



Administering Splunk Enterprise Security

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document
- Do not distribute

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

Course Prerequisites

- Prerequisites:
 - What is Splunk?
 - Intro to Splunk
 - Using Fields
 - Introduction to Knowledge Objects
 - Creating Knowledge Objects
 - Creating Field Extractions
 - Enriching Data with Lookups
 - Data Models
 - Splunk Enterprise System Administration
 - Splunk Enterprise Data Administration

Course Prerequisites (cont.)

- Recommended:
 - Scheduling Reports and Alerts
 - Search Optimization
 - Using Splunk Enterprise Security
 - Splunk Enterprise Cluster Administration
 - Architecting Splunk Deployments
 - Splunk Cloud Administration

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

Course Goals

- Overview of Enterprise Security (ES)
- Explain how an ES administrator can customize the Security Posture and Incident Review dashboards
- Examine the ES Risk framework and risk-based alerting information provided for risk notable events
- Discuss how an ES admin can customize the Investigation Workbench
- Perform initial ES installation and configuration
- Manage data intake and normalization in ES
- Create and tune correlation searches
- Configure ES lookups
- Configure the different ES frameworks including Assets & Identities and Threat Intelligence

Important!



All labs must be completed for course credit

Course Outline

- 1. Introduction to ES
- 2. Security Monitoring
- 3. Risk-Based Alerting
- 4. Incident Investigation
- 5. Installation
- 6. Initial Configuration
- 7. Validating ES Data
- 8. Custom Add-ons
- 9. Tuning Correlation Searches
- 10. Creating Correlation Searches
- 11. Asset & Identity Management
- 12. Threat Intelligence Framework

Appendix A: Analyst Tools & Dashboards

Appendix B: Use Case Library

Appendix C: Event Sequencing Engine

Appendix D: ES On-prem Deployment

Appendix E: Using ES Overview

Generated for Splunk University (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

- Review how ES functions
- Understand how ES uses data models
- Configure ES roles and permissions

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

Data Flow in Enterprise Security

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



ES Searches for Threats and Anomalies

ES creates notable events which are stored in summary indexes and are searchable by data models

Data Model Summary Searches Run

CIM DM normalization is applied, CIM DM key/value pairs are stored (acceleration) in DM

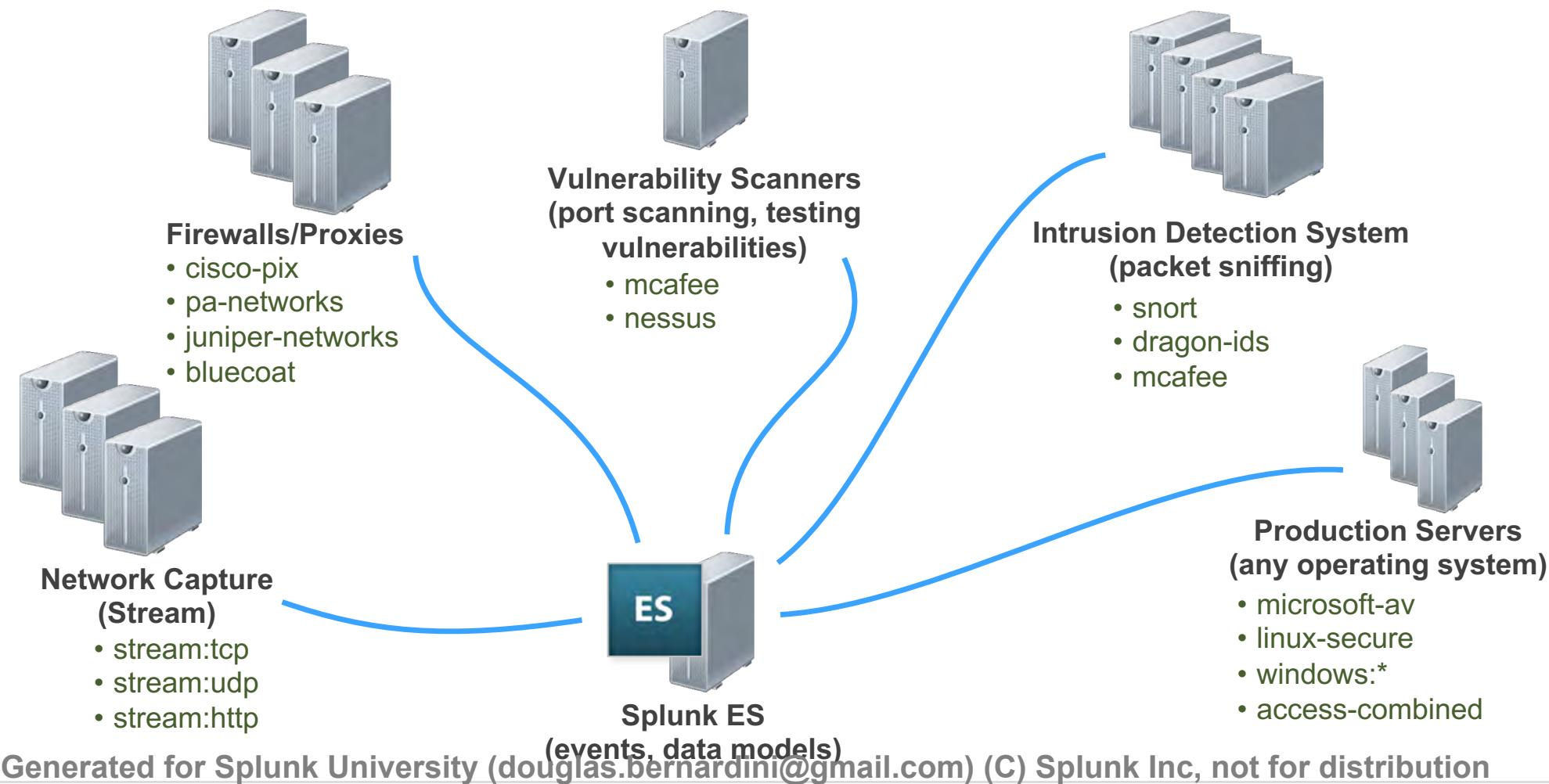
TSIDX

ES Background Searches (content) Process Data

Correlation Searches, trackers, and threat intelligence search data models

ES Data Flow

- 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



Data Models

- ES depends heavily on accelerated data models
 - ES uses the Common Information Model (CIM) that helps you to normalize your data to match a common standard
- Data models show normalized data
- Acceleration provides a “speedup” factor
- Use `| tstats` searches with `summariesonly = true` to search accelerated data

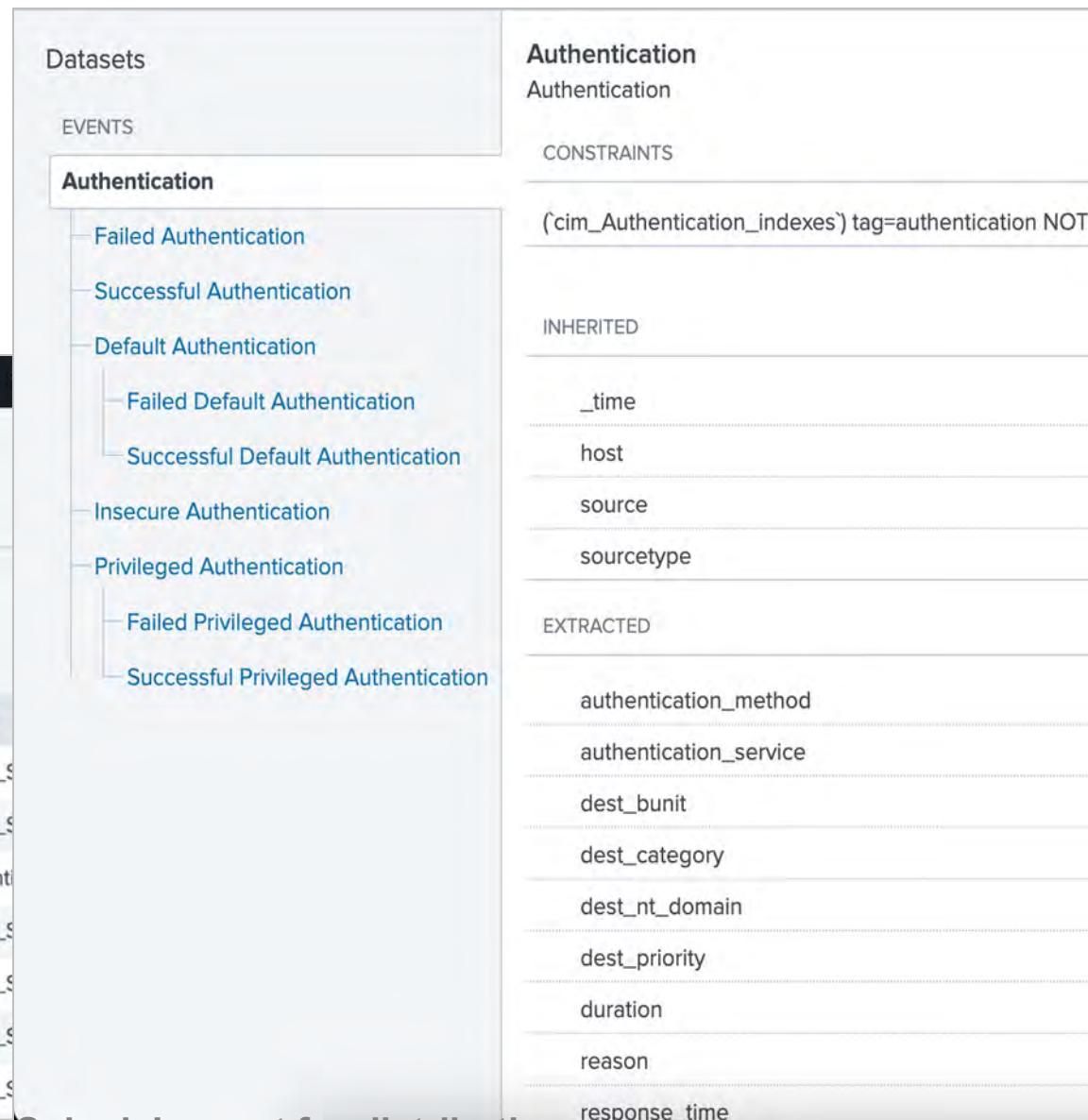
Data Models

Splunk Enterprise > Settings > Data models

Tech add-ons normalize events based on source types which associates events with specific data models

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

- Header: splunk>enterprise Apps ▾ admin ▾ 2 Messages ▾
- Section: Data Models
- Text: Data models enable users to easily create reports in the Pivot tool. [Learn More](#)
- Statistics: 32 Data Models App: Enterprise Security (SplunkEnterpriseSecuritySuite) ▾
- Filters: Visible in the App ▾ Owner: Any ▾ filter
- Table Headers: i Title ▾ Type Actions App
- Table Rows:
 - > Alerts data model Edit ▾ Pivot Splunk_S...
 - > Application State (Deprecated) data model Edit ▾ Pivot Splunk_S...
 - > Assets And Identities data model Edit ▾ Pivot SA-Ident...
 - > Authentication data model Edit ▾ Pivot Splunk_S...
 - > Certificates data model Edit ▾ Pivot Splunk_S...
 - > Change data model Edit ▾ Pivot Splunk_S...
 - > Change Analysis (Deprecated) data model Edit ▾ Pivot Splunk_S...



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

tstats Search Example

The screenshot shows a Splunk search interface titled "New Search". The search bar contains the command: `| tstats summariesonly=true count FROM datamodel=Authentication WHERE Authentication.action=failure BY Authentication.app`. Below the search bar, it says "1,866,840 events (6/21/20 10:00:00.000 PM to 6/22/20 10:00:30.000 PM)" and "No Event Sampling". On the right, there are buttons for "Save As", "Close", "Last 24 hours", and a magnifying glass icon. The main area displays a table with the following data:

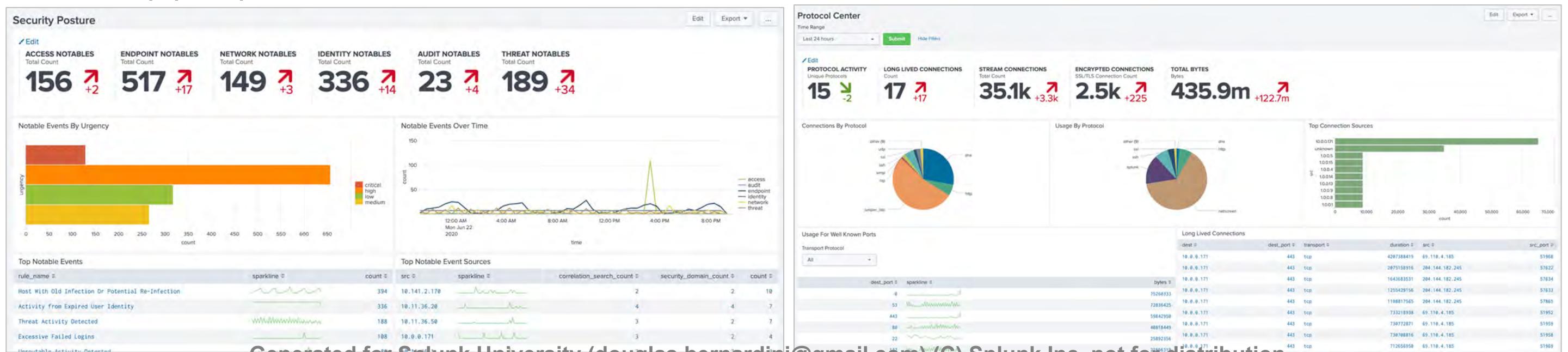
Authentication.app	count
Authentication Manager	33
login	90764
netscreen	192
oracle	21182
sshd	1753027

- ES uses `| tstats` to create reports based on accelerated data models
 - Use `| tstats summariesonly=t` to restrict results to accelerated data
- Use Search > Datasets to search datasets using ES data models

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

Looking for Trouble

- ES runs real-time and with scheduled searches on accelerated Data Model data, looking for indicators of threats, vulnerabilities, or attacks
 - If a search discovers something that needs attention, ES displays it on one or more dashboards
 - You can then investigate the issue, track it, analyze it, and take the appropriate action



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

Correlation Searches

- Correlation Searches run continually in the background looking for known types of threats and vulnerabilities such as anomalies and suspicious/malicious behavior
 - There are a number of built-in correlation searches in ES, and more in the Use Case Library. You can also add your own searches
- When a correlation search detects any Indicators of Compromise (IOC), ES raises an adaptive response. A frequently used adaptive response is a notable event also called 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) (C) Splunk Inc, not for distribution

Correlation Searches (cont.)

- Correlation searches run either in real-time or on a schedule
- Correlation searches can be modified and extended as needed
- Each search looks for a specific type of threat, vulnerability, or sign of malicious attack
 - Example Correlation Searches
 - *Activity from Expired User Identity*
 - *Brute Force Access Behavior Detected*
 - *Excessive Failed Logins*
 - *Threat Activity Detected*
 - Generating a notable event (also referred to as an incident) is a typical AR, others include sending email, running a script, and updating a risk score

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

ES Content

Configure > Content > Content Management

Content Management

Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, and reports.

[Create New Content ▾](#)

[Back to ES Configuration](#)

Filter by Type, App, Status, or text

1722 Objects	Edit selection ▾	1 selected	Clear	Type: All (1) ▾	App: All (1) ▾	Status: All ▾	filter	Next Scheduled Time	Actions
<input checked="" type="checkbox"/>   Nan	Export Enable Disable	Number of En		<input type="text" value="filter"/> 	<input type="text" value="filter"/> 	<input checked="" type="checkbox"/> All	<input type="text" value="App"/> 	DA-ESS-EndpointProtection	Enable Disabled Clone
<input type="checkbox"/> > Access - Access App Tracker -				<input type="checkbox"/> All			DA-ESS-NetworkProtection	Jan 14, 2022 8:50 PM UTC	
<input type="checkbox"/> > Access - Access Over Time				<input type="checkbox"/> All			SA-AccessProtection	Jan 14, 2022 8:15 PM UTC	
<input type="checkbox"/> > Access - Access Over Time By Action				<input type="checkbox"/> All			DA-ESS-AccessProtection		
<input type="checkbox"/> > Access - Access Over Time By App				<input type="checkbox"/> All			DA-ESS-AccessProtection		
<input type="checkbox"/> > Click a title to edit				<input type="checkbox"/> All			DA-ESS-AccessProtection		
<input type="checkbox"/> > Expired Identities				<input type="checkbox"/> All			Swim Lane Search	DA-ESS-AccessProtection	
<input type="checkbox"/> > Access - All Authentication By Asset - Swimlane				<input type="checkbox"/> All					

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

Active Correlation Searches

- View which correlation searches are enabled
- By default, only ES Admins can enable, disable, clone, modify, or add new correlation searches
- Clone a correlation search, make changes, and save as a new search

Content Management
Manage knowledge objects and other content specific to your organization.

[Create New Content ▾](#)

[Filter by Correlation Search and Enabled](#)

28 Objects	Edit selection ▾	1 selected Clear	Type: Correlation ... (1) ▾	App: All (1) ▾	Status: Enabled ▾	filter	Clear filters	< Prev	1	2	Next >	25 per page ▾
List of Correlation Searches												
#	Name	Type	App	Next Scheduled Time	Actions							
<input checked="" type="checkbox"/>	Abnormally High Number of Endpoint Changes By User	Correlation Search	DA-ESS-EndpointProtection	Jul 6, 2021 2:05 PM CDT	Enabled Disable Clone							
<input type="checkbox"/>	Abnormally High Number of HTTP Method Events By Src	Correlation Search	DA-ESS-NetworkProtection	Jul 6, 2021 1:50 PM CDT	Enabled Disable Clone							
<input type="checkbox"/>	Activity from Expired User Identity	Correlation Search	SA-IdentityManagement	Jul 6, 2021 1:35 PM CDT	Enabled Disable Clone							
<input type="checkbox"/>	Anomalous Audit Trail Activity Detected	Correlation Search	SA-AuditAndDataProtection	Jul 6, 2021 1:35 PM CDT	Enabled Disable Clone Change to scheduled							
<input type="checkbox"/>	ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days	Correlation Search	SA-ThreatIntelligence	Jul 6, 2021 1:40 PM CDT	Enabled Disable Clone							
<input type="checkbox"/>	Brute Force Access Behavior Detected	Correlation Search	SA-AccessProtection	Jul 6, 2021 1:35 PM CDT	Enabled Disable Clone							
<input type="checkbox"/>	Concurrent Login Attempts Detected	Correlation Search	DA-ESS-AccessProtection	Jul 6, 2021 2:10 PM CDT	Enabled Disable Clone							
<input type="checkbox"/>	Default Account Activity Detected	Correlation Search	SA-AccessProtection	Jul 6, 2021 1:35 PM CDT	Enabled Disable Clone Change to scheduled							

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

Notable Events

- Correlation searches create **notable events** in the **notable** index
- 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)
- Search notable events in the **notable** index
 - In ES, select **Search > Search** to run a manual search
 - Search **index=notable** for a given time period
 - Event source field shows the correlation search that created the notable event

Notable Events Example

From ES > Search > Search, run a search for all events in the notable index

The screenshot shows the Splunk Enterprise Security interface with a search query "1 index = notable" selected. The search results show 66 events from July 7, 2021, between 9:22:00.000 AM and 10:22:54.000 AM. The "Events (66)" tab is active. A callout box highlights the "source" field, stating: "The **source** field shows which correlation searches generated notable events". The "source" field details table shows the following data:

Values	Count	%
Endpoint - Old Malware Infection - Rule	20	30.303%
Threat - Threat List Activity - Rule	11	16.667%
Endpoint - High Or Critical Priority Host With Malware - Rule	2	3.03%
Web - Abnormally High Number of HTTP Method Events By Src - Rule	2	3.03%
Access - Inactive Account Usage - Rule	1	1.515%

Below the table, a list of event snippets is shown, starting with:

- r Identity - Rule", count="3", info_max_time="1625671500.00000000", info_min_time="1625670900.0000005671122", orig_raw="Jul 07 15:18:42 cm1.acmetech.net auth|security:info su: [ID 366847 auth.info] 's
- Activity from Expired User Identity - Rule | sourcetype = stash
- ule", dayDiff="604.8", dest="ACME-006", firstTime="1573412224", info_max_time="1625671620.0000000625671203.784498000", lastTime="1625670808", signature="unknown"
- Old Malware Infection - Rule | sourcetype = stash
- ule", dayDiff="604.8", dest="ACME-001", firstTime="1573412430", info_max_time="1625671620.0000000625671203.784498000", lastTime="1625670814", signature="unknown"
- Old Malware Infection - Rule | sourcetype = stash
- ule", dayDiff="604.8", dest="COREDEV-002", firstTime="1573414157", info_max_time="1625671620.0000000625671203.784498000", lastTime="1625670796", signature="Mal/Packer"

ES Roles

ES Roles (required for ES login)

ES User
ess_user

Runs real-time searches
and views all ES
dashboards

User

ES Analyst
ess_analyst

Owns notable events
and performs notable
event status changes

Power

ES Admin
ess_admin

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

Admin

Standard Splunk Roles

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

Enabling Role Capabilities

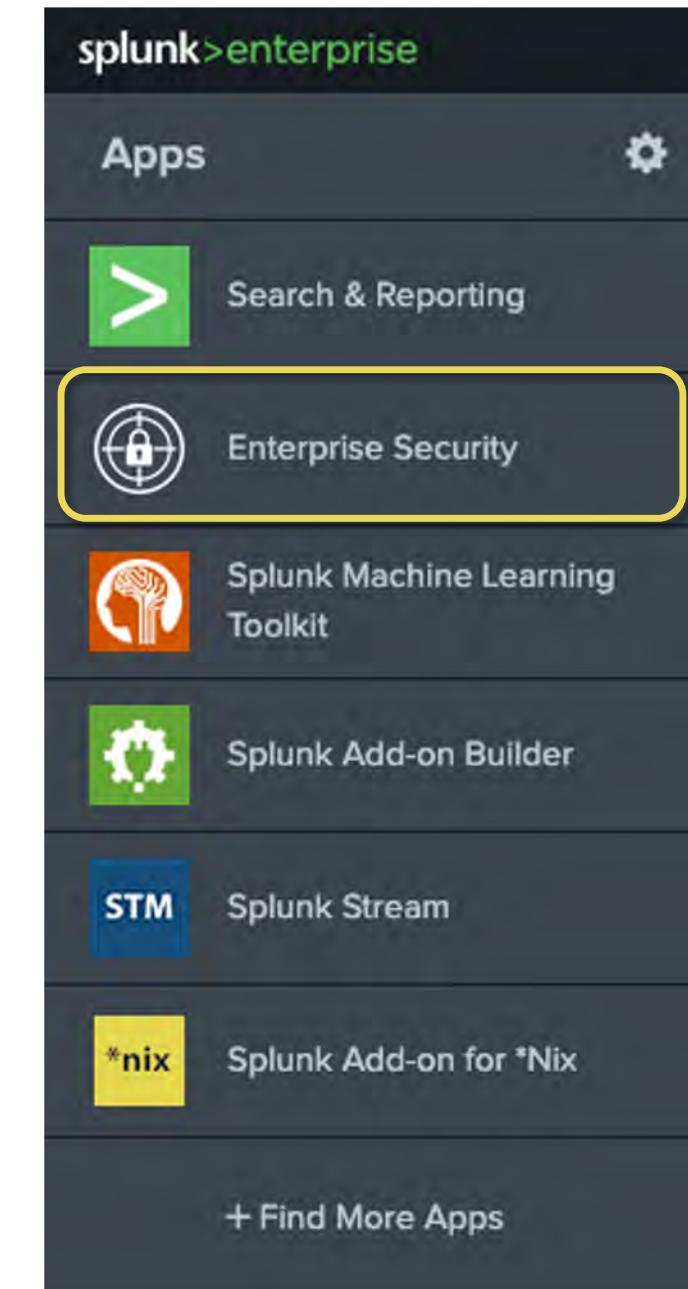
- Users should not be added to the ES Admin role
- Instead, enable or disable ES component permissions for the `ess_analyst` or `ess_user` role

ES > Configure > General > Permissions

ES Component	ess_analyst	ess_user
Create New Notable Events Permits the role to create new (ad-hoc) Notable Events. Capabilities: <code>edit_notable_events</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit Advanced Search Schedule Settings Permits the role to edit advanced search schedule settings. Capabilities: <code>schedule_search</code> , <code>edit_search_schedule_priority</code> , <code>edit_search_schedule_window</code>	<input type="checkbox"/>	<input type="checkbox"/>
Edit Analytic Story Permits the role to edit analytic stories. Capabilities: <code>edit_analyticstories</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit Correlation Searches Permits the role to edit Correlation Searches. Capabilities: <code>edit_correlationsearches</code> , <code>schedule_search</code>	<input type="checkbox"/>	<input type="checkbox"/>

Accessing ES

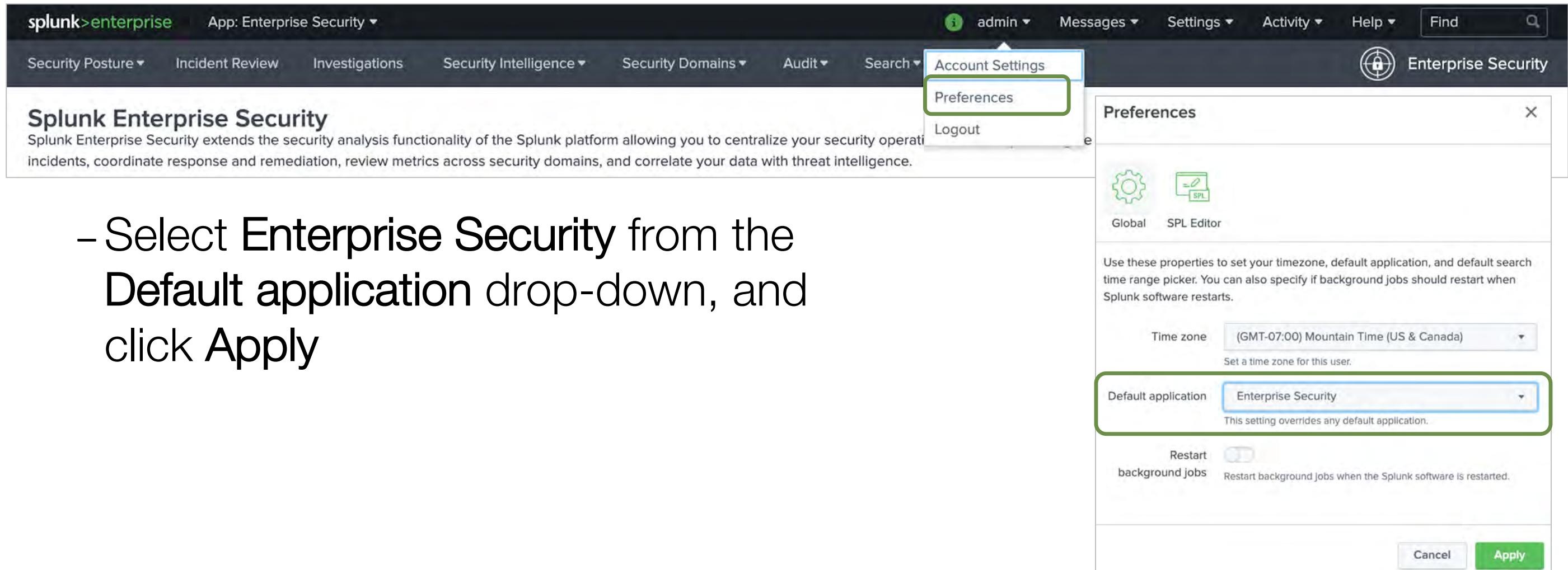
- Access Splunk Web using a URL similar to:
<https://eshostname:8000>
- To access ES a user must have an assigned ES role on the ES server
(`ess_admin`, `ess_analyst`, `ess_user`)
- Once logged on, ES displays in the list of apps on the Splunk home page
 - Apps can be made "visible" in **Manage Apps**. Click **Edit Properties** for an app, and click the **Yes** button for **Visible**



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

Setting ES as the Default App

- Users can configure ES to be the default app to open in Splunk Web
 - Click the username on the top menu bar and select Preferences



The screenshot shows the Splunk Web interface with the 'Enterprise Security' app selected. In the top navigation bar, the 'admin' dropdown is open, and the 'Preferences' option is highlighted with a green box. A modal window titled 'Preferences' is displayed, containing settings for time zone, default application, and background jobs. The 'Default application' dropdown is set to 'Enterprise Security', which is also highlighted with a green box.

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

Module 1 Lab: Overview of Splunk ES

Time: 10 minutes

Tasks:

1. Log on to the lab Splunk server and navigate to the ES home page
2. Change the preferences for the administrator (*admin*) account
3. Examine the source events ES is using to monitor the security environment and notable events

Module 2: Security Monitoring

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

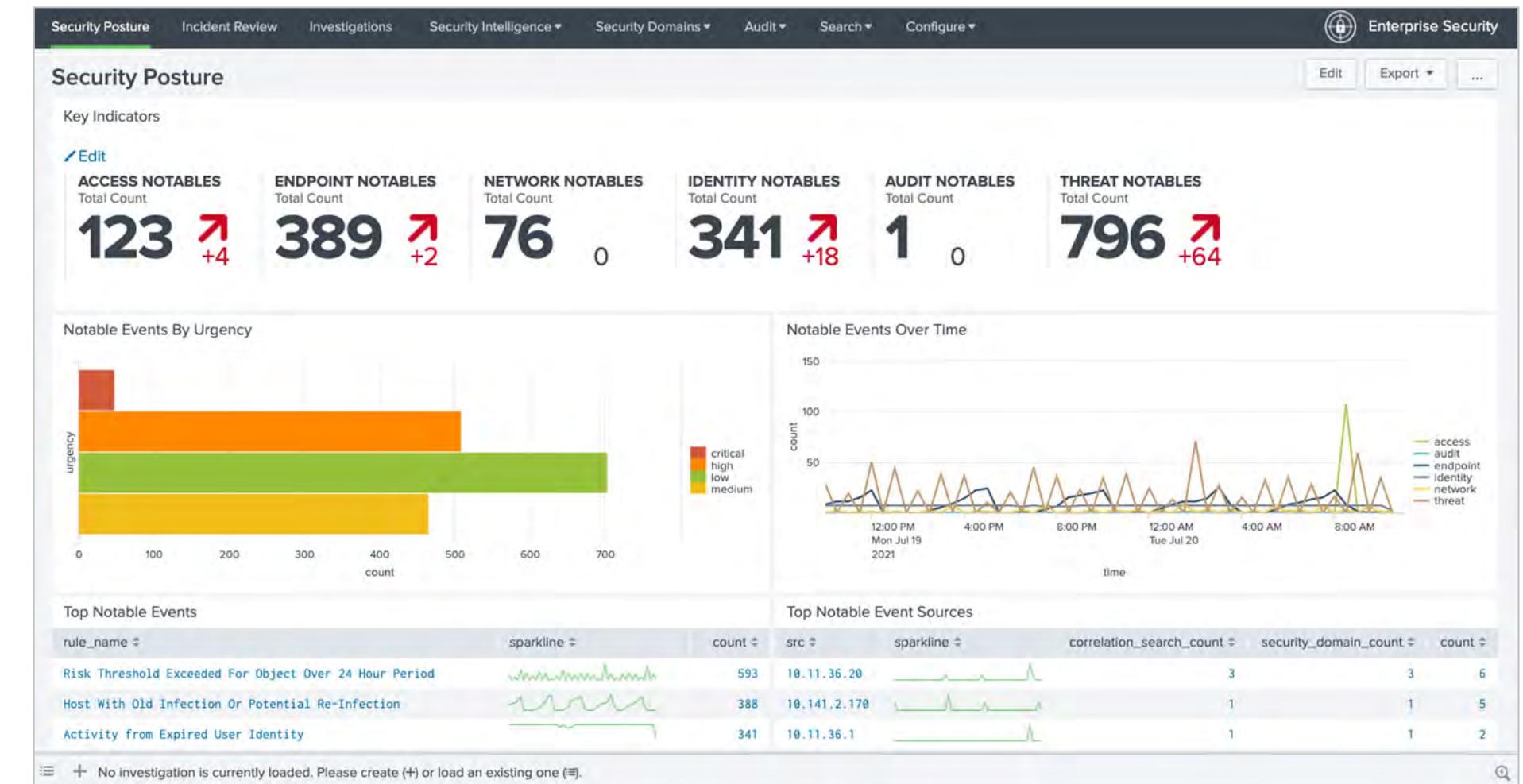
Objectives

- Customize the Security Posture dashboard
- Customize the Incident Review dashboard
- Create ad hoc notable events
- Suppress notable events

Security Posture Dashboard

- Provides an overview of Notable Events

- Key Indicators (KI) at the top provide an at-a-glance view of notable event status over the last 24 hours

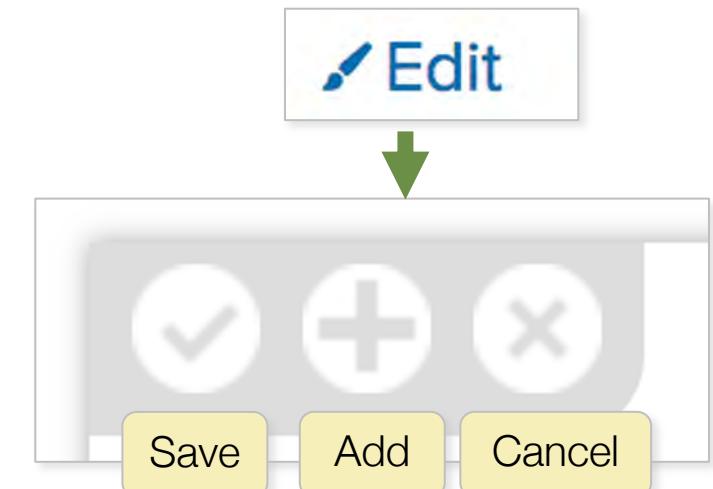
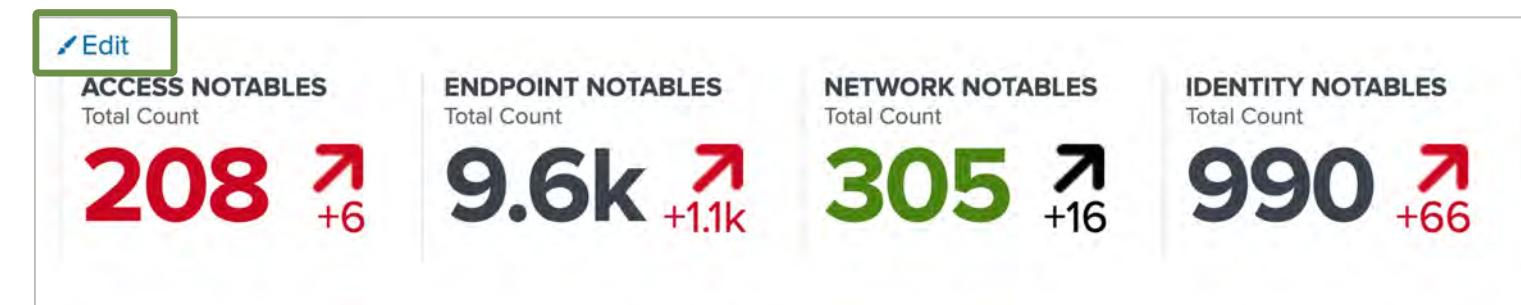


- The four panels provide additional summary information categorized by urgency, time, and most common notable event types and sources

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

Configuring Key Indicators

- Key Indicators (KIs) appear in many ES views
- By default, KIs do not have a threshold set, so the current count is displayed in black
- You can configure thresholds for each KI
 - If the count is above the threshold, the value is shown in red
 - Green indicates a value below the threshold
- You can also re-order, delete, or add KIs
- Click **Edit** to display the edit tools



Editing Key Indicators

Save changes

Drag and drop to re-arrange

The screenshot shows the Splunk Enterprise Security interface for managing Key Indicators (KIs). On the left, there is a horizontal row of six KI cards:

- ACCESS NOTABLES: Total Count 159, +5 (red arrow)
- ENDPOINT NOTABLES: Total Count 593, +83 (red arrow)
- NETWORK NOTABLES: Total Count 181, +32 (red arrow)
- IDENTITY NOTABLES: Total Count 341, +5 (red arrow)
- AUDIT NOTABLES: Total Count 20, -3 (green arrow)
- THREAT NOTABLES: Total Count 151, -54 (green arrow)

Each card has a 'Threshold' input field below it. A yellow callout bubble with a green arrow points to the 'Remove KI from display' link next to the Endpoint Notables card.

A yellow callout bubble with a green arrow points to the 'Drag and drop to re-arrange' text above the cards.

On the right, there is a modal window titled 'Add Indicators' containing a list of available indicators:

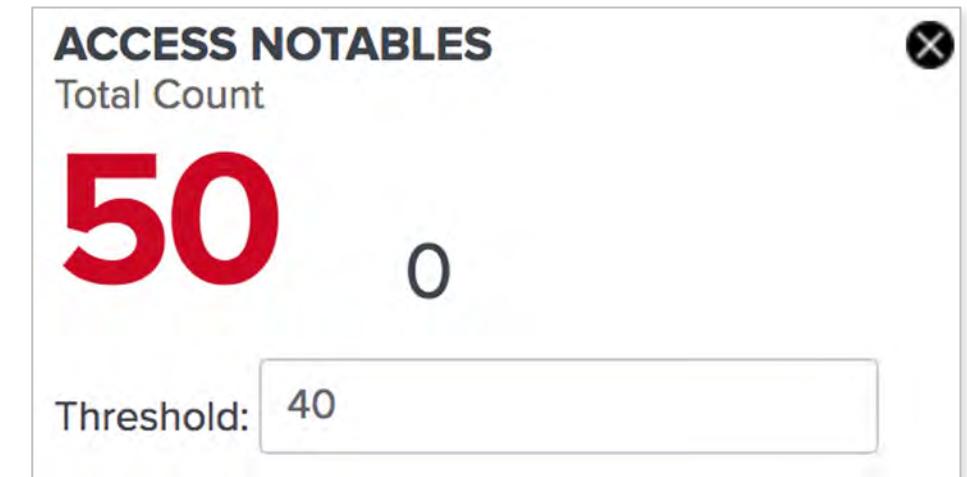
- Access - Distinct Apps
- Access - Distinct Destinations
- Access - Distinct Sources
- Access - Distinct Users
- Access - Number Of Default Accounts In Use
- Access - Total Access Attempts
- Change - Number Of Account Lockouts
- DNS - Errors
- DNS - Messages
- DNS - Query Sources
- DNS - Unique Queries

At the bottom of the modal are 'Close' and 'Add Indicators' buttons. A yellow callout bubble with a green arrow points to the 'Add a new Key Indicator' link at the bottom of the list.

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

Changing KI Thresholds

- You may want to use different threshold values
 - For instance, if you have a very large organization, you may expect a few minor security threats per day, and therefore would want to increase some of the thresholds above their defaults
- Edit the Key Indicator panel
- Enter a value in the Threshold field
- Save the new panel settings



Incident Review Dashboard

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

Search... Hide Charts Hide Filters

Domain Hide the donut charts or filters

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... 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

Notable Events

Actions menu

Expand for details

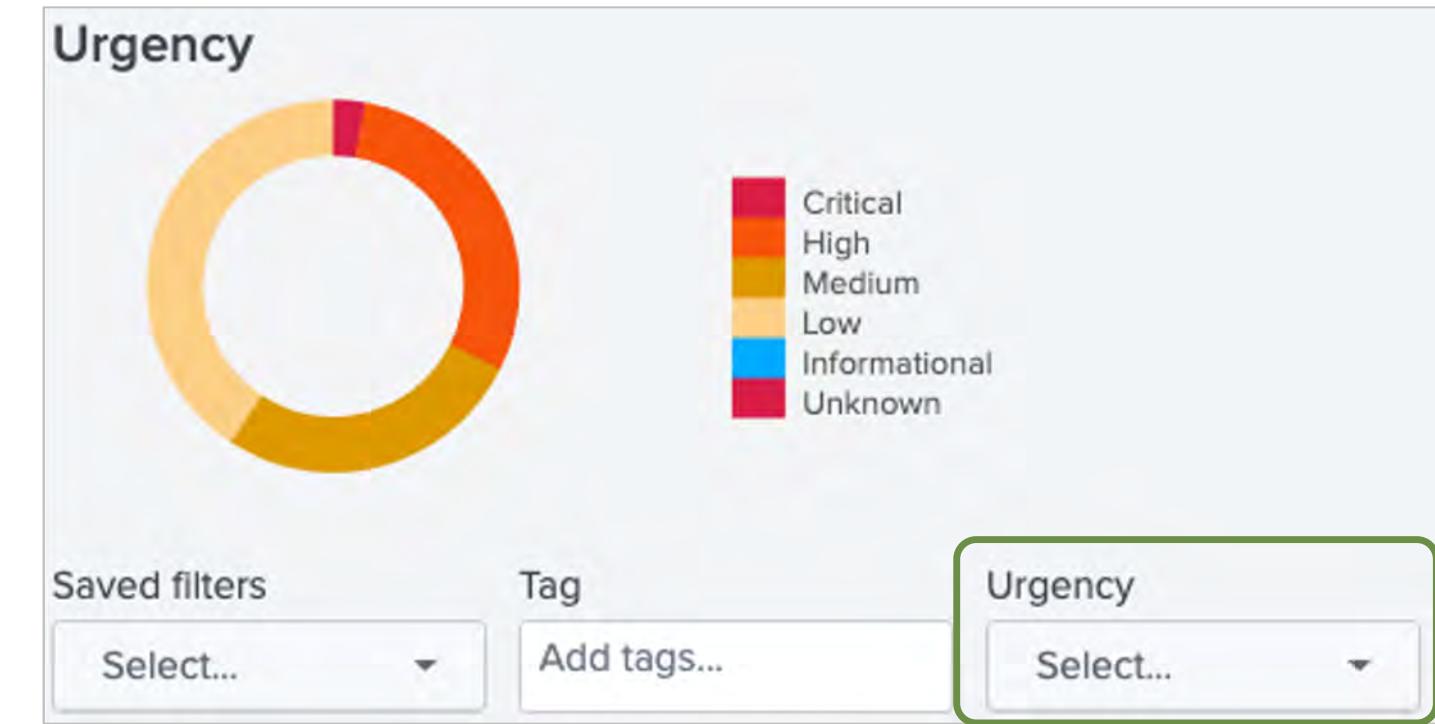
No investigation is currently loaded. Please create (+) or load an existing one (≡).

Investigation bar

#	Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
1	Activity from Expired User Identity (dmsys)	-	--	-	Notable	Today, 5:05 PM	Undetermined	Identity	High	New	unassigned	<input type="button" value="More"/>
2	Host With Old Infection Or Potential Re-Infection (Mal/Packer On ops-sys-003)	-	--	-	Notable	Today, 5:00 PM	Undetermined	Identity	High	New	unassigned	<input type="button" value="More"/>
3	24 hour risk threshold exceeded for user=root	root	600	2	Risk Notable	Today, 5:00 PM	Undetermined	Endpoint	High	New	unassigned	<input type="button" value="More"/>

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

Calculating Urgency

- 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

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

Modifying Urgency Lookup

Configure > Content > Content Management > Managed Lookup > Urgency Levels

- ES Admins can edit the lookup to change the matrix that determines how correlation severity and asset/identity priority combine to set urgency
 - Each row is a combination of severity and priority with the result displaying in the urgency column

1	severity	priority	urgency
2	unknown	unknown	low
3	unknown	low	low
4	unknown	medium	low
5	unknown	high	medium
6	unknown	critical	medium
7	informational	unknown	informational
8	informational	low	informational
9	informational	medium	informational
10	informational	high	informational
11	informational	critical	informational
12	low	unknown	low
13	low	low	low
14	low	medium	low
15	low	high	medium
16	low	critical	medium
17	medium	unknown	low
18	medium	low	low
19	medium	medium	medium
20	medium	high	medium
21	medium	critical	high
22	high	unknown	medium
23	high	low	medium
24	high	medium	high
25	high	high	high
26	high	critical	critical
27	critical	unknown	high
28	critical	low	high
29	critical	medium	critical
30	critical	high	critical
31	critical	critical	critical

Make changes and remember to save!

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

Adding a New Status Value

ES Admins can define new status values and assign values to different roles for both notable events and ES investigations

Configure > Incident Management > Status Configuration

Enterprise Security

Status Configuration

Configure notable event and investigation statuses

< Back to ES Configuration

New

Notable Investigation

filter

End Status designates the label is the final stage of notable examination

Label	End Status	Description	Status
Closed	•	Issue has been resolved and verified.	Enabled Disable
In Progress		Investigation or response is in progress.	Enabled Disable
New (default)		Event has not been reviewed.	Enabled Disable
Pending		Closure is pending some action.	Enabled Disable
Resolved		Issue has been resolved and awaits verification.	Enabled Disable
Unassigned		An error is preventing the issue from having a valid status assignment.	Enabled

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

Editing a Status

- Change the name or description of a status
- Check **Default Status** to make this label the initial status of all notable events
- Check **End Status** to make this label the final status of notable events

Edit Status

Label

Description

Status Type Notable Investigation

Default Status

End Status

Transitions
Select the roles that can transition a notable event from this status to another status. [Learn more](#)

Cancel **Save**

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

Editing Status Transitions

- Change which roles can transition a notable from the selected status to another status
- The example shows the transitions for In Progress
- To restrict users with the `ess_analyst` role from transitioning a notable to Closed from In Progress, uncheck the `ess_analyst` box

Transitions
Select the roles that can transition a notable event from this status to another status. [Learn more ↗](#)

Status	Roles
Unassigned	Select...
New	admin (inherited), ess_admin (inherited), ess_analyst (3)
Pending	admin (inherited), ess_admin (inherited), ess_analyst (3)
Resolved	admin (inherited), ess_admin (inherited), ess_analyst (3)
Closed	admin (inherited), ess_admin (inherited)

Transitions that are imported from an inherited role cannot be edited. This is because the role is being inherited.

admin (inherited)
 ess_admin (inherited)
 ess_analyst
 can_delete
 ess_user
 power
 user
 windows-admin

filter

[Select All](#) [Clear All](#)

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

Adding a New Status

New Status

- Select the **Status Type**. Will this be for notable events or for investigations
- Enter a label and description and configure the status options and transitions
- Remember to save your changes

New Status

Label

Description

Status Type Notable Investigation

Default Status End Status

Transitions

Select the roles that can transition a notable event from this status to another status. [Learn more ↗](#)

Role	Action
Unassigned	Select...
New	Select...
In Progress	Select...
Pending	Select...
Resolved	Select...
Closed	Select...

Transitions that are imported from an inherited role can be removed by disabling the transition for the role that is being inherited.

Cancel Save

Customizing Incident Review

Configure > Incident Management > Incident Review Settings

- **Allow Overriding of Urgency** – allows analysts to change notable urgency (default = on)
- **Comments**
 - **Required** – requires comments when changing status (default = off)
 - **Minimum Length** – sets the minimum length of the comment
- **Default Time Range** – set the default time range used in Incident Review (default is last 24 hours)

Incident Review Settings
Configuration settings for Incident Review.
[Back to ES Configuration](#)

Notable Events

Allow Overriding of Urgency Allows analysts to override and replace the calculated urgency of a notable.

Comments

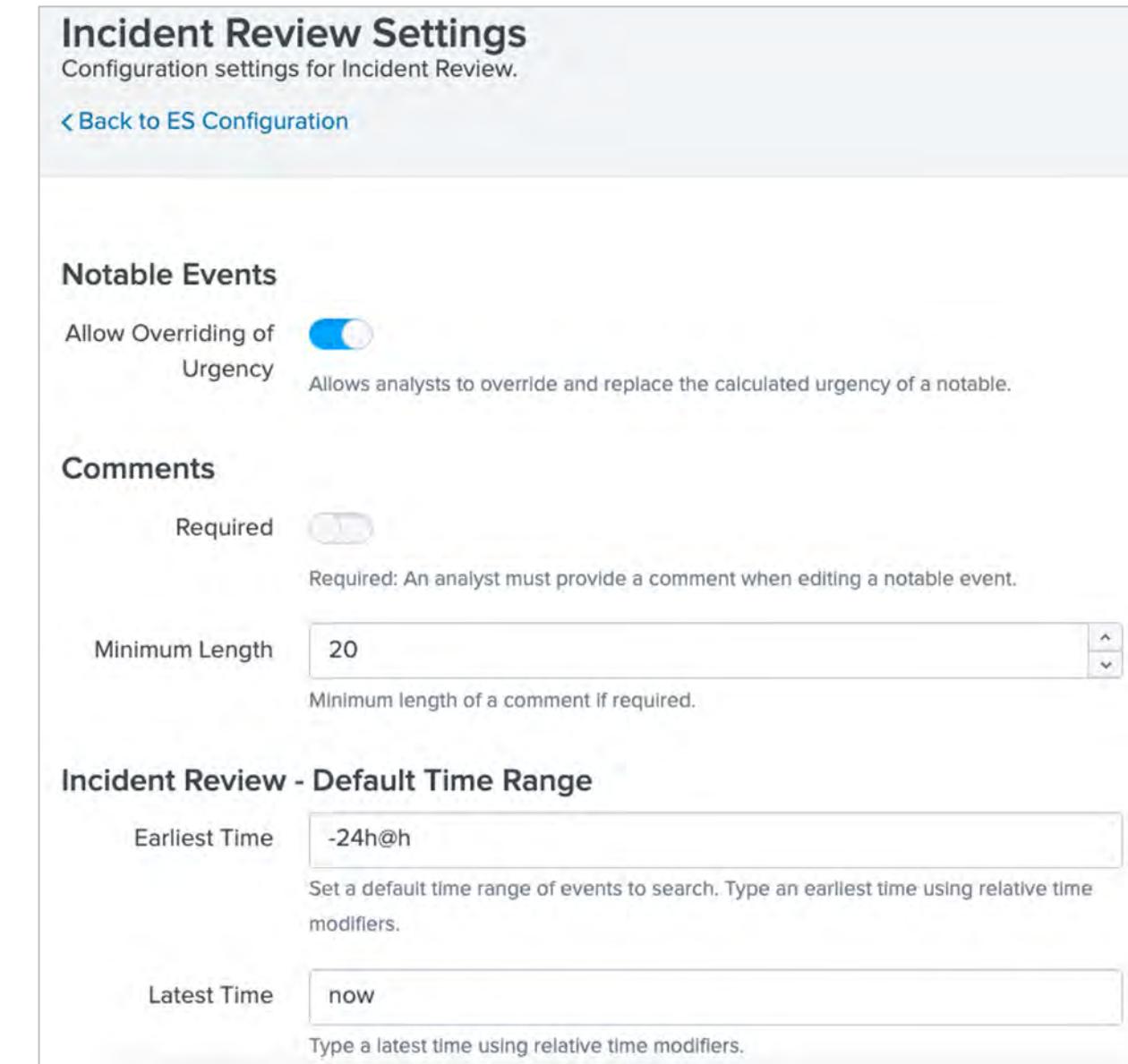
Required Required: An analyst must provide a comment when editing a notable event.

Minimum Length Minimum length of a comment if required.

Incident Review - Default Time Range

Earliest Time Set a default time range of events to search. Type an earliest time using relative time modifiers.

Latest Time Type a latest time using relative time modifiers.



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

Customizing Incident Review (cont.)

Configure > Incident Management >
Incident Review Settings

- Incident Review - Table Attributes
 - Add, remove, or reorder columns in Incident Review
- Incident Review - Event Attributes
 - Add or remove fields that display in notable event details in Incident Review

The screenshot shows the 'Incident Review' configuration page in Splunk. It is divided into two main sections: 'Table Attributes' and 'Event Attributes'.

Incident Review - Table Attributes

Field	Label	X
rule_title	Title	X
risk_object	Risk Object	X
risk_score	Aggregated Risk Score	X
risk_event_count	Risk Events	X
notable_type	Type	X
_time	Time	X
disposition_label	Disposition	X
security_domain	Security Domain	X
urgency	Urgency	X
status_label	Status	X
owner_realname	Owner	X

+ Add Column

Incident Review - Event Attributes

Field	Label	
action	123Action	Edit Remove
app	Application	Edit Remove
bytes_in	Bytes In	Edit Remove
bytes_out	Bytes Out	Edit Remove
category	Category	Edit Remove

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

Add a Column to Incident Review

- Example: display the `src` (IP) field to the right of the **Title** column
 - Under **Table Attributes** click **+ Add Column**
 - Enter `src` for the field and **Source** for the label
 - Use the double ellipsis to move the **Source** field under the **Title** field and click **Save**

1737 Notables [Edit Selected](#) | [Edit All Matching Events \(1737\)](#) | [Add Selected to Investigation](#) [« Prev](#)

<input type="checkbox"/>	<input type="checkbox"/> i	Title	Source	Risk Object	Aggregated Risk Score	Risk Events	Type
		Threat Activity Detected (223.172.48.27)	6.86.15.150	--	--	--	Notable

Incident Review - Table Attributes [?](#)

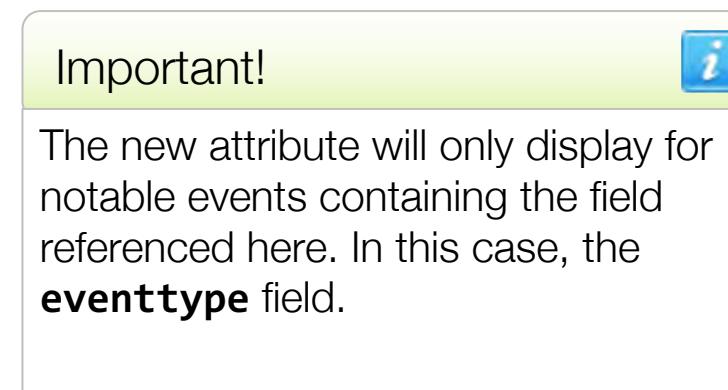
rule_title	Title
src	Source
risk_object	Risk Object
risk_score	Aggregated Risk Score
risk_event_count	Risk Events
notable_type	Type
_time	Time
disposition_label	Disposition
security_domain	Security Domain
urgency	Urgency
status_label	Status
owner_realname	Owner

+ Add Column

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

Add a Field to Event Attributes

- Example: add a field called **Event Type** to events
 - Under **Event Attributes** click **+Add Field**
 - Enter **eventtype** for the field and **Event Type** for the label
 - Click **Edit**



Incident Review - Event Attributes [?](#)

Field	Label	
action	123Action	Edit Remove
app	Edit Event Attribute	X
bytes_in		Move
bytes_out		Move
category		Move
change_id		Move
channel		Move
command		Move
cpu_load		Move
creator	Creator	Edit Remove
creator_realname	Creator Realname	Edit Remove
cve	CVE	Edit Remove

[+ Add Field](#)

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

Add a Field to Event Attributes (cont.)

The new **Event Type** field is added to notable events containing the **eventtype** field

Activity from	--
Expired User	--
Identity (HaxOr)	--
Description:	
Activity from an expired identity was observed. This is indicative of activity from a user whose access should have been disabled.	
Additional Fields	Value
User	HaxOr 17010.0
User Business Unit	americas
User Email	htrapper@acmetech.com
User First Name	hershel
User Identity	haxOr
User Last Name	trapper
User Work City	san francisco

Activity from	--	--	--	Notable	Today, 12:45 PM
Expired User Identity (HaxOr)					
Description:					
Activity from an expired identity was observed. This is indicative of activity from a user whose access should have been disabled.					
Additional Fields	Value	Additional Fields	Value	Action	
User	HaxOr 17010.0	Event Type	modnotable_results		
User Business Unit	americas	User	notable		
User Email	htrapper@acmetech.com	User Business Unit	HaxOr 17010.0		
User First Name	americas	User Email	americas		
User Identity	hershel	User First Name	htrapper@acmetech.com		
User Last Name	hershel	User Identity	hershel		
User Work City	haxOr	User Last Name	haxOr		
		User Work City	htrapper@acmetech.com		
			trapper		
			san francisco		

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

Add a Workflow Action to Incident Review

- Enhances the data available for a field in Incident Review
 - Add a workflow action to a field's Action menu to display workbench specific panel data
 - For example, add a workbench panel called \$dest\$ Installed OS for the Destination field
 - When selected, \$dest\$ Installed OS displays the data for the **workbench_context_os_updates** workbench panel

	Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time
<input type="checkbox"/>	Host With Old Infection Or Potential Re-Infection (unknown On ops-sys-006)	--	--	--	Notable	Today 10:40 AM
Description:						
The device ops-sys-006 was detected with malware 'unknown' that was present 639.9 days ago. This is either an old infection or a re-infection.						
Additional Fields		Value	Action			
Destination		ops-sys-006 3480	▼			
Destination Business Unit		americas	Workbench - Investigate Pass the Ticket Attempts			
Destination Category		pci				
Destination City		dallas	Workbench - Investigate Previous Unseen User			
Destination Country		usa				
Destination Expected		true	Workbench - Investigate Successful Remote Desktop Authentications			
Destination Latitude		32.93127				
Destination Longitude		-96.81816	Workbench - Network Traffic (dest)			
Destination NT Hostname		ops-sys-006	Workbench - Network Traffic (src)			
Destination PCI Domain		trust	Workbench - Risk (risk_object) as Asset			
Destination Requires Antivirus		true				
Destination Should Time Synchronize		true	ops-sys-006 Installed OS			

Workbench Panels

View workbench panels: Configure > Content > Content Management. Filter Type as Panel and filter on *workbench*

The screenshot shows two windows. On the left is the 'Content Management' window, which lists '89 Objects'. A search bar at the top has 'Type: Panel (1)', 'App: All (1)', and 'Status: All'. Below the search bar is a table with columns 'Name', 'Type', and 'Status'. The table contains several rows, with the first row 'workbench_context_os_updates' highlighted. A yellow callout bubble points to this row with the text: 'Click a panel name to view the search behind the panel'. On the right is a modal window titled 'Edit workbench_context_os_updates'. It shows the 'Destination app' as 'Enterprise Security'. Under 'Prebuilt panel XML', the code is:

```
1 <panel>
2   <table>
3     <search>
4       <query>| tstats `summariesonly` latest(_time) as _time, latest("Updates.status") as status from
          datamodel="Updates"."Updates" where ($os_updates_asset_dest_filter$ OR
          $os_updates_identity_user_filter$) by "Updates.dest", "Updates.signature_id", "Updates
          .signature", "Updates.vendor_product" | head 10000 | `drop_dm_object_name("Updates")` | table
          _time, dest, signature_id, status, signature, vendor_product</query>
5     </search>
6     <option name="drilldown">cell</option>
7     <option name="wrap">false</option>
8   </table>
9 </panel>
```

A yellow callout bubble points to the XML code with the text: 'For example, the search behind the **workbench_context_os_updates** panel'. At the bottom right of the modal are 'Cancel' and 'Save' buttons.

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

Create a Workflow Action

To apply a workbench panel to a field's **Action** menu, create a new **Workflow Action**

1. From Splunk Enterprise Settings > Fields > Workflow Actions
2. Click **New Workflow Action**
3. Complete the new workflow action as shown

The screenshot shows the 'Add new' configuration page for a Workflow action. The 'Destination app' is set to 'SplunkEnterpriseSecuritySuite'. The 'Name' field contains 'workflow_computer_inventory', with a note below stating: 'Enter a unique name without spaces or special characters later on within Splunk Settings.' The 'Label' field contains '\$dest\$ Computer Inventory', with a note below stating: 'Enter the label that appears for this action. Optionally in dollar signs, e.g. "Search for ticket number : \$ticket\$"'.

The 'Apply only to the following fields' section has 'dest, destination' selected, with a note below stating: 'Specify a comma-separated list of fields. When fields are specified, the action appears in all field menus.'

The 'Apply only to the following event types' section is empty, with a note below stating: 'Specify a comma-separated list of event types to apply to it.'

The 'Show action in' section has 'Fields menus' selected.

The 'Action type' is set to 'link'.

In the 'Link configuration' section, the 'URI' field contains '/app/\$@namespace\$/ess_workbench_panel?type_asset=\$@field_value\$&panel=workbench_context_computer_inventory&...'. A note below states: 'Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$'. The 'Open link in' dropdown is set to 'New window', and the 'Link method' dropdown is set to 'get'.

At the bottom right are 'Cancel' and 'Save' buttons.

Annotations:

- Name** - for the Workflow action
- Label** - How it will appear in the field **Action** menu. In this example, `<dest name>` Computer Inventory
- Apply only to the following fields** – which fields will display the `<dest name>` Computer Inventory workflow action in Incident Review
- Fields menus** – workflow will appear in the **Action** menu for an **Incident Review** notable event as a **link**
- URI** – composed of tokens and query parameters. Must include the name of the workbench panel.
... `$&panel=workbench_context_computer_inventory&...`

docs.splunk.com/Documentation/ES/latest/Admin/Embeddedworkbench
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Using Workflow Actions

The screenshot shows a Splunk interface for managing risk objects. A specific risk object, "High Or Critical Priority Host With Malware Detected", is selected. The "Description" field indicates a host was detected with malware. The "Additional Fields" table includes various destination-related fields. An "Action" button is highlighted with a green box, and a tooltip says: "From the Destination field Action menu, select the <dest name> Installed OS link". A modal window titled "Embedded Workbench" displays "Latest OS Updates: ACME-003" for the selected host. The table lists three recent updates:

_time	dest	signature_id	status	signature
2021-07-21 11:40:14	ACME-003	KB975562	installed	Security Update for Windows Server 2008 x64 Edition (KB975562)
2021-07-21 13:33:22	ACME-003	KB979559	installed	Security Update for Windows Server 2008 x64 Edition (KB979559)
2021-07-20 21:41:43	ACME-003	KB982535	installed	Microsoft .NET Framework 3.5 SP1 Update for Windows Vista SP1 and Windows Server 2008 for x64-based

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

Creating Ad hoc Notable Events

- `ess_admin` and `ess_analyst` have the capability to create notable events
- Other roles can be given the Create New Notable Events permission

Configure > General > Permissions

Permissions
Assign permissions to edit ES components based on user roles. Administrative roles implicitly have all permissions and cannot be modified. Changes on permissions could take a few minutes to take effect.

[Back to ES Configuration](#)

ES Component	ess_analyst	ess_user
Create New Notable Events Permits the role to create new (ad-hoc) Notable Events. Capabilities: <code>edit_notable_events</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Why create an Ad hoc notable event?

There is an event in Splunk that has not been detected by a correlation search, but you feel it should be investigated

The screenshot shows a Splunk event detail page. At the top right, there is a "Event Actions" dropdown menu with several 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. To the right of the actions, there is a table with event details:

Value
ip-10-0-0-169.us-
/opt/splunk/var/s
snort
Attempted Denia
102.168.1.12

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

Create a Notable Event

Steps:

1. From a Splunk search, expand an event
2. Select **Event Actions**
3. Select **Create notable event**
4. Enter the desired data for the notable event
5. Click **Save**

The screenshot shows a Splunk search results page with an event expanded. An 'Event Actions' dropdown menu is open, with 'Create notable event' selected. A modal window titled 'New Notable Event' is displayed, containing fields for Title, Security Domain, Urgency, Owner, Status, and Description. The 'Title' field is set to 'Snort is not approved on the network'. The 'Security Domain' is set to 'Access', 'Urgency' to 'High', 'Owner' to 'unassigned', and 'Status' to 'New'. The 'Description' field is empty.

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

Suppressing Notable Events

- Event suppression hides notable events from appearing in Incident Review
- It does not change count of notable events on Security Posture or Audit dashboards
- Example suppression: remove events from a group of servers that have been temporarily misconfigured
- By default, only ES Admins have the ability to suppress notable events

Permission to Suppress Events

- Grant users with the `ess_analyst` or `ess_user` role permission to create and edit event suppressions

Configure > General > Permissions > Edit Notable Event Suppressions

Permissions
Assign permissions to edit ES components based on user roles. Administrative roles implicitly have all permissions and cannot be modified. Changes on permissions could take a few minutes to take effect.

[Back to ES Configuration](#)

ES Component	ess_analyst	ess_user
Edit Notable Event Suppressions Permits the role to edit Notable Event Suppressions. Capabilities: <code>edit_suppressions</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Create a Suppression

1. Select Suppress Notable Events from a notable event's Actions menu

2. Set a Suppression Name

3. Optional settings:

- Description
- Suppress To date - if left blank, *all*/future events from the **Selected Fields (host, security, and user)** are suppressed
- Selected Fields, review or click change to add or delete fields

4. Click Save

The screenshot shows a Splunk interface for creating a suppression. At the top, there is a header with columns: Disposition (Undetermined), Security Domain (Identity), Urgency (High), Status (New), Owner (unassigned), and Actions. A green box highlights the 'Actions' button. Below the header, a modal window titled 'Suppress Notable Events' is open. It contains the following fields:

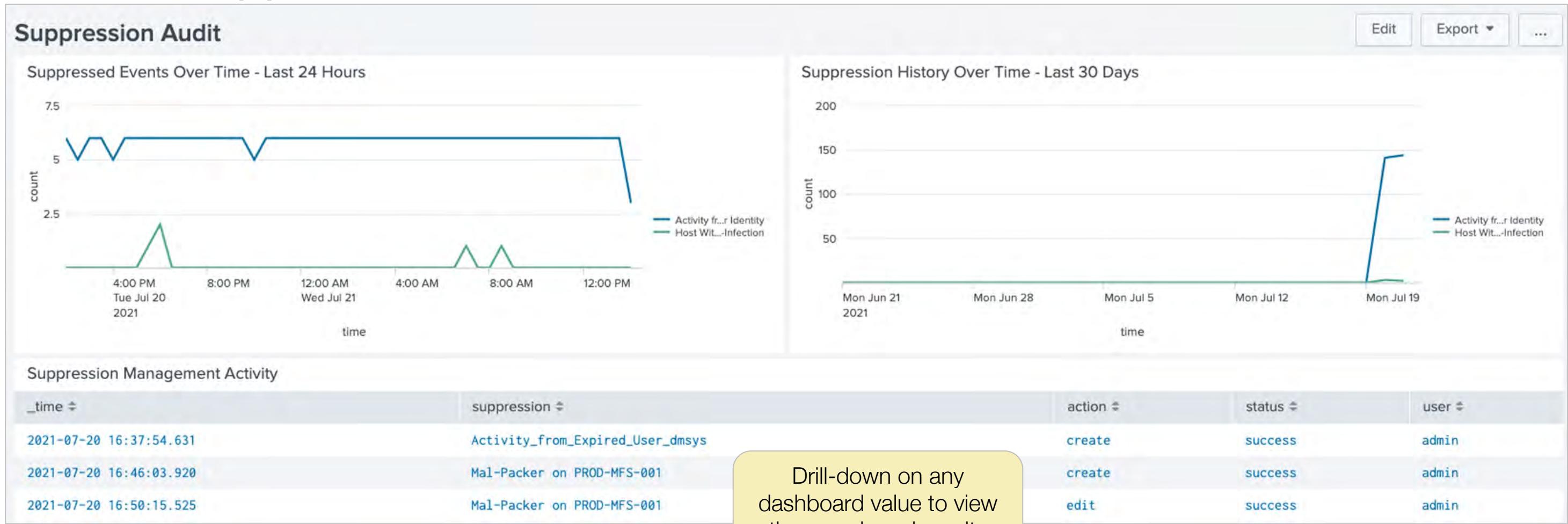
- Suppression Name: Activity_from_Expired_User_dmsys
- Description (optional): User "dmsys" should not be in use.
- Suppress From: 07/20/2021 To 10/31/2021
- Selected Fields: host, security_domain, user (with a note: 'Selected fields with this suppression. change')
- Search Preview: A search preview showing the query: get_notable_index source="Identity - Activity from Expired User Identity - Rule" host="10.10.169.us-west-2.computes.internal" security_domain="Identity" user="dmsys" time>=1626760800 _time<1635660000

At the bottom right of the modal are 'Cancel' and 'Save' buttons, with 'Save' being highlighted by a green box.

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

Suppression Audit

Audit > Suppression Audit



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

Module 2 Lab: Monitoring with ES

Time: 30 minutes

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

Tasks:

1. Use the **Security Posture** dashboard
2. Use the **Incident Review** dashboard to research unauthorized network access
3. Begin working the issue
4. Resolve the issue

Module 3: Risk-Based Alerting

Generated for Splunk University (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 an ES admin can change an object's risk score
- Review the Risk Analysis dashboard
- Describe annotations

Risk Score

- 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
- Risk scores simplify the threat investigation process by helping prioritize suspicious behavior
- ES Admins can configure an object's risk value:
 - by creating an **ad-hoc risk score** for an object in the **Risk Analysis** dashboard
 - by editing the **Risk Analysis** response action in a correlation search
 - by creating a **Risk Factor** under **Content Management**

Generated for Splunk University (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

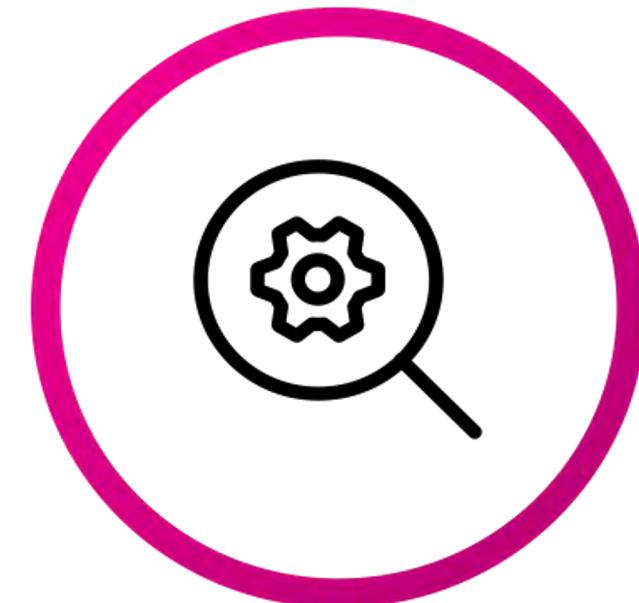


- Abandoned alerts
- Suppressed alerts
- Slow detection / response

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

Risk Framework

Analytics / Correlations



Alerting



Create risk rules to create risk attributions for entities when something suspicious happens. Instead of triggering an alert, risk attributions are sent to the **risk index**

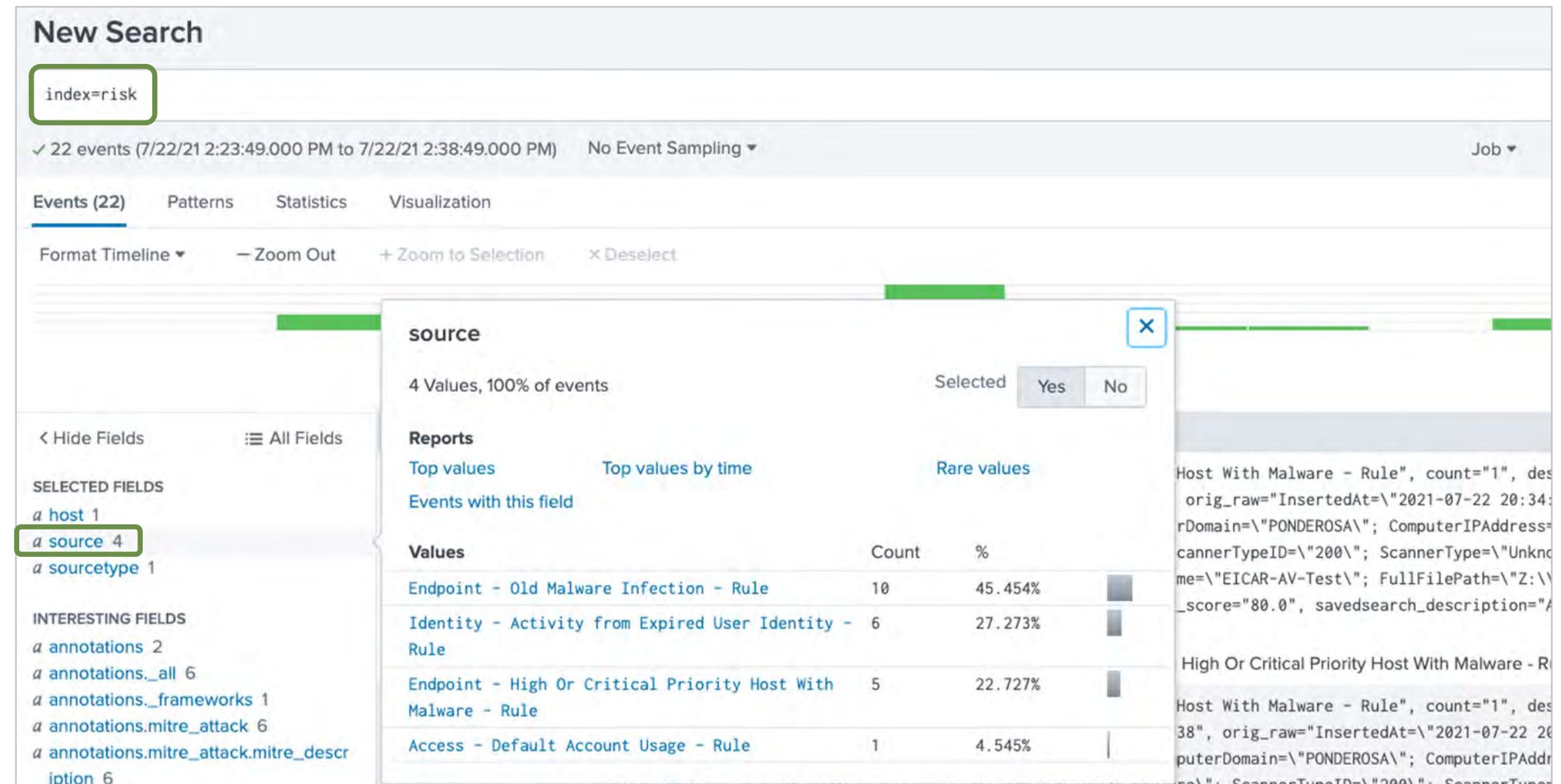
Enrich risk attributions by appending relevant context like a risk score or a MITRE ATT&CK technique

When an entity's risk score or behavioral pattern meets the predetermined threshold, a notable event is triggered

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

Risk Rules

- Risk Rules feed results (risk attributions) into the **risk** index
- Risk Rules are any correlation search that has the **Risk Analysis** adaptive response action configured



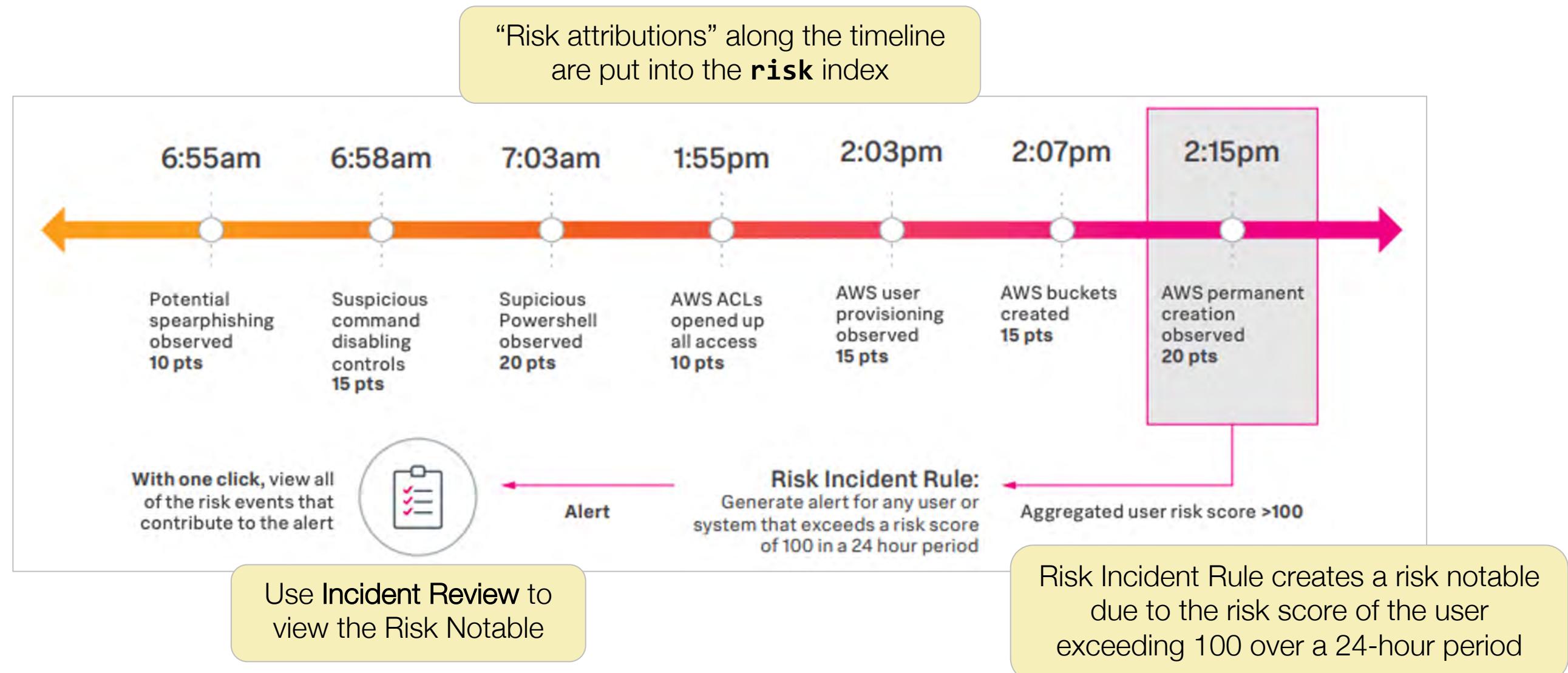
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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
- Create custom Risk Incident Rules to suit your environment

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

The screenshot shows the Splunk Enterprise Security interface under the 'Incident Review' tab. A yellow callout box points to the 'Type' filter dropdown, which is set to 'Risk Notable (1)'. Another yellow callout box points to a risk object row in the table, specifically the 'Risk Object' column which displays 'ip-10-0-0-169.us-west-2.compute.internal'. A tooltip for this field states: 'Fields display risk information for risk objects'.

Filter Incident Review to show only Risk Notables

Type: Risk Notable

Fields display risk information for risk objects

Time	Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Disposition	Security Domain	Urgency	Status	Actions
Today, 3:00 PM	24 hour risk threshold exceeded for system=ip-10-0-0-169.us-west-2.compute.internal	ip-10-0-0-169.us-west-2.compute.internal	120	1	Risk Notable	Undetermined	Threat	Low	New	
Today, 3:00 PM	24 hour risk threshold exceeded for user=dmsys	dmsys				Undetermined	Threat	High	New	
Today, 3:00 PM	24 hour risk threshold exceeded for user=HaxOr	HaxOr	7544	276	Risk Notable	Undetermined	Threat	High	New	
Today, 3:00 PM	24 hour risk threshold exceeded for system=ACME-003	ACME-003	5219	124	Risk Notable	Undetermined	Threat	High	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: 243

Risk Events: 6

Type: Risk Notable

Click Risk Events to view the details

Risk Events

PROD-POS-005

Risk Score: 243.0 | Threshold: 100

Event Count: 6

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

Risk Score: 80

Infection

Infection

Infection

Infection

Infection

Infection

Infection

Click an individual event for the details

Contributing Risk Events

filter

i	Time	Risk Rule	Risk Score	Annotations	Threat Object
>	Today, 1:30 AM	Host With Old Infection Or Potential Re-Infection	80	-	--
>	Today, 1:30 AM	Host With Old Infection Or Potential Re-Infection	80	-	--
>	Today, 1:00 AM	Host With Old Infection Or Potential Re-Infection	80	-	--

Expand for details

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

Risk Objects

- The default risk objects are system, user, and other
- ES Admins can create and edit risk objects to categorize anything as a risk object so it can be assigned a risk score, for example a file or URL
- To add or change objects, edit the **Risk Object Types** lookup under **Content Management**

Configure > Content> Content Management > Managed Lookup

Edit Lookup File / risk_object_types_lookup
Modify the contents of a lookup table.

[< Back to Content Management](#)

1	risk_object_type
2	system
3	user
4	other
5	

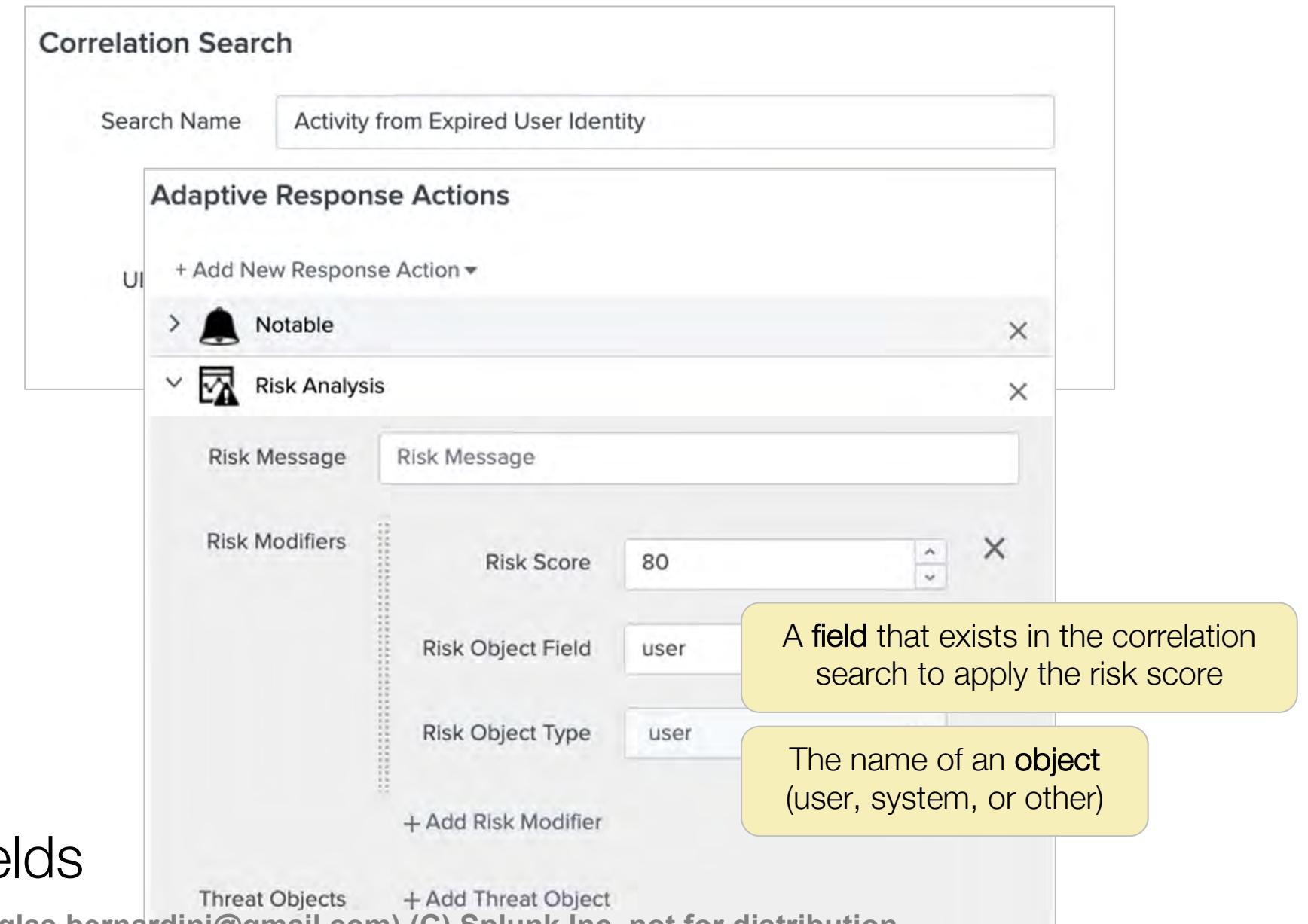
[Cancel](#) [Save](#)

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

Changing Risk – Adaptive Response Action

- Change the risk score for an object in a notable event that is created by a **correlation search**
- From a correlation search, scroll to the bottom to edit the **Risk Analysis** adaptive response action
- Edit the risk score, object field, and object type
- Use the plus sign (+) to add different risk scores to different fields

Configure > Content > Content Management



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

Changing Risk – Ad-hoc Risk Entry

- From the Risk Analysis dashboard, use **Create Ad-Hoc Risk Entry** to change the score of a specific object
- This is a one-time adjustment
- The value entered is added (or subtracted) to/from the object's overall risk score

The screenshot shows the 'Ad-Hoc Risk Score' creation interface. At the top right is a green button labeled 'Create Ad-Hoc Risk Entry'. Below it is a 'Risk Message' input field containing 'admin set risk for HOST-001'. To the right of the message is a yellow callout box with the text 'Add a message'. In the center is a 'Risk Score' input field with the value '500', accompanied by a yellow callout box 'Add a score (positive or negative)'. Below the score is a 'Risk Object' input field with the value 'HOST-001', with a yellow callout box 'Enter the object's name (asset or identity)'. To the right of the object field is a dropdown menu for 'Risk Object Type' with options 'Select...', 'system' (which is highlighted with a blue border), 'user', and 'other'. A yellow callout box next to 'system' says 'Select the object type'. Further down are sections for 'Threat Objects' (with '+ Add Risk Modifier' and 'Threat Object' fields), 'Threat Object Type' (with 'i.e. file_hash'), and 'Annotations' (with '+ Add Threat Object'). At the bottom right are 'Cancel' and 'Save' buttons, with a yellow callout box 'Remember to Save!' positioned between them.

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

Changing Risk - Risk Factors

- Use **Risk Factors** to specify conditions to **dynamically** adjust risk scores for specific objects
 - For example: increase the risk score by a factor of five for a user that is a contractor
- Risk Factors help the risk score to be more precise based on threat
- Adjust risk scores without creating new searches
- Risk Factor configuration is saved in the `risk_factors.conf` file of the SA-ThreatIntelligence app
- Behind the scenes the **Risk Analysis** data model is updated with “factor” calculated fields

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

Risk Factor Example

Configure > Content > Content Management

Risk Factor Editor [Back to Content Management](#)

Find and sort risk factors

Contractor User X

Sort By Name

Show Disabled

5 Contractor User

+ Add Risk Factor

Create a custom risk factor

Enable Enable the risk factor

Name Contractor User

Description Increase the risk when the user is a contractor.

Operation Addition

Determines how to adjust the score of a matching risk modifier. Note: Given multiple matching risk factors, all addition factors will be applied before multiplication.

Factor 5

The value to adjust the risk modifier by. It can be a positive, negative, or decimal number.

SPL PREVIEW

Delete Clone Save Save All

Namespace SA-ThreatIntelligence

Similar Risk Factors Admin User

Matching Risk Events Calculate

View the number of events that match the selected risk factor

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 tab with either the like or regex comparator.

This screenshot shows the Splunk Risk Factor Editor interface. On the left, there's a sidebar with search, sort, and visibility filters. Below that is a list of existing risk factors, with one selected ('Contractor User'). A '+' button for adding new risk factors is also present. In the main panel, the selected risk factor is detailed: it's named 'Contractor User', its description is 'Increase the risk when the user is a contractor.', and its operation is set to 'Addition'. A note below explains that addition factors are applied before multiplication. The 'Factor' field contains the value '5'. An 'SPL PREVIEW' button shows the corresponding SPL code: 'if('user_category'='contractor',5,0)'. On the right, the 'Namespace' is listed as 'SA-ThreatIntelligence'. Under 'Similar Risk Factors', 'Admin User' is shown. Under 'Matching Risk Events', a 'Calculate' button is available. A callout box points to this button with the text 'View the number of events that match the selected risk factor'. At the bottom, 'Conditions' are defined with 'Basic' and 'Advanced' tabs. The 'Basic' tab shows 'Risk Event Field' set to 'user_category' and 'Risk Event Value' set to 'contractor'. A note for the 'Advanced' tab states: 'Value that the Risk Event Field should match. For wildcard matches, use the Advanced tab with either the like or regex comparator.'

Risk Analysis Dashboard

Risk Analysis

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

DISTINCT MODIFIER SOURCES: Source Count 18 ↑ +1

DISTINCT RISK OBJECTS: Object Count 6k ↓ -196

MEDIAN RISK SCORE: Overall Median Risk minimal no change (delta is zero) Currently is: 80

AGGREGATED SYSTEM RISK: Total System Risk minimal ↑ increasing minimally Currently is: 577.7k

AGGREGATED USER RISK: Total User Risk extreme ↑ increasing minimally Currently is: 416.7k

Create Ad-Hoc Risk Entry: minimal no change (delta is zero) Currently is: 1.4k

Risk Modifiers Over Time: Timeline of most active risk-increasing events

Risk Modifiers By Annotations: Annotations effecting risk

Risk Score By Object: Object and risk score

risk_object	risk_object_type	risk_score
unknown	user	2502684.0
unknown	system	1262844.0
dmsys	user	160611.0
Hax0r	user	26263.0

Most Active Sources: Threat - Threat List Activity - Rule

source	risk_objects	count
Threat - Threat List Activity - Rule	9085764.0	25272
	967040.0	12014
	185874.0	2
	215920.0	86

Risk scores by correlation search

source	risk_object	risk_score
dmsys	user	160611.0
Hax0r	user	26263.0

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

Risk Analysis Data Model

- The Risk data model is the data source for the panels on the Risk Analysis dashboard
- Each panel has its own search
- Use the spyglass to view the search behind the panel

44720	491	559
550	544	550
25200	59	420
9920	4	124
4760	48	119
1760	1	22
Open in Search		2 Next »
<input type="button"/>	<input type="button"/>	<input type="button"/>
	1m ago	

```
| tstats summariesonly=false sum(All_Risk.calculated_risk_score) as risk_score,dc(source) as source_count,count from datamodel  
=Risk.All_Risk where * All_Risk.risk_object_type="*" (All_Risk.risk_object="*" OR risk_object="*") by All_Risk.risk_object  
,All_Risk.risk_object_type | `drop_dm_object_name("All_Risk")` | sort 1000 - risk_score
```

Annotations

- Use annotations to enrich correlation search results with the context from industry-standard mappings
- Used as field labels in the **Risk Analysis** dashboard
- Stored in **savedsearches.conf** under **action.correlationsearch.annotations**

For Example:

```
[Identity - Activity from Expired User Identity - Rule]
action.correlationsearch.annotations =
{"mitre_attack": ["T1546.004", "T1003.008", "T1558.004"]}
```

- MITRE ATT&CK definitions pre-populated in:
`$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/lookups/security_framework_annotations.csv`

The screenshot shows the 'Correlation Search' configuration page. The 'Annotations' section is highlighted with a green border. It contains four entries: 'CIS 20', 'Kill Chain', 'MITRE ATT&CK', and 'NIST', each with a text input field labeled 'Type an attribute and press enter'.

Correlation Search

Search Name: Activity From Expired User Identity

App: SA-IdentityManagement

UI Dispatch Context: Enterprise Security

Description: 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).

Mode: Guided

Search: | from datamodel:"Identity_Management"."Expired_Identity_Activity" | stats max(_time) as "lastTime",latest(_raw) as "orig_raw",count by "user"

Annotations

Annotation Type	Value
CIS 20	Type an attribute and press enter
Kill Chain	Type an attribute and press enter
MITRE ATT&CK	Type an attribute and press enter
NIST	Type an attribute and press enter

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

Annotations (cont.)

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

Example industry-standard mappings:

Security Framework	Mapping Examples
Center for Internet Security (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 mitre_attack_lookup lookup definition
National Institute For Standards and Technology (NIST)	PR.IP, PR.PT, PR.AC, PR.DS, DE.AE

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

View Annotation Details

Risk Analysis

Source Risk Object Type Risk Object Time

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

Edit

DISTINCT MODIFIER SOURCES Source Count **17** 0

DISTINCT RISK OBJECTS Object Count **5.8k** -113

MEDIAN RISK SCORE Overall Median Risk **minimal** no change (delta is zero) Currently is: 80

AGGREGATED SYSTEM RISK Total System Risk **minimal** ↑ increasing minimally Currently is: 581.7k

AGGREGATED USER RISK Total User Risk **extreme** ↓ decreasing minimally Currently is: 402k

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

Click an annotation to view details in the Risk data model

Risk Modifiers Over Time

Risk Modifiers By Annotations

Risk Score By Annotations

Recent Risk Modifiers

_time	risk_object	risk_object_type	source	risk_message	risk_score	annotations_all	annotations_frameworks
2021-01-02 11:05:11	ThisISMama	user		Access - Geographically Improbable Access Detected - Rule	80.0	T1021	mitre_attack
2021-01-02 11:05:08	dmsys	user		Identity - Activity from Expired User Identity - Rule	80.0	T1546.010	mitre_attack

Generated for Saptuk University (douglas.born@vt.edu) (C) Saptuk Inc. 2021. All rights reserved.

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

View Annotation Details (cont.)

Events in the Risk Analysis data model show annotation details

New Search

```
| from datamodel:"Risk"."All_Risk" | search risk_object="dmsys" risk_object_type="user"
```

✓ 6 events (1/2/21 11:07:30.000 AM to 1/2/21 11:22:30.000 AM) No Event Sampling ▾

Events (6) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

◀ Hide Fields ▪ All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a annotations 1
- a annotations_all 5
- a annotations_frameworks 1
- a annotations_mitre_attack 5
- a annotations_mitre_attack.mitre_description 5

Click “annotation” fields to view details such as description or which platforms a MITRE ATT&CK-pattern applies to

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

Save As ▾ Close

annotations.mitre_attack.mitre_description

X

Selected Yes No

5 Values, 100% of events

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Adversaries may attempt to dump the contents of <code>/etc/passwd</code> and <code>/etc/shadow</code> to enable offline password cracking.	6	100%
Most modern Linux operating systems use a combination of <code>/etc/passwd</code> and <code>/etc/shadow</code> to store user account information including password hashes in <code>/etc/shadow</code>. By default, <code>/etc/shadow</code> is only readable by the root user. (Citation: Linux Password and Shadow File Formats) The Linux utility, unshadow, can be used to combine the two files in a format suited for password cracking utilities such as John the Ripper: (Citation: nixCraft - John the Ripper) <code># /usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db</code>	008\", \"T1558.00	
	"T1557.002", ann	
	3.008", annotati	
	ty", info_min_ti	
	ucceeded for roo	
	ered from a user	
	008\", \"T1558.00	
	"T1557.002", ann	
	3.008", annotati	
	ty". info_min ti	

Risk Permissions

ES Admins can give `ess_analyst` or `ess_user` the ability to edit the Risk Analysis adaptive response action, or manage Risk Factors by giving the role the following permissions

Configure > General > Permissions

ES Component	ess_analyst	ess_user
Edit Correlation Searches Permits the role to edit Correlation Searches.	<input type="checkbox"/>	<input type="checkbox"/>
Edit Risk Factors Permits the role to edit risk factors.	<input type="checkbox"/>	<input type="checkbox"/>

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

Module 3 Lab: Risk-Based Alerting

Time: 15 minutes

Scenario:

Tasks:

1. Use the Incident Review dashboard to review Risk Notable details including MITRE ATT&CK tactics and techniques
2. Examine the Risk Incident Rules (correlation searches) creating the Risk Notables

Module 4: Incident Investigation

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

Objectives

- Review the Investigations dashboard
- Customize the Investigation Workbench
- Give an overview of the Investigation Workbench
- Assign collaborators and update the status of an investigation

Investigations

- By default, only `ess_admin` and `ess_analyst` have permission to start investigations
- `ess_analyst` can only manage investigations they have created
- `ess_admin` can manage all investigations
- `ess_user` cannot view or manage investigations
- Give permission to roles to manage investigations

Permissions

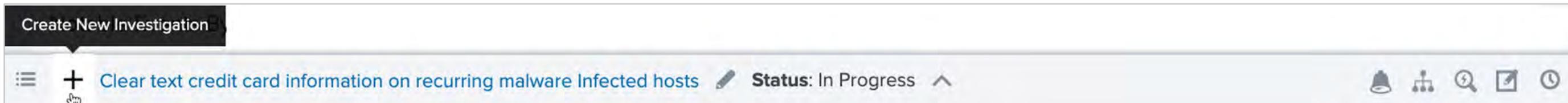
Assign permissions to edit ES components based on user roles. Administrative roles implicitly have all permissions and cannot be modified. Changes on permissions could take a few minutes to take effect.

[Back to ES Configuration](#)

ES Component	ess_analyst	ess_user
Manage All Investigations Permits the role to read/write all investigations.	<input type="checkbox"/>	<input type="checkbox"/>
Manage Your Investigations Permits users with this role to read/write investigations on which they collaborate.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Investigations (cont.)

- An investigation has an owner and any number of collaborators
 - Owners and collaborators can work and modify the investigation
 - Any user that has been granted the `manage_all_investigations` permission by an ES admin can add an event to an open investigation, even if they are not an owner or collaborator on the investigation
- Ways to start an investigation:
 - from the **Incident Review** dashboard **Actions** menu
 - on the **Investigations** dashboard
 - when searching raw events, from the **Event Actions** menu
 - Using the **Investigation Bar** at the bottom of ES windows



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

Investigations Dashboard

Lists all investigations

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

Investigations
Track and manage investigations

Create New Investigation

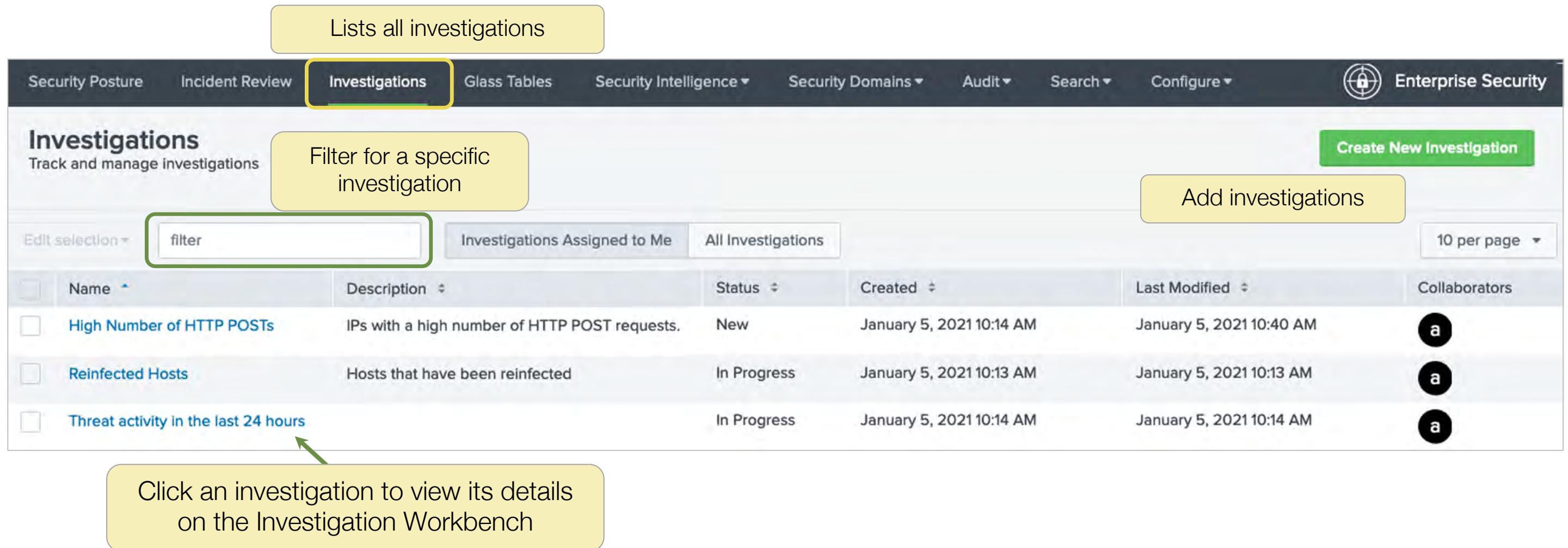
Filter for a specific investigation

Add investigations

filter Investigations Assigned to Me All Investigations 10 per page ▾

Name	Description	Status	Created	Last Modified	Collaborators
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	a
Reinfected Hosts	Hosts that have been reinfected	In Progress	January 5, 2021 10:13 AM	January 5, 2021 10:13 AM	a
Threat activity in the last 24 hours		In Progress	January 5, 2021 10:14 AM	January 5, 2021 10:14 AM	a

Click an investigation to view its details on the Investigation Workbench



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 5, 2021 10:14 AM
Last Modified January 5, 2021 10:48 AM
Status New

[Edit](#) [Print](#) [Download](#)

[Back to Investigations](#)

[Workbench](#) [Timeline](#) [Summary](#)

Time range [+ a](#)

Using suggested time range:
Between December 15, 2020 1:50 PM and January 6, 2021 9:50 AM

[Custom time](#)

Tabs

Artifacts

1 22 out of 22 are selected.
[Clear selected.](#)

Filter artifacts

All Identities Assets

1 Select Artifact(s)

2 Use Explore to add selected artifacts to the workbench

+ Add Artifact [Explore](#)

Risk Scores

1 Gain context into the investigated artifacts associated with this investigation.

IDS Alerts

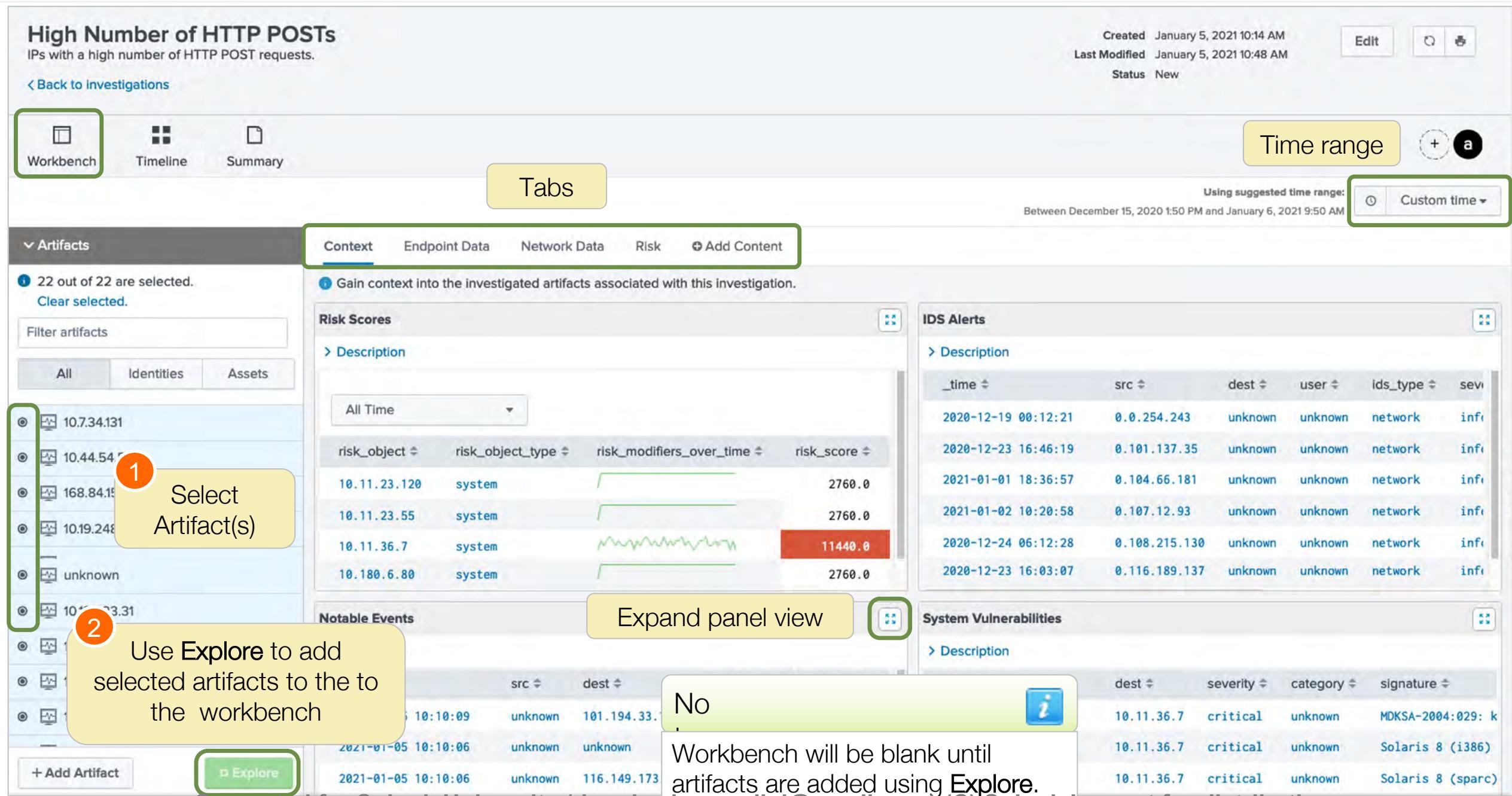
Notable Events

System Vulnerabilities

Expand panel view

No

Workbench will be blank until artifacts are added using Explore.



Workbench Tabs & Panels

The screenshot shows the Splunk Workbench interface for investigating a 'High Number of HTTP POSTs' alert. The top navigation bar displays the title 'High Number of HTTP POSTs' and a subtitle 'IPs with a high number of HTTP POST requests.' Below the title is a link '[Back to investigations](#)'. The main navigation bar includes three tabs: 'Workbench' (selected), 'Timeline', and 'Summary'. A secondary navigation bar at the bottom includes 'Artifacts' (selected), 'Context' (highlighted with a green border), 'Endpoint Data', 'Network Data', 'Risk', and a '+ Add Content' button.

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

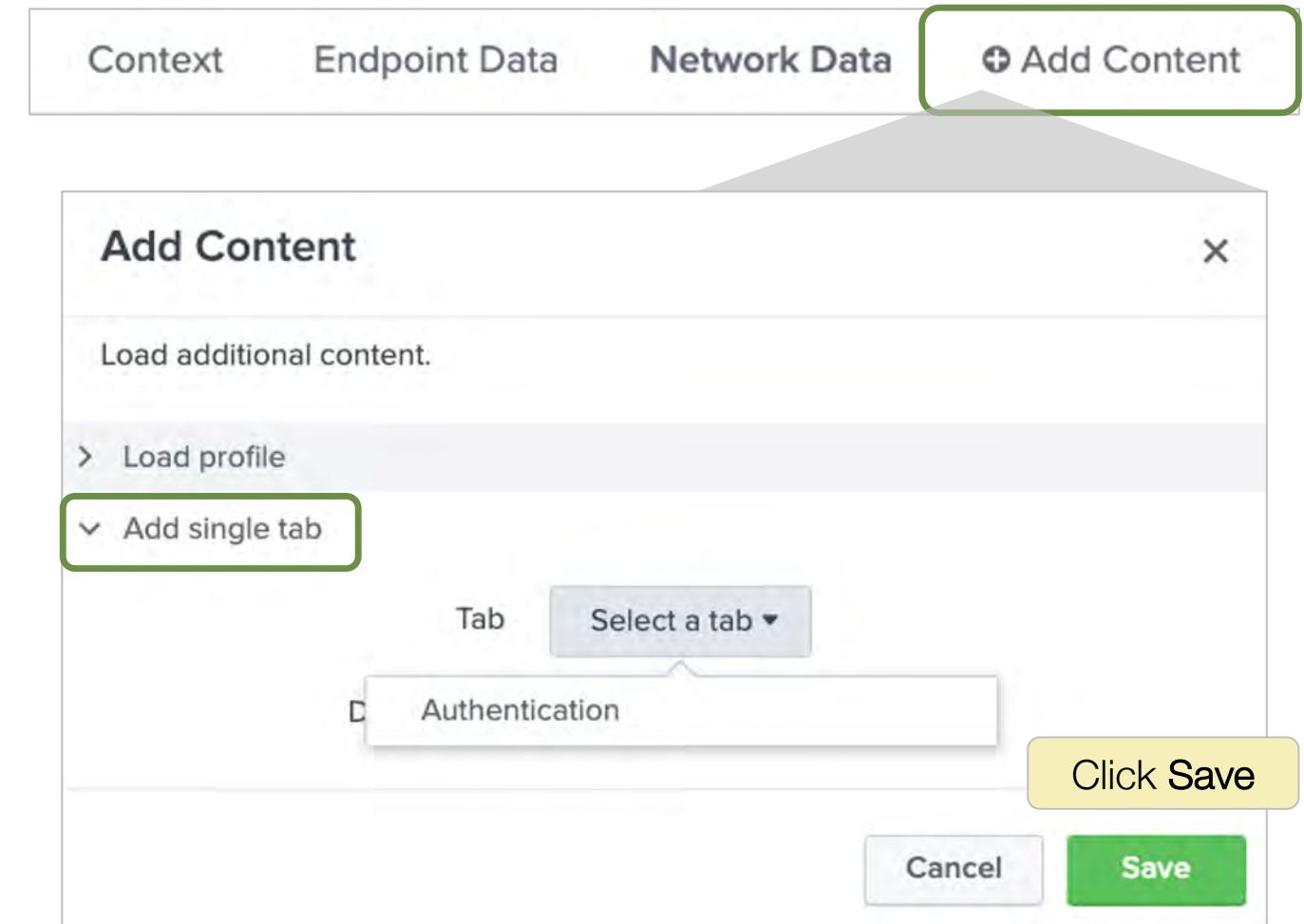
Add a Tab to the Investigation

- 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

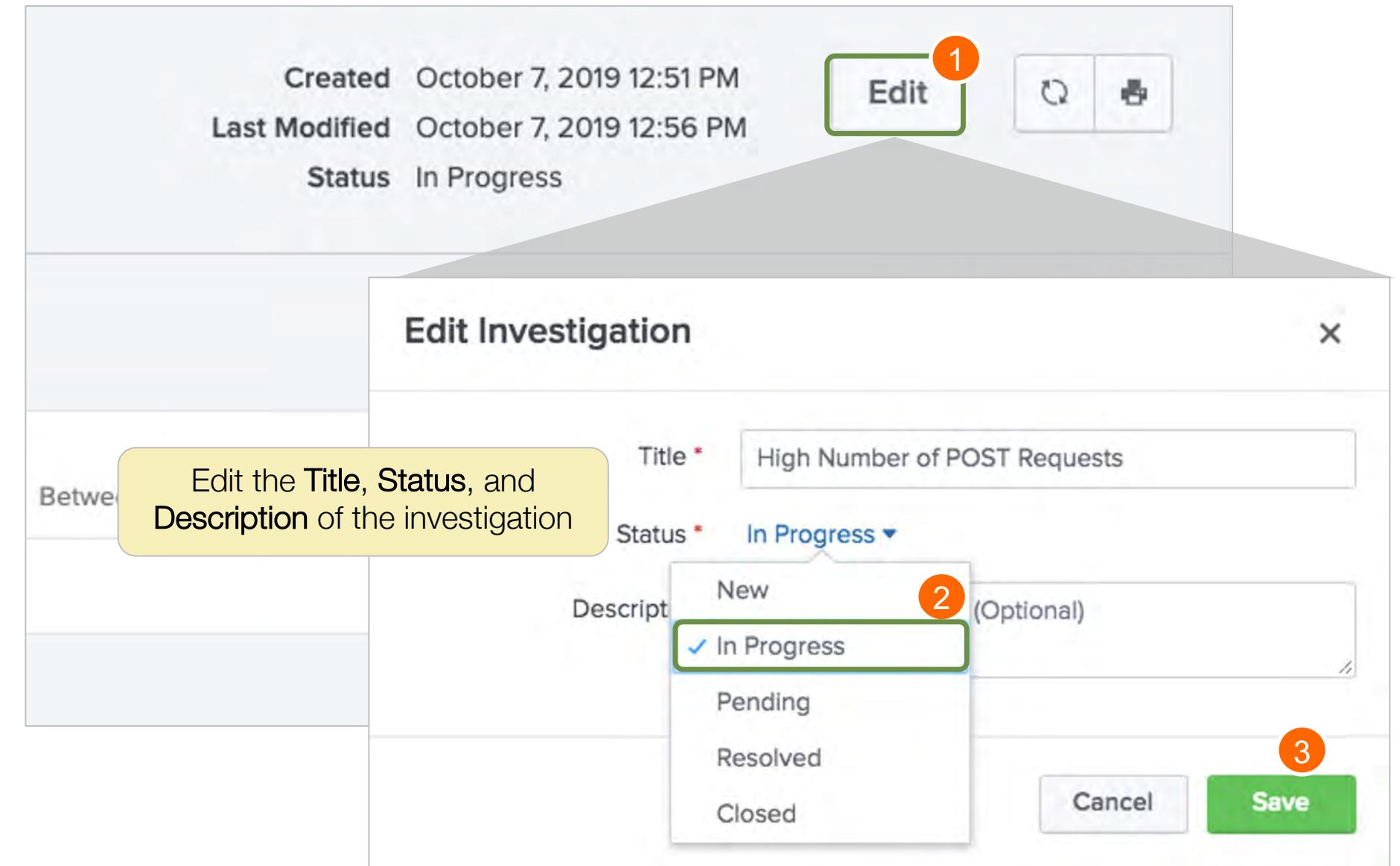
- By default, the tabs do not persist, you must add them each time you view the investigation



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

Update 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

Add Collaborators to an Investigation

The screenshot shows the Splunk Enterprise Security interface for managing an investigation titled "High HTTP Post Requests".

Top Bar: Shows the investigation title "High HTTP Post Requests", a "Back to investigations" link, and three navigation tabs: "Workbench" (selected), "Timeline", and "Summary".

Left Sidebar: Displays an "Artifacts" section with a note: "20 out of 20 are selected." and a "Clear selected" link.

Center Content: An "Edit Collaborator" dialog is open, showing the "User" field set to "admin" and the "Name" field set to "Administrator". Below these fields is a "Write Permission" section with "Yes" and "No" buttons. A yellow callout box points to this section with the text: "Select a user to change write permissions or remove as a collaborator". At the bottom of the dialog are "Remove" and "Done" buttons.

Right Sidebar: Shows investigation metadata: Created October 5, 2019, Last Modified October 7, 2019 at 12:56 PM, and Status In Progress. It also displays a list of collaborators under the heading "Administrator". A yellow callout box points to the "A" button with the text: "Hover over a collaborator to view the name, or click to edit". Another yellow callout box points to the "+" button with the text: "Click to add a collaborator". A search bar labeled "filter" is present. Two users are listed: "instructor" (unchecked) and "sr_analyst" (checked).

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

Investigation Overview Dashboard

Audit > Investigation Overview

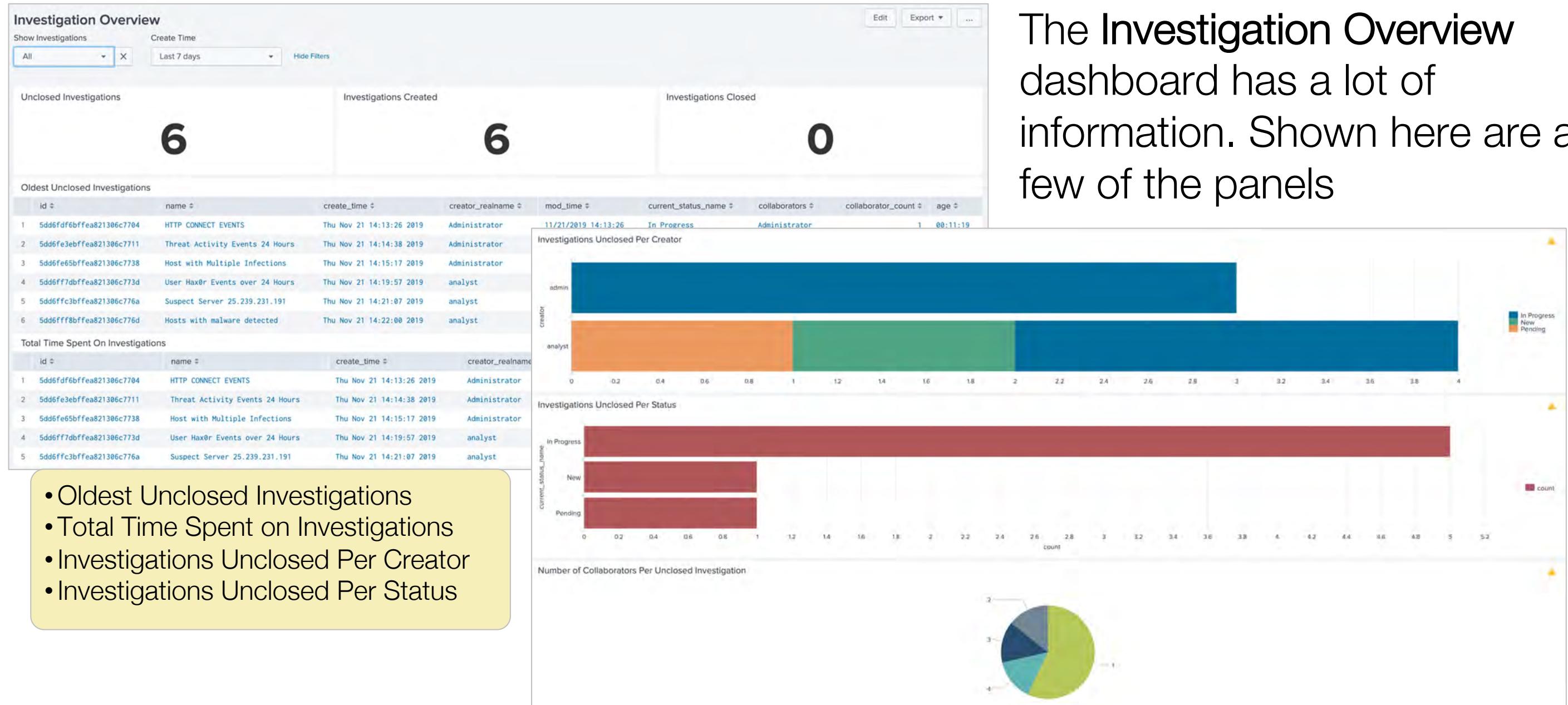
- Dashboard gives insight into investigations
 - Monitoring open investigations
 - Shows time to completion
 - Displays the number of collaborators
- ES analyst can only see investigations they created by default
- ES users will not see any data on the Investigations dashboard
- Give users one of the manage investigation permissions

Configure > General > Permissions

ES Component	ess_analyst	ess_user
Manage All Investigations Permits the role to read/write all investigations.	<input type="checkbox"/>	<input type="checkbox"/>
Manage Your Investigations Permits users with this role to read/write investigations on which they collaborate.	<input type="checkbox"/>	<input type="checkbox"/>

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

Investigation Overview Dashboard (cont.)



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

Customizing the Workbench

- ES admins can customize the **Investigation Workbench** by:
 - Creating new types of panels and tabs
 - Creating investigation profiles that correspond to specialized investigation types
 - Applying profiles to notable events from correlation searches
- Example:

Create workbench tab named **IDS / IPS Activity** that displays detailed information on panels focused on **Cisco Sourcefire** activity. The tab will not display by default, analyst will have to add this content to the investigation manually

docs.splunk.com/Documentation/ES/latest/Admin/Customizeinvestigations

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

Creating Workbench Panels

- Add pre-defined panels to be used in a new Investigation Workbench tab
 - Follow this process for each panel you want to display in the new tab

Configure > Content > Content Management

The screenshot shows the Splunk Content Management interface. A modal window titled "New Workbench Panel" is open, prompting the user to enter panel details. The "Panel Name" field contains "Cisco Sourcefire - Severity by Dest IP". The "App" dropdown is set to "Enterprise Security". The "Label" and "Description" fields are empty. A "Tokens" section with an "Add Token" button is present. In the background, the main Content Management page lists various objects, including several "Abnormally High" entries and an "Access - Access App Tracker - Lookup Gen" entry. A sidebar on the right lists content types: Panel, Saved Search, Search-Driven Lookup, Sequence Template, Swim Lane Search, View, Workbench Panel (which is highlighted with a green border), Workbench Profile, and Workbench Tab.

Select a pre-defined panel from the **Panel Name** drop-down, select Enterprise Security as the App.

Optional, define a **Label** to replace the default panel title on the workbench, and **Description** of the panel data.

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

Adding Workbench Panels (cont.)

- Add one or more tokens to the panel search to limit the search results to the artifacts investigated on the workbench
- Use multiple tokens to substitute more than one type of artifact

New Workbench Panel

Panel Name: Cisco Sourcefire - Severity by Dest IP

Label: Cisco Sourcefire - Severity by Dest IP

App: Enterprise Security

Description:

Tokens:

Add a token to replace the token in the panel search.

Cancel Save

New Workbench Panel

Enter a Token Name in the format of \$token\$.

Token Name: \$dest\$

Prefix:

Suffix:

Value Prefix:

Value Suffix:

Delimiter:

Default:

Type: Asset

Choose the Type: Notable Event, Investigation ID, Asset, Identity, File, or URL.

Is Null

Is Null

Preview

Available Artifacts: 0 | 1 | 2+

Token Value: <Asset_Value_1>

Cancel Apply

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

Adding a Workbench Profile

Add a profile to display a specific set of tabs and panels

The screenshot shows the Splunk Content Management interface for creating a new Workbench Profile. The main area displays a modal window titled "New Workbench Profile". Inside the modal, there are fields for "Profile Name" (set to "Intrusion Detection"), "App" (set to "Enterprise Security"), and optional fields for "Label" and "Description". A large yellow callout points to the "App" field with the instruction: "Select Enterprise Security as the App.". Another yellow callout points to the "Label" field with the instruction: "Optional, enter a Label if you want the profile tab to named something different than the profile name.". A third yellow callout points to the "Description" field with the instruction: "Optional, enter a Description of the profile.". The background shows a list of objects and a sidebar with various content types.

Content Management
Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, and reports.

< Back to ES Configuration

2122 Objects Edit selection Type: All (1)

New Workbench Profile

Profile Name: Intrusion Detection

App: Enterprise Security

Optional Fields

Label: Intrusion Detection

Description:

Select Enterprise Security as the App.

Cancel Save

Risk Factor
Saved Search
Search-Driven Lookup
Sequence Template
Swim Lane Search
View
Workbench Panel
Workbench Profile **Workbench Profile**
Workbench Tab

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

Adding a Workbench Tab

The screenshot shows the Splunk interface with the 'Content Manager' page open. A modal window titled 'New Workbench Tab' is displayed, prompting the user to enter a tab name ('IDS / IPS Activity') and select an app ('Enterprise Security'). The 'Optional Fields' section includes fields for 'Label' (set to 'IDS / IPS Activity'), 'Workbench Profile' (set to 'Intrusion Detection'), and 'Workbench Panels' (listing four Cisco Sourcefire panels). The 'Load By Default' field has 'True' selected. The 'Description' field is empty. At the bottom are 'Cancel' and 'Save' buttons.

New Workbench Tab

Tab Name: IDS / IPS Activity

App: Enterprise Security

Optional Fields

Label: IDS / IPS Activity

Workbench Profile: Intrusion Detection

Workbench Panels:

- Cisco Sourcefire - Activity by Dest
- Cisco Sourcefire - Activity by Severity
- Cisco Sourcefire - Severity by Dest IP
- Cisco Sourcefire - Severity by Src IP

Load By Default: True

Description:

Cancel Save

Content Manager
Manage knowledge
< Back to ES Configuration

2122 Objects Edit selection

Type: All (1) App:

- Name
- Abnormally High
- Abnormally High Number of HTTP Method Events By Src
- Access - Access
- Access - Access
- Access - Access
- Access - Access

Risk Factor

Saved Search

Search-Driven Lookup

Sequence Template

Swim Lane Search

View

Workbench Panel

Workbench Profile

Workbench Tab

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

Displaying a Workbench Profile

The screenshot illustrates the process of creating and selecting a new profile in Splunk Workbench. It consists of two main panels:

- Left Panel (Workbench View):** Shows a search titled "High Number of HTTP POSTs" for IPs with a high number of HTTP POST requests. The interface includes tabs for Workbench, Timeline, and Summary, and sub-tabs for Artifacts, Context, Endpoint Data, Network Data, Risk, and Add Content. A callout box highlights the "Add Content" button.
- Right Panel (Add Content Dialog):** A modal window titled "Add Content" with the sub-section "Load profile". It shows a "Profile" tab selected and a dropdown menu "Select a profile" set to "IDS / IPS Activity". Another callout box highlights this selection. The dialog also includes a "Cancel" and "Save" button.

A large callout box on the left panel contains the following text:

Click Add Content and select the newly created profile. The new IDS/IPS Activity tab is displayed with the configured panels.

The bottom section of the screenshot shows the final state where the "IDS / IPS Activity" tab is selected in the Workbench, displaying two panels: "Cisco Sourcefire - Severity by Dest IP" (a world map with colored dots) and "Cisco Sourcefire - Activity by Dest" (a line chart showing activity over time).

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

Module 4 Lab: Customizing the Investigation Workbench

Time: 30 minutes

Scenario: Customize the investigation workbench to add a new workbench tab to view data specific to Cisco Sourcefire

Tasks:

1. Add a tab called *IDS / IPS Activity* that displays detailed information on panels focused on Cisco Sourcefire activity
2. View the newly created tab and panels in an investigation

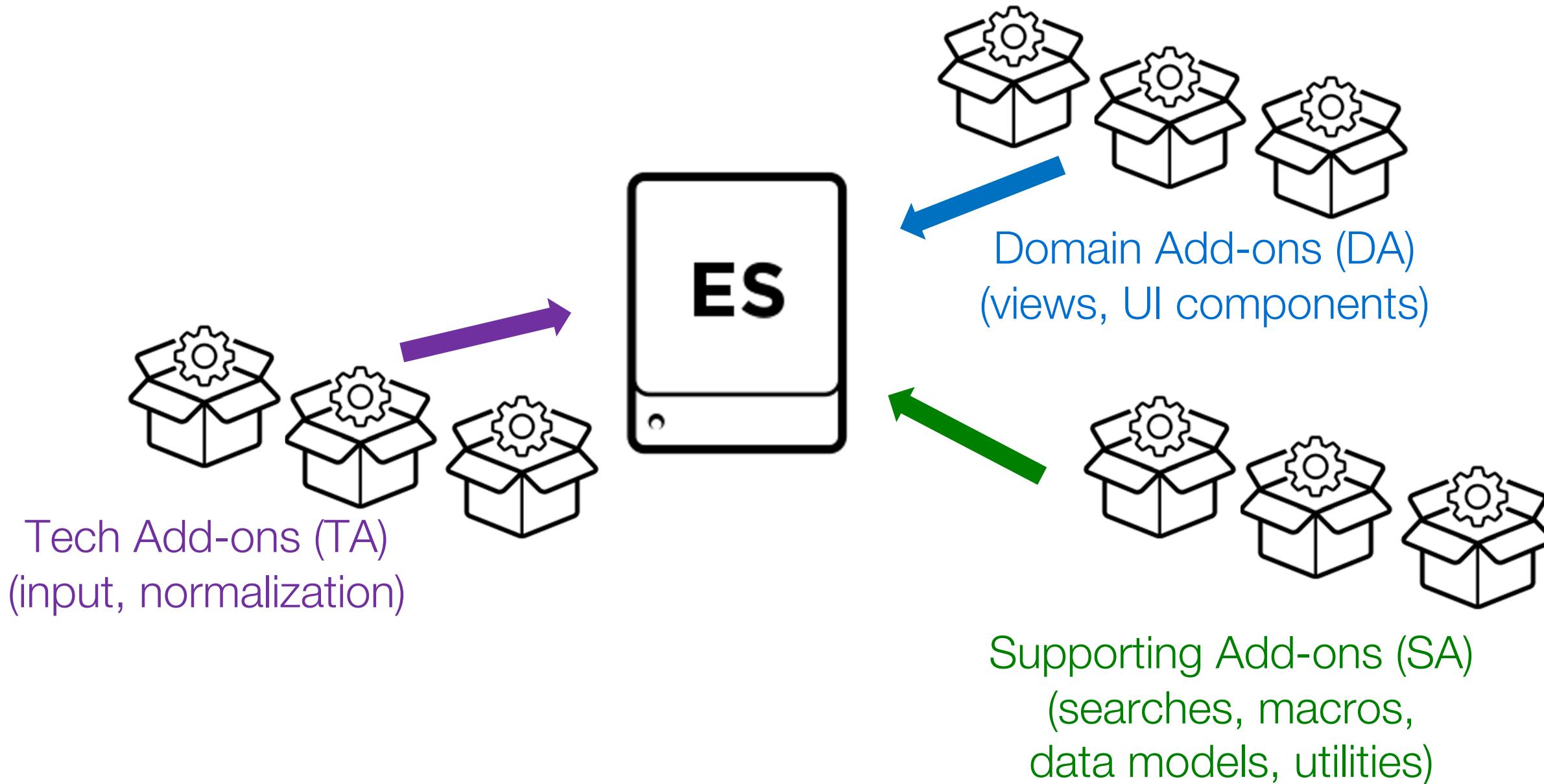
Module 5: Installation

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

Objectives

- Explain the different add-ons and where they are installed
- List ES pre-installation requirements
- Identify steps for downloading and installing ES
- Describe the Splunk_TA_ForIndexers app and where it is installed

ES App and Add-ons



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

ES Included Add-ons

These add-ons are distributed with the ES installer and are only required to be on Splunk search heads. Generally, you will not need to edit any of their configuration files directly; most settings are available via the admin user interface

Main ES Application

- SplunkEnterpriseSecuritySuite

Domain add-ons

- DA-ESS-AccessProtection
- DA-ESS-EndpointProtection
- DA-ESS-IdentityManagement
- DA-ESS-NetworkProtection
- DA-ESS-ThreatIntelligence

Supporting add-ons

- SA-AccessProtection
- SA-AuditAndDataProtection
- SA-EndpointProtection
- SA-IdentityManagement
- SA-NetworkProtection
- SA-ThreatIntelligence
- SA-UEBA
- SA-Utils
- Splunk_SA_CIM
- Splunk_ML_Toolkit

ES Technology Add-ons

- Technology add-ons (TA's) can configure inputs on forwarders, parsing on indexers, and normalizing (CIM compliance) on search heads
- Only the User Behavior Analytics (UBA) add-on `Splunk_TA_ueba` is included in the ES install
- Download and install other add-on's from Splunkbase as needed for the technologies in your environment (<https://splunkbase.splunk.com/>)

ES supported TA's:

- Splunk Add-on for Blue Coat ProxySG
- Splunk Add-on for Zeek (Bro) IDS
- Splunk Add-on for McAfee
- Splunk Add-on for Juniper
- Splunk Add-on for Microsoft Windows
- Splunk Add-on for Oracle Database
- Splunk Add-on for OSSEC
- Splunk Add-on for RSA SecurID
- Splunk Add-on for Sophos
- Splunk Add-on for FireSIGHT
- Splunk Add-on for Symantec Endpoint Protection
- Splunk Add-on for Unix and Linux
- Splunk Add-on for Websense Content Gateway

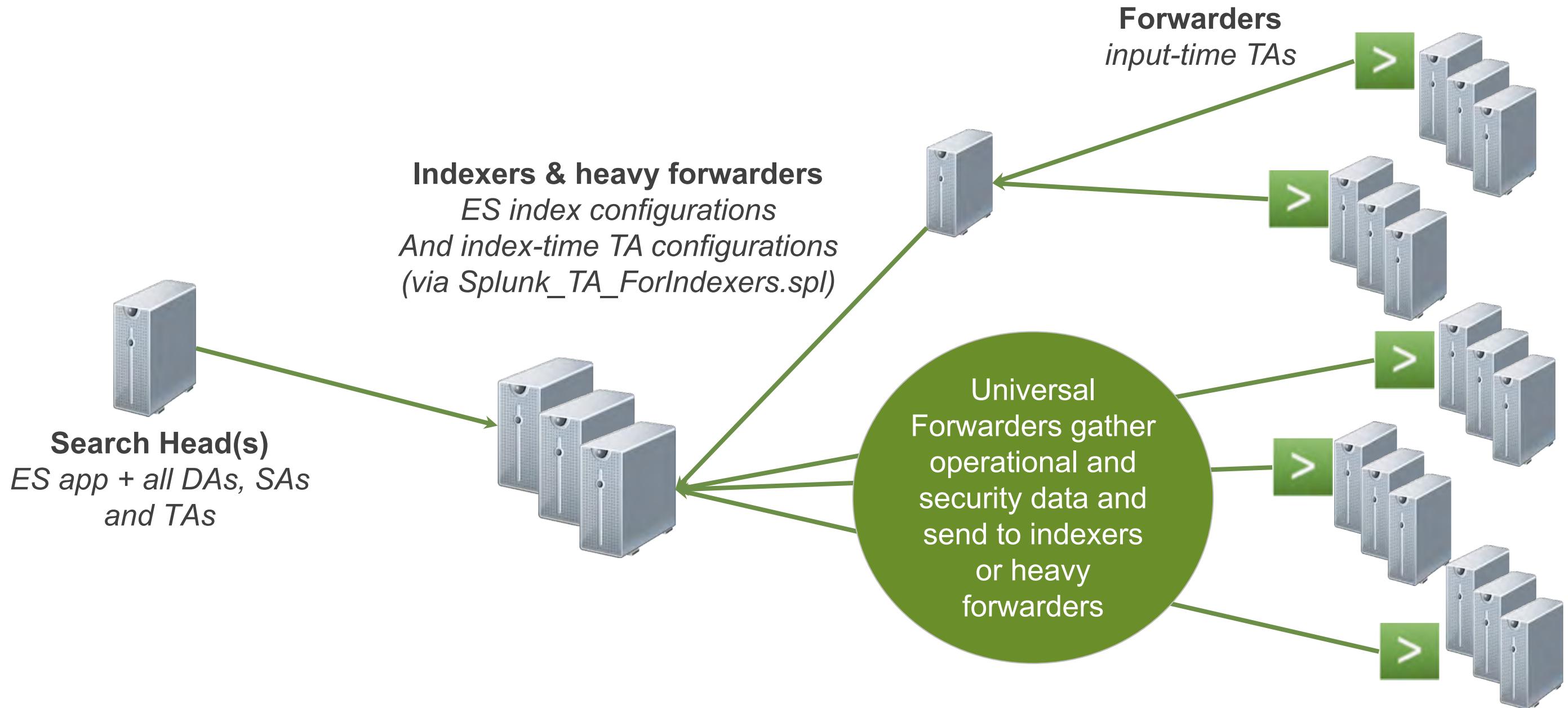
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

What Gets Installed Where?

- Install the full ES app on the search head
 - Includes
 - DAs, SAs, and UBA TA
 - Machine Learning Toolkit (MLTK)
- Install TAs on search head, and on forwarders if they perform input phase actions
 - See TA readme files and configuration files
- Create **Splunk_TA_ForIndexers** on search head
- Install **Splunk_TA_ForIndexers** on indexers and heavy forwarders
 - Includes all configurations from all enabled TAs, as well as **indexes.conf** settings

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

Typical Server Architecture



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

Installation Checklist

- Follow these steps for a single server or distributed (non-clustered) site:
 1. Confirm the environment meets the minimum system requirements for Splunk Enterprise and ES
 2. Increase the Splunk Web upload size limit in `web.conf` (version 6.0.0+)
 3. Install ES app on search head
 4. Install any required TA's
 5. Create `Splunk_TA_ForIndexers` and deploy to indexers
 6. Deploy input-time technical add-ons (TAs) to forwarders
- If using deployment server to deploy ES-installed apps and add-ons, disable it before the installation, and re-enable after installation

Important!

ES 6.0.x is the last major release that is compatible with Python 2 and with MLTK 4.0. ES 6.1+ is compatible with Python 3 only. ES 6.1+ is compatible with versions of Splunk Enterprise that ship with the Python 3 interpreter only, as well as MLTK 5.0+ only.

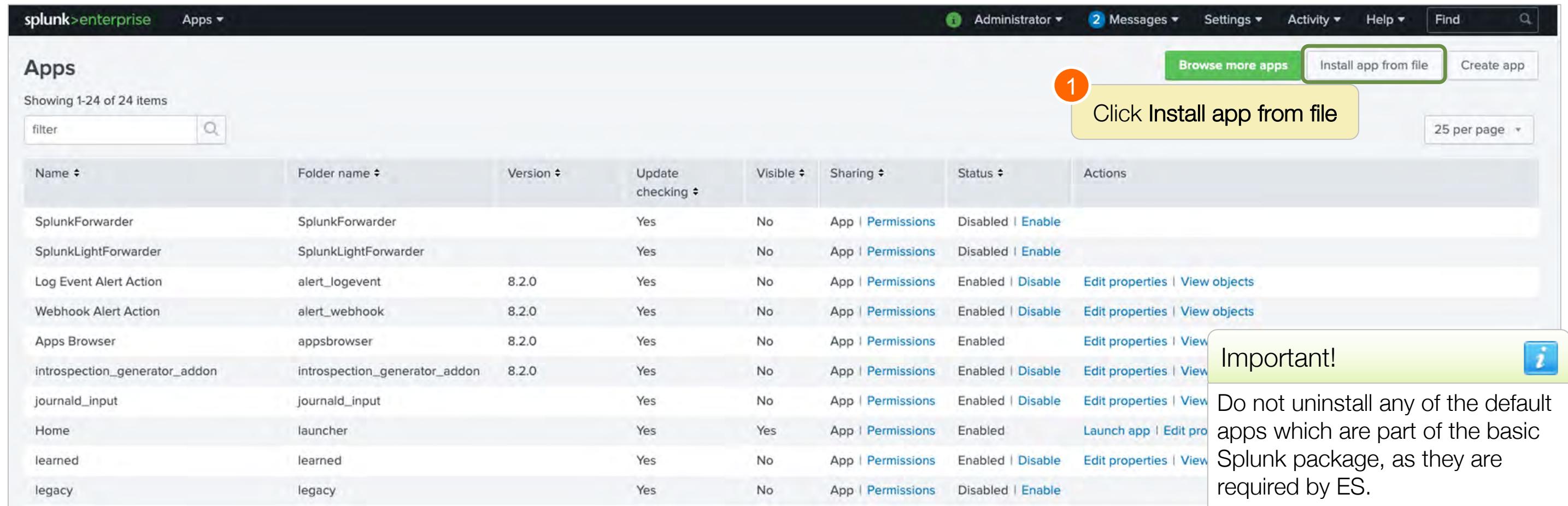
Increase the Splunk Web Upload Size

- The 6.0.0+ installer is larger than the default upload limit for Splunk Web
- Increase the Splunk Web upload size in `web.conf`
- Create the `$SPLUNK_HOME/etc/system/local/web.conf` file and add the following stanza (requires restart)

```
[settings]
max_upload_size = 1024
```

Install ES on a Single Search Head

- Start with a clean basic Splunk installation
- ES functions best without the installation of additional apps on top of the basic Splunk package



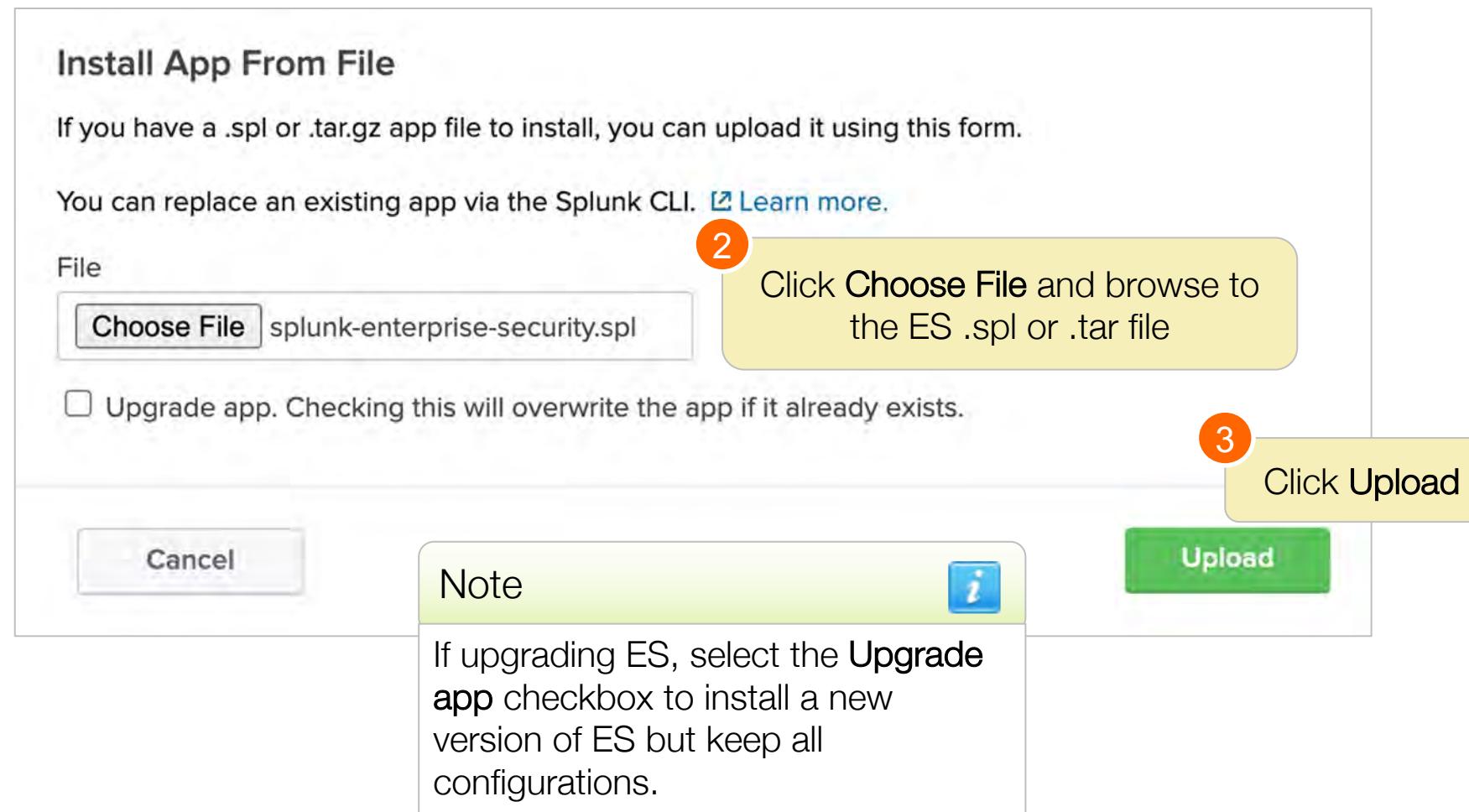
The screenshot shows the Splunk Apps interface. At the top, there's a navigation bar with 'splunk>enterprise' and various dropdown menus like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a search bar. The main area is titled 'Apps' and shows a list of 24 items. The columns include 'Name', 'Folder name', 'Version', 'Update checking', 'Visible', 'Sharing', 'Status', and 'Actions'. A yellow callout box with the number '1' points to the 'Install app from file' button in the top right corner of the list area. To the right of the list, there's a 'Browse more apps' button, a 'Create app' button, and a '25 per page' dropdown. A tooltip box labeled 'Important!' contains the text: 'Do not uninstall any of the default apps which are part of the basic Splunk package, as they are required by ES.'

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Log Event Alert Action	alert_logevent	8.2.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	8.2.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	8.2.0	Yes	No	App Permissions	Enabled	Edit properties View
introspection_generator_addon	introspection_generator_addon	8.2.0	Yes	No	App Permissions	Enabled Disable	Edit properties View
journald_input	journald_input		Yes	No	App Permissions	Enabled Disable	Edit properties View
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit pro
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View
legacy	legacy		Yes	No	App Permissions	Disabled Enable	

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

Upload the ES App

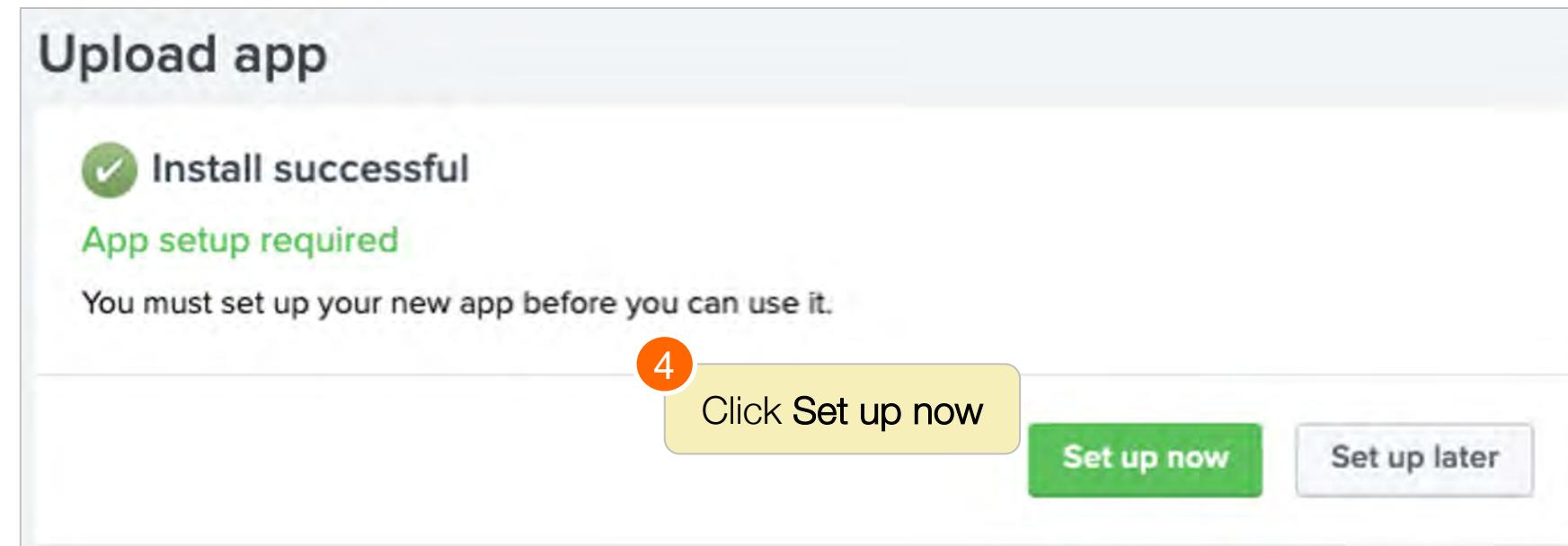
Obtain the ES app from Splunk and upload the file on the designated ES search head



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

Setup the App

Once the file is installed, you are prompted to set up the app

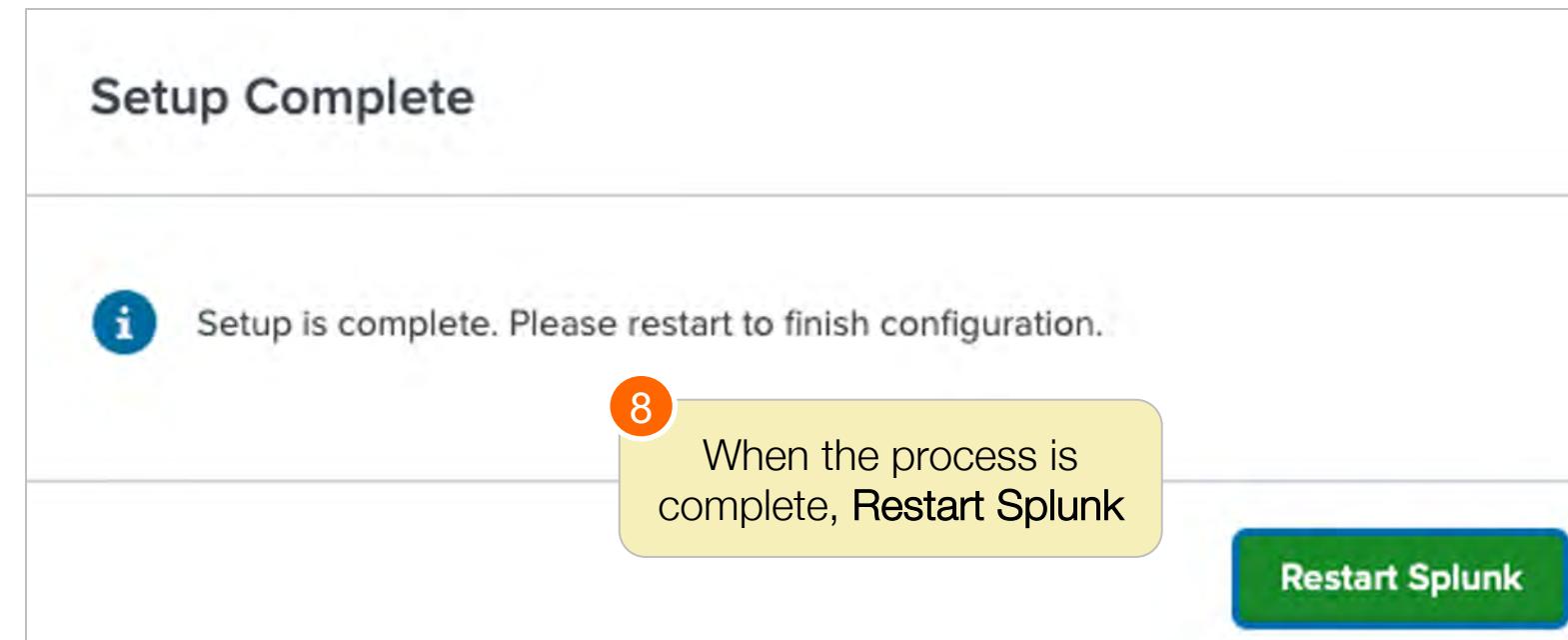
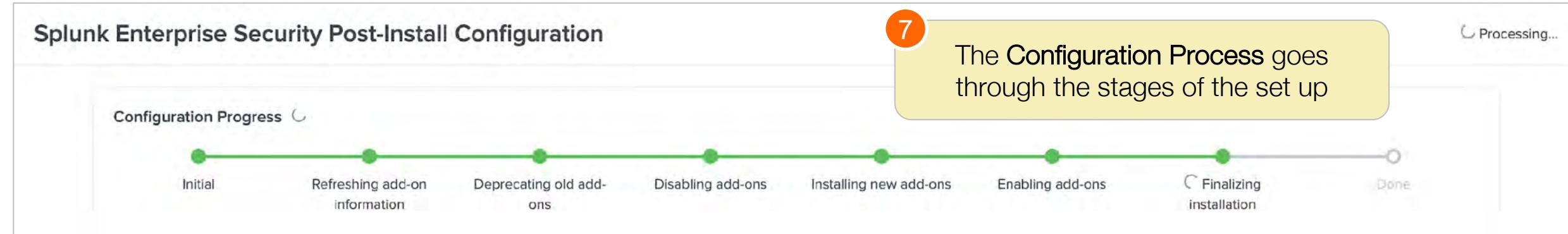


Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

App Setup

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

Setup Complete



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

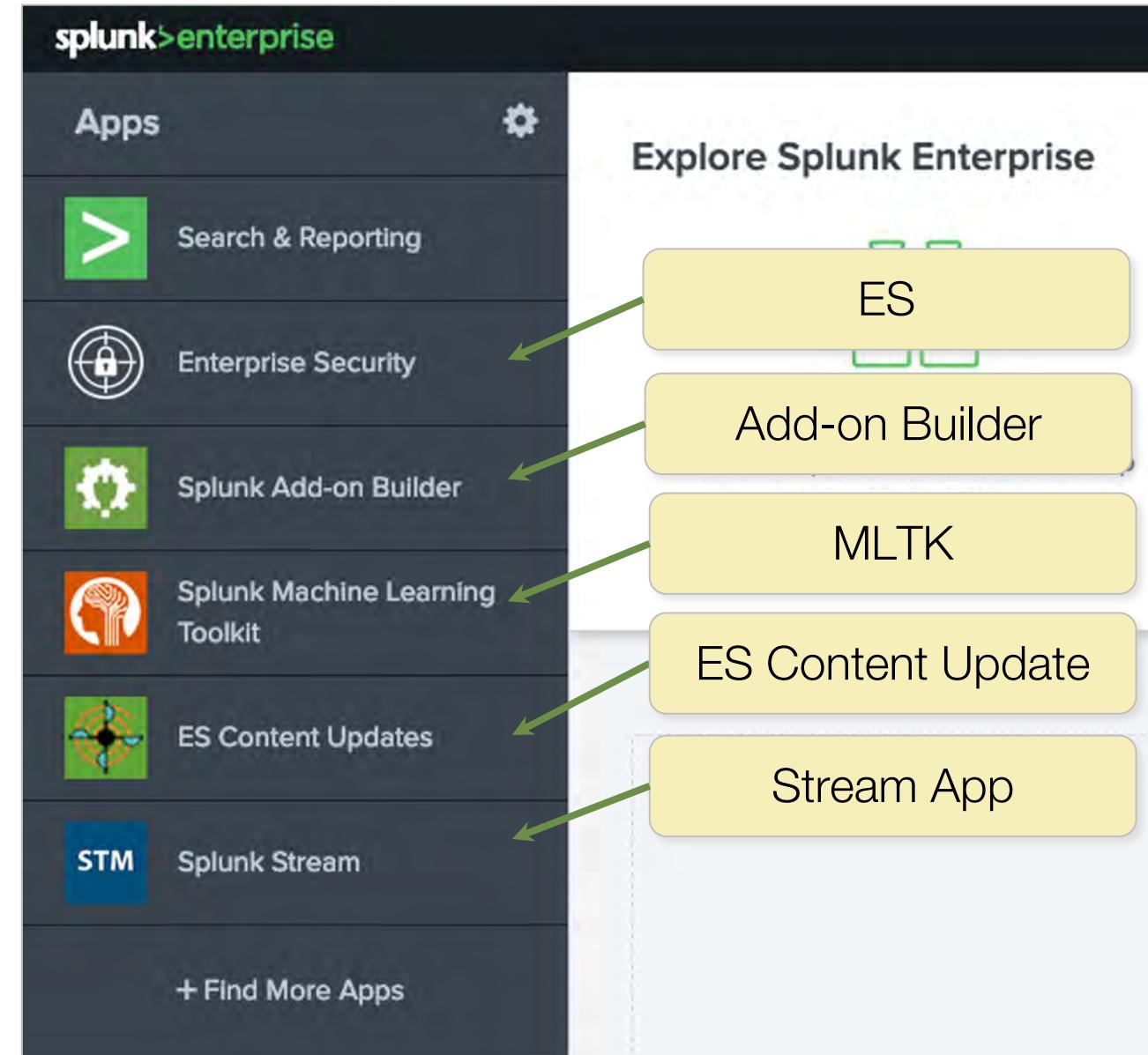
Splunk Web Restarts

- If SSL is enabled, Splunk Web restarts using an address similar to `https://<ip-address>:8000`
 - Port stays as default port 8000
 - Can be changed in `web.conf`, or
`Settings > Server Settings > General Settings`
- If using HTTPS, the pre-loaded SSL certificates are self-signed
 - This causes a browser warning, but they are completely secure
 - You can install your own externally signed certificates

docs.splunk.com/Documentation/Splunk/latest/Security/Howtogetthird-partycertificates

ES Is Installed on the Search Head!

- ES also installs:
 - Machine Learning Toolkit (MLTK)
 - UBA add-on
- The Stream app, if installed, can be integrated with ES
- If additional add-ons or apps are needed like Splunk Add-on Builder or ES Content Updates, install them from Splunkbase



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

ES Technical Add-Ons

- There are several technical add-ons (TAs) for common security data sources that can be installed with Enterprise Security
 - For a complete list:
docs.splunk.com/Documentation/ES/latest/Install/InstallTechnologyAdd-ons
- Each TA is related to a specific vendor product or technology
- Each has a specific add-on name and one or more event source types
- Some, like the *NIX, and Windows add-ons, are designed to input OS data and will require configuration before use
- See the **README** file in each add-on to for configuration steps

Disable Unused ES Add-ons

- Tech add-ons are intended for use with specific technologies
 - For example, Splunk Add-on for Websense, Splunk Add-on for Zeek (Bro) IDS, Splunk Add-on for Juniper
- If this is an upgrade, there may be add-ons that are no longer required. They can be disabled under Apps > Manage Apps

Apps

Showing 1-8 of 8 items

TA-

100 per page ▾

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Splunk Add-on for AirDefense	TA-airdefense	6.1.1	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for Alcatel Wireless IDS	TA-alcatel	6.1.1	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for CEF	TA-cef	6.1.1			Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for Fortinet	TA-fortinet	5.2.0			Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for FTP	TA-ftp	6.1.1			Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for Nmap	TA-nmap	6.1.1			Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for Tipping Point	TA-tippingpoint	6.1.1	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for Trend Micro	TA-trendmicro	5.2.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects

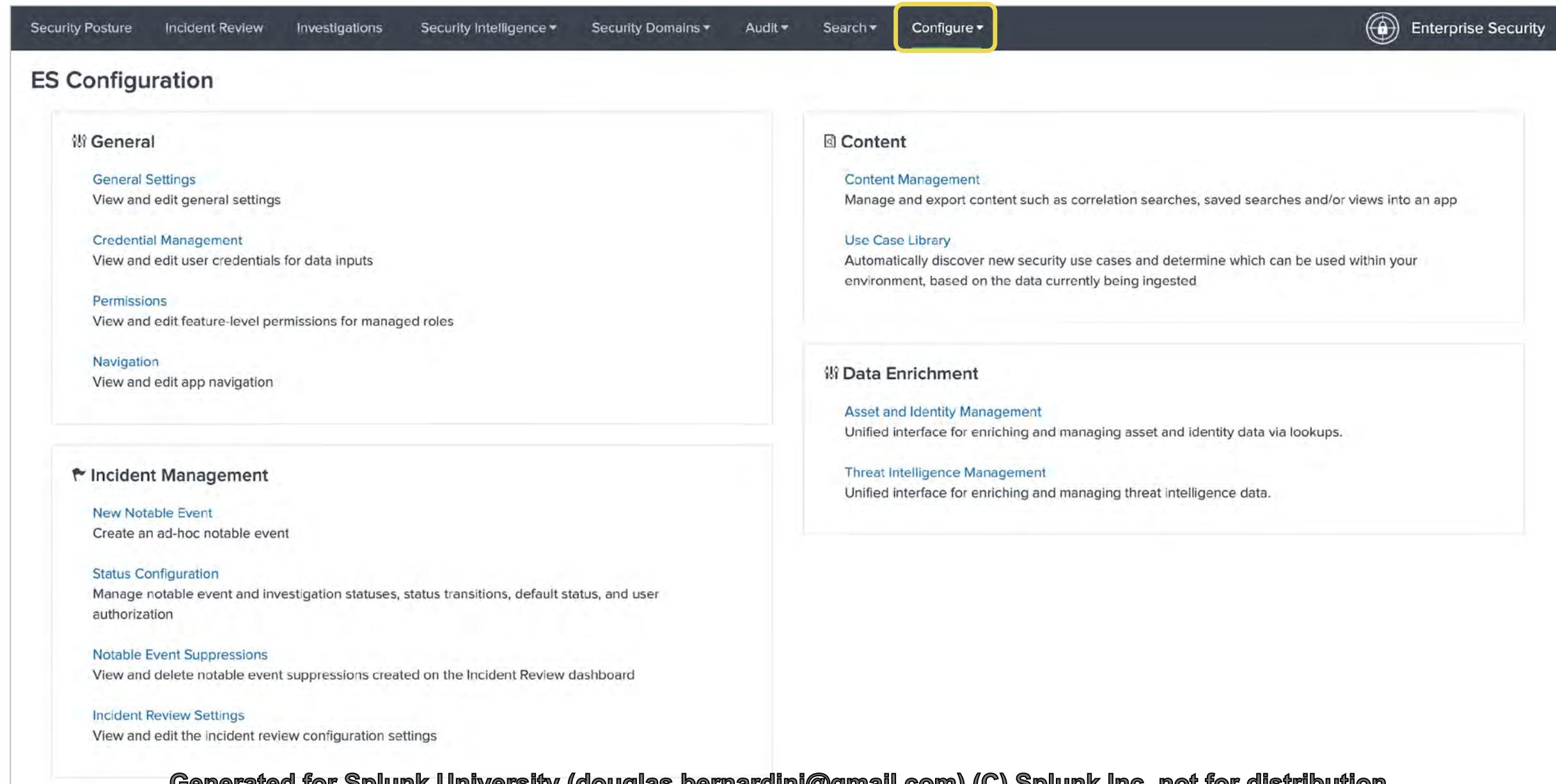
Listed are some of the TAs installed on the system. Notice you can disable add-ons not being used

Installing ES on a Search Head Cluster

- The installer will dynamically detect if you are installing in a single search head environment or search head cluster environment
- Install ES on the Deployer
 1. On the Splunk toolbar, select **Apps > Manage Apps** and click **Install app from file**
 2. Click **Choose File** and select the **Splunk Enterprise Security** file
 3. Click **Upload** to begin the installation
 4. Click **Continue to app setup page**
 5. Click **Start Configuration Process**, and wait for it to complete
 6. Use the **Deployer** to deploy ES to the cluster members. From the Deployer run:
splunk apply shcluster-bundle

ES Configuration Page

Navigate to ES > Configure > All Configurations



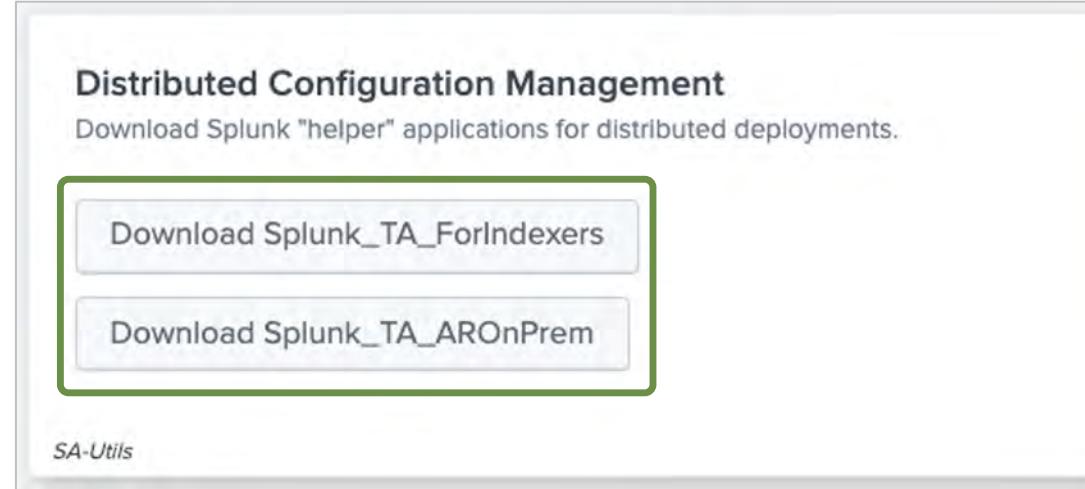
The screenshot shows the 'Configure' section of the Splunk Enterprise Security interface. The 'Configure' button in the top navigation bar is highlighted with a yellow box. The page is divided into several sections:

- General**:
 - [General Settings](#): View and edit general settings.
 - [Credential Management](#): View and edit user credentials for data inputs.
 - [Permissions](#): View and edit feature-level permissions for managed roles.
 - [Navigation](#): View and edit app navigation.
- Content**:
 - [Content Management](#): Manage and export content such as correlation searches, saved searches and/or views into an app.
 - [Use Case Library](#): Automatically discover new security use cases and determine which can be used within your environment, based on the data currently being ingested.
- Data Enrichment**:
 - [Asset and Identity Management](#): Unified interface for enriching and managing asset and identity data via lookups.
 - [Threat Intelligence Management](#): Unified interface for enriching and managing threat intelligence data.
- Incident Management**:
 - [New Notable Event](#): Create an ad-hoc notable event.
 - [Status Configuration](#): Manage notable event and investigation statuses, status transitions, default status, and user authorization.
 - [Notable Event Suppressions](#): View and delete notable event suppressions created on the Incident Review dashboard.
 - [Incident Review Settings](#): View and edit the incident review configuration settings.

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

Distributed Configuration Management

ES > Configure > General > General Settings



Download Splunk_TA_ForIndexers

- Creates the **Splunk_TA_ForIndexers.spl** add-on
- Collects index-time configurations and basic index definitions into one package to simplify the deployment of add-on configurations to on-premises indexers

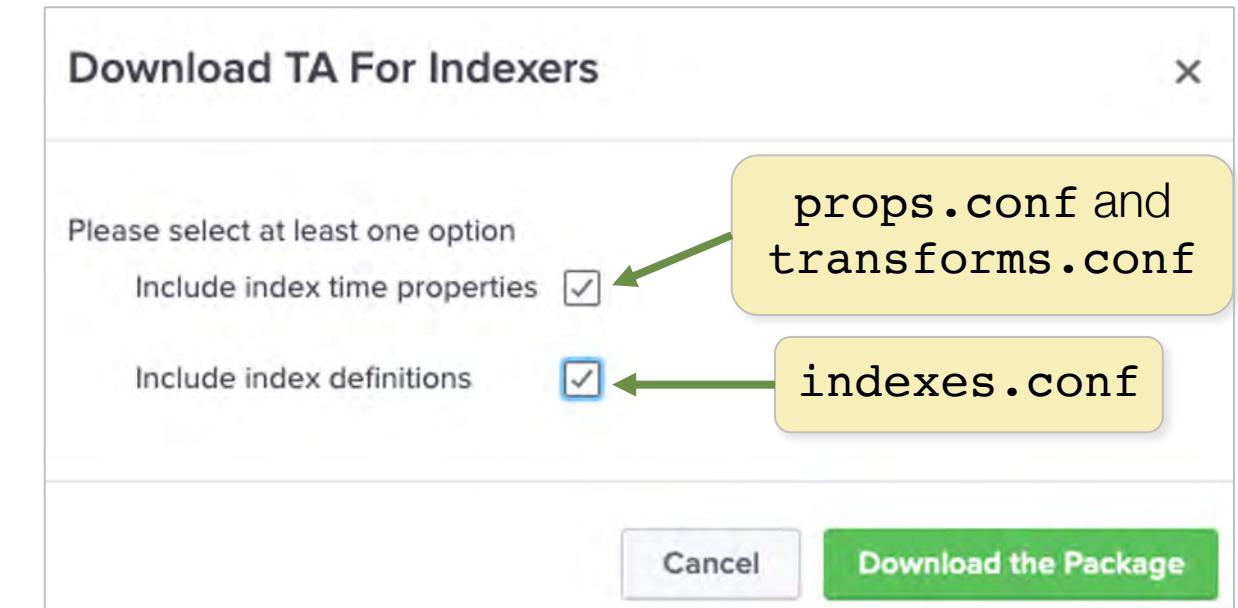
Download Splunk_TA_AROnPrem

- Creates the **Splunk_TA_AROnPrem** add-on that is used when setting up an adaptive response relay from an ES Cloud SH to an On-prem HF

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

Deploy Indexer Configurations

- To create the `Splunk_TA_ForIndexers.spl`, click Download `Splunk_TA_ForIndexers`
- Select at least one option and click Download the Package
 - Include index time properties: adds the `props.conf` and `transforms.conf` files to the package
 - Include index definitions adds the `indexes.conf` file to the package
- Copy the downloaded `.spl` file to your indexers

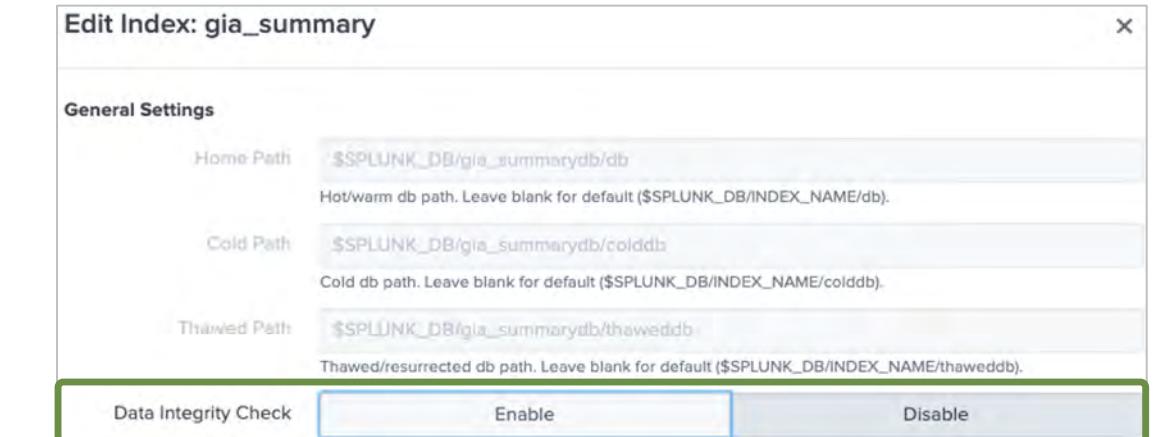


Data Integrity Control

- An ES Admin can enable **data integrity control** to ensure that the data ES relies on in the indexes is not tampered with
 - Data integrity applies hashes on indexed data
- Ways to configure data integrity control:
 - In **indexes.conf**, create a stanza per index
 - **Settings > Indexes**, enable **Data Integrity Check** per index
 - Re-start Splunk
 - Only new inputs will be hashed
- Test integrity from the command line or script:
`./splunk check-integrity -index <indexname>`

Indexes.conf

```
[gia_summary]
enableDataIntegrityControl=true
```



Data Protection Audit

Audit > Data Protection

- Displays status of data protection settings per index
- Also displays status for sensitive data if the **Personally Identifiable Information Detected** correlation search is enabled

The screenshot shows the Splunk Enterprise Security interface with the 'Audit' tab selected. The main content area is titled 'Data Protection'. It contains two sections: 'Data Integrity Control By Index' and 'Anonymizing Sensitive Data'. The 'Data Integrity Control By Index' section includes a table with columns for index, splunk_server, and enableDataIntegrityControl. The 'Anonymizing Sensitive Data' section provides information about log data containing sensitive data like PII and credit cards, and how the Luhn algorithm is used to detect it. A large red banner at the bottom right reads 'Events with sensitive data 1'.

index	splunk_server	enableDataIntegrityControl
_audit	ip-10-0-0-169.us-west-2.compute.internal	1
_internal	ip-10-0-0-169.us-west-2.compute.internal	1
bro	ip-10-0-0-169.us-west-2.compute.internal	1
gia_summary	ip-10-0-0-169.us-west-2.compute.internal	1
main	ip-10-0-0-169.us-west-2.compute.internal	1

Events with sensitive data 1

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

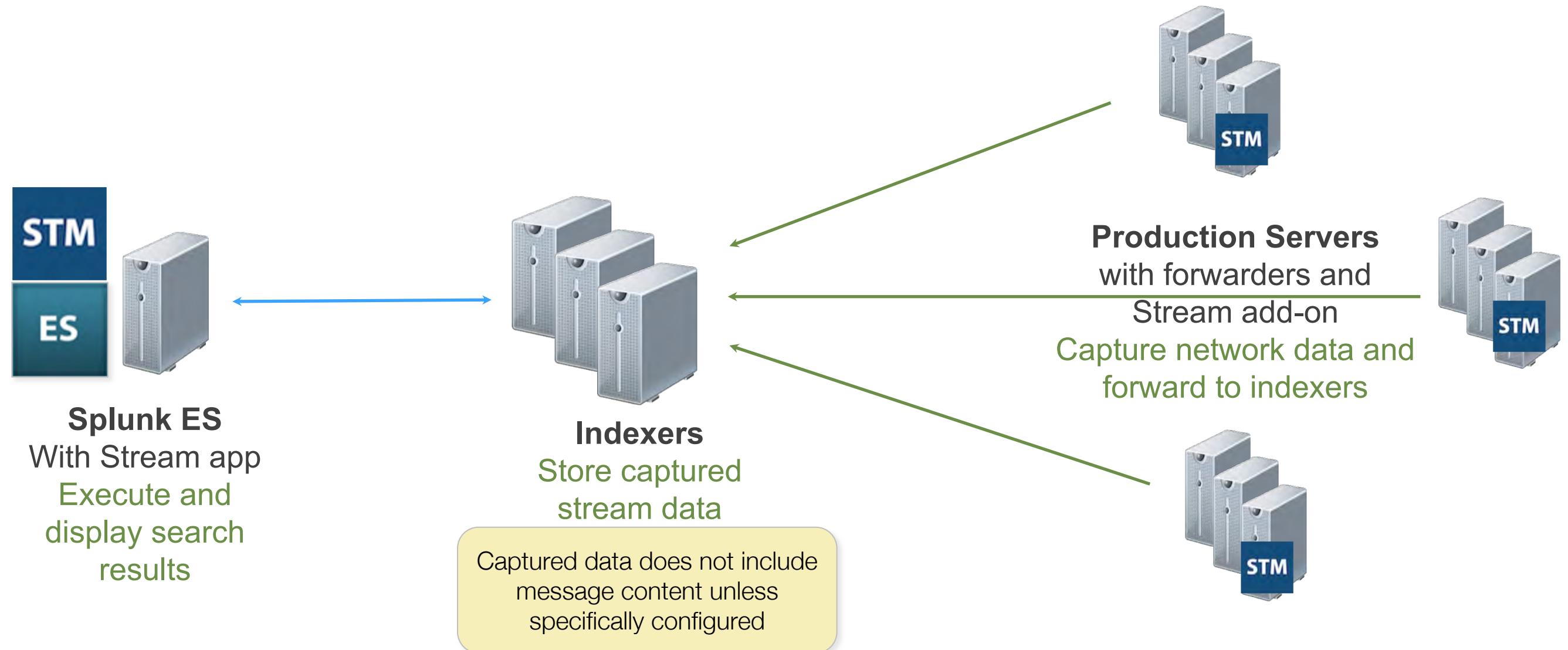
Splunk Stream and ES

- ES can use wire data captures from the Splunk Stream app
 - Supports Protocol Intelligence
- Install the Splunk Stream app on the ES server
- Install the Stream add-on (`Splunk_TA_stream`) on machines where you want to capture data
- Details on installing and configuring Stream:
docs.splunk.com/Documentation/StreamApp
- Details on integrating Stream with ES:
<https://docs.splunk.com/Documentation/ES/latest/Install/IntegrateSplunkStream>



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

Module 5 Lab: Post-installation Tasks

Time: 15 minutes

Tasks:

1. Following an ES upgrade, disable un-needed add-ons
2. Create an app package for your indexer(s) (Splunk_TA_ForIndexers)

Module 6: Initial Configuration

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

Objectives

- Set general configuration options
- Add external integrations
- Configure local domain information
- Customize navigation
- Configure Key Indicator searches

General ES Configurations

Configure > General >
General Settings

- Set or modify various ES parameters
- For example:
 - Enable the Event Sequencing Engine
 - Set the size in bytes for the Large Email Threshold
 - Set HTTP Category Analysis and HTTP User Agent Analysis sparkline limits

The screenshot shows the 'General Settings' page in the Splunk Enterprise Security interface. At the top, there's a search bar labeled 'Filter by app and/or text'. Below it, there are several configuration sections:

- Auto Pause:** A field set to 120 seconds before a drilldown search pauses, with a 'Save' button.
- Default Watchlist Search:** A search filter for defining watchlisted events for the 'Watchlisted Events' correlation search, with a 'Save' button.
- Distributed Configuration Management:** Options to download Splunk "helper" applications for distributed deployments, with buttons for 'Download Splunk_TA_ForIndexers' and 'Download Splunk_TA_AROnPrem'.
- Domain Analysis:** A section to enable/disable WHOIS tracking for Web domains, with 'Enable' and 'Disable' buttons.
- Domain From URL Extraction Regex:** A regular expression to extract domain (url_domain) from url, currently set to '^:(http|https|ftp):\/\/([a-zA-Z0-9\.\-]+)(:[a-zA-Z0-9\+]+)?@)?([^\:/\+])(:[0-9\+]+)?', with a 'Save' button.
- Event Sequencing Engine:** A section to enable the main Event Sequencing Engine, with 'Enable' and 'Disable' buttons.

A yellow callout box in the top right corner states: 'Some settings require that you Save your changes, some auto-save when you make changes'.

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

Configuring Local and Cloud Domains

- Some correlation searches need to differentiate between your local domain vs. external domains
 - For instance, if you work at Acme Corp, you may have local domains ending in `acme.com`, `acmecorp.com`, etc.
- Also, there are external cloud domains you may use frequently that are not suspicious
 - External vendors for accounting, expenses, document sharing, etc.
- Your email system may use different email domains from your standard corporate domain
 - Due to acquisitions, mergers, etc.

Editing Domain Tables

- Select Configure > Content > Content Management and select Type: Managed Lookup
- Edit any of the Domain lookups:
 - Corporate Web Domains
 - Corporate Email Domains
 - Cloud Domains (external vendor sites)

Edit Lookup File / cim_corporate_email_domain_lookup

Modify the contents of a lookup table.

< Back to Content Management

1	domain
2	*acmetech.com
3	

Cancel Save

Right-click a row, select Insert row below and add your domains.
Right-click and delete any sample rows.
Remember to click Save!

Insert row above
Insert row below
Insert column left
Insert column right
Remove row
Remove column
Undo
Redo

Configuring Domain Analysis

- The New Domain Analysis dashboard, **Security Intelligence > Web Intelligence**, relies on domain name lookup information retrieved via a modular input from **domaintools.com**
 1. Add your **domaintools.com** credentials in the **Credentials Manager**
 2. Configure the settings for the **Network Query** input
 3. Enable **whois** checking
 4. Check for events in the **whois** index

docs.splunk.com/Documentation/ES/latest/User/ThreatListActivitydashboard#Configure_the_external_API_for_WHOIS_data

Adding Credentials

- In ES, navigate to Configure > General > Credential Management and click New Credential
- Enter the domaintools.com credentials, an app, and click Save

The screenshot shows the 'Credential/Certificate Management' page in Splunk Enterprise. At the top left, there's a 'Back to ES Configuration' link. Below it, there are two main sections: 'Credentials' and 'Certificates'. The 'Credentials' section has a 'New Credential' button highlighted with a green box. The 'Certificates' section also has a 'New Certificate' button. The background shows some credential entries with dropdown menus for 'Username', 'Realm', and 'App'. The 'Username' dropdown shows 'Splunk_TA_nessus_proxy', 'Realm' shows 'Splunk_TA_nessus', and 'App' shows 'Splunk_TA_ne'. A large green callout box points from the 'New Credential' button to the 'Create Credential' modal window.

Create Credential

User	domtoolsuser	(dropdown menu)
Realm	domaintools.com	(dropdown menu)
Password	(eye icon)
Confirm Password	(eye icon)
App	Enterprise Security	(dropdown menu)

Actions: Cancel, Save

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

Configuring the whois_domaintools Input

- Select Configure > Data Enrichment > Whois Management
- Edit the **whois_domaintools** entry:
 - API Host: URI to your account's server
 - API User: domaintools.com username (password is retrieved from credential manager automatically)
 - App: the app you stored the credentials in
 - Leave other fields with default values unless you have a proxy or want to alter defaults for queue interval, etc
- Click Save

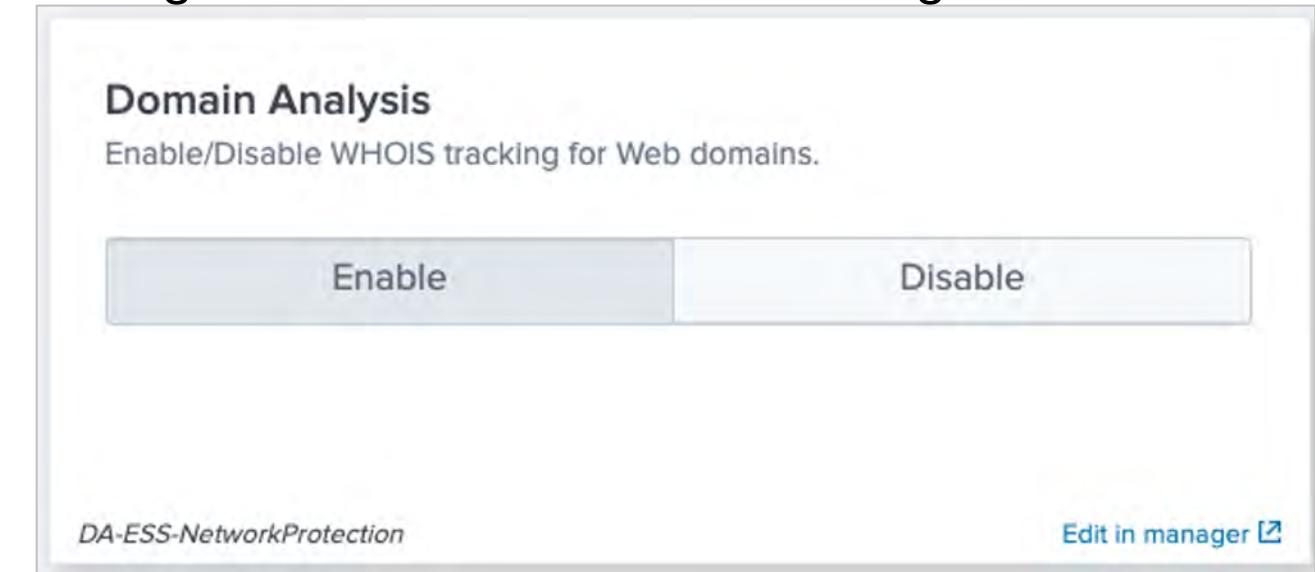
The screenshot shows the 'whois_domaintools' configuration page in the Splunk UI. The form includes fields for Name (None), API Host (An API host, if required by the provider. Defaults to http if protocol is unspecified.), API User (A user account to use for API access, if required by the provider.), API User Realm (A value used to differentiate between multiple credentials that have the same username. If present, must correspond to a credential realm in Splunk's secure credential store.), App (alert_logevent, Splunk application context used to retrieve stored credentials.), Owner (A Splunk user that has access to any stored credentials in use.), Provider (The data provider. Must correspond to the name of the Python class that implements the provider.), Proxy Port (A proxy server port.), Proxy Server (A proxy server name (Must exclude http:// and https:// from url).), Proxy User (A proxy server user name. If present, must correspond to a credential name in Splunk's secure credential store.), Proxy User Realm (A value used to differentiate between multiple credentials that have the same username. If present, must correspond to a credential realm in Splunk's secure credential store.), Queue Interval (The interval (in seconds) between successive queries.), Query Interval (A proxy server name.), Reverse DNS Enabled (Attempt to resolve IP address to domain names. Disabled by default. WARNING: Enabling reverse DNS resolution may expose the existence of your system to an attacker.), and Debug (If True, the whois modular input will run in debug mode. Defaults to False.). At the bottom right are 'Cancel' and 'Save' buttons.

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

Enabling the Domain Analysis Setting

- Modify the domain analysis setting
 - Enable Domain Analysis

Configure > General > General Settings



- The **whois** system is now enabled
 - Domain name lookup happens when events with IP addresses are indexed
 - Domain info is stored in the **whois** index and used by the **New Domain Analysis** dashboard

ES and User Behavior Analytics (UBA)

- Splunk User Behavior Analytics (UBA) is a separate solution that extends your ability to detect insider threats
 - Send threats and anomalies from UBA to ES to adjust risk scores and create notable events
 - Send correlation search results from ES to UBA to be processed for anomalies
 - Retrieve user and device association data from UBA to view it in ES



Integrating ES and SOAR

- Install the Splunk App for SOAR Export (Formerly known as Phantom App for Splunk) to be able to send ES events to SOAR using an ES Adaptive Response Action
 - Send to SOAR sends ES search results to SOAR
 - Run Playbook in SOAR Runs a SOAR playbook on the ES event

The screenshot shows the Splunk Adaptive Response Actions interface. At the top right is a logo for 'splunk> SOAR'. The main area has a title 'Adaptive Response Actions' and a sub-section 'Select actions to run.' with a button '+ Add New Response Action'. Below this are three listed actions:

- Run Playbook in SOAR**: Run a SOAR playbook on this event. Category: Orchestration | Task: Automation | Subject: Phantom | Vendor: Splunk
- Send To UBA**: Forwards search results from Splunk Enterprise to UBA. Category: Information Conveyance | Task: create | Subject: uba.anomaly | Vendor: Splunk
- Send to SOAR**: Send search results to SOAR. Category: Orchestration | Task: Automation | Subject: Phantom | Vendor: Splunk

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

Incident Review KV Store

- All incident review status changes and comments are stored in the `incident_review` KV Store collection
- Use the ``incident_review`` macro to retrieve information from this lookup
- Example: you are working on a new incident that is similar to one you worked on before and you want to search for comments related to the incident

```
|`incident_review` | search comment = "*...text...*"
```

Incident Review KV Store Maintenance

- Periodically clear data from the incident review KV Store:

```
| inputlookup incident_review_lookup  
| eval age = (now()-time)/86400 | search age < 30  
| fields - age  
| outputlookup incident_review_lookup append=f
```
- Use the **splunk clean** command to completely clear out the incident review collection:

```
splunk clean kvstore -app SA-ThreatIntelligence  
-collection incident_review
```
- Splunk must be running to use **splunk clean kvstore**
- See additional KV store maintenance commands at:
<https://docs.splunk.com/Documentation/Splunk/latest/Admin/BackupKVstore>

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

Untriaged Incident Alert

- The **Untriaged Notable Events** correlation search can be configured and customized for your site as needed
- By default, it prepares a list of all notable events in **new** status or **unassigned** owner over the last 48 hours
- Configure its adaptive response actions to send email to a group, run a script, or create a new notable event with a specific owner responsible to assign incidents to analysts

ES Configuration Health Audit

Audit > ES Configuration Health

- Compare the latest installed version of ES to prior releases and identify configuration anomalies
- Useful to check ES status after initial configuration or upgrade

ES Configuration Health

Mode Previous ES Version

All 5.3.1-2 Submit Hide Filters

Introduction

The ES Configuration Health dashboard identifies three types of configuration anomalies.

Unshipped Items

Unshipped items are identified as items present in the current ES installation that did not ship with the latest ES version. This is expected for items that live in /local or known backup files, so these have been filtered automatically. Please examine the remaining items and determine if they are in fact needed.

Removed Stanzas

Removed stanzas are identified as stanzas that existed in a previous ES version but do not ship with the latest ES version. If any of these removed stanzas are still present in the current ES installation they will be identified. Please examine any removed stanzas and determine if they are in fact needed.

Local Overrides

Changed parameters are identified as parameters that were modified between the previous and latest ES versions. If any of these changed parameters differ from the latest ES version they are considered to be locally overridden. Please reconcile any local overrides with the newly shipped defaults.

Per-panel Filter

Configuration Items

Per-panel Filter	item	item_type	es_version
<input type="checkbox"/>	SplunkEnterpriseSecuritySuite/lookups/F00_assets.csv	unshipped	6.0.0-3
<input type="checkbox"/>	SplunkEnterpriseSecuritySuite/install/SplunkEnterpriseSecuritySuite-6.0.0_20191110181455_163811	unshipped	6.0.0-3
<input type="checkbox"/>	SplunkEnterpriseSecuritySuite/install/SplunkEnterpriseSecuritySuite-6.0.0	unshipped	6.0.0-3
<input type="checkbox"/>	SA-ThreatIntelligence/lookups/__mlspl_total_risk_by_object_type_1d.csv	unshipped	6.0.0-3
<input type="checkbox"/>	SA-ThreatIntelligence/lookups/__mlspl_total_risk_1d.csv	unshipped	6.0.0-3

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

Controlling and Customizing Views

- Set permissions on dashboards and reports to control access
 - Only the views that the current user can access are displayed in navigation
- Clone views and edit to create custom alternatives

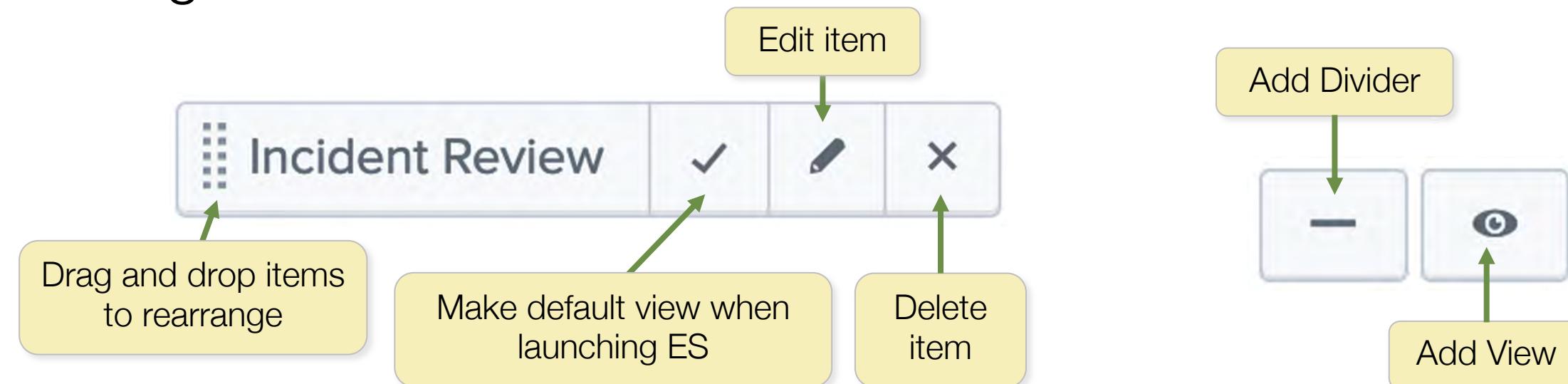
The screenshot shows the Splunk interface with a navigation bar at the top labeled "Audit ▾", "Search ▾", and "Configure ▾". A dropdown menu is open under "Configure", showing options: "Dashboards" (selected and highlighted with a green border), "Reports", "Datasets", and "Search". Below this, a "Dashboards" page is displayed. The page title is "Dashboards" and it includes a subtitle: "Dashboards include searches, visualizations, and input controls that capture and present available data." It shows a list of 91 Dashboards, ordered by Title. The first few items in the list are: "Access Anomalies", "Access Center", "Access Search", "Access Tracker", "Account Management", "Adaptive Response Action Center", "Analytic Story Detail", and "App Analytics". To the right of the list, there are buttons for "All", "Yours", "This App's", "filter", and a search icon. A detailed Actions menu is open for the "Access Anomalies" dashboard, listing options: "Edit Panels", "Edit Source", "Convert to HTML", "Edit Title or Description", "Edit Permissions" (selected and highlighted with a green border), "Schedule PDF Delivery", "Set as Home Dashboard", and "Clone" (highlighted with a green border).

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

Customizing ES Menus

Configure > General > Navigation

- Customize menus by adding, removing, or moving items
- Change the default page when logging into ES (default is ES Home)
- Changes affect all users
- Customizing tools:



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

Navigation Example

Example, move Content Management to the main ES menu

Edit Navigation

Add a new menu drop-down

Revert changes

Save

Restore Default Navigation

Add a New View

Add a New Collection

No updated content.

Home Security Posture Incident Review Content Manag... Investigations

Security Domains

Access

Access Center Access Tracker Access Search

Account Mana... Default Accoun...

Audit

Incident Revie... Investigation O... Suppression A... Adaptive Resp...

Per-panel Filter... Threat Intellige... Machine Learni...

Configure

All Configuratio... CIM Setup UBA Setup Risk Factor Edit...

General

General Settings

Add new view or dashboard

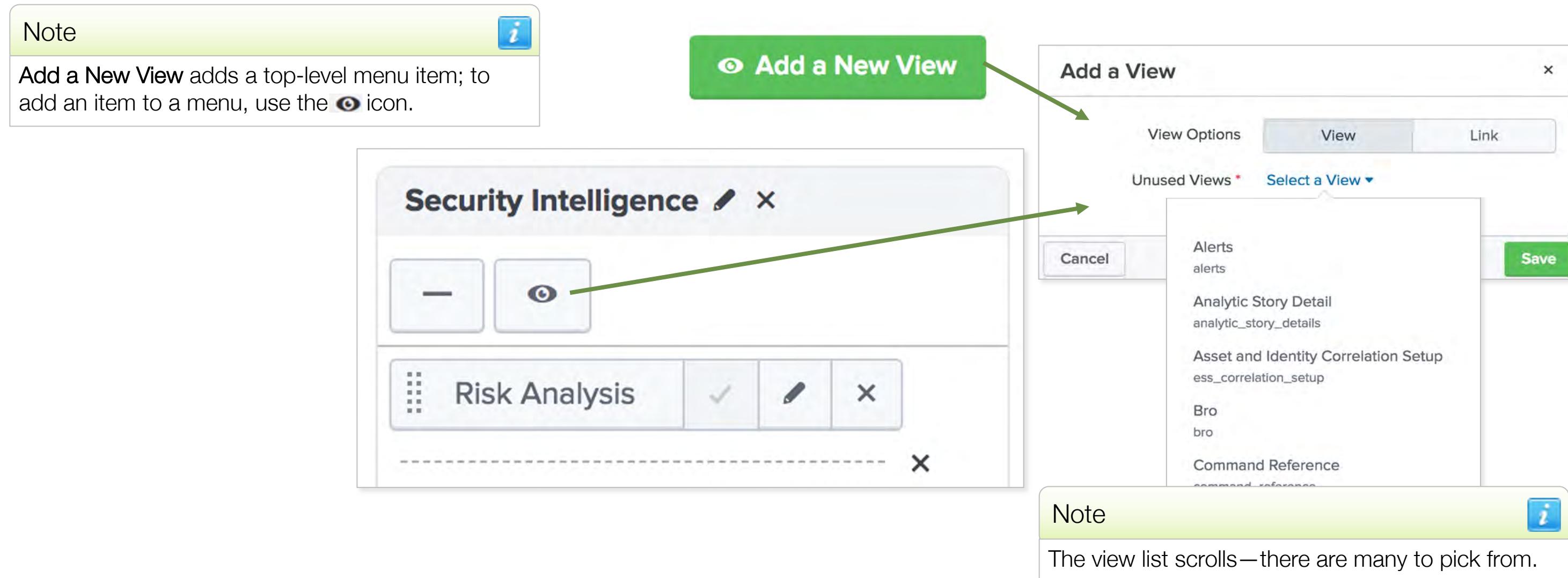
The check mark makes the item the default view instead in ES

Drag and drop items to the top to add them to the main ES menu

Rearrange items using drag and drop

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

Adding a Menu Item



Adding links to filtered Incident Review results:

docs.splunk.com/Documentation/ES/latest/Admin/Customizemenubar#Add_a_link_to_a_filtered_view_of_Incident_Review

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

Edit Navigation Permissions

- By default, only users with the `ess_admin` role can edit ES navigation
- Admins can give users with the `ess_analyst` and `ess_user` role the Edit ES Navigation permission

ES Component	<code>ess_analyst</code>	<code>ess_user</code>
Edit ES Navigation Permits the role to edit Enterprise Security navigation.	<input type="checkbox"/>	<input type="checkbox"/>

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

Editing Key Indicator Searches

- Configure > Content > Content Management and select Type : Key Indicator
- Select a search name to edit indicator search definition
 - Click Edit Acceleration to configure an acceleration search schedule
- To make a new Key Indicator search, click Create New Content > Key Indicator Search

The screenshot shows the Splunk Content Management interface. At the top, there's a header with 'Content Management' and a sub-header: 'Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, glass tables, and reports.' Below the header, there's a breadcrumb navigation: '< Back to ES Configuration'. The main area displays a table of '119 Objects' with columns for Name, Type, App, Next Scheduled Time, and Actions. A green box highlights the 'Type: Key Indicator' dropdown menu. A yellow callout box with the text 'Click to edit' points to the 'Name' column of the first row. On the right side, a sidebar titled 'Create New Content' lists various content types: Analytic Story, Correlation Search, Data Model, Key Indicator Search (which is highlighted with a green box), Managed Lookup, Panel, Saved Search, Search-Driven Lookup, and Sequence Template.

Name	Type	App	Next Scheduled Time	Actions
Access - Distinct Apps	Key Indicator	DA-ESS-AccessProtection		Edit acceleration
Access - Distinct Destinations	Key Indicator	DA-ESS-AccessProtection		Edit acceleration
Access - Distinct Sources	Key Indicator	DA-ESS-AccessProtection		Edit acceleration
Access - Distinct Users	Key Indicator	DA-ESS-AccessProtection		Edit acceleration
Access - Number Of Default Accounts In Use	Key Indicator	DA-ESS-AccessProtection		Edit acceleration
Access - Total Access Attempts	Key Indicator	DA-ESS-AccessProtection		Edit acceleration

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

Adding a Key Indicator Search: 1

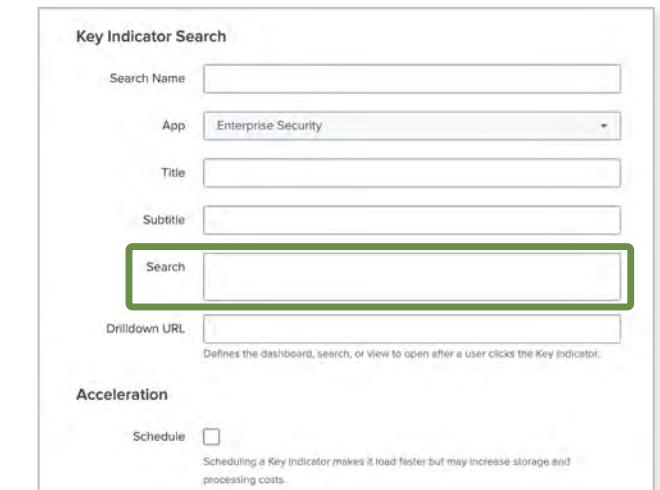
- Enter Name, App, Title and Subtitle
Add a search that generates a current and delta value
- Drilldown URL can be a search, dashboard or view to open on click
- Add optional acceleration settings

The screenshot displays the 'Key Indicator Search' configuration interface. On the left, there's a preview card for 'IDENTITY NOTABLES' showing a 'Total Count' of 10 with a red upward arrow and '+10'. Two green arrows point from the 'Title' and 'Subtitle' input fields in the configuration panel to the respective text in the preview card. The configuration panel includes fields for 'Search Name', 'App' (set to 'Enterprise Security'), 'Title', 'Subtitle', 'Search', 'Drilldown URL' (with a note about defining what opens on click), and 'Acceleration' (with a 'Schedule' checkbox and a note about performance trade-offs).

Example Key Indicator Search

- Example Key Indicator search:
 - The `get_delta` macro looks for fields `current_count` and `historical_count` and outputs delta
 - The two counts should be based on the two previous 24-hour periods
 - Use `tstats `summariesonly`` if possible for performance

```
| tstats `summariesonly` count as current_count  
from datamodel=Risk.All_Risk  
where All_Risk.risk_object_type="user" All_Risk.risk_score>60  
earliest=-24h@h latest=+0s  
| appendcols [|tstats `summariesonly` count as historical_count  
from datamodel=Risk.All_Risk  
where All_Risk.risk_object_type="user" All_Risk.risk_score>60  
earliest=-48h@h latest=-24h@h ]  
| `get_delta`
```



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

Adding a Key Indicator Search: 2

- **Value** contains the current value for the previous 24-hour period
- **Delta** contains the difference between the value for the previous 24-hour period and the preceding 24-hour period
- **Rendering Options** for threshold coloring, suffix notation, and inversion
- Click **Save**

Fields

Value
Specifies the name of the field that contains the current value of the Key Indicator.

Delta
Specifies the name of the field that contains the change (delta) in the Key Indicator.

Rendering Options

Threshold
The threshold can also be set on the dashboard.

Value Suffix
The suffix is displayed after the value on a dashboard. Useful to specify units.

Invert
Inverting means that a low number is worse and a high number is better.

Module 6 Lab: Initial Configuration

Time: 45 minutes

Tasks:

1. Configure Key Indicators and examine the search behind a KI
2. Modify dashboard permissions
3. Customize navigation
4. Review the capabilities of the **soc_analyst** user account with the **ess_user** role
5. Create a **SOC manager** role and give it specific permissions
6. Confirm the capabilities of the new **SOC manager** account
7. Enable specific ES permissions for the **ess_user** and **ess_analyst** roles

Module 7: Validating ES Data

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

Objectives

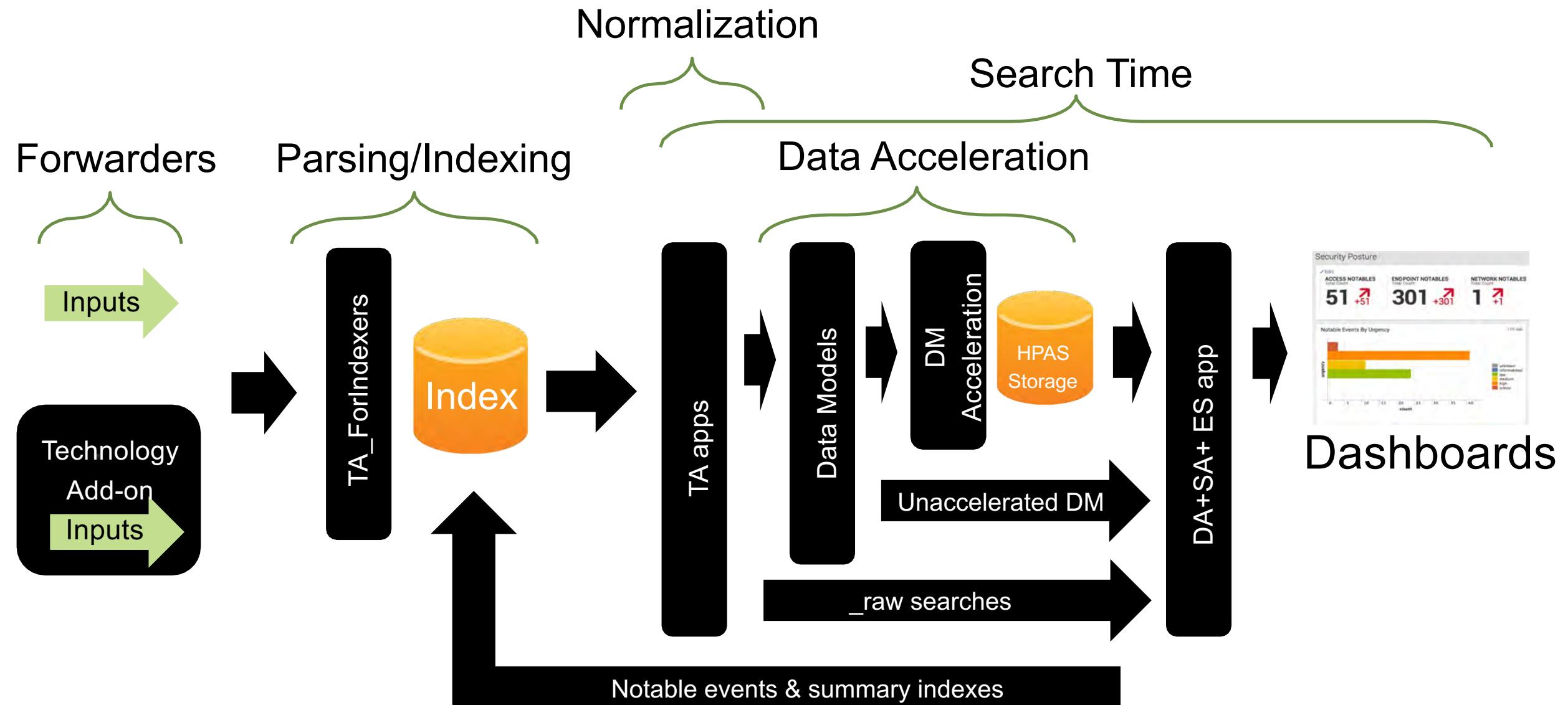
- Verify data is correctly configured for use in ES
- Validate normalization configurations
- Install additional add-ons

ES Data Flow

ES uses Splunk events for all correlation and analytical searches using the following process:

1. Data is input from its source, indexed into events and a sourcetype is applied
2. Tech add-ons apply **normalization** configurations based on the source types that assign the events to a **data model**
3. The data model events are **accelerated** and placed into accelerated storage, with retention periods up to 1 year
4. Most ES correlation searches and dashboard searches are based on accelerated data model events

From Input to Dashboard



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

ES Data Models

- ES uses data models in the **Common Information Model (CIM)**
docs.splunk.com/Documentation/CIM/latest/User/Howtouseltheserefencetables
- Each data model defines a standard set of field names for events that share a logical context, such as:
 - **Malware**: anti-virus logs
 - **Performance**: OS metrics like CPU and memory usage
 - **Authentication**: log-on and authorization events
 - **Network Traffic**: network activity
- Data models are conceptual maps, not containers

Data Normalization

- **Normalization** converts non-standard field names and values into a uniform set of standardized fields within a data model
- Report designers can build report searches based on these standard terms without knowing where the data originally came from

Example: one sourcetype has events with an **ACCESS** field, containing numeric codes like 0 (access allowed) and 1 (access denied). Another sourcetype has an **Action** field, with values “allowed” and “denied”. After normalization, both source types will have the **action** field with the same values (success or failure), making it easier to build reports

Normalization Process

- Normalization is a search-time process based on event source types and includes steps such as:
 - Adding tags, which control which events are displayed by which data models
 - Changing field aliases and values to conform to data model specifications
- Add-ons automatically normalize most common source types
- You may have to adjust normalization rules, or create new normalization add-ons for custom data

CIM Setup

ES > Configure > CIM Setup

- Use the CIM add-on to change data model settings like acceleration, index whitelist, and tag whitelist
- Enable acceleration for the data model to return results faster for searches, reports, and dashboard panels that reference the data model

The screenshot shows the 'CIM Setup' page in Splunk Enterprise Security. The 'Data Models' tab is active, displaying a list of data models with their current restriction status. The 'Alerts' data model is highlighted with a green box. The 'Settings' section on the right provides configuration options for the selected data model, including acceleration, summarization, and rebuild settings. A 'Save' button is located at the bottom right of the form.

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

CIM Setup (cont.)

ES > Configure > CIM Setup

- **Indexes whitelist** - improve performance by constraining the indexes that each data model searches (default, is all indexes)
- **Tags whitelist** - restrict the tag attribute of a data model to specific tag values to improve performance
 - By default, whitelists use the tags for the child datasets in the data model

The screenshot shows the 'CIM Setup' page in Splunk Enterprise Security. On the left, there is a list of data models: Alerts, Application State, Authentication, Certificates, Change Analysis, Change, Compute Inventory, Data Access, Databases, and DLP. Each item has a 'No restriction' note below it. On the right, there are several configuration options under the 'Settings' section:

- Acceleration: A checkbox labeled 'Accelerate' is unchecked.
- Backfill Range: A dropdown menu set to 'N/A'.
- Summary Range: A dropdown menu set to 'N/A'.
- Max Summarization Search Time: A text input field set to '3600'.
- Accelerate until maximum time: A checkbox labeled 'Accelerate until maximum time' is unchecked.
- Max Concurrent Summarization Searches: A text input field set to '3'.
- Manual rebuilds: A checkbox labeled 'Manual rebuilds' is checked.
- Schedule priority: A dropdown menu set to 'highest'.
- Indexes whitelist: An empty text input field with a 'Edit in Splunk Settings' link.
- Tags whitelist: A text input field containing 'pci,cloud'.

A green box highlights the 'Indexes whitelist' and 'Tags whitelist' fields. At the bottom right is a green 'Save' button.

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

ES Data Input Troubleshooting

- Ideally, after installing ES you will find that all the searches and dashboards work automatically
- However, if any events have non-standard source types, the normalization configurations in the tech add-ons won't work
 - Example: an admin created a sourcetype and the name is incorrect
 - Fix: specify the correct sourcetype name in your configuration files
- If you have incoming data from a technology that requires a tech add-on that does not ship with ES, you'll have to install it
- If you have custom data to use in ES, you might have to create your own TA (discussed later in the course)

Confirming Normalization

- Match your enabled TAs to CIM data models and verify the events are being added to the correct data models
 - Use the dashboard requirements matrix to determine which data models support each dashboard
docs.splunk.com/Documentation/ES/latest/User/DashboardMatrix
 - Also useful: https://www.splunk.com/en_us/blog/tips-and-tricks/relating-add-ons-to-cim.html
- If a sourcetype is not showing up in a data model:
 - Check the sourcetype
 - Make sure the TA is installed

Steps for Initial Data Verification

1. Make a list of all source types required by ES
 - This will be dependent on the exact set of technologies and security products in use at your site
2. Map the sourcetype to the TA that normalizes it
3. Confirm that the correct sourcetype name is being used
 - Verify against the TA documentation
4. Install additional TAs if needed
5. Verify that normalization is happening
 - Make sure the sourcetype is appearing in the correct data model and that all searches are executing as expected

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

Map Source Types to Tech Add-ons

1. Match each sourcetype to the tech add-on that will normalize it
 - Use add-on documentation to determine which source types are supported
docs.splunk.com/Documentation/AddOns
2. Make sure the correct sourcetype name is being set
 - Change the sourcetype setting to the correct one, or
 - Edit the TA to use the local sourcetype name variant if necessary
3. Install (or create) any missing tech add-ons
4. Disable un-needed ES tech add-ons

Finding More Add-ons

- Splunkbase has additional add-ons available for ES
<https://splunkbase.splunk.com/>
- Add-ons must be CIM-compliant to be compatible with ES
- Search Splunkbase and/or the add-on documentation for the vendor or technology names related to the sourcetype you are trying to normalize

Examining Data Model Contents

- Use the `datamodel` command to examine the source types contained in the data model
 - | `tstats count from datamodel=Network_Traffic.All_Traffic by sourcetype`
- If the sourcetype is present, the events are correctly tagged and fields can be checked for normalization
- If the sourcetype or fields are missing:
 - Locate an add-on in Splunkbase that corresponds to the vendor or technology for the sourcetype, or
 - Build your own (discussed later in the course)

Problem: Missing Cisco ASA Events

1. As you audit the data in Splunk, you find that you want to use events from the Cisco router logs with the **cisco:asa** source type
2. You confirm the data is present in Splunk indexes, but ES is not displaying it in any dashboards
3. The **Network Traffic** data model does not contain events with the **cisco:asa** source type
 - This is because the events are not being tagged with the **network** and **communicate** tags, and the fields are not being aliased to the proper names required in the data model

Solution: the Cisco Add-on

- In Splunkbase, the Splunk Add-on for Cisco ASA is:
 - CIM-compliant
 - Designed for use with ES
- Source type:
 - `cisco:asa`: Authentication, Change Analysis, Network Sessions, Network Traffic, Malware

<https://docs.splunk.com/Documentation/CIM/latest/User/NetworkTraffic>

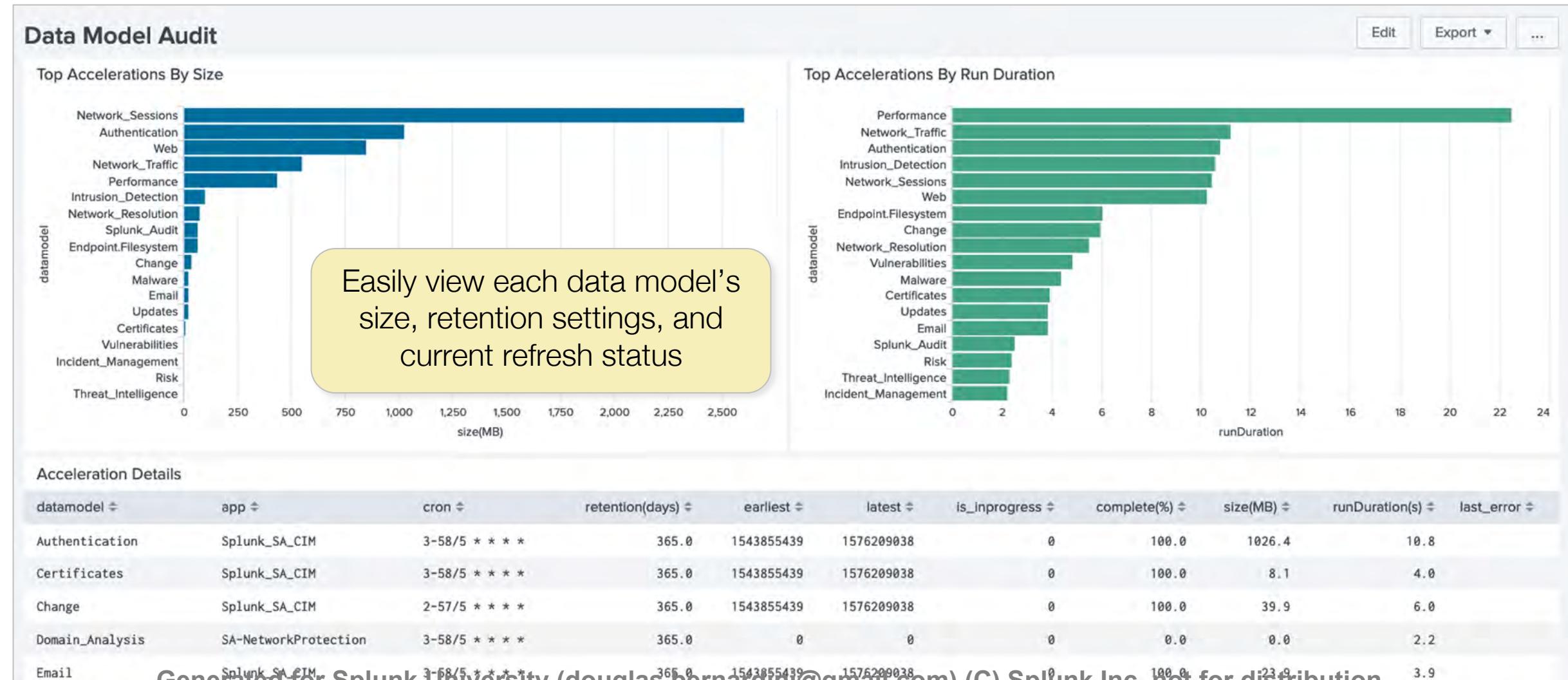
Installing Add-ons on the ES Search Head

- Not all add-ons and apps require you to restart Splunk. Check the add-on documentation on Splunkbase for individual instructions
- Knowledge objects in add-ons and apps that are installed on the same search head as ES, and are exported to other apps or exported system-wide (`export = system`) are automatically visible in ES
- Check the TA Readme file for specific add-on information
 - If it indicates it performs index-time actions, re-generate and re-deploy the `Splunk_TA_ForIndexers` add-on
 - Carry out any additional TA setup in the Readme

Data Model Audit

Audit > Data Model Audit

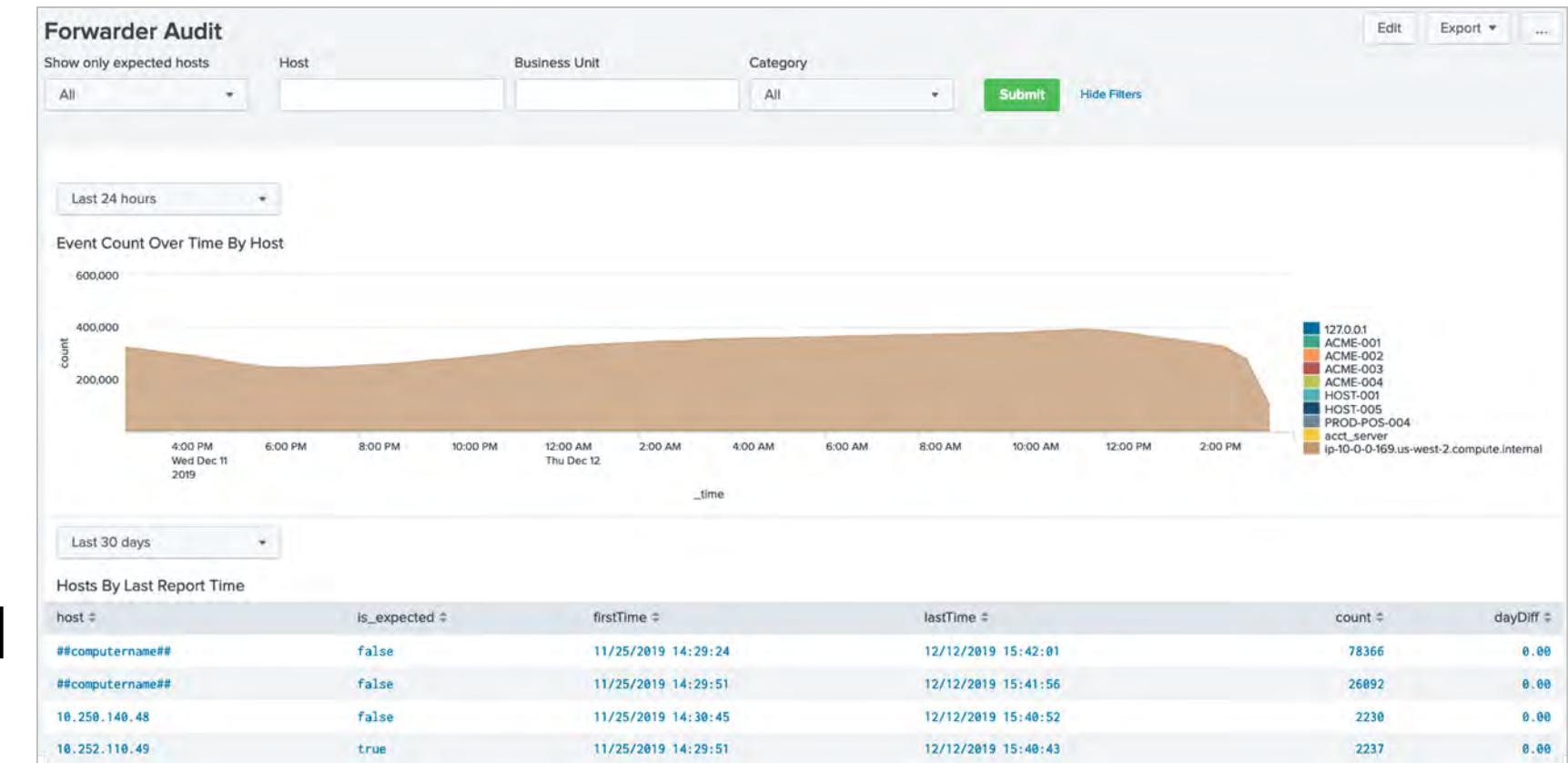
Determine which data models are using the most storage or processor time



Forwarder Audit

Audit > Forwarder Audit

- Ensures hosts are properly forwarding data to Splunk
- Detects forwarders that have failed
- Can be set to monitor all hosts, or only hosts configured as `is_expected` in the ES Assets lookup table

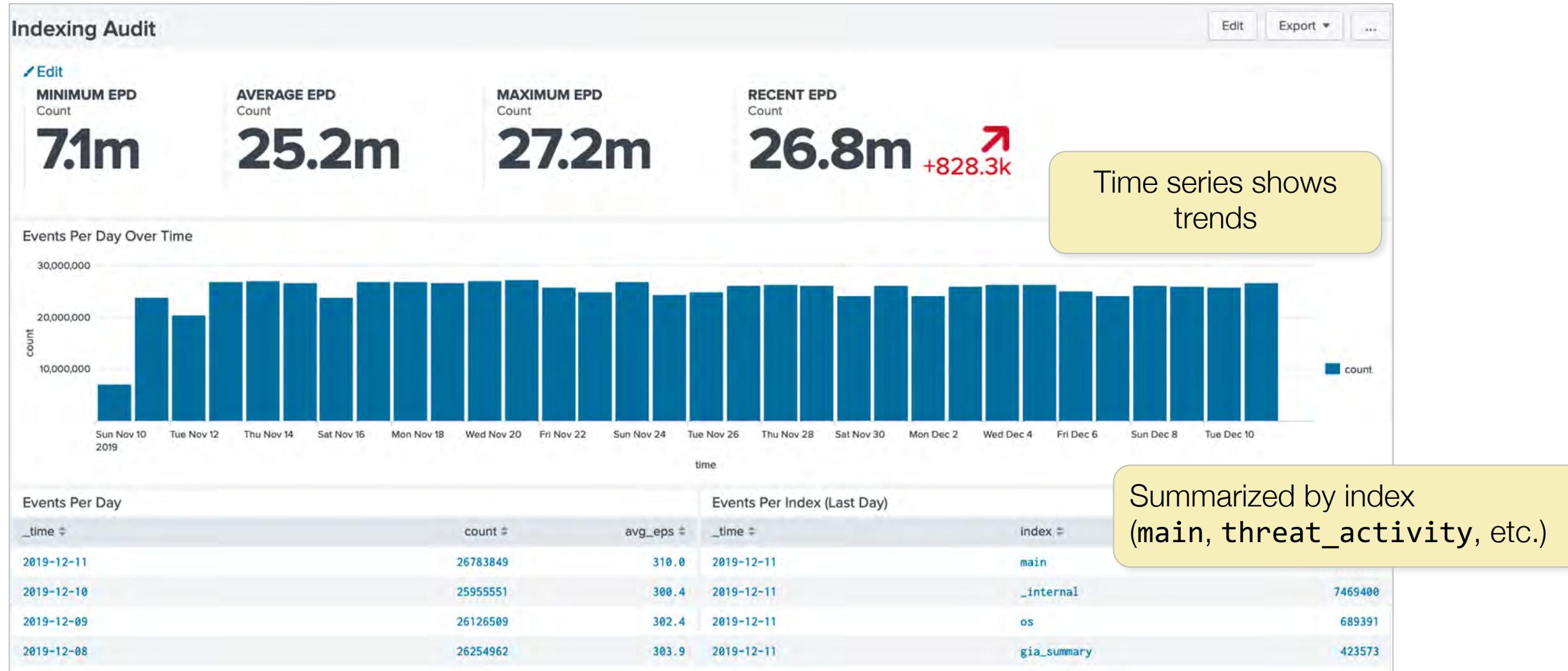


Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Indexing Audit

Audit > Indexing Audit

Summary of events indexed per day (EPD)



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

Module 7 Lab: Validate ES Data

Time: 25 minutes

Tasks:

1. Plan and verify inputs
2. Examine data model activity
3. Install a new Splunk technology add-on to automatically normalize Cisco ASA events

Module 8: Custom Add-ons

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

Objectives

- Use custom data in ES
- Create an add-on for a custom sourcetype
- Describe add-on troubleshooting

Custom Data Input

- If you have custom data sources you want ES to recognize, create an add-on to make your custom events CIM-compliant
- Your add-on should contain:
 - Data inputs and parsing (if required)
 - Field extractions (if required)
 - A tagged event type that maps your sourcetype to the appropriate CIM data model
 - Field aliases to map non-standard field names to CIM field names
 - Eval statements (calculated fields) or lookups to map non-standard field values to CIM field values

Data Models and the CIM

- Your custom events are referenced by CIM data models
 - See the CIM documentation for a list of all the data models and their contents (docs.splunk.com/Documentation/CIM)
- Once you determine which data model should reference your events, plan which CIM fields relate to your custom fields
- Example:
 - You want the **Network Traffic** data model to return your events
 - At docs.splunk.com/Documentation/CIM/latest/User/NetworkTraffic, you see the list of required and optional fields for this data model
 - You make a mapping of your fields to CIM fields

Normalization Strategy

- Not all of the source fields will match CIM fields
 - You can ignore the extra source fields as appropriate
- Not all of the CIM fields will be present in the source events
 - Use `eval` statements or regex-based field extractions to generate these fields with valid values if possible, or with placeholder values if no valid values can be determined
- Should you populate every CIM field in the target data model?
 - You need to at least populate the fields used by ES dashboards and correlation searches
 - Mapping as many of the data model fields as possible will make your events more robust for future use in new views, searches or reports

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

Planning Normalization Requirements

- Determine the dashboards that will display your events
- Use the dashboard requirements matrix to determine the data model(s) and field names the dashboard(s) require:

docs.splunk.com/Documentation/ES/latest/User/DashboardMatrix

Dashboard Name	Panel Title	Data Model	Data Model Dataset
Traffic Center	Traffic Over Time By Action	Network Traffic	All_Traffic.action
	Traffic Over Time By Protocol		All_Traffic.transport
	Scanning Activity (Many Systems)		All_Traffic.dest, .src
	Top Sources		All_Traffic.src

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

Data Model Definitions

- The data model names in the dashboard requirements matrix are linked to the data model's CIM documentation
- Use this documentation to determine the tags, field names and field values your events must use to be CIM-compliant

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Traffic	action	string	The action taken by the network device.	<ul style="list-style-type: none">• recommended• required for pytest-splunk-addon• prescribed fields: allowed blocked , teardown
All_Traffic	app	string	The application protocol of the traffic.	required for pytest-splunk-addon
All_Traffic	bytes	number	Total count of bytes handled by this device/interface (bytes_in + bytes_out).	recommended
All_Traffic	bytes_in	number	How many bytes this device/interface received.	recommended
All_Traffic	bytes_out	number	How many bytes this device/interface transmitted.	recommended

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

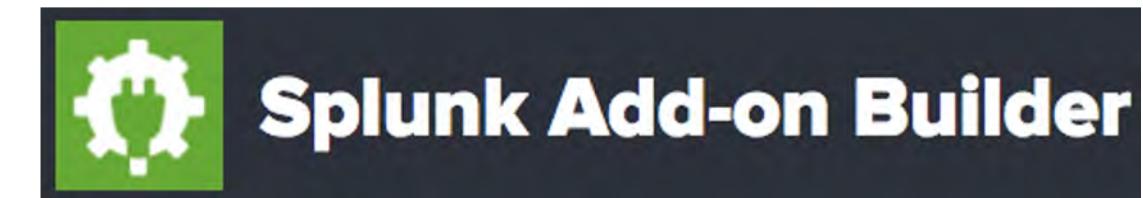
Mapping Original Fields to CIM Fields

- Plan your normalization settings using a table
- List the required CIM-compliant field names
- Match them to corresponding original source fields
- Determine if normalization is required for each field's name and value

Original	CIM	Procedure
sender	src	alias
receiver	dest	alias
method	app	alias
user	user	none
account	unused	ignore
missing	signature	Use eval to create default value
SSID	unused	regex to mask all but last 4 digits
status	action	Use eval to translate source numeric codes to CIM terms
...	...	

Splunk Add-on Builder

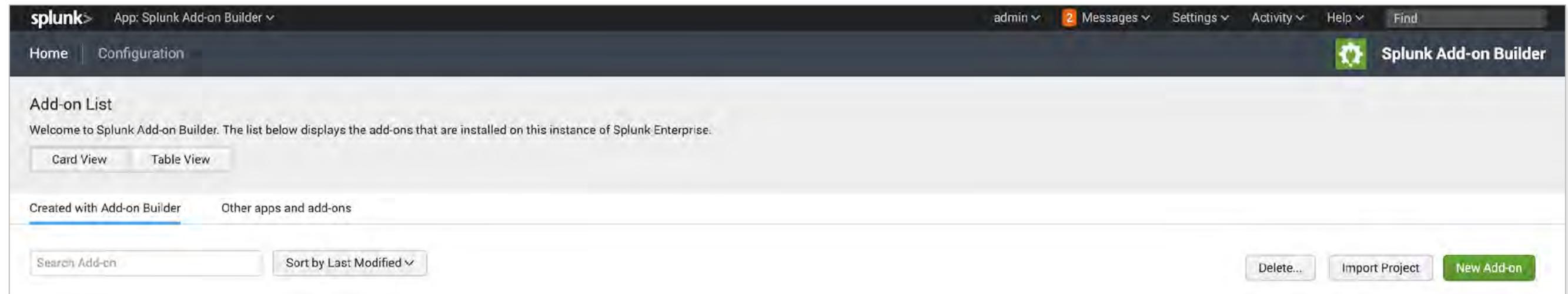
- Very fast way to build out the initial TA
- Use it to create source types, extractions, and data model mapping
- TAs can:
 - Automatically input data into Splunk
 - Extract fields and map fields to the CIM
 - Create alert actions



<https://docs.splunk.com/Documentation/AddonBuilder/latest/UserGuide/Overview>

Add-on Builder: Getting Started

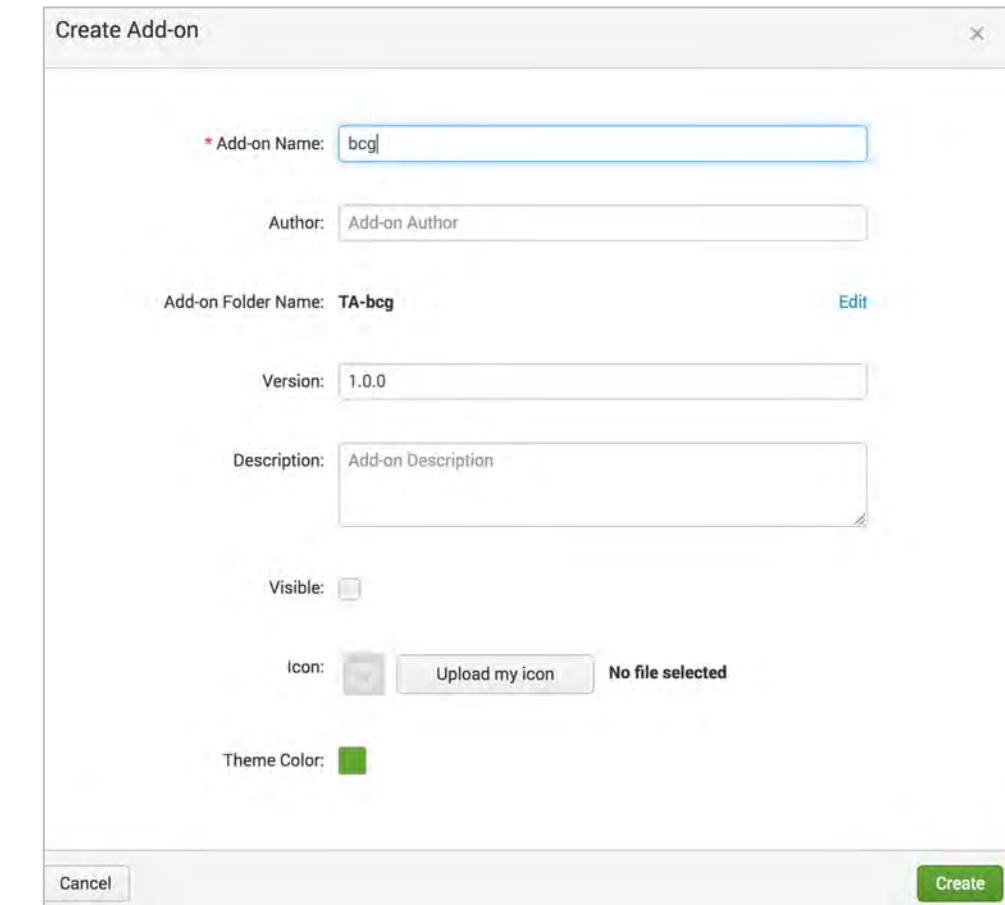
- Install the Add-on Builder from Splunkbase
- Navigate to the Add-on Builder home page
- Click **New Add-on**



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

Add-on Builder: Create Add-on

- Enter a name for the add-on
 - This field becomes the name of the new app
 - The builder adds a TA- prefix
- Add other optional project items
- Click **Create**
 - This creates a new add-on app on the local Splunk server
- Your add-on home page is displayed
- You may see a system message to restart Splunk – you can defer this until done with the new add-on



Add-on Builder Home Page

Screenshot of the Splunk Add-on Builder Home Page.

The top navigation bar includes:

- b6g | Configure Data Collection
- Manage Source Types (highlighted)
- Extract Fields
- Map to Data Models (highlighted)
- Create Alert Actions
- Validate & Package (highlighted)
- Splunk Add-on Builder

The main content area features three large yellow callout boxes numbered 1, 2, and 3:

- 1 Manage Source Types
- 2 Map to Data Models
- 3 Validate and Package

Below these are two large green icons:

- A cylinder icon with a downward arrow, representing **Configure Data Collection**.
- A gear icon with arrows, representing **Create Alert Actions**.

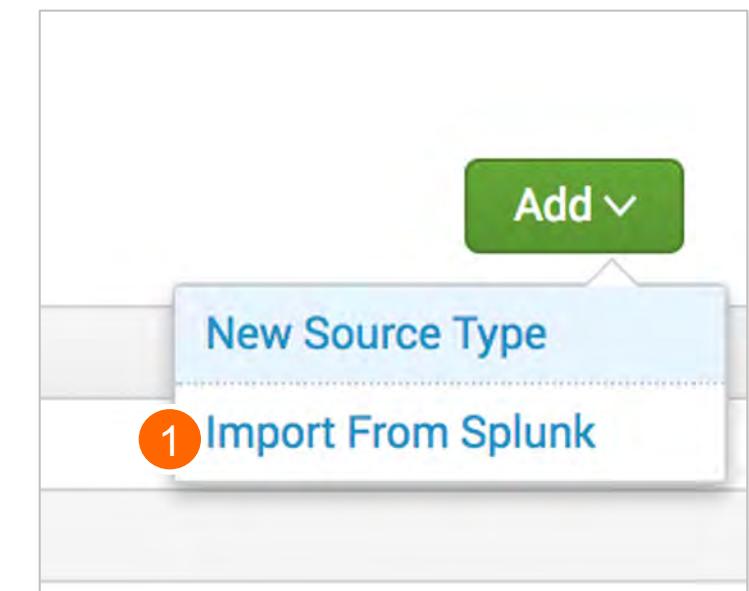
The **Add-on Summary** section displays the following metrics:

Validation Score	Data Inputs	Extracted Fields	Event Types	Alert Actions
-	0	0	0	Note The Add-on Builder can do a lot of things, but for CIM normalization you only need to add sample data and the CIM mapping function.

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

Add-on Builder: Sample Data

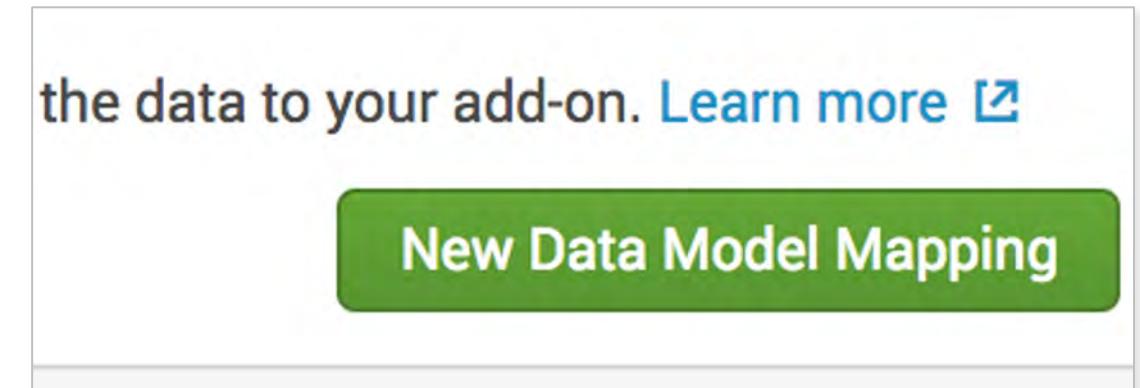
- Select **Manage Source Types**
 - May need to reboot first if add-on is newly created
- If your sample data is already in Splunk, use **Add > Import from Splunk**
 - Select from a sourcetype list and click **Save**
 - You also specify event breaks, time-stamping and other settings
- You can add multiple source types if desired

A screenshot of the 'Import from Splunk' configuration dialog. At the top left is a header 'Import from Splunk'. On the right are 'Cancel' and 'Save' buttons, with a red circle containing the number '3' over the 'Save' button. The main area contains a dropdown menu with 'bcg_accounting' selected, a search bar with 'bcg' typed, and an 'Upload Data (optional)' field showing 'No file selected'. Below these fields are two tabs: 'Time' and 'Event'. A red circle containing the number '2' is placed over the 'bcg' search input field.

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

Data Model Mapping

- Select Map to Data Models
- Click New Data Model Mapping
- Enter a name for the new event type
- Select the source type you are mapping
- Click Save
- The Data Model Mapping Details view opens



A screenshot of a "Data Model Mapping > Define Event Type" dialog box. The dialog has a title bar with "Data Model Mapping > Define Event Type", a "Cancel" button, and a "Save" button. The main area contains fields for "Enter a name for the event type" (with "bcg_acct" typed in), "Select one or more source types" (with "bcg_accounting" selected), and "Enter a search" (with the search term "(sourcetype=bcg_accounting)" entered). A green arrow points from the bottom left towards the "Save" button. The dialog also includes a "Learn more" link and some descriptive text about defining event types.

Add-on Builder: Event Types

- Before you can add data model mappings, you must identify your sourcetype(s) with an event type
 - This is used to generate the correct tags for your events to match the CIM target data model's constraints
- On the **Data Model Mapping Details** page, each sourcetype you added in the sample data must map to one event type
 - More than one sourcetype can map to the same event type
- You can also add search criteria to filter out unwanted events from your data model mapping
 - This excludes the events from the data model acceleration

CIM Mapping

Data Model Mapping >> Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type. Starting by selecting the data models and datasets you want to use, then click **New Knowledge Object** to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. [Learn more](#)

Event Type Fields

- Edit Event Type...
- Search event type fields
- bcg_acct
 - action
 - src
 - src_port
- CRC
- date_hour
- date_mday
- date_minute
- date_month
- date_second
- date_wday
- date_year
- date_zone

Data Model Mapping List

Source Type	Object Type	Event Type Field or E...	Data Model Field	Actions
* bcg_accounting	FIELDALIAS	dst_port	dest_translated_port	OK Cancel
bcg_accounting	EVAL	case(action="allow", ...	action	Edit Delete
bcg_accounting	FIELDALIAS	host_from	src	Edit Delete

Note

The source event type or expression field can be an **eval** statement (to transform the source value to the CIM required format).

1 Select one or more target data models

2 Select FIELDALIAS or EVAL from the New Knowledge Object drop-down

3 Select a source field

4 Select a target field

5 Click OK

6 Click Done

Done

Data Model Fields

- Select Data Model(s)...
- Search model fields
- Splunk_SA_CIM
 - All Traffic(47)
 - action
 - src
 - src_port
 - app
 - channel
 - dest_interface
 - dest_ip
 - dest_mac
 - dest_translated_ip
 - dest_translated_port

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

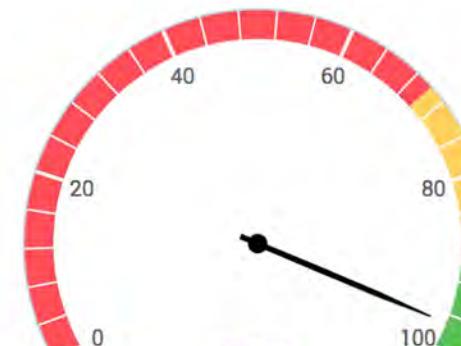
Add-on Builder: Validate and Package

- You can validate your add-on for best practices, CIM mapping, and field extractions
 - Any errors indicate a problem that should be corrected
 - Warnings are non-fatal but might need attention
 - If you select **App pre-certification**, a Splunkbase login is required
- Use Download Package to create an **SPL package** you can deploy to your production environment
 - The add-on is already active on the local system

Add-on Builder: Validate and Package (cont.)

Validate & Package
Click **Validate** to validate your add-on against best practices and other rules, and to determine whether your app is ready for Splunk App Certification. When you have finished creating your add-on, click **Download Package** to create and download the SPL package file. [Learn more](#)

Overall Health Report



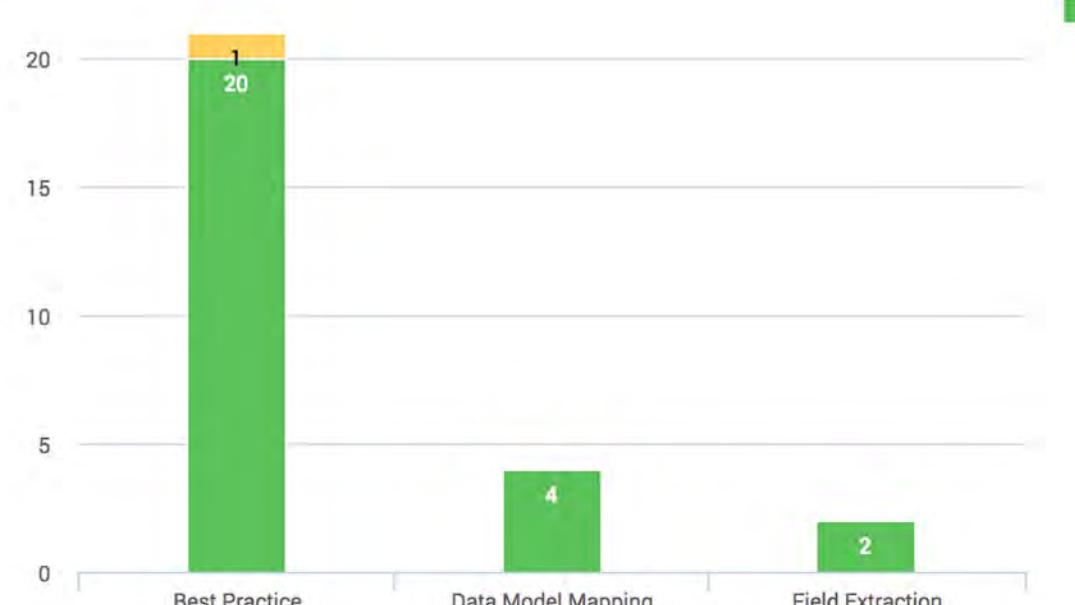
1 Select validations to apply

2 Click to start validation

3 Click to download

No results for certification
App precertification validation has not been performed.

0 Error 1 Warning 26 Pass



Validation Results

Rule Name	Severity	Category	Description	Solution Suggestion
No underscores in sourcetypes	Warning	Best Practice Validation	The bcg_accounting and bcg_accounting) sourcetype contains an underscore (_).	Change the unders
Validate field conflicts	Pass	Field Extraction Validation	Pass the field validation for knowledge object "EVAL-action" in sourcetype "bcg_accounting".	

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

Module 8 Lab: Building a Custom Add-on

Time: 30 minutes

Tasks:

1. Plan a new add-on for custom data
2. Create the add-on with the Splunk Add-on Builder
3. Validate the new add-on

Module 9: Tuning Correlation Searches

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

Objectives

- Describe correlation search operation
- Customize correlation searches
- Describe numeric vs. conceptual thresholds

Plan, Install, Evaluate, Refine

- Start with a base level of enabled correlation searches
 - Security events in the enterprise
 - Anomalous audit trails
- Adjust correlation search sensitivity
 - False positives: returning results when none are actually there
 - False negatives: returning no results when something is expected
- Revisit and adjust thresholds as needed
 - New security data is added to your ES install
 - The size of what is monitored shrinks or grows
 - Decreased number of open issues (i.e., ES is working!!)

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

ES Managed Content

- Correlation searches are one type of ES content
 - Correlation searches are stored as saved searches
 - Content in ES is any search or view that can be shared and used between multiple ES sites
- Examples:
 - Correlation and Key Indicator searches
 - Entity (asset or identity) swim lane searches
 - Lookups
 - Views (dashboards and panels)
 - Saved searches

Content Management Functions

Configure > Content > Content Management

Add new content

Create New Content ▾

Content Management

Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, and reports.

< Back to ES Configuration

Filter by Type, App, Status, or text

1702 Objects Edit selection ▾ 1 selected Clear Type: All (1) ▾ App: All (1) ▾ Status: All ▾ filter ⏪ Prev 1 2 3 4 ⏩ Next > 25 per page ▾

<input type="checkbox"/>	<input type="checkbox"/>	Name	Type	App	Next Scheduled Time	Actions
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Number of Endpoint Changes By User	Correlation Search	DA-ESS-EndpointProtection		Enable Disabled Clone
<input type="checkbox"/>	<input type="checkbox"/>	Number of HTTP Method Events By Src	Correlation Search	DA-ESS-NetworkProtection	Jul 13, 2021 4:50 PM UTC	Enabled Disable Clone
Lookup Gen			Lookup Generating Search	SA-AccessProtection	Jul 13, 2021 4:30 PM UTC	Enable , disable or clone content
Access - Access Over Time By Action			Saved Search	DA-ESS-AccessProtection		
Access - Access Over Time By App			Saved Search	DA-ESS-AccessProtection		
Access - Account Usage For Expired Identities			Saved Search	DA-ESS-AccessProtection		
Access - All Authentication By Asset - Swimlane			Swim Lane Search	DA-ESS-AccessProtection		
Click a title to edit Identity - Swimlane			Swim Lane Search	DA-ESS-AccessProtection		
Access - Authentication Failures By Source - Model Gen			Saved Search	SA-AccessProtection	Jul 14, 2021 3:00 AM UTC	
Access - Authentication Failures By Source Per Day - Model Gen			Saved Search	SA-AccessProtection	Jul 14, 2021 5:00 AM UTC	

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

Content Management Functions (cont.)

Configure > Content > Content Management

The screenshot shows the 'Content Management' page in Splunk Enterprise Security. At the top, there's a header with 'Content Management', a sub-header 'Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, and reports.', and a 'Create New Content' button. Below the header are filters for 'Type' (Correlation ... (1)), 'App' (All (1)), 'Status' (All), a search bar, and a 'Clear filters' button. The main area displays a table of 346 objects, with the first item being 'Activity from Expired User Identity'. A yellow callout box points to the 'Name' column header, stating 'Expand the Information (i) column to verify dependency and usage information'. Another yellow callout box points to the details section for 'Activity from Expired User Identity', stating 'The details for each type of content, and each individual knowledge object vary'. The table columns include Name, Type, App, Next Scheduled Time, and Actions. The 'Actions' column for the first item shows 'Enable | Disabled | Clone'. The 'Statistics' and 'Data Models' sections are also visible on the left.

Name	Type	App	Next Scheduled Time	Actions
Activity from Expired User Identity	Correlation Search	DA-ESS-EndpointProtection		Enable Disabled Clone
	Correlation Search	DA-ESS-NetworkProtection	Jul 13, 2021 4:50 PM UTC	Enabled Disable Clone
	Correlation Search	SA-AccessProtection		Enable Disabled Clone Change to scheduled
	Correlation Search	SA-IdentityManagement	Jul 13, 2021 4:30 PM UTC	Enabled Disable Clone

Activity from Expired User Identity
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).

Statistics

- Avg. Event Count ... 5.663
- Avg. Result Count ... 1.143
- Avg. Run Time 0:00:01
- Invocations 294
- Skipped 0
- Success 294
- Update Time Jul 13, 2021 11:30:00 AM

Data Models

- Identity_Management

<http://docs.splunk.com/Documentation/ES/latest/Admin/Expandcontentmanagementsearches>

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

Enabling Correlation Searches

- Only enable correlation searches that make sense for your environment
- Consider:
 - Types of vulnerabilities or threats you have determined might exist
 - Type of security operations you are focused on, i.e., malware, intrusion detection, audit, change monitoring, etc.
 - You may need to increase hardware specs if you have many correlation searches running
 - You can improve overall performance by making less critical correlation searches scheduled instead of real-time

Scheduling a Correlation Search

- By default, all correlation searches run in indexed real-time mode
- If changed to scheduled, it will execute every 5 minutes by default
- When editing the scheduled search, you can change the time range settings **Start time**, **End time**, and **Cron Schedule**

Next Scheduled Time	Actions
Jan 5, 2021 1:05 PM MST	Enabled Disable Clone
Jan 5, 2021 12:50 PM MST	Enabled Disable Clone
	Enable Disabled Clone Change to scheduled
Jan 5, 2021 12:10 PM MST	Enabled Disable Clone
Jan 5, 2021 12:10 PM MST	Enabled Disable Clone Change to scheduled
	Enable Disabled Clone

Time Range

Earliest Time: -1h@h
Set a time range of events to search. Type an earliest time using relative time modifiers.

Latest Time: +5m@m
Type a latest time using relative time modifiers.

Cron Schedule: */5 * * * *
Enter a cron-style schedule. For example "*/5 * * * *" (every 5 minutes) or "0 21 * * *" (every day at 9 PM). Real-time searches use a default schedule of "*/5 * * * *".

Scheduling: Real-time Continuous
Controls the way the scheduler computes the next execution time of a scheduled search. This controls the realtime_schedule setting. [Learn more](#)

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

Tuning Correlation Searches

- **Threshold:** the criteria that causes a correlation search to trigger
- **Scheduling and throttling:** how often to run the search and how often to generate notable events for the same type of incidents
- **Adaptive Responses:** list of actions to take, including possibly creating a notable event or setting risk
 - **Notable event settings:** severity, default owner, default status, etc.
 - **Risk:** assigning, increasing, or decreasing the risk score for a given type of threat or incident
 - Other adaptive responses include sending email, running scripts

Correlation Thresholds

- Some correlation searches may generate more (or fewer) notable events than you want
- Examine the search string and look for comparison terms in `search` or `mltk` models and modify as appropriate for your environment
- Two types of thresholds:
 - Numeric
 - Conceptual (Machine Learning Based)

docs.splunk.com/Documentation/ES/latest/User/ConfigureCorrelationSearches

Numeric Thresholds

- Simple numeric comparisons
- Example: **Excessive DNS Failures**
- Note where command with numeric comparison
- Change the numeric value if you need to alter how frequently notable events are generated in your environment

Search

```
I tstats summariesonly=true allow_old_summaries=true count from  
datamodel="Network_Resolution"."DNS" where "DNS.reply_code"!="No  
error" AND "DNS.reply_code"!="NoError" by "DNS.src" I rename  
"DNS.src" as "src" I where 'count'>100
```

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

Conceptual Thresholds

- Uses Machine Learning Tool Kit (MLTK) functions
- Note the `mltk_apply_upper` macro is using “high” as a threshold
- Macro arguments:

- **model**

Name of the model for applying data and comparing against standards to find outliers. For example:

`app:failures_by_src_count_1h`

- **Qualitative_id**

Default IDs that correspond to percentages of deviation, representing where on the distribution curve to look for outliers. For example: `high`, `medium`, `low`

- **field**

Where to search for or count outliers, such as `failure`

Brute Force Access Behavior Detected correlation search

```
| tstats `summariesonly` values(Authentication.app) as app,count from  
datamodel=Authentication.Authentication by Authentication.action  
,Authentication.src | `drop_dm_object_name("Authentication")` | eval  
success=if(action="success",count,0),failure=if(action="failure",count  
,0) | stats values(app) as app,sum(failure) as failure,sum(success) as  
success by src | where success > 0 | `mltk_apply_upper("app  
:failures_by_src_count_1h", "high", "failure")`
```

Correlation Search Throttling

- Once a correlation search has been triggered, you probably don't want it to immediately re-trigger again for the same issue
- Most OOTB correlation searches throttle alerts to once a day
- If you want to modify this, change the **Window duration**
- In most cases, leave the **Fields to group by** alone

Throttling

Window duration second(s) ▾

How much time to ignore other events that match the field values specified in Fields to group by.

Fields to group by

Type the fields to consider for matching events for throttling. [Learn more ↗](#)

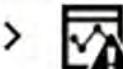
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Adaptive Response Actions

- When a correlation search detects an issue, it can initiate one or more adaptive response actions
- The most common response is to create a notable event
- Many also add risk to the objects associated with the issue
- Other responses can include sending email, running a script, stream capture, and sending data to UBA

Adaptive Response Actions

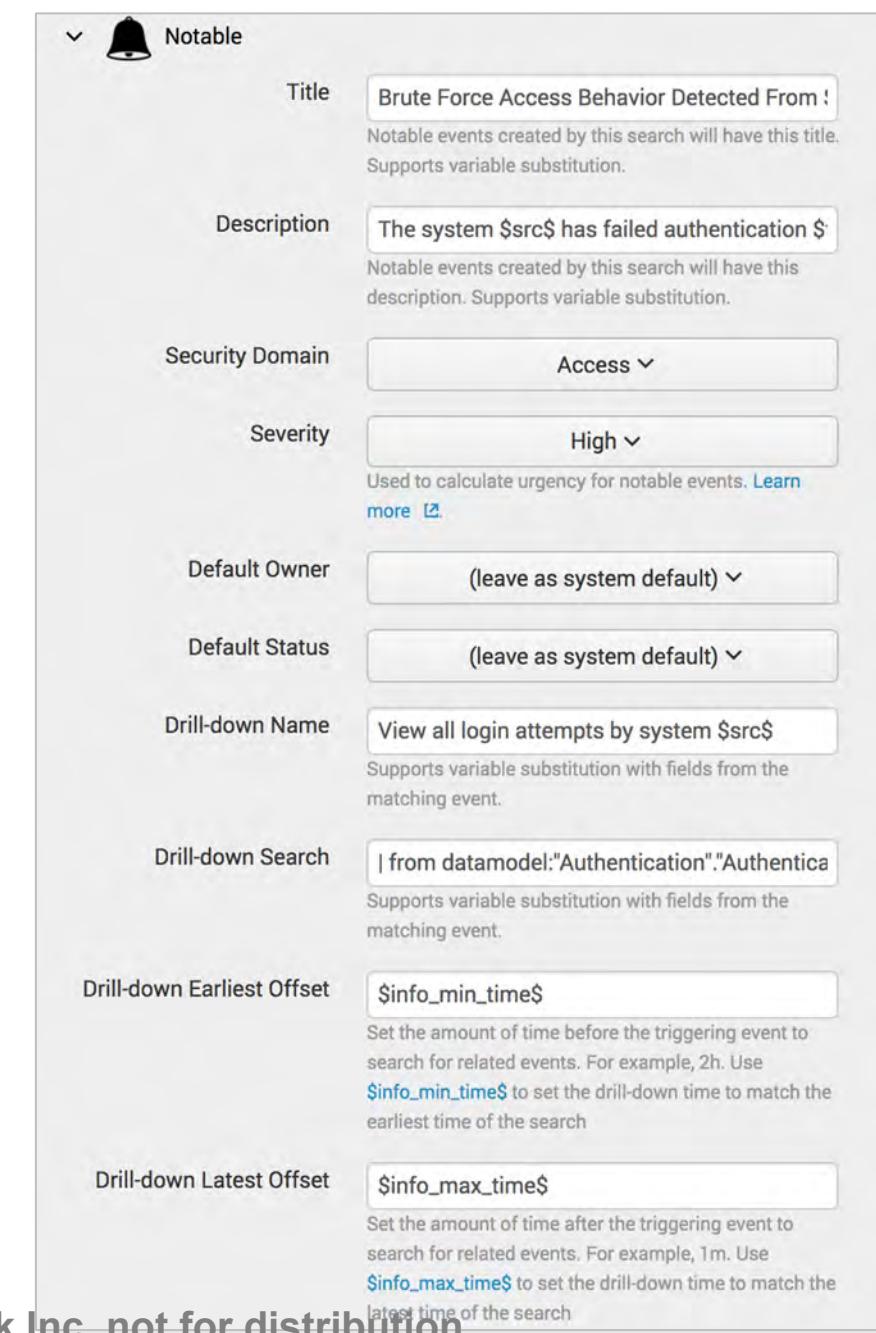
[+ Add New Response Action ▾](#)

>  Risk Analysis	x
>  Notable	x

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

Customizing Notable Event Default Values

- Expand the notable adaptive response
- You can modify all the properties of the notable event that is created by a triggered correlation search – typically:
 - Severity
 - Default Owner
 - Default Status



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

Module 9 Lab: Tuning Correlation Searches

Time: 15 minutes

Tasks:

1. Identify thresholds in correlation searches

Module 10: Creating Correlation Searches

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

Objectives

- Create a custom correlation search
- Manage adaptive responses
- Manage content import/export

Creating a New Correlation Search

1. Determine a pattern of events that indicates an issue you want to respond to with a notable event or other action
2. Create a new correlation search in the UI using **Configure > Content > Content Management** and select **Create New Content > Correlation Search**
 - Use Guided Mode if desired
3. Configure scheduling and throttling
4. Configure the adaptive responses (notable event, etc.)

Correlation Search Example: Risk

- This example creates a new correlation search that generates a notable event once a day for any server with a risk score over 100
- On the **Content Management** page, select **Create New Content > Correlation Search**
- Enter the search name, App, UI Dispatch Context, and Description
- Select **Guided Mode** to create the actual search

Correlation Search

Search Name: High Risk Asset Detected

App: Enterprise Security

UI Dispatch Context: Enterprise Security

Description: an object with a risk score over 100 has been detected.

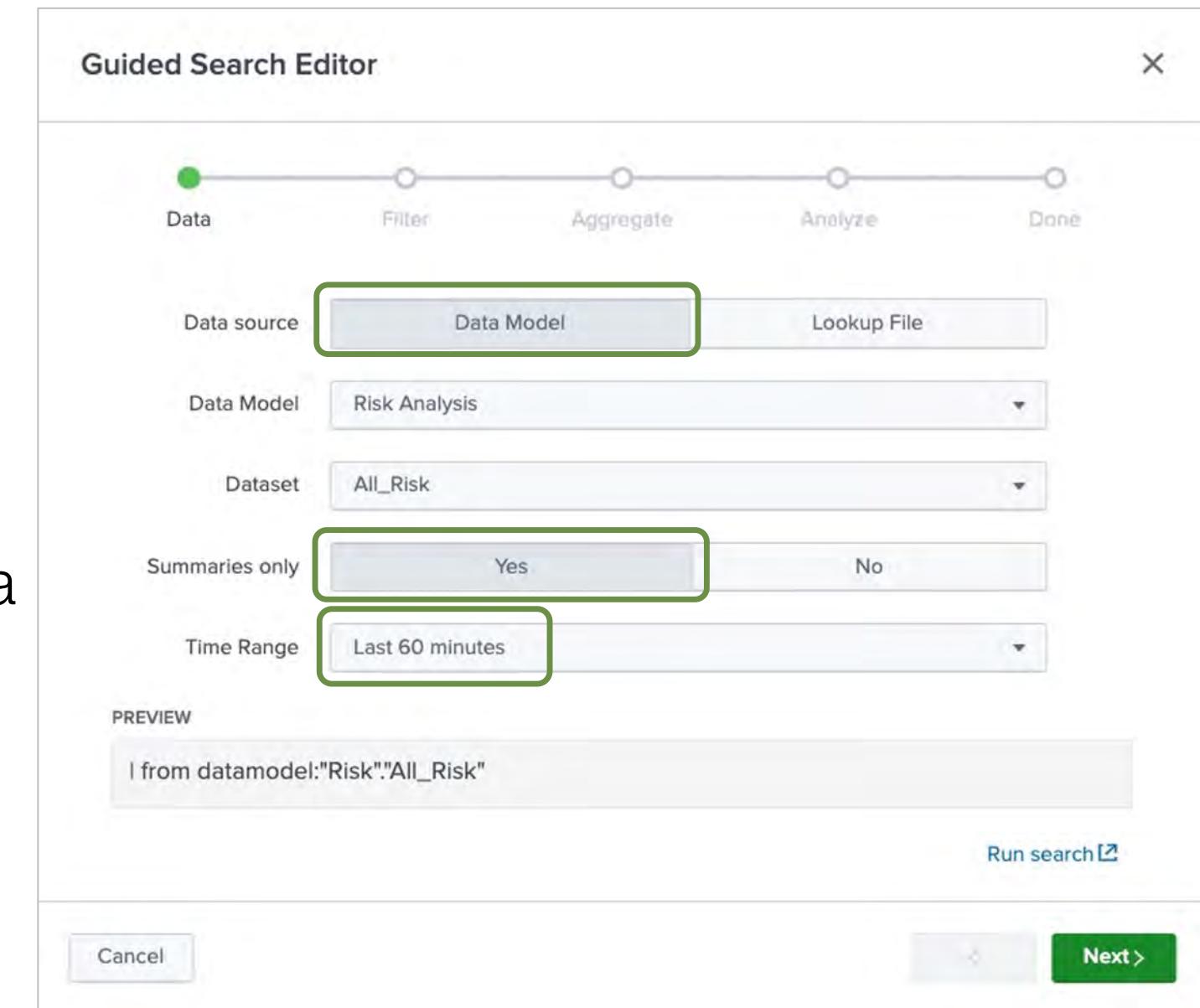
Mode: Guided (highlighted)

Manual

Search: [Edit search in guided mode](#)

Correlation Search Example: Risk (cont.)

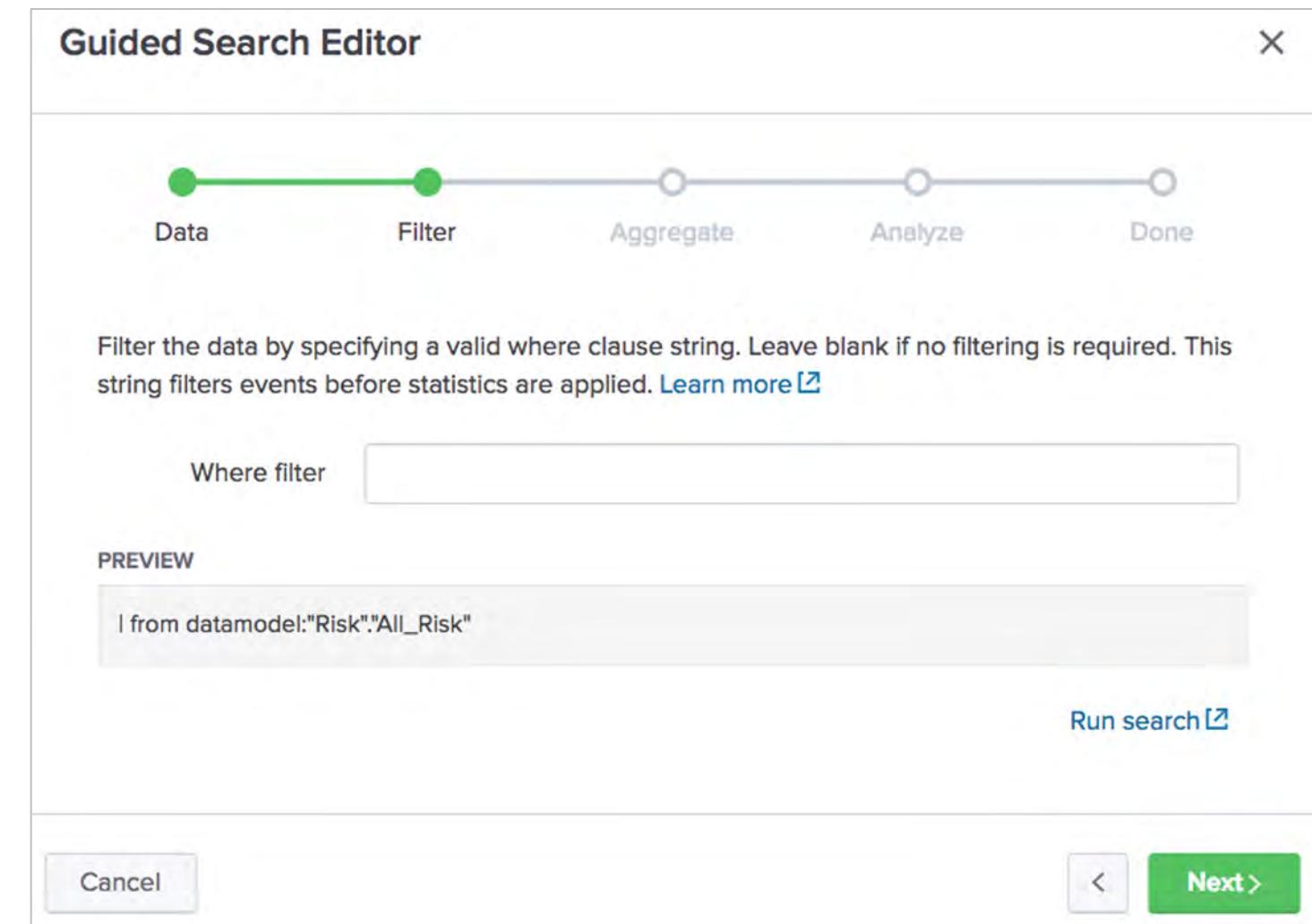
- From the **Guided Search Editor**, select the **Risk Analysis** data model and the **All_Risk** dataset
- Set **Summaries only** to **Yes**
 - The correlation search will only search in accelerated data
 - This is faster, but un-accelerated data is ignored
- Select the time range for the search
- Click **Next**



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

Adding a Where Filter

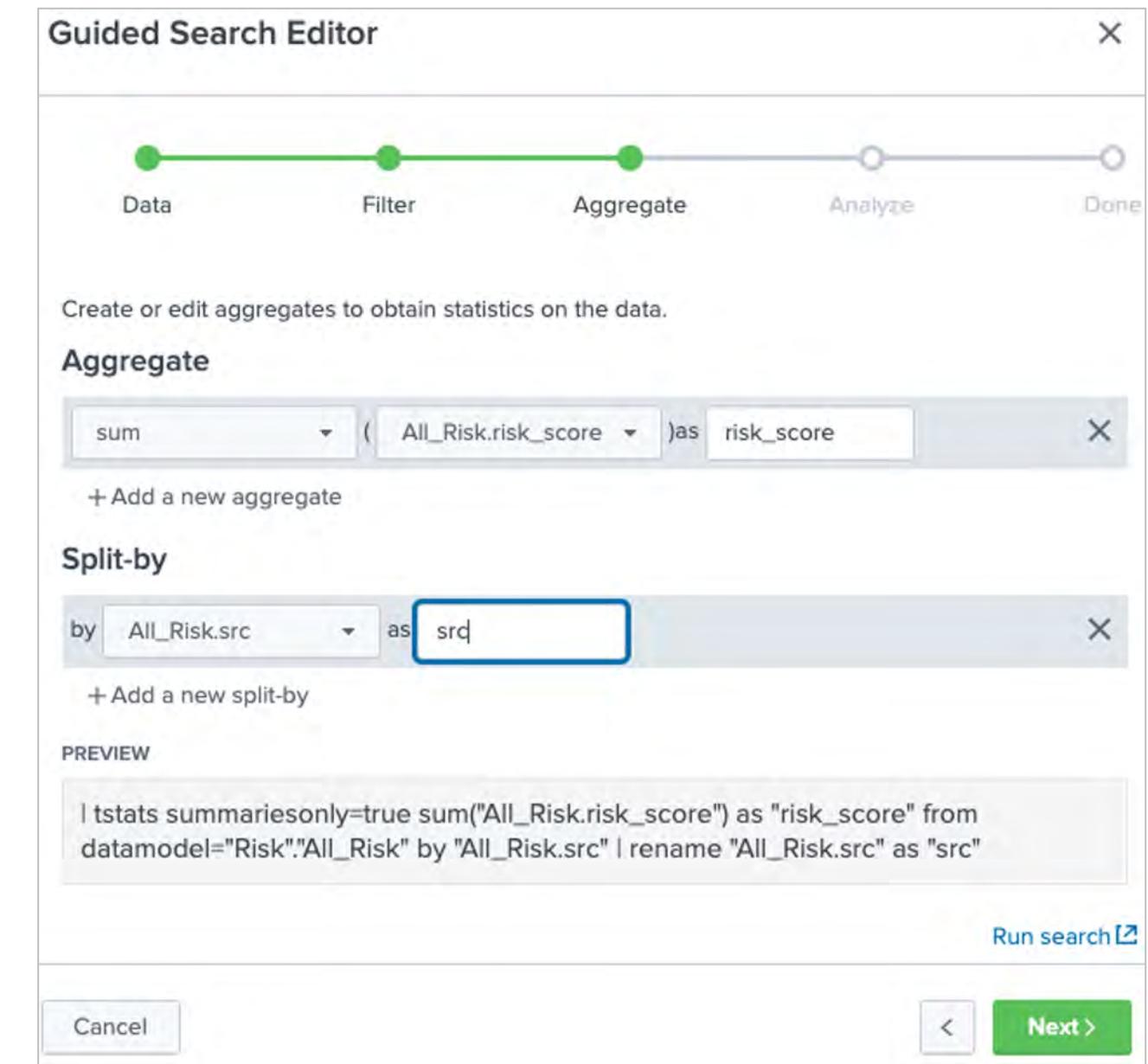
- Next, add filter expressions to limit the source events the correlation search retrieves
 - This could be used to focus on high priority assets or specific business units



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

Adding Aggregate and Split-by Functions

- Next, add aggregate functions to perform operations like count, sum, or average on fields in the data model
- Optionally, add split-by conditions to aggregate values categorically
 - The example takes the sum of all risk per source (src)
- Click **Next**



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

Adding Filters

- Define the logic to determine what condition will trigger a new notable event
- In this case, a notable event is generated if the risk score for any one source is greater than 100
- Click **Next**

Guided Search Editor

Data Filter Aggregate Analyze Done

Filter

Field: risk_score

Comparator: Greater than

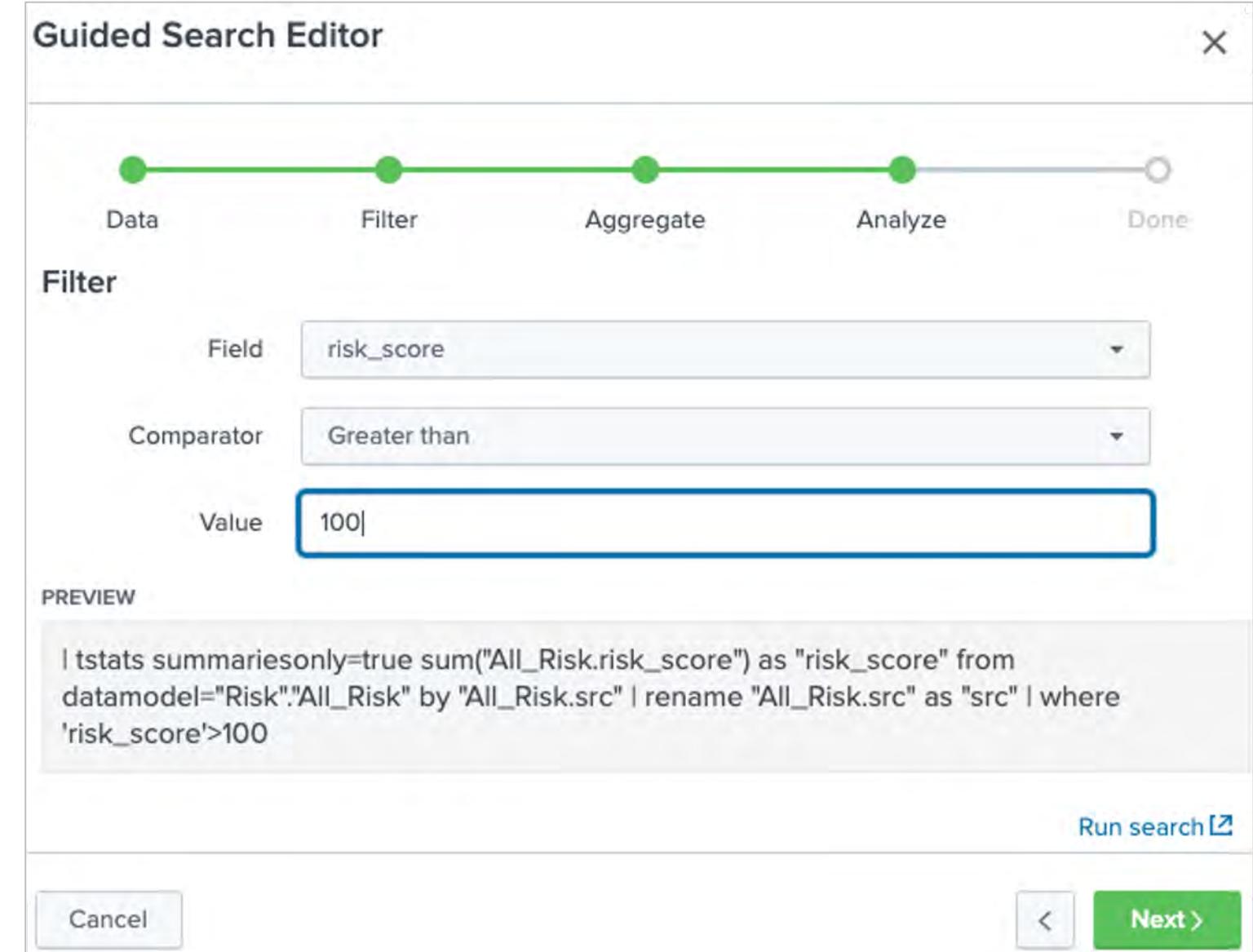
Value: 100

PREVIEW

```
I tstats summariesonly=true sum("All_Risk.risk_score") as "risk_score" from datamodel="Risk"."All_Risk" by "All_Risk.src" | rename "All_Risk.src" as "src" | where 'risk_score'>100
```

Run search ↗

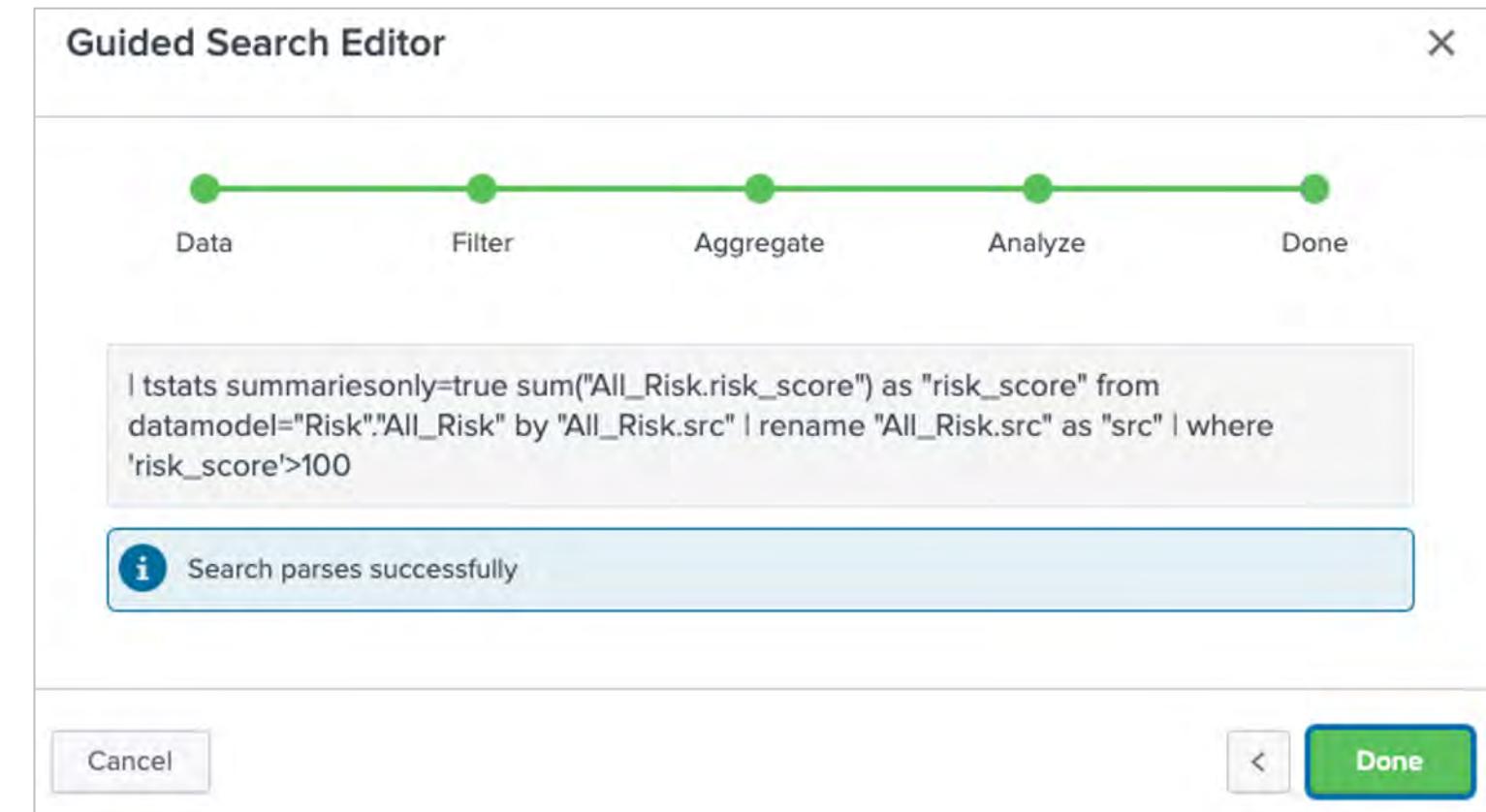
Cancel < Next >



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

Parsing the Search

- Finally, the search is parsed and displayed
- After verifying the test, select **Done** to save the correlation search criteria and continue configuring the rest of the correlation search fields
- If you edit the search string manually later, you will not be able to use guided mode to modify the search string



Setting the Time Range

- Configure time range options
 - Earliest Time and Latest Time are relative to the scheduled start time
 - Cron schedule is how often to run the search
 - The default is `*/5 * * * *` which is every five minutes
 - This is overruled if the correlation search is set to real time

Time Range

Earliest Time
-60m@m

Set a time range of events to search. Type an earliest time using relative time modifiers.

Latest Time
now

Type a latest time using relative time modifiers.

Cron Schedule
`*/5 * * * *`

Enter a cron-style schedule. For example `*/5 * * * *` (every 5 minutes) or `0 21 * * *` (every day at 9 PM). Real-time searches use a default schedule of `*/5 * * * *`.

Setting Annotations

- Annotations can enrich correlation search results with the context from industry-standard mappings
 - Enter any annotation attributes for CIS 20, Kill Chain, or NIST
 - For MITRE ATT&CK, choose the attributes from the dropdown list

Annotations

CIS 20	Type an attribute and press enter
Kill Chain	Type an attribute and press enter
MITRE ATT&CK	T1546.004 × T1003.008 ×
NIST	Type an attribute and press enter

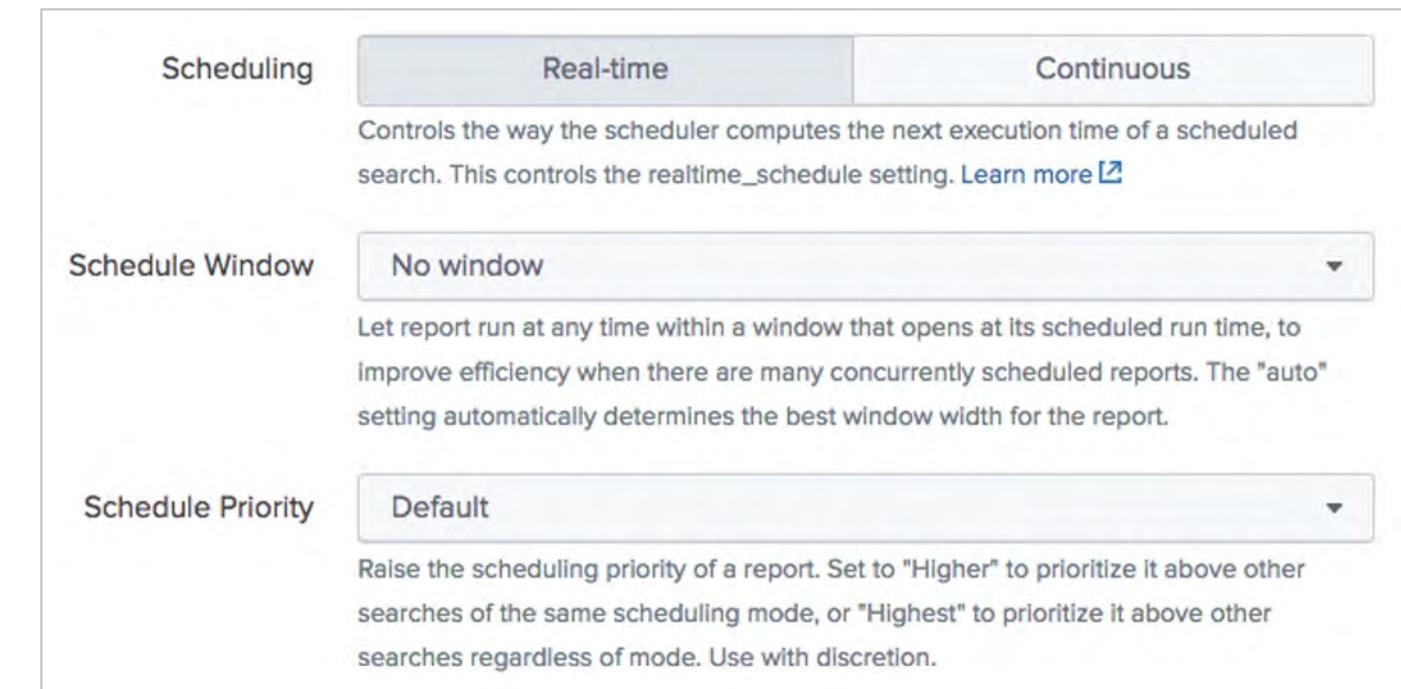
A dropdown menu is open over the NIST input field, listing several MITRE ATT&CK tactics:

- T1557.002 (highlighted with a blue border)
- T1558.004
- T1548
- T1134
- T1546.008
- T1531
- T1087
- T1098
- T1583
- T1595
- T1098.003

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

Scheduling Settings

- **Scheduling:** real-time or continuous
 - Manages real-time scheduling
 - Typically, leave the default of real-time
- **Schedule Window:** seconds (or “auto”)
 - Allow some flexibility in scheduling to improve scheduling efficiency
- **Scheduling Priority:** higher-priority searches will be selected first by scheduler if a conflict occurs
docs.splunk.com/Documentation/Splunk/latest/Admin/Savedsearchesconf#Scheduling_options



The screenshot shows the 'Scheduling' section of the configuration file. It includes three tabs: 'Real-time' (selected), 'Continuous', and 'Schedule Window'. The 'Real-time' tab contains a note about controlling execution time via the `realtime_schedule` setting. The 'Schedule Window' tab is set to 'No window', which allows reports to run at any time within their scheduled run time to improve efficiency. The 'Schedule Priority' tab is set to 'Default', which prioritizes searches based on mode.

Scheduling	Real-time	Continuous
Controls the way the scheduler computes the next execution time of a scheduled search. This controls the <code>realtime_schedule</code> setting. Learn more		

Schedule Window	No window
Let report run at any time within a window that opens at its scheduled run time, to improve efficiency when there are many concurrently scheduled reports. The "auto" setting automatically determines the best window width for the report.	

Schedule Priority	Default
Raise the scheduling priority of a report. Set to "Higher" to prioritize it above other searches of the same scheduling mode, or "Highest" to prioritize it above other searches regardless of mode. Use with discretion.	

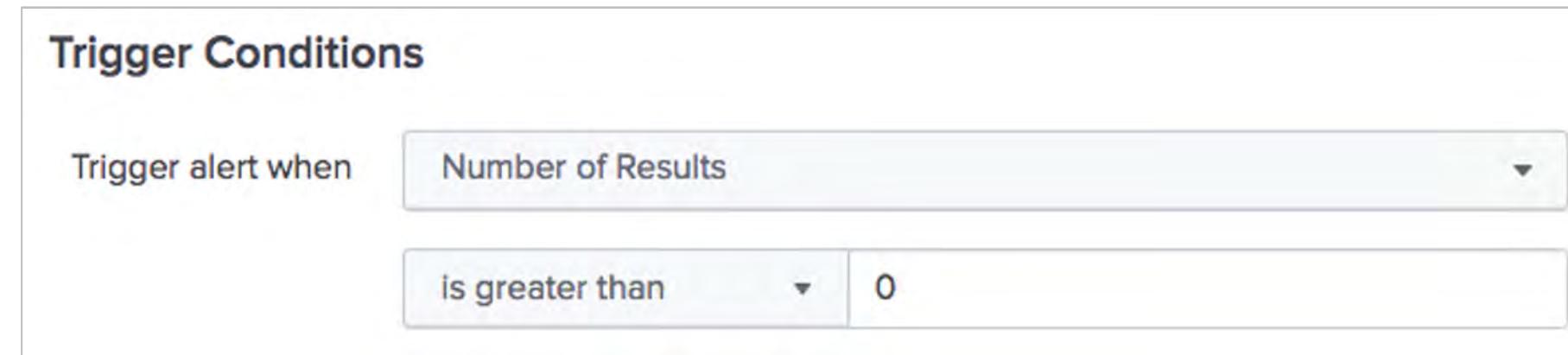
Setting Trigger Conditions

- Normally, a correlation search will trigger its adaptive responses (notable, etc.) if any results are found by the search
- You can use the **Trigger Conditions** to alter this default

Trigger Conditions

Trigger alert when

0



Setting Throttling

- Throttling: You should throttle based on a field's value
 - Example: no more than one notable event per host per day (86,400 seconds)
- More than one field can be selected
 - Throttling is based on all the field values ANDed together

Throttling

Window duration second(s) ▾

How much time to ignore other events that match the field values specified in Fields to group by.

Fields to group by

Type the fields to consider for matching events for throttling. [Learn more](#) ↗

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

Adding Adaptive Responses

Category All ▾



i Recommended actions and errors are highlighted

✉ Send email

Send an email notification to specified recipients

Category: [others](#) | Task: [others](#) | Subject: [others](#) | Vendor: [unknown](#)

LOG Log Event

Send log event to Splunk receiver endpoint

Category: [others](#) | Task: [others](#) | Subject: [others](#) | Vendor: [unknown](#)

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](#)

Notable

Creates notable events

Category: [Information Conveyance](#) | Task: [create](#) | Subject: [splunk.event](#) | Vendor: [Splunk](#)

Select the Notable response

Note



Each time Response Actions are modified, you must update the Splunk_TA_AROnPrem app.

Configuring Notable Event Fields

- Configure notable event field values
 - Title, description, security domain, severity
 - Default owner and status
 - Drill-down settings
- Embed field values in title, description, and drill-down fields using `$fieldname$` format
- Description fields support URLs to external locations
 - Useful for best practices documents, investigation procedures, etc.

+ Add New Response Action ▾

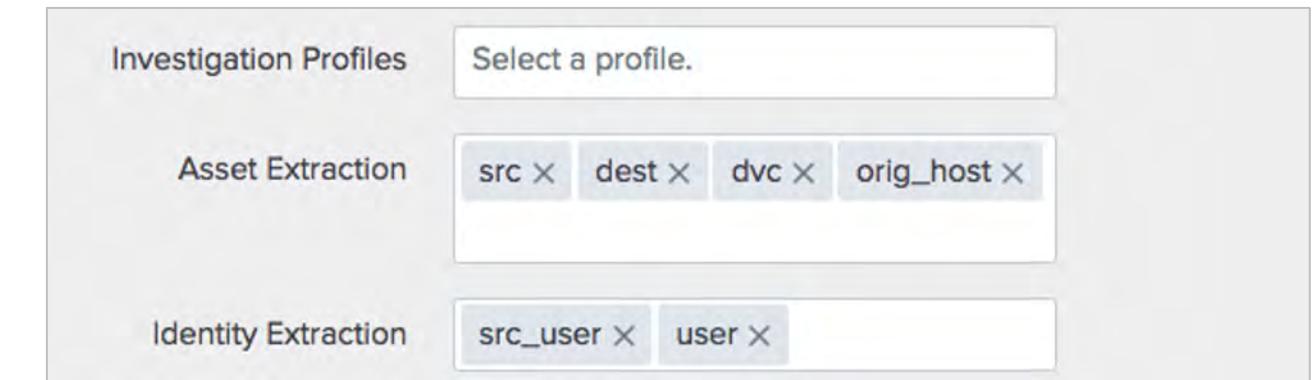
Notable

Title	High risk detected on \$host\$ Notable events created by this search will have this title. Supports variable substitution.
Description	Risk score = \$RiskByHost\$ Notable events created by this search will have this description. Supports variable substitution.
Security Domain	Network ▾
Severity	High ▾ Used to calculate urgency for notable events. Learn more ↗
Default Owner	(leave as system default) ▾
Default Status	(leave as system default) ▾
Drill-down Name	View risk generating events on \$host\$ Supports variable substitution with fields from the matching event.
Drill-down Search	!datamodel Risk All_Risk search search Supports variable substitution with fields from the matching event.
Drill-down Earliest Offset	\$info_min_time\$ Set the amount of time before the triggering event to search for related events. For example, 2h. Use <code>\$info_min_time\$</code> to set the drill-down time to match the earliest time of the search.
Drill-down Latest Offset	\$info_max_time\$ Set the amount of time after the triggering event to search for related events. For example, 1m. Use <code>\$info_max_time\$</code> to set the drill-down time to match the latest time of the search.

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

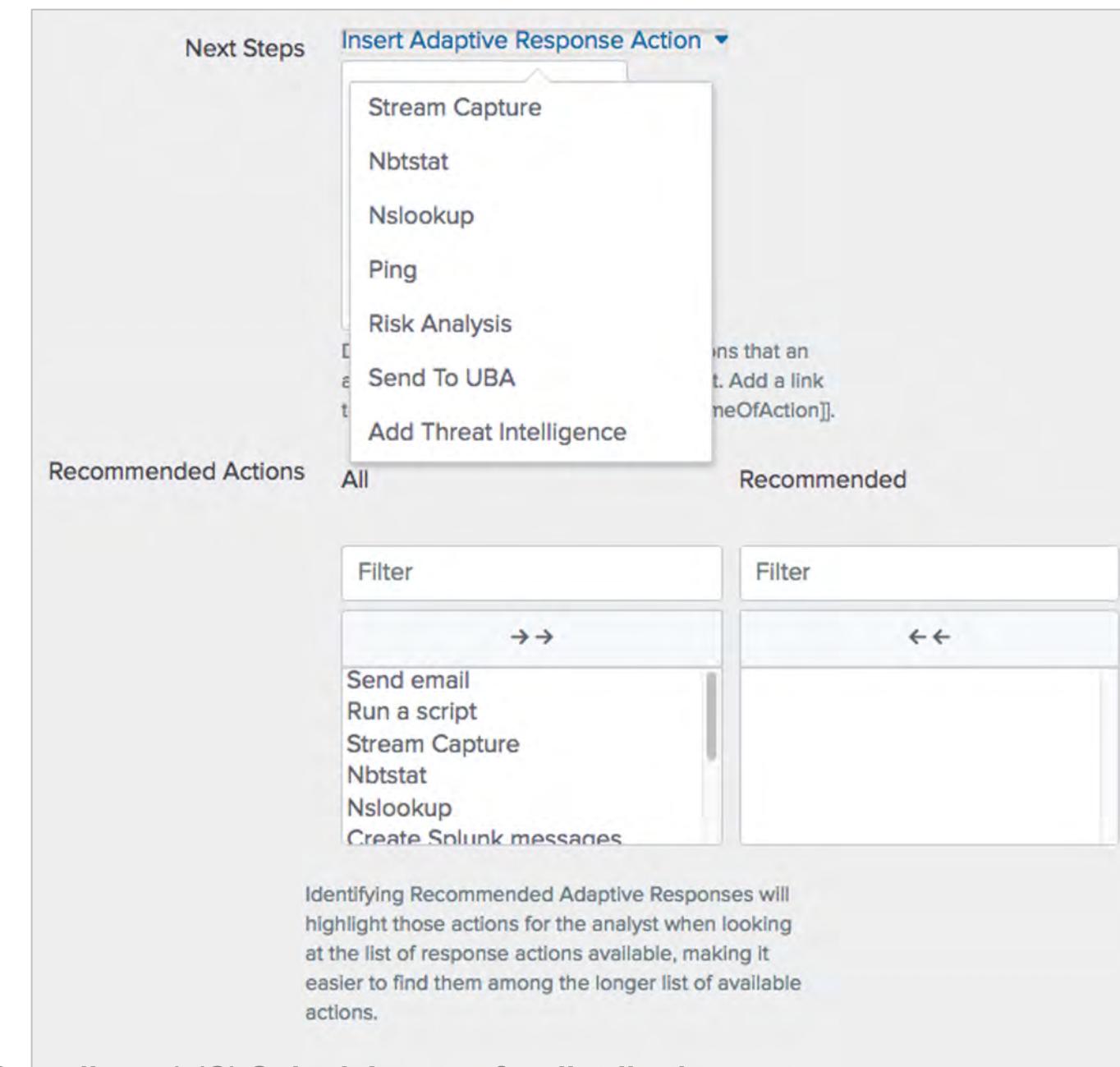
Configuring Notable Event Fields (cont.)

- Control actions taken when a notable is added to an investigation
 - Select an investigation profile to apply to the investigation
 - Automatically extract artifacts that will be added to the investigation



Configuring Notable Event Fields (cont.)

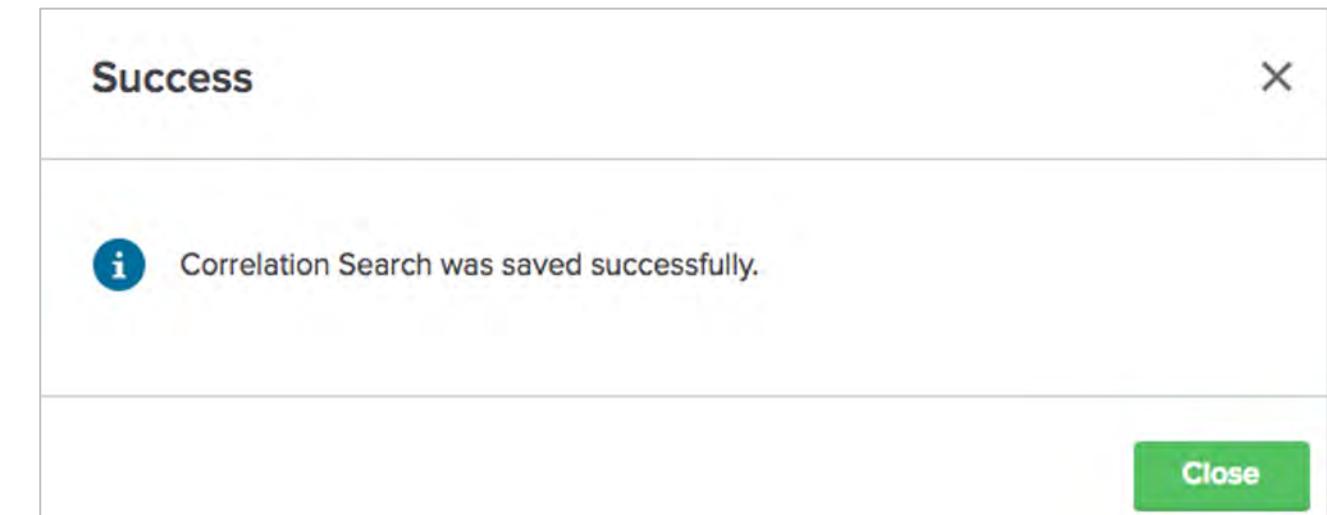
- You can control the “next steps” and “recommended actions” adaptive responses that appear in Incident Review
 - Next steps appear as links in the notable event details
 - Recommended Actions appear in the notable event’s Actions menu



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

Saving the Correlation Search

- Click **Save** to create the new correlation search
- Click **Close** and navigate back to the **Content Management** page
- Your new search will now display in the list of correlation searches for the ES app
- You can enable, disable, and change to scheduled or real-time as desired



Adaptive Response Actions

- Besides (or instead of) creating notable events, adaptive response actions can automate other critical tasks
- One or more adaptive response actions can be added to each correlation search
 - The action will be executed if the correlation search finds any matches
- ES ships with a set of default adaptive responses
- You can also install additional adaptive responses, and control who can access each adaptive response

docs.splunk.com/Documentation/ES/latest/Admin/Setupadaptiveresponse

Default Adaptive Response Actions

Notable, Risk	Create a notable event or add to an object's risk score
Send email, create Splunk message	Send email to one or more people, or add a system message in the Splunk web interface
Run script	Execute an automated script. Example: when a correlation search indicates a host is infected with malware, run a script to quarantine the target server
Stream capture	Automatically begin collecting detailed network information
Nbstat, nslookup, ping	Execute diagnostic command and attach output to the notable event to assist in analysis
Send to UBA/output to telemetry endpoint	If User Behavior Analytics is installed and integrated, send the notable event to UBA for analysis/send to Splunk telemetry
Add Threat Intelligence	Create a threat intel artifact. Example: a new type of infection is discovered; add the characteristics of the infection (file name, source IP, code hash, etc.) to the threat intel database so that future similar attacks will be immediately alerted

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

Edit Adaptive Responses

Settings > Alert actions

An ES Admin can use the Alert actions page in Splunk to make changes to Adaptive Responses

Alert action	App	Sharing	Status	Usage	Log	Setup
Add Threat Intelligence Creates threat artifacts	DA-ESS-ThreatIntelligen...	Global Permissions	Enabled Disable	Usage statistics	View log events	
Create Splunk messages Create messages in Splunk Web	SA-Utils	Global Permissions	Enabled Disable	Usage statistics	View log events	
ESCU-Investigate Investigate this alert further	DA-ESS-ContentUpdate	Global Permissions	Enabled Disable	Usage statistics	View log events	
Log Event Send log event to Splunk receiver endpoint	alert_logevent	Global Permissions	Enabled Disable	Usage statistics	View log events	
Nbtstat Runs the nbtstat command	SA-ThreatIntelligence	Global Permissions	Enabled Disable	Usage statistics	View log events	Setup SA-ThreatIntelligence
Notable Creates notable events	SA-ThreatIntelligence	Global Permissions	Enabled Disable	Usage statistics	View log events	Setup SA-ThreatIntelligence
Nslookup Runs the nslookup command	SA-ThreatIntelligence	Global Permissions	Enabled Disable	Usage statistics	View log events	Setup SA-ThreatIntelligence

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

Adaptive Response Permissions

Select Permission for a specific alert action to make changes

The screenshot shows the Splunk Enterprise interface with the title bar "splunk>enterprise" and various navigation links like "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". The main area is titled "Alert Actions" with the sub-instruction "Review and manage available alert actions". A yellow callout box points to the "Permissions" link in the "Sharing" column of the alert action table, with the text "Select Read, Write, or both permissions for each role".

The "Alert Actions" table lists the following alert actions:

Alert action	App	Sharing	Status
Add Threat Intelligence	DA-ESS-ThreatIntelligen...	Global Permissions	Enabled Disa
Create Splunk messages	SA-Utils	Global Permissions	Enabled Disa
ESCU-Investigate	DA-ESS-ContentUpdate	Global Permissions	Enabled Disa
Log Event	alert_logevent	Global Permissions	Enabled Disa
Nbtstat	SA-ThreatIntelligence	Global Permissions	Enabled Disa
Notable	SA-ThreatIntelligence	Global Permissions	Enabled Disa
Nslookup	SA-ThreatIntelligence	Global Permissions	Enabled Disa

A modal dialog titled "Edit Permissions" is open, showing the permissions for the "notable" alert action. It includes a table with columns for "Role" and "Permissions" (Read, Write). The "Owner" role has "Read" checked and "Write" unchecked. Other roles listed include "nobody", "SA-ThreatIntelligence", "Everyone", "admin", "can_delete", "ess_admin", "ess_analyst", "ess_user", "power", "splunk-system-role", "user", and "windows-admin".

Role	Read	Write
Owner	<input checked="" type="checkbox"/>	<input type="checkbox"/>
nobody	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SA-ThreatIntelligence	<input type="checkbox"/>	<input type="checkbox"/>
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
ess_admin	<input type="checkbox"/>	<input type="checkbox"/>
ess_analyst	<input type="checkbox"/>	<input type="checkbox"/>
ess_user	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>
windows-admin	<input type="checkbox"/>	<input type="checkbox"/>

Buttons at the bottom of the dialog are "Cancel" and "Save".

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

Adaptive Response Action Center

Audit > Adaptive Response Action Center

Adaptive Response Action Center

Action Mode Action Name Action Status User Search ID (sid) Edit Export ...

All All All All Last 24 hours Submit Hide Filters

[Edit](#)

Action Invocations count	Action Names Distinct Count	Action Search Names Distinct Count	Action Users Distinct Count	Action Searches Distinct Count	Action Duration Average (ms)
26.1k <small>+305</small>	2 <small>0</small>	20 <small>0</small>	1 <small>0</small>	806 <small>+78</small>	12.9 <small>-0.4</small>

Action Invocations Over Time By Name

notable risk

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 - Inactive Account Usage - Rule	admin	667	19798	11.5

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

splunk® turn data into doing™

230

Administering Splunk Enterprise Security
Copyright © 2022 Splunk, Inc. All rights reserved | 7 April 2022

Content Import/Export

- You can export any of the content types on the Content Management page by selecting them in the custom search list and choosing **Export**
- Enter an app name, prefix, label, version and build number, and click **Export**
 - The content will be downloaded to your workstation as an **.spl** file
 - It can then be installed as a new app into another ES search head
- Import content by installing an app

Example: Content Export

The screenshot illustrates the process of exporting content from Splunk. On the left, a list of objects is shown with a checkbox selected for 'Abnormally High A'. An 'Export' button is highlighted with a green box and a green arrow points to a modal window titled 'Export Content Into An App'. The modal contains fields for 'App name' (my-searches), 'App name prefix' (DA-ESS-), 'Label' (My Searches), 'Version' (1.0), and 'Build number' (1). A note in the bottom-left corner states: 'DA-ESS is a recommended prefix for content add-ons but is not required.' On the right, a success message in a separate window says 'Content successfully exported.' with a 'Download app now' link.

1233 Objects Edit selection ▾ 1 selected Clear

Name

Abnormally High A

Abnormally High A

Abnormally High Number

Abnormally High Number

Note

DA-ESS is a recommended prefix for content add-ons but is not required.

Export

Enable

Launched by User

Disable

Export Content Into An App

App name: my-searches

App name prefix: DA-ESS- No Prefix

Choose the "DA-ESS-" prefix to be able to import the app without modifying default import settings.

Label: My Searches

Version: 1.0

Build number: 1

Cancel Export

Content successfully exported.

Download app now

The exported app will contain any alert actions associated with the exported searches; this could include sensitive information such as email addresses (for example, if one of the searches use an email alert action).

Close

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

Content Export Best Practices

- The app name for the content export is uploaded to the `etc/apps` directory of the receiving server
- Be careful when exporting updates to your content
 - Example: you export `correlation1`, naming it `correlations.spl`, and upload it to another ES server. Later you export `correlation2`, again using `correlations.spl` as the export name. When you upload `correlations.spl` to the second server, it overwrites the old version of `correlations.spl`, deleting `correlation1`
- Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export

Module 10 Lab: New Correlation Searches

Time: 20 minutes

Tasks:

1. Create a custom correlation search
 - SSH logins are prohibited in your environment. Create a custom correlation search that detects successful SSH logins and generates a notable event to alert analysts

Module 11:

Asset & Identity Management

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

Objectives

- Review the Asset and Identity Management interface
- Describe Asset and Identity KV Store collections
- Configure and add asset and identity lookups to the interface
- Configure settings and fields for asset and identity lookups
- Explain the asset and identity merge process
- Describe the process for retrieving LDAP data for an asset or identity lookup

Assets & Identities Overview

- Asset and identity configuration enhances the information available for users and systems in the **notable** index and ES dashboards
- **SA-IdentityManagement** is the supporting add-on that maintains macros, lookups, knowledge objects, etc.
- CRUD (create, read, update, and delete) operations maintain the attributes defined in the lookups
- View the contents of a lookup table. For example:
| `inputlookup demo_identities.csv`

Asset & Identity Management Interface

Configure > Data Enrichment > Asset and Identity Management

Asset and identity lookups and settings are configured in this interface

The screenshot shows the Asset and Identity Management interface. At the top, there's a header with the title "Asset and Identity Management" and a sub-header "Unified interface for enriching and managing asset and identity data via lookups." On the right, there's a red button labeled "Reset Collections". Below the header, there are navigation links: "Back to ES Configuration", "Asset Lookups" (which is underlined), "Asset Fields", "Identity Lookups", "Identity Fields", "Global Settings", "Correlation Setup", and "Search Preview". A green "New" button with a dropdown arrow is located on the right side of the main content area. The main content area is a table with columns: Rank, Name, Category, Description, Source, Blacklist, and Status. It contains two rows of data:

Rank	Name	Category	Description	Source	Blacklist	Status
1	demo_assets	demo_assets	Demonstration asset list.	demo_asset_lookup ↗	Enabled	Enable Disabled
2	static_assets	static_assets	List containing static assets.	simple_asset_lookup ↗	Enabled	Enabled Disable

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

Assets & Identity KV Store Collections

- Asset and Identity lookups are stored as KV Store collections
 - `assets_by_str` collection – `asset_lookup_by_str` lookup
 - `assets_by_cidr` collection – `asset_lookup_by_cidr` lookup
 - `identities_expanded` collection – `identity_lookup_expanded` lookup
- Prior to 6.2 assets and identities were only defined in lookup tables
- Using the KV Store allows for larger tables for assets and identities
- Lookups are defined in SA-IdentityManagement `transforms.conf`

```
[asset_lookup_by_cidr]
external_type = kvstore
match_type = CIDR(asset)
collection = assets_by_cidr
fields_list =
_delete,_key,_last_updated,_sources,asset,asset_tag,bunit,category,city,country,dns,ip,is_expected,lat,
long,mac,nt_host,owner,pci_domain,priority,requires_av,should_timesync,should_update max_matches = 1
case_sensitive_match = false
filter = NOT _delete="true"
```

Example lookup configuration

Uploading Assets and Identities

- Update the lookups provided in the management interface under **Asset Lookups** and **Identity Lookups** with your corporate data (static_assets, static_identities, administrative_identities)
- Or create lookup .csv files with the proper fields and add them to the management interface
- Initially pull corporate asset and identity data using a Splunk add-on such as LDAP Search or DB Connect
 - The add-on pulls the information to be used in the lookup files
 - Periodically re-run to keep assets and identities updated

Important!



Do not include every piece of hardware or every person – focus on the ones with the most significance.

Not every column needs to be populated.

Asset Lookups

- The Asset Lookups tab lists all configured asset lookups
- New lookups can be added here, and existing lookups can be edited

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

Add a new asset lookup

Rank files, lowest rank takes precedence

Rank	Name	Category	Description	Source	Blacklist
1	demo_assets	demo_assets	Demonstration asset list.	demo_asset_lookup	Enabled
2	static_assets	static_assets	List containing static assets.	simple_asset_lookup	Enabled

Click a Name to change the lookup settings

Open and edit the Source lookup file

Reset Collections at any time, rather than waiting for the automated process to clear out the KV store collection

Reset Collections

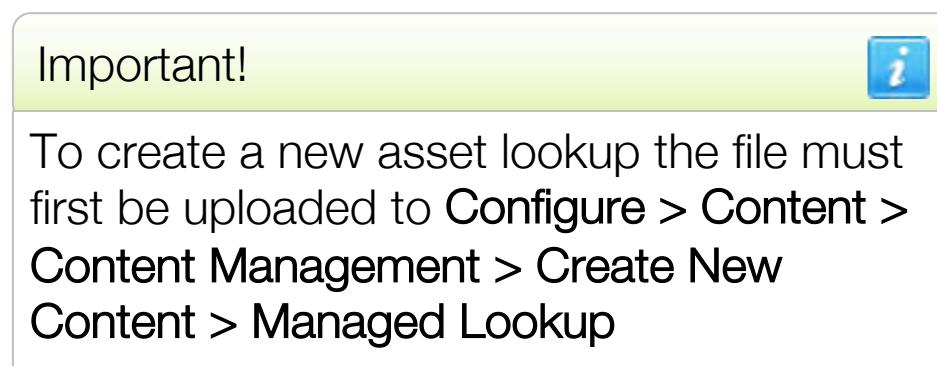
New Configuration
LDAP Lookup
Cloud Services Lookup
Enabled | Disable

Enable | Disable a lookup

Add a New Asset Lookup

New > New Configuration

1. From the **New Asset Manager** window select the lookup file from the **Source** drop-down menu
2. **Name** is auto-filled with the file name
3. Complete the **Category** and **Description**
4. **Type** defaults to **asset**
5. From **Field Exclusion List**, select fields to ignore when merging assets



New Asset Manager

Source	FOO_assets
The source for this asset or identity list.	
Name	FOO_assets
The identity manager stanza name.	
Category	FOO_domain
A short descriptive category for this asset or identity list, for example: 'AD_domain_1'.	
Description	FOO servers and workstations
A description of the contents of this asset or identity list.	
Blacklist	<input checked="" type="checkbox"/>
Exclude the lookup file from bundle replication.	

Lookup List Type

Type	asset
The type of list; must be 'asset' or 'identity'.	
Field Exclusion List	Select...
List of fields to ignore when merging assets or identities.	

Buttons: Cancel | Save

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

Add a New Asset Lookup (cont.)

The new asset list displays in the Asset Lookup Configuration tab

Asset and Identity Management
Unified interface for enriching and managing asset and identity data via lookups.
[< Back to ES Configuration](#)

[Reset Collections](#)

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

New

Rank	Name	Category	Description	Source	Blacklist	Status
1	demo_assets	demo_assets	Demonstration asset list.	demo_asset_lookup ↗	Enabled	Enable Disabled
2	static_assets	static_assets	List containing static assets.	simple_asset_lookup ↗	Enabled	Enabled Disable
3	FOO_assets	FOO_domain	FOO servers and workstations	FOO_assets ↗	Enabled	Enabled Disable

The lookup is added to

\$SPLUNK_HOME/etc/apps/SA-IdentityManagement/local/inputs.conf

```
[identity_manager://foo_assets] ← Stanza Name  
blacklist = true  
category = FOO_domain  
description = FOO servers and workstations  
rank = 3  
target = asset  
url = lookup://FOO_assets ← CSV File
```

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

Remove an Asset Lookup

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](#)

Rank	Name	Category	Description
1	demo_assets	demo_assets	Demonstra
2	static_assets	static_assets	List contain
3	FOO_assets	FOO_domain	FOO serve

Click an added lookup configuration to edit or delete it

Note 
The default configurations **demo_assets** and **static_assets** cannot be removed

Edit Asset Manager

Source: FOO_assets
The source for this asset or identity list.

Name: FOO_assets
The Identity manager stanza name.

Category: AD_domain_FOO
A short descriptive category for this asset or identity list, for example: 'AD_domain_1'.

Description: Assets in the FOO domain.
A description of the contents of this asset or identity list.

Blacklist:
Exclude the lookup file from bundle replication.

Lookup List Type

Type: asset
The type of list; must be 'asset' or 'identity'.

Field Exclusion List: Select...
List of fields to ignore from the source file.

Delete  **Cancel** **Save**

Asset Fields

Asset Lookups					Asset Fields					Identity Lookups					Identity Fields					Global Settings					

Changing Default Asset Fields

The screenshot shows the Splunk UI for managing asset fields. The 'Asset Fields' tab is selected. A modal window titled 'Edit Asset Field' is open for the field 'bunit'. The 'Field Name' is set to 'bunit'. Under 'Key', there is a checked checkbox with a tooltip explaining it makes the field a key for merging assets or identities. Under 'Tag', there is a checked checkbox with a tooltip explaining it can be used as an asset or identity tag. Under 'Multivalue', there is a checked checkbox with a tooltip explaining it can output multiple values. The 'Multivalue Limit' is set to 25. At the bottom of the modal are 'Cancel' and 'Save' buttons. The background shows a list of other asset fields: 'category', 'city', 'country', 'dns (key)', 'ip (key)', 'is_expected', 'lat', 'long', 'mac (key)', 'nt_host (key)', 'owner', 'pci_domain', 'priority', and 'requires_av'. A green button labeled '+Add New Field' is visible on the left.

- For default fields, these settings can be changed:
 - Key
 - Tag
 - Multivalue
 - Multivalue Limit

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

Adding Custom Asset Fields

Add up to 20 custom header fields

Name	Tag	Multivalue	Multivalue Limit
bunit	✓	✓	25
category	✓	✓	25
city	✗	✓	25
country	✗	✓	25
dns (key)	✗	✓	6
ip (key)	✗	✓	6
is_expected	✓	✗	-
lat	✗	✓	25
long	✗	✓	25
mac (key)	✗	✓	6
nt_host (key)	✗	✓	6
owner	✗	✓	25
pci_domain	✗	✓	25
priority	✗	✗	-
requires_av	✓	✗	-

+Add New Field

Enable case sensitive asset matching

Enable asset collection replication

Click +Add New Field and give the field a name. Select **Multivalue** if the field can output multiple values and set a limit. Check the **Key** box to use the field in the merge process. Check the **Tag** box if the field can be used as an asset tag.

Field Name: 0/5
Lookup field name.

Key: Make this field a key. When merge is enabled, assets or identities with the same values for this field will be merged.

Tag: Check the box if the field can be used as an asset or identity tag. [Learn more](#)

Multivalue: Check the box if the field can output multiple values.

Multivalue Limit: 25
Limits the number of values in a multivalued field. Increasing this number may impact search performance. Must be between 1 and 25. [Learn more](#)

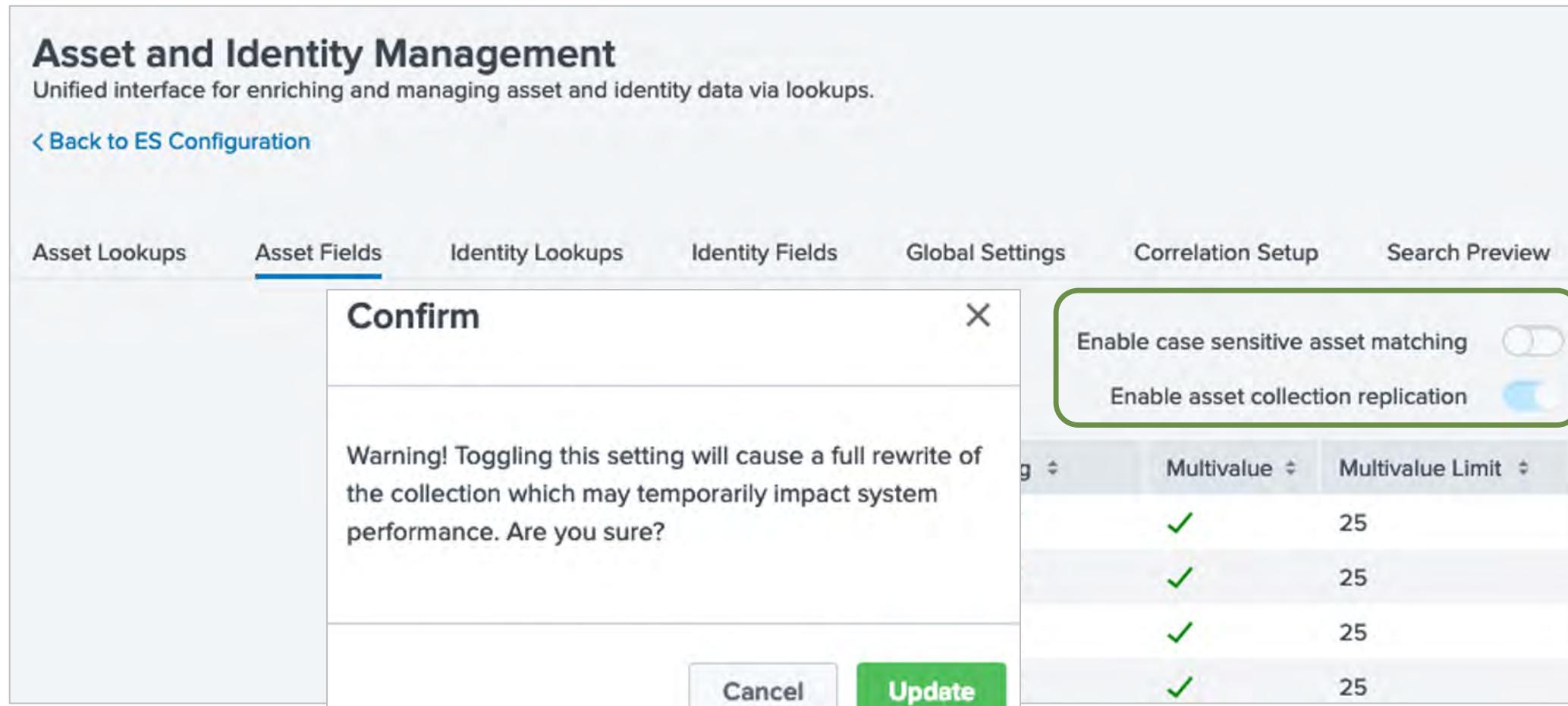
Delete Field

Cancel Save

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

Case Sensitive Matching

- Enable case sensitive matching
 - A warning displays that there will be a full rewrite of the collection
 - Click **Update** to continue



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

Identity Lookups

- The Identity Lookups tab has the same features as the Asset Lookups configuration tab
 - Change lookup settings, open and edit the source lookup file, enable and disable the lookups
 - Change the Rank of the lookups using the double ellipsis



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

[Reset Collections](#)

[Back to ES Configuration](#)

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

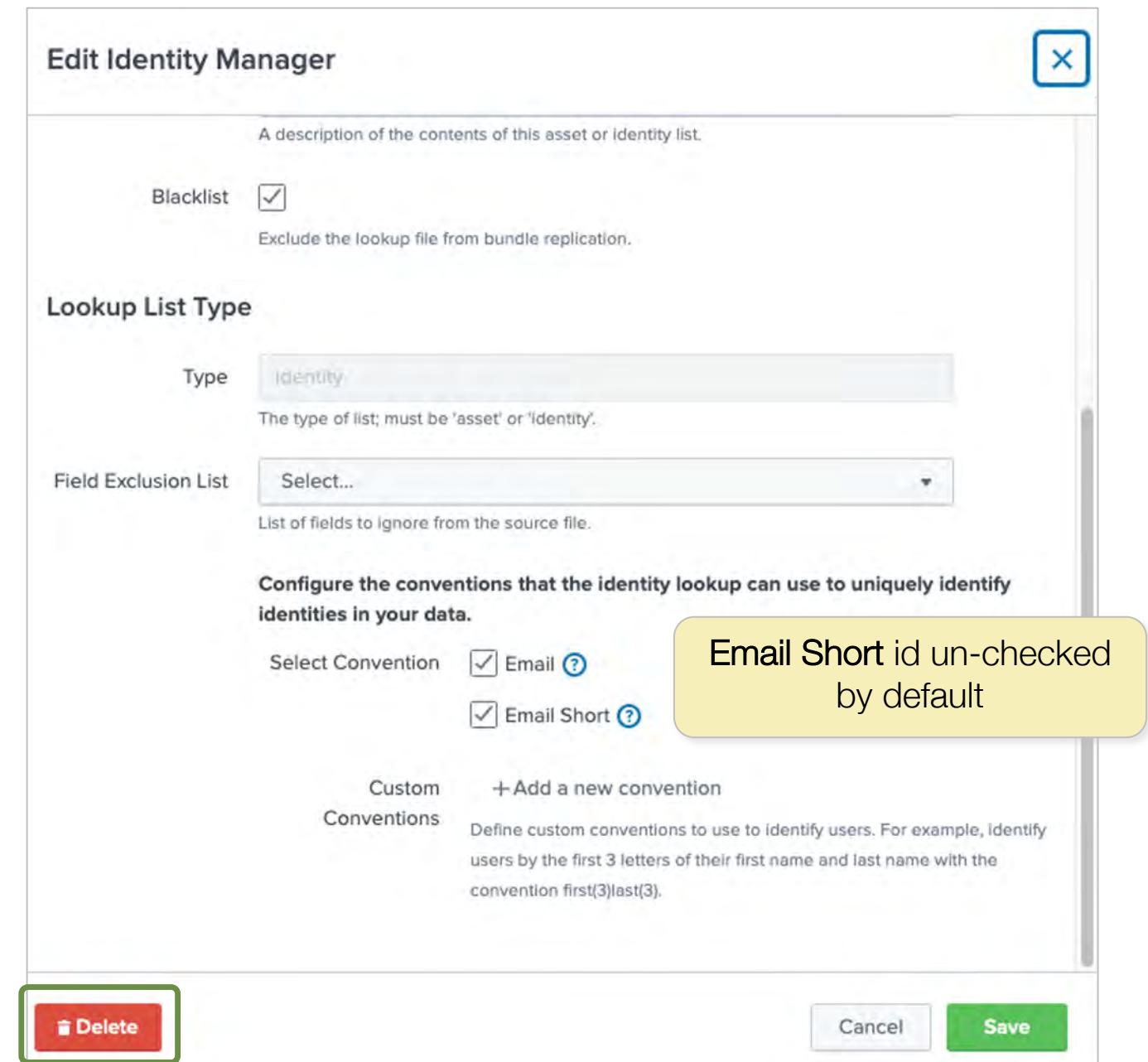
New

Rank	Name	Category	Description	Source	Blacklist	New Configuration
1	administrative_identities	administrative_identities	List of commonly-used administrative or privileged identities.	administrative_identity_lookup ↗	Enabled	LDAP Lookup
2	demo_identities	demo_identities	Demonstration identity list.	demo_identity_lookup ↗	Enabled	Cloud Services Lookup
3	static_identities	static_identities	List containing static identities.	simple_identity_lookup ↗	Enabled	Enabled Disable

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

Identity Lookups (cont.)

- Similar to the configuration of an asset lookup, the exception is the **email convention**
- If selected, email conventions can be used to uniquely identify the identities in the data
 - Email address or Email Short (username in email address)
 - Custom Conventions – for example, identify users by the first letter of their first name and their last name
- Added configurations can be deleted



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

Identity Fields

- Similar to the setup of asset fields
 - Add up to 20 custom fields
 - Key – field is used in merge process
 - Tag - can be used as an asset tag
 - Enable case sensitive matching
 - Multivalue - field can output multiple values
 - By default, the only “Key” field is **identity** - Multivalue Limit (1-100). The default is 25
 - Non-key fields - Multivalue Limit is 1 – 100. The default is 25

Name	Tag	Multivalue	Multivalue Limit
bunit	✓	✓	25
category	✓	✓	25
email	✗	✓	25
endDate	✗	✗	-
first	✗	✓	25
identity (key)	✗	✓	25
last	✗	✓	25
managedBy	✗	✓	25
nick	✗	✓	25
phone	✗	✓	25
prefix	✗	✓	25
priority	✗	✗	-
startDate	✗	✗	-
suffix	✗	✓	25
watchlist	✓	✗	-
work_city	✗	✓	25
work_country	✗	✓	25
work_lat	✗	✓	25
work_long	✗	✓	25

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

Global Settings Overview

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

Settings are described in detail in the next few slides

Reset Collections

Configure the global settings of the identity manager modular input

Enable Merge for Assets or Identities
Merge assets or identities. [Learn more](#)

Assets Identities

Enable Zones for Assets or Identities
For advanced use cases such as overlapping address spaces. [Learn more](#)

Assets Identities Default
Specify a default zone name.

Asset Ignored Values
Define what values are ignored when creating assets. [Learn more](#)

null
n/a
unknown
undefined

+ Add Row

Identity Ignored Values
Define what values are ignored when creating identities. [Learn more](#)

null
n/a
unknown
undefined

+ Add Row

Enforcements

Enforce props
Enforce macros
Enforce transforms
Enforce replicate
Enforce identityLookup

Miscellaneous Settings

Time(s) 300
Set how much time (seconds) to wait between each identity manager run.

Master host
Set the host the identity manager runs on. Defaults to captain.

Overlay CIDR

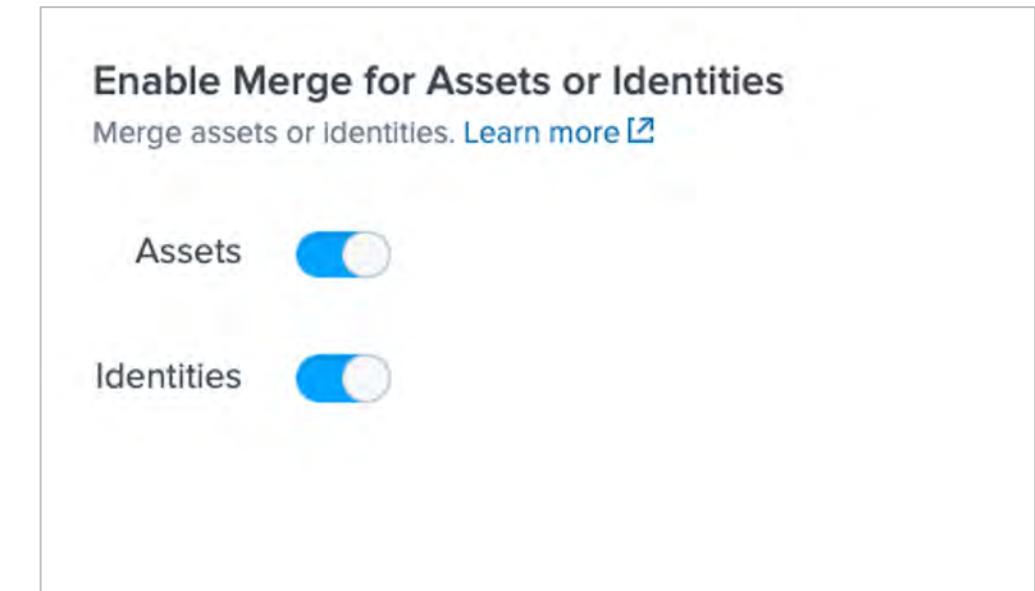
Debug mode

This screenshot shows the 'Global Settings' section of the Splunk Asset and Identity Management interface. It includes sections for enabling merge, zones, and asset/identity ignored values, as well as enforcement rules and miscellaneous settings like timeouts and master hosts. A yellow callout box highlights that settings are described in detail in the next few slides.

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

Enable Merge

- The default behavior is to merge rows of source data based on a match in any one of the “key” fields
- Enabled by default for assets and identities
- Disable the merge process here if you need to stop the process
 - For example, if you have a source file with duplication in the “key” fields, and you cannot groom the file to make sure that the information belongs to the same asset or identity, disable the merge process



Asset Merge Example

- Example: the source file has duplicates in the `nt_hosts` key field:

```
ip,mac,nt_hosts,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires _av
192.0.2.2,,host1,.....
192.0.2.120,,host1,.....
192.0.2.135,,host1,.....
192.0.2.242,,host2,.....
192.0.2.65,,host2,.....
```

- By default, the three `host1` entries defined by the `nt_hosts` field are merged into one asset and the two `host2` entries are merged into another
- With merge disabled, the collection remains the same as the source file
- When you do a lookup on a `non-merged` collection, there is no context for how to resolve the overlapping key field values
 - For example, the `asset_lookup_by_str` lookup in `transforms.conf` has `max_matches=1`, so the first host it matches in the `assets_by_str` collection is the only one you will see in the search results

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

Enable Zones

- Create Zones for entries that overlap, like IP addresses
 - For example, two companies are merging who use the same IP address scheme. Assign all entries with a **location** of **palo_alto** to a zone called **flowmill**, and entries with a **location** of **boulder** to a zone called **victorops**

Enable Zones for Assets or Identities
For advanced use cases such as overlapping address spaces. [Learn more](#)

Assets

Identities

Default
Specify a default zone name.

Configure Zones

Configure Zones

Condition	Zone
If location=palo_alto	assign flowmill
+ Add	

Configure Zones

Condition	Zone
If location=boulder	assign victorops
+ Add Clause	

Cancel **Confirm**

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

Ignore Values

- The default behavior in ES is to merge rows of source data based on a match in any one of the key fields
- Source data may have placeholder values that span multiple rows, causing them to merge into one large multivalue row
- Solution: define the placeholder values as null and clean them during the merge process. Independent rows are maintained in the final lookups
- Ignore values are case sensitive, you may have to enter more than one value, like “unknown” and “Unknown”

Ignore Values

- Define values to be ignored when creating assets and identities
 - By default, **null**, **n/a**, **unknown**, and **undefined** are ignored
 - Ignored values apply to any type of field (key, non-key, multivalue, single value)
 - Strings are saved as **ignored_values** in
/SA-IdentityManagement/local/inputs.conf

Asset Ignored Values
Define what values are ignored when creating assets. [Learn more ↗](#)

null	X
n/a	X
undefined	X
unknown	X

+ Add Row

Identity Ignored Values
Define what values are ignored when creating identities. [Learn more ↗](#)

null	X
n/a	X
undefined	X
unknown	X

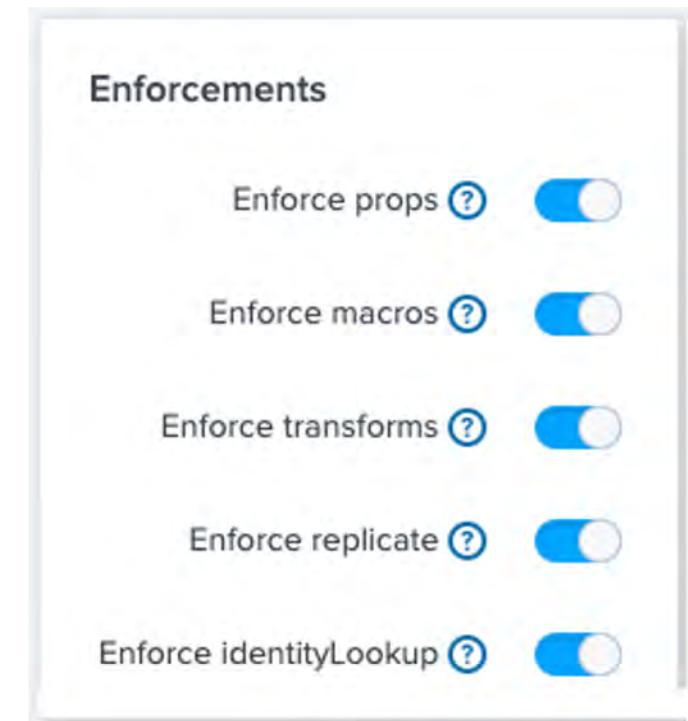
+ Add Row

Use +Add Row to define custom ignore values

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

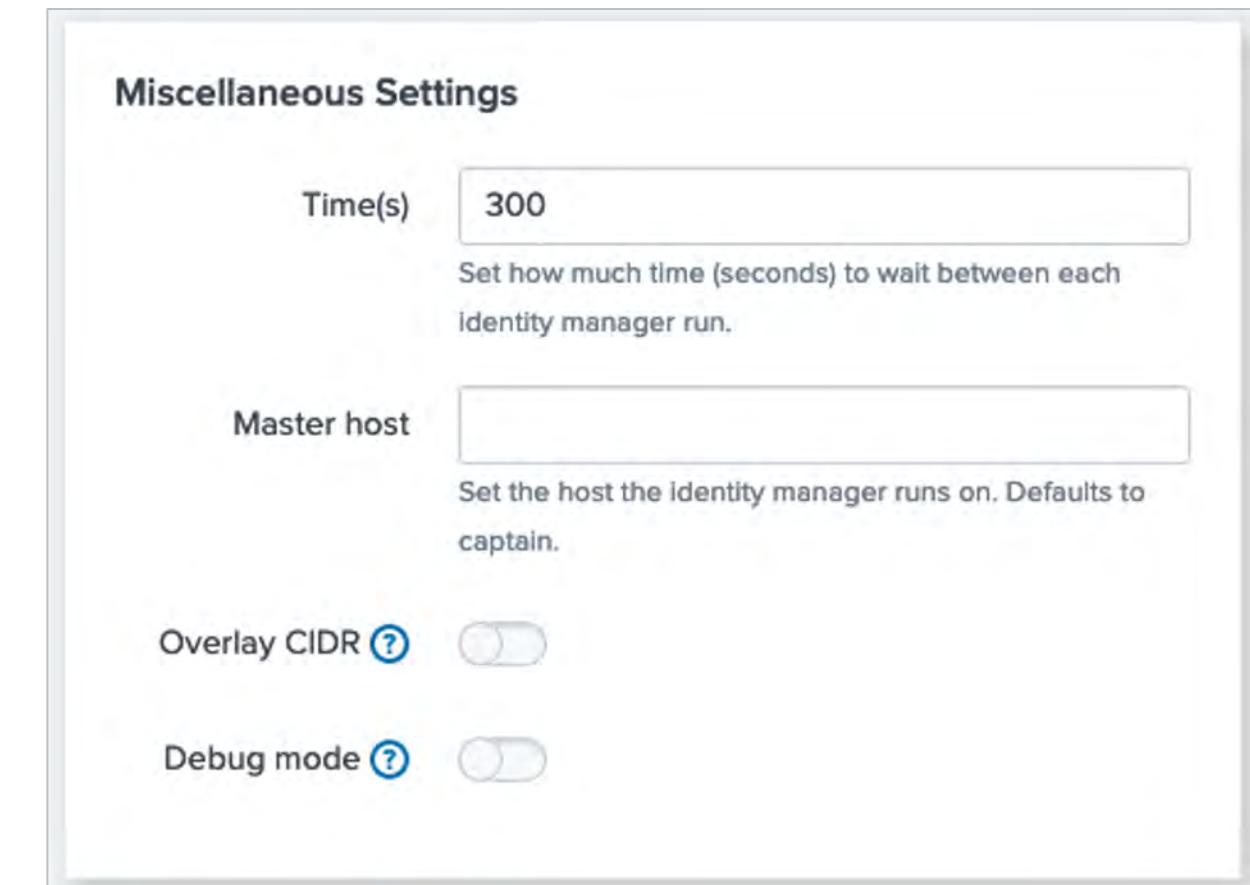
Enforcements

- How ES verifies the following in SA-IdentityManagement each time the identity manager runs (every 5 minutes):
 - Enforce props – automatic lookups that are defined in `props.conf`
 - Enforce macros – macros that read from the CSV files into the KV Store collections. Best to always enforce them!
Settings > Advanced Search > Search macros > SA-IdentityManagement
 - Enforce transforms – `transforms.conf` defines the .csv filenames and settings like case sensitive matching
 - Enforce replicate – collection replication settings defined in `collections.conf`
 - Enforce identityLookup – IdentityLookup conventions



Miscellaneous Settings

- Settings specific to the Identity Manager framework
 - **Time(s)** – how often Identity Manager runs
 - Default is 300 seconds (5 minutes)
 - Can be increased for better performance
 - **Master host** – host where the Identity Manager runs, defaults to SHC captain
 - **Overlay CIDR** – `asset_lookup_by_str` will include CIDR data
 - **Debug mode** – enable debug logging for Asset and Identity Management



Correlation Setup

- Choose how to use asset and identity correlation to enrich events
 - By Default, correlation is enabled

Choose whether to enable or disable asset and identity correlation via this setup

Enable for all sourcetypes

Disable for all sourcetypes

Enable selectively by sourcetype

Note

Typically, this should not need to be changed from the default: "Enable for all sourcetypes".

Save

Sourcetype: bcg:accounting

Sourcetype bcg:accounting

Enable asset correlation

Enable identity correlation

Done

- Disabling correlation prevents events from being enriched with asset and identity information from the lookups
- Another option is to restrict correlation to occur only for select source types

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

Search Preview

Search Preview creates custom-built searches with what is currently in `inputs.conf`, running a search displays the merge data from all asset or identity lookups

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

Preview the searches that build the Asset and Identity Tables

Will output only new, updated, or deleted data.

asset_lookup_by_str
Asset table that uses string matching to enrich events | [Open in search ↗](#)

Test the merge process on your data without actually performing the merge!

```
| 'add_entity_source("FOO_assets","FOO_assets")' | 'add_entity_source("simple_asset_lookup","static_assets")' | table *_source*,cim_entity_zone*,O/S*,bunit*,category*,city*,country*,dns*,ip*,is_expected*,lat*,long*,mac*,nt_host*,owner*,pci_domain*,priority*,requires_av*,should_timesync*,should_update* | 'make_ip_str' | inputlookup append=T "asset_lookup_by_str" | entitymerge "asset"
```

asset_lookup_by_cidr
Asset table that uses CIDR matching to enrich events | [Open in search ↗](#)

```
| 'add_entity_source("FOO_assets","FOO_assets")' | 'add_entity_source("simple_asset_lookup","static_assets")' | table *_source*,cim_entity_zone*,O/S*,bunit*,category*,city*,country*,dns*,ip*,is_expected*,lat*,long*,mac*,nt_host*,owner*,pci_domain*,priority*,requires_av*,should_timesync*,should_update* | 'make_ip_cidr' | inputlookup append=T "asset_lookup_by_cidr" | entitymerge "asset"
```

identity_lookup_expanded
Identity table that uses string matching to enrich events | [Open in search ↗](#)

```
| 'add_entity_source("administrative_identity_lookup","administrative_identities")' | 'add_entity_source("demo_identity_lookup","demo_identities")' | 'add_entity_source("simple_identity_lookup","static_identities")' | eval identity=split(identity, "|"),identity;if(_source=="administrative_identities", mvappend(identity,'get_mv_item0("email)'), identity),identity;if(_source=="demo_identities", mvappend(identity,'get_mv_item0("email)'), identity),identity;if(_source=="static_identities", mvappend(identity,'get_mv_item0("email")'), identity),identity=mvjoin(mvdedup(identity), "|") | table *_source*,cim_entity_zone*,bunit*,category*,email*,endDate*,first*,identity*,last*,managedBy*,nick*,phone*,prefix*,priority*,startDate*,suffix*,watchlist*,work_city*,work_country*,work_lat*,work_long* | eval 'iden_mktime_meval(startDate)', 'iden_mktime_meval(endDate)',identity=mvsort(identity) | sort 0 +identity | inputlookup append=T "identity_lookup_expanded" | entitymerge "identity"
```

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

Search Preview (cont.)

- Each search is dynamic and generates each time you refresh or load the page
 - For example, the `asset_lookup_by_str` search changes when the new `FOO_assets` table is added

asset_lookup_by_str

Asset table that uses string matching to enrich events | [Open in search](#)

```
| inputlookup append=T "demo_asset_lookup" | fillnull value="demo_assets" _source | inputlookup append=T "simple_asset_lookup" | fillnull value="static_assets" _source | fields "bunit","category","city","country","is_expected","lat","long","owner","pci_domain","priority","requires_av","should_timesync","should_update","dns","ip","mac","nt_host" | `make_ip_str` | where isnotnull('dns') OR isnotnull('ip') OR isnotnull('mac') OR isnotnull('nt_host') | inputlookup append=T "asset_lookup_by_str" | entitymerge "asset"
```

asset_lookup_by_str

Asset table that uses string matching to enrich events | [Open in search](#)

```
| inputlookup append=T "demo_asset_lookup" | fillnull value="demo_assets" _source | inputlookup append=T "FOO_assets" | fillnull value="FOO_assets" _source | inputlookup append=T "simple_asset_lookup" | fillnull value="static_assets" _source | fields "bunit","category","city","country","is_expected","lat","long","owner","pci_domain","priority","requires_av","should_timesync","should_update","dns","ip","mac","nt_host" | `make_ip_str` | where isnotnull('dns') OR isnotnull('ip') OR isnotnull('mac') OR isnotnull('nt_host') | inputlookup append=T "asset_lookup_by_str" | entitymerge "asset"
```

If nothing has changed in the source files since the last merge, you will not see any output

Onboarding LDAP Data

- Use the Splunk Supporting Add-on for AD (SA-ldapsearch) to pull LDAP data from an AD database and create a lookup of assets or identities
- From Asset Lookups or Identity Lookups, select LDAP Lookup from the New menu

The screenshot shows the Asset and Identity Management interface. At the top, there's a header with 'Asset and Identity Management' and a 'Reset Collections' button. Below the header, a sub-header says 'Unified interface for enriching and managing asset and identity data via lookups.' There's a back-link '[Back to ES Configuration](#)'. The main navigation bar includes tabs for 'Asset Lookups' (which is active), 'Asset Fields', 'Identity Lookups', 'Identity Fields', 'Global Settings', 'Correlation Setup', and 'Search Preview'. On the right side, there's a 'New' button with a dropdown menu. The dropdown menu has three options: 'New Configuration' (highlighted with a blue border), 'LDAP Lookup' (highlighted with a green border), and 'Cloud Services Lookup'. The main table below the navigation bar lists two asset lookups:

Rank	Name	Category	Description	Source	Blacklist	New Configuration
1	demo_assets	demo_assets	Demonstration asset list.	demo_asset_lookup	Enabled	LDAP Lookup
2	static_assets	static_assets	List containing static assets.	simple_asset_lookup	Enabled	Cloud Services Lookup

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

Data Onboarding for LDAP

- Complete the Lookup Builder
 - Notice the window says either **LDAP Lookup Builder (Asset) or (Identity)**
 - Give the search a name and enter the name of the domain
 - Give the lookup file a Label and Lookup name
 - Splunk populates the **Lookup filename** field with the lookup name and .csv

LDAP Lookup Builder (Asset) ×

Search

Search name: Test_LDAP_Assets

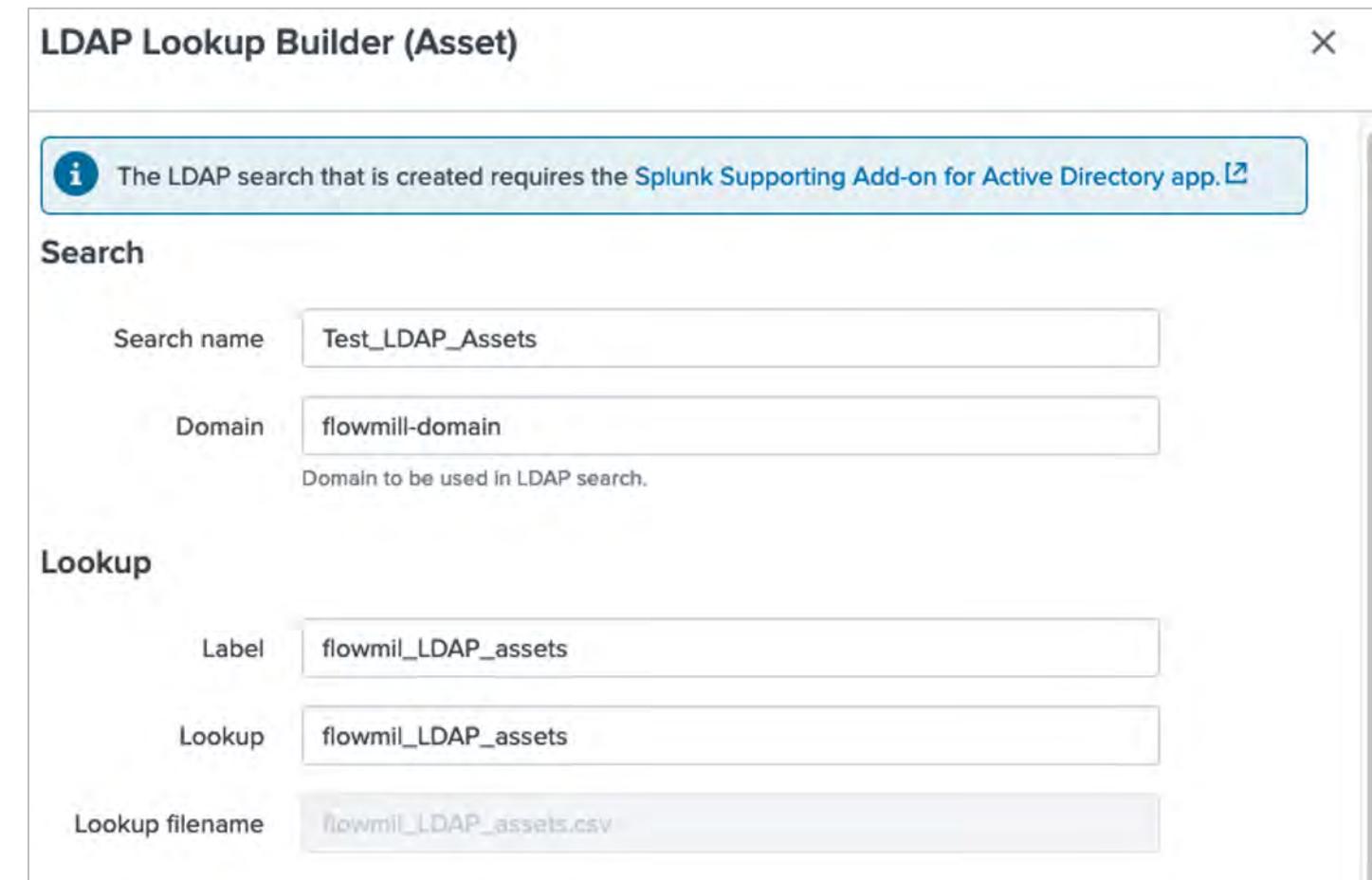
Domain: flowmill-domain
Domain to be used in LDAP search.

Lookup

Label: flowmil_LDAP_assets

Lookup: flowmil_LDAP_assets

Lookup filename: flowmil_LDAP_assets.csv



Data Onboarding for LDAP (cont.)

- Scroll down to enter a cron schedule for how often the search should run
- Select the scheduling
 - Real-time: run at the scheduled time or not at all
 - Continuous: if a report cannot run now, it will run in the future, after other reports finish
- PREVIEW displays the search that will pull asset or identity data from LDAP, create a lookup, and merge data into the KV Store

Search Schedule

Cron Schedule */30 * * * *

Enter a cron-style schedule. For example */5 * * * * (every 5 minutes) or 0 21 * * * (every day at 9 PM). Real-time searches use a default schedule of */5 * * * *.

Scheduling Real-time Continuous

Controls the way the scheduler computes the next execution time of a scheduled search. This controls the realtime_schedule setting. [Learn more](#)

PREVIEW

```
| ldapsearch domain=flowmill-domain search="(&(objectClass=computer))" attrs="distinguishedName, dNSHostName, managedBy, sAMAccountName" | rex max_match=5 field=distinguishedName "OU=(?<dn_parsed>[^,]+)" | eval nt_host=replace(sAMAccountName, "\$", ""), dns='dNSHostName', owner='managedBy', bunit_split=split(dn, ","), category=lower(replace(mvjoin(dn_parsed, "|"), " ", "_")), priority=case(match(category, "domain_controllerexchange|citrix"), "critical", match(category, "serverdisabled"), "high", match(category, "workstation|desktop|mobile|laptop"), "medium", category IN ("staging", "test"), "low", 1==1, "unknown"), is_expected;if(priority IN ("critical", "high"), "true", "false") | rex field=bunit_split "(OUCN)=(?<bunit>.+)" | table ip, mac, nt_host, dns, owner, priority, lat, long, city, country, bunit, category, pci_domain, is_expected, should_timesync, should_update, requires_av | outputlookup flowmill_LDAP_assets
```

[Run search](#)

Cancel Save

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

Example: LDAP Search Identity Upload

- Example search for collecting identity data from Active Directory
 - Use as a guide to construct and test a working search
 - Rename the lookup to something appropriate for your environment

```
|ldapsearch domain=<domain_name> search="(&(objectclass=user)(!(objectClass=computer)))"  
|makemv userAccountControl  
|search userAccountControl="NORMAL_ACCOUNT"  
|eval suffix=""  
|eval priority="medium"  
|eval category="normal"  
|eval watchlist="false"  
|eval endDate=""  
|table sAMAccountName,personalTitle,displayName,givenName,sn,suffix,mail,telephoneNumber,mobile,manager,  
priority,department,category,watchlist,whenCreated,endDate  
|rename sAMAccountName as identity, personalTitle as prefix, displayName as nick, givenName as first, sn  
as last, mail as email, telephoneNumber as phone, mobile as phone2, manager as managedBy, department as  
bunit, whenCreated as startDate  
|outputlookup my_identity_lookup
```

Troubleshooting Assets and Identities

- Examine CSV files

`$SPLUNK_HOME/etc/apps/SA-IdentityManagement/lookups`

- Verify that all CSV files are properly formatted

- Examine lookup configuration

`$SPLUNK_HOME/etc/apps/SA-IdentityManagement/default/transforms.conf`

- Check log files (over all time)

`index=_internal sourcetype=python_modular_input collection=assets_by_str OR collection=identities_expanded`

- Test an asset match:

```
| makeresults | eval src="1.2.3.4" | `get_asset(src)`
```

- Test an identity match:

```
| makeresults | eval user="hax0r" | `get_identity4events(user)`
```

Asset Matching Algorithm

- For assets, ES takes the value from an event's `src`, `dvc`, or `dest` field and tries to match it to these columns in this order

Order	Column	Description
1	ip	match the IP address or address range
2	mac	match on a Media Access Control address
3	dns	match on DNS name
4	nt_host	match on Windows Machine Name (a.k.a. NetBIOS name)

- ES uses the above order to make its first match, then checks CIDR-based matches for IP addresses

CIDR Asset Matching Algorithm

- For `ip` and `mac` field ranges, if more than one range matches, ES matches on the smallest range

1	
1	<code>ip</code>
2	<code>1.2.3.1-1.2.3.255</code>
3	<code>1.2.3.1-1.2.3.4</code>

For example, `host=1.2.3.4` matches both the first and second IP ranges; however, it only matches on the second one since that's the smaller range.

- Asset matching allows you to create large, catch-all categories on MAC or IP ranges, yet still single out smaller groups or individual IPs within the larger group

Identity Matching

- For identities, ES takes a value from an event's `user`, `src_user`, `email`, or `src_email` field and tries to match it to a value in the "identities" lookup in the order shown here

Order	Column	Description
1	identity	Exact match on any one of a list of usernames in <code>identity</code> column
2	Email	Exact match
3	Email	First part of email, i.e. "htrapper" of "htrapper@acmetech.com"
4	Any	Disabled by default—see "conventions" in <code>identityLookup.conf.spec</code>

Watchlisting Assets and Identities

- Add identities and assets to a **watchlist** to highlight them in various dashboards and searches
 - Watchlisted assets or identities trigger the **Watchlisted Event Observed** correlation search, if enabled
 - Watchlisted users display on the **User Activity** dashboard
- Watchlist users by setting **watchlist** to **true** in the Identities lookup

1	identity	prefix	nick	first	last	suffix	email	phone	managedBy	priority	bunit	category	watchlist	startDate
2		Mr.		Martin	Awe		mawe@acmetech.com	+1 (800)555-1562 +1 (800)555-3327		critical	americas		TRUE	5/1/2003 0:00:00
3			Nene	Ranee	Majcher		rmajcher@acmetech.com	+1 (800)555-8762 +1 (800)555-8549			americas	contractor	TRUE	9/15/96 1:55:00
4		Ms.		Elouise	Jennifer		ejennifer@acmetech.com	+1 (800)555-7388 +1 (800)555-2669			americas			132388260
5		Mrs.		Larisa	Kerst		lkerst@acmetech.com	+1 (800)555-4897 +1 (800)555-4311	pepper	low	americas			12/12/2004
6		Miss		Miki	Pickle		mpickle@acmetech.com	+1 (800)555-5501 +1 (800)555-7321		medium	americas	pci		8/29/99 2:50:00
7	pepperla.koski	Dr.	Al	Allen	Seykoski		aseykoski@acmetech.com	+1 (800)555-2111 +1 (800)555-9996		high	americas		TRUE	105802380

- Add websites to watchlists
 - Configure > General > General Settings
 - Edit Website Watchlist Search and add asset IP or DNS

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

Asset and Identity Investigators

Asset Investigator

acme-004

acme-004

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 view: a day 6 minutes 16:03:20

Selecting an individual bar in a swim lane shows details on the right

Area graph shows activity over time period

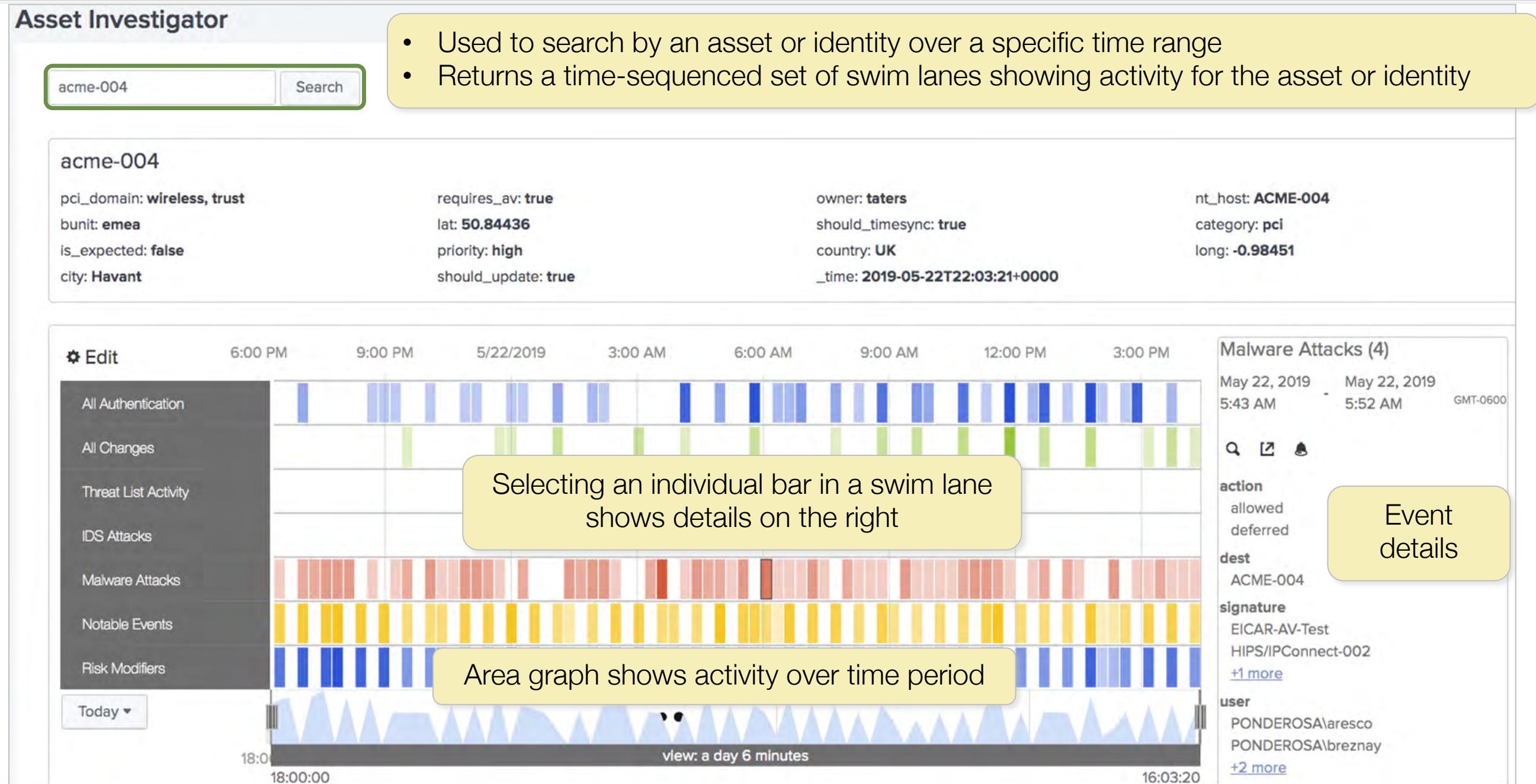
Malware Attacks (4)

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](#)

Event details

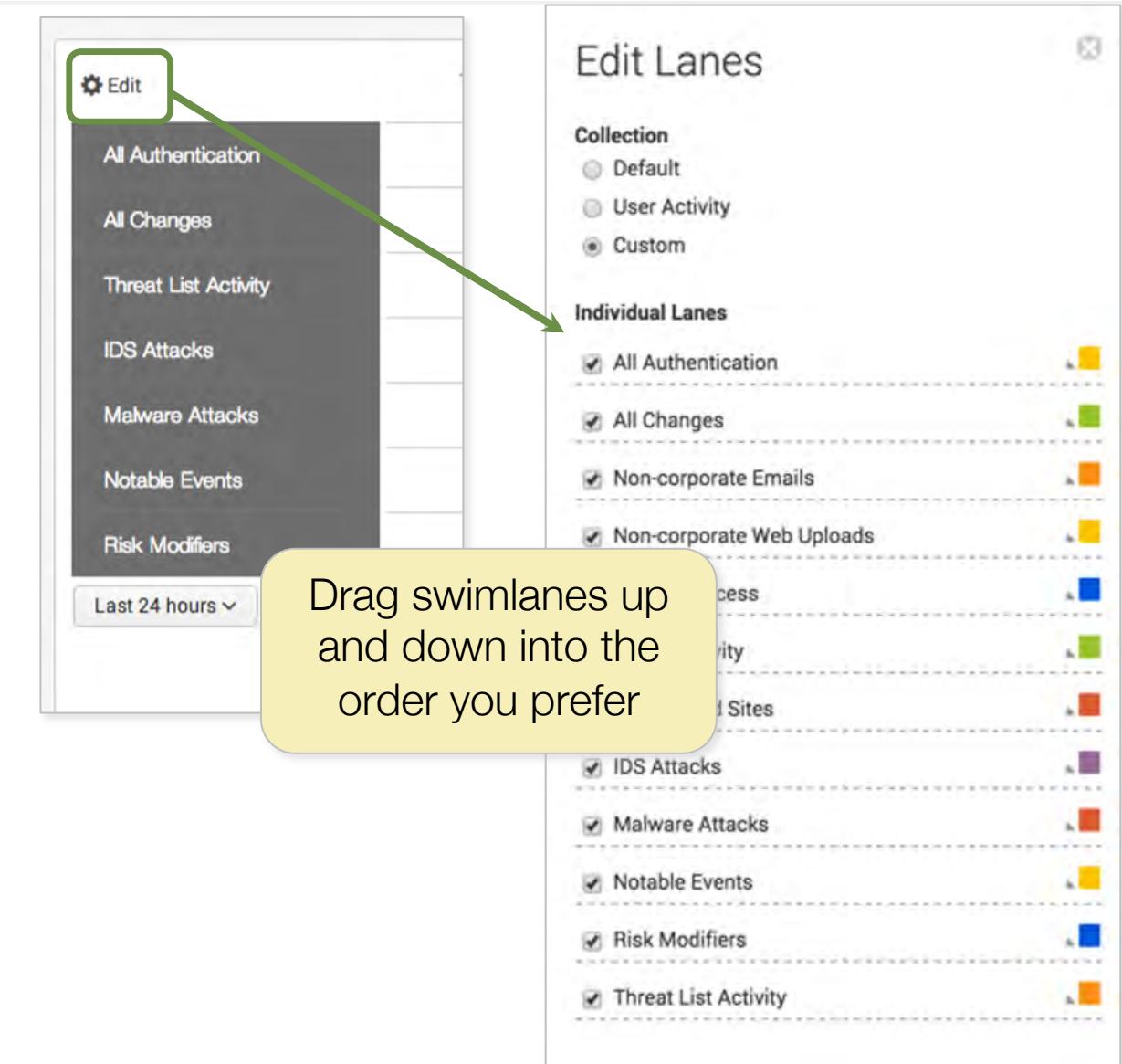


The screenshot displays the Asset Investigator interface. At the top, there's a search bar with 'acme-004' and a 'Search' button. Below the search bar, the asset details for 'acme-004' are shown, including its PCI domain, location, owner, and timestamp. The main area features a timeline visualization with various colored bars representing different event types like authentication, changes, and malware attacks over a 24-hour period. A tooltip indicates that selecting a bar in a swim lane shows details on the right. Another tooltip points to the area graph at the bottom, stating it shows activity over time. To the right, a sidebar titled 'Malware Attacks (4)' lists four specific events with their details: action (allowed/deferred), destination (ACME-004), signature (EICAR-AV-Test/HIPS/IPConnect-002), and user (PONDEROSA\aresco/PONDEROSA\breznay). A large yellow callout box labeled 'Event details' points to the sidebar.

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 lane searches and set overall defaults and permissions per role



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

Create a Swim Lane Search

From Content Management, select Swim Lane Search from the Create New Content menu and complete the information

Swim Lane Search

Search Name	Authentication Failures
App	Enterprise Security
Search Title	Authentication Failures
Search	<pre> tstats `summariesonly` values(Authentication.action) as action,values(Authentication.app) as app,values(Authentication.src) as src,values(Authentication.dest) as dest,values(Authentication.user) as user,count from datamodel=Authentication.Authentication where Authentication.action=failure AND (\$constraints\$) by _time span=\$span\$</pre>
Drilldown Search	<pre> from datamodel:"Authentication"."Authentication" search Authentication.action=failure AND (\$constraints\$)</pre> <p>Defines the view to redirect users to when they click a swim lane item.</p>
Color	Purple
Entity Type	Identity
Constraint Fields	Authentication.src_user <input type="button" value="X"/> user <input type="button" value="X"/>

Valid constraint fields: user, src_user, risk_object, threat_match_value [Learn more](#)

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

Module 11 Lab: Working with Assets & Identities

Time: 30 minutes

Tasks:

1. Modify asset priority for *PROD-MFS* servers
2. Create two swim lane searches that track successful and failed logins for identities
3. Use the Identity Investigator to confirm the newly created swim lanes

Module 12:

Managing Threat Intelligence

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

Objectives

- Understand and configure threat intelligence
- Use the Threat Intelligence Management interface to configure a new threat list

The 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

<https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/threatintelligenceframework/#How-Splunk-Enterprise-Security-processes-threat-intelligence>

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

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

ES Component	ess_analyst	ess_user
Edit Intelligence Downloads Permits the role to edit intelligence download settings.	<input type="checkbox"/>	<input type="checkbox"/>

- 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

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

Configuring Threat Intelligence

- ES can download the following threat intelligence types:
 - Threat lists: IP addresses of known malicious sites
 - STIX/TAXII: detailed information about known threats, including threat type, source, etc.
 - OpenIOC: additional detailed information about known threats
- Threat lists can also be configured locally
- Many intel sources require regular refresh from external sources
- This information is used by the **Threat Activity Detected** correlation search

Included Generic Intel Sources

- Generic intelligence included in ES by default
- These intelligence sources are not added to the threat intelligence KV Store collections, but are used to enrich data in ES

Data List	Data Provider	URL
Cisco Umbrella Top 1 Million Sites	Cisco	https://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip
ICANN Top-level Domains List	IANA	https://data.iana.org/TLD/tlds-alpha-by-domain.txt
MaxMind GeoIP ASN IPv4 database	MaxMind	https://download.maxmind.com/app/geoip_download?edition_id=GeoLite2-ASN-CSV&license_key=YOUR_LICENSE_KEY&suffix=zip
MaxMind GeoIP ASN IPv6 database	MaxMind	https://download.maxmind.com/app/geoip_download?edition_id=GeoLite2-ASN-CSV&license_key=YOUR_LICENSE_KEY&suffix=zip
Mozilla Public Suffix List	Mozilla	https://publicsuffix.org/list/effective_tld_names.dat
MITRE ATT&CK framework	Mitre	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

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

Threat Intelligence Audit

Threat Intelligence Audit **Audit > Threat Intelligence Audit** [Edit](#) [Export](#) [...](#)

Details regarding updates to ES Threat Intelligence

Download Enabled/Disabled Download Location

Enabled All

Display status and time for all downloads

_time	stanza	disabled	type	url	weight	exit_status	download_status	run_duration
2021-01-02 12:21:45	iblocklist_logmein	0	threatlist	https://list.iblocklist.com/?list=logmeintoit	1	0	retrying download	0.0
2021-01-02 02:15:18	iblocklist_piratebay	0	threatlist	https://list.iblocklist.com/?list=nzldzlpkgrcncomnttb	60	0	threat list downloaded	1.0
2021-01-02 02:15:19	iblocklist_proxy	0	threatlist	https://list.iblocklist.com/?list=bt_proxy	60	0	threat list downloaded	2.0
2021-01-02 02:15:18	iblocklist_rapidshare	0	threatlist	https://list.iblocklist.com/?list=zfucwtjkfwkalystktyiw	60	0	threat list downloaded	1.0
2021-01-02 02:15:18	iblocklist_spyware	0	threatlist	https://list.iblocklist.com/?list=bt_spyware	60	0	threat list downloaded	1.0

< Prev 1 2 3 Next >

Sourcetype Level Intelligence Source Time Range

All x All x All Last 24 hours

View details of downloads including errors like
“No content returned” and “retrying download”

i	Time	Event
>	1/21 12:21:46.418 PM	2021-01-02 19:21:46,418+0000 INFO pid=20445 tid=MainThread file=threatlist.py:download_threatlist_file:543 stanza="iblocklist_logmein" retries_remaining="3" status="retrying download" retry_interval="60" url="https://list.iblocklist.com/?list=logmeintoit" host = ip-10-0-0-169.us-west-2.compute.internal source = /opt/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download
>	1/21 12:21:46.418 PM	2021-01-02 19:21:46,418+0000 ERROR pid=20445 tid=MainThread file=protocols.py:run:191 No content returned when querying https://list.iblocklist.com/?list=logmeintoit host = ip-10-0-0-169.us-west-2.compute.internal source = /opt/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download

Intelligence Audit Events

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

Intelligence Management Interface

Configure > Data Enrichment > Threat Intelligence Management

Threat Intelligence Management
Unified interface for enriching and managing threat intelligence data.

[Back to ES Configuration](#)

Sources Threat Matching Global Settings

filter Search icon

The Threat Intelligence Management interface has three tabs for creating and managing threat intel: Sources, Threat Matching, and Global Settings

Name	Description	Interval	Type	URL	Weight	Status	Actions
alexa_top_one_million_sites	Alexa Top 1 Million Sites, copyright 2014, Alexa Internet (www.alexa.com)	86400	alexa	https://s3.amazonaws.com/alexa-static/top-1m.csv.zip	60	Enable	Advanced Edit
cisco_top_one_million_sites	Cisco Umbrella Top 1 Million Sites, copyright 2018, Cisco Umbrella	86400	cisco	https://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip	60	Enable	Advanced Edit
emerging_threats_compromised_ip_blocklist	Emerging Threats compromised IPs blocklist	43200	threatlist	https://rules.emergin.../blockrules/compromised-ips.txt	60	Enable	Advanced Edit
emerging_threats_ip_blocklist	Emerging Threats fwip rules	43200	threatlist	https://rules.emergin.../fwrules/emerging-Block-IPs.txt	60	Enable	Advanced Edit
hailataxii_malware	Hail a TAXII.com malware domain host list	86400	taxii	http://hailataxii.com/taxii-data	60	Enable	Advanced Edit
iblocklist_logmein	Addresses that are used by the LogMeIn product to enable unauthorized remote access	43200	threatlist	https://list.iblocklist.com/?list=logmeintoit	1	Enabled	Advanced Edit

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

Sources Tab

Configure > Data Enrichment > Threat Intelligence Management

Threat Intelligence Management
Unified interface for enriching and managing threat intelligence data.

< Back to ES Configuration

Sources Threat Matching Global Settings

The Sources tab lists all configured intel downloads

Create a new download by selecting the type

New

Name	Description	Interval	Type	URL	Weight	Status	Line Oriented
alexa_top_one_million_sites	Alexa Top 1 Million Sites, copyright 2014, Alexa Internet (www.alexa.com)	86400	alexa	https://s3.amazonaws.com/alexa-static/top-1m.csv.zip	60	Enabled	IOC/STIX/STIX2
cisco_top_one_million_sites	Cisco Umbrella Top 1 Million Sites, copyright 2018, Cisco Umbrella	86400	cisco	https://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip	60	Enabled	Local
emerging_threats_compromised_ips	Emerging Threats compromised IPs blocklist	43200	threatlist	https://rules.emergingthreats.net/blockrules/compromised-ips.txt	60	Enabled	Advanced Edit
emerging_threats_fwp_rules	Emerging Threats fwip rules	43200	threatlist	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt	60	Enabled	Advanced Edit
hailataxii_malware	Hail a TAXII.com malware domain host list	86400	taxii	http://hailataxii.com/taxii-data			Advanced Edit
iblocklist_logmein	Addresses that are used by the LogMeIn product to enable unauthorized remote access	43200	threatlist	https://list.iblocklist.com/?list=logmeintoit			Advanced Edit

Click a download name to display the Edit Intelligence Document form. Allows you to edit the fields relevant only to the selected document

Use Advanced Edit to change all Settings for the download

filter

< Prev 1 2 3 Next >

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

Add a Threat Download

Add Intelligence Document

General **Parsing** **Advanced**

Name: **Download name (no spaces)**
The intelligence document name.

Description:

Type:

Url: **Valid URL for the download location**
The intelligence document URL.

Weight: **60**
An integer used to calculate the risk score of an indicator on the threat document.

Interval: **43200**
The interval at which to process the intelligence.

Max Age: **-30d**
The retention period for threat intelligence from this source (expressed as a Splunk relative time string). For example, "-7d".

Max Size: **52428800**
The maximum size in bytes. 52428800 is 50 MB.

Archive Member:

POST arguments:

Threat Intelligence:
Classify the intelligence document as threat intelligence.

Check Threat Intelligence to use information as threat intel for the _intel KV collections

Save

Add Intelligence Document

General **Parsing** **Advanced**

File Parser: **auto**
The file parser used to interpret the downloaded threat intel. Such as auto, line, ioc, stix, stix2, or stix_taxii.

Delimiting regular expression: **,**
A delimiter used to split the lines in the file, comma, semi colon, etc.

Extracting regular expression:

Ignoring regular expression: **(^#|^s*\$)**
A regular expression by default, ignores blank lines and lines beginning with #

Fields: **,**
A transforms.conf-style list of fields.

Skip header lines: **0**
The number of header lines to skip. Should be "1" for lookup tables.

Save

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

Add a Threat Download (cont.)

The screenshot shows the 'Add Intelligence Document' dialog box with the 'Advanced' tab selected. The configuration options include:

- Intelligence file encoding:** Encoding of intelligence file, if not ascii.
- User Agent:** A custom user agent string used to replace the default sent by Enterprise Security.
- Retries:** 3 (number of attempts to download the file)
- Retry Interval:** 60 (seconds to wait between download attempts)
- Timeout:** 30 (seconds to wait before marking the download as failed)
- Remote site user:** A username to use in remote authentication, if required (only if the threat feed requires authentication). This must be configured in Splunk Credential Management.
- Remote Site User Realm:** The Splunk Enterprise secure storage realm of the corresponding site user. This is distinct from proxy credentials. If present, used in conjunction with remote site user to build the ID of the Splunk Enterprise secure storage entry.
- Sinkhole:** (Delete threat intelligence files after processing. Does not delete generic intelligence files.)
- Debug:** (true, debug logging is enabled)

Annotations with callouts explain the following settings:

- Retries:** number of attempts to download the file
- Retry Interval:** seconds to wait between download attempts
- Timeout:** seconds to wait before marking the download as failed
- Remote site user and realm:** only if the threat feed requires authentication. Must be configured in Splunk Credential Management
- Sinkhole:** delete file after downloading
- Enable debug logging**

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

Upload an Intel File

Threat Intelligence Management
Unified interface for enriching and managing threat intelligence

[Back to ES Configuration](#)

Sources Threat Matching Global Settings

filter

Name	Description
alexa_top_one_million_sites	Alexa Top 1 Mil copyright 2014 (www.alexa.co...)
cisco_top_one_million_sites	Cisco Umbrella copyright 2018

Add Intelligence Document

General Parsing Advanced

Drop your file here or [browse...](#)

File names will be edited to:

Overwrite Overwrite The original file

Name

Description

Type
An arbitrary name representing the type of intelligence in this download, such as "malware". Must be "taxii" for TAXII feeds.

Weight An integer used to calculate the risk score of an asset or identity associated with an indicator on the threat document.

Interval The interval at which to process the intelligence document.

Max Age The retention period for threat intelligence from this source (expressed as a Splunk relative time string). For example, "-7d".

Max Size The maximum size in bytes that an intelligence download can be. For example, 52428800 is 50 MB.

Archive Member
The regular expression pointer to a member (file) within a multi-file zip archive.

Threat Intelligence Classify the intelligence document as threat intelligence.

Manually upload a threat intel file by selecting **Upload** from the **New** menu

	Weight	Status	Line Oriented
azonaws.com/alexa-static.ip	60	Enabled	IOC/STIX/STIX2
west-1.amazonaws.com/tic/top-1m.csv.zip	60	Enabled	TAXII
		Disabled	Local
		Disabled	Upload

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

Threat Matching

Edit the Threat Match settings that generate the SPL for threat match searches and enrich data with threat intelligence

Source: type of threat match sources enabled. Click to edit

Interval: how often the search runs

Earliest and Latest: when the search starts and completes

Match Fields: what fields to match against to generate threats

Unified interface for enriching and managing threat intelligence data.

Back to ES Configuration

Sources Threat Matching Global Settings

Source	Interval	Earliest Time	Latest Time	Match Fields	Status
> certificate_common_name	0,30 ****	-40m@m	-10m@m	<ul style="list-style-type: none">All_Certificates.SSL.ssl_issuer_common_nameAll_Certificates.SSL.ssl_subject_common_name	Enabled Disable
> certificate_serial	5,35 ****	-40m@m	-10m@m	<ul style="list-style-type: none">All_Certificates.SSL.ssl_issuer_organizationAll_Certificates.SSL.ssl_subject_organization	Enabled Disable
> certificate_unit	10,40 ****	-40m@m	-10m@m		Enabled Disable
> dest	15,45 ****	-40m@m	-10m@m	<ul style="list-style-type: none">All_Certificates.SSL.ssl_issuer_unitAll_Certificates.SSL.ssl_subject_unit	Enabled Disable
				<ul style="list-style-type: none">DNS.answerAll_Traffic.destIDS_Attacks.destWeb.dest	Enabled Disable

Open in search ↗

```
| multisearch [
| tstats prestats=true summariesonly=true values("sourcetype"),values("DNS.src"),values("DNS.dest") from datamodel="Network_Resolution"."DNS" by "DNS.answer"
| `truncate_domain_dedup(DNS.answer, DNS.answer_truncated)`
| lookup "threatintel_by_cidr" value as "DNS.answer" OUTPUT threat_collection as tc0,threat_collection_key as tck0
| lookup "threatintel_by_domain" value as "DNS.answer" OUTPUT threat_collection as tc1,threat_collection_key as tck1
| lookup "threatintel_by_domain" value as "DNS.answer_truncated" OUTPUT threat_collection as tc2,threat_collection_key as tck2
| lookup "threatintel_by_system" value as "DNS.answer" OUTPUT threat_collection as tc3,threat_collection_key as tck3
| where isip($src) OR isip($dest) OR isip($tc0) OR isip($tc1) OR isip($tc2) OR isip($tc3)
]
```

Expand a Source to see the threat match configuration

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

Threat Matching (cont.)

The screenshot shows the Splunk Threat Match Configuration interface. On the left, the main configuration window displays fields for Name, Source, Earliest Time, Latest Time, Interval, Multilookup, and Max Aggregate Values. A yellow callout points to the 'Earliest Time' and 'Latest Time' fields, explaining they define the time range for threat generation. On the right, a modal window titled 'Add a dataset' lists datasets with their status, datamodel, summaries, object, and match field. A yellow callout points to this window, explaining it allows editing, removing, or adding datasets to the configuration.

Edit Threat Match Configuration

- Name: threatmatch/dest
- Source: dest
- Earliest Time: -40m@m
- Latest Time: -10m@m
- Interval: 20,50 ****
- Multilookup:
- Max Aggregate Values: 10

Edit Threat Match Configuration

Datasets: + Add dataset

- Status: Enabled | Disable
Datamodel: Network_Resolution
Summaries Only: ✓
Object: DNS
Match Field: DNS.answer
- Status: Enabled | Disable
Datamodel: Network_Traffic
Summaries Only: ✓
Object: All_Traffic
Match Field: All_Traffic.dest
- Status: Enabled | Disable
Datamodel: Intrusion_Detection
Summaries Only: ✓
Object: IDS_Attacks
Match Field: IDS_Attacks.dest
- Status: Enabled | Disable
Datamodel: Web_Events
Summaries Only: ✓
Object: Web_Events.dest
Match Field: Web_Events.dest

Add a dataset

- Datamodel: Select...
- Object: Select...
- Summaries Only:
- Event Filter: (empty)
- Match Field: Select...
- Aggregates: + Add aggregate

Save Dataset **Cancel**

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

Global Settings

Threat Intelligence Management

Unified interface for enriching and managing threat intelligence data.

[Back to ES Configuration](#)

Sources Threat Matching Global Settings

Configure the global settings of the threatlist modular input

Proxy server settings

Proxy server settings for threatlist downloads. [Learn more](#)

Proxy server [?](#)

Proxy port [?](#)

Proxy user [?](#)

If a proxy server is used to send intel to ES, configure that information here

Proxy user realm [?](#)

Note



Proxy user must be configured in Splunk Credential Management

Parse modifier settings

Settings for parsing fields from other fields. [Learn more](#)

Certificate attribute breakout [?](#)

IDNA encode domains [?](#)

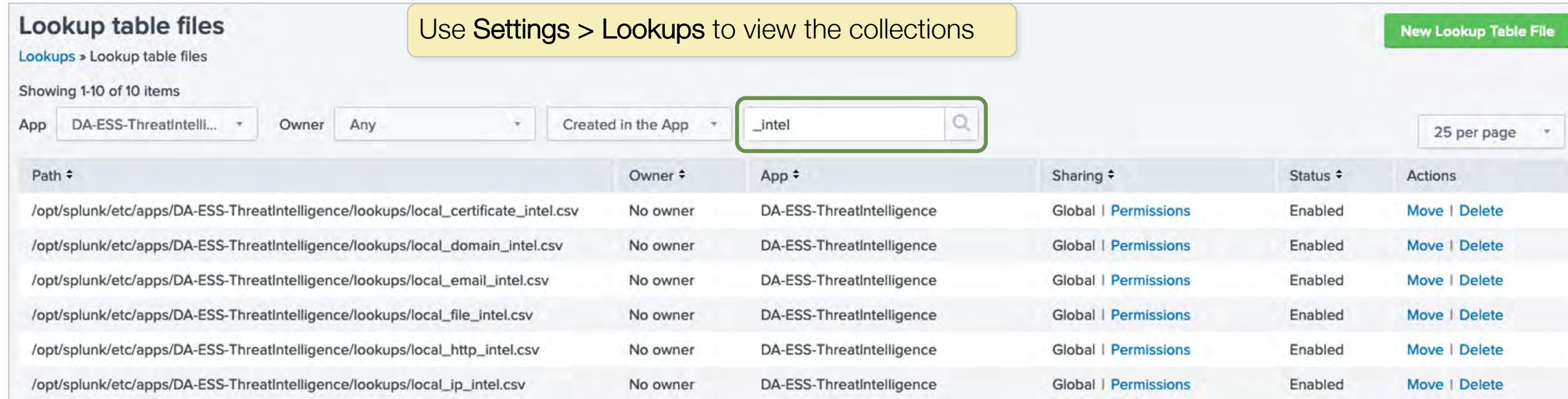
Parse domain from URL [?](#)

Configure ES to extract fields and values embedded in other fields, such as extracting the domain name from a URL

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

Viewing Threat Intel Collections

- After download, threat intel data is stored in KV store collections with the “_intel” suffix



The screenshot shows the Splunk interface for managing lookup table files. A yellow callout box highlights the search bar with the text "Use Settings > Lookups to view the collections". The search bar contains the query "_intel", which is highlighted with a green rectangle. The table below lists 10 items, all of which contain the "_intel" suffix in their paths.

Path	Owner	App	Sharing	Status	Actions
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_certificate_intel.csv	No owner	DA-ESS-ThreatIntelligence	Global Permissions	Enabled	Move Delete
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_domain_intel.csv	No owner	DA-ESS-ThreatIntelligence	Global Permissions	Enabled	Move Delete
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_email_intel.csv	No owner	DA-ESS-ThreatIntelligence	Global Permissions	Enabled	Move Delete
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_file_intel.csv	No owner	DA-ESS-ThreatIntelligence	Global Permissions	Enabled	Move Delete
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_http_intel.csv	No owner	DA-ESS-ThreatIntelligence	Global Permissions	Enabled	Move Delete
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_ip_intel.csv	No owner	DA-ESS-ThreatIntelligence	Global Permissions	Enabled	Move Delete

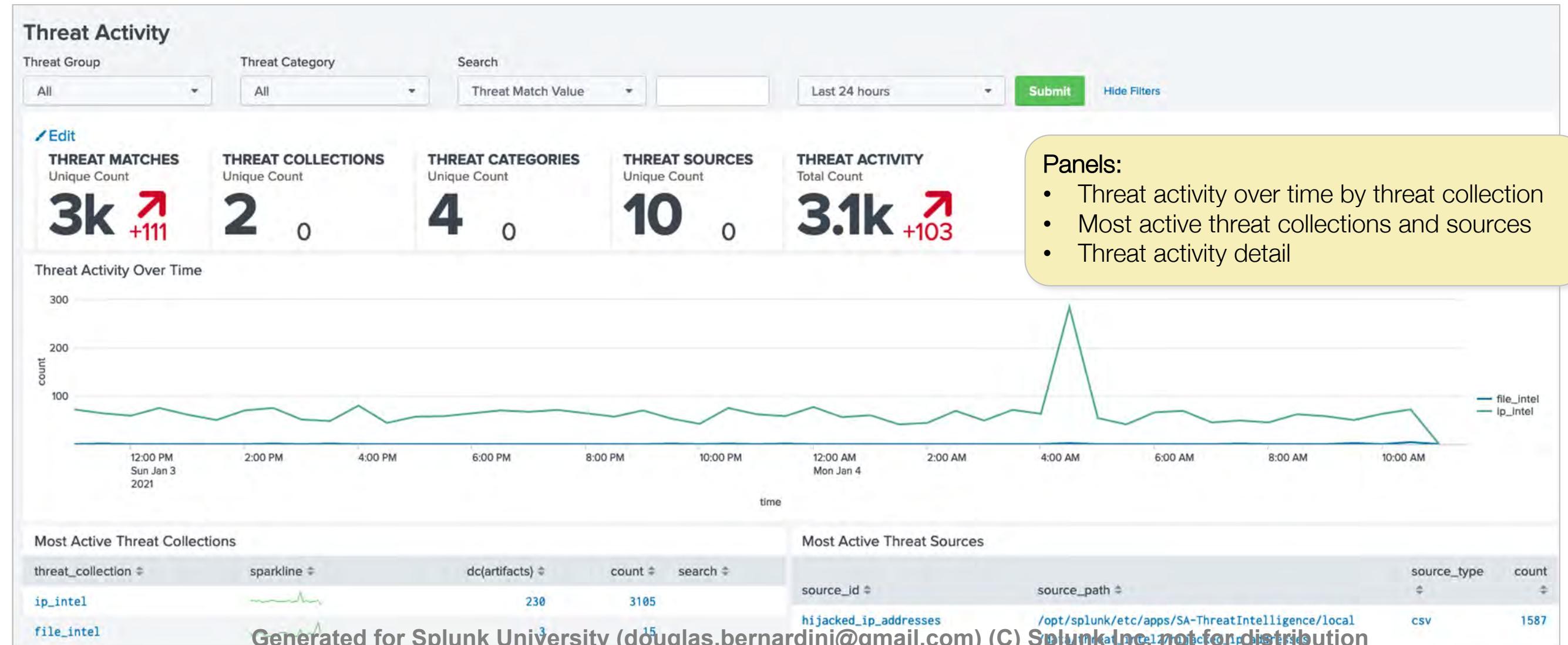
- Use `|inputlookup` to examine the contents of a collection
- Use the Threat Artifacts dashboard to examine the overall contents of the entire threat intelligence framework

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

Threat Activity Dashboard

Security Intelligence > Threat Intelligence > Threat Activity

Display details related to known threat sites over a period of time



Threat Artifacts

Security Intelligence > Threat Intelligence > Threat Artifacts
Displays the current content of the downloaded threat intel

Threat Artifacts													
Threat Artifact	Threat Category	Threat Group	Malware Alias	Intel Source ID	Intel Source Path		Submit	Hide Filters					
Threat ID	All	All											
Threat Overview													
Threat Overview													
source_id	source_path	source_type	threat_group	threat_category									
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)	+ APT (and 2 more)									
hijacked_ip_addresses	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel2/hijacked_ip_addresses	csv	hijacked_ip_addresses	hijacks									
iblocklist_logmein	/opt/splunk/var/lib/splunk/modinputs/threatlist/iblocklist_logmein	csv	iblocklist_logmein	threatlist									
iblocklist_piratebay	/opt/splunk/var/lib/splunk/modinputs/threatlist/iblocklist_piratebay	csv	iblocklist_piratebay	threatlist									
iblocklist_proxy	/opt/splunk/var/lib/splunk/modinputs/threatlist/iblocklist_proxy	csv	iblocklist_proxy	threatlist									
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	threat_group
file_intel	stix	undefined	undefined		1356	ip_intel	csv	5801	0	0	0	5801	iblocklist
file_intel	stix	F	APT		194	ip_intel	csv	3644	0	0	0	3644	iblocklist
file_intel	stix	admin338	APT		194	ip_intel	csv	604	0	0	0	604	hijacked_i
file_intel	stix	japanorus	APT		194	ip_intel	stix	164	145	0	0	309	F

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

Module 12 Lab: Threat Intel Framework

Time: 10 minutes

Tasks:

Add a new threat list download

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

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



Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None



Splunk Enterprise Security Certified Admin Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete the following course:

- [Administering Splunk Enterprise Security](#)



Congratulations! You are a...



Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

Recommended Next Steps

- [Splunk Phantom Certified Admin](#)

See [here](#) for registration assistance.

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

Splunk Security Courses

- For more Splunk security training, please review these courses on
https://www.splunk.com/en_us/training.html
 - *Splunk User Behavior Analytics*
 - *Administering Splunk SOAR*
 - *Developing SOAR Playbooks*
 - *Advanced SOAR Implementation*

Community

- Splunk Community Portal

splunk.com/en_us/community.html

- Splunk Answers

answers.splunk.com

- Splunk Apps

splunkbase.com

- Splunk Blogs

splunk.com/blog/

- .conf

conf.splunk.com

- Slack User Groups

splk.it/slack

- Splunk Dev Google Group

groups.google.com/forum/#!forum/splunkdev

- Splunk Docs on Twitter

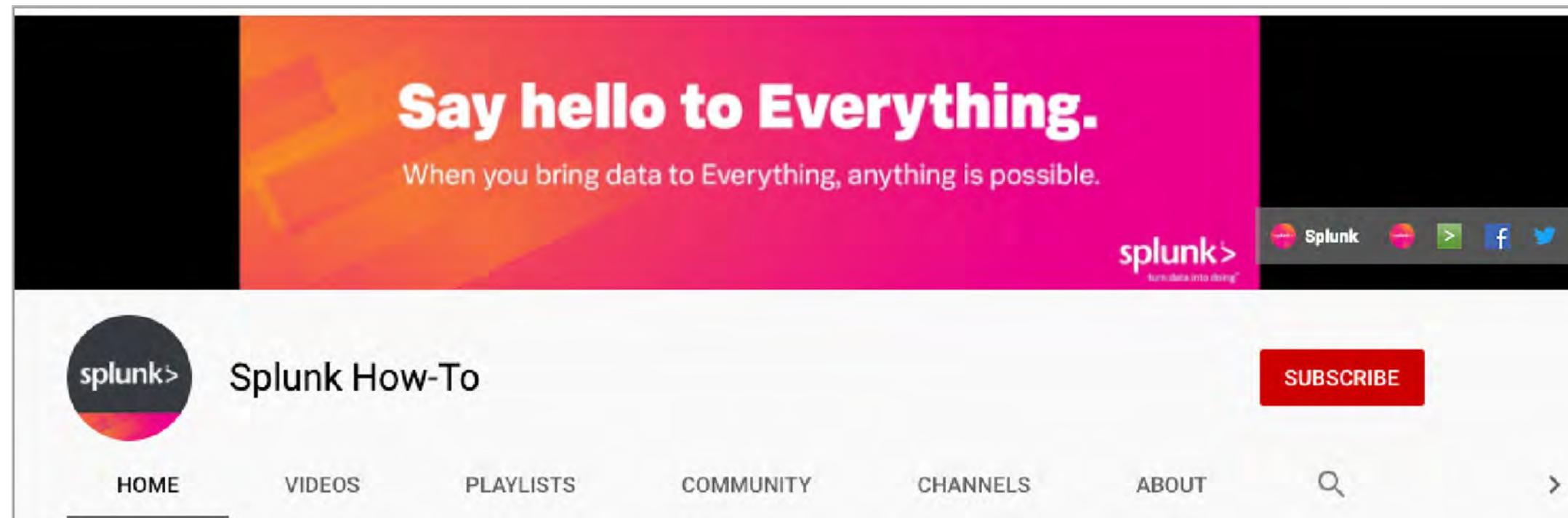
twitter.com/splunkdocs

- Splunk Dev on Twitter

twitter.com/splunkdev

Splunk How-To Channel

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



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

Support Programs

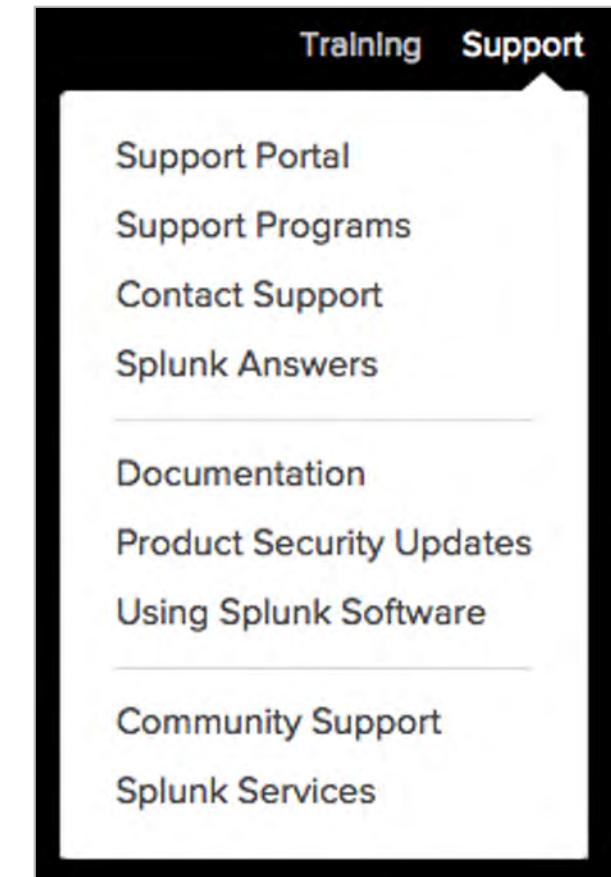
- **Web**
 - Documentation: dev.splunk.com and docs.splunk.com
 - Wiki: wiki.splunk.com
- **Splunk Lantern**

Guidance from Splunk experts

 - 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
 - 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)



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



MGM Grand, Las Vegas, NV | June 13–16
Virtual | June 14–15

**Join us for a hybrid experience and learn why
data is key to achieving better outcomes.**

“.conf21 gave me the ability to immerse myself in all things Splunk for two full days, I learned so much.”

— John Whitefield

Progressive Insurance, IT DevOps Eng. Senior

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



Thank You

splunk>

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

Appendix A: Analyst Tools & Dashboards

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

Objectives

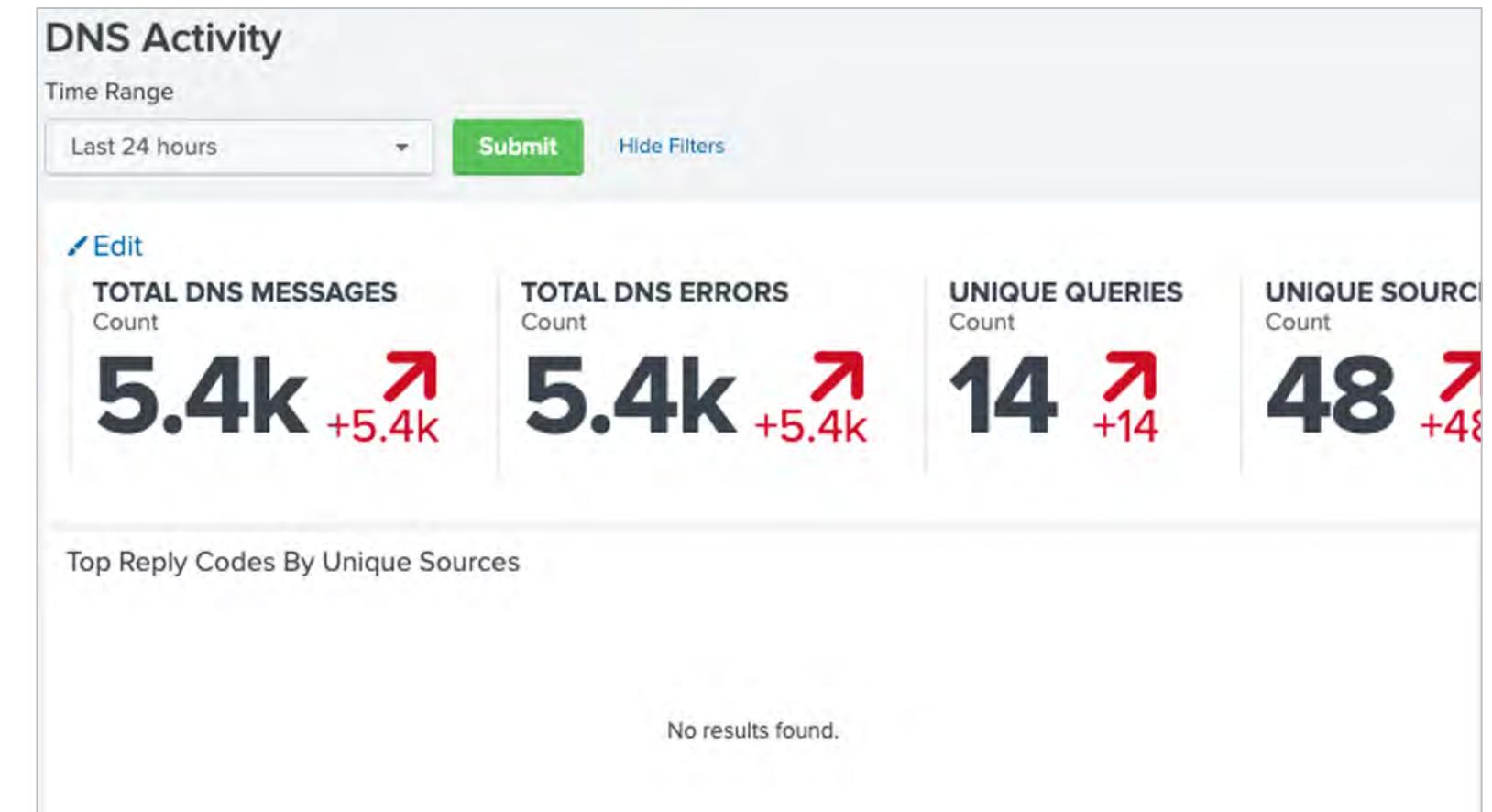
- Troubleshoot missing dashboard data
- Explain dashboard dependencies including data models and searches

Dashboard Data Dependencies

- Each dashboard panel's search pulls events from a data model
 - If a panel is missing data, examine the panel's search to see which data model is used; this can help you understand why the data is missing
 - Causes:
 - The data is not in Splunk: install and enable add-ons to input the data
 - The data is present in Splunk but is not normalized correctly: modify normalization settings
- docs.splunk.com/Documentation/ES/latest/User/DashboardMatrix

Example: DNS Activity Missing Data

- The example shows that the **Top Reply Codes By Unique Sources** panel in the DNS Activity dashboard is empty
- Using **Open in Search** shows that the data for this panel is taken from the **Network_Resolution** data model and DNS data set



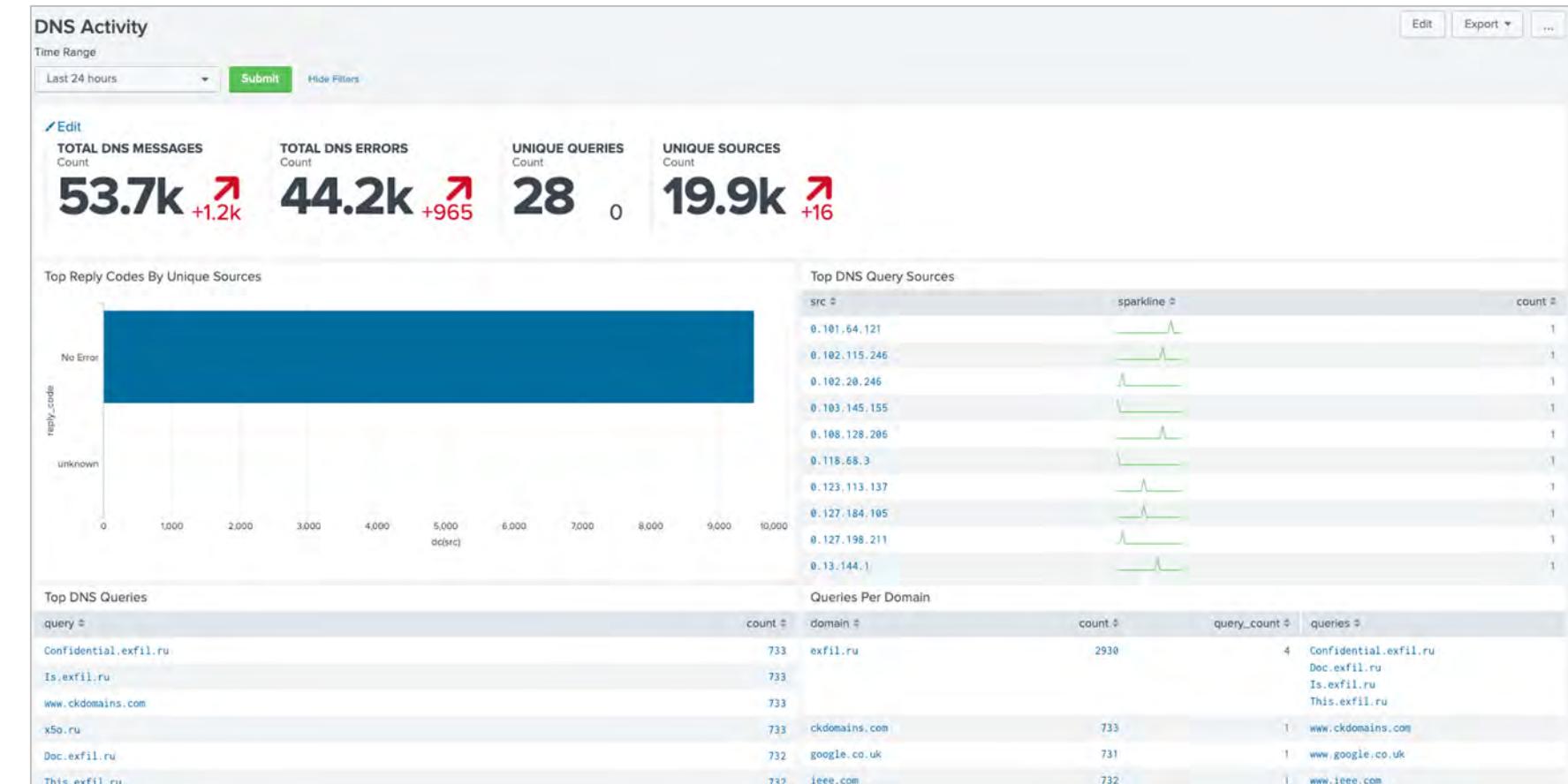
The screenshot shows a 'New Search' interface. The search bar contains the following SPL query:
| tstats 'summariesonly' dc(DNS.src) as dc(src) from datamodel=Network_Resolution.DNS where DNS.message_type="RESPONSE" by DNS.reply_code | 'drop_dm_object_name("DNS")' | sort 10 - dc(src)
The search results area below the bar shows '0 results (before 11/11/19 11:17:48.000 AM)' and 'No Event Sampling'. On the right side of the search interface, there are various buttons and a 'Save As' and 'Close' option. A green callout box highlights the 'Open in Search' button at the bottom right of the search bar.

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

Example: DNS Activity Missing Data (cont.)

Things to check if a dashboard is empty

- Is your data normalized to the data model?
- If collecting data from a streaming app like Splunk Stream, is it configured to collect the correct type of data?
- Is your data tagged properly?



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

Data Models

- Data models use tags to identify events relevant to the data model
 - For example, the **Network_Resolution.DNS** datamodel uses the **network**, **dns**, and **resolution** tags to match relevant events
 - If an event is not tagged with these constraints, it will not be referenced by the data model

Splunk Enterprise > Settings > Data models

The screenshot shows the Splunk Enterprise Settings interface with the 'Data models' section selected. Under 'Network Resolution (DNS)', the 'DNS' tab is active. A constraint is highlighted with a green border: `(cim_Network_Resolution_indexes) tag=network tag=resolution tag=dns`. Other constraints listed are '_time' (Time), 'host' (String), and 'source' (String). On the left, under 'Datasets', the 'EVENTS' tab is active, and the 'DNS' tab is also visible.

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

Searching Data Models

Use the **|from** command to search all events from the data model

New Search

```
| from datamodel:Network_Resolution.DNS
```

✓ 52,475 events (11/14/19 12:00:00.000 PM to 11/15/19 12:05:48.000 PM) No Event Sampling ▾

Events (52,475) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

sourcetype

2 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
bro_dns	32,452	61.843%
stream:dns	20,023	38.157%

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

Example: Protocol Center Missing Data

- Protocol Center is missing information for `juniper.idp`, `junos_firewall`, and `netscreen`
- Open in Search confirms the missing events are not being referenced by the `Network_Traffic.All_Traffic` data model

| tstats `summariesonly` count from datamodel=Network_Traffic.All_Traffic where `cim_filter_unknown_values(All_Traffic.app)`

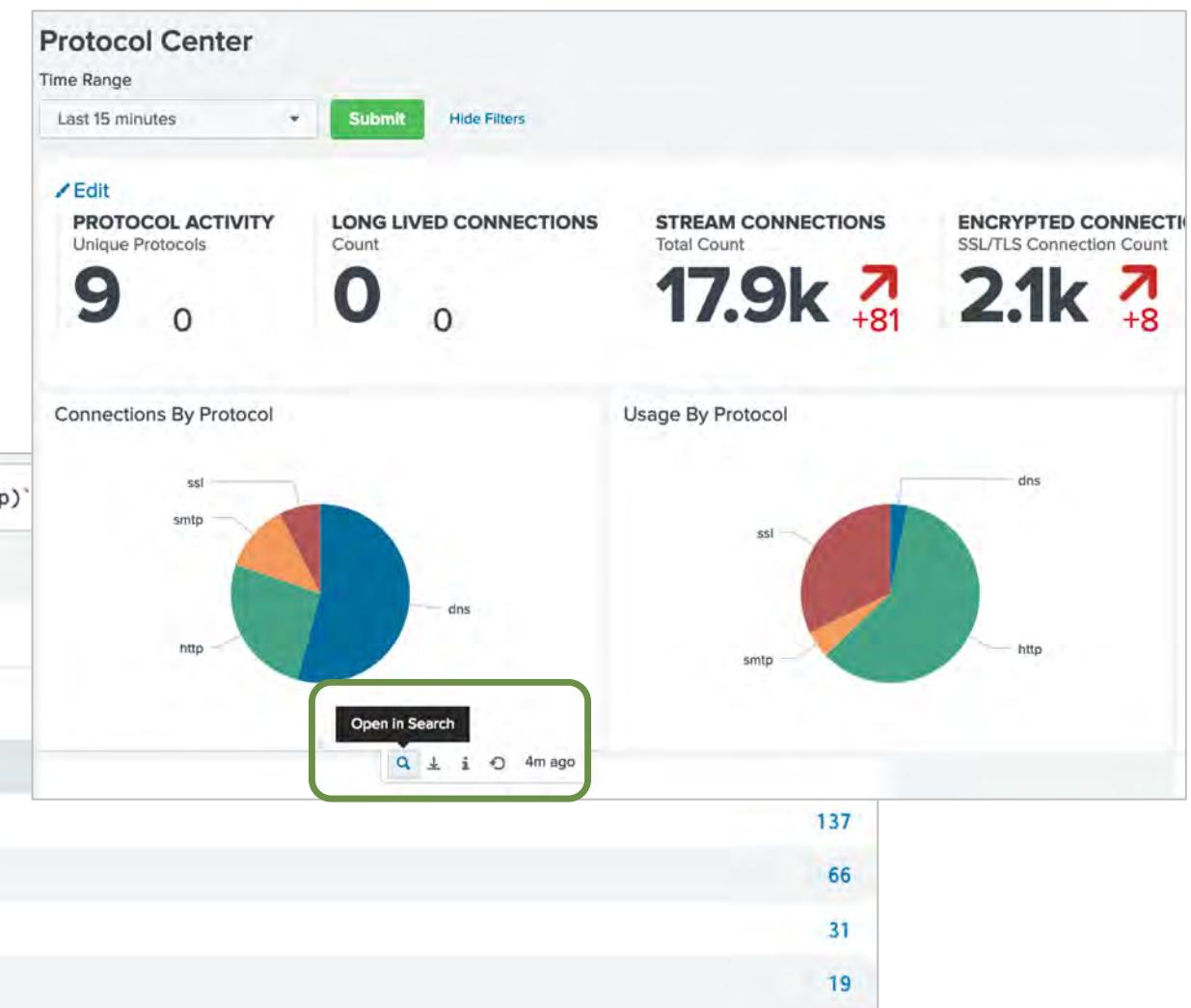
✓ 486 events (12/12/19 12:02:55.000 PM to 12/12/19 12:17:55.000 PM) No Event Sampling ▾

Events Patterns Statistics (4) Visualization

20 Per Page ▾ Format Preview ▾

all_traffic.app ▾

Protocol	Count
dns	137
http	66
smtp	31
ssl	19



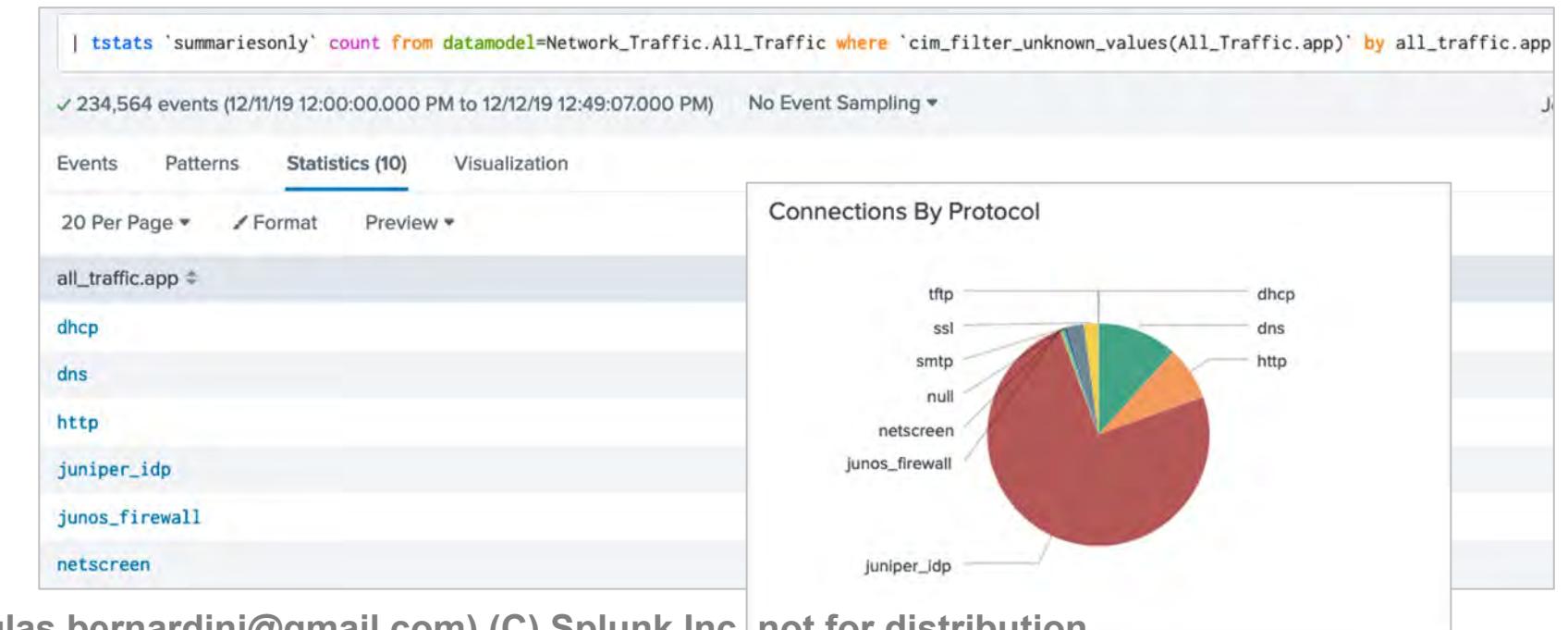
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Example: Protocol Center Missing Data (cont.)

- Apps > Manage Apps shows that the **Splunk_TA_juniper** app is disabled

The screenshot shows the Splunk 'Manage Apps' page. A search bar at the top contains the text 'Juniper'. Below it is a table with the following columns: Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. The table has one row for the 'Splunk Add-on for Juniper' app, which is version 1.0.2, has 'Yes' for update checking, 'No' for visible, 'Global | Permissions' for sharing, and 'Disabled | Enable' for status. A green box highlights the 'Status' column header and the 'Disabled | Enable' link.

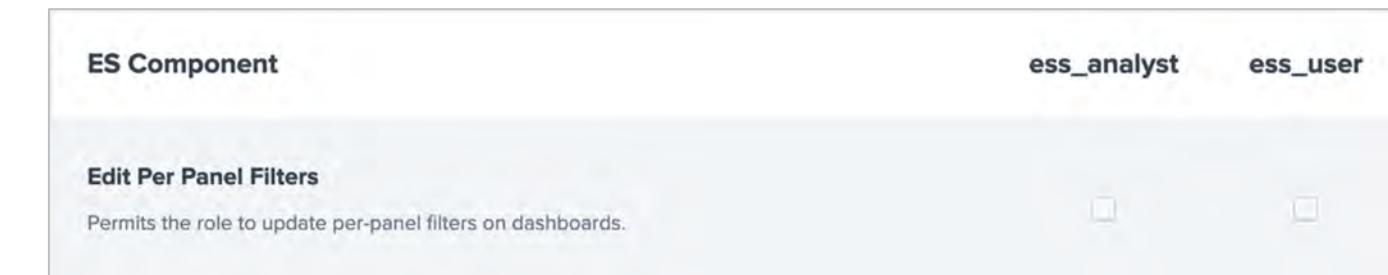
- Juniper data is now referenced by the data model and displays on the dashboard



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

Per-panel Filtering Dashboards

- Some ES dashboards allow highlighting or filtering of items on dashboard views
 - If it is determined that an event is **not a threat**, it can be added to a whitelist to remove it from the dashboard view
 - If an event is determined to be a **threat**, use the **Per-panel filter** button to add the item to the blacklist of known threats
- For Example, on **HTTP Category Analysis** filter out expected categories and highlight unwanted categories
- Permission for Per-panel filtering can be granted for **ess_analyst** and **ess_user** roles



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

Creating Per-panel Filters

The screenshot shows the 'HTTP Category Analysis' dashboard. At the top left, there are search and time range controls ('False', 'Last 24 hours', 'Submit', 'Hide Filters'). On the right are 'Edit', 'Export', and a three-dot menu.

Key statistics are displayed: MINIMUM COUNT (24), MEAN COUNT (151.6), MAXIMUM COUNT (2.3k), STDEV COUNT (329.5). Below these are 'Category Distribution' charts and a table of 'Category Details'.

A 'Per Panel Filter' modal is open on the right. It contains the following steps:

1. Select one or more events (highlighted in yellow).
2. Click Per-panel Filter (highlighted in yellow).
3. Choose to either filter out or highlight the events (yellow callout box).
4. Take action on the 2 results selected (radio buttons for 'Filter out these results' or 'Highlight these results').

The 'Category Details' table lists three items:

Per-panel Filter	category	src	dc(dest)	count	Z	lastTime
<input checked="" type="checkbox"/>	unknown	1	1	2315	6.57	12/10/2019 09:37:22
<input checked="" type="checkbox"/>	expand	1	1	290	0.42	12/10/2019 10:06:20
<input type="checkbox"/>	Website Translation	1	1	69	-0.25	12/10/2019 09:37:22

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

Filtered vs. Highlighted Events

- Filtered events are no longer displayed, though summary statistics continue to calculate
- Highlighted events are marked yellow in the **Per-panel Filter** column and are displayed at the top of the list by default



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

Managing Per-panel Filtering Lookups

- Edit filters in the corresponding lookup table
- Access the lookup table by
 - clicking View/edit existing filters in the Per-panel Filter window
 - by selecting the lookup table under **Configure > Content > Content Management**

Content Management

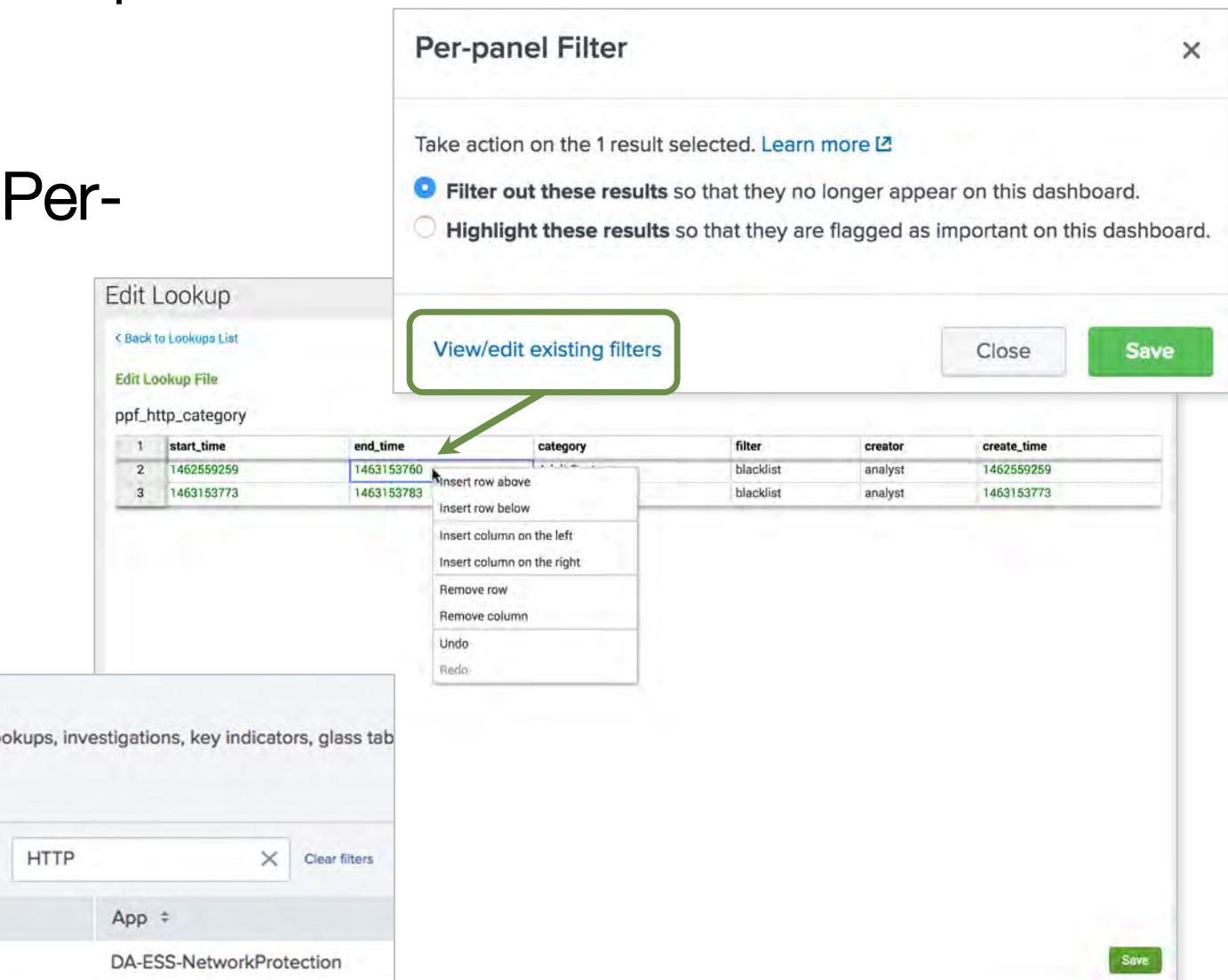
Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, glass tabs

[Back to ES Configuration](#)

3 Objects [Edit selection](#) Type: **Lookup** ▾ App: All ▾ Status: All ▾ HTTP [Clear filters](#)

Name	Type	App
HTTP Category Analysis Filter	Lookup (ppf)	DA-ESS-NetworkProtection
HTTP User Agent Analysis	Lookup (ppf)	DA-ESS-NetworkProtection
Local HTTP Intake	Lookup (other)	DA-ESS-The latest logon

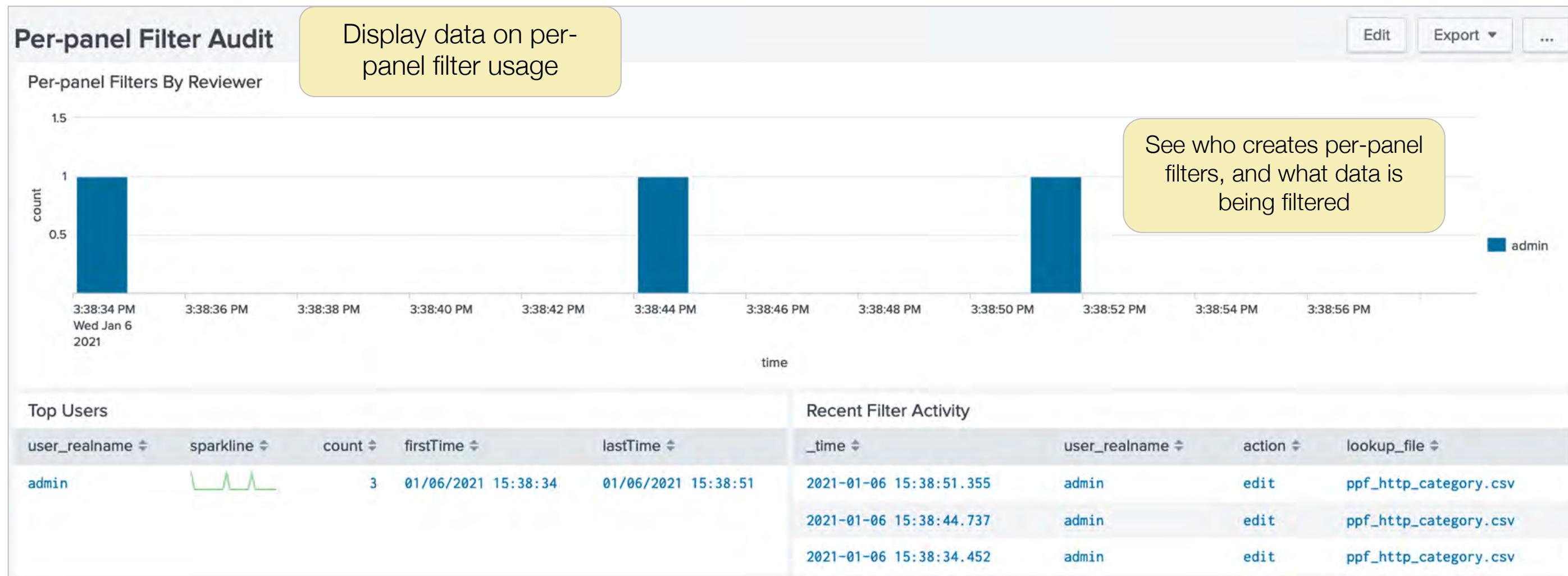
[Save](#)



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

Per-panel Filter Audit

Audit > Per-panel Filter Audit



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: ES On-Prem Deployment

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

Objectives

- Identify on-prem deployment topologies
- Examine the deployment checklist
- Understand pre-deployment requirements

Deployment Checklist

1. Determine size and scope of installation
2. Configure additional servers if needed
3. Obtain the ES software
4. Determine software installation requirements for search heads, indexers, and forwarders
5. Install all ES apps on search head(s)
6. Deploy indexer configurations

ES Impact on Resources

- ES generally requires a new, dedicated search head or search head cluster
 - ES is only compatible with other CIM-compatible apps
 - ES adds a large number of searches and search results
- Hardware must meet or exceed Splunk minimum requirements:
docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware
- ES increases some hardware requirements:
docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning#Splunk_Enterprise_system_requirements

Supported Architectures

- Single server (proof of concept, testing, dev)
- Distributed search (single search head, multiple indexers)
- Search head clustering

docs.splunk.com/Documentation/ES/latest/Install/InstallEnterpriseSecuritySHC

- Indexer clustering (including multi-site)

docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning

Adding ES to an Existing Site

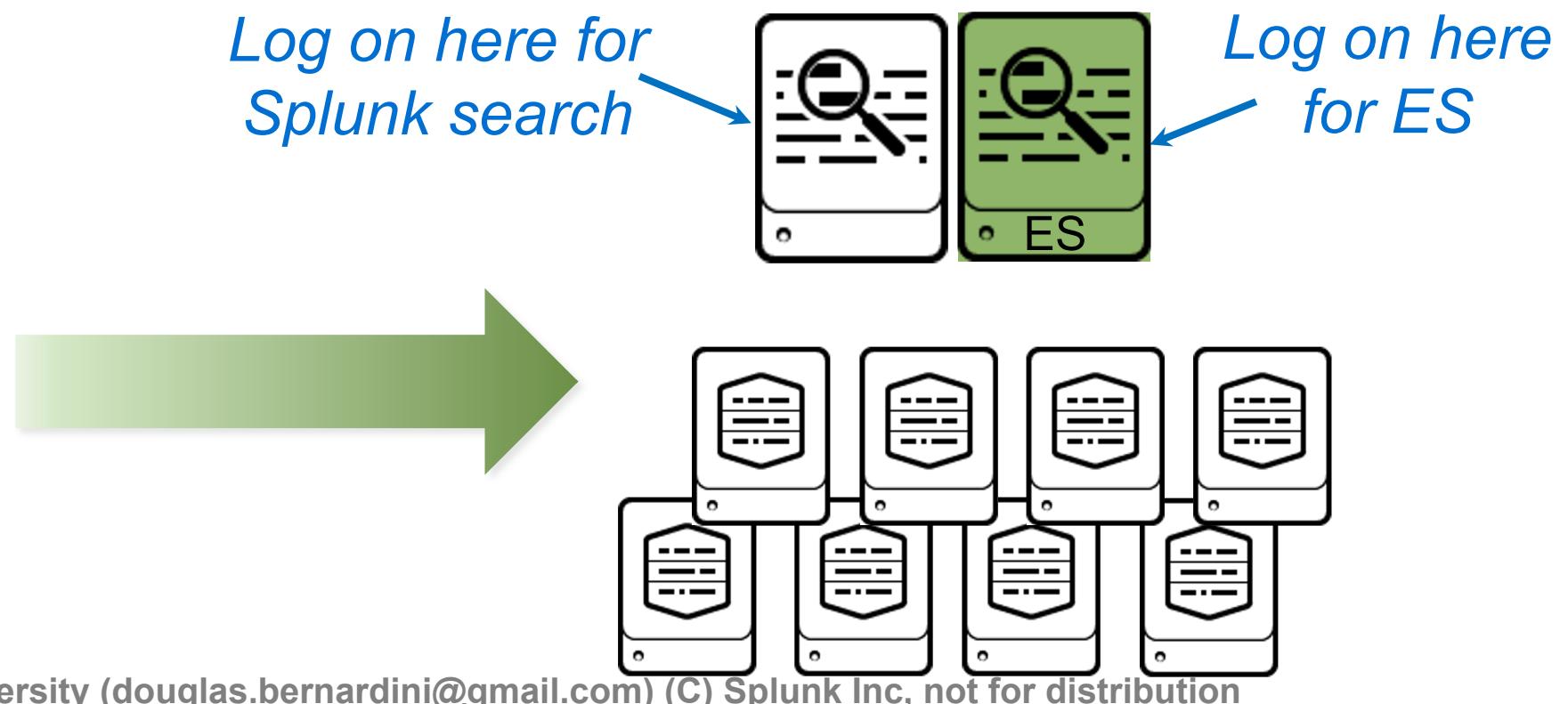
Before ES

Pre-ES site with a single search head
and 3 indexers supporting
~500GB/day of indexed data



After ES

After ES install, ES increases
search requirements, adds an extra
search head and an additional 5 indexers



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

Search Head Requirements

- A dedicated server or cluster for the ES search head(s) with only CIM-compliant apps installed
- 64-bit OS, minimum 32 GB RAM of memory and 16 processor cores
 - Additional memory and CPU capacity may be needed depending on number of concurrent users, searches, etc.
- Configure search head forwarding:
docs.splunk.com/Documentation/Splunk/latest/DistSearch/Forwardsearchheaddata
- If enabling **Monitoring Console**, do not use distributed mode
docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning#Monitoring_Console

Indexer Requirements

- Increased search load in ES typically requires more indexers
 - Assume at most 100GB/day per indexer. For deployment planning use 80GB/day to be on the safe side
 - Hardware minimum: 16 CPU cores, 32 GB RAM of memory
 - The exact number of indexers required depends on:
 - Types and amounts of data being used by ES
 - Number of active correlation searches
 - Number of real-time correlation searches
- <https://docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning>

Indexer Cluster Requirements

- You can only enable ES on one search head or search head cluster for each indexer cluster
- On a multisite indexer cluster:
 - Enable summary replication to improve performance
docs.splunk.com/Documentation/Splunk/latest/Indexer/Clustersandsummaryreplication
 - Disable search affinity
docs.splunk.com/Documentation/Splunk/latest/Indexer/Multisitesearchaffinity
- Deploy ES add-ons to the indexer cluster using the Splunk_TA_ForIndexers app from cluster master

Accelerated Data Model Storage

- In addition to index storage requirements, ES requires space for accelerated data models
- Acceleration requires approximately $3.4 \times$ (daily input volume) of additional space per year, or more if replicated in an indexer cluster
- Example: input volume of 500 GB per day with one year retention
 - $500 \text{ GB} * 3.4 = 1700 \text{ GB}$ additional space for accelerated data model storage
- Space is added across all indexers
 - Example: if there are 5 indexers, $1700 \text{ GB} / 5 = \sim 340\text{GB}$ per indexer additional space is required

More About Accelerated Data Models

- Most ES searches are executed on accelerated data models
- The storage volumes allocated for acceleration should be tuned for best performance and replicated if in a cluster
- By default, acceleration storage is allocated in the same location as the index containing the raw events being accelerated
- Use the `tstatsHomePath` setting in `indexes.conf` if needed to specify alternate locations for your accelerated storage

docs.splunk.com/Documentation/ES/latest/Install/Datamodels#Configuring_storage_volumes

Indexed Real Time Search

- ES automatically configures Splunk to use indexed real time searching
docs.splunk.com/Documentation/Splunk/latest/Search/Aboutrealtimesearches#Indexed_real-time_search
- Improves concurrent real time search performance at the cost of a small delay in delivering real time results from searches
- Leave turned on in ES for best performance

Forwarder Requirements

- In general, forwarders are unaffected by ES installation
- However, some add-ons that ES depends on must be deployed to forwarders to collect data
- Examples:
 - Windows add-on
 - *NIX add-on
 - Splunk Stream add-on

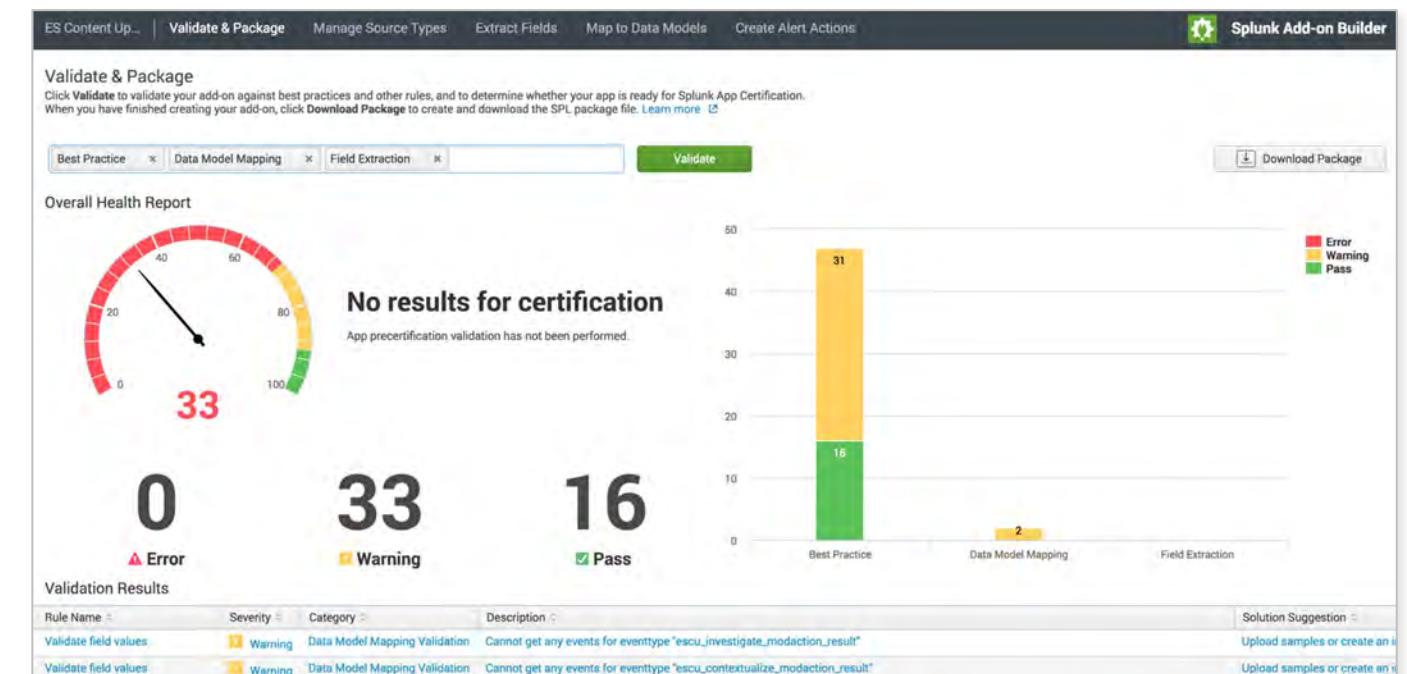
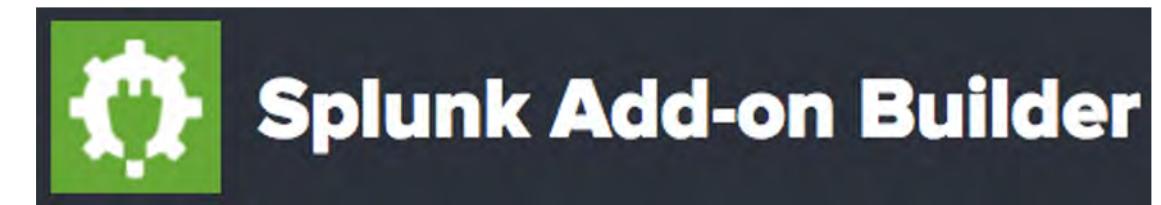
App/Add-on Deployment Options

- Depending on your requirements, you may need to distribute add-ons to other Splunk instances like search heads, indexers, and heavy forwarders
- Use the appropriate app and add-on deployment methodology:
 - Forwarders and non-clustered Indexers: use Forwarder Management (Deployment Server)
 - Indexer clusters: use the master node to deploy apps to peer nodes
 - Search head clusters: use the deployer to deploy apps to cluster members

docs.splunk.com/Documentation/ES/latest/Install/InstallTechnologyAdd-ons

Add-on Builder

- splunkbase.splunk.com/app/2962/
- Builds add-ons for custom ES data
- Normalizes custom data into the Common Information Model
- Built-in validation
- Should not be used on production servers



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

Important Resources

- Splunk Education courses
 - *Splunk Data Administration*
 - *Splunk System Administration*
 - *Splunk Cluster Administration*
 - *Architecting and Deploying Splunk*
- Distributed Splunk overview:
docs.splunk.com/Documentation/Splunk/latest/Deploy/Distributedoverview
- Capacity planning:
docs.splunk.com/Documentation/Splunk/latest/Capacity/Accommodatemany simultaneoussearches

Appendix C: Use Case Library

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

Use Case Library

Configure > All Configurations > Content > Use Case Library

- The Use Case Library contains analytic stories which are ready-to-use examples of how to use ES to quickly identify the scope of attacks, determine mitigation options, and take remedial action
- Analytic stories:
 - Contain the searches needed to implement the story in your own ES environment
 - Provide an explanation of what the searches achieve and how to convert a search into adaptive response actions, where appropriate
- Uses the Enterprise Security Content Update app

Enterprise Security Content Update

- Splunk Enterprise Security Content Update (ESCU) add-on delivers analytic stories to customers as part of a content subscription service and is updated often with new stories
- The app can be downloaded from Splunkbase
- Check ESCU app version: App > Manage Apps > ES Content Updates

A screenshot of the Splunk Apps interface. The top navigation bar includes "splunk>enterprise", "Apps", "admin", "Messages", "Settings", "Activity", "Help", and a search bar. Below the navigation is a toolbar with "Browse more apps", "Install app from file", and "Create app". The main area is titled "Apps" and shows "Showing 1-66 of 66 items". A search bar and a "filter" button are at the top left. On the right, there are buttons for "100 per page" and a dropdown menu. A table lists three apps: "DA-ESS-AccessProtection", "ES Content Updates", and "DA-ESS-EndpointProtection". The "ES Content Updates" row is highlighted with a green border. The table columns are: Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. The "Actions" column for each row contains links like "Edit properties" and "View objects".

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
DA-ESS-AccessProtection	DA-ESS-AccessProtection	6.2.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
ES Content Updates	DA-ESS-ContentUpdate	1.0.54	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects ↗
DA-ESS-EndpointProtection	DA-ESS-EndpointProtection	6.2.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects

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

Use Case Library Permissions

- All ES users can *view* the analytic stories in the Use Case Library
- By default, `ess_admin` and `ess_analyst` roles have the ability to edit the stories
- An admin can assign the `ess_user` role the **Edit Analytic Story** permission

Enterprise Security > Configure > General > Permissions

Permissions

Assign permissions to edit ES components based on user roles. Administrative roles implicitly have all permissions and cannot be modified. Changes on permissions could take a few minutes to take effect.

[◀ Back to ES Configuration](#)

ES Component	ess_analyst	ess_user
Edit Analytic Story Permits the role to edit analytic stories.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Use Case Library (cont.)

Configure > All Configurations > Content > Use Case Library

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

- Abuse**

- Adversary Tactics**

- Best Practices**


57 Analytic Stories found in categories: Cloud Security, Best Practices, Vulnerability, Abuse, Adversary Tactics, Malware

In use	Analytic Story	Use Case	Description	App	Last Updated	Bookmark
>	0 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"/>
>	0 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"/>
>	0 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 type="checkbox"/>
>	0 AWS Suspicious Provisioning Activities	Cloud Security	Monitor your AWS provisioning activities for behaviors originating from unfamiliar or unusual locations. These behaviors may indicate that malicious activities are occurring somewhere within your network.	ES Content Updates	Mar 19, 2018	<input type="checkbox"/>
>	0 AWS User Monitoring	Cloud Security	Detect and investigate dormant user accounts for your AWS environment that have become active again. Because inactive and ad-hoc accounts are common attack targets, it's critical to enable governance within your environment.	ES Content Updates	May 17, 2018	<input checked="" type="checkbox"/>
>	0 Access Protection	Best Practices	Monitoring account activity and securing authentication are important parts of securing an environment. This analytic story includes searches to detect suspicious account activity and alert you to the use of protocols that authenticate in cleartext (non-encrypted).	DA-ESS-AccessProtection	Sep 13, 2018	<input type="checkbox"/>
>	0 Account Monitoring and...	Best Practices	A common attack technique is to leverage user accounts to gain unauthorized access to the target's network. This Analytic Story minimizes opportunities for attack by helping you actively manage creation/use/dormancy/deletion—the lifecycle of system and application accounts.	ES Content Updates	Jan 5, 2018	<input type="checkbox"/>
>	0 Vulnerability	Vulnerability	Detect and investigate activities—such as unusually long ‘Content-Type’ length or web servers executing suspicious processes—consistent with attempts to exploit Apache Struts vulnerabilities.	ES Content Updates	Nov 1, 2017	<input type="checkbox"/>
>	0 Asset Tracking	Best Practices	Keep a careful inventory of every asset on your network to make it easier to detect rogue devices. Unauthorized/unmanaged devices could be an indication of malicious behavior that should be investigated further.	ES Content Updates	Nov 1, 2017	<input type="checkbox"/>

Choose a topic to focus on related use cases

Bookmark stories specific to your duties

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

Use Case Specifics

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

- Abuse
- Adversary Tactics
- Best Practices

Expand an Analytic Story

6 Analytic Stories found in category: Abuse

In use	Analytic Story	Use Case	Description
0	Brand Monitoring	Abuse	Detect and investigate activity that may indicate that an adversary is using malicious infrastructure. Monitor DNS, email, and web traffic for permanent changes in behavior.

Detection Searches

- ESCU - Monitor DNS For Brand Abuse - Rule
- ESCU - Monitor Email For Brand Abuse - Rule
- ESCU - Monitor Web Traffic For Brand Abuse - Rule

Detection Searches are correlation searches that populate the story results

Recommended Data Sources

- Splunk Stream
- Bro
- Microsoft Exchange
- Bluecoat
- Palo Alto Firewall

Sourcetypes use by the detection searches for this analytic story

Data Models

- Network_Resolution
- Email
- Web

Lookups

- brandMonitoring_lookup

Recommended Data Sources that are likely to provide valuable data

Data Models used by the detection searches for this analytic story

Lookups used by the detection searches for this analytic story

See all 15 Data Sources

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

Analytic Story Details

Select a story from the library to view the details

Analytic Story Details: Brand Monitoring

Use Case: Abuse

< Back to Use Case Library

Description

Detect and investigate activity that may indicate DNS, email, and web traffic for permutations of your brand.

Narrative

While you can educate your users and customers about the persistent fact of life. Of course, your adversary will always be looking for ways to possibly phishing with lookalike addresses that closely mimic your corporate servers. This Analytic Story, to generate permutations of your brand, to provide you with early warning of potential threats based on DNS, URLs, and user data. Drilling down on these searches to help you scope the problem, and quickly respond to it.

Correlation Searches

ESCU - Monitor DNS For Brand Abuse - Rule

Description

This search looks for DNS requests for faux domains similar to the domains that you want to have monitored for abuse.

Explanation

This search gathers all the answers to each system's DNS query, then filters out all queries that do not appear on the list of faux "look-a-like" domains that have been generated from the brand abuse domains you are monitoring.

Search

```
| tstats 'summariesonly' values(DNS.answer) as IPs min(_time) as firstTime from datamodel=Network_Resolution by DNS.src, DNS.query | 'drop_dm_object_name("DNS")' | 'ctime(firstTime)' | 'brand_abuse_dns'
```

How to Implement

You need to ingest data from your DNS logs. Specifically you must ingest the domain that is being queried and the IP of the host originating the request. Ideally, you should also be ingesting the answer to the query and the query type. This approach allows you to also create your own localized passive DNS capability which can aid you in future investigations. You also need to have run the search "ESCU - DNSTwist Domain Names", which creates the permutations of the domain that will be checked for.

Known False Positives

None at this time

Cyber Security Framework Attributes

KILL CHAIN PHASES Delivery Actions on Objectives

Data Sources (technology add-ons)

Splunk Stream
Bro

Details on how to implement the story

Edit Correlation Search

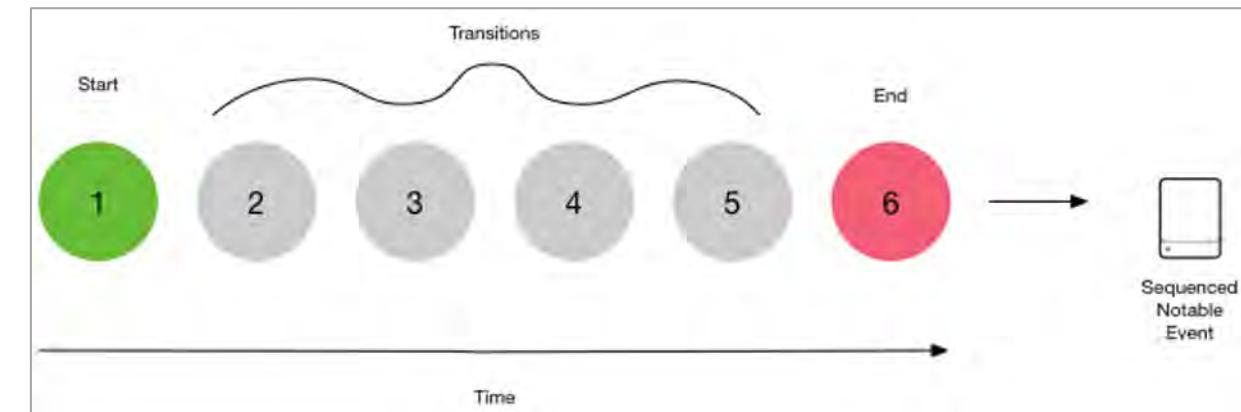
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Appendix D: Event Sequencing Engine

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

Event Sequencing Engine

- The Event Sequencing Engine groups correlation searches into batches of events, in a specific sequence, by specific attributes, or both
- Event sequencing is configured in Sequence Templates
- Sequence Templates:
 - Define which Start, Transition, and End correlation searches need to occur, and the match conditions
 - Define if the transitional searches must occur in a given order, or if they can occur in *any* order
- Templates run as a real-time searches and listen for incoming notable events and risk modifiers that are triggered by the correlation searches



Scenario

Create a template to detect high priority hosts with multiple malware infections, excluding test host ACME-004. Then, detect if the host has an abnormally high number of HTTP method events, excluding any “unknown” methods

1 Give the template a name and description, and select the ES app.

2 Set the starting correlation search to Endpoint – High Or Critical Priority Host With Malware. Set the expression to detect all destinations (dest) except ACME-004.

Sequence Template

Name: Hosts with malware infections & high http_method events

Description: Detects if high priority hosts have malware infections (except test host ACME-004), and detects if those hosts have a high number of http_method events

App: Enterprise Security

Start

Correlation Search: Endpoint - High Or Critical Priority Host With Malware - Rule

Expression: 'dest' != "ACME-004"

State: + Add State

<https://docs.splunk.com/Documentation/ES/latest/Admin/Sequencecorrelationsearches>
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Scenario (cont.)

The screenshot shows the configuration of a security scenario template. It includes sections for **Transitions**, **End**, and **Actions**.

Transitions:

- Enforce Ordering:** A checkbox labeled "Enforces chronological order of transitions, otherwise just checks for existence. Saving state on transitions is disabled when ordering is disabled." Step 3 highlights this section.
- Aggregate Matches:** A checkbox labeled "Keep accumulating matched events that may occur multiple times while template is running. Accumulated events will be added to the final sequenced event."

Multiple Infections: A sub-section under Transitions with the following fields:

- Title:** Multiple Infections
- Correlation Search:** Endpoint - Host With Multiple Infections - Rule
- Expression:** 'dest' != "ACME-004"

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

Note: In this template, the Enforce Ordering box has been unchecked. Therefore, the transitional searches do not have to happen in order, they just have to exist for the template to trigger.

End:

- Correlation Search:** Web - Abnormally High Number of HTTP Method Events By Src - Rule
- Expression:** 'http_method' != "unknown"

Field value should be enclosed in single quotes, and the matching value enclosed in double quotes. Ex: 'host' = "127.0.0.1"
- Time Limit:** 60 day(s)

Actions:

- Sequenced Event:**
 - Event Title:** High Priority hosts with malware infections

Supports state token substitution.
 - Event Description:** High priority host has multiple malware infections (except test host ACME-004), and a

Supports state token substitution.
 - Urgency:** Critical
 - Security Domain:** Endpoint
 - Output Fields:** + Add Field

Step 3: Add the transitional correlation search Endpoint – Host With Multiple Infections with the expression to detect all destinations (dest) except ACME-004.

Step 4: Set the ending correlation search to Web – Abnormally High Number of HTTP Method Events By Src, and the expression to detect all methods except unknown. Also, set the time limit for the template to run to 60 days.

Step 5: Add a title, urgency, and security domain for the notable events that are created when the template is triggered.

Results

The screenshot shows the 'Incident Review' dashboard. At the top, there are several filter fields: 'Saved filters', 'Tag', 'Urgency', 'Status', 'Owner', and 'Security Domain'. Below these are dropdowns for 'Type' (with 'Sequenced Event' selected), 'Time or Associations', and time range controls ('Time' and 'Last 24 hours'). There are also buttons for 'Search...', 'Show Charts', 'Hide Filters', 'Submit', 'Save new filters', 'Uptime', and 'Clear all'. At the bottom, it shows 'Source: Sequenced Event' and 'Time Range: Last 24 hours'.

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

This screenshot shows a detailed view of a sequenced event. At the top, it displays the timestamp (12/13/18 7:51:09.000 PM), endpoint (High Priority hosts with malware infections), priority (Critical), status (New), and owner (unassigned). The main content area includes:

- Sequenced Event Description:** High priority host has multiple malware infections (except test host ACME-004), and a high number of http_method events.
- Template Title:** Hosts with malware infections & high http_method events
- Template Description:** Detects if high priority hosts have malware infections (except test host ACME-004), and detects if those hosts have a high number of http_method events. A link to 'View events' is provided.
- Transitions:** A table showing correlation searches matched in the template:

Stage	Time	Match
start	Dec 13, 2018 7:45 PM	High Or Critical Priority Host With Malware Detected View original events
Multiple Infections	Dec 13, 2018 7:50 PM	Host With Multiple Infections (BUSDEV-004) View original events
end	Dec 13, 2018 7:50 PM	Abnormally High Number of HTTP CONNECT Request Events By 192.168.3.153 View original events
- Additional Fields:** End Time (Dec 13, 2018 12:57 PM) and Start Time (Dec 13, 2018 12:45 PM).
- Event Details:** event_id (70C7FFBE-40BB-43BF-B9DB-1EE21986AC11@sequenced_events@53d2179996acc905bf15dda5ea33af21), event_hash (53d2179996acc905bf15dda5ea33af21), eventtype (sequenced_event), and source (sequenced_event).

A yellow callout box on the right states: "Transitions display the correlation searches matched in the template."

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

Appendix E: Using ES Overview

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

The Security Posture Dashboard

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

Security Posture

Key Indicators

Edit

ACCESS NOTABLES	ENDPOINT NOTABLES	NETWORK NOTABLES	IDENTITY NOTABLES	AUDIT NOTABLES	THREAT NOTABLES
Total Count 26 +6	Total Count 192 +89	Total Count 314 +109	Total Count 906 +258	Total Count 481 +124	Total Count 404 +247

Key Indicators (KI) provide an at-a-glance view of notable event status over the last 24 hours

Notable Events By Urgency

Notable Events Over Time

Top Notable Events

rule_name	sparkline	count
Activity from Expired User Identity		906
Personally Identifiable Information Detected		10.12.34.56
Risk Threshold Exceeded For Object Over 24 Hour Period		1
Abnormally High Number of HTTP Method Events By Src		1

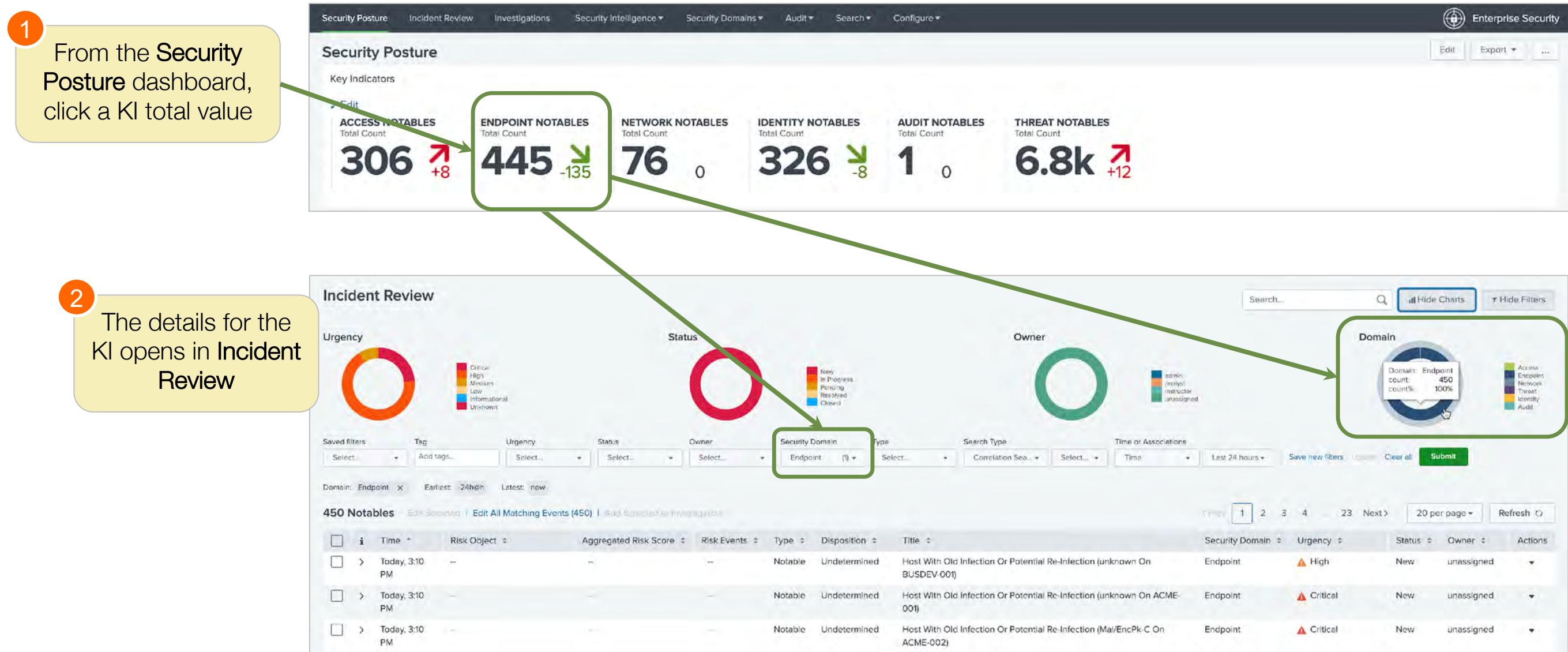
The panels provide additional summary information categorized by urgency, time, and most common notable event types and sources

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
10.12.34.56		1	1	97
1		1	1	97
1		1	1	97
2		2	2	29

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

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 Tag, Urgency, Status, Owner, Security Domain, Type, Search Type, and Time or Associations. The results show 761 Notables, with the first two listed being:

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

Incident Review

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

Search... Hide Charts Hide Filters

Urgency

Status

Owner

Domain

Hide the donut charts or filters

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

Select... Add tags... 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

Notable Events

Actions menu

Expand for details

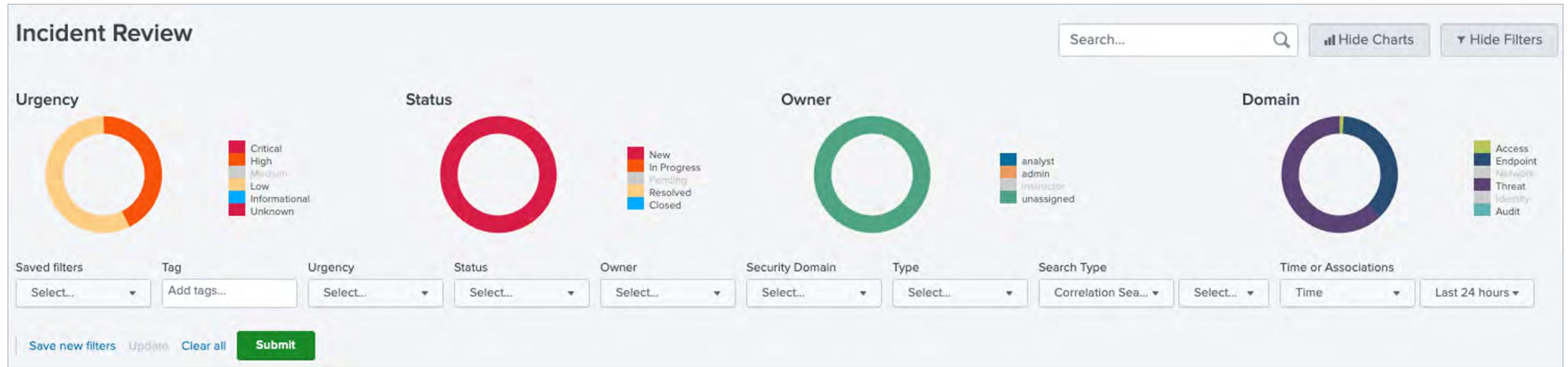
No investigation is currently loaded. Please create (+) or load an existing one (≡).

Investigation bar

#	Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
1	Activity from Expired User Identity (dmsys)	-	--	-	Notable	Today, 5:05 PM	Undetermined	Identity	High	New	unassigned	⋮
2	Host With Old Infection Or Potential Re-Infection (Mal/Packer On ops-sys-003)	-	--	-	Notable	Today, 5:00 PM	Undetermined	Identity	High	New	unassigned	⋮
3	24 hour risk threshold exceeded for user=root	root	600	2	Risk Notable	Today, 5:00 PM	Undetermined	Endpoint	High	New	unassigned	⋮

Generated for Splunk University (douglas.sherman@gmail.com), © 2022 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. At the top, there's a header with various filters and a main table row for an event titled "Excessive Failed Logins". The table includes columns for Title, Risk Object, Aggregated Risk Score, Risk Events, Type, Time, Disposition, Security Domain, Urgency, Status, Owner, and Actions.

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 (Listed on the left): Application, Source, Source Business Unit, Source Category, Source City, Source Country, Source Latitude, Source Longitude, Source PCI Domain, Source Should Time Synchronize, Source Should Update.

Event Details: (Listed on the left): event_id: 406BED13-4DD4-4AB3-B4A3-4349824AAFE0, event_hash: 003c6c529e9cf426d4325689e25fe140, eventtype: modnotable_results, nix-all-logs, notable, Short ID: Create Short ID.

Fields for the notable event, with Action menus for each field (Callout pointing to the event details table).

Action (Callout pointing to the "Action" button in the "Value" column of the event details table).

Field Action menus (Callout pointing to the dropdown arrow next to the "Action" button in the event details table).

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: (Listed on the right):

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: (Listed on the right): No next steps defined.

Note (Callout pointing to the note message): You cannot expand an event until the search is complete. Not all incidents have all the same detail items.

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

The screenshot shows two views of the Splunk interface for creating a Short ID.

Top View: The "Event Details" section displays various event properties. A green box highlights the "Create Short ID" button. A callout bubble with number 1 points to this button, explaining: "Click Create Short ID for ES to automatically generate a short ID that makes it easier to find and share a notable event".

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

Bottom View: The "Event Details" section shows the same event properties. The "Create Short ID" button has been replaced by a generated "Short ID" field containing "VM4NAE". A callout bubble with number 2 points to this field, explaining: "The Short ID replaces the Create Short ID link".

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

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

Create a Short ID: Notable Event Actions

A screenshot of the Splunk interface showing a list of notable events. The 'Actions' column contains a dropdown menu for each event. The 'Share Notable Event' option is highlighted with a green box and circled with a green arrow, indicating step 1.

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	12/16/19 3:40:54.000 PM	Identity	Activity from Expired User Identity (dmsys)	High	New	unassigned	<ul style="list-style-type: none">Add Event to InvestigationBuild Event TypeExtract FieldsRun Adaptive Response ActionsShare Notable EventSuppress Notable EventsShow Source
>	12/16/19 3:40:09.000 PM	Network	Unroutable Activity Detected (0.195.11.148)	Medium			
>	12/16/19 3:35:53.000 PM	Identity	Activity from Expired User Identity (dmsys)	High			
>	12/16/19 3:35:06.000 PM	Endpoint	Host With Multiple Infections (89.11.192.18)	Medium			
>	12/16/19 3:30:52.000 PM	Identity	Activity from Expired User Identity (dmsys)	High			
>	12/16/19 3:25:51.000 PM	Identity	Activity from Expired User Identity (dmsys)	High			
>	12/16/19 3:20:50.000 PM	Identity	Activity from Expired User Identity (dmsys)	High			
>	12/16/19 3:15:49.000 PM	Identity	Activity from Expired User Identity (dmsys)	High			

1 From the notable event **Actions** dropdown, creating a Short ID is possible using **Share Notable Event**

A screenshot of the 'Share Event' dialog box. It shows a 'Short ID : 9UBI48' button highlighted with a green box and circled with a green arrow, indicating step 2. Below it is a 'Link To Event : http://35.162.153.23/en-US/app...' field with a 'Bookmark' button next to it, also highlighted with a green box and circled with a green arrow. A note below says 'Click the right icon to copy the link, or drag the icon into your bookmarks bar to bookmark the link.' At the bottom is a 'Close' button highlighted with a green box and circled with a green arrow, indicating step 3.

2 In addition to creating a Short ID, this 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

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 the following steps highlighted:

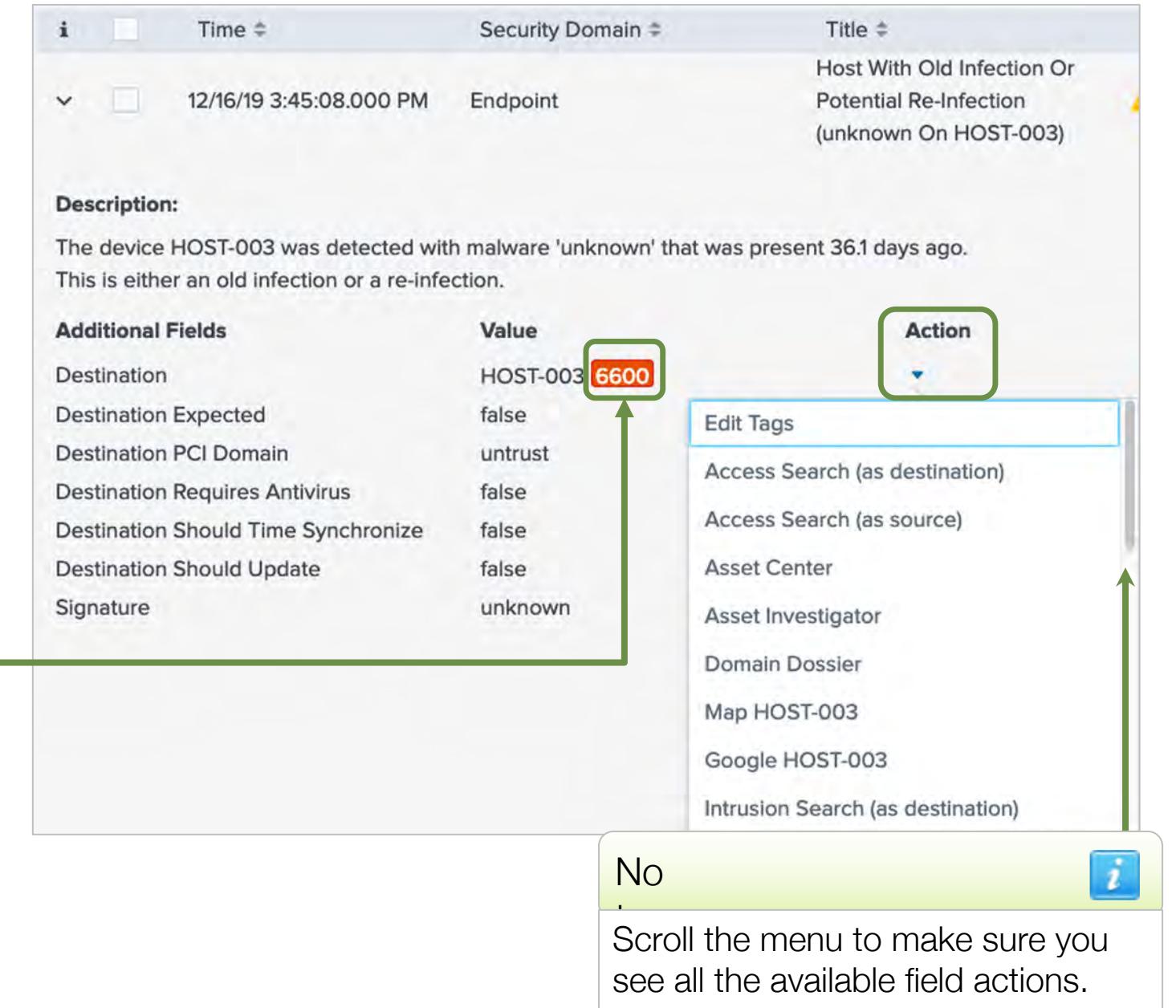
- Step 1:** Select Associations from the Time or Associations menu, and Short ID from the Associations menu.
- Step 2:** Click inside the filter field and enter all or part of a Short ID (drop-down appears and filters as you type) Or Click and scroll to the Short ID.
- Step 3:** Click Submit.

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

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

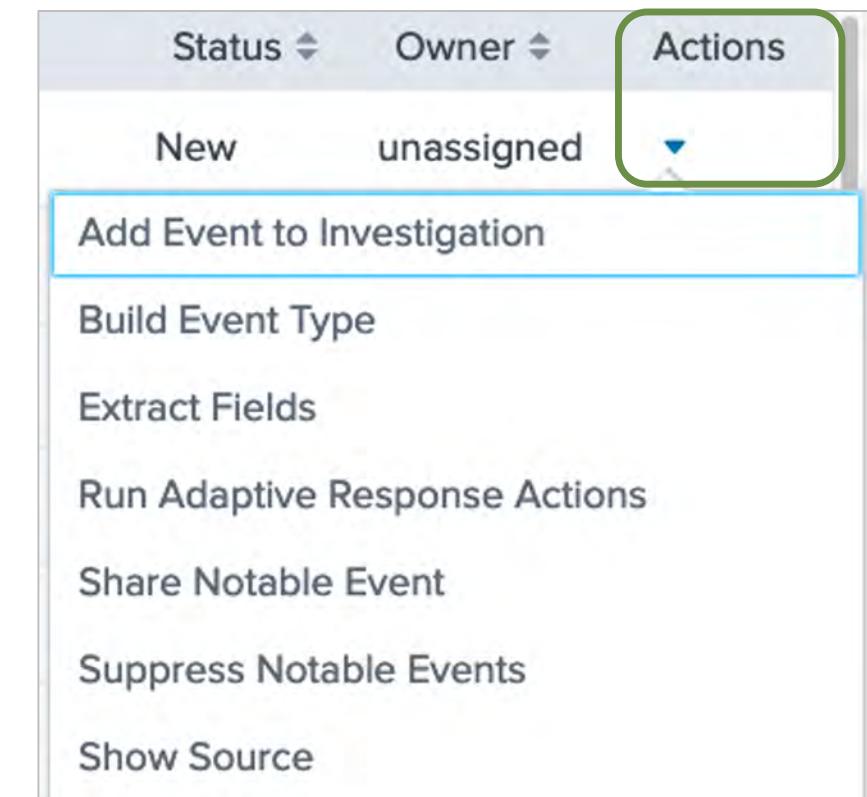
Field Action Menu

- 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 hosts or users are displayed next to fields
 - Click a risk score to open the Risk Analysis dashboard for that asset or identity



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: Procedures

The screenshot shows the Splunk Enterprise Security interface with two main panels. The left panel displays a list of 'Notables' (events) with checkboxes. Step 1: 'Select one or more events' is indicated by a callout over the checkboxes. Step 2: 'Click Edit Selected' is indicated by a callout over the 'Edit Selected' button. The right panel shows the 'Edit Events' dialog for selected incidents. Step 3: 'Set Status, Urgency, Owner, and Disposition. Optionally, add a Comment' is indicated by a callout over the form fields. Step 4: 'Click Save changes' is indicated by a callout over the 'Save changes' button. A large yellow box at the bottom left provides general investigation tips.

1201 Notables

Edit Selected

Edit All Matching Events (1201)

Add Selected to Investigation

Risk Object

As needed, add selected event(s) to an investigation. It will appear under **Related Investigations** in the event details

1 Select one or more events

2 Click Edit Selected

Investigation Bar

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

Close

Cancel

Save changes

61 Next > 20 per page ▾ Refresh

Edit Events

4 event(s) selected. You are editing selected events.

Status: In Progress

Urgency: High

Owner: analyst

Disposition: True Positive - Suspicious Activity

Comment: Adding a comment is optional.

3 Set Status, Urgency, Owner, and Disposition. Optionally, add a Comment

4 Click Save changes

As needed, click the + icon on the **Investigation Bar** to view an investigation, add a new one, or click the spy glass to perform a quick search

Incident Review History

Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
Abnormally High Number of HTTP GET Request Events By 129.188.147.104	-	-	-	Notable	Today, 8:50 AM	True Positive - Suspicious Activity	Network	⚠️ High	In Progress	analyst	▼

Description:
A system (129.188.147.104) was detected as generating an abnormally high number of GET request events.

Additional Fields

	Value	Action	Correlation Search:
HTTP Method	GET	▼	Web - Abnormally High Number of HTTP Method Events By Src - Rule
Source	129.188.147.104	▼	

Related Investigations:
Currently not investigated.

History:

Date	User
2021 Aug 4 9:00:49 AM	admin

Adding a comment is optional.

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

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

```
|`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
```

Last 24 hours 

✓ 1 result (8/3/21 9:00:00.000 AM to 8/4/21 9:10:02.000 AM)

Events (0) Patterns Statistics (1) Visualization

100 Per Page ▾ Format Preview ▾

_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), and Owner (unassigned). The 'Actions' button is highlighted with a green border. A dropdown menu lists several options: Add Event to Investigation, Build Event Type, Extract Fields, Run Adaptive Response Actions (which is also highlighted with a green border), Share Notable Event, Suppress Notable Events, and Show Source.

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 ↗](#)

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/???

Adaptive Responses: Previously executed actions

Response	Mode	Time	User	Status
Risk Analysis	saved	2021-08-04T09:15:06-0600	admin	✓ success
Notable	saved	2021-08-04T09:15:05-0600	admin	✓ success

[View Adaptive Response Invocations ↗](#)

Next Steps:
The next step is to [Ping](#) the host to see if it is active on the network.

Next Steps: If configured in the correlation search, suggested actions to trigger next

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 and a dropdown menu for "Category" set to "All". A tooltip "Recommended action" points to the first item in the list. The list includes:

- 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
- Nslookup**: Runs the nslookup command. Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System

A yellow callout box on the right says: "Enter some, or all the action name to filter (list filters as you type)".

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 **3**

Host Field: Destination (dest)

Max Results: 4 **4**

Index: main

Worker Set: local

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

Run **5**

Adaptive Responses:					
Response	Mode	Time	User	Status	Action
Ping 6	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

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" is open, showing a list of actions to run. A button labeled "+ Add New Response Action" is highlighted with a red circle containing the number 1. Below it, another button labeled "Add Threat Intelligence" is also highlighted with a red circle containing the number 2. The main interface shows a "Select actions to run" section with a dropdown menu "+ Add New Response Action". Underneath, there is a section for "Add Threat Intelligence" which includes 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 "Run" button is at the bottom right. Callout boxes provide additional context: one for the "Add Threat Intelligence" button explaining it creates threat artifacts and relates to a threat group; another for the "Field from event" field explaining it's a field in the event containing information (i.e., dest); and a third for the "Threat Collection" field explaining it adds the threat artifact to a specific collection (i.e., ip_intel).

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, which is highlighted with a green border and numbered '2'. Another callout box points to the 'Severity' field, which is also highlighted with a green border and numbered '1'. The 'Send To UBA' action is described as 'Forwards search results from Splunk Enterprise to UBA'. Below it, details are provided: Category: Information Conveyance | Task: create | Subject: uba.anomaly | Vendor: Splunk.

Note

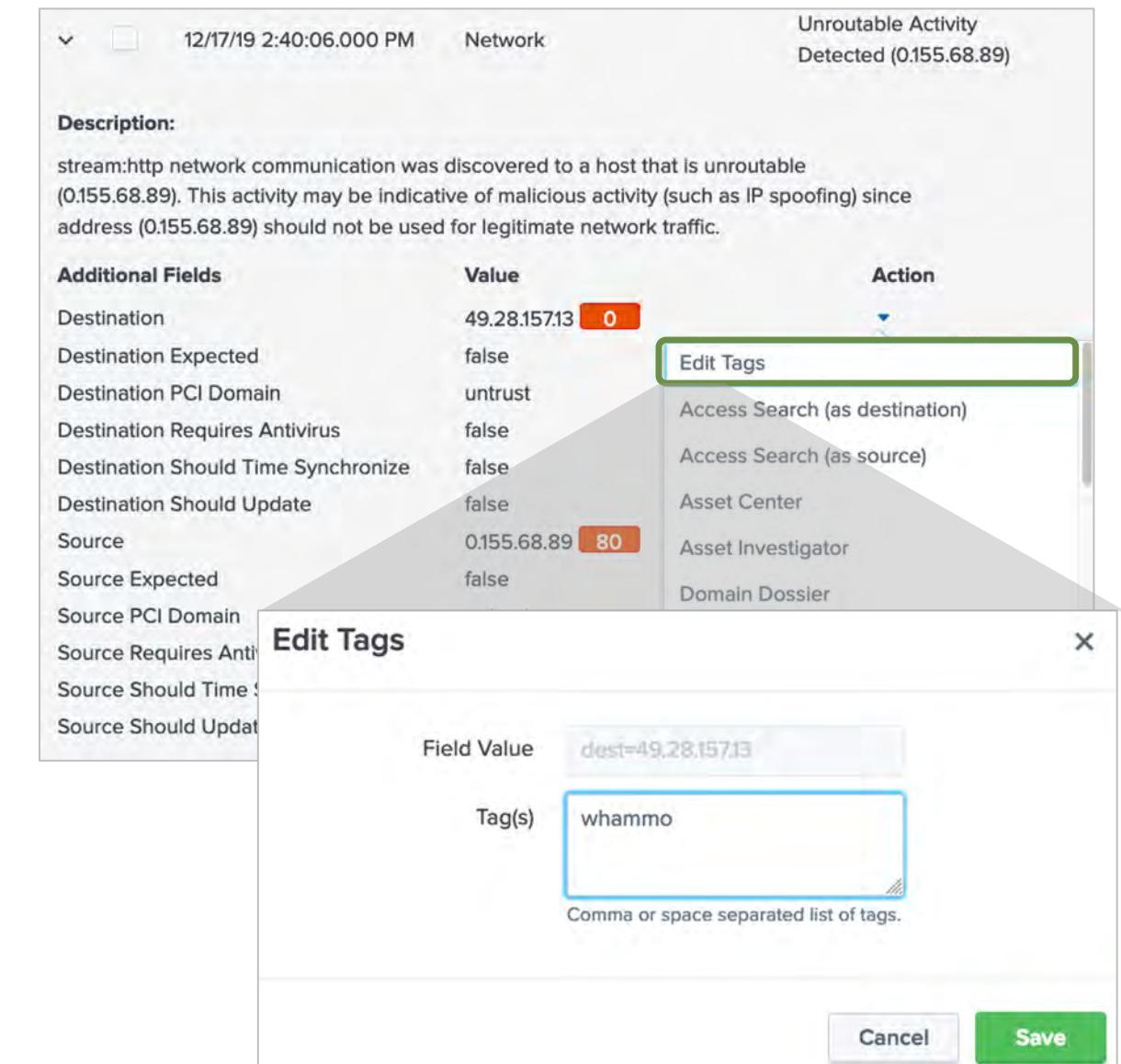
UBA must be installed on the ES search head for this Response Action to be available.

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 callout box highlights the 'Category in UBA' dropdown, which is set to 'Insider Threat'. A list of categories is shown, with 'Insider Threat' being checked. A 'Run' button is at the bottom right.

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

Tagging Incidents

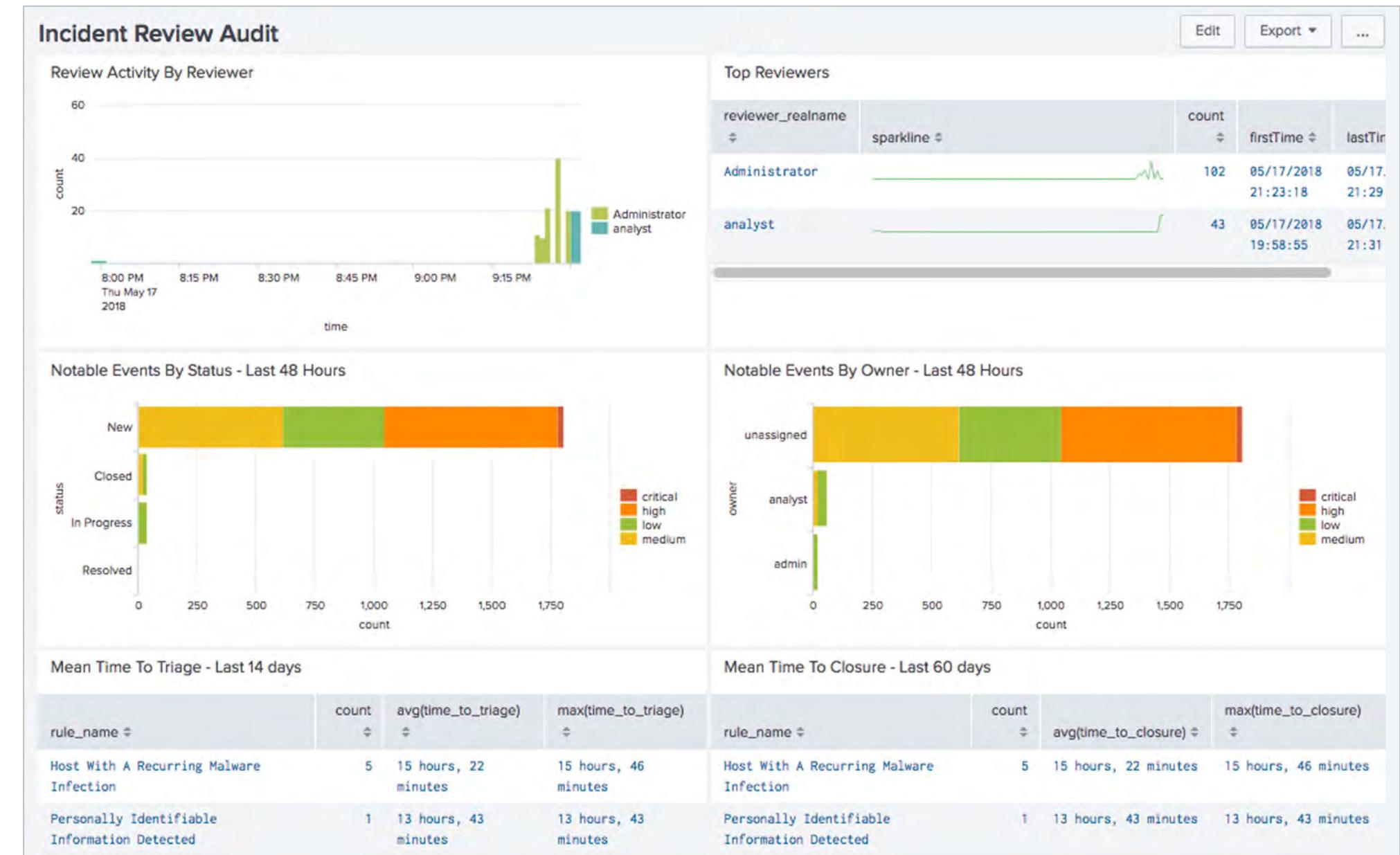
- Associate significant incidents with tags
 - Example: quickly find all incidents related to servers being used by project “whammo”
- Add a tag to each server using Action > **Edit Tags** for the dest, src or ip field (for this example)
- Search for tag name “whammo” in the Tag filter in Incident Review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



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

Audit > Incident Review Audit

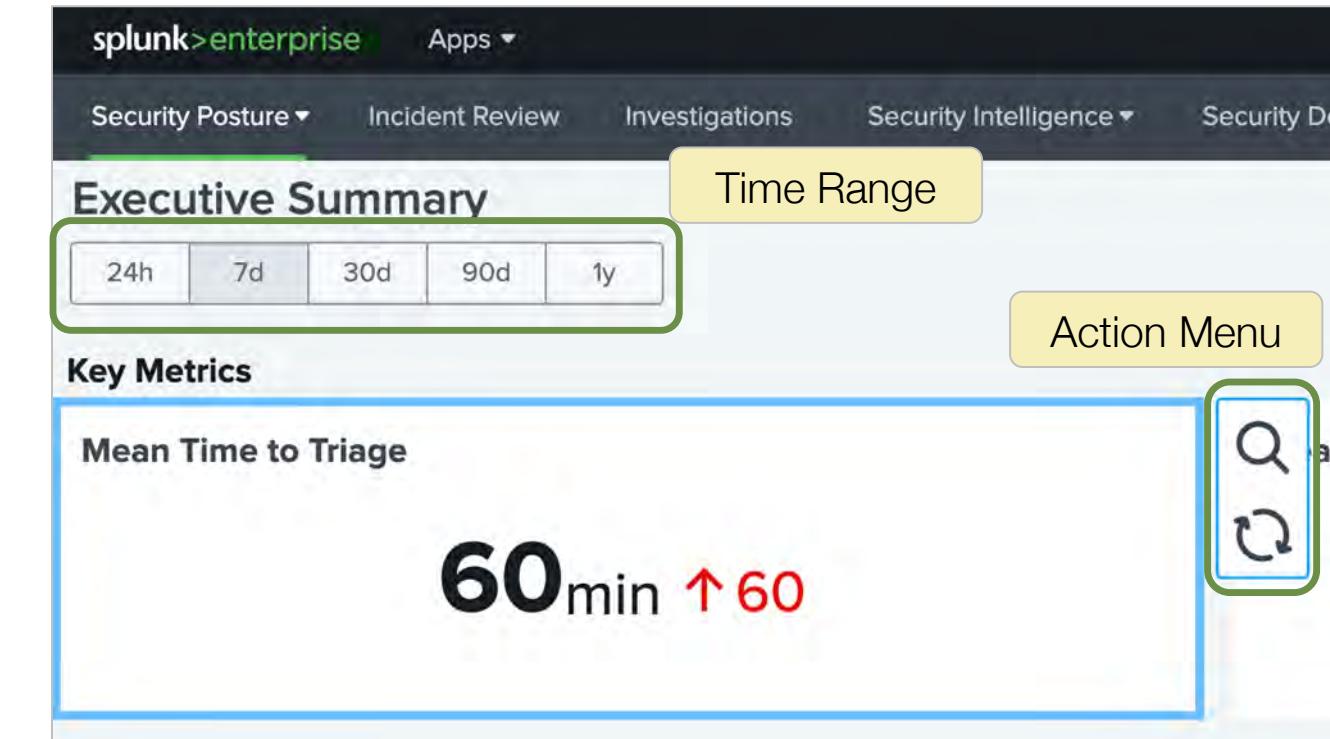
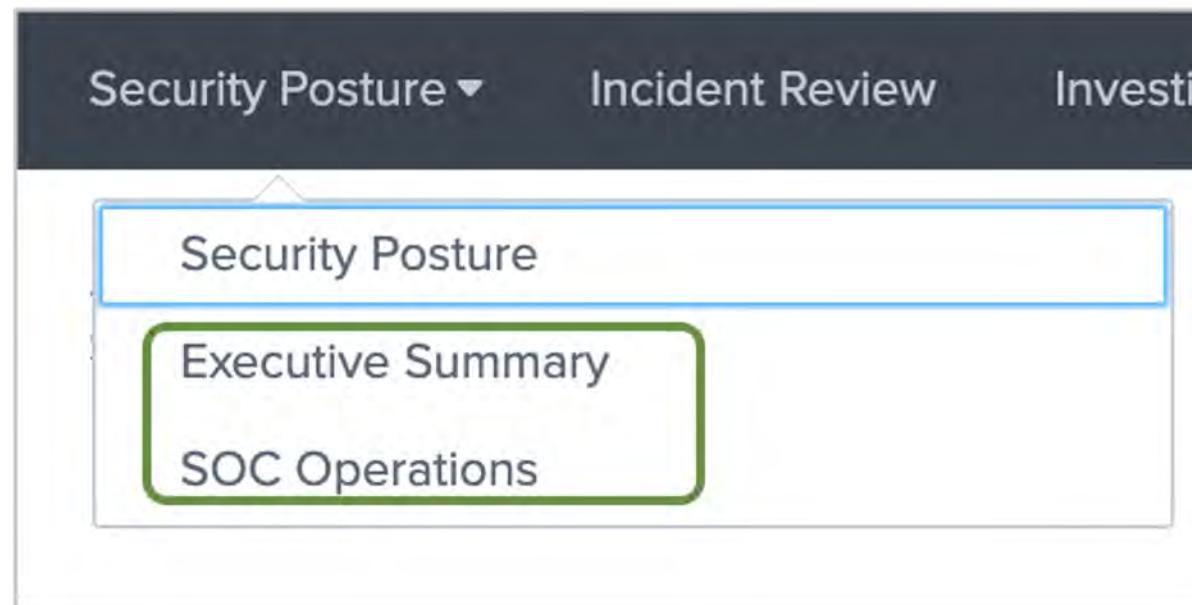
- Overview of analyst notable event handling
- Volume of incidents reviewed and by whom
- Incident aging over last 48 hours, by status and by reviewer
- Statistics on triage time and closure time



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

The Executive Summary Dashboards

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



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 tabs: Security Posture, Incident Review, Investigations, Security Intelligence, Security Domains, Cloud Security (which is highlighted with a yellow box), Audit, and Search. Below the navigation bar, there is a section titled "Splunk Enterprise Security" with a brief description. To the right of this section is a "Security Groups" dropdown menu containing options: IAM Activity, Network ACLs, Access Analyzer, and Microsoft 365. Further down the page, there are several cards representing different features: "Security Posture" (with a circular icon), "Incident Review" (with a flag icon), "App Configuration" (with a wrench icon), "Documentation" (with a question mark icon), "Community" (with a speech bubble icon), and "Product Tour" (with a green arrow icon). A callout box labeled "Important!" contains the text: "To onboard Cloud data sources and examine your Cloud Security environment, you must install and set up Splunk Add-on for Amazon Kinesis Firehose and Splunk Add-on for Microsoft Office 365 from Splunkbase." An information icon (a blue square with an 'i') is located in the top right corner of the callout box.

Important!

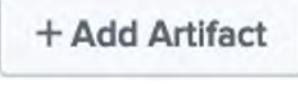
To onboard Cloud data sources and examine your Cloud Security environment, you must install and set up Splunk Add-on for Amazon Kinesis Firehose and Splunk Add-on for Microsoft Office 365 from Splunkbase.

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

Using ES Investigations

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

Investigation Artifacts

- 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)

Manually Add Artifacts

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 interface for investigating network traffic. On the left, the 'Artifacts' sidebar is open, showing a list of selected artifacts (22 out of 22) and a 'Risk Scores' section. A tooltip (1) points to a value in the risk scores table, with the text: "When exploring, click a value to add it as an artifact". In the center, the 'Add Artifacts' dialog is displayed. It contains fields for 'Artifact' (10.11.23.120), 'Type' (Asset), 'Description' (Server for PROD-MFS), and 'Labels' (PROD-MFS). A tooltip (2) points to the 'Labels' field with the text: "Enter details and click Add to Scope". On the right, a table of correlated artifacts is shown.

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

< Back to investigations

Workbench Timeline Summary

Artifacts

22 out of 22 are selected.
Clear selected.

Filter artifacts

All Identities Assets

10.7.34.131
10.44.54.58
168.84.158.72
10.19.248.223
10.31.16.162
10.13.199.55

+ Add Artifact Explore

Add Artifacts

Add artifact

Artifact: 10.11.23.120

Type: Asset

Description: Server for PROD-MFS

Labels: PROD-MFS

Correlated Artifacts

10.13.199.55
10.13.223.31
10.14.66.55

Cancel Add to Scope

5, 2021 10:14 AM
5, 2021 11:12 AM

Edit (a)

Custom time

dest	user	ids_type
14.243	unknown	unknown
45.250	unknown	unknown
137.35	unknown	unknown
66.181	unknown	unknown
8.74	unknown	unknown
unknown	unknown	network

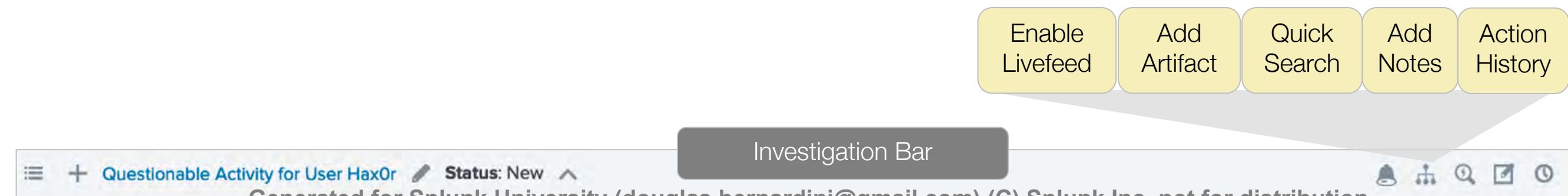
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

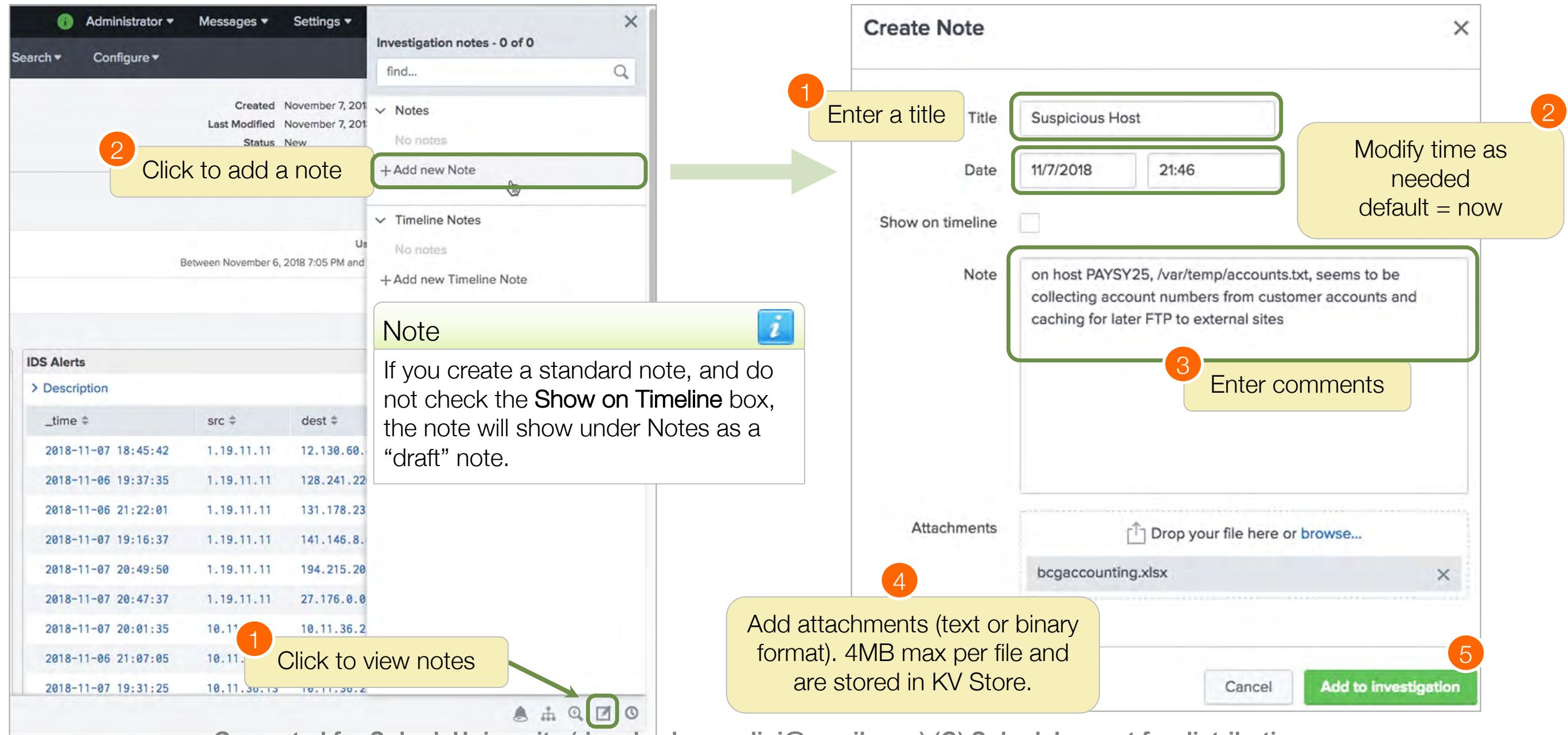
Add Items to an Investigation

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 Splunk interface with the following steps highlighted:

- 2 Select type: A yellow callout points to the "Select type" dropdown in the top-left corner.
- 3 Modify time as needed: A yellow callout points to the search time range dropdown ("Last 30 minutes") and the search icon.
- 4 Filter search as needed: A yellow callout points to the filter search input field and its button.
- 5 Select items: A yellow callout points to the "Select items" button at the bottom of the list table.
- 6 Done: A green button labeled "Done" is shown at the bottom right.
- 1 Notifications: A green box highlights the notifications icon in the bottom navigation bar.

Table Data (Search Results):

Dashboard Viewed										
	user	content.host	content.source	content.sourcetype	content.search	content.search_type	content.info	content	conten	conten
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										
✓ Search Run	08:54 PM	admin	ip-10-0-0-169.us-west-2.compute	audittrail	audittrail	search index=main user=haxOr	adhoc	granted	158144	
Add to Investigation	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	

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

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 interface with the following numbered steps:

1. The magnifying glass icon in the Investigation Bar is highlighted with a green box.
2. The "Enter search criteria" input field contains the IP address "10.12.34.56".
3. The search button next to the input field is highlighted with a green box.
4. A callout bubble points to the search results table, which lists two events. The first event is detailed below:

i	Time	Event
>	12/19/19 2:13:27.000 PM	2019-12-19 21:13:27 10.12.34.56 5783 139 TCP_NC_MISS 200 200 5716 21 2 - - OBSERVED POST 199.9.251.150 HTTP/1.0 218 http://199.9.251.150/ idle/1021363361/6500 - application/x-fcs "Shockwave Flash" - host = ip-10-0-0-169.us-west-2.compute.internal source = /opt/splunk/var/spool/splunk/http_log.large.bluecoat sourcetype = bluecoat:proxysg:access:file
5. A green button at the bottom right of the search results table says "Add Search String to Investigation".

A yellow callout bubble also points to the search window, stating: "Click and drag to resize the search window. Double click to toggle full screen to minimized".

- Analyst can run the saved search to view the results while investigating

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 interface for managing notable events. At the top, there's a header with '38 Notables' and buttons for 'Edit Selected' and 'Edit All Matching Events (38)'. A green box highlights the 'Add Selected to Investigation' button. Below the header is a table of notable events with columns for Title, Risk Object, Aggregated Risk Score, Risk Events, Type, Time, Disposition, Security Domain, Urgency, Status, Owner, and Actions. Several rows are selected, indicated by checked checkboxes in the first column.

Two yellow callout boxes point to different methods of adding events:

- A yellow box with a green arrow points from the 'Actions' column to the 'Add Event to Investigation' option in the context menu. It contains the text: "Add notable events from Incident Review".
- A yellow box with an orange circle containing the word "or" points from the 'Event Actions' dropdown to the 'Add source events from a search result' option in the context menu. It contains the text: "Add source events from a search result".

At the bottom of the interface, there's a table showing event details with columns for Value and Actions. The 'Value' column lists fields like 'ip-10-0-0-169.us-west-2.compute.internal', '/opt/splunk/var/spool/splunk/auth.nix', 'linux_secure', 'failure (failure)', and 'sshd'. The 'Actions' column contains dropdown arrows for each value.

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

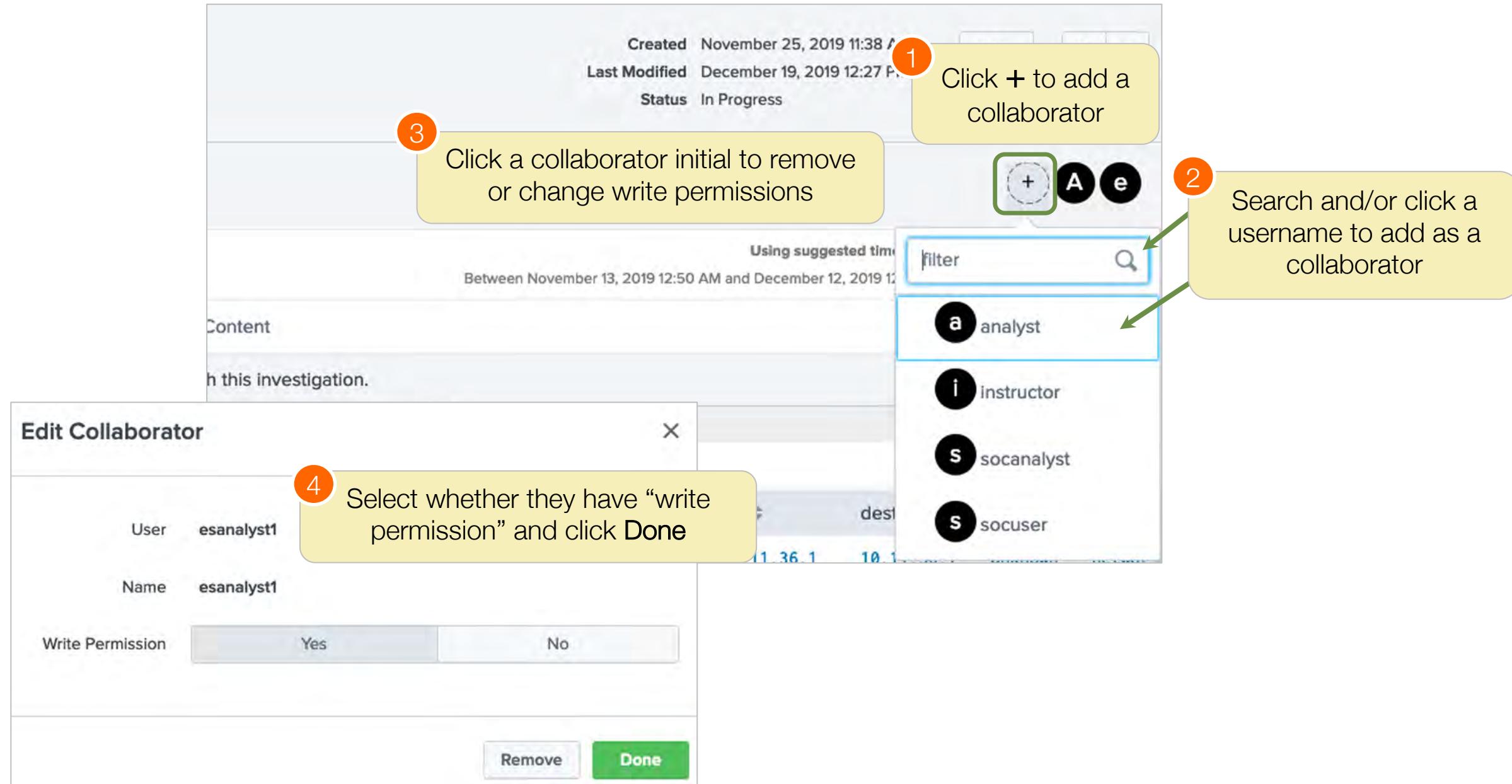
Enable notification

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

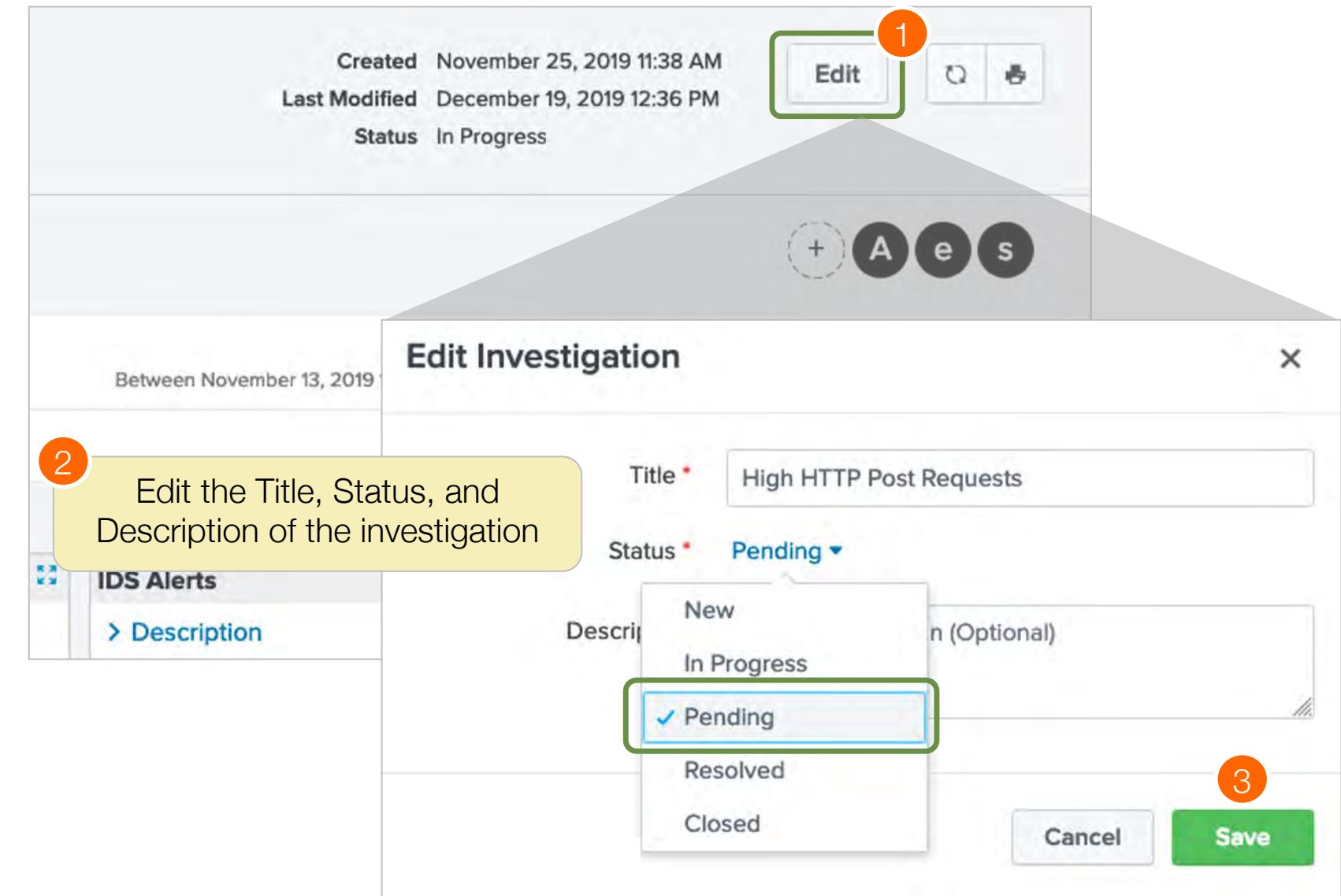
Adding Collaborators to an Investigation



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

Updating Investigation Status

- When you open an investigation, its 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

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