSec_App_Demo	1.0.0	Yes	No	App Permissions	Enabled Disa
InfoSec	InfoSec_App_for_Splunk	1.7.0	Yes	Yes	Global Permissions	Enabled Disa
SplunkDeploymentServerConfig	SplunkDeploymentServerConfig		Yes	No	App Permissions	Enabled Disa
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Ena
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Ena
Splunk Common Information Model	Splunk_SA_CIM	5.3.2 Update to 6.0.1	Yes	Yes	Global Permissions	Enabled Disa
Splunk Security Essentials	Splunk_Security_Essentials	3.8.0 Update to 3.8.1	Yes	Yes	App Permissions	Enabled

TA Data Sources Mapped

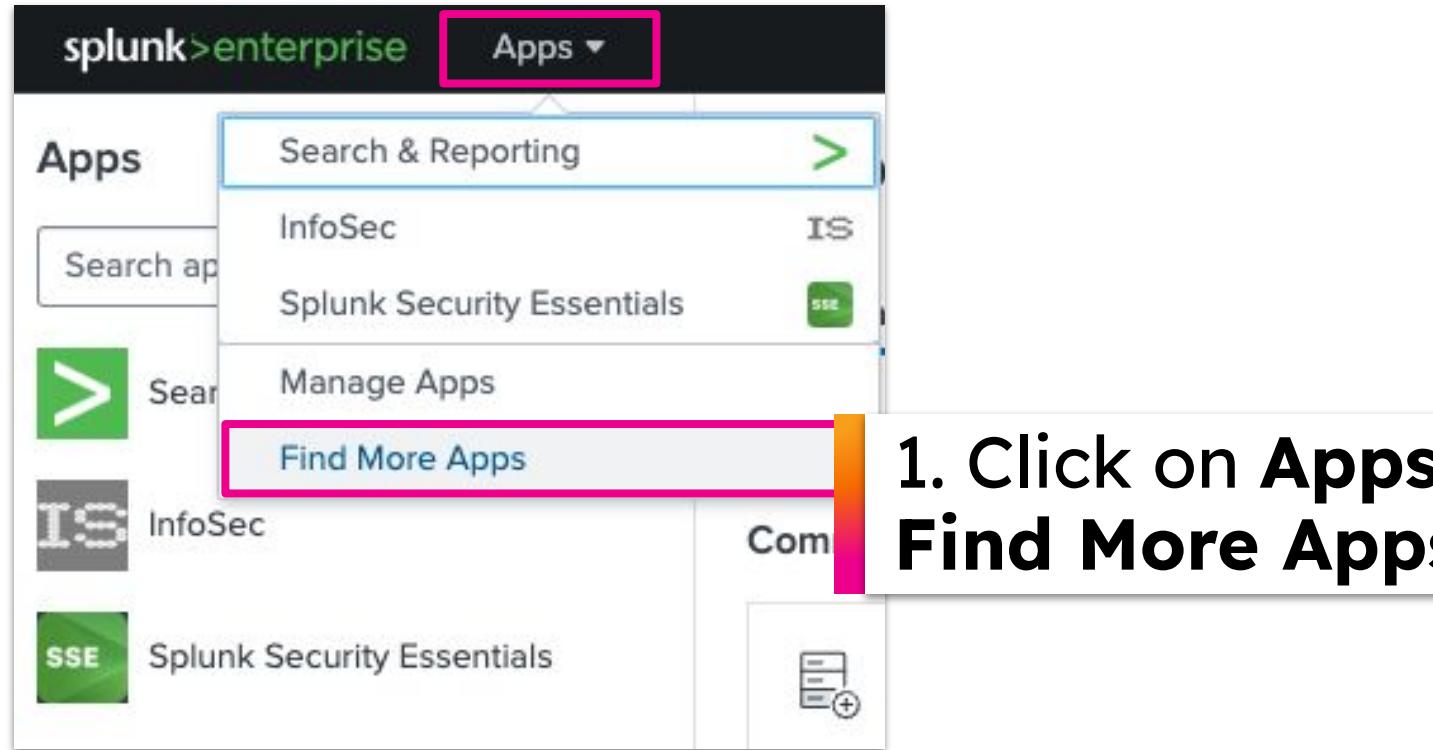
Looking at all the installed add-ons we notice that the Splunk Add-on for AWS is missing.

In order to make sure that all our data is CIM compliant and the data is showing up in our InfoSec App dashboards we need to install the Splunk Add-on for AWS.

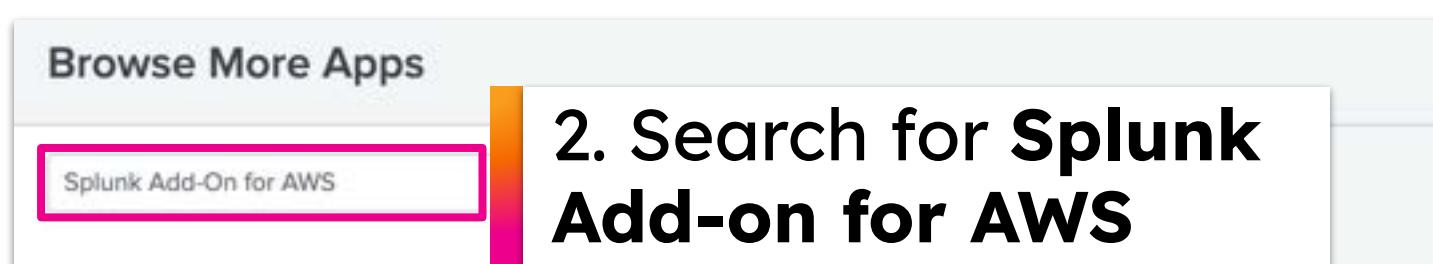
Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
InfoSec App Demo	InfoSec_App_Demo	1.0.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
InfoSec	InfoSec_App_for_Splunk	17.0	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects View details on
SplunkDeploymentServerConfig	SplunkDeploymentServerConfig		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Splunk Common Information Model	Splunk_SA_CIM	5.3.2	Yes	Yes	Global Permissions	Enabled Disable	Set up Edit properties View objects View details on
Splunk Security Essentials	Splunk_Security_Essentials	3.8.0	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects View details on
Splunk Add-on for Check Point OPSEC LEA	Splunk_TA_checkpoint-opseclea	5.0.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on
Splunk Add-on for Oracle	Splunk_TA_oracle	41.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on
Palo Alto Networks Add-on	Splunk_TA_paloalto	8.11 Update to 8.1.3	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on
Splunk Add-on for Symantec Endpoint Protection	Splunk_TA_symantec-ep	3.41	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on
Splunk Add-on for Microsoft Windows	Splunk_TA_windows	8.8.0 Update to 8.9.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on

Install the Splunk Add-on for AWS

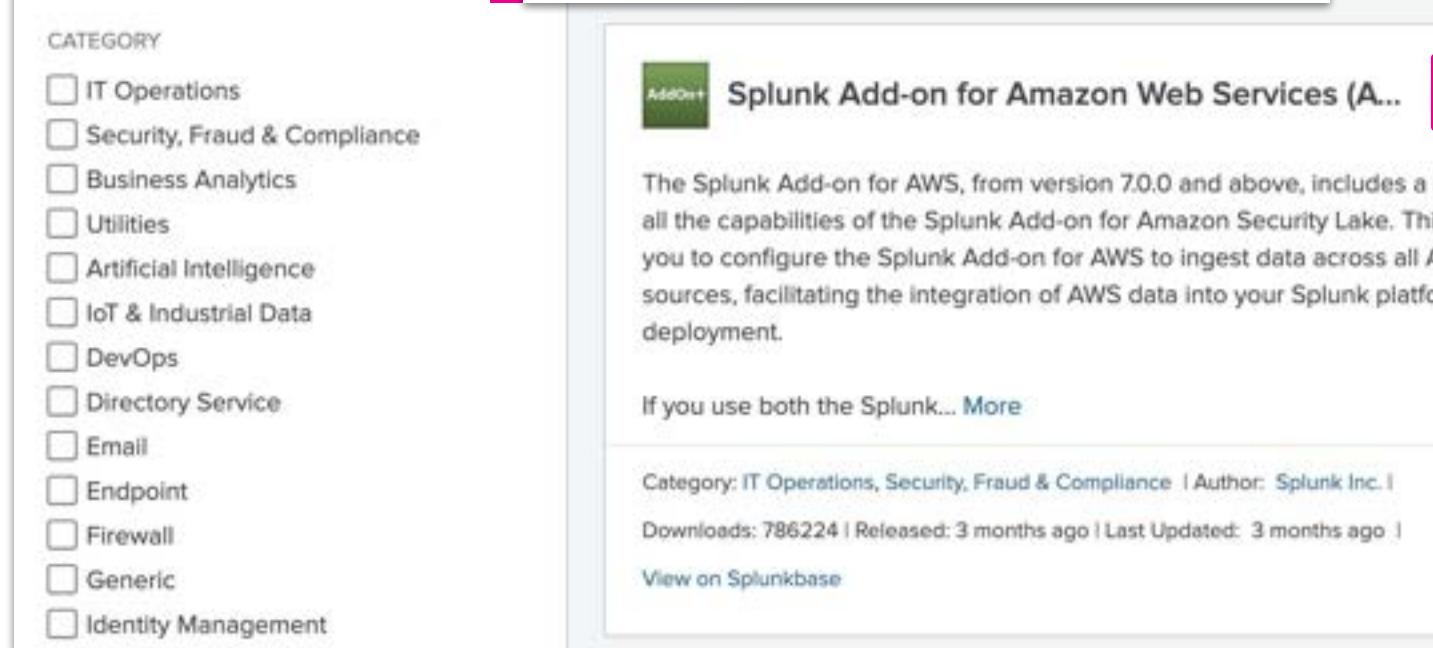
Via Splunk Web



1. Click on Apps >
Find More Apps



2. Search for Splunk
Add-on for AWS



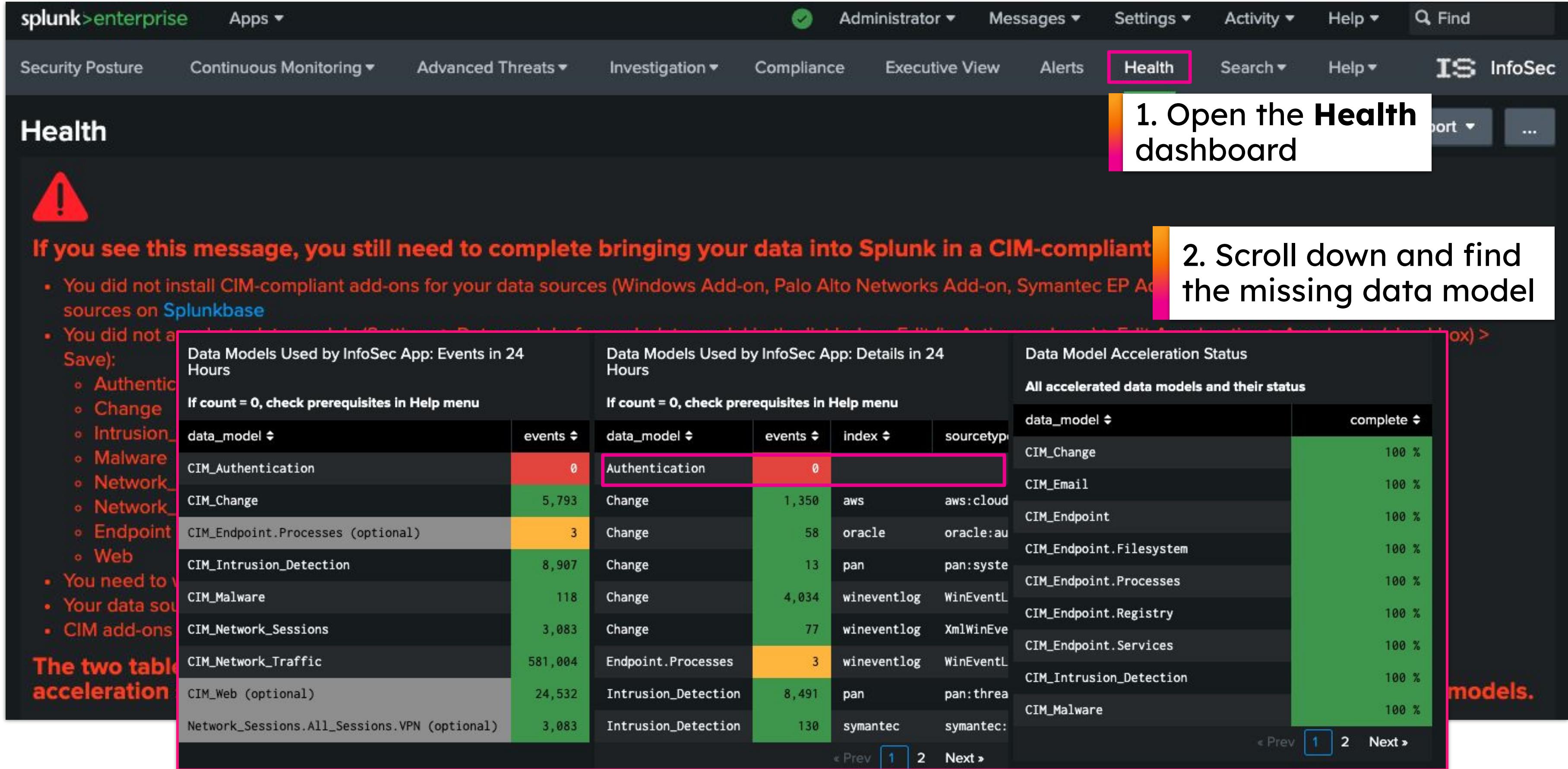
3. Click Install

The screenshot shows a 'Login and Install' dialog box. It contains fields for 'Enter your Splunk.com username and password to download the app.' with the email 'shelly.kornbloom@splunktshirtcompany.com' and a password field. Below the fields are links for 'Forgot your password?' and terms of service. The main text area states that Splunk is not responsible for third-party apps and provides a link to the 'Splunk General Terms'. At the bottom, there are 'Cancel' and 'Agree and Install' buttons, with 'Agree and Install' highlighted with a pink border.

4. Login with your
splunk.com credentials

5. Click
Agree and Install

Check the Health Dashboard in the InfoSec App



1. Open the Health dashboard

If you see this message, you still need to complete bringing your data into Splunk in a CIM-compliant way.

- You did not install CIM-compliant add-ons for your data sources (Windows Add-on, Palo Alto Networks Add-on, Symantec EP Add-on, and others).
- You did not add the data source to the Acceleration Box (optional).
- You did not save the Acceleration Box (optional).
- Authentications
- Changes
- Intrusion_Detection
- Malware
- Network_Events
- Network_Traffic
- Endpoints
- Web
- You need to verify your data source.
- Your data source is not CIM compliant.
- CIM add-ons are not installed.

The two tables below show the status of data model acceleration.

Data Model	Count	Type	Index	Source Type
CIM_Change	5,793	Change	aws	aws:cloud
CIM_Endpoint.Processes (optional)	3	Change	oracle	oracle:au
CIM_Intrusion_Detection	8,907	Change	pan	pan:system
CIM_Malware	118	Change	wineventlog	WinEventLog
CIM_Network_Sessions	3,083	Change	wineventlog	XmlWinEventLog
CIM_Network_Traffic	581,004	Endpoint.Processes	wineventlog	WinEventLog
CIM_Web (optional)	24,532	Intrusion_Detection	pan	pan:threat
Network_Sessions.All_Sessions.VPN (optional)	3,083	Intrusion_Detection	symantec	Symantec

Data Model	Acceleration Status
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 %
CIM_Malware	100 %

2. Scroll down and find the missing data model.

Accelerate the Authentication Data Model

Edit the data model acceleration settings

The screenshot shows the Splunk navigation bar with 'Administrator', 'Messages', 'Settings' (highlighted with a red box), 'Activity', and 'Help'. Below the navigation is a sidebar with 'Add Data' and 'Monitoring' sections. The main area has 'KNOWLEDGE' and 'DATA' tabs. Under 'KNOWLEDGE', 'Searches, reports, and alerts' is selected, while 'Data models' (highlighted with a red box) is shown as a sub-section. Other options like 'Event types', 'Tags', 'Fields', 'Lookups', 'User interface', and 'Alert actions' are also listed.

1. Browse to the Data models settings

The dialog title is 'Edit Acceleration'. It shows two tabs: 'Data Model' (selected) and 'Authentication'. Under 'Data Model', the 'Accelerate' checkbox is checked (highlighted with a red box). A note says 'Acceleration may increase storage and processing costs.' Below it is a 'Summary Range?' dropdown set to '1 Year'. At the bottom are 'Cancel' and 'Save' buttons (the 'Save' button is highlighted with a green box).

The screenshot shows the 'Data Models' list. It lists 27 data models, including 'Alerts', 'Application State (Deprecated)', and 'Authentication'. The 'Authentication' row is expanded, showing its details: MODEL (Datasets: 10 Events, Edit), Permissions (Shared Globally, Owned by nobody, Edit), and ACCELERATION (Model is not accelerated, Add). The 'Add' button in the ACCELERATION section is highlighted with a red box.

2. Expand the Authentication section and click Add

3. Check Accelerate and click Save

Check Health Dashboard in InfoSec App

After 5-10 min the Authentication Data Model should be accelerated

The screenshot shows the Splunk Enterprise interface with the InfoSec app open. The top navigation bar includes links for Security Posture, Continuous Monitoring, Advanced Threats, Investigation, Compliance, Executive View, Alerts, **Health**, Search, Help, and the InfoSec logo. The Health tab is selected.

Data Models Used by InfoSec App: Events in 24 Hours

data_model	events
CIM_Authentication	1,130,539
CIM_Change	4,384
CIM_Endpoint.Processes (optional)	583
CIM_Intrusion_Detection	1,162
CIM_Malware	101
CIM_Network_Sessions	2,239
CIM_Network_Traffic	456,349
CIM_Web (optional)	2,552
Network_Sessions.All_Sessions.VPN (optional)	2,239

If count = 0, check prerequisites in Help menu

Data Models Used by InfoSec App: Details in 24 Hours

data_model	events	index	sourcetype
Authentication	4	_audit	audittrail
Authentication	2,000	botsv3	ms:aad:signin
Authentication	1,097,000	botsv3	o365:management:a
Authentication	29,002	botsv4	WinEventLog
Authentication	18	botsv4	XmlWinEventLog
Authentication	2,190	botsv4	aws:cloudtrail
Authentication	83	botsv4	oracle:audit:unif
Authentication	226	botsv4	oracle:audit:xml
Authentication	16	botsv4	pan:system

If count = 0, check prerequisites in Help menu

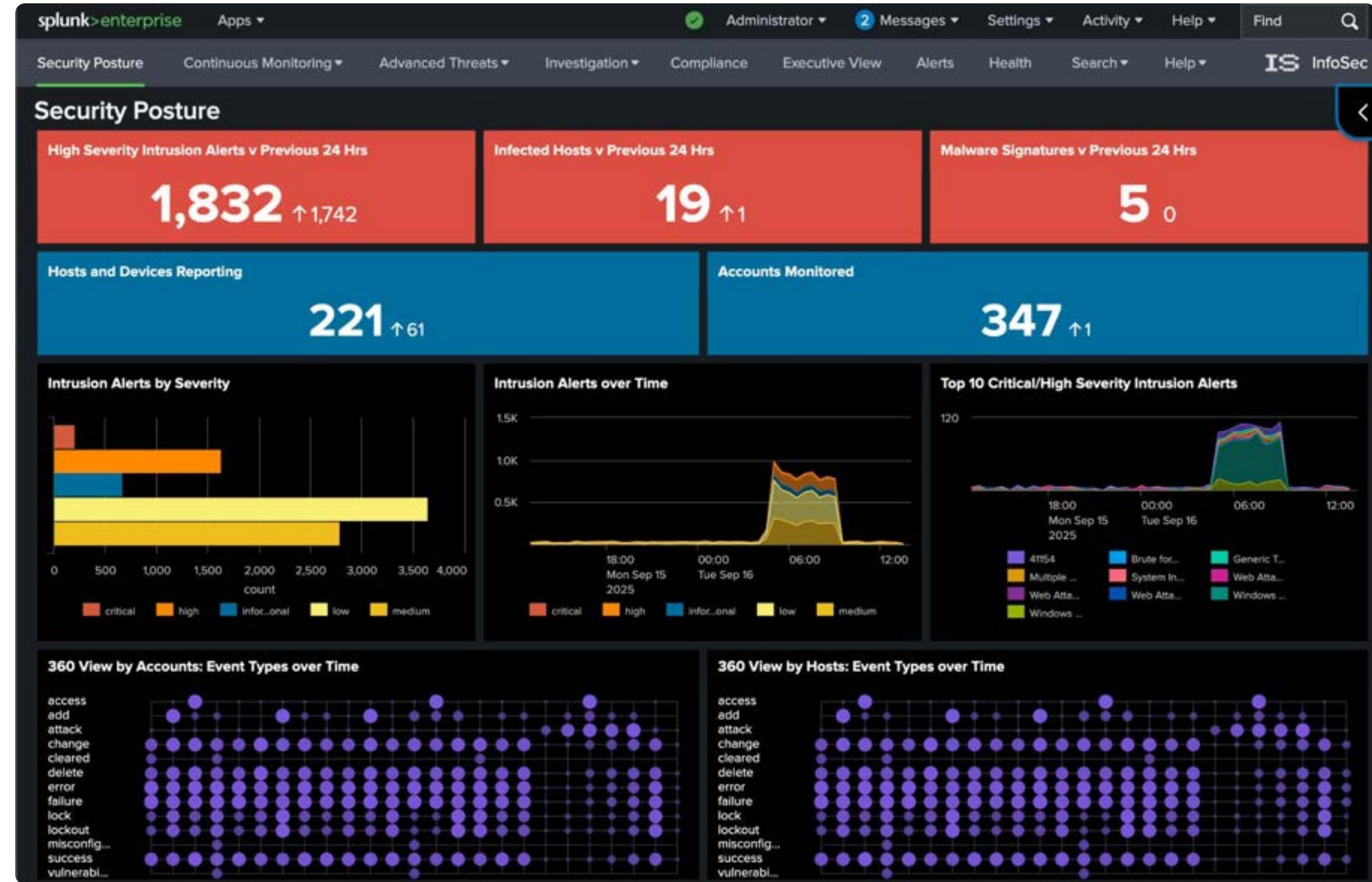
Data Model Acceleration Status

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

All accelerated data models and their status

Wait for the acceleration status to reach 100%

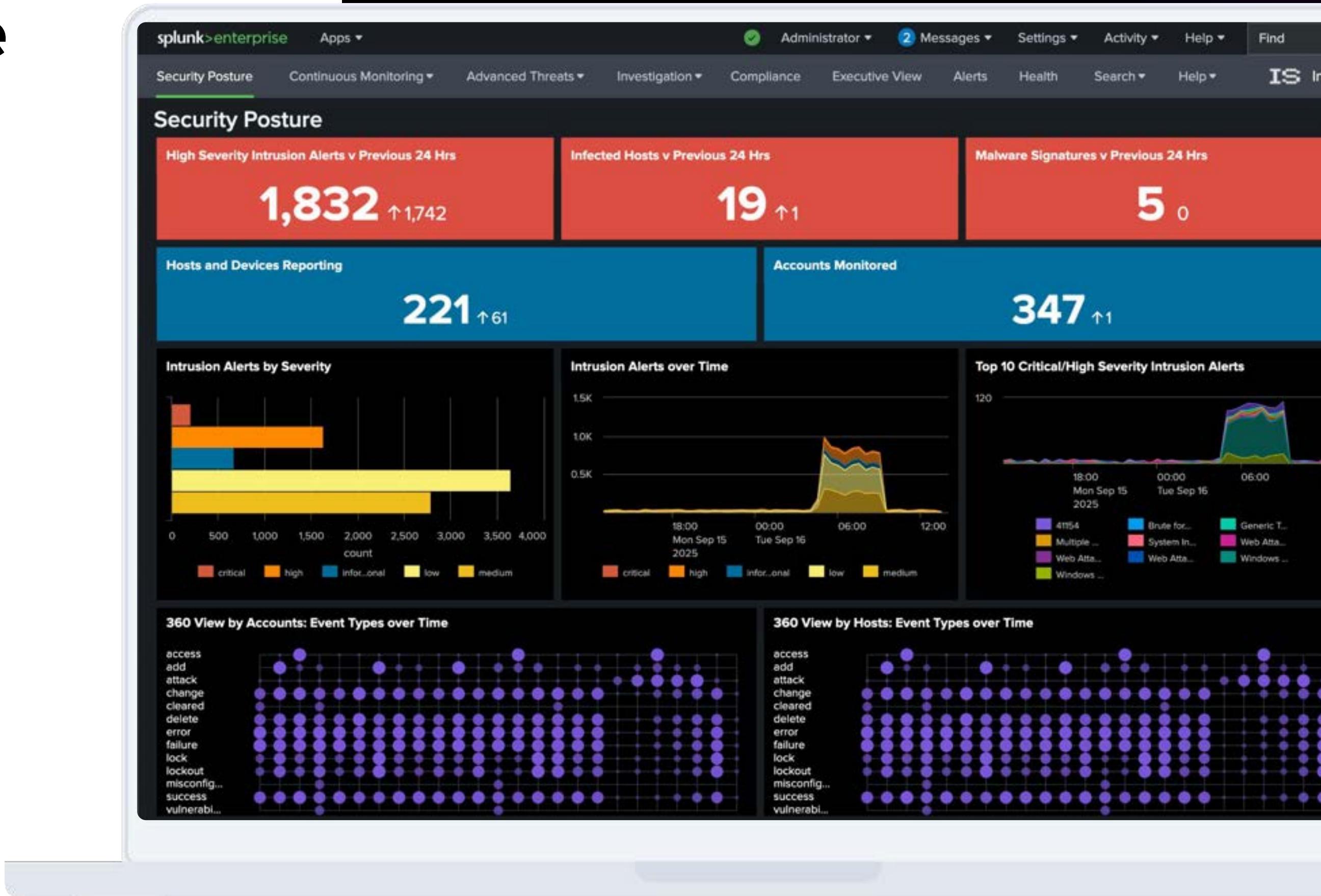
InfoSec App UI



Security Posture

InfoSec Landing Page

- Get a high-level view of your security posture
- Compare your current state to yesterday's
- Identify bursts of activity needing investigation



InfoSec App Investigation

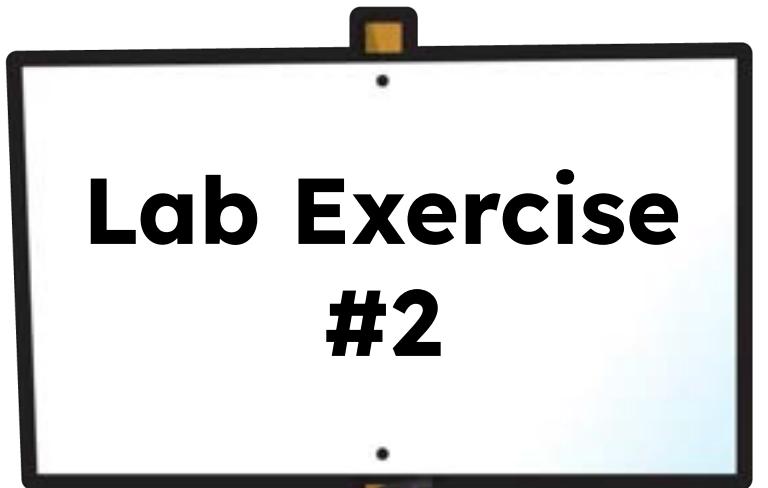
Leveraging drilldowns for data insights



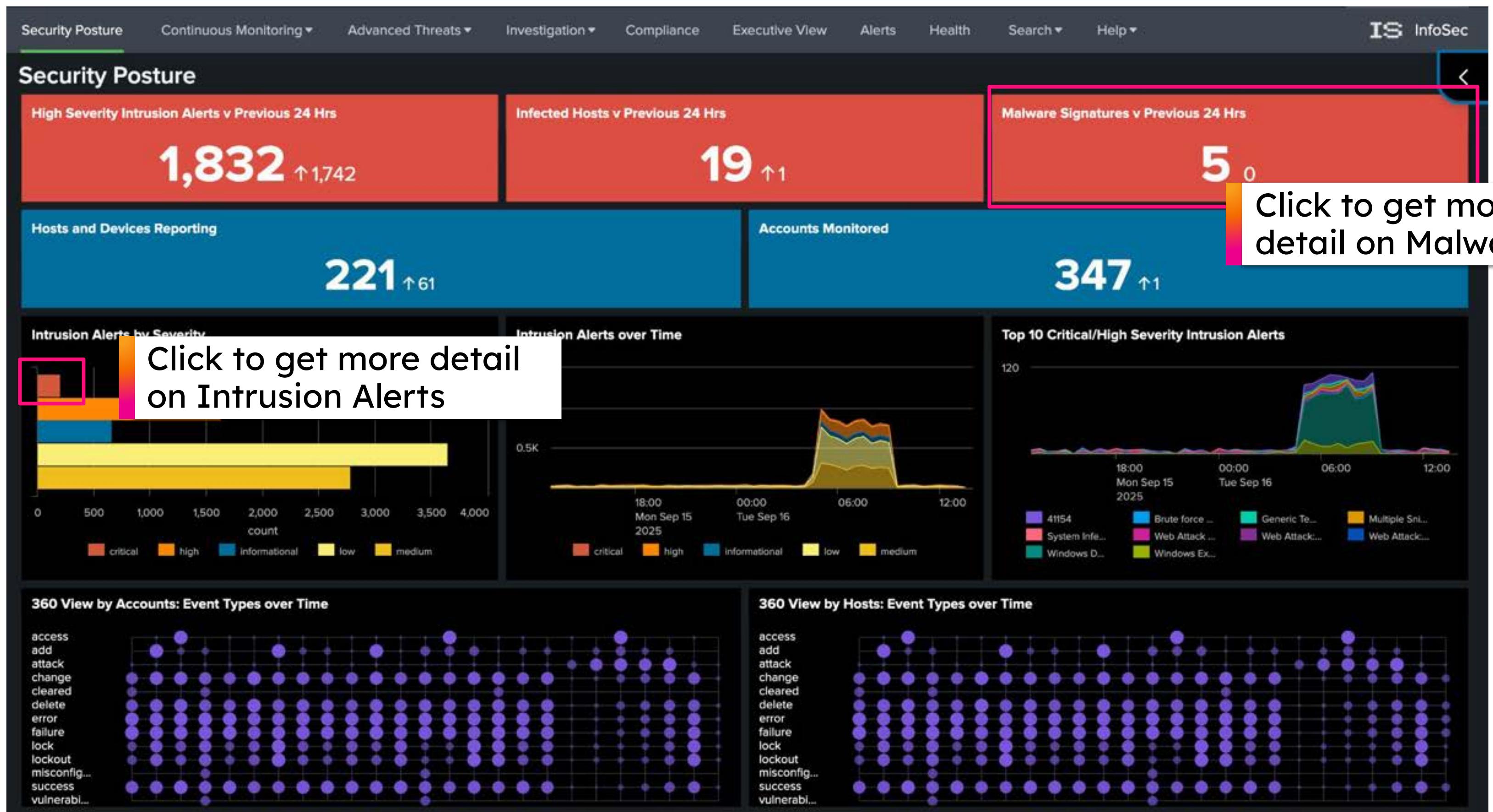
Tasks

Start your investigation on the Security Posture dashboard, identify following:

1. How many critical **Intrusion Alerts** are displayed?
 - a. Drill down and filter on critical alerts
 - b. What are the top 3 signatures?
2. How many **Malware** were detected in the last 24 hours?
 - a. Which are the top 3?



Check Security Posture Dashboard



Security Posture Continuous Monitoring ▾ Advanced Threats ▾ Investigation ▾ Compliance Executive View

Intrusion Detection (IDS/IPS) [Show Filters](#)

Allowed Intrusion Attempts

983

Critical Severity Alerts High Severity Alerts Medium Severity Alerts

62

Click to filter down on critical Alerts

Intrusion Signatures

signature	severity	count
'Application and Device Control is ready'	critical	3
'C:\Program Files (x86)\splunktshirtcompany.com\Product\2.3.4.5\Bin64\yyyy.exe'	critical	3
AC9-1.1 Block access to autorun.inf	critical	4
AC9-1.1 Block access to autorun.inf - Caller MD5=xxxxxx66c5d511fdcaa2d7445d21aeb1	critical	10
AC9-1.1 Block access to autorun.inf - Caller MD5=xxxxxx8920ba0ddebaf5ea68ff97a93c	critical	3
AC9-1.1 Block access to autorun.inf - Caller MD5=xxxxxb1435662fc6c872e25beb37be3	critical	3
Adobe Flash Player Remote Code Execution Vulnerability	critical	2

severity ▾ count ▾

< Prev 1 2 3 4 5 6 7 8 9 10 Next >

Security Posture Continuous Monitoring ▾ Advanced Threats ▾ Investigation ▾ Compliance Executive View Alerts Health Search ▾ Help ▾ IS InfoSec

Malware [Show Filters](#)

Unresolved Infections Deferred Infections Blocked Infections

90 11 0

Malware Activity

Malware by Signature

Top Malware

Signature	Count
Trojan.Gen.2	10
SON_c121	6
Trojan.Gen	5
Backdoor.Jogger	4
WS_Reputation	1

Find top 3 Malware here

Intrusion Detection (IDS/IPS)

InfoSec App Dashboard

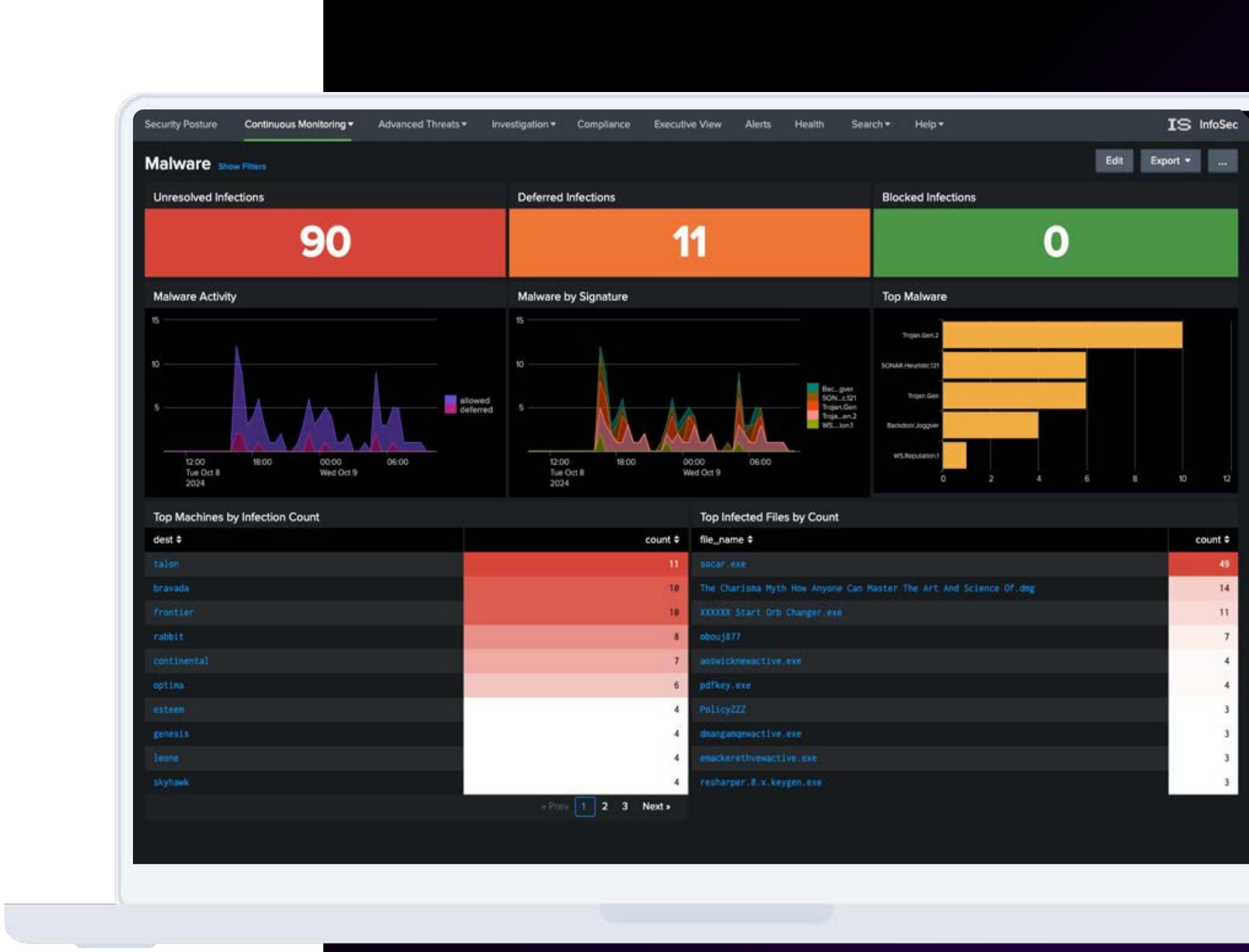
- Breakdown of total events by action/severity over the last 24 hours
- Drill-down to underlying Splunk search results for detailed analysis
- Monitoring and analyzing intrusion detection and prevention system events
- Identifying trends and anomalies in IDS/IPS data



Malware

InfoSec App Dashboard

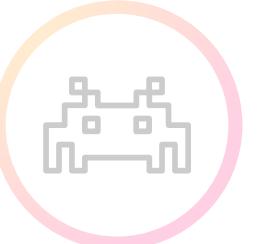
- Provides an overview of Anti-Virus events and malware detections
- Identifies trends and spikes in malware activity for investigation
- Breaks down events by malware type (virus, Trojan, spyware)
- Shows top malware by host and file name



Our progress so far



IT team: Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly



Malware: Find Malware-infected files and setup an alert for future detections



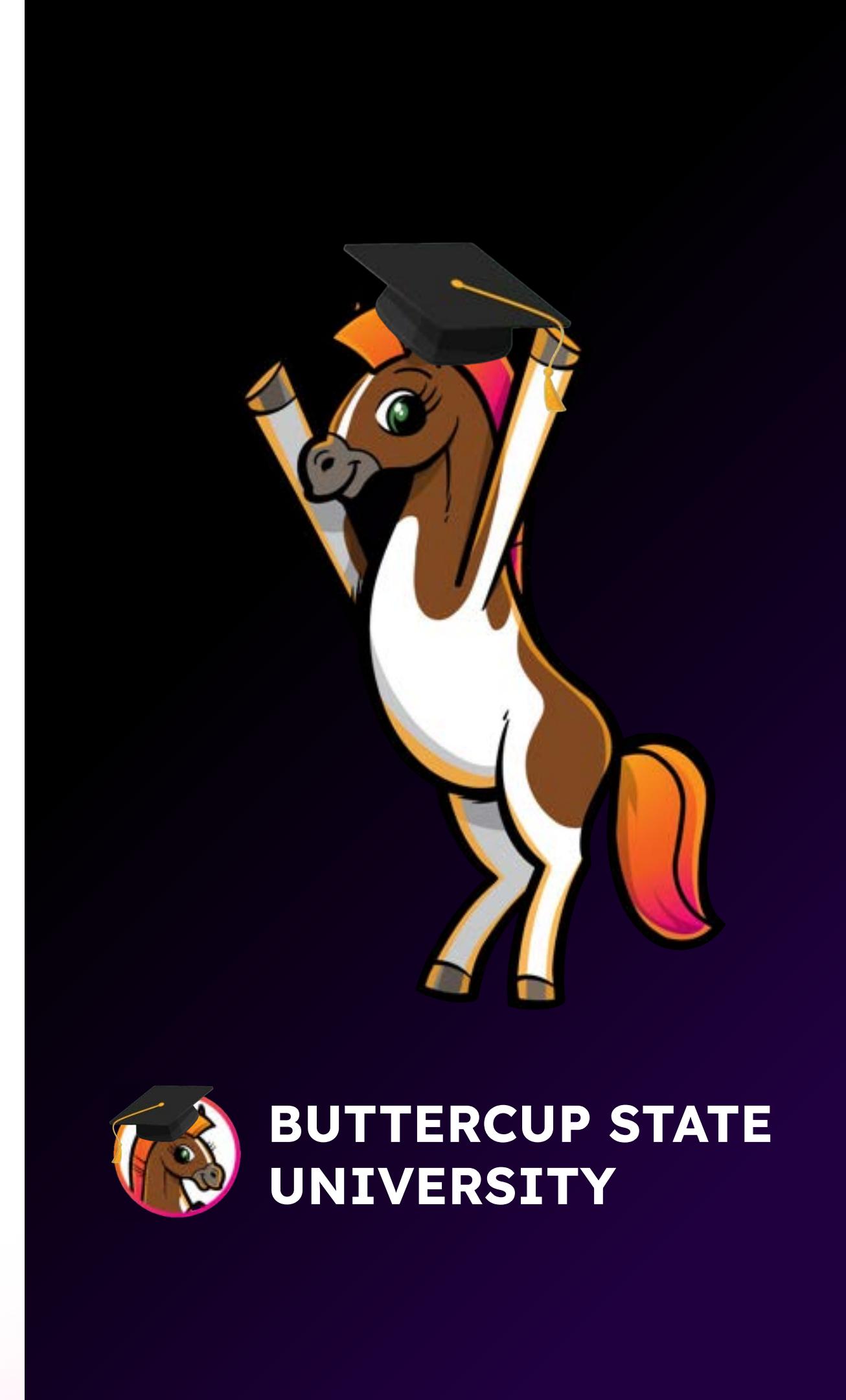
User behavior: Look for sudden access changes, unauthorized role modifications, or unusual activity



Customize the InfoSec App: Look for ways to customize the content for Buttercup State University



Add additional security content: Review the content in Splunk Security Essentials and add any new use cases you think might be valuable



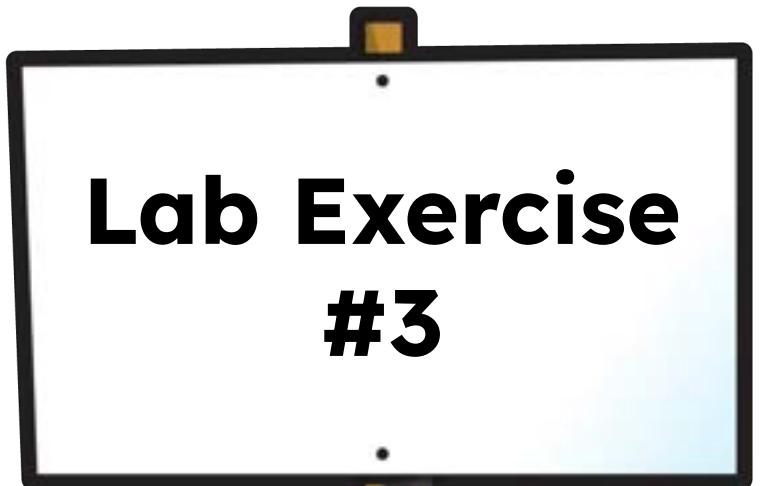
Malware Investigation

Find Malware-infected files and setup an alert for future detections



Tasks

1. Find the **top malware-infected file** using the **Malware** dashboard
2. Drill down on the search and use interesting fields to:
 - a. Identify **which hosts are compromised**
 - b. Find the **file path** of the infected file
3. **Create an alert** to trigger if this infected file is seen again



Check Continuous Monitoring - Malware Dashboard

Security Posture Continuous Monitoring ▾ Advanced Threats ▾ Investigation ▾ Compliance Executive View Alerts Health Search ▾ Help ▾

IS InfoSec

Malware Show Filters

Unresolved Infections: 110 Deferred Infections: 12 Blocked Infections: 0

Malware Activity: A line chart showing malware activity over time from 12:00 AM to 8:00 PM on Thursday, July 18, 2024. The chart shows two series: 'allowed' (purple) and 'deferred' (pink). Both series show peaks around 4:00 AM, 8:00 AM, 4:00 PM, and 8:00 PM.

Malware by Signature: A line chart showing malware activity by signature over the same time period. The legend includes: Backdoor.Joggver (teal), SONAR...istic.121 (orange), Trojan.Gen (dark red), Trojan.Gen.2 (light red), and WS.Reputation.1 (green).

Top Malware: A horizontal bar chart ranking the top malware by count. The top five are: Trojan.Gen.2 (10), SONAR.Heuristic.121 (6), Trojan.Gen (6), Backdoor.Joggver (4), and WS.Reputation.1 (1).

Top Machines by Infection Count:

Machine	Count
dest	12
bravada	12
frontier	12
talon	9
optima	8
continental	8
rabbit	8
metro	5
boxster	4
elan	4
esteem	4

Top Infected Files by Count:

File Name	Count
socar.exe	61
The Charisma Myt...	17
XXXXXX Start Orb...	12
obouj877	8
PolicyZZZ	4
aoswicknewactive.exe	4
dmangamqewactive.exe	4
emackerethvewactive.exe	4
pdfkey.exe	4
resharper.8.x.keygen.exe	4

Click on the file name to drill down

« Prev 1 2 3 Next »

q ↴ i ↵ <1m ago

Investigate beyond the original panel

Security Posture Continuous Monitoring ▾ Advanced Threats ▾ Investigation ▾ Compliance Executive View Alerts Health Search ▾ Help ▾ **IS InfoSec**

New Search Save As ▾ Create Table View Close Last 24 hours ▾

'infosec-indexes' tag=malware tag=attack file_name="socar.exe"

✓ 61 events (7/18/24 12:00:00.000 AM to 7/19/24 12:27:20.000 AM) No Event Sampling ▾

Events (61) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

Hide Fields All Fields

SELECTED FIELDS

- # host 1
- # source 1
- # sourcetype 1

INTERESTING FIELDS

- # action 1
- # Actual action 2
- # Application hash 15
- # Application name 3
- # Application type 2
- # Application version 4
- # Application_Hash 15
- # Application_Name 3
- # Application_Type 2
- # Application_Version 4
- # category 4
- # COH Engine Version 1
- # COH_Engine_Version 1
- # Company name 10
- # Company_Name 10
- # Computer name 13
- # Computer_Name 13
- # Confidence 4
- # date 2
- # Description 2
- # dest 13
- # dest_nt_domain 4
- # Detection score 4
- # Detection Source 1
- # Detection type 4
- # Detection_Score 4
- # Detection_Type 4
- # Disposition 2
- # Domain 4
- # Domain_Name 4
- # Download site 10
- # Download_Site 10

src_ip

8 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
10.0.0.1	13	20.968%
10.0.1.7	12	19.355%
10.0.0.2	8	12.903%
10.0.1.8	8	12.903%
10.0.2.9	8	12.903%
10.0.8.1	5	8.064%
10.0.2.3	4	6.452%
10.0.5.2	4	6.452%

file_path

3 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

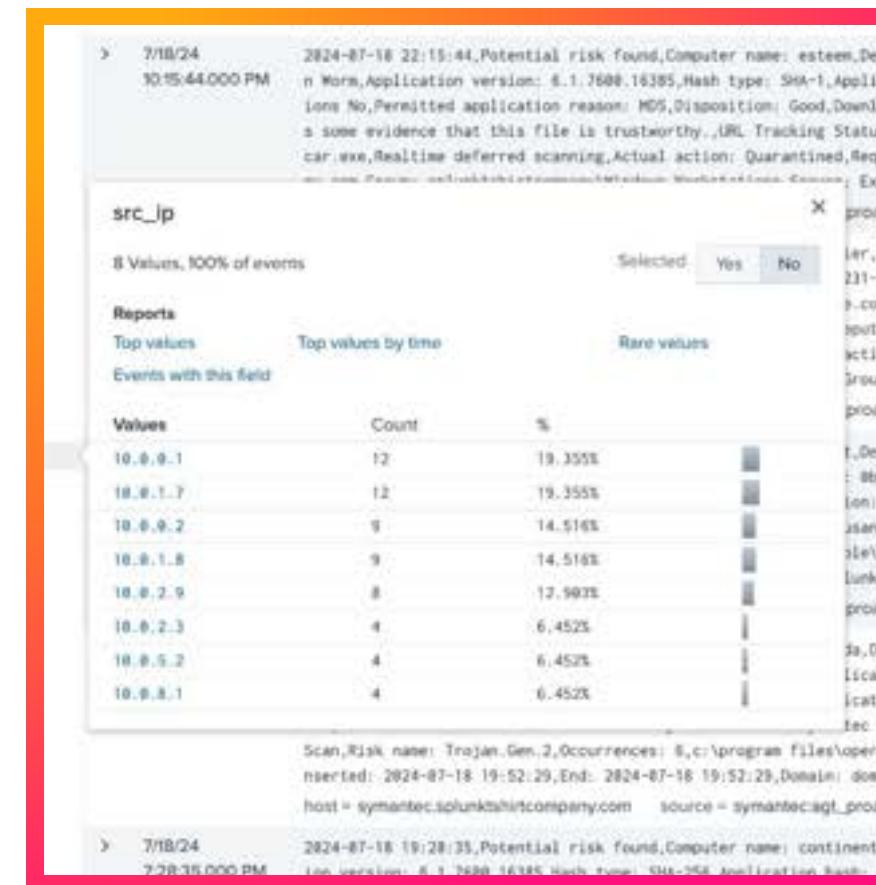
Values	Count	%
c:\users\example\Desktop\socar.exe	25	40.322%
c:\program files\opera\48.0.2685.52\socar.exe	21	33.871%
c:\users\example\appdata\splunktshirtcompany.com\temp\example\socar.exe	16	25.806%

Use interesting fields for further investigation

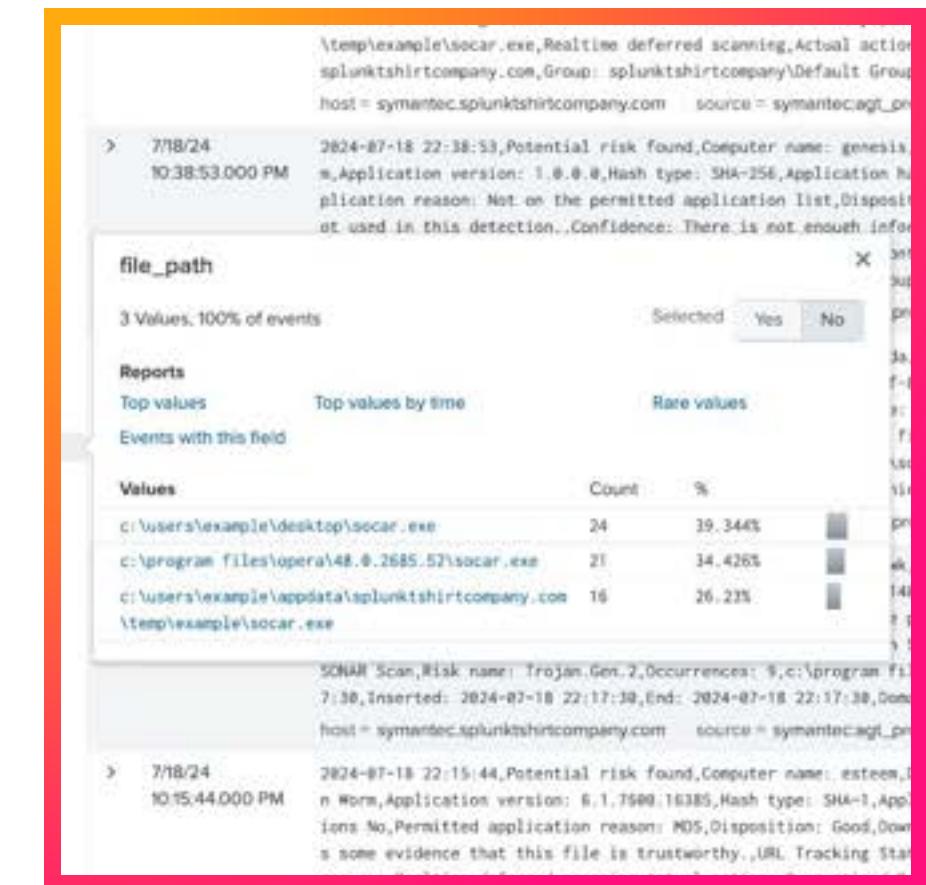
© 2025 SPLUNK LLC

Leveraging Interesting Fields

Interesting fields can help your investigating



src_ip



file_path

Alert when this infected files is seen again



1. Click on the search button of the detection

```
| 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
```

124 events (02/12/2024 19:00:00.000000)

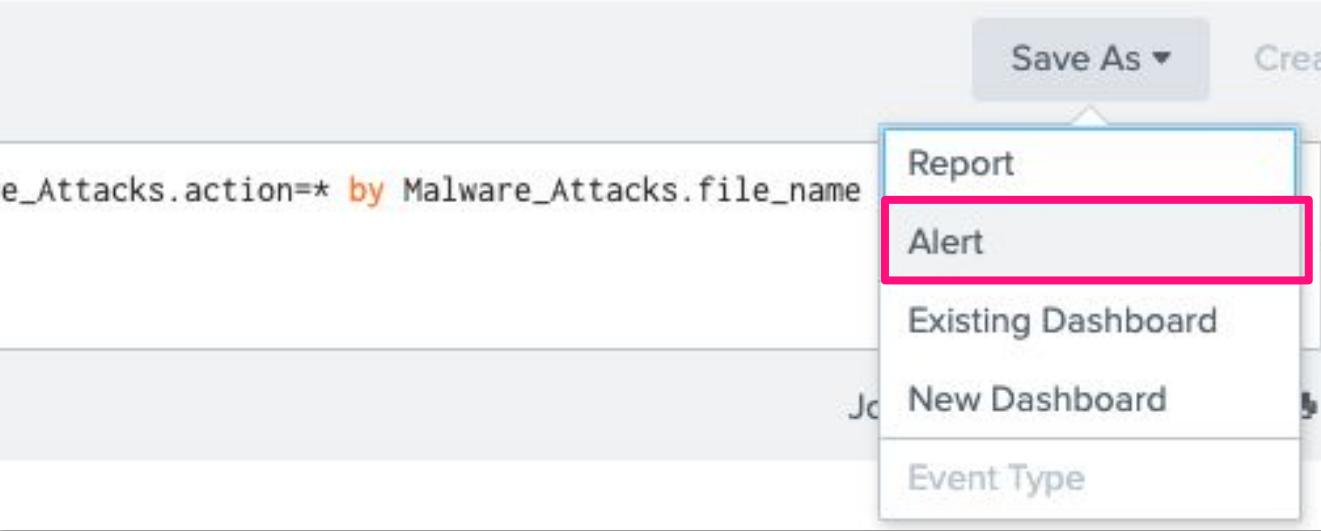
Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

file_name ▾

socar.exe

Alert when this infected files is seen again



3. Click on **Save As > Alert**

Trigger Actions

+ Add Actions ▾

When triggered

Add to Triggered Alerts

Severity: Medium

5. Add Alert Action: “Add to Triggered Alerts” with Severity: Medium

4. Create an alert that runs every hour, to be triggered when **socar.exe** is detected

Save As Alert

Settings

Title: Infected "socar.exe" detected

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 0 minutes past the hour

Expires 24 hour(s)

Trigger Conditions

Trigger alert when Number of Results

is greater than 0

Trigger Once | For each result

Throttle?

Alert Trigger Conditions

Alert conditions in Splunk are **criteria that determine when an alert should be triggered** based on search results

- Types of Alerts
 - Scheduled Alerts: run on a set schedule and can have custom trigger conditions
 - Real-time alerts: Trigger immediately when matching events occur
- Why is this important?
 - Monitors Specific Event Patterns
 - Prioritizes Critical Events
 - Enhances Notification Quality
 - Reduces Alert Fatigue
 - Customizes Alert Criteria



Alert Trigger Actions

Alert actions help you **respond to triggered alerts**.

- You can enable one or more alert actions
- Email Notification Action
 - Webhook Alert Action
 - Output to CSV lookup
 - Log Events
 - Monitor Triggered Alerts
 - Splunk Mobile Alerts
 - Custom Alert actions
- Why is this important?
 - Automated Response
 - Improved Operational Efficiency
 - Enhanced Timely Notifications
 - Supporta Integrations with other providers



Alert Dashboard

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Q Find

Security Posture Continuous Monitoring ▾ Advanced Threats ▾ Investigation ▾ Compliance Executive View Alerts Health Search ▾ Help ▾ IS InfoSec

Alerts

Last 24 hours Hide Filters

List of Triggered Alerts

_time	alert	severity	alert_actions
2024-12-11 14:15:00.299	High Severity Intrusion	High	
2024-12-11 14:15:00.282	Critical Severity Intrusion	Critical	
2024-12-11 14:30:00.544	Suspected Network Scanning	Low	
2024-12-11 15:30:00.928	High Severity Intrusion	High	
2024-12-11 15:30:00.899	Suspected Network Scanning	Low	
2024-12-11 15:30:00.744	Critical Severity Intrusion	Critical	
2024-12-11 15:15:00.636	High Severity Intrusion	High	
2024-12-11 15:00:01.600	Locked Out Accounts	Low	
2024-12-11 15:00:00.780	Suspected Network Scanning	Low	
2024-12-11 15:00:00.741	High Severity Intrusion	High	

x Prev 1 2 Next »

Triggered Alerts over Time

4:00 PM 8:00 PM 12:00 AM 4:00 AM 8:00 AM 12:00 PM
Tue Dec 10 Wed Dec 11 2024

Brute Force Attack
Suspected Network Scanning
Critical Severity Intrusion
High Severity Intrusion
Locked Out Accounts

Configure Alerts

Edit Existing Alerts

Add Alerts

To set up a new alert either:

- hover over a report you want to be alerted on and click on the magnifying glass icon to open a search; save the search: Save As > Alert or
- follow instructions in [this video](#)

What we have identified

Findings:

- The top infected file is **socar.exe**
- Looking at **src_ip** we found compromised hosts
- Looking at **server** we could identify the infected hosts
- Looking at **file_path** we now know where the malware is located
- We created an alert to be notified if socar.exe is infected again

Next Steps you can take:

- Investigate other activity from those IPs to uncover additional malware or lateral movement
- Isolate infected servers to prevent lateral movement
- Investigate how the malware propagated to these servers to close vulnerabilities
- Remove the malware executable from infected systems



Our progress so far



IT team: Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly



Malware: Find Malware-infected files and setup an alert for future detections



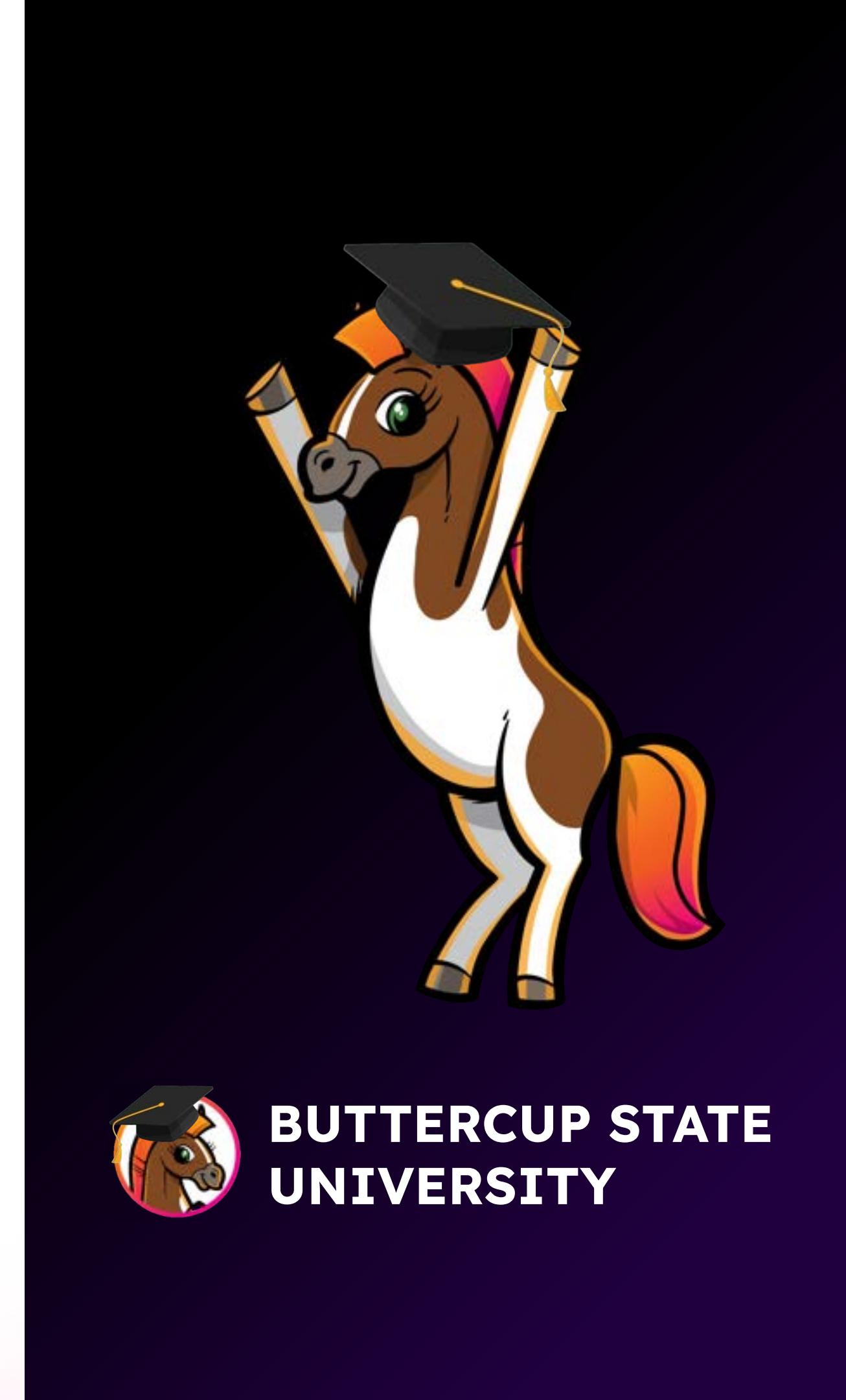
User behavior: Look for sudden access changes, unauthorized role modifications, or unusual activity



Customize the InfoSec App: Look for ways to customize the content for Buttercup State University



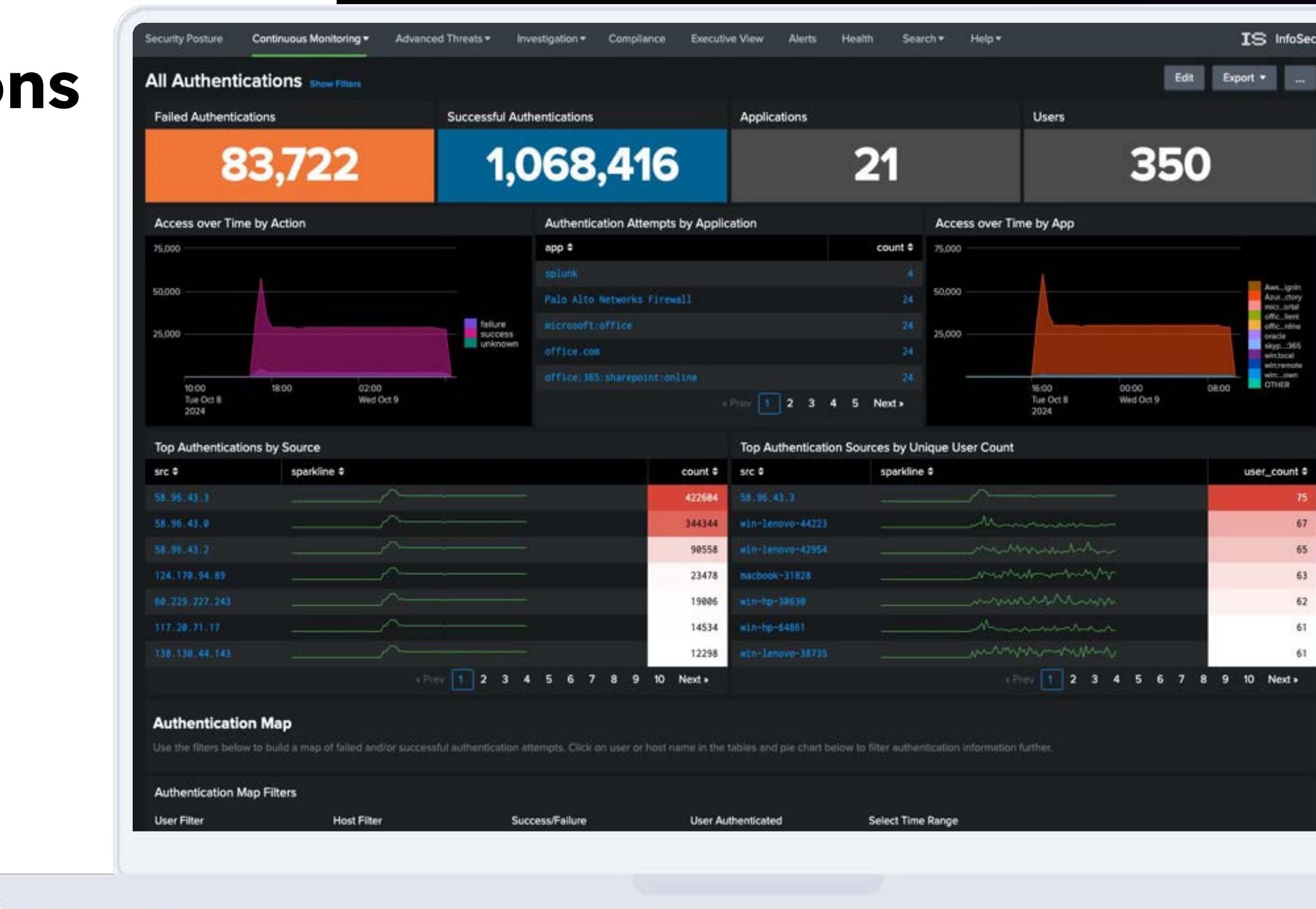
Add additional security content: Review the content in Splunk Security Essentials and add any new use cases you think might be valuable



All Authentications

InfoSec App Dashboard

- Consolidated view of authentication actions
- Breaks down attempts by application
- Counts successful and failed events
- Identifies unusual authentication patterns
- Monitor user access and authentication activity
- Detect potential threats related to unauthorized access



Access Anomalies

InfoSec App Dashboard

- Identifies spikes in access to hosts
- Detects brute force attacks by source or user
- Monitors accounts with high logon failure rates
- Flags users performing new privileged actions
- Highlights geographically improbable access
- Detecting potential security risks
- Investigating unusual access patterns

The screenshot shows the InfoSec App Dashboard with the following sections:

- Access Anomalies**:
 - Spike in # of Hosts Accessed**: Value 1 (Over 24 hours compared to 30-day baseline)
 - Brute Force Attack by Source**: Value 123
 - Brute Force Attack by User**: Value 123
 - Users Failing Auth Over 80%**: Value 30
- Successful Auth Sources With the Greatest # of Users**:

src #	num_users #	users #
58.96.43.3	75	Amanda.Gray@splunktshirtcompany.com, Andy.Yang@splunktshirtcompany.com
58.96.43.0	53	Aaron.Matthews@splunktshirtcompany.com, Alexandra.Copland@splunktshirt
58.96.43.2	34	Andrew.Jones@splunktshirtcompany.com, Blake.Vesey@splunktshirtcompany.c
win-lenovo-82744	33	abroughtonm, aemerit, aswafford2b, btreeby2d, carkleb, ccabottolk, dsh
macbook-96816	32	adams, adrainz, amadin18, aswafford2b, cchilde1g, ccogant4, cstanelan
- Failed Auth Sources With the Greatest # of Users**:

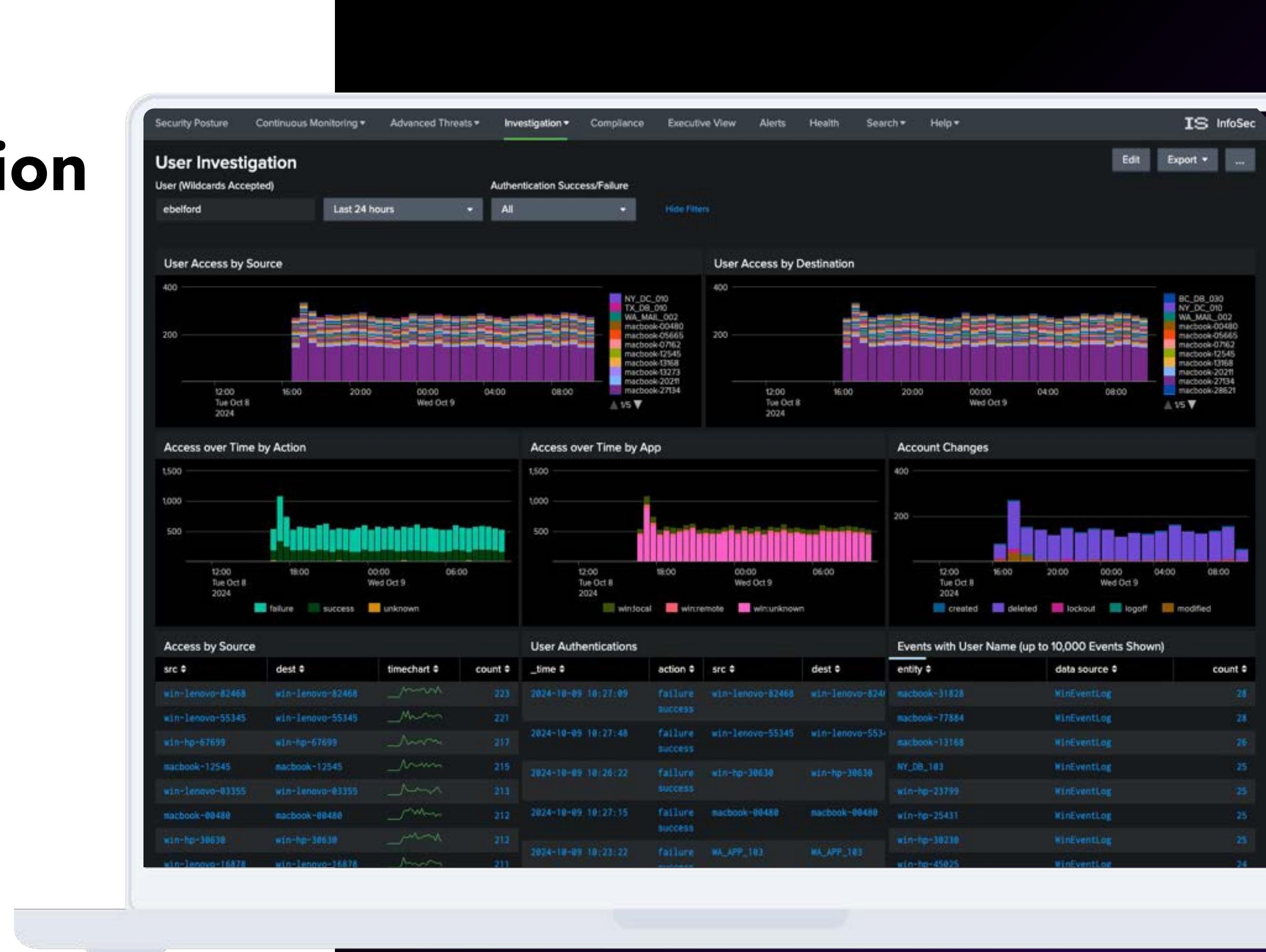
src #	num_users #	users #
win-lenovo-44223	57	adams, adrainz, aemerit, amadin18, aswafford2b, btreeby2d, carkleb, ccabottolk, dsh
macbook-84160	49	abroughtonm, aemerit, akwon, bmaccourtb, bpargetera, bsiamaker2b, carkle
macbook-31555	47	adams, abecken15, abroughtonm, aemerit, aswafford2b, bghiroldi2n, bpa
macbook-31828	47	adams, abroughtonm, adrainz, aemerit, bghiroldi2n, bmaccourtb, bparget
win-hp-30030	47	abecken15, adrainz, aemerit, aswafford2b, bghiroldi2n, bpargetera, cchil
- Users Taking Privileged Actions First Time in 30 Days**: Value 128
- Users Taking Privileged Actions**: Value 29
- Short Lived Windows Accounts**:

user #	dest #	user #	sparkline #	count #
SegurotBH	Server_B.com	ebelford	sparkline	99
ebelford	server_A.com	ebelford	sparkline	99

User Investigation

InfoSec App Dashboard

- Provides an interface to investigate user behaviors
- Allows drill-down into specific user actions
- Offers filters for detailed searches
- Displays underlying search results for analysis
- Analyzing user activity and identifying anomalies
- Supporting incident response and threat investigations



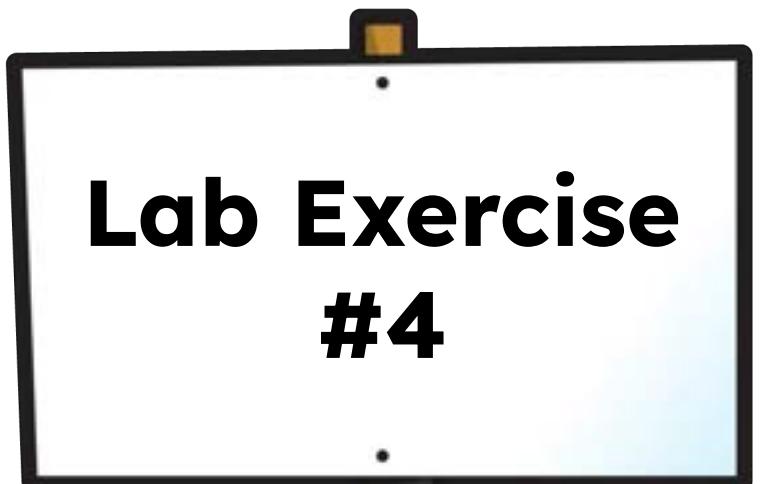
User Behavior Investigation

Look for sudden access changes, unauthorized role modifications, or unusual activity

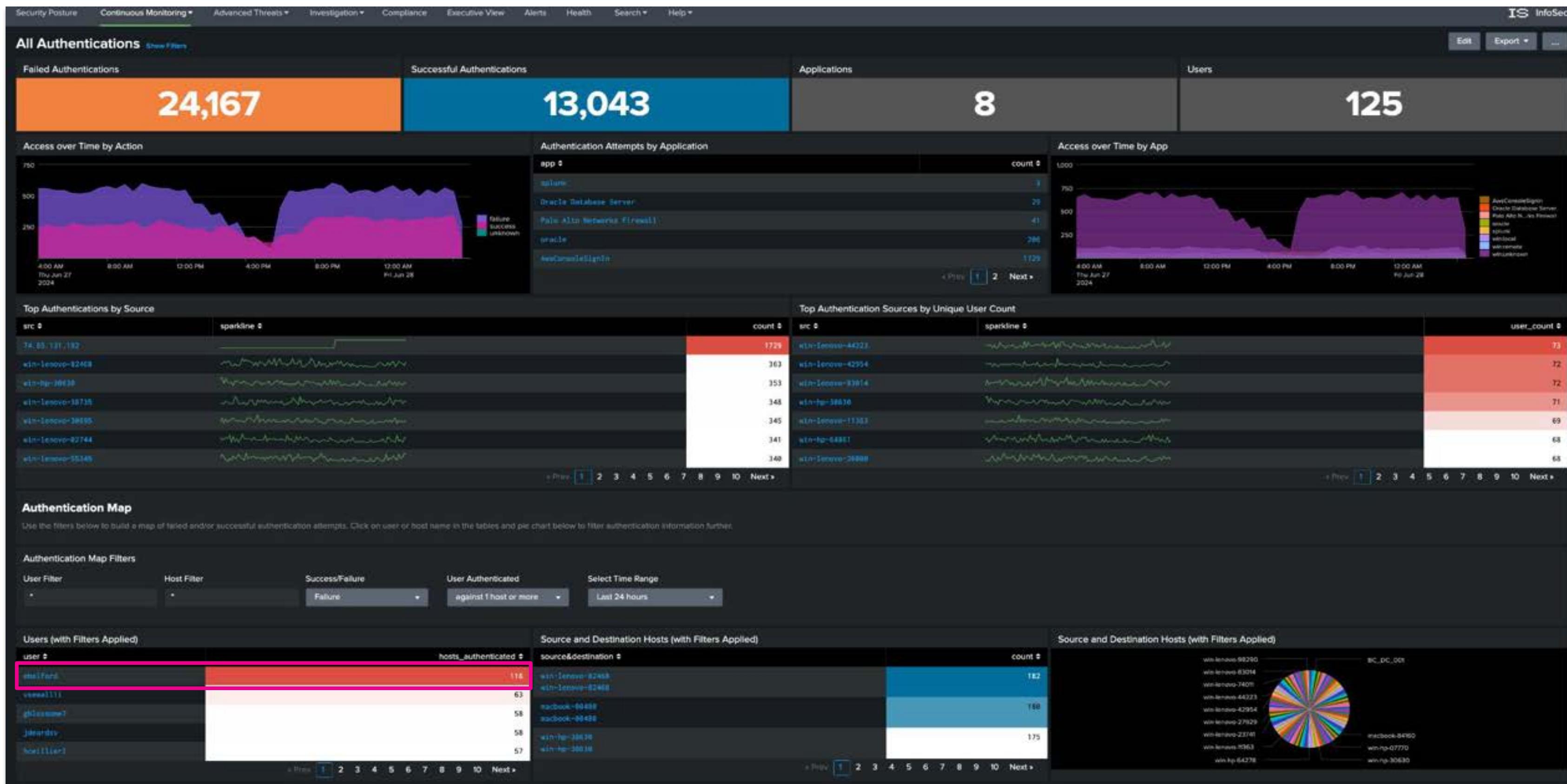


Tasks

1. Use the **All Authentications** dashboard to identify which user accessed an unusual amount of hosts
2. Use the **Access Anomalies** dashboard to identify:
 - a. The user with most failures
 - b. The user taking the most privileged actions
3. Drill into the user identified and review the account changes made



Check Continuous Monitoring - All Authentications Dashboard



Check Advanced Threats - Access Anomalies Dashboard

Security Posture Continuous Monitoring Advanced Threats Investigation Compliance Executive View Alerts Health Search Help IS InfoSec Edit Export ...

Access Anomalies Show Filters

Spike in # of Hosts Accessed **0** Over 24 hours compared to 30-day baseline

Brute Force Attack by Source **118**

src #	failures
win-lenovo-02448	256
win-tp-18838	246
win-70-55558	237
win-tp-64275	234
win-lenovo-7481	233

No results found.

Brute Force Attack by User **115**

user #	failures
abelford	115
vaseek111	87
(benny)	81
mluscott8	79
phlossome7	77

Users Failing Auth Over 80% **4**

user #	success	failure	%
abelford	18	73	88
root	4	41	100
SYSTEM	1	34	81
SYSTEM	0	14	100

Successful Auth Sources With the Greatest # of Users

src #	num_users	users
win-lenovo-38735	39	abeckens, beaccourtb, bairgetera, balmaker2k, carkleb, ccabottak, coogans14, dfranceschino4, dswalbek, ebelford, esake1, ffincj12, gkeling, win-lenovo-44223
macbook-00816	38	adams, adrainz, akwon, anadini8, awafford2b, cthildeg, coogan14, citaneland24, ctombe29, dswalbek, ebelford, fmidlers, gblowsome7, gert2, win-lenovo-83814
macbook-16648	37	amerit, anadini8, lighrolid2b, balmaker2k, cthildeg, coebaggan, cmesa2a, djelakene, dtesauri1, ebelford, ebelford11, ecutting10, kharly, 80_DC_ME
NY_08_183	35	adams, adrainz, lighrolid2b, bairgetera, ctombe29, dfranceschino4, dyiscken, dtesauri1, ebelford, fmattiacce, fmidlers9, gkeling17, gmc, win-tp-07779
win-lenovo-03744	35	abroughton, amerit, awafford2b, spark, streyny2d, carkleb, ccabottak, dswalbek, ebelford, ekaroly1t, folisterh, fmattiacce, fmidlers

Failed Auth Sources With the Greatest # of Users

src #	num_users	users
win-lenovo-44223	64	adams, adrainz, amerit, anadini8, awafford2b, spark, balmaker2k, streyny2d, ccabottak, cthildeg, vdebaggin, ctombe29, dfranceschino4, 80_DC_ME
win-lenovo-83814	59	abeckens, abroughton, adrainz, amerit, akwon, anadini8, lighrolid2b, bairgetera, carkleb, ccabottak, cdebaggin, citaneland24, ctombe29, dfranceschino4, dyiscken, fmidlers, gert2, gkeling, gmc, win-tp-06036
80_DC_ME	56	adams, abroughton, amerit, akwon, awafford2b, lighrolid2b, bairgetera, streyny2d, cthildeg, cmesa2a, dfranceschino4, dyiscken, fmidlers, gert2, gkeling, gmc, win-tp-06036
ctombe29	56	abeckens, adrainz, amerit, akwon, awafford2b, lighrolid2b, bairgetera, folisterh, fmattiacce, fmidlers9, gkeling17, gmc, win-tp-06036

Users Taking Privileged Actions First Time in 30 Days **0**

Users Taking Privileged Actions **33**

Check Investigation - User Investigation Dashboard

Security Posture Continuous Monitoring Advanced Threats Investigation Compliance Executive View Alerts Health Search Help IS InfoSec Edit Export ...

User Investigation

User (Wildcards Accepted): *ebelford*

Authentication Success/Failure: Last 24 hours, All, Hide Filters

User Access by Source

User Access by Destination

Access over Time by Action

Access over Time by App

Account Changes

Access by Source

src #	dest #	timechart #	count #
win-lenovo-82448	win-lenovo-82448	~	268
win-lenovo-55345	win-lenovo-55345	~	253
macbook-06489	macbook-06489	~	258
win-lenovo-83355	win-lenovo-83355	~	256
win-hp-16638	win-hp-16638	~	251
win-lenovo-38735	win-lenovo-38735	~	248
macbook-09125	macbook-09125	~	249
win-hp-07699	win-hp-07699	~	243
win-lenovo-08298	win-lenovo-08298	~	243
win-lenovo-29115	win-lenovo-29115	~	242

Events with User Name (up to 10,000 Events Shown)

_time #	action #	src #	dest #	count #	app #	user #	src_user	entity #	data source #	count #
2024-06-28 04:11:43	failure	win-lenovo-82448	win-lenovo-82448	215	win:unknown	ebelford		macbook-06489	KinEventLog	119
2024-06-28 04:35:58	failure	win-lenovo-55345	win-lenovo-55345	213	win:unknown	ebelford		win-hp-30638	KinEventLog	113
2024-06-28 04:28:29	failure	macbook-06489	macbook-06489	210	win:unknown	ebelford		win-lenovo-38735	KinEventLog	109
2024-06-28 04:38:14	failure	win-hp-16638	win-hp-16638	216	win:unknown	ebelford		NY_DC_018	KinEventLog	106
2024-06-28 04:31:42	failure	win-lenovo-43255	win-lenovo-08298	286	win:unknown	ebelford		macbook-27124	KinEventLog	102
2024-06-28 04:38:42	failure	win-lenovo-38735	win-lenovo-38735	286	win:unknown	ebelford		win-hp-64278	KinEventLog	100
2024-06-28 04:31:42	failure	win-lenovo-43255	win-lenovo-08298	286	win:unknown	ebelford		win-lenovo-92184	KinEventLog	98
2024-06-28 04:38:42	failure	win-hp-07699	win-hp-07699	286	win:unknown	ebelford		win-lenovo-82448	KinEventLog	96
2024-06-28 04:31:22	failure	win-hp-94892	win-hp-94892	198	win:unknown	ebelford		win-lenovo-11383	KinEventLog	95
								macbook-12545	KinEventLog	93

What we have identified

Findings:

- We identified ebelford with the following unusual behaviors:
 - ebelford was the user accessing a high number of hosts within a 24 hour period
 - ebelford has taken the highest amount of privileged actions
 - ebelford is the user with the most failed login attempts
- ebelford did delete a large number of accounts

Next Steps you can take:

- Lock out the user account and force them to reset the password
- Document all malicious activities and reverse the malicious activities
- Identify all servers accessed and see if there where other malicious activities taking place



Our progress so far



IT team: Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly



Malware: Find Malware-infected files and setup an alert for future detections



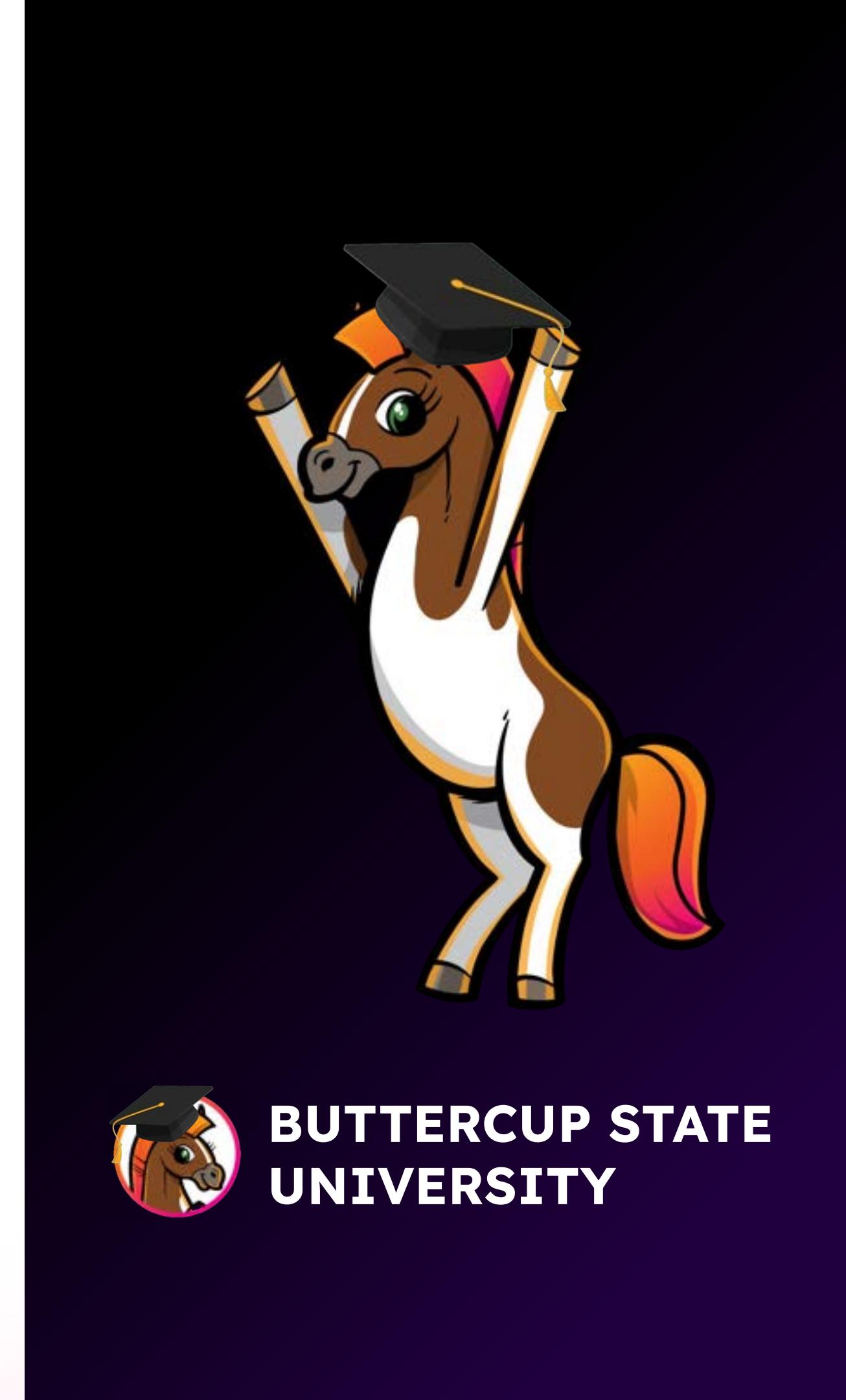
User behavior: Look for sudden access changes, unauthorized role modifications, or unusual activity



Customize the InfoSec App: Look for ways to customize the content for Buttercup State University



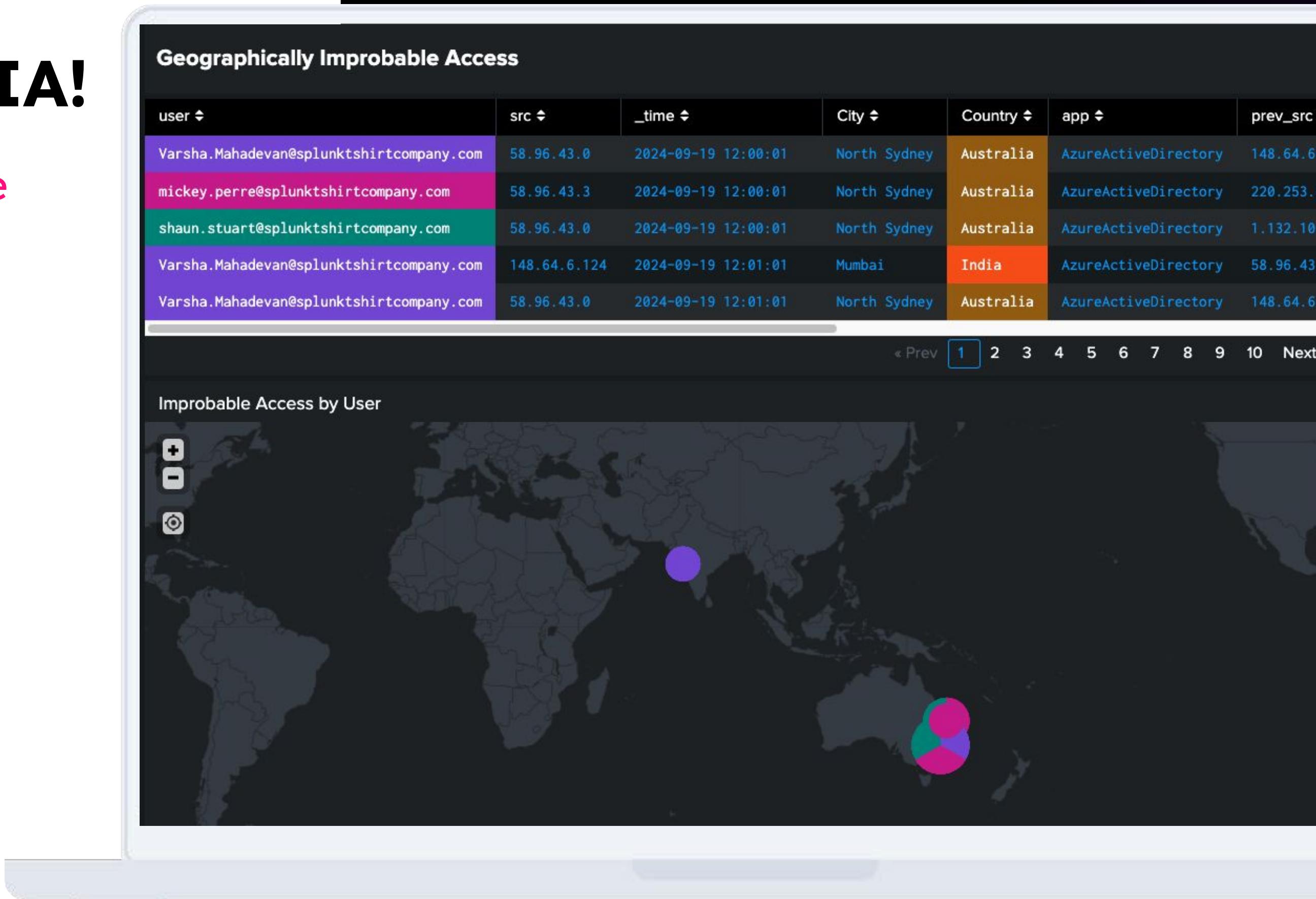
Add additional security content: Review the content in Splunk Security Essentials and add any new use cases you think might be valuable



Let's focus on GIA!

Geographically Improbable Accesses and Allowlists

- Triggers alerts when a user authenticates from 2 distant locations in a too short time frame
- Can trigger numerous false positives
- You may need Splunk to take into account expected behaviors, such as use of an authentication system or a VPN.



Lookups

Use lookups to customize your search queries

- Add CSVs to your Splunk to enable use of new information
- Unlock new possibilities by enriching your events data
- Read file with command:
| `inputlookup filename.csv`

The screenshot shows the Splunk interface with a search bar containing the query `| inputlookup vpn_ip.csv`. The search results table displays one result: `148.64.6.124`. The table has columns for `Events`, `Patterns`, `Statistics (14)`, and `Visualization`.

The screenshot shows the Splunk 'Lookup table files' page under the 'Knowledge' category. It lists 265 items, with the first few paths shown:

- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/AnonymizedBruteForce.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/Anonymized_Email_Logs.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/AppDependencies.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/AppSettings.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/CISA-alerts- 2020-2023.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/ColorScheme.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/Example_Legacy_Pass_The_Hash.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/Local_Short_Lived_Account.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/Local_User_Account_Creation.csv
- /opt/splunk/etc/apps/Splunk_Security_Essentials/lookups/PrivilegedRiskScores.csv

A red arrow points to the 'Add Data' button in the top right corner of the page.

Learn more: <https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutlookupsandfieldactions>

Customize the InfoSec App

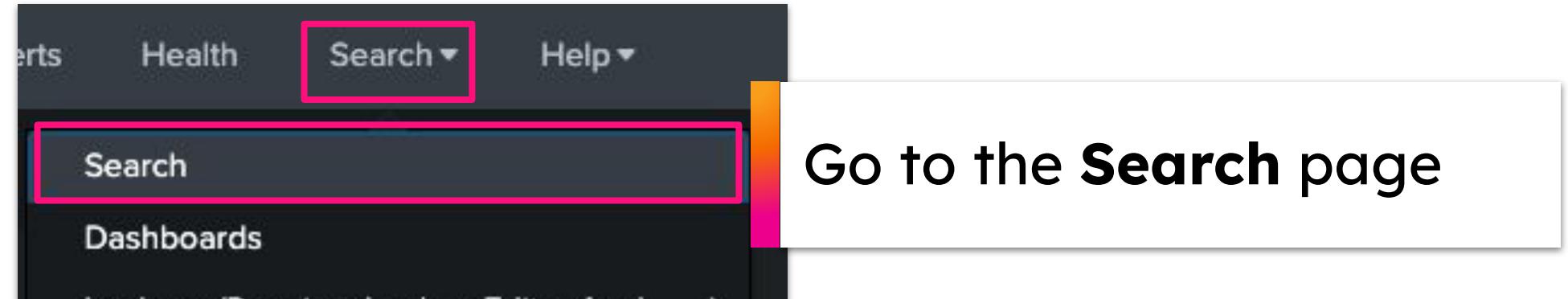
Look for ways to customize the content for Buttercup State University

Tasks

1. Check the contents of the **vpn_ip.csv** lookup, which contains the University's VPN IP ranges
2. Customize the **Geographically Improbable Access** table on the **Access Anomalies** dashboard to ignore these ranges
3. (Optional) Edit the **Geographically Improbable Access** map visualization using the same logic



Customize the Geographically Improbable Access Table



Go to the **Search** page

New Search

| inputlookup vpn_ip.csv

✓ 14 results (28/11/2024 11:00:00.000 to 29/11/2024 11:51:00)

No Event Sampling ▾

Events Patterns Statistics (14) Visualization

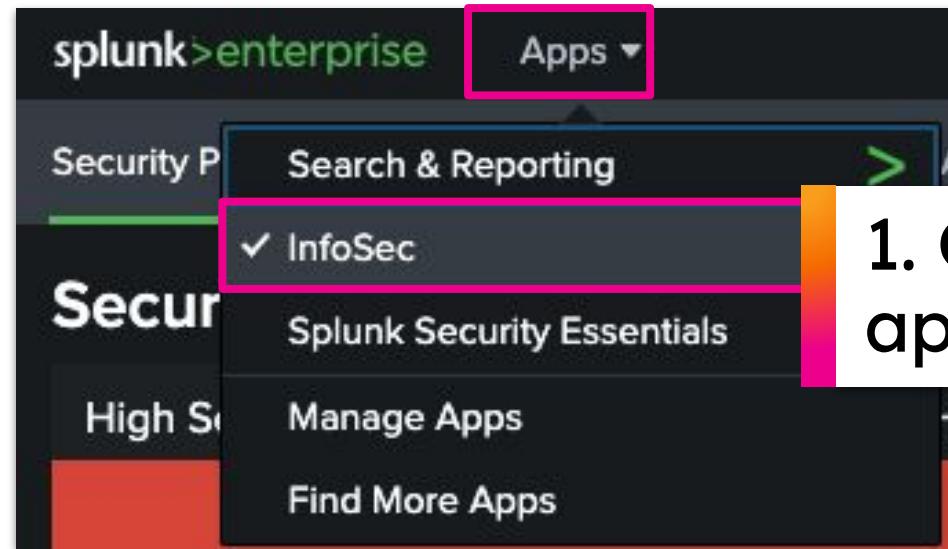
20 Per Page ▾ Format Preview ▾

vpn_ip ▾

vpn_ip
148.64.6.124
104.200.132.102
139.28.218.29
139.28.218.3
139.28.218.5
141.98.103.75

Check the **content of the CSV** by using the **inputlookup** command:
| [inputlookup](#) vpn_ip.csv

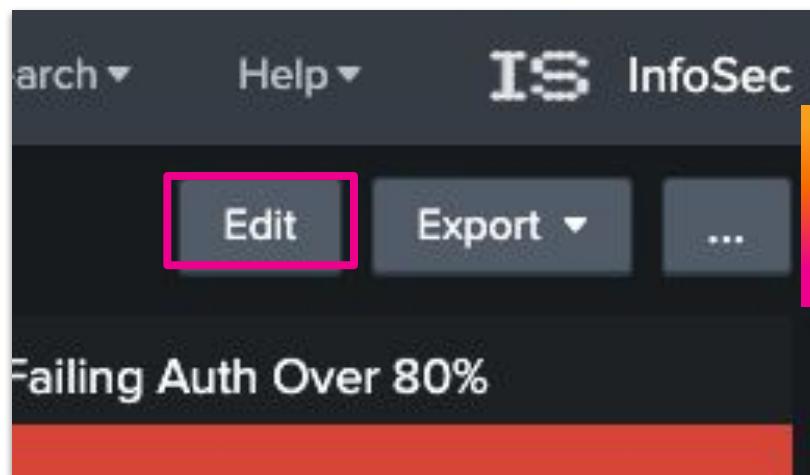
Customize the Geographically Improbable Access Table



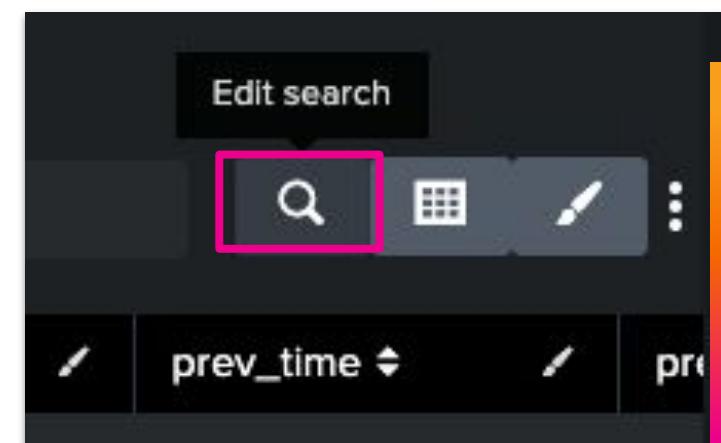
1. Open the **InfoSec** app



2. Go to **Advanced Threat > Access Anomalies**



3. Switch to **Edit** mode



4. Scroll down to the **Geographically Improbable Access** table and click **Edit search** (magnifying glass)

Customize the Geographically Improbable Access Table

Edit Search

Title

Search String

```
| eval _time=_time*1000  
| eval prev_time=_time-60000  
| eval time_diff=_time-prev_time  
| eval speed=round((distance*3600)/time_diff,2)  
| eval lat1_r=lat1*1000000  
| eval long1_r=long1*1000000  
| eval lat2_r=lat2*1000000  
| eval long2_r=long2*1000000  
| eval distance=round(sqrt(pow(lat1_r-lat2_r,2)+pow(long1_r-long2_r,2)),2)  
  
| where (speed > 500)  
| eval prev_time= strftime(prev_time,"%Y-%m-%d %H:%M:%S")  
| table user, src, _time, City, Country, app, prev_src, prev_time, prev_city,  
    prev_country, prev_app, distance, speed  
  
| 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
```

Run Search

Time Range Shared Time Picker (field1)

Auto Refresh Delay No auto refresh

Refresh Indicator Progress bar

Cancel Convert to Report **Apply**

6. Click on Apply

5. At the end of the search, add the following SPL:

```
| 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
```

Geographically Improbable Access

No title

No title

user	src	_time	City	Country	app	prev_src	prev_time	prev_city	prev_country	prev_
mickey.perre@splunktshirtcompany.com	58.96.43.3	2024-10-24 09:23:31	North Sydney	Australia	AzureActiveDirectory	228.253.98.44	2024-10-24 09:23:31	Kelvin Grove	Australia	Azur
shaun.stuart@splunktshirtcompany.co	58.96.43.8	2024-10-24 09:23:31	North Sydney	Australia	AzureActiveDirectory	1.132.197.15	2024-10-24 09:23:31	Woolloongabba	Australia	Azur
mickey.perre@splunktshirtcompany.com	228.253.98.44	2024-10-24 09:24:31	Kelvin Grove	Australia	AzureActiveDirectory	58.96.43.3	2024-10-24 09:23:31	North Sydney	Australia	Azur
mickey.perre@splunktshirtcompany.com	58.96.43.3	2024-10-24 09:24:31	North Sydney	Australia	AzureActiveDirectory	228.253.98.44	2024-10-24 09:24:31	Kelvin Grove	Australia	Azur
shaun.stuart@splunktshirtcompany.co	1.132.197.15	2024-10-24 09:24:31	Woolloongabba	Australia	AzureActiveDirectory	58.96.43.8	2024-10-24 09:23:31	North Sydney	Australia	Azur

(Optional)

Customize the Improbable Access by User Map

Edit Search

Title

Search String

```
| tstats summariesonly=true allow_old_summaries=true values(Authentication.app  
as app from datamodel=Authentication.Authentication where Authentication  
.action=success by Authentication.user, Authentication.src _time span=1s  
| rename "Authentication.*" as "*"  
| eventstats dc(src) as src_count by user  
| search src_count>1  
| sort 0 + _time  
| iplocation src  
| lookup vpn_ip.csv vpn_ip AS src OUTPUT vpn_ip AS matched_src  
| where isnull(matched_src)  
| where isnotnull(lat) AND isnotnull(lon)  
| streamstats window=2 global=false earliest(lat) as prev_lat, earliest(lon) as  
prev_lon earliest(_time) as prev_time earliest(src) as prev_src earliest  
Run Search
```

Time Range

Shared Time Picker (field1) ▾

Auto Refresh Delay ?

No auto refresh ▾

Refresh Indicator

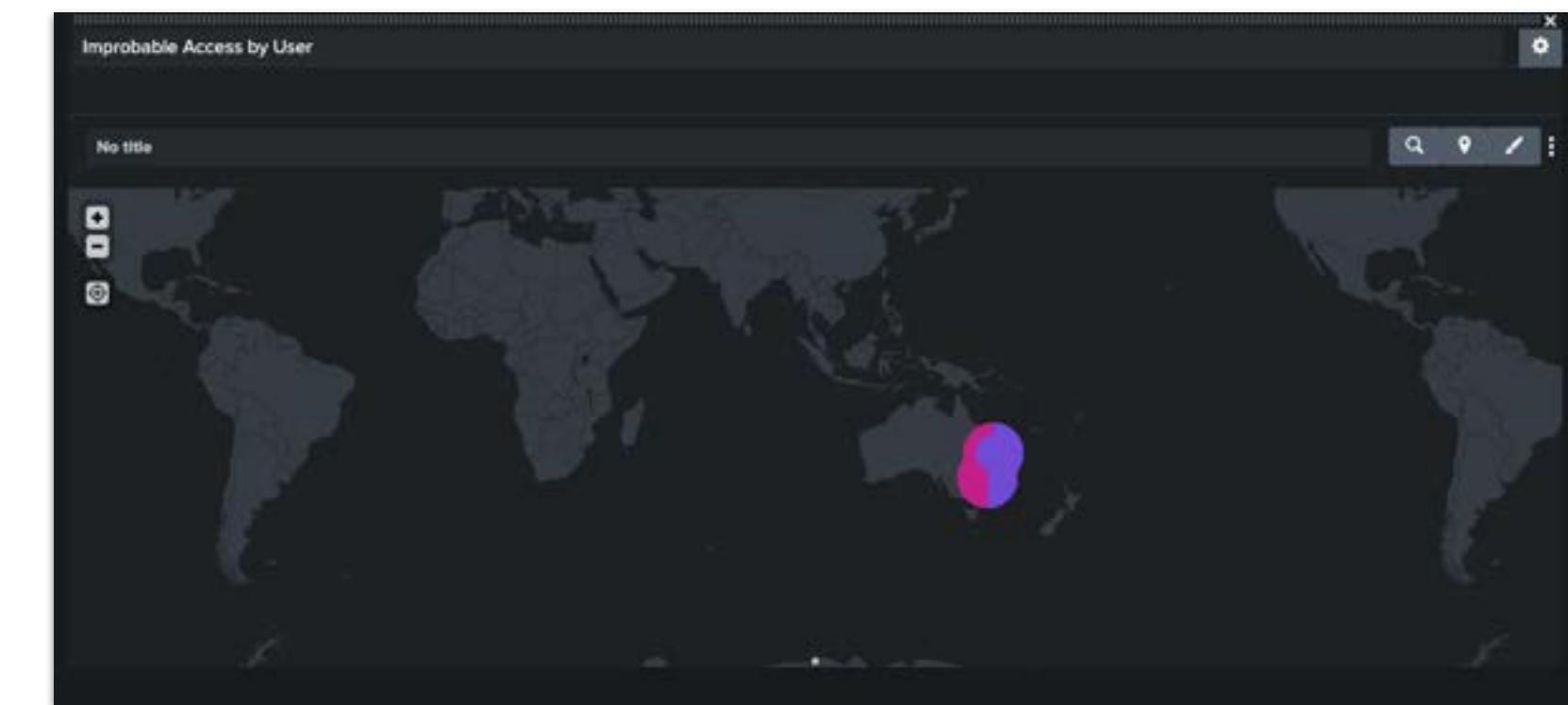
Progress bar ▾

Cancel Convert to Report **Apply**

8 Click on Apply

7. Edit the search of the **map visualisation** 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)
```



Save Your Dashboard!

The screenshot shows the Splunk dashboard editor interface. At the top, there is a navigation bar with links: Security Posture, Continuous Monitoring, Advanced Threats (which is the active tab), Investigation, Compliance, Executive View, Alerts, Health, Search, and Help. To the right of the tabs is the 'IS InfoSec' logo. Below the navigation bar is a toolbar with buttons for Edit Dashboard, UI, Source, + Add Panel, + Add Input, Dark Theme, Cancel, Save as..., and a prominent green Save button, which is highlighted with a pink border. The main area of the dashboard is titled 'Access Anomalies' and has a subtitle 'No description'. It features a time range selector set to 'Last 24 hours'. The dashboard contains four panels arranged in a grid. The first panel is a green card with the value '0' and the text 'Over 24 hours compared to 30-day baseline'. The other three panels are red cards with the values '123', '123', and '30' respectively. Each panel has a title: 'Spike in # of Hosts Accessed', 'Brute Force Attack by Source', 'Brute Force Attack by User', and 'Users Failing Auth Over 80%'. Below each panel is a row of search, edit, and more options buttons. A legend in the top right corner indicates that blue squares represent 'Autorum dashboard'. The bottom of the dashboard shows a series of dropdown menus for 'src', 'failures', 'user', and 'success'.

Click Save

Our progress so far



IT team: Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly



Malware: Find Malware-infected files and setup an alert for future detections



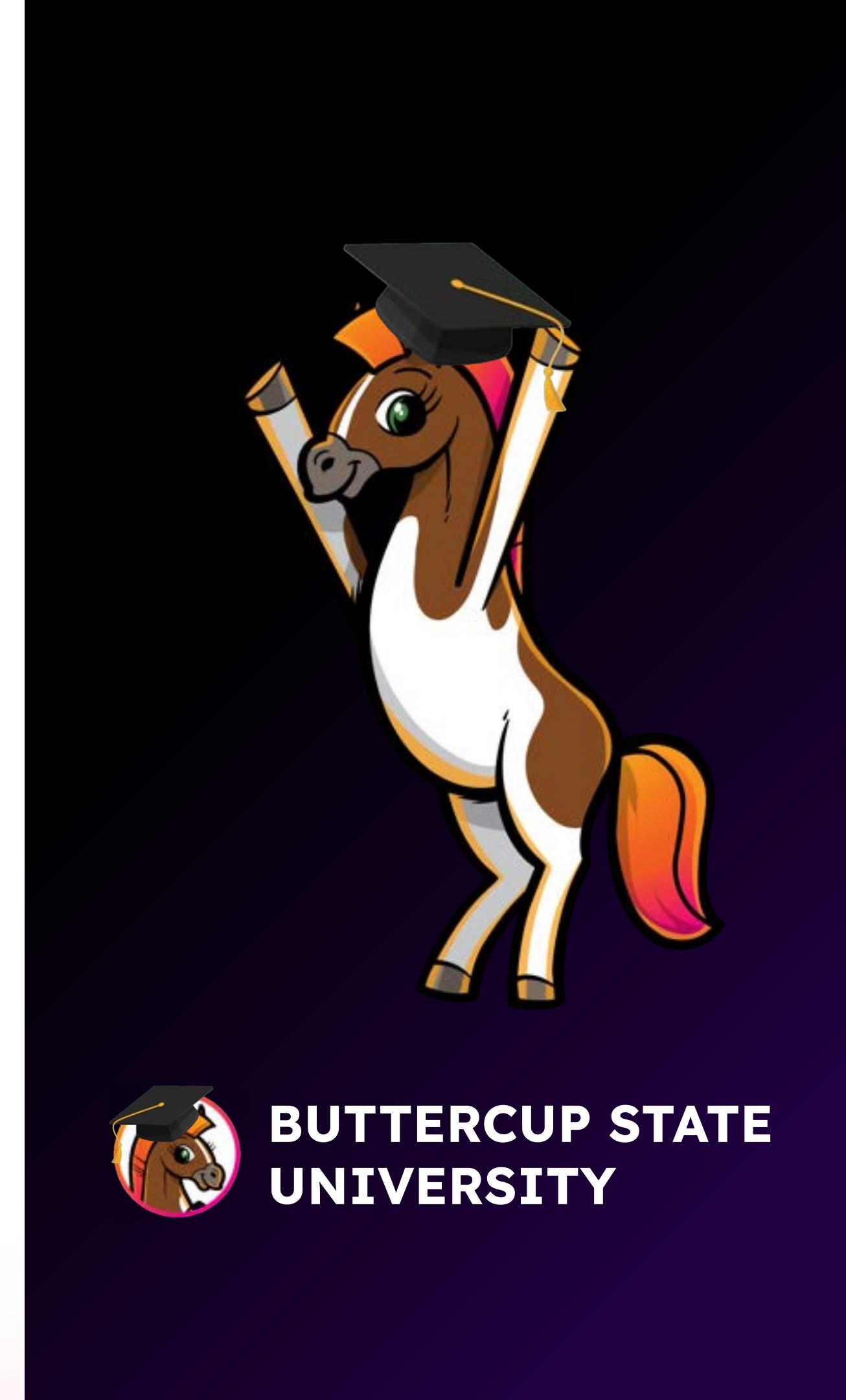
User behavior: Look for sudden access changes, unauthorized role modifications, or unusual activity



Customize the InfoSec App: Look for ways to customize the content for Buttercup State University



Add additional security content: Review the content in Splunk Security Essentials and add any new use cases you think might be valuable



Splunk Security Essentials

Free security app on Splunkbase

- Works on Splunk Enterprise and Cloud
- Repository of over 1600 searches and detections out-of-the-box (OOTB)
- Maps detections to the MITRE ATT&CK framework
- Data inventory checking capabilities
- Categorized into sections:
 - Compliance
 - Insider Threat
 - Security Monitoring

The screenshot shows the Splunkbase application page for 'Splunk Security Essentials' (SSE). At the top, there's a navigation bar with 'splunkbase', 'Collections', 'Apps', a search bar ('Find an app'), a 'Submit an App' button, and a 'Log In' button.

The main content area features a green icon with 'SSE' and a brief description: 'Get started with Splunk for Security with Splunk Security Essentials (SSE). Explore security use cases and discover security content to start address threats and challenges. Security Content Library Find security content for Splunk Cloud and Splunk's SIEM and SOAR offerings and deploy out-of-the-box security detections and analytic stories to enhance your investigations and improve your security posture.' Below this is a 'Login to Download' button.

Key stats are displayed in boxes: 'Latest Version 3.8.0' (March 26, 2024), 'Compatibility' (Splunk Enterprise, Splunk Cloud, Platform Version: 9.3, 9.2, 9.1, 9.0, CIM Version: 5.X), 'Rating' (4 stars from 56 reviews), 'Support' (Splunk Supported App), and 'Ranking' (#4 in Security, Fraud & Compliance).

Below these are tabs for 'Summary', 'Details', 'Installation', 'Troubleshooting', 'Contact', and 'Version History'. A sidebar on the right lists 'Categories' (Security, Fraud & Compliance), 'Created By' (Splunk Inc.), and 'Contributors'.

Adding Security Content: New Use Case

The Security team wants a new dashboard panel to show recurring infections on hosts

Tasks

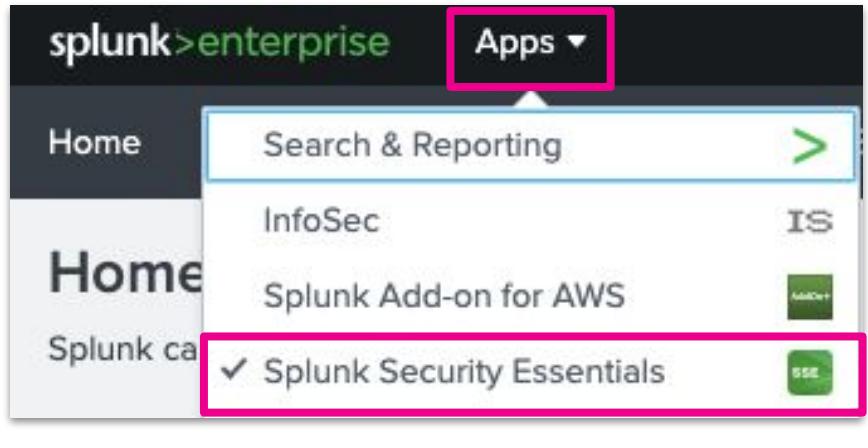
The Security team would like you to:

1. Add the '**Recurring Infection on Host**' use case from SSE to the InfoSec App's **Custom Use Cases** dashboard
2. Edit the search so only the **Risk_Name**, **Computer_Name** and **count** fields are displayed
3. Format the table to highlight the **count** in **red** if it's **greater than 10**

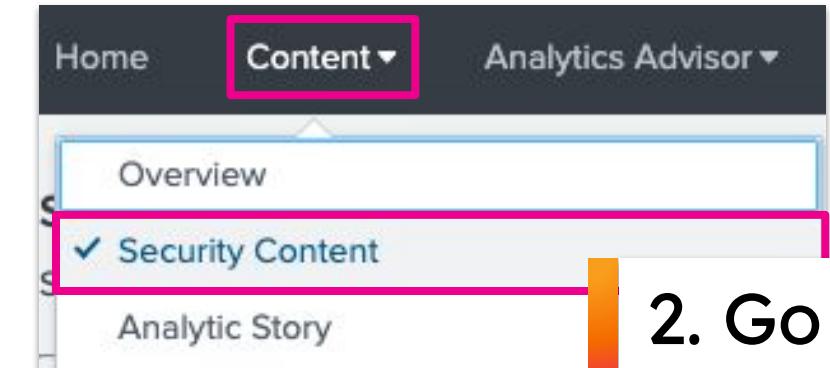


Edit the Custom Use Case Dashboard

Add new content from Splunk Security Essentials



1. Open Splunk Security Essentials



2. Go to Content > Security Content

3. Search for
“Recurring
Infection on Host”

The screenshot shows the search results for 'Recurring Infection on Host'. The search bar at the top contains the query 'Recurring Infection on Host'. Below the search bar are filters for 'Security Data Journey' (Level 1 (1085), Level 2 (585), ... (4)), 'Category' (Abuse (7), Account Compro... (31)), and 'Data Sources' (AWS (108), Anti-Virus or). There are buttons for 'Bookmark All' and 'Remove All Bookmarks'. The results section is titled 'Level 1: Foundational data insights' and contains two items:

- Recurring Infection on Host** (sse icon): Looks for the same malware occurring multiple times on the same host. It is categorized under 'Execution' and 'Initial Access' and includes tags for 'Drive-by Compromise', 'User Execution', 'Delivery', and 'None'.
- Windows hosts file modification** (escu icon): The search looks for modifications to the hosts file on all Windows endpoints across your environment. It is categorized under 'Command and Control' and 'CIS 10' and includes a tag for 'DE.CM'.

4. Click on the
Recurring Infection
on Host use case

Edit the Custom Use Case Dashboard

Add new content from Splunk Security Essentials

1. Under to the View section click on Live Data

2. Review the predefined search

3. Run the search

4. Scroll down and preview the output of the search under Raw Data Preview

5. Now copy the search to your clipboard

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=-30d  
| stats count range(_time) as 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)
```


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

Last 24 hours ▾ **Q**

Raw Data Preview
(Click Detect New Values above to find outliers.)

Risk_Name	Computer_Name	count	TimeRange	TimeRange_In_Days	TimeRange_In_Hours
Trojan.Gen.2	bravada	2	5589	0.06	1.55
Trojan.Gen.2	optima	2	2908	0.03	0.81

Enter a search

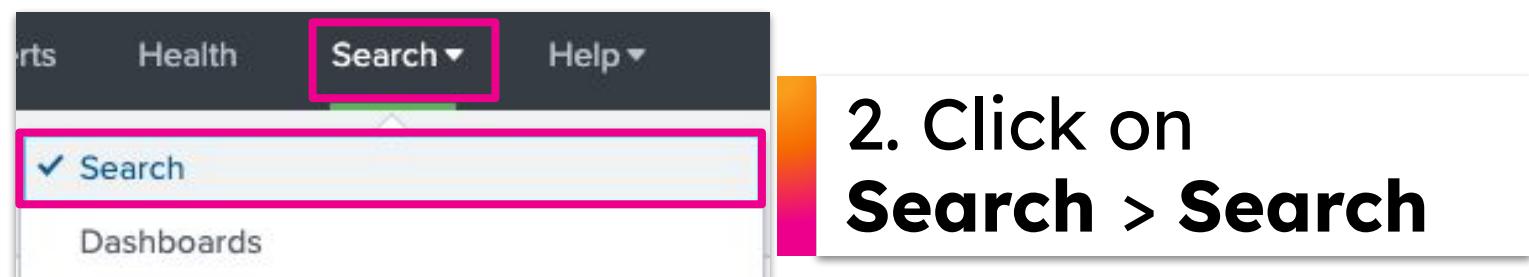
```
index=* sourcetype=symantec:* earliest=-30d  
| stats count range(_time) as TimeRange by Risk_Name, Computer_Name  
| where TimeRange>1800  
| eval TimeRange_In_Hours = round(TimeRange/3600,2), TimeRange_In_Days = round(TimeRange/3600/24,2)
```

Edit the Custom Use Case Dashboard

Add the new content to the Custom Use Case dashboard



1. Return to the InfoSec app



2. Click on Search > Search

The screenshot shows the 'New Search' interface. A pink box highlights the SPL code area where the following code is pasted:

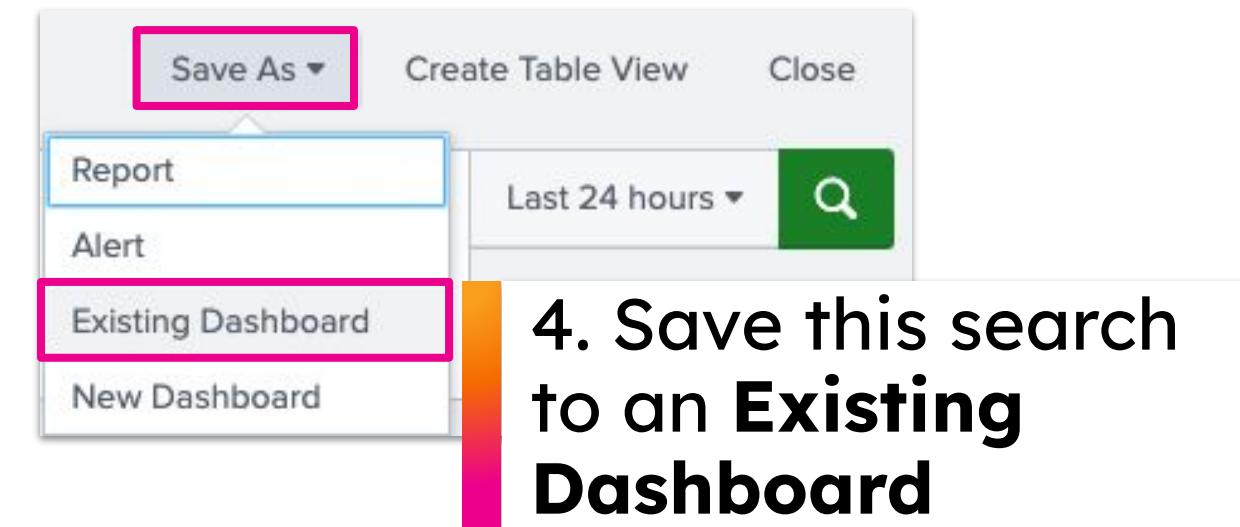
```
index=* sourcetype=symantec:* earliest=-30d  
| stats count range(_time) as TimeRange by Risk_Name, Computer_Name  
| where TimeRange>1800  
| eval TimeRange_In_Hours = round(TimeRange/3600,2), TimeRange_In_Days = round(TimeRange/3600/24,2)  
| fields Risk_Name, Computer_Name, count
```

Below the code, a pink box highlights the search results table showing two entries: 'Trojan.Gen.2' and 'Trojan.Gen.2' under 'Risk_Name' and 'bravada' and 'optima' under 'Computer_Name'. The 'count' column shows values of 2 for both rows.

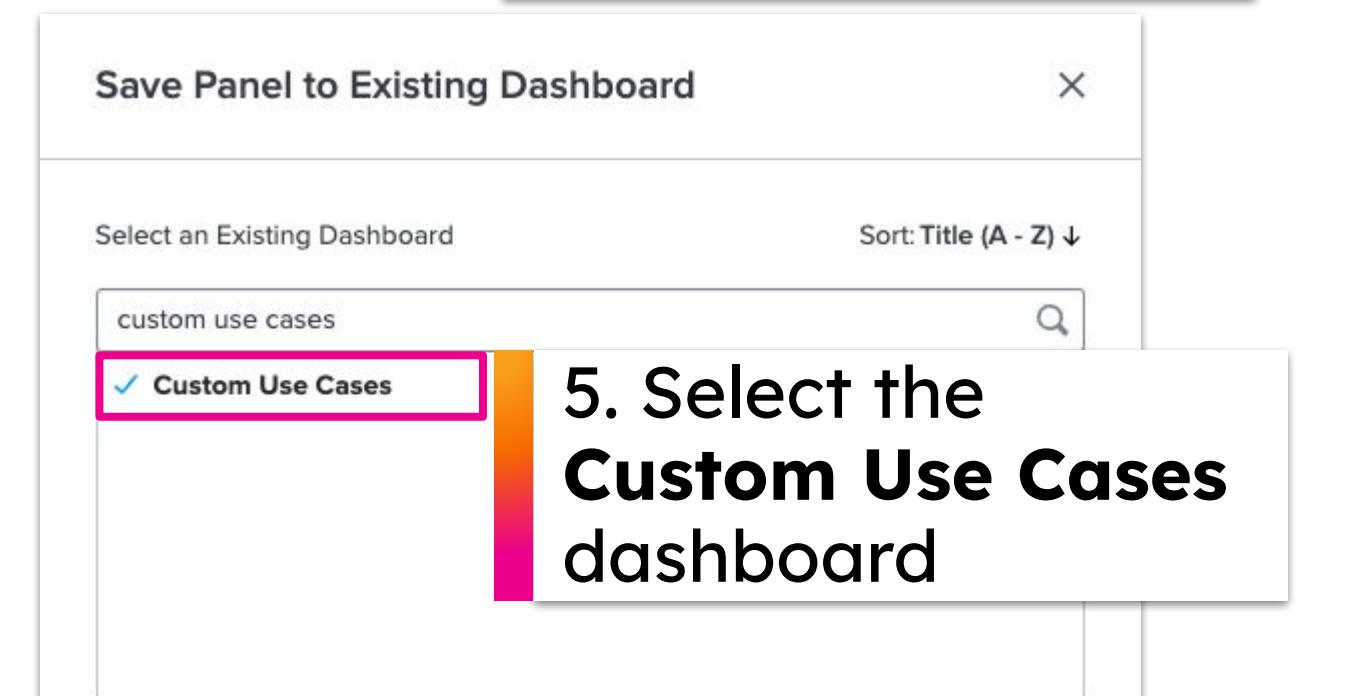
3. Paste in your SPL and add a line to only show the Risk_Name, Computer_Name and count fields

Line to add:

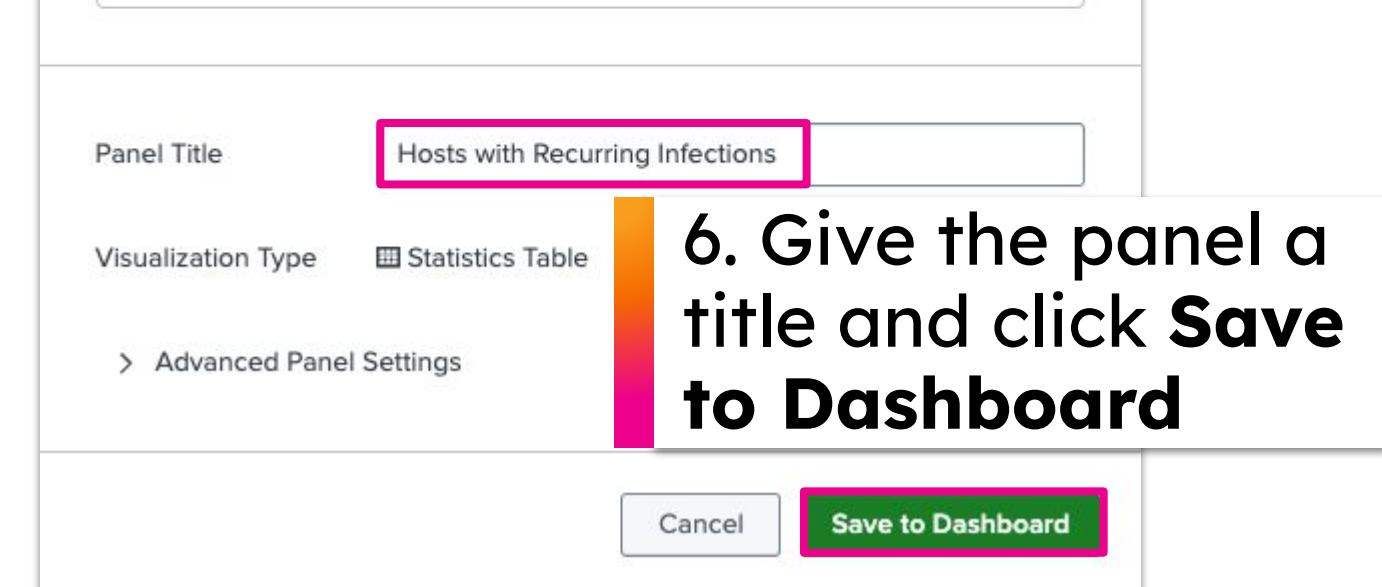
```
| fields Risk_Name, Computer_Name, count
```



4. Save this search to an Existing Dashboard



5. Select the Custom Use Cases dashboard



6. Give the panel a title and click Save to Dashboard

Edit the Custom Use Case Dashboard

Add color to the new dashboard panel

The screenshot shows the 'Custom Use Cases' dashboard under the 'Advanced Threats' tab. The top navigation bar includes 'Security Posture', 'Continuous Monitoring', 'Advanced Threats' (selected), 'Investigation', 'Compliance', 'Executive View', 'Alerts', 'Health', 'Search', 'Help', and the 'InfoSec' logo. Below the navigation is a toolbar with 'Edit' (highlighted in pink), 'Export', and a three-dot menu. A sidebar on the left shows filters for 'Last 24 hours' and 'Hide Filters'. The main content area contains text about the dashboard's purpose and available use cases, followed by a table titled 'Hosts with Recurring Infections'. The table has columns for 'Risk_Name', 'Computer_Name', and 'count'. It lists two rows: 'Trojan.Gen.2' with 'bravada' and 'continental' under Computer_Name, both having a count of 2. On the far right, there is a column header 'count'. Below the table, there is a section for 'Number Formatting' with a 'Color' button highlighted in pink, and a 'Ranges' section with two ranges defined: one from min to 10 (blue square) and another from 10 to max (red square). A '+ Add Range' button is also present. A large pink callout box labeled '2. Format the count column' points to the 'Color' button. Another callout box labeled '3. Edit the color ranges as shown so a count of 10 or greater will be red' points to the 'Ranges' section. A final callout box at the bottom right labeled 'Make sure you save your dashboard!' points to a green 'Save' button.

1. Edit the dashboard

This is a dashboard you can add your custom reports to.

You can explore hundreds of additional security use cases available in the free [Splunk Security Essentials app](#).

Some of the common use cases from Security Essentials app are already implemented in this InfoSec app under Access Anomalies and Network Anomalies.

Hosts with Recurring Infections

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

2. Format the count column

Color

Ranges

Number Formatting

from min to 10

from 10 to max

+ Add Range

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

Make sure you **save** your dashboard!

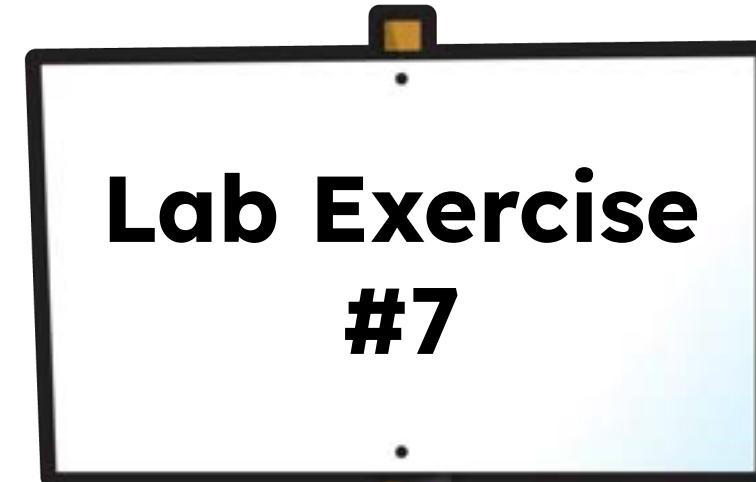
Save

Adding Security Content: New Dashboard

The Security team wants a new custom dashboard showing network security insights

Tasks

1. Use SSE's **Setup** menu to create a new "**Posture Dashboard**"
2. Create a new "**Essential Network Security**" dashboard containing the following insights:
 - Rare Internal Destination IPs
 - Rare Internal Source IPs
 - Hosts that communicate with the greatest number of destinations on SMB Ports
3. Add the dashboard to the **Continuous Monitoring** section of the InfoSec App



Create a Dashboard from Splunk Security Essentials

The screenshot shows the Splunk Security Essentials (SSE) setup process. A vertical navigation menu on the left lists four steps: 1 - Data Inventory, 2 - Content Mapping, 3 - Review App Configuration, and 4 - Create Posture Dashboards (optional). Step 4 is highlighted with a pink border. The main area shows a progress bar with four segments corresponding to these steps. To the right, there are two buttons: 'Start Searches' (green) and 'Retrieve Last Result' (pink), with 'Retrieve Last Result' also having a pink border. Below these buttons is a 'Create Posture Dashboards' button, which is also highlighted with a pink border. The bottom section shows a list of available visualizations under 'Available Visualizations'. The 'Essential Network Security' visualization is selected, indicated by a checked checkbox and a pink border around its row.

1. In SSE click on **Setup > 4 - Create Posture Dashboards**
2. Click on **Retrieve Last Result**
3. Click on **Create Posture Dashboards**
4. Select **Essential Network Security**

Create a Dashboard from Splunk Security Essentials

5. Select the detections shown here

Hosts that Communicate with the Greatest Number of Destinations
Shows the systems that have sent traffic to the greatest number of other hosts, indicating a higher risk of scanning activity.

Hosts that Communicate with the Greatest Number of Destinations on SMB Ports
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.

Rare Internal Source IPs
Shows the RFC1918 hosts that create the least amount of traffic.

Rare Internal Destination IPs
Shows the RFC1918 hosts that receive the least amount of traffic.

Number of Firewall Events Over Time
Shows the overall trend for the number of firewall events over time.

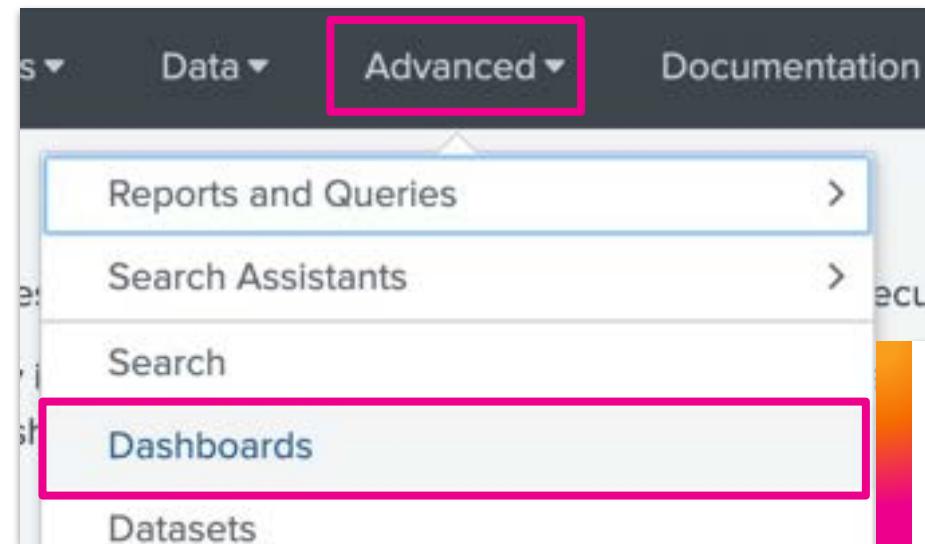
Hosts Sending to the Greatest Number of External SMB Destinations
Shows the systems that have sent traffic on SMB ports to the greatest number of non-RFC1918 hosts.

App Awareness

Create Dashboards

6. Click on Create Dashboards

Create a Dashboard from Splunk Security Essentials



7. Click on Advanced > Dashboards



8. Find the new dashboard and verify it contains the chosen detections

A screenshot of the 'Essential Network Security' dashboard. The dashboard has three main sections: 'Network Traffic', 'Hosts that Communicate with the Greatest Number of Destinations on SMB Ports', and 'Rare Internal Source IPs'. The 'Network Traffic' section shows a table of hosts and their traffic counts. The 'Hosts that Communicate with the Greatest Number of Destinations on SMB Ports' section shows a table of hosts and their destination counts. The 'Rare Internal Source IPs' section shows a table of source IP addresses and their counts. A pink arrow points from the 'Essential Network Security' item in the previous dashboard to this dashboard.

All_Traffic.src_ip	count
66.1.1.7	3
66.1.1.10	2
66.1.1.2	2
10.154.10.24	1
10.154.10.26	1
10.154.10.29	1
10.154.10.31	1
66.1.1.4	1
66.1.1.5	1
66.1.1.6	1

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.

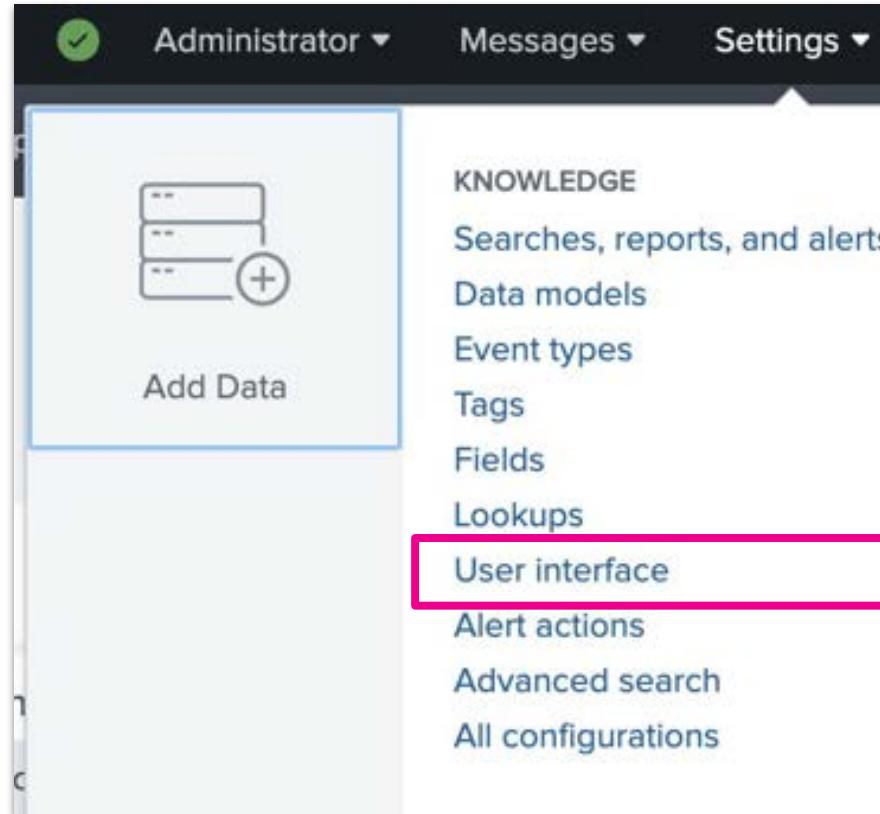
All_Traffic.src_ip	count
10.154.1.71	6
10.154.10.169	6
10.154.127.222	6
10.154.13.38	6
10.154.13.93	6
10.154.14.21	6
10.154.15.16	6
10.154.15.8	6
10.154.216.135	6
10.154.217.70	6

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

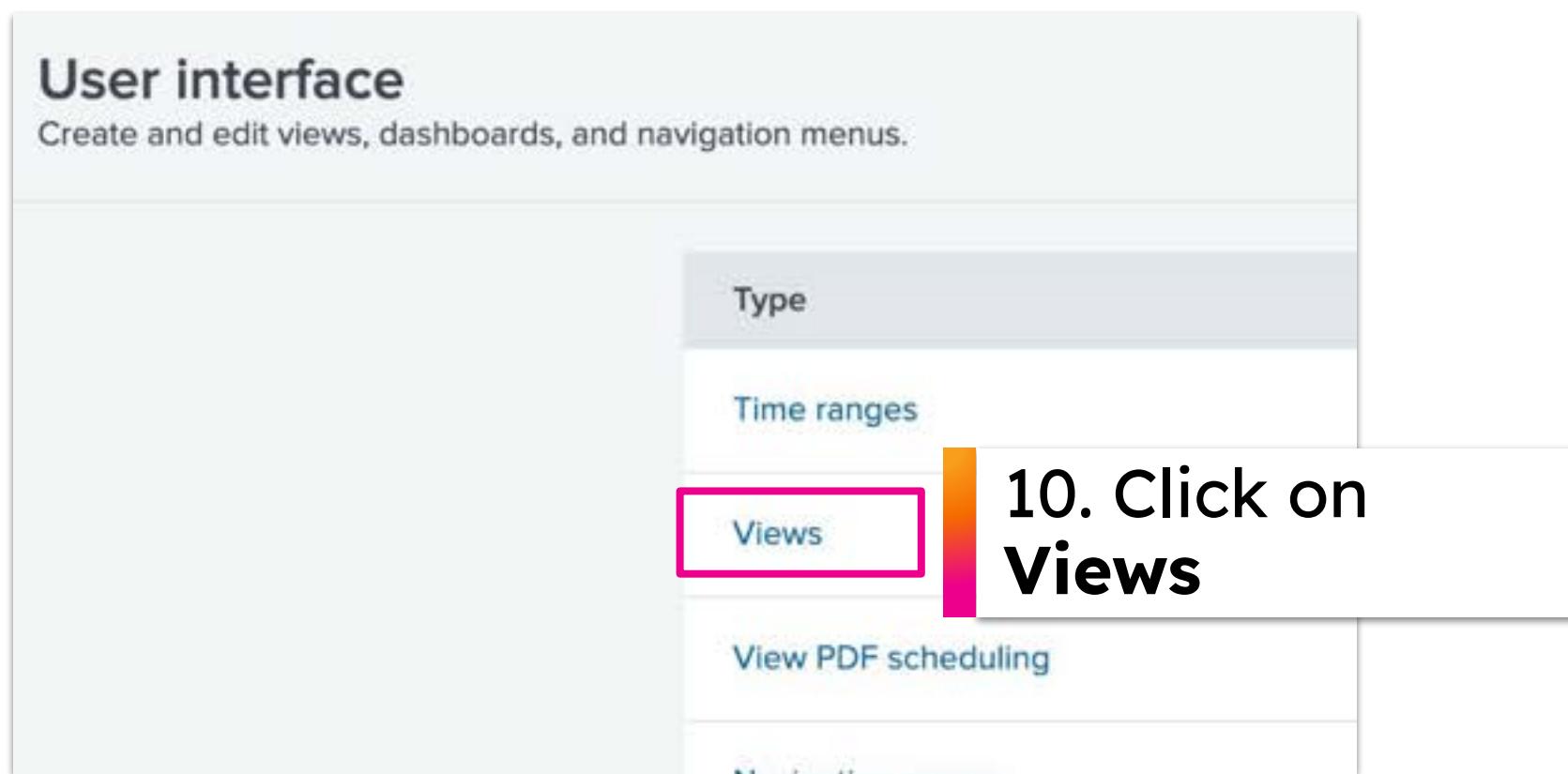
All_Traffic.dest_ip	count
10.154.1.88	6
10.154.10.283	6
10.154.10.247	6
10.154.10.77	6
10.154.114.26	6
10.154.122.128	6
10.154.135.14	6
10.154.252.92	6
10.154.8.283	6
10.68.28.45	6

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

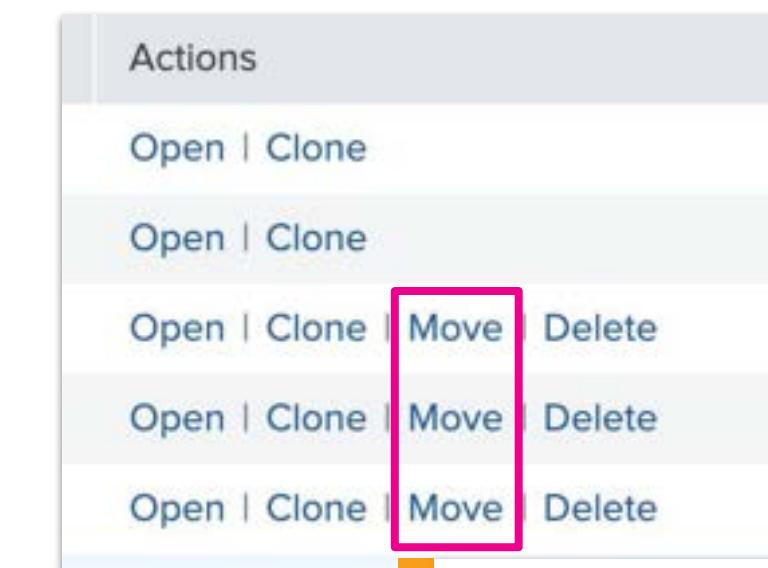
Move the Dashboard from SSE to the InfoSec App



9. Click on **Settings > User Interface**

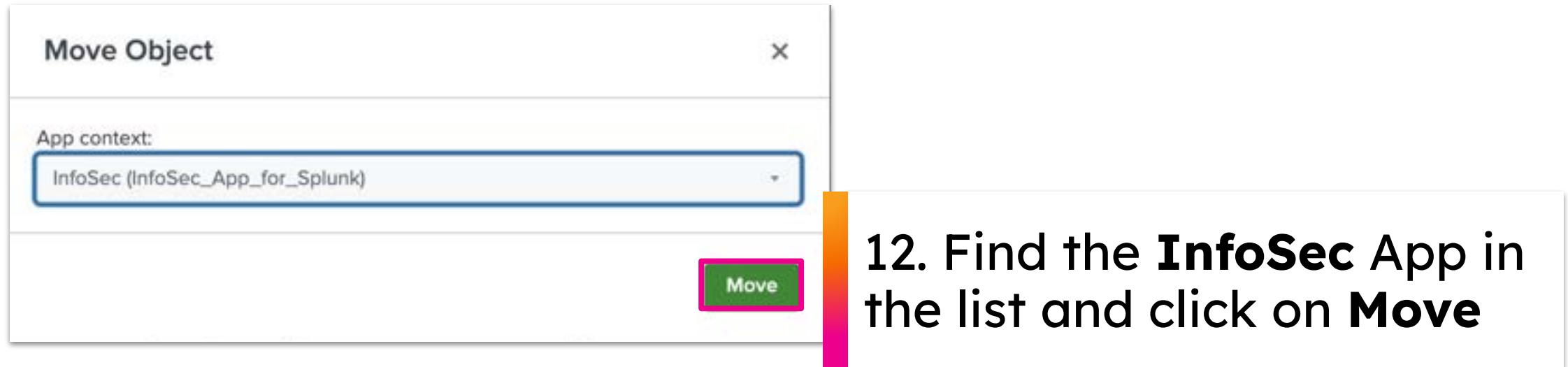


10. Click on **Views**

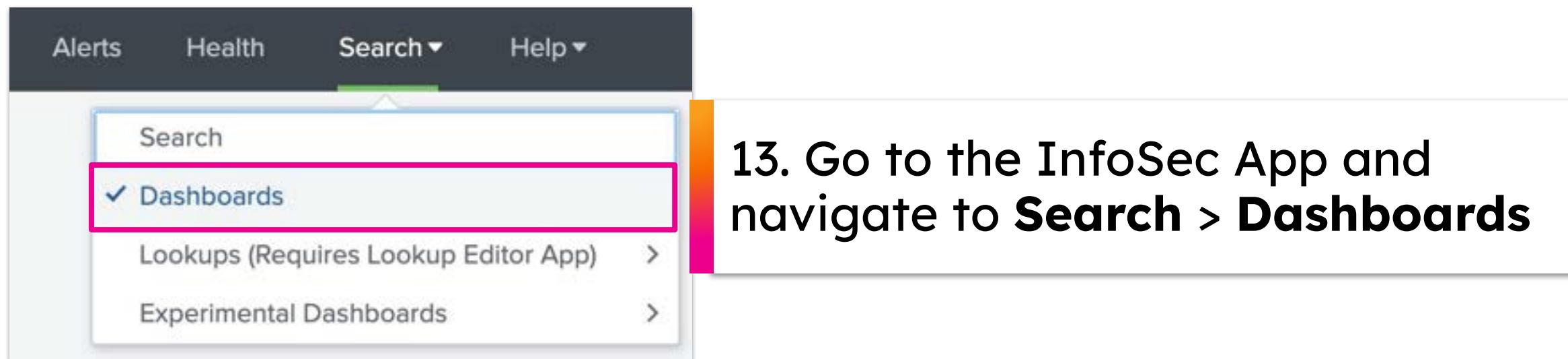


11. Find your dashboard and click on **Move**

Move the Dashboard from SSE to the InfoSec App



12. Find the **InfoSec** App in the list and click on **Move**



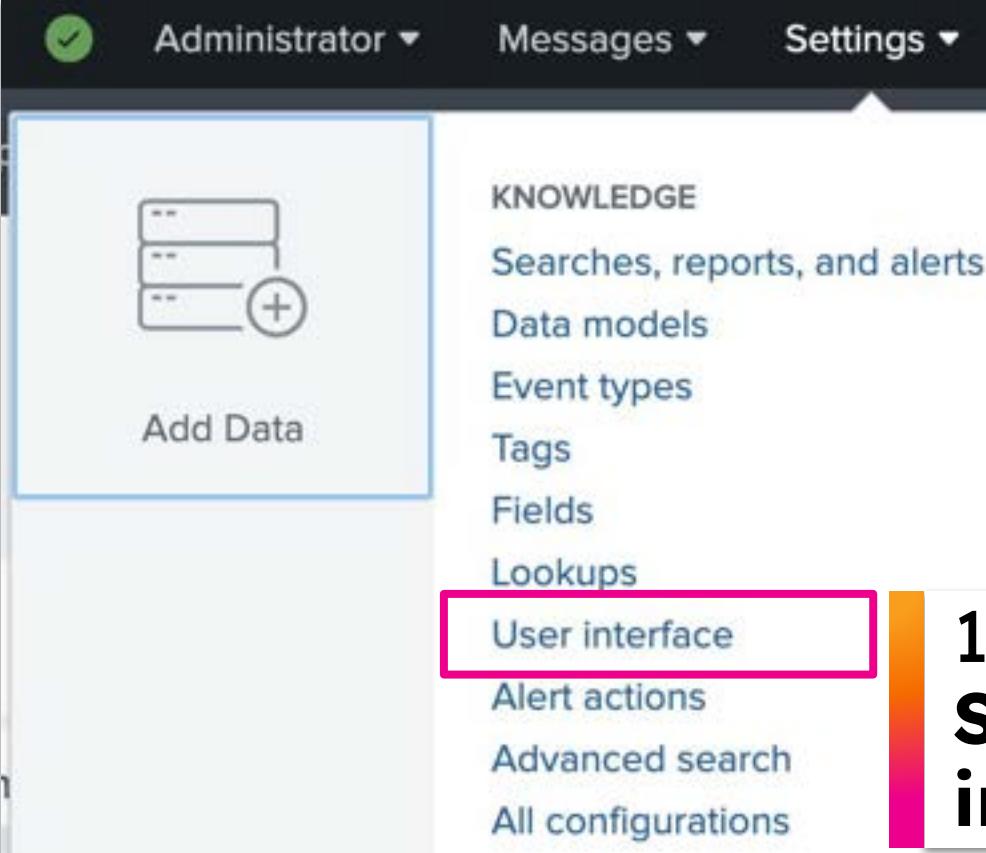
13. Go to the InfoSec App and navigate to **Search > Dashboards**

A screenshot of a list of dashboards. The list includes: 'Data Model Audit', 'Endpoints', 'Error Details', 'Essential Network Security' (which is highlighted with a pink border), 'Executive View', 'Firewalls', 'Health', and 'Health Overview'. To the right of each dashboard name are columns for 'Edit', 'Owner', and 'Name'. The 'Edit' column shows dropdown menus, the 'Owner' column shows names like 'nobody' or 'admin', and the 'Name' column shows names like 'Splunk_SA_CIM' or 'InfoSec_App_for_Spl...'. The background of the dashboard list is white.

> Data Model Audit	Edit ▾	nobody	Splunk_SA_CIM
> 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...
> Health	Edit ▾	nobody	InfoSec_App_for_Spl...
> Health Overview	Edit ▾	nobody	Splunk_TA_aws

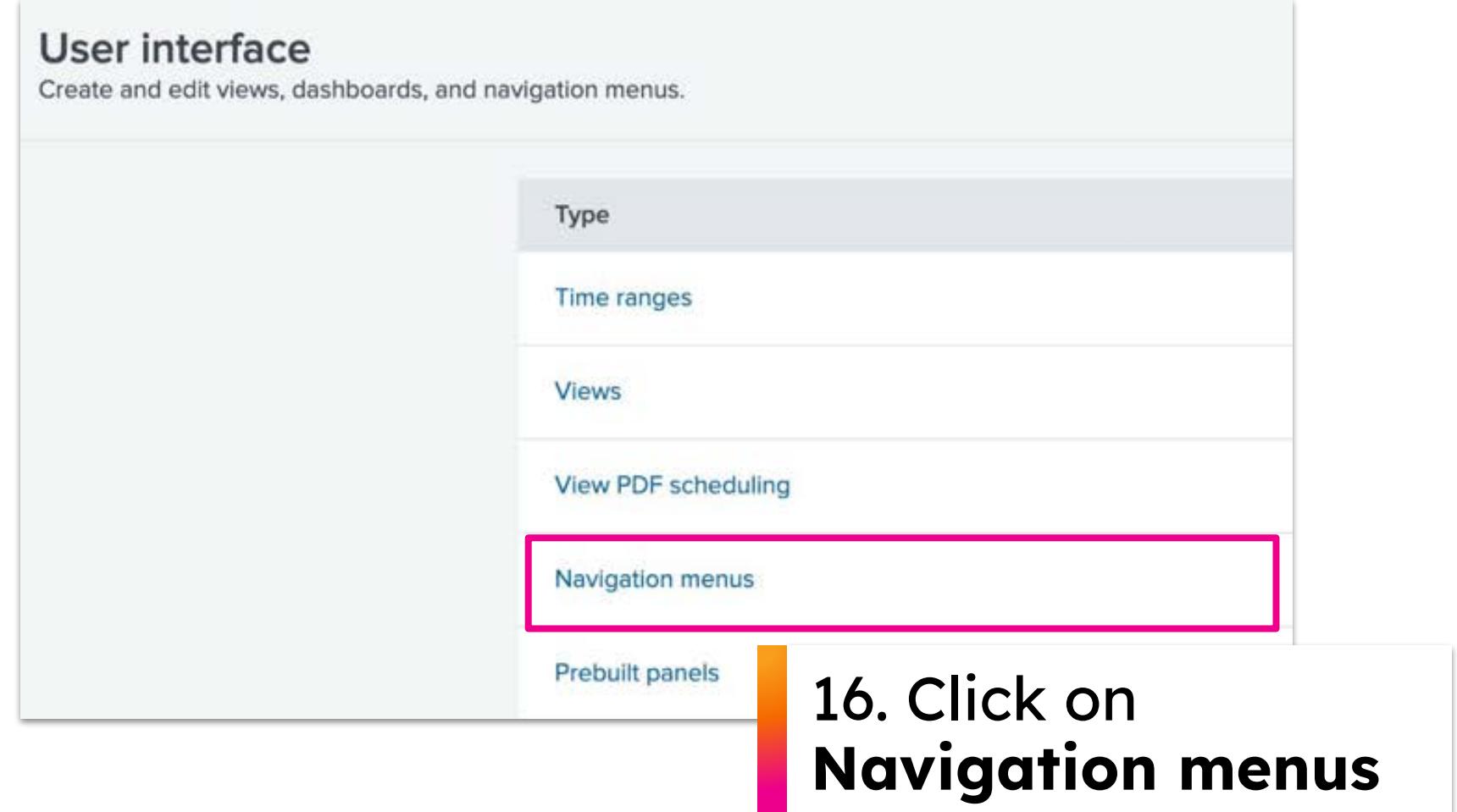
14. Locate your new dashboard in the list

Add the Dashboard to the Navigation Menu



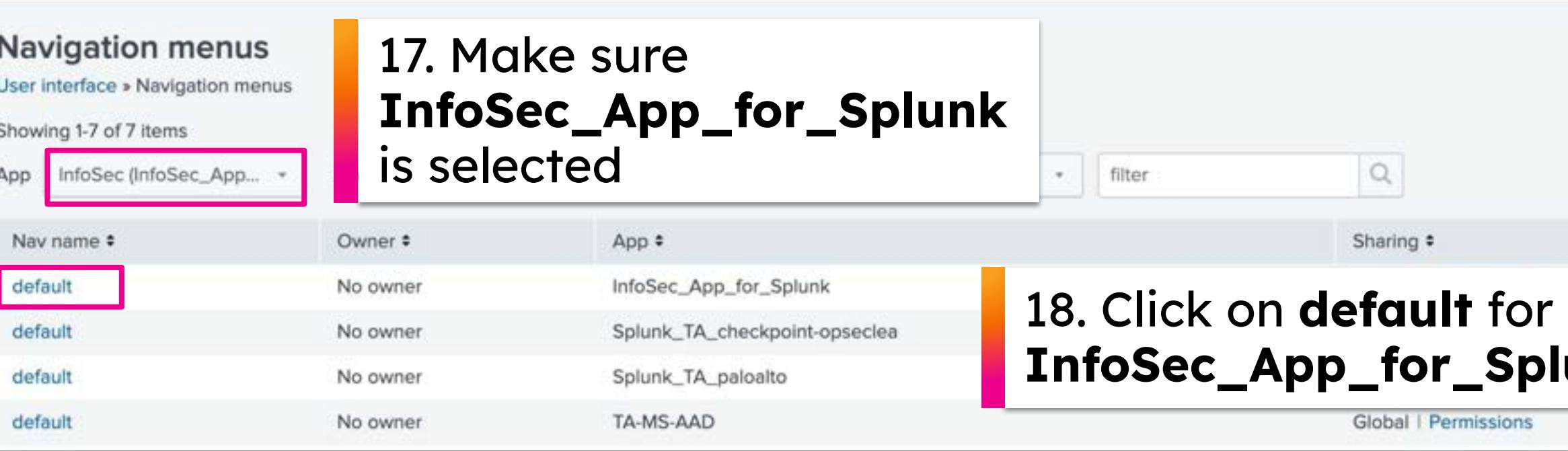
The screenshot shows the Splunk Settings menu. The 'User interface' option is highlighted with a pink border. The menu includes options like 'Add Data', 'KNOWLEDGE' (Searches, reports, and alerts, Data models, Event types, Tags, Fields, Lookups), 'User interface' (highlighted), 'Alert actions', 'Advanced search', and 'All configurations'.

15. Go to Settings > User interface



The screenshot shows the 'User interface' settings page. The 'Navigation menus' option is highlighted with a pink border. Other options include 'Time ranges', 'Views', 'View PDF scheduling', 'Prebuilt panels', and 'Navigation menus' (highlighted).

16. Click on Navigation menus



The screenshot shows the 'Navigation menus' list page. The 'App' filter is set to 'InfoSec (InfoSec_App...)' and the 'Nav name' column has 'default' highlighted with a pink border. The table lists four navigation items, all associated with the 'InfoSec_App_for_Splunk' app.

Nav name	Owner	App
default	No owner	InfoSec_App_for_Splunk
default	No owner	Splunk_TA_checkpoint-opseclea
default	No owner	Splunk_TA_paloalto
default	No owner	TA-MS-AAD

17. Make sure InfoSec_App_for_Splunk is selected

18. Click on default for the InfoSec_App_for_Splunk

Add the Dashboard to the Navigation Menu

Enter and edit navigation menu XML configuration.

Plain Text

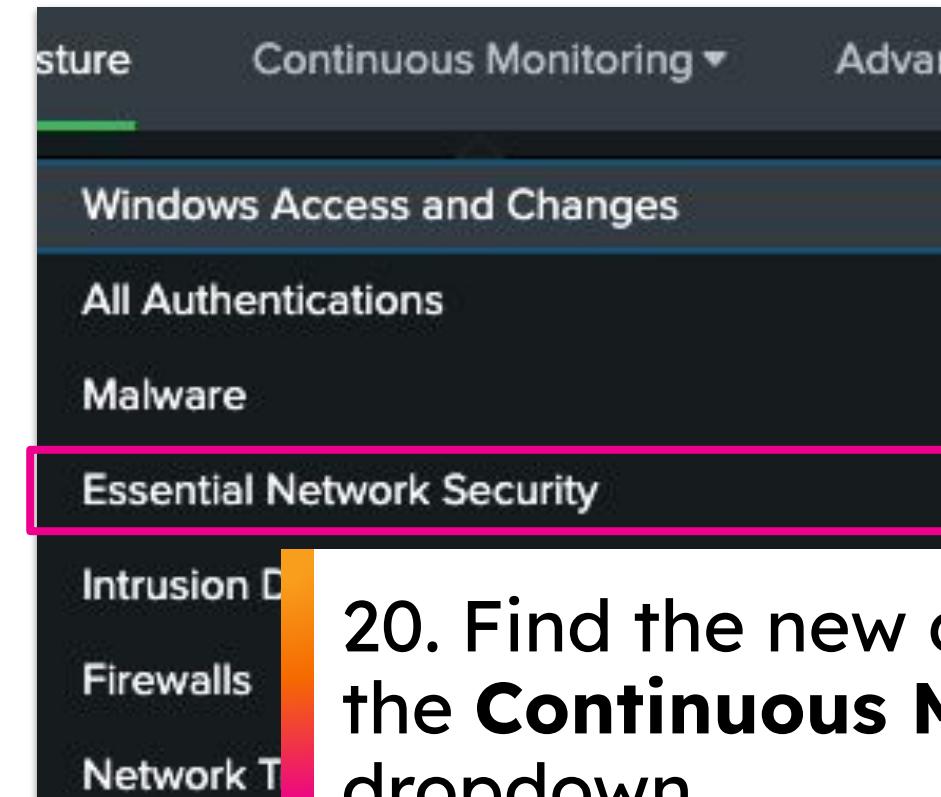
```
<nav>
    <view name="security_posture" default='true' />
    <collection label="Continuous Monitoring">
        <view name="windows" />
        <view name="access" />
        <view name="malware" />
        <view name="Essential_Network_Security"/> ←
        <view name="ids" />
        <view name="firewalls" />
        <view name="network" />
    </collection>

    <collection label="Advanced Threats">
        <view name="access_anomalies" />
        <view name="network_anomalies" />
        <view name="custom_use_cases" />
    </collection>

    <view name="security_monitoring" />
    <collection label="Investigation">
        <view name="user_investigation" />
        <view name="asset_investigation" />
    </collection>
    <view name="compliance"/>
    <view name="executive_dashboard"/>
```

Cancel Save

19. Edit the XML and add the “**Essential_Network_Security**” view after “**malware**” and save
Note: The view name is case sensitive!



20. Find the new dashboard in the **Continuous Monitoring** dropdown

XML to add:

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

You've Finished the Hands-on Exercises!



IT team: Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly



Malware: Find Malware-infected files and setup an alert for future detections



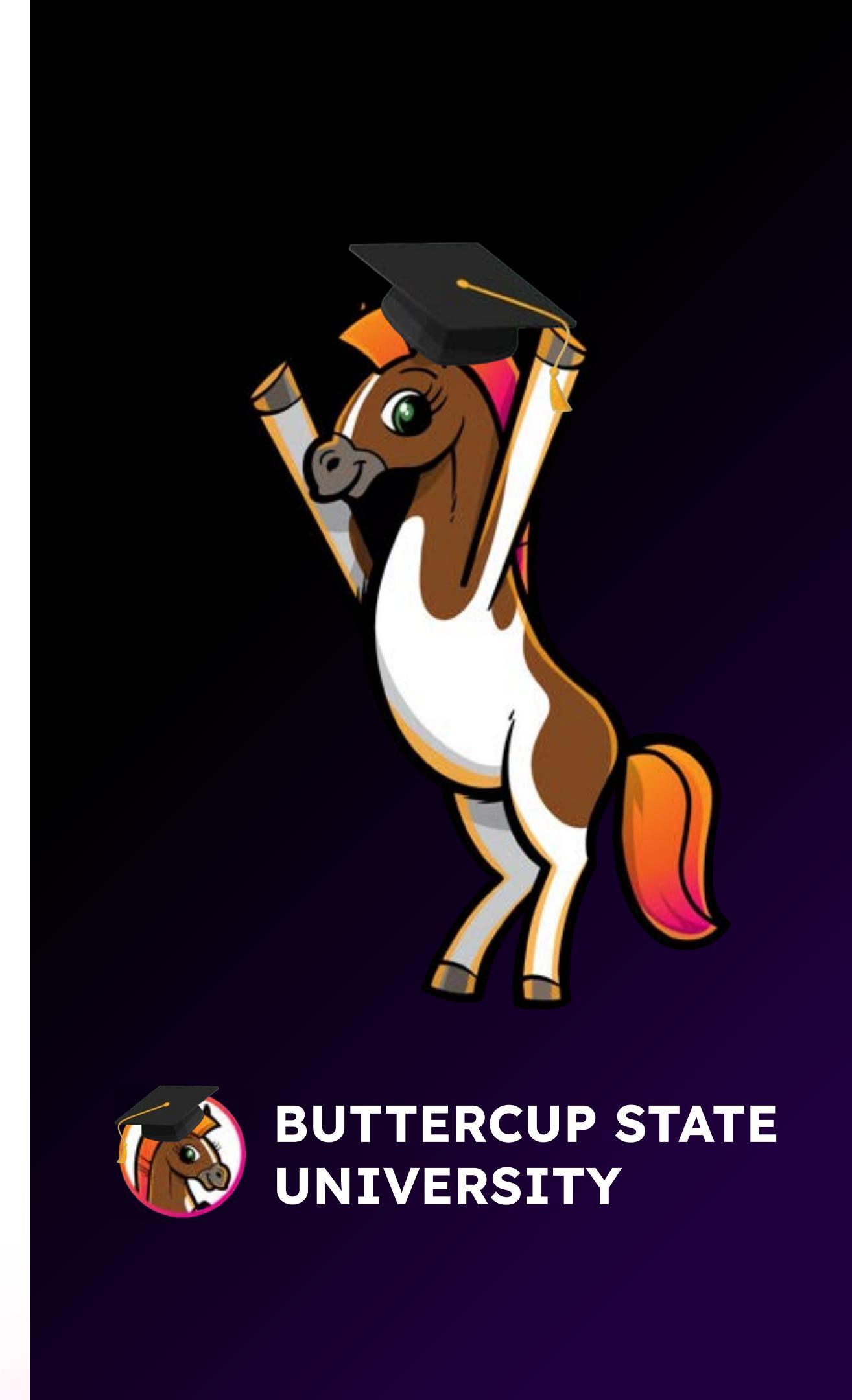
User behavior: Look for sudden access changes, unauthorized role modifications, or unusual activity



Customize the InfoSec App: Look for ways to customize the content for Buttercup State University

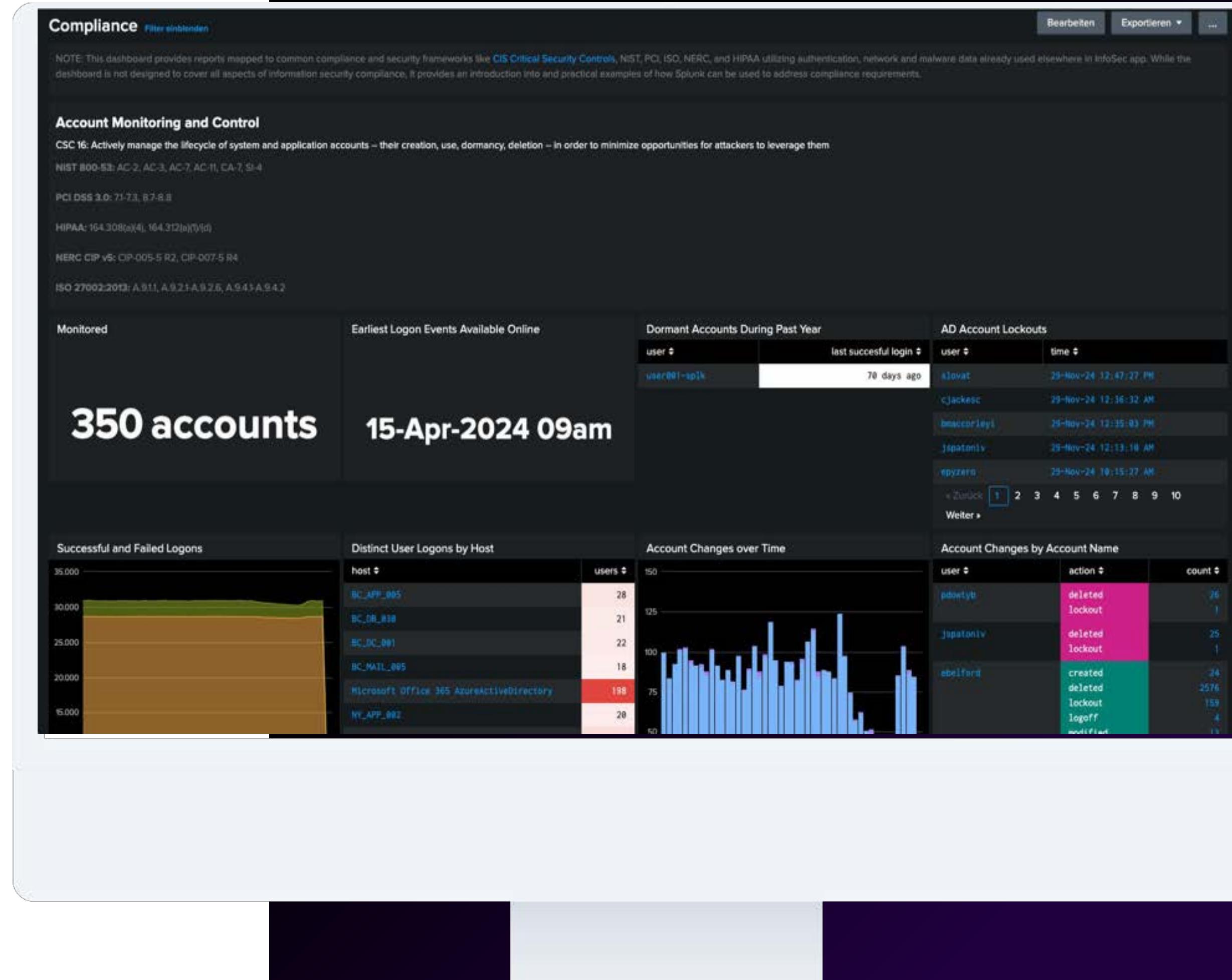


Add additional security content: Review the content in Splunk Security Essentials and add any new use cases you think might be valuable



Compliance Dashboard

- Out of the box reports mapped to common compliance and security frameworks like NIST, PCI, ISO, NERC, and HIPAA.
- Utilizes authentication, network, and malware data
- Edit and customize based on your requirements
- Helpful for regular audits!



What We've Covered Today

- ✓ Setting up the InfoSec App for Splunk
- ✓ Investigating using InfoSec App dashboards
- ✓ Creating an alert
- ✓ Customizing a built-in dashboard
- ✓ Creating a new dashboard
- ✓ Using Splunk Security Essentials to enrich and add new content



Splunk Resources

Where to go after today's workshop



Splunk4Ninjas - Common Information Model (CIM)

Hands-on Workshop

- **Go from Splunk CIM zero to hero in 3 hours!**
In-person and remote options available
- **Learn how data maps to CIM data models**
Discover how you can use Splunk add-ons and custom knowledge objects to make data CIM compliant
- **Apply SPL best practices for CIM data**
Learn the SPL commands available to search data mapping to CIM data models and accelerated data models
- **Basic Splunk experience required**
Ideal for those who have experience using the stats command, creating Splunk dashboards and using add-ons



Normalize and visualize custom data using CIM data models and tstats!



[Workshop Flyer](#)

BOSS Platform

<https://bots.splunk.com>

- 24x7 Access
- Login with Splunk.com account (just like Splunkbase)
- Used for all BOTS competition events
- Learn how to use Splunk for security use cases

The screenshot displays the BOSS Platform interface. At the top, there's a navigation bar with links: HOME, PLAY NOW, LEARN, BOSS EVENTS, and HISTORY. Below this, the "Play Now" section features three cards:

- corelight**: A card for Corelight Partner Experience, featuring the Corelight logo, a green "PLAY" button, and a brief description: "Adding Corelight's open NDR platform to Splunk provides the detections and evidence that deliver vital context to analysts and visibility to threat hunters. In just 15...".
- Hunting the Known Unknown: Supply Chain Attack Detection with JA3/s**: A card for Hunting the Known Unknown: Supply Chain Attack Detection, featuring a background image of metal bolts and nuts, a green "PLAY" button, and a description: "This is the companion event to the workshop Hunting the Known Unknown: Supply Chain Attack Detection. We will explore using JA3/s hashes to help...".
- BOSS OF THE SOC**: A card for Boss of the SOC Version 1, featuring the BOSS logo, a green "PLAY" button, and a description: "Experience the original! Boss of the SOC(BOTS) Version 1 debuted at Splunk .conf in October 2016. Since then, thousands of security practitioners have learned how...".

Below the "Play Now" section is a "Learn" section with four cards:

- .conf21**: A card for Securing the Software Factory With Splunk, featuring the .conf21 logo, a green "PLAY" button, and a description: "Securing the Software Factory With Splunk".
- corelight**: A card for Introduction to the Corelight Partner, featuring the Corelight logo, a green "Enrolled" button, and a description: "Introduction to the Corelight Partner".
- Hunting the Known Unknown: Supply Chain Attack Detection with JA3/s**: A card for Hunting the Known Unknown: Supply Chain Attack Detection, featuring a background image of metal bolts and nuts, a green "Enrolled" button, and a description: "Hunting the Known Unknown: Supply Chain Attack Detection with JA3/s".
- Investigating Ransomware with Splunk**: A card for Investigating Ransomware with Splunk, featuring a screenshot of a Windows desktop with multiple command-line windows, a green "Enrolled" button, and a description: "Investigating Ransomware with Splunk".

Splunk Community

<https://community.splunk.com>

- Connect, learn, have fun, and find success with Splunk
- Ask questions, get answers, and find solutions from experts
- Meet in-person or virtually with like-minded enthusiasts
- Search for, vote on, or submit ideas for product enhancements

The screenshot shows the homepage of the Splunk Community website. At the top, there's a navigation bar with links for Community, Splunk Answers, News & Education, Community Lounge, Apps and Add-ons, User Groups, and Resources. A "Sign In" button is also visible. Below the navigation is a large banner featuring four diverse individuals cheering. To the right of the banner is a search bar with the placeholder "Search the community". Below the banner, a red bar displays statistics: 260K Members, 2,030 Online, and 147K Posts. The main content area has a light gray background. It includes a welcome message: "Welcome to the Splunk Community! Get started by visiting our [welcome hub](#) to learn more about the site. We're so glad you're here!" followed by a challenge notice: "Check out the Splunk Community Dashboard [Challenge](#) for a chance to win prizes". Below this, there are five cards with icons and descriptions: "Getting Started" (paper airplane icon), "Community Blog" (person icon), "Splunk Answers" (speech bubbles icon), "User Groups" (people icon), and "Office Hours" (building icon). Each card also has a brief description below its title.

Welcome to the Splunk Community! Get started by visiting our [welcome hub](#) to learn more about the site. We're so glad you're here!

Check out the Splunk Community Dashboard [Challenge](#) for a chance to win prizes

Getting Started
Learn more about the Splunk Community and how we can help

Community Blog
Community happenings, product announcements, and Splunk news

Splunk Answers
Troubleshoot problems with help from the community

User Groups
Meet up with other Splunk practitioners, virtually or in-person

Office Hours
Webinar-style deep dives and workshops for hands-on guidance

Splunk Events

<https://splunk.com/events>

- Expand your network and connect with the global and local Splunk community



<https://conf.splunk.com>

- Join us at .conf!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!

The screenshot shows the Splunk Events page. At the top, there's a navigation bar with links for Products, Solutions, Why Splunk?, Resources, Company, Support, a search icon, a globe icon, a user icon, and a 'Free Splunk' button. Below the navigation is a section titled 'Splunk Events' with the subtext: 'Join us at an event near you to gain new skills, expand your network and connect with the Splunk Community.' On the left, there's a sidebar with a search bar, a 'Filter all' button (set to '28 Results'), and dropdown menus for 'Regions', 'Event Types', and 'Solutions'. The main content area is divided into two sections: 'Featured Events' and 'Upcoming Events'.
Featured Events:

- Black Hat USA 2024**
INDUSTRY EVENT
LAS VEGAS
AUG 03, 2024 - AUG 08, 2024
[Register Now >](#)
- Gartner IT Symposium/Xpo**
INDUSTRY EVENT
ORLANDO
OCT 21, 2024 - OCT 24, 2024
[Register Now >](#)
- AWS re:Invent 2024**
INDUSTRY EVENT
LAS VEGAS
DEC 01, 2024 - DEC 06, 2024
[Register Now >](#)

Upcoming Events:

Documentation

<https://docs.splunk.com>

- Search reference for SPL

- Step-by-step tutorials

Search:

<https://splk.it/SplunkSearchTutorial>

Dashboard Studio:

<https://splk.it/SplunkDashStudioTutorial>

- Product references

- Procedures/guides

- And more!



Products ▾ Solutions ▾ Why Splunk? ▾ Resources ▾ Splexicon

Support ▾



Documentation

Q Search in docs

[Splexicon](#) the Splunk glossary



Platform

Splunk Cloud Platform™
Splunk® Enterprise
Splunk® Universal Forwarder
Splunk® Data Stream Processor
Splunk® Cloud Services



Security

Splunk® Attack Analyzer
Splunk® Asset and Risk Intelligence
Splunk® Enterprise Security
Splunk® Mission Control
Splunk® SOAR (Cloud)
Splunk® SOAR (On-premises)
Splunk® User Behavior Analytics
Splunk® Security Essentials
Splunk® Security Content
[Show more ▾](#)



IT

IT Operations Overview
Splunk® IT Service Intelligence
Splunk® IT Essentials Work
Splunk® IT Essentials Learn
Splunk® App for Content Packs
Splunk® On-Call



Observability

Splunk® Observability Cloud
Splunk® Infrastructure Monitoring
Splunk® APM
Splunk® Log Observer Connect
Splunk® Real User Monitoring
Splunk® Synthetic Monitoring



Apps and add-ons

Splunk® Supported Add-ons
Splunk® OpenTelemetry Collector for Kubernetes
Splunk® Add-on for OpenTelemetry Collector
Splunk® Add-on Builder
Splunk® Firehose Nozzle for VMware Tanzu
Splunk® Connect for Kafka
Splunk® Connect for Zoom
[Splunk® Connected Experiences](#)



Developer tools

Splunk® Add-on Builder
Splunk® SDKs
Splunk® Web Framework

Splunk Lantern

<https://lantern.splunk.com>

- Use case library
- Product tips
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to increase the value of Splunk across your organisation

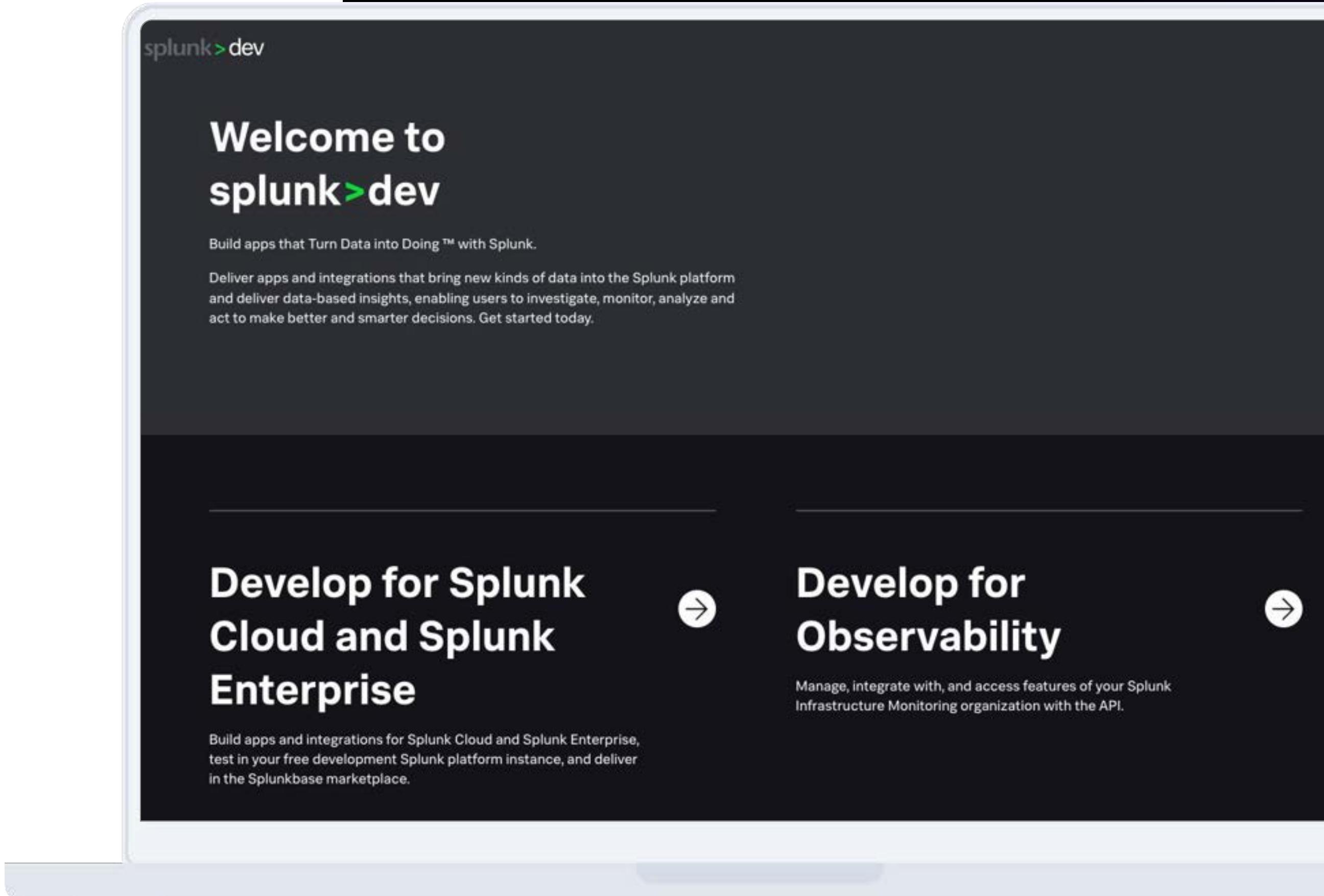
The screenshot shows the Splunk Lantern Customer Success Center homepage. At the top, there's a navigation bar with the Splunk logo, a CISCO company badge, "Lantern Home", and links for Documentation, Community, Training & Certification, Support Portal, User Groups, and a user icon. On the far right, a "Free Splunk" button is visible. The main header is "Splunk Lantern Customer Success Center". Below it, a sub-header reads: "Let Splunk experts light your path toward gaining valuable data insights, achieving your key use cases, and managing Splunk more efficiently." A call-to-action link "Click here to learn more." is present. To the right is a large graphic featuring a lantern icon inside a circle, set against a background of overlapping colored bands (pink, red, orange). A search bar is located below the main header. The page content is organized into three columns of featured articles:

FEATURED: SPLUNK APM	FEATURED: EDGE PROCESSOR	FEATURED: MISSION CONTROL
Monitoring applications using OpenAI API and GPT models with OpenTelemetry and Splunk APM By leveraging OpenTelemetry and Splunk Application Performance Monitoring, you can gain valuable insights into the performance of an AI assistant application and the effectiveness of different GPT models. The integration provides a comprehensive monitoring solution that ensures your application's	Scaling Edge Processor infrastructure There are a number of factors that can affect the required scale of your Splunk Edge Processor infrastructure, including changes in data volume, use cases, and pipeline complexity. This article series looks at scaling Splunk Edge Processor using Amazon EKS.	Enhancing endpoint monitoring with threat intelligence When investigating endpoints, SOC analysts need as much telemetry as possible because there are often many attack vectors in play. Using Splunk Mission Control or Splunk Enterprise Security provides you the most flexibility for configuring many threat intelligence sources to get you the information you need.

Developer Resources

<https://dev.splunk.com>

- Developer Guide
- API Reference
- Tutorials
- Downloads
APIs, libraries, tools
- Code examples
- Free Developer licence



Splunk Apps & Add-ons

<https://splunkbase.splunk.com>

- 2100+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!

The screenshot shows the Splunkbase homepage with a dark background. At the top, there's a navigation bar with the 'splunkbase' logo, 'Collections', 'Apps', 'Submit an App', and 'Log In' buttons. Below the navigation, a large white text box contains the slogan 'Get more out of Splunk with applications'. A search bar with the placeholder 'Search for apps' is positioned below the slogan. To the right of the search bar is a graphic of several colorful 3D-style app icons floating over a gradient background of orange and red. Below this graphic, a section titled 'Trending Apps on Splunkbase' displays four app cards. Each card includes the app icon, name, developer, rating, and a brief description. The cards are:

- Splunk Add-on for Microsoft Windows** By Splunk Inc. Rating: ★★★★☆ (45) Description: *** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on f... Platform: Splunk Enterprise, Splunk Cloud...
Rating: ★★★★☆ (45)
- Splunk DB Connect** By Splunk Inc. Rating: ★★★★☆ (132) Description: Splunk DB Connect is a generic SQL database extension for Splunk that enables easy integration of database... Platform: Splunk Enterprise, Splunk Cloud...
Rating: ★★★★☆ (132)
- Splunk Add-on for Unix and Linux** By Splunk Inc. Rating: ★★★★☆ (52) Description: *** Important: Read upgrade Instructions and test add-on update before deploying to production *** There are changes to... Platform: Splunk Enterprise, Splunk Cloud...
Rating: ★★★★☆ (52)
- Splunk Enterprise Security** By Splunk Inc. Rating: ★★★★★ (216) Description: Splunk Enterprise Security (ES) solves a wide range of security analytics and operations use cases including... Platform: Splunk Enterprise, Splunk Cloud
Rating: ★★★★★ (216)

Training & Certification

<https://splunk.com/training>

- **Online education classes**
Instructor-led and self-paced eLearning
- **Certification tracks for different roles**
User, Power User, Admin, Architect and Developer
- **Splunk Education Rewards**
Complete training and receive points that you can redeem for Splunk swag!
- **Free education!**
Single-subject eLearning courses to kick start your Splunk learning

The screenshot shows the Splunk Course Catalog page. At the top, there's a navigation bar with links for Products, Solutions, Why Splunk?, Resources, Company, Support, a search icon, and user icons. Below the navigation is a secondary navigation bar with links for Training & Certification, Learning Paths, Course Catalog (which is highlighted in pink), Free Training, Certification, Partnerships, and Learning Rewards. The main heading is "Course Catalog". Below it, a sub-headline reads: "See all of the courses available to help you turn data into doing, shown in recommended order. Expand your knowledge and understanding of Splunk." A "Start Your Journey" button is located below this text. To the right, there's a photograph of three people (two women and one man) smiling and interacting. One woman is holding a tablet displaying a course dashboard. Below the photo, there's a search bar and a "Filter Courses" section with dropdown menus for Content Type, Certification, and Role, each showing 119 Results and a "Clear All" link. Three course cards are visible: "Intro to Splunk" (eLearning course for power users to learn how to use Splunk to create reports and dashboards), "Using Fields" (three-hour course for power users to learn about fields and how to use them in searches), and "Scheduling Reports & Alerts" (eLearning course for students to learn how to use scheduled reports and alerts to automate processes). The footer of the page is dark blue.

Thank you



Appendix

Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



Public or private cloud

On-premise

Searches are run on **Splunk Search Heads**



(Scalable)

- Distribute searches to Indexers
- Can be clustered (active-active)

Data is processed on **Splunk Indexers**



(Scalable)

- Receive and store raw data
- Data is analysed and indexed
- Can be clustered (active-active)

Collect data using a variety of data collection methods, such as **Splunk Forwarders**



Wire Data



API



SDKs



HEC



HTTP



TCP/UDP



RDBMS



Containers



Apps



Cloud Services



OpenTelemetry



Splunk Forwarders

- Collect/monitor and forward data to Indexers
- Collection options for a variety of data sources

Apps and Add-ons

- 2100+ free apps and add-ons available from <https://splunkbase.splunk.com/>
- Built either by Splunk, our technology partners or members of our user community
- Prebuilt packages that help to enhance and extend the Splunk platform
- Provide content and capabilities – such as reports, dashboards and integrations – for a specific technology, purpose or use case, with the flexibility to customise for your own needs



Apps

Content designed to bring fast time-to-value from your data in Splunk, including pre-built **dashboards, reports, alerts, visualisations and workflows**



Add-ons

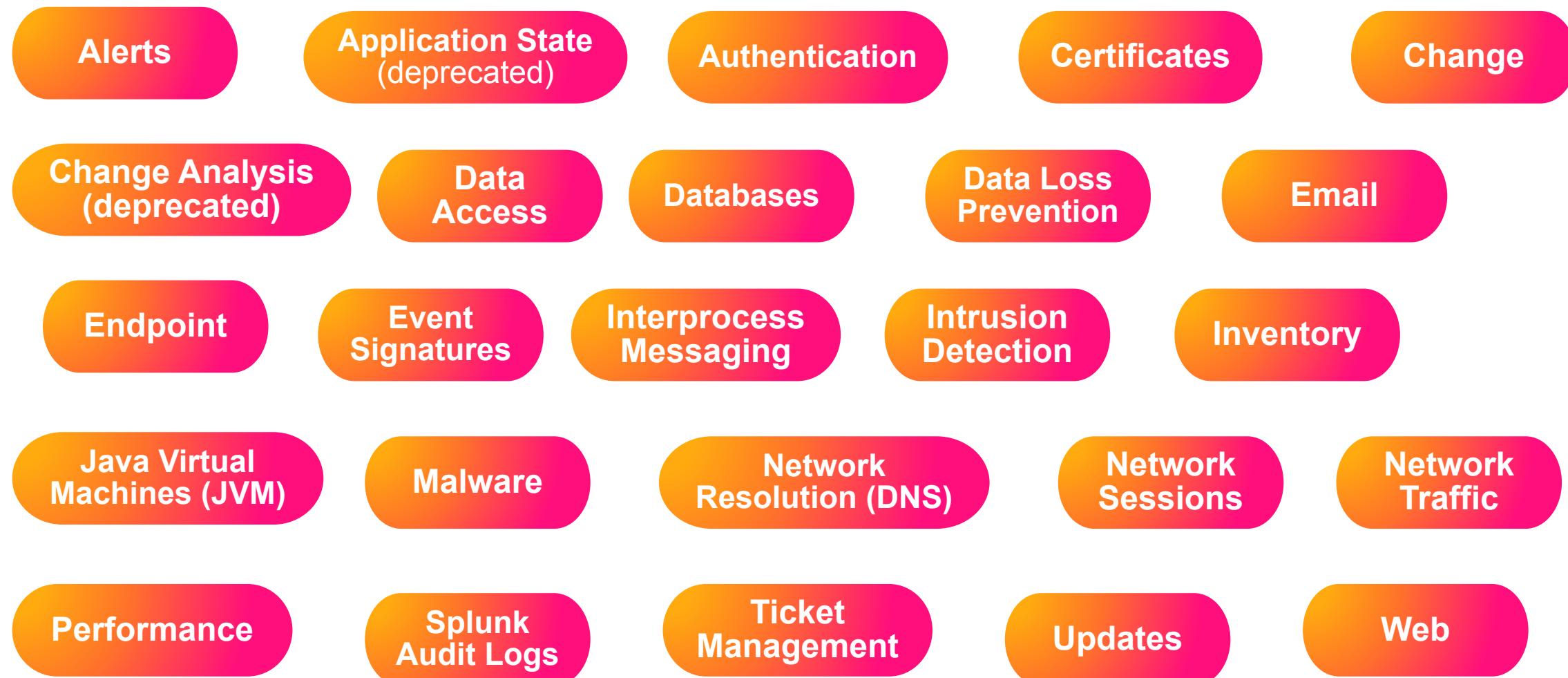
Provide specific capabilities to Splunk, such as **getting data in, mapping data, or providing saved searches and macros**

List of Data Models in the CIM Add-On

Free Splunk Add-On

JSON implementations of the data models in:

\$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/default/data/models



Splunk Common
Information Model
(CIM)

Refer to: <https://docs.splunk.com/Documentation/CIM/5.3.1/User/CIMfields>