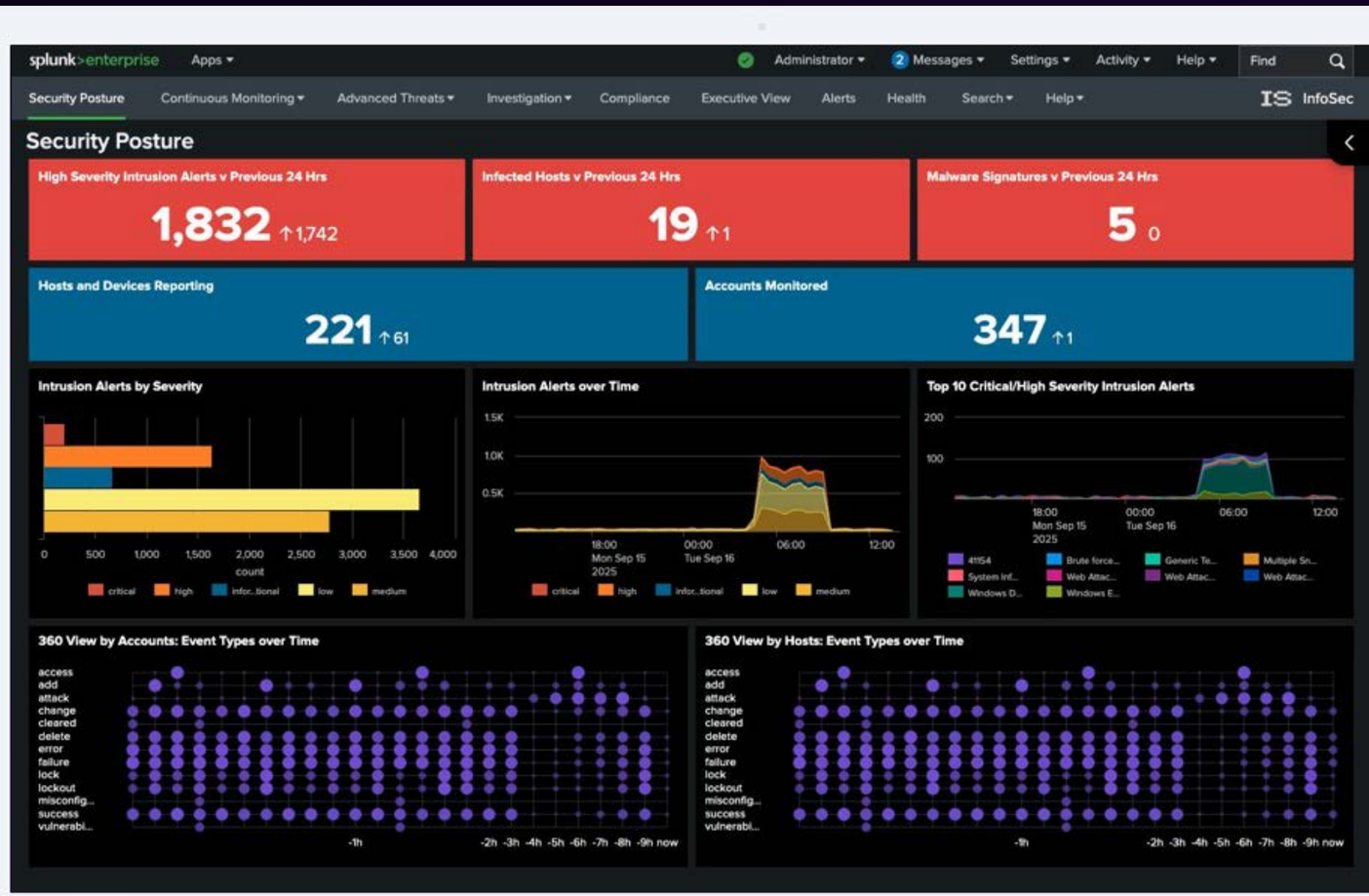
InfoSec App for Splunk

Hands-On Workshop



splunk>
a CISCO company

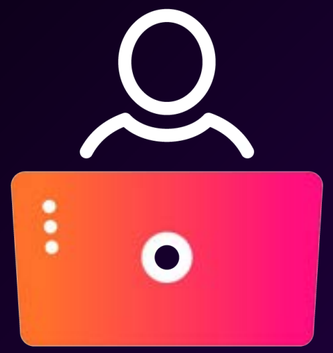
Forward-looking statements

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>
a CISCO company

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

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

FREE Splunk Security Essentials

FREE InfoSec App for Splunk

Foundational Visibility

See across environments

Search, monitor and investigate for real-time security monitoring

PAID Enterprise Security (SIEM)

FREE Machine Learning Toolkit

Guided Insights

Detect threats and issues with context

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

PAID Security Orchestration, Automation & Response (SOAR)

PAID Attack Analyzer

Proactive Response

Get ahead of issues

Accelerate incident investigations and response using automation

PAID User Behavior Analytics (UBA)

Unified Workflows

Collaborate seamlessly

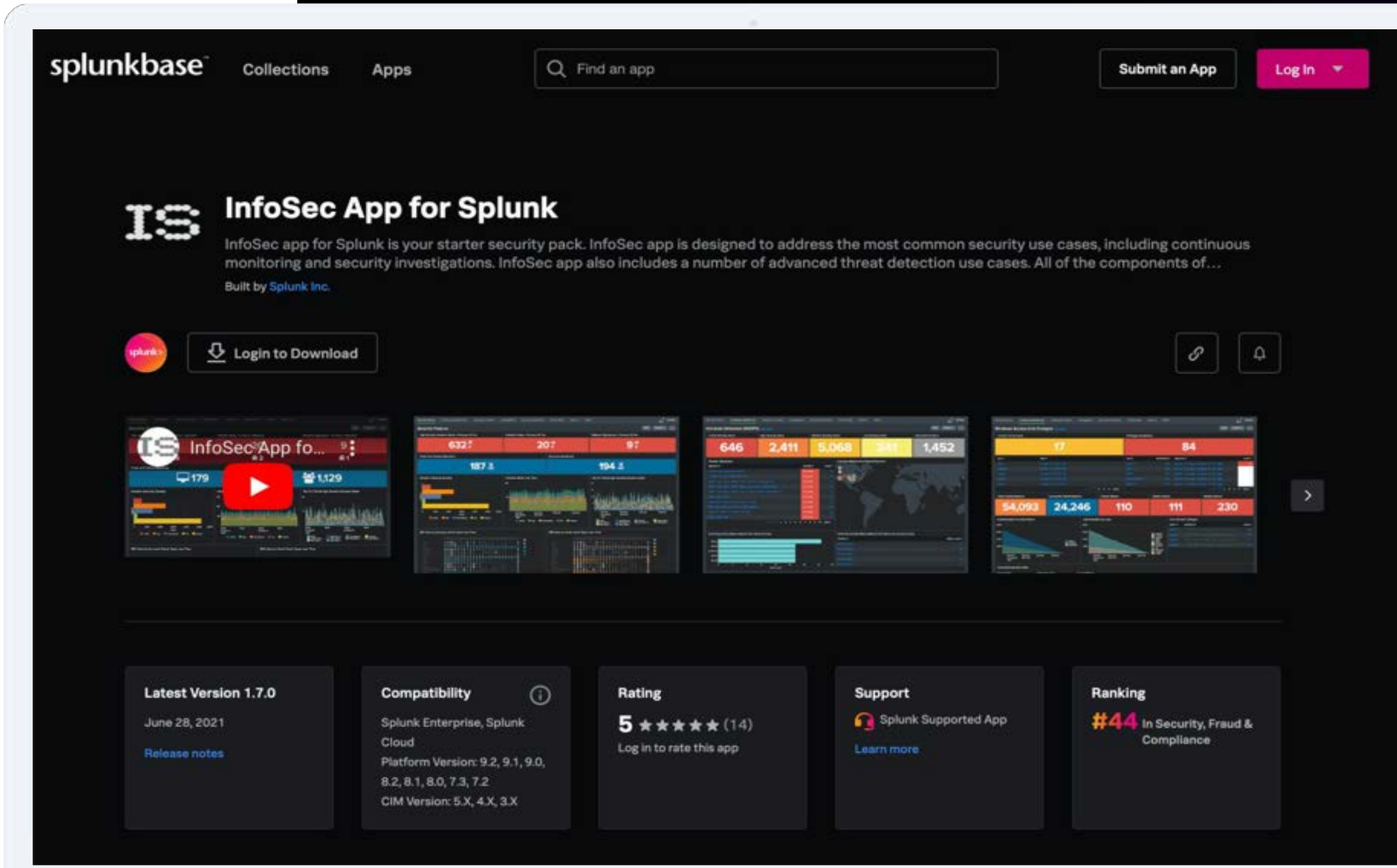
Maximize SOC efficiency with integrated threat detection, investigation and response

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

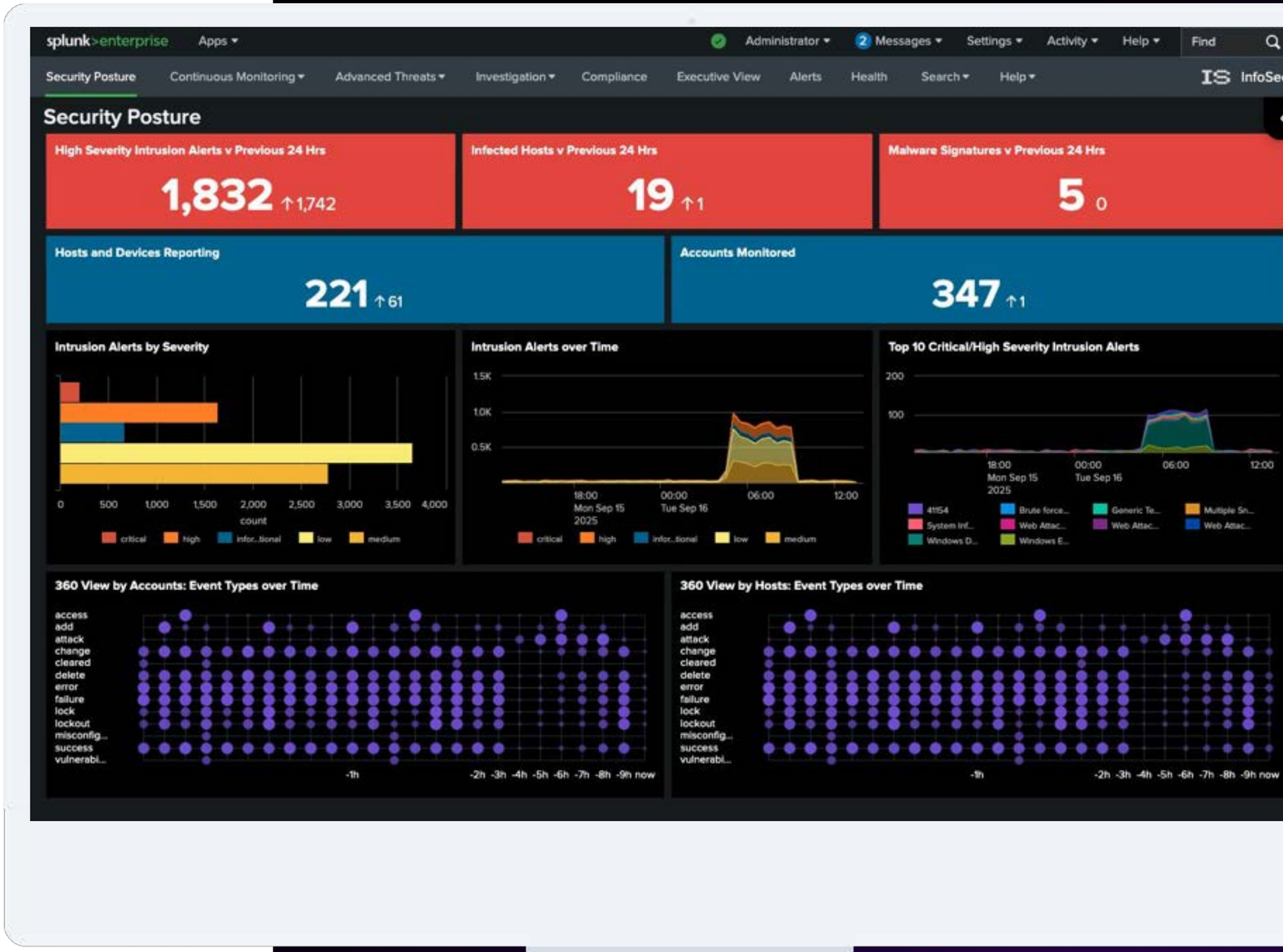


Learn more: https://docs.splunk.com/Documentation/InfoSec

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?

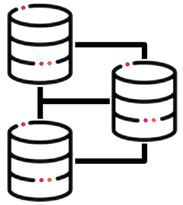
A data model is a search-time mapping of data into a hierarchical structure

- 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

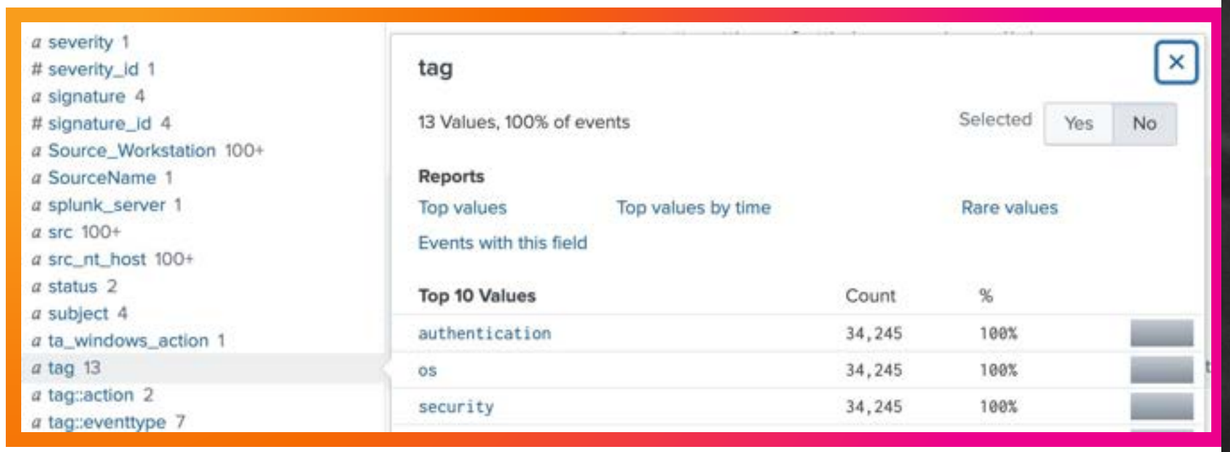
E.g. Create a “critical_error” tag for events that contain “error” and “high severity”. Then you can simply search for “tag=critical_error”

Learn More about Splunk Add-ons and the Common Information Model:
https://docs.splunk.com/Documentation/AddOns/released/Overview/Add-onsandCIM

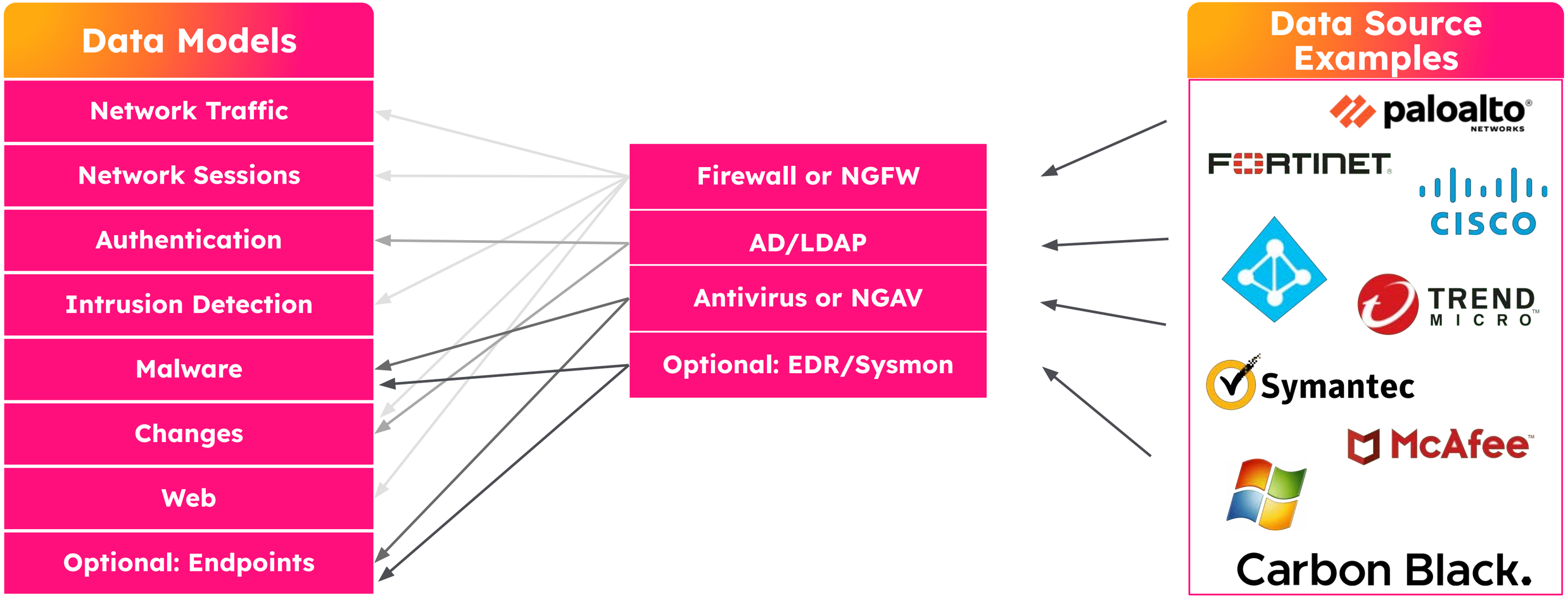
How do you ensure your data is CIM compliant?

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



InfoSec App Data Sources



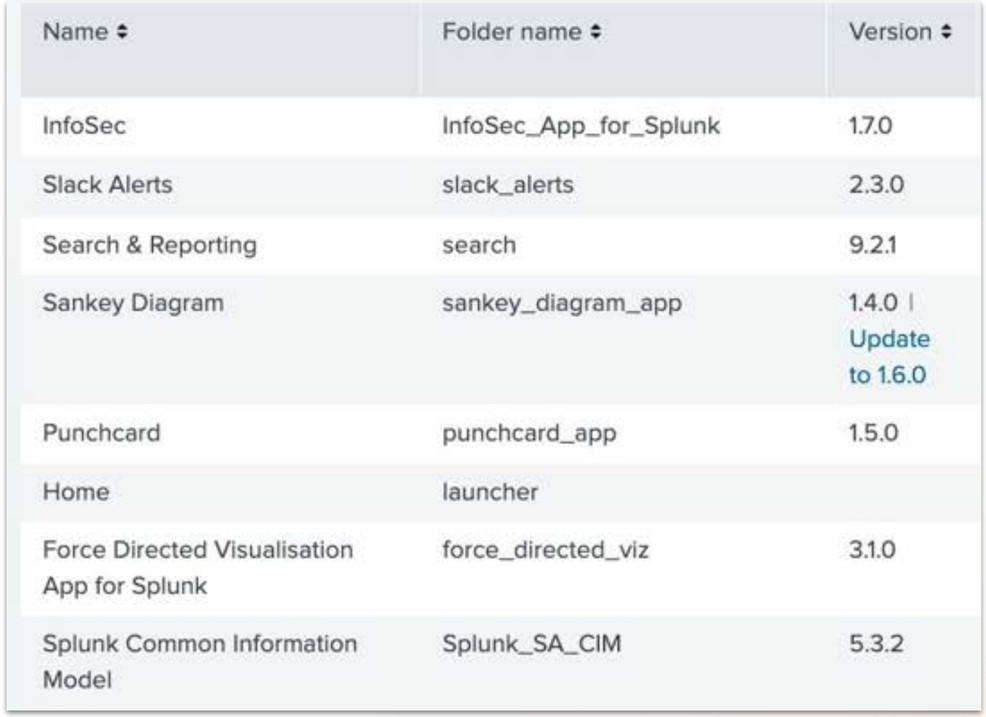
Splunk **Common Information Model** allows using **many other data sources** in the InfoSec App

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

BUTTERCUP STATE UNIVERSITY

Set Up the InfoSec App

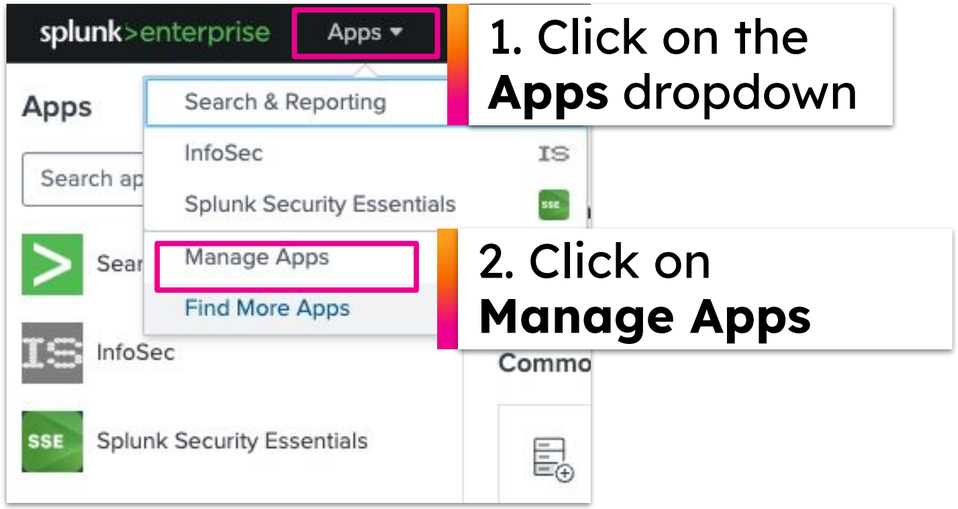
Install the Splunk Add-on for AWS and finish setting up the InfoSec App for Splunk

Tasks

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

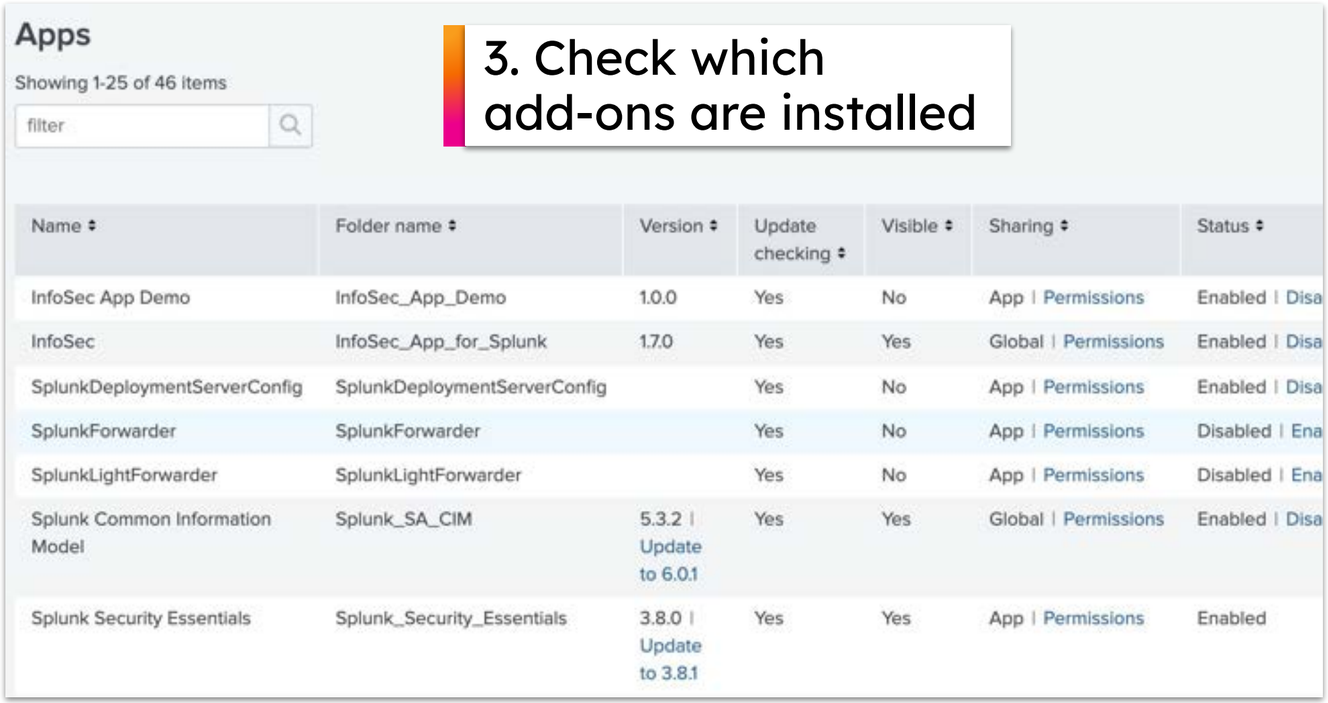
Check Which Add-ons are Installed

Via Splunk Web



1. Click on the **Apps** dropdown

2. Click on **Manage Apps**

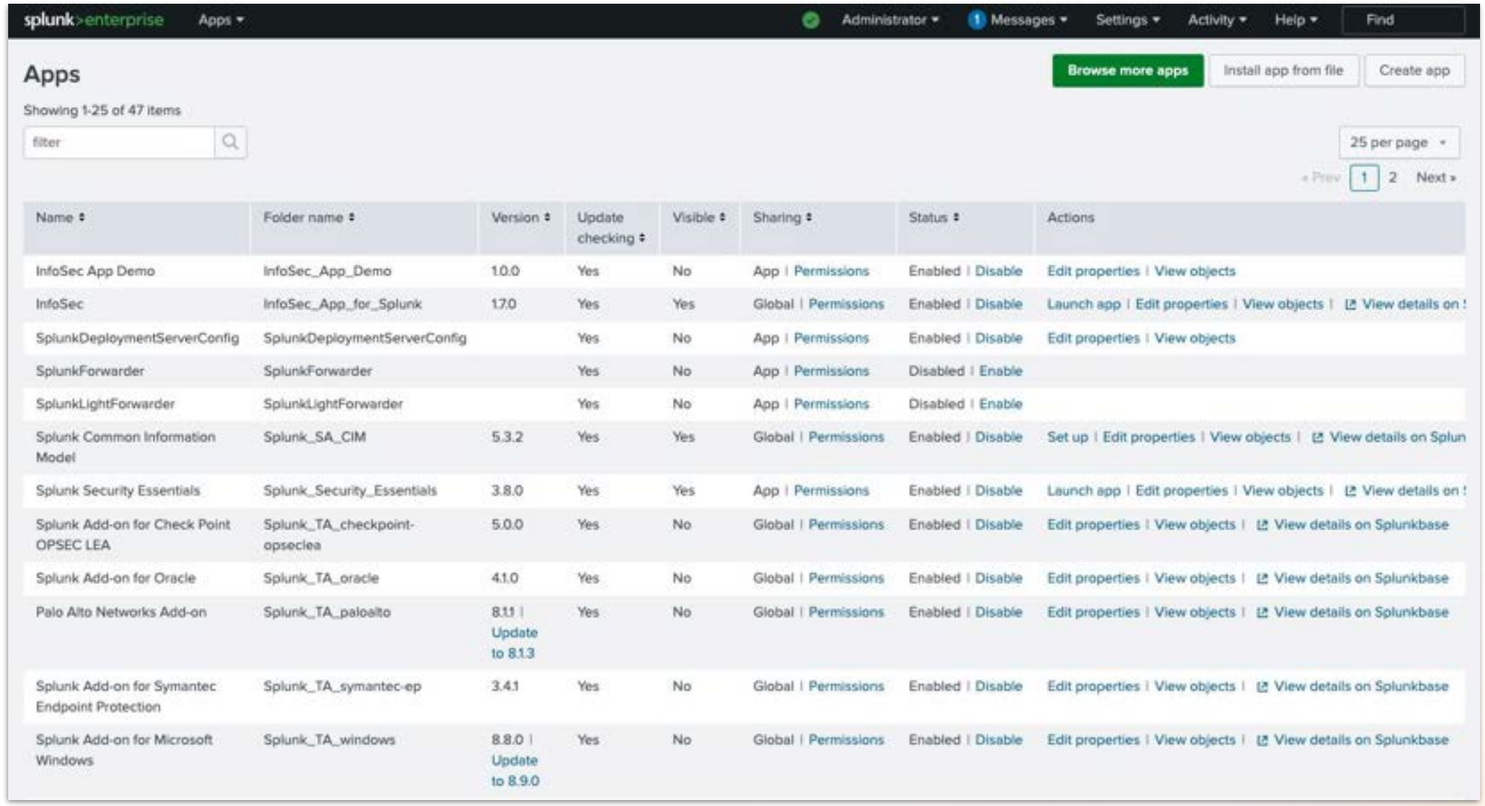


3. Check which add-ons are installed

TA Data Sources Mapped

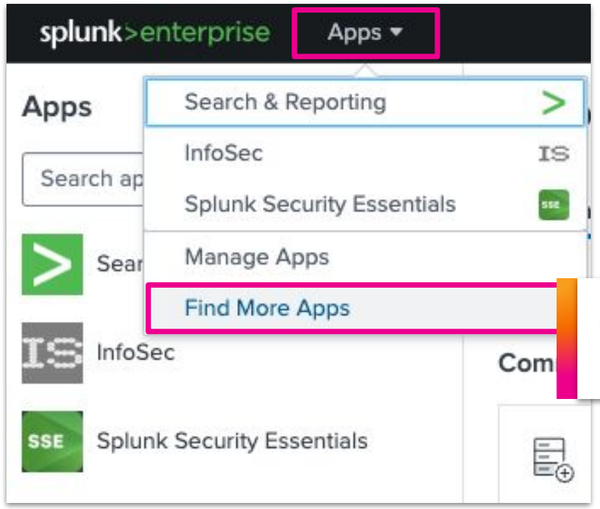
Looking at all the installed add-ons we notice that the Splunk Add-on for AWS is missing.

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.

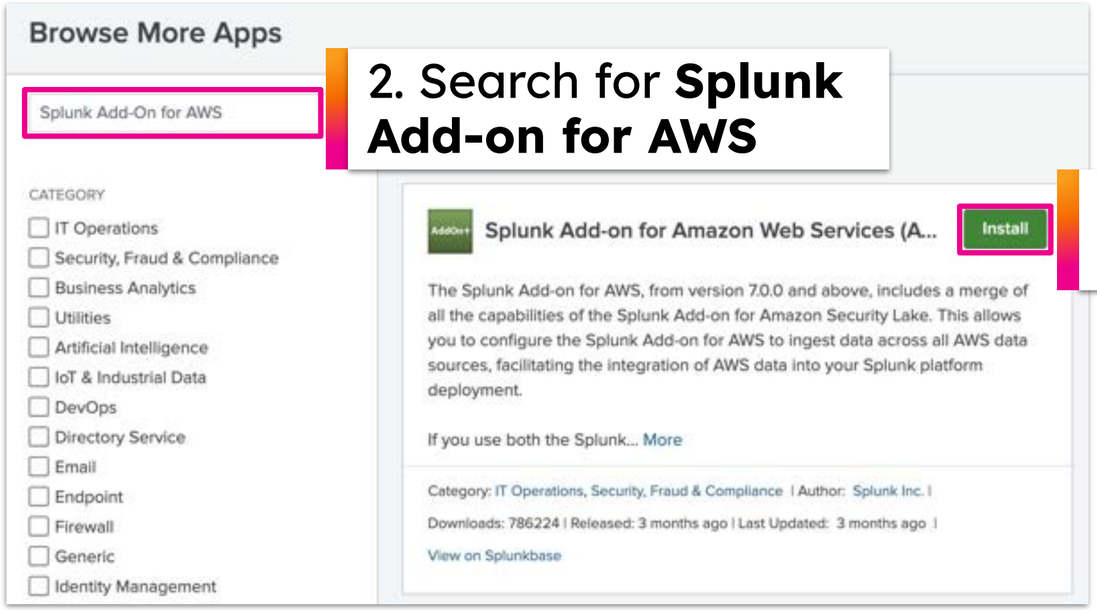


Install the Splunk Add-on for AWS

Via Splunk Web

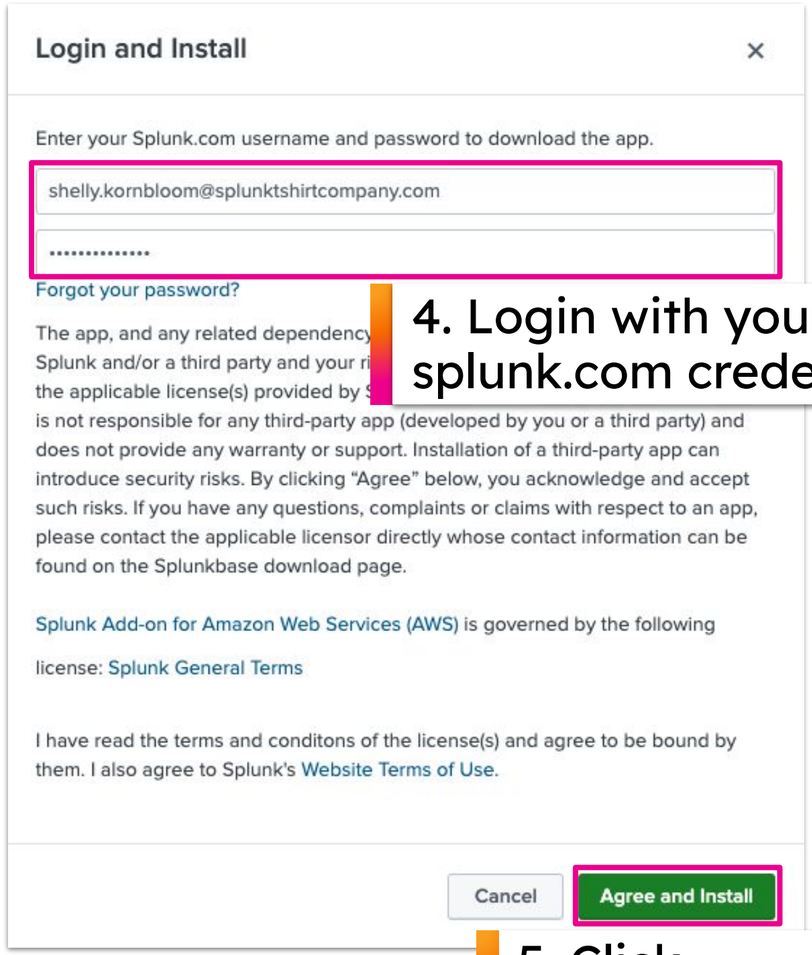


1. Click on **Apps** > **Find More Apps**



2. Search for **Splunk Add-on for AWS**

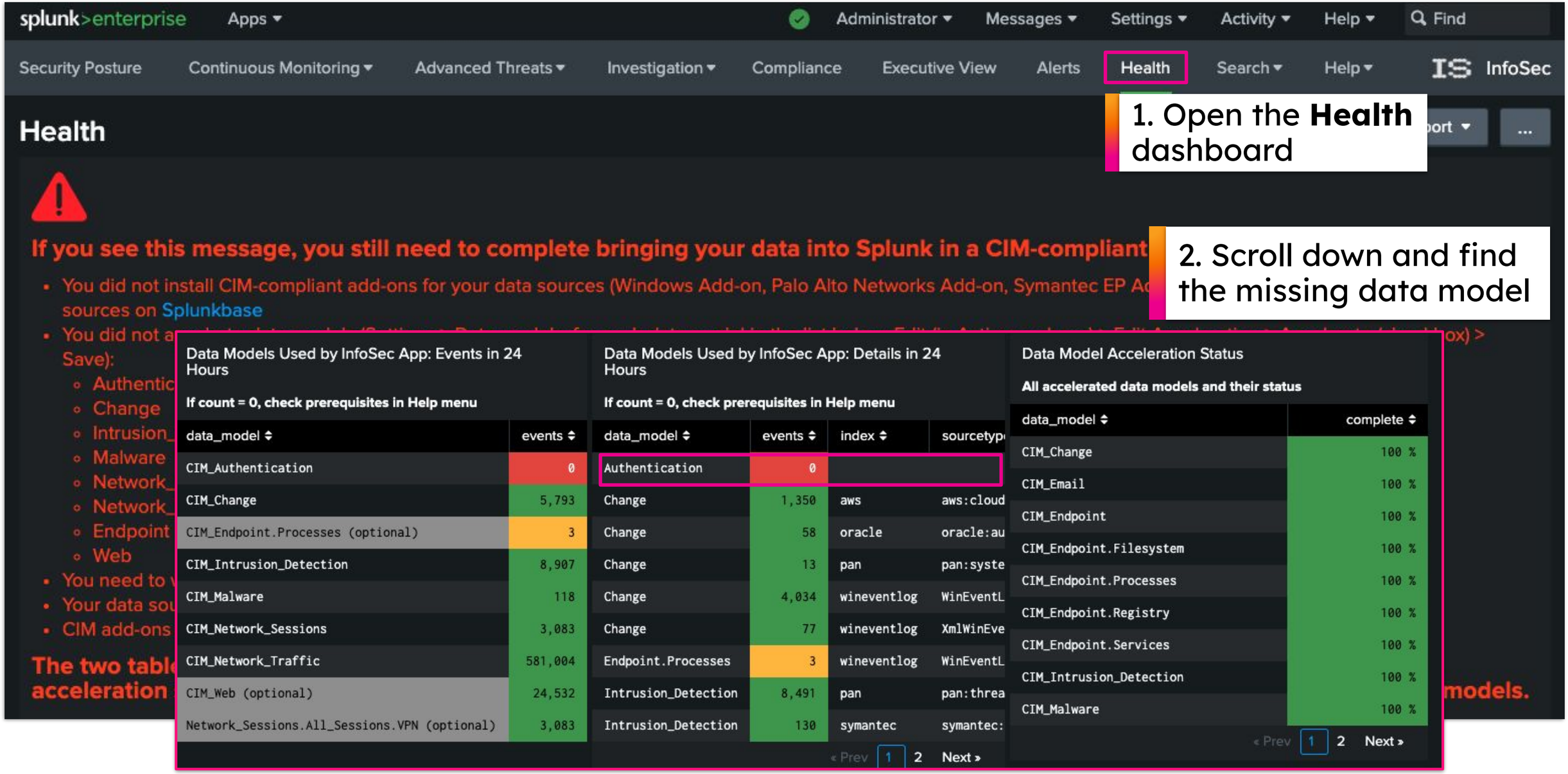
3. Click **Install**



4. Login with your splunk.com credentials

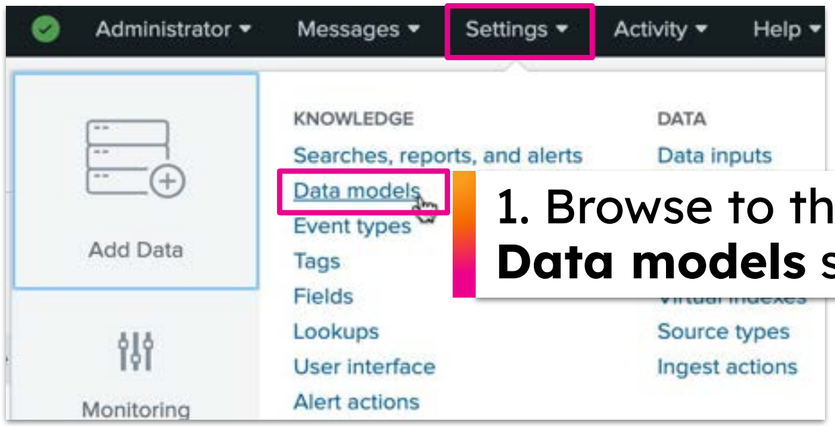
5. Click **Agree and Install**

Check the Health Dashboard in the InfoSec App

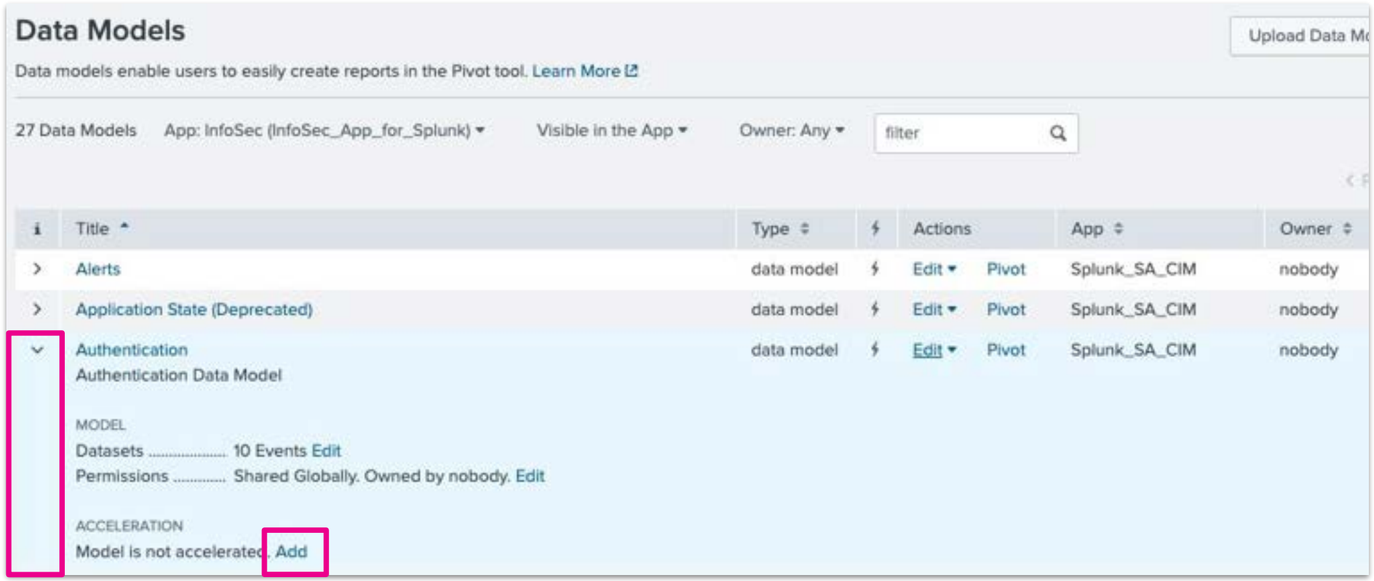


Accelerate the Authentication Data Model

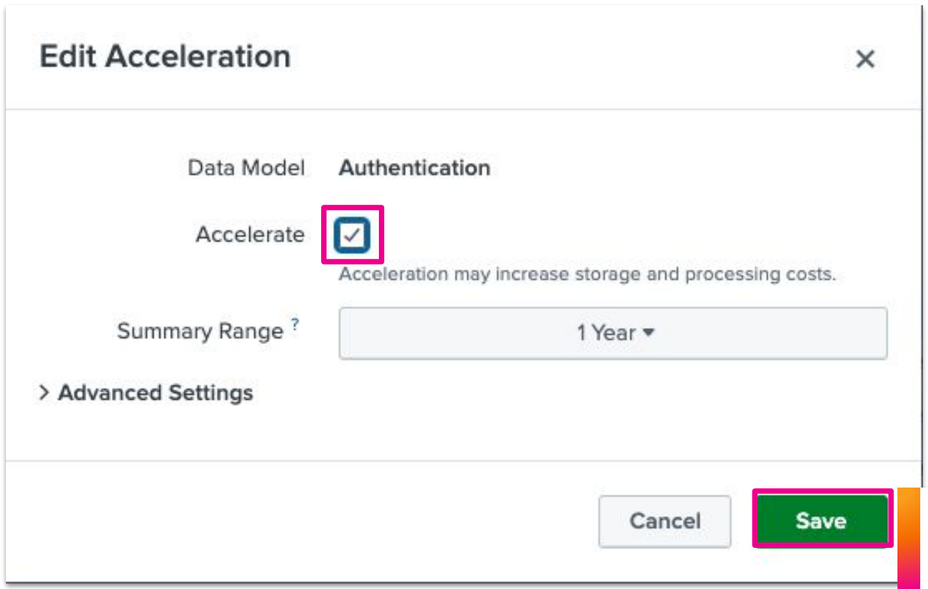
Edit the data model acceleration settings



1. Browse to the **Data models** settings



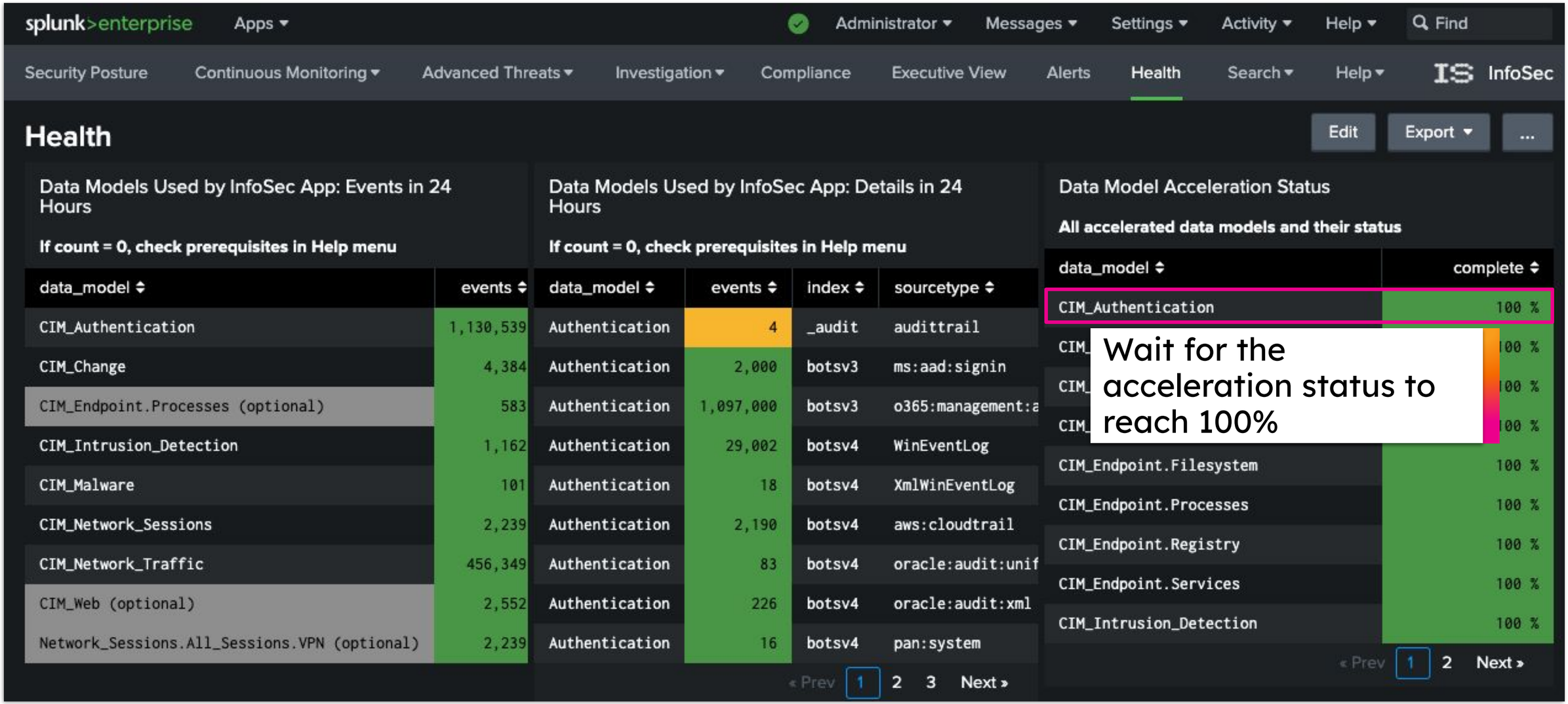
2. Expand the **Authentication** section and click **Add**



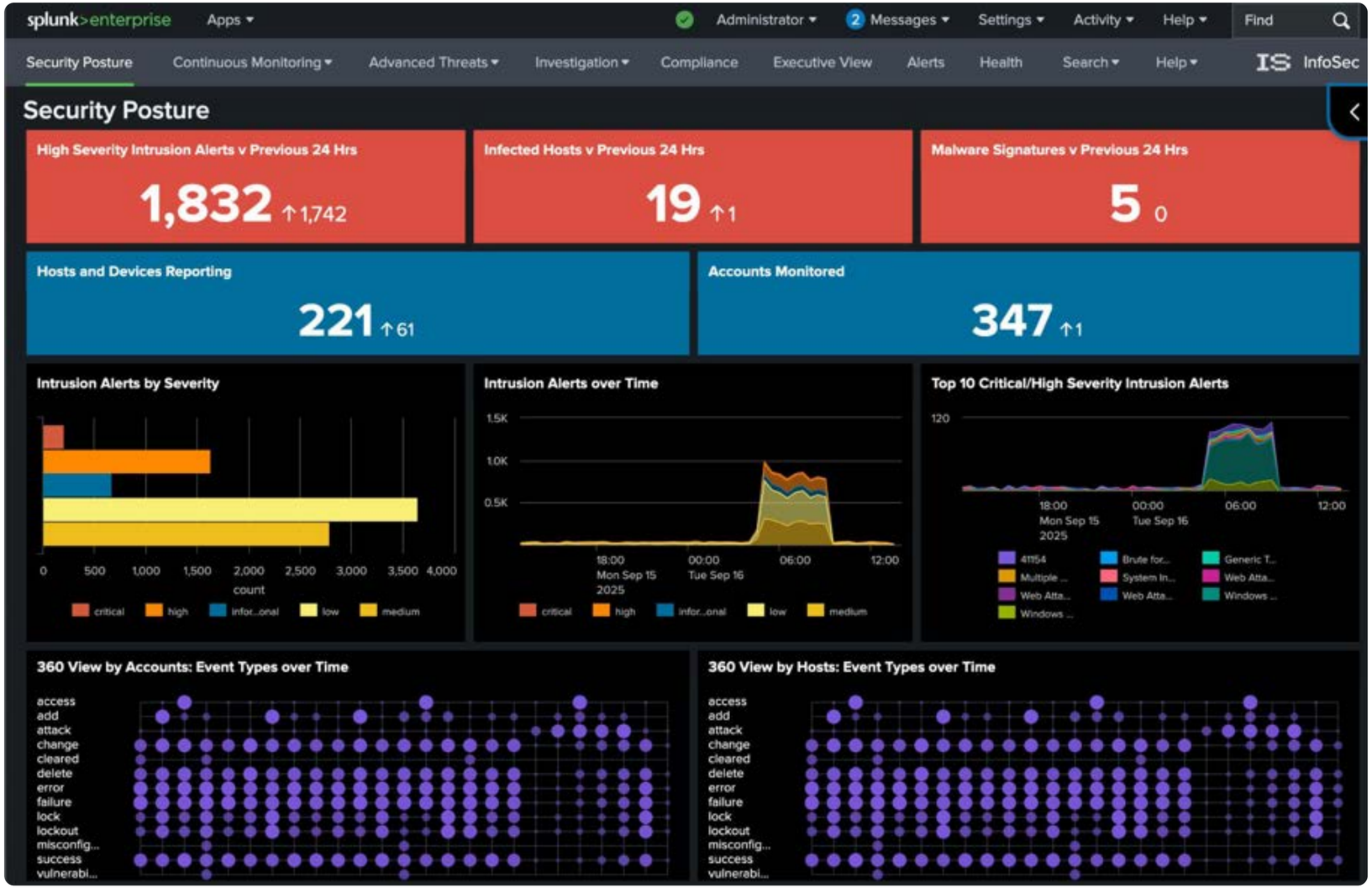
3. Check **Accelerate** and click **Save**

Check Health Dashboard in InfoSec App

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



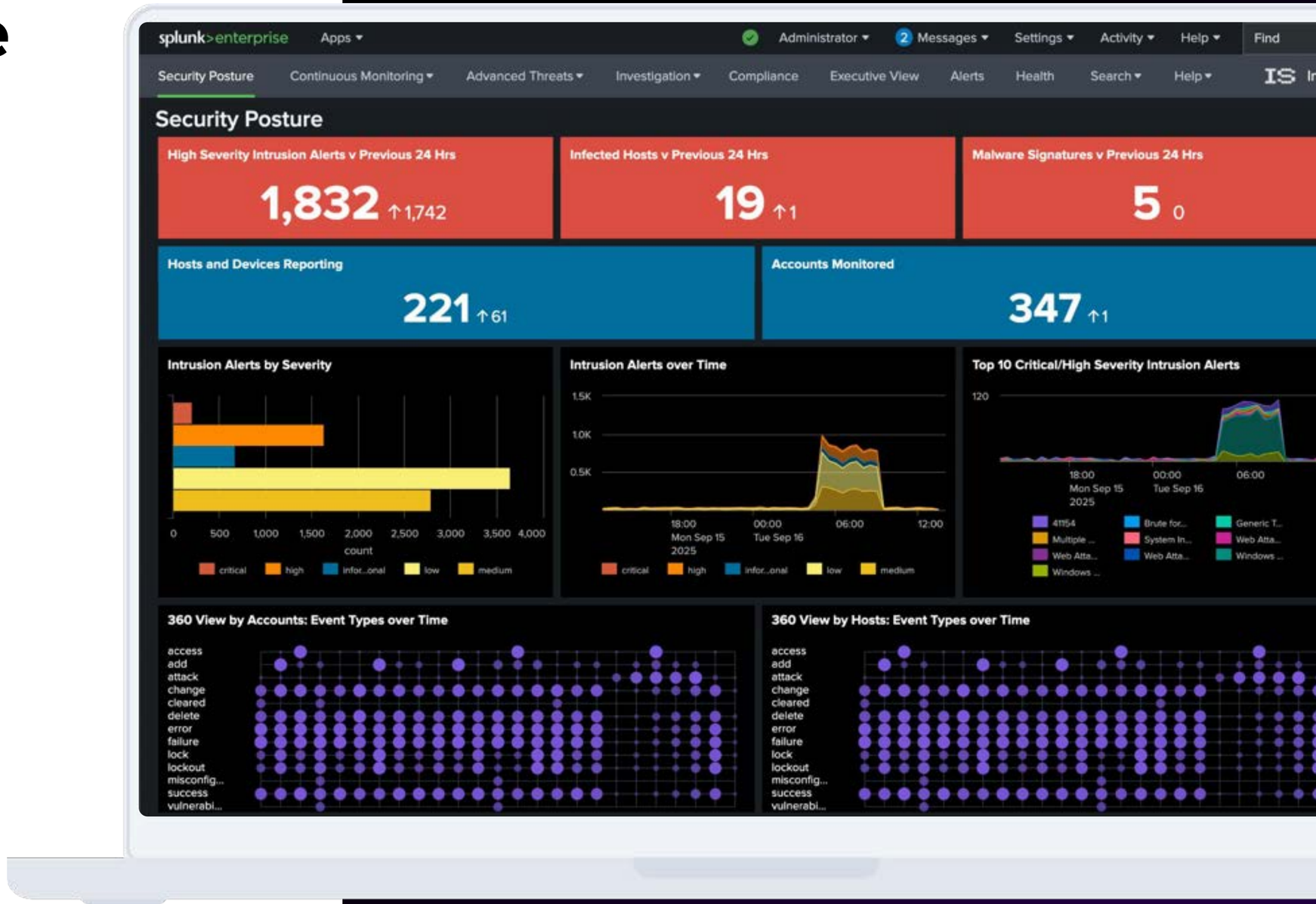
InfoSec App UI



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

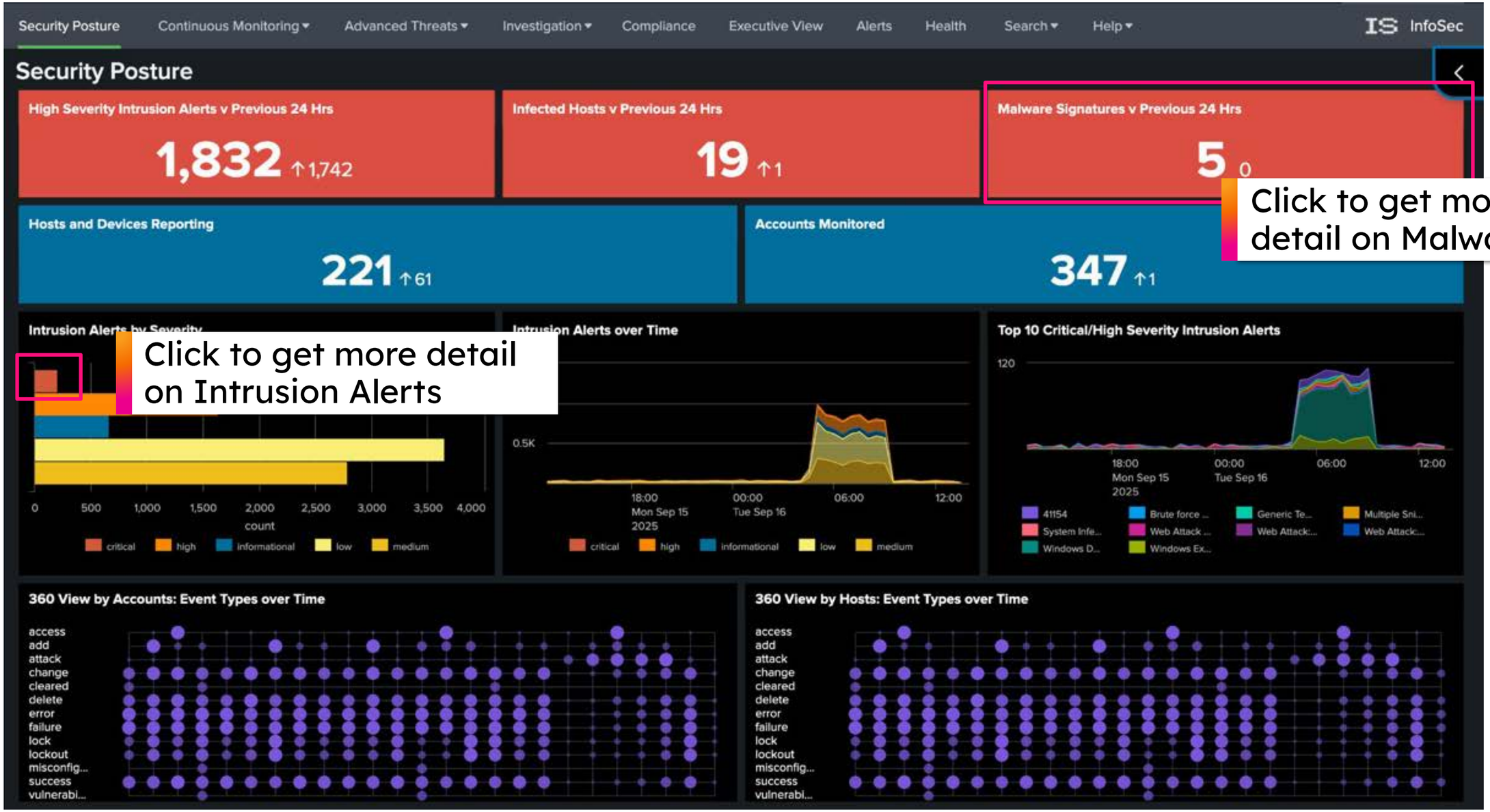
Leveraging drilldowns for data insights

Tasks

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

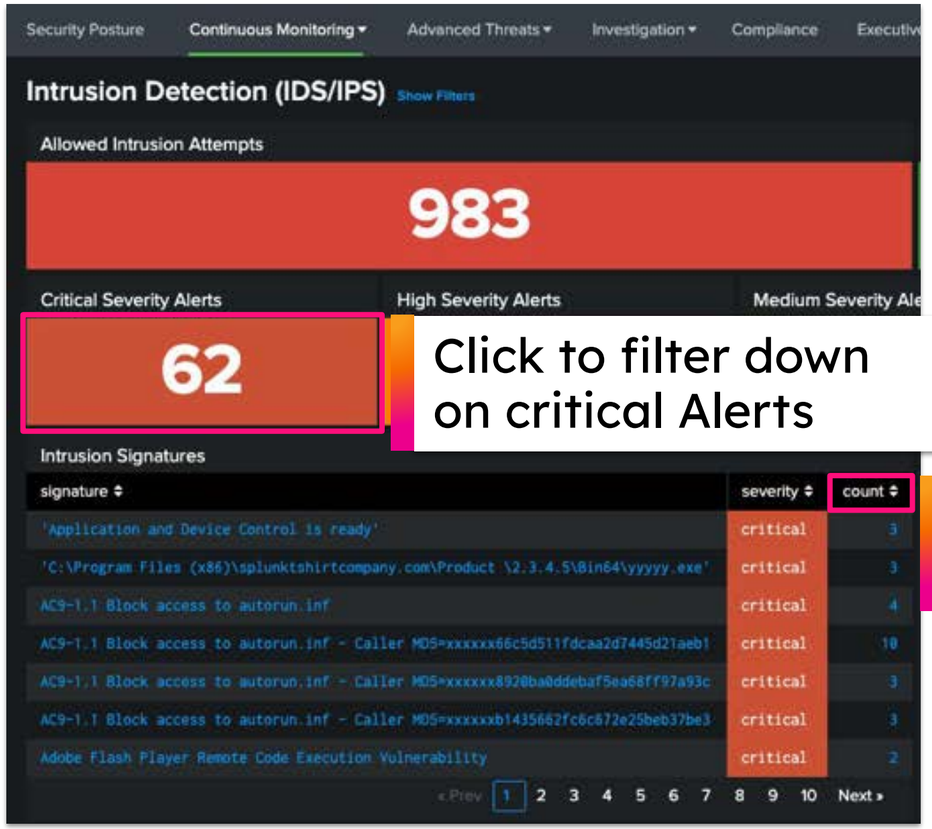
1. How many critical **Intrusion Alerts** are displayed?
   a. Drill down and filter on critical alerts
   b. What are the top 3 signatures?
2. How many **Malware** were detected in the last 24 hours?
   a. Which are the top 3?

Check Security Posture Dashboard



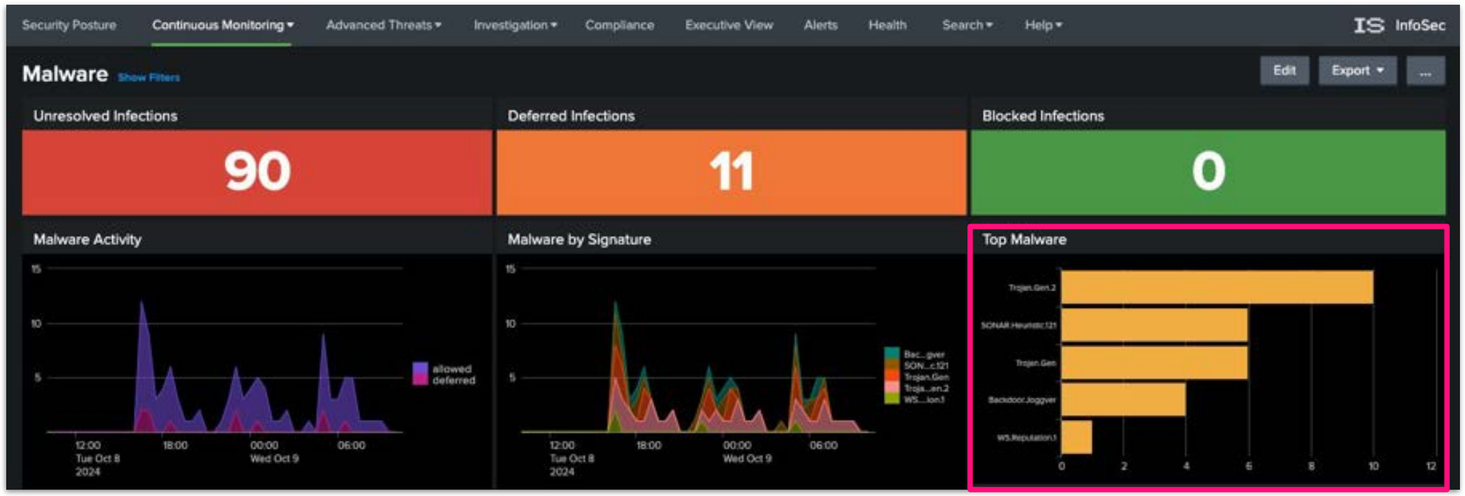
Click to get more detail on Malware

Click to get more detail on Intrusion Alerts



Click to filter down on critical Alerts

Click to sort from highest to lowest #



Find top 3 Malware here

Intrusion Detection (IDS/IPS)

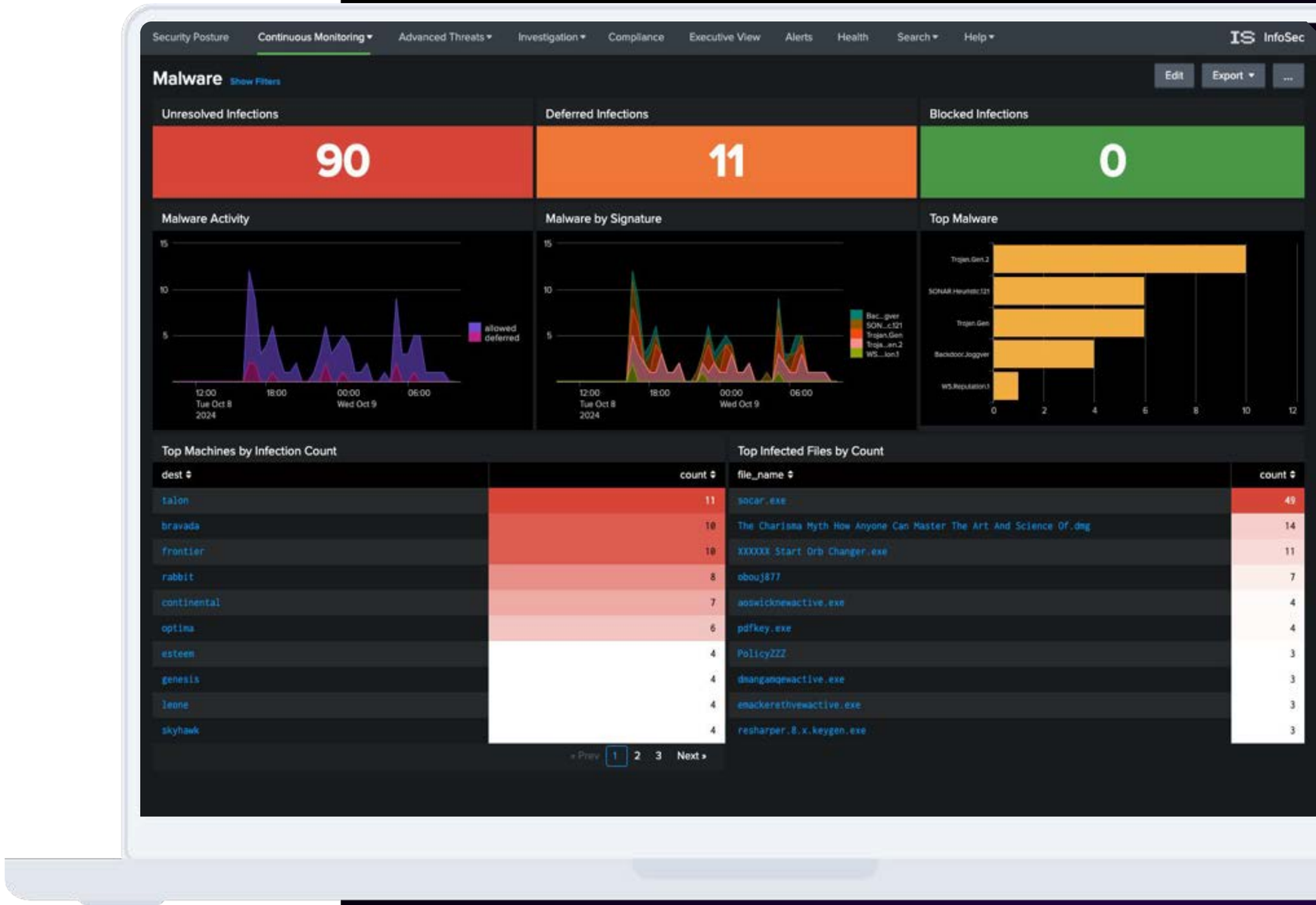
InfoSec App Dashboard

- 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

BUTTERCUP STATE UNIVERSITY

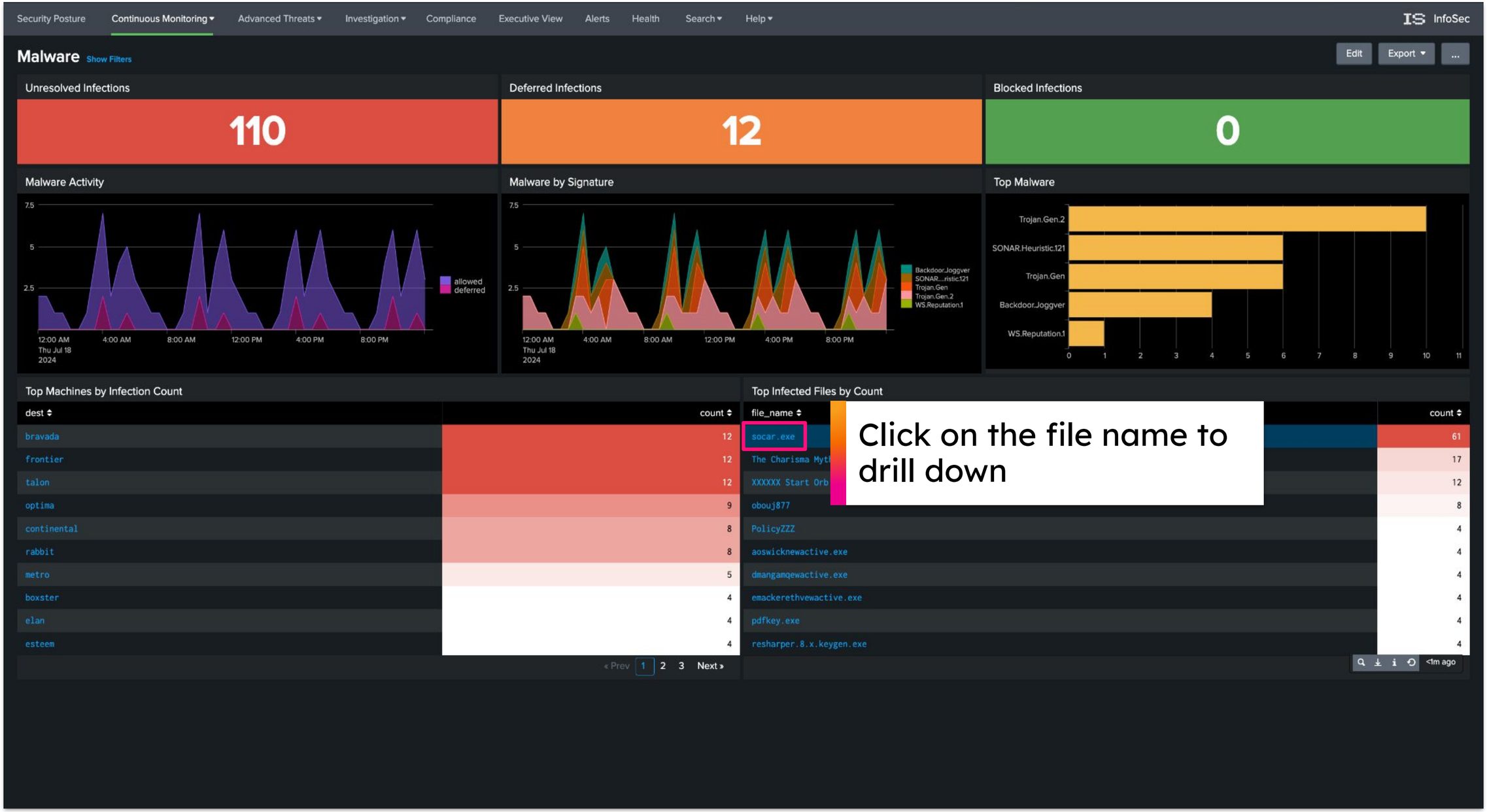
Malware Investigation

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

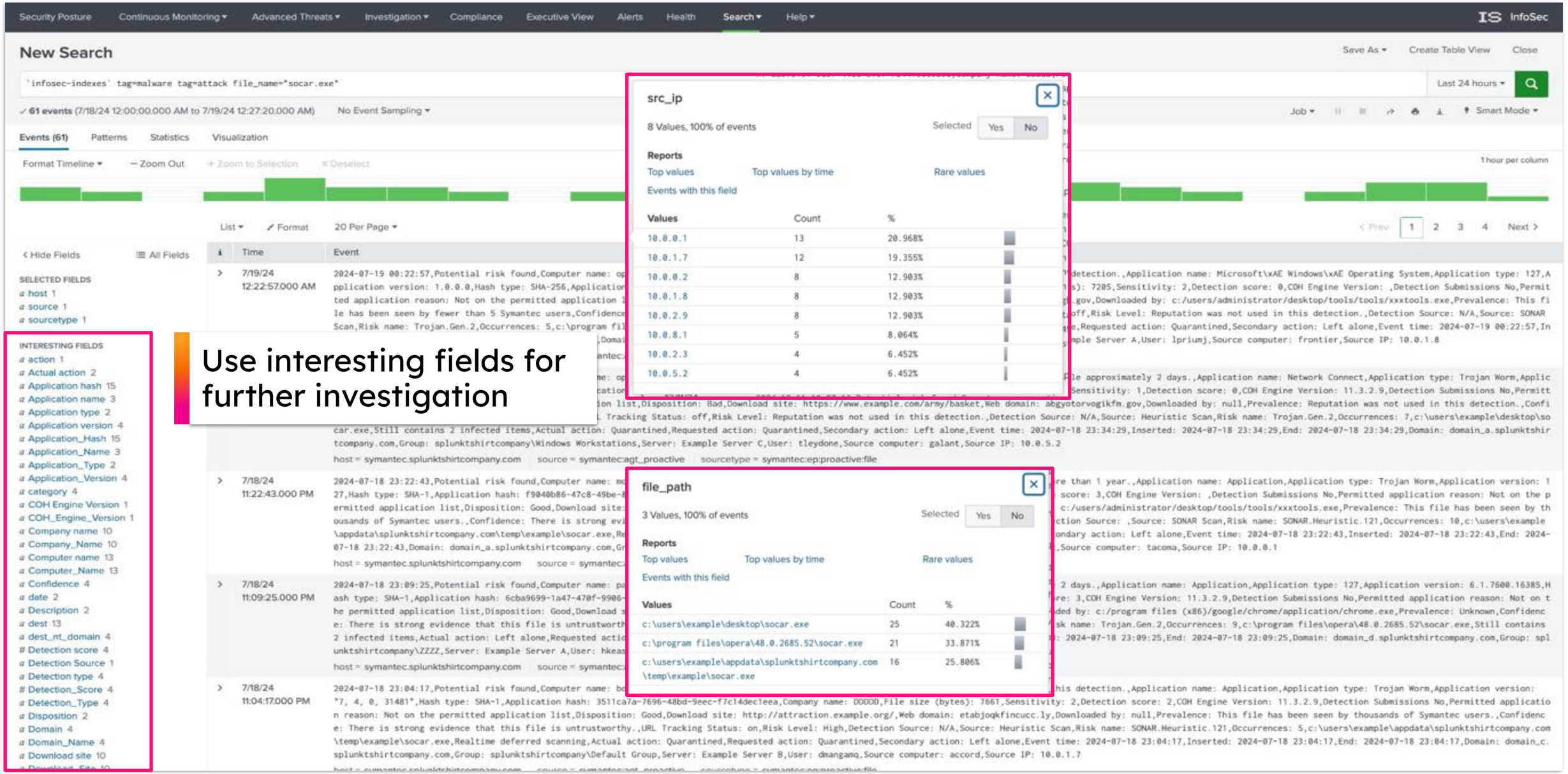
Tasks

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



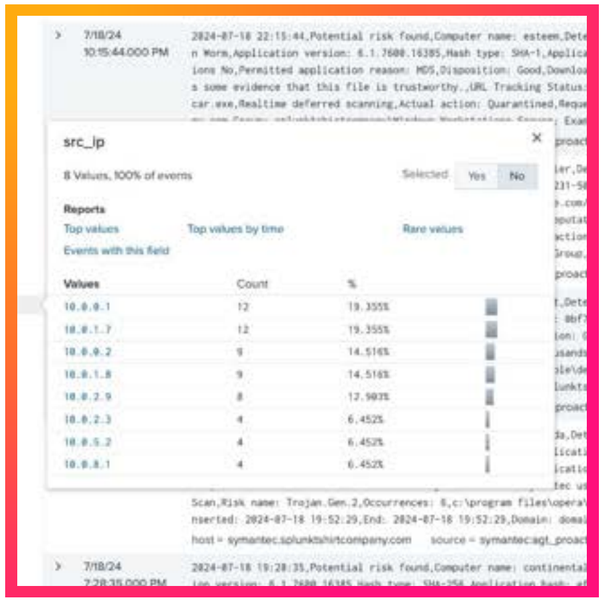
Investigate beyond the original panel



Use interesting fields for further investigation

Leveraging Interesting Fields

Interesting fields can help your investigating



src_ip

file_path

Alert when this infected files is seen again

Top Infected Files by Count

file_name	count
socar.exe	61
The Charisma Myth How Anyone Can Master The Art And Science Of.dmg	17
XXXXXX Start Orb Changer.exe	12
obouj877	8
PolicyZZZ	4
aoswicknewactive.exe	4
dmangamqewactive.exe	4
emackerethvewactive.exe	4
pdfkey.exe	4
resharper.8.x.keygen.exe	4

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
```

2. Add a filter for `file_name = socar.exe`

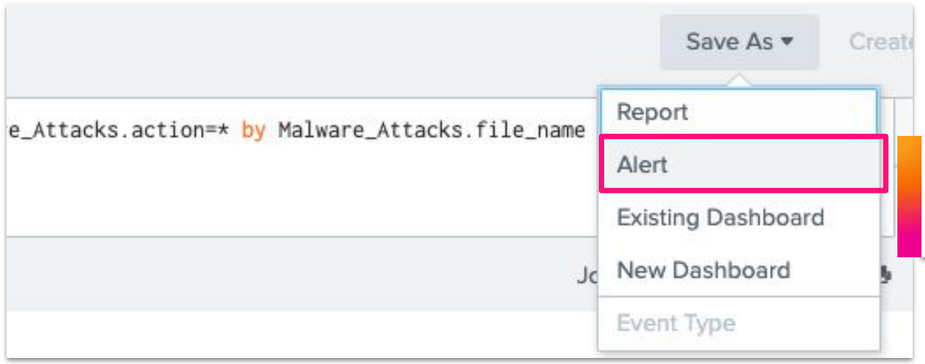
✓ **124 events** (02/12/2024 19:00:00.000

Events Patterns **Statistics (1)** Visualization

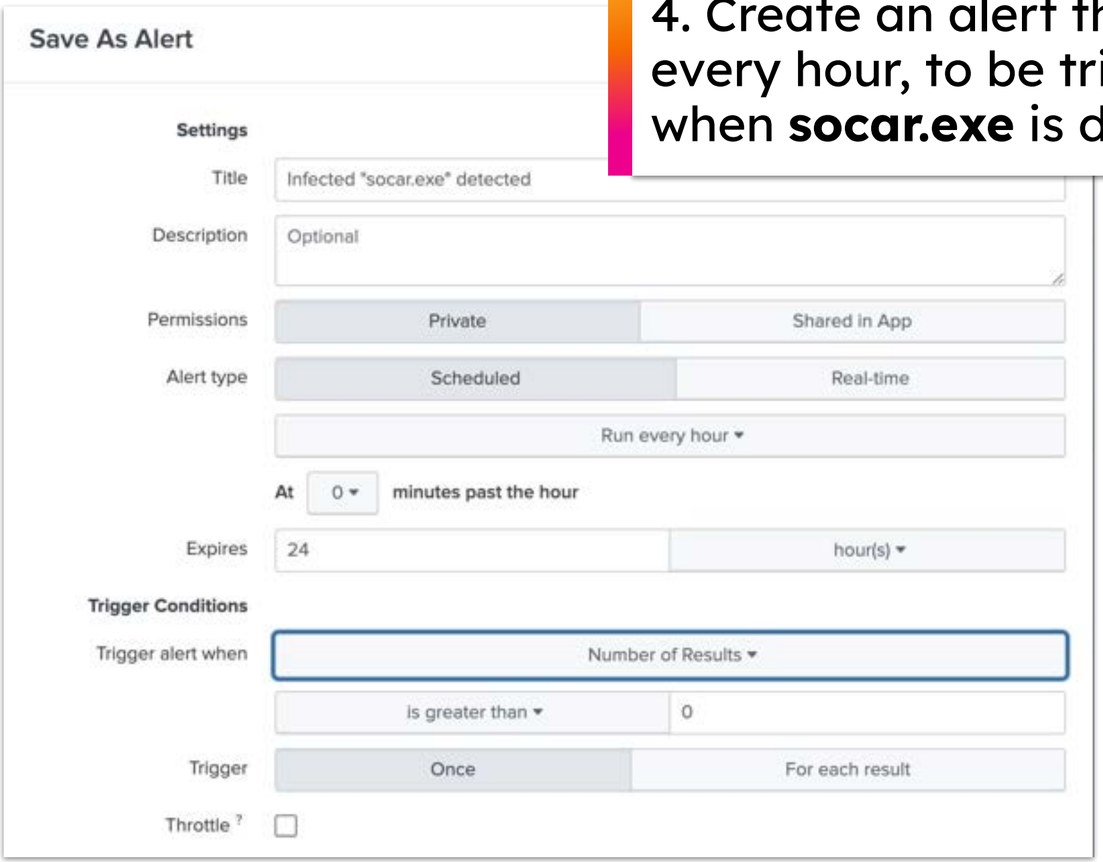
20 Per Page ▾ Format Preview ▾

file_name
socar.exe

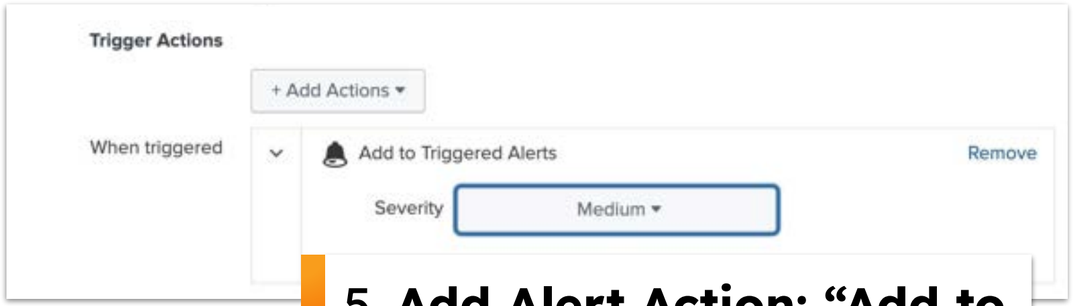
Alert when this infected files is seen again



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



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



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

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

Refer to: https://docs.splunk.com/Documentation/Splunk/latest/Alert/AlertTriggerConditions

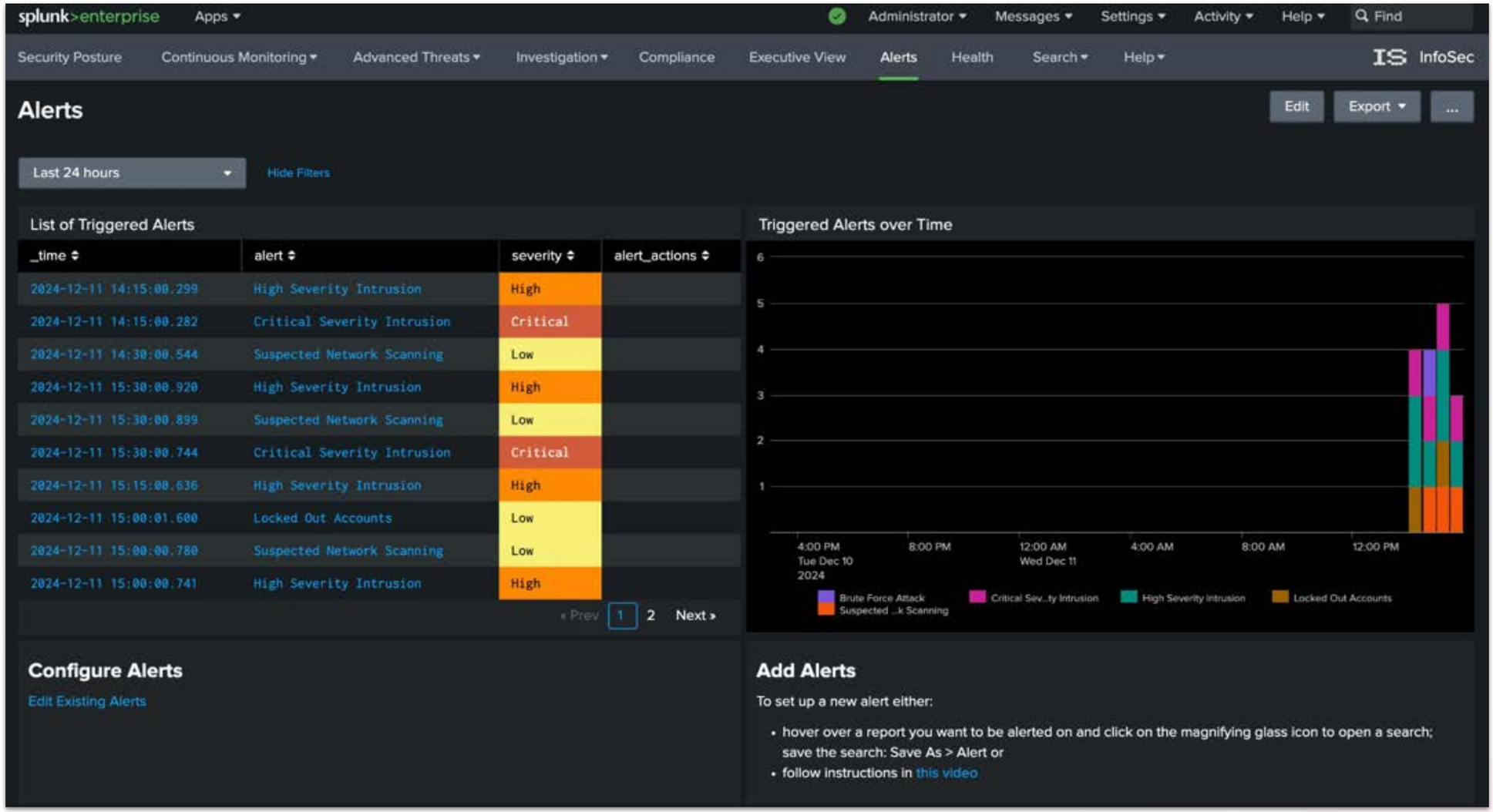
Alert Trigger Actions

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

Refer to: https://docs.splunk.com/Documentation/SplunkCloud/latest/Alert/Setupalertactions

Alert Dashboard



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

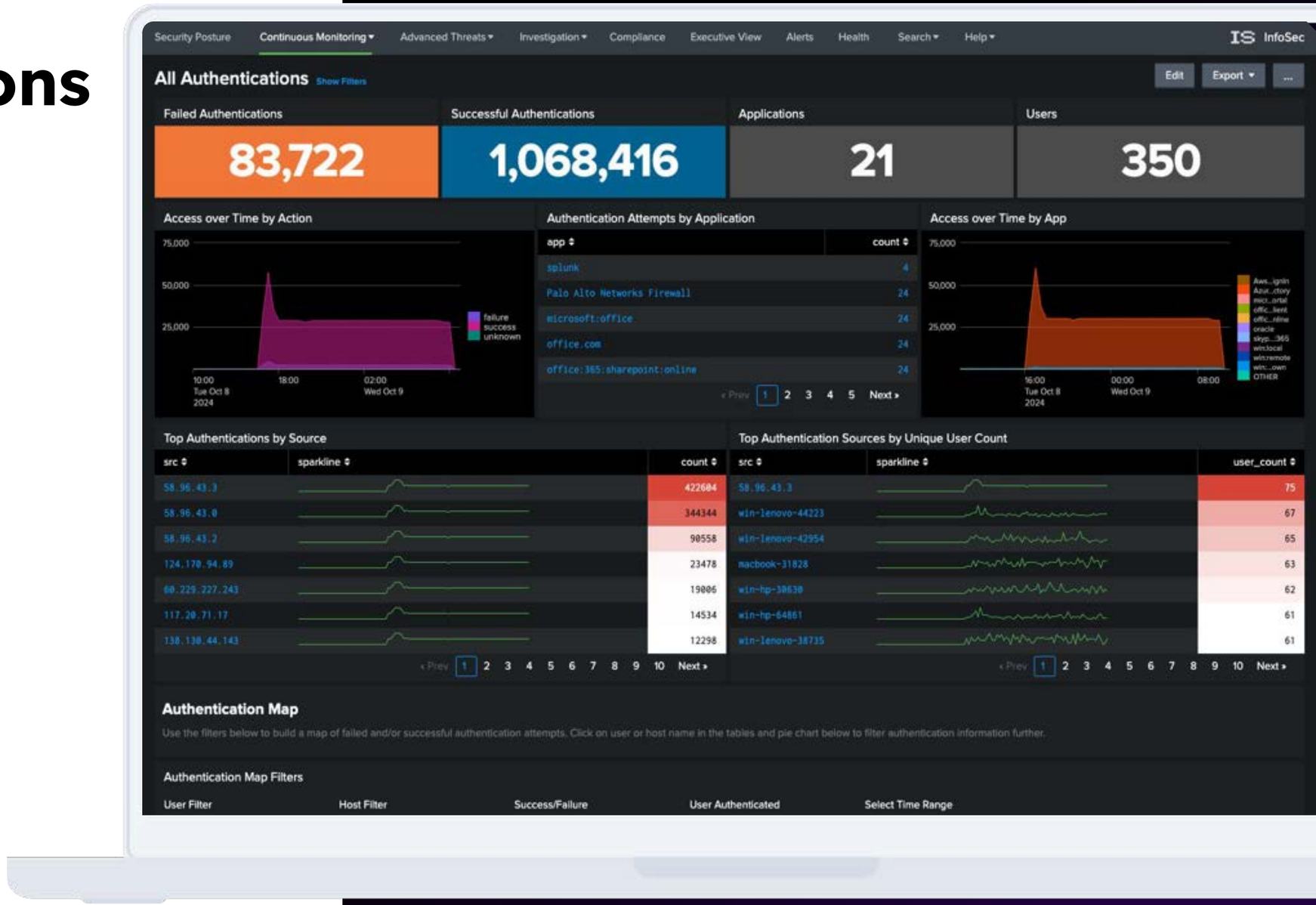
Add additional security content: Review the content in Splunk Security Essentials and add any new use cases you think might be valuable

BUTTERCUP STATE UNIVERSITY

All Authentications

InfoSec App Dashboard

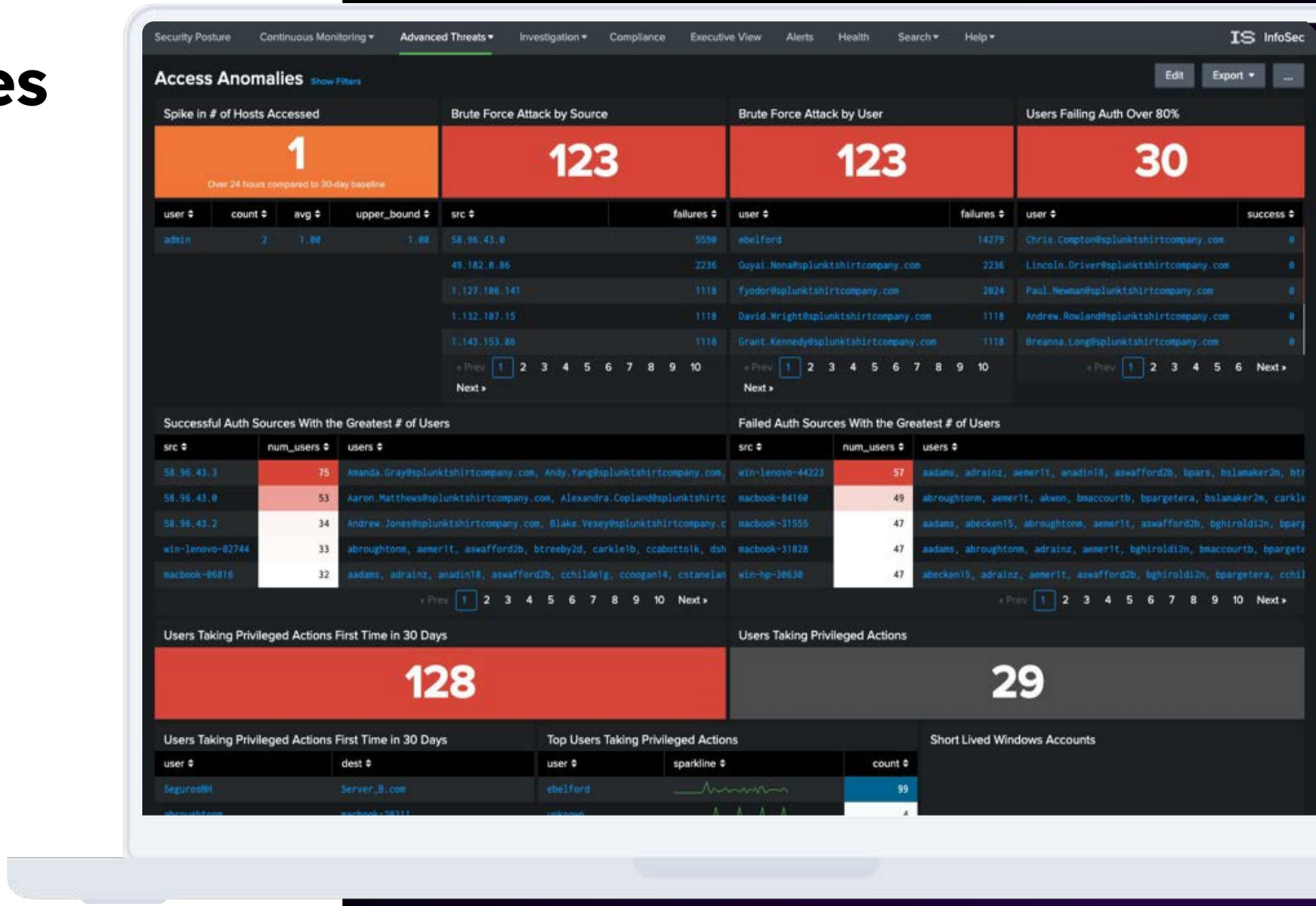
- Consolidated view of authentication actions
- Breaks down attempts by application
- Counts successful and failed events
- Identifies unusual authentication patterns
- Monitor user access and authentication activity
- Detect potential threats related to unauthorized access



Access Anomalies

InfoSec App Dashboard

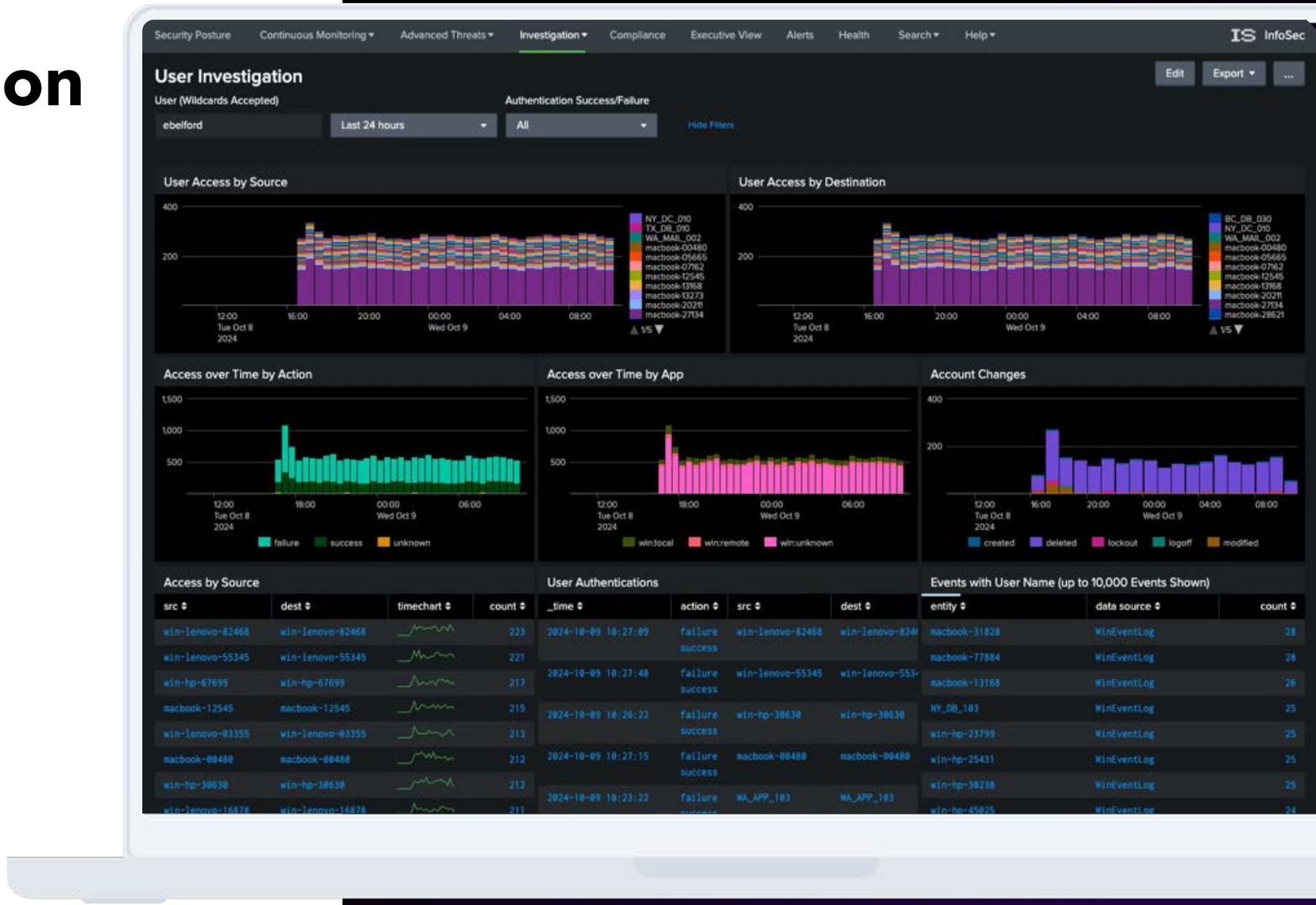
- Identifies spikes in access to hosts
- Detects brute force attacks by source or user
- Monitors accounts with high logon failure rates
- Flags users performing new privileged actions
- Highlights geographically improbable access
- Detecting potential security risks
- Investigating unusual access patterns



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



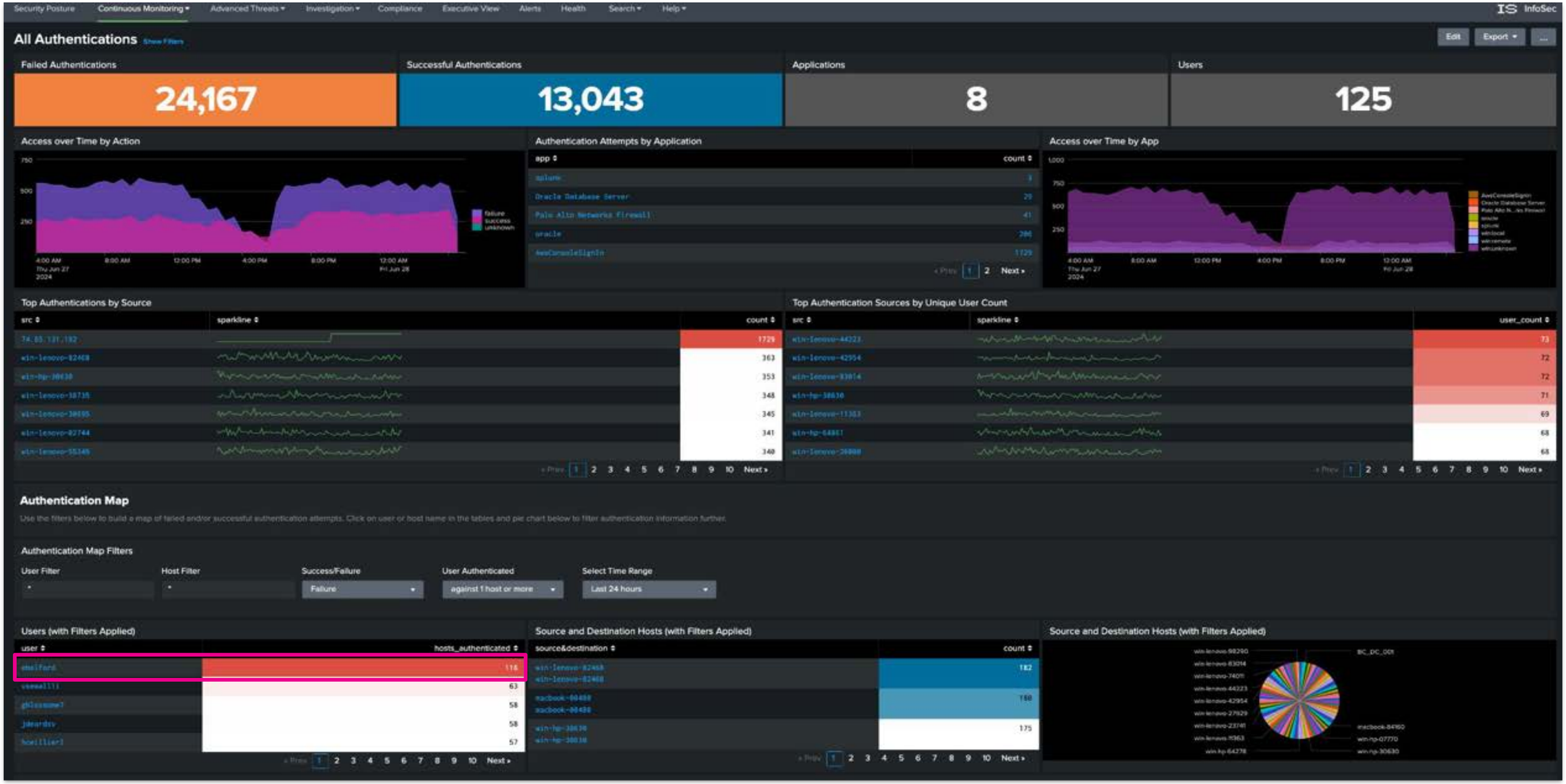
User Behavior Investigation

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

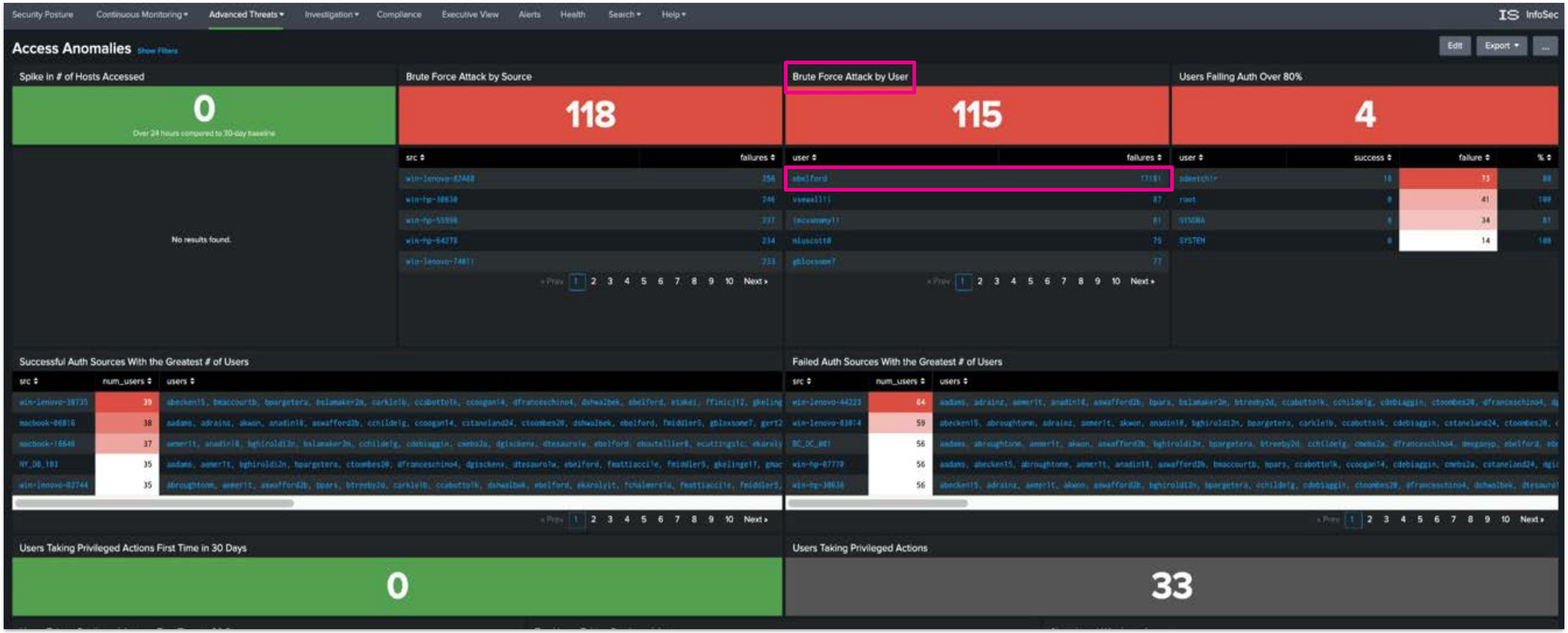
Tasks

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



Check Investigation - User Investigation Dashboard

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

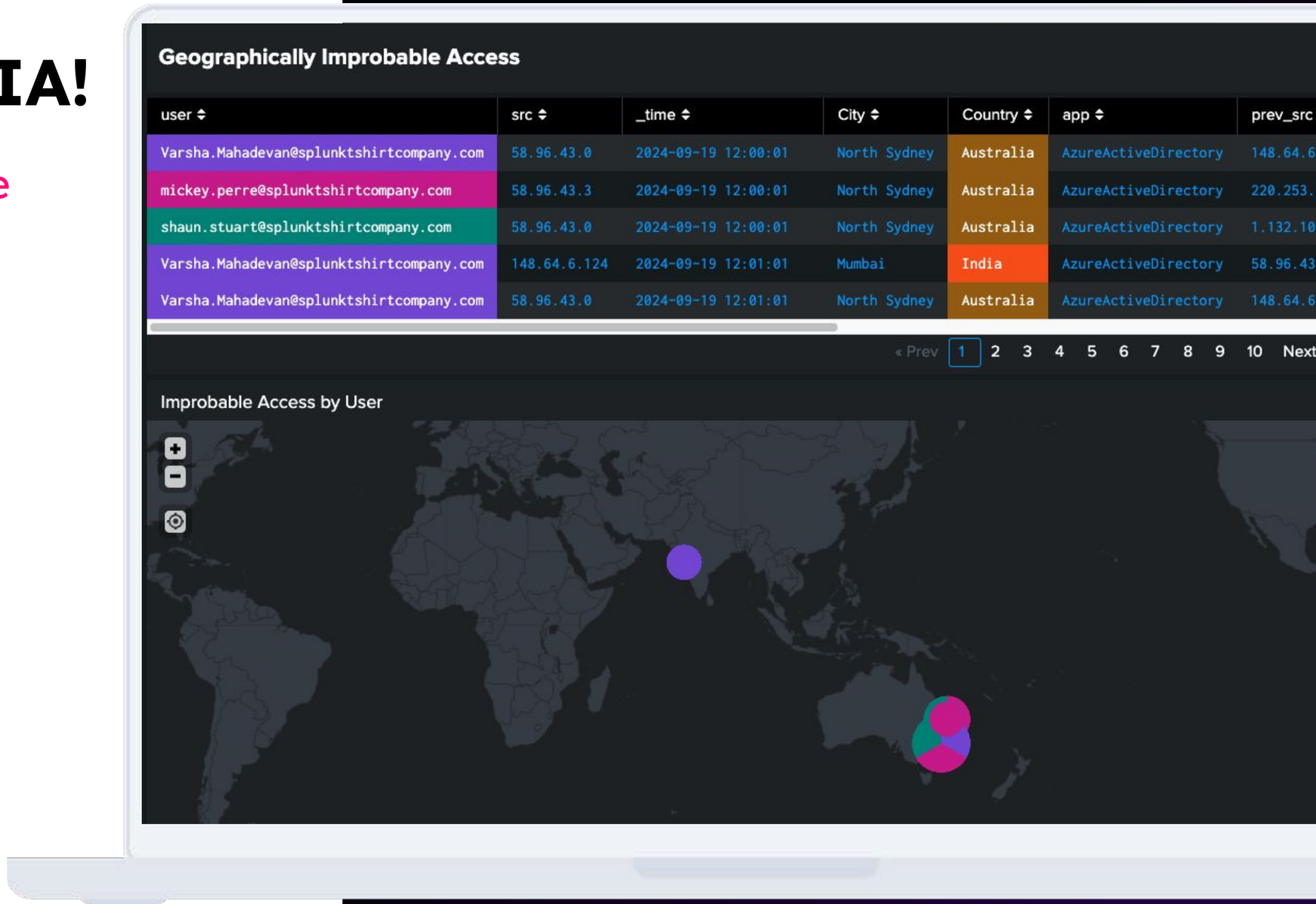
- **IT team:** Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly
- **Malware:** Find Malware-infected files and setup an alert for future detections
- **User behavior:** Look for sudden access changes, unauthorized role modifications, or unusual 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

BUTTERCUP STATE UNIVERSITY

Let’s focus on GIA!

Geographically Improbable Accesses and Allowlists

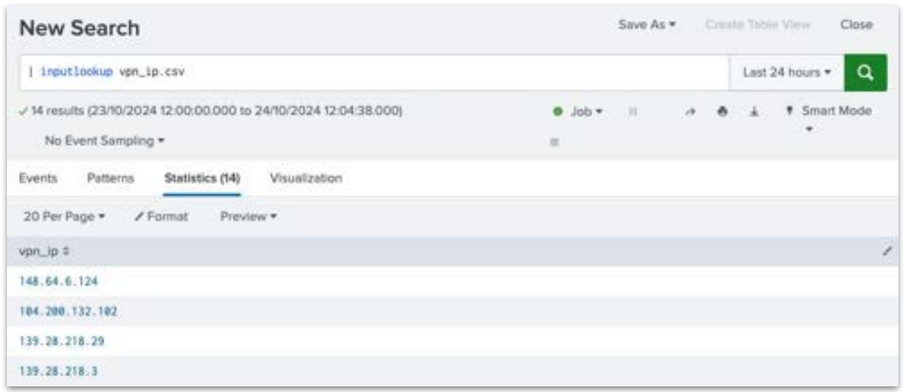
- Triggers alerts when a user authenticates from 2 distant locations in a too short time frame
- Can trigger numerous false positives
- You may need Splunk to take into account expected behaviors, such as use of an authentication system or a VPN.

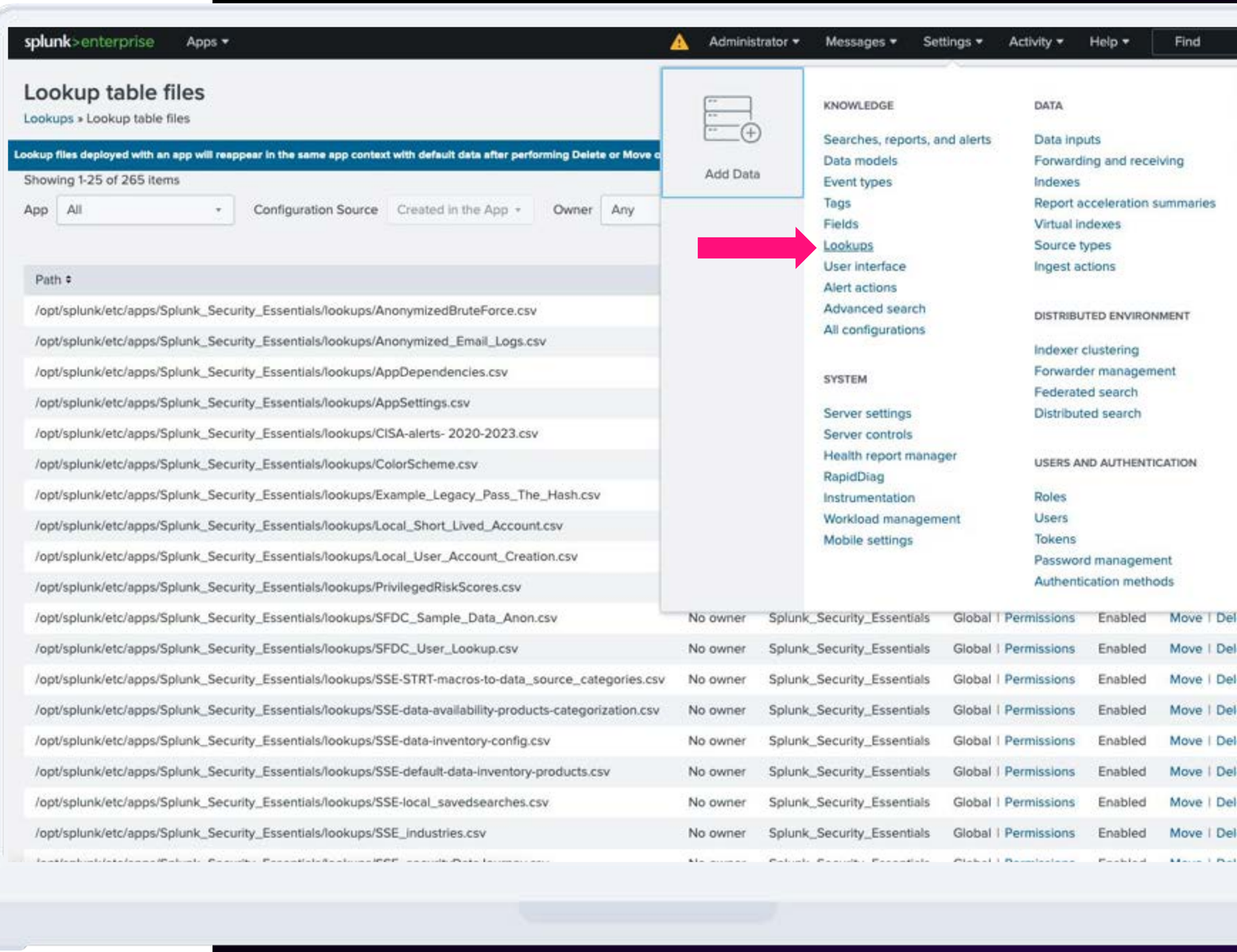


Lookups

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`





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

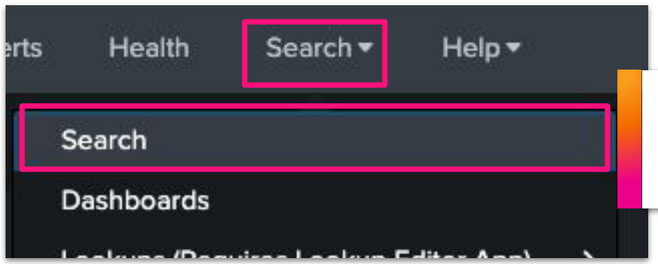
Customize the InfoSec App

Look for ways to customize the content for Buttercup State University

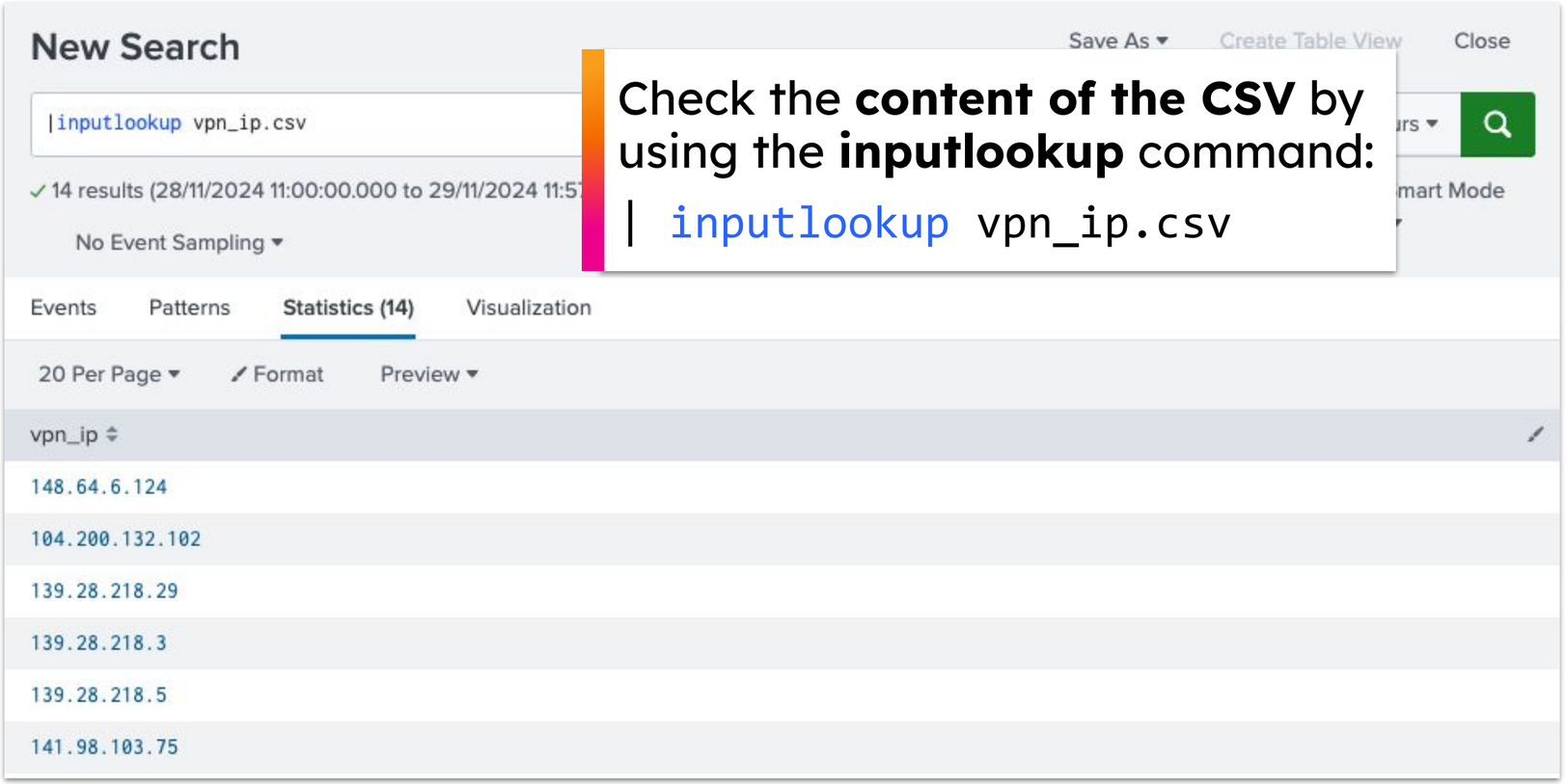
Tasks

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



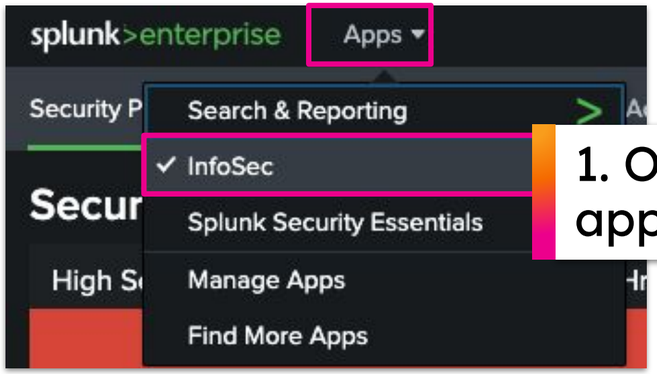
Go to the **Search** page



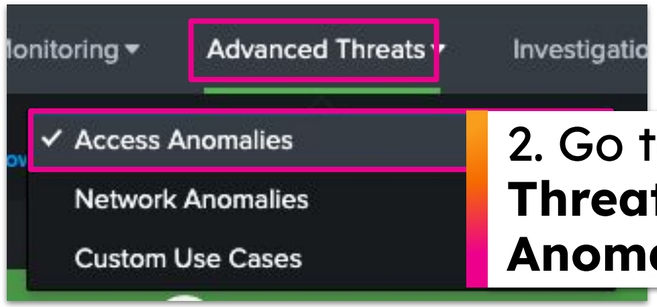
Check the **content of the CSV** by using the **inputlookup** command:

```
| inputlookup vpn_ip.csv
```

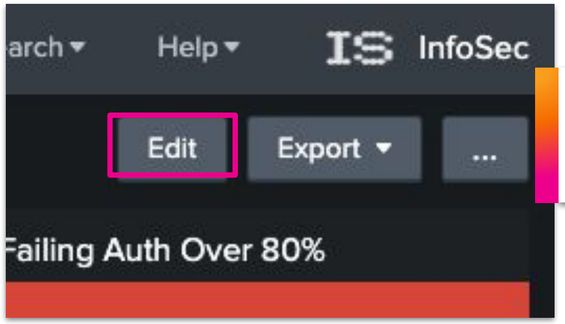
Customize the Geographically Improbable Access Table



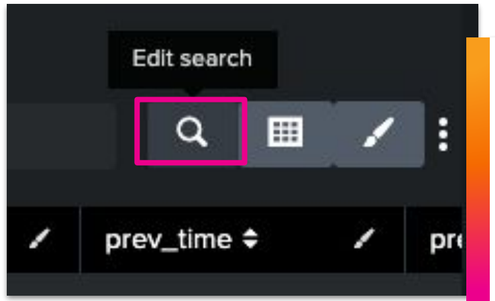
1. Open the **InfoSec** app



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

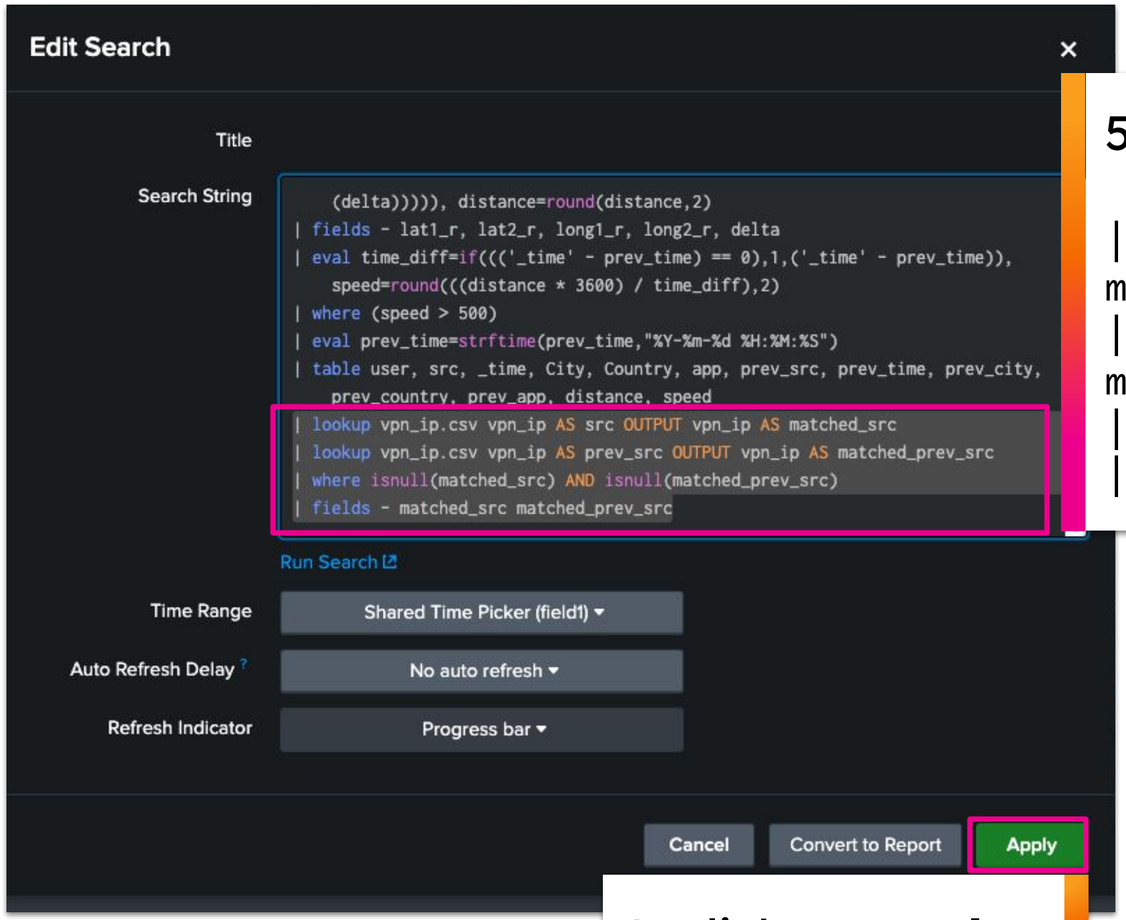


3. Switch to **Edit** mode



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

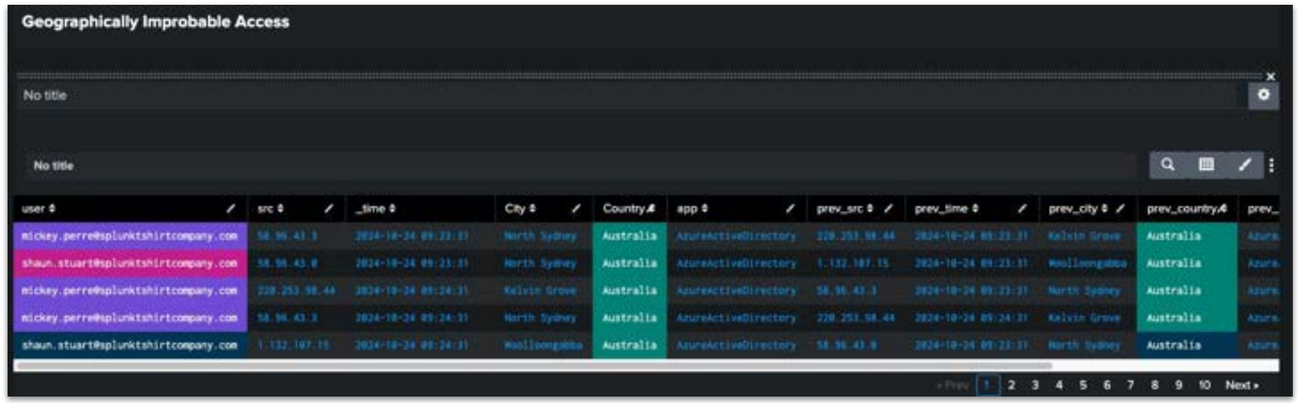
Customize the Geographically Improbable Access Table



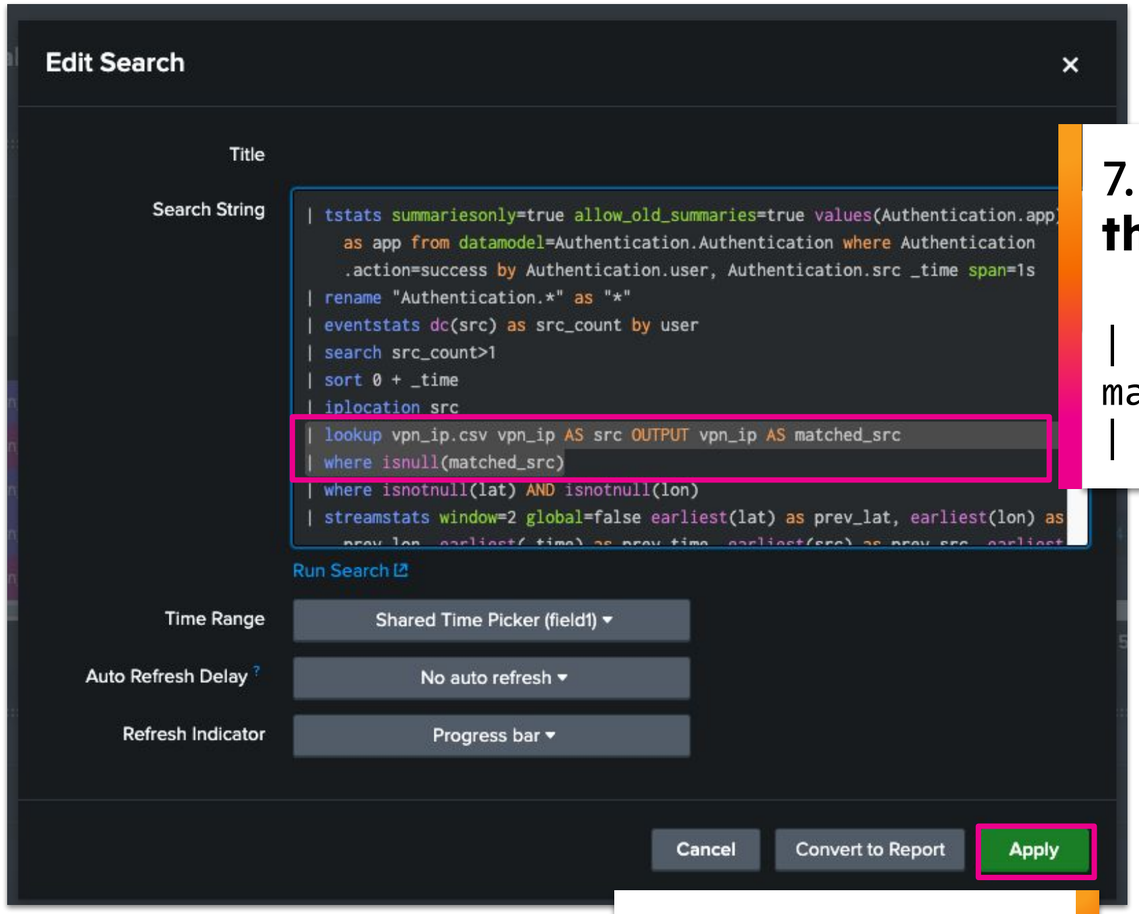
6. Click on **Apply**

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
```



(Optional)
Customize the Improbable Access by User Map

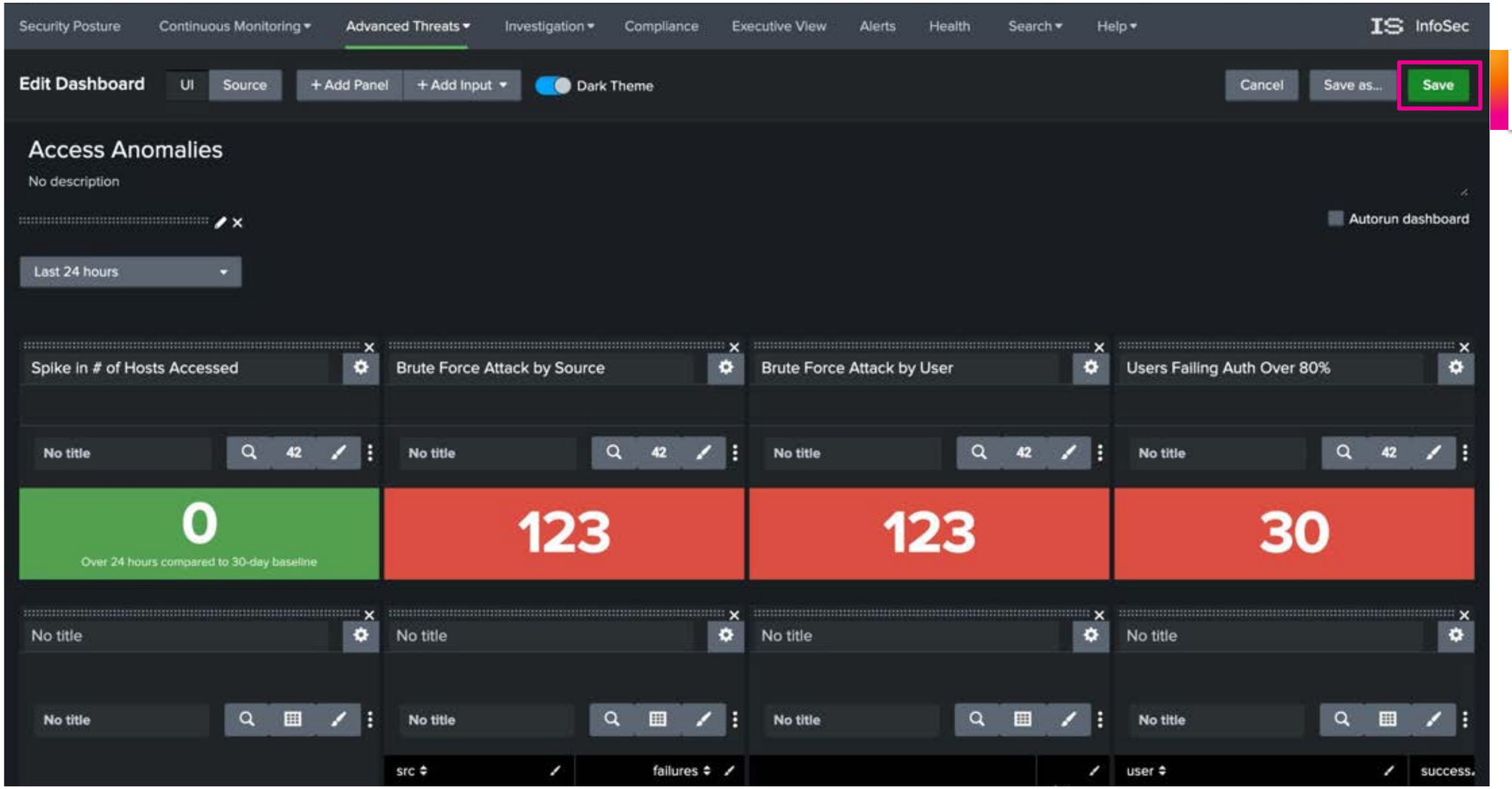


7. Edit the search of the **map visualisation** and **add these two lines** under the iplocation line:

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

8 Click on **Apply**

Save Your Dashboard!



Click **Save**

Our progress so far

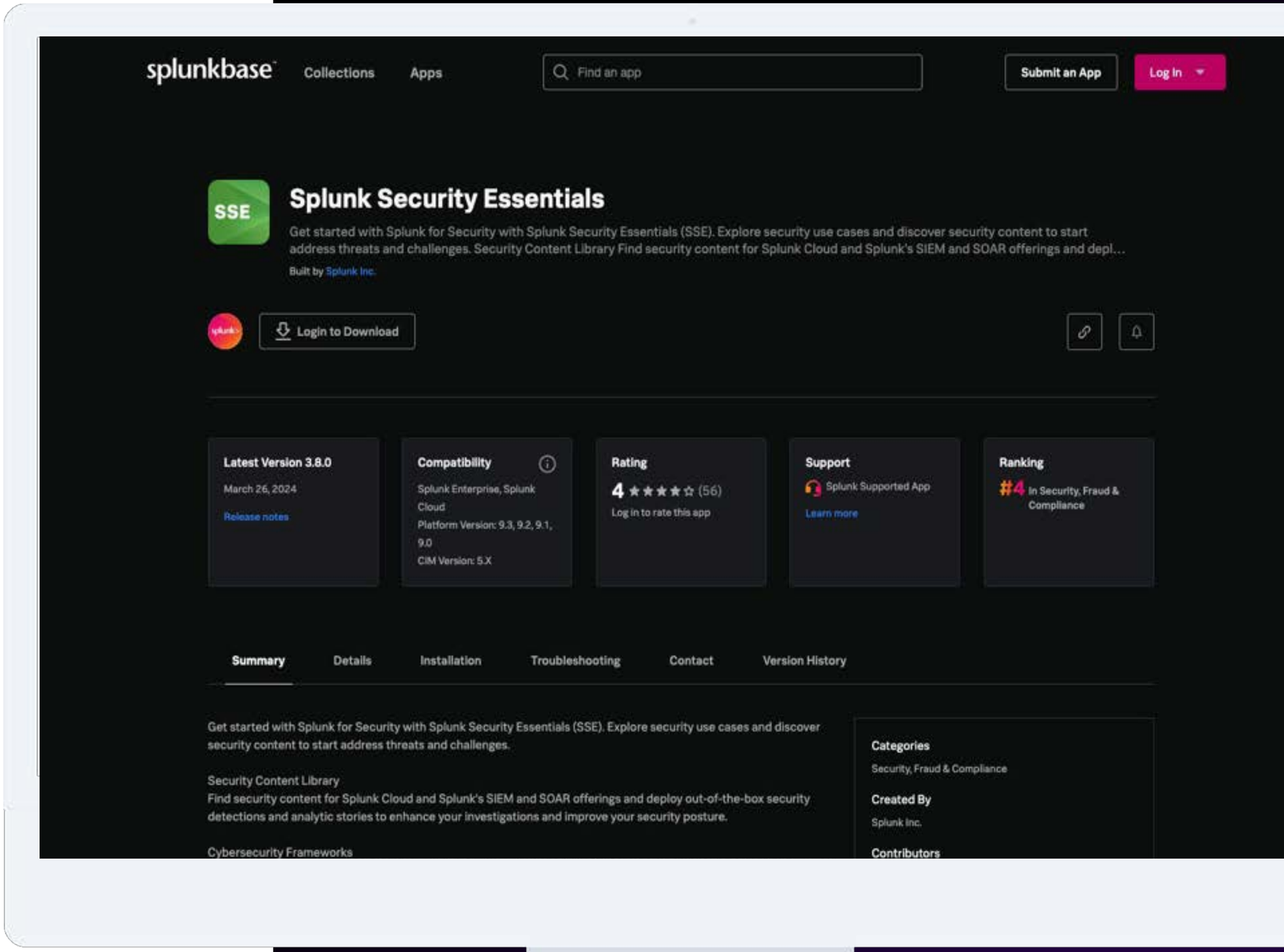
- **IT team:** Install the Splunk Add-on for AWS and finish setting up the InfoSec app so the dashboards populate correctly
- **Malware:** Find Malware-infected files and setup an alert for future detections
- **User behavior:** Look for sudden access changes, unauthorized role modifications, or unusual 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

BUTTERCUP STATE UNIVERSITY

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



Adding Security Content: New Use Case

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

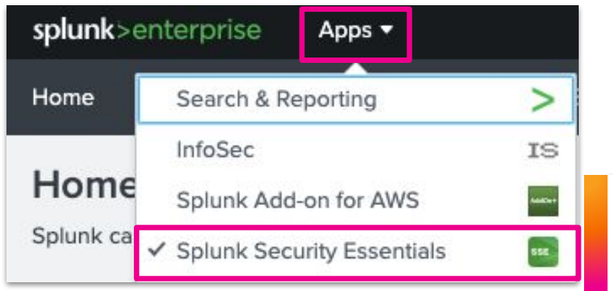
Tasks

The Security team would like you to:

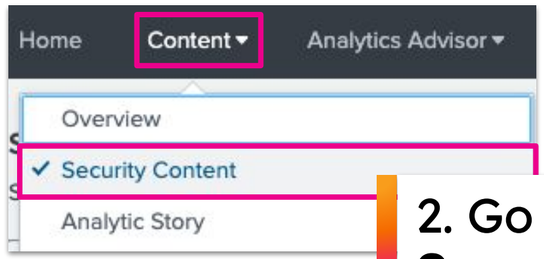
1. Add the '**Recurring Infection on Host**' use case from SSE to the InfoSec App's **Custom Use Cases** dashboard
2. Edit the search so only the **Risk_Name**, **Computer_Name** and **count** fields are displayed
3. Format the table to highlight the **count** in red if it's **greater than 10**

Edit the Custom Use Case Dashboard

Add new content from Splunk Security Essentials



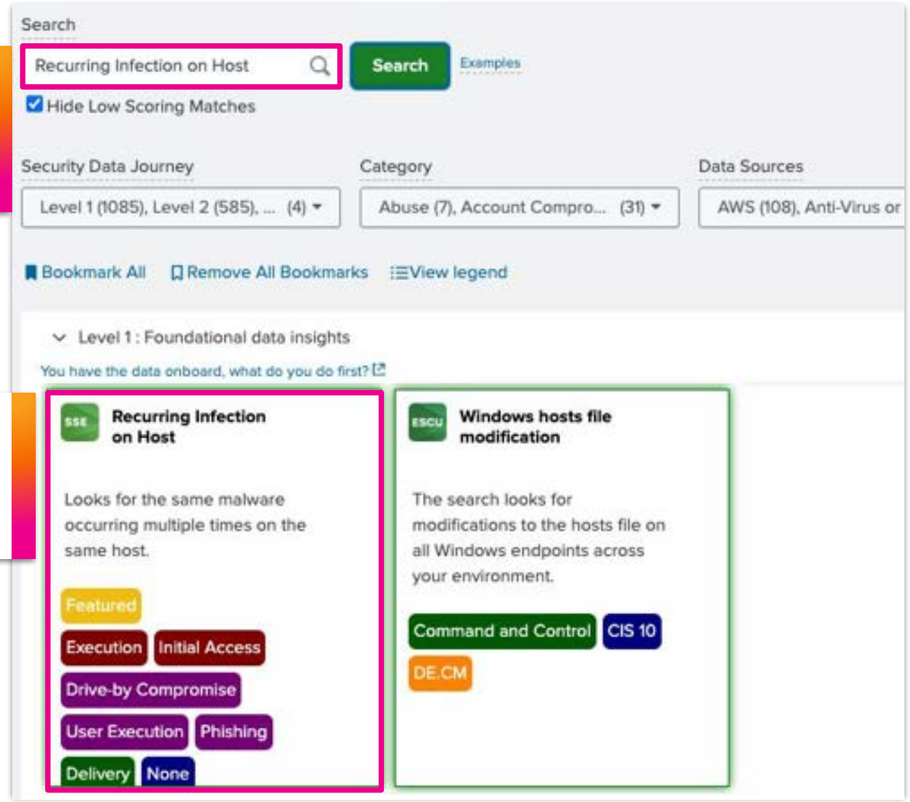
1. Open **Splunk Security Essentials**



2. Go to **Content > Security Content**

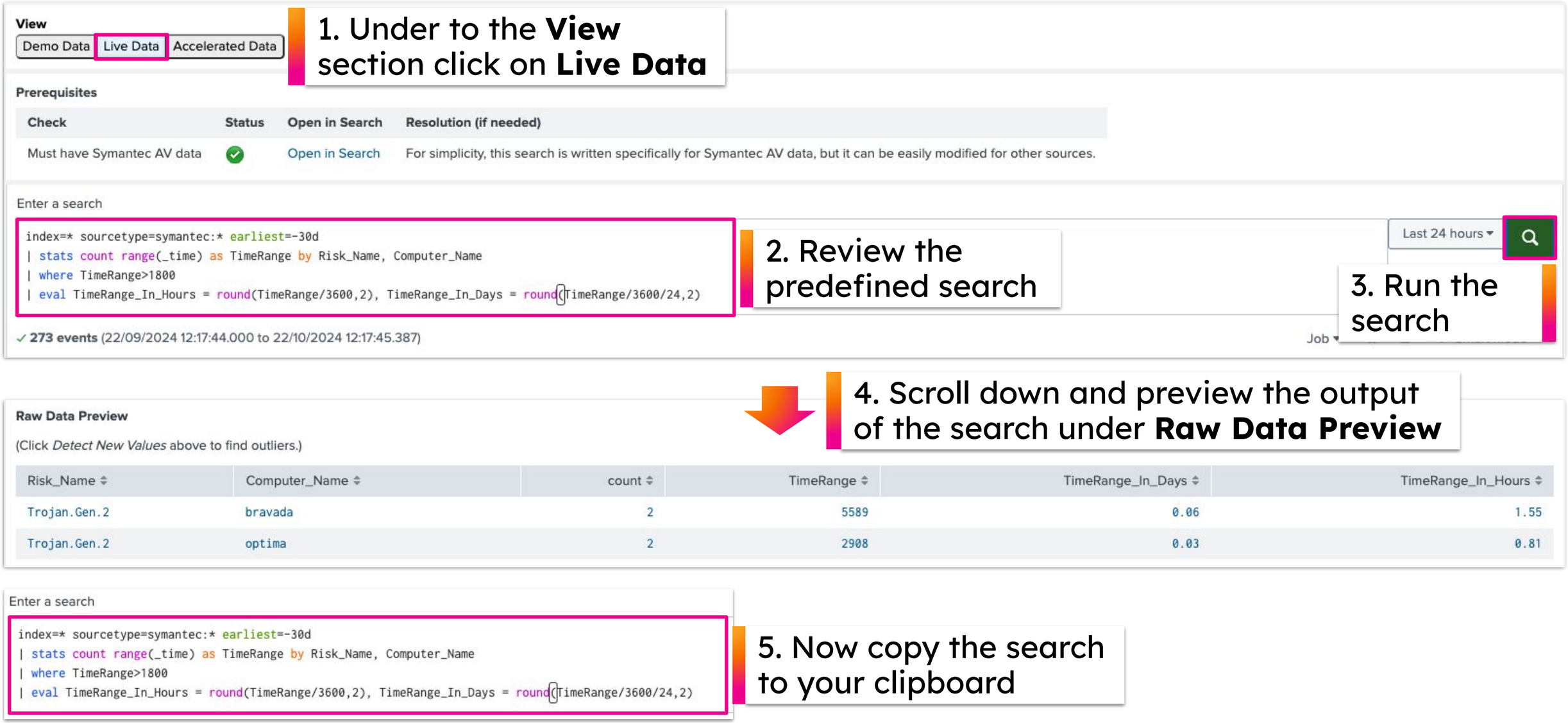
3. Search for **“Recurring Infection on Host”**

4. Click on the **Recurring Infection on Host** use case



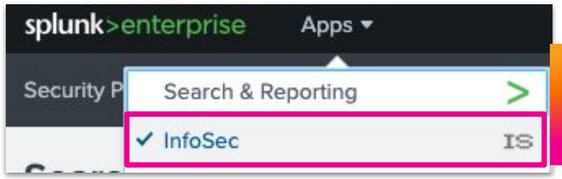
Edit the Custom Use Case Dashboard

Add new content from Splunk Security Essentials

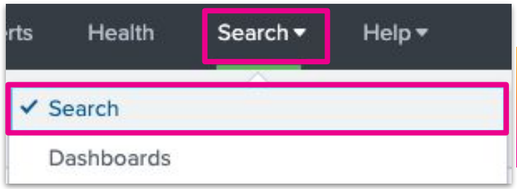


Edit the Custom Use Case Dashboard

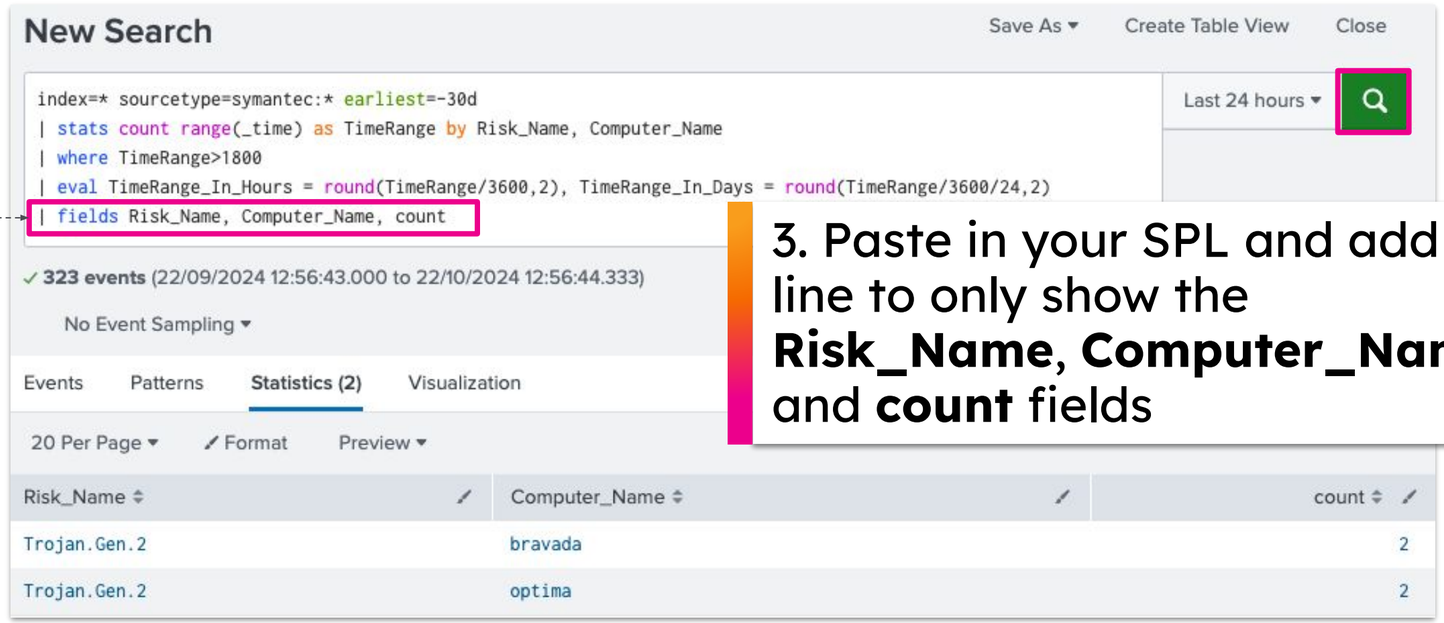
Add the new content to the Custom Use Case dashboard



1. Return to the **InfoSec** app



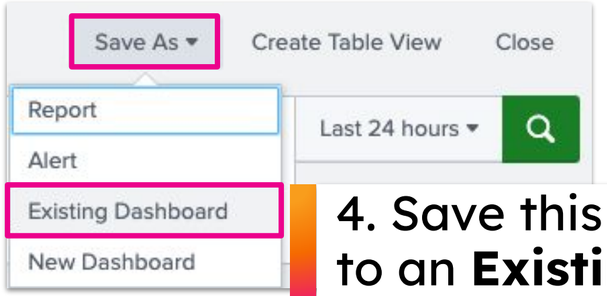
2. Click on **Search > Search**



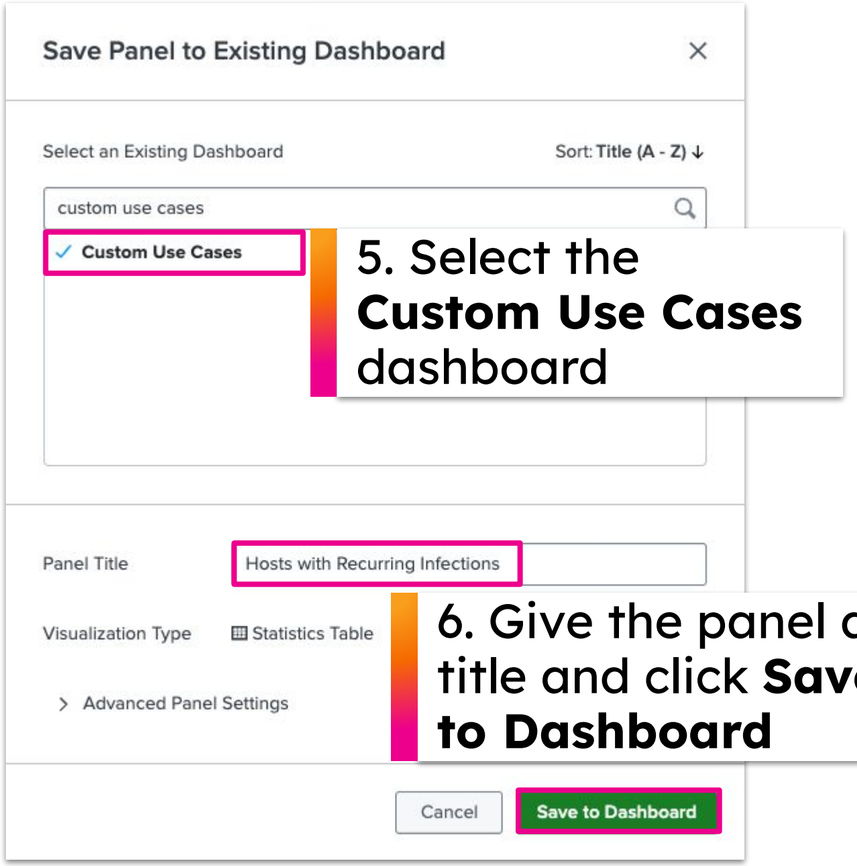
3. Paste in your SPL and add a line to only show the **Risk_Name**, **Computer_Name** and **count** fields

Line to add:

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



4. Save this search to an **Existing Dashboard**

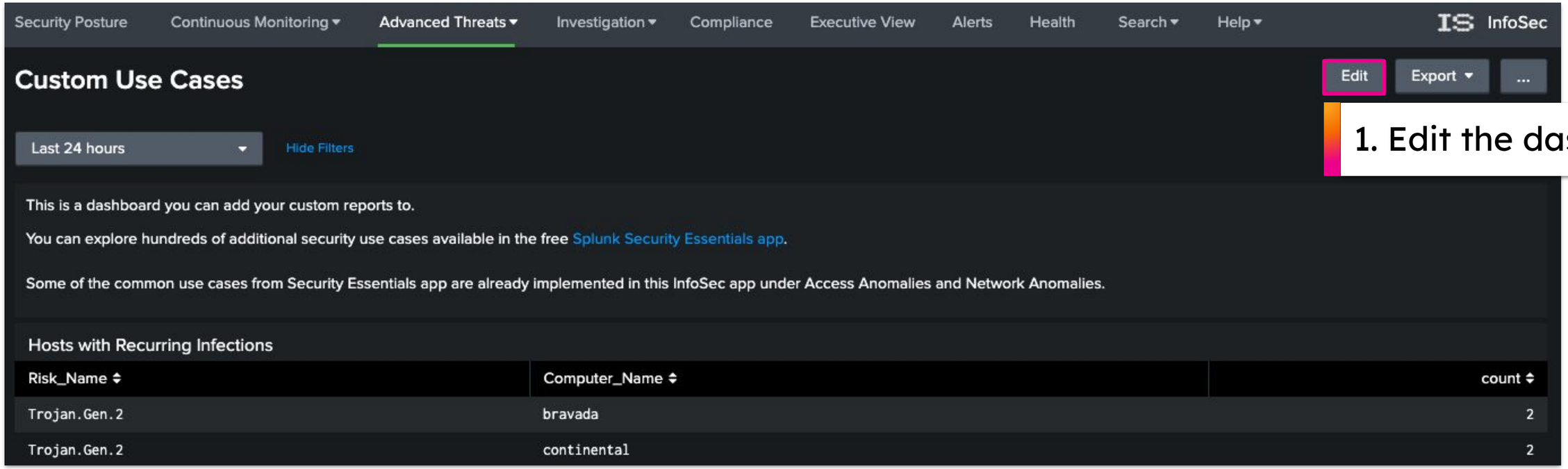


5. Select the **Custom Use Cases** dashboard

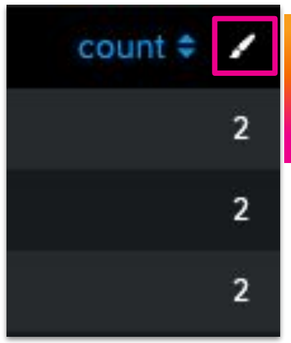
6. Give the panel a title and click **Save to Dashboard**

Edit the Custom Use Case Dashboard

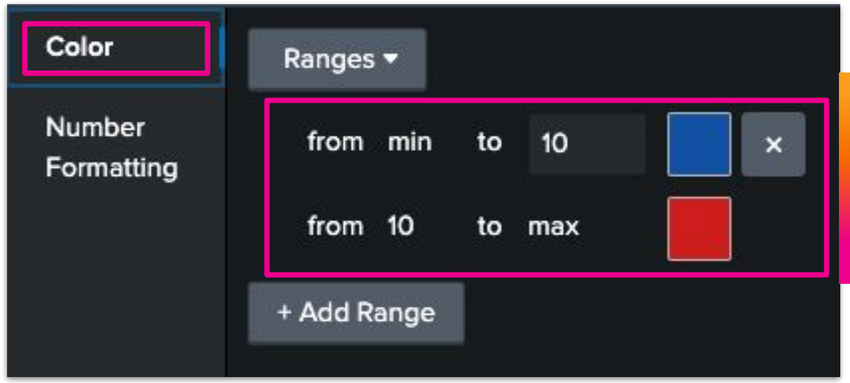
Add color to the new dashboard panel



1. Edit the dashboard



2. Format the **count** column



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

Make sure you **save** your dashboard!

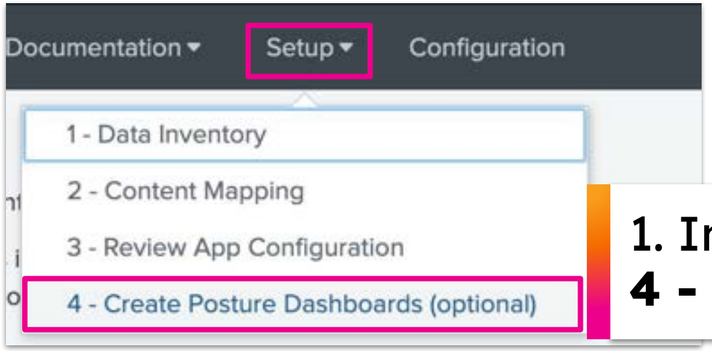
Adding Security Content: New Dashboard

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

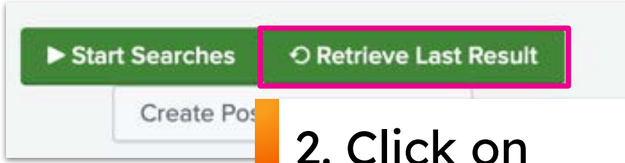
Tasks

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



1. In SSE click on **Setup > 4 - Create Posture Dashboards**



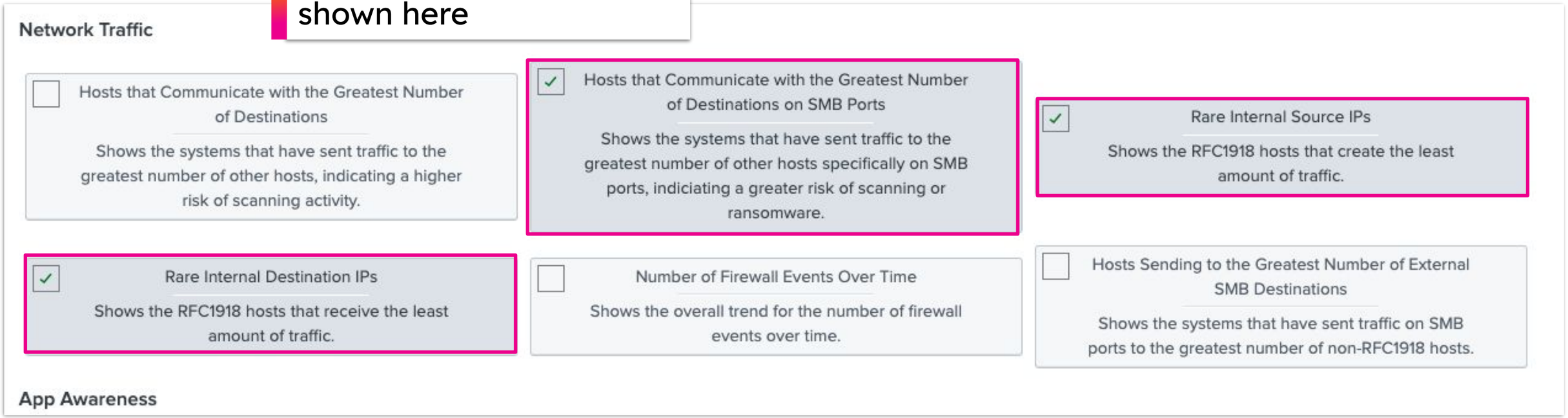
2. Click on **Retrieve Last Result**

3. Click on **Create Posture Dashboards**

4. Select **Essential Network Security**

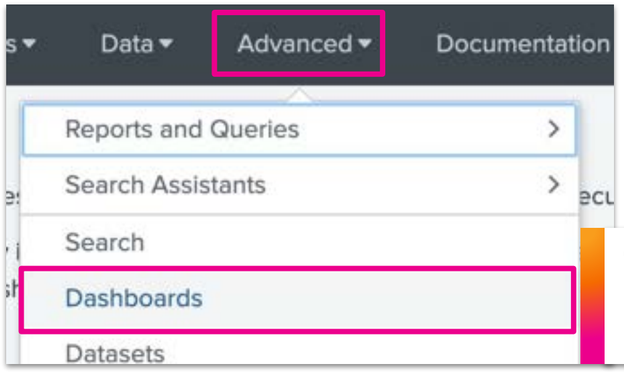
Create a Dashboard from Splunk Security Essentials

5. Select the detections shown here



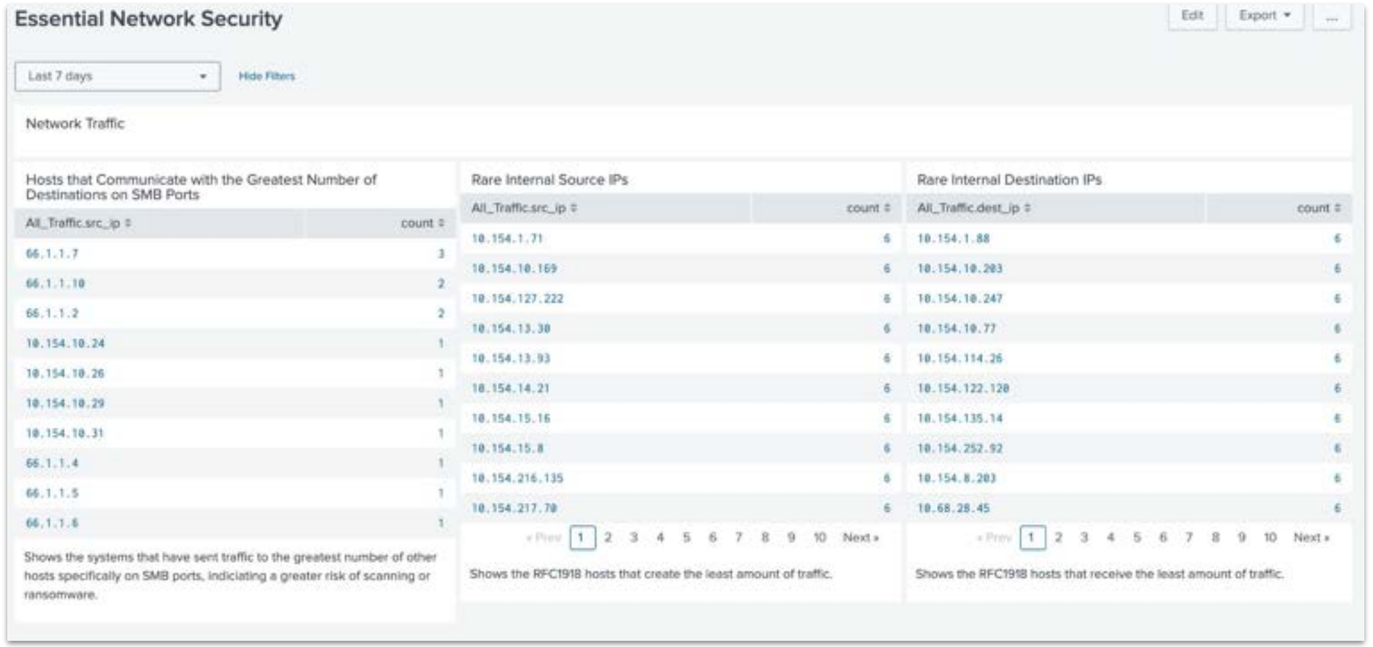
6. Click on **Create Dashboards**

Create a Dashboard from Splunk Security Essentials

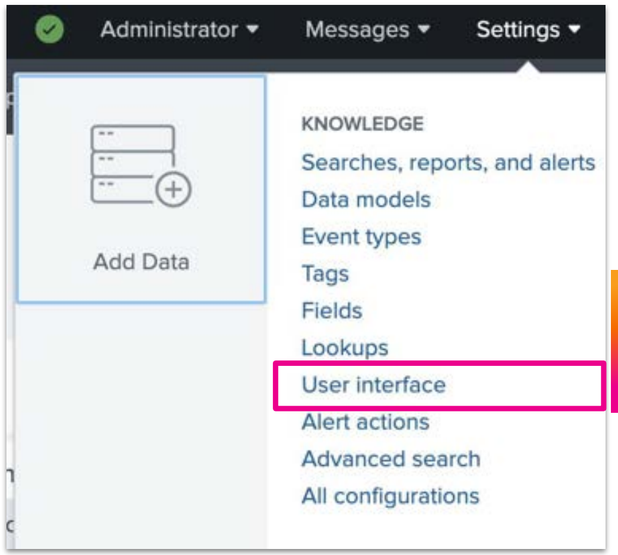


7. Click on **Advanced** > **Dashboards**

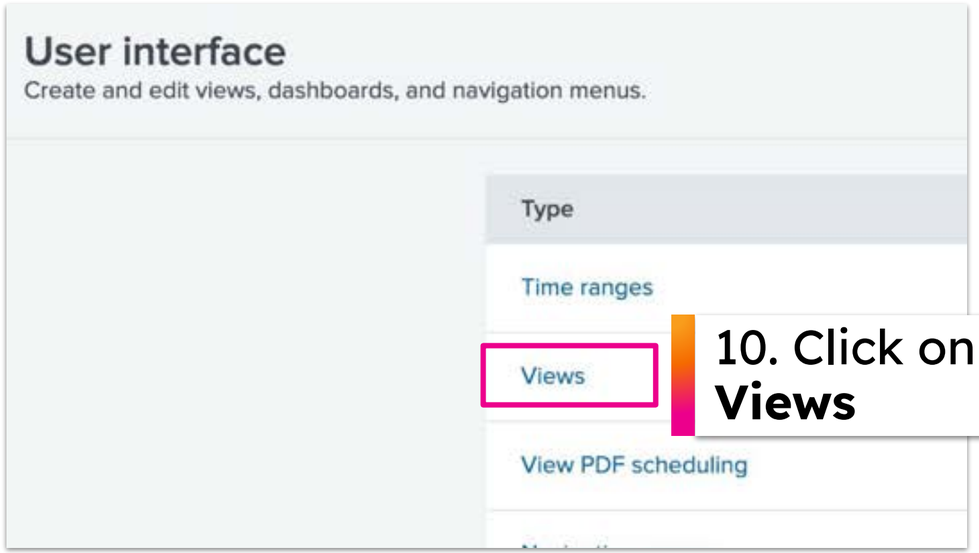
8. Find the new dashboard and verify it contains the chosen detections



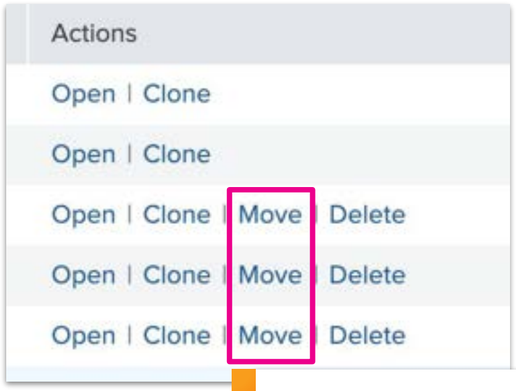
Move the Dashboard from SSE to the InfoSec App



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



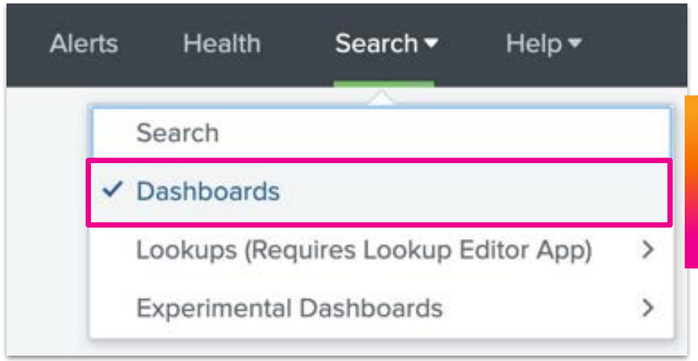
10. Click on **Views**



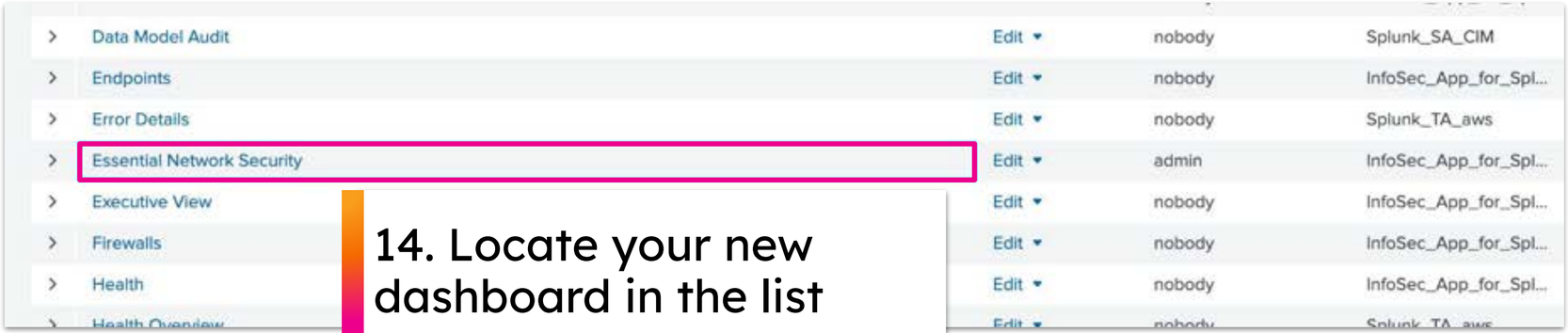
11. Find your dashboard and click on **Move**

Move the Dashboard from SSE to the InfoSec App

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

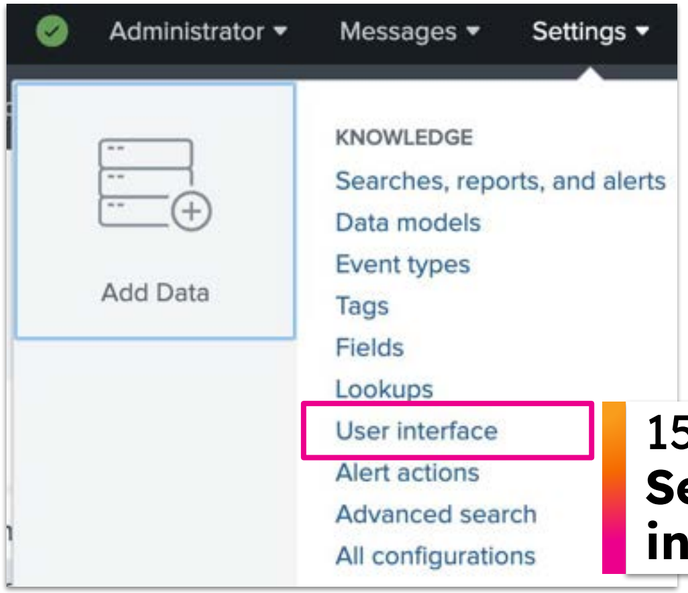


13. Go to the InfoSec App and navigate to **Search** > **Dashboards**

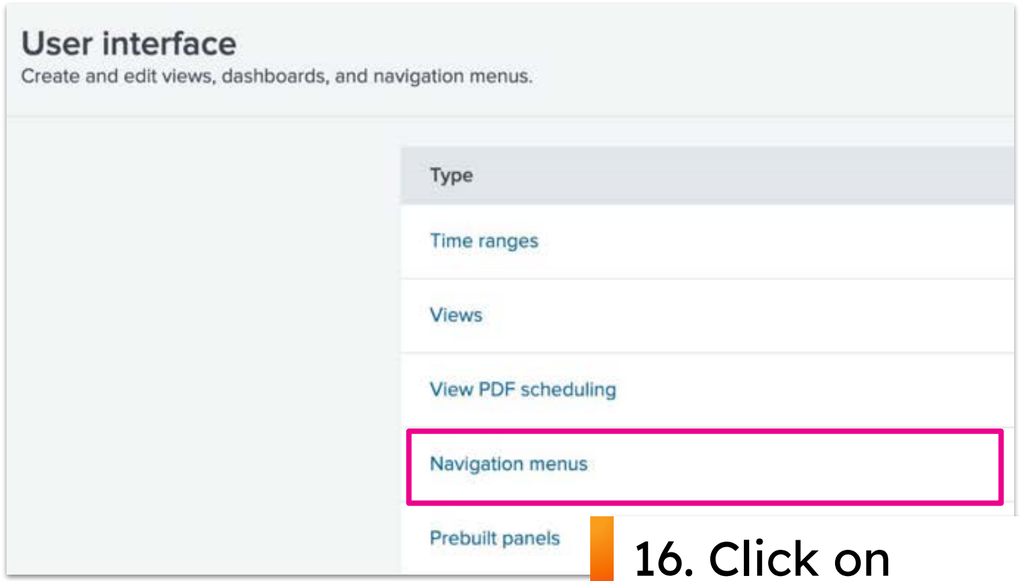


14. Locate your new dashboard in the list

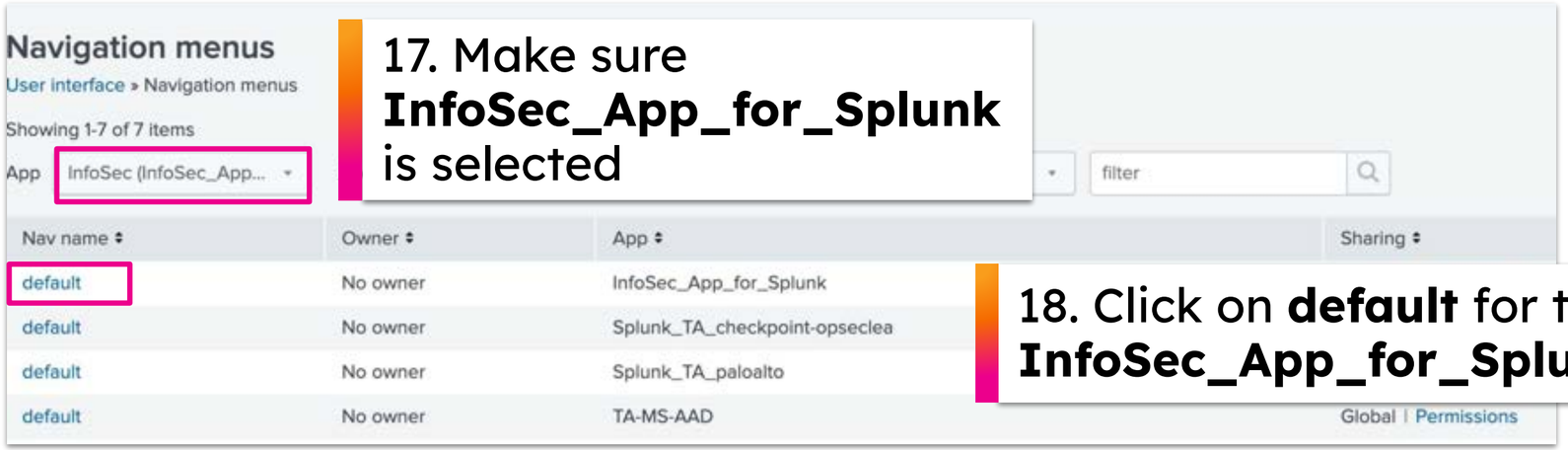
Add the Dashboard to the Navigation Menu



15. Go to **Settings > User interface**



16. Click on **Navigation menus**



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

Navigation menu XML *

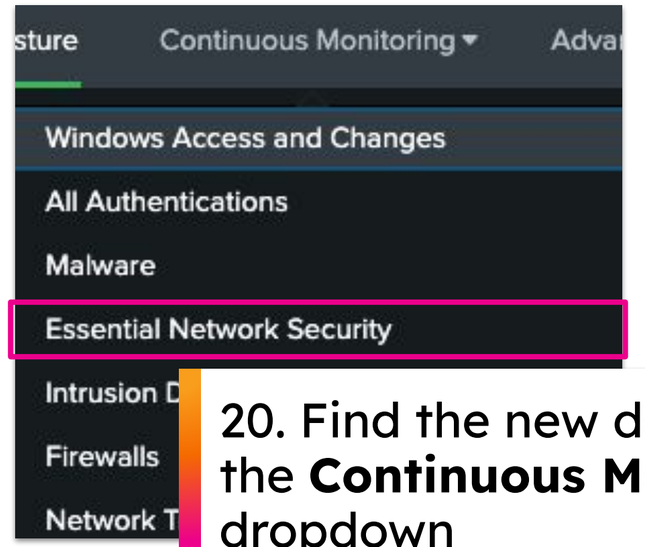
Enter and edit navigation menu XML configuration.

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"/>
```

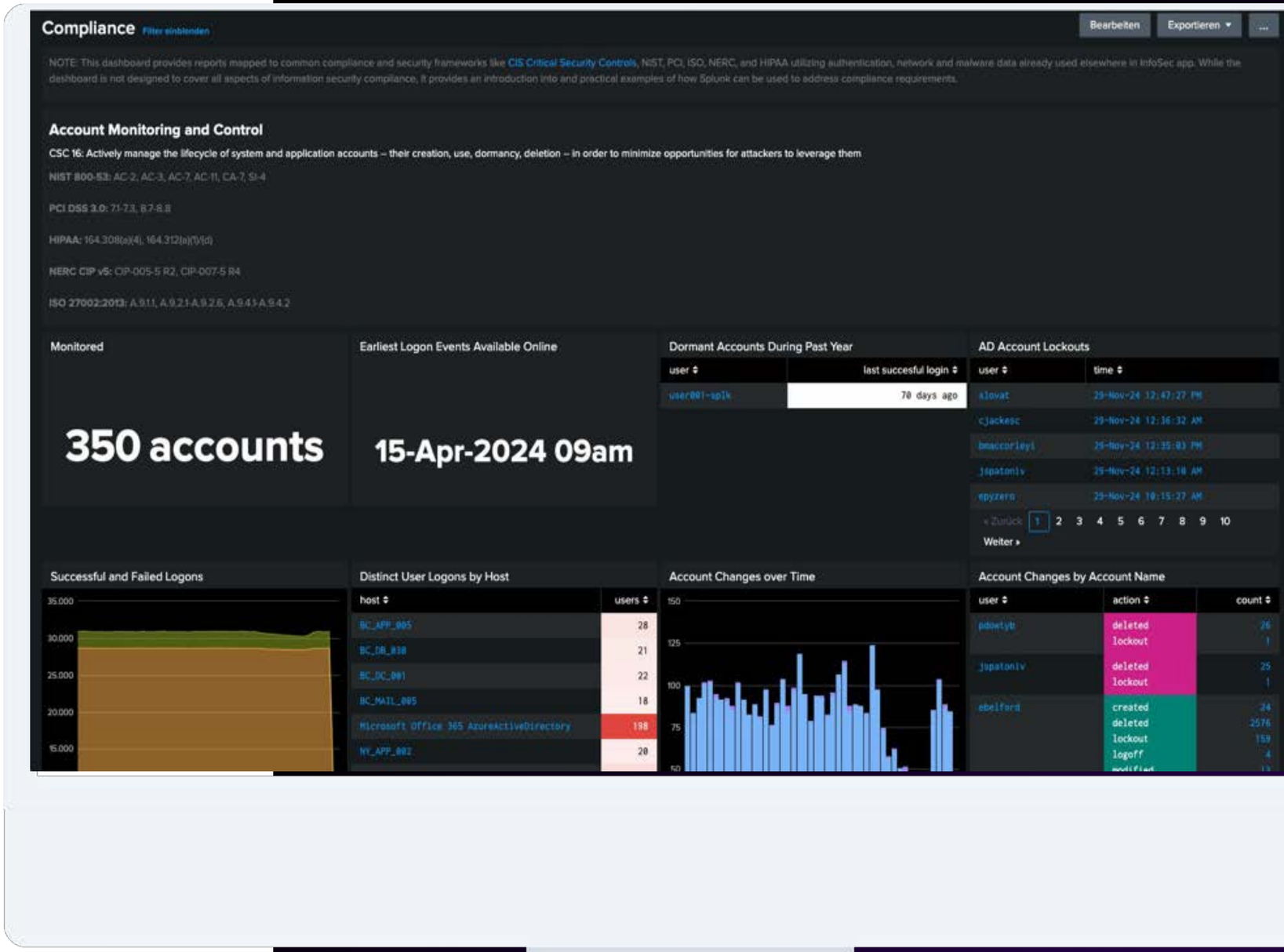
You've Finished the Hands-on Exercises!

- **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

BUTTERCUP STATE UNIVERSITY

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

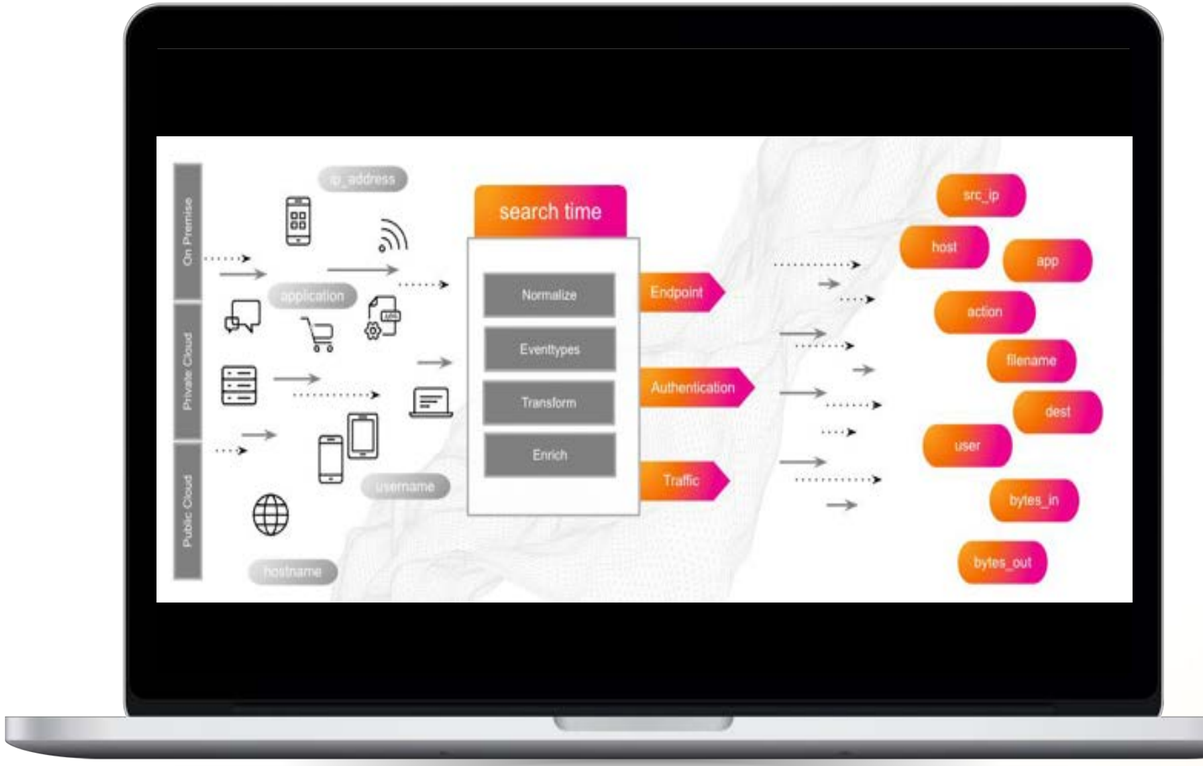
Splunk Resources

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



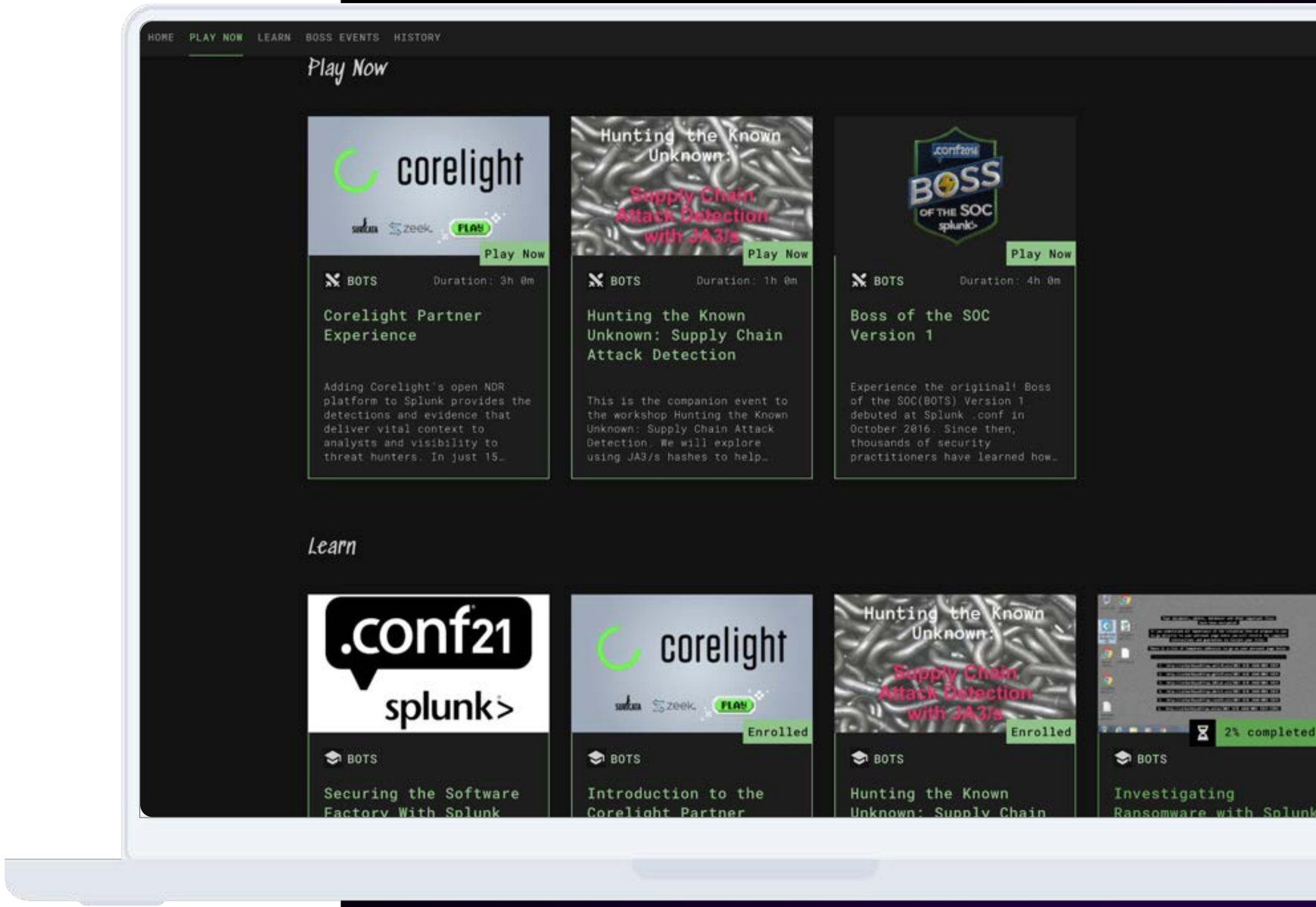
Normalize and visualize custom data using CIM data models and tstats!

Workshop Flyer

BOSS Platform

https://bots.splunk.com

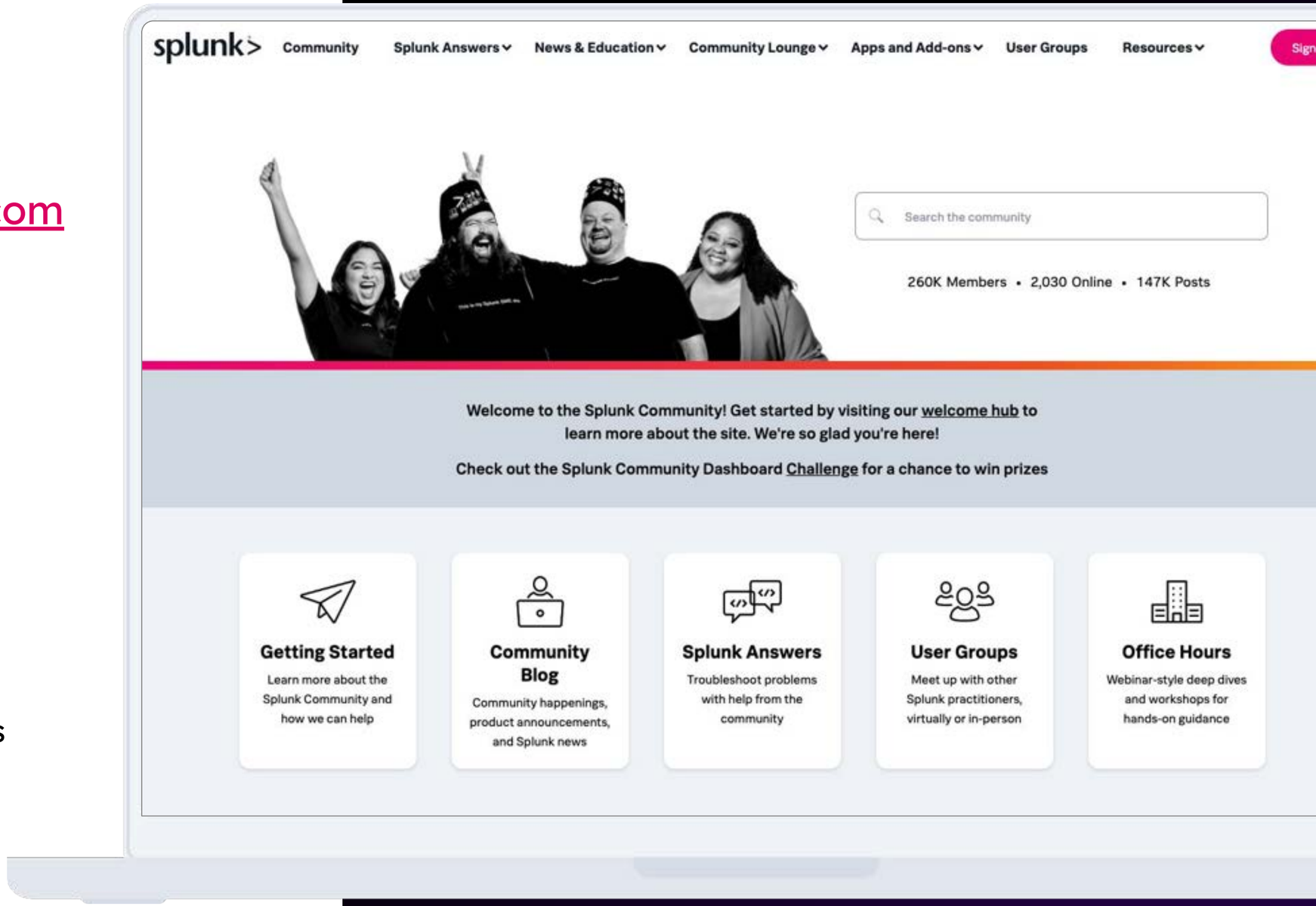
- 24x7 Access
- Login with Splunk.com account (just like Splunkbase)
- Used for all BOTS competition events
- Learn how to use Splunk for security use cases



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



Splunk Events

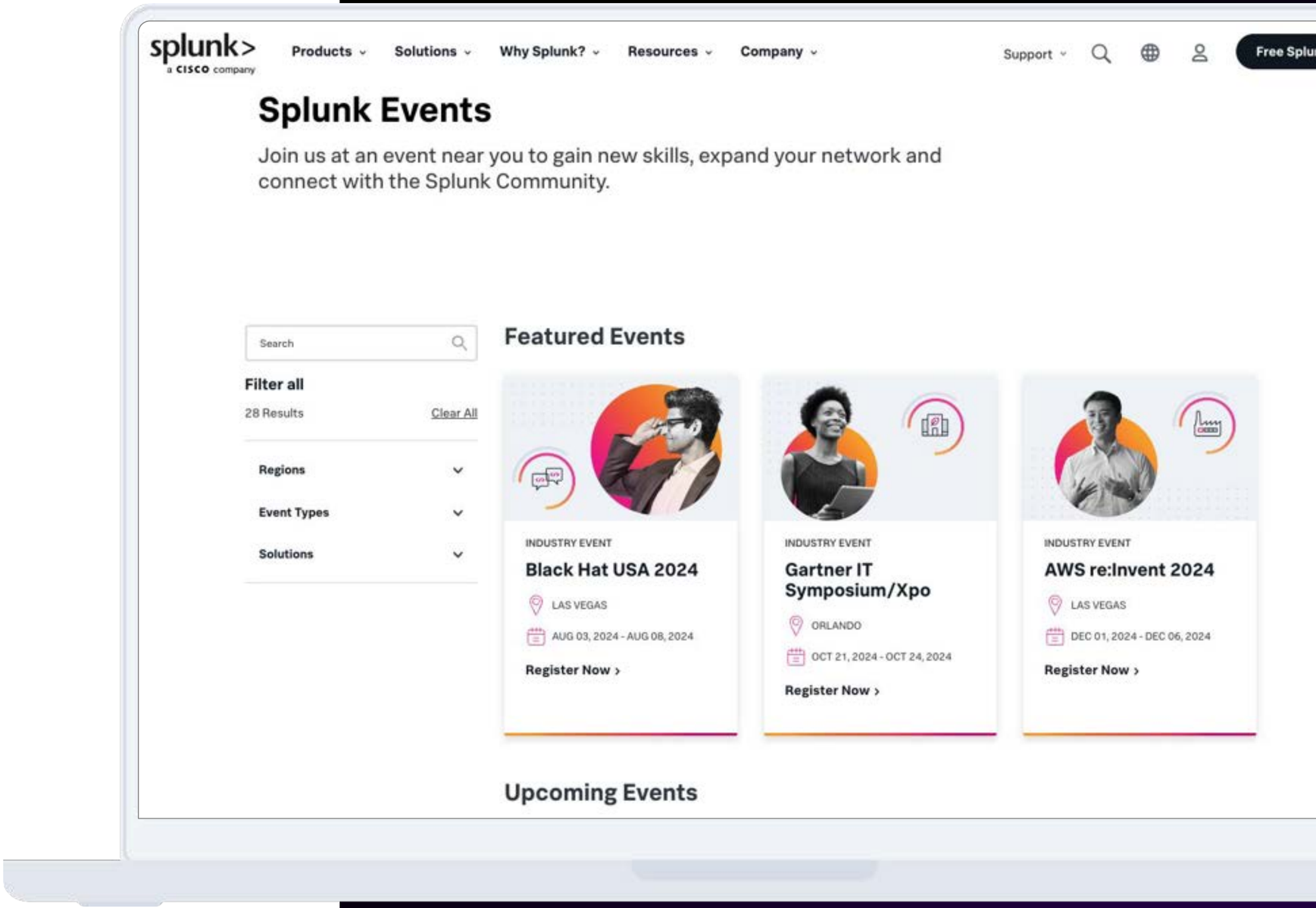
https://splunk.com/events

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

.conf

https://conf.splunk.com

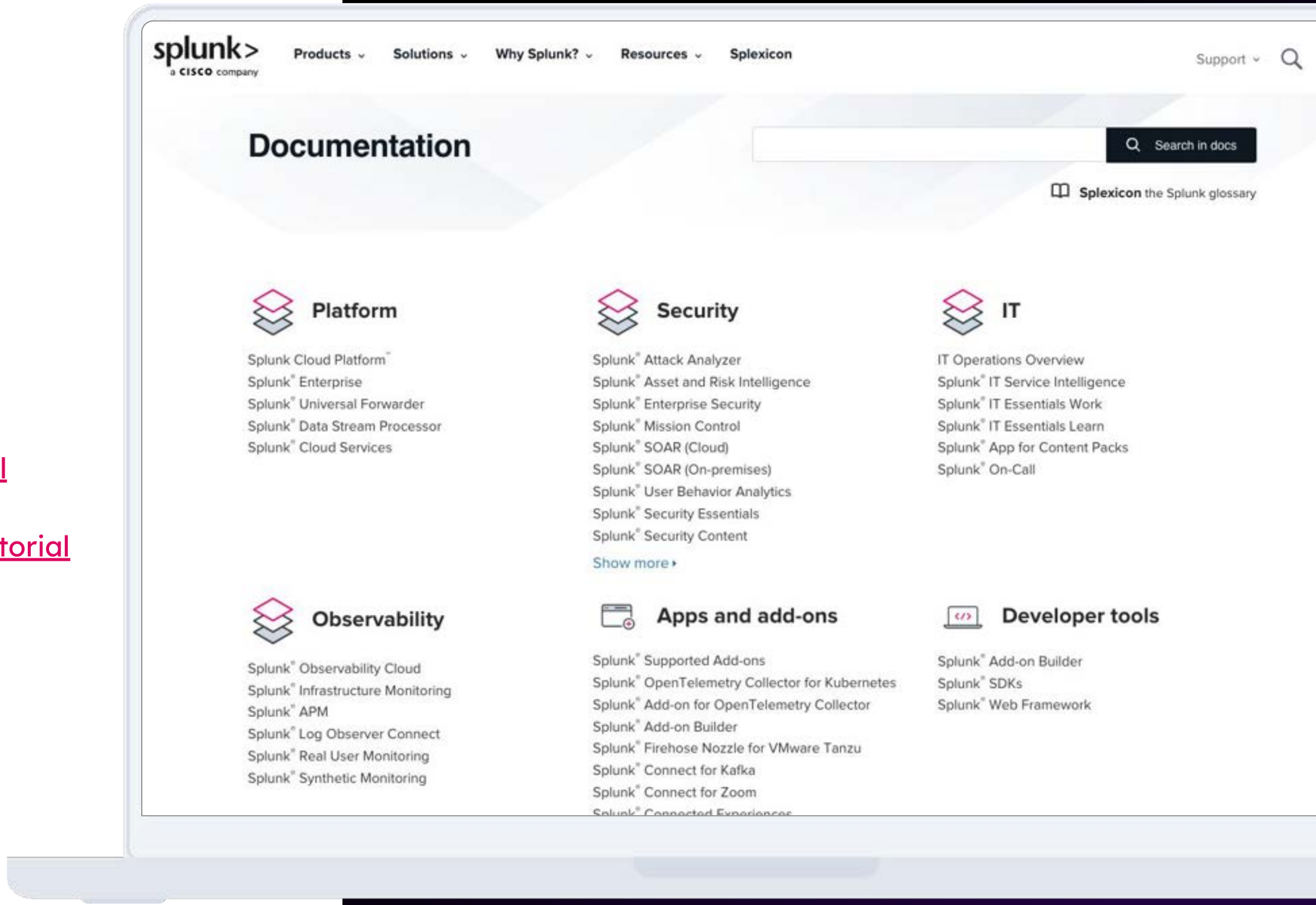
- Join us at .conf!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!



Documentation

https://docs.splunk.com

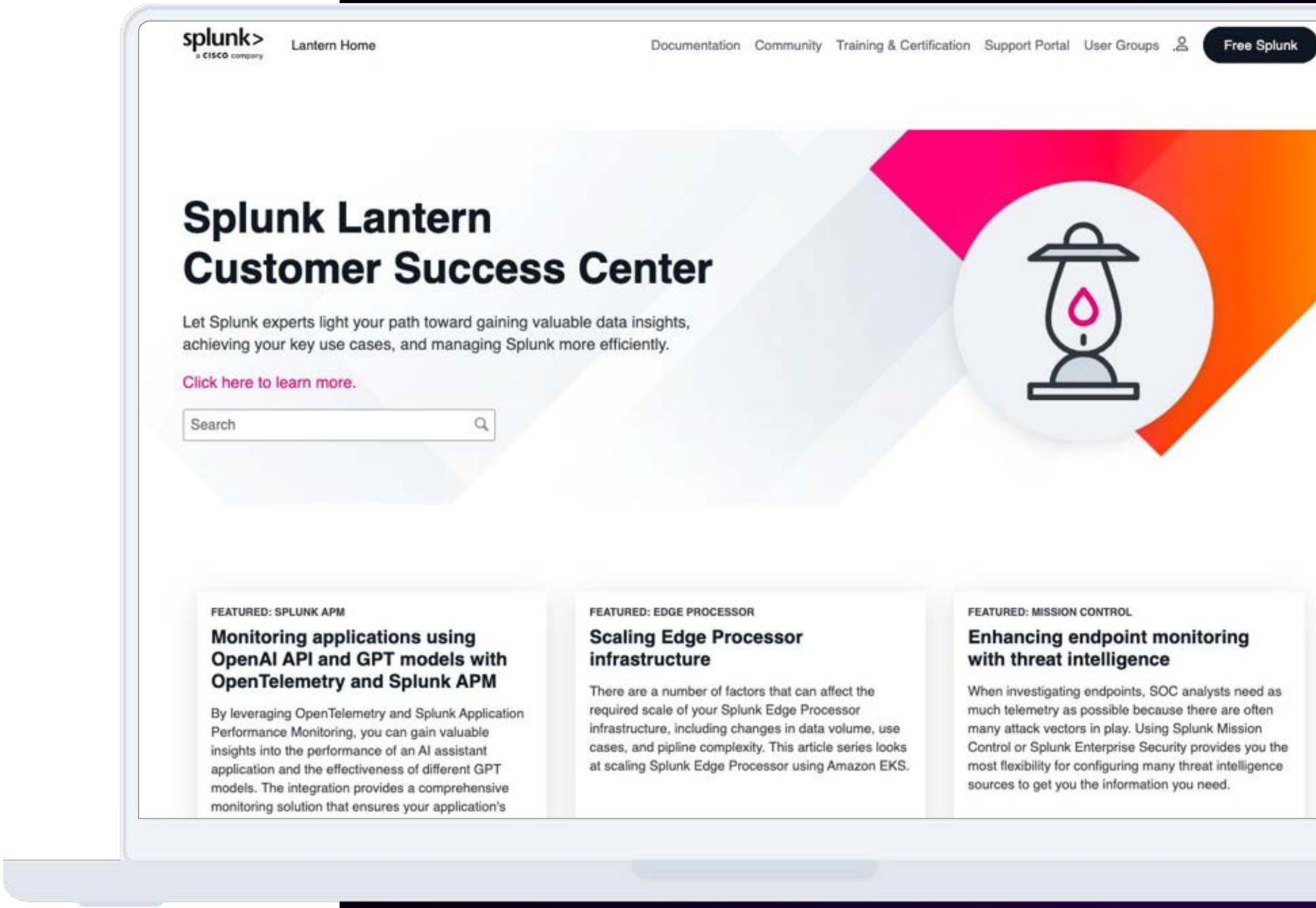
- Search reference for SPL
- Step-by-step tutorials
  Search:
  https://splk.it/SplunkSearchTutorial
  Dashboard Studio:
  https://splk.it/SplunkDashStudioTutorial
- Product references
- Procedures/guides
- And more!



Splunk Lantern

https://lantern.splunk.com

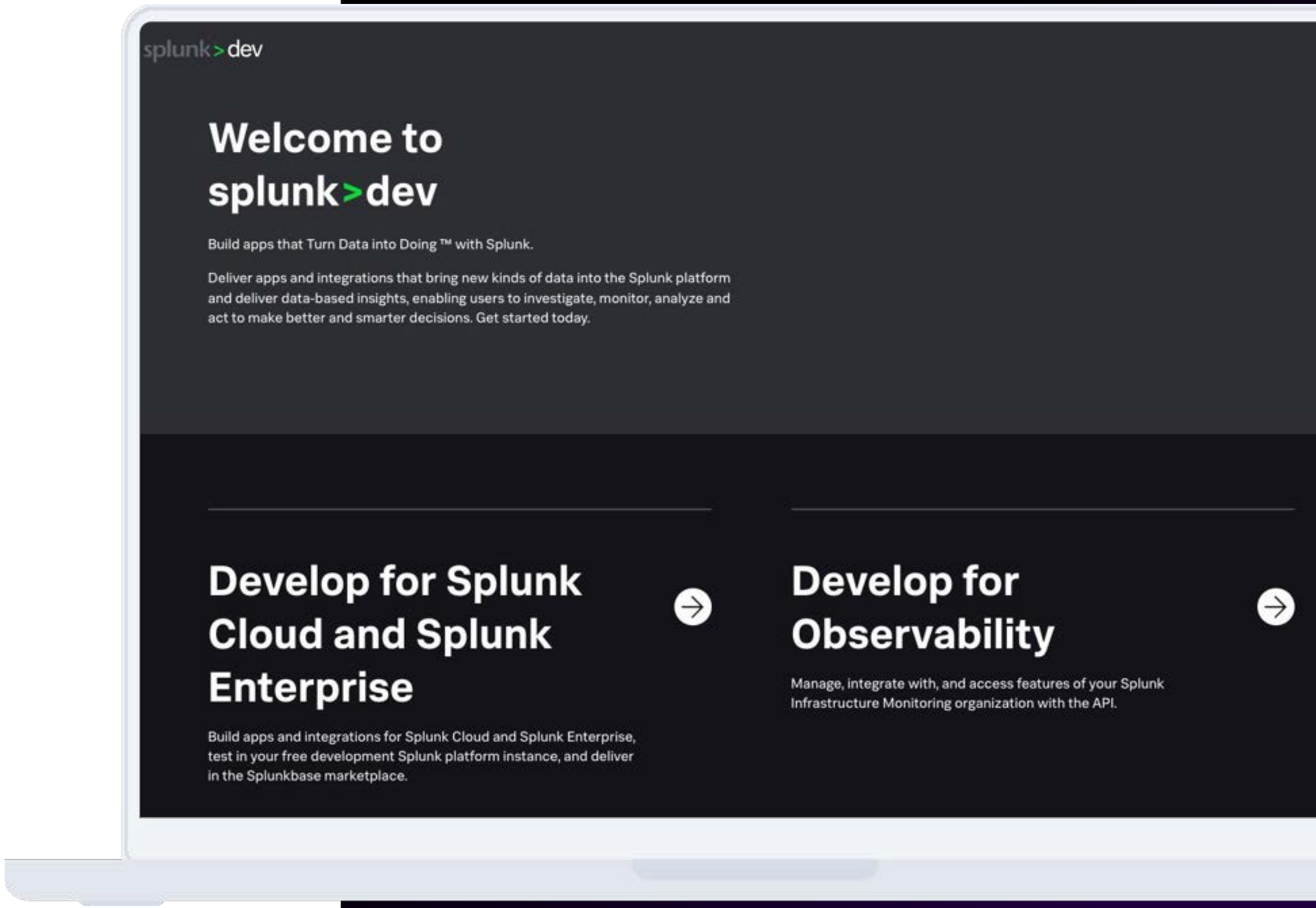
- Use case library
- Product tips
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to increase the value of Splunk across your organisation



Developer Resources

https://dev.splunk.com

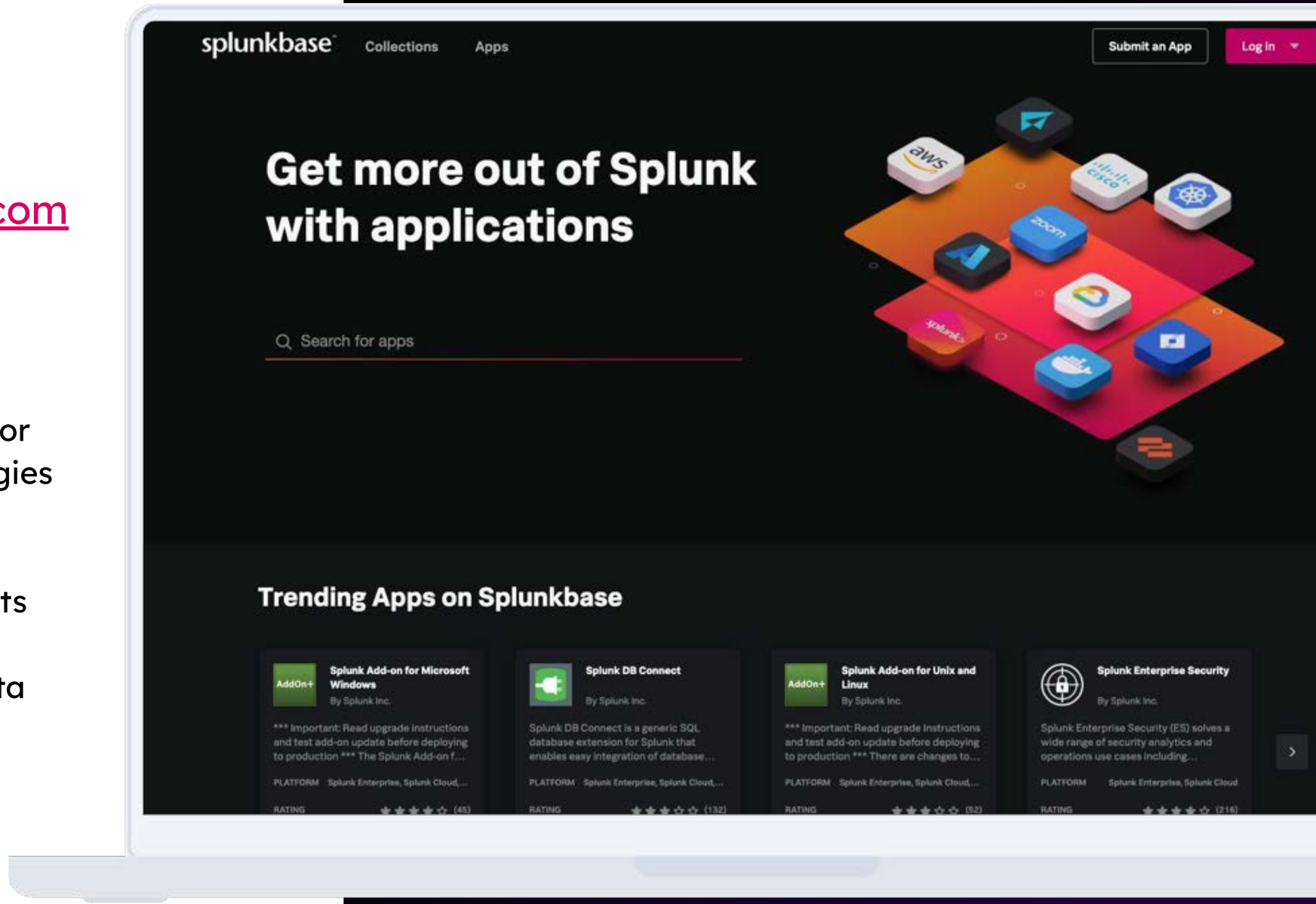
- Developer Guide
- API Reference
- Tutorials
- Downloads
  APIs, libraries, tools
- Code examples
- Free Developer licence



Splunk Apps & Add-ons

https://splunkbase.splunk.com

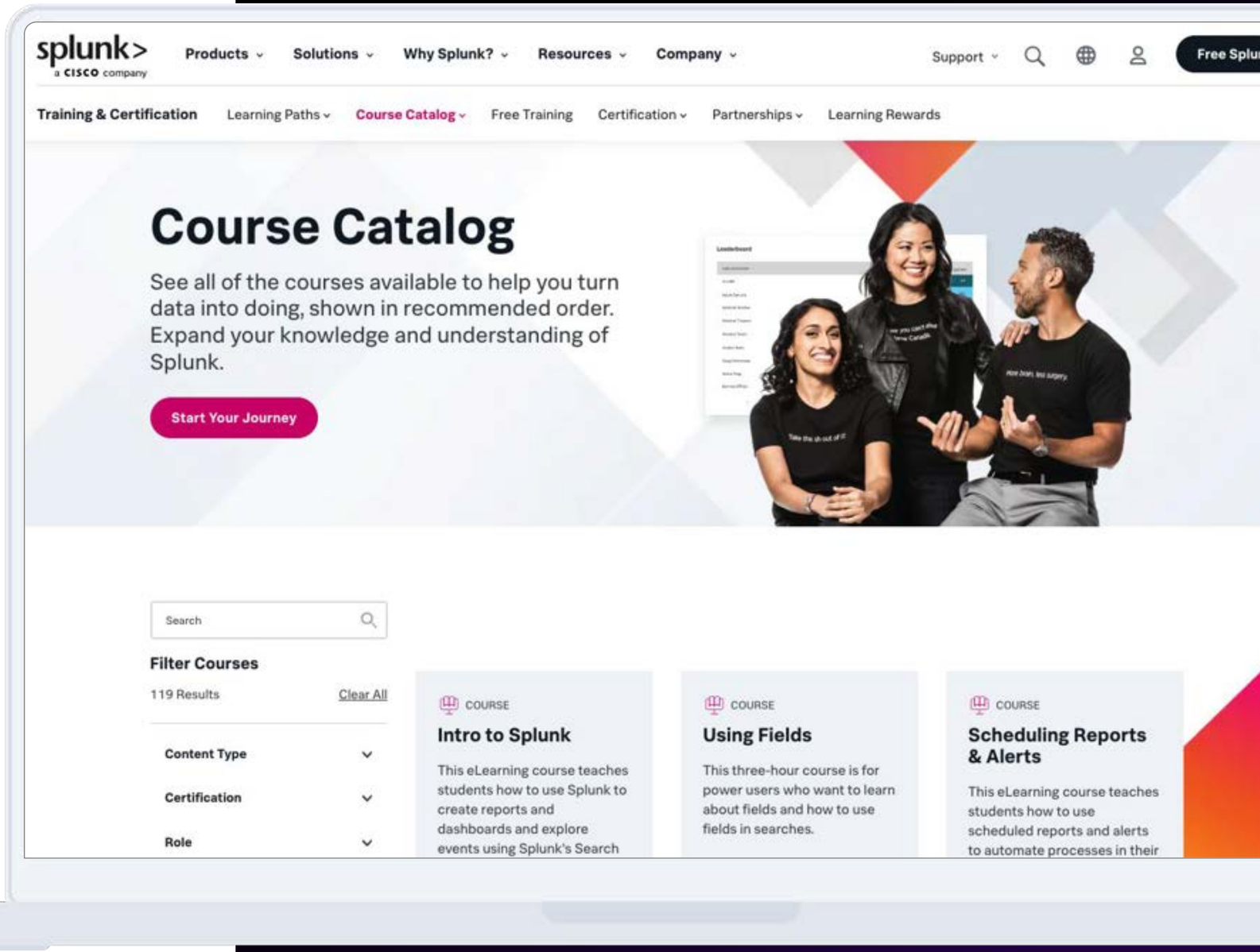
- 2100+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



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



Thank you

splunk> a CISCO company

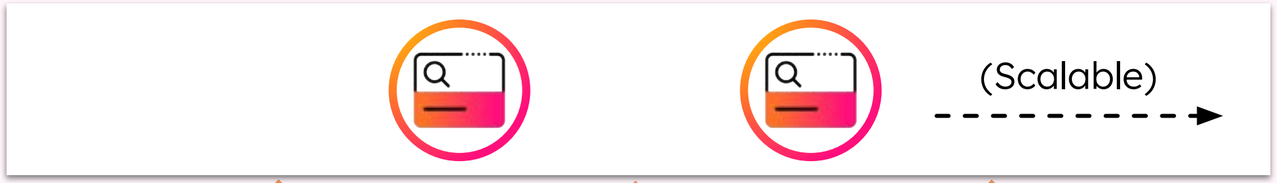
Appendix

Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability

splunk>cloud
Public or private cloud
On-premise

Searches are run on **Splunk Search Heads**



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

Data is processed on **Splunk Indexers**

- 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**

- 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`

- Alerts
- Application State (deprecated)
- Authentication
- Certificates
- Change
- Change Analysis (deprecated)
- Data Access
- Databases
- Data Loss Prevention
- Email
- Endpoint
- Event Signatures
- Interprocess Messaging
- Intrusion Detection
- Inventory
- Java Virtual Machines (JVM)
- Malware
- Network Resolution (DNS)
- Network Sessions
- Network Traffic
- Performance
- Splunk Audit Logs
- Ticket Management
- Updates
- Web

Splunk Common Information Model (CIM)

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