



# Using Splunk Enterprise Security

# Document Usage Guidelines

---

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Do not distribute

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

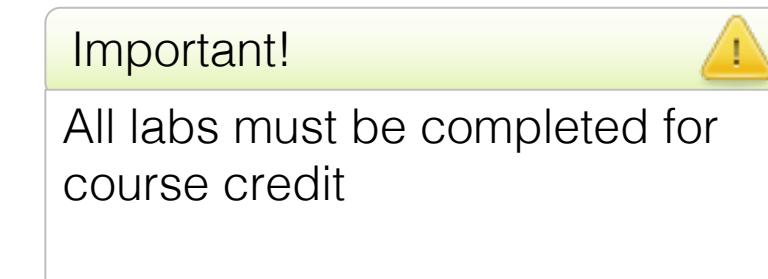
# Foundational Knowledge

---

- To be successful, students should have a solid understanding of the following courses:
  - What is Splunk?
  - Intro to Splunk
  - Using Fields
  - Visualizations
  - Search Under the Hood
  - Introduction to Knowledge Objects
  - Introduction to Dashboards

# Course Goals

- Use Splunk Enterprise Security (ES) to detect and identify security-related threats
- Create investigations to determine root causes of malicious or anomalous events
- Discover previously unknown types of potential threats



# Course Outline

---

Module 1: Introduction to ES

Module 2: Security Monitoring & Incident Investigation

Module 3: Risk-Based Alerting

Module 4: Assets & Identities

Module 5: Investigations

Module 6: Security Domain Dashboards

Module 7: User Intelligence

Module 8: Web Intelligence

Module 9: Threat Intelligence

Module 10: Protocol Intelligence

Appendix A: Reports, Dashboards, Data Models, and ES Content Updates

Appendix B: Event Sequence Engine

Appendix C: Interfacing with Splunk Intelligence Management (TrueSTAR)

Appendix D: Cloud Security Dashboards

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Module 1: Introduction to Enterprise Security

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

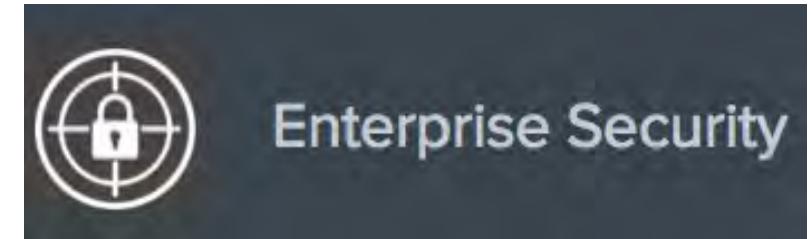
# Objectives

---

- Explain how Splunk Enterprise Security (ES) helps security practitioners prevent, detect, and respond to threats
- Give an overview of the features and capabilities of ES
- Describe data models, correlation searches, and notable events
- Define ES user roles
- Explain Splunk Web access to Splunk for Enterprise Security

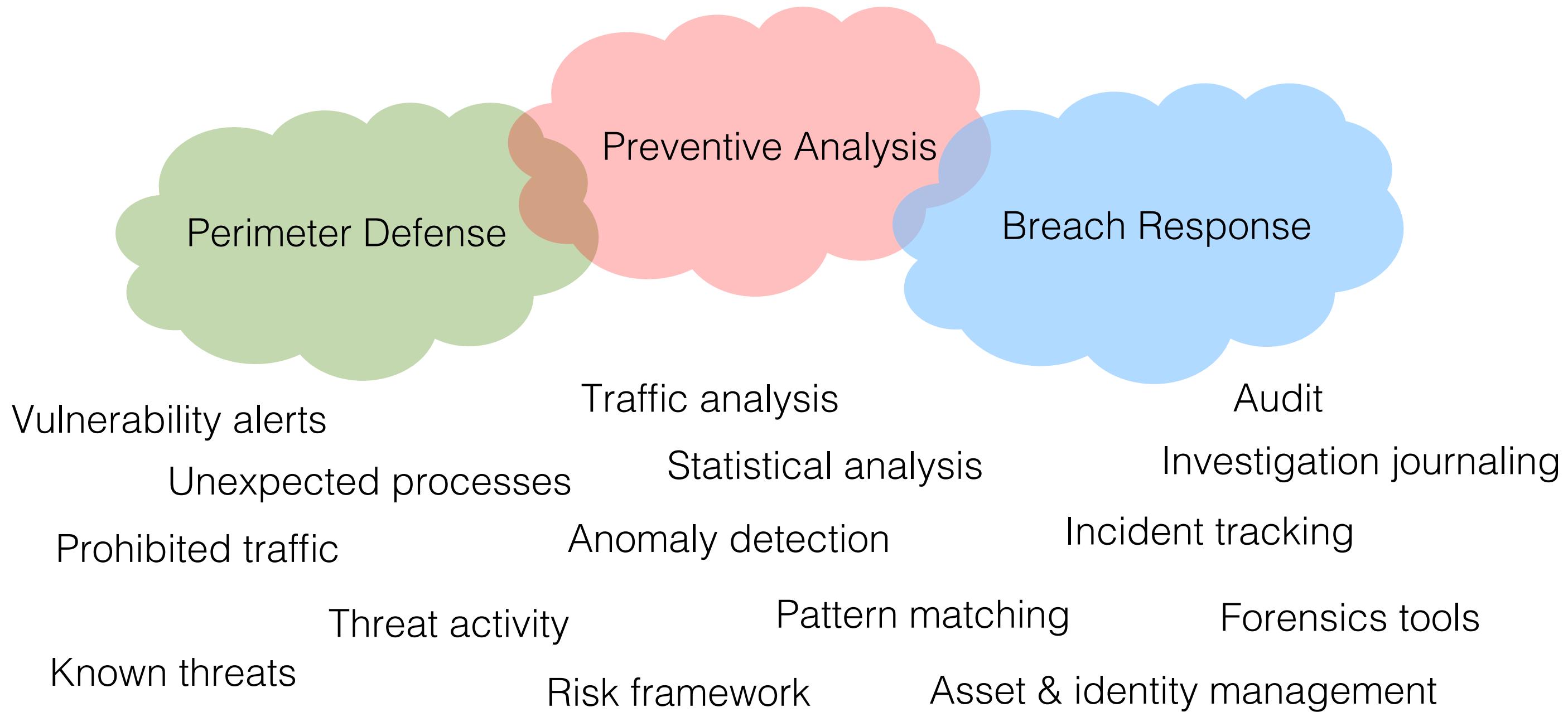
# Overview of Splunk Enterprise Security

- Built on the Splunk Operational Intelligence platform
  - ES is a Splunk app, installed on a Splunk server
- Leverages Splunk's powerful search capabilities
- Provides tools for security practitioners to detect and respond to security threats and incidents
- Efficiently manage, analyze, and mitigate security breaches
- Highly customizable for your specific enterprise requirements
- Real-time, scalable, context-aware, focused on content
- Makes all data — not just your “security data”— relevant to your security effort



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# ES Functional Areas



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# ES Use Cases

- Malware protection
  - Detection
  - Use DNS data to identify “Patient Zero”
  - Zero-day investigations
- Insider threat
  - Data exfiltration
  - Suspicious privileged account activity
- User Behavior
  - Track threatening user behavior
  - Classify accounts based on privileged access

Note 

Refer to the [Splunk Enterprise Security Use Cases](#) documentation for a detailed list.

# ES Detecting APTs

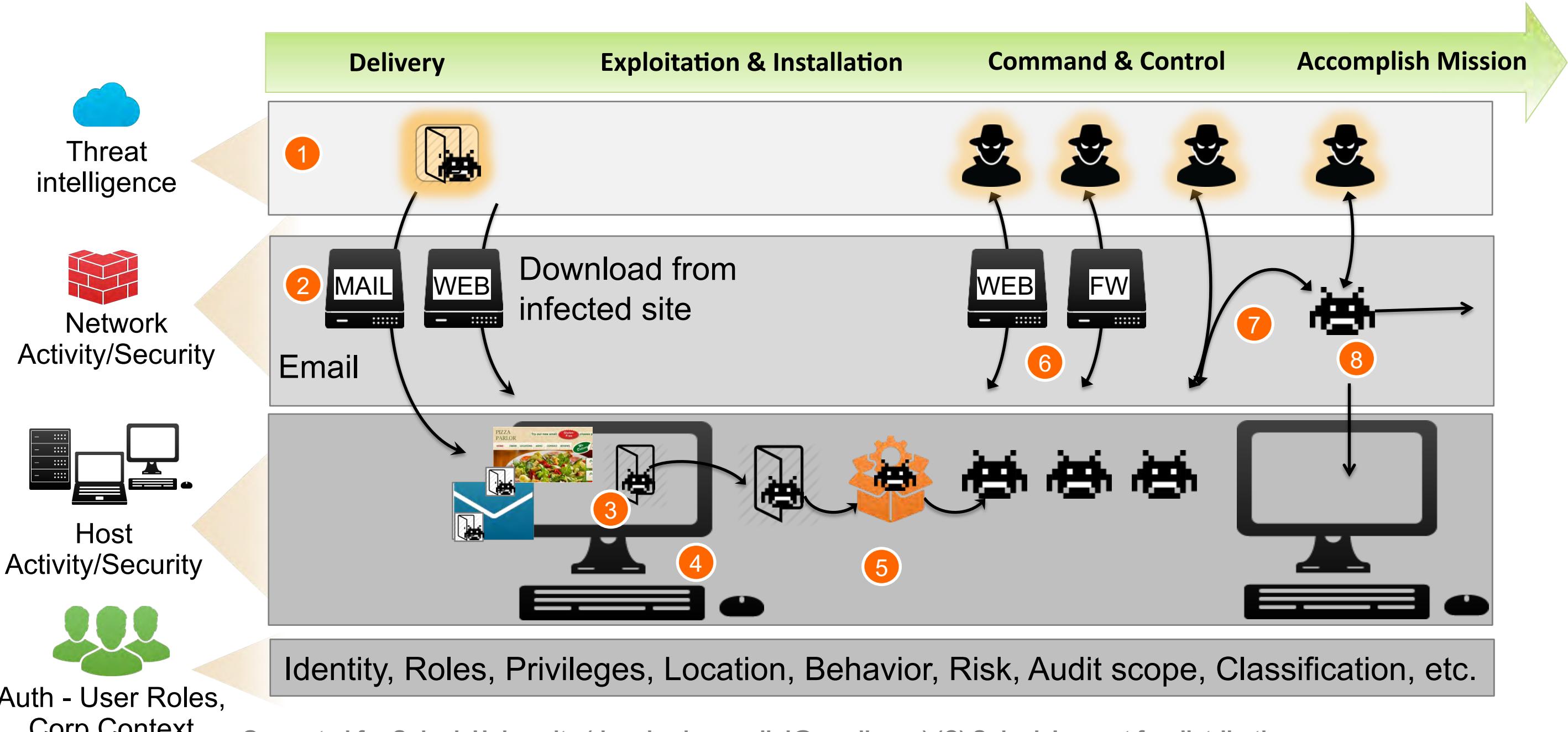
---

- Enterprise Security can help detect and prevent malicious cyber attacks like Advanced Persistent Threats (APTs)
- An APT is a growing, global threat aimed at undetected insertion, long-term viability, extraction/delivery of valuable information
  - Focused attack on specific systems like Equifax (130 million people), Petya, WannaCry
  - Targets: business, government, individuals
  - Many delivery methods
  - Metamorphic/polymorphic coding
  - Constantly changing and adapting

<https://www.splunk.com/blog/2015/06/17/opm-apt-and-the-need-for-personalized-threat-intelligence.html>

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# APT Attack - Example



# The Kill Chain

Attackers use the kill chain methodology to devise and implement their attacks, but defenders can also use the kill chain to counter and those prevent attacks

Stage	Attacker Activity	ES Countermeasures
Delivery	Email, website malware, social engineering, etc.	Threat lists, vulnerability scanning, real-time monitoring, access monitoring
Exploitation / Installation	Open attachment, download from site, upload from memory stick, etc.	Protocol Intelligence, file system alerts, intrusion detection, port monitoring
Command and Control	Execute code, open/copy files, change configuration, etc.	Malware tracking, process alerts, change alerts, analytics
Accomplish mission	Upload payload to remote server, disable services, etc.	Traffic alerts, network analysis, audits

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

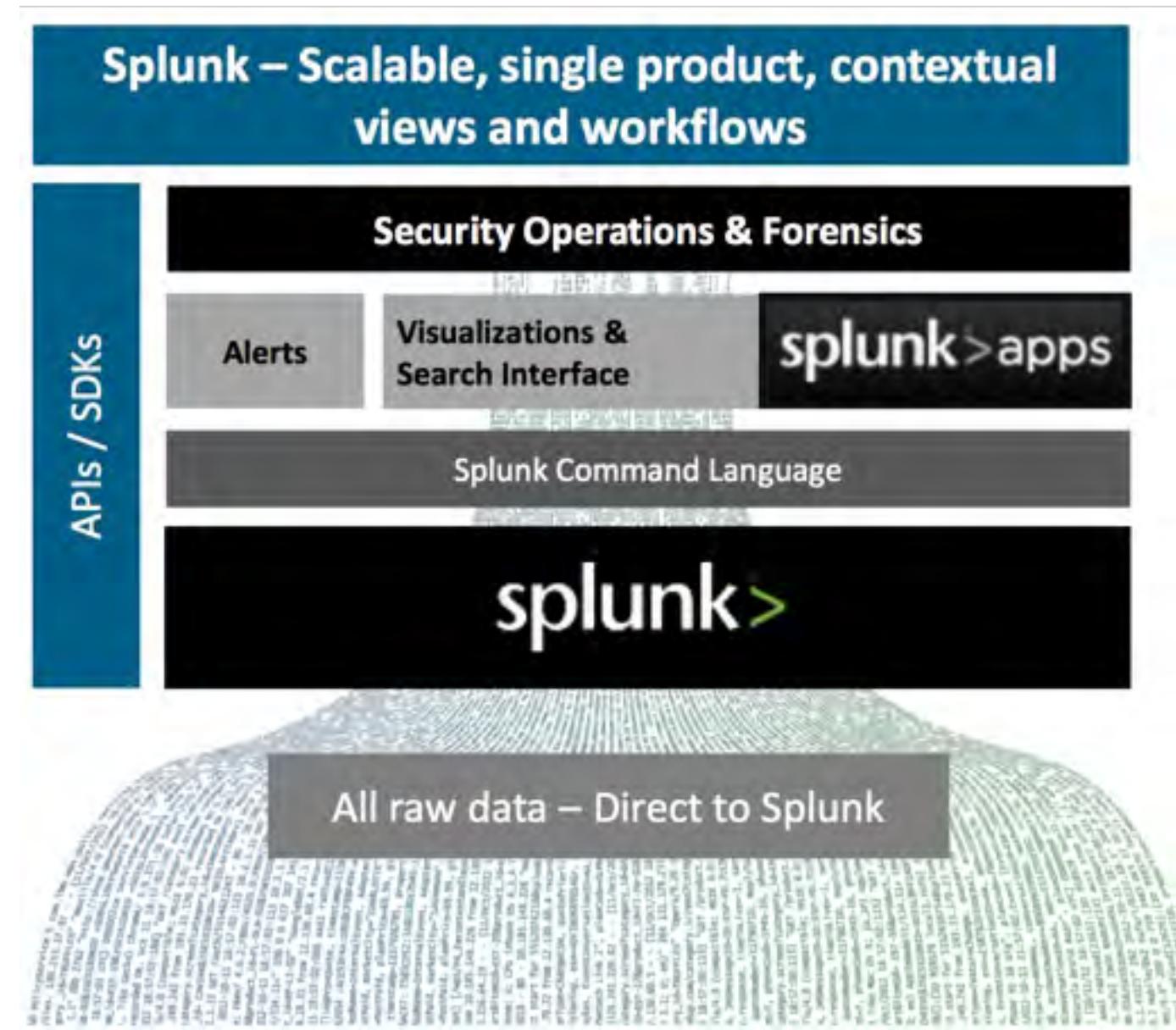
# Who Uses ES?



Security Analysts



SOC Staff



**Splunk – Scalable, single product, contextual views and workflows**

**Security Operations & Forensics**

**APIs / SDKs**

**Alerts**

**Visualizations & Search Interface**

**splunk>apps**

**Splunk Command Language**

**splunk>**

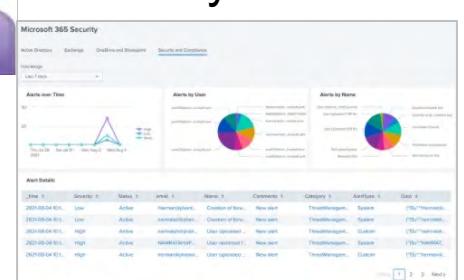
All raw data – Direct to Splunk



Security Exec/Managers



Security Auditors



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# How ES Works

## Raw Events are Indexed

Data is generated, forwarded, and indexed into Splunk



**Data is available for ES**  
| **tstats** queries and dashboards can now use the data



## Data Model Summary Searches Run

CIM DM normalization is applied, CIM DM key/value pairs are stored in DM TSIDX

**ES Searches for Threats and Anomalies**  
ES creates notable events which are stored in summary indexes and are searchable by data models



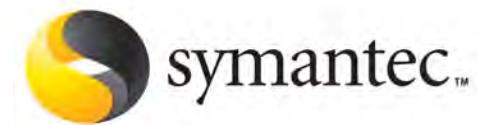
## ES Background Searches (content) Process Data

Correlation Searches, trackers, and threat intelligence search data models

# How ES Works (cont.)

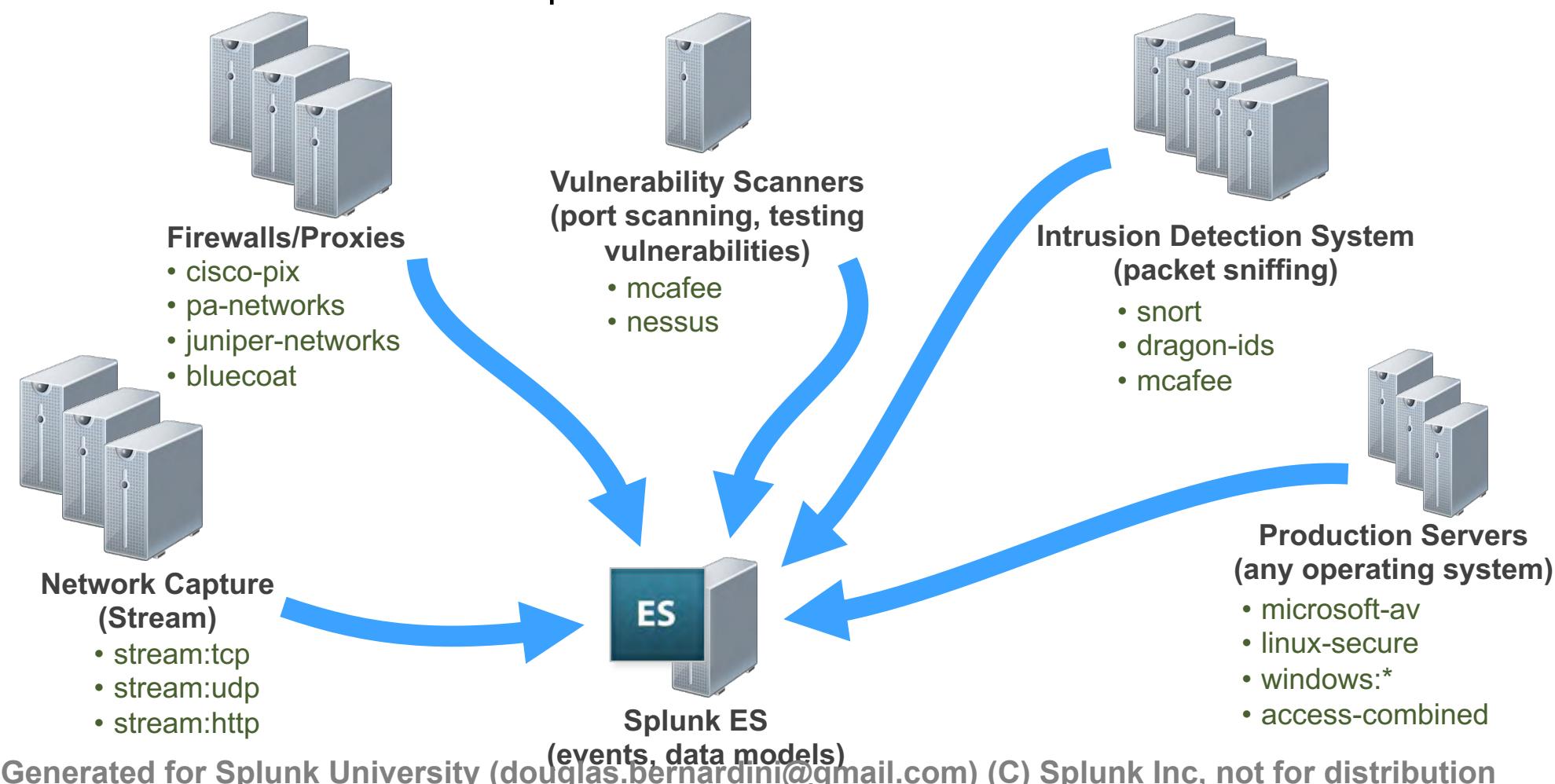
- Security-related data is acquired by add-ons in your enterprise from servers, routers, etc.
  - This data is forwarded to Splunk indexers and stored as events
- ES runs searches (real-time or scheduled) for indicators of threats, vulnerabilities, or attacks
  - If a search discovers something that needs attention, ES displays it on one or more of its dashboards
  - You can then investigate the issue, track it, analyze it, and take the appropriate action

vmware® Carbon Black



# ES Data Flow

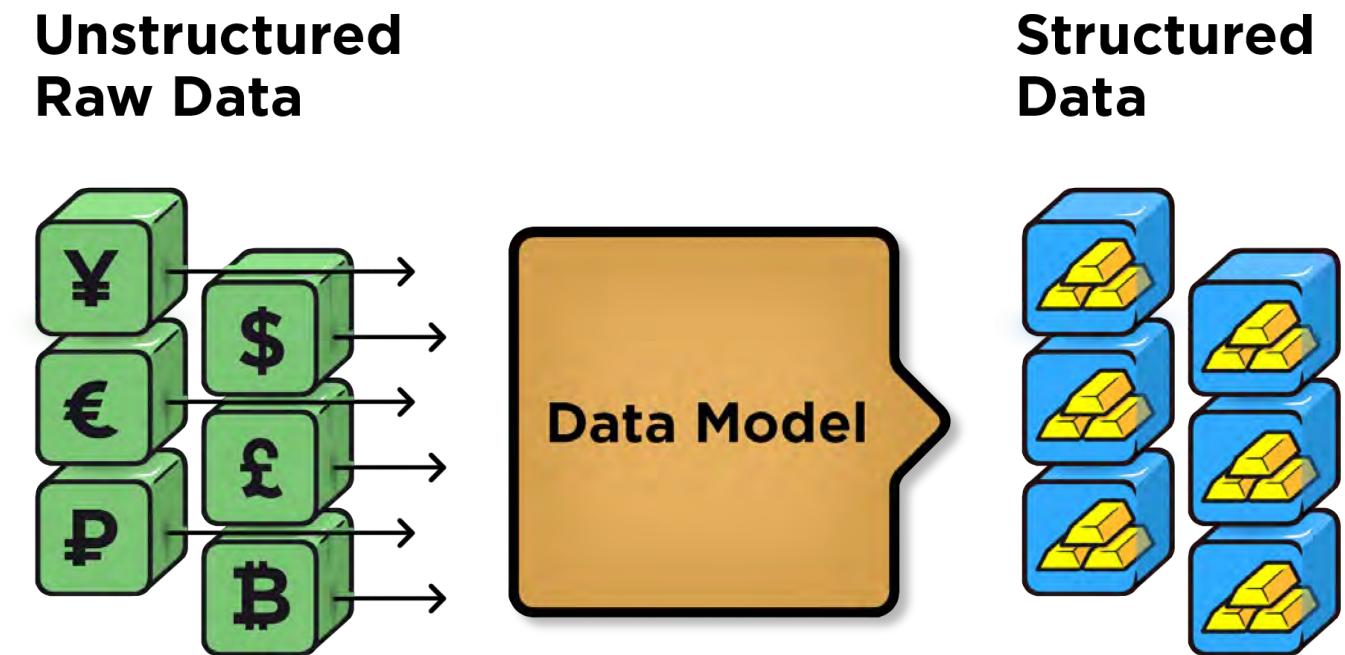
- Security-related data is acquired by add-ons in your enterprise from servers, routers, firewalls, and other network appliances
  - This data is forwarded to Splunk indexers and stored as events



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Data Models

- Data models normalize data
- Data models provide a more meaningful representation of unstructured raw data
- ES depends heavily on *accelerated* data models
- Accelerated data models provide a “speedup” factor
- Use `| tstats` searches with `summariesonly = true` to search accelerated data



# ES Dashboards and Data Models

---

- How does raw security data become available to ES dashboards?
  1. Splunk or a custom add-on indexes and sourcetypes the raw data
  2. Events are mapped and normalized to Splunk Common Information Model (CIM) data models
  3. Events are referenced by the accelerated CIM data models
- Most ES correlation searches, dashboards, and reports use the accelerated data models
- You can create your own custom searches based on the events in your index(es) or associated with your accelerated data models

# tstats Search Example

The screenshot shows a Splunk search interface titled "New Search". The search bar contains the command: `| tstats summariesonly=t count FROM datamodel=Authentication WHERE Authentication.action=failure by Authentication.app`. The results section displays 37,663,097 events from before December 16, 2019, at 1:37:08.000 PM. The "Statistics (10)" tab is selected, showing a table of event counts by application:

Authentication.app	count
Authentication Manager	1015
login	1928794
netscreen	4064
oracle	445901
splunk	8

- Use `| tstats` to create reports based on accelerated data models
  - Use `| tstats summariesonly=t` to restrict results to accelerated data for performance improvement
- Use **Search > Datasets** to build datasets using ES data models

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# ES and The KV Store

- The KV Store stores data as key-value pairs in collections on the search head
  - Collections are containers for data, similar to a database table
  - Collections exist within the context of a given app, like SA-IdentityManagement or SA-ThreatIntelligence
  - Provides a way to manage and maintain the state of the app
- ES utilizes the KV Store to:
  - track workflow of notable events
  - store incident review status changes and comments
  - manage lookups, like assets & identities and threat intel collections  
**(inputlookup / outputlookup)**

Important!



ES relies on the KV Store.  
Never disable the KV Store!

# Correlation Searches

---

- Correlation Searches run continually in the background looking for known types of threats and vulnerabilities
  - There are a number of built-in correlation searches in ES, and more in the Use Case Library. You can also create your own searches
- When a correlation search detects any Indicators of Compromise (IOC), ES creates an alert called a **notable event**
- When a notable event is assigned to an analyst it is referred to as an **incident**
- ES enables you to track, update, and resolve incidents
  - **Security Posture** dashboard provides a cross-domain SOC overview
  - **Incident Review** dashboard is used to inspect and manage incidents

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Notable Events

---

- Correlation searches create notable events in the **notable** index
  - A notable event might indicate a breach, vulnerability, or other issue
- Notable events are created with fields, event types, and tags that provide information necessary for incident investigation and a link to the original source event(s)
- You can search for the notable events in the **notable** index
  - In ES, select Search > Search to run a manual search
  - Run a search like `index=notable` for a given time period to see the notable events
  - Event **source** field shows the correlation search that created the notable event

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Assets and Identities

---

- Notable event urgency is based on the priority of the **assets and identities** in your environment
  - **Assets**: devices in your enterprise, like routers and servers
    - Identified by IP address or MAC address
  - **Identities** are people in your enterprise
    - Identified by username, email address, etc.
- Both are managed in the KV Store with lookup tables
  - ES can show a meaningful name and descriptive information for a server or person instead of an IP address or user ID

# Beyond Notable Events

---

- ES provides many advanced tools which can be used to examine security data in detail, such as:
  - Risk and threat analysis
  - Web and user intelligence
  - Protocol (stream) intelligence
  - Other adaptive responses (send email, run script, etc.)
- These tools assist analysts to:
  - Perform forensic investigation of existing breaches
  - Analyze the environment for new threats
  - Examine the history of old breaches, understand how they happened and prevent them in the future

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# ES Roles

## ES Roles (required for ES login)

**ES User**  
*ess\_user*

Runs real-time searches  
and views all ES  
dashboards

**ES Analyst**  
*ess\_analyst*

Owns notable events  
and performs notable  
event status changes

**ES Admin**  
*ess\_admin*

Configures ES system-  
wide, including adding  
ES users, managing  
correlation searches, and  
adding new data sources

User

Power

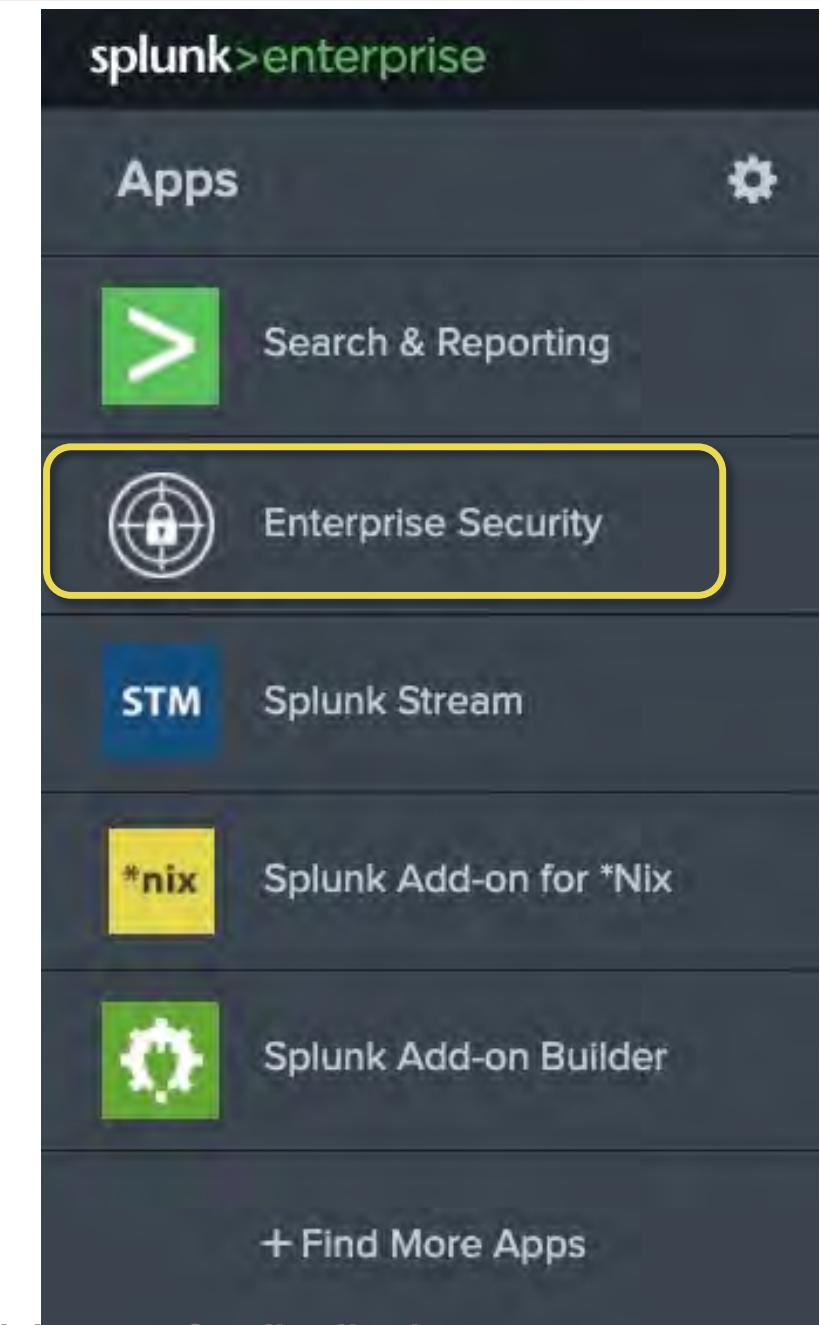
Admin

## Standard Splunk Roles

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Accessing ES

- Access Splunk Web using a URL similar to:  
**https://eshostname:8000**
- To access ES a user must have an assigned ES role on the ES server (**ess\_admin, ess\_analyst, ess\_user**)
- Once logged on, ES displays in the list of apps on the Splunk home page



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# The ES Home Page

Security Posture ▾ Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Cloud Security ▾ Audit ▾ Search ▾ Configure ▾  Enterprise Security

**ES Menus**

**Splunk Enterprise Security**  
Splunk Enterprise Security extends the security analysis functionality of the Splunk platform allowing you to centralize your security operations and easily investigate your data. Discover, triage, and investigate potential security incidents, coordinate response and remediation, review metrics across security domains, and correlate your data with threat intelligence.

**Security Posture**  
  
See real-time status of the organization's security posture over the last 24 hours  
Security Posture: monitor status

**Incident Review**  
  
Work directly with notable events  
Incident Review: work on issues

**App Configuration**  
  
Configure the application  
Configuration tools

**Documentation**  
  
View the User manual, Use Cases, and the Installation and Upgrade manual  
Documentation site

**Community**  
  
Explore Splunk Community for relevant questions and answers  
Community support

**Product Tour**  
  
Go through a product tour to understand Splunk Enterprise Security at a high level  
Product tutorial

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Module 1 Lab: Introduction to ES

---

- Time: 15 minutes
- Tasks:
  - Log into your Splunk classroom server, configure your user account, and navigate to the ES home page
  - Examine the source events ES is using to monitor the security environment and notable events

# Module 2: Security Monitoring and Incident Investigation

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Objectives

---

- Use the **Security Posture** dashboard to monitor ES status
- Use the **Executive Summary** dashboards to view security operations at high level
- Use the **Incident Review** dashboard to analyze notable events
- Take ownership of a notable event and move it through the incident workflow
- Create notable events
- Suppress notable events

# Monitoring and Response

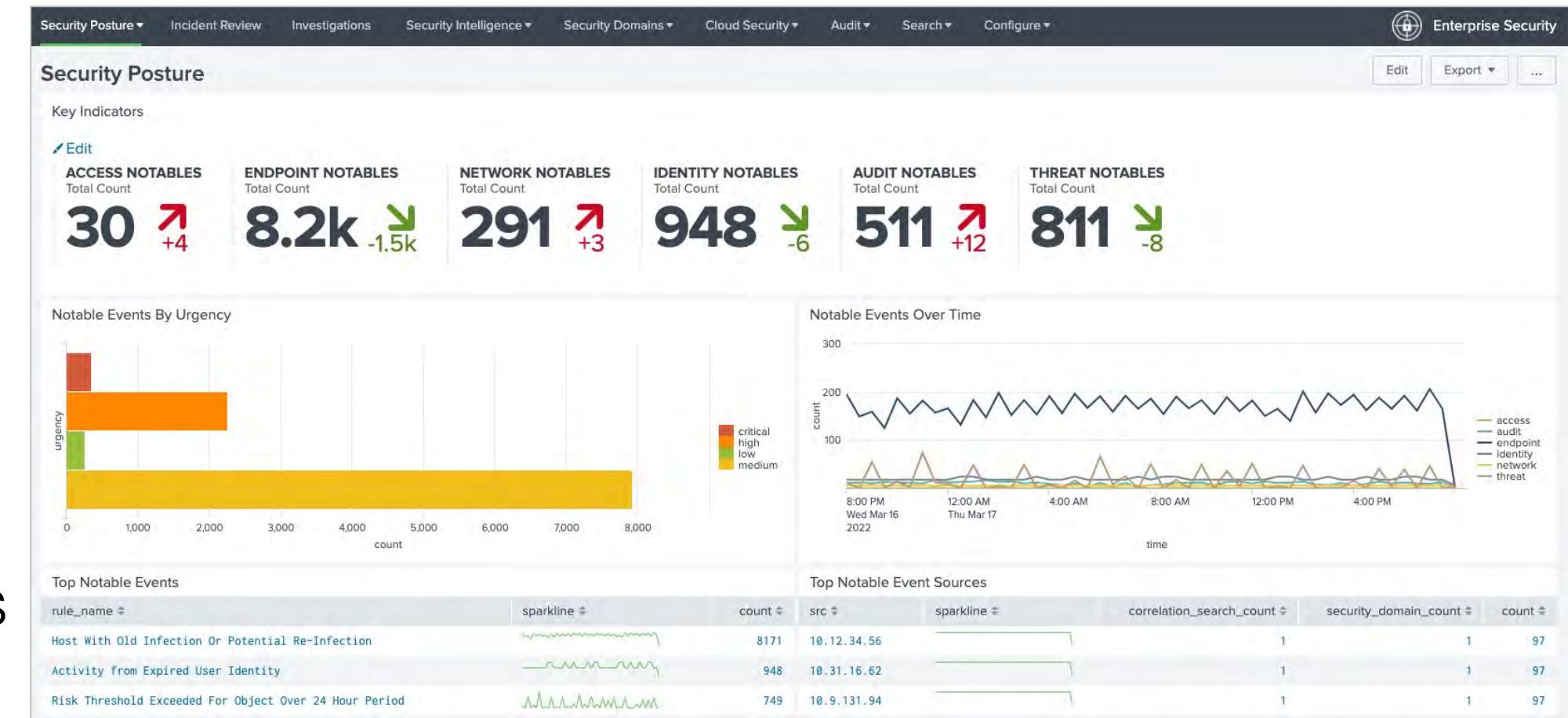
---

- ES continually runs correlation searches for known threats, vulnerabilities, authentication patterns, malware, or suspicious network traffic
  - There are over 60 built-in correlation searches, and more with the Enterprise Security Content Update (ESCU) app installed
  - Or you can create your own
- When a correlation search detects any Indicators of Compromise (IOC), ES creates an adaptive response one of which is a notable event or incident
- ES enables you to track, update, and resolve incidents
  - Security Posture dashboard provides a cross-domain SOC overview
  - Executive Summary dashboards to evaluate security trends
  - Incident Review dashboard to inspect and manage incidents

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

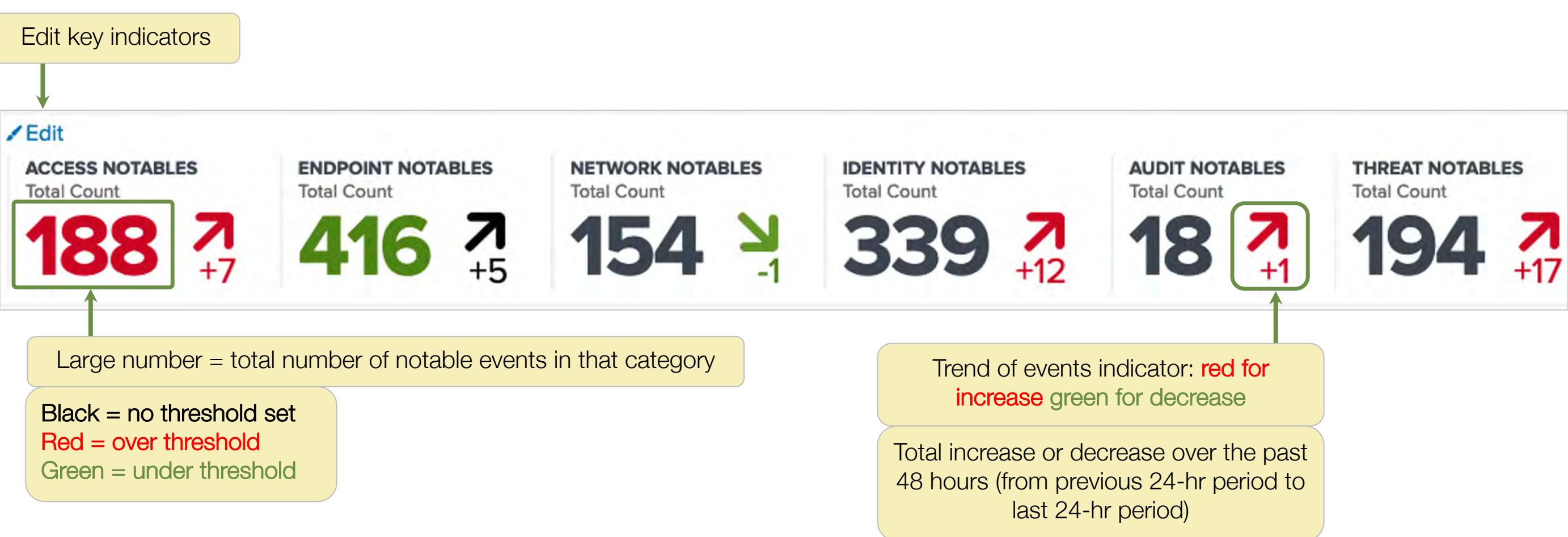
# The Security Posture Dashboard

- An overview of your Enterprise Security status
- Key Indicators (KI) at the top provide an at-a-glance view of notable event status over the last 24 hours
- The four panels provide additional summary information categorized by urgency, time, and top notable event types and sources



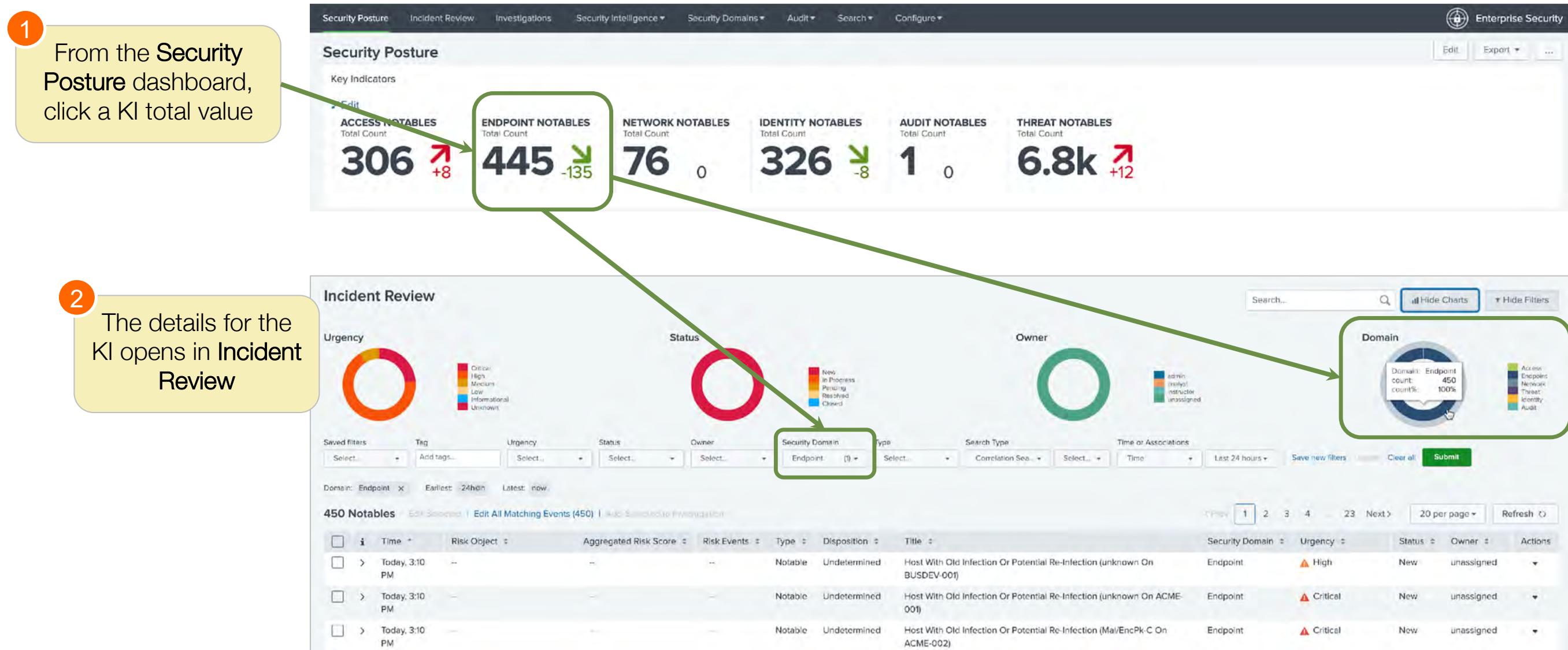
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Key Indicators (KI)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# KI Drilldown to Incident Review



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

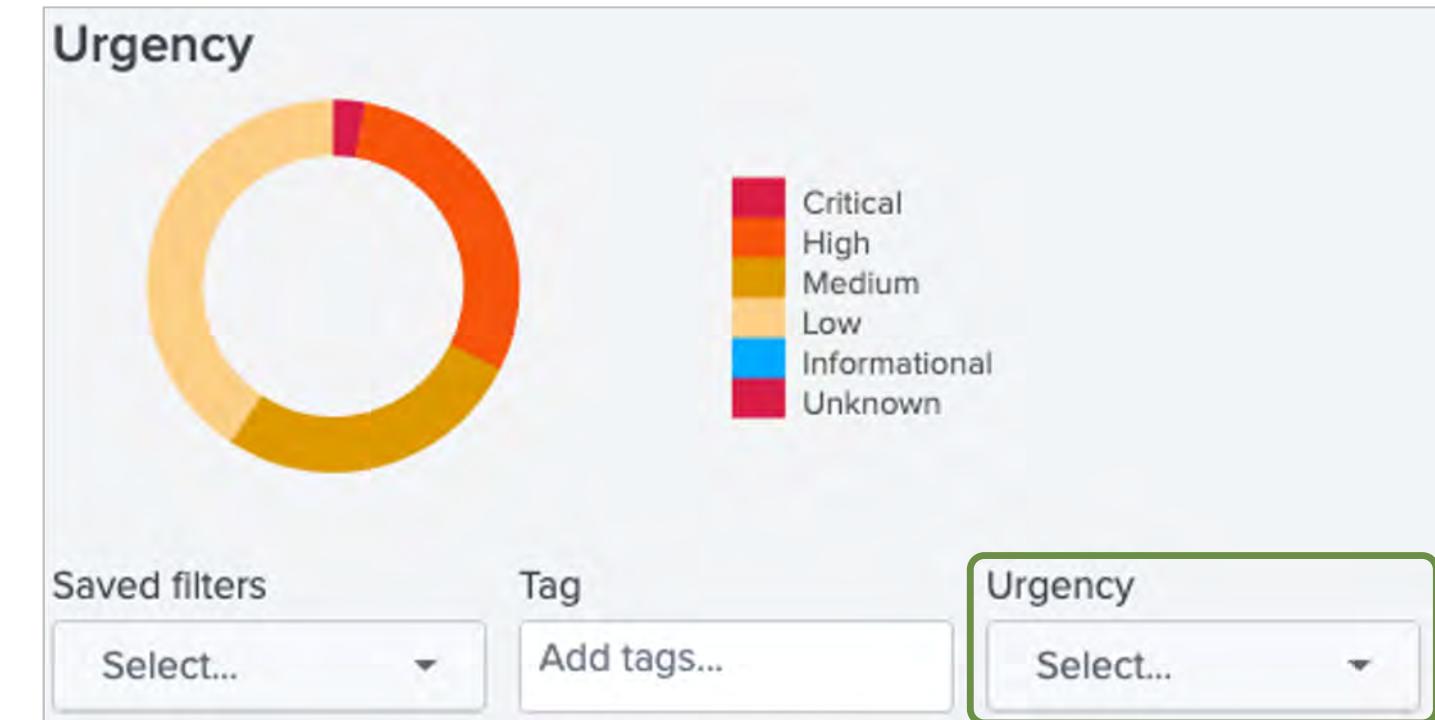
# Security Posture Panels



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Notable Event Urgency

- Each notable event has an **Urgency** field, ranging from Unknown to Critical
- Urgency is a combination of two factors:
  - **Severity**
    - Based on the severity added to the notable event by the correlation search
  - **Priority**
    - Assigned to the associated assets or identities—i.e., the server or user
    - If more than one asset or identity is involved in a single notable event, the one with the highest priority determines the urgency



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Urgency Table

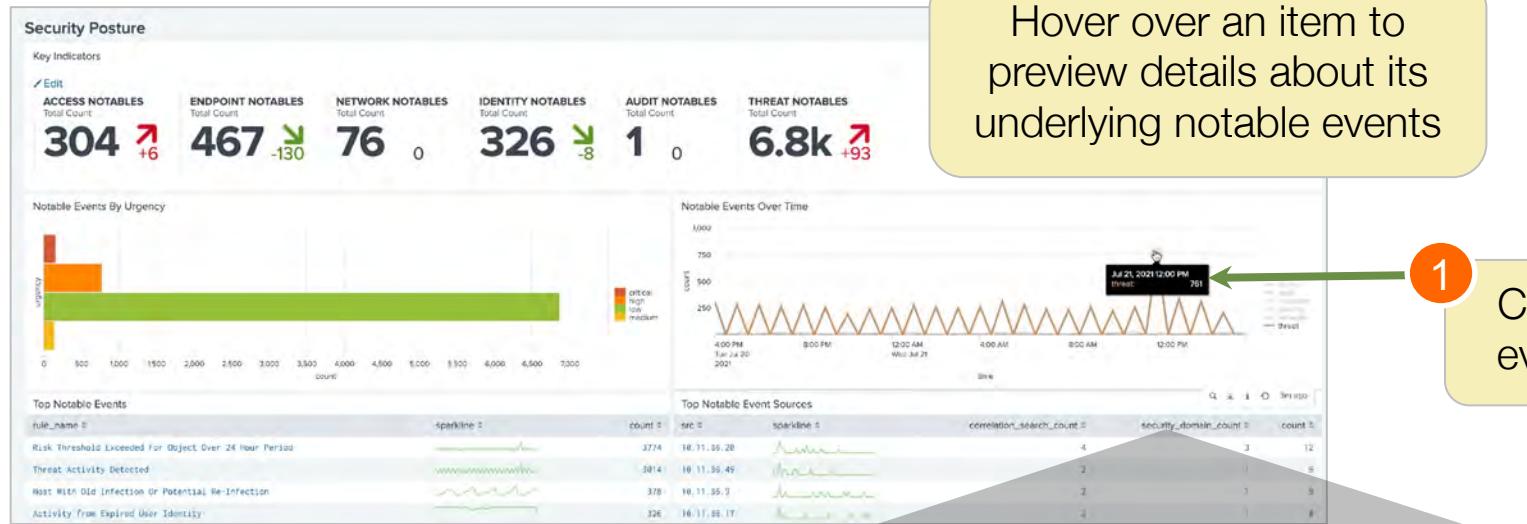
- How urgency values are calculated in notable events by default
- Can be overwritten by modifying asset/identity priority and rank, correlation search syntax, or **Urgency Levels** lookup

		Event Severity					
		Informational	Unknown	Low	Medium	High	Critical
Asset/Identity Priority	Unknown	Informational	Low	Low	Low	Medium	High
	Low	Informational	Low	Low	Low	Medium	High
	Medium	Informational	Low	Low	Medium	High	Critical
	High	Informational	Medium	Medium	Medium	High	Critical
	Critical	Informational	Medium	Medium	High	Critical	Critical

**Asset/Identity Priority + Event Severity = Urgency**

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Drilldown Support



Hover over an item to preview details about its underlying notable events

1 Click an item to open the related notable events in the Incident Review dashboard

The Incident Review dashboard allows filtering by various criteria such as Tag, Urgency, Status, Owner, Security Domain, Type, Search Type, and Time or Associations. The results show a list of 761 Notables, each with details like Time, Risk Object, Aggregated Risk Score, Risk Events, Type, Disposition, Title, Security Domain, Urgency, Status, Owner, and Actions.

761 Notables

Time	Risk Object	Aggregated Risk Score	Risk Events	Type	Disposition	Title	Security Domain	Urgency	Status	Owner	Actions
Today, 12:20 PM	unknown	33781.5	564	Risk Notable	Undetermined	24 hour risk threshold exceeded for user=unknown	Threat	High	New	unassigned	
Today, 12:20 PM	unknown	16981.5	284	Risk Notable	Undetermined	24 hour risk threshold exceeded for system=unknown	Threat	High	New	unassigned	
			2	Risk Notable	Undetermined	24 hour risk threshold exceeded for system=95.217.94.163	Threat	Low	New	unassigned	
			2	Risk Notable	Undetermined	24 hour risk threshold exceeded for network_artifacts=95.217.94.163	Threat	Low	New	unassigned	

2

- From the Incident Review dashboard:
- Drilldown into notables' details
  - Take ownership
  - Work the issue

# Incident Review Dashboard

Use charts, filters, and search to focus on specific notable events

Search... Hide Charts Hide Filters

Domain

Urgency

Status

Owner

Domain

Saved filters Tag Urgency Status Owner Security Domain Type Search Type Time or Associations

Select... Add tags... Select... Select... Select... Select... Select... Select... Select... Correlation Sea... Select... Time Last 24 hours

Save new filters Update Clear all Submit

Earliest: -24h@h Latest: now

1689 Notables Edit Selected | Edit All Matching Events (1689) Add Selected to Investigation

Disposition

Activity from Expired User Identity (dmsys)

Expand for details

Add event(s) to an investigation

Notable Events

Host With Old Infection Or Potential Re-Infection (Mal/Packer On ops-sys-003)

24 hour risk threshold exceeded for user=root

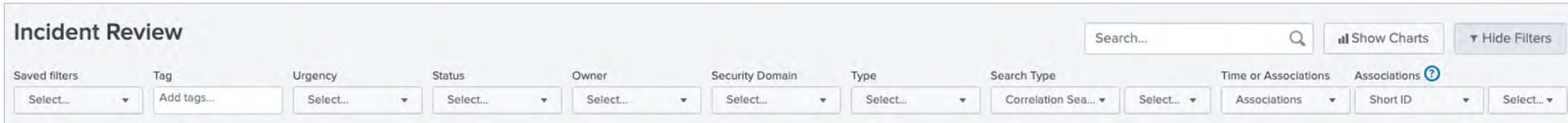
Investigation bar

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Actions menu

The dashboard displays four donut charts: Urgency (Critical: red, High: orange, Medium: yellow, Low: light green, Informational: teal, Unknown: grey), Status (New: red, In Progress: orange, Pending: yellow, Resolved: light green, Closed: teal), Owner (admin: blue, analyst: orange, instructor: green, unassigned: grey), and Domain (Access: dark blue, Endpoint: purple, Network: dark grey, Threat: yellow, Identity: light green, Audit: teal). Below the charts are filter dropdowns for Saved filters, Tag, Urgency, Status, Owner, Security Domain, Type, Search Type, and Time or Associations, along with buttons for Save new filters, Update, Clear all, and Submit. The time range is set from -24h@h to now. A table titled '1689 Notables' shows rows for various incidents, each with a checkbox, title, risk object, aggregated risk score, risk events, type, time, disposition, security domain, urgency, status, owner, and actions. A tooltip 'Expand for details' points to the first row, and another tooltip 'Add event(s) to an investigation' points to the second row. A 'Notable Events' button is centered over the table. The bottom navigation bar includes icons for investigation, search, and help, with the text 'Generated for Splunk University (douglas.borrelli@gmail.com, 2022-05-25, Splunk Inc, not for distribution)'.

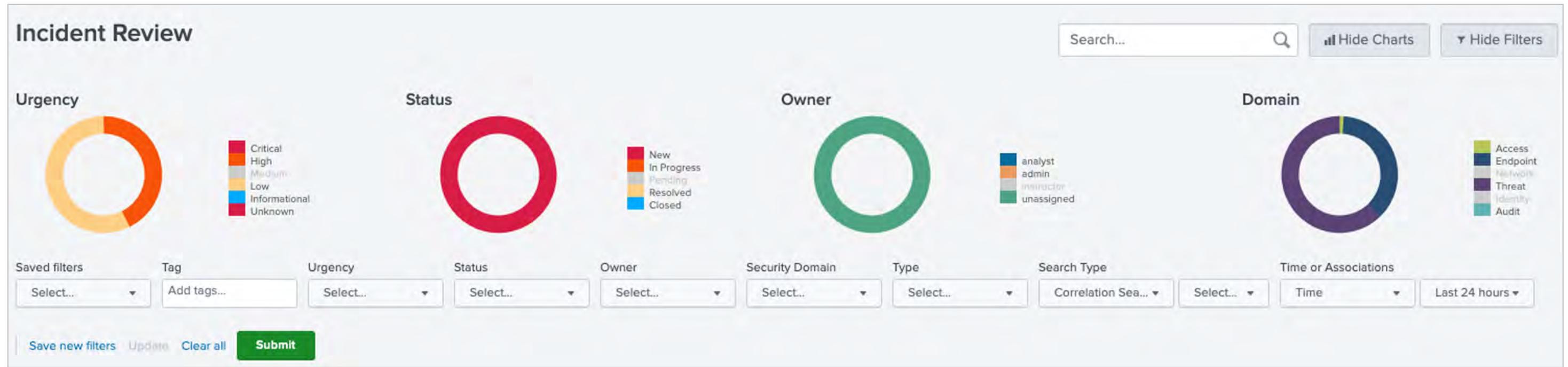
# Incident Review Filter Fields



- **Saved filters:** any filters created and saved on the IR dashboard
- **Search:** Splunk search language expressions
- **Tag:** tags configured for key/value pairs
- **Urgency:** Informational, Low, Medium, High, Critical, Unknown
- **Status:** New, In Progress, Pending, Resolved, Closed
  - Along with Owner, is used to track the status of an incident
- **Owner:** user assigned to investigate and resolve an incident
- **Security Domain:** Access, Endpoint, Identity, Network, Threat, Audit
- **Type:** Notable or Risk Notables
- **Search Type:** The title of a correlation search or configured sequence template
- **Time or Associations:** time range, short ID or Running Template

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Using the Incident Review Dashboard



- Search supports full SPL and wildcard search
- Adding one or more values per field, values are ORed together
- Urgency values can be toggled on and off
  - Gray values are “off” and will not be searched
- If values are set for more than one field, the fields are ANDed together
- Status, Owner, Security Domain and Tag support multiple OR values

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Notable Event Details

The screenshot shows the Notable Event Details page in Splunk Enterprise Security. The top navigation bar includes columns for Title, Risk Object, Aggregated Risk Score, Risk Events, Type, Time, Disposition, Security Domain, Urgency, Status, Owner, and Actions. A notable event titled "Excessive Failed Logins" is selected, highlighted by a green border around its title and the "Actions" button.

**Description:**  
The system 10.11.36.9 has failed sshd authentication 1133 times using 104 username(s) against 1 target(s) in the last hour.

**Additional Fields**

	Value	Action
Application	sshd	▼
Source	10.11.36.9 <span style="background-color: red; color: white; padding: 2px 5px;">1800</span>	▼
Source Business Unit	emea	▼
Source Category	pci	▼
Source City	havant	▼
Source Country	uk	▼
Source Latitude	50.84436	▼
Source Longitude	-0.98451	▼
Source PCI Domain	wireless	▼
Source Should Time Synchronize	trust	▼
Source Should Update	true	▼
Short ID	true	▼

**Event Details:**

	Value
event_id	406BED13-4DD4-4AB3-B4A3-4349824AAFE0@@notable@@003c6c529e9cf426d4325689e25fe140
event_hash	003c6c529e9cf426d4325689e25fe140
eventtype	modnotable_results
	nix-all-logs
	notable
Short ID	<a href="#">Create Short ID</a>

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
[Access - Excessive Failed Logins - Rule](#)

**History:**  
[View all review activity for this Notable Event](#)

**Contributing Events:**  
[View all login failures by system 10.11.36.9 for the application sshd](#)

**Adaptive Responses:**

Response	Mode	Time	User	Status
Notable	saved	2021-08-03T14:16:11+0000	admin	✓ success
Risk Analysis	saved	2021-08-03T14:16:11+0000	admin	✓ success

[View Adaptive Response Invocations](#)

**Next Steps:**

No next steps defined.

**Note**

You cannot expand an event until the search is complete. Not all incidents have all the same detail items.

Fields for the notable event, with Action menus for each field

Notable event Actions menu

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Create a Short ID from Event Details

Scroll to the bottom of the details for a notable event to see the Event Details section and create a Short ID for the event

**Event Details:**

event_id	406BED13-4DD4-4AB3-B4A3-4349824AAFE0@@notable@@2877f9bafcdc4471bec35fddf44093b8
event_hash	2877f9bafcdc4471bec35fddf44093b8
eventtype	modnotable_results
nix-all-logs	
notable	

**Short ID**    **Create Short ID**

1 Click Create Short ID for ES to automatically generate a short ID that makes it easier to find and share a notable event

**Event Details:**

event_id	406BED13-4DD4-4AB3-B4A3-4349824AAFE0@@notable@@2877f9bafcdc4471bec35fddf44093b8
event_hash	2877f9bafcdc4471bec35fddf44093b8
eventtype	modnotable_results
nix-all-logs	
notable	

**Short ID**    **VM4NAE**

2 The Short ID replaces the Create Short ID link

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Create a Short ID: Notable Event Actions

The screenshot shows a table of Notable events for 'Excessive Failed Logins'. The 'Actions' dropdown menu is open, listing options: Add Event to Investigation, Build Event Type, Extract Fields, Run Adaptive Response Actions, Share Notable Event (which is highlighted with a green border), Suppress Notable Events, and Show Source.

1 From the notable event Actions drop-down, creating a Short ID is possible using Share Notable Event

The 'Share Event' dialog box displays a 'Short ID : BAKQU0' button (highlighted with a green border) and a 'Link To Event : https://44.242.173.100/en-US/ap...' field with a copy icon (highlighted with a green border). Below the link, instructions say: 'Click the right icon to copy the link, or drag the icon into your bookmarks bar to bookmark the link.'

2 In addition to creating a Short ID, it enables sharing the event via a link:

- Click the Bookmark button to copy the link for sharing  
or
- Click and drag the Bookmark button to your Bookmarks bar to save the link

3 Close

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Search for a Short ID or Investigation

The screenshot shows the Splunk search interface with three main sections:

- Top Bar:** Shows "Time or Associations" (highlighted with a green box), "Associations ?" (dropdown menu open), "Short ID" (dropdown menu open), and "BAKQU0 (1)" (dropdown menu open).
- Search Results Panel:** A modal window titled "BAKQU0" contains:
  - "Select All Matches" button
  - "Clear All Matches" button
  - A dropdown menu with "BAKQU0" selected (highlighted with a blue box and checked checkbox).
- Bottom Panel:** Includes buttons for "Save new filters", "Update", "Clear all", and a large green "Submit" button. Below these buttons is the text "Associations: Short ID: BAKQU0".

Three numbered callouts provide instructions:

- Step 1:** Select Associations from the Time or Associations menu, and Short ID from the Associations menu.
- Step 2:** Click inside the filter field and enter all or part of a Short ID (drop-down appears and filters as you type)  
Or  
Click and scroll to the Short ID
- Step 3:** Click Submit

**Note:** You can search for one or multiple Short IDs.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Field Action Menu

- Each notable event field has an **Action** menu allowing you to:
  - Investigate the asset, set tags or search Google. Depending on the field type other options may be available
- Risk scores for systems or users are displayed next to fields
  - Click a risk score to open the **Risk Analysis** dashboard for that asset or identity

The screenshot shows a Splunk interface for managing notable events. A specific event is selected, displaying its title, risk object, aggregated risk score, and risk events. The event title is "High Or Critical Priority Host With Malware Detected". The aggregated risk score is 9560, which is highlighted with a red box and an arrow pointing to a note at the bottom right. The note says, "Scroll the menu to make sure you see all the available field actions." The interface includes a "Description" section with a summary of the event and a "Additional Fields" table. The table lists various destination-related fields with their corresponding values. An "Action" button is located in the top right corner of the table area.

Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time
High Or Critical Priority Host With Malware Detected	-	-	--	Notable	Toda AM

**Description:**  
A high or critical priority host (HOST-003) was detected with malware.

**Additional Fields**

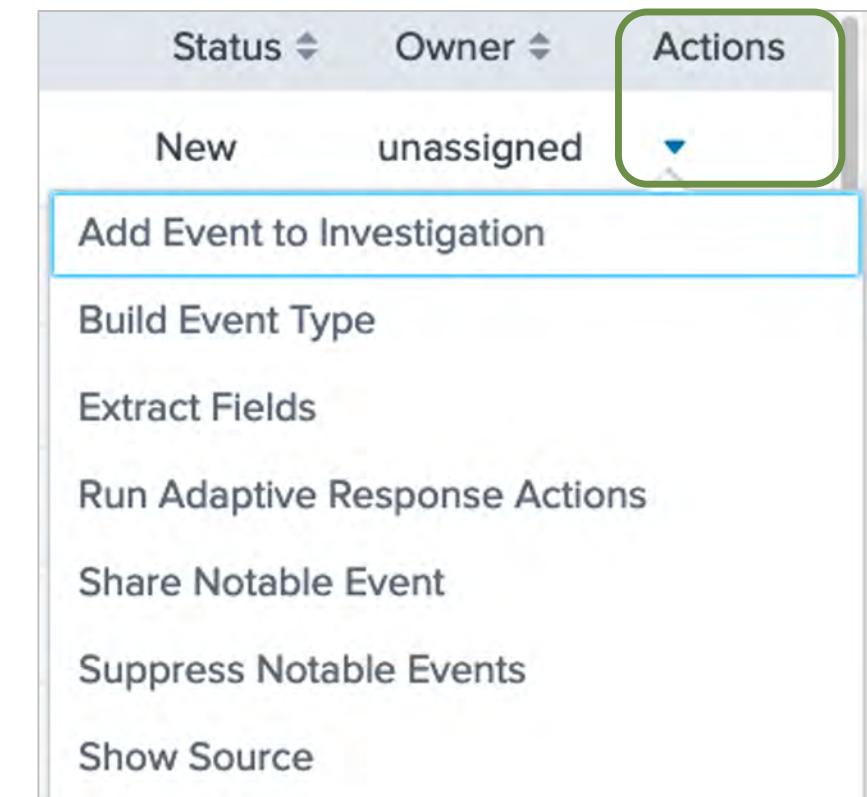
Value	Action
HOST-003	9560
emea	Edit Tags
pci	Access Search (as destination)
havant	Access Search (as source)
uk	Asset Center
50.84436	Asset Investigator
-0.98451	Map HOST-003
host-003	Intrusion Search (as destination)
wireless	Intrusion Search (as source)
trust	
true	
true	
Le	

**Note**  
Scroll the menu to make sure you see all the available field actions.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Notable Event Actions Menu

- Each notable event has an **Actions** menu with options related to the event, such as:
  - Adding the event to an investigation
  - Suppressing the notable event
  - Sharing the notable event with others
  - Initiating further adaptive response actions



# Incident Workflow: Concepts

1. Assign an owner
2. Examine the incident
3. Implement corrective measures

Analysts are responsible for changing workflow status values as they work incidents

ES Admins can define, add new status values and assign values to different roles, so the statuses in your environment may differ

**New** - not yet being worked

**In Progress** - analysis underway

**Pending** - various: work in progress, awaiting action, etc.

**Resolved** - fixed, awaiting verification

**Closed** - fix verified

Note



When a notable is assigned an owner, it is tracked as an incident in the KV Store.

# Incident Workflow: Procedures

The screenshot shows the Splunk Enterprise Security interface with two main panels: '1201 Notables' and 'Edit Events'.

**1201 Notables Panel:**

- Header: 1201 Notables, Edit Selected, Edit All Matching Events (1201), Add Selected to Investigation.
- Left sidebar: Title, Host With Old Potential Re-Infection (unknown On SE), Abnormally High Number of HTTP GET Request Events By, Abnormally High Number of HTTP GET Request Events By 10.5.26.95.
- Right sidebar: Risk Object, Risk Event.
- Actions: A green box highlights the 'Edit Selected' button, with a callout '2 Click Edit Selected'. A yellow box contains the text: 'As needed, add selected event(s) to an investigation. It will appear under Related Investigations in the event details'.
- Bottom: Investigation Bar with icons for list, plus, and search, and the message: 'No investigation is currently loaded. Please create (+) or load an existing one (≡)'.

**Edit Events Panel:**

- Header: Edit Events, 61 Next >, 20 per page ▾, Refresh.
- Table: Shows four selected events with columns: Risk ID, Status, Urgency, Owner, Disposition, and Comment.
- Form:
  - 4 event(s) selected. You are editing selected events.
  - Status: In Progress (dropdown).
  - Urgency: High (dropdown).
  - Owner: analyst (dropdown).
  - Disposition: True Positive - Suspicious Activity (dropdown).
  - Comment: Adding a comment is optional.
- Buttons: Close, Cancel, Save changes (green button). A callout '3 Set Status, Urgency, Owner, and Disposition. Optionally, add a Comment' points to the form fields.
- Bottom: Callout '4 Click Save changes' points to the 'Save changes' button.

# Incident Review History

The screenshot shows the Splunk Enterprise Security interface with the following components:

- Top Bar:** A table with columns: Title, Risk Object, Aggregated Risk Score, Risk Events, Type, Time, Disposition, Security Domain, Urgency, Status, Owner, Actions.
- Event Detail:** An event titled "Abnormally High Number of HTTP GET Request Events By 129.188.147.104".
  - Description:** A system (129.188.147.104) was detected as generating an abnormally high number of GET request events.
  - Additional Fields:** HTTP Method (GET), Source (129.188.147.104).
  - Related Investigations:** Currently not investigated.
  - Correlation Search:** Web - Abnormally High Number of HTTP Method Events By Src - Rule [link]
  - History:** A log entry: 2021 Aug 4 9:00:49 AM by admin. Note: Adding a comment is optional. A button: View all review activity for this Notable Event [link].
  - Contributing Events:** A list of contributing events.
- Tip:** The `incident\_review` macro can be used in custom searches and reports for incident status tracking by directly accessing the KV Store.
- New Search:** A search bar with the query: `|`incident\_review` | search rule\_id="406BED13-4DD4-4AB3-B4A3-4349824AAFE0@notable@91e43fb854e11fdb7d7867023e4176e" | rename status\_label as status | fields \_time, rule\_id, reviewer, urgency, status, owner, comment`. The results show 1 result from 8/3/21 to 8/4/21. The Statistics tab is selected, showing 0 events. The results table shows a single row with the following details:

_time	rule_id	reviewer	urgency	status	owner	comment
2021-08-04 09:00:49.924	406BED13-4DD4-4AB3-B4A3-4349824AAFE0@notable@91e43fb854e11fdb7d7867023e4176e	admin	high	In Progress	analyst	Adding a comment is optional.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Notable Event Adaptive Response

- Notable events may contain further adaptive responses that an analyst can initiate (ping, nslookup, change risk, run script, etc.)
- Depending on the type of notable event, different actions are available
- Use Actions > Run Adaptive Response Actions to trigger an action

The screenshot shows a Notable Event details page. At the top, there are fields for Disposition (Undetermined), Security Domain (Identity), Urgency (High), Status (New), Owner (unassigned), and Actions. A dropdown menu under Actions includes options like Add Event to Investigation, Build Event Type, Extract Fields, Run Adaptive Response Actions (which is highlighted with a green border), Share Notable Event, Suppress Notable Events, and Show Source.

Below the header, there are sections for Related Investigations (Currently not investigated), Correlation Search (Identity - Activity from Expired User Identity - Rule), History (View all review activity for this Notable Event), Contributing Events (View activity from dmsys), and Original Event (Aug 04 15:12:56 cml.acmetech.net auth|security:info su: [ID 366847 auth.info] 'su dmsys' succeeded for root on /dev/??).

A yellow callout box points to the Adaptive Responses section, which lists two entries: Risk Analysis (Mode: saved, Time: 2021-08-04T09:15:06-0600, User: admin, Status: ✓ success) and Notable (Mode: saved, Time: 2021-08-04T09:15:05-0600, User: admin, Status: ✓ success). Another yellow callout box points to the Next Steps section, which suggests "Ping the host to see if it is active on the network".

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Triggering Actions

## Actions > Run Adaptive Response Actions

- Choose from a list of actions to run
- This list is configured by your ES admin
- You may see different options depending on availability and permissions

The screenshot shows a modal window titled "Adaptive Response Actions". Inside, there's a heading "Select actions to run." with a button "+ Add New Response Action". Below it is a search bar with a magnifying glass icon. A dropdown menu is open over a "Category All" button, listing "All", "Information Gathering", "Information Conveyance", and "Information Tracking". A yellow callout bubble points to the search bar with the text "Enter some, or all the action name to filter (list filters as you type)". The main list contains three items:

- STM Stream Capture**: Creates stream capture. Category: Information Gathering | Task: create | Subject: network.capture | Vendor: Splunk
- Nbtstat**: Runs the nbtstat command. Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System
- DNS Nslookup**: Runs the nslookup command. Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Ping Example

As you investigate, you may need to see if the affected server is up

**Adaptive Response Actions**

Select actions to run.

+ Add New Response Action **1**

**Ping**  
Runs the ping command **2**

Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System

**Adaptive Response Actions**

Select actions to run.

+ Add New Response Action

**Ping**

Host Field: Destination (dest) **3**

Max Results: 4 **4**

Index: main

Worker Set: local

Learn more about ping scans [Learn more](#)

**Run** **5**

Response	Mode	Time	User	Status	Action
Ping	adhoc	2020-05-06T16:12:03-0600	admin	✓ success	Add to Current Investigation
Notable				✓ success	Add to Current Investigation
Risk Analysis				✓ success	Add to Current Investigation

**6** Find your action in the notable event's list of **Adaptive Responses** and click **Ping** to view the results

**Note** 

If there is an investigation selected in the Investigation Bar, **Adaptive Responses** will display an Action column with the option to add the response to the current investigation.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Threat Intel Example

Similarly, you can add threat artifacts to a threat collection  
(needs to be configured by your admin first)

The screenshot shows the 'Adaptive Response Actions' interface. On the left, a modal window titled 'Adaptive Response Actions' has a step-by-step process: 'Select actions to run.' followed by '+ Add New Response Action'. Step 1 is highlighted with a red circle. Below this, a button labeled 'Add Threat Intelligence' is shown, with a callout indicating it 'Creates threat artifacts'. Step 2 is highlighted with a red circle. The main interface shows a 'Select actions to run.' section with a dropdown for '+ Add New Response Action' and a collapsed section for 'Add Threat Intelligence'. A callout for 'Add Threat Intelligence' specifies 'Threat Group to attribute this artifact to (i.e. iblocklist\_logmein (threatlist))'. The right side of the interface contains fields for 'Threat Group' (set to 'iblocklist\_logmein (threatlist)'), 'Threat Collection' (set to 'ip (ip\_intel)'), 'Field from event\*' (set to 'Destination (dest)'), 'Description\*', 'Weight' (set to '1'), and 'Max Results' (set to '100'). A callout for 'Field from event\*' specifies 'Field from event: a field in the event containing the information (i.e. dest)'. At the bottom right is a green 'Run' button.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Send to UBA Example

Automatically send correlation search results to Splunk User Behavior Analytics (UBA)

The screenshot shows the 'Adaptive Response Actions' interface. A callout box points to the 'Send To UBA' action with the text: 'Severity sets the score in UBA for the notable event (optional)'. The 'Send To UBA' action is highlighted with a green border and has a red number '2' above it. Another red number '1' is above the '+ Add New Response Action' button.

## Note

UBA must be installed on the ES search head for this Response Action to be available.

The screenshot shows the 'Send To UBA' configuration dialog. It includes fields for 'Category' (set to 'Insider Threat'), 'Severity' (set to 5), and a 'filter' search bar. A list of categories is shown, with 'Insider Threat' checked. A green 'Run' button is at the bottom right.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Adaptive Response Action Center

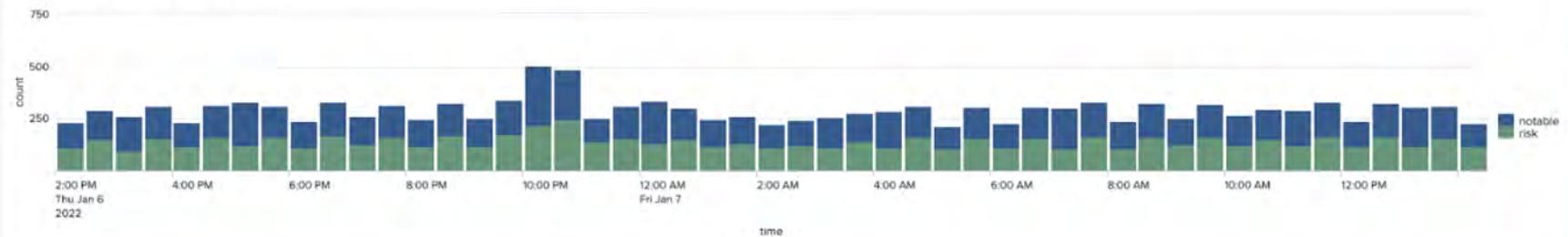
Adaptive Response Action Center

Action Mode: All | Action Name: | Action Status: All | User: All | Search ID (sid): | Last 24 hours | Submit | Hide Filters

**Edit**

<b>ACTION INVOCATIONS</b> count <b>14.3k</b> <span style="color:red">+463</span>	<b>ACTION NAMES</b> Distinct Count <b>2</b> 0	<b>ACTION SEARCH NAMES</b> Distinct Count <b>17</b> 0	<b>ACTION USERS</b> Distinct Count <b>1</b> 0	<b>ACTION SEARCHES</b> Distinct Count <b>395</b> <span style="color:red">+23</span>	<b>ACTION DURATION</b> Average (ms) <b>13.1</b> <span style="color:green">-0.2</span>
--	---	---	---	---	---

Action Invocations Over Time By Name



Top Actions By Name

action_name	cam_category	cam_subject	action_mode	search_name	user	search_count	result_count	avg_duration (ms)
notable	Information Conveyance	splunk.event	saved	Access - Excessive Failed Logins - Rule Access - Short-lived Account Detected - Rule Audit - Personally Identifiable Information Detection - Rule Endpoint - High Number Of Infected Hosts - Rule Endpoint - High Or Critical Priority Host With Malware - Rule Endpoint - Old Malware Infection - Rule Identity - Activity from Expired User Identity - Rule Risk - 24 Hour Risk Threshold Exceeded - Rule Threat - Threat List Activity - Rule Threat - Watchlisted Events - Rule Web - Abnormally High Number of HTTP Method Events By Src - Rule	admin	314	7439	9.7

Top Actions By Search

search_name	action_name	action_mode	user	search_count	result_count
Endpoint - Old Malware Infection - Rule	notable	saved	admin	49	11422

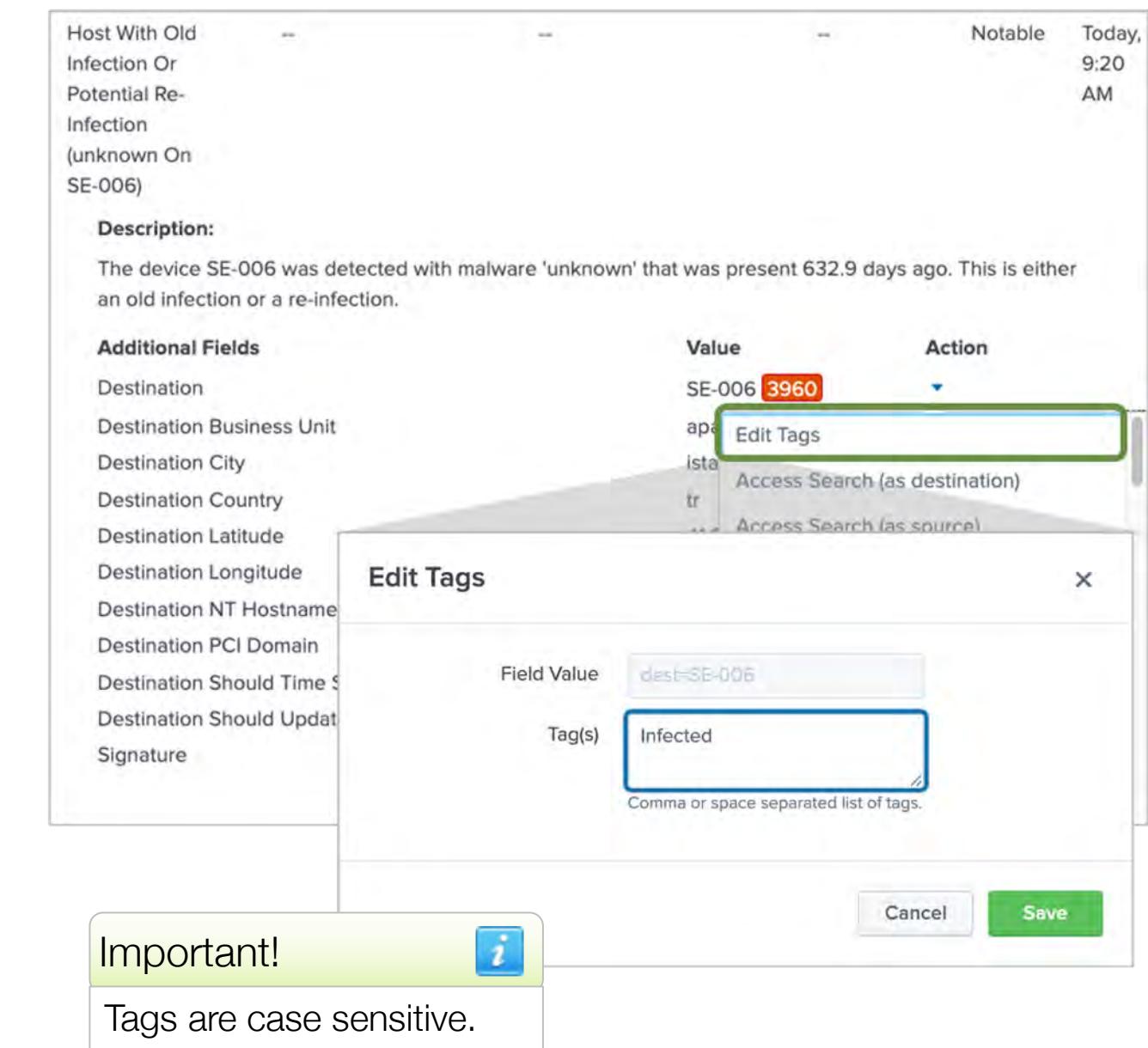
Recent Adaptive Response Actions

i	Time	Event
>	1/7/22 2:20:07.936 PM	2022-01-07 14:20:07,936+0000 INFO sendmodaction - worker="ip-10-0-0-169.us-west-2.compute.internal" signature="Modular action script duration" action_name="risk" search_name="Identity - Activity from Expired User Identity - Rule" sid="scheduler__admin_U0EtSWRlbNpdhINY5hZ2VtZW50__RND550e62b2dee006a67_at_1641565200_28167" rid="1" app="SA-IdentityManagement" user="admin" digest_mode="1" action_mode="saved" component="main" duration="7"

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Tagging Incidents

- Associate significant incidents with tags
  - Example: quickly find all incidents related to servers infected with malware
- Add a tag to each server using **Action > Edit Tags** for the **dest**, **src** or **ip** field (for this example)
- Search for tag “Infected” using the Tag filter on Incident Review
- Now only notable events with this tag value will display



# Creating and Suppressing Notable Events

---

- **Manual creation:** useful when you have source event data that has not (yet) been identified by ES as suspicious, and you want to create a notable event that will identify the issue and allow you to track it
- **Suppression:** useful if you are getting false positives from a host or a user, and you want to exclude future notable events from that host or user
- ES Analysts do not have permission to perform these actions
  - An ES Admin must give the `ess_analyst` and `ess_user` roles the **Edit Notable Event Suppressions** permission

# Creating Notable Events

- Create ad-hoc notable events
  - For instance: if you find an event in Splunk that has not triggered a correlation search's parameters, but you feel it should be investigated
- Steps:
  1. Run a search on the source events
  2. Expand an event and select **Event Actions**
  3. Select **Create notable event**
  4. Enter the desired data for the notable event and click **Save**

The screenshot shows the Splunk Enterprise Security interface. At the top, there is a timeline entry: "8/4/21 10:36:15.000 AM Aug 04 16:36:15 dhcp-sac-1s.acmetech.com dhcpcd: DHCPREQUEST for 10.11.36.30 fr". Below the timeline is a dropdown menu labeled "Event Actions ▾" with the following options: "Add Event to Investigation", "Create notable event", "Build Event Type", "Extract Fields", and "Show Source". The "Create notable event" option is highlighted with a green border. A modal window titled "New Notable Event" is open, containing fields for configuration:

- Title: DHCP – High Number of Requests
- Security Domain: Network
- Urgency: High
- Owner: analyst
- Status: In Progress
- Description: Investigate high number of DHCP requests

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Suppressing Notable Events

Suppress notable events that are false positives, like a server that has been temporarily misconfigured

From Incident Review:

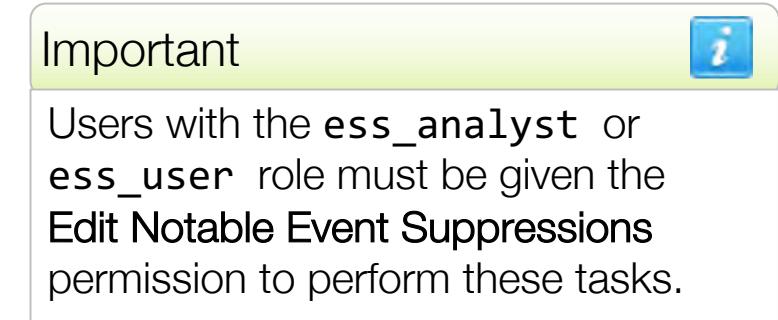
1. Click the notable event's Actions drop-down
2. Select Suppress Notable Events
3. Give the suppression a name
4. Set description and dates
5. Click Save

The screenshot shows the Splunk Enterprise Security interface. At the top, there is a header with columns: Time, Disposition, Security Domain, Urgency, Status, Owner, and Actions. Below this, a row of details is shown: Today, 12:50 PM; Undetermined; Network; Low; New; unassigned. In the Actions dropdown menu, three options are listed: 'Add Event to Investigation' (highlighted in blue), 'Suppress Notable Events' (highlighted in green), and 'Show Source'. A modal window titled 'Suppress Notable Events' is open. It contains fields for Suppression Name (Abnormally\_High\_Number\_of\_HTTP\_POSTS), Description (optional), Suppress From (08/04/2021 to 10/04/2021), Selected Fields (src, http\_method), and a Search Preview showing a search query. A note at the bottom of the modal states: 'The end date is optional. If left blank, all future notable events from the **dest** field AND **signature** are suppressed.' There are 'Cancel' and 'Save' buttons at the bottom right of the modal.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Managing Notable Event Suppressions

- View, edit, and create suppressions
- Select a suppression **Label** to edit
- Enable or disable a suppression



Configure > Incident Management > Notable Event Suppressions

The screenshot shows the Notable Event Suppressions page under the Configure menu. The top navigation bar includes links for Security Posture, Incident Review, Investigations, Security Intelligence, Security Domains, Audit, Search, and Configure. The Configure link is highlighted. On the right, there's a "Create New Suppression" button. The main table displays two suppressions:

Label	Description	Start Time	Expiration Time	Status
Activity_from_Expired_User_dmsys	User "dmsys" should not be in use.	Jul 20, 2021 12:00:00 AM	Oct 31, 2021 12:00:00 AM	Enabled   Disable
Mal-Packer on PROD-MFS-001	Malware Mal/Packer on all PROD-MFS-* hosts.	Jul 20, 2021 12:00:00 AM	Sep 20, 2021 12:00:00 AM	Enabled   Disable

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# The Executive Summary Dashboards

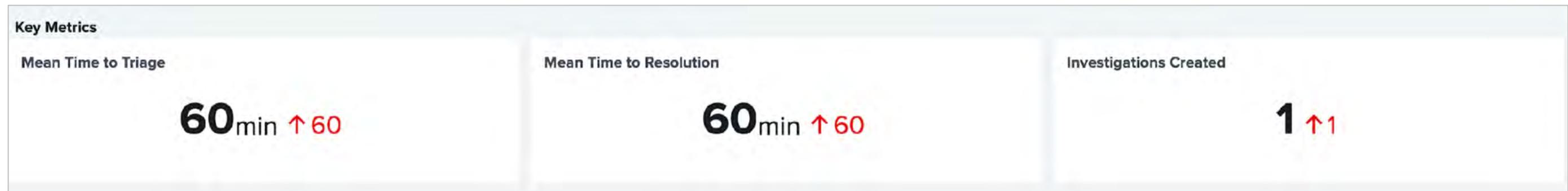
- Select Executive Summary or SOC Operations dashboards
- Provides summary of data over several time range options
- Action menus allow for search and refresh

The image displays two side-by-side screenshots of Splunk dashboards. The left screenshot shows the 'Security Posture' dashboard with three main sections: 'Security Posture' (highlighted with a blue border), 'Executive Summary' (highlighted with a green rounded rectangle), and 'SOC Operations'. The right screenshot shows the 'Executive Summary' dashboard, which includes a 'Time Range' selector with options like 24h, 7d, 30d, 90d, and 1y (the 1y option is highlighted with a green border). Below the time range is a 'Key Metrics' section showing 'Mean Time to Triage' with a value of '60min ↑ 60' (the entire metric box is highlighted with a blue border). To the right of the metrics is an 'Action Menu' containing a magnifying glass icon (highlighted with a green rounded rectangle) and a circular arrow icon.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Key Metrics Section

- Available in Executive Summary and SOC Operations dashboards
- Mean Time to Triage: time between when a notable was detected, and any action done on that notable
- Mean Time to Resolution: time between when a notable was detected and when its status changed to end status
- Investigations Created: number of investigations created over time period

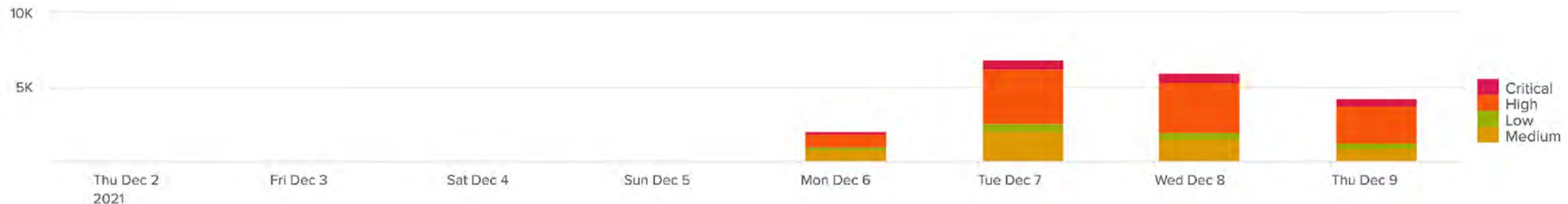


Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

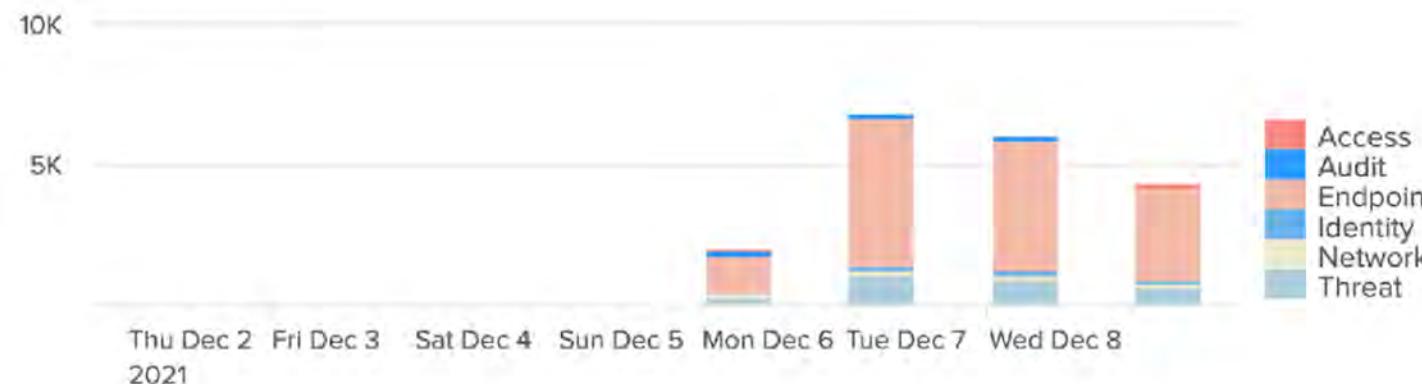
# Notables Section

## Notables

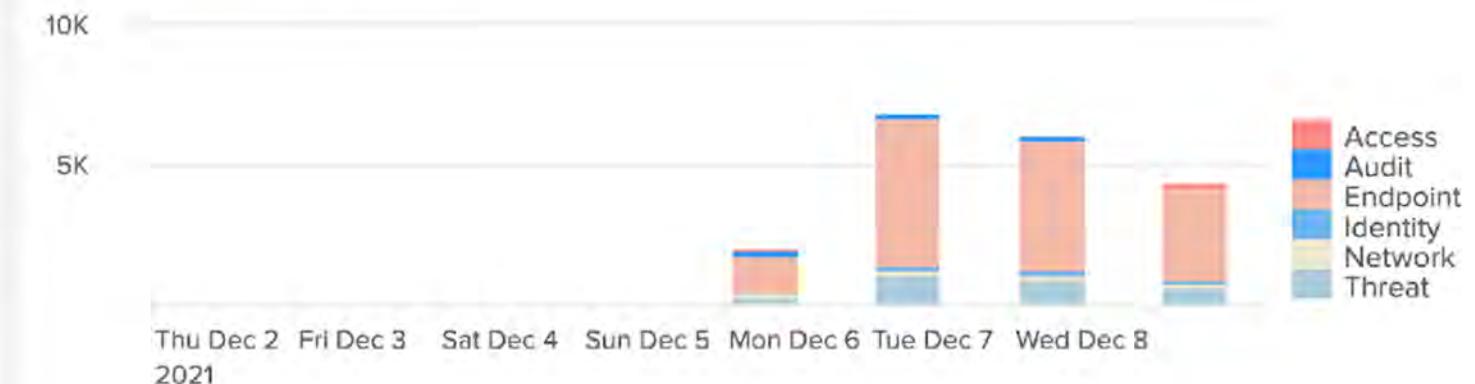
### Distribution by Urgency



### Notables by Domain



### Untriaged Notables by Domain



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Notables Section (cont.)

Top 10 Untriaged Notables by Sources



- Host With Old Infection Or Potential Re-Infection
- Risk Threshold Exceeded For Object Over 24 Hour Period
- Activity from Expired User Identity
- Threat Activity Detected
- Excessive Failed Logins
- High Or Critical Priority Host With Malware Detected
- Abnormally High Number of HTTP Method Events By Src
- Short-lived Account Detected
- Personally Identifiable Information Detected
- High Number Of Infected Hosts

Untriaged Notables by Type



Frequent Notable Event Sources



- Host With Old Infection Or Potential Re-Infection
- Excessive Failed Logins
- Activity from Expired User Identity
- High Or Critical Priority Host With Malware Detected
- Host Sending Excessive Email
- Threat Activity Detected
- Abnormally High Number of HTTP Method Events By Src
- threatmatch://src
- threatmatch://dest
- Anomalous Audit Trail Activity Detected

Rare Notable Event Sources



- /opt/splunk/var/spool/splunk/auth.nix
- /opt/splunk/var/spool/splunk/bro.http.log
- High Number Of Infected Hosts
- Watchlisted Event Observed
- Personally Identifiable Information Detected
- Geographically Improbable Access Detected
- Default Account Activity Detected
- Concurrent Login Attempts Detected
- Unroutable Activity Detected
- threatmatch://domain

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Risk Section

- Shows the number of regular notables versus risk notables over time
- Displays number of risk events that generated risk notables versus risk events that did not generate risk notables over time
- Lists risk event sources not contributing to any risk notables



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Additional Metrics Section

- Displays number of adaptive response actions fired in the system over time
- Shows how many enabled sources have risk actions versus notable actions over time
- Displays distribution of correlation searches enabled versus disabled over time



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

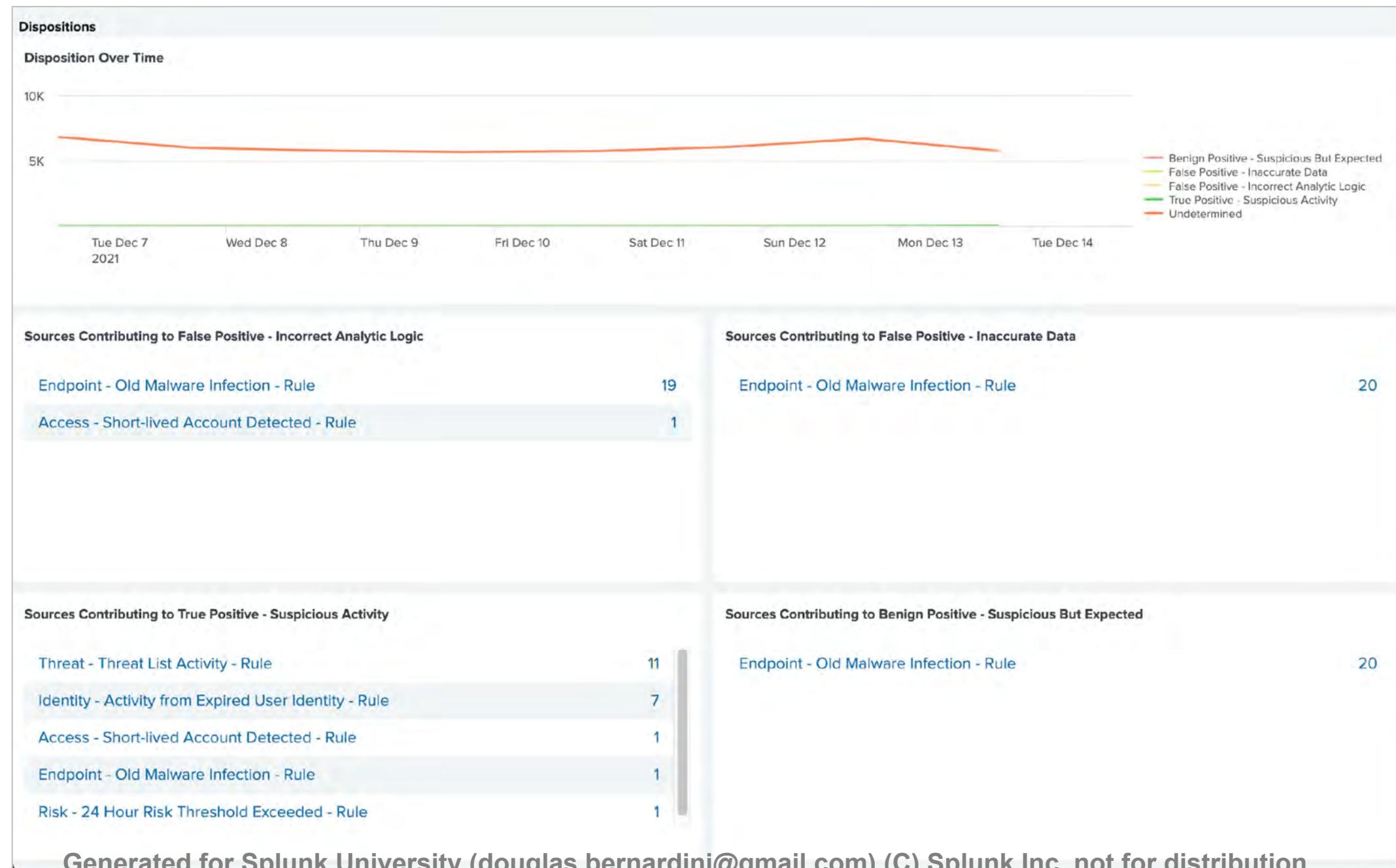
# Workload Section

- Displays assigned versus unassigned notables over time
- Shows notables assigned versus notables resolved over time
- Presents assigned open versus closed notables by analyst over time



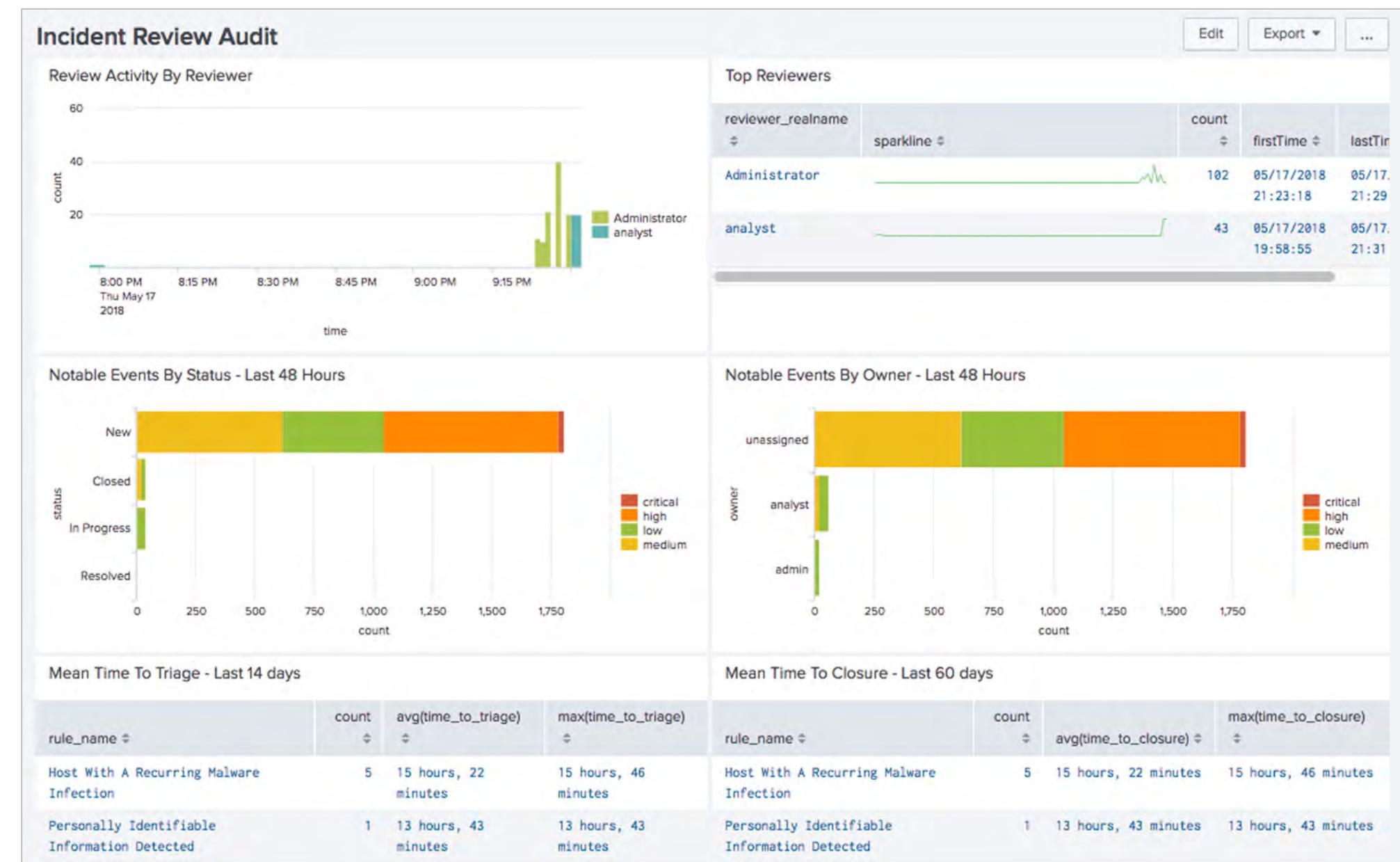
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Dispositions Section



# Audit > Incident Review Audit

- Overview of Incident Review activity
- Volume of incidents reviewed and by whom
- Incident aging over last 48 hours, by status and by reviewer
- Statistics on triage time and closure time



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Module 2 Lab: Monitoring & Investigating

---

**Time:** 30 minutes

**Description:** An expired user account has been detected attempting to log on to high priority resources

**Tasks:**

- Use the Security Posture dashboard
- Continue researching unauthorized network access
- Begin working the issue
- Test workstation status
- Remove the false positives from the list of incidents
- Resolve your incident
- Suppress notable events

# Module 3: Risk-Based Alerting

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Objectives

---

- Give an overview of Risk-Based Alerting
- View Risk Notables and risk information on the Incident Review dashboard
- Explain risk scores and how to change an object's risk score
- Review the Risk Analysis dashboard
- Describe annotations

# Risk Overview

---

- A risk score is a single metric that shows the relative risk of an object (system, user, or other) in the network over time
- Risk is increased by the adaptive response associated with the correlation search
- ES Admins can configure an object's risk value manually or by editing the correlation search
  - Edit the **Risk Analysis Response Action** in a correlation search to modify the risk score that is assigned to an object
- How is risk different from priority, severity, or urgency?
  - You can see cumulative risk caused by multiple events over time
  - You can fine-tune the way you interpret threats or vulnerabilities

# Risk Overview (cont.)

- ES Admins can configure an object's risk value:
  - by editing the **Risk Analysis Response Action** in a correlation search
  - by creating a **Risk Factor** under **Content Management**
    - Risk Factors specify conditions to dynamically adjust risk scores to specific objects
- ES Admins *and* ES Analysts can add ad-hoc risk scores for objects from the **Risk Analysis** dashboard

The screenshot shows the 'Risk Factor' configuration page in Splunk Content Management. A yellow callout box highlights the 'Name' field set to 'Contractor User' and provides an example: 'For example: a Risk Factor can add 5 to the risk score of any identity with a user\_category of "contractor"'.

**Enable:**

**Name:** Contractor User

**Description:** Increase the risk when the user is a contractor.

**Operation:** Addition

**Factor:** 5

**SPL PREVIEW:** `if('user_category'='contractor',5,0)`

**Conditions:**

**Basic** **Advanced**

**Risk Event Field:** user\_category

Field to match in the risk event. [Learn more](#)

**Risk Event Value:** contractor

Value that the Risk Event Field should match. For wildcard matches, use the advanced editor to select the like or regex comparator.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Risk Activity Examples

---

- User risk
  - An employee who begins moving files to a local workstation and emailing attachments to external sites
  - A contractor who begins logging on from many different geographically remote systems throughout the organization
- Asset risk
  - A restricted system (like a point-of-sale station) begins running new processes
  - A server shows connections to known malicious sites on the internet
- Correlation searches can detect these events and add to the objects' risk score automatically

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Why Risk-Based Alerting?

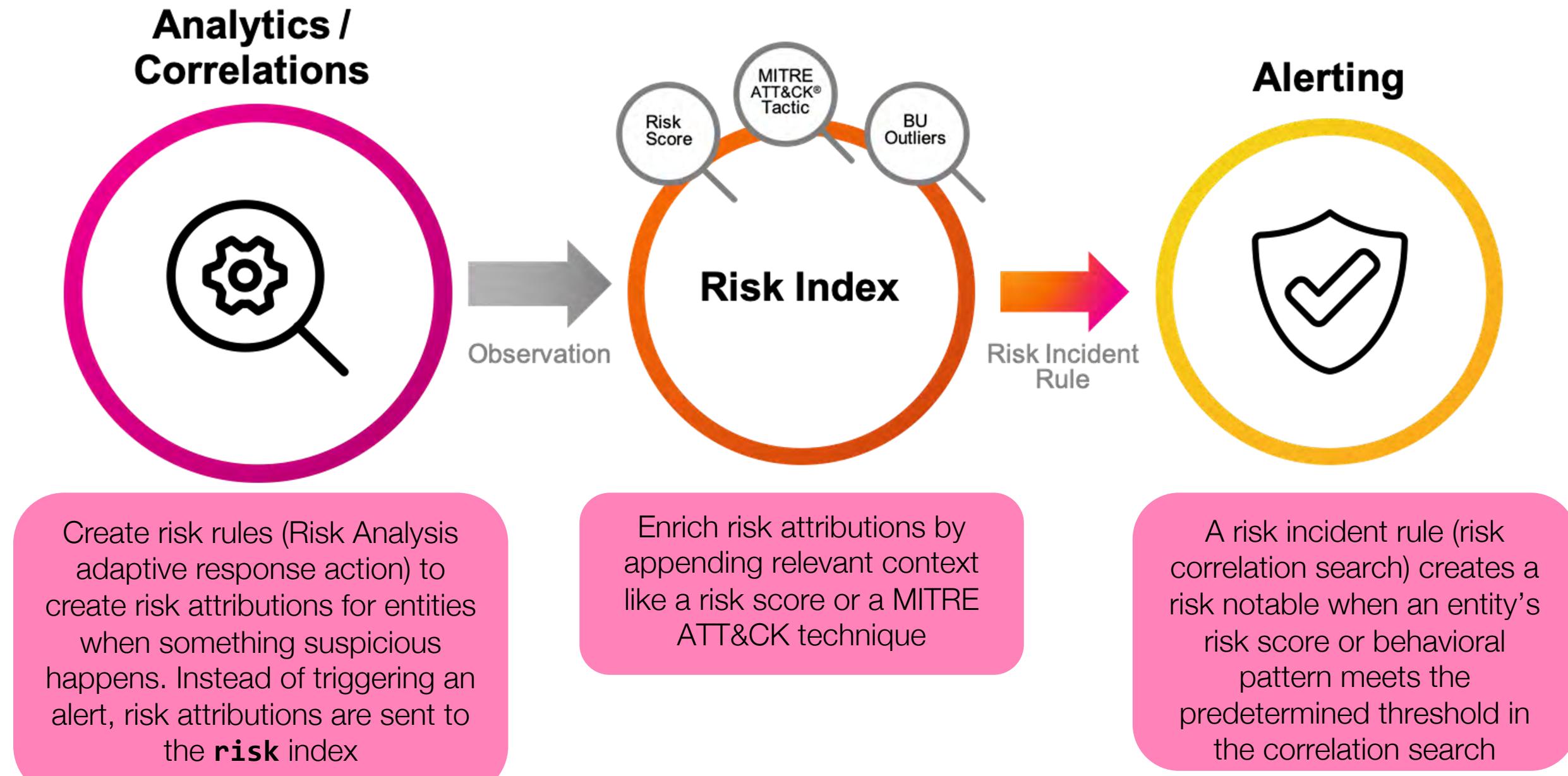
- Address alert fatigue!
- Improve detection of sophisticated threats like low-and-slow attacks that traditional SIEMs miss
- Seamlessly align to cyber security frameworks like MITRE ATT&CK, Kill Chain, CIS 20, and NIST
- Scale analyst resources to optimize SOC productivity and efficiency



- Abandoned alerts
- Suppressed alerts
- Slow detection / response

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Risk Framework

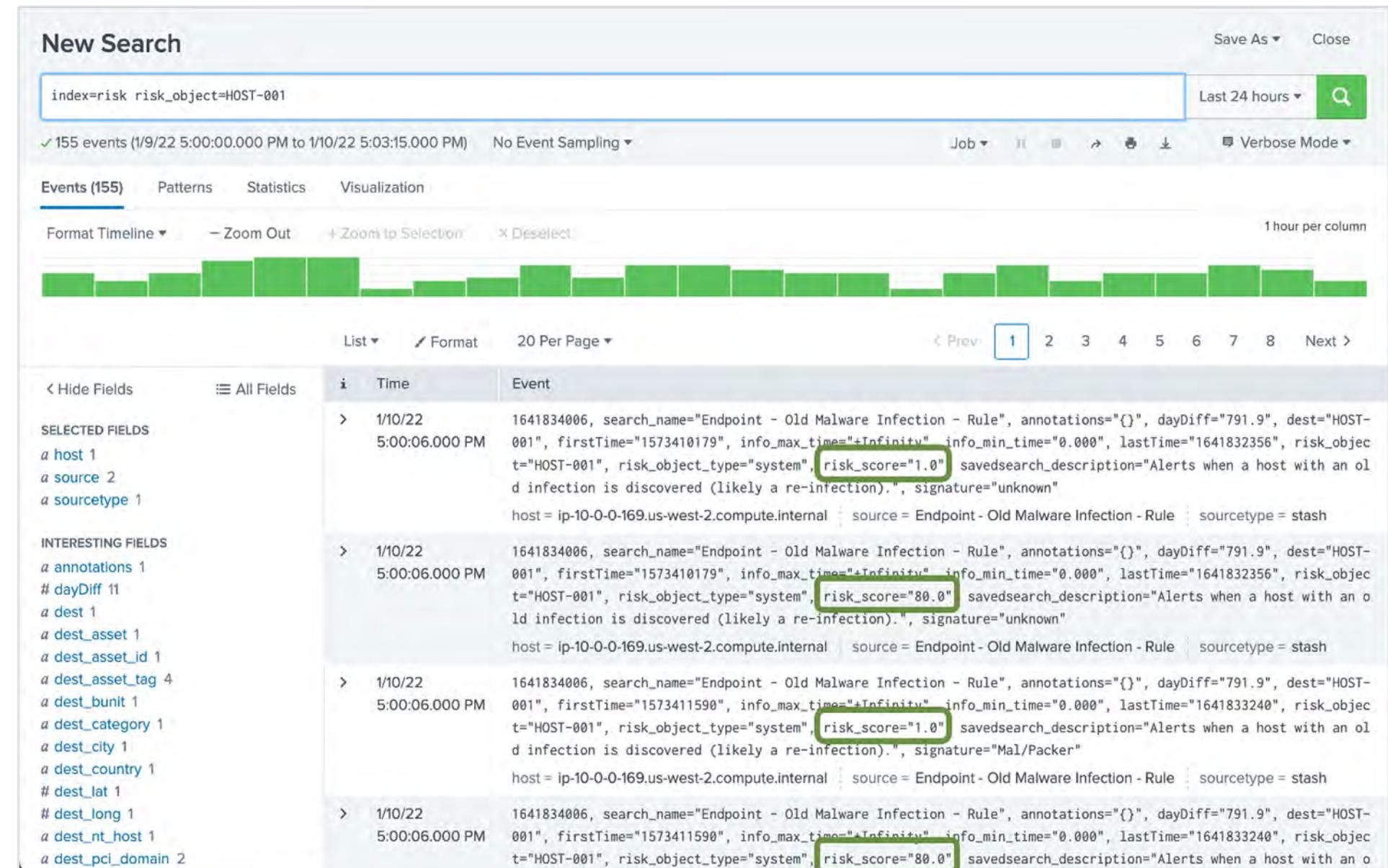


Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Risk Rules

- The Risk Analysis adaptive response action, if configured in a correlation search, is considered a Risk Rule

- A Risk Rule feeds results (risk attributions) into the **risk** index



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

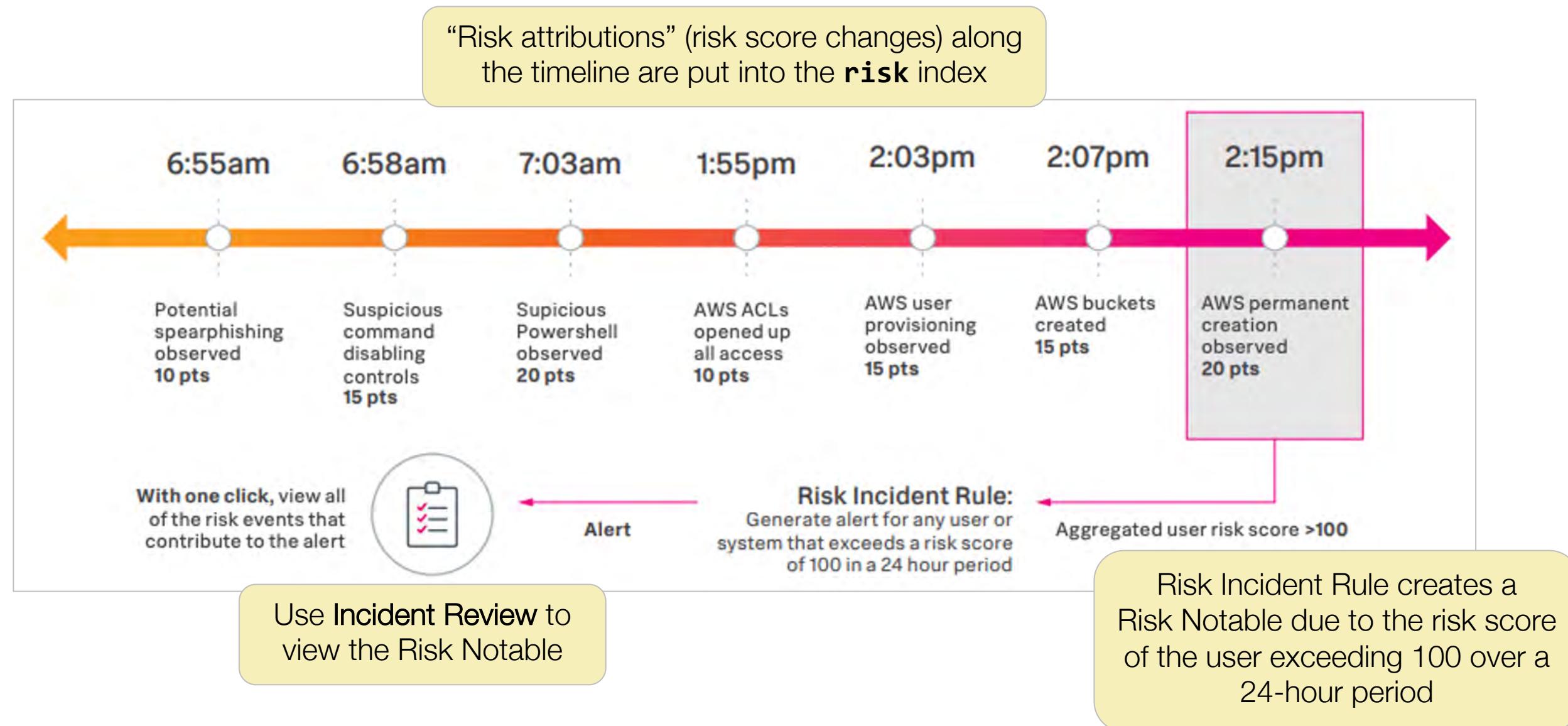
# Risk Correlation Searches

---

- Risk Incident Rules are the “risk” correlation searches that run against the **risk** index
- Risk Incident Rules create “Risk Notables”
- There are two out-of-the-box Risk Incident Rules
  - ATT&CK Tactic Threshold Exceeded for Object Over Previous 7 days
    - Creates a notable when the number of MITRE attacks exceeds 3 over the last 7 days
  - Risk Threshold Exceeded for Object Over 24 Hour Period
    - Creates a notable when the risk score for an object exceeds 100 over the last 24 hours
- Custom risk incident rules can be created

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Risk-Based Alerting Example



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Risk Notables

Filter Incident Review to show only Risk Notables

Type: Risk Notable (1)

filter

Select All Clear All

Risk Notable

Notable

	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status
<input type="checkbox"/>	unkno wn	● 16656.5	321	Risk Notable	Today, 4:00 PM	Undetermined	Threat	High	New
<input type="checkbox"/>	unkno wn	● 240	3	Risk Notable	Today, 4:00 PM	Undetermined	Threat	High	New
<input type="checkbox"/>	splunk ertest	● 600	2	Risk Notable	Today, 4:00 PM	Undetermined	Threat	Low	New

Fields display risk information for risk objects

The screenshot shows the Splunk Enterprise Security interface with the 'Incident Review' tab selected. A yellow callout bubble points to the 'Type' filter dropdown which is set to 'Risk Notable (1)'. Another yellow callout bubble points to a specific row in the results table, highlighting the 'Risk Object' column which displays user and system names like 'unkno wn', 'splunk ertest', and 'root'. A third yellow callout bubble points to the 'Risk Score' column, which shows values such as '16656.5', '240', and '600'. The results table lists 45 Notables, each with a checkbox, title, risk score, event count, type, time, disposition, security domain, urgency, and status.

	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status
<input type="checkbox"/>	unkno wn	● 16656.5	321	Risk Notable	Today, 4:00 PM	Undetermined	Threat	High	New
<input type="checkbox"/>	unkno wn	● 240	3	Risk Notable	Today, 4:00 PM	Undetermined	Threat	High	New
<input type="checkbox"/>	splunk ertest	● 600	2	Risk Notable	Today, 4:00 PM	Undetermined	Threat	Low	New

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Risk Notable Details

Title: 24 hour risk threshold exceeded for system=PROD-POS-005

Risk Object: PROD-POS-005

Aggregated Risk Score: 720

Risk Events: 9

Type: Risk Notable

**Click Risk Events to view the details**

**Risk Events**

PROD-POS-005 Aggregated Risk Score: 680 | Threshold: 100 Event Count: 9

**Click an individual event for the details**

**Risk Score: 80**

**Event Name:** Host With Old Infection Or Potential Re-Infection

**Description:** Alerts when a host with an old infection is discovered (likely a re-infection).

**Time:** 22:30

Tue 20 July 2021      Wed 21      Thu 22      Fri 23

**Contributing Risk Events**

filter

i	Time	Risk Rule	Risk Score	Annotations	Threat Object
>	Today, 3:00 PM	Host With Old Infection Or Potential Re-Infection	80	-	-
>	Today, 2:40 PM	Host With Old Infection Or Potential Re-Infection	80	-	-
>	Today, 12:50 PM	Host With Old Infection Or Potential Re-Infection	80	--	--

**Expand for details**

# Risk Analysis Example

---

A priority firewall server is attacked periodically over time

1. A few attacks are expected, but as they accumulate over weeks, the **risk score** for that server increases
2. If other low priority events are also accumulating for that server, like minor vulnerabilities and low-grade anomalous network activity, they also contribute to the **risk score** for the server
3. If the risk for that server increases more than other servers due to this continuing activity, you can be alerted and investigate

These types of issues are difficult to detect without this cumulative approach

# Risk Analysis Dashboard

Security Intelligence > Risk Analysis

**Risk Analysis**

Source: All | Risk Object Type: All | Risk Object: \* | Time: Last 7 days | Submit | Hide Filters | Create Ad-Hoc Risk Entry

**Edit**

**DISTINCT MODIFIER SOURCES**  
Source Count: 15

**DISTINCT RISK OBJECTS**  
Object Count: 1.1k +60

**MEDIAN RISK SCORE**  
Overall Median Risk: minimal (no change (delta is zero))  
Currently is: 60

**AGGREGATED SYSTEM RISK**  
Total System Risk: low (increasing minimally)  
Currently is: 117.6k

**AGGREGATED USER RISK**  
Total User Risk: high (increasing minimally)  
Currently is: 59.3k

**Create Ad-Hoc Risk Entry**

**Risk Modifiers Over Time**

Timeline of most active risk-increasing events

Risk score vs. time. The chart shows a sharp increase in risk score starting around July 27, peaking on July 28, and then remaining relatively stable. A callout highlights the peak on July 28.

**Risk Modifiers By Annotations**

A pie chart illustrating the distribution of risk modifiers based on their annotations. The largest segments include Brute Force, Valid Accounts, and CIS 16.

**Risk Score By Annotations**

A pie chart illustrating the distribution of risk scores across various annotations, similar to the one above but showing different proportions.

**Risk Modifiers By Threat Object**

A pie chart illustrating the distribution of risk modifiers by threat object, showing a large segment for Hax0r (user) and a smaller segment for dmsys (user).

**Risk Score By Object**

Object and risk score

risk_object	risk_object_type	risk_score	source_count	count	source	risk_score	risk_objects	count
dmsys	user	161273.0	1	3984	Threat - Threat List Activity - Rule	726315.0	4944	13672
unknown	user	126632.5	2	2381	Identity - Activity from Expired User Identity - Rule	186141.0	2	4599
Hax0r	user	24868.0	1	615	Access - Excessive Failed Logins - Rule	45360	57	756

Most Active Sources

Risk scores by correlation search

risk_object	risk_object_type	risk_score	source_count	count	source	risk_score	risk_objects	count
dmsys	user	161273.0	1	3984	Threat - Threat List Activity - Rule	726315.0	4944	13672
unknown	user	126632.5	2	2381	Identity - Activity from Expired User Identity - Rule	186141.0	2	4599
Hax0r	user	24868.0	1	615	Access - Excessive Failed Logins - Rule	45360	57	756

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Ad-hoc Risk Entry

- ES Analysts can perform a one-time ad-hoc risk adjustment for an object
- Useful to change an object's risk based on your own investigation
- The risk value you enter is added to (or subtracted from) the object's overall risk score

Create Ad-Hoc Risk Entry

Ad-Hoc Risk Score

Risk Modifiers

Risk Message: a description of the adjustment

Risk Message: admin ad-hoc risk entry

+ Risk Score: 300 Risk Score: positive or negative

Risk Object: HOST-001 Risk object: object name (user or system)

Risk Object Type: system Risk Object Type: use other for an unspecified object

system  
user  
other

X Remove

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Ad-hoc Risk Entry – Threat Objects

- Threat objects can also be added to an ad-hoc risk adjustment
- Correlate threat objects with risk events to make adjustments to the risk score



# Ad-hoc Risk Entry - Annotations

- Also available on the **Create Ad-hoc Risk Entry** window is the ability to add annotations
- Use annotations to enrich correlation search results with the context from industry-standard mappings
- Used as field labels in the **Risk Analysis** dashboard

**Create Ad-Hoc Risk Entry**

**Ad-Hoc Risk Score**

**Annotations**

Enter annotation attributes or choose MITRE ATT&CK annotations from the included list

CIS 20 Type an attribute and press enter

Kill Chain Type an attribute and press enter

MITRE ATT&CK T1499.003 × T1071 × T1550.001 ×

NIST Type an attribute and press enter

**Unmanaged Annotations**

Create a custom annotation  
+ Framework

T1557.002

T1558.004

T1548

T1134

T1546.008

T1531

T1087

**Save the ad-hoc entry** **Cancel** **Save**

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc. not for distribution

# Annotations

ES includes the following annotations for common security frameworks, or you can create custom annotations

## Example industry-standard mappings:

Security Framework	Mapping Examples
CIS 20	CIS 3, CIS 9, CIS 11, CIS 7, CIS 12
Kill Chain	Reconnaissance, Actions on Objectives, Exploitation, Delivery, Lateral Movement
MITRE ATT&CK	T1015, T1138, T1084, T1068, T1085 Also contains MITRE technique IDs from the <b>mitre_attack_lookup</b> lookup definition
NIST	PR.IP, PR.PT, PR.AC, PR.DS, DE.AE

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# View Annotation Details

**Risk Analysis**

Source Risk Object Type Risk Object Time

All All \* Last 7 days Submit Hide Filters Create Ad-Hoc Risk Entry

**Edit**

**DISTINCT MODIFIER SOURCES** Source Count **15** 0

**DISTINCT RISK OBJECTS** Object Count **1.1k** +60

**MEDIAN RISK SCORE** Overall Median Risk **m** Current is: 59.3k

**AGGREGATED SYSTEM RISK** Total System Risk **high** increasing minimally Currently is: 59.3k

**AGGREGATED USER RISK** Total User Risk **high** increasing minimally Currently is: 59.3k

**AGGREGATED OTHER RISK** Total Other Risk **minimal** no change (delta is zero) Currently is: 1.4k

**Risk Modifiers Over Time**

**Risk Modifiers By Annotations**

**Risk Score By Annotations**

**Risk Modifiers By Threat Object**

**Recent Risk Modifiers**

_time	risk_object	risk_object_type	threat_object	threat_object_type	source	risk_message	risk_score	annotations_all	annotations_frameworks
2021-08-03 21:40:12	0.213.6.179	system			Network - Unroutable Host Activity - Rule	Alerts when activity to or from a host that is unroutable is detected.	80	T1041	mitre_attack
2021-08-03 21:40:10	dmsys	user	dmsys	user	Identity - Activity from Expired User Identity - Rule	Alerts when an event is discovered from a user associated with identity that is now expired (that is, the end date of the identity has been passed).	1.0	T1003.008 T1134 T1558.004 T1557.002 T1546.004	mitre_attack

Hover over an annotation to view the risk modifier count or risk score

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Module 3 Lab: Risk-Based Alerting

---

**Time:** 25 minutes

**Description:** Examine risk-based information and high-risk assets or users in your environment

**Tasks:**

- Review the risk-based information for a risk notable
- Examine user risk information
- Manually adjust a risk score

# Module 4: Assets & Identities

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Objectives

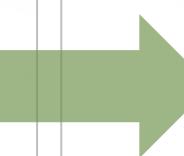
---

- Give an overview of the ES Assets and Identities framework
- Show examples where asset or identity data is missing from ES dashboards or notable events
- View the Asset & Identity Management Interface
- View the contents of an asset or identity lookup table

# Assets & Identities Overview

Asset and identity configuration enhances the information available for users and systems in notable events and ES dashboards

	i	Time	Title	Risk Object	Aggregated Risk Score
<b>Description:</b>					
A high or critical priority host (HOST-003) was detected with malware.					
<b>Additional Fields</b>		<b>Value</b>		<b>Action</b>	
Destination		HOST-003	8417.0		
Signature		EICAR-AV-Test			



	i	Time	Title	Risk Object	Aggregated Risk Score
<b>Description:</b>					
A high or critical priority host (HOST-003) was detected with malware.					
<b>Additional Fields</b>		<b>Value</b>		<b>Action</b>	
Destination		HOST-003	8417.0		
Destination Business Unit		emea			
Destination Category		pci			
Destination City		havant			
Destination Country		uk			
Destination Latitude		50.84436			
Destination Longitude		-0.98451			
Destination NT Hostname		host-003			
Destination PCI Domain		wireless			
Destination Requires Antivirus		trust			
Destination Should Time Synchronize		true			
Destination Should Update		true			
Signature		EICAR-AV-Test			

ES admins add the enhanced data for assets and identities to ES in lookup tables

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Missing Data Example 1

If enhanced data is not included in the Assets & Identities configuration for a user or system, notable event and dashboard data is still available for the object, though the additional information is not provided

The screenshot shows two views of the Splunk Identity Investigator interface. On the left, a search for 'admin' returns the message 'admin is not a known identity.' A large green arrow points from this message to the right-hand detailed view. The right-hand view shows a detailed object for 'admin'. The object has the following fields:

Field	Value
identity_id	61d3743770d9b024253eb893
bunit	americas
category	default, privileged
email	admin@bcc.com
first	administrator
identity_id	61d3743770d9b024253eb893
nick	admin
phone	555-719-8807
priority	critical
watchlist	true
work_city	san francisco
work_country	us

A yellow callout box above the right-hand view states: 'For example, objects may show as "not known" in the Asset or Identity Investigator'.

A green box labeled 'Important!' with an info icon contains the text: 'If you are expecting to see enhanced data for a particular object, double check the configuration in the Assets & Identities Management interface.'

At the bottom of the interface, it says 'Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution'

# Missing Data Example 2

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Asset & Identity Management Interface

Asset and identity lookups and settings are configured in  
**Configure > Data Enrichment > Asset and Identity Management**

**Asset and Identity Management**  
Unified interface for enriching and managing asset and identity data via lookups.

[Back to ES Configuration](#)

Asset Lookups Asset Fields **Identity Lookups** Identity Fields Global Settings Correlation Setup Search Preview

**Important!** Default `ess_analyst` view. Users must have the `edit_modinput_identity_manager` capability to make changes in the A&I Management interface.

You need `edit_modinput_identity_manager` capability to edit this information.

Rank	Name	Category	Description	Source	Blacklist	Status
1	administrative_identities	administrative_identities	List of commonly-used administrative or privileged identities.	<a href="#">administrative_identity_lookup</a>	Enabled	Enabled
2	demo_identities	demo_identities	Demonstration identity list.	<a href="#">demo_identity_lookup</a>	Enabled	Enabled
3	static_identities	static_identities	List containing static identities.	<a href="#">simple_iden</a>	Enabled	Enabled
4	GFD_identities	GFD_domain_IDs	Identities on the GFD domain	<a href="#">GFD_identities</a>	Enabled	Enabled
5	BCC_identities	BCC_ids	Identities from the BCC domain.	<a href="#">BCC_identities</a>	Enabled	Enabled

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# View Asset & Identity Lookups

- View the contents of a lookup table using | inputlookup
  - For Example: | inputlookup demo\_identities.csv
  - | inputlookup demo\_assets.csv

New Search

| inputlookup demo\_assets.csv

Last 24 hours

✓ 89 results (1/23/22 6:00:00.000 PM to 1/24/22 6:23:30.000 PM) No Event Sampling Job Verbose Mode

Events (0) Patterns Statistics (89) Visualization

100 Per Page Format Preview

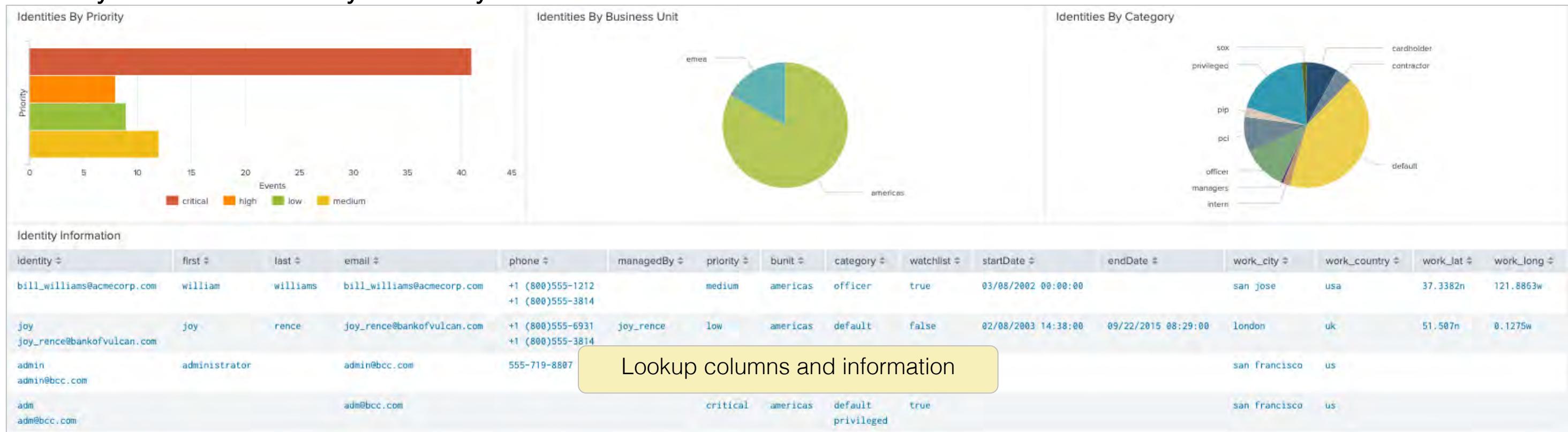
bunit	category	city	country	dns	ip	is_expected	lat	long	mac	nt_host	owner	pci_domain	priority	requires_av	should_timesync
americas	virtual	Denver	USA		111.125.30.2				00:17:71:92:cf:6f				critical		TRUE
apac		Istanbul	TR		6.0.0.1-6.0.0.20		41.040855	28.986183					low		TRUE
americas		Washington D.C.	USA		1.2.3.4		38.959405	-77.04	00:15:70:91:df:6c				medium		TRUE
americas	pci cardholder	Pleasanton	USA	CORP1.acmetech.com		TRUE	37.694452	-121.894461				trust	high		TRUE
americas	pci	Dallas	USA		192.168.12.9-192.168.12.9	TRUE	32.931277	-96.818167		storefront		trust	critical		TRUE
emea	pci sox	Havant	UK		2.0.0.0/8	TRUE	50.84436	-0.98451				dmz	low		TRUE
americas	pci hipaa	Washington D.C.	USA		192.168.15.8-192.168.15.10		38.959405	-77.04				trust	medium		TRUE

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Identity Center & Asset Center Dashboards

View the contents of the asset or identity configuration added to ES in the Identity Center or Asset Center dashboard

Security Domains > Identity > Identity Center



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Module 5: Investigations

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Objectives

---

- Use investigations to manage incident response activity
- Use the **Investigation Workbench** to manage, visualize and coordinate incident investigations
- Add various items to investigations (notes, action history, collaborators, events, assets, identities, files and URLs)
- Use investigation timelines, lists, and summaries to document and review breach analysis and mitigation efforts

# Investigations

An investigation is a collection of activities and notes related to work done on a specific issue, such as a breach

**Example:** customers are reporting unauthorized use of their account numbers (from your store). Start an investigation and begin researching the issue:

1. Examine notable events related to the payment processing system and add them to an investigation
2. Add relevant artifacts (i.e., assets and identities) and explore them within the Investigation Workbench – this will help identify other identities involved
3. Add collaborators with expertise in a specific field
4. Run ad-hoc searches and add the results to the timeline
5. Add Action History items, such as a “source” or “non-notable event”
6. Add notes detailing actions taken to mitigate the breach
7. Modify the investigation status. Helpful for analysts in the future, especially if you solved the problem!

Note



By default, only **ess\_admin** and **ess\_analyst** have permission to start investigations.

# Investigations Dashboard

Lists all investigations

Security Posture   Incident Review   **Investigations**   Security Intelligence ▾   Security Domains ▾   Audit ▾   Search ▾   Configure ▾   Enterprise Security

**Investigations**  
Track and manage investigations

Create New Investigation

Filter for a specific investigation

Start a new investigation

filter   Investigations Assigned to Me   All Investigations   10 per page ▾

Name	Description	Status	Created	Last Modified	Collaborators
<input type="checkbox"/> High Number of HTTP POSTs	IPs with a high number of HTTP POST requests.	New	January 5, 2021 10:14 AM	January 5, 2021 10:40 AM	
<input type="checkbox"/> Reinjected Hosts	Hosts that have been reinfected	In Progress	January 5, 2021 10:13 AM	January 5, 2021 10:13 AM	
<input type="checkbox"/> Threat activity in the last 24 hours		In Progress	January 5, 2021 10:14 AM	January 5, 2021 10:14 AM	

Click an investigation to open it



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Investigation Workbench

**High Number of HTTP POSTs**  
IPs with a high number of HTTP POST requests.

Created January 3, 2022 4:03 PM  
Last Modified January 3, 2022 4:06 PM  
Status In Progress

Workbench Timeline Summary

Time range

Between December 14, 2021 11:50 AM and January 4, 2022 11:50 AM

Custom time ▾

**Artifacts**

3 out of 6 are selected.  
Clear selected. Select all.

Filter artifacts

All Identities Assets

10.12.34.56  
199.9.251.150  
10.11.23.120  
Hax0r  
10.7.34.131  
10.11.36.7

1 Select Artifact(s)

2 Click Explore to display selected artifacts in the workbench

**Context** Endpoint Data Network Data Risk + Add Content

Gain context into the investigated artifacts associated with this investigation.

**Risk Scores**

Description

All Time

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
10.11.23.120	system		2520
10.11.36.7	system		18463.0
10.12.34.56	system		2580
10.7.34.131	system		2520
Hax0r	user		529146.0

**IDS Alerts**

Description

_time	src	dest	user	ids_type	severity
2021-12-29 04:05:35	10.11.36.1	10.11.36.7	unknown	network	high
2021-12-24 08:45:09	10.11.36.1	10.11.36.7	unknown	network	high
2021-12-25 19:42:45	10.11.36.1	10.11.36.7	unknown	network	low
2021-12-29 15:52:50	10.11.36.1	10.11.36.7	unknown	network	medium
2022-01-01 17:13:59	10.11.36.10	10.11.36.7	unknown	network	low
2021-12-23 02:52:25	10.11.36.10	10.11.36.7	unknown	network	medium
2021-12-30 10:34:12	10.11.36.10	10.11.36.7	unknown	network	medium
2022-01-01 08:05:47	10.11.36.11	10.11.36.7	unknown	network	low

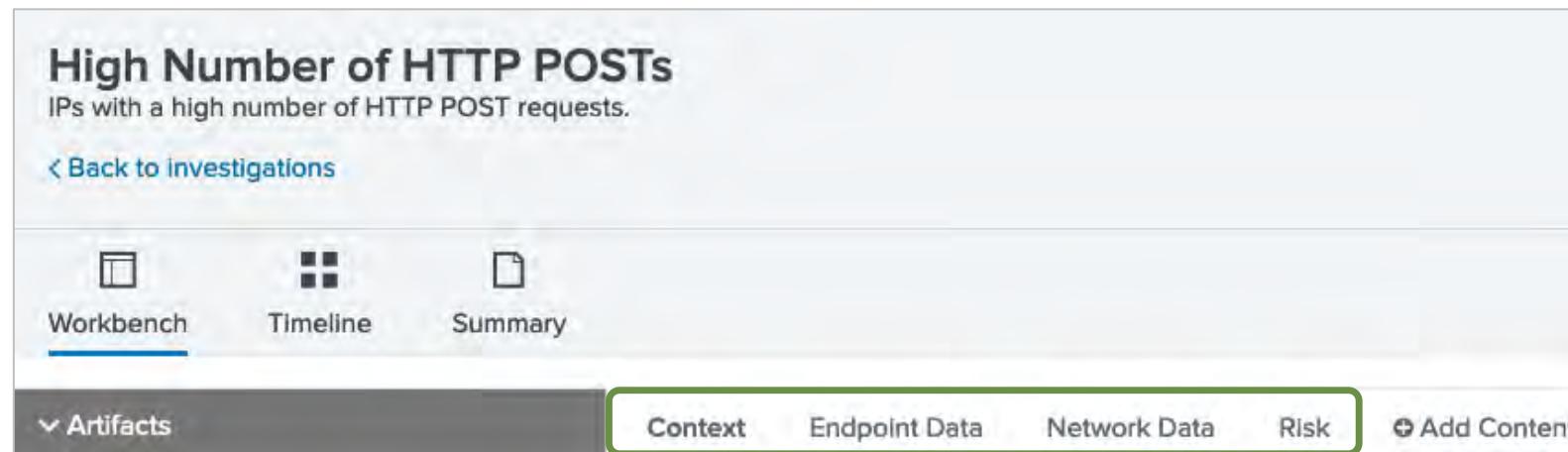
**System Vulnerabilities**

Note

Workbench will be blank until you select artifact(s) and click Explore.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Tabs & Panels



## Context Panels

- Risk Scores
- IDS Alerts
- Notable Events
- System Vulnerabilities
- Latest OS Updates
- Computer Inventory

## Endpoint Data Panels

- File System Changes
- Registry Activity
- Process Activity
- Service Activity
- User Account Changes
- Port Activity
- Authentication Data

## Network Data Panels

- Web Activity
- Email Data
- Network Traffic Data
- DNS Data
- Certificate Activity
- Network Session Data

## Risk Panels

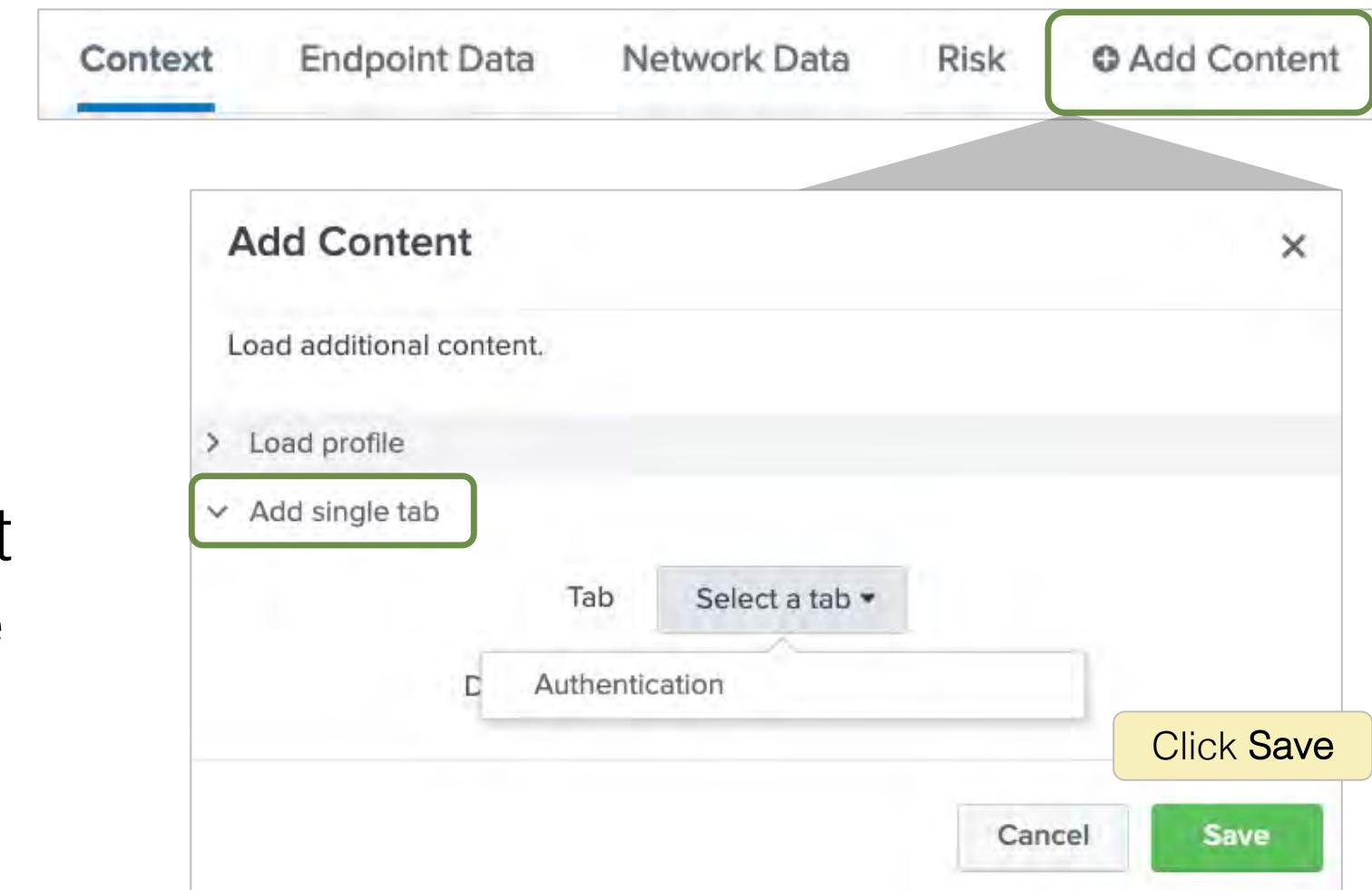
- Risk Scores
- Recent Risk Modifiers
- MITRE ATT&CK Techniques
- MITRE ATT&CK tactics

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Add a Tab to the Investigation

- Add other tabs to the investigation
  - For example, add the Authentication tab
- Content > Add single tab > Select a tab > Authentication

- Imports cloud-authentication-related notable events into the investigation
- Displays authentication related data relevant to the investigation



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Add Artifacts to an Investigation

---

- Artifacts are assets or identities you may add to an investigation to determine whether they are involved in the overall incident
- There are several ways to add an artifact to an investigation
  - From a notable event (set up by an admin)
    - ▶ Actions > Add Event to Investigation
  - Manually
    - ▶ Add Artifact button 
    - ▶ Add Artifact icon  on the Investigation Bar
  - From a workbench panel (select any item)
  - From an investigation event (Timeline View > Details > click a value)

# Add Artifacts Manually

---

1. Click Add Artifact button or click 
2. Select Add artifact or Add multiple artifacts and enter the artifact(s)  
(all artifacts added must be the same type: assets or identities)
3. Select either Asset or Identity artifact
4. To separate multiple artifacts, click New Line or use a comma
5. Optionally, add a Description and Label(s) (separate labels with <Enter> or <,>)
6. Optionally, Expand artifact (seeks correlated items from lookups)
7. Click Add to Scope

# Add Artifacts within the Investigation

The screenshot shows the Splunk Enterprise Security interface. On the left, there's a sidebar titled "Artifacts" with a message "3 out of 6 are selected." It includes a "Filter artifacts" input and three tabs: "All", "Identities", and "Assets". Under "Assets", several IP addresses are listed: 10.12.34.56 (selected), 199.9.251.150, 10.11.23.120, Hax0r, 10.7.34.131, and 10.11.36.7. A yellow callout with orange circle "1" points to the "10.11.23.120" entry, with the text: "When exploring, click a value to add it as an artifact". At the bottom of the sidebar are buttons for "+ Add Artifact" and "Explore".

The main area has tabs for "Context", "Endpoint Data", "Network Data", and "Risk". The "Context" tab is active, showing a table of correlated artifacts. One row for "10.11.23.120" is highlighted with a green border and orange circle "1". The table columns include "risk\_object", "risk\_object\_type", and "risk". Rows show "system", "system", "system", "system", and "user".

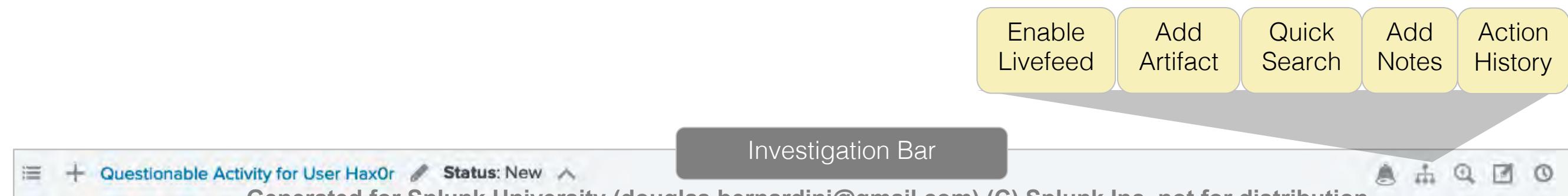
A modal window titled "Add Artifacts" is open on the right. It has fields for "Artifact" (10.11.23.120), "Type" (Asset), "Description" (PROD-MFS Server), and "Labels" (PROD-MFS). A yellow callout with orange circle "2" points to the "Add to Scope" button at the bottom right, with the text: "Enter details and click Add to Scope".

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

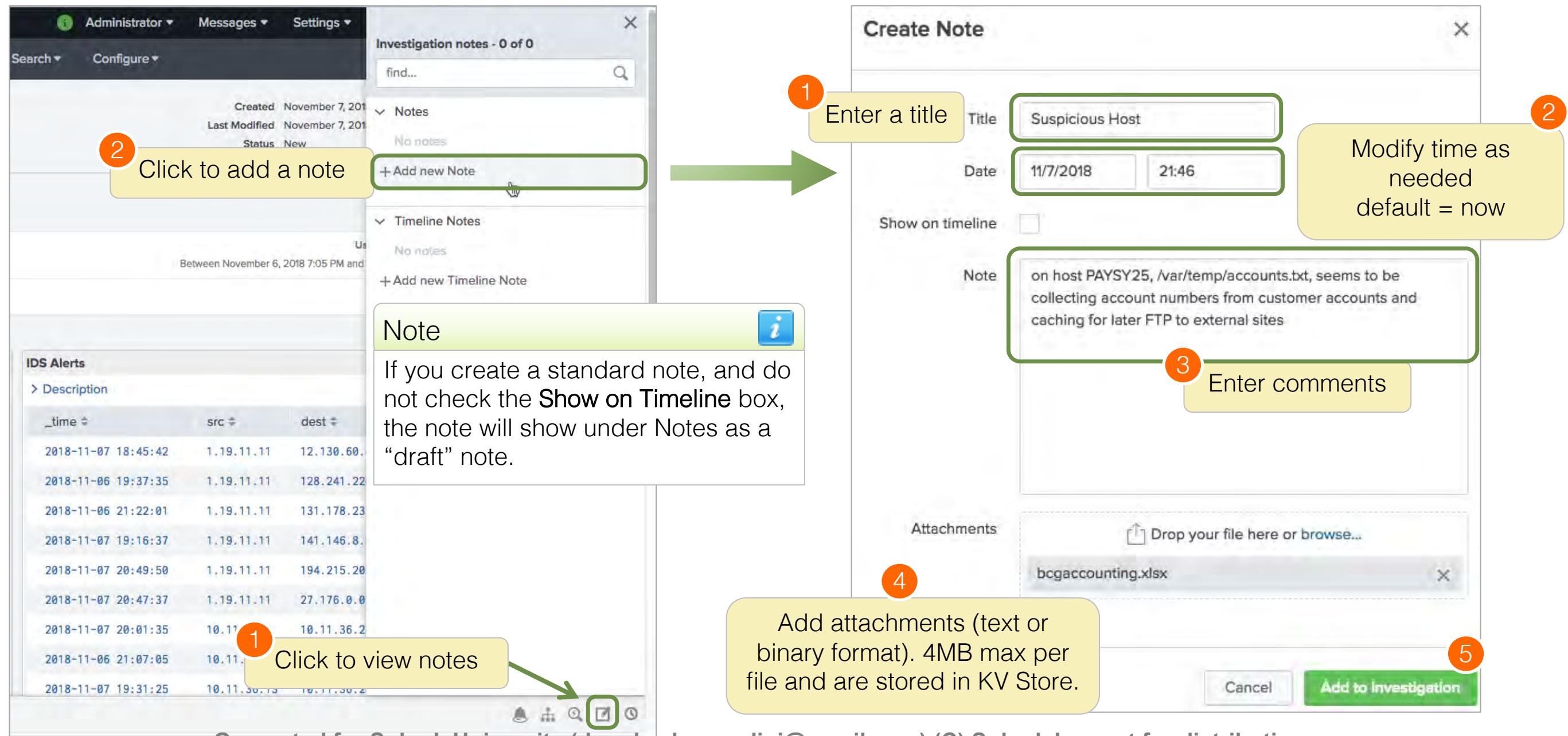
# Add Items to an Investigation

It is important to add items to investigations to document the purpose of the steps you have taken to research the issue and to provide any details that may be useful to your team's future investigation work. You can add several types of entries:

- Notes
- Search strings
- Notable or source events
- Action History items:
  - Dashboards viewed
  - Notable Event Updated
  - Notable Event Suppression Updated
  - Panel Filtered
  - Search Run



# Adding a Note



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Adding an Action History Item

The screenshot shows the 'Add Action History' interface. The steps are numbered as follows:

- 2 Select type: A yellow callout points to the 'Select type' button.
- 3 Modify time as needed: A yellow callout points to the search filters ('Search Run', 'Last 30 minutes', and a magnifying glass icon).
- 4 Filter search as needed: A yellow callout points to the 'Filter' button.
- 5 Select items: A yellow callout points to the 'Select items' button, which has a green arrow pointing to the 'Add to Investigation' link for the second row.
- 6 Done: A green callout points to the 'Done' button.

The table below lists the action history items:

Dashboard Viewed	user	content.host	content.source	content.sourcetype	content.search	content.search_type	content.info	content
Notable Event Updated								
Notable Event Suppression Updated	10:17 PM	admin	ip-10-0-0-169.us-west-2.compute	audittrail	audittrail	search `notable`   search event_id	adhoc	granted 158144
Panel Filtered	08:54 PM	admin	ip-10-0-0-169.us-west-2.compute	audittrail	audittrail	search index=main user=haxOr	adhoc	granted 158144
✓ Search Run	Feb 11, 2020 5:08:42 PM	admin	ip-10-0-0-169.us-west-2.compute	audittrail	audittrail	search index=notable	adhoc	granted 158144
Add to Investigation	Feb 11, 2020 5:08:09 PM	admin	ip-10-0-0-169.us-west-2.compute	audittrail	audittrail	(`risk_object_types`)	adhoc	granted 158144

# Adding a Search String (Quick Search)

- Perform a search from the Investigation Bar and add the string to an investigation

The screenshot shows the Splunk Enterprise Security interface. At the top, there's a navigation bar with tabs like 'Questionable Activity for User Hax0r' and 'Status: New'. On the right side of the bar are several icons, with the magnifying glass icon (Search) highlighted by a green box and a red circle containing the number 1.

A large gray triangle points downwards towards a 'Quick Search' dialog window. The dialog has a title bar 'Quick Search' with a close button 'X'. It contains a search input field 'Enter search criteria' with a placeholder '10.12.34.56' and a dropdown menu 'Last 24 hours'. A green search button with a white magnifying glass icon is on the right, with a red circle containing the number 3 above it.

Below the search input is a table with columns 'Time' and 'Event'. The first row shows a timestamp '12/19/19 2:13:27.000 PM' and an event log entry. The second row shows another timestamp '12/19/19' and a longer event log entry.

On the left side of the main area, there's a yellow callout box with the text: 'Click and drag to resize the search window. Double click to toggle full screen to minimized'.

Numbered callout boxes are overlaid on the interface:

- 1: Points to the magnifying glass icon in the top right of the navigation bar.
- 2: Points to the search input field in the 'Quick Search' dialog.
- 3: Points to the green search button in the 'Quick Search' dialog.
- 4: Points to the yellow callout box on the left.
- 5: Points to the green 'Add Search String to Investigation' button at the bottom right of the 'Quick Search' dialog.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Adding Events

There are several ways to add events to an investigation

The screenshot shows a Splunk search results page for '38 Notables'. At the top, there are buttons for 'Edit Selected' and 'Edit All Matching Events (38)', followed by a prominent green button labeled 'Add Selected to Investigation'. A green arrow points from this button to a callout box containing the text 'Add notable events from Incident Review'.

To the right of the main table, a vertical menu is open under the 'Actions' button. It includes options like 'Add Event to Investigation' (which is highlighted with a blue border), 'Build Event Type', 'Extract Fields', 'Run Adaptive Response Actions', 'Share Notable Event', 'Suppress Notable Events', and 'Show Source'. A green arrow points from this menu to another callout box containing the text 'Add source events from a search result'.

At the bottom left, a secondary vertical menu is shown under 'Event Actions'. It includes 'Add Event to Investigation' (highlighted with a blue border), 'Create notable event', 'Build Event Type', 'Extract Fields', and 'Show Source'. A green arrow points from this menu to a third callout box containing the text 'Add source events from a search result'.

Time	Event
8/4/21 4:01:10.000 PM	Aug 04 22:01:10 acmepayroll sshd[14051]: Failed password for irc from 10.11.36.46 port 43341

Value Actions

Value	Actions
ip-10-0-0-169.us-west-2.compute.internal	▼
/opt/splunk/var/spool/splunk/auth.nix	▼
linux_secure	▼
failure ( failure )	▼
sshd	▼
ip-10-0-0-169.us-west-2.compute.internal	▼

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Enabling Notable Event Livefeed

- Get a visual notification when a notable event occurs for assets or identities included in the investigation
  - Select an investigation, click the bell icon, and toggle **Enable Notification**
  - Bell icon turns orange within five minutes of the next occurrence

Questionable Activity for User HaxOr Status: New

Enable Livefeed

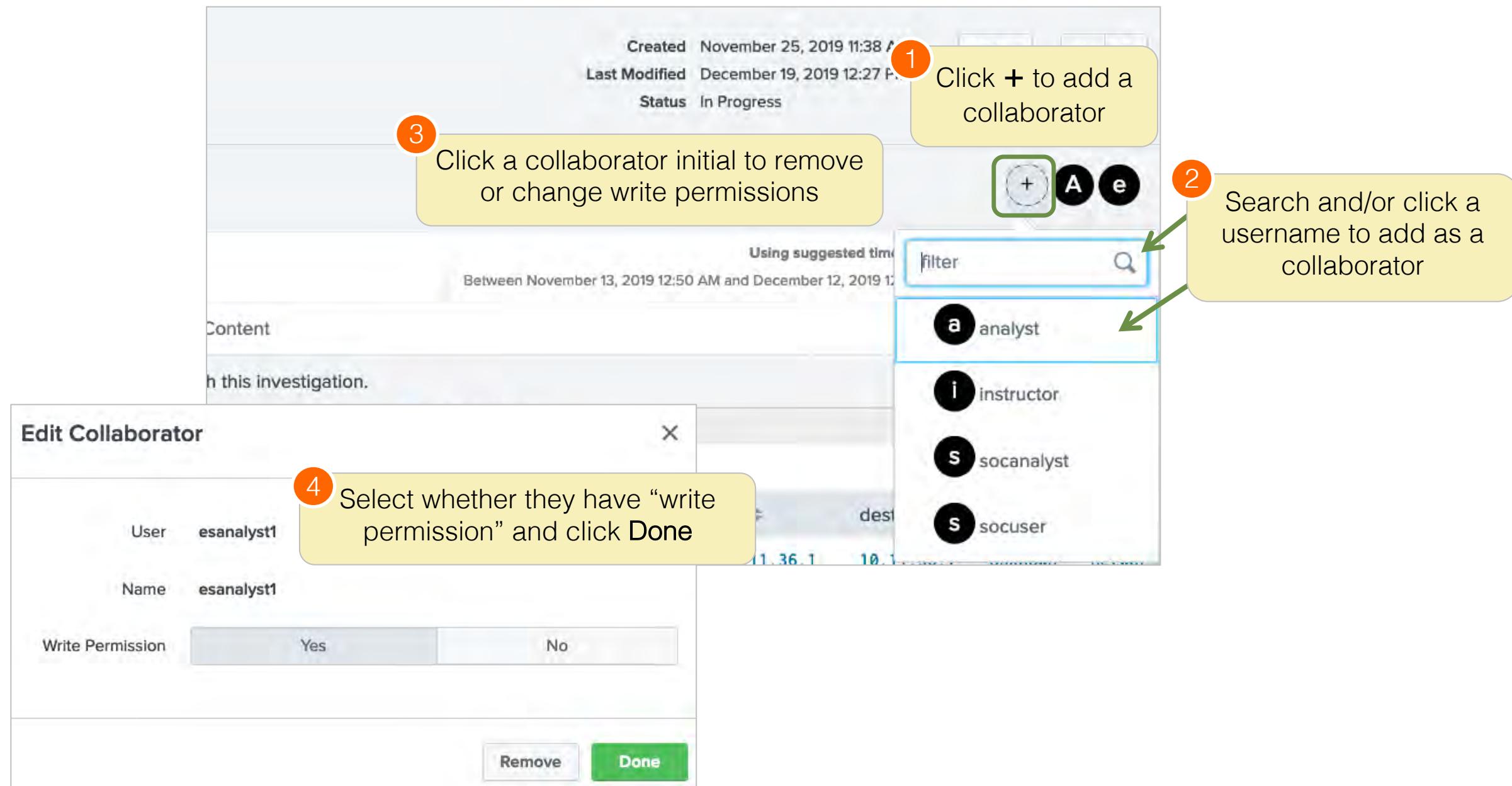
Enable notification

Review events and use the plus sign (+) to add events to the investigation

Affected Artifacts	Time	Event ID	Title	Security Domain	Urgency	Status	Owner
+ • unknown • unknown • unknown	January 6, 2021 5:10 PM	...9fd4de2a	Threat Activity Detected (106.98.164.19)	Threat	Low	New	unassigned
+ • unknown • unknown • unknown	January 6, 2021 5:10 PM	...a68f81fb	Threat Activity Detected (116.169.109.53)	Threat	Low	New	unassigned

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

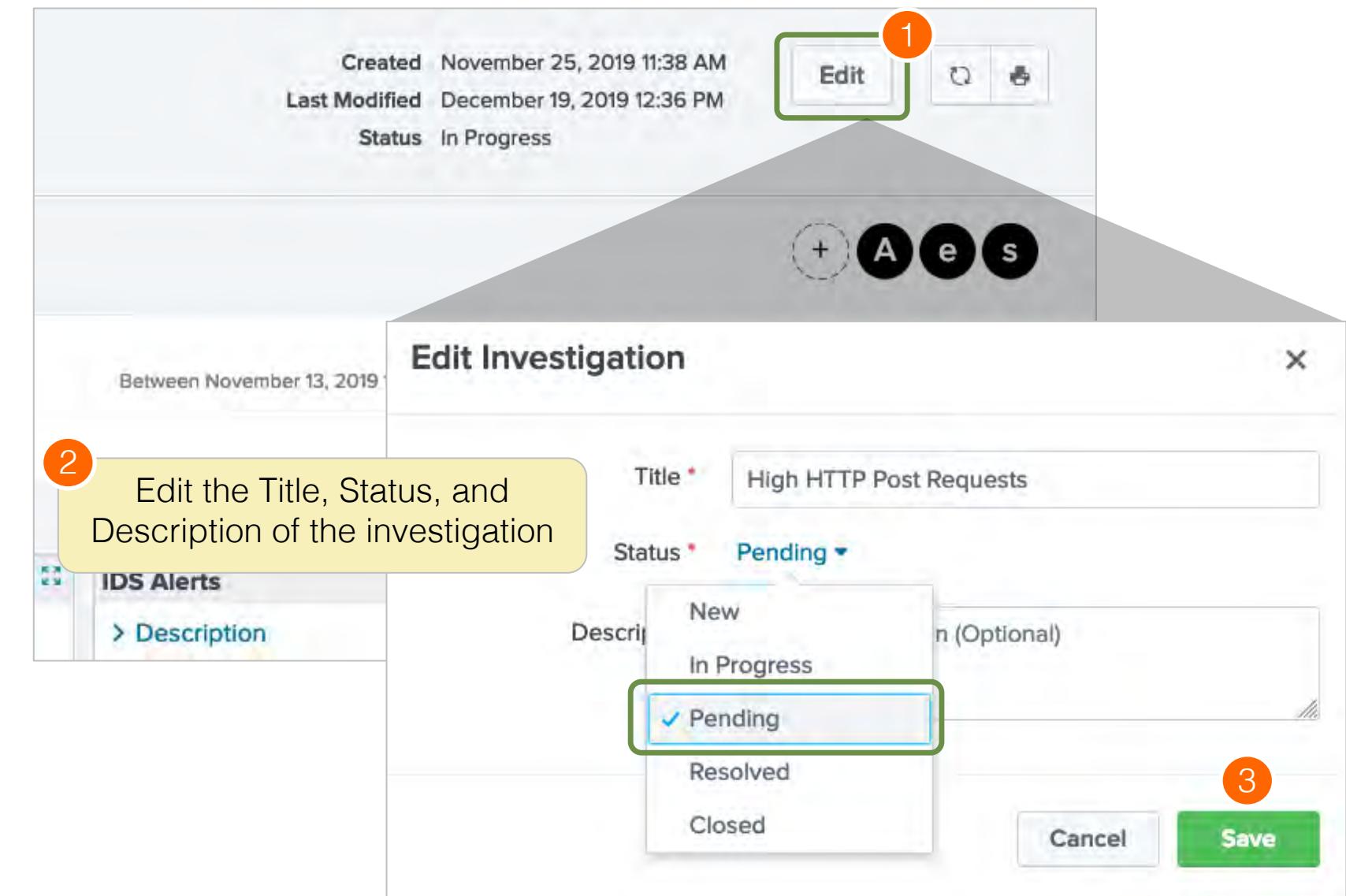
# Adding Collaborators to an Investigation



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Updating Investigation Status

- When you open an investigation, the status is New
- Investigations can only be deleted by admins
- Analysts can delete investigation entries



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Investigation Summary View

Workbench Timeline Summary

**Notable Events**

Expand for details

Urgency: Low Time: December 11, 2019 12:50 AM Security Domain: Network Title: Abnormally High Number of HTTP POST Request Events By 10.12.34.56 Status: New Owner: unassigned

▼

**Correlation Search**  
Web - Abnormally High Number of HTTP Method Events By Src - Rule ↗

**Incident Review**  
Open in Incident Review ↗

**History**  
No History

**Description**  
A system (10.12.34.56) was detected as generating an abnormally high number of POST request events.

**Event Details**

event\_id ..... 406BED13-4DD4-4AB3-B4A3-4349824AAFE0@@notable@@bb1ed9b97dfab4f19c616503d78874b7  
event\_hash ..... bb1ed9b97dfab4f19c616503d78874b7  
eventtype ..... modnotable\_results, notable

**Investigation Artifacts**

Time	Type	Value	Labels	Source Event	Created by
November 25, 2019 11:39 AM	asset	10.12.34.56		Notable event	a admin
November 25, 2019 11:41 AM	asset	10.11.36.7		Notable event	a admin

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Timeline: Slide View

The screenshot shows the Splunk Enterprise Security interface in 'Timeline' mode. The top navigation bar includes 'Workbench', 'Timeline' (highlighted with a green box), 'Summary', 'Slide View' (highlighted with a green box), 'List View', 'Type: All', 'Filter', and a search bar. To the right are user initials 'A e s' and a '+' button.

A yellow callout box points to the 'Type' dropdown with the text: 'Filter by Type: Action History, Adaptive Response Action, Search String, Notable Event, Note, Splunk Event'.

The main content area displays a 'Notable Event' titled 'Abnormally High Number of HTTP POST Request Events By 10.12.3.4.56'. Below the title are tabs for 'Overview' and 'Details'. The 'Details' tab is active, showing:

- Urgency**: high
- Status**: New
- Owner**: unassigned
- Description**: A system (10.12.34.56) was detected as generating an abnormally high number of POST request events.
- Event Details**:
  - event\_id: 406BED13-4DD4-4AB3-B4A3-4349824AAFE0@@notable@@1b8d514ad4c0a19b001bdfa803aaeae8
  - event\_hash: 1b8d514ad4c0a19b001bdfa803aaeae8
  - eventtype: modnotable\_results, notable

To the right of the event details is a vertical 'Action' dropdown menu with options: 'Edit Entry', 'Delete Entry', and 'Open in Incident Review' (highlighted with a green box).

On the left side of the event details, a yellow callout box says 'Scroll left (newer)'. On the right side, another yellow callout box says 'Scroll right (older)'.

At the bottom, a timeline shows dates from Nov 19 to Nov 30. A specific event entry for November 26 is highlighted with a callout box: 'Click an item to view its details in upper panel'.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Timeline Details View to Add Artifacts

The screenshot illustrates the process of adding artifacts from a timeline details view. It shows three main panels:

- Timeline Details View (Left):** Shows a list of fields and their values for a notable event. A callout (1) points to the "Details" tab with the text: "Click Details for a detailed view of all fields and values".
- Timeline Details View (Middle):** A detailed view of the same fields and values. A callout (2) points to the "notable-20~406BED13-4DD4-4AB3-B4A3-4349824AAFE0" entry with the text: "Click an item to add it as an artifact".
- Add Artifacts View (Right):** An open modal window. A callout (3) points to the "Type", "Description", and "Labels" fields with the text: "Add Artifacts view opens and auto-populates". Another callout (4) points to the "Add to Scope" button at the bottom right.

**Timeline Details View Fields and Values:**

Field	Value
_***critical	0
_***high	12
_***informational	0
_***low	0
_***medium	0
_bkt	notable~20~406BED13-4DD4-4AB3-B4A3-4349824AAFE0
_cd	20:117592
_eventtype_color	none
_indextime	1574236207
_serial	5428

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Timeline: List View

From Timeline, change view to List View

Use the Action menu to delete selected entries

View details

Edit or delete entries or open in Incident Review

			Action	Type	Actions
<input checked="" type="checkbox"/>	<a href="#">Action History</a>	November	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input checked="" type="checkbox"/>	<a href="#">Adaptive Response Action</a>	November	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input checked="" type="checkbox"/>	<a href="#">Notable Event</a>	November	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	<a href="#">Note</a>	November	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	<a href="#">Search String</a>	November	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	<a href="#">Splunk Event</a>	November	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	<a href="#">Notable Event: Abnormally High Number of HTTP POST Request Events By 10.12.34.56</a>	November 20, 2019 12:50 AM	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	<a href="#">Notable Event: Abnormally High Number of HTTP POST Request Events By 10.12.34.56</a>	November 21, 2019 12:50 AM	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	<a href="#">Notable Event: High Or Critical Priority Host With Malware Detected</a>	November 21, 2019 11:44 PM	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	<a href="#">Notable Event: Threat Activity Detected (25.205.98.114)</a>	November 22, 2019 12:10 AM	<a href="#">Delete</a>	Notable Event	<a href="#">Edit Entry</a>   <a href="#">Delete Entry</a>   <a href="#">Open in Incident Review</a>

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Edit Investigation Entry

The screenshot shows a Splunk interface for an investigation entry. At the top left, the timestamp is 12:50 AM November 20, 2019. The title of the entry is "Notable Event: Abnormally High Number of HTTP POST Request Events By 10.12.3 4.56". Below the title is a table of fields and their values:

Field	Value
***critical	0
***high	12
***informational	0
***low	0
***medium	0
_bkt	notable~20~406BED13-4DD4-4AB3-B4A3-4349824AAFE0
_cd	20:117592
_eventtype_color	none
_indexetime	1574236207
_serial	5428

To the right of the table is a context menu with the following options: Action ▾ (highlighted with a green box and circled 1), Edit Entry (highlighted with a green box and circled 1), Delete Entry, and Open in Incident Review.

A callout bubble points to the "Edit Entry" option with the text: "Click Action and select Edit Entry to change the title of the entry".

A modal window titled "Edit Entry" is open. It contains a text input field labeled "Title" with the value "High Number of HTTP POST Request Events By 10:". Below the input field are two buttons: "Cancel" and "Save". A callout bubble points to the "Save" button with the text: "Enter new title and Save".

Numbered callouts: 1 points to the "Edit Entry" menu item; 2 points to the "Save" button in the modal window.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Investigation Bar and Inline Timeline View

Select an investigation from the list or click + to add a new one

The screenshot shows the Splunk Enterprise Security interface. At the top, there's a navigation bar with icons for Home, + New, Questionable Activity for User HaxOr, Status: New, and a dropdown arrow. Below the navigation bar is a sidebar titled "All Investigations" with a search input field. The sidebar lists several investigation types: HTTP CONNECT EVENTS, High HTTP Post Requests, Host with Multiple Infections, and Questionable Activity for User HaxOr. A yellow callout box points to the "Questionable Activity for User HaxOr" item. To the right of the sidebar is the main content area. The top right of the content area has icons for Bell, Filter, Search, Checkmark, and Refresh. A yellow callout box points to the "Status: New" status indicator. Below the status is a button labeled "Toggle the Investigation Timeline". The main content area is titled "Inline Investigation Timeline". It features a timeline with a horizontal axis representing time from 11:11 AM to 2:51 PM. On the timeline, there are several "Notable Event" boxes. One event at 12:33 PM is highlighted with a yellow callout box labeled "Investigation Entries". A green arrow points from this callout to the event box. To the left of the timeline, there are two buttons: "Timeline Zoom" and "Jump to start", both enclosed in yellow callout boxes. The bottom of the interface has a footer with the same navigation bar and status indicators as the top.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Module 5 Lab: Working with ES Investigations

---

**Time:** 50 minutes

**Description:** Create and manage an ES investigation

**Tasks:**

- Create an investigation to monitor user *HaxOr* over time
  - Add notable events to your investigation
  - Add an alert for results of future related notable events
- Create an investigation to monitor Snort activity
  - Find Snort events and add a Quick Search
  - Create a notable event to track status
  - Investigate source systems
  - Review your investigation from Timeline and Summary views

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Module 6: Security Domain Dashboards

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Objectives

---

- Use ES to inspect events containing information relevant to active or past incident investigation
- Identify security domains in ES
- Use ES security domain dashboards
- Launch security domain dashboards from Incident Review and from action menus in search results

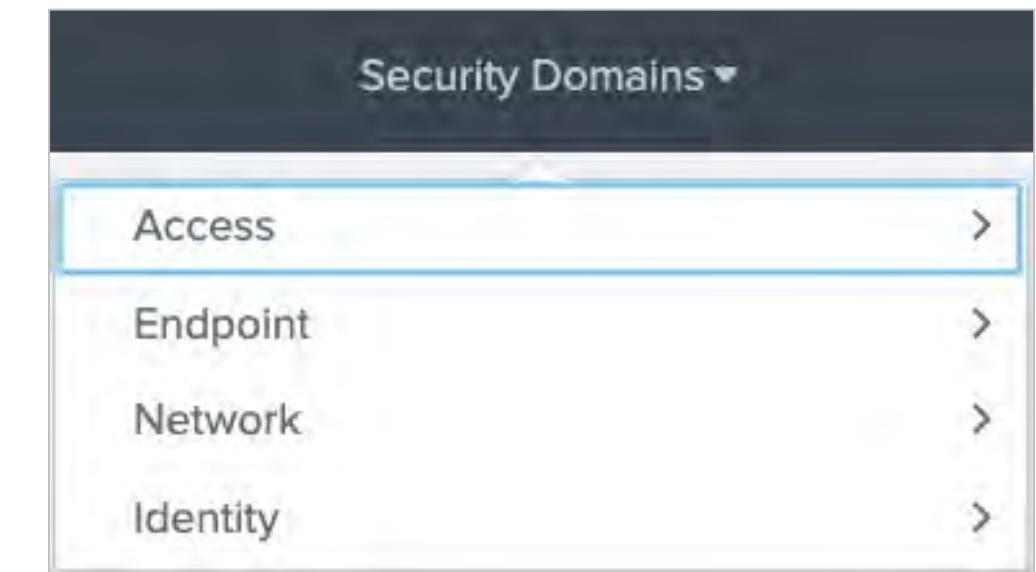
# ES and Forensic Investigation

---

- When a breach occurs, you need to examine the details related to the incident to determine a root cause and eliminate the risk
- The Security Domain dashboards provide the necessary tools to examine related log and stream data in depth
- You can also use these dashboards as part of a periodic security status evaluation
- The dashboards are organized by security domain

# Security Domains

- **Access:** authentication attempts and access control related events (login, access allowed, access failure, etc.)
- **Endpoint:** malware infections, system configuration, system state (CPU usage, open ports, uptime), patch status and history (which updates have been applied), and time synchronization information
- **Network:** information about network traffic provided from devices such as firewalls, routers, network-based intrusion detection systems, and hosts
- **Identity:** examine identity and asset collection data



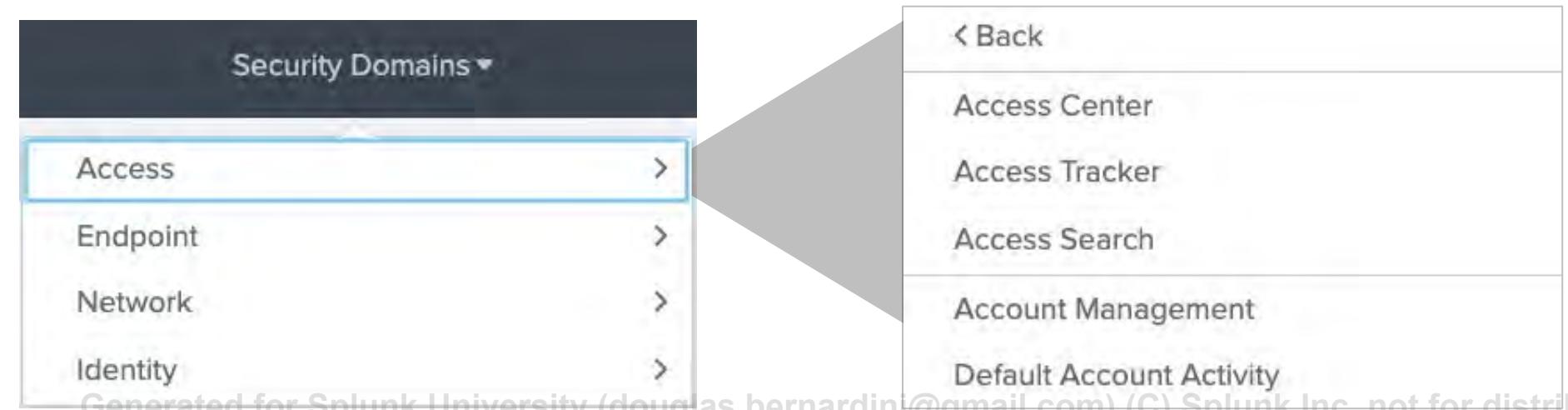
# How to Use Domain Dashboards

---

- Use the dashboards:
  - During forensic investigation of current or past security incidents
  - To drill down into root causes of notable events
  - Examining events related to an asset or identity you are investigating
  - To periodically evaluate the status of security-related events
- Access the Security Domain dashboards from:
  - The **Security Domains** menu
  - Field Action menu in Incident Review search results

# Access Domain

- The Access domain focuses on user identity and authentication
- Dashboards provide tools to research:
  - Brute force attacks
  - Privileged account misuse (i.e., root)
  - Access by rare or new accounts
  - Access by expired or disabled accounts
  - Access by unusual applications (i.e., SSH, VNC, etc.)



# Access > Access Center

**Action**: failure    **App**: sshd    **Business Unit**: americas    **Category**: cardholder    **Special Access**: Privileged    **Time Range**: Last 24 hours

**Key Indicators**

**AUTH. APPS**: Distinct Count: 16 **AUTH. SOURCES**: Distinct Count: 182 **AUTH. DEST'S**: Distinct Count: 102 **AUTH. USERS**: Distinct Count: 3.3k **AUTH. ATTEMPTS**: Total Count: extreme

**Access Over Time By Action**

Large failure rates indicate brute force probing

**Access Over Time By App**

High access rates from a single app like sshd can be malicious

**Top Access By Source**

src	sparkline
10.11.36.34	
10.11.36.28	

**Top Access By Unique Users**

count	src	sparkline	user_count
36142	10.11.36.1		104
6000	10.11.36.0		104

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

**splunk**® turn data into doing™

132

Using Splunk Enterprise Security  
Copyright © 2022 Splunk, Inc. All rights reserved | 25 May 2022

# Access > Access Search

Clicking a **src** or **user\_count** under the Top Access By Unique Users panel on the Access Center displays the details on who is accessing the Source

Action	App	Source	Destination	User	Count		
All	All	10.11.36.41			Between Date-times		
<b>Hide Filters</b>							
_time	action	app	src	src_user	dest	user	count
2021-12-15 22:17:47	failure	sshd	10.11.36.41		ip-10-0-0-169.us-west-2.compute.internal	naughtyuser	1724
	success						
2021-12-15 22:15:45	failure	sshd	10.11.36.41		ip-10-0-0-169.us-west-2.compute.internal	test	1460
2021-12-15 22:04:36	failure	sshd	10.11.36.41		ip-10-0-0-169.us-west-2.compute.internal	oracle	1239
2021-12-15 22:15:51	failure	sshd	10.11.36.41		ip-10-0-0-169.us-west-2.compute.internal	user	796
2021-12-15 22:06:21	failure	sshd	10.11.36.41		ip-10-0-0-169.us-west-2.compute.internal	test3	656

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

i	Time	Event
>	12/15/21 10:28:36.000 PM	Dec 15 22:28:36 acmepayroll sshd[14003]: Invalid user cvs from 10.11.36.41 action = failure failure   app = sshd   dest = ip-10-0-0-169.us-west-2.compute.internal   src = 10.11.36.41   src_user = unknown   user = cvs
>	12/15/21 10:28:14.000 PM	Dec 15 22:28:14 10.84.34.20 auth security:notice login: [ID 143248 auth.notice] Login failure on /dev/pts/17 from 10.11.36.41 action = failure failure   app = login   dest = ip-10-0-0-169.us-west-2.compute.internal   src = 10.11.36.41   src_user = unknown   user = unknown

Expand the events to view more details, create a notable event, or add the event to an investigation

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Other Access Domain Dashboards

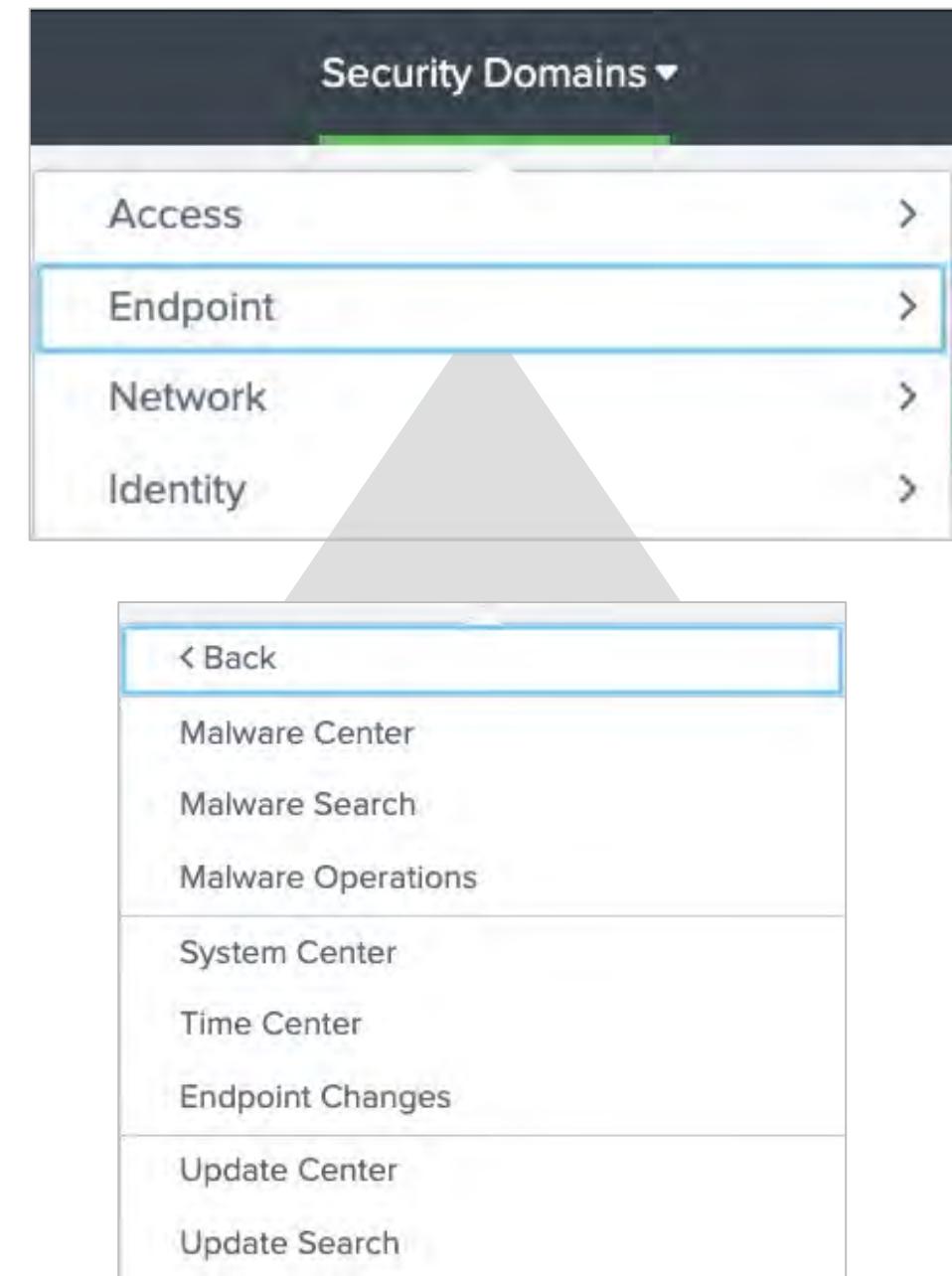
Access Tracker	Account activity over time for: <ul style="list-style-type: none"><li>• first time access</li><li>• inactive accounts</li><li>• expired identities</li></ul>
Account Management	Account actions, like: <ul style="list-style-type: none"><li>• creation</li><li>• deletion</li><li>• lockout</li></ul>
Default Account Activity	Usage of default accounts, which are built-in to an operating system, such as: <ul style="list-style-type: none"><li>• root/administrator</li><li>• SYSTEM</li><li>• guest</li></ul>

\*\*Splunk is adding new Correlation Searches all the time. Check the Enterprise Security documentation to view the specific searches available for your version ES

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Endpoint Domain

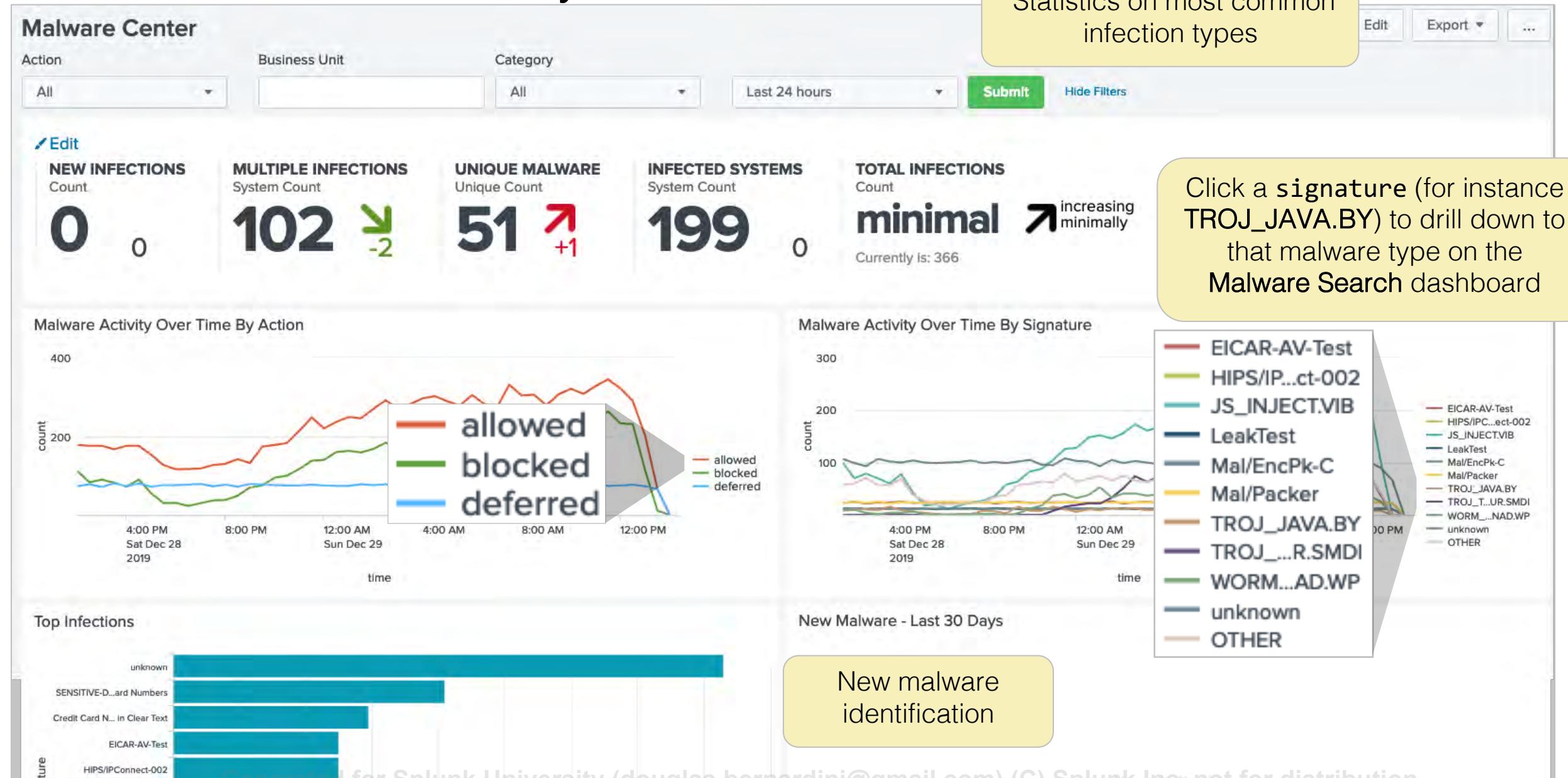
- The Endpoint domain watches over user systems, such as:
  - Workstations, PCs, notebooks
  - Handheld devices
  - Point-of-sale systems
- Potential issues include:
  - Vulnerabilities: missing updates or patches
  - Malware: spyware, ransomware, or other malicious code
  - Unexpected running processes or services
  - Unexpected registry changes



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Endpoint > Malware Center

## Overview of malware in your environment



# Endpoint > Malware Search

**Malware Search**

Action Signature File Destination User

All TROJ\_JAVA.BY Since 1970 Submit

**Hide Filters**

\_time file\_name dest user count

2021-12-15 TROJ\_JAVA.BY KAK\NED\NOD32.class NOODLE1 Mark 1359  
KAK\NED\crime4u.class  
KAK\NED\sexxxy.class  
jar\_cache2477643956744743216.tmp  
jar\_cache5098539579616777024.tmp  
jar\_cache541963562908274498.tmp

2021-12-15 21:49:43 allowed TROJ\_JAVA.BY KAK\NED\NOD32.class IRONHIDE-PC iron.hide 1193  
KAK\NED\crime4u.class  
KAK\NED\sexxxy.class  
jar\_cache6011667656060081086.tmp  
jar\_cache6706099793089863807.tmp  
jar\_cache8012177679726229753.tmp

i Time Event

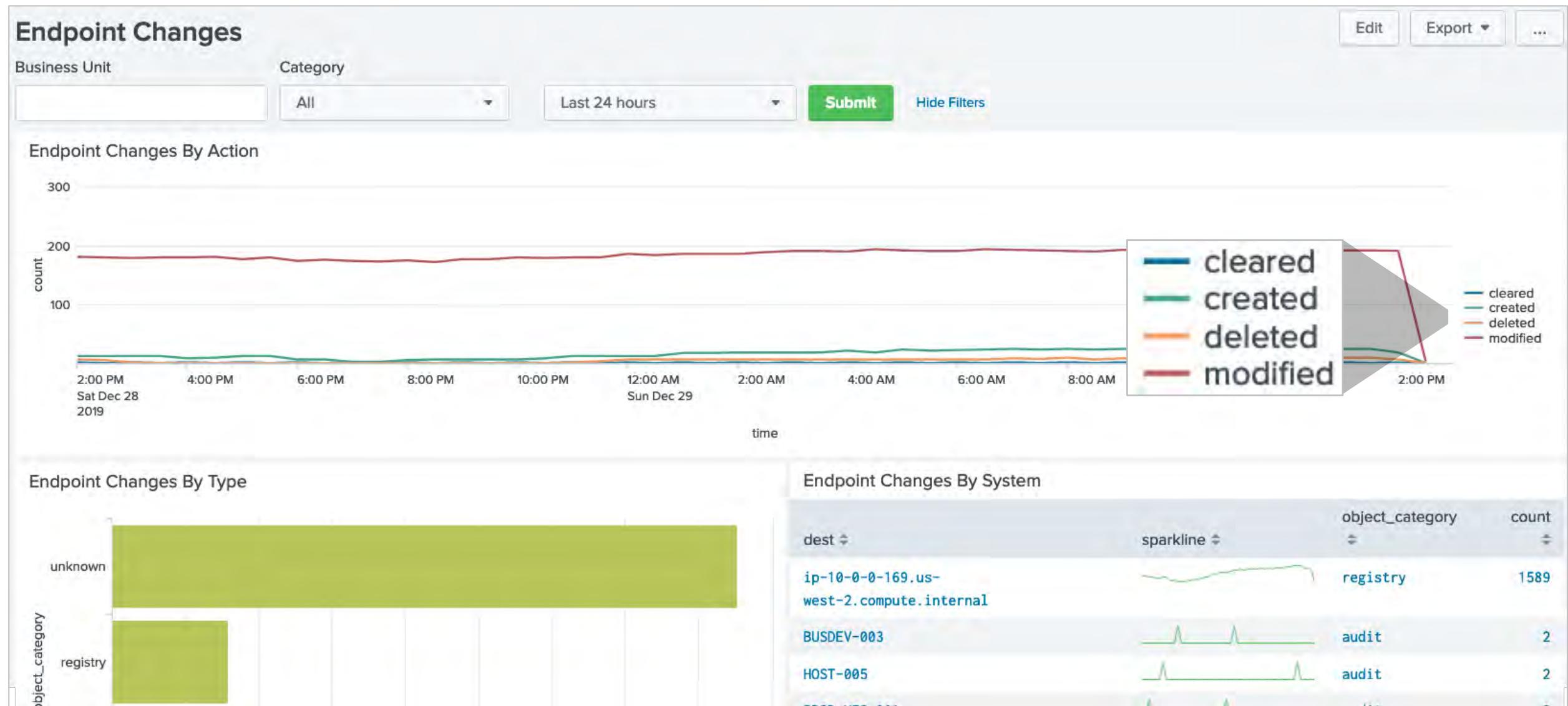
> 12/15/21 12/15/2021 09:49:43 PM  
9:49:43.000 PM LogName=Application  
SourceName=Trend Micro OfficeScan Server  
EventCode=10  
EventType=2  
Show all 18 lines

action = allowed | dest = IRONHIDE-PC | file\_name = KAK\NED\crime4u.class file\_name = jar\_cache6706099793089863807.tmp | signature = TROJ\_JAVA.BY | user = iron.hide

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Endpoint > Endpoint Changes

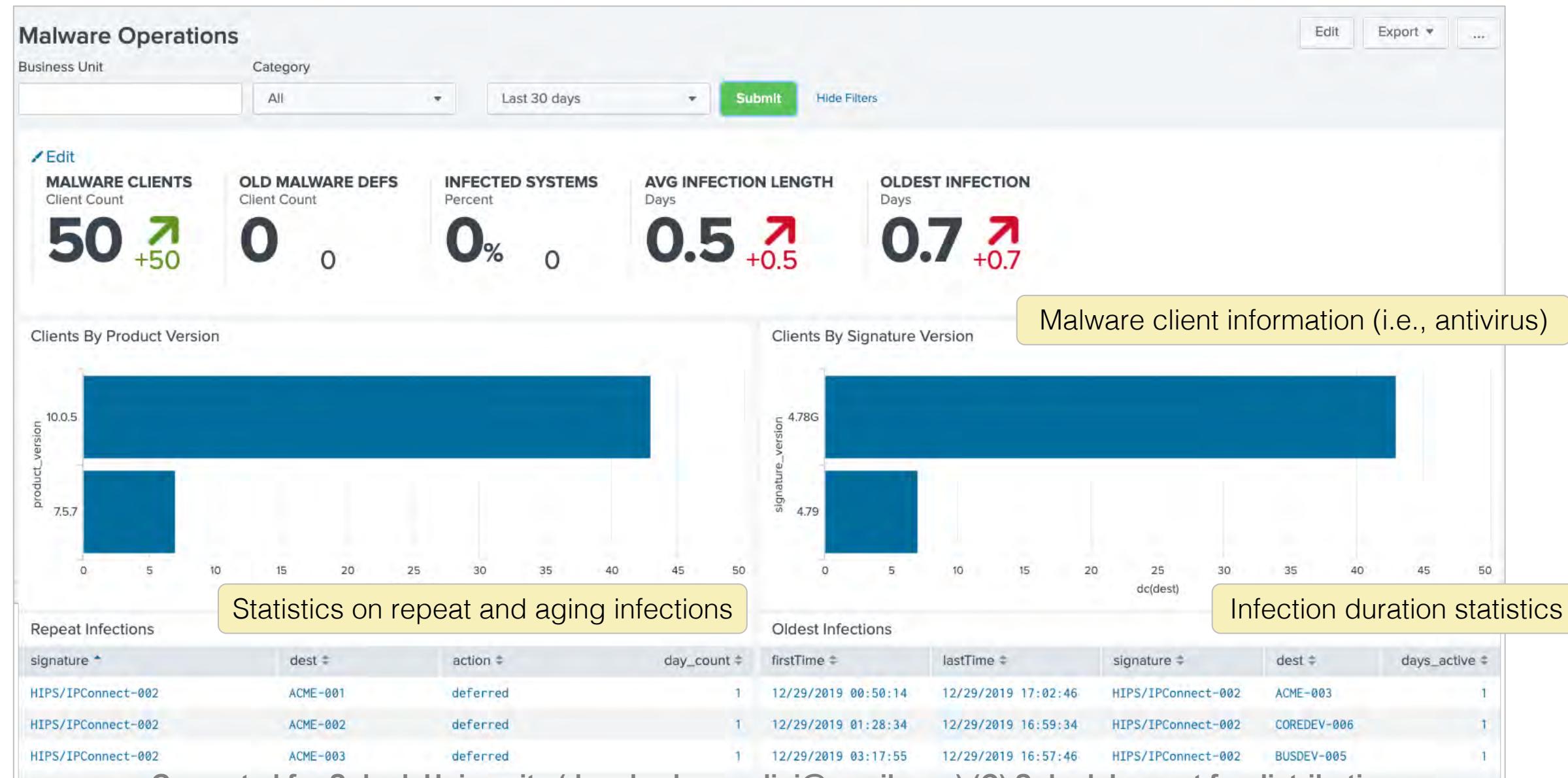
Track changes on your systems by type (file, registry, etc.) or by system



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Endpoint > Malware Operations

## Malware status overview



# Endpoint > Time Center

Report the status of time synchronization in your environment

### Time Center

Show only systems that should timesync

System Business Unit Category

All All Last 30 days

Edit Export ...

Submit Hide Filters

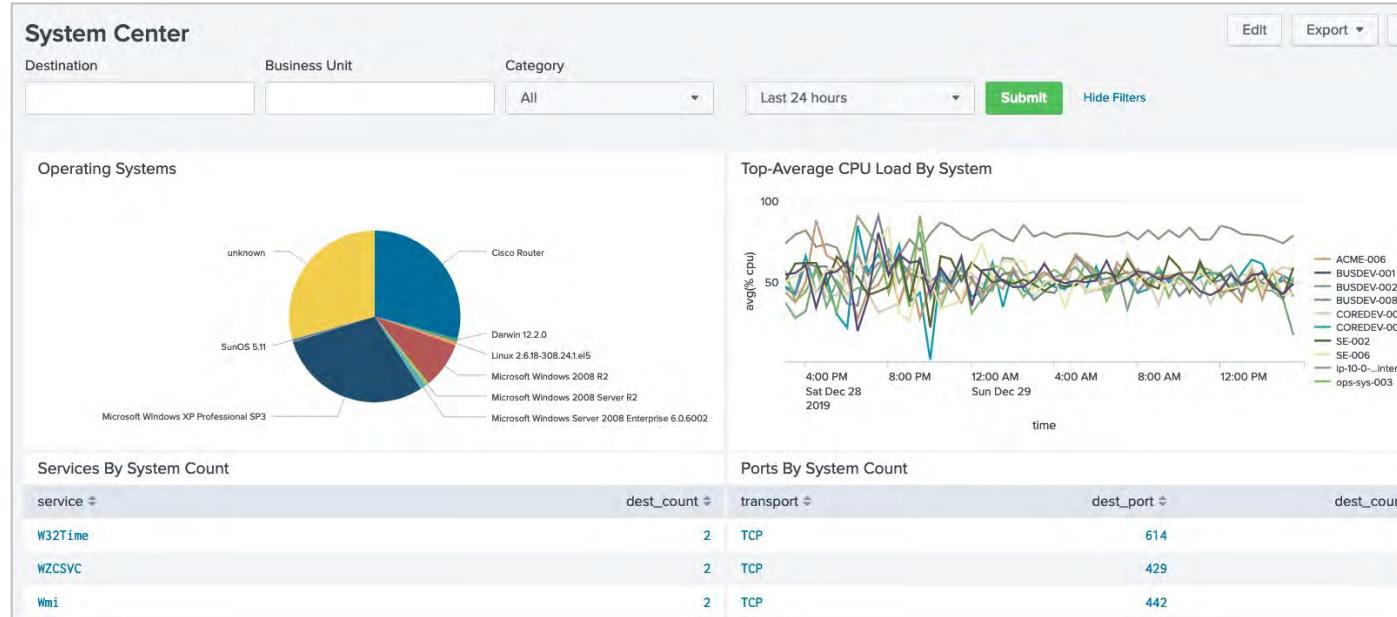
Time Synchronization Failures					Systems Not Time Syncing				
_time	action	dest	dest_should_timesync	count	firstTime	lastTime	dest	dest_should_timesync	
2021-01-07 16:16:12	failure	HOST0167		7542	12/09/2020	01/07/2021	HOST0201	true	
Systems not properly synchronizing will not send correct time-stamped data to Splunk Can lead to search failure and false negatives in ES					00:21:17	16:16:28	ip-10-0-0-169.us-west-2.compute.internal		
					12/09/2020	01/07/2021	ip-10-0-0-169.us-west-2.compute.internal		
					00:00:06	16:59:46			

Indexing Time Delay					Time Service Start Mode Anomalies				
host	host_should_timesync	min_diff(minutes)	avg_diff(minutes)	max_diff(minutes)	_time	dest	dest_should_timesync	service	start_mode
COREDEV-002	true	5.0	5.0	5.0	2021-01-07 16:55:18	SJCDCSV012ERP01	true	W32Time	Manual
HOST-005	true	5.0	5.0	5.0	2021-01-07 16:55:59	ip-10-0-0-169.us-west-2.compute.internal		W32Time	Manual
PROD-MFS-004	true	5.0	5.0	5.0					

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Other Endpoint Domain Dashboards

O/S statistics & versions in use



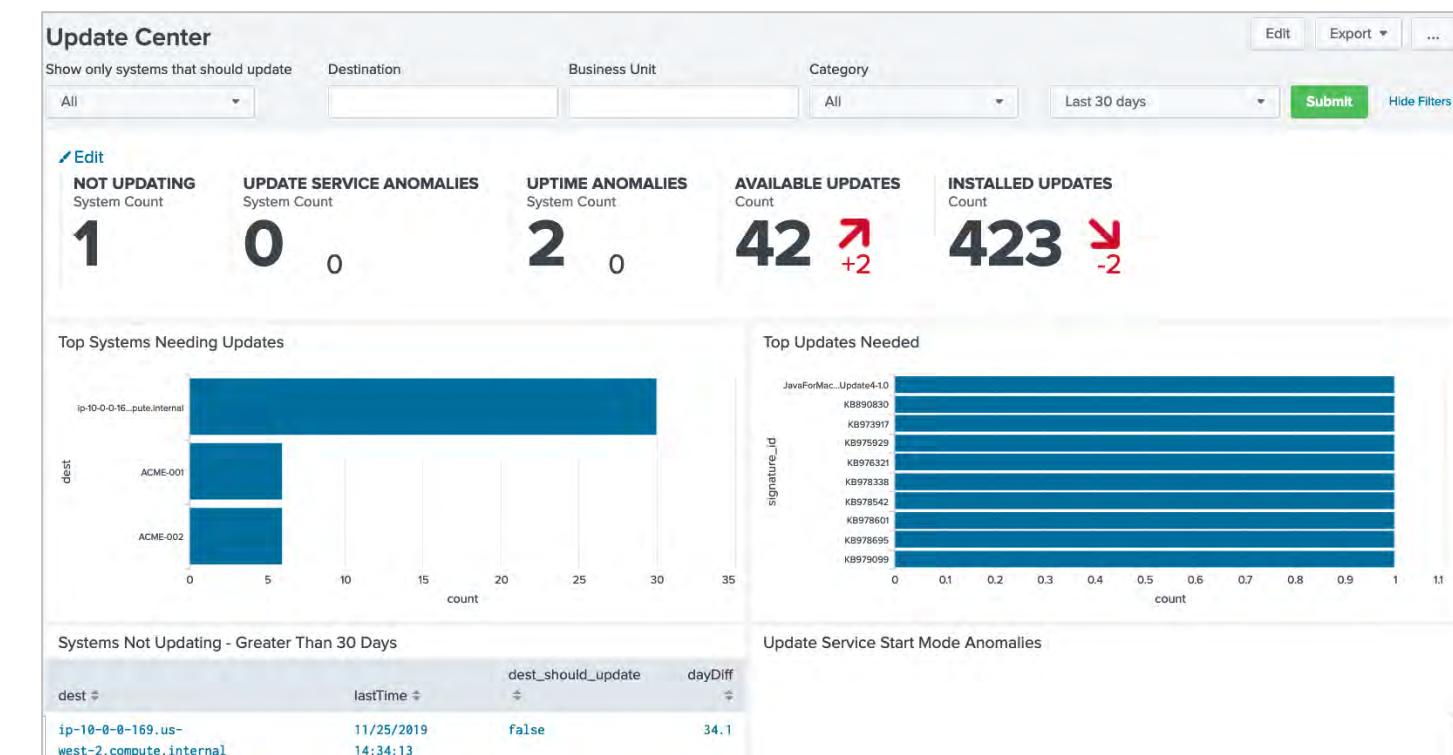
Search interface for update events

The Update Search interface allows filtering by update status (All Systems, All Status), signature, and destination. It shows a table of recent update events with columns for \_time, status, signature\_id, signature, dest, and dest\_should\_update. Below the table is a detailed log of specific events, including timestamp, package name, and status.

_time	status	signature_id	signature	dest	dest_should_update
2019-12-29 15:44:47	available	iMacFirmwareUpdate-1.3	iMacFirmwareUpdate-1.3	ACME-002	false
2019-12-29 15:44:39	available	OpenIPMI-libs.x86_64	OpenIPMI-libs.x86_64	ACME-001	false
2019-12-29 15:44:38	installed	KB950050	Update (KB950050)	ip-10-0-0-169.us-west-2.compute.internal	false
2019-12-29 15:44:29	installed	KB938464	Security Update (KB938464)	ip-10-0-0-169.us-west-2.compute.internal	false
2019-12-29 15:44:27	available	alsa-utils.x86_64	alsa-utils.x86_64	ACME-001	false

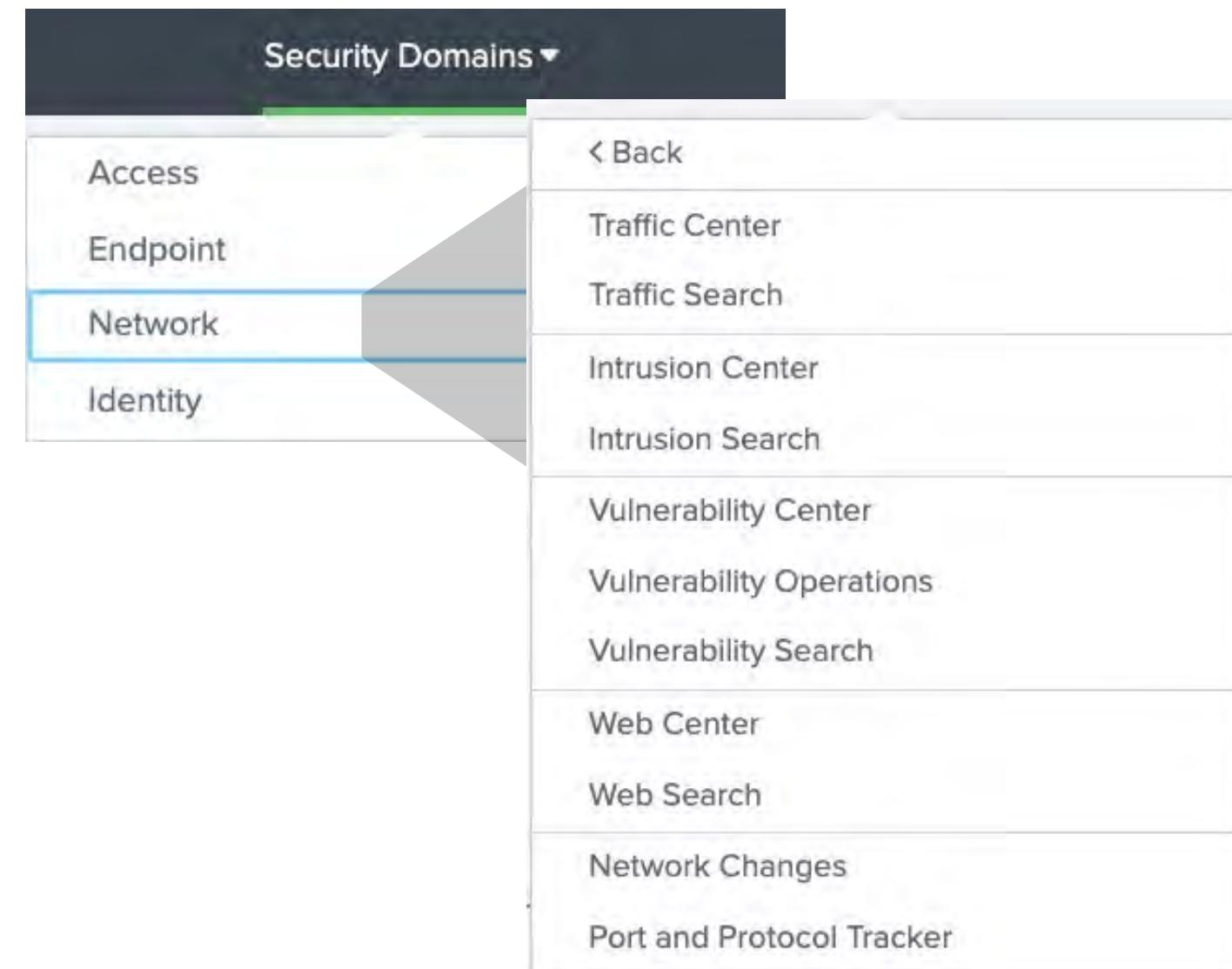
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Patches and other software update statistics



# Network Domain

- Many Network domain scenarios are preventative in nature:
  - Suspicious activity spotted by intrusion detection systems (IDS)
  - Vulnerabilities
  - Unusual ports being opened
  - Suspicious DNS activity
  - Port scanning



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Network > Intrusion Center

Events logged from intrusion detection systems (IDS)

IDS Type: network   IDS Category: trojan-activity   Severity: All   Business Unit:   Category: All   Last 24 hours   Submit

**HIGH SEV. ATTACKS** Count: **20.8k** -2.4k   **ATTACK CATEGORIES** Unique Count: **30** 0   **ATTACK SIGNATURES** Unique Count: **104** 0   **ATTACK SOURCES** Unique Count: **2.2k** +163   **ATTACK DESTINATIONS** Unique Count: **1.4k** +98

Use filters to focus on types of attacks. The example focuses on trojan activity on the network

Attacks Over Time By Severity

Dec 15, 2021 7:30 AM  
high: 4

Top Attacks

signature	src_count	dest_count	count
A Network Trojan was Detected	34	39	72

Click a result to drill down to the **Intrusion Search** dashboard

Scanning Activity (Many Attacks)

New Attacks - Last 30 Days

No results found.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Network > Intrusion Search

Clicking on a result in the **Intrusion Center** displays the specifics of the attack in the **Intrusion Search** dashboard

**Intrusion Search**

IDS Category Severity Signature Source Destination Between Date-times

All A Network Trojan was Detected

Submit

Hide Filters

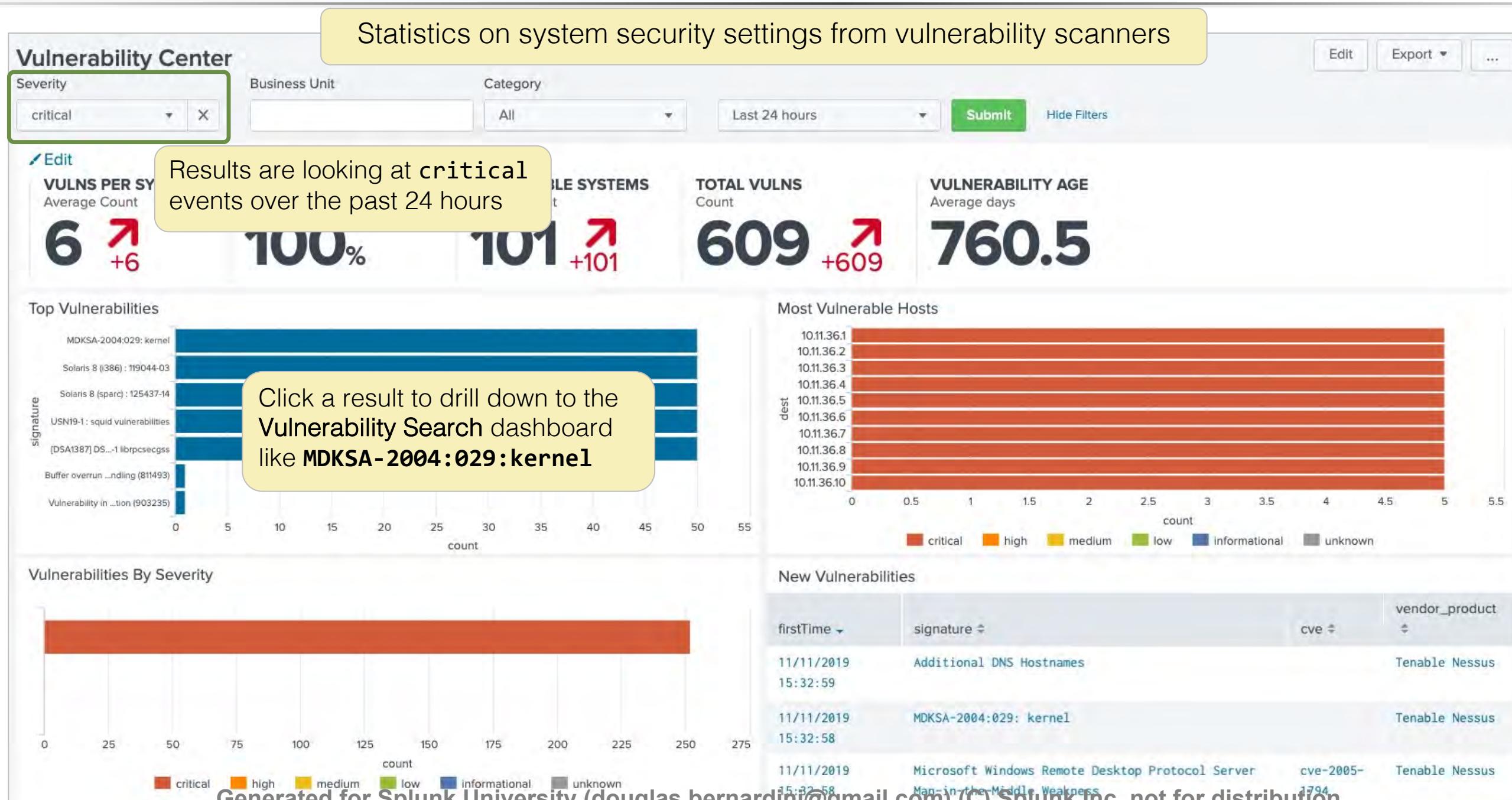
_time	severity	category	Signature	dest	count
2021-12-15 16:51:26	high	trojan-activity	A Network Trojan was Detected	173	10.11.36.27
2021-12-15 08:36:47	high	trojan-activity	A Network Trojan was Detected	173	10.11.36.19
2021-12-15 11:20:38	high	trojan-activity	A Network Trojan was Detected	172.30.16.173	10.11.36.42
2021-12-15 20:46:57	high	trojan-activity	A Network Trojan was Detected	172.30.16.173	10.11.36.43
2021-12-15 16:11:02	high	trojan-activity	A Network Trojan was Detected	10.11.36.10	10.11.36.39

< Prev 1 2 3 4 5 6 7 8 9 10 Next »

i	Time	Event
>	12/15/21 11:34:20.000 PM	Wed Dec 15 23:34:20 2021 archive_timestamp=1354031565 sensor_id=56 event_id=67582 event_sec=1354032623 event_usec=73789 sid=18341 gen=1 rev=7 class=21 priority=1 src_addr=10.11.36.31 dst_addr=10.11.36.2 src_port=56902 dst_port=80 ip_proto=6 impact_flag=99 category = trojan-activity   dest = 10.11.36.2   dest_port = 80   severity = high   signature = A Network Trojan was Detected   src = 10.11.36.31   src_port = 56902   user = unknown   vendor_product = Sourcefire IDS
>	12/15/21 11:09:40.000 PM	Wed Dec 15 23:09:40 2021 archive_timestamp=1354032323 sensor_id=56 event_id=67589 event_sec=1354033380 event_usec=966871 sid=23246 gen=1 rev=3 class=21 priority=1 src_addr=172.30.16.173 dst_addr=10.11.36.29 src_port=51727 dst_port=80 ip_proto=6 impact_flag=35 category = trojan-activity   dest = 10.11.36.29   dest_port = 80   severity = high   signature = A Network Trojan was Detected   src = 172.30.16.173   src_port = 51727   user = unknown   vendor_product = Sourcefire IDS

Drilling down from the **A Network Trojan was Detected** entry on the **Intrusion Center** populates the search fields

# Network > Vulnerability Center



# Network > Vulnerability Search

Clicking on a result in the **Vulnerability Center** displays the specifics of the issue in the **Vulnerability Search** dashboard

Signature **MDKSA-2004:029: kernel**

Drilling down from the **MDKSA-2004:029: kernel** entry on the **Vulnerability Center** populates the **Signature** field

_time	category	severity	dest	count
2021-12-15 22:38:00	unknown	critical	10.11.36.16	18
2021-12-15 22:29:55	unknown	critical	10.11.36.18	17
2021-12-15 23:02:14	unknown	critical	10.11.36.5	17
2021-12-15 22:56:10	unknown	critical	10.11.36.14	16
2021-12-15 22:33:58	unknown	critical	10.11.36.21	16

Time Event

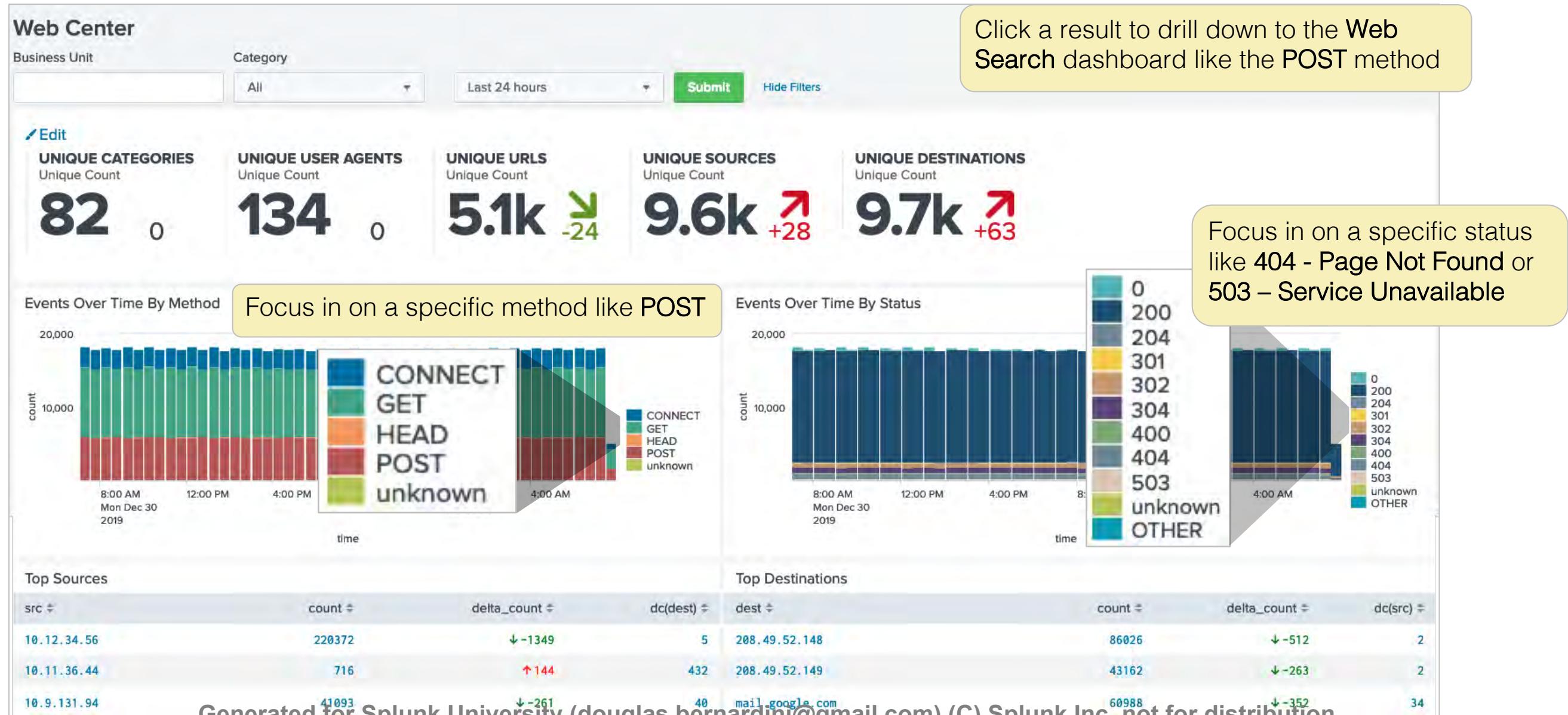
> 12/15/21 start\_time="Wed Dec 15 22:32:58 2021" end\_time="Wed Dec 15 22:55:42 2021" dest\_ip="10.11.36.39" os="Cisco Router" dest\_port\_proto="el-random(2426/tcp)" severity\_id="4" signature\_id="14128" signature="MDKSA-2004:029: kernel"  
11:14:20.000 PM category = unknown | dest = 10.11.36.39 | dvc = unknown | severity = critical | signature = MDKSA-2004:029: kernel

> 12/15/21 start\_time="Wed Dec 15 22:23:44 2021" end\_time="Wed Dec 15 22:35:37 2021" dest\_ip="10.11.36.44" os="Cisco Router" dest\_port\_proto="el-random(2426/tcp)" severity\_id="4" signature\_id="14128" signature="MDKSA-2004:029: kernel"  
11:12:19.000 PM category = unknown | dest = 10.11.36.44 | dvc = unknown | severity = critical | signature = MDKSA-2004:029: kernel

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Network > Web Center

HTTP activity insights from web server, proxy, and firewall logs



# Network > Web Search

Drilling down from the POST entry on the **Web Center** populates the search fields

HTTP Method	HTTP Status	Source	Destination	URL
POST				

Between Date-times  Hide Filters

_time	http_method	status	src	dest	url	count
2019-12-31 07:47:36	POST	200	10.7.12.70	propertyroom.com	http://propertyroom.com/ActionListingsService.asmx/GetActionListings	2367
2019-12-31 07:47:41	POST	302	145.1.147.59	10.79.57.221	http://10.79.57.221/secreg/secreg.dll?l=2	1483
2019-12-31 07:44:53	POST	200	10.22.62.188	www.facebook.com	http://www.facebook.com/ajax/wallkit_get.php	1037

\* Prev 1 2 3 4 5 6 7 8 9 10 Next »

i	Time	Event
>	12/31/19 7:47:41.000 AM	2019-12-31 14:47:41 10.19.248.223 0 87 TCP_NC_MISS 200 200 368 1804 - - OBSERVED POST mail.google.com HTTP/1.1 1810 http://mail.google.com/mail/channel/bind?VER=6&it=71945207&at=xn3j387ckdqwlctokcfyssmwohav2&ui=2&SID=C32FF7AB76D3A71D&RID=60514&zx=3be4w8-47pmu7&t=1 http://mail.google.com/mail/?ui=2&view=js&name=js&ver=IAd6MtWKi0g.en.&am!=_SV7VRCFDgHpRd_gfwf0QnAuW3EiMBRKreZkWYtn text/plain;%20charset=utf-8 "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; InfoPath.1; MS-RTC LM 8; yie8)" "HSID=A12UjR2EZ71YdTxe0" dest = mail.google.com   http_method = POST   http_referrer = http://mail.google.com/mail/?ui=2&view=js&name=js&ver=IAd6MtWKi0g.en.&am...   http_user_agent = Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50...   src = 10.19.248.223   status = 200   url = http://mail.google.com/mail/channel/bind?VER=6&it=71945207&at=xn3j387ckdq...
>	12/31/19 7:47:41.000 AM	2019-12-31 14:47:41 10.12.34.56 946 357 TCP_NC_MISS 200 200 879 218 - - OBSERVED POST 208.49.52.148 HTTP/1.0 224 http://208.49.52.148/idle/GdWmYD8QsRMm0fIf/5125 - application/x-fcs "Shockwave Flash" - dest = 208.49.52.148   http_method = POST   http_referrer = unknown   http_user_agent = Shockwave Flash   src = 10.12.34.56   status = 200   url = http://208.49.52.148/idle/GdWmYD8QsRMm0fIf/5125

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Other Network Domain Dashboards

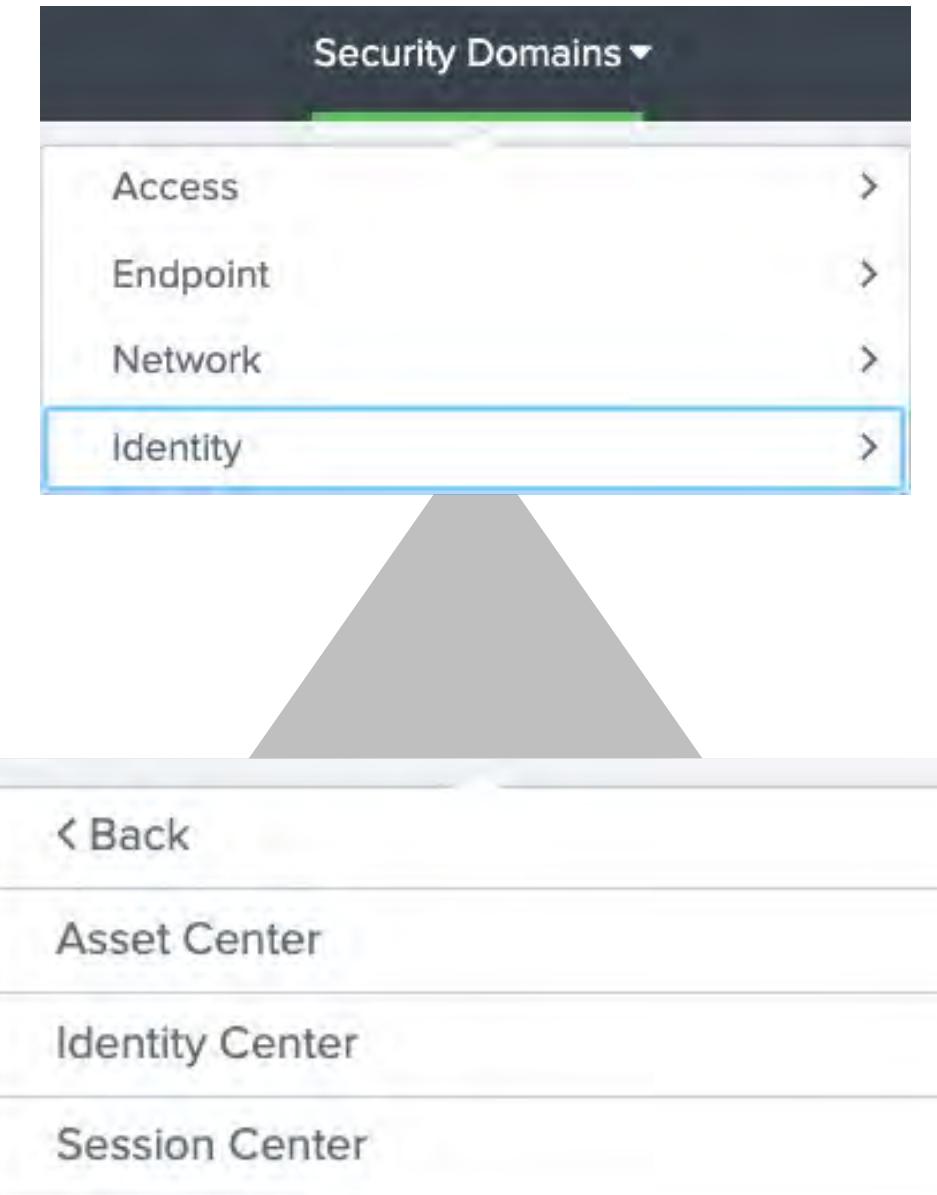
Vulnerability Operations	Statistics on vulnerability aging and scan activity
Network Changes	Events recording changes to network configurations on routers, firewalls, etc.
Port and Protocol Tracker	Analysis of network activity by port type or protocol type

\*\*Splunk is adding new Correlation Searches all the time. Check the Enterprise Security documentation to view the specific searches available for your version ES

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Identity Domain

- Identity domain dashboards provide information about the assets and identities defined in ES
- Use the **Asset Center** or **Identity Center** to view lists of objects used by the Assets and Identity framework
- View assets or identities by priority level, business unit, or category
- Troubleshoot network sessions by device or user



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Identity > Asset Center

## Security Domains > Identity > Asset Center

### Asset Center

Asset Priority Business Unit Category Owner

\* All All All Submit Hide Filters

Assets By Priority Distribution of assets by priority

Priority	Events
critical	~8
high	~24
low	~17
medium	~36

Assets By Business Unit Distribution of assets by business unit

Business Unit	Percentage
apac	~50%
americas	~30%
emea	~15%
other	~5%

Assets By Category Distribution of assets by category

Category	Percentage
pci	~50%
emea	~20%
virtual	~10%
sox	~5%
other	~5%

Asset Information

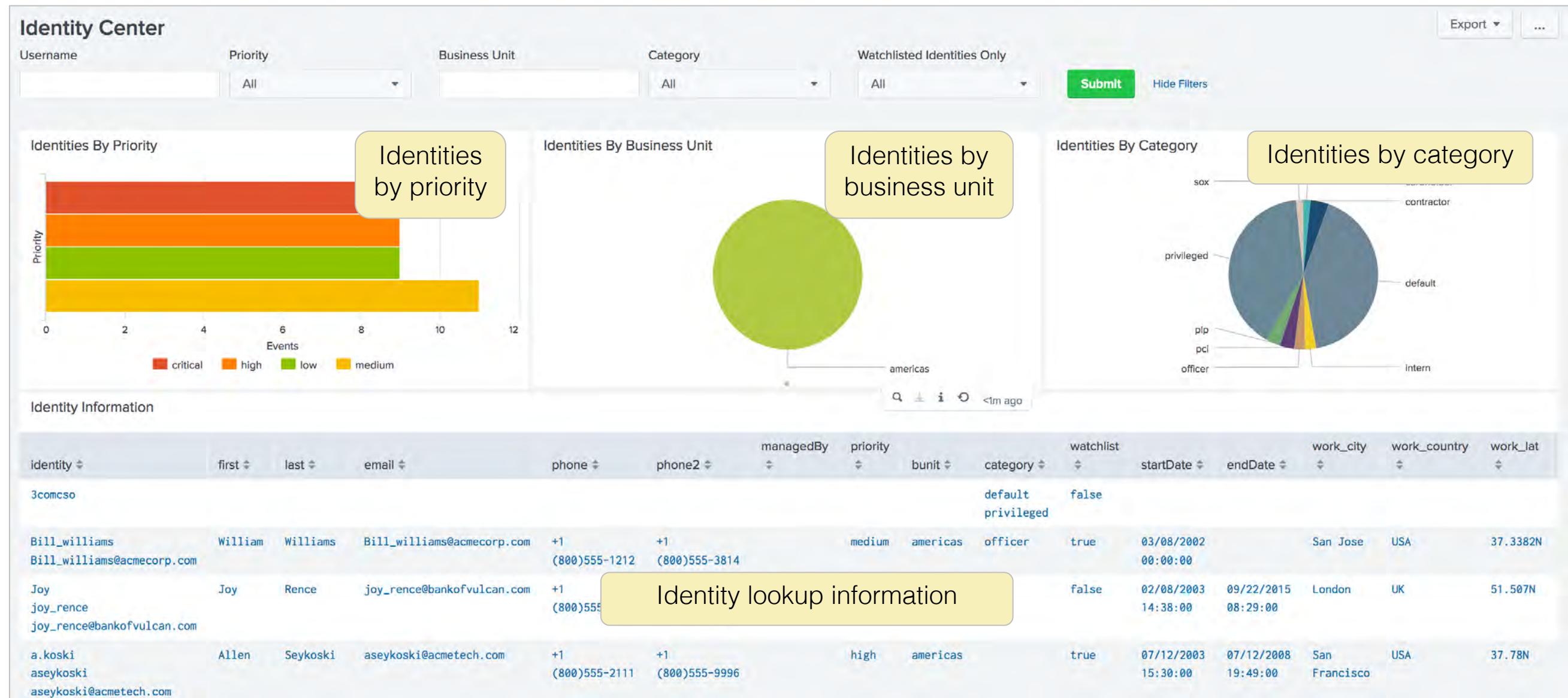
ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_update	requires_av
		ACME-006			high	50.84436	-0.98451	Havant	UK	emea	pci	trust wireless	false	true	true	true
		ops-sys-005			medium	32.931277	-96.					trust	true	true	true	true
		HOST0202			medium	37.694452	-121.894461	Pleasanton	USA	americas		untrust	true	false	true	true
00:25:ac:42:f4:60	00:25:cc:42:f4:60				medium	38.959405	-77.04	Washington D.C.	USA	americas		untrust	false	true	true	false

Asset lookup information

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Identity > Identity Center

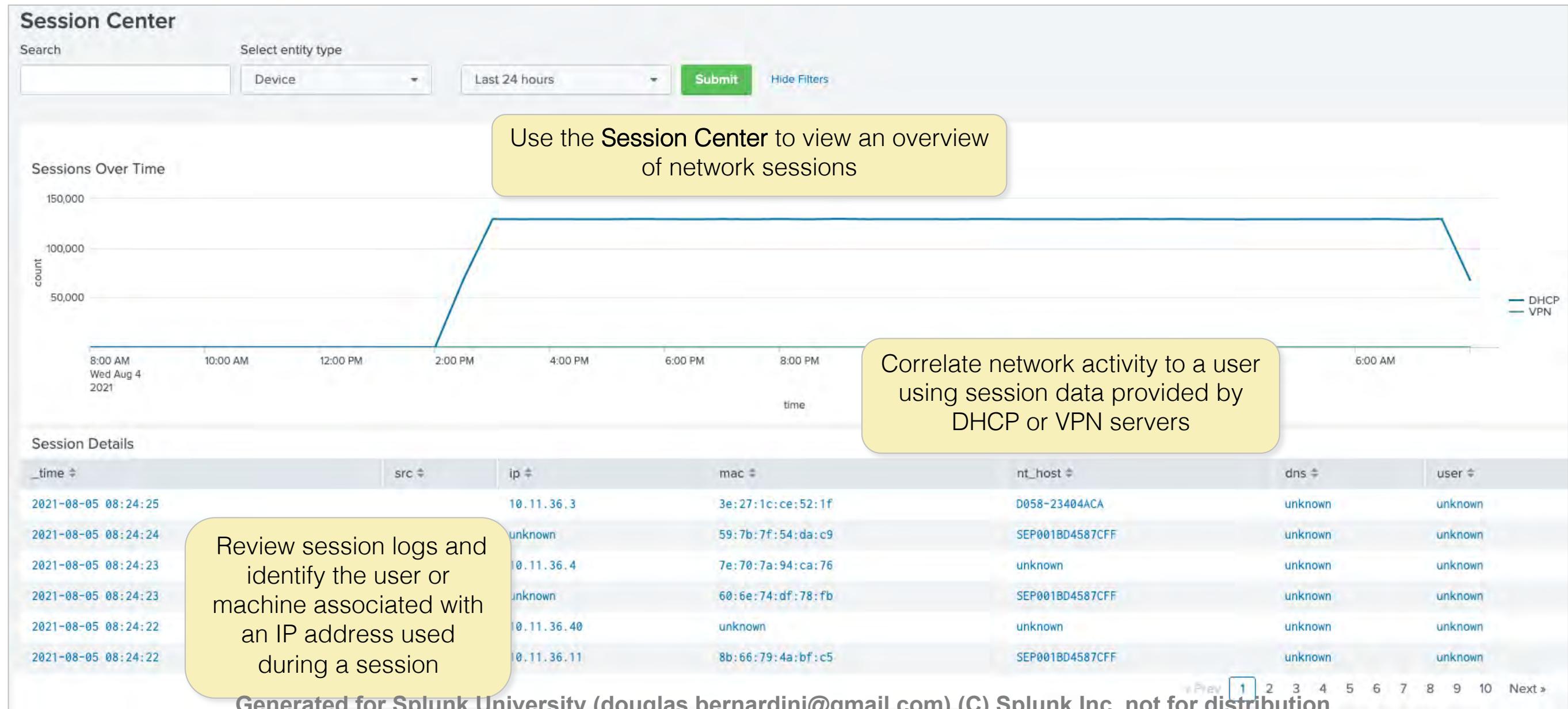
## Security Domains > Identity > Identity Center



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Identity > Session Center

## Security Domains > Identity > Session Center



# Module 6 Lab: Using Security Domain Dashboards

---

- Time: 30 minutes
- Scenario:
  - Work in the role of a network analyst performing forensic analysis on an open incident
- Tasks:
  - Use the Access Domain dashboard
  - Use the Malware Search and Center dashboards
  - Use the Vulnerability Center and Search dashboards
  - Use the Intrusion Center dashboard

# Module 7: User Intelligence

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

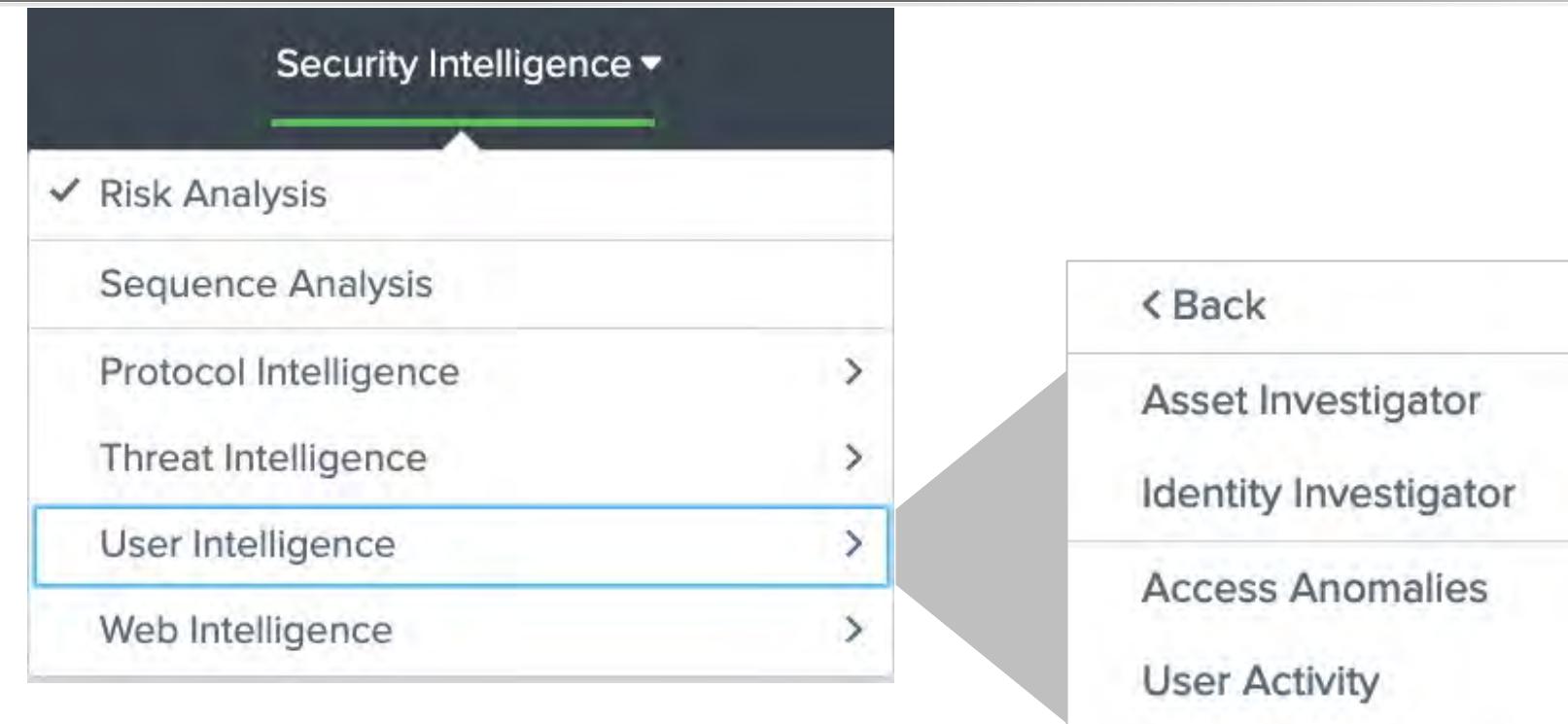
# Objectives

---

- Understand and use user activity analysis
- Use investigators to analyze events related to an asset or identity
- Use access anomalies to detect suspicious access patterns

# Security Intelligence > User Intelligence

User intelligence tools provide the security practitioner with analytical tools to find potential internal threats



Asset Investigator	Examine a specific asset, such as a server or workstation, and compare events over time in parallel lanes showing different types of activity
Identity Investigator	Examine a specific identity and compare events over time in parallel lanes showing different types of activity
Access Anomalies	A survey of network activity by users, highlighting anomalous access (one user account being used multiple times)
User Activity	A survey of people and their actions, focused on watchlisted or high-risk users

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Asset and Identity Investigators

- Investigator dashboards allow you to search by an asset or identity for a specific time range
- Both return a time-sequenced set of **swim lanes** showing activity for that asset or identity

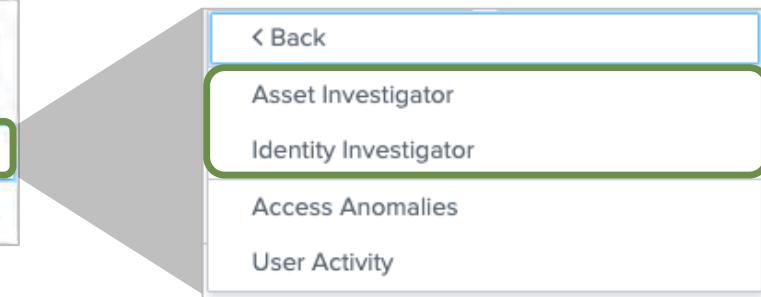


# Accessing the Investigators

Access investigators

From the User Intelligence menu →

The screenshot shows a Splunk interface for managing Notables. At the top, it says "18 Notables" and includes links for "Edit Selected" and "Edit All Matching Events (18)". A single notable is selected, showing details: "Threat Activity Detected (106.96.142.200)". Below this is a "Description" section stating: "Threat activity (106.96.142.200) was discovered in the "src" field based on threat intelligence available in the ip\_intel collection". Under "Additional" fields, there are entries for Destination (141.116.105.229), Source (unknown 720), and Source User (unknown 1440). Threat Category is listed as hijacks, and Threat Collection is ip\_intel. Key Threat Description is "List of IPs hijacked by people who are spammers or general". Threat Group is hijacked\_ip\_addresses, Threat Key is hijacked\_ip\_addresses, Threat Match is src, and Threat Field is Field. On the right, there is an "Action" button with a dropdown menu titled "Asset Investigator" which is highlighted with a green box.



From a field Action menu  
in an Incident Review event

- ▶ Asset: dest, src, ip, host
- ▶ Identity: user, src\_user

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Asset Investigator

Asset Investigator

Search by asset name

acme-004

Asset information

pci_domain: wireless, trust	requires_av: true	owner: taters	nt_host: ACME-004
bunit: emea	lat: 50.84436	should_timesync: true	category: pci
is_expected: false	priority: high	country: UK	long: -0.98451
city: Havant	should_update: true	_time: 2019-05-22T22:03:21+0000	

>Edit

6:00 PM 9:00 PM 5/22/2019 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM

All Authentication

All Changes

Threat List Activity

IDS Attacks

Malware Attacks

Notable Events

Risk Modifiers

Today ▾

18:00 18:00:00 16:03:20

view: a day 6 minutes

Selecting an individual bar (set of events) shows the details in the right panel. A darker bar has more events

Area graph shows activity over time period

Malware Attacks (4)

May 22, 2019 May 22, 2019  
5:43 AM 5:52 AM GMT-0600

action allowed deferred  
dest ACME-004  
signature EICAR-AV-Test HIPS/IPConnect-002  
[+1 more](#)

user PONDEROSA\aresco PONDEROSA\breznay  
[+2 more](#)

Details about the selected events

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Identity Investigator

Identity Investigator

Hax0r  Search

Search by identity name

Hax0r hax0r, htrapper@acmetech.com, htrapper

bunit: americas watchlist: true last: Trapper prefix: Mr.  
phone: +1 (800)555-3039 first: Hershel email: htrapper@acmetech.com phone2: +1 (800)555-3154  
endDate: 3/2/98 22:53 \_time: 2016-11-11T12:50:21-0800 priority: critical startDate: 6/15/93 20:07

**Edit**

All Authentication

All Changes

Threat List Activity

IDS Attacks

Malware Attacks

Notable Events

Risk Modifiers

Today ▾

12:00 AM 1:00 AM 2:00 AM 3:00 AM 4:00 AM 5:00 AM 6:00 AM 7:00 AM 8:00 AM 9:00 AM 10:00 AM 11:00 AM 12:00 PM

Search returned no results

Same tools and functionality as the Asset Investigator

Search returned no results

view: 12 hours an hour

00:00 00:00:00 12:50:19

All Authentication (25)

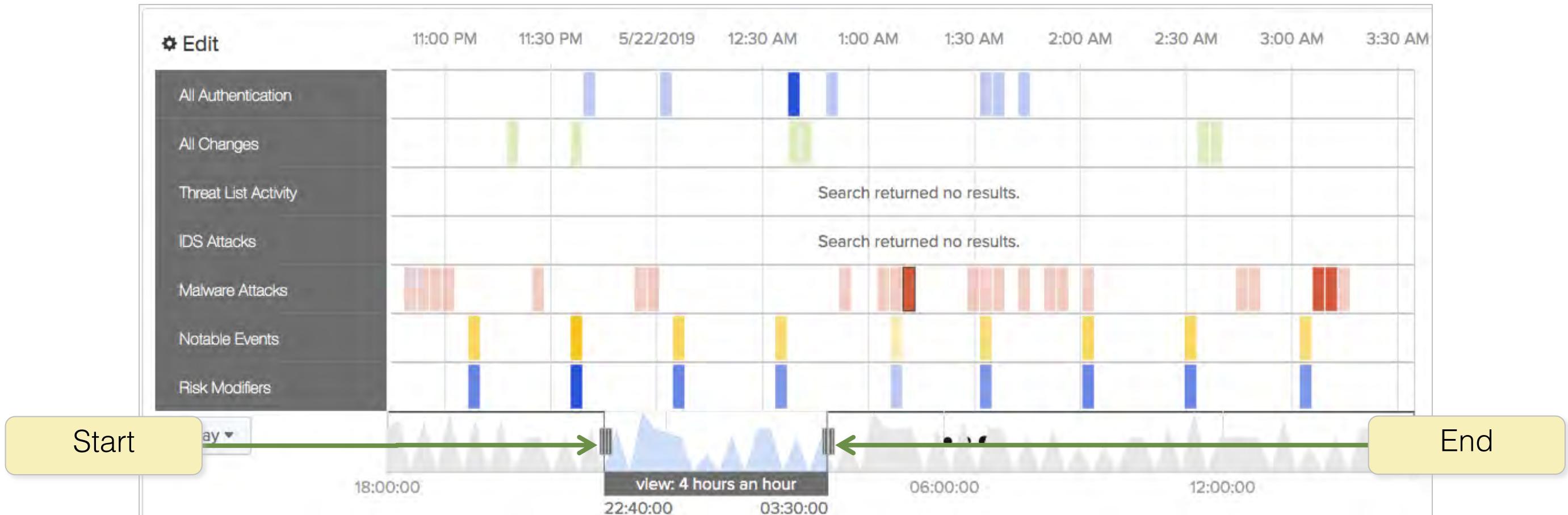
Fri Nov 11 Fri Nov 11  
05:36:18 05:50:19  
GMT-0800

action failure  
app win:local  
dest HOST-001  
src 10.11.36.20  
user Hax0r

The screenshot shows the Splunk Identity Investigator interface. At the top, there's a search bar with 'Hax0r' and a 'Search' button. A yellow callout box points to the search bar with the text 'Search by identity name'. Below the search bar, detailed user information for 'Hax0r' is displayed, including fields like bunit, phone, end date, watchlist status, first name, last name, email, priority, and start date. The main area features a timeline visualization with three horizontal tracks: blue bars for 'All Authentication', yellow bars for 'Notable Events', and blue bars for 'Risk Modifiers'. A tooltip 'Same tools and functionality as the Asset Investigator' points to the timeline area. On the left, a sidebar lists navigation options: All Authentication, All Changes, Threat List Activity, IDS Attacks, Malware Attacks, Notable Events, and Risk Modifiers. A 'Today ▾' dropdown is also present. To the right, a sidebar titled 'All Authentication (25)' shows event details for November 11, 2018, at 05:36:18 and 05:50:19, including action (failure), app (win:local), dest (HOST-001), src (10.11.36.20), and user (Hax0r). The bottom of the interface includes a footer with copyright information.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Pan and Zoom

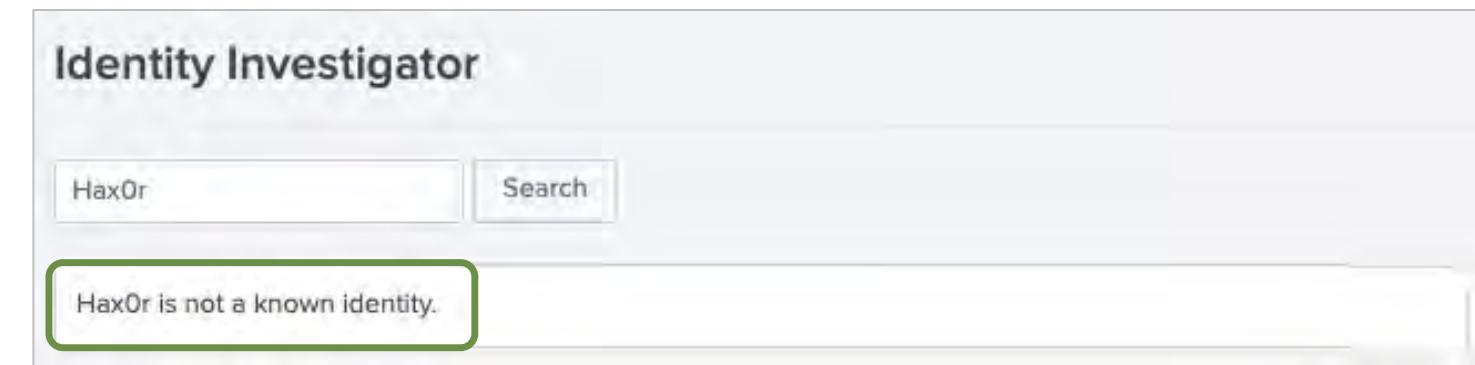


Dragging the pan/zoom controls changes the time frame for the search and re-executes the search, showing only the activity in the selected range

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Missing Information

- If an **Investigator** does not find the enhanced data for an asset/identity, you will see an error that the asset or identity is “unknown”
- Check that the asset or identity configuration is correct *and* enabled in the **Assets and Identity Management** interface



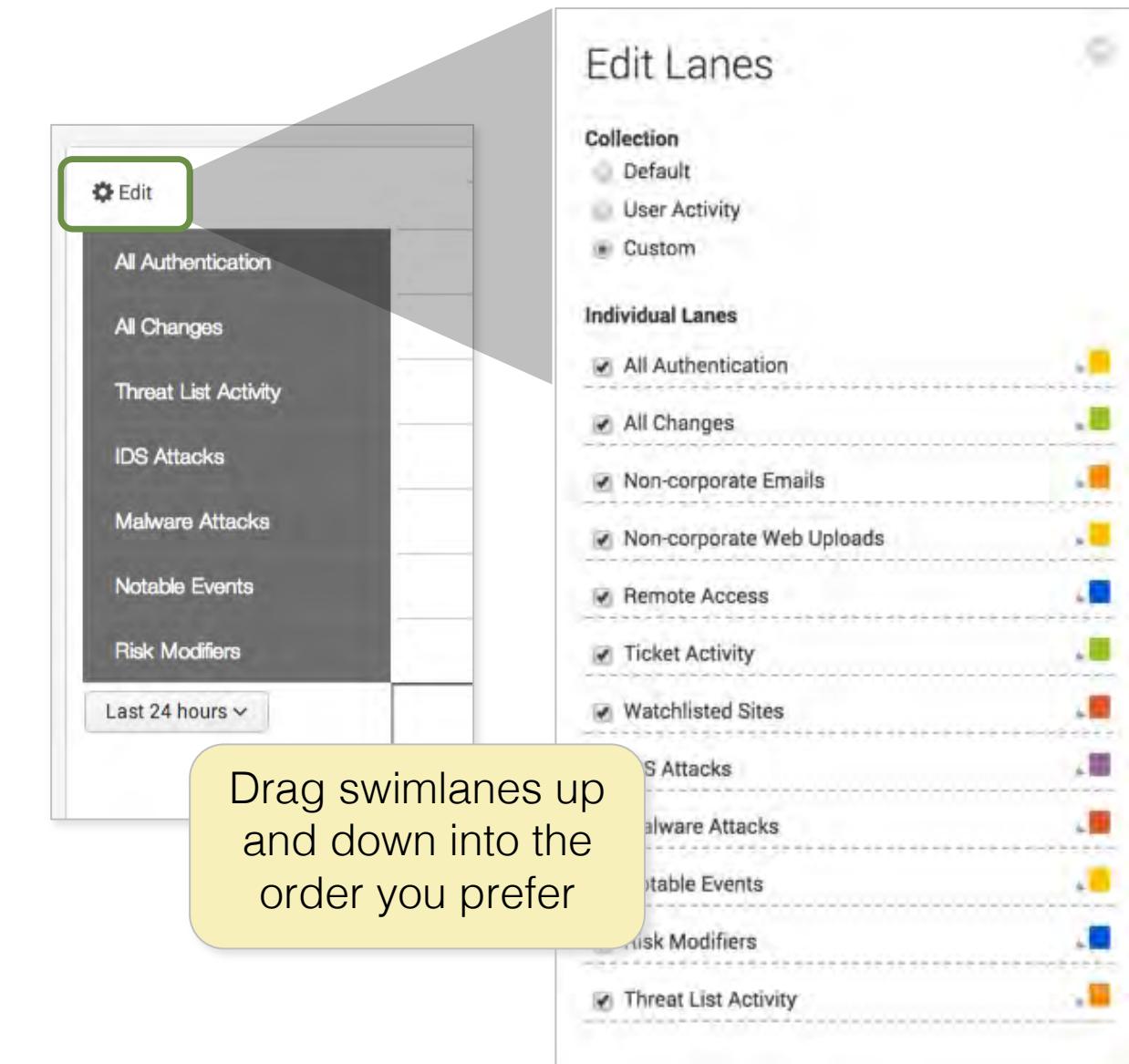
A screenshot of the Identity Investigator interface showing detailed asset information for "HaxOr". The search bar at the top contains "HaxOr". The results table includes the following fields:

Field	Value
email	htrapper@acmetech.com
_time	2021-12-01T23:26:29+0000
bunit	americas
first	hershel
identity_id	61a8049370d9b0187d6e3e61
last	trapper
prefix	mr.
priority	critical
work_city	san francisco
work_country	usa
endDate	Mon Mar 02 1998 15:53:00 GMT-0700 (Mountain Standard Time)
phone	+1 (800)555-3039, +1 (800)555-3154
watchlist	true
work_long	122.41w
work_lat	37.78n

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Configuring Swim Lanes

- Click Edit and select a collection of swim lanes
- Use the Custom collection to select specific swim lanes
- Customize swim lane colors
- ES Admins can add new swim lanes and set overall defaults and permissions per role
- Changes are not saved



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# User Intelligence > User Activity

**User Activity**

User Business Unit Watchlisted Users

Last 24 hours Submit Hide Filters

**Edit**

**TOTAL HIGH RISK USERS** Count **740** +740 **TOTAL HIGH RISK USER EVENTS** Count **36** +36 **NONCORP WEB VOLUME** Bytes **5.2b** +5.2b **NONCORP EMAIL VOLUME** Bytes **4.7b** +4.7b **WATCHLISTED WEBSITES** Access Count **0** 0

**Users By Risk Scores**

user	user_first	user_last	user_email	user_bunit	risk_score	watchlist	user	user_first	user_last	user_bunit	user_email	size	watchlist
3380361295858995909					57600	false	-					4702364229	false
-7633062664915826898					530	false	wohler	Wendell	Ohler	americas	wohler@acmetech.com	249156528	true
1611712837644153600					450	false	unknown					188569938	false
6309206957053858891					440	false	aseykoski	Allen	Seykoski	americas	aseykoski@acmetech.com	16659240	true
9031437491474763820					420	false	agasiewski	Anton	Gasiewski	americas	agasiewski@acmetech.com	3218568	false
-3052562275269326153					340	false	admin					1872696	false
					340	false	LDAP://user1					159122	false
					290	false	LDAP://user11					119586	false
					280	false	LDAP://user13					119121	false
					280	false	LDAP://user7					116396	false

Click a user to open the Identity Investigator

Risk assigned by various correlation searches on user activity

Sorted by risk

Non-corporate Web Uploads

user	user_first	user_last	user_email	user_bunit	risk_score	watchlist	user	user_first	user_last	user_bunit	user_email	size	watchlist
3380361295858995909					57600	false	-					4702364229	false
-7633062664915826898					530	false	wohler	Wendell	Ohler	americas	wohler@acmetech.com	249156528	true
1611712837644153600					450	false	unknown					188569938	false
6309206957053858891					440	false	aseykoski	Allen	Seykoski	americas	aseykoski@acmetech.com	16659240	true
9031437491474763820					420	false	agasiewski	Anton	Gasiewski	americas	agasiewski@acmetech.com	3218568	false
-3052562275269326153					340	false	admin					1872696	false
					340	false	LDAP://user1					159122	false
					290	false	LDAP://user11					119586	false
					280	false	LDAP://user13					119121	false
					280	false	LDAP://user7					116396	false

Sorted by size

Non-corporate Email Activity

src_user	src_user_first	src_user_last	src_user_bunit	src_user_email	size	watchlist
agasiewski@acmetech.com	Anton	Gasiewski	americas	agasiewski@acmetech.com	717378397	false
aseykoski@acmetech.com	Allen	Seykoski	americas	aseykoski@acmetech.com	485574119	true

Watchlisted Site Activity

src_user	src_user_first	src_user_last	src_user_bunit	src_user_email	size	watchlist
agasiewski@acmetech.com	Anton	Gasiewski	americas	agasiewski@acmetech.com	717378397	false
aseykoski@acmetech.com	Allen	Seykoski	americas	aseykoski@acmetech.com	485574119	true

Users accessing external sites that have been added to a watchlist

Connecting from remote locations

user	src	session_city	session_country	user_work_city	user_work_country
agasiewski@acmetech.com	Anton	Gasiewski	americas	agasiewski@acmetech.com	717378397
aseykoski@acmetech.com	Allen	Seykoski	americas	aseykoski@acmetech.com	485574119

Ticket Activity

Incident opened in an external tracking system

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

splunk® turn data into doing™

165

Using Splunk Enterprise Security

Copyright © 2022 Splunk, Inc. All rights reserved

25 May 2022

# Access User Activity from a Source Event

The screenshot shows a Splunk search interface and a User Activity dashboard. In the search results, a user field is selected. A callout with number 1 points to the Actions menu for the user field. In the User Activity dashboard, a user is selected, and a callout with number 3 points to the User Activity card, stating "User Activity dashboard only displays activity for the user selected". A callout with number 2 points to the User Activity link in the sidebar.

1 From a Splunk search result, click the Actions menu for the **user** field

2 User Activity

3 User Activity dashboard only displays activity for the user selected

**User Activity**

User: HaxOr

Business Unit:

Watchlisted Users:

Last 24 hours

Submit Hide Filters

**TOTAL HIGH RISK USERS**  
Count: 5 +5

**TOTAL HIGH RISK USER EVENTS**  
Count: 5 +5

**NONCORP WEB VOLUME**  
Bytes: 250.3m +250.3m

**NONCORP EMAIL VOLUME**  
Bytes: 48k +48k

**WATCHLISTED WEBSITES**  
Access Count: 0

**Users By Risk Scores**

user	user_first	user_last	user_email	user_bunit	risk_score	watchlist
HaxOr	Hershel	Trapper	htrapper@acmetech.com	americas	80	true
hax0r	Hershel	Trapper	htrapper@acmetech.com	americas	80	true

**Non-corporate Web Uploads**

user	user_first	user_last	user_email	user_bunit	risk_score	watchlist
HaxOr	Hershel	Trapper	htrapper@acmetech.com	americas	80	true
hax0r	Hershel	Trapper	htrapper@acmetech.com	americas	80	true

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc. not for distribution

# Access Anomalies Dashboard

## Security Intelligence > User Intelligence > Access Anomalies

View authentication attempts from different IP addresses and improbable travel anomalies using internal user credentials and location-relevant data

Important!



This search is disabled by default; enable it to use this dashboard.

**Access Anomalies**

App User Business Unit

All Last 60 minutes Submit Hide Filters

Geographically Improbable Accesses

user	user_bunit	src_time	src_app	src	src_city	src_country	dest_time	dest_app	dest	dest_city	dest_country	distance
reigh		1576053347	win:local	ACMEAPP	dallas	usa	1576053398	win:remote	BUSDEV-084	pleasanton	usa	1446.99
user11		1576059416	Authentication Manager	186.54.21.159	Maldonado	Uruguay	1576046770	Authentication Manager	7.10.140.125	istanbul	tr	7467.98

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

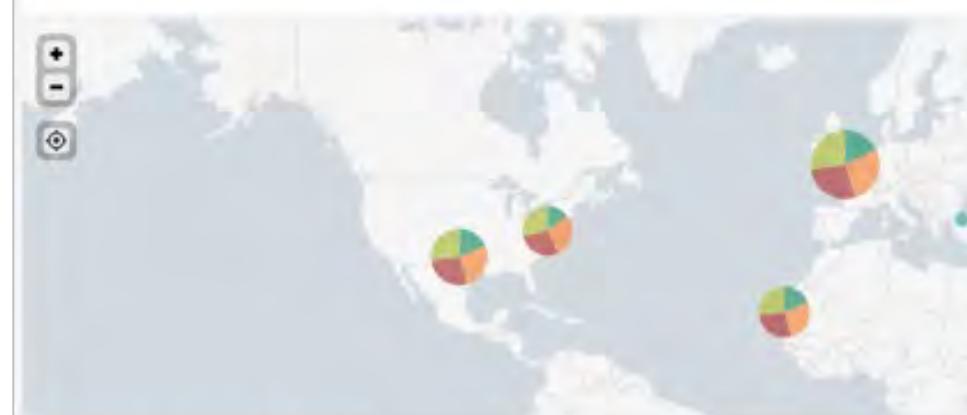
Concurrent Application Accesses

Action

All

user	app	src	_time	prev_src	prev_time	time_diff	count
test	sshd	10.11.36.30	2019-12-11 12:35:00	10.11.36.3	12/11/2019 12:35:00	0	1
admin2	sshd	10.11.36.4	2019-12-11 12:35:01	10.11.36.36	12/11/2019 12:35:01	0	1

This dashboard is dependent on the **gia\_summary** index, which is filled by the Access - Geographically Improbable Access - Summary Gen scheduled search hourly



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Module 7 Lab: User Intelligence

---

- Time: 30 minutes
- Scenario:
  - You are investigating potential internal threats
- Tasks:
  - Examine and learn more about the Hax0r user account
  - Investigate the server that Hax0r is attempting to access
  - Use the User Activity and Access Anomalies dashboards
  - Use the Access Anomalies and Access Search dashboards

# Module 8: Web Intelligence

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

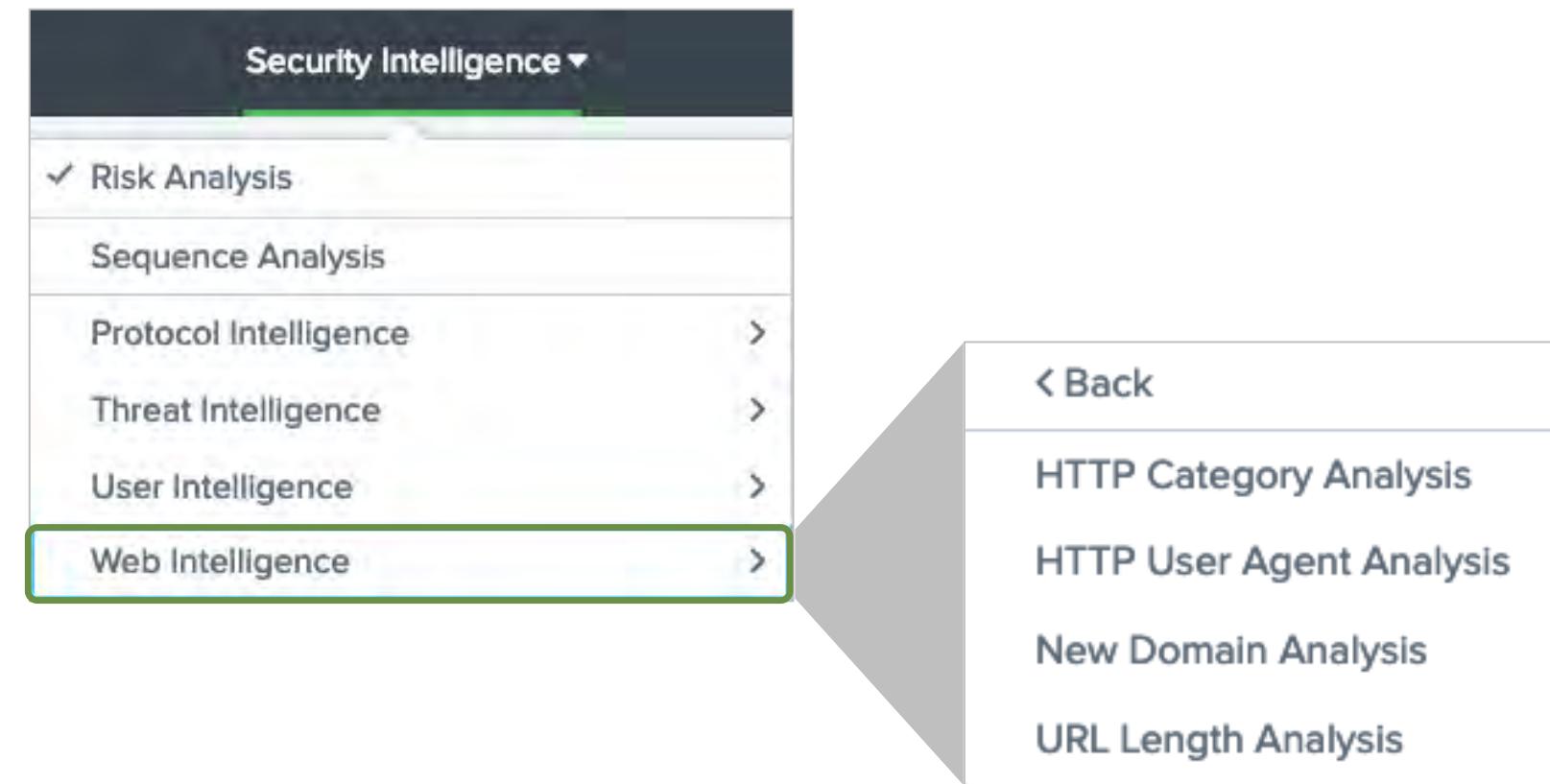
# Objectives

---

- Use the Web Intelligence dashboards to analyze your network environment
- Filter and highlight events

# Security Intelligence > Web Intelligence

Web Intelligence contains analytical dashboards that are useful for inspecting various aspects of your website network activity



HTTP Category	Explore the types of websites being accessed in the network
HTTP User Agent	Examine the web user agents being used on the network
New Domain	See what external domains are being accessed
URL Length	Examine request URLs for unusual contents

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Uses for Web Intelligence Dashboards

---

- Find URLs associated with unwanted activity
  - HTTP Category Analysis
- Identify malicious activity in the form of long or malformed user agent strings
  - HTTP User Agent Analysis
- Detect botnet or trojan attacks by high counts of new domains
  - New Domain Analysis
- Look for embedded SQL, cross-site scripting, etc.
  - URL Length Analysis

[docs.splunk.com/Documentation/ES/latest/User/ThreatListActivitydashboard](https://docs.splunk.com/Documentation/ES/latest/User/ThreatListActivitydashboard)

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# HTTP Category Analysis

Enterprise Security

HTTP Category Analysis Gives an overview of websites used by category

Show only unknown categories

False Last 60 minutes Submit Hide Filters

Edit Export ...

MINIMUM COUNT Count 24 +24

MEAN COUNT Count 158.8 +158.8

MAXIMUM COUNT Count 2.5k +2.5k

STDEV COUNT Count 348.9 +348.9

UNIQUE CATEGORIES Unique Count 82 +82

Category Distribution

dc(src) count

Per-panel Filter

Category Details

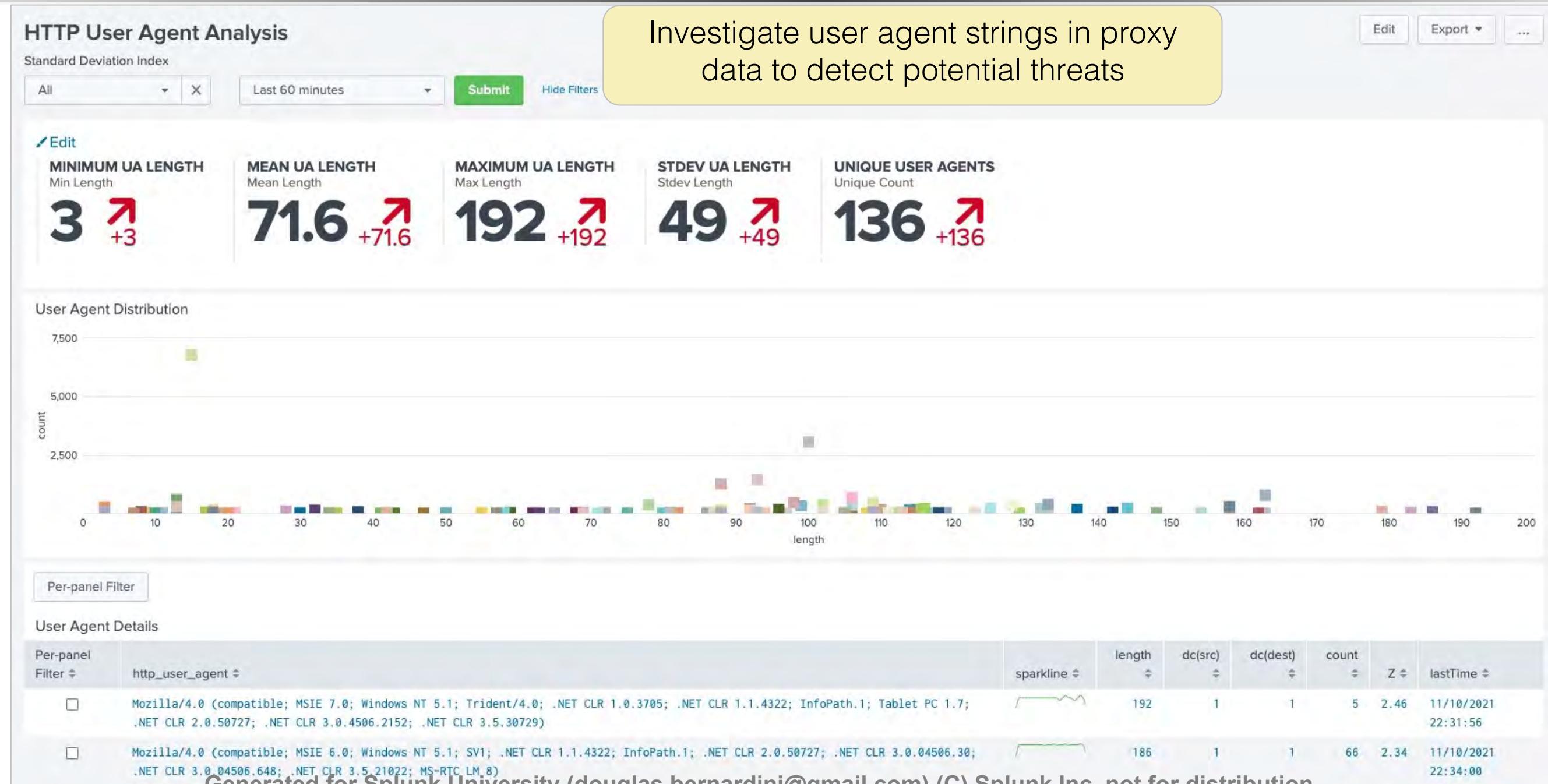
Per-panel Filter	category	sparkline	dc(src)	dc(dest)	count	Z	lastTime
<input type="checkbox"/>	Health		1	1	1	-0.40	11/10/2021 21:50:51
<input type="checkbox"/>	Instant Messaging		1	1	1	-0.40	11/10/2021 21:50:51
<input type="checkbox"/>	Military		1	1	1	-0.40	11/10/2021 21:50:51
<input type="checkbox"/>	Abused Drugs		1	1	2	-0.34	11/10/2021 21:50:51
<input type="checkbox"/>	Cultural Institutions		1	1	2	-0.34	11/10/2021 21:50:51
<input type="checkbox"/>	Entertainment		1	1	2	-0.34	11/10/2021 21:50:51

<http://www.websense.com/content/support/library/web/v85/siem/siem.pdf>

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

1 2 3 4 5 6 7 Next »

# HTTP User Agent Analysis

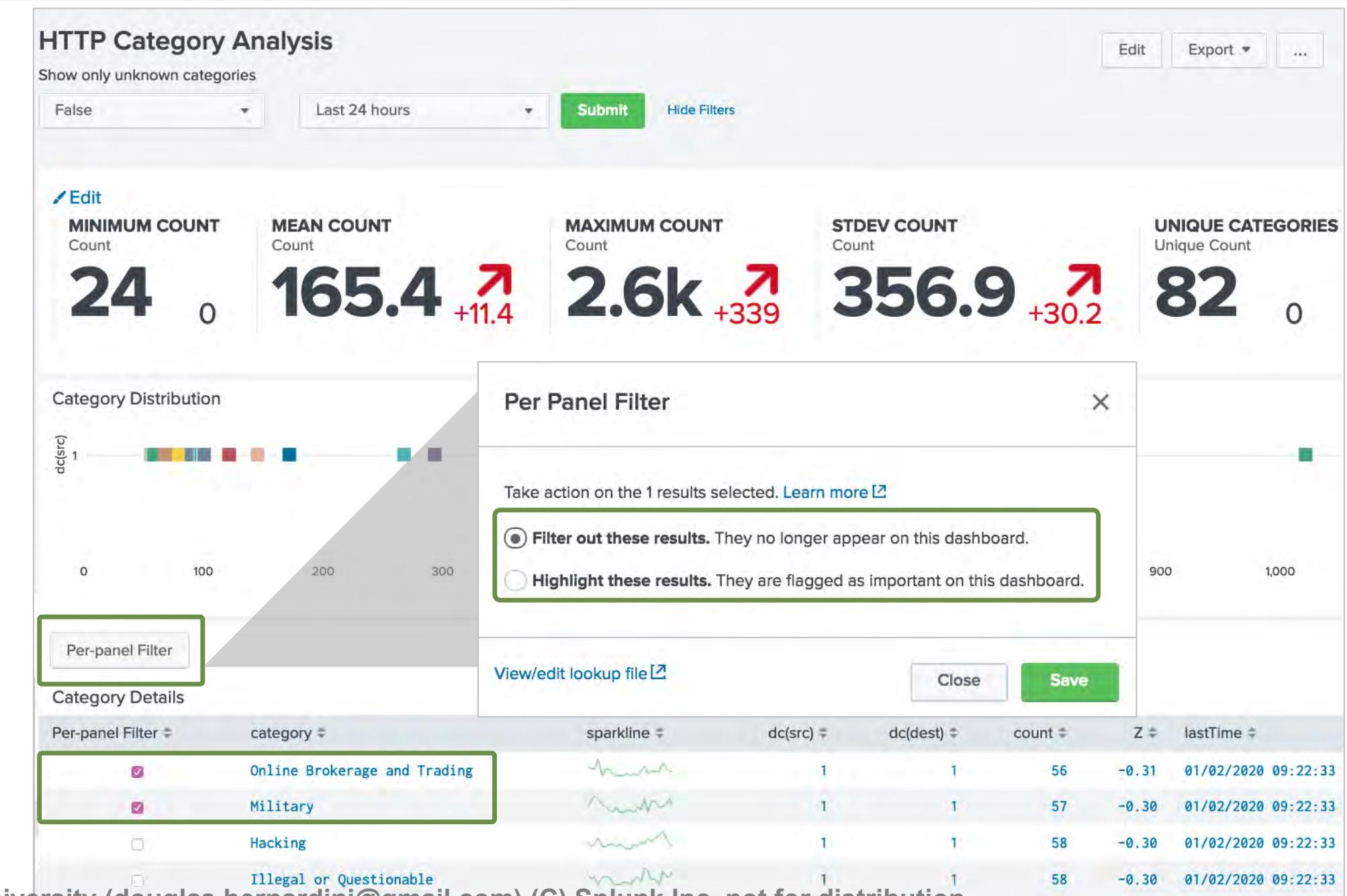


# Per Panel Filter

- Some ES dashboard views have a Per-Panel Filter button which is used to highlight or filter items out of the dashboard search
- Unavailable by default for ES Analysts but can be enabled by an ES Admin

**Note**

In the lab environment for this course, the **Edit Per Panel Filters** permission has been enabled for ES analysts



# Filtered vs. Highlighted Events

- Filtered events are no longer displayed
- Highlighted events are:
  - Highlighted in the Per-panel Filter column
  - Displayed at the top of the list by default

Category Details							
Per-panel Filter	category	sparkline	dc(src)	dc(dest)	count	Z	lastTime
<input checked="" type="checkbox"/>	Online Brokerage and Trading		1	1	56	-0.31	01/02/2020 09:22:33
<input checked="" type="checkbox"/>	Military		1	1	57	-0.30	01/02/2020 09:22:33
<input type="checkbox"/>	Hacking		1	1	58	-0.30	01/02/2020 09:22:33
<input type="checkbox"/>	Illegal or Questionable		1	1	58	-0.30	01/02/2020 09:22:33
<input type="checkbox"/>	Traditional Religions		1	1	59	-0.30	01/02/2020 09:22:33
<input type="checkbox"/>	Information Technology		1	1	60	-0.30	01/02/2020 09:22:33

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Managing Per Panel Filtering Lookups

The screenshot illustrates the steps for managing per-panel filtering lookups:

1. In the main interface, the "Per-panel Filter" button is highlighted.
2. A modal window titled "No Results Selected" shows the message "Select one or more rows to apply a filter". The "View/edit lookup file" link is highlighted.
3. A callout bubble provides instructions: "To remove a highlighted or filtered field, right-click on the row and click Remove rows. In the example, the category 'unknown' has been filtered out and is shaded in blue in the lookup".
4. The "Edit Lookup File / ppf\_http\_category.csv" window shows a table with several rows. A context menu is open over the last row, with the "Remove rows" option highlighted.

1	start_time	end_time	category	filter	creator	create_time
2	1578608048		117	whitelist	admin	1578608048
3	1578608048		9	whitelist		1578608048
4	1578608048		68	whitelist		1578608048
			121	whitelist		1578608048
			146	whitelist		1578608048
			76	whitelist		1578608048
			17	whitelist		1578608061
			113	whitelist		1578608061
			4	whitelist		1578608061
			Military	blacklist		1639776464
			Online Brokerage and Trading	blacklist	admin	1639776464
			unknown	whitelist	admin	1639776659

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

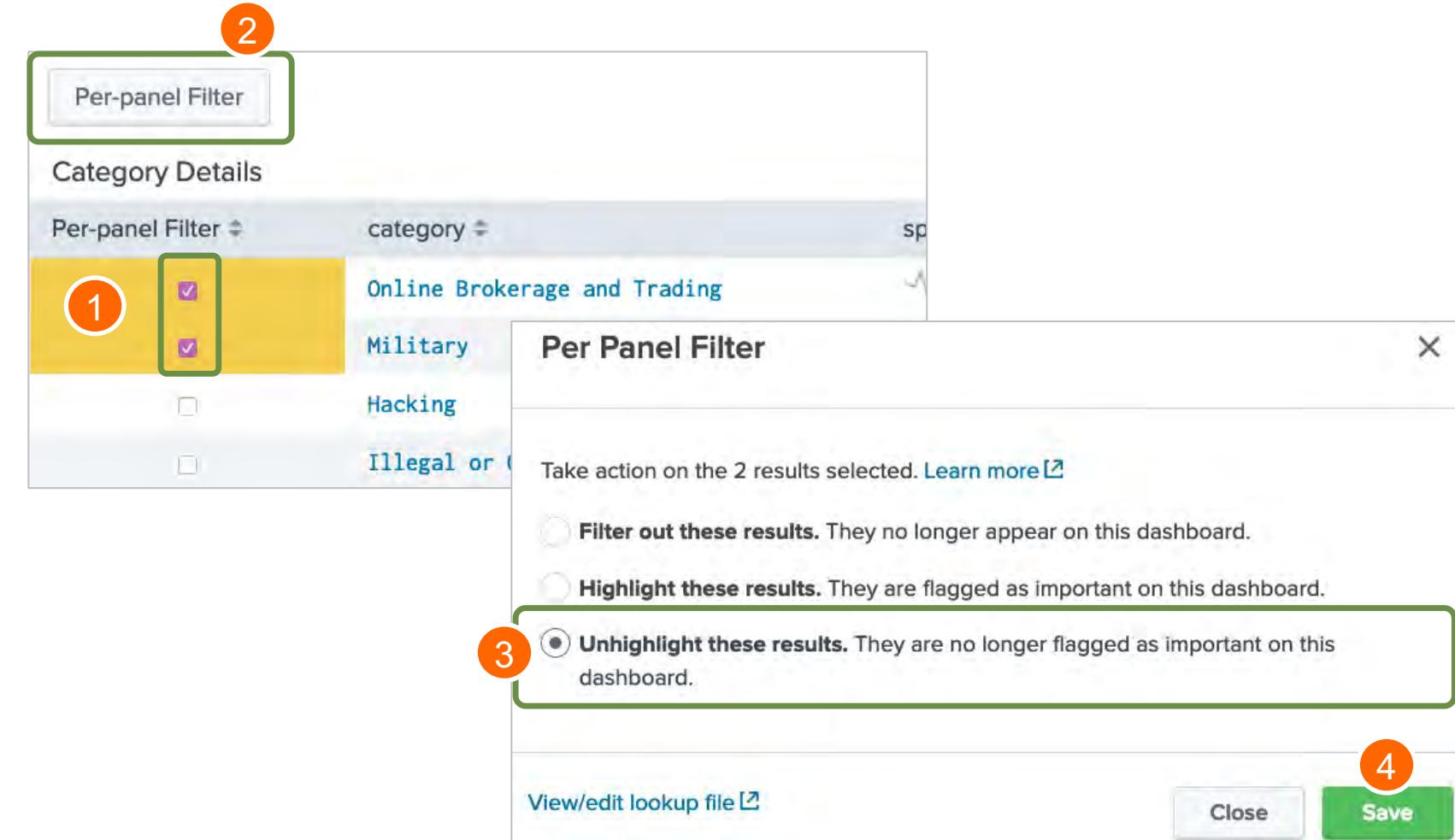
# Unhighlighting an Event

If an event is already highlighted

1. Select it
2. Click Per-panel Filter
3. Remove the highlight or change to filtering
4. Click Save

**Note** 

Events can only be "unfiltered" directly from the lookup by removing the corresponding row. (Filtered events are not visible from the UI).



# Module 8 Lab: Web Intelligence

---

- Time: 25 minutes
- Scenario:
  - You are using the HTTP User Agent dashboard and notice some unusual activity
- Tasks:
  - Perform HTTP User Agent analysis
  - Use a per-panel filter
  - Use the HTTP Category Analysis dashboard

# Module 9: Threat Intelligence

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

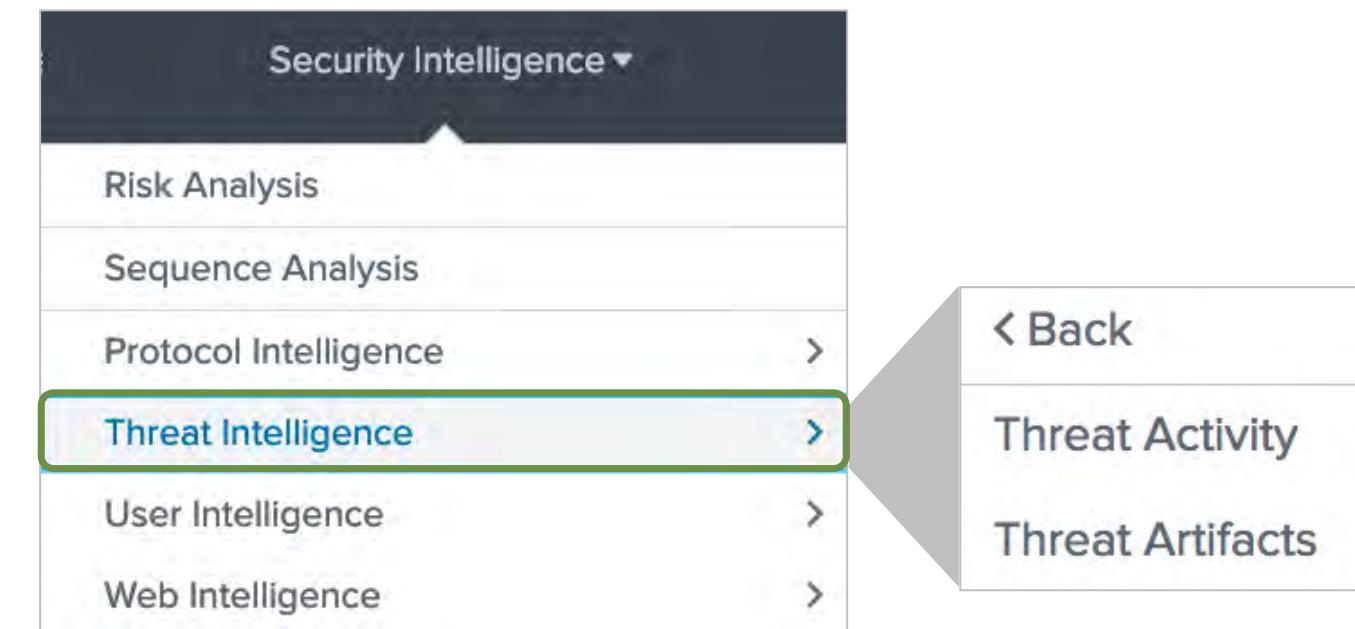
# Objectives

---

- Give an overview of the Threat Intelligence framework and how threat intel is configured in ES
- Use the Threat Activity dashboard to see which threat sources are interacting with your environment
- Use the Threat Artifacts dashboard to examine the status of threat intelligence information in your environment

# Security Intelligence > Threat Intelligence

Threat Intelligence provides tools to help security practitioners find and prevent potential external threats in your environment



Threat Activity	Examine activity from a threat perspective: <ul style="list-style-type: none"><li>• which threats have been identified</li><li>• which systems or users are affected</li></ul>
Threat Artifacts	Examine the details of threat intel that has been downloaded from online threat libraries, or have been added locally

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Threat Intelligence Framework

---

- Threat intel is downloaded regularly from external and internal sources by the **Threat Download Manager** modular input
  - Data is parsed into KV store collections with “`_intel`” suffixes
  - Collections are used as lookups during threat generation searches
- **Threat Gen** searches run by default every 5 minutes and scan for threat activity related to any of the threat collections
  - When threat matches are found, events are generated in the `threat_activity` index and appear in the **Threat Intelligence** data model
- The data model is scanned by the **Threat Activity Detected** correlation search and new notables for threat activity are created

# Threat Intelligence Administration

---

- ES Admins are tasked with managing ES threat intelligence
- Analysts and users can be given the **Edit Intelligence Downloads** permission to manage threat intelligence downloads
- Threat Intelligence can be added to ES by
  - downloading a feed from the Internet
  - uploading a structured file
  - inserting threat intelligence directly from events in ES
  - as an “Add Threat Intelligence” adaptive response action in a correlation search

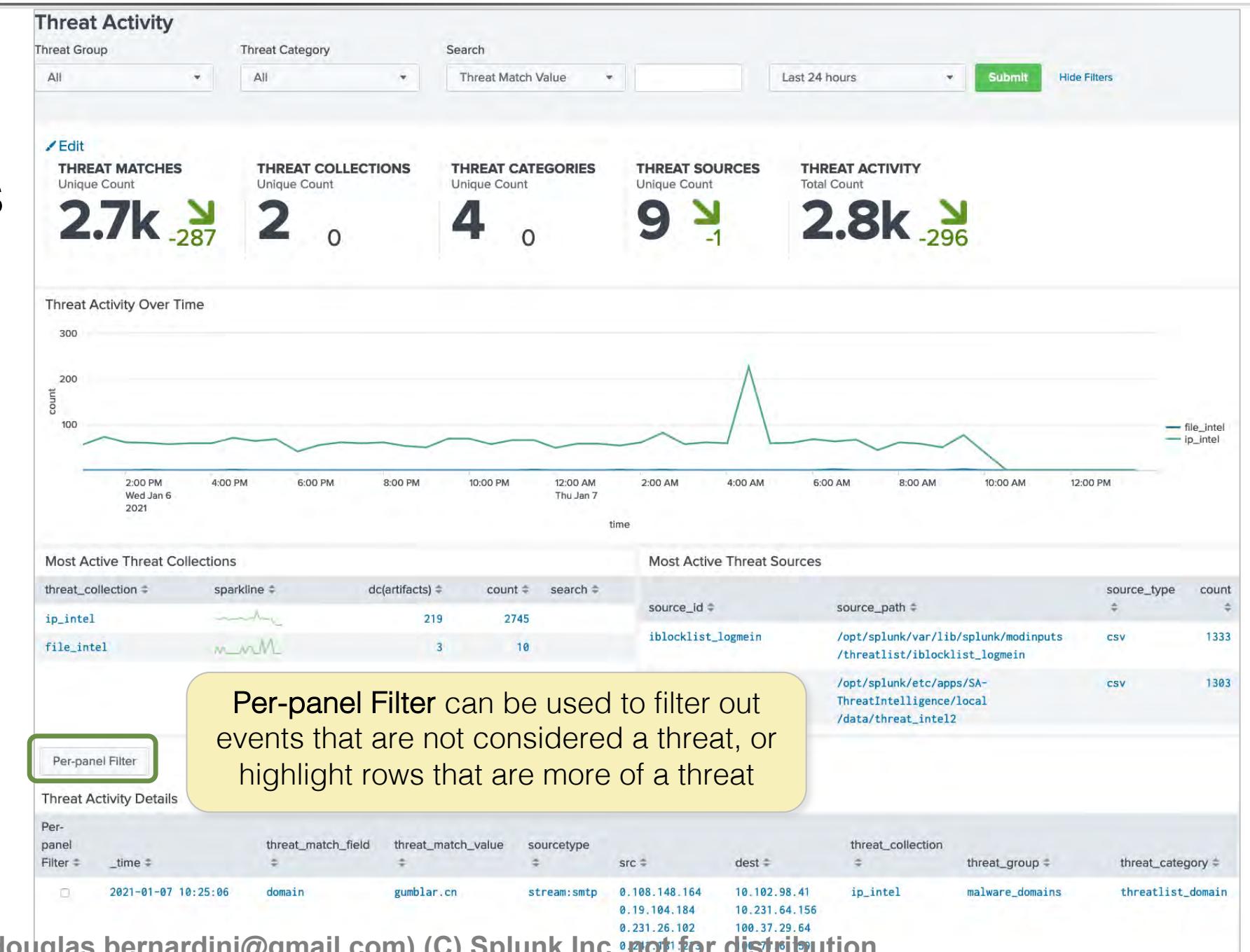
# Threat Intelligence Configuration

---

- Threat Intel is configured in the **Threat Intelligence Management** interface  
Configure > Data Enrichment > Threat Intelligence Management
- ES can download the following types of threat intelligence
  - Threat lists: IP addresses of known malicious sites
  - STIX/TAXII: details about known threats, including threat type and source
  - OpenIOC: additional information about known threats
- Many intel sources require regular refresh from external sources
- This information is used by the **Threat Activity Detected** correlation search

# Threat Activity

- The Threat Activity dashboard displays events related to known threat sites over the desired time
- Details include:
  - Threat activity over the last 24 hours and which collection it is from (file\_intel, ip\_intel, etc.)
  - Which sources (download name/URL) are most active
  - The details of the threat



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Using the Threat Activity Dashboard

## Filter the Threat Activity dashboard

The screenshot shows the Threat Activity dashboard interface. On the left, there's a sidebar with a dropdown for 'Threat Group' set to 'All' and a search bar with 'filter' and a magnifying glass icon. Below these are several threat source entries: 'iblocklist\_logmein', 'iblocklist\_piratebay', 'iblocklist\_proxy', 'iblocklist\_rapidshare', 'iblocklist\_spyware', 'iblocklist\_tor', 'iblocklist\_web\_attacker', 'malware\_domains', and 'sans'. A yellow callout box points to the 'iblocklist' entries with the text: 'Threat source: download feed or local file name'. In the center, there's a dropdown for 'Threat Category' with 'All' selected, and a list of categories: 'All', 'threatlist', 'threatlist\_domain'. A yellow callout box points to the 'threatlist' category with the text: 'Threat category, such as advanced persistent threat (APT), financial threat, backdoor, etc.'. On the right, there's a 'Search' section with a dropdown set to 'Source' and the value '10.0.0.100'. A yellow callout box points to this section with the text: 'Choose a field from the Search drop-down and enter a value for the search'. The background of the dashboard shows some blurred data tables.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Threat Artifacts

Filter to select a threat artifact type or filter by fields relevant to the selected artifact type

Threat Artifacts

Threat Artifact Threat Category Threat Group Malware Alias Intel Source ID Intel Source Path

Threat ID All All [ ] [ ] [ ]

Submit Hide Filters

Threat Overview

source_id	source_path	source_type	threat_group
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	+ F (and 6 more)
hijacked_ip_addresses	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/1.0.0.1/data/threat_intel/hijacked_ip_addresses	csv	hijacked_ip_addresses
iblocklist_logmein	/opt/	csv	iblocklist_logmein
iblocklist_piratebay	/opt/	csv	iblocklist_piratebay
iblocklist_proxy	/opt/splunk/var/lib/splunk/modinputs/threatlist/iblocklist_proxy	csv	iblocklist_proxy

Threat Overview displays the items that have been downloaded from threat lists or STIX/TAXII sources

Endpoint Artifacts Network Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count	threat_collection	source_type	ip_count	domain_count	url_count	http_count	total
file_intel	stix	undefined	undefined		1356	ip_intel	csv	5801				5801
file_intel	stix	F	APT		194	ip_intel	csv	760				760
file_intel	stix	admin338	APT		194	ip_intel	csv	604				604
file_intel	stix	japanorus	APT		194	ip_intel	stix	164				309

Each category has an “artifact” panel (i.e., Endpoint, Network, Email Certificate) that displays details for the threat collection

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Using the Threat Artifacts Dashboard

---

- Get more information about an active threat with the Threat Artifacts dashboard
- Example: On the Threat Activity dashboard **Most Active Threat Sources** panel, you see that **iblocklist\_proxy** is one of the most common threat sources
  - In Threat Artifacts, you enter **iblocklist\_proxy** in the Intel Source ID field and search
  - You learn that **iblocklist\_proxy** is a CSV type threat list
  - Use the **Network** tab to inspect the full list of known IP addresses from this threat list, including locations when known

# Add Threat Intelligence from a Search

---

- Admins can insert threat intel directly from a Splunk event
  - Write a search that produces threat indicators, add the following to the end of the search:  
| outputlookup local\_<threat intelligence type>\_intel append=t
  - Types of <threat intelligence type> include **ip**, **email**, or **certificate**
- For example: write a search that produces a list of IP addresses that are testing a web server for vulnerabilities and add them to the **local\_ip\_intel** lookup to be processed by the modular input and added to the **ip\_intel** KV Store collection

# Module 9 Lab: Threat Intelligence

---

- Time: 20 minutes
- Scenario:
  - You are investigating potential external threats
- Tasks:
  1. Review threat activity
  2. Add a local IP address to the **ip\_intel** KV Store

# Module 10: Protocol Intelligence

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Objectives

---

- Explain how network data is input into Splunk events
- Describe stream events
- Give an overview of the **Protocol Intelligence** dashboards and how they can be used to analyze network data

# Security Intelligence > Protocol Intelligence

Protocol Intelligence is ES's set of tools for analyzing network traffic

The screenshot shows a navigation menu titled 'Security Intelligence'. The 'Protocol Intelligence' option is highlighted with a blue selection bar. To the right of the main menu is a sidebar with various analysis tools:

- < Back
- Protocol Center
- Traffic Size Analysis
- DNS Activity
- DNS Search
- SSL Activity
- SSL Search
- Email Activity
- Email Search

Protocol Center	An overview dashboard showing protocol activity across the network
Traffic Size Analysis	An analytical dashboard showing network traffic rates and trends
DNS	Dashboards showing an overview of activity of DNS queries <b>and</b> a search interface
SSL	Dashboards for analyzing SSL certificate activity
Email	Dashboards for analyzing email activity

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

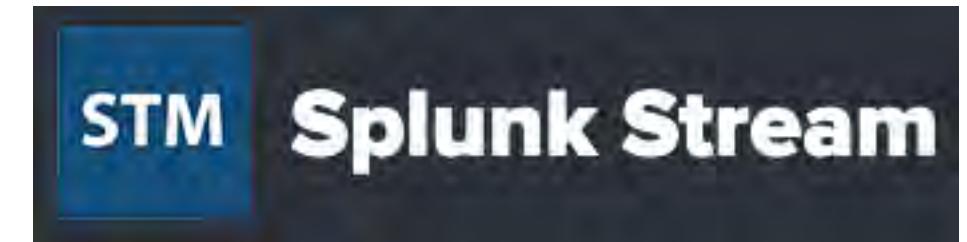
# Getting Data In

---

- Capture network traffic using the Splunk Stream app or by normalizing network log data (DNS, SSL, SMTP, HTTP)
- Uses Cases:
  - Monitor suspicious network traffic
  - Correlate logged vs. actual activity
  - Gain direct access to network traffic for SSL, HTTP, DNS, and SMTP
  - Configure correlation searches that can monitor network traffic

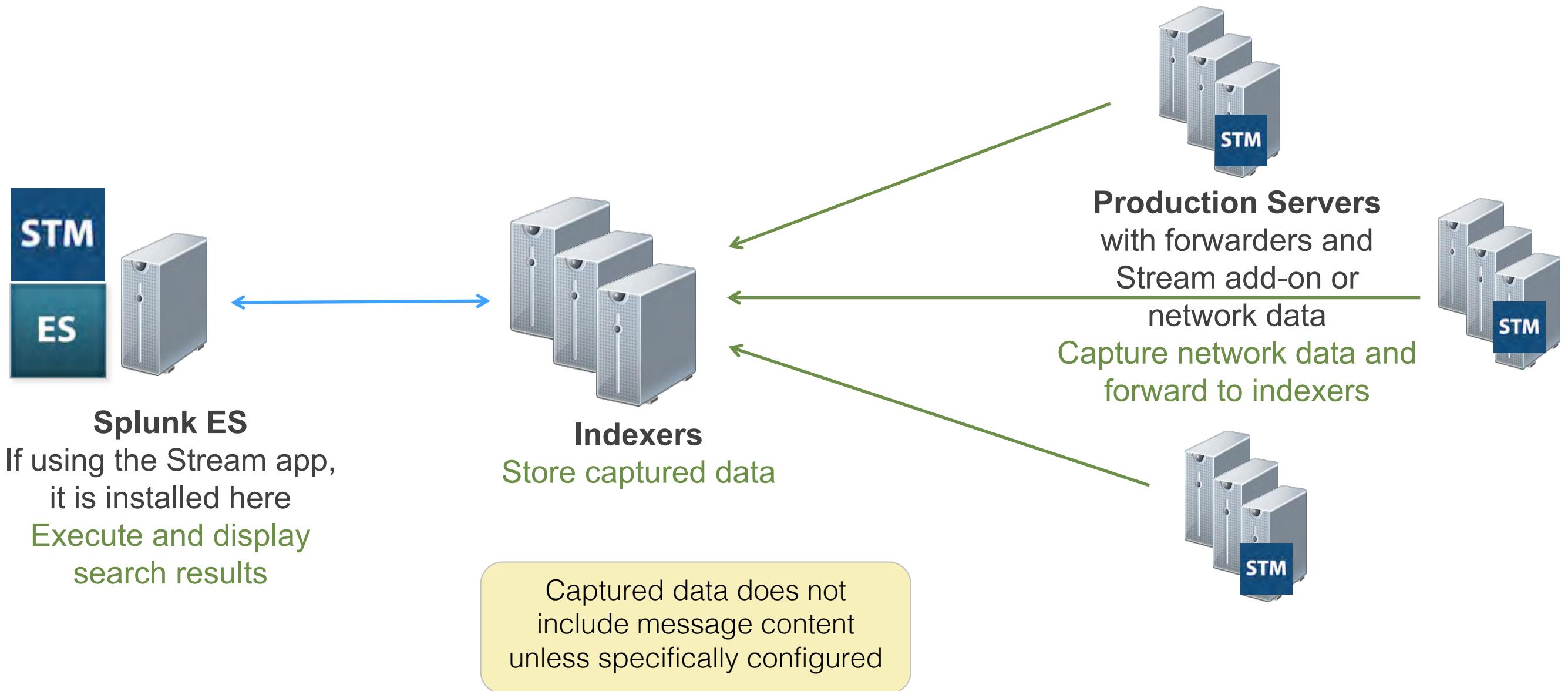
# Splunk Stream

- Traffic can be captured using the Splunk Stream add-on  
[docs.splunk.com/Documentation/StreamApp](https://docs.splunk.com/Documentation/StreamApp)
- Deployed on forwarders and listens to traffic
- Traffic data is forwarded to indexers and made available to ES
- Additional captures can be set up within ES



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

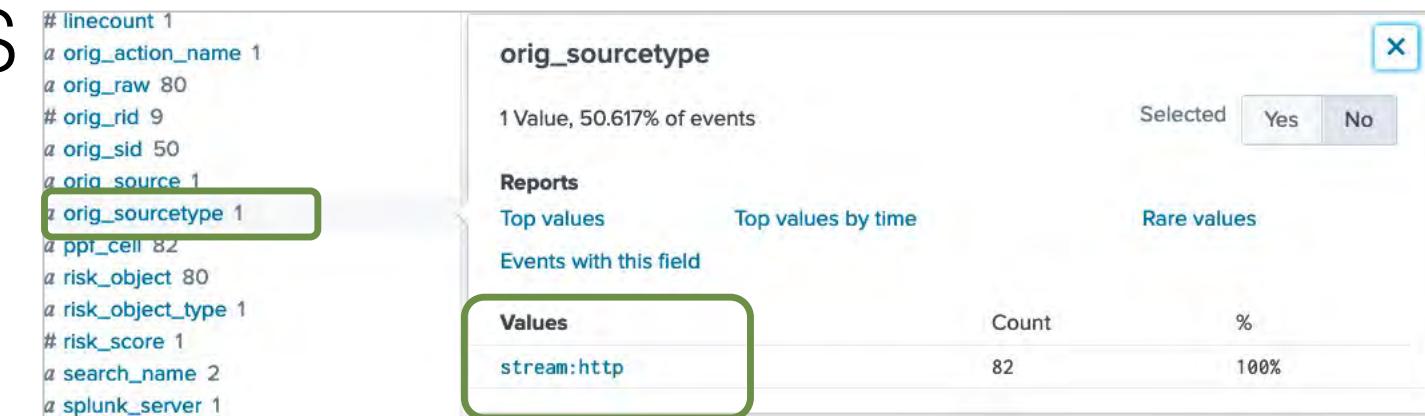
# Stream Data Flow



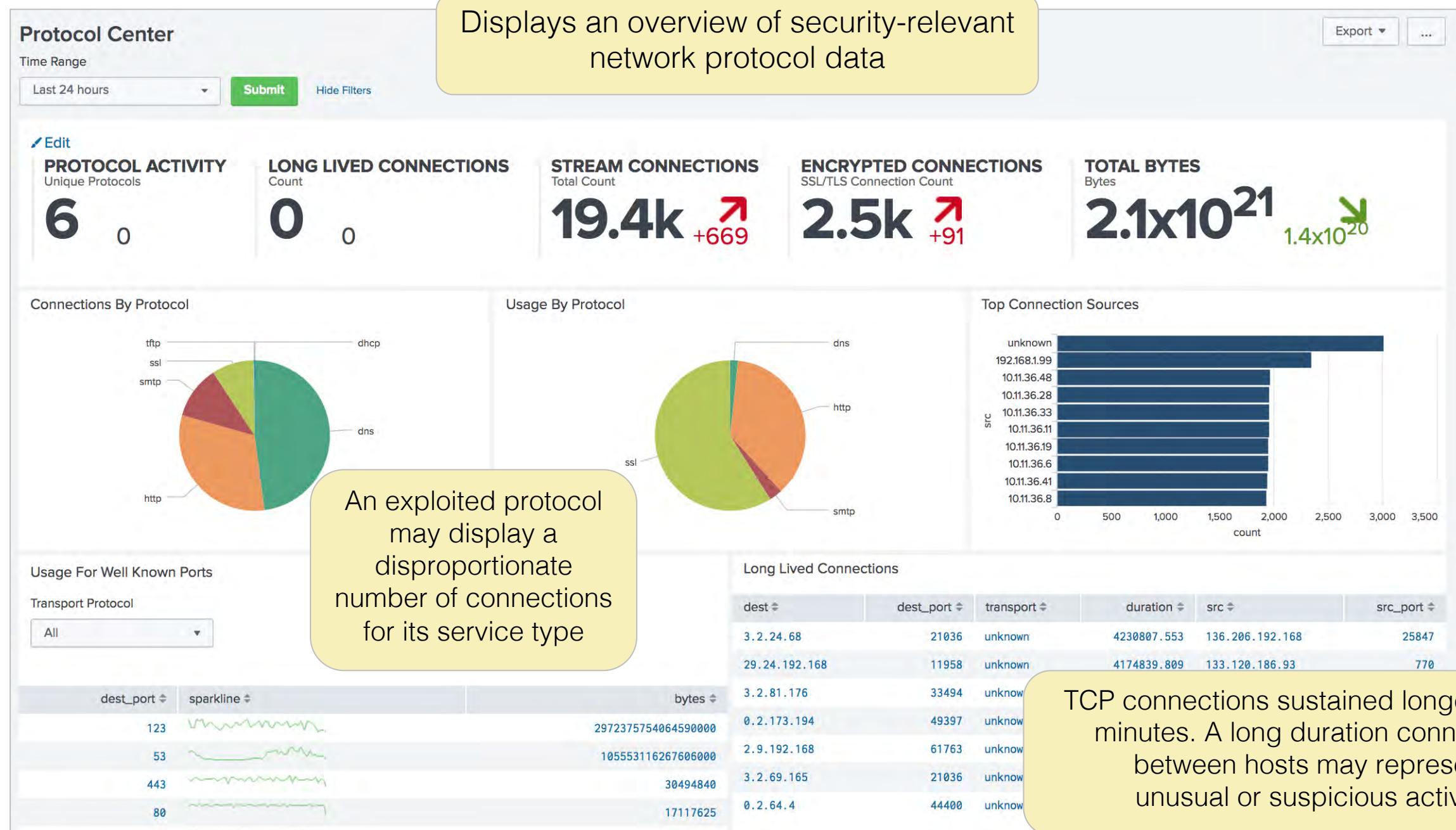
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Stream Events

- Stream events are generated from the Splunk Stream app, or other streaming apps like Zeek (Bro) IDS
- Splunk Stream events in the **notable** index are stored with the **orig\_sourcetype** field as **stream:xxxx** (**stream:tcp**, **stream:http** etc.)
- Standard fields are extracted, as well as additional fields for the specific source type
  - HTTP: cookies, request parameters, etc.
  - SMTP: sender, receiver, subject, summary of body
  - DNS: DNS query, query type, DNS host, etc.



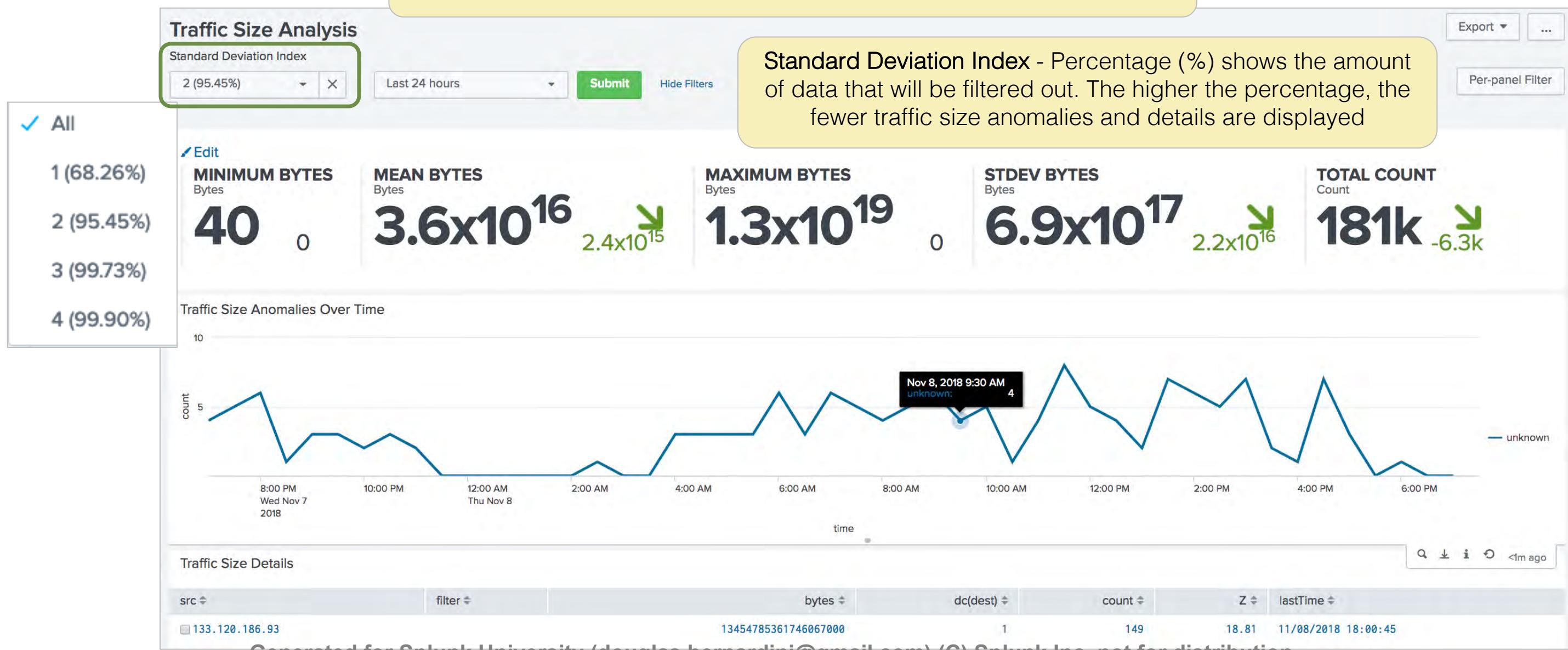
# Protocol Intelligence > Protocol Center



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Protocol Intelligence > Traffic Size Analysis

Compare traffic data with statistical data to find outliers. Displays traffic data from firewalls, routers, switches, or network flows



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Protocol Intelligence > DNS Activity

Displays an overview of data relevant to the DNS infrastructure being monitored

For example, a host initiating a large number of DNS queries to unknown or unavailable domains will report a large number of DNS lookup failures with some successes. That pattern of DNS queries may represent an exfiltration attempt or suspicious activity

The screenshot shows the Splunk DNS Activity dashboard with the following data points:

- TOTAL DNS MESSAGES Count:** 6.2k +6.2k
- TOTAL DNS ERRORS Count:** 5.1k +5.1k
- UNIQUE QUERIES Count:** 29 +29
- UNIQUE SOURCES Count:** 2.3k +2.3k

**Top Reply Codes By Unique Sources:** Bar chart showing the count of unique sources for different reply codes. The data is as follows:

reply_code	Count
No Error	~1,200
unknown	~100

**Top DNS Query Sources:** Table showing the top DNS query sources with their counts. The data is as follows:

src	sparkline	count
1.2.3.4	/	34
0.103.35.225	/	1
0.127.46.176	/	1
0.133.186.6	/	1
0.14.70.214	/	1
0.146.65.33	/	1
0.158.120.87	/	1
0.249.140.239	/	1
0.25.99.67	/	1
1.212.3.97	/	1

**Top DNS Queries:** Table showing the top DNS queries with their counts. The data is as follows:

query	count
Confidential.exfil.ru	83
Doc.exfil.ru	83
Is.exfil.ru	83

**Queries Per Domain:** Table showing the queries per domain with their counts. The data is as follows:

domain	count	query_count	queries
exfil.ru	332	4	Confidential.exfil.ru Doc.exfil.ru Is.exfil.ru This.exfil.ru
olddomaine.com	93	1	www.olddomaine.com

**Recent DNS Queries:** Table showing recent DNS queries with their details. The data is as follows:

_time	name	record_type	query_type	query	answer	City	Country	Region
2018-05-22 00:42:56	vega.vulcan.com		Host address	vega.vulcan.com	unknown			
2018-05-22 00:42:50	www.ieee.com		Host address	www.ieee.com	unknown			

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Protocol Intelligence > SSL Activity

**SSL Activity**

Time Range  
Last 24 hours  Hide Filters

Edit

**CLOUD SESSIONS**  
Session Count  
**989** +66

**SHORT VALIDITY CERTS**  
Session Count  
**1.5k** +34

**EXPIRED CERTS**  
Session Count  
**2.2k** +52

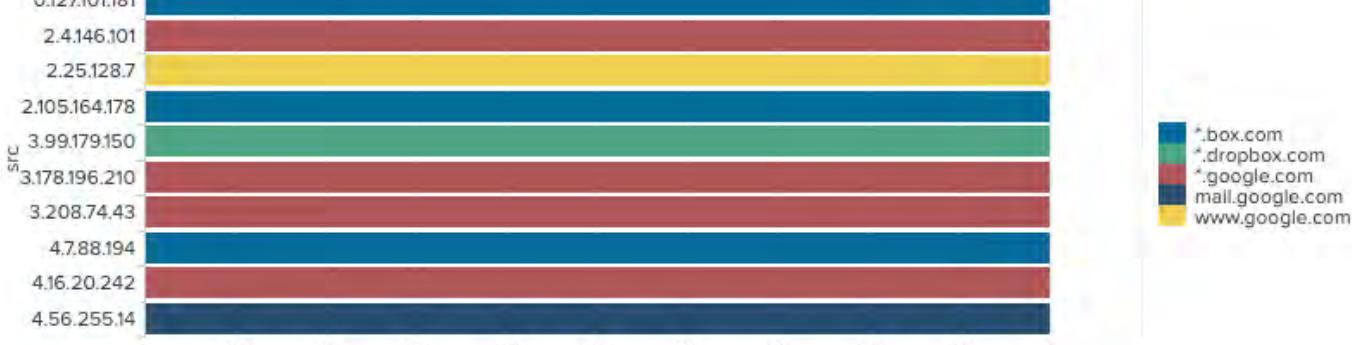
**TOTAL SSL SESSIONS**  
Session Count  
**2.2k** +52

Provides an overview of the traffic and connections that use SSL. Analysts can use these dashboards to view and review SSL encrypted traffic by usage, without decrypting the payload

**SSL Activity By Common Name**



**SSL Cloud Sessions**



src #	dest #	ssl_subject_common_name	ssl_subject_email	ssl_issuer_common_name	ssl_issuer_organization	ssl_start_time	ssl_end_time	ssl_validity_window	ssl_is_valid
15.18.57.221	141.244.85.158	www.google.com		VeriSign Class 3 Public Primary Certification Authority - G5	"VeriSign, Inc."	04/10/2014 21:21:59	Jun 10 21:21:59 2014 UTC (expired)	5270400.000000	0
62.143.58.71	126.107.74.223	*.box.com		RapidSSL CA	"GeoTrust, Inc."	04/10/2014 21:21:59	Jun 10 21:21:59 2014 UTC (expired)	5270400.000000	0

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Protocol Intelligence > Email Activity

Email Activity

Email Protocol: All | Last 24 hours | Submit | Hide Filters | Export | ...

**Edit**

**UNIQUE SENDERS**  
Sender Count  
**10**  +10

**UNIQUE RECEIVERS**  
Receiver Count  
**11**  +11

**CLOUD ACTIVITY**  
Email Count  
**391**  +391

Provides an overview of the data relevant to the email infrastructure being monitored. Data can be used to find suspect emails including, top email sources, large emails, and rare senders or receivers

Top Email Sources		Large Emails						
src	sparkline	count	protocol	src	src_user	dest	count	avg_size
10.11.36.27		73	smtp	0.171.177.26	aloha_care@ymail.com	203.113.7.231	1	364
10.11.36.45		73	smtp	0.50.90.163	atria@c1z.at	173.208.76.190	1	364
10.11.36.7		73	smtp	1.13.225.212	aloha_care@ymail.com	79.79.211.225	1	364
10.11.36.20		72	smtp	1.2.3.4	evilsender@update.defenceonline.net	4.5.6.7	35	364
10.11.36.11		71	smtp	1.2.3.4	iamnot@home.com	4.5.6.7	35	364
1.2.3.4		70	smtp	100.17.180.62	aloha_care@ymail.com	190.82.24.45	1	364
10.11.36.15		69	smtp	100.212.131.36	aloha_care@ymail.com	162.113.160.25	1	364
10.11.36.2		69	smtp	101.114.117.26	atria@c1z.at	103.234.59.148	1	364
10.11.36.8		68	smtp	101.146.141.165	atria@c1z.at	114.120.15.104	1	364
10.11.36.9		68	smtp	101.154.249.204	kel_yupptv@media.com	48.203.129.101	1	364

Rarely Seen Senders

src_user	protocol	src_count	recipient_count	count	recipient	protocol	src_count	src_user_count	count
evilsender@update.defenceonline.net	smtp	1	1	35	bruce_leemachio@inbox.com	smtp	46	7	46
iamnot@home.com	smtp	1	1	35	joy_rence@gmail.com	smtp	53	7	53
n1two@edianagar.cz.cc	smtp	62	9	62	rex_aviator@inbox.com	smtp	53	7	53
atria@c1z.at	smtp	66	9	66	neo_phil@formuria.com	smtp	54	7	54
aloha_care@ymail.com	smtp	72	9	72	ccare@capuccinocups.com	smtp	55	7	55

Rarely Seen Receivers

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

splunk® turn data into doing™

203

Using Splunk Enterprise Security

Copyright © 2022 Splunk, Inc. All rights reserved

| 25 May 2022

# Creating a Stream Capture

- Investigating a notable or source event?
  - You can create a temporary stream capture for the source or destination server
    - ▶ Then investigate the stream data for that server
- You can also Stream capture using:
  - Correlation search
  - Adaptive response action

The screenshot illustrates the process of creating a stream capture. It consists of three main panels:

- Top Panel:** A threat detail view for a threat activity on 10.141.2.170 at 1/7/21 9:10:05.000 AM. It shows additional fields like Destination (unknown 1229924.0), Source (10.141.2.170 4240.0), and Threat Category (hijacks). An 'Action' button (1) is highlighted.
- Middle Panel:** A 'Create Stream Capture' dialog box. It includes fields for 'Description' (Stream to/from 10.141.2.170), 'Protocols to capture' (All), 'Capture duration' (15 minutes), and a 'Create capture' button (3). A dropdown menu on the right lists various actions: Nslookup 10.141.2.170, Ping 10.141.2.170, Session Center, Stream Capture (2), Traffic Search (as destination), Traffic Search (as source), Update Search, Vulnerability Search, and Web Search (as destination).
- Bottom Panel:** A confirmation message 'Stream successfully created' with a 'View streams' link (4).

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Scenarios: Data Exfiltration

---

- Detect data exfiltration using protocol intelligence dashboards:
  - Email Activity? Examine Top Email Sources
    - Look for sudden spikes in email output from single accounts or
    - Spikes in the Large Emails display
  - DNS Activity? Examine Queries per Domain
    - Look for unfamiliar domains getting large numbers of lookups
- See an endpoint / server that may be involved in data exfiltration?
  1. Create a **stream capture** for it and analyze the data
  2. Look for sensitive information, intellectual property, etc.

# Module 10 Lab: Protocol Intelligence

---

- Time: 10 minutes
- Tasks:
  - Use Protocol Intelligence and related tools to investigate a suspected data exfiltration event

# Wrap Up

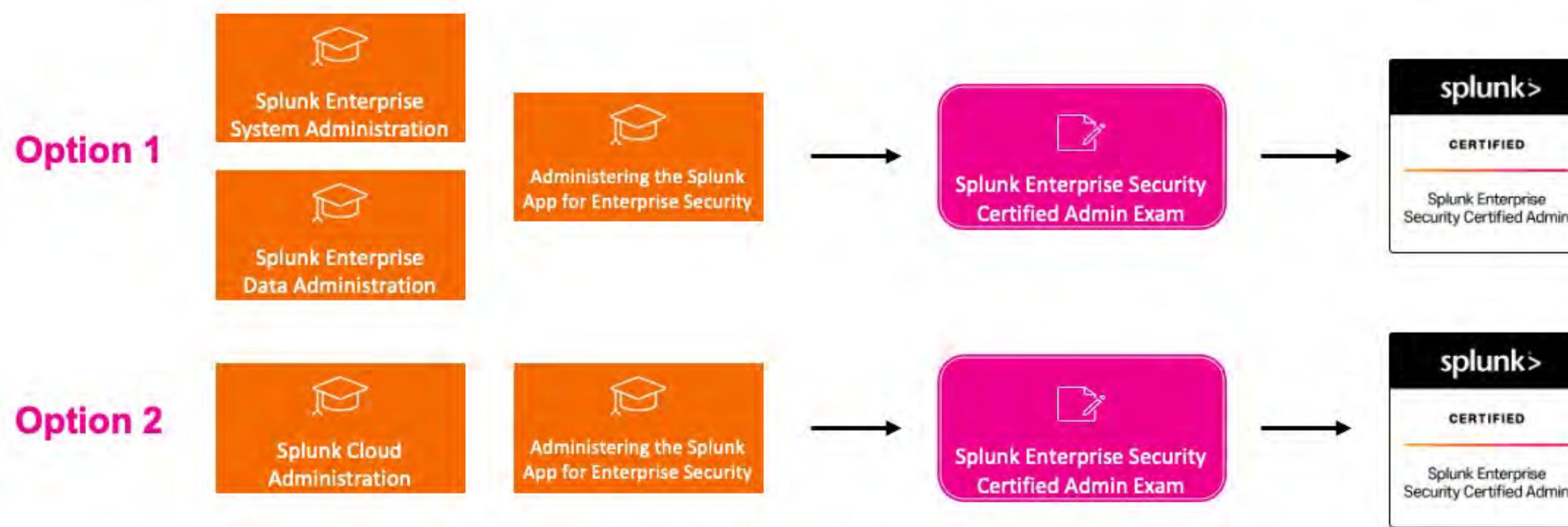
---

- Understand how to use ES
- Define correlation searches and notable events
- Use the Security Posture and Incident Review dashboards
- Use the Asset and Identity Investigators
- Perform forensic investigation on current and past incidents
- Use adaptive response actions
- Use risk-based alerting to monitor risk in your security environment
- Analyze network events for suspicious behavior
- Detect insider threats
- Use the Threat Intelligence framework
- Use Protocol Intelligence to examine live network data

# What's Next?

## Become a Splunk Enterprise Security Certified Admin

This certification demonstrates an individual's ability to install, configure, and manage a Splunk Enterprise Security deployment



Splunk Education Course(s) (recommended, but not required for this certification track). Either course path is acceptable



Exam registration assistance [here](#). Study Guide [here](#)

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Splunk Security Courses

---

For more Splunk security training, please review the Splunk Enterprise Security, Splunk SOAR, and Splunk User Behavior Analytics courses on

[https://www.splunk.com/en\\_us/training.html](https://www.splunk.com/en_us/training.html)

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Community

---

- Splunk Community Portal

[splunk.com/en\\_us/community.html](https://splunk.com/en_us/community.html)

- Splunk Answers

[answers.splunk.com](https://answers.splunk.com)

- Splunk Apps

[splunkbase.com](https://splunkbase.com)

- Splunk Blogs

[splunk.com/blog/](https://splunk.com/blog/)

- Splunk Live!

[splunklive.splunk.com](https://splunklive.splunk.com)

- .conf

[conf.splunk.com](https://conf.splunk.com)

- Slack User Groups

[splk.it/slack](https://splk.it/slack)

- Splunk Dev Google Group

[groups.google.com/forum/#!forum/splunkdev](https://groups.google.com/forum/#!forum/splunkdev)

- Splunk Docs on Twitter

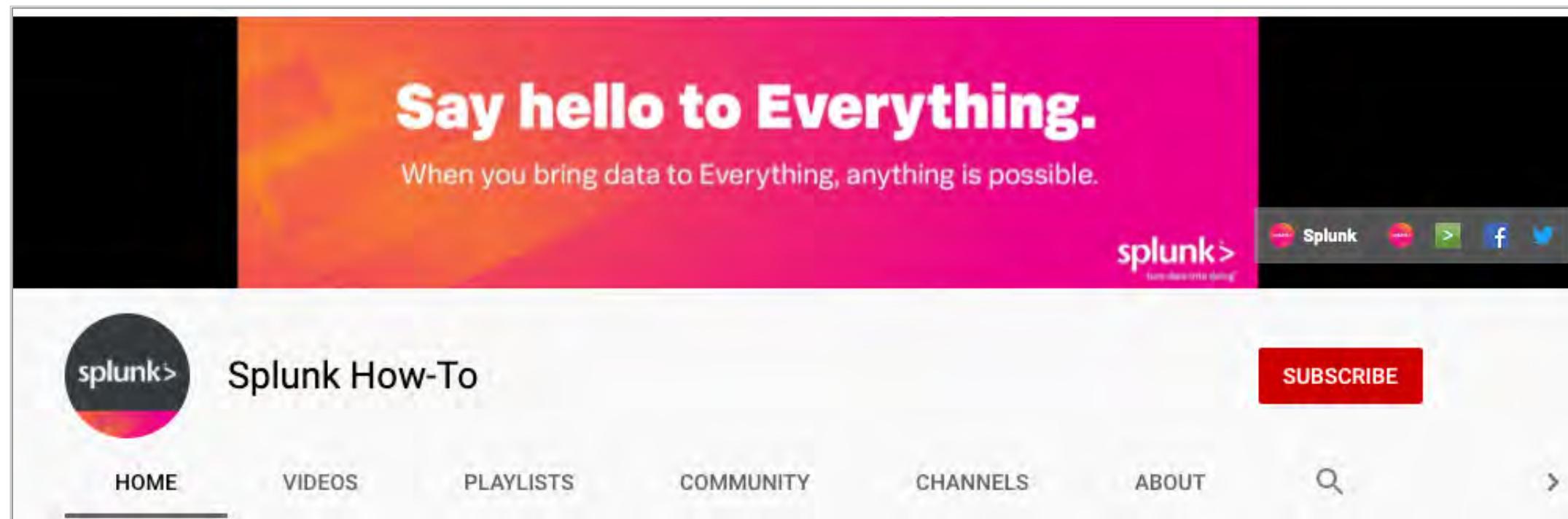
[twitter.com/splunkdocs](https://twitter.com/splunkdocs)

- Splunk Dev on Twitter

[twitter.com/splunkdev](https://twitter.com/splunkdev)

# Splunk How-To Channel

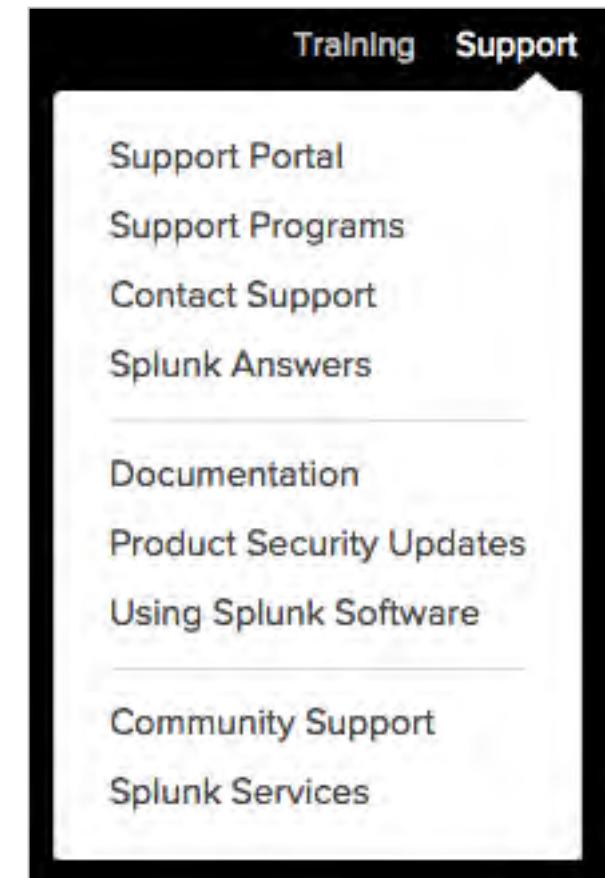
- Check out the Splunk Education How-To channel on YouTube:  
[splk.it/How-To](https://splk.it/How-To)
- Free, short videos on a variety of Splunk topics



Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Support Programs

- **Web**
  - Documentation: [dev.splunk.com](https://dev.splunk.com) and [docs.splunk.com](https://docs.splunk.com)
  - Wiki: [wiki.splunk.com](https://wiki.splunk.com)
- **Splunk Lantern**  
Guidance from Splunk experts
  - [lantern.splunk.com](https://lantern.splunk.com)
- **Global Support**  
Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365
  - Web: [splunk.com/index.php/submit\\_issue](https://splunk.com/index.php/submit_issue)
  - Phone: (855) SPLUNK-S or (855) 775-8657
- **Enterprise Support**
  - Access customer support by phone and manage your cases online 24 x 7 (depending on support contract)



# Thank You

splunk>

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Appendix A: Reports, Dashboards, Data Models & Use Cases

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

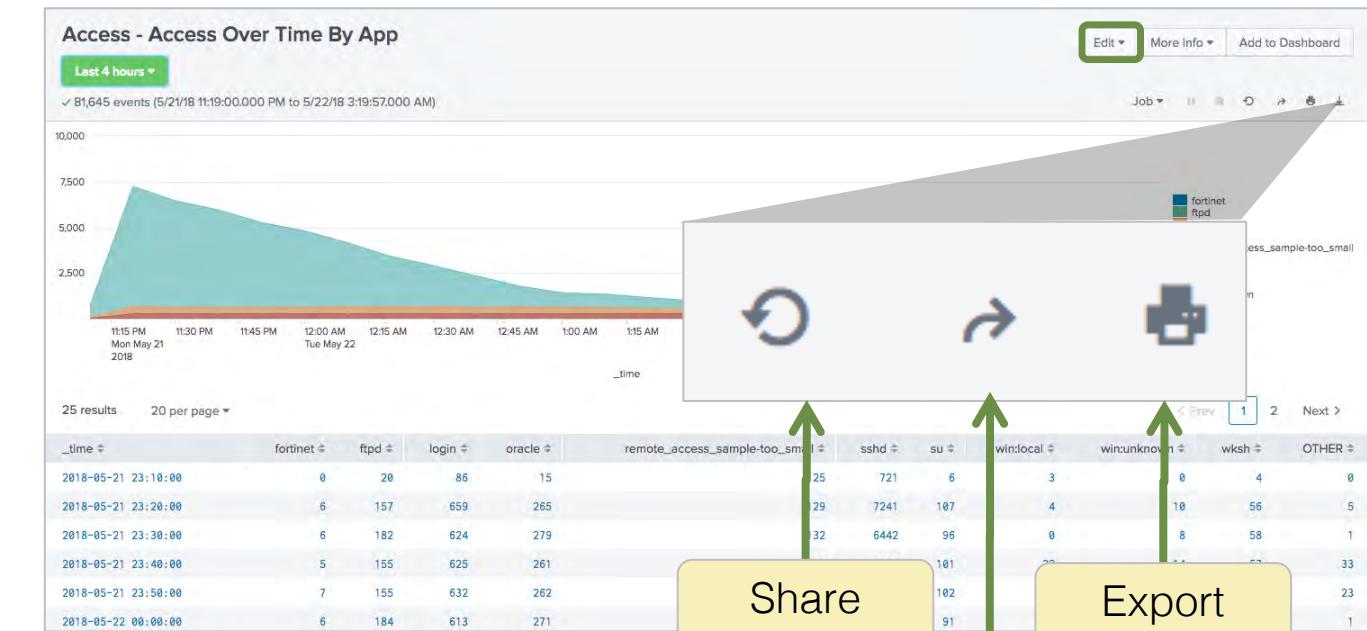
# Objectives

---

- Use and customize ES reports
- Use and customize ES dashboards
- Explore ES Correlation Searches
- Understand ES data models
- Use ES Content Updates or Use Case Library to pinpoint potential issues and share them in ES

# ES Reports

- Select Search > Reports
- Over 200 reports in more than 20 categories
- Execute any report by selecting its name
- Select Edit to open in search, modify, and save as a new report
- Use Share, Print or Export as appropriate



# ES Datasets to Build New Reports

- Access ES data models via the **Search > Datasets** menu
- **Explore > Visualize with Pivot** to quickly build new reports
  - Reports can then be enhanced with charts and saved for future use

**Datasets**

Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Select Explore > Visualize in Pivot to design a visualization-rich report based on the dataset. Select Explore > Investigate in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.

[Learn more about Datasets.](#)

944 Datasets

All	Yours	This App's	Filter by title, description, fields	Actions	Owner	App	Sharing		
Alerts > Alerts				data model	Accelerated	Edit Explore	nobody	Splunk_SA_CIM	Global
Application State (Deprecated) > All Application State				data model	Accelerated	Edit Explore	nobody	Splunk_SA_CIM	Global
Application State (Deprecated) > All Application State > Ports				data model	Accelerated	Visualize with Pivot	nobody	Splunk_SA_CIM	Global
Application State (Deprecated) > All Application State > Processes				data model	Accelerated	Investigate in Search	nobody	Splunk_SA_CIM	Global
Application State (Deprecated) > All Application State > Services				data model	Accelerated	Edit Explore	nobody	Splunk_SA_CIM	Global
Assets And Identities > All Assets				data model	Accelerated	Edit Explore	nobody	SA-IdentityManagem...	Global

[Create Table View](#)

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Lists of ES Correlation Searches

| rest splunk\_server=local count=0 /services/saved/searches  
| where match('action.correlationsearch.enabled', "1|[Tt]|[Tt][Rr][Uu][Ee]") | rename eai:acl.app as app, title as csearch\_name, action.correlationsearch.label as csearch\_label, action.notable.param.security\_domain as security\_domain | table csearch\_name, csearch\_label, app, security\_domain, description

Last 24 hours 

174 results (5/21/18 3:00:00.000 AM to 5/22/18 3:25:24.000 AM) No Event Sampling  Job  Smart Mode

Events Patterns Statistics (174) Visualization

20 Per Page  Format  Preview

Table of app, security domain, name and description of all correlation searches in your environment

csearch\_name ▾ / csearch\_label ▾ / app ▾ / security\_domain ▾ / description ▾

csearch_name	csearch_label	app	security_domain	description
Access - Account Deleted - Rule	Account Deleted	SA-AccessProtection	access	Detects user and computer account deletion
Access - Brute Force Access Behavior Detected - Rule	Brute Force Access Behavior Detected	SA-AccessProtection	access	Detects excessive number of failed login attempts along with a successful attempt (this could indicate a successful brute force attack)

1 2 3 4 5 6 7 8 9 Next >

| rest splunk\_server=local count=0 /services/saved/searches  
| where match('action.correlationsearch.enabled', "1|[Tt]|[Tt][Rr][Uu][Ee]")  
| where disabled=0 | eval actions=split(actions, ",")  
| table title ,actions

Last 24 hours 

11 results (5/21/18 3:00:00.000 AM to 5/22/18 3:31:30.000 AM) No Event Sampling  Job  Smart Mode

Events Patterns Statistics (11) Visualization

20 Per Page  Format  Preview

title ▾ / actions ▾

title	actions
Access - Brute Force Access Behavior Detected - Rule	notable risk
Audit - Anomalous Audit Trail Activity Detected - Rule	notable risk

Enabled correlation searches and the adaptive response actions

Note 

For a list of all enabled and disabled correlation searches, remove | where disabled=0.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Common Information Model

---

- The Common Information Model (CIM) is a library of data models
- The CIM is built into the data models that are included with ES
  - Many of the data models used by ES are actually configured in the CIM app
- One important service provided by the CIM is normalization
- Different data sources might use different names for one logical field name
  - Example: “Sev”, “Severity”, “SevCode”, etc. all map to the logical field name “Severity”

[docs.splunk.com/Documentation/CIM/latest/User/Overview](https://docs.splunk.com/Documentation/CIM/latest/User/Overview)

# ES Content Updates: Analytic Stories

- Self-documented searches that solve a specific problem
  - Threat / focus of the Analytic Story
  - How to implement the searches (data required)
- Tied to security frameworks (Critical Security Controls, Kill Chain, Mitre ATT&CK)
- Works in ES, Splunk Enterprise or Splunk Cloud



<https://splunkbase.splunk.com/app/3449/>

# Content Library > Analytics Stories Stats

Search > Dashboards > Content Library  
Overview of content by Analytics Stories or the searches that comprise them

The dashboard displays the following key metrics:

- Total Analytic Stories: 82 (highlighted with a green box)
- ESCU App Version: 3.10.0 (highlighted with a yellow box)
- Story Categories (Horizontal Bar Chart):
  - Abuse: 6
  - Adversary Tactics: 28
  - Best Practices: 7
  - Cloud Security: 23
  - Malware: 13
  - Vulnerability: 5
- Analytic Stories by CIS Critical Security Control (Bar Chart):

Critical Security Control	Analytic Stories
1	15
2	8
3	28
4	3
5	12
6	8
7	10
8	35
9	11
10	5
11	7
12	20
13	15
14	3
16	15
18	8
- Kill Chain Phases (Gauge Chart):
  - Reconnaissance: 5
  - Weaponization: 0
  - Delivery: 14
  - Exploitation: 10
  - Installation: 10
  - Command & Control: 22
  - Actions on Objectives: 56
- Filtering and Search Options:
  - Category, Kill Chain Phases, Data Models, CIS Critical Security Controls dropdown menus.
  - Clear All button.
- Analytic Story Details (Table):

Category	Kill Chain Phases	CIS	Data Models	Created	Last Updated
Apache Struts Vulnerability	Detect and investigate activities--such as unusually long 'Content-Type' length, suspicious java classes and web server behavior--such as processes--such as attempting to download specific scripts and libraries.	Vulnerability	Actions on Objectives	12	Endpoint 2018-12-06 2018-12-06

Applicability to frameworks: Kill Chain, CIS Critical Security Controls, etc.

1 Click items in visualizations or use drop-downs to filter details

2 Click a story row to go to its Analytics Story Detail page

Generated for Splunk University (douglas.bernardin@gmail.com) (C) Splunk Inc, not for distribution

# Content Library > Search Summary

The Search Summary tab has a similar structure and process to the Analytics Stories Stats but for searches

**Total Searches**

**361**

**Searches by CIS Critical Security Control**

Critical Security Control	Searches
1	25
2	10
3	40
4	10
5	20
6	15
7	20
8	85
9	15
10	10
11	20
12	25
13	20
14	5
15	10
16	40
17	10
18	10

**Search Types**

Search Type	Count
Detection	250
Investigative	50
Support	60

**Search Details**

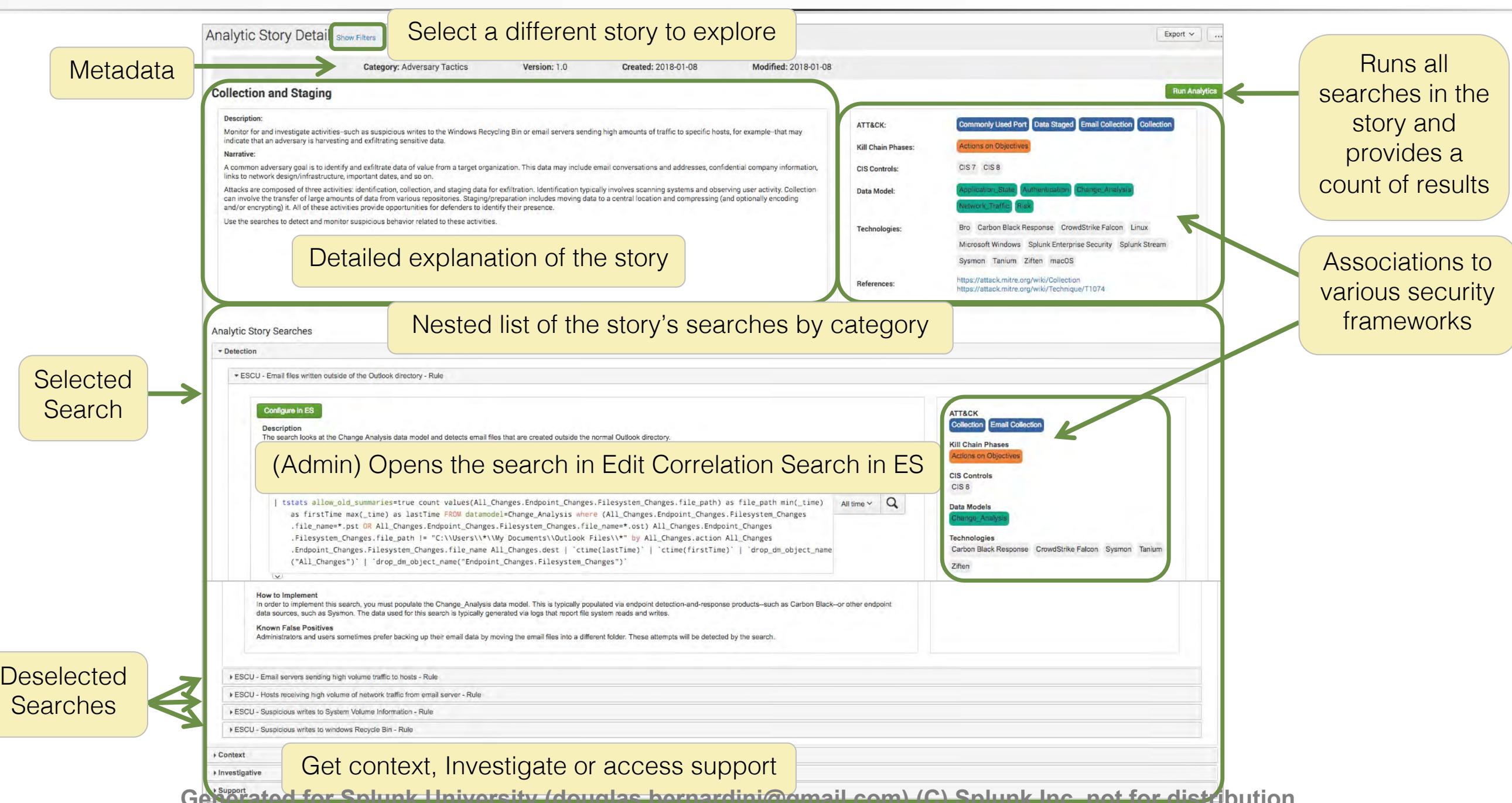
Search Name: ESCU - Abnormally High AWS Instances Launched  
description: This search looks for CloudTrail events where a user successfully launches an abnormally high number of instances.  
by User - MLTK - Rule

Kill Chain Phases: All  
CIS Critical Security Controls: All  
Data Models: All

Actions on Objectives: 13 -  
Kill Chain Phases: All  
CIS: All  
Data Models: All

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Analytic Story Detail



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Configure > Content > Use Case Library

If your admin has installed ESCU and enabled Use Case Library, you can view ESCU analytic stories from within ES, bookmark them, and add your own

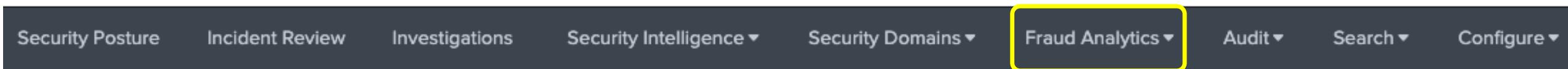
**Use Case Library**  
Explore the Analytic Stories included with Enterprise Security that provide analysis guidance on how to investigate and take actions on threats that ES detects.

**Use Cases**

	Framework Mapping: All	Data Model: All	App: All	In Use: All	Bookmarked: All	filter...	Search
Abuse							
							
	57 Analytic Stories found in categories: Cloud Security, Best Practices, Vulnerability, Abuse, Adversary Tactics, Malware						
	<input type="checkbox"/> In use	Analytic Story	Use Case	Description	App	Last Updated	Bookmark
	>	∅ AWS Cross Account Activity	Cloud Security	Track when a user assumes an IAM role in another AWS account to obtain cross-account access to services and resources in that account. Accessing new roles could be an indication of malicious activity.	ES Content Updates	Jun 8, 2018	<input checked="" type="checkbox"/>
	>	∅ AWS Cryptomining	Cloud Security	Monitor your AWS EC2 instances for activities related to cryptojacking/cryptomining. New instances that originate from previously unseen regions, users who launch abnormally high numbers of instances, or EC2 instances started by previously unseen users are just a few examples of potentially malicious behavior.	ES Content Updates	Mar 15, 2018	<input checked="" type="checkbox"/>
	▼	∅ AWS Network ACL Activity	Cloud Security	Monitor your AWS network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper, when the facts warrant it.	ES Content Updates	May 21, 2018	<input checked="" type="checkbox"/>
Adversary Tactics							
							
Best Practices							
							
Cloud Security							
							
<b>Detection Searches</b>				Recommended Data Sources	Sourcetypes	Data Models	Lookups
				AWS	aws:cloudtrail	No items found	No items found
				Splunk Enterprise Security			
<ul style="list-style-type: none"><li>∅ ESCU - AWS Network Access Control List Created with All Open Ports - Rule <a href="#">[?]</a></li><li>∅ ESCU - AWS Network Access Control List Deleted - Rule <a href="#">[?]</a></li><li>∅ ESCU - Detect Spike in blocked Outbound Traffic from your AWS - Rule <a href="#">[?]</a></li><li>∅ ESCU - Detect Spike in Network ACL Activity - Rule <a href="#">[?]</a></li></ul>							
<b>Framework Mapping</b>							
CIS 20 <a href="#">CIS 11</a> <a href="#">CIS 12</a> <a href="#">CIS 16</a>							
KILL CHAIN PHASES <a href="#">Actions on Objectives</a> <a href="#">Command and Control</a>							

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Splunk & Fraud Analytics



- Leverages Splunk Enterprise Security
  - Analyst can work in a familiar incident review tab
  - Fraud Incident Review includes workflow link to Investigate dashboard
  - Visual link analysis to make fraud investigations quick
  - Leverages Risk-based Alerting (RBA) principles
- Extensible and configurable
  - All fraud rules available as correlation searches and can be modified
  - Application designed with data models as the source of all searches
  - Macros used to define constraints (sources for data models)



**Splunk App for Fraud Analytics**

# Appendix B: Event Sequence Engine

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Event Sequencing Engine

- The **Event Sequencing Engine** allows you to create a group of correlation searches looking for specific fields and values
- Admins create a workflow called a **Sequence Template** that defines the correlation searches and variables, and if configured, the order in which the notable events need to occur
- A **Sequenced Event** is created when the workflow triggers notable events with the configured fields and values
- Similar to writing a script to automate things that you would have to do manually when tracking a variety of notable events and variables through a variety of correlation searches

Note 

Only ES admins, or users given the [Edit Sequence Templates](#) permission can create Sequence Templates. ES analysts can view the resulting events and add them to investigations.

# Example Use Case

---

## Start (correlation search)

1. Brute Force Access Behavior Detected

## Transitions (correlation searches)

1. Unusually Long Command Line
2. Uncommon Processes On Endpoint
3. Web Uploads to Non-corporate Sites by Users
4. Suspicious Reg.exe Process

## End (correlation search)

6. Abnormally High Number of Endpoint Changes by User

# Example Configuration

Configure > Content > Content Management > Create New Content > Sequence Template

- The Content Management window has been filtered to show only Sequence Templates

The screenshot shows the Splunk Enterprise Security interface with the following details:

- Top Navigation Bar:** Security Posture, Incident Review, Investigations, Security Intelligence, Security Domains, Audit, Search, Configure (highlighted), and Enterprise Security.
- Content Management Section:** Manage knowledge objects and other content specific to Splunk Enterprise Security.
- Filter Bar:** Type: Sequence T... (1) (highlighted with a green box), App: All (1), Status: All, filter, and Clear filters.
- Table View:** Displays two objects: "ES Demo Template" and "Suspicious Behavior - Brute Force".

	Name	Type	App	Next Scheduled Time
<input type="checkbox"/>	ES Demo Template	Sequence Template	Enterprise Security	
<input type="checkbox"/>	Suspicious Behavior - Brute Force	Sequence Template	Enterprise Security	
- Right Panel:** A sidebar with the following options:
  - Risk Factor
  - Saved Search
  - Search-Driven Lookup
  - Sequence Template** (highlighted with a green box)
  - Swim Lane Search
  - View
  - Workbench Panel
  - Workbench Profile
  - Workbench Tab
- Bottom Footer:** Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution.

# Example Configuration (cont.)

**New Sequence Template**

< Back to Content Management

**Sequence Template**

Name: Suspicious Behavior

Description: Detect end users with suspicious behavior like long command line, web uploads on non-corporate sites, reg.exe processes, etc.

App: Enterprise Security

Defines the app in which the .conf entries will be created.

**Start**

Correlation Search: Access - Brute Force Access Behavior Detected - Rule

Expression: 'dest' = "198.18.0.101"

Field: user

Label: questionable\_user

**Transitions**

Enforce Ordering:  Enforces chronological order of transitions, otherwise just check transitions is disabled when ordering is disabled.

Aggregate Matches:  Keep accumulating matched events that may occur multiple times. Accumulated events will be added to the final sequenced event.

**Uncommon Processes**

Title: Uncommon Processes

Correlation Search: ESCU - Uncommon Processes On Endpoint - Rule

Expression: 'user' = "\$questionable\_user\$"

**Long CLI**

Title: Long CLI

Correlation Search: ESCU - Unusually Long Command Line - Rule

Expression: 'user' = "\$questionable\_user\$"

**End**

Correlation Search: Change - Abnormally High Number of Endpoint Changes By User - Rule

Expression: 'user' = "\$questionable\_user\$"

Field value should be enclosed in single quotes, and the matching value enclosed in double quotes. Ex: 'host' = "127.0.0.1"

Time Limit: 2 day(s)

**Actions**

**Sequenced Event**

Event Title: Suspicious Endpoint Behavior

Supports state token substitution.

Event Description: Questionable processes on endpoints.

Supports state token substitution.

Urgency: High

Security Domain: Endpoint

Output Fields: + Add Field

The value field can be populated with either static values or saved state tokens from transitions.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Resulting Sequence Event

The results of the Sequence Templates are Sequenced Events, which are viewed in Incident Review

The screenshot shows the Splunk Enterprise Security Incident Review interface. At the top, there are various filter options like Tag, Urgency, Status, Owner, Security Domain, and Type. A dropdown for 'Search Type' is open, showing 'Sequenced Event' selected. Below the filters, a table displays a single result: 'Host with Old Infections Sequence'. This row has a green border. The table columns include Title, Risk Object, Aggregated Risk Score, Risk Events, Type, Time, and Disposition. Under 'Title', it says 'Host with Old Infections Sequence'. Under 'Template Title', it says 'ES Demo Template'. Under 'Template Description', it says 'No Description' and 'View events'. Under 'Transitions', there is a table with three rows: 'start' at Aug 4, 2021 3:27 PM, 'Old Malware' at Aug 4, 2021 3:30 PM, and 'end' at Aug 4, 2021 3:30 PM. A callout bubble points to the 'Transitions' table with the text: 'Transitions display the correlation searches matched in the template'. The bottom of the interface has a footer with 'Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution'.

Incident Review

Source: Sequenced Event    Earliest: -24h@h    Latest: now

Search... Search Type ? Show Charts Hide Filters

Saved filters Tag Urgency Status Owner Security Domain Type

Select... Add tags... Select... Select... Select... Select... Select... Select...

Save new filters Update Clear all Submit

Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition
Host with Old Infections Sequence	--	--	--	Notable	Today, 3:31 PM	Undetermined

**Sequenced Event Description:**  
Detects hosts with malware infections and access issues

**Template Title:**  
[ES Demo Template](#)

**Template Description:**  
No Description  
[View events](#)

**Transitions:**

Stage	Time	Match
start	Aug 4, 2021 3:27 PM	High Or Critical Priority Host With Malware Detected <a href="#">View original events</a>
Old Malware	Aug 4, 2021 3:30 PM	Host With Old Infection Or Potential Re-Infection (EICAR-AV-Test On BUSDEV-002) <a href="#">View original events</a>
end	Aug 4, 2021 3:30 PM	Activity from Expired User Identity (dmsys) <a href="#">View original events</a>

Transitions display the correlation searches matched in the template

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

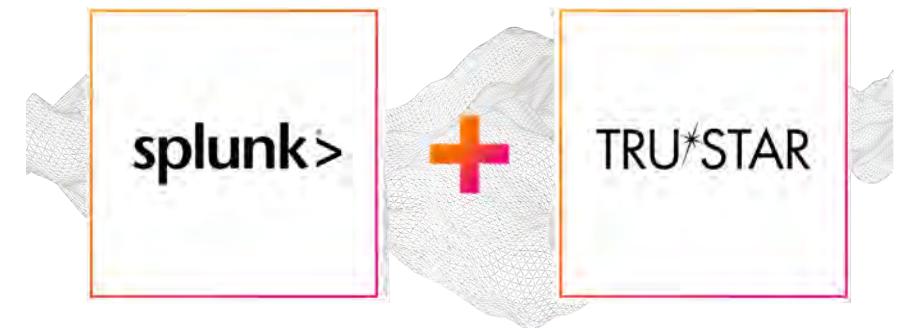
# Appendix C: Interfacing with Splunk Intelligence Management (TrueSTAR)

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Splunk Intelligence Management

In addition to the Ingest of Indicators from multiple Intelligence Sources into Splunk KV stores for alerting, the TruSTAR Unified app enables two Adaptive Response actions:

- Enrich threat activity notable events
- Submit events to TruSTAR

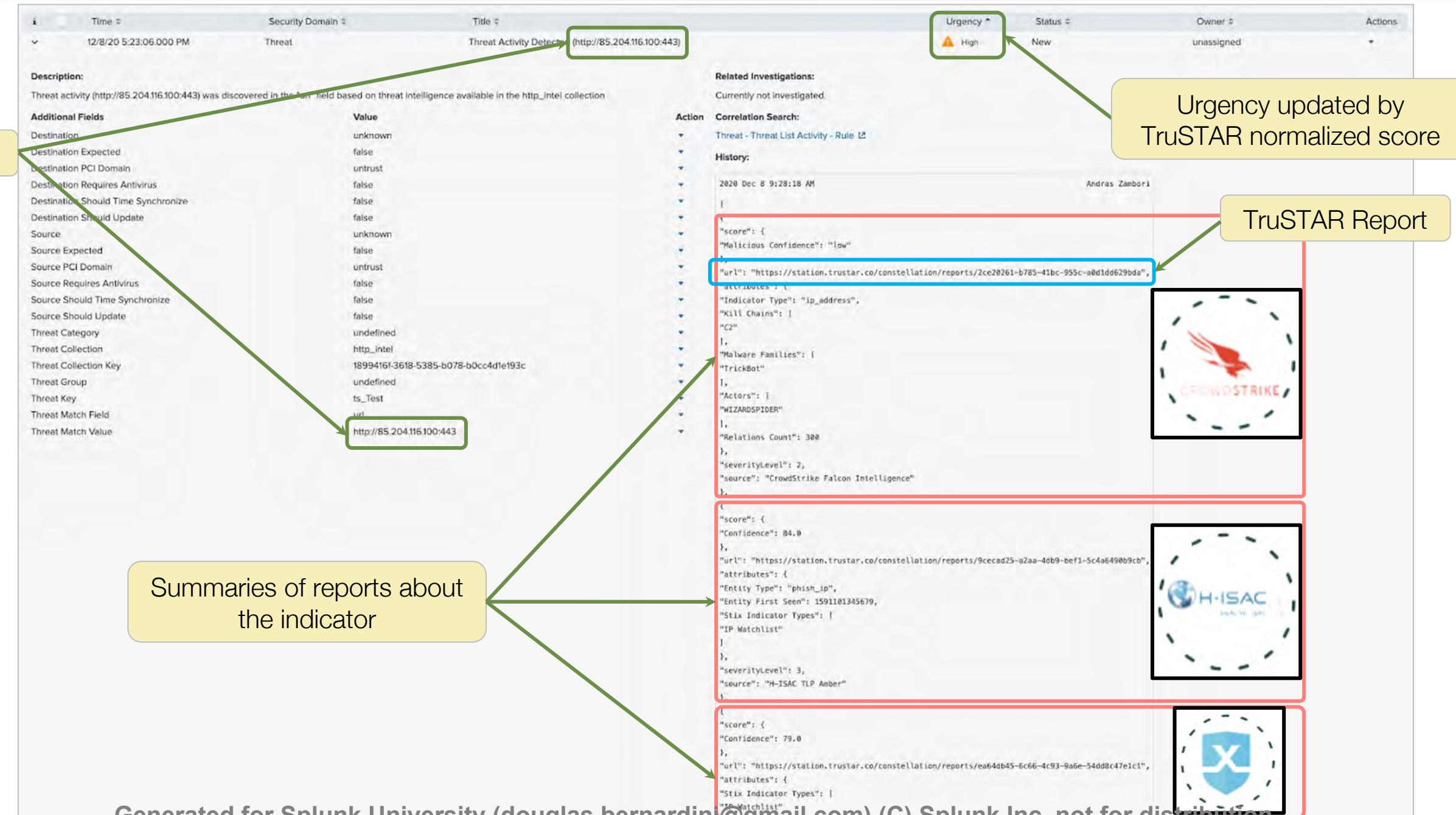


 TruSTAR - Enrich Threat Activity NEs  
Enrich notable events generated by ES's "Threat Activity Detected" correlation search.  
Category: [Information Gathering](#) | Task: [create,update](#) | Subject: [threat.artifact](#) |  
Vendor: [Splunk](#)

 TruSTAR - Submit  
Submit an event to TruSTAR.  
Category: [Information Conveyance](#),[Information Gathering](#) | Task: [create,update,allow,scan](#) |  
Subject: [splunk.event,threat.artifact](#) | Vendor: [Splunk](#)

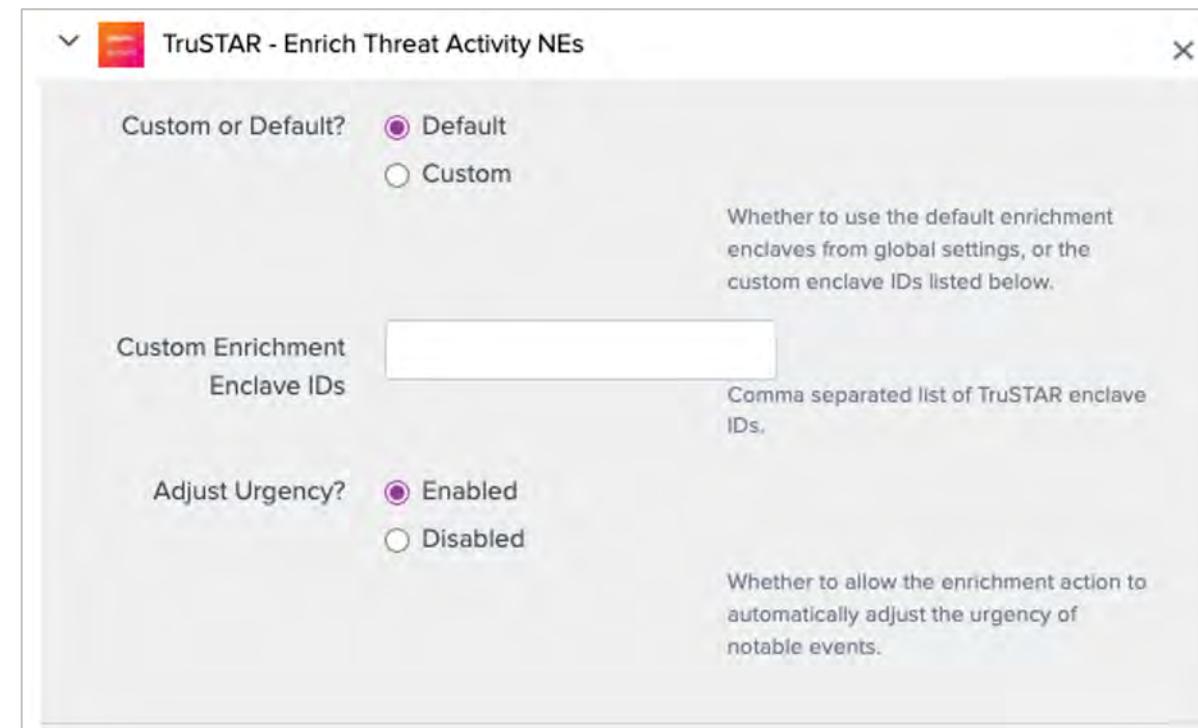
Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution

# Enrich Threat Activity Notable Events



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Enrich Threat Activity Notable Events (cont.)



```
{  
  "score": {  
    "Malicious Confidence": "high"  
  },  
  "url": "https://station.trustar.co/constellation/reports/74e8d28b-f7b6-44f4-8522-  
afa2dc6c60a3",  
  "attributes": {  
    "Indicator Type": "url",  
    "Kill Chains": [  
      "C2"  
    ],  
    "Relations Count": 300,  
    "Actors": [  
      "WIZARDSPIDER"  
    ],  
    "Malware Families": [  
      "TrickBot"  
    ],  
    "severityLevel": 3,  
    "source": "CrowdStrike Falcon Intelligence"  
  }  
}
```

The JSON object represents the enriched notable event. Key fields highlighted with green boxes include 'Malicious Confidence', 'url', 'Kill Chains', 'Relations Count', 'Actors' (with 'WIZARDSPIDER'), 'Malware Families' (with 'TrickBot'), and 'severityLevel'. A yellow box labeled 'Pass-through/Original Score' surrounds the top section of the JSON. A yellow box labeled 'Actor(s)' surrounds the 'Actors' array. A yellow box labeled 'Malware Families' surrounds the 'Malware Families' array. A yellow box labeled 'Normalized Score' surrounds the bottom section of the JSON.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Appendix D: Cloud Security Dashboards

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Cloud Security Dashboards

Visualize the security of your cloud infrastructure (AWS, Azure) through several dashboards

The screenshot shows the Splunk Enterprise Security interface. At the top, there is a navigation bar with various tabs: Security Posture, Incident Review, Investigations, Security Intelligence, Security Domains, Cloud Security (which is highlighted with a yellow box), Audit, and Search. A tooltip labeled "Important!" is overlaid on the Cloud Security tab, containing the text: "To onboard Cloud data sources and examine your Cloud Security environment, you must install and setup Splunk Add-on for Amazon Kinesis Firehose and Splunk Add-on for Microsoft Office 365 from Splunkbase." Below the navigation bar, there is a section titled "Splunk Enterprise Security" with a brief description. To the right of this, a dropdown menu is open under the "Cloud Security" tab, listing "Security Groups", "IAM Activity", "Network ACLs", "Access Analyzer", and "Microsoft 365". Further down the page, there are several cards: "Security Posture" (with a green circular icon), "Incident Review" (with a green flag icon), "App Configuration" (with a green wrench icon), "Documentation" (with a green question mark icon), "Community" (with a green speech bubble icon), and "Product Tour" (with a green double arrow icon).

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

# Prerequisites

1. Create indexes to populate the **Cloud Security** dashboards
2. Provide index name in ES app settings
  - Select **Configure > General > General Settings**
  - Navigate to **AWS Index** or **Microsoft 365**
  - Populate index name
3. Install **Amazon Kinesis Firehose** and **Microsoft 365** add-ons
4. Configure add-ons to send data to Splunk and prepare Splunk to receive data

Note

If you are already using AWS or Microsoft 365 TAs, you can use these instructions to configure your existing indexes rather than create a new one.

# Available Dashboards

---

- Use the **Security Group** dashboard to monitor activity in your AWS environment
- Use the **IAM Activity** dashboard to monitor user activity in your AWS environment
- Use the **Network ACLs** dashboard to monitor your network ACL activity in the AWS environment
- Use the **Access Analyzer** dashboard to monitor your AWS public facing queues, lambdas, and S3 buckets
- Use the **Microsoft 365 Security** dashboard to monitor security activity in your Microsoft 365 applications

Generated for Splunk University ([douglas.bernardini@gmail.com](mailto:douglas.bernardini@gmail.com)) (C) Splunk Inc, not for distribution