Using Splunk Enterprise Security

Document Usage Guidelines

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

Foundational Knowledge

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

Course Goals

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

Important!

All labs must be completed for course credit

Course Outline

Module 1: Introduction to ES
Module 2: Security Monitoring & Incident Investigation
Module 3: Risk-Based Alerting
Module 4: Assets & Identities
Module 5: Investigations
Module 6: Security Domain Dashboards
Module 7: User Intelligence
Module 8: Web Intelligence
Module 9: Threat Intelligence
Module 10: Protocol Intelligence

Appendix A: Reports, Dashboards, Data Models, and ES Content Updates
Appendix B: Event Sequence Engine
Appendix C: Interfacing with Splunk Intelligence Management (TrueSTAR)
Appendix D: Cloud Security Dashboards

Module 1: Introduction to Enterprise Security

Objectives

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

Overview of Splunk Enterprise Security

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

ES Functional Areas

Vulnerability alerts

Unexpected processes

Prohibited traffic

Threat activity

Known threats

Traffic analysis

Statistical analysis

Anomaly detection

Pattern matching

Risk framework

Audit

Investigation journaling

Incident tracking

Forensics tools

Asset & identity management

ES Use Cases

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

Note

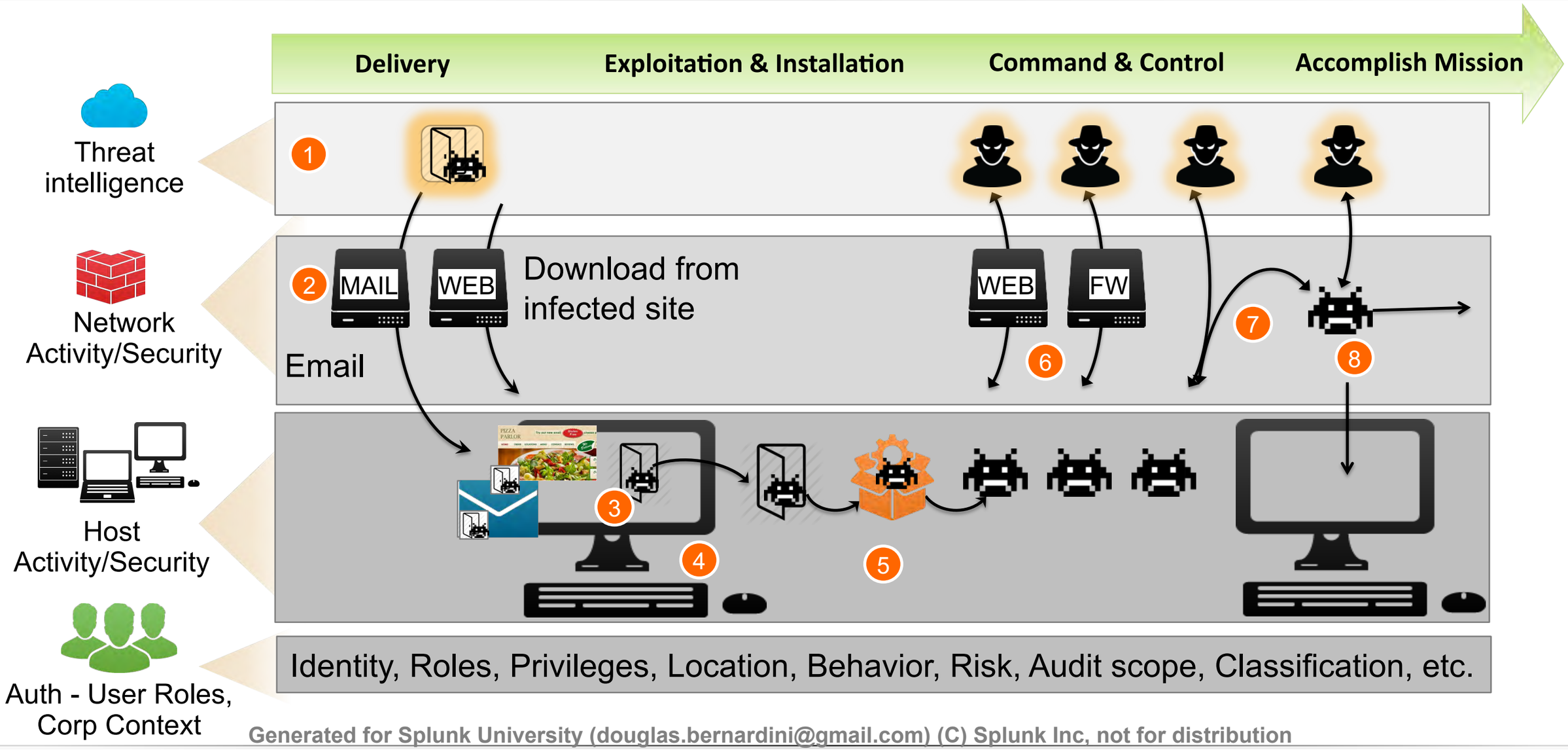
Refer to the *Splunk Enterprise Security Use Cases documentation* for a detailed list.

ES Detecting APTs

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

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

APT Attack - Example



The Kill Chain

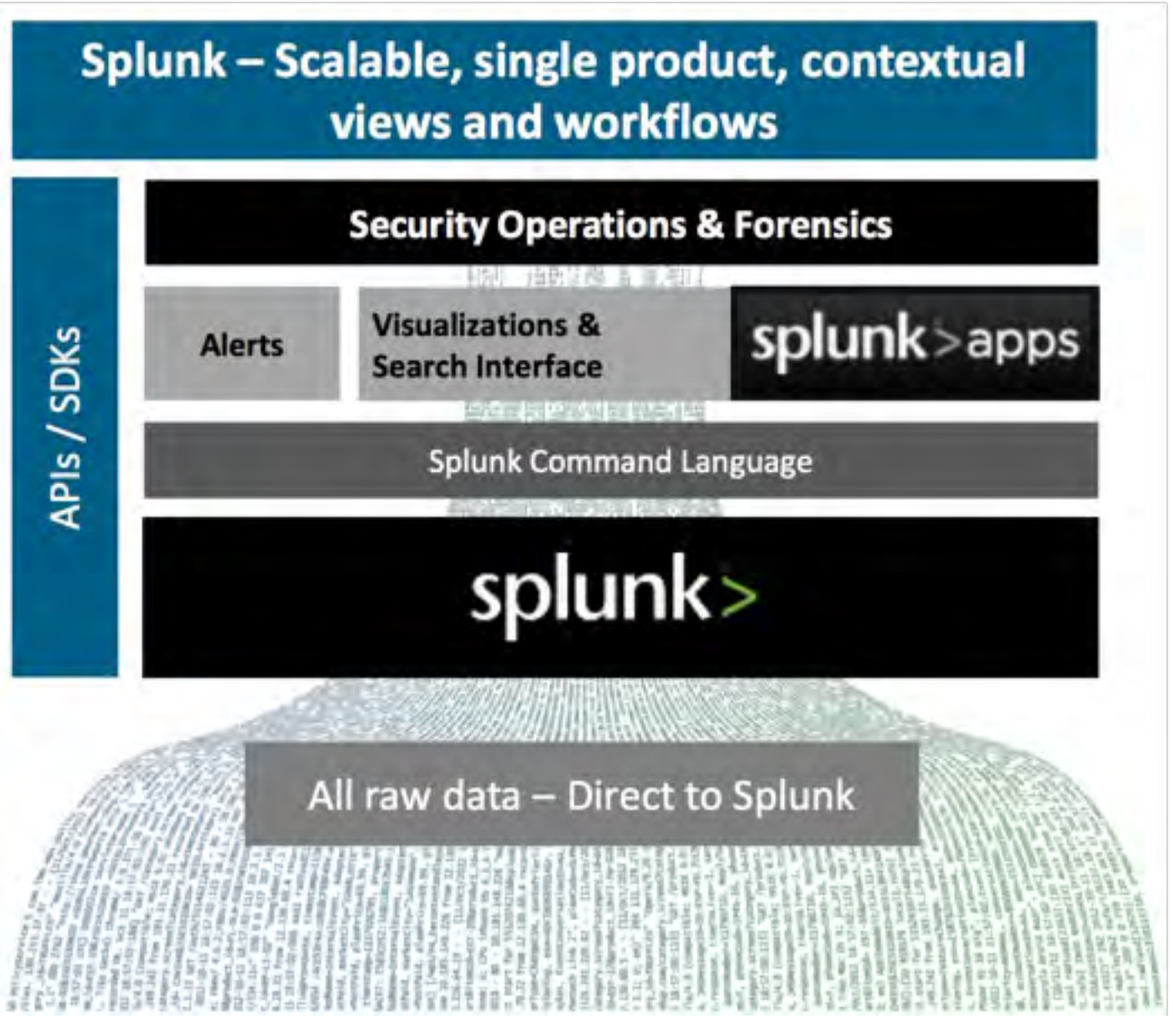
Attackers use the kill chain methodology to devise and implement their attacks, but defenders can also use the kill chain to counter and those prevent attacks

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

Who Uses ES?

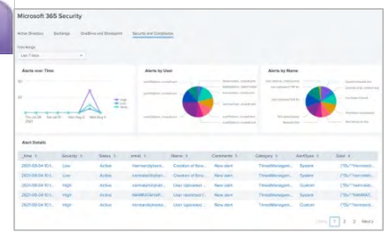
Security Analysts

SOC Staff



Security Exec/Managers

Security Auditors



How ES Works

Raw Events are Indexed

Data is generated, forwarded, and indexed into Splunk

Data Model Summary Searches Run

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

Data is available for ES

`| tstats` queries and dashboards can now use the data

ES Background Searches (content) Process Data

Correlation Searches, trackers, and threat intelligence search data models

ES Searches for Threats and Anomalies

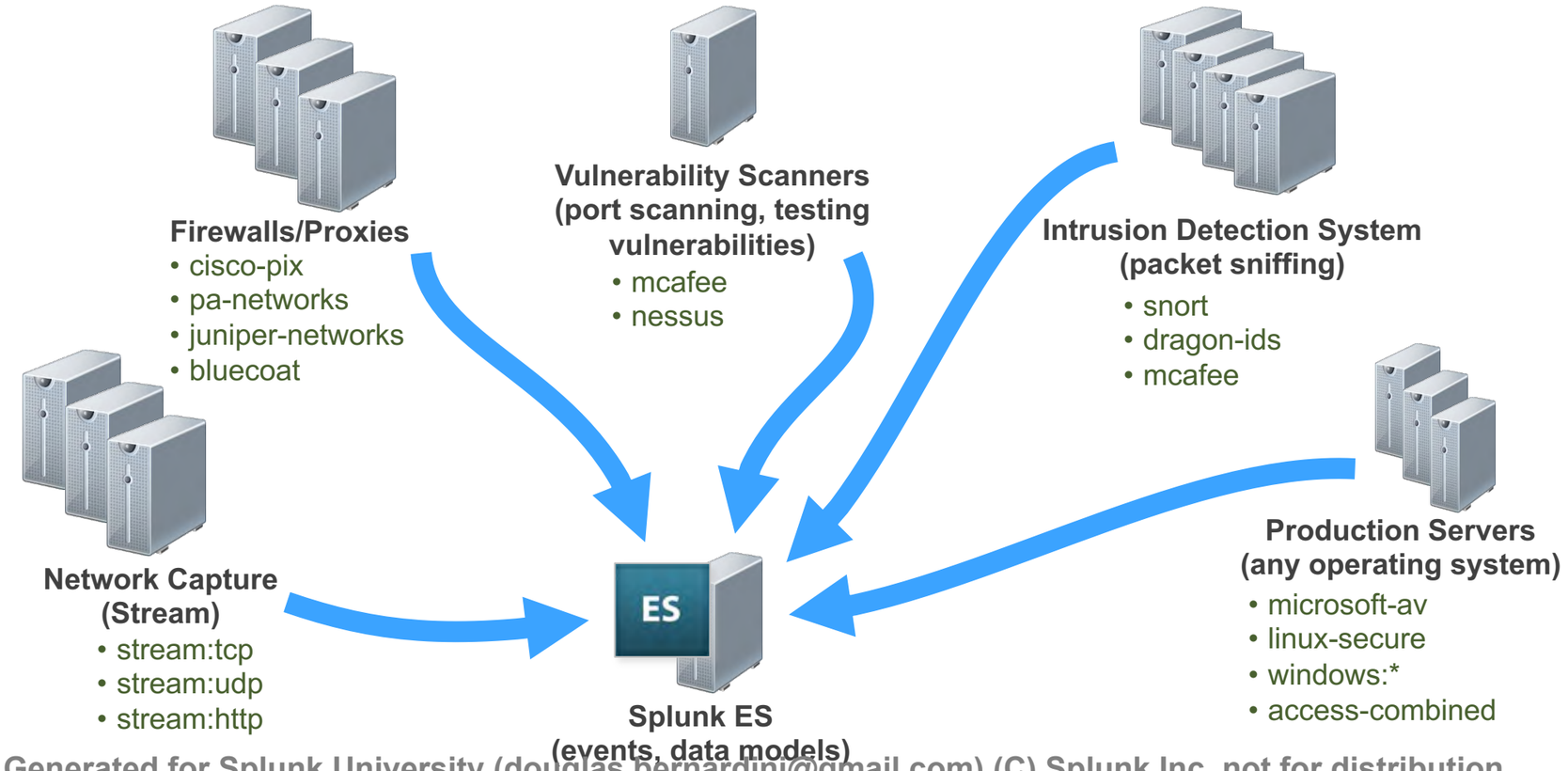
ES creates notable events which are stored in summary indexes and are searchable by data models

How ES Works (cont.)

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

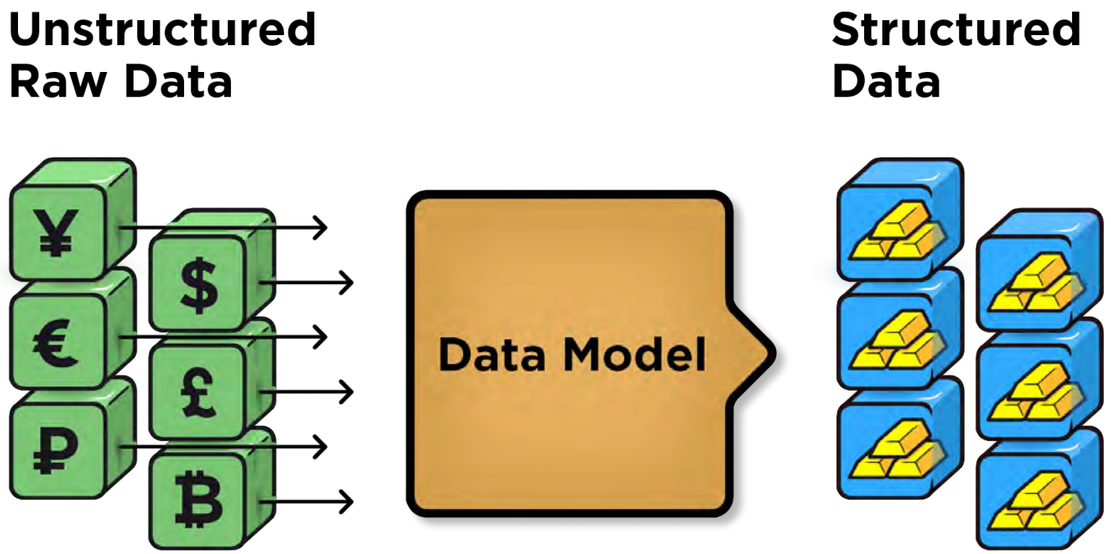
ES Data Flow

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



Data Models

- Data models normalize data
- Data models provide a more meaningful representation of unstructured raw data
- ES depends heavily on *accelerated* data models

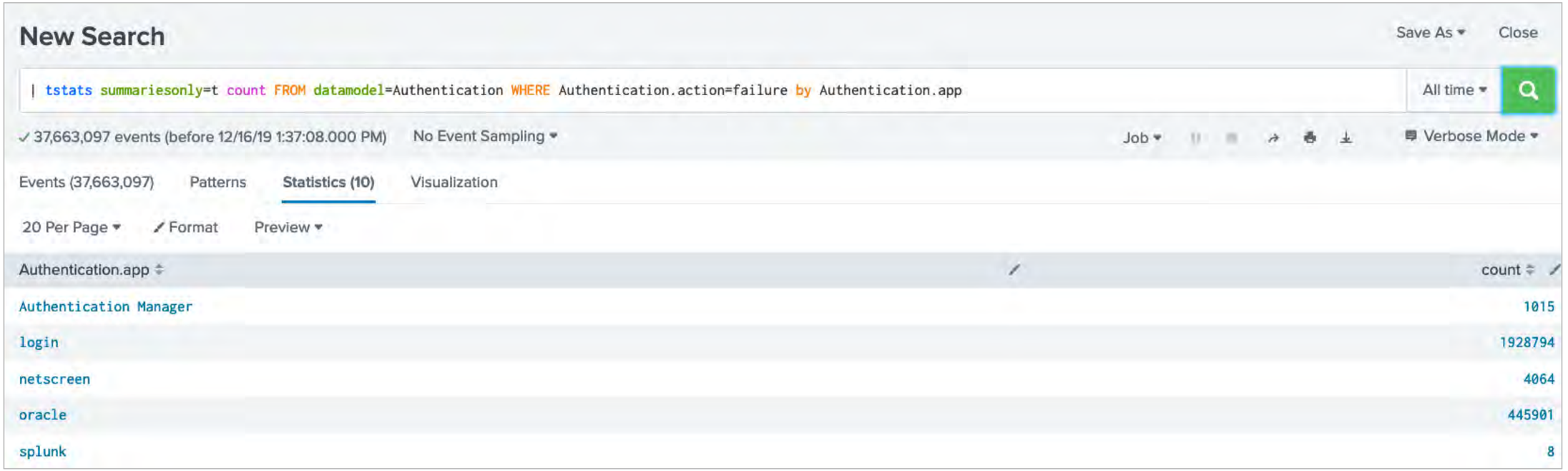


- Accelerated data models provide a “speedup” factor
- Use `| tstats summariesonly = true` to search accelerated data

ES Dashboards and Data Models

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

`tstats` Search Example



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

ES and The KV Store

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

Important!

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

Correlation Searches

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

Notable Events

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

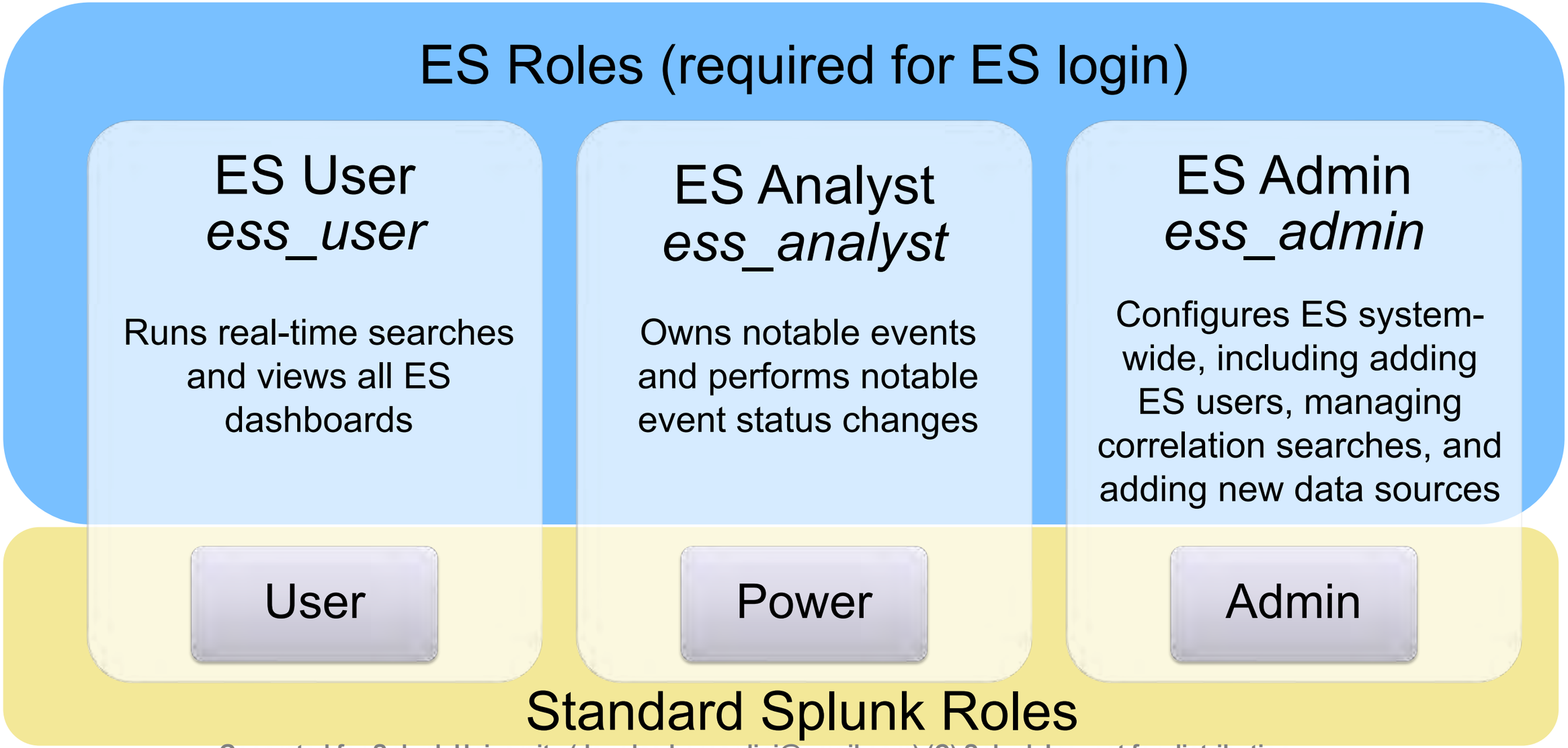
Assets and Identities

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

Beyond Notable Events

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

ES Roles

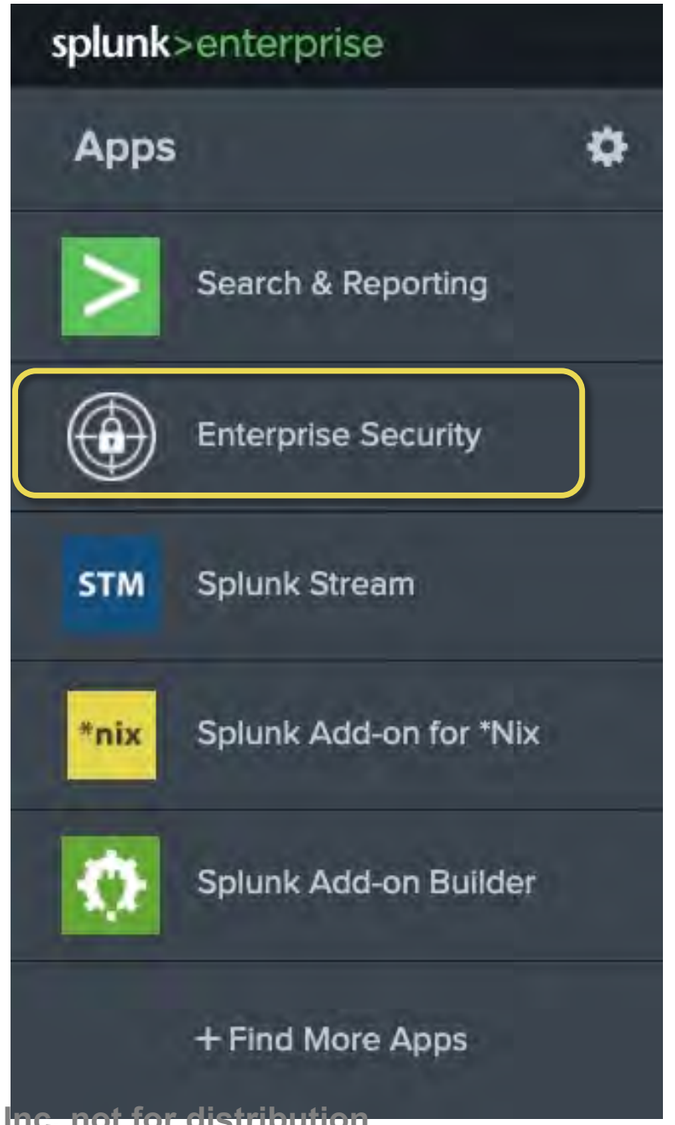


Accessing ES

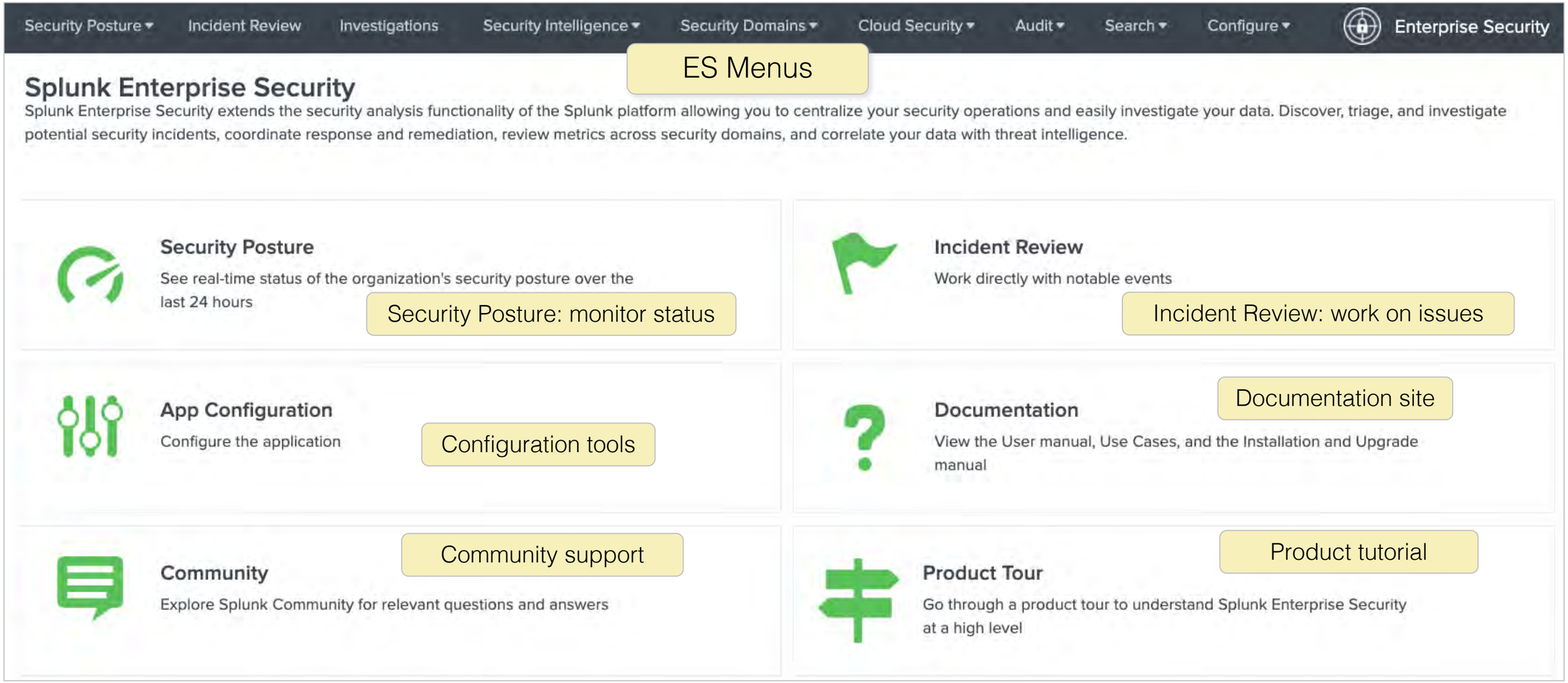
- Access Splunk Web using a URL similar to: **`https://eshostname:8000`**

- 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



The ES Home Page



Module 1 Lab: Introduction to ES

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

Module 2:
Security Monitoring and Incident Investigation

Objectives

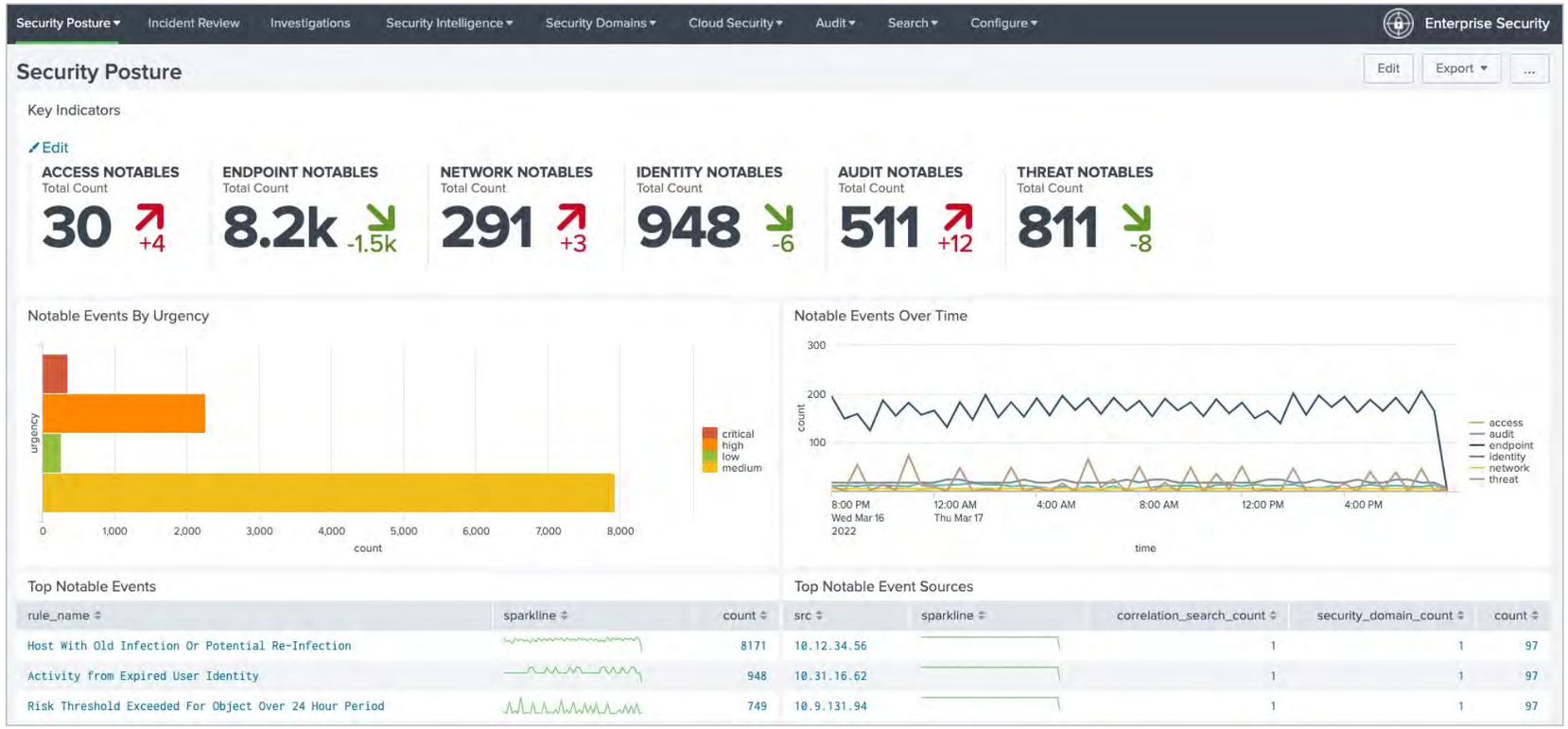
- Use the **Security Posture** dashboard to monitor ES status
- Use the **Executive Summary** dashboards to view security operations at high level
- Use the **Incident Review** dashboard to analyze notable events
- Take ownership of a notable event and move it through the incident workflow
- Create notable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

Monitoring and Response

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

The Security Posture Dashboard

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



Key Indicators (KI)

Edit key indicators

Large number = total number of notable events in that category

Black = no threshold set
Red = over threshold
Green = under threshold

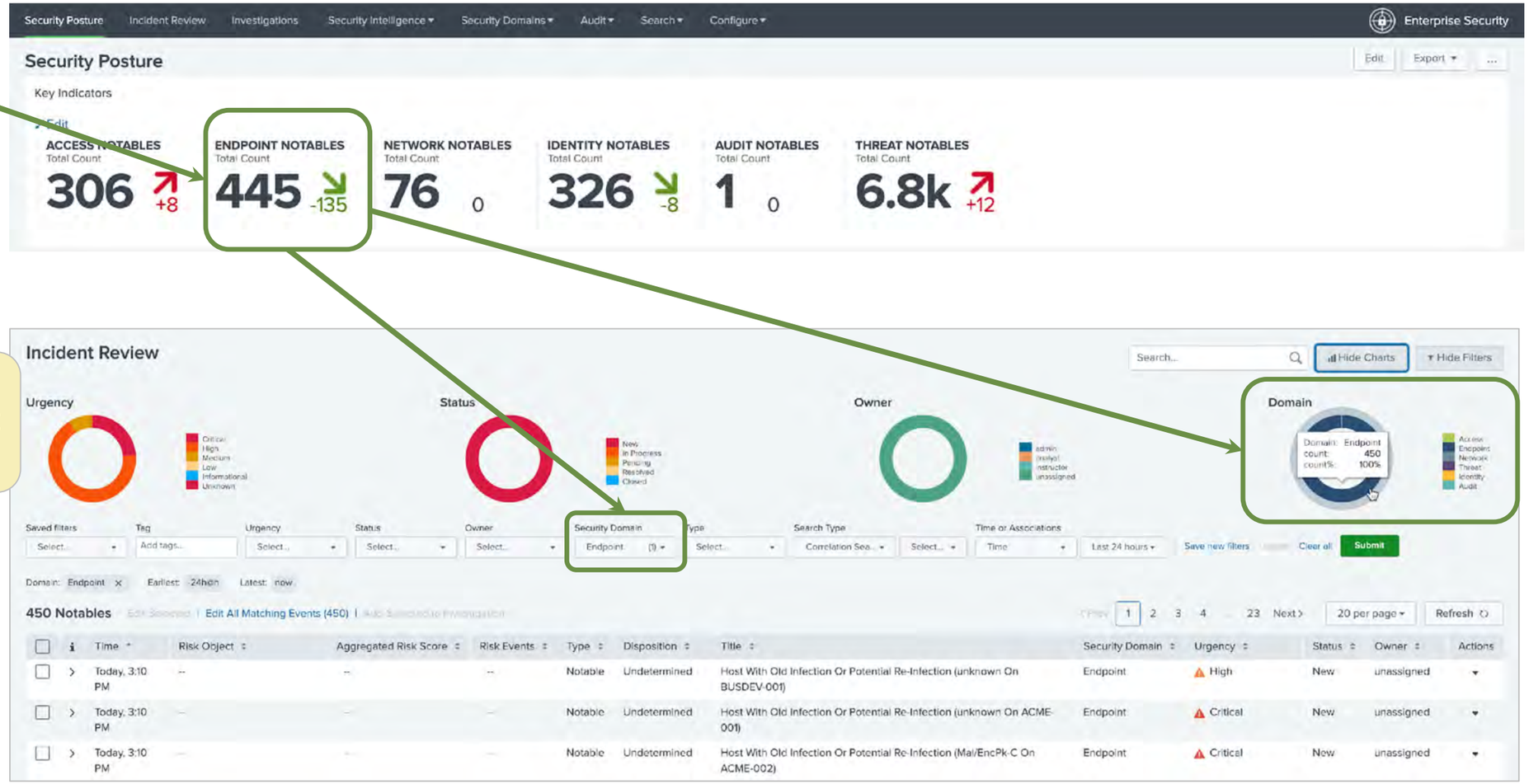
Trend of events indicator: red for increase green for decrease

Total increase or decrease over the past 48 hours (from previous 24-hr period to last 24-hr period)

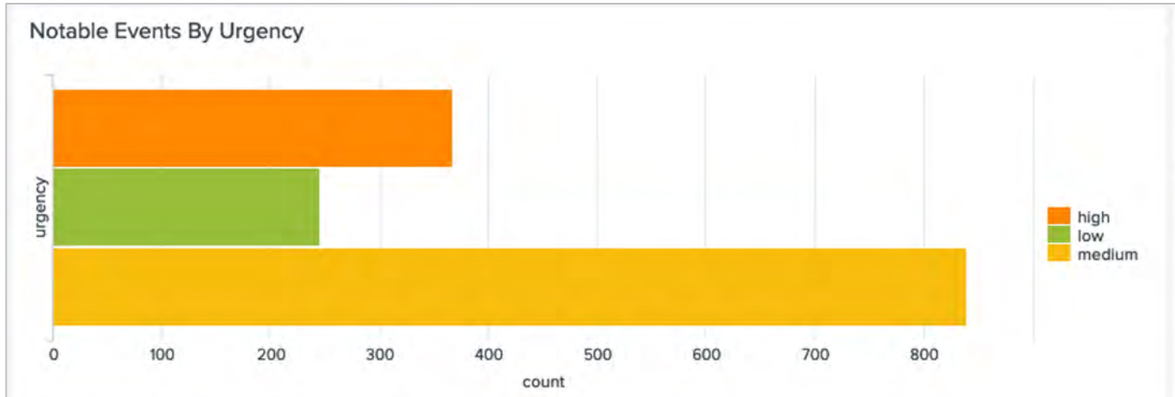
KI Drilldown to Incident Review

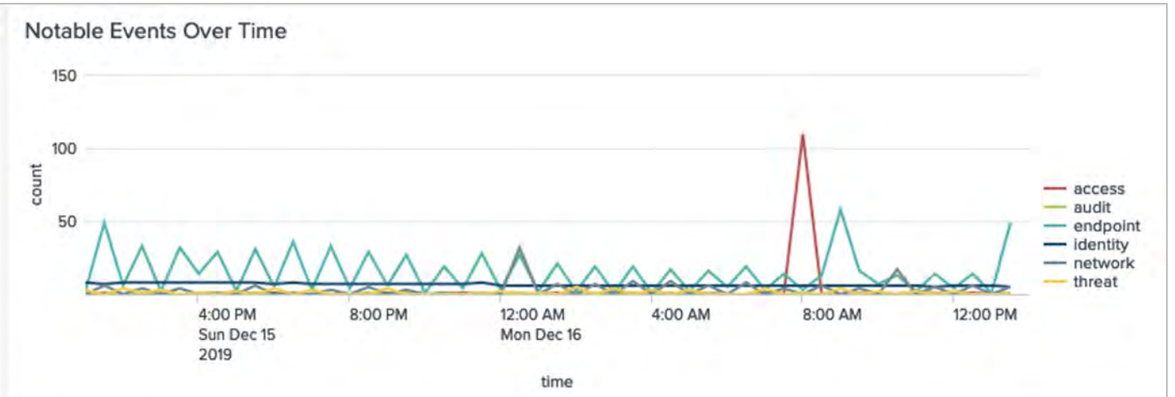
1. From the **Security Posture** dashboard, click a KI total value

2. The details for the KI opens in **Incident Review**



Security Posture Panels





Top Notable Events

rule_name	sparkline	count
Host With Old Infection Or Potential Re-Infection		521
Activity from Expired User Identity		331
Host With Multiple Infections		168
Excessive Failed Logins		108
Unroutable Activity Detected		96
High Or Critical Priority Host With Malware Detected		70
Abnormally High Number of HTTP Method Events By Src		63
Threat Activity Detected		57
Short-lived Account Detected		19
Anomalous Audit Trail Activity Detected		14

« Prev 1 2 Next »

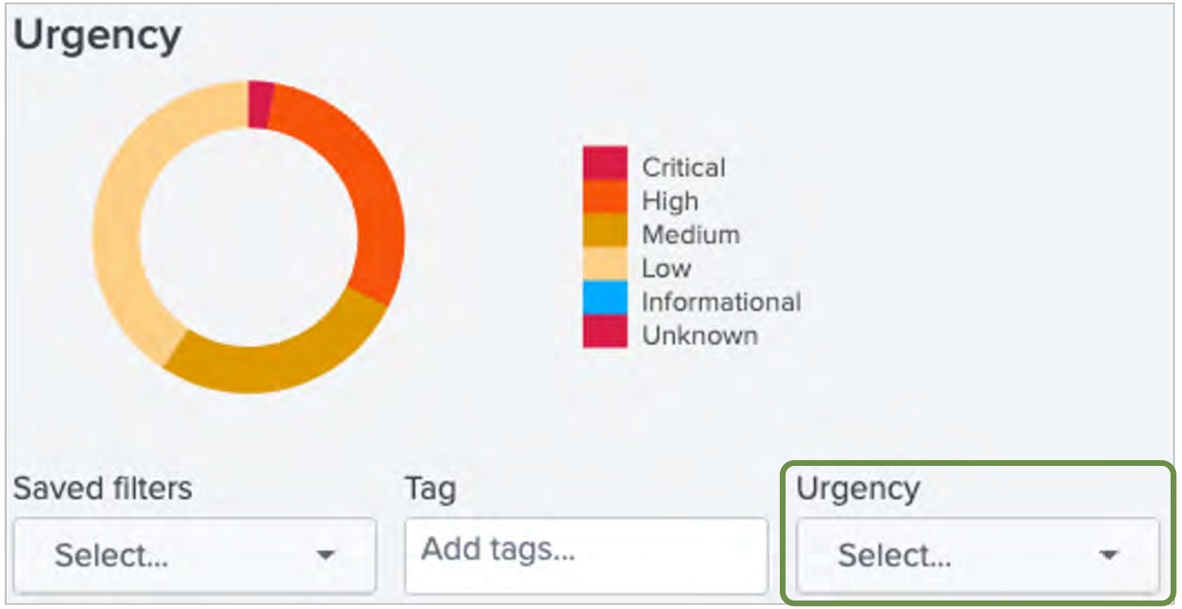
Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
10.11.36.20		3	3	6
10.141.2.170		1	1	5
10.11.36.1		1	1	2
10.11.36.10		1	1	2
10.11.36.11		1	1	2
10.11.36.12		1	1	2
10.11.36.13		1	1	2
10.11.36.14		1	1	2
10.11.36.15		1	1	2
10.11.36.16		1	1	2

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

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



Urgency Table

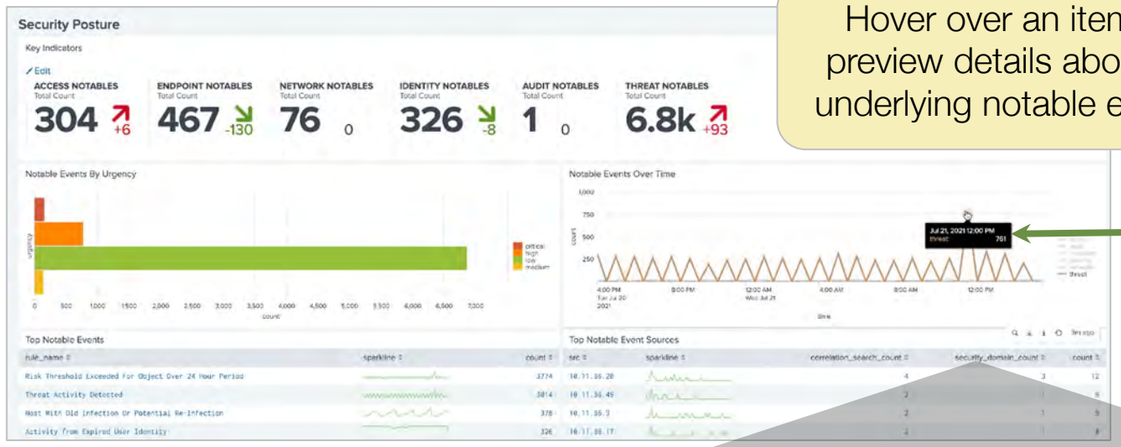
- How urgency values are calculated in notable events by default
- Can be overwritten by modifying asset/identity priority and rank, correlation search syntax, or **Urgency Levels** lookup

Event Severity

Asset/Identity Priority	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

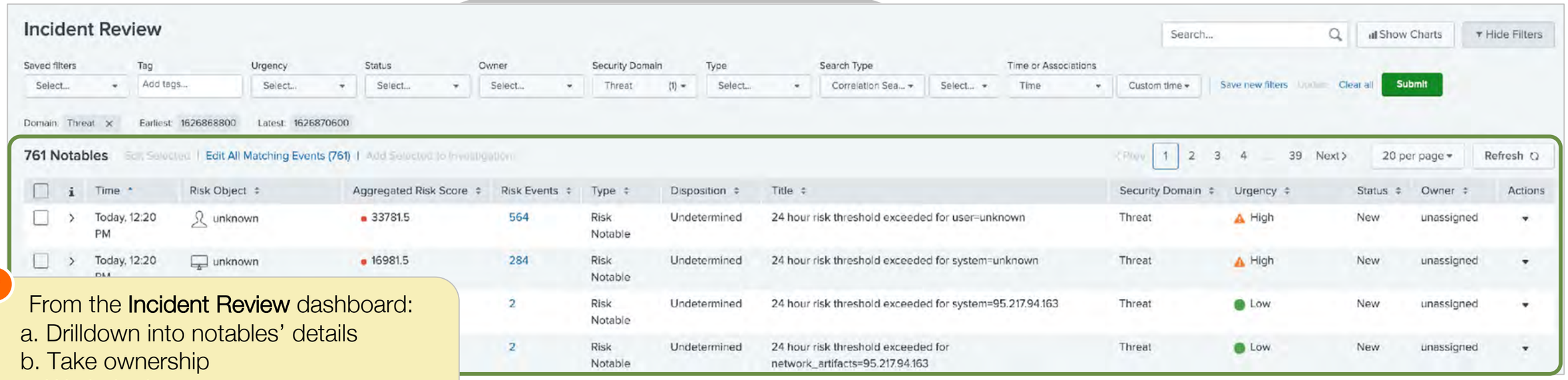
Asset/Identity Priority + Event Severity = Urgency

Drilldown Support



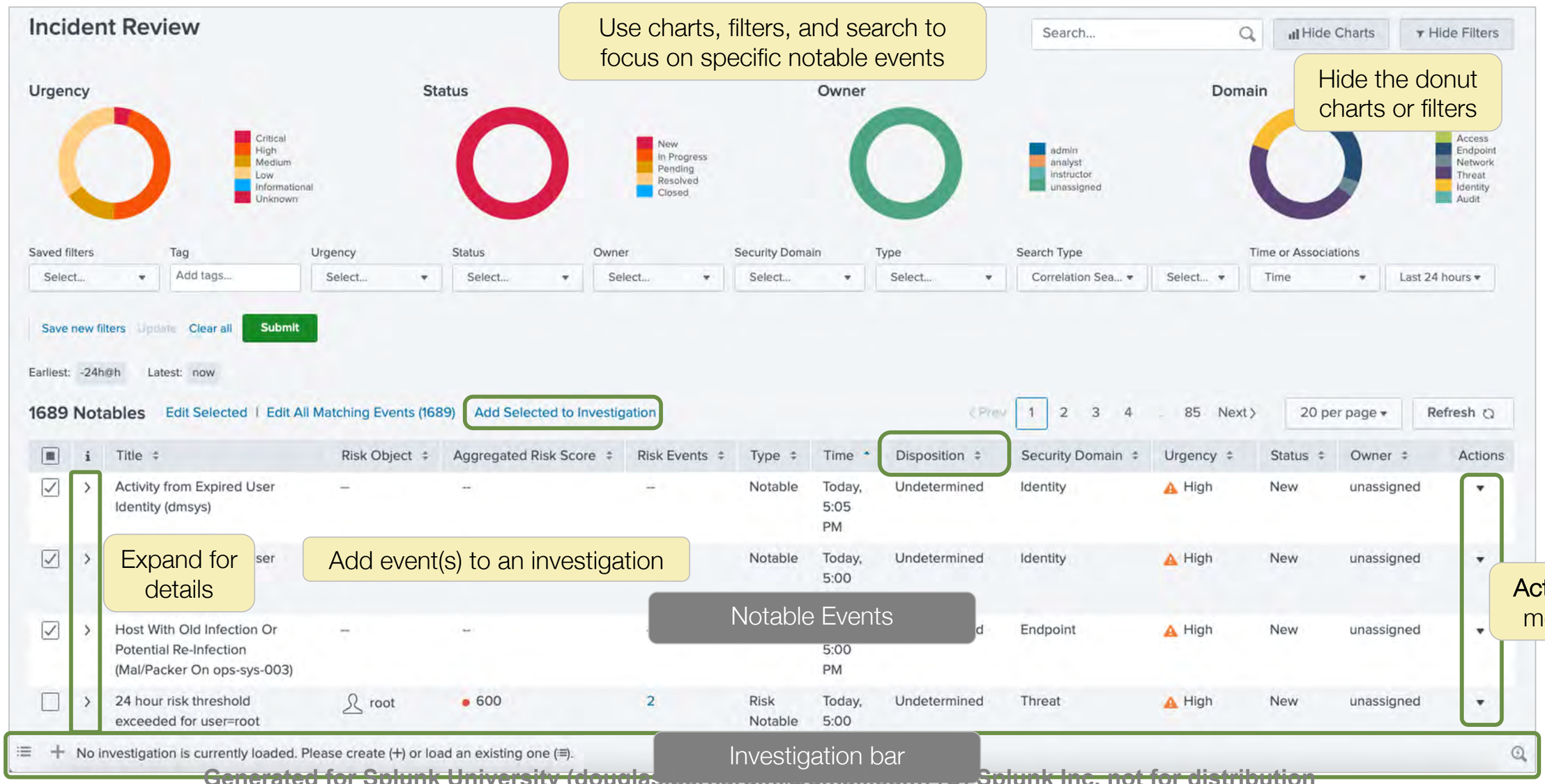
Hover over an item to preview details about its underlying notable events

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

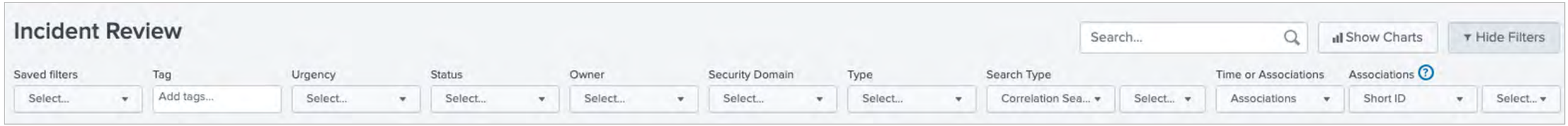


2 From the **Incident Review** dashboard:
a. Drilldown into notables' details
b. Take ownership
c. Work the issue

Incident Review Dashboard



Incident Review Filter Fields

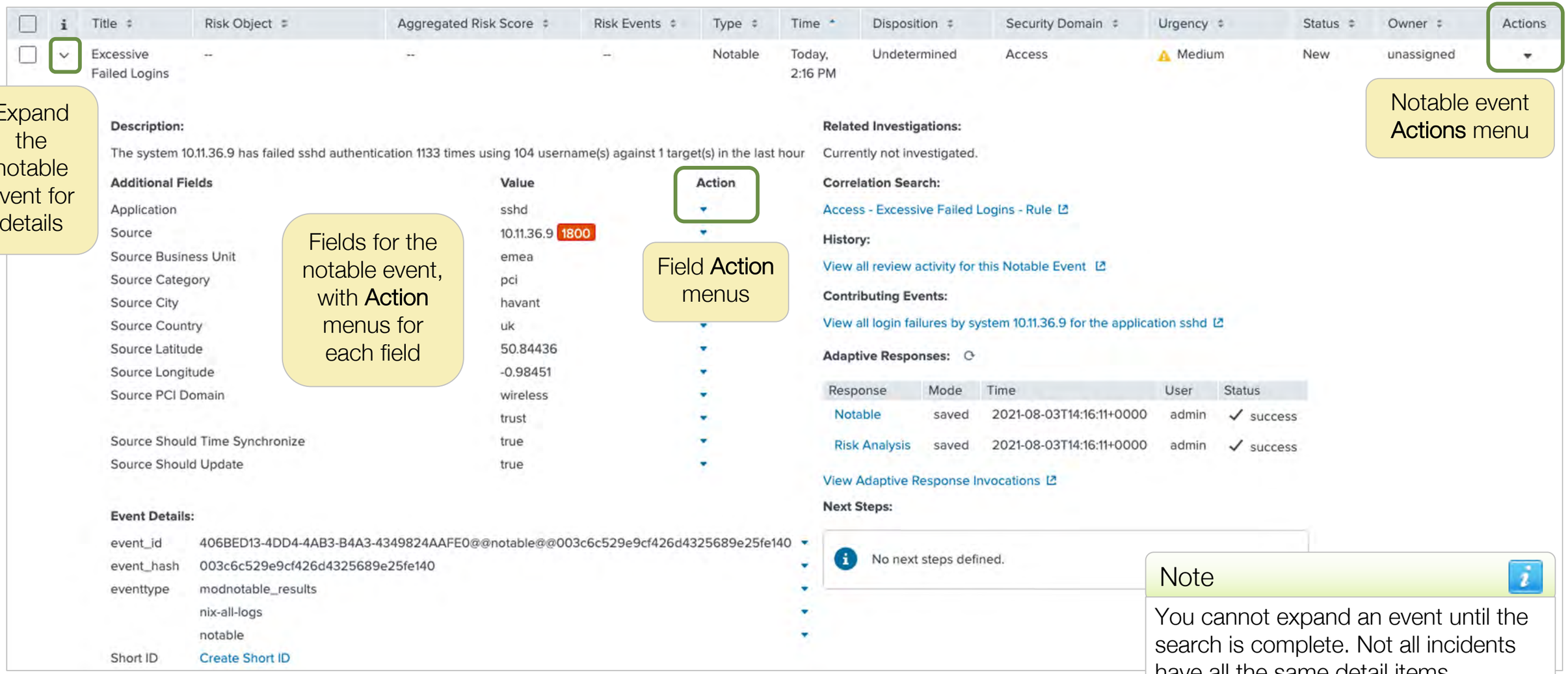


- **Saved filters:** any filters created and saved on the IR dashboard
- **Search:** Splunk search language expressions
- **Tag:** tags configured for key/value pairs
- **Urgency:** Informational, Low, Medium, High, Critical, Unknown
- **Status:** New, In Progress, Pending, Resolved, Closed
  - Along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

Using the Incident Review Dashboard

- **Search** supports full SPL and wildcard search
- Adding one or more values per field, values are **OR**ed 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 **AND**ed together
- **Status**, **Owner**, **Security Domain** and **Tag** support multiple **OR** values

Notable Event Details

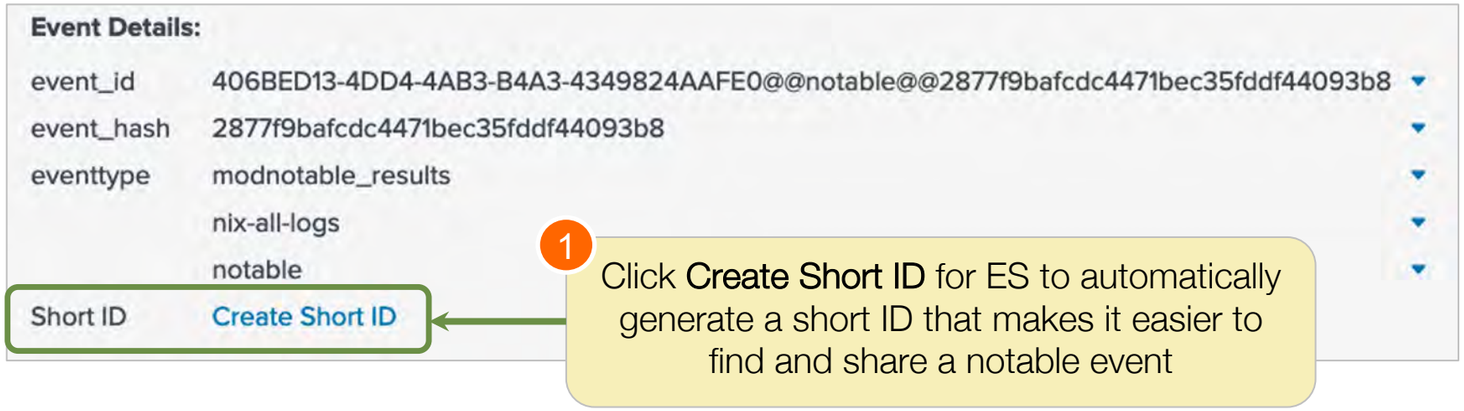


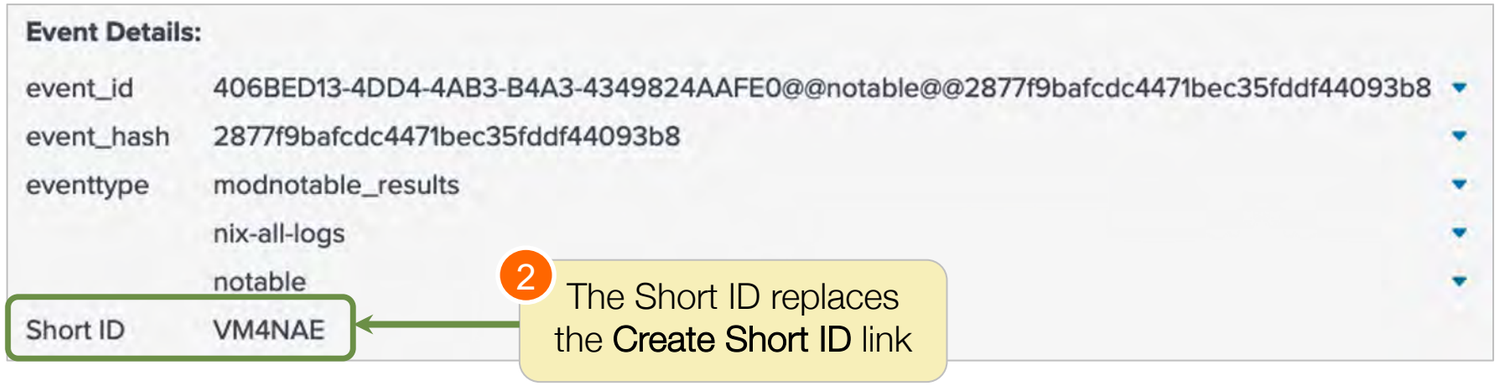
Note

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

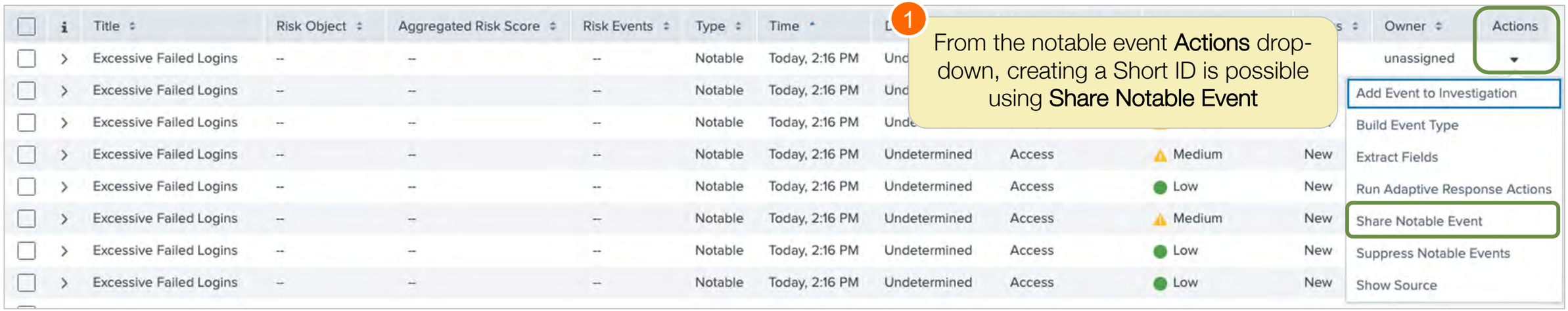
Create a Short ID from Event Details

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

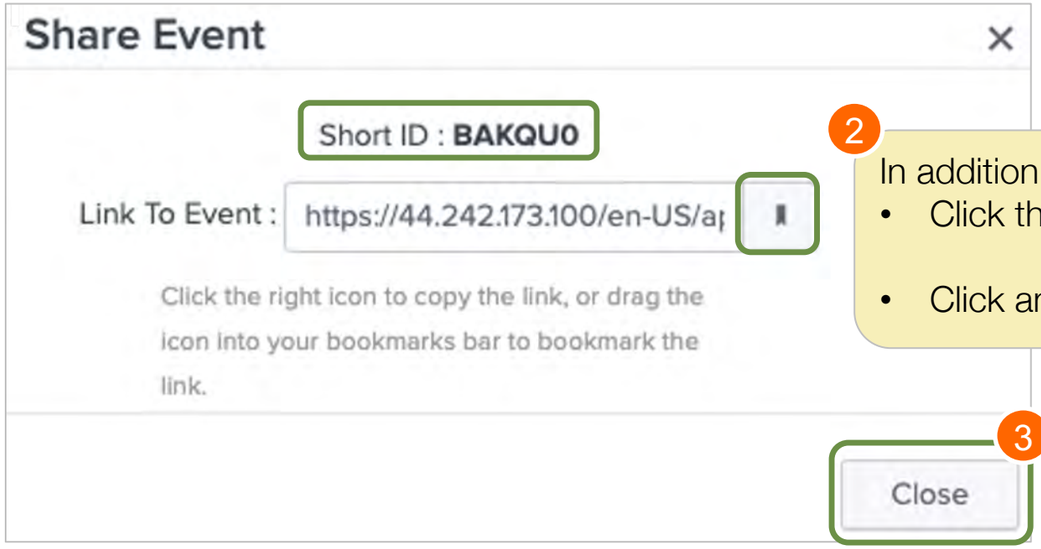




Create a Short ID: Notable Event Actions



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



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

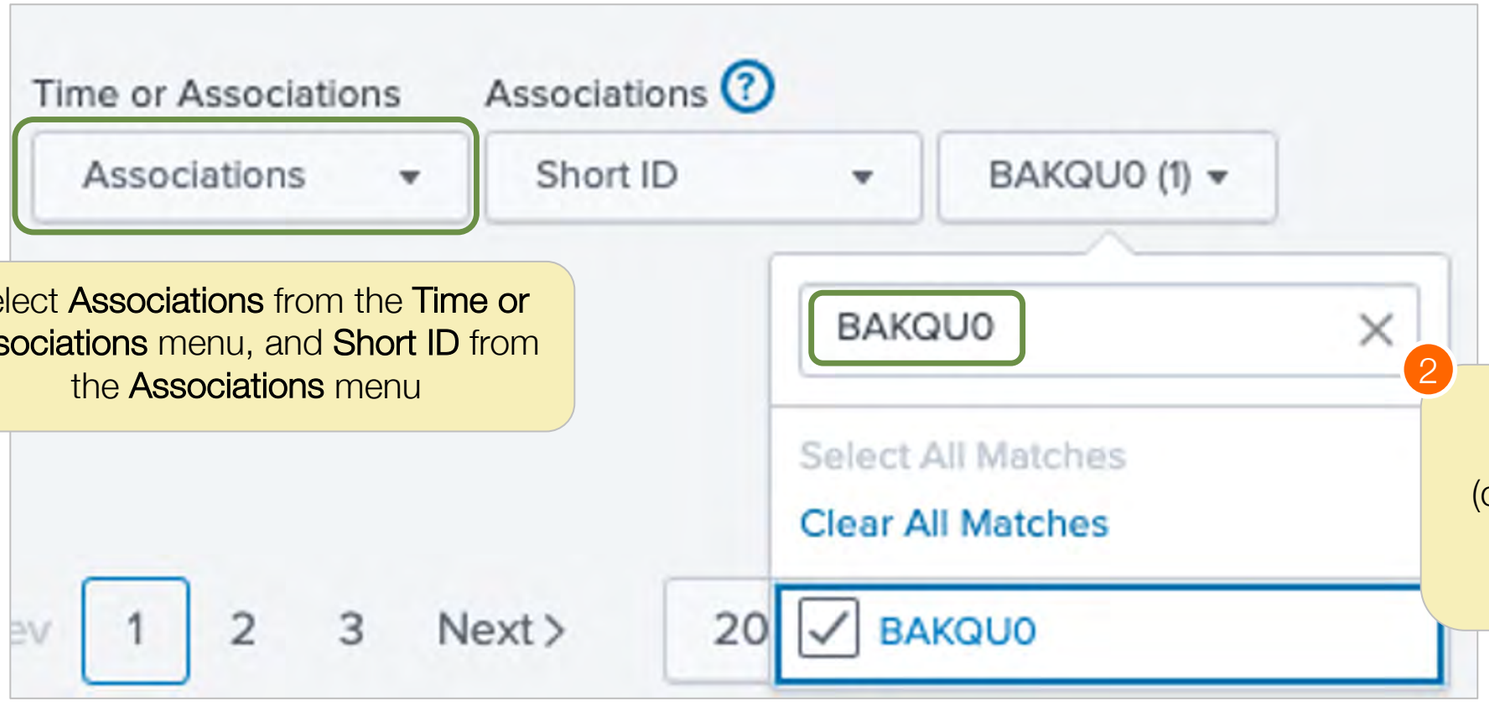
- Click the **Bookmark** button to copy the link for sharing

or

- Click and drag the **Bookmark** button to your Bookmarks bar to save the link

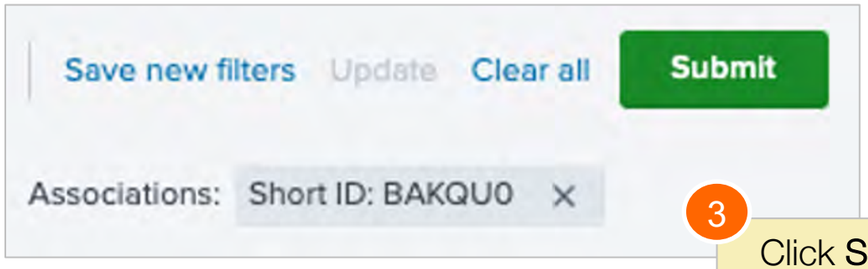
3

Search for a Short ID or Investigation



1 Select **Associations** from the **Time or Associations** menu, and **Short ID** from the **Associations** menu

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



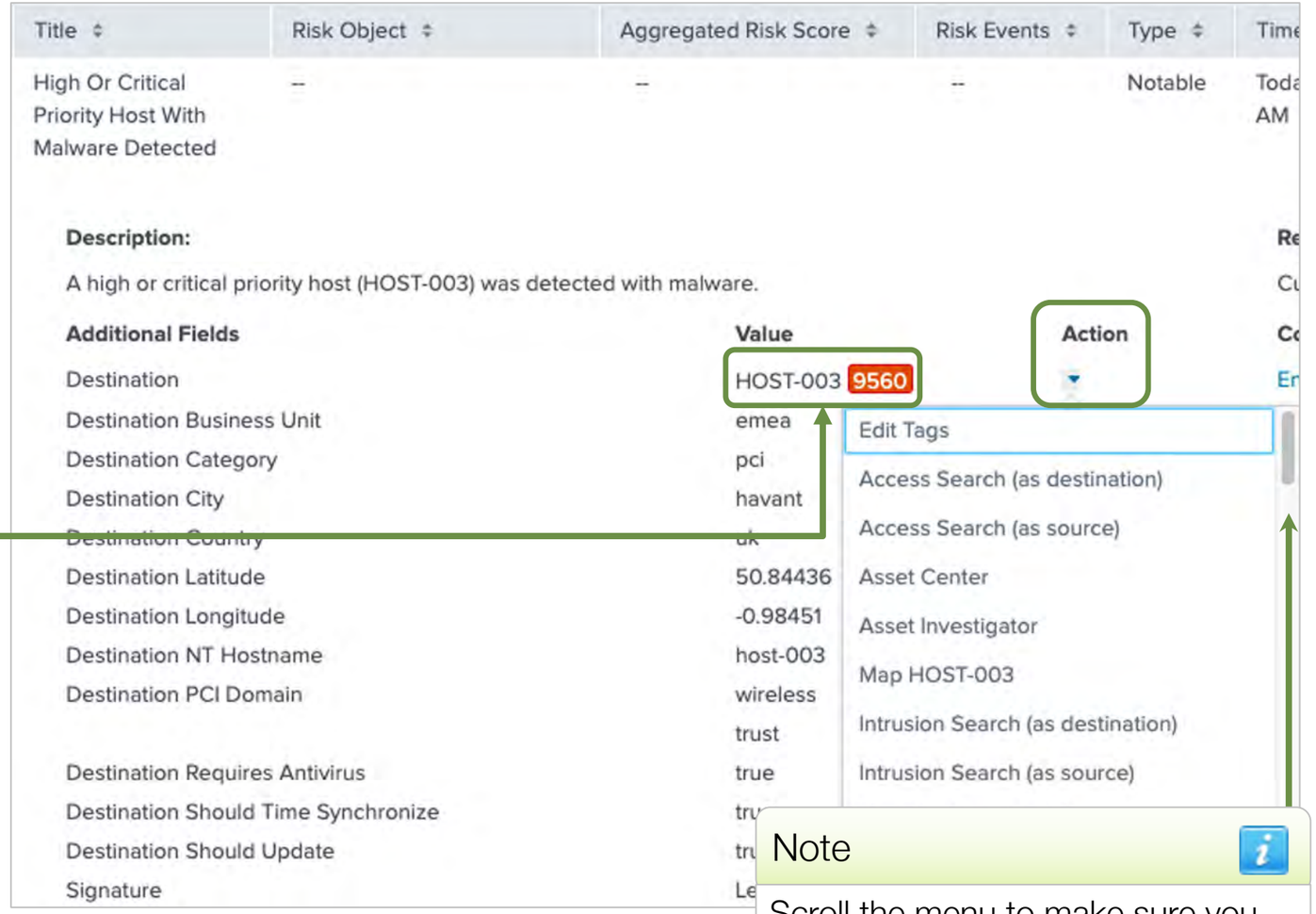
3 Click **Submit**

Note

You can search for one or multiple Short IDs.

Field Action Menu

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

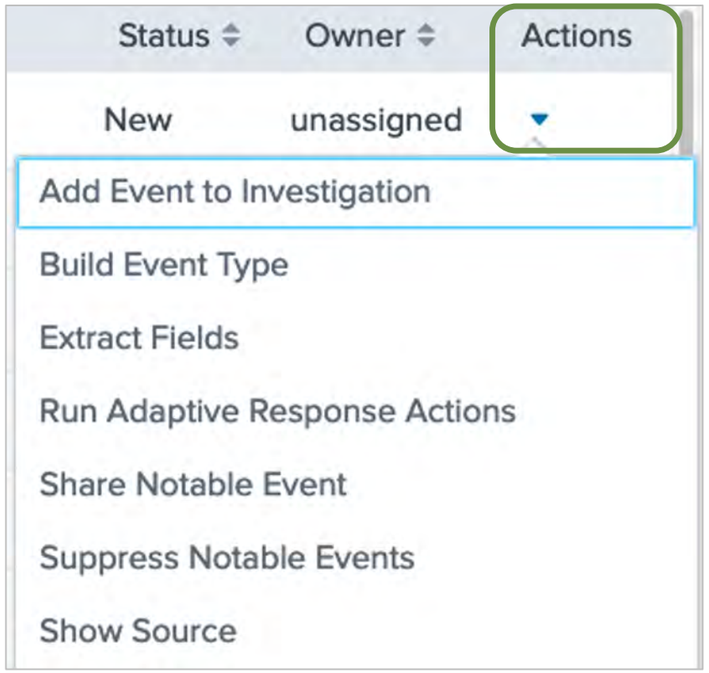


Note

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

Notable Event Actions Menu

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



Incident Workflow: Concepts

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

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

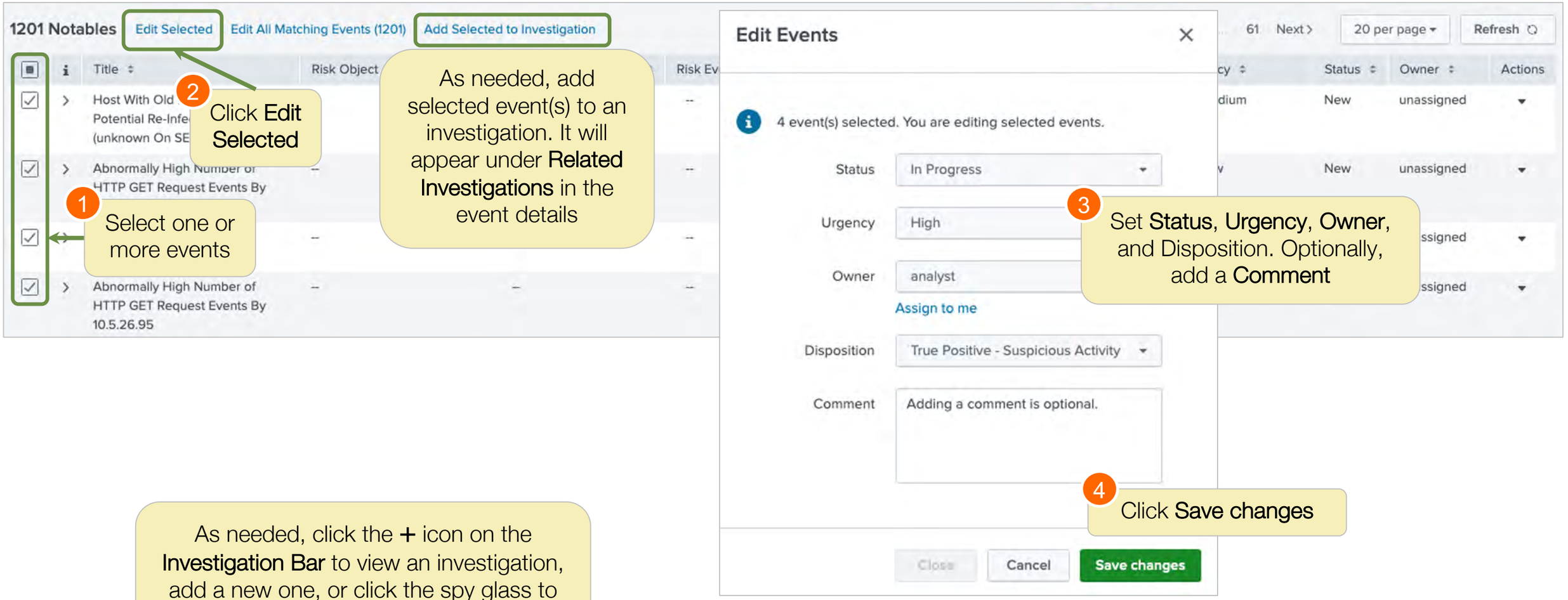
ES Admins can define, add new status values and assign values to different roles, so the statuses in your environment may differ

New - not yet being worked
In Progress - analysis underway
Pending - various: work in progress, awaiting action, etc.
Resolved - fixed, awaiting verification
Closed - fix verified

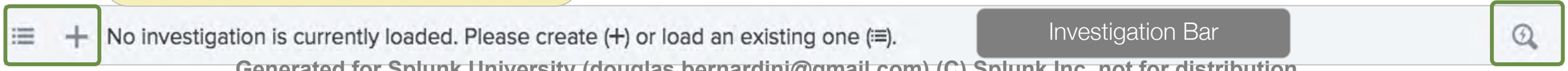
Note

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

Incident Workflow: Procedures



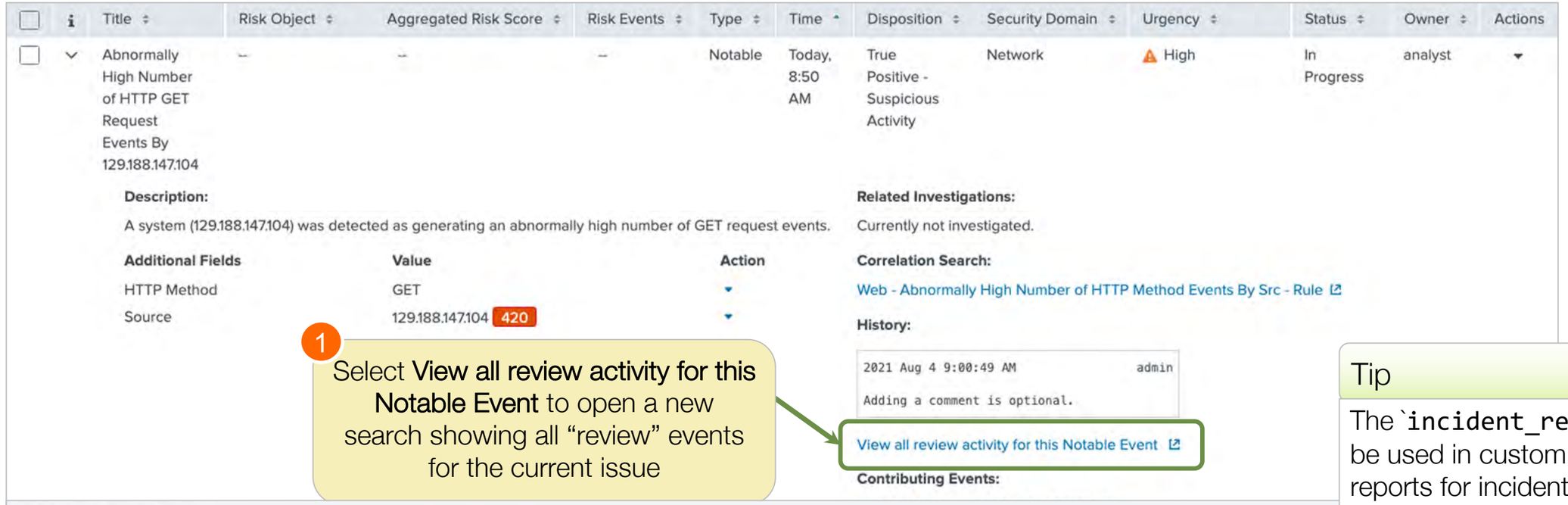
As needed, click the + icon on the **Investigation Bar** to view an investigation, add a new one, or click the spy glass to perform a quick search



Investigation Bar

 | 25 May 2022

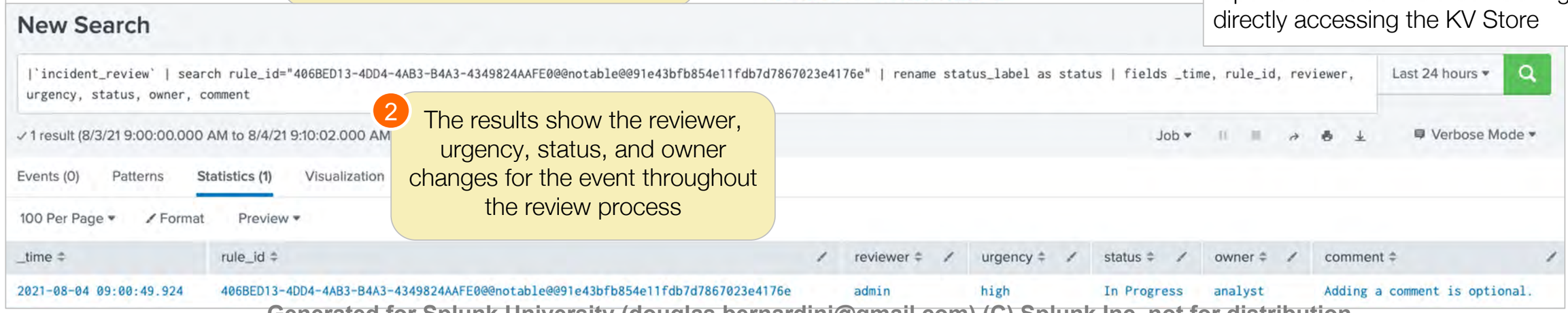
Incident Review History



1 Select **View all review activity for this Notable Event** to open a new search showing all "review" events for the current issue

Tip

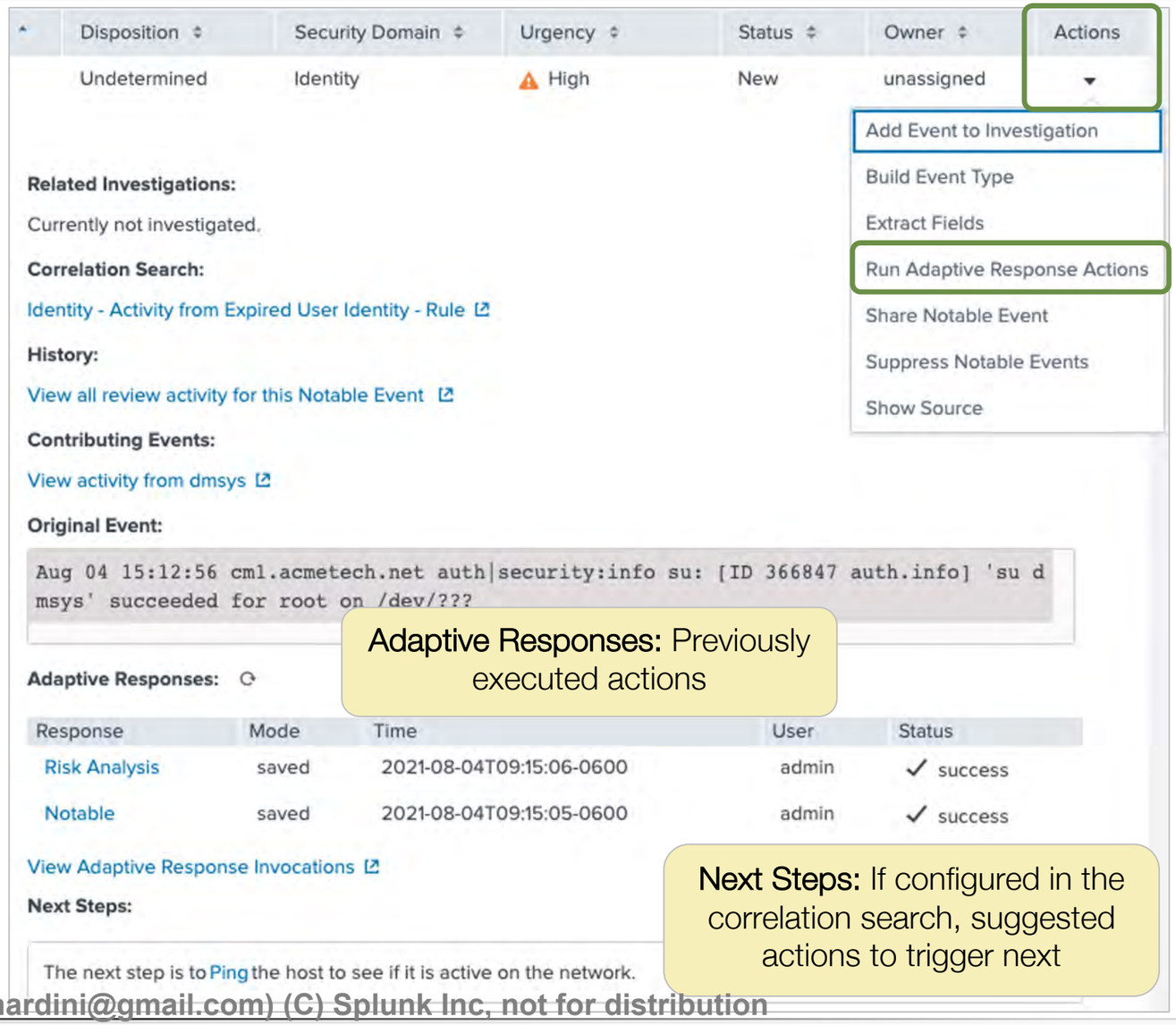
The `` `incident_review` `` macro can be used in custom searches and reports for incident status tracking by directly accessing the KV Store



2 The results show the reviewer, urgency, status, and owner changes for the event throughout the review process

Notable Event Adaptive Response

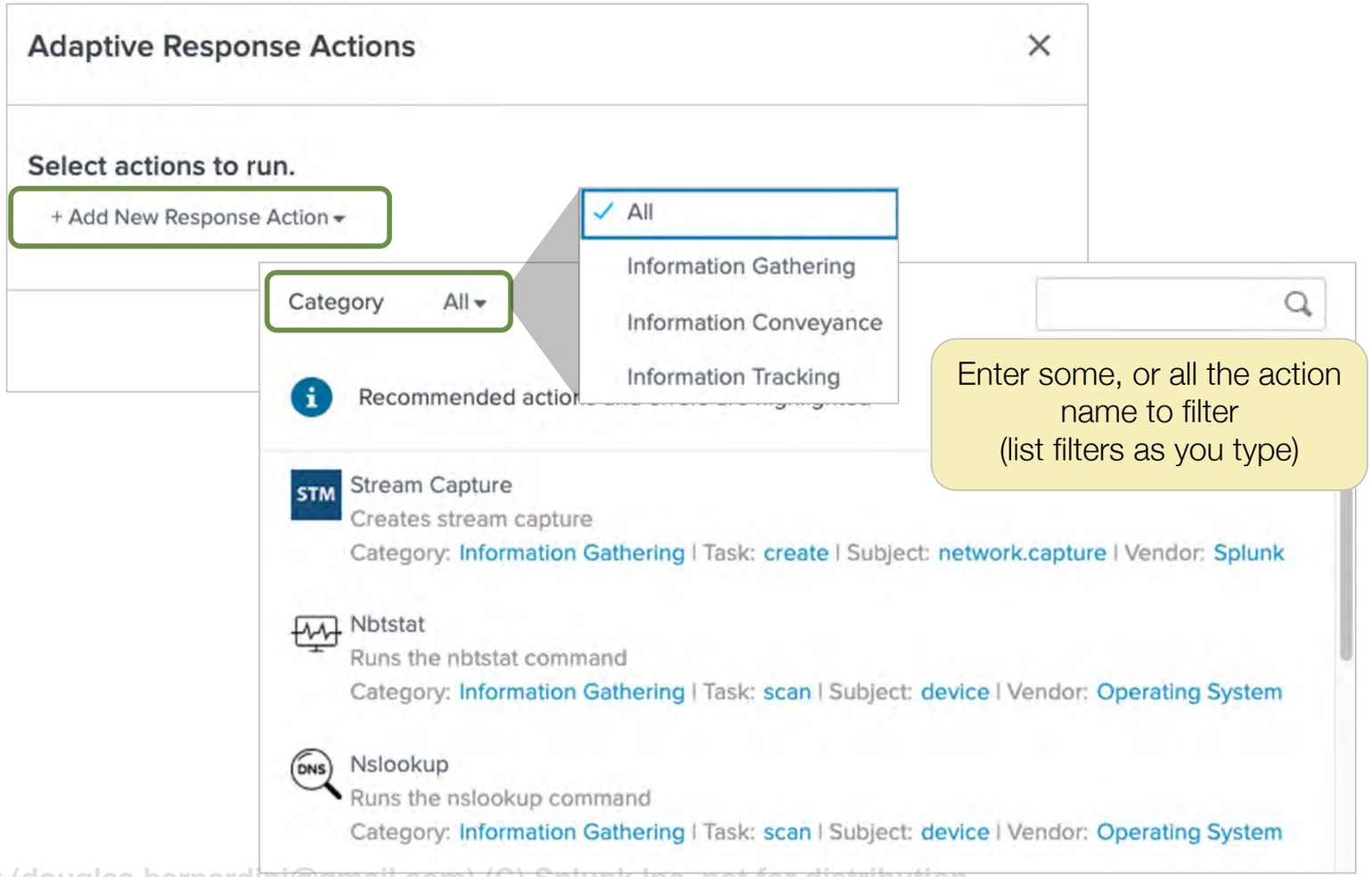
- Notable events may contain further adaptive responses that an analyst can initiate (ping, nslookup, change risk, run script, etc.)
- Depending on the type of notable event, different actions are available
- Use **Actions > Run Adaptive Response Actions** to trigger an action



Triggering Actions

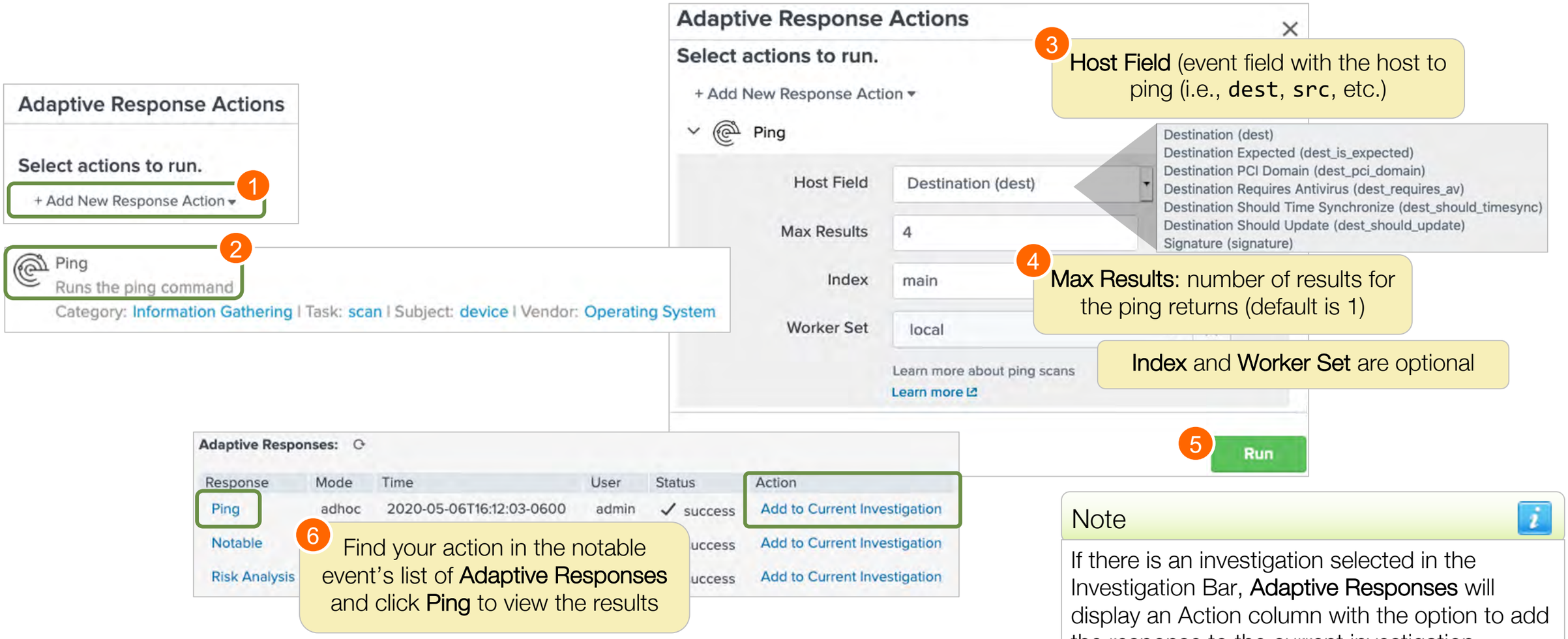
Actions > Run Adaptive Response Actions

- 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



Ping Example

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

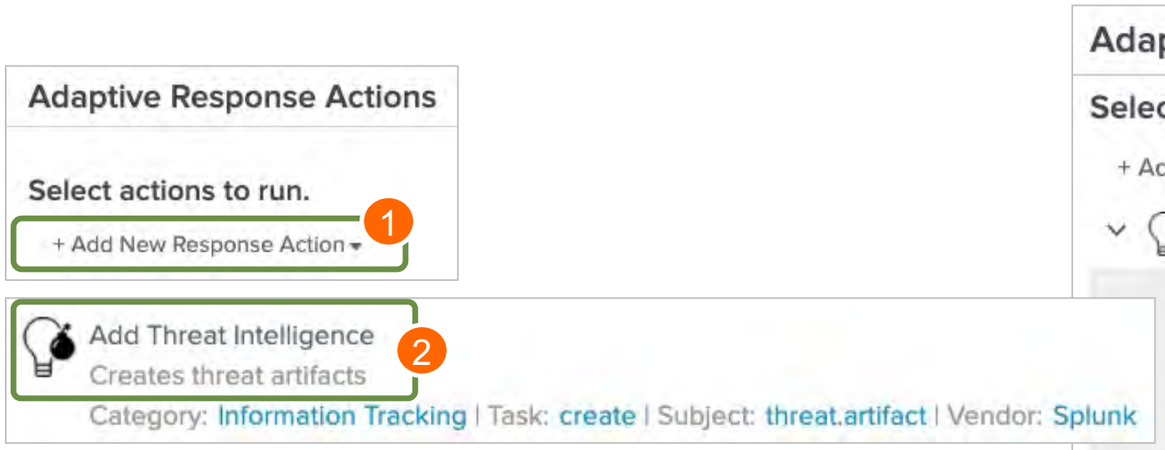


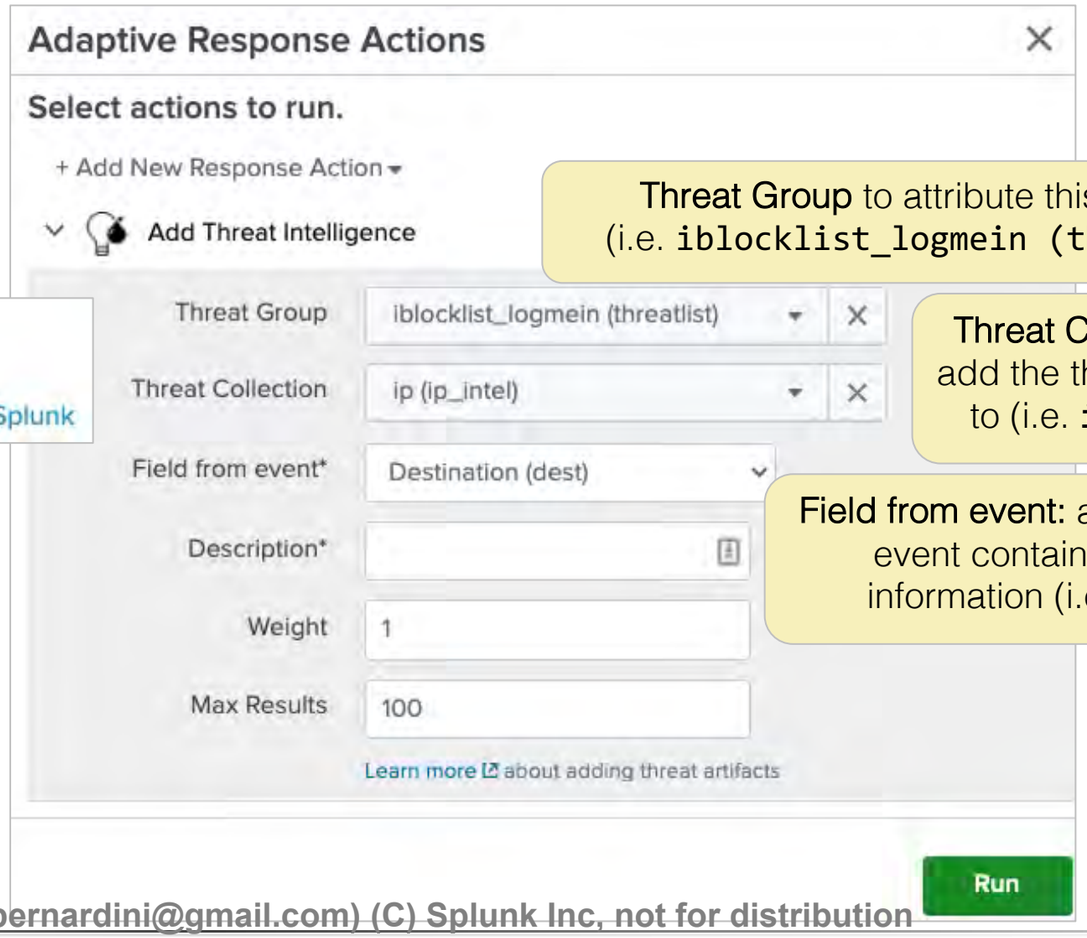
Note

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

Threat Intel Example

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





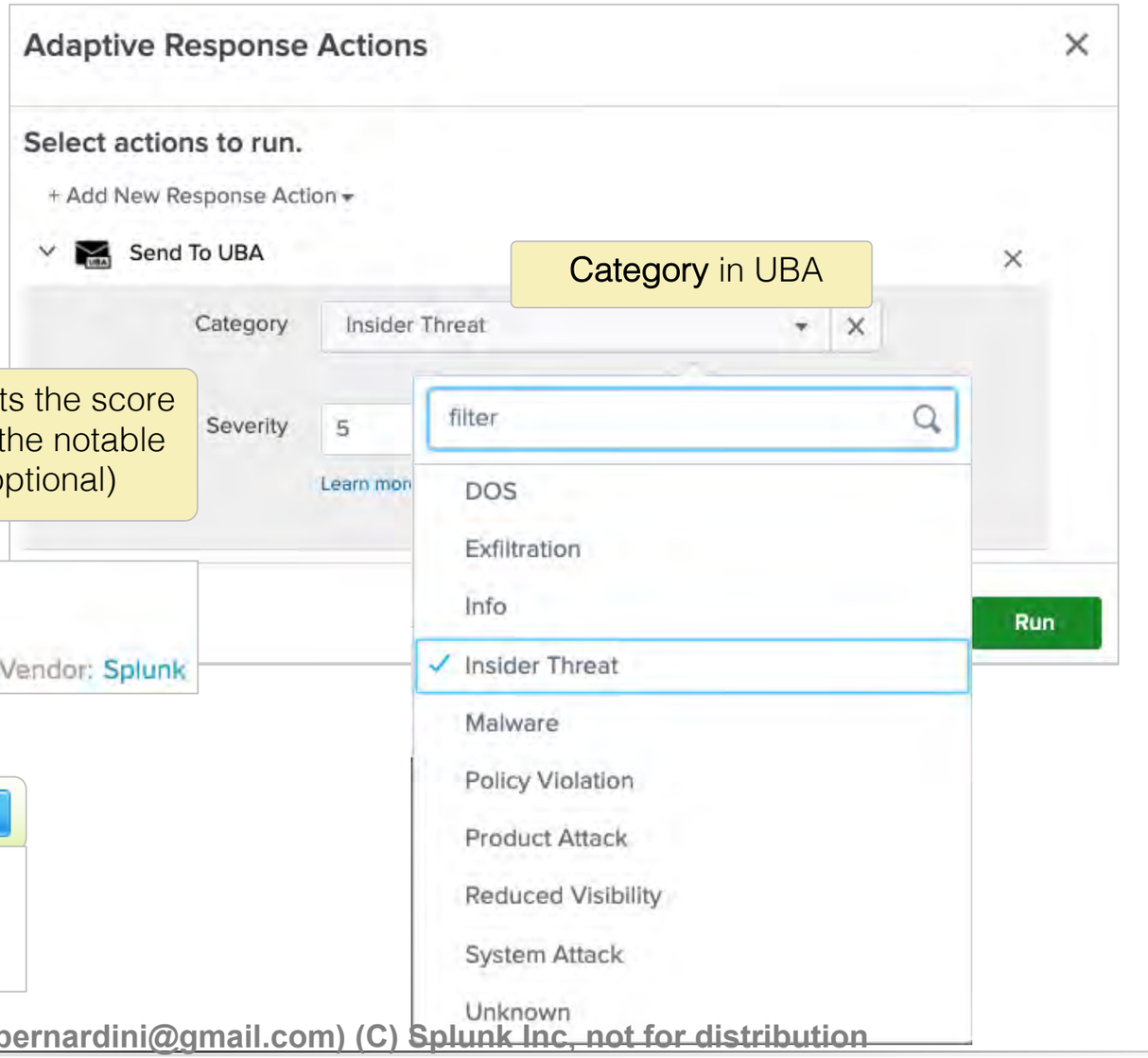
Threat Group to attribute this artifact to (i.e. `iblocklist_logmein (threatlist)`)

Threat Collection to add the threat artifact to (i.e. **`ip_intel`**)

Field from event: a field in the event containing the information (i.e.**`dest`**)

Send to UBA Example

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



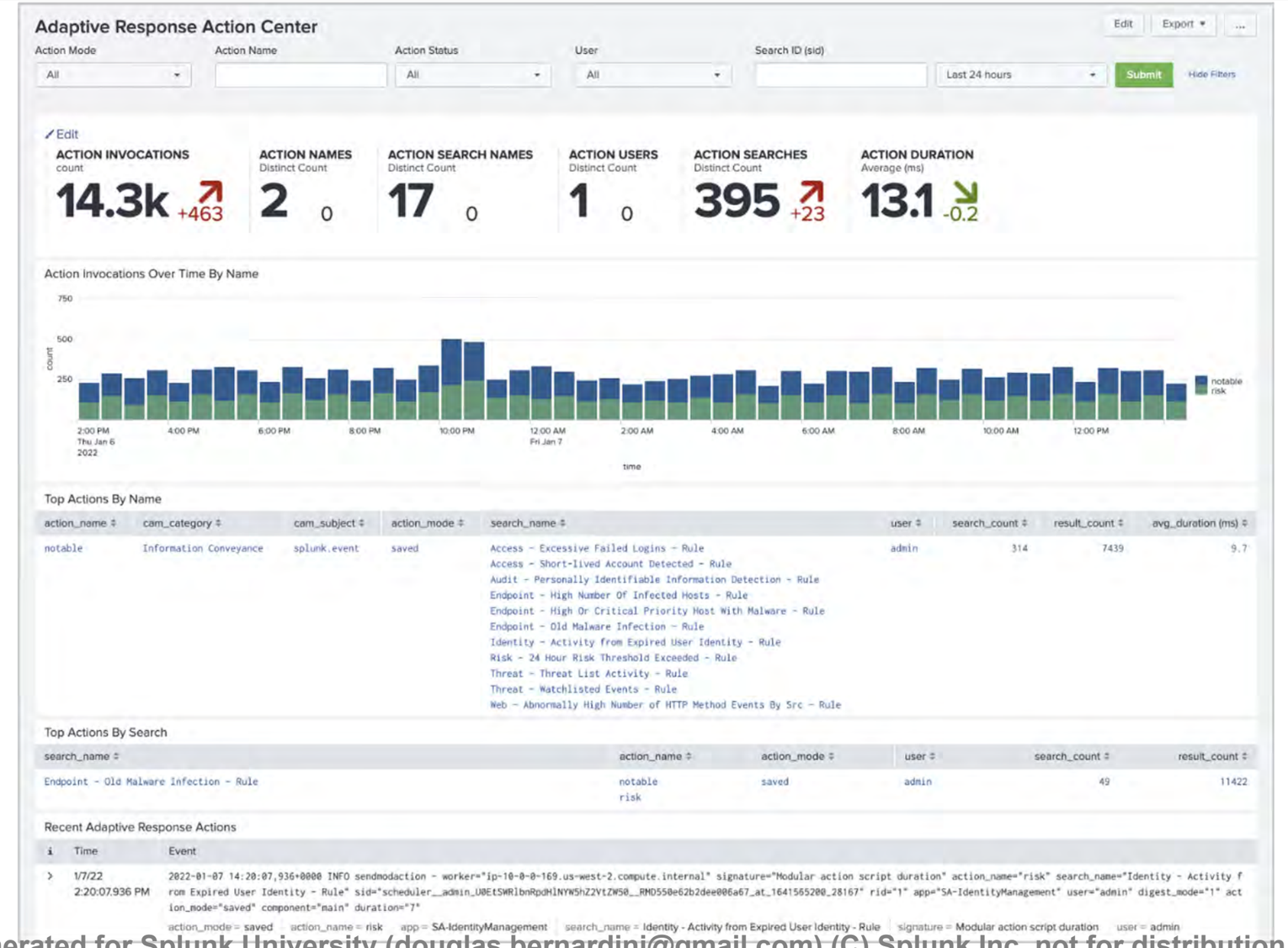
Category in UBA

Severity sets the score in UBA for the notable event (optional)

Note

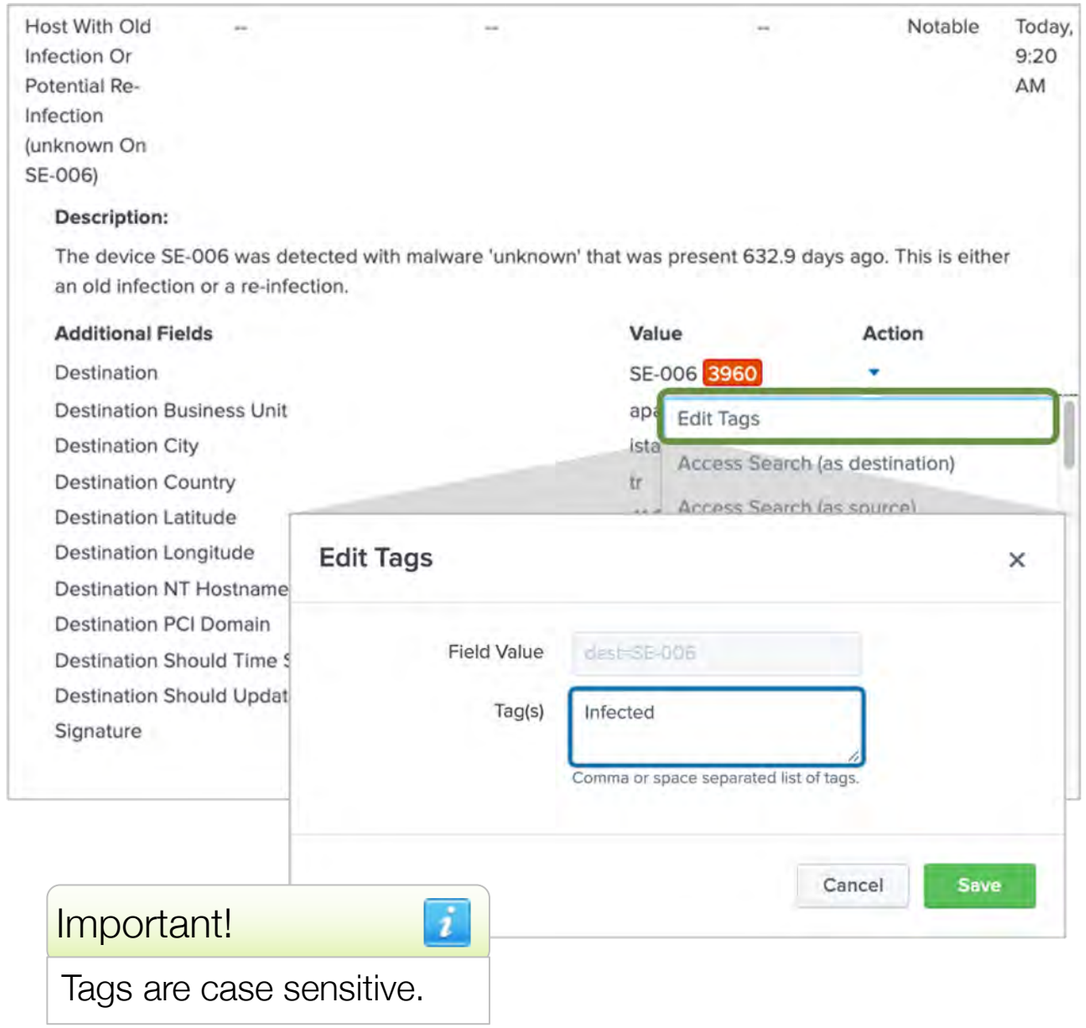
UBA must be installed on the ES search head for this Response Action to be available.

Adaptive Response Action Center



Tagging Incidents

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

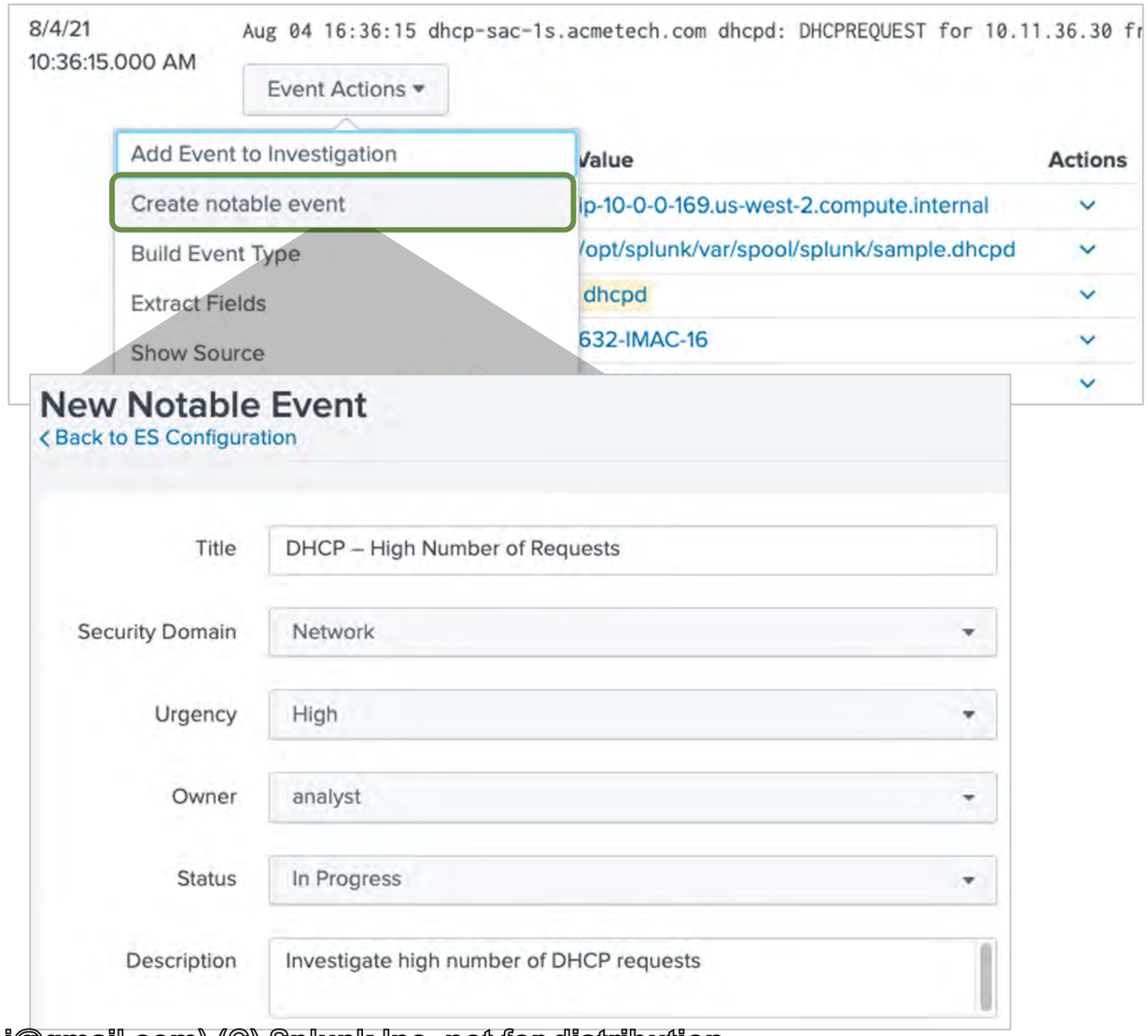


Creating and Suppressing Notable Events

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

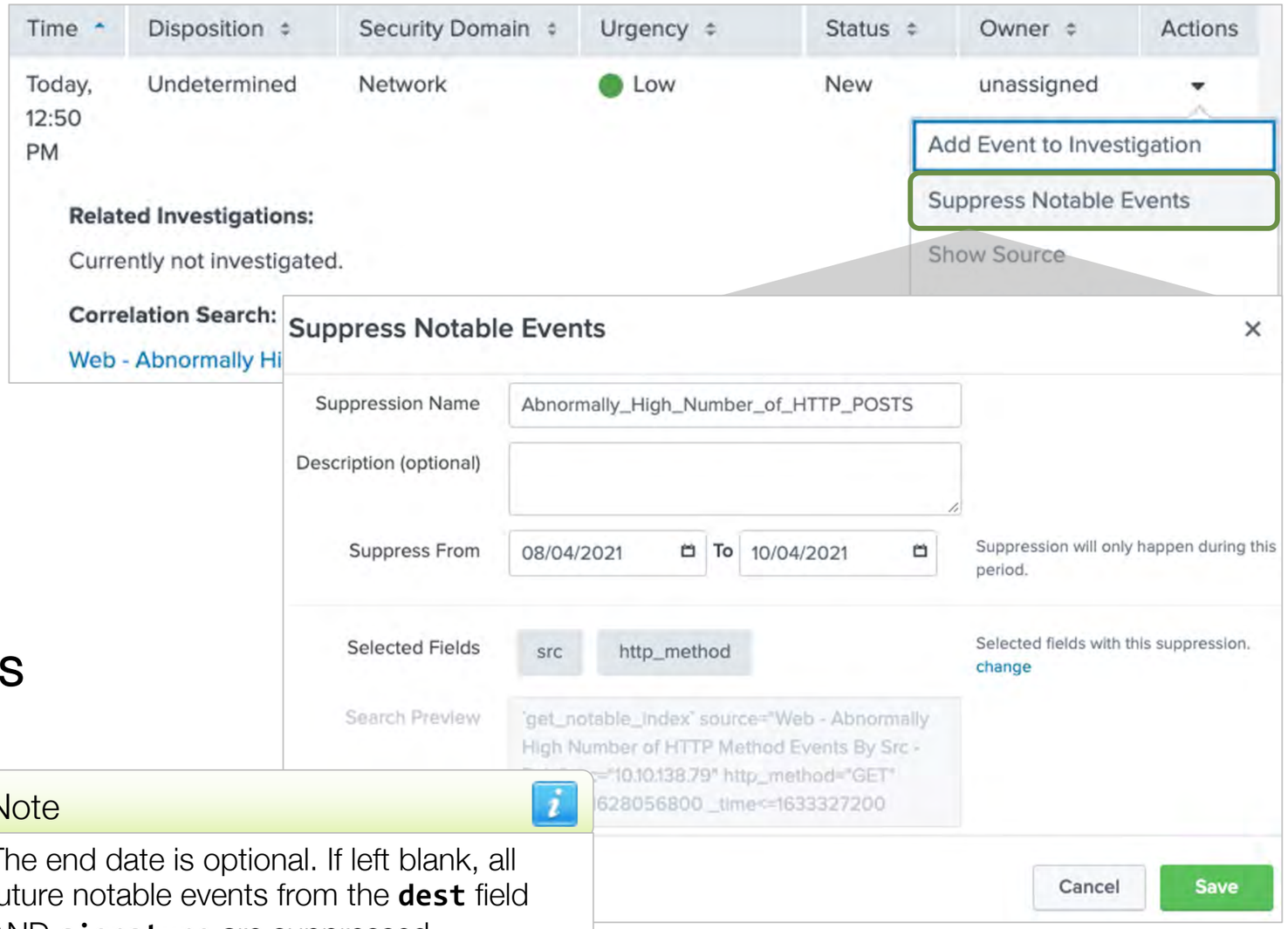
Creating Notable Events

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



Suppressing Notable Events

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



From Incident Review:

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

Note

The end date is optional. If left blank, all future notable events from the **`dest`** field AND **`signature`** are suppressed.

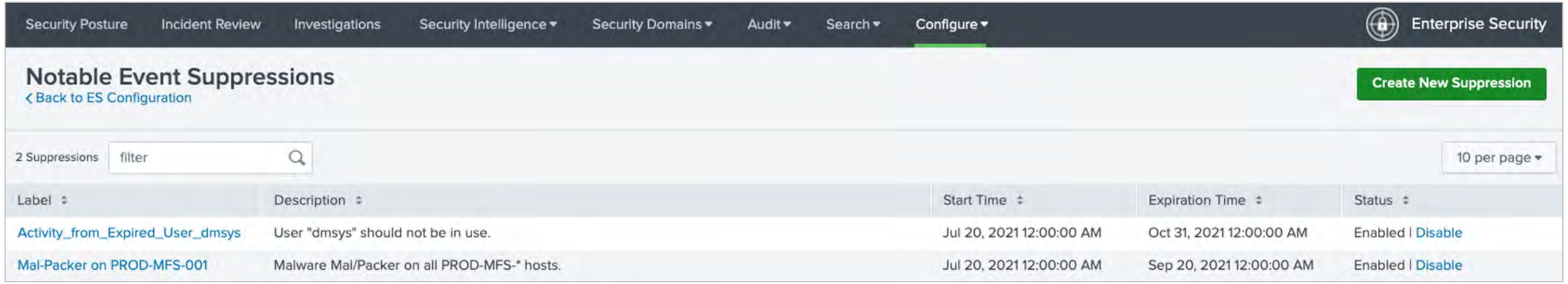
Managing Notable Event Suppressions

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

Important

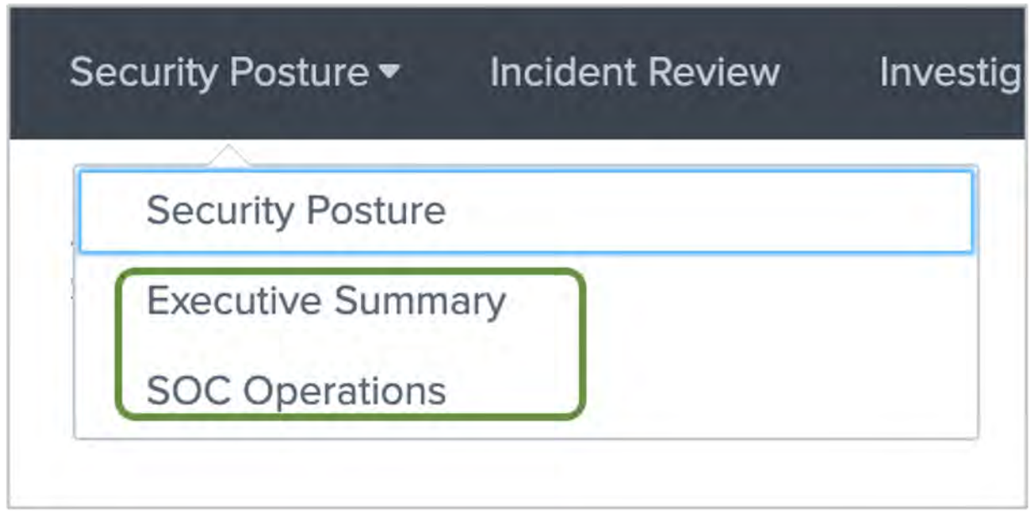
Users with the `ess_analyst` or `ess_user` role must be given the **Edit Notable Event Suppressions** permission to perform these tasks.

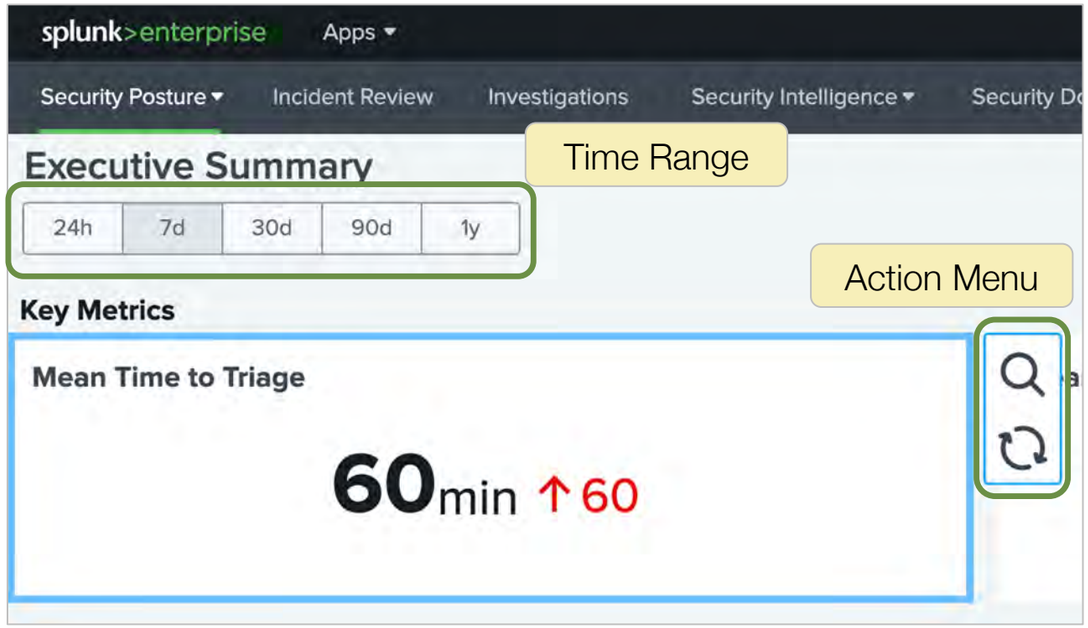
Configure > Incident Management > Notable Event Suppressions



The Executive Summary Dashboards

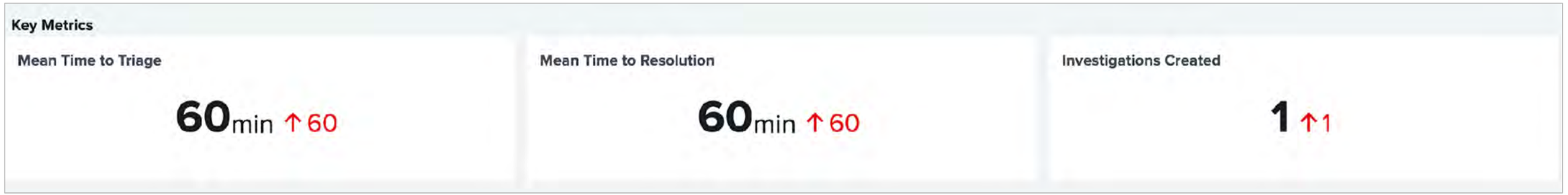
- Select **Executive Summary** or **SOC Operations** dashboards
- Provides summary of data over several time range options
- **Action** menus allow for search and refresh



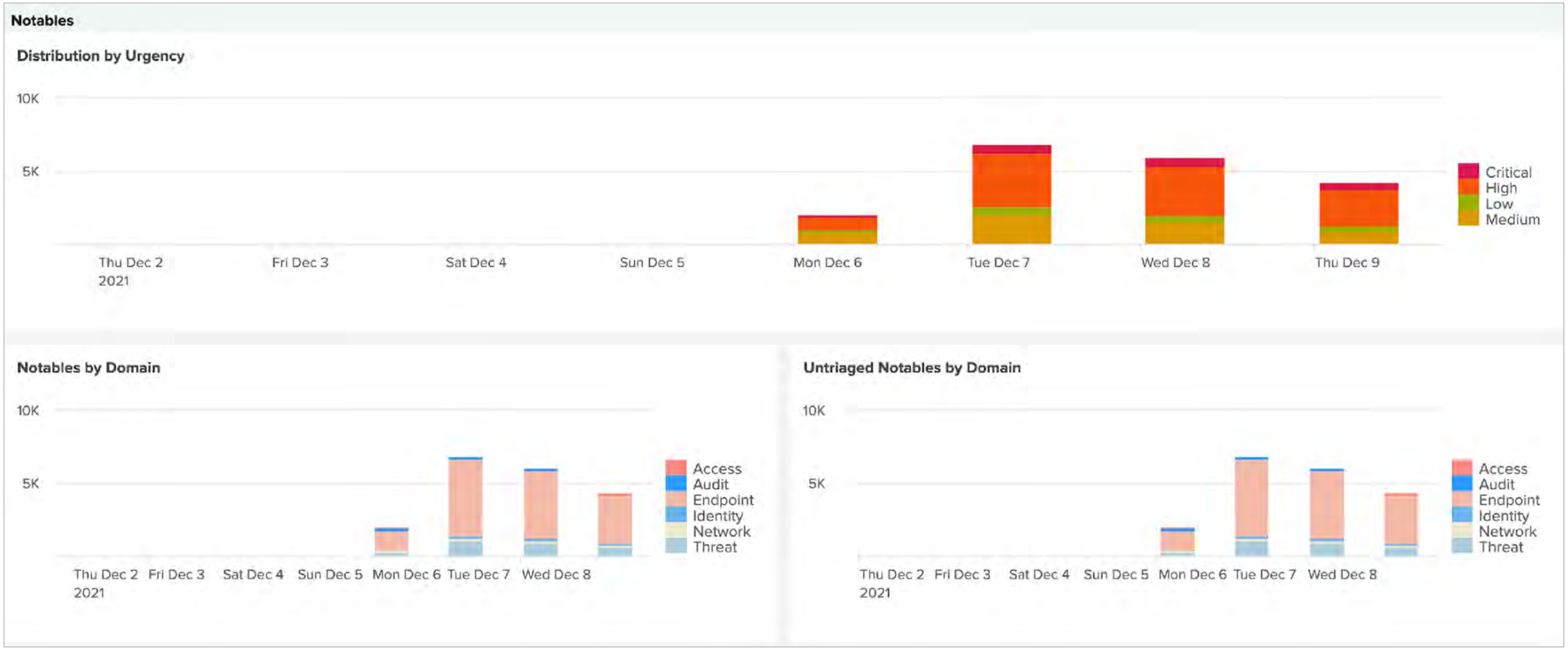


Key Metrics Section

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



Notables Section



Notables Section (cont.)

Top 10 Untriaged Notables by Sources

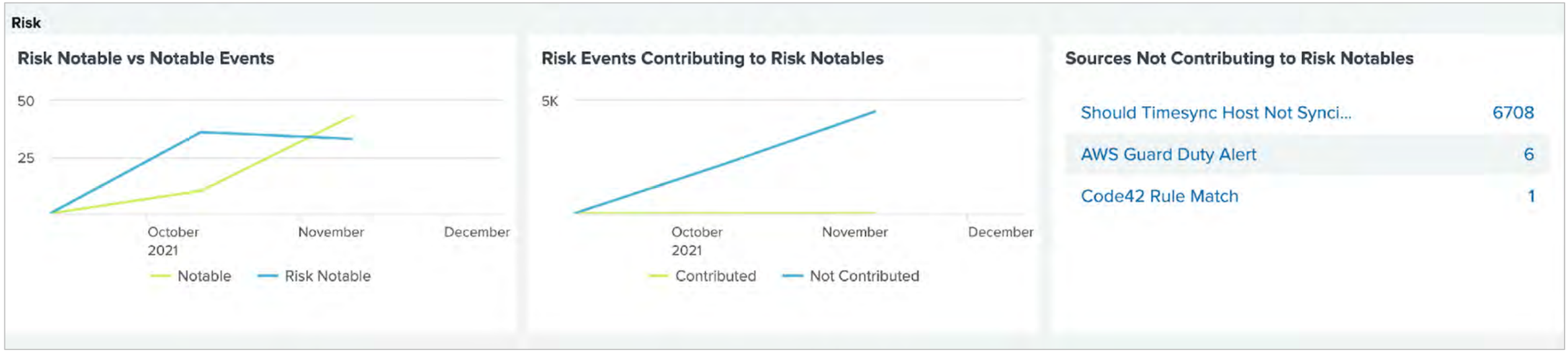
Untriaged Notables by Type

Frequent Notable Event Sources

Rare Notable Event Sources

Risk Section

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

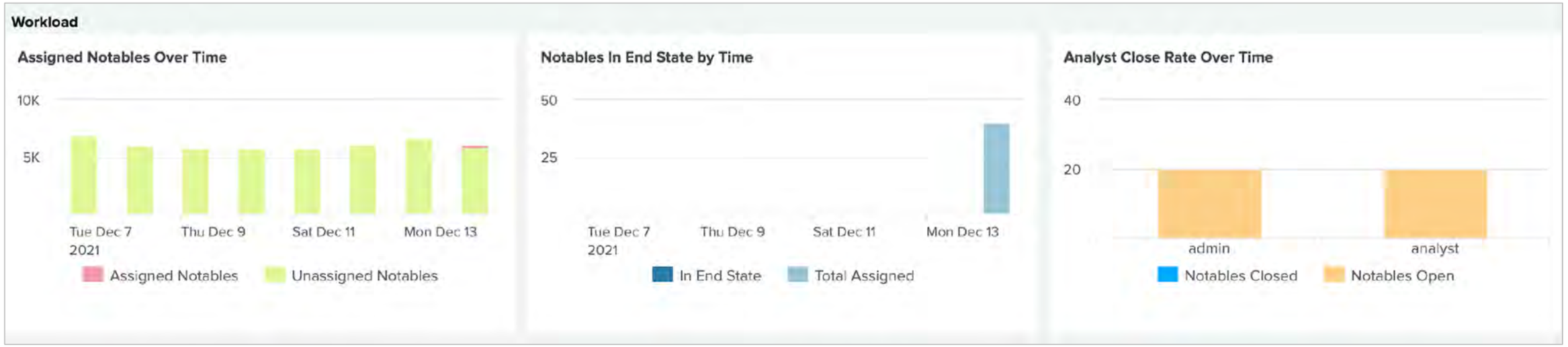


Additional Metrics Section

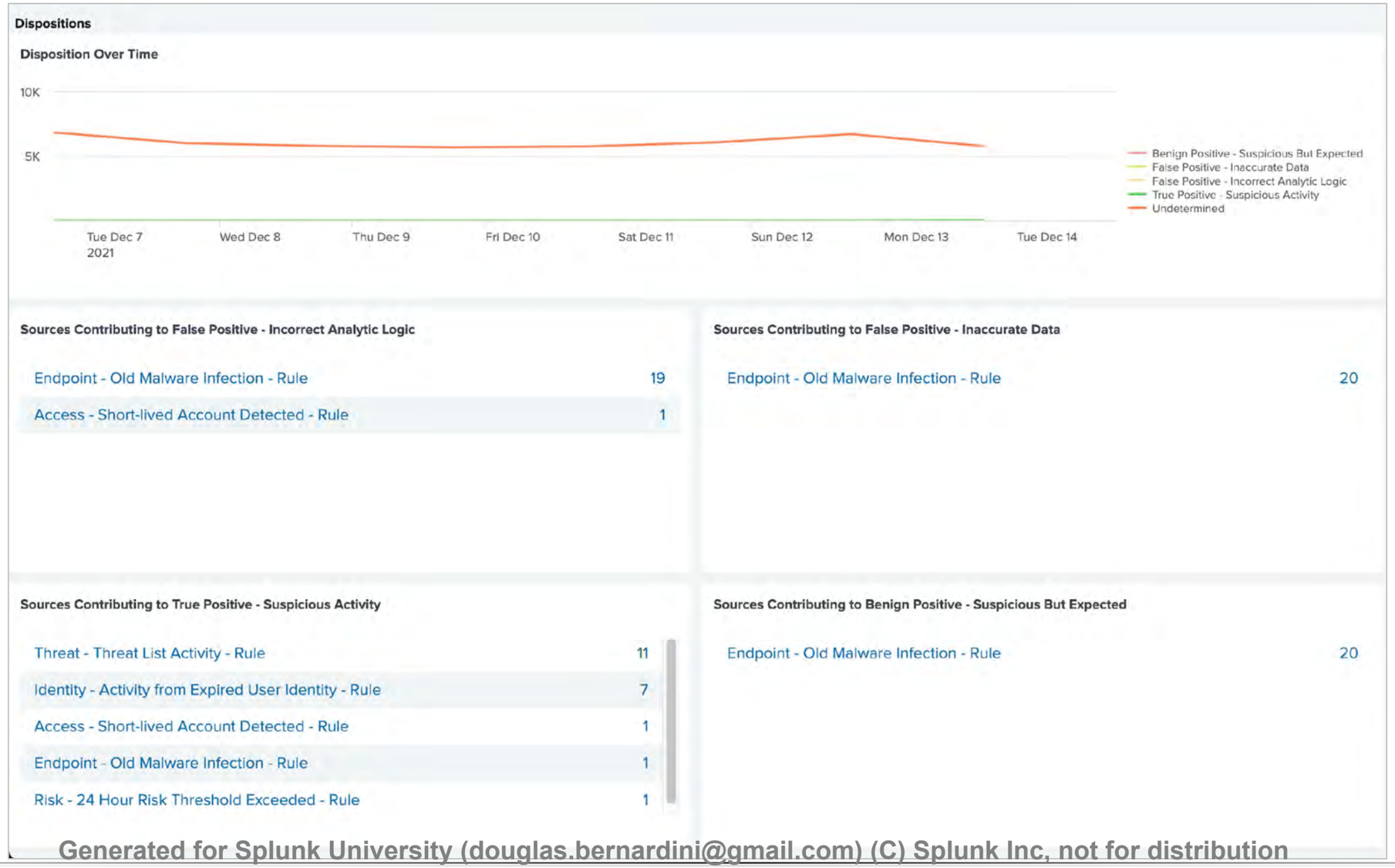
- Displays number of adaptive response actions fired in the system over time
- Shows how many enabled sources have risk actions versus notable actions over time
- Displays distribution of correlation searches enabled versus disabled over time

Workload Section

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

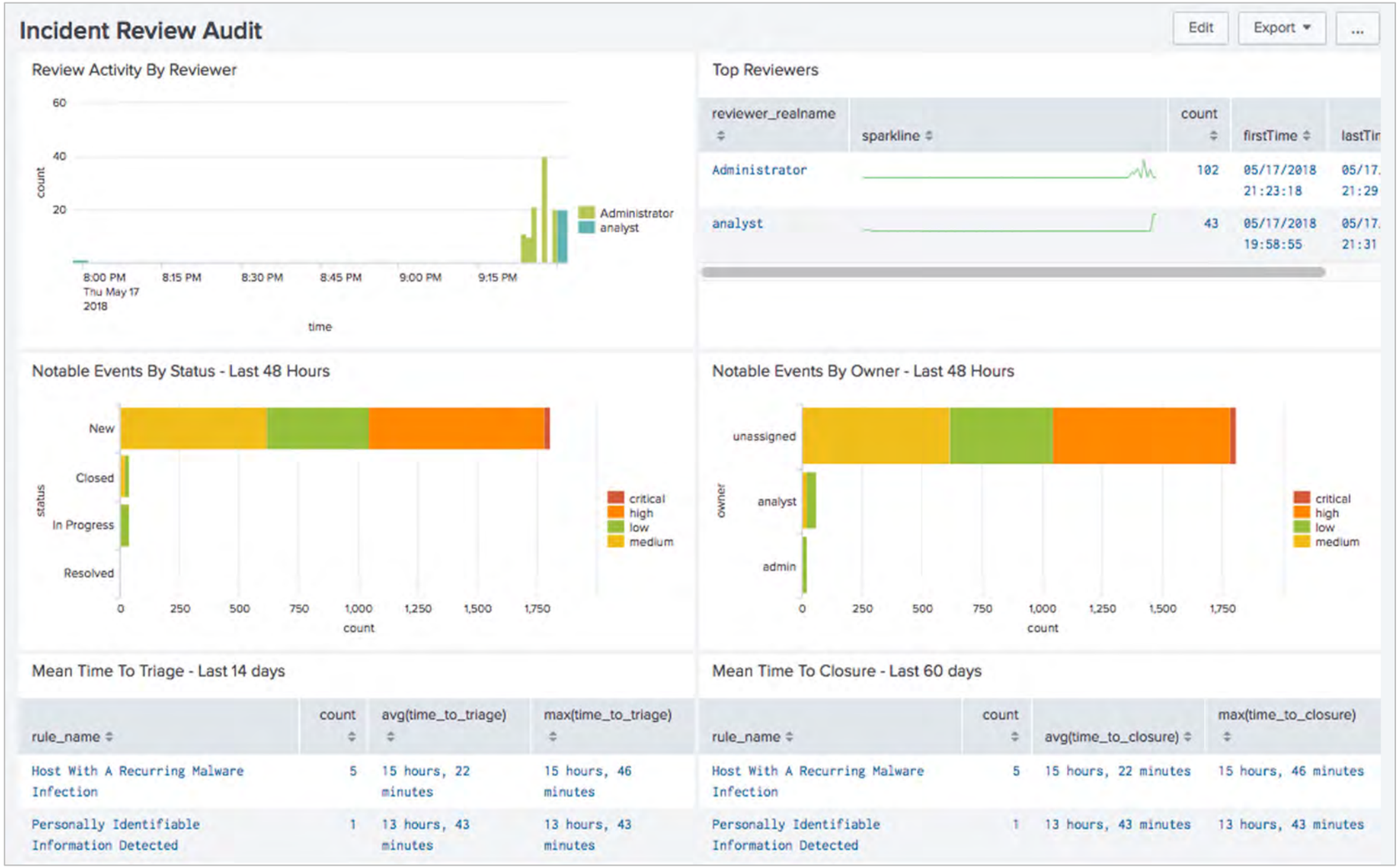


Dispositions Section



Audit > Incident Review Audit

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



Module 2 Lab: Monitoring & Investigating

Time: 30 minutes

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

Tasks:

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

Module 3:
Risk-Based Alerting

Objectives

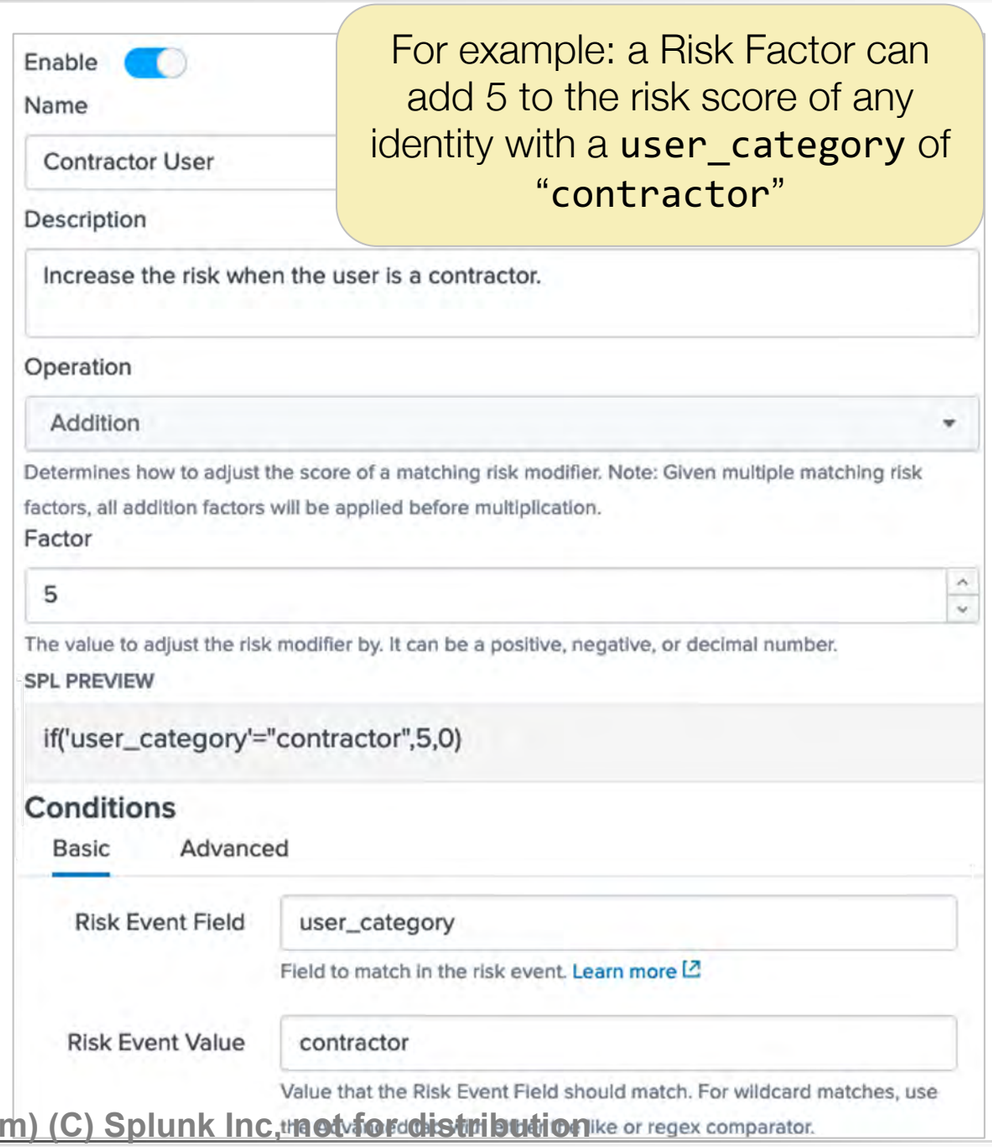
- Give an overview of Risk-Based Alerting
- View Risk Notables and risk information on the Incident Review dashboard
- Explain risk scores and how to change an object's risk score
- Review the Risk Analysis dashboard
- Describe annotations

Risk Overview

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

Risk Overview (cont.)

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



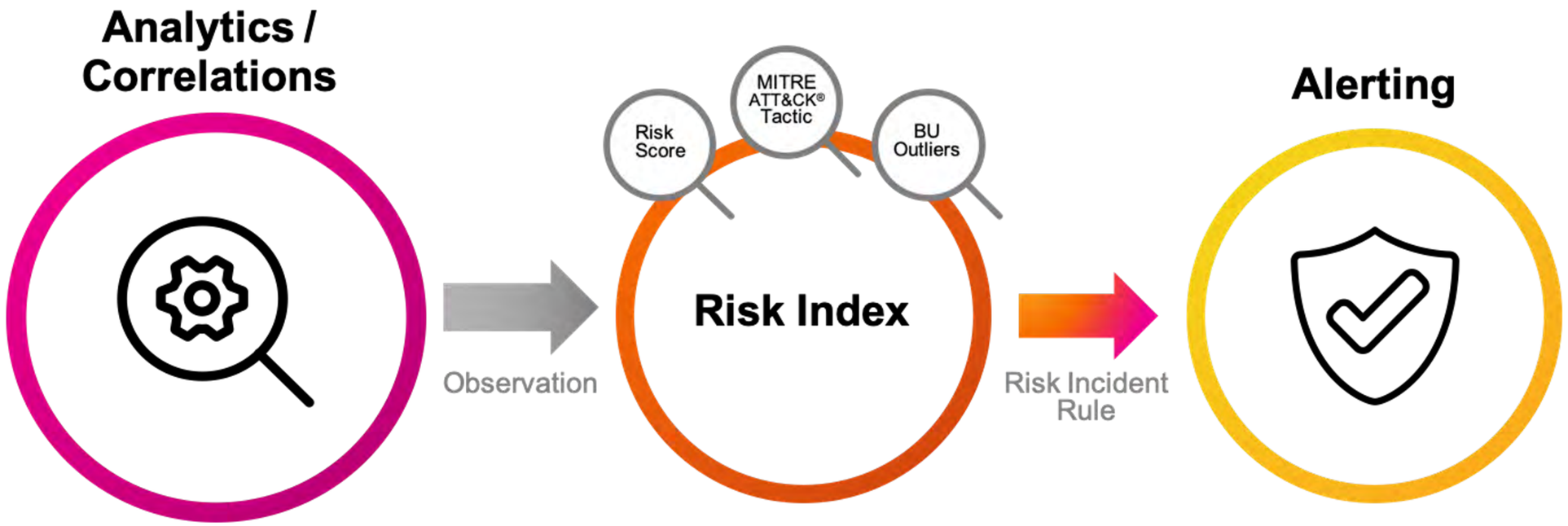
Risk Activity Examples

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

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

Risk Framework



Create risk rules (Risk Analysis adaptive response action) to create risk attributions for entities when something suspicious happens. Instead of triggering an alert, risk attributions are sent to the **`risk`** index

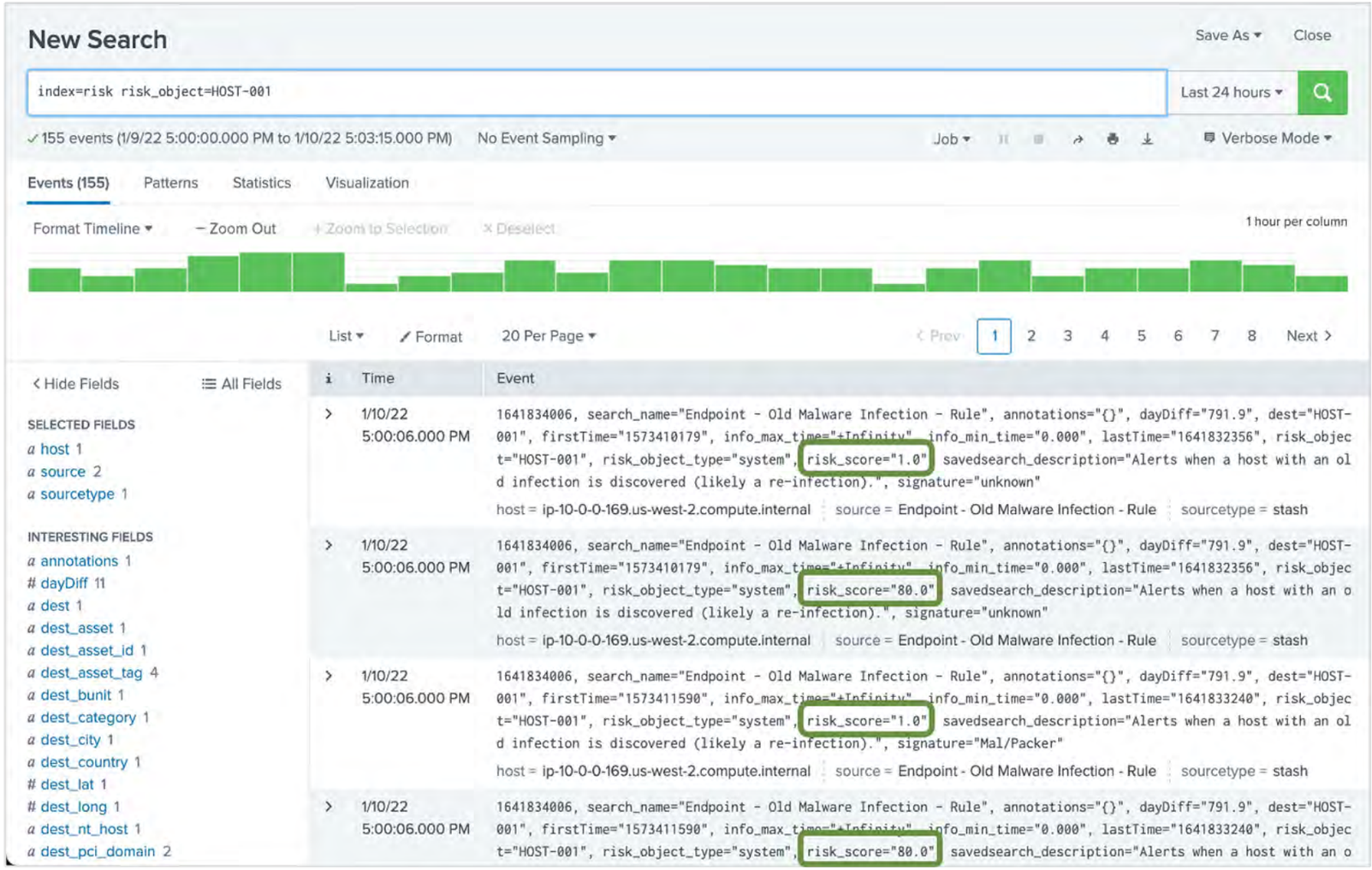
Enrich risk attributions by appending relevant context like a risk score or a MITRE ATT&CK technique

A risk incident rule (risk correlation search) creates a risk notable when an entity's risk score or behavioral pattern meets the predetermined threshold in the correlation search

Risk Rules

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

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

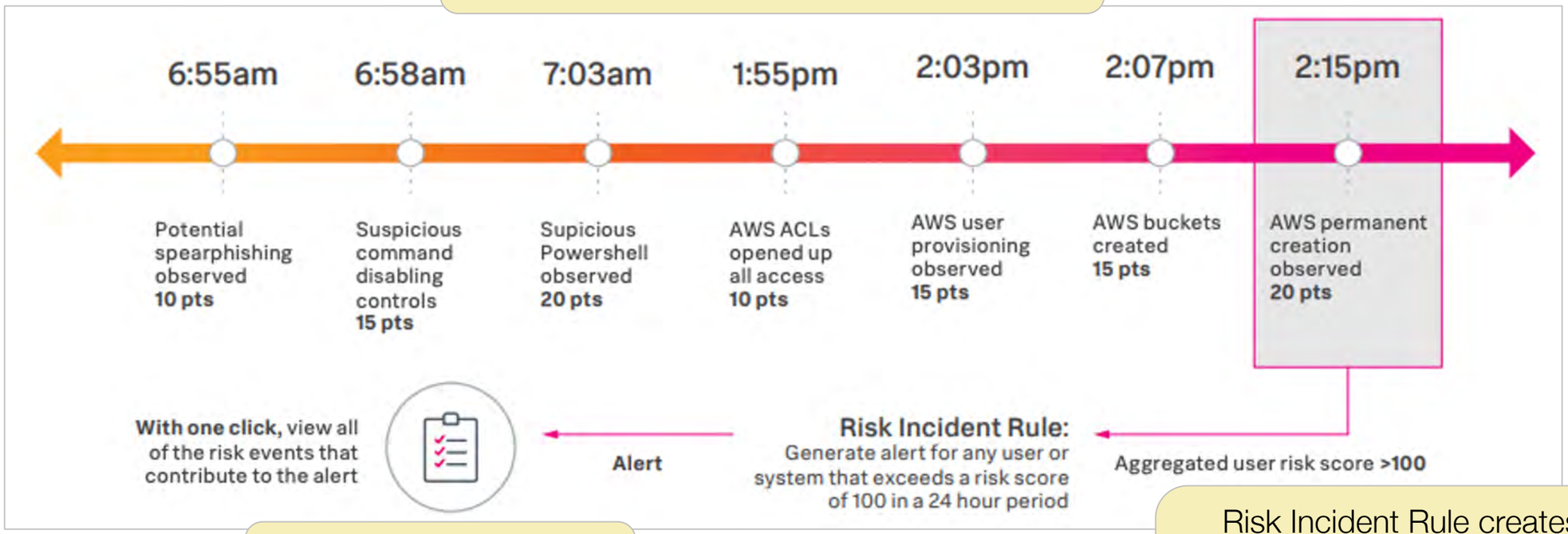


Risk Correlation Searches

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

Risk-Based Alerting Example

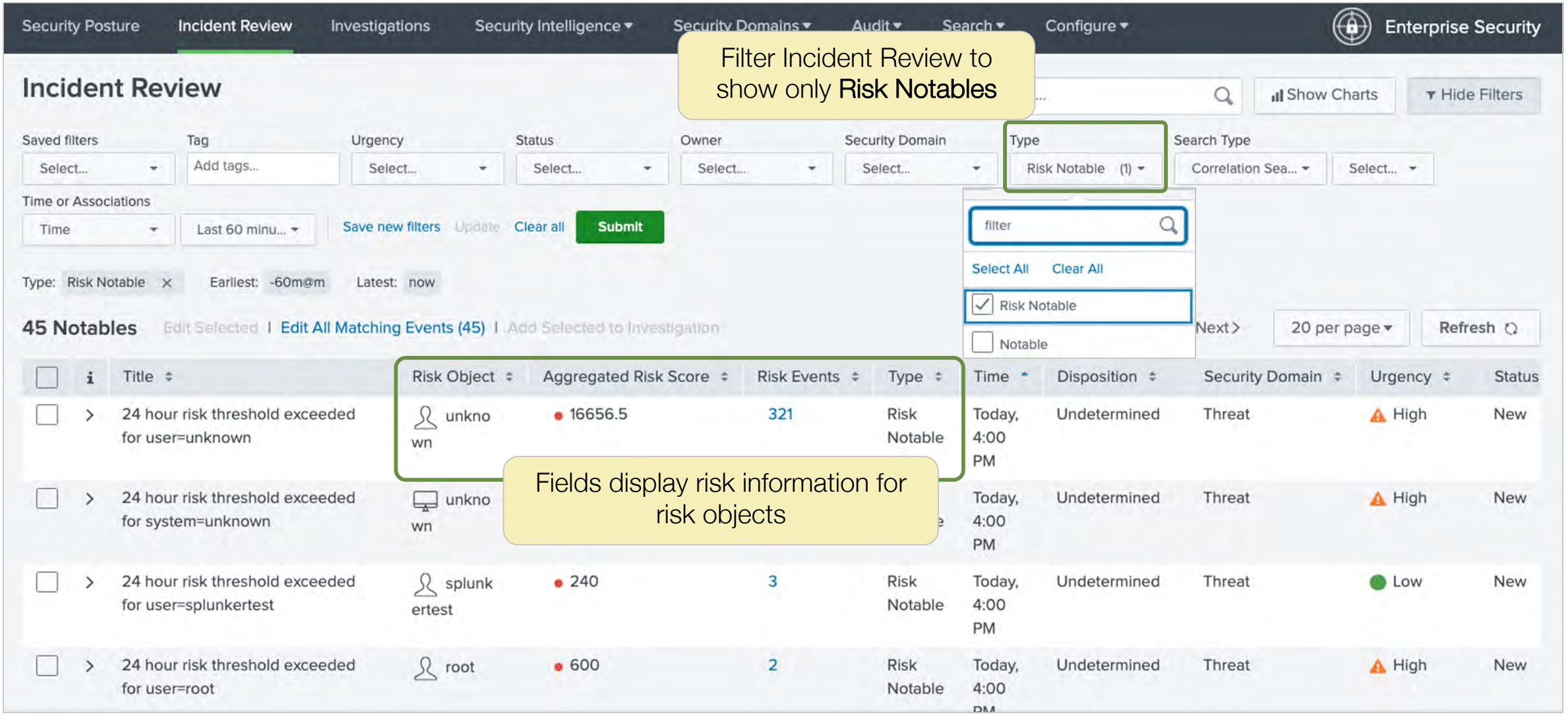
"Risk attributions" (risk score changes) along the timeline are put into the **`risk`** index



Use **Incident Review** to view the Risk Notable

Risk Incident Rule creates a Risk Notable due to the risk score of the user exceeding 100 over a 24-hour period

Risk Notables



Risk Notable Details

Title	Risk Object	Aggregated Risk Score	Risk Events	Type
24 hour risk threshold exceeded for system=PROD-POS-005	PROD-POS-005	720	9	Risk Notable

Click **Risk Events** to view the details

Risk Events

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

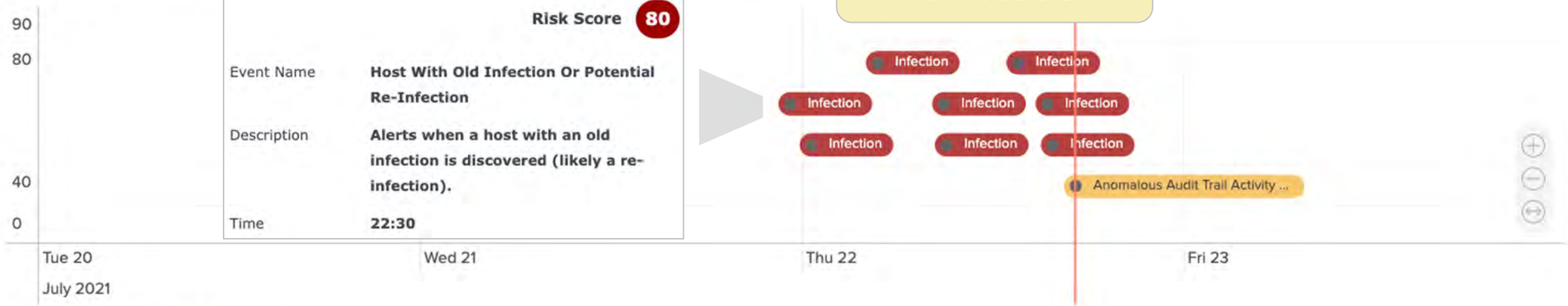
Click an individual event for the details

Risk Score 80

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

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

Time: **22:30**



Contributing Risk Events

filter

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

Expand for details

 | 25 May 2022

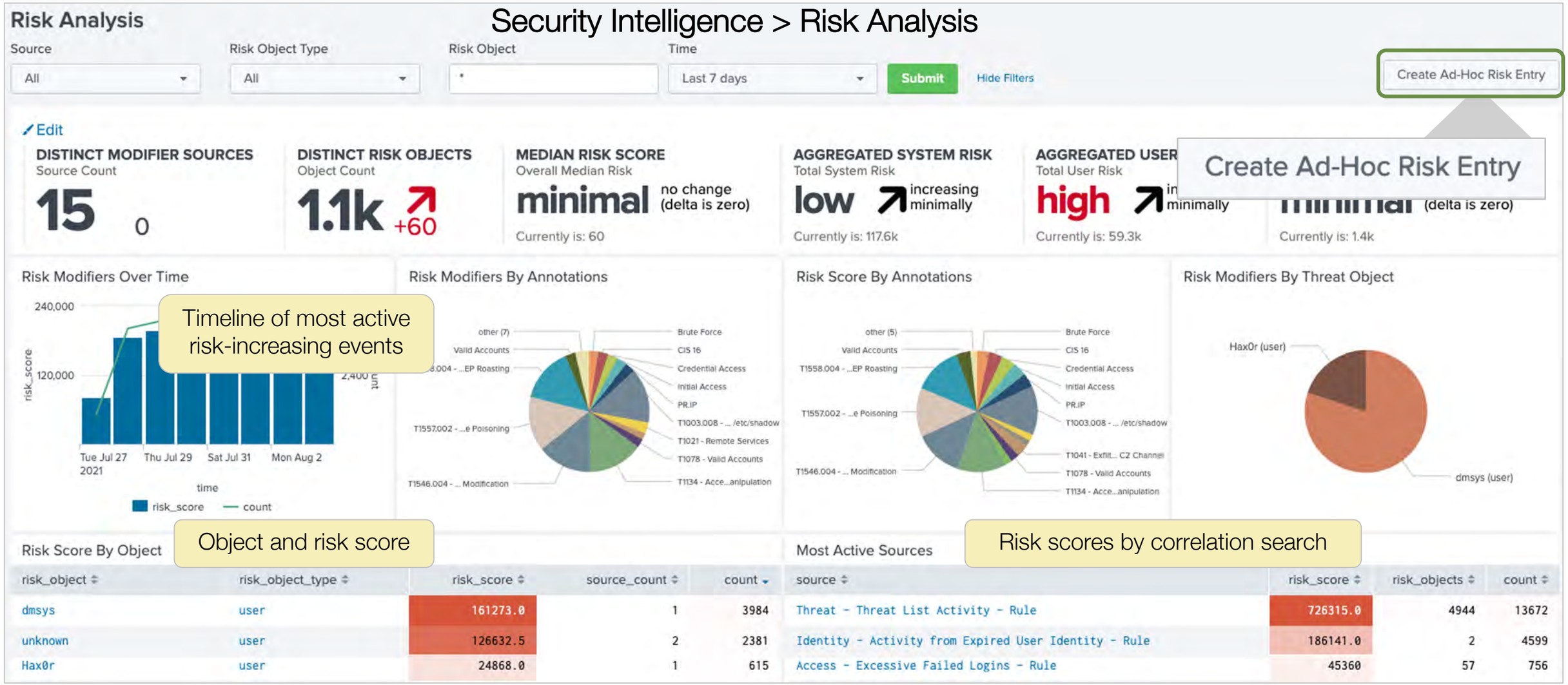
Risk Analysis Example

A priority firewall server is attacked periodically over time

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

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

Risk Analysis Dashboard

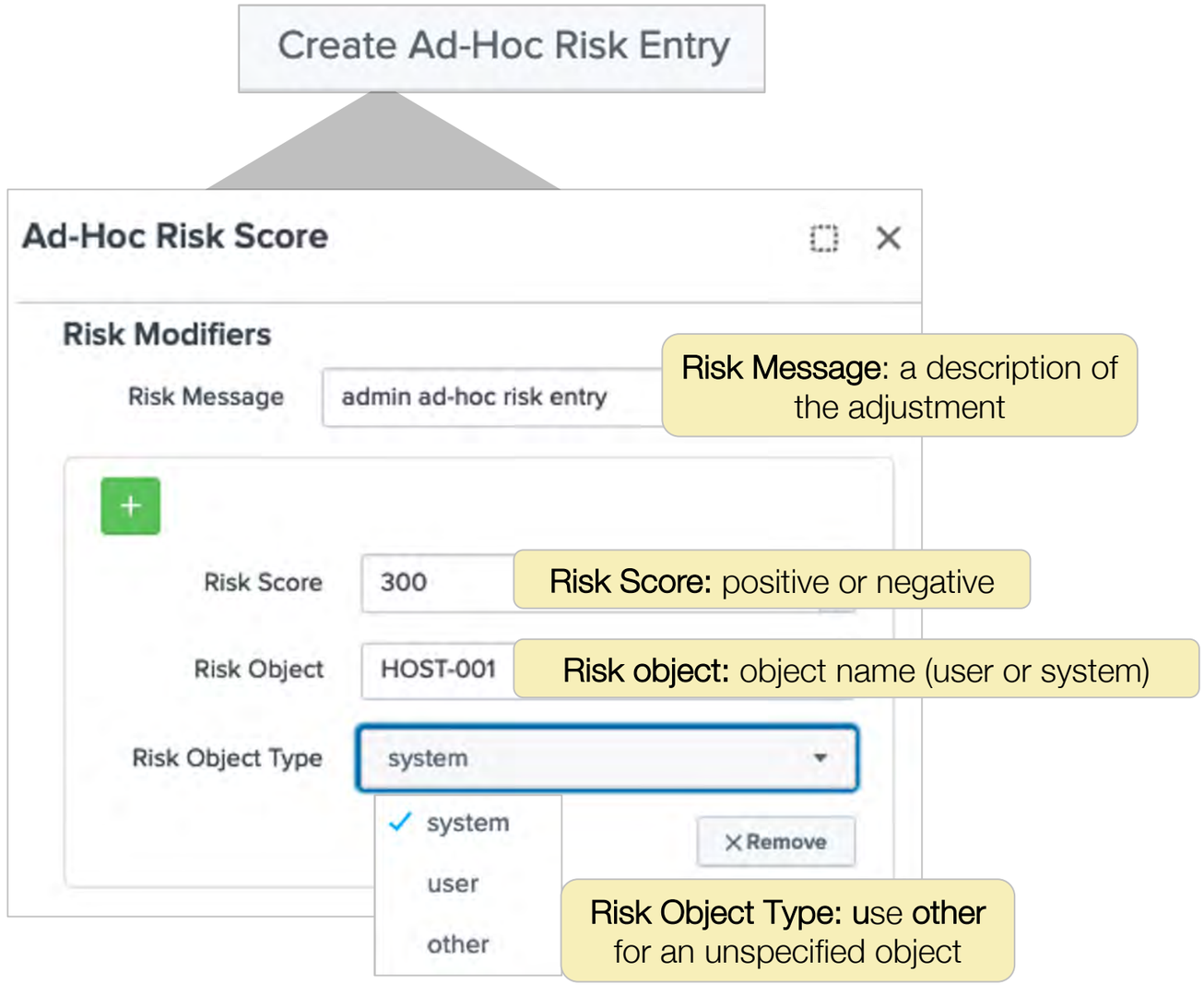


risk_object	risk_object_type	risk_score	source_count	count
dmsys	user	161273.0	1	3984
unknown	user	126632.5	2	2381
Hax0r	user	24868.0	1	615

source	risk_score	risk_objects	count
Threat - Threat List Activity - Rule	726315.0	4944	13672
Identity - Activity from Expired User Identity - Rule	186141.0	2	4599
Access - Excessive Failed Logins - Rule	45360	57	756

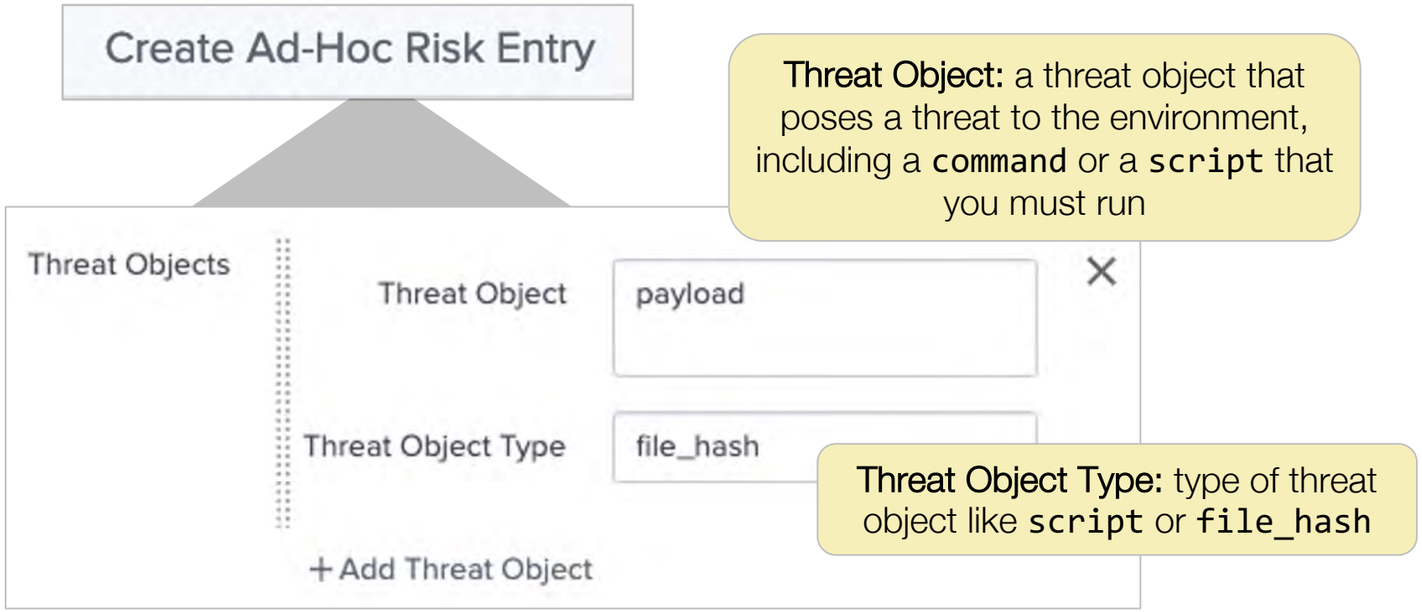
Ad-hoc Risk Entry

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



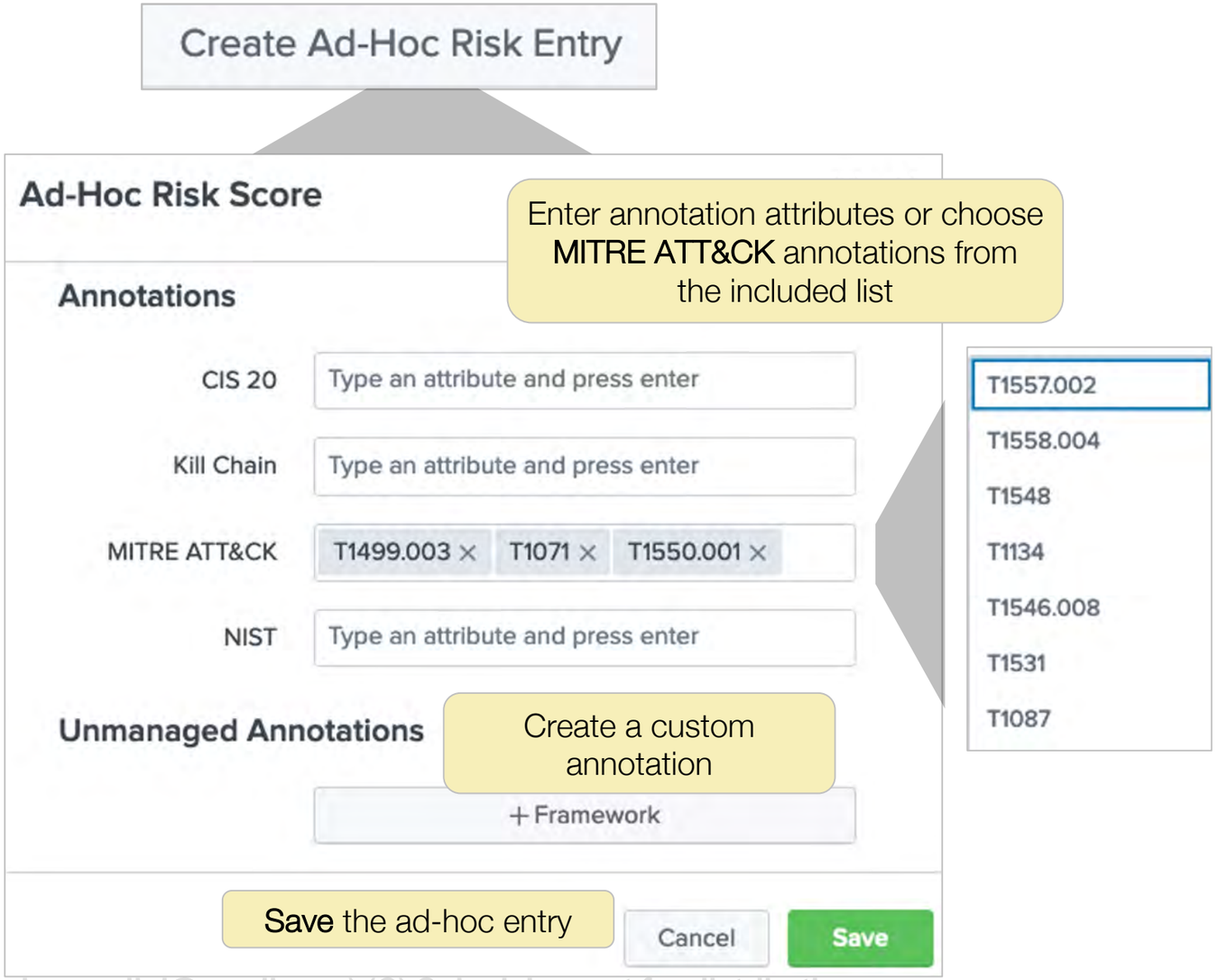
Ad-hoc Risk Entry – Threat Objects

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



Ad-hoc Risk Entry - Annotations

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



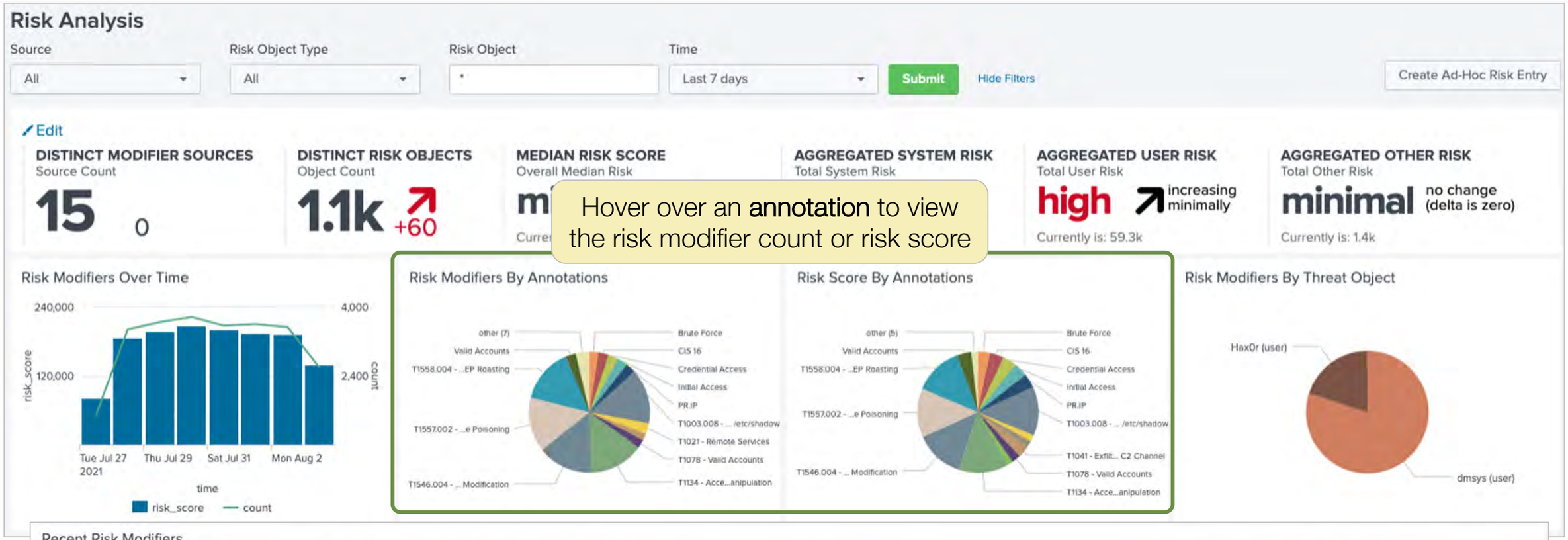
Annotations

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

Example industry-standard mappings:

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

View Annotation Details



Recent Risk Modifiers

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

Module 3 Lab: Risk-Based Alerting

Time: 25 minutes

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

Tasks:

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

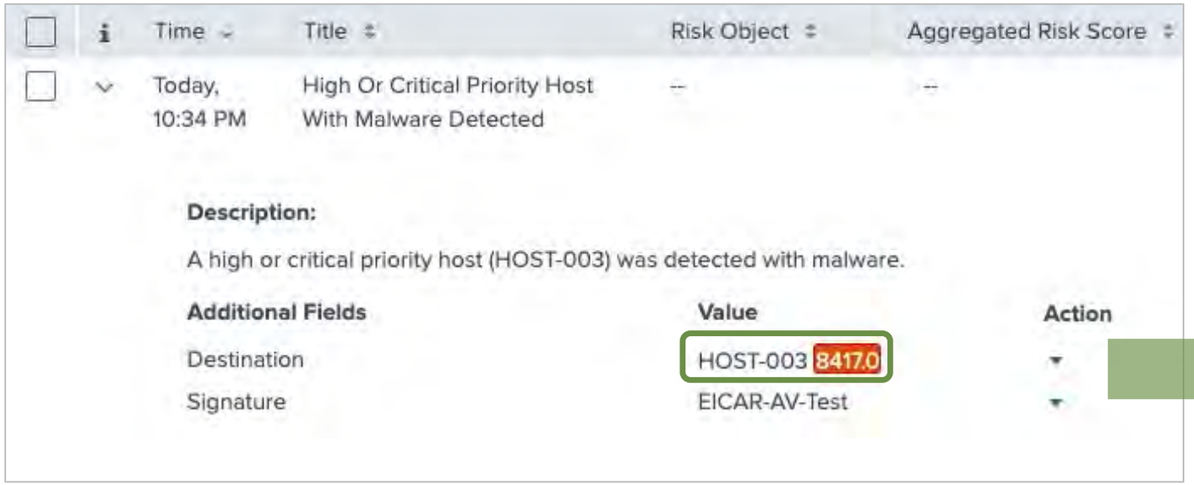
Module 4:
Assets & Identities

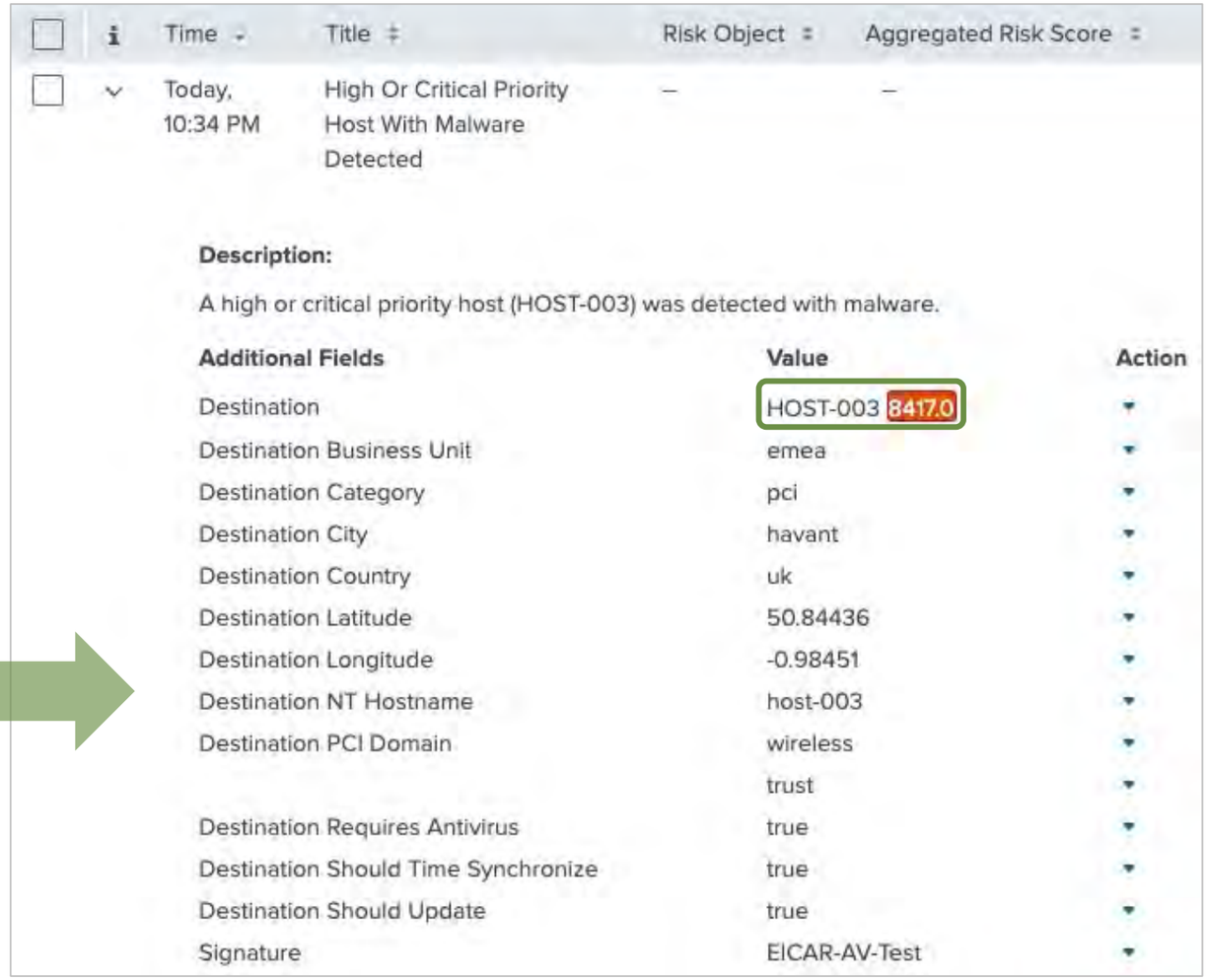
Objectives

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

Assets & Identities Overview

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

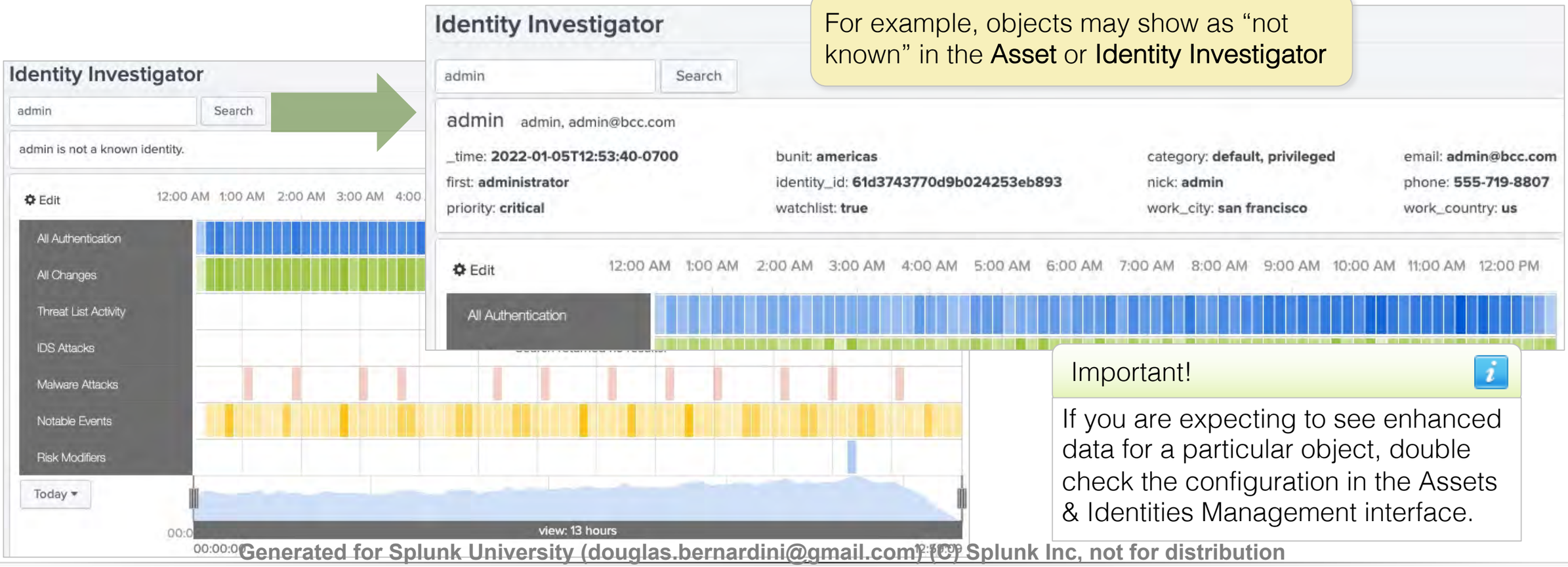




ES admins add the enhanced data for assets and identities to ES in lookup tables

Missing Data Example 1

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

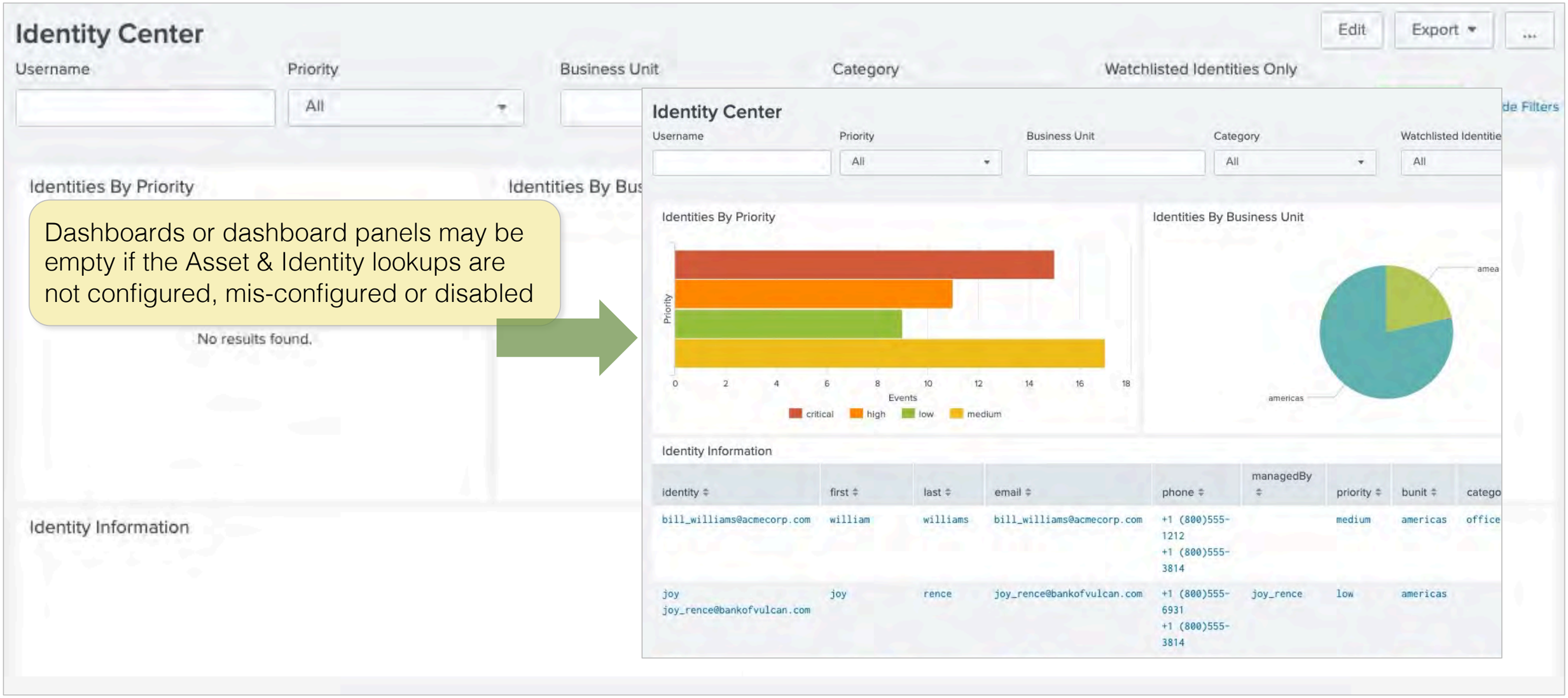


For example, objects may show as “not known” in the **Asset** or **Identity Investigator**

Important!

If you are expecting to see enhanced data for a particular object, double check the configuration in the Assets & Identities Management interface.

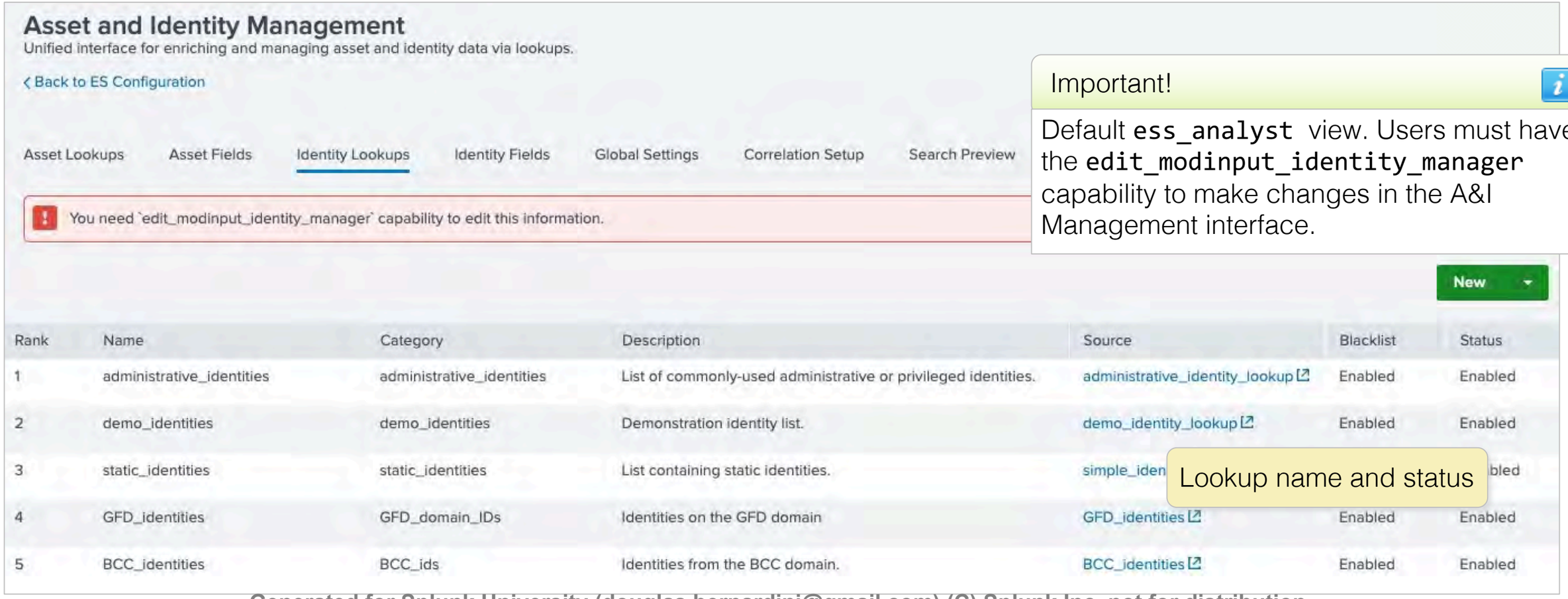
Missing Data Example 2



Dashboards or dashboard panels may be empty if the Asset & Identity lookups are not configured, mis-configured or disabled

Asset & Identity Management Interface

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



Important!

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

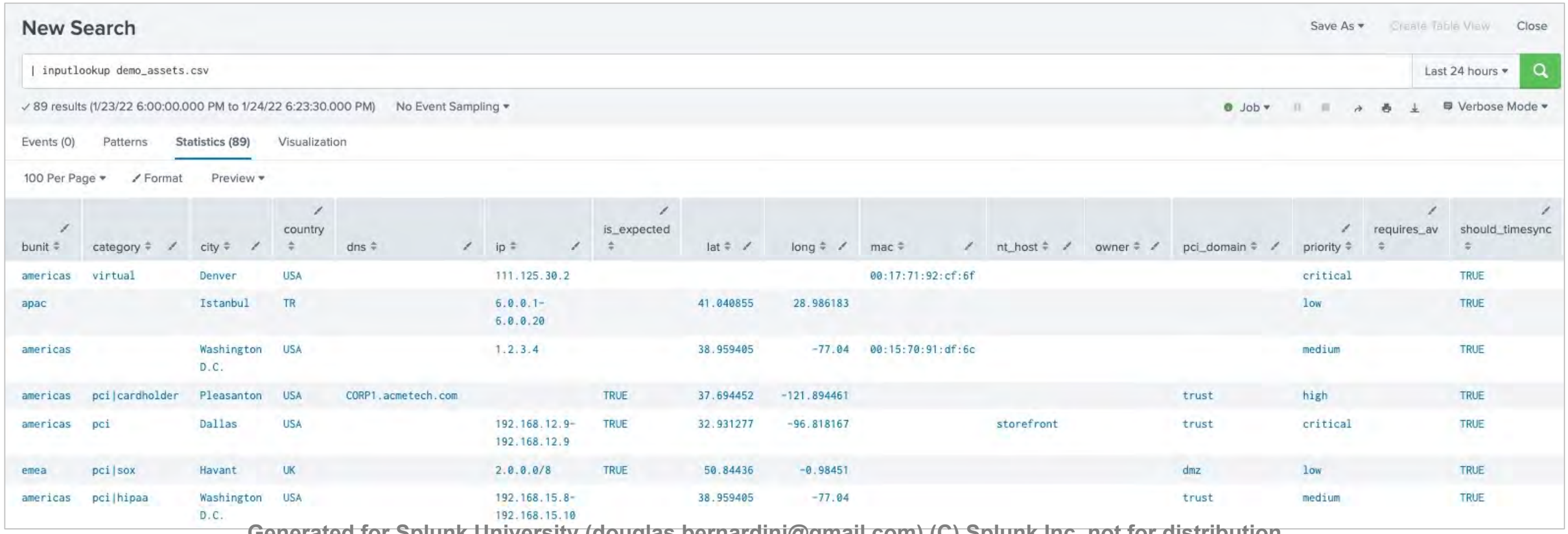
Lookup name and status

View Asset & Identity Lookups

- View the contents of a lookup table using `| inputlookup`

For Example:

```
| inputlookup demo_identities.csv
| inputlookup demo_assets.csv
```

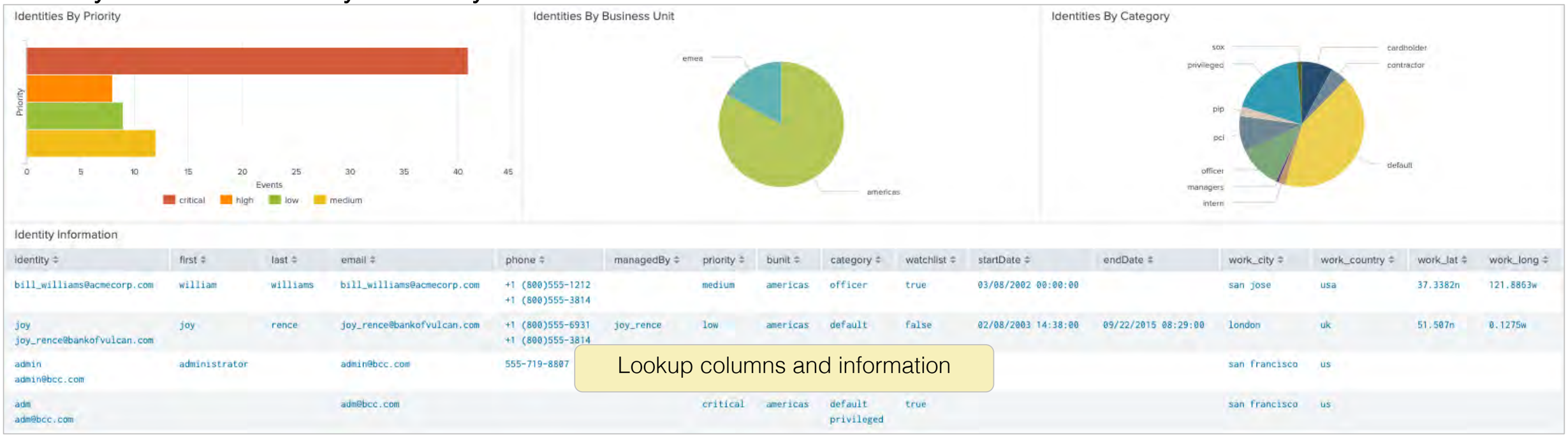


bunit	category	city	country	dns	ip	is_expected	lat	long	mac	nt_host	owner	pci_domain	priority	requires_av	should_timesync
americas	virtual	Denver	USA		111.125.30.2				00:17:71:92:cf:6f				critical		TRUE
apac		Istanbul	TR		6.0.0.1-6.0.0.20		41.040855	28.986183					low		TRUE
americas		Washington D.C.	USA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

Identity Center & Asset Center Dashboards

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

Security Domains > Identity > Identity Center



Module 5: Investigations

Objectives

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

Investigations

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

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

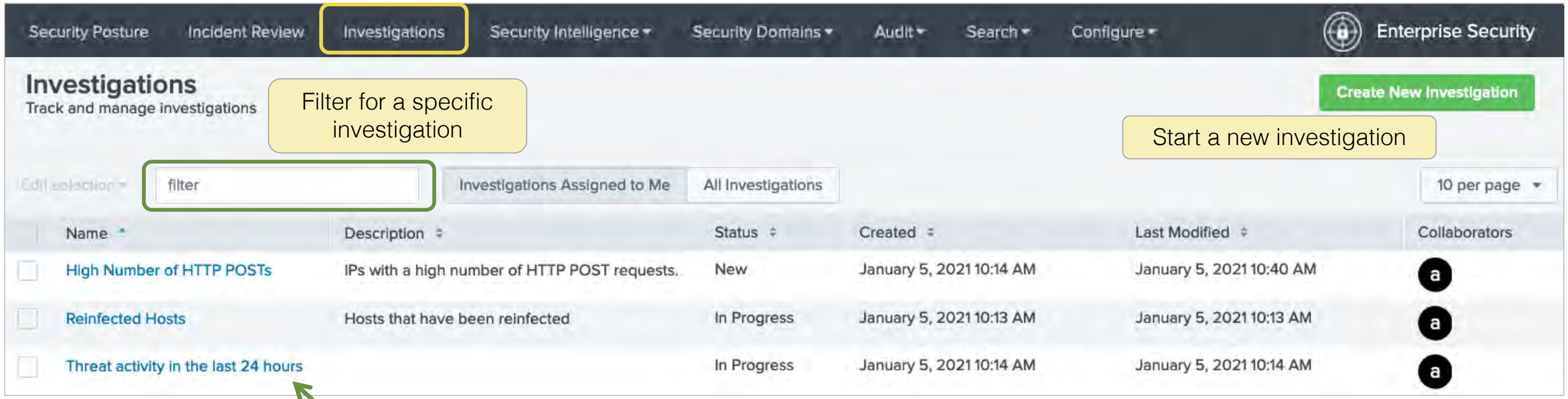
1. Examine notable events related to the payment processing system and add them to an investigation
2. Add relevant artifacts (i.e., assets and identities) and explore them within the Investigation Workbench – this will help identify other identities involved
3. Add collaborators with expertise in a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

Note

By default, only **ess_admin** and **ess_analyst** have permission to start investigations.

Investigations Dashboard

Lists all investigations

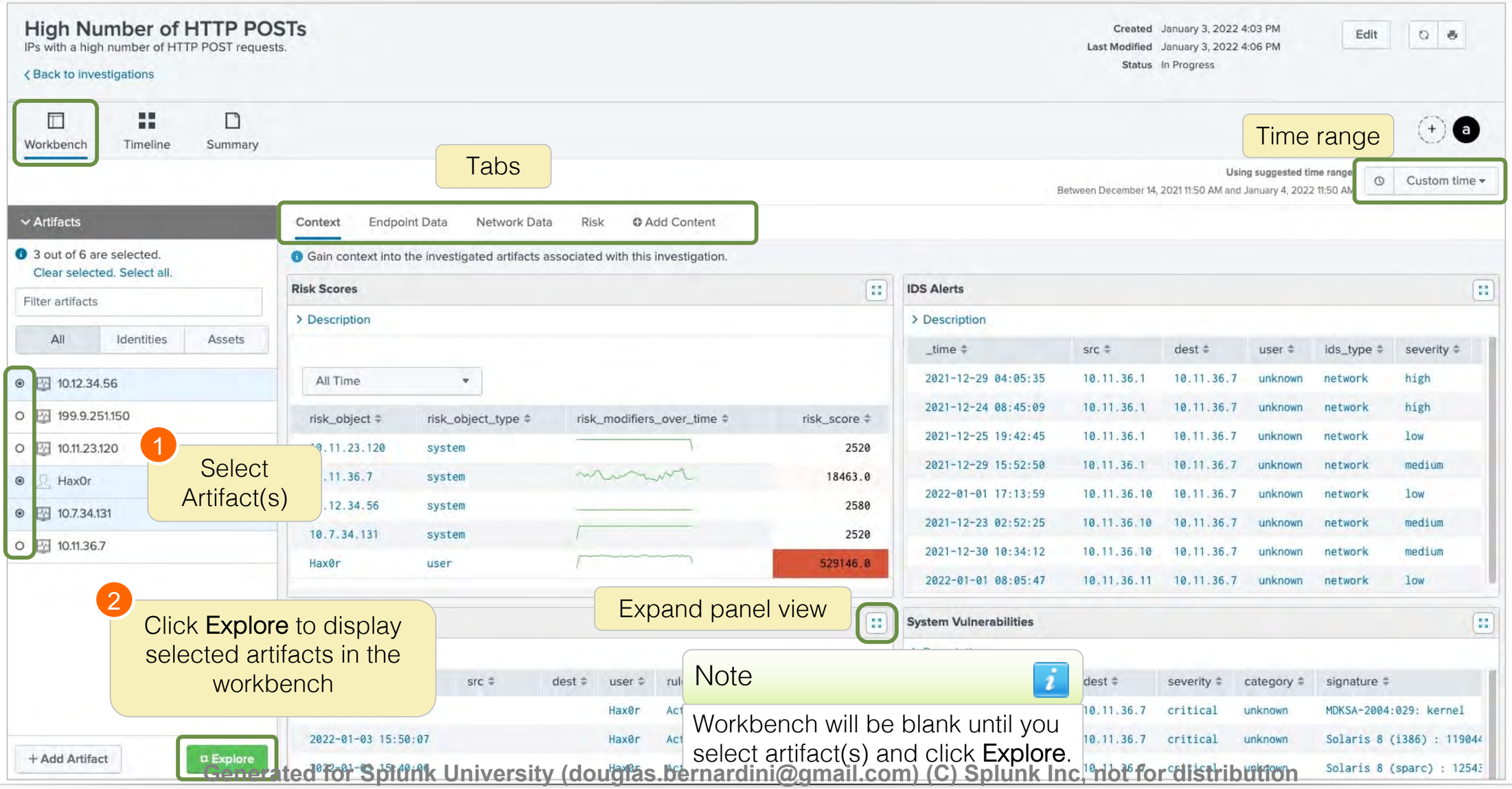


Filter for a specific investigation

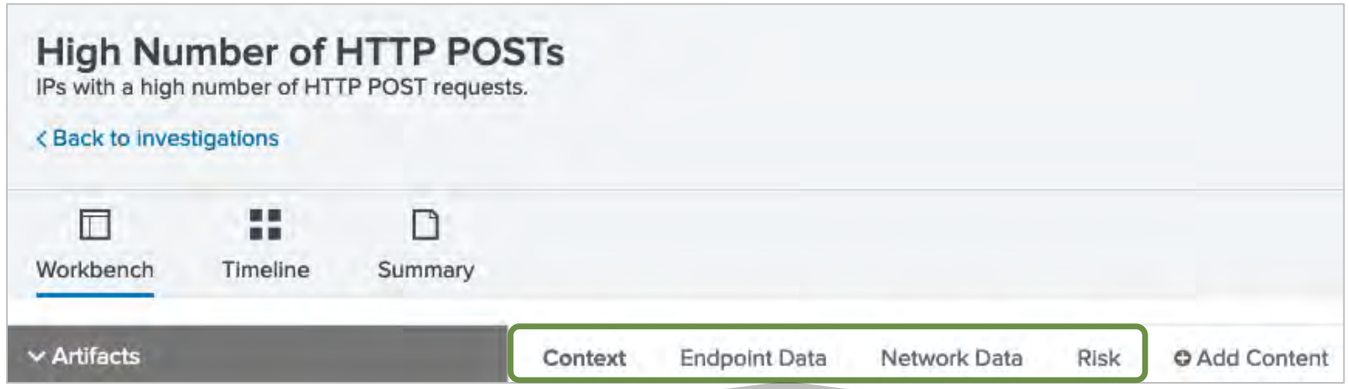
Start a new investigation

Click an investigation to open it

Investigation Workbench



Tabs & Panels



Context Panels

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

Endpoint Data Panels

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

Network Data Panels

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

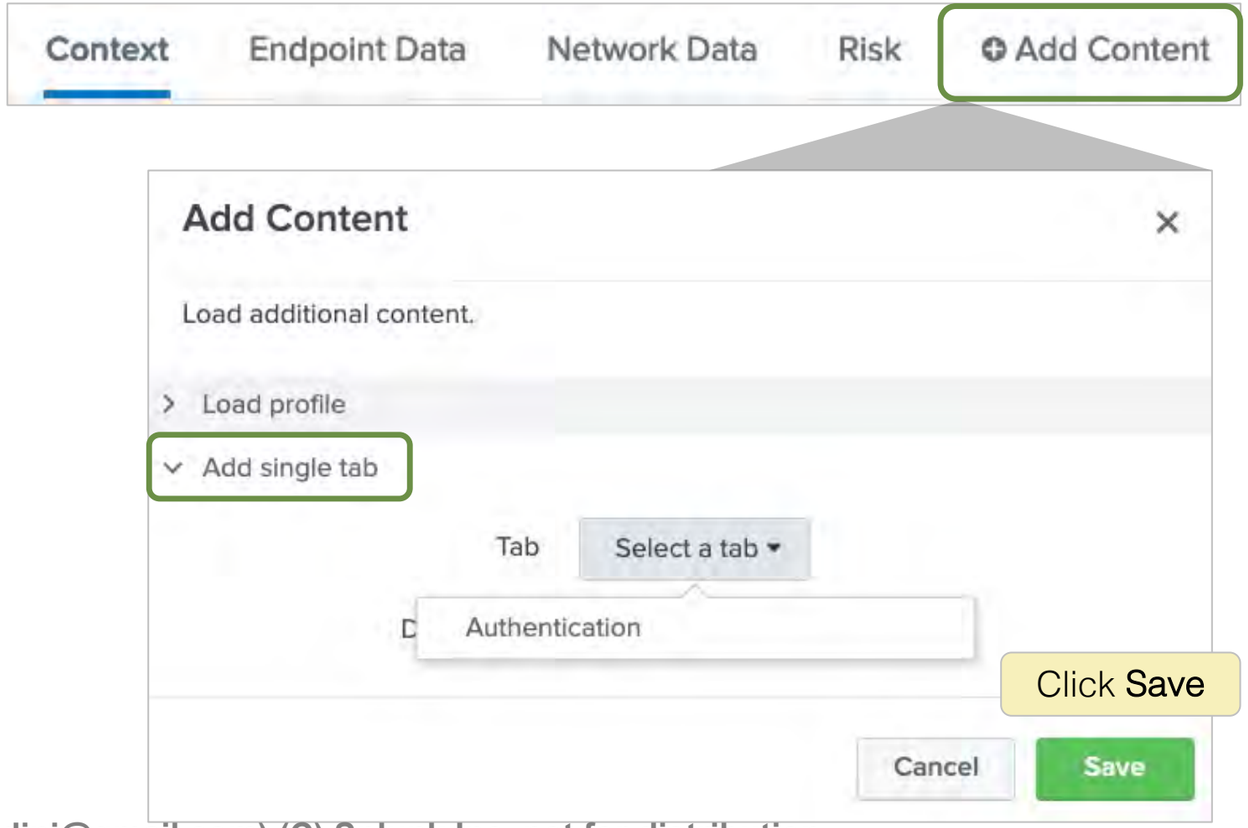
Risk Panels

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

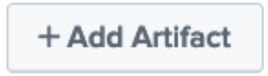
Add a Tab to the Investigation

- 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

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



Add Artifacts to an Investigation

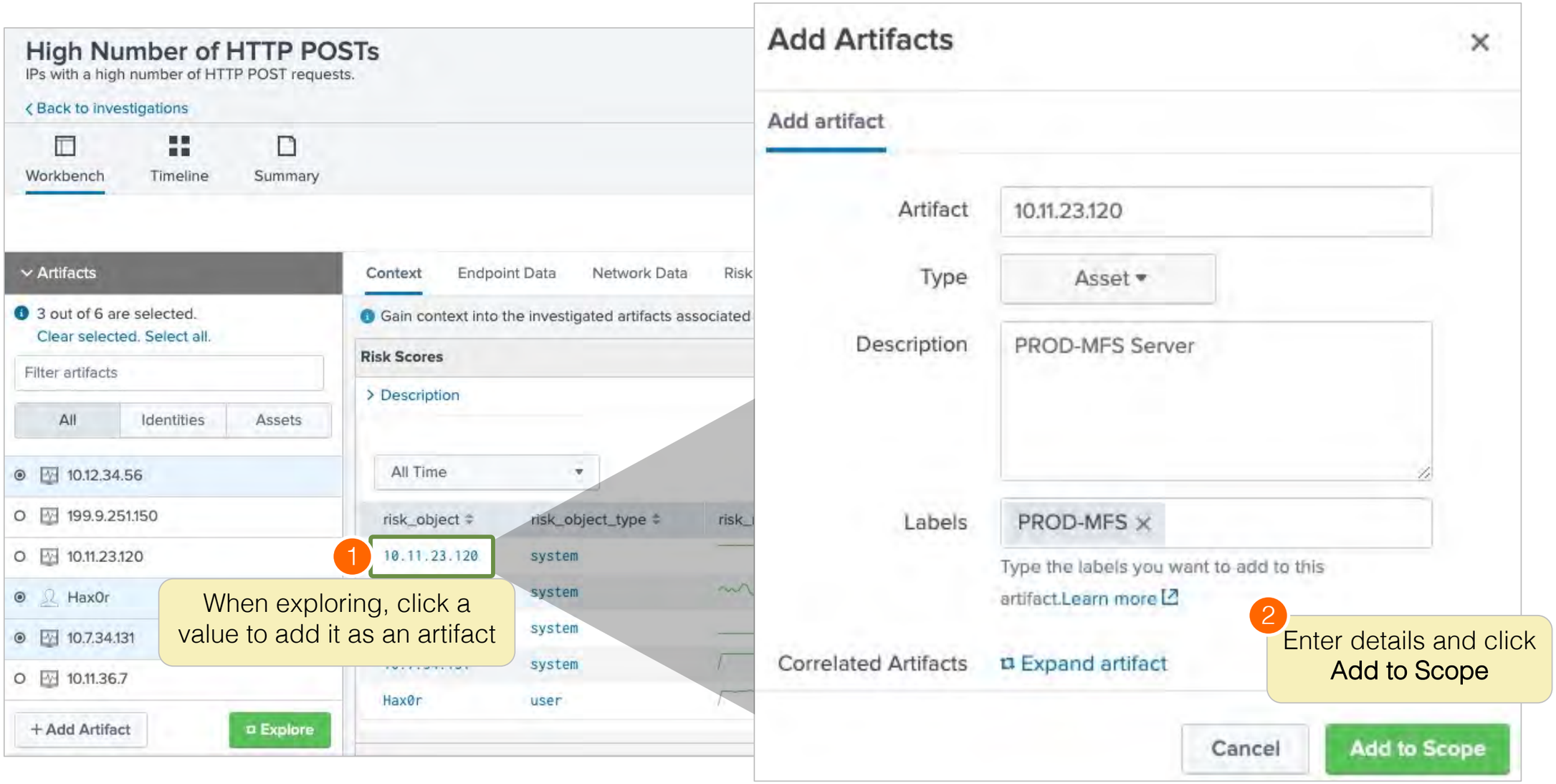
- Artifacts are assets or identities you may add to an investigation to determine whether they are involved in the overall incident
- There are several ways to add an artifact to an investigation
  - From a notable event (set up by an admin)
    - **Actions > Add Event to Investigation**
  - Manually
    - **Add Artifact** button 

    - **Add Artifact** icon  on the **Investigation Bar**
  - From a workbench panel (select any item)
  - From an investigation event (**Timeline View > Details > click a value**)

Add Artifacts Manually

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

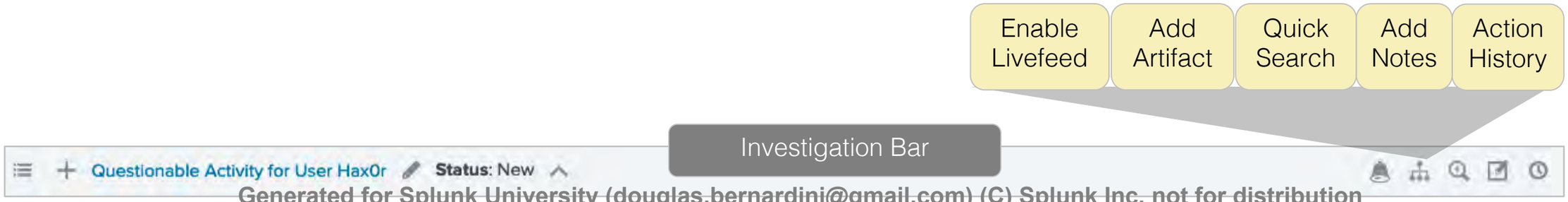
Add Artifacts within the Investigation



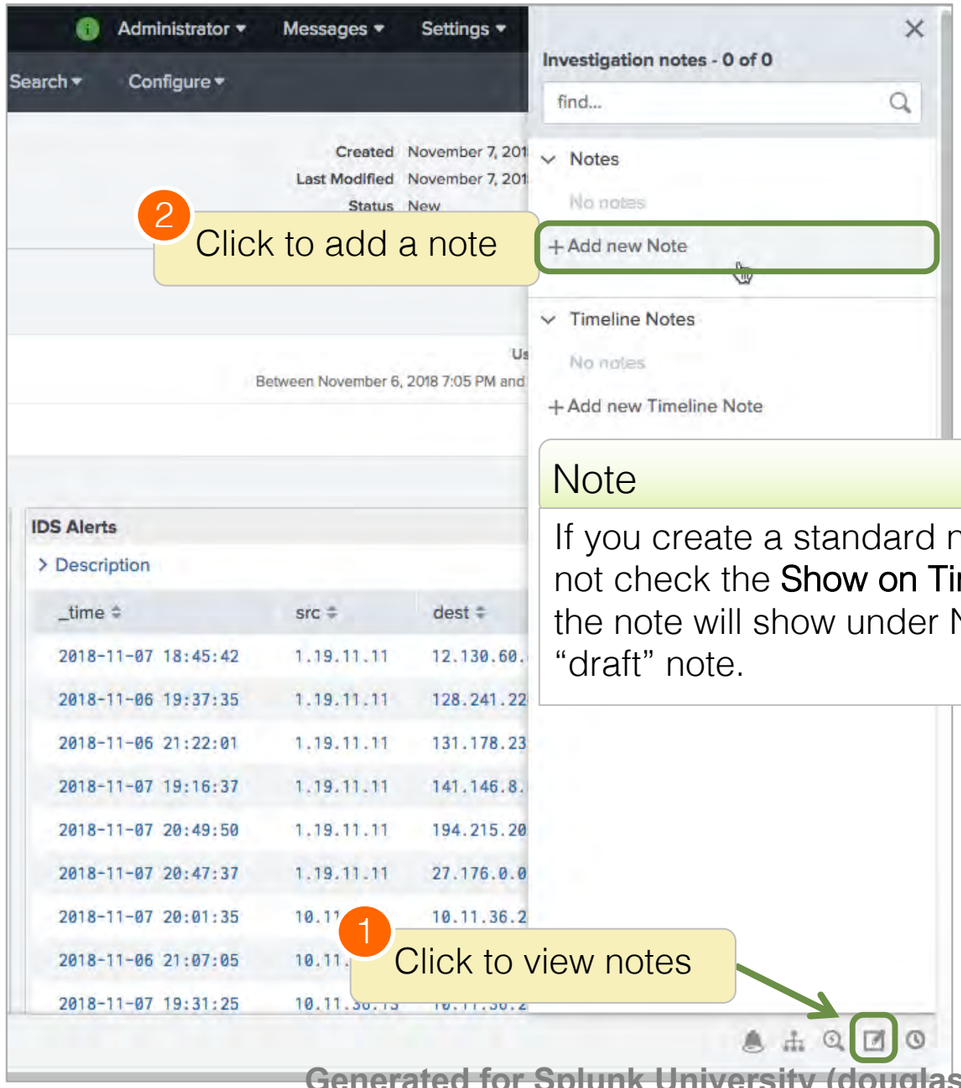
Add Items to an Investigation

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

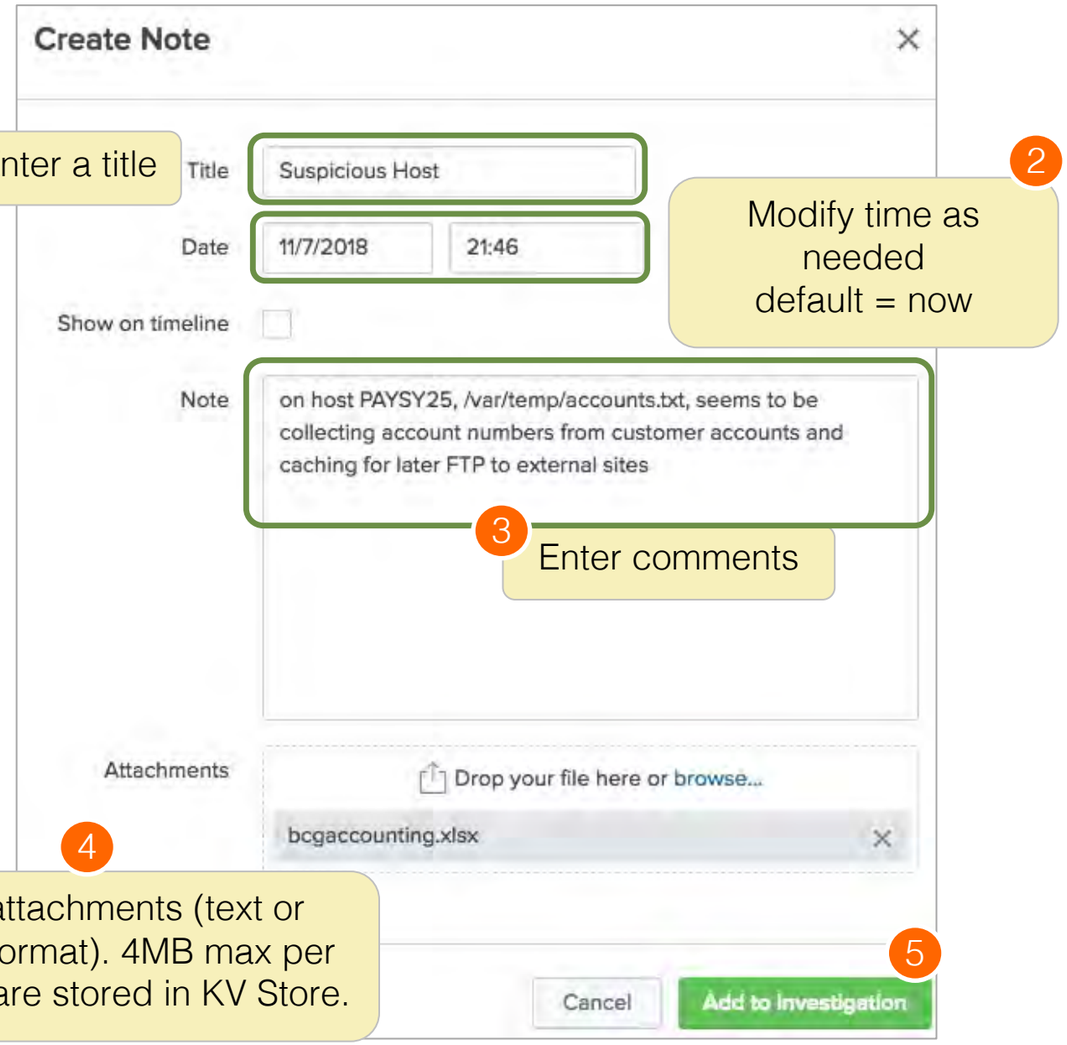


2 Click to add a note

1 Click to view notes

Note

If you create a standard note, and do not check the **Show on Timeline** box, the note will show under Notes as a "draft" note.



1 Enter a title

2 Modify time as needed default = now

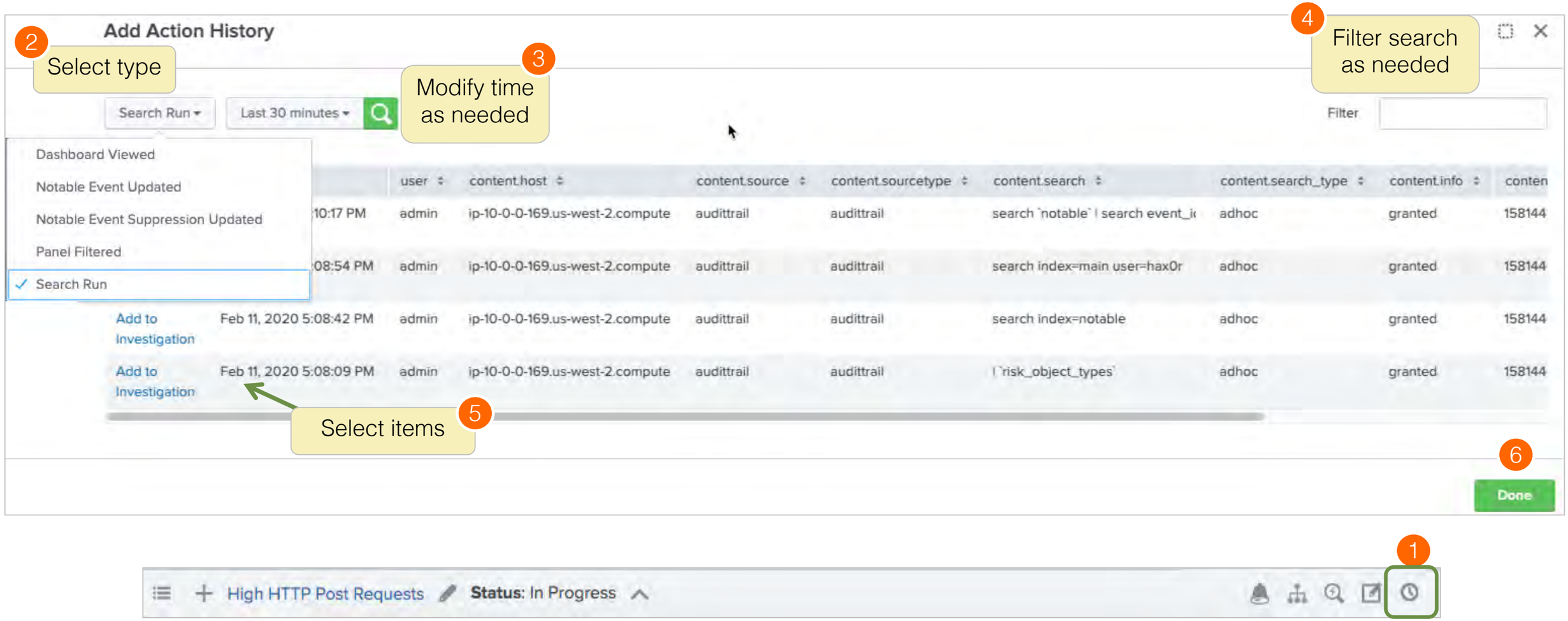
3 Enter comments

4 Add attachments (text or binary format). 4MB max per file and are stored in KV Store.

5

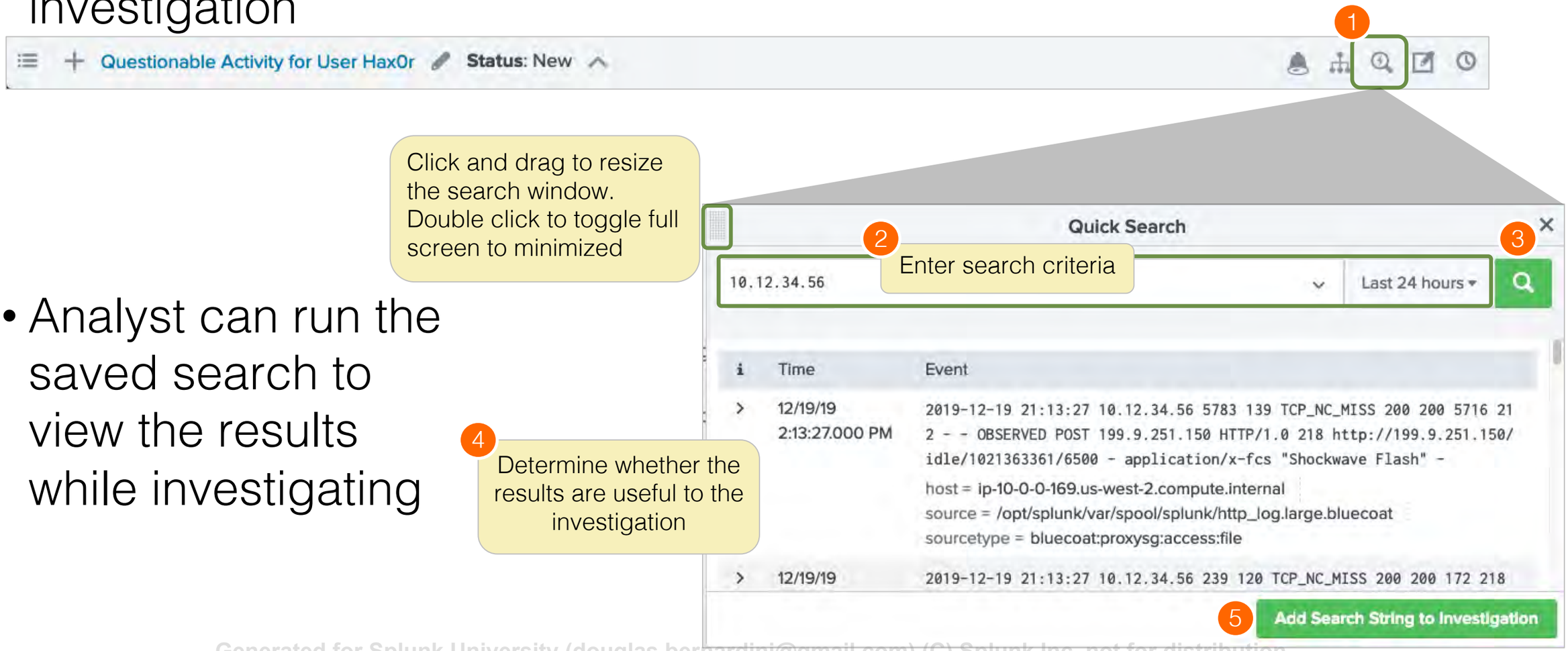
 | 25 May 2022

Adding an Action History Item



Adding a Search String (Quick Search)

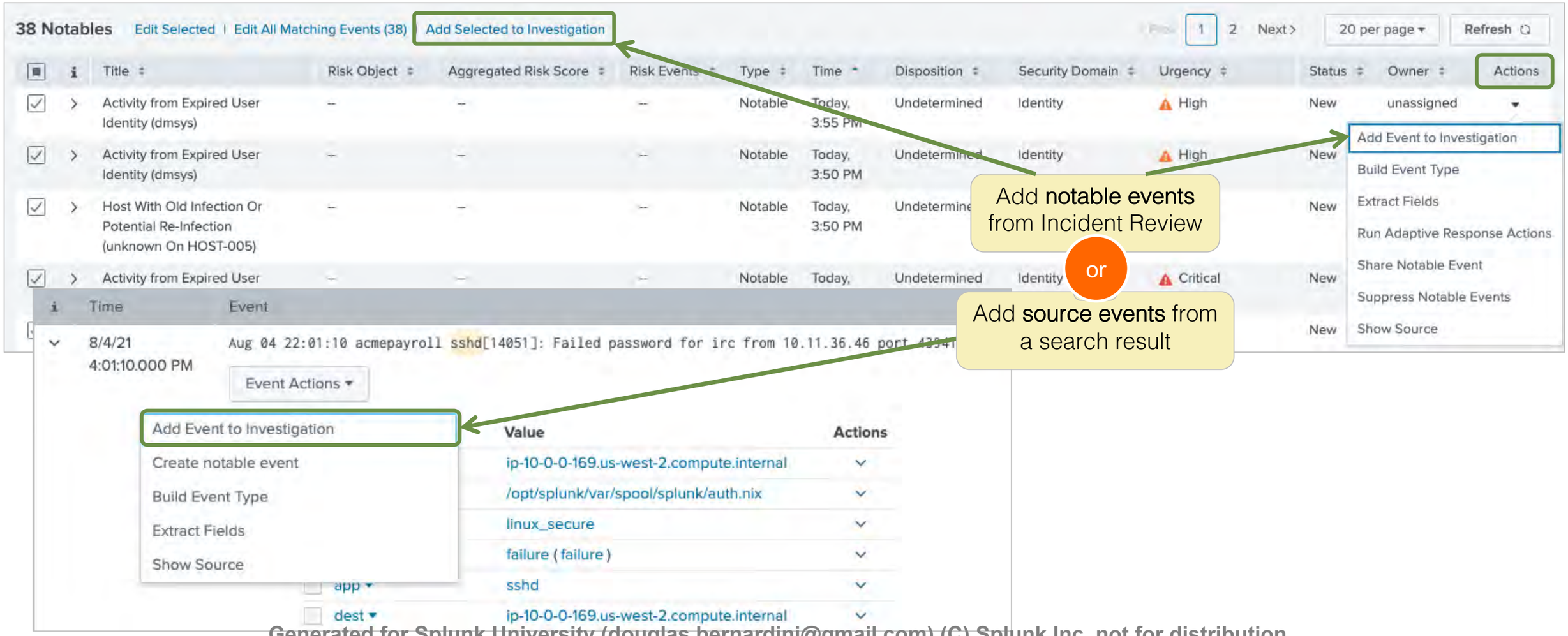
- Perform a search from the **Investigation Bar** and add the string to an investigation



- Analyst can run the saved search to view the results while investigating

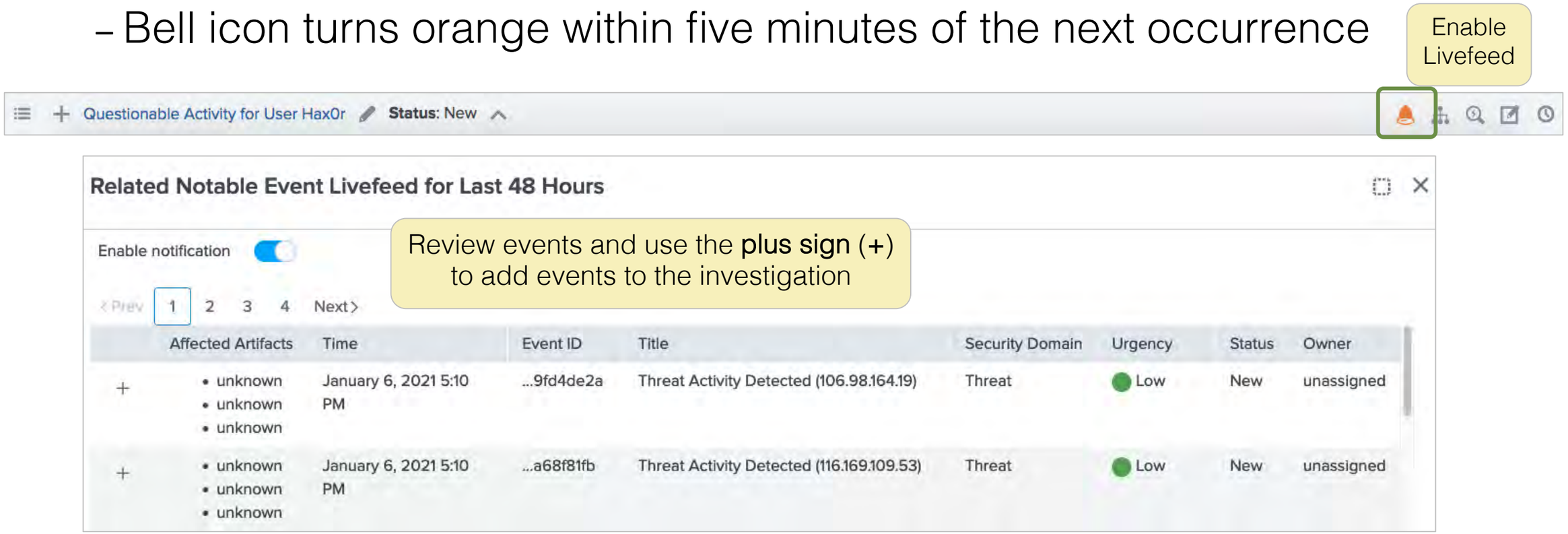
Adding Events

There are several ways to add events to an investigation

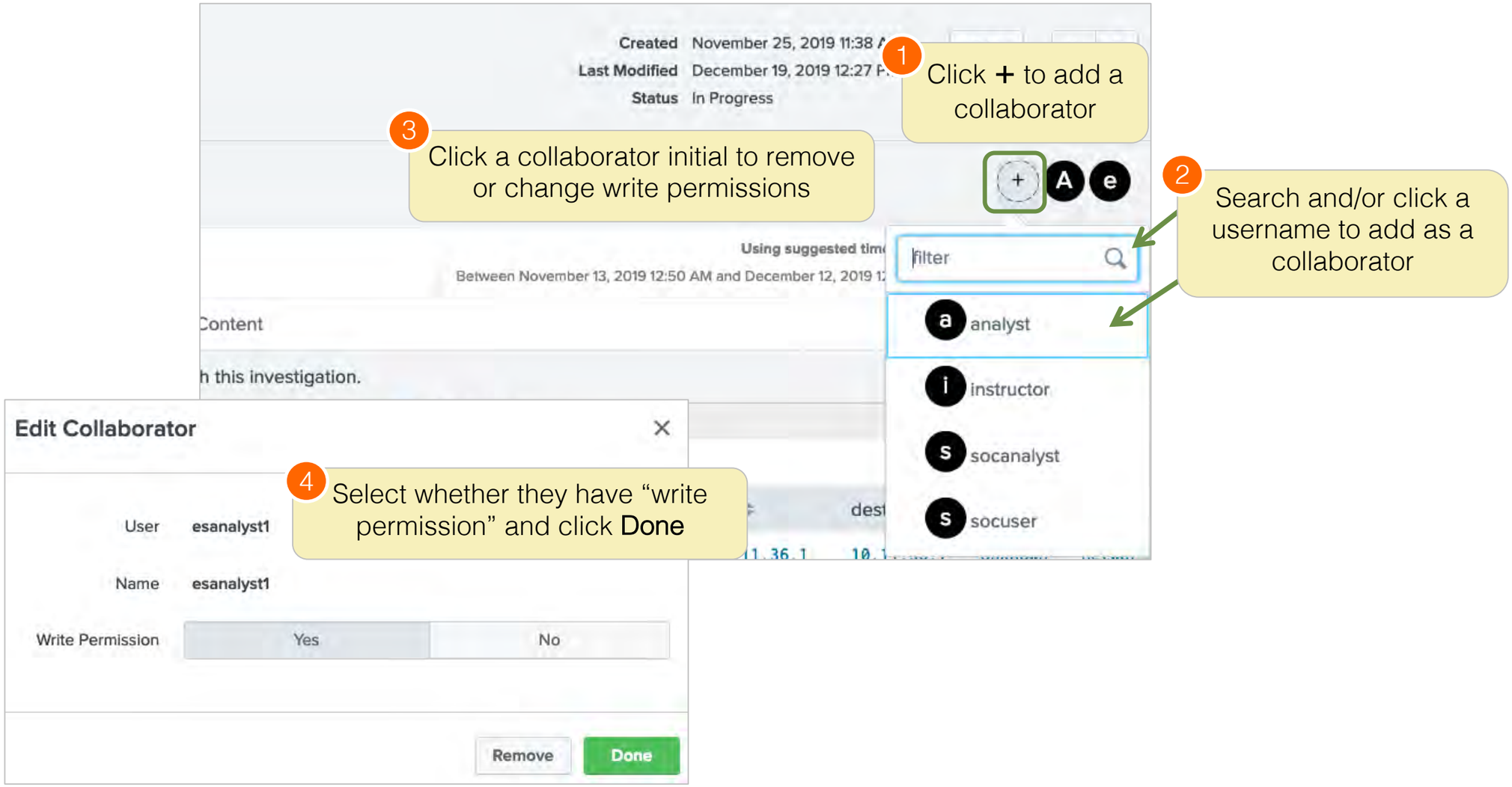


Enabling Notable Event Livefeed

- 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

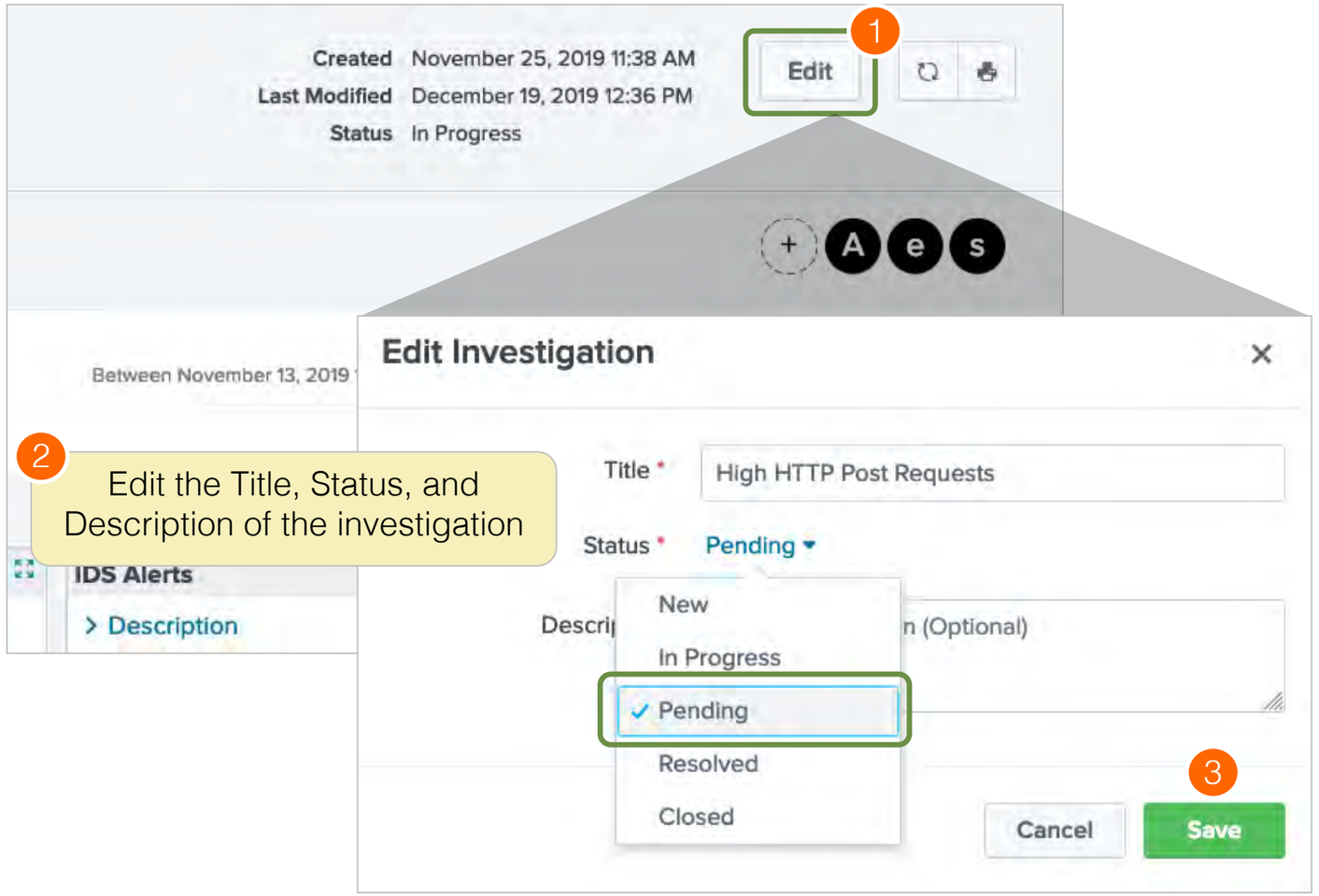


Adding Collaborators to an Investigation

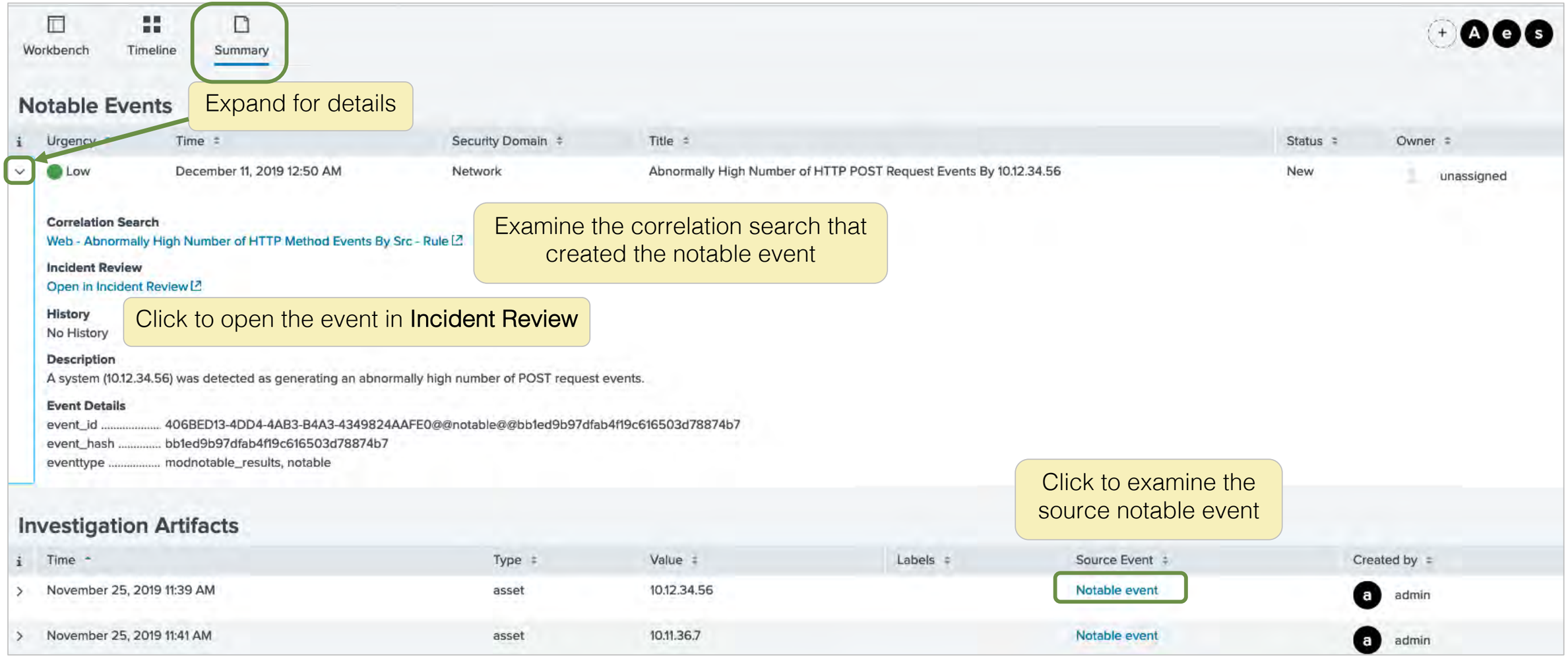


Updating Investigation Status

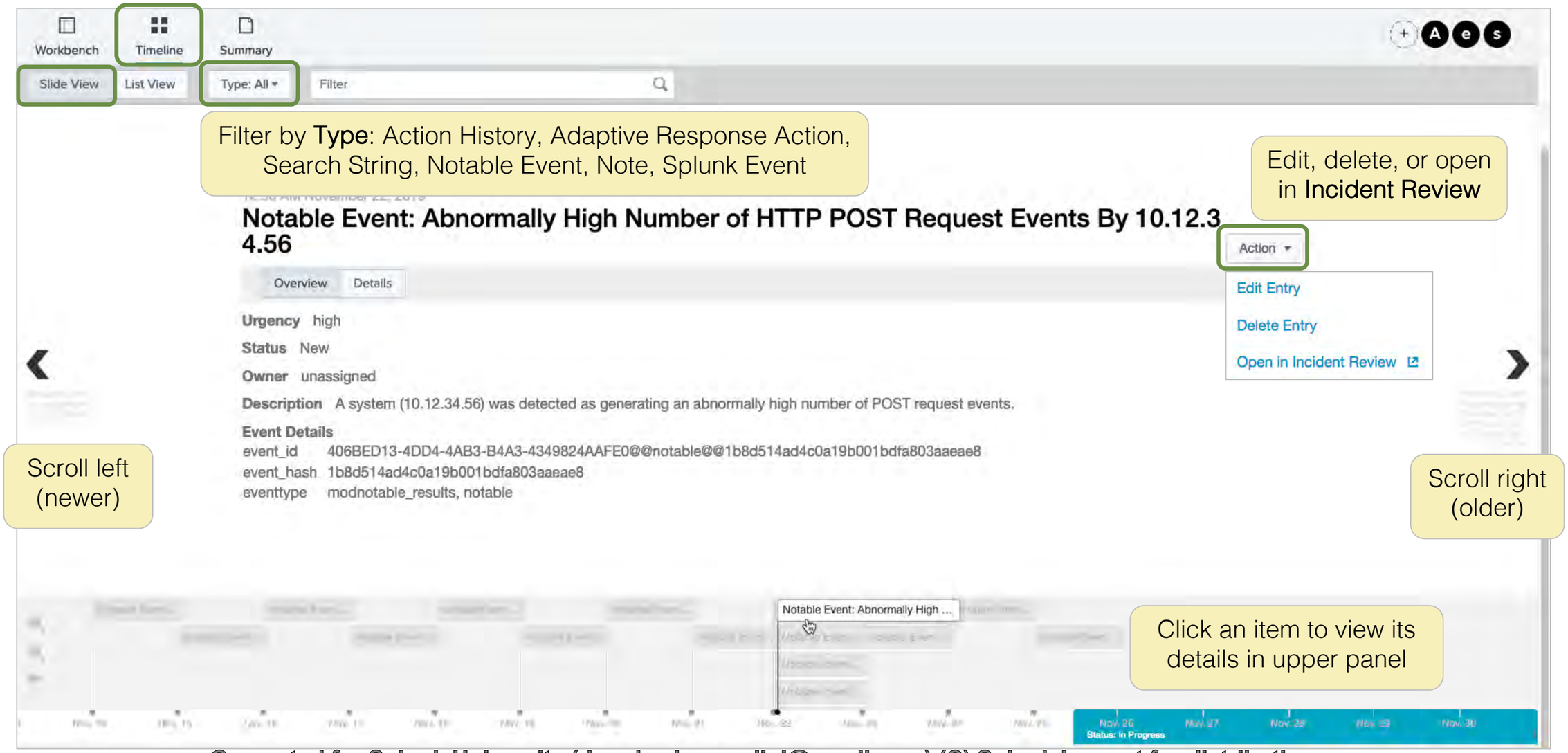
- When you open an investigation, the status is New
- Investigations can only be deleted by admins
- Analysts can delete investigation **entries**



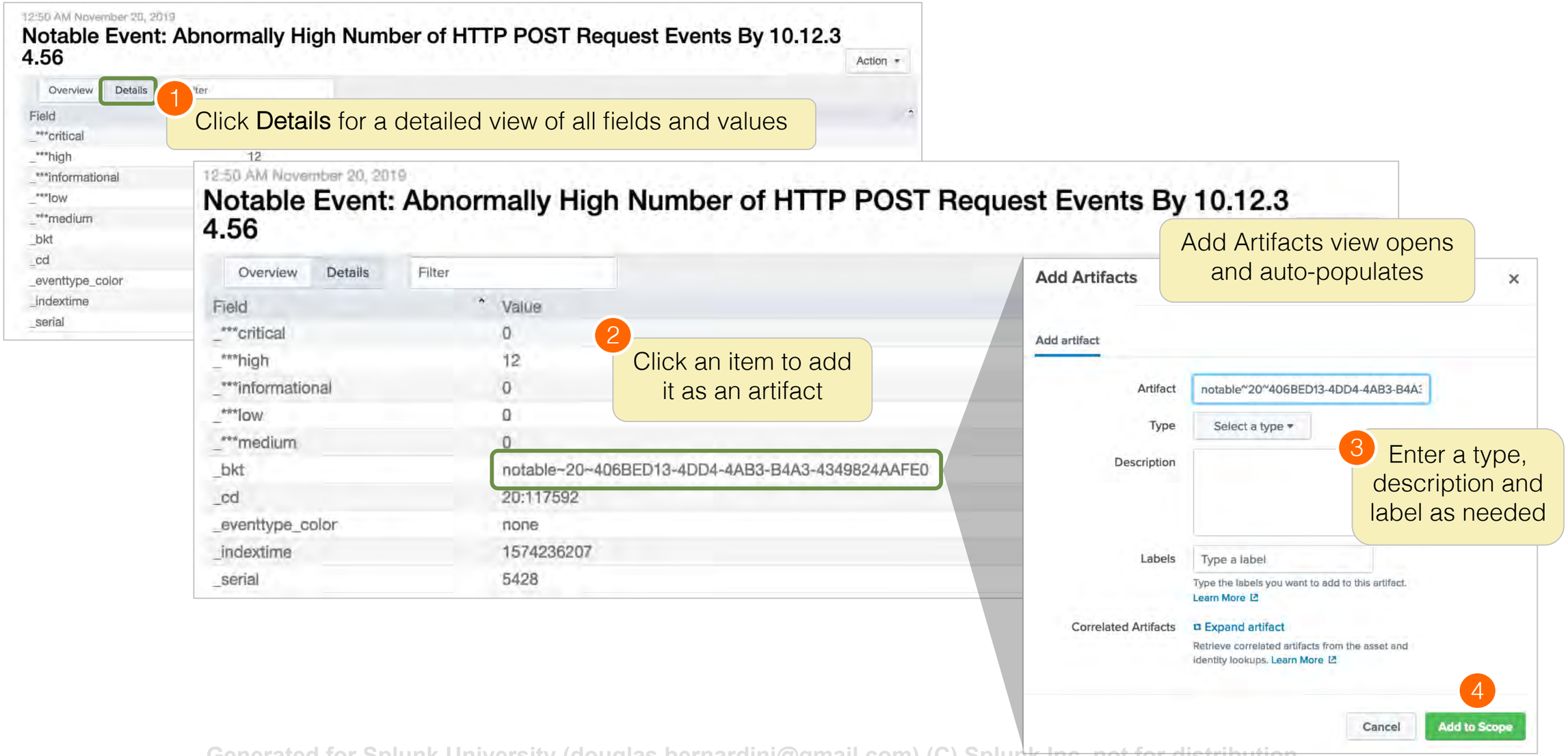
Investigation Summary View



Timeline: Slide View



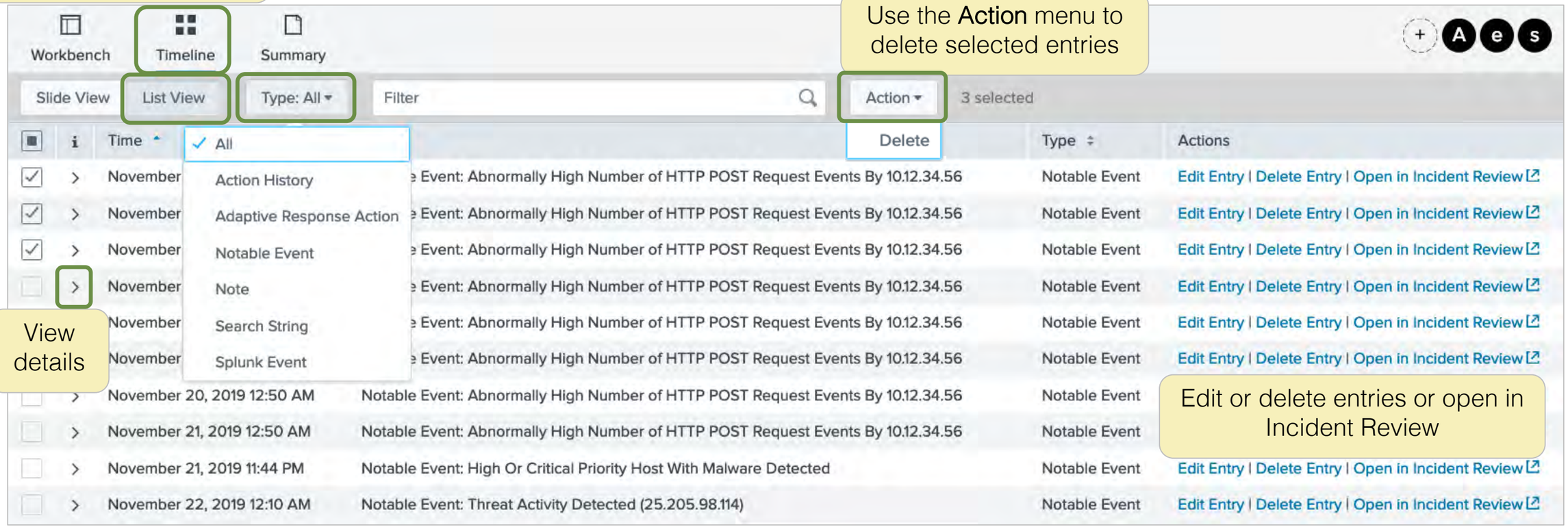
Timeline Details View to Add Artifacts



Timeline: List View

From **Timeline**, change view to **List View**

Use the **Action** menu to delete selected entries

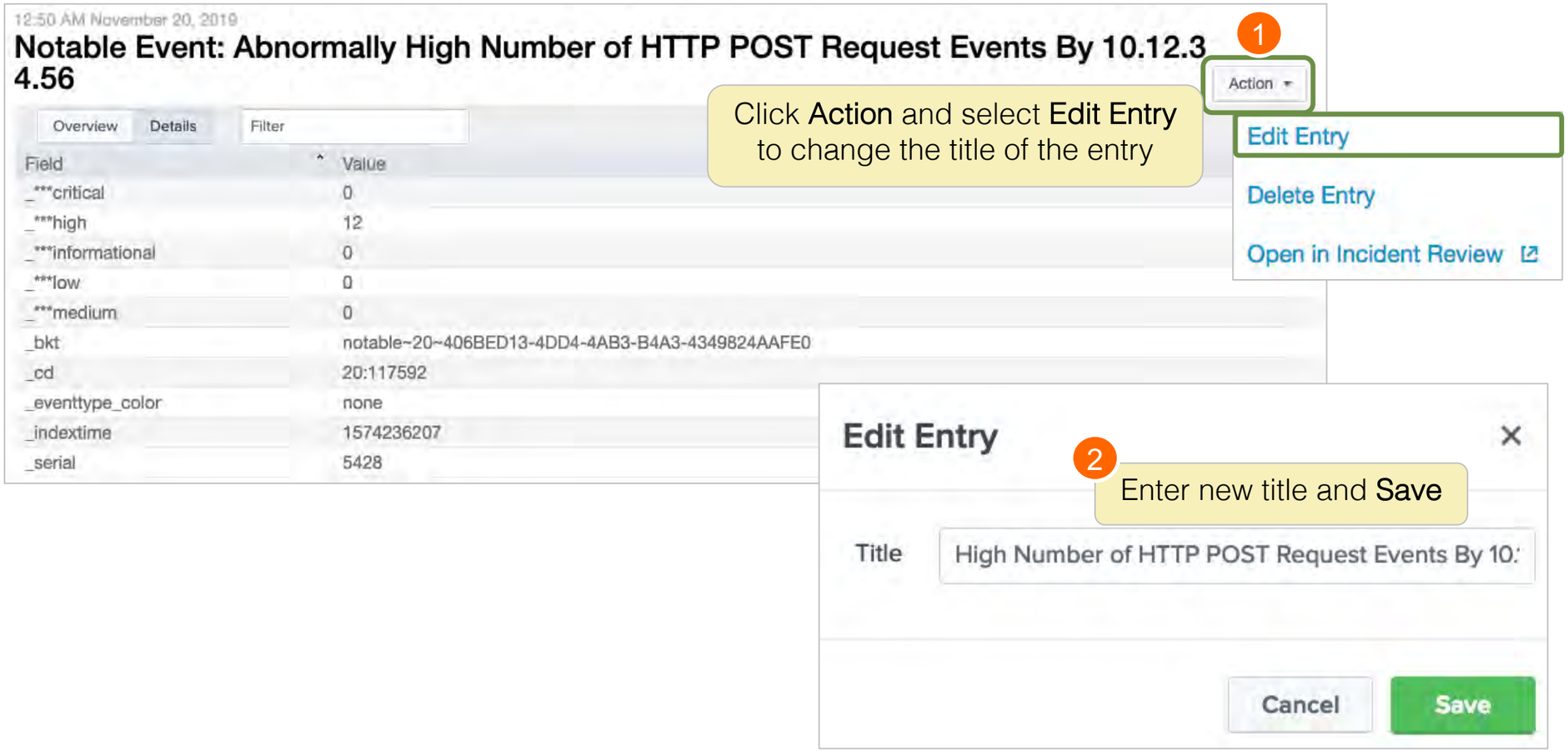


View details

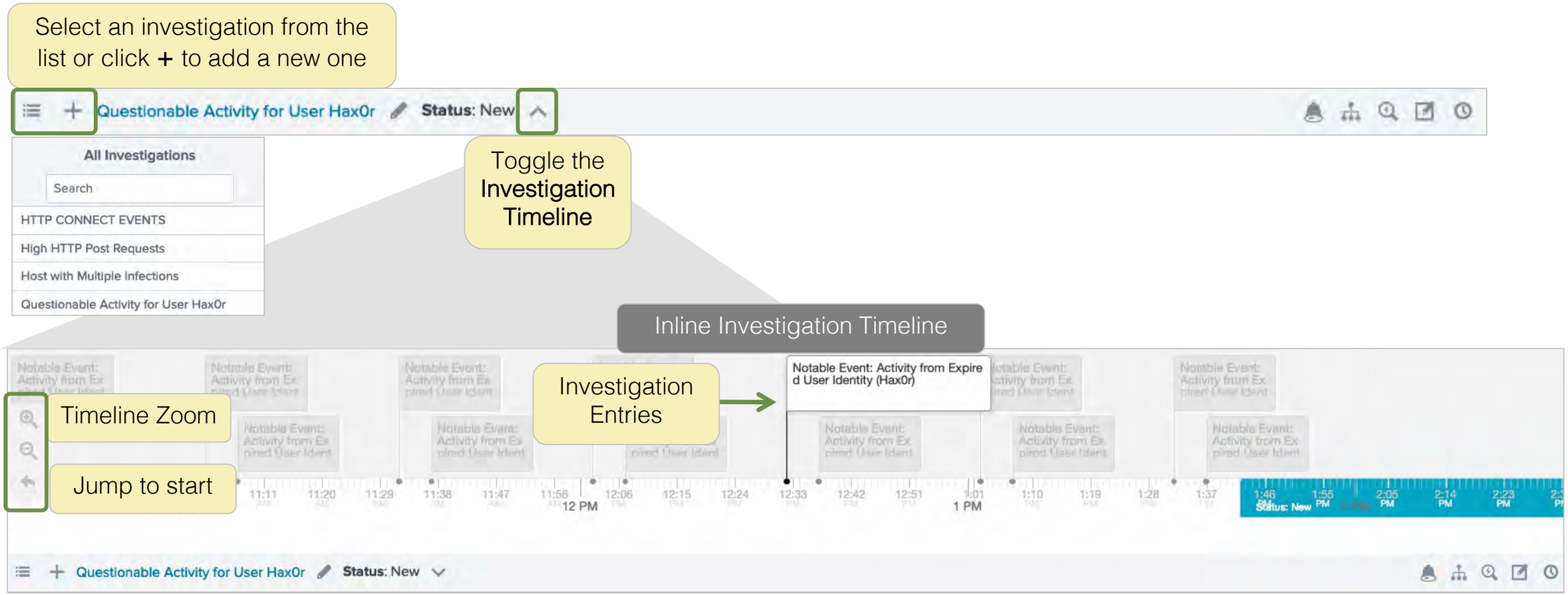
Edit or delete entries or open in Incident Review

 | 25 May 2022

Edit Investigation Entry



Investigation Bar and Inline Timeline View



Module 5 Lab: Working with ES Investigations

Time: 50 minutes

Description: Create and manage an ES investigation

Tasks:

- Create an investigation to monitor user *Hax0r* over time
  - Add notable events to your investigation
  - Add an alert for results of future related notable events
- Create an investigation to monitor Snort activity
  - Find Snort events and add a Quick Search
  - Create a notable event to track status
  - Investigate source systems
  - Review your investigation from Timeline and Summary views

Module 6:
Security Domain Dashboards

Objectives

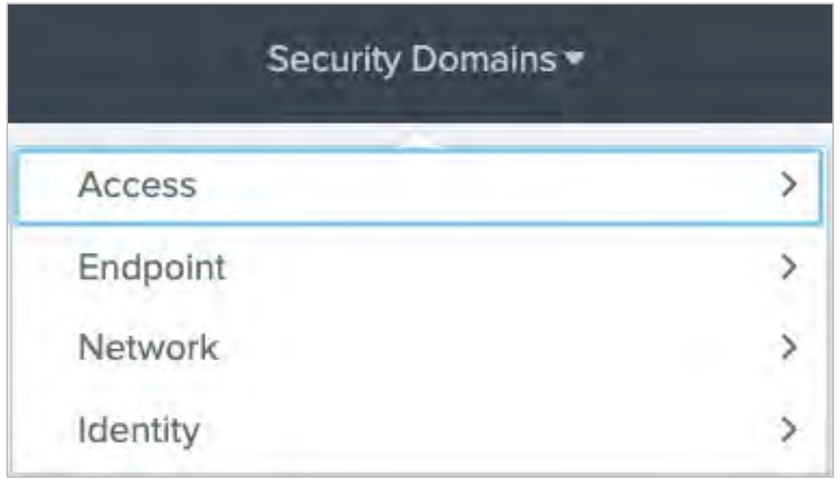
- Use ES to inspect events containing information relevant to active or past incident investigation
- Identify security domains in ES
- Use ES security domain dashboards
- Launch security domain dashboards from Incident Review and from action menus in search results

ES and Forensic Investigation

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

Security Domains

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



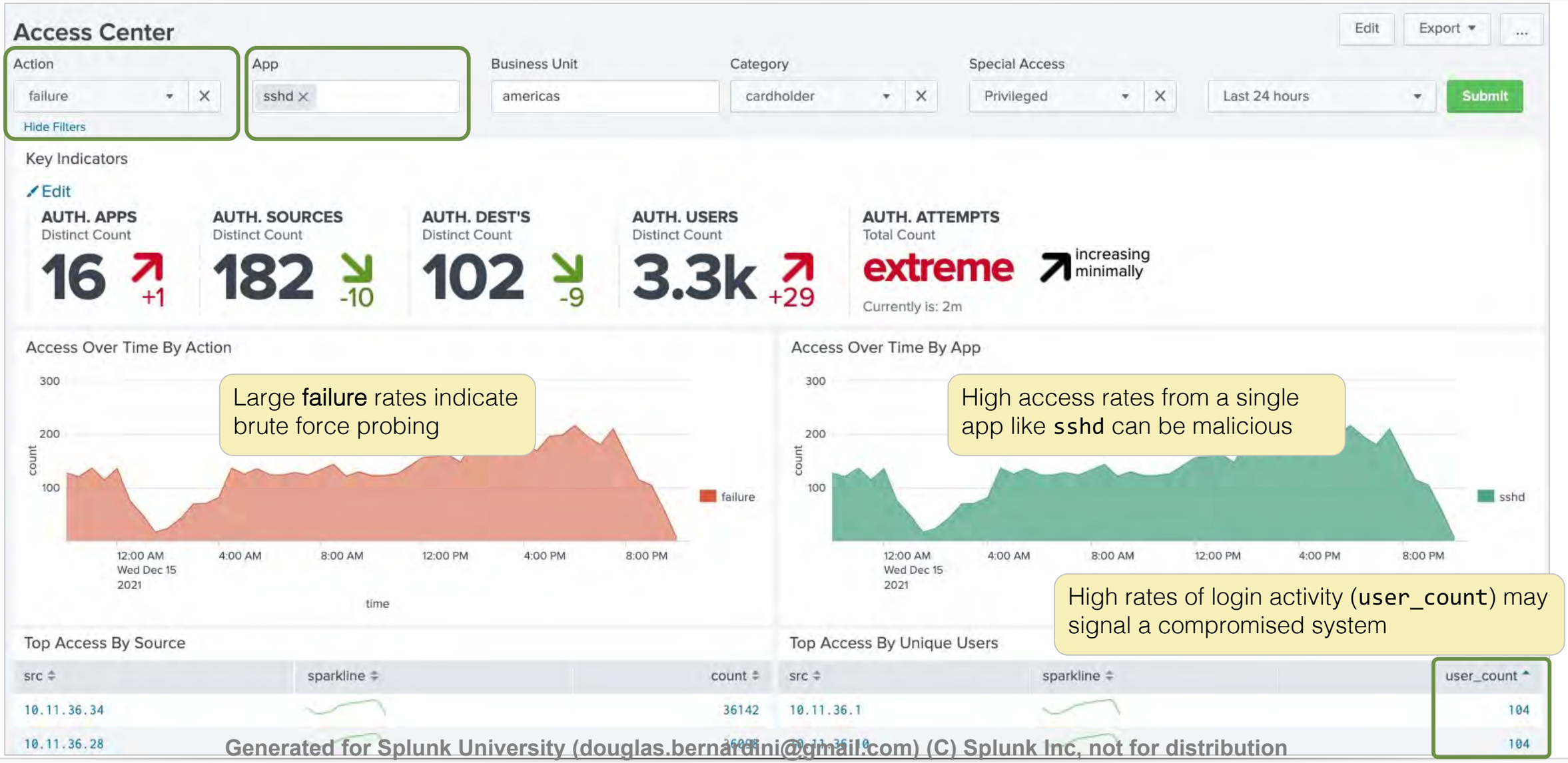
How to Use Domain Dashboards

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

Access Domain

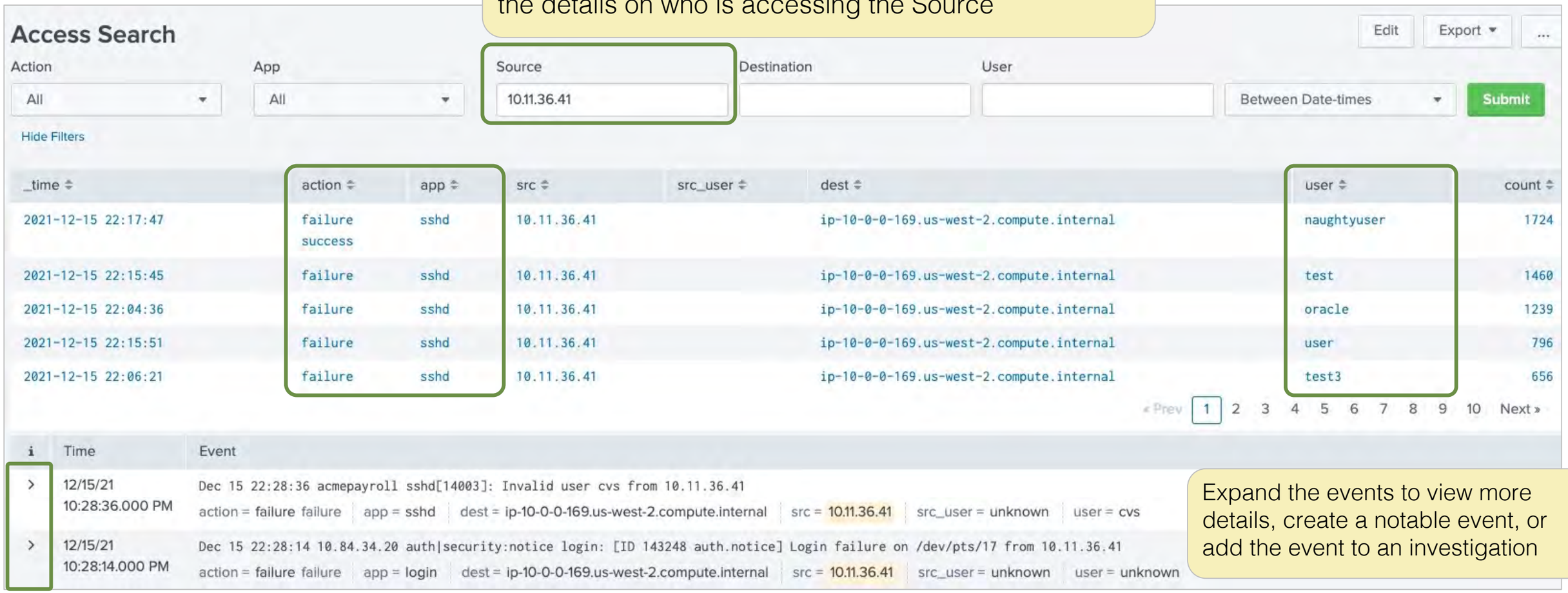
- The Access domain focuses on user identity and authentication
- Dashboards provide tools to research:
  - Brute force attacks
  - Privileged account misuse (i.e., **`root`**)
  - Access by rare or new accounts
  - Access by expired or disabled accounts
  - Access by unusual applications (i.e., SSH,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

Access > Access Center



Access > Access Search

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



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

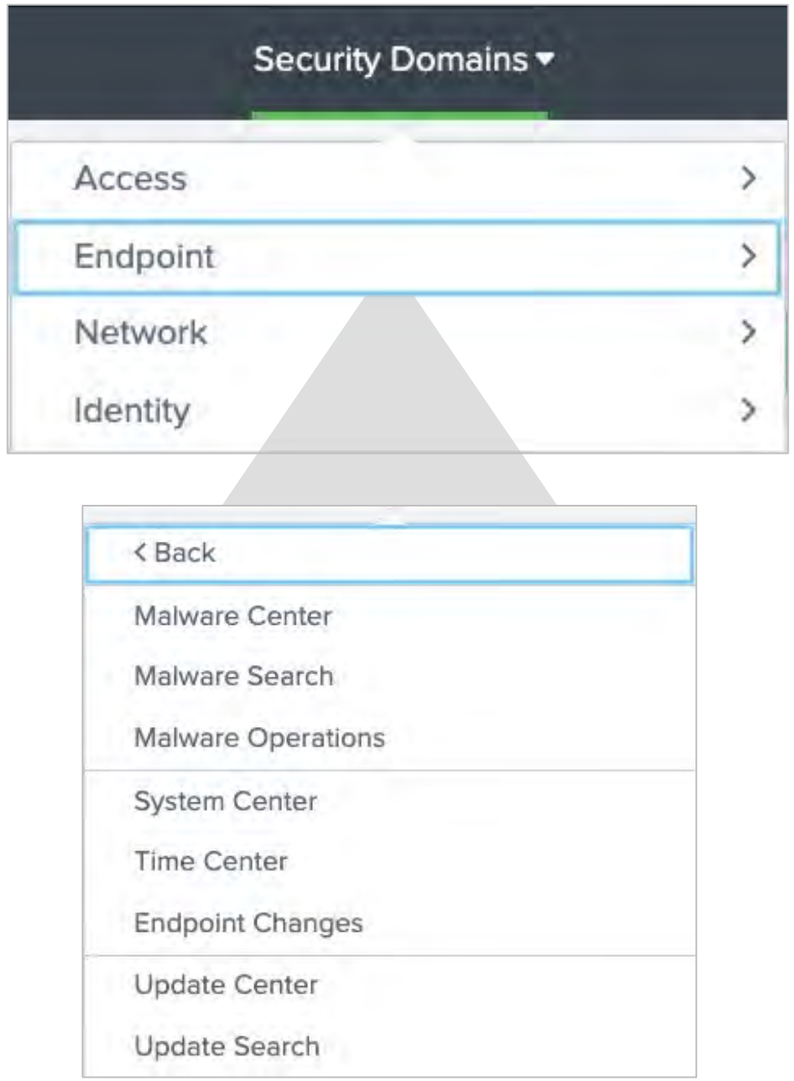
Other Access Domain Dashboards

Access Tracker	Account activity over time for: • first time access • inactive accounts • expired identities
Account Management	Account actions, like: • creation • deletion • lockout
Default Account Activity	Usage of default accounts, which are built-in to an operating system, such as: • root/administrator • SYSTEM • guest

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

Endpoint Domain

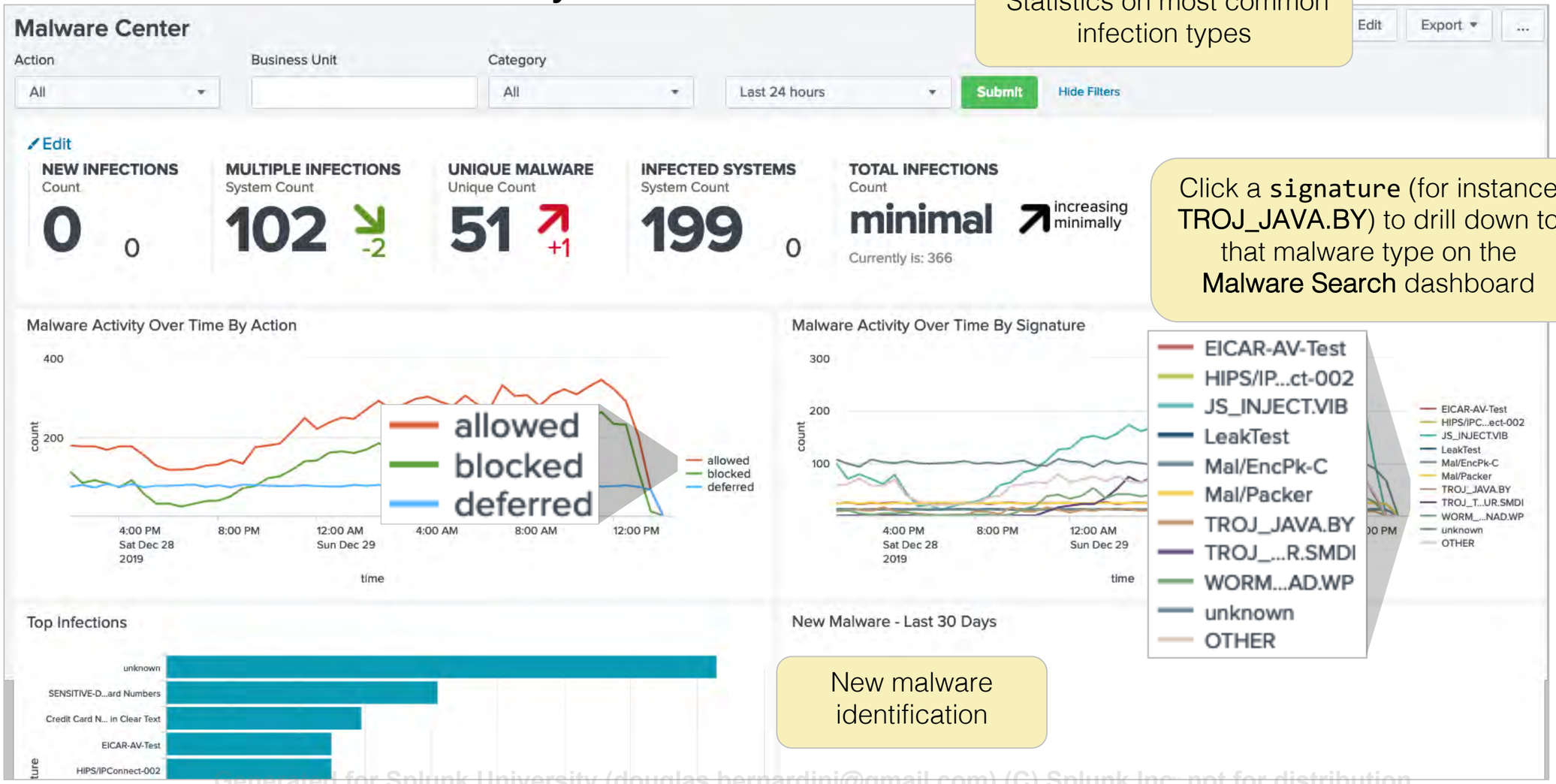
- The Endpoint domain watches over user systems, such as:
  - Workstations, PCs, notebooks
  - Handheld devices
  - Point-of-sale systems
- Potential issues include:
  - Vulnerabilities: missing updates or patches
  - Malware: spyware, ransomware, or other malicious code
  - Unexpected running processes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



Endpoint > Malware Center

Overview of malware in your environment

Statistics on most common infection types

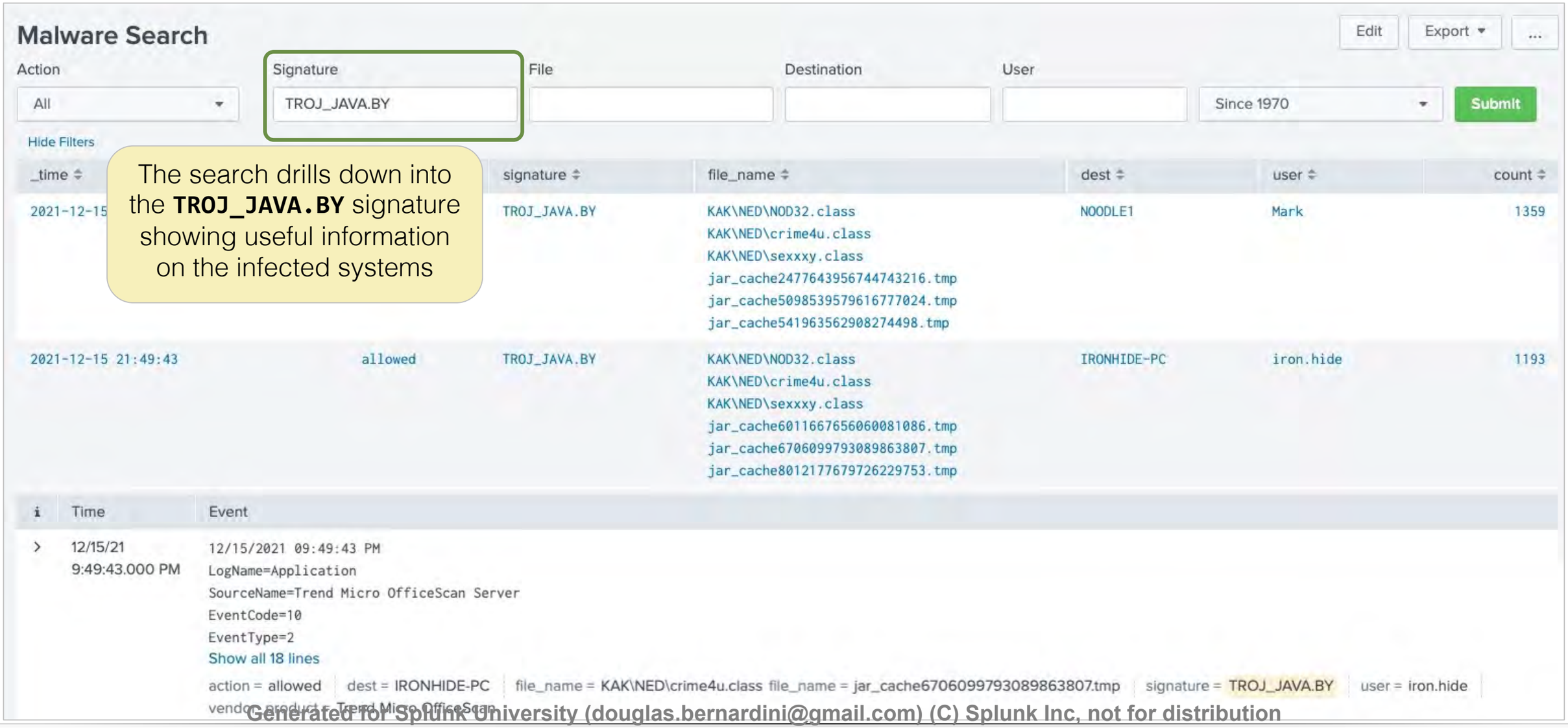


Click a **signature** (for instance TROJ_JAVA.BY) to drill down to that malware type on the **Malware Search** dashboard

New malware identification

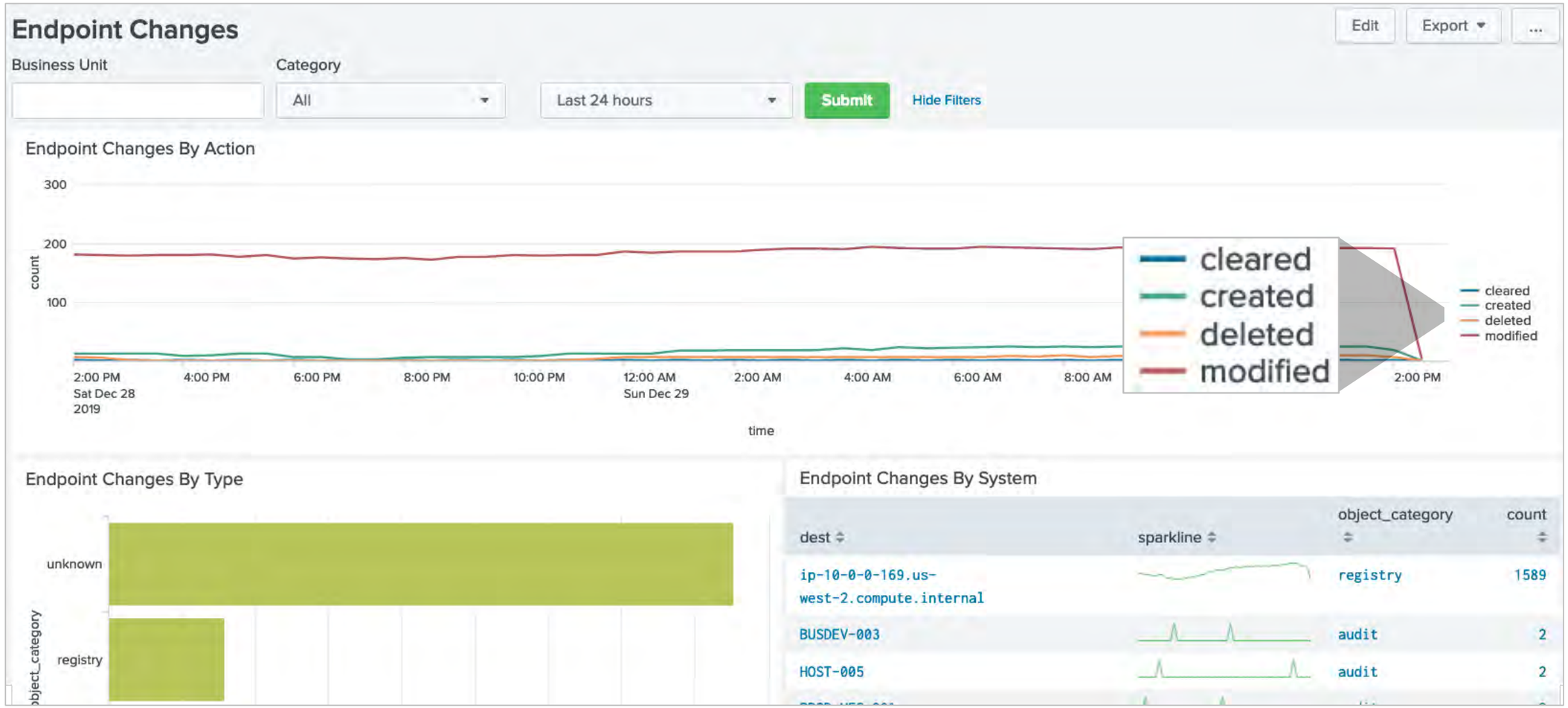
 | 25 May 2022

Endpoint > Malware Search



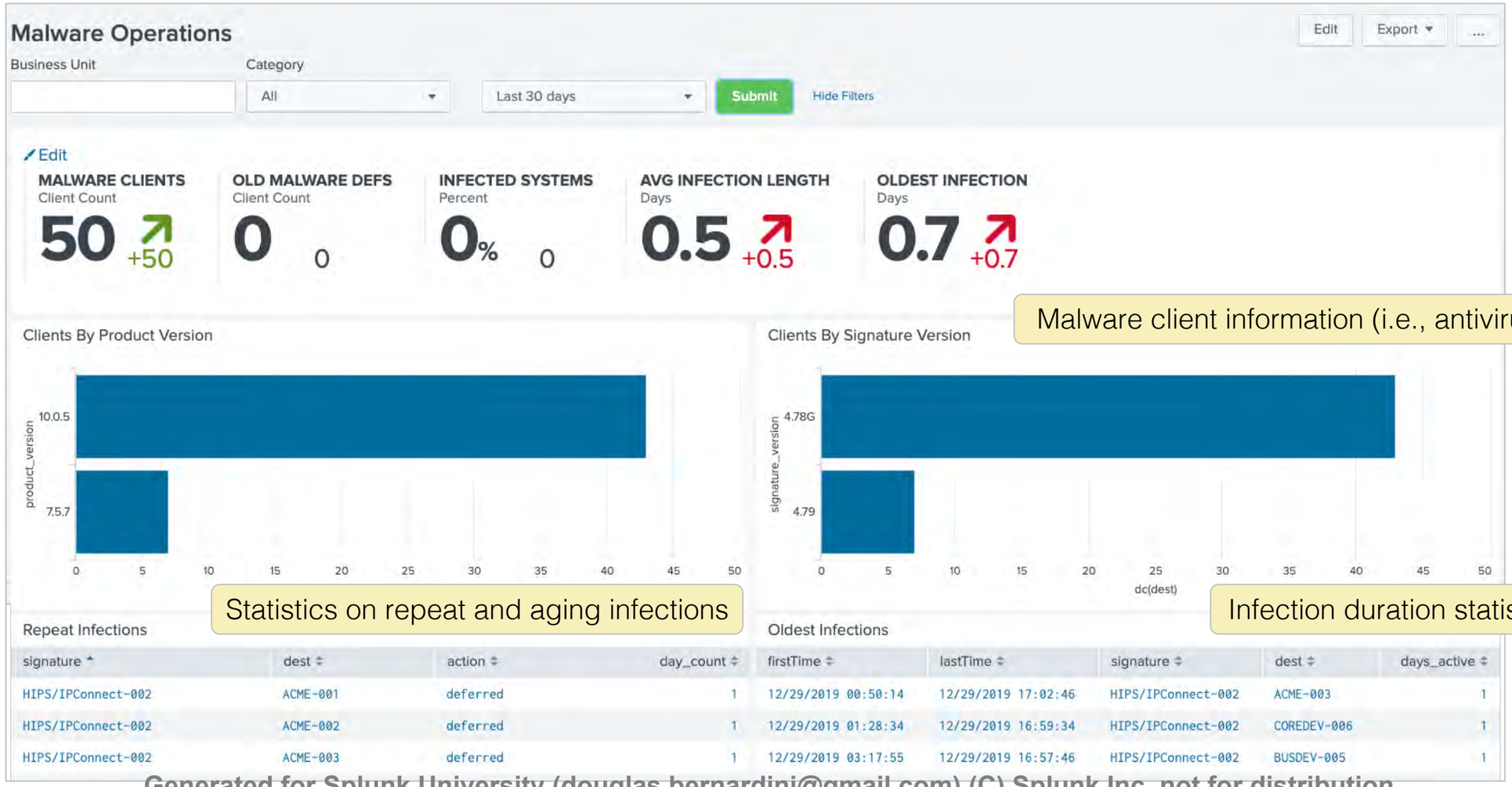
Endpoint > Endpoint Changes

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



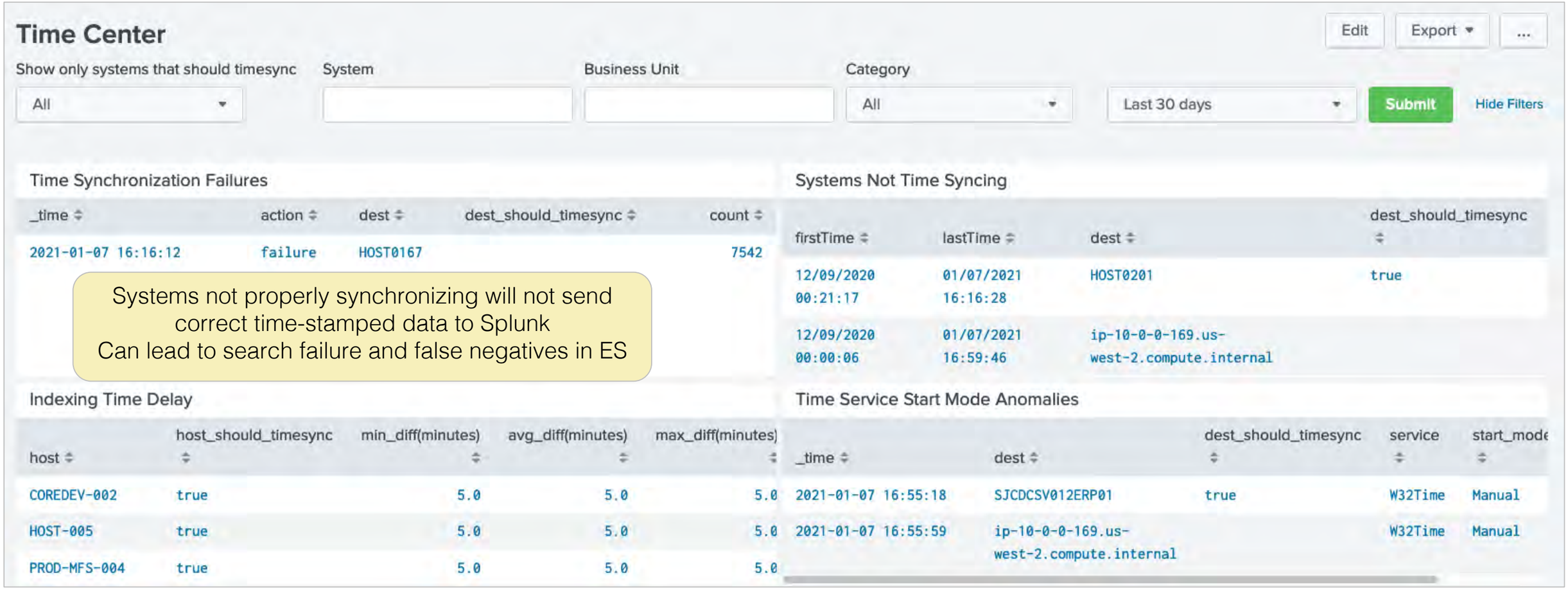
Endpoint > Malware Operations

Malware status overview



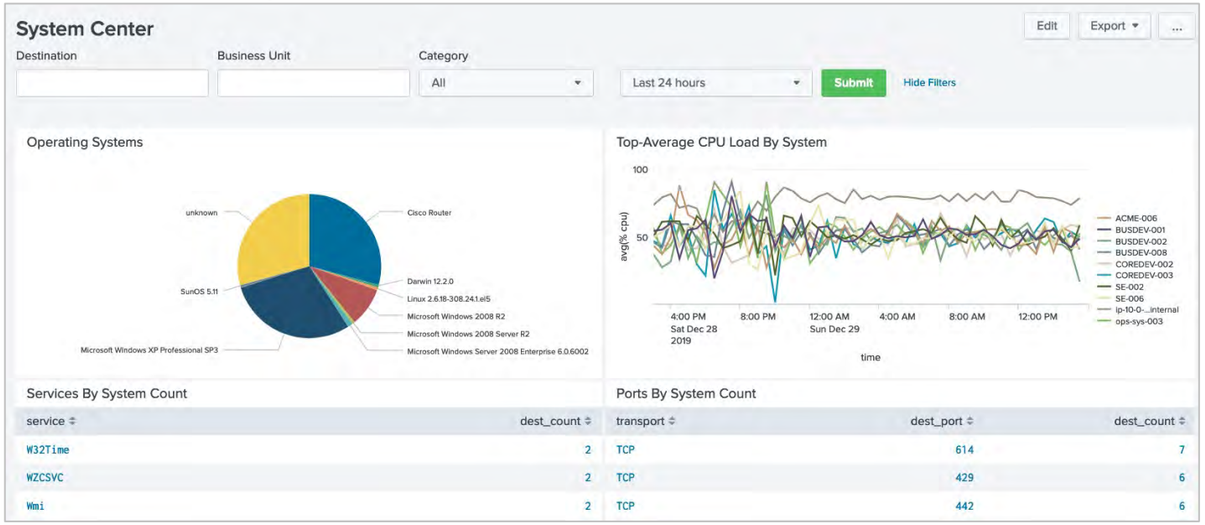
Endpoint > Time Center

Report the status of time synchronization in your environment

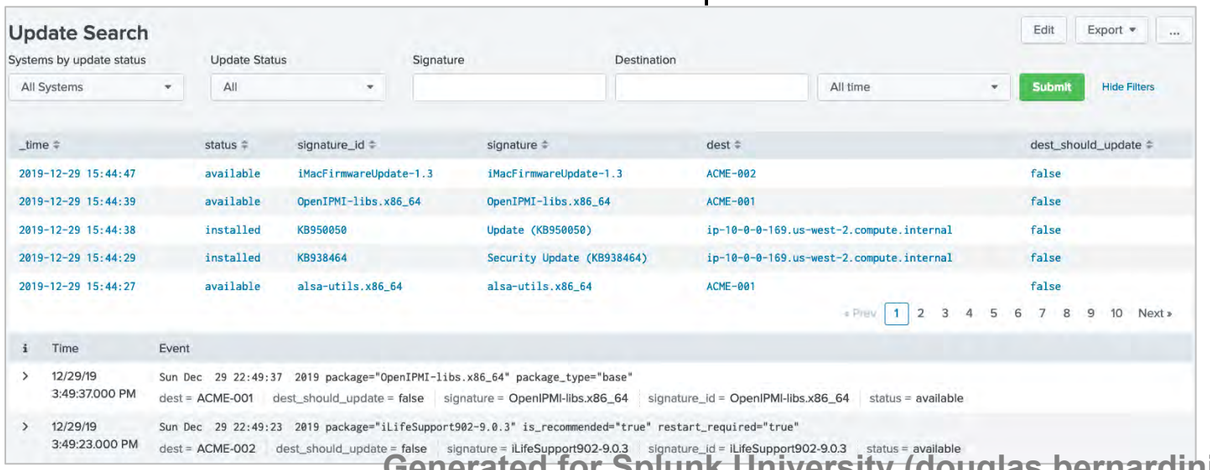


Other Endpoint Domain Dashboards

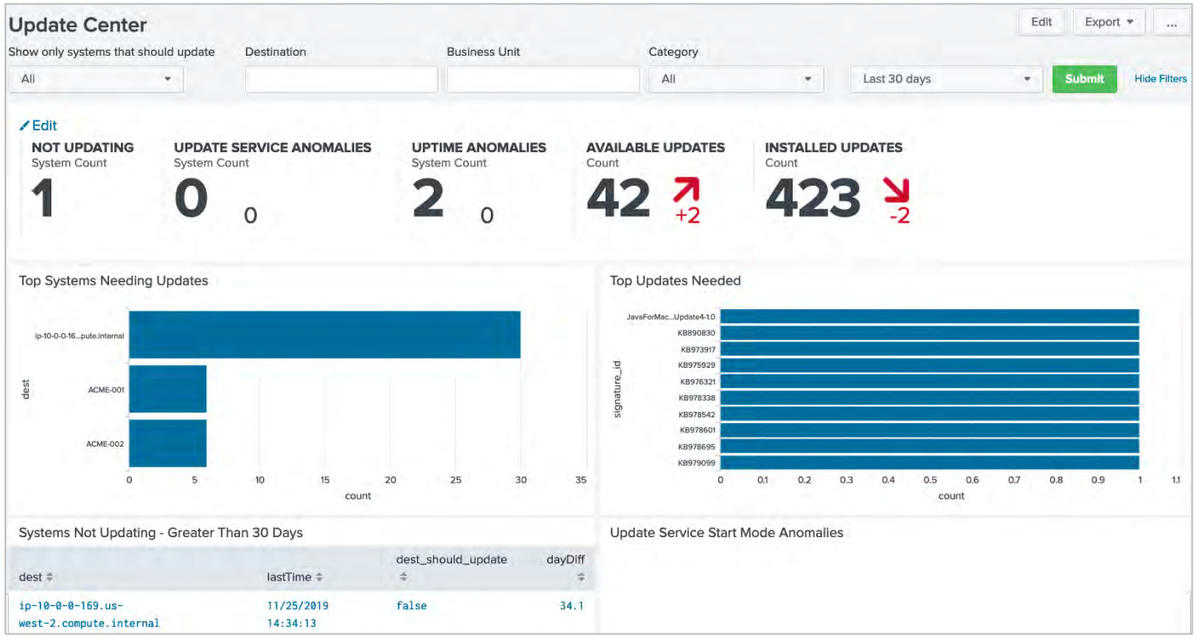
O/S statistics & versions in use



Search interface for update events

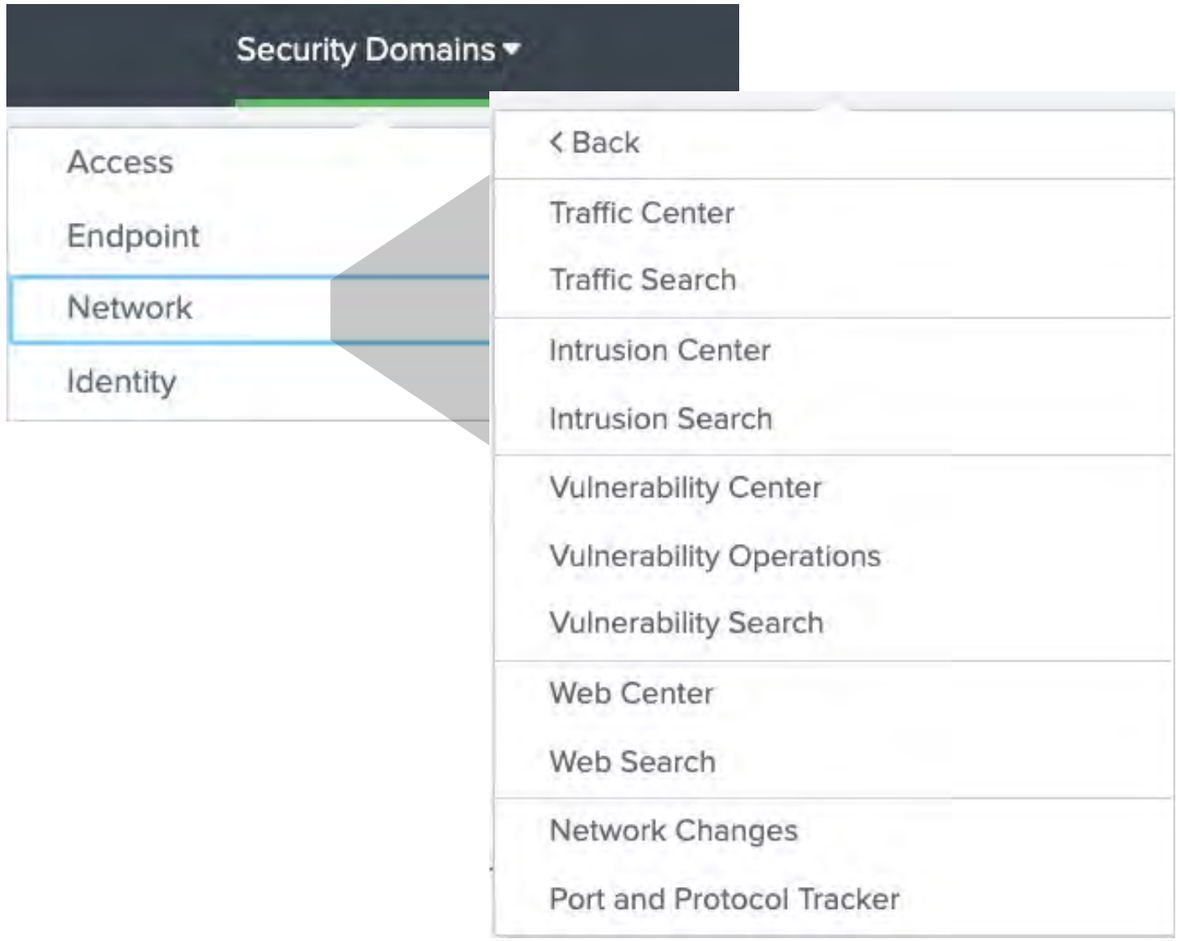


Patches and other software update statistics



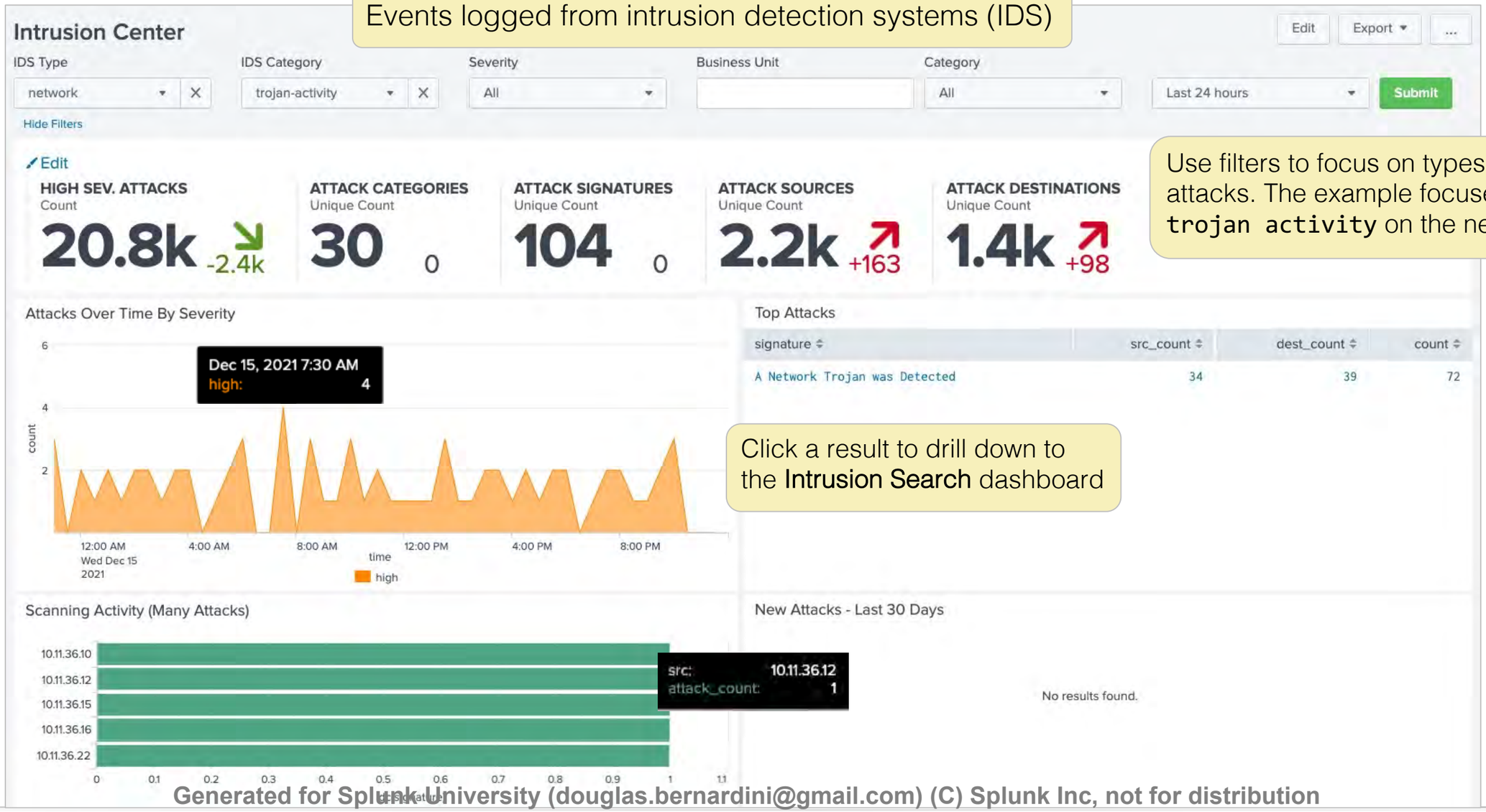
Network Domain

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



Network > Intrusion Center

Events logged from intrusion detection systems (IDS)

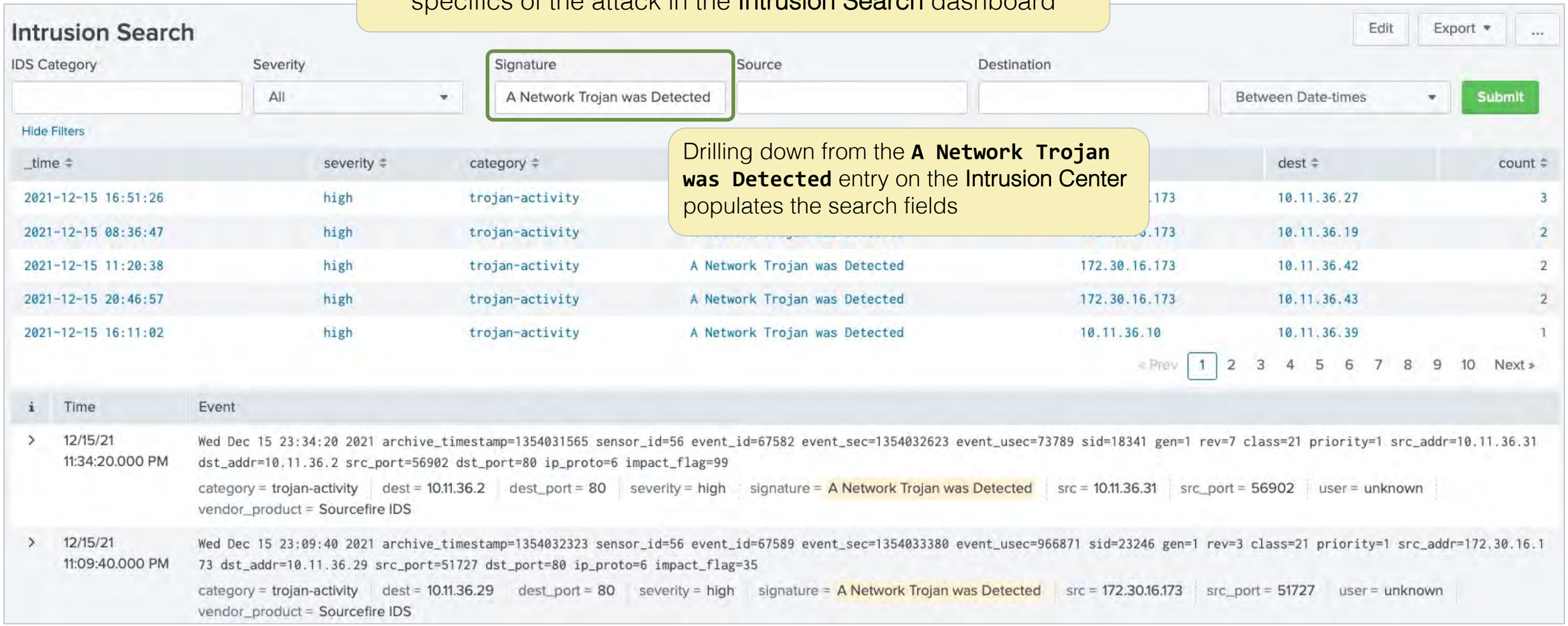


Use filters to focus on types of attacks. The example focuses on `trojan activity` on the network

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

Network > Intrusion Search

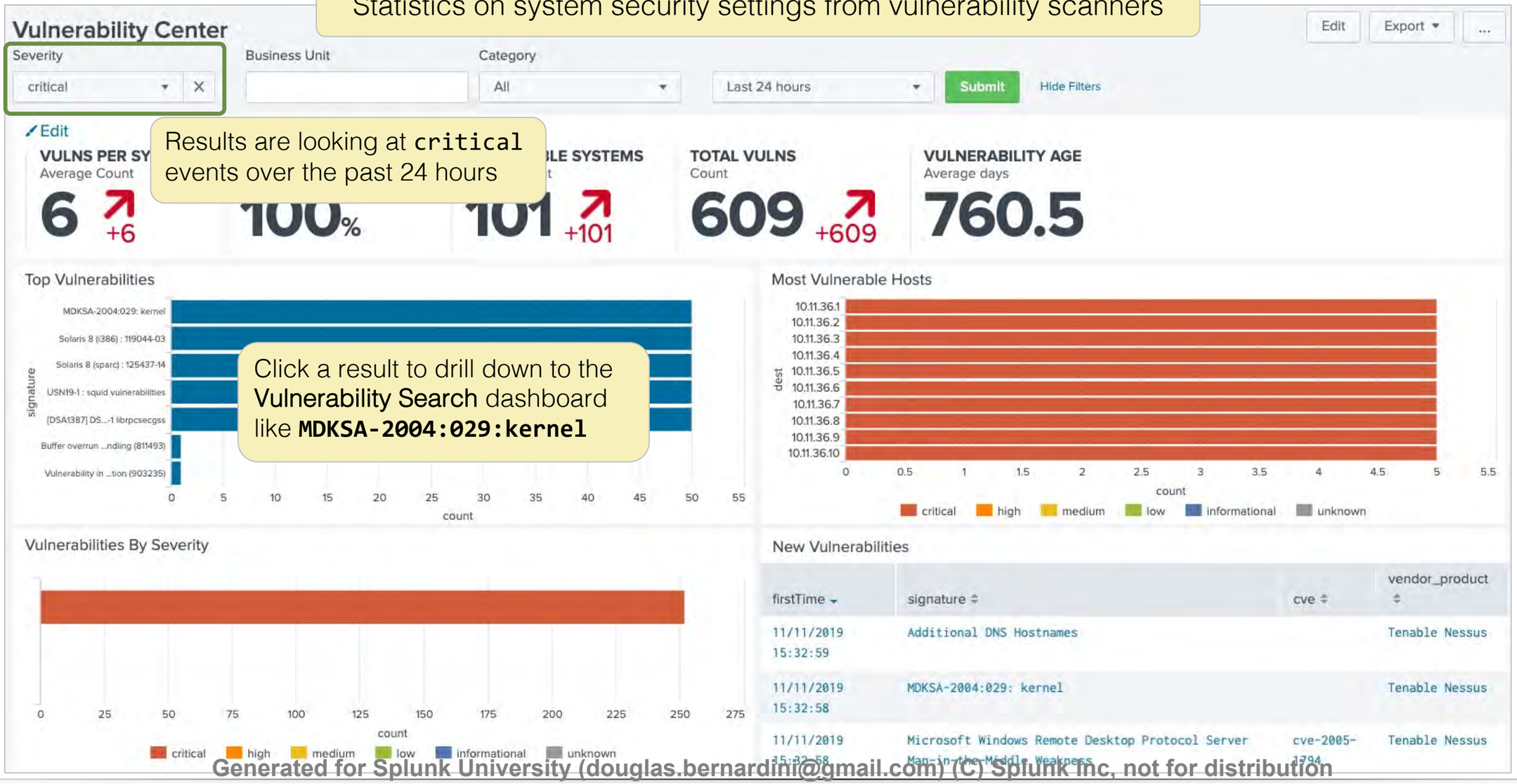
Clicking on a result in the **Intrusion Center** displays the specifics of the attack in the **Intrusion Search** dashboard



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

Network > Vulnerability Center

Statistics on system security settings from vulnerability scanners

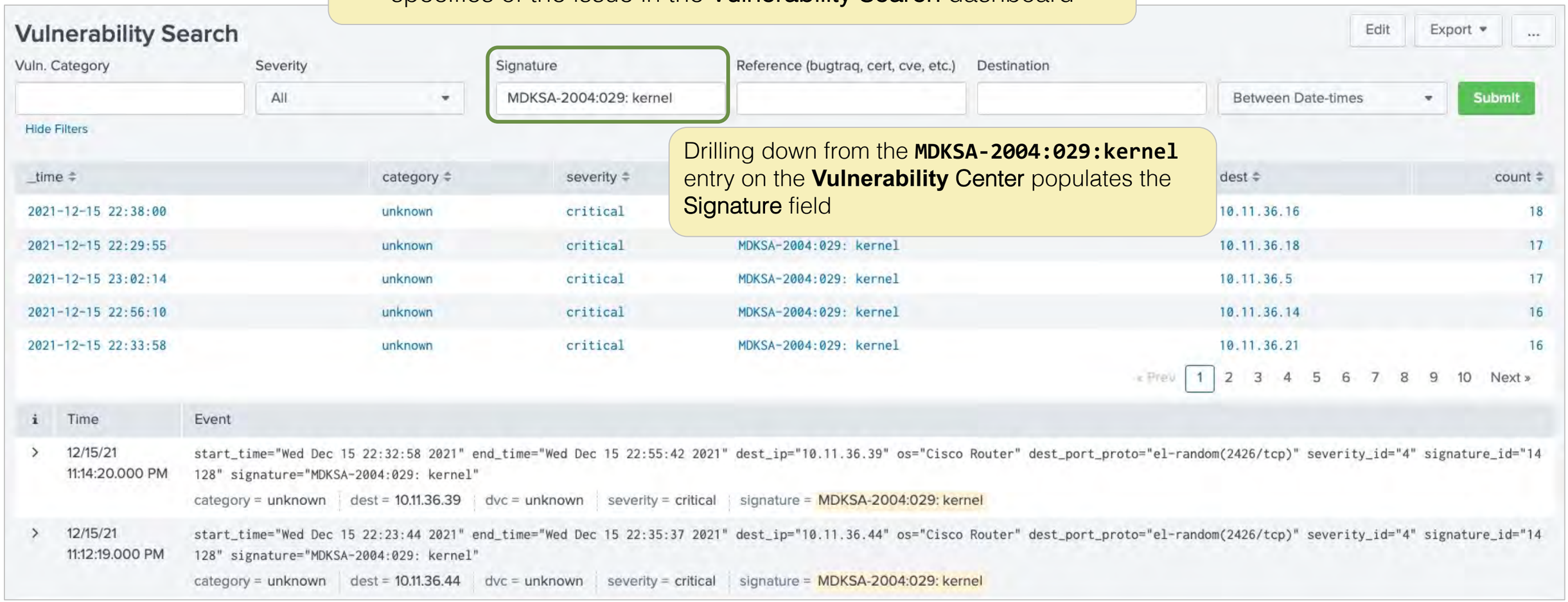


Results are looking at **`critical`** events over the past 24 hours

Click a result to drill down to the **Vulnerability Search** dashboard like **`MDKSA-2004:029:kernel`**

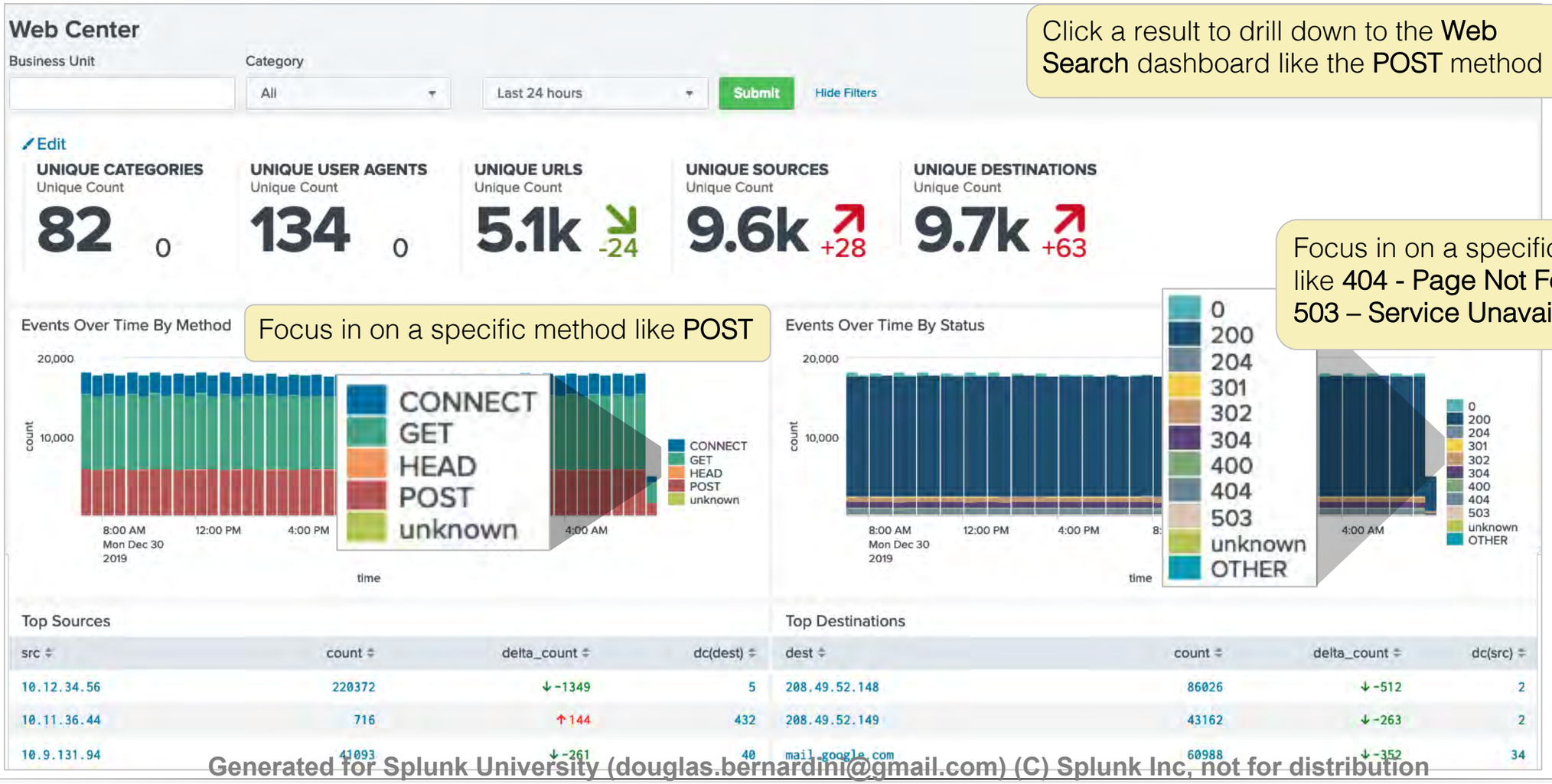
Network > Vulnerability Search

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



Network > Web Center

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



Click a result to drill down to the **Web Search** dashboard like the **POST** method

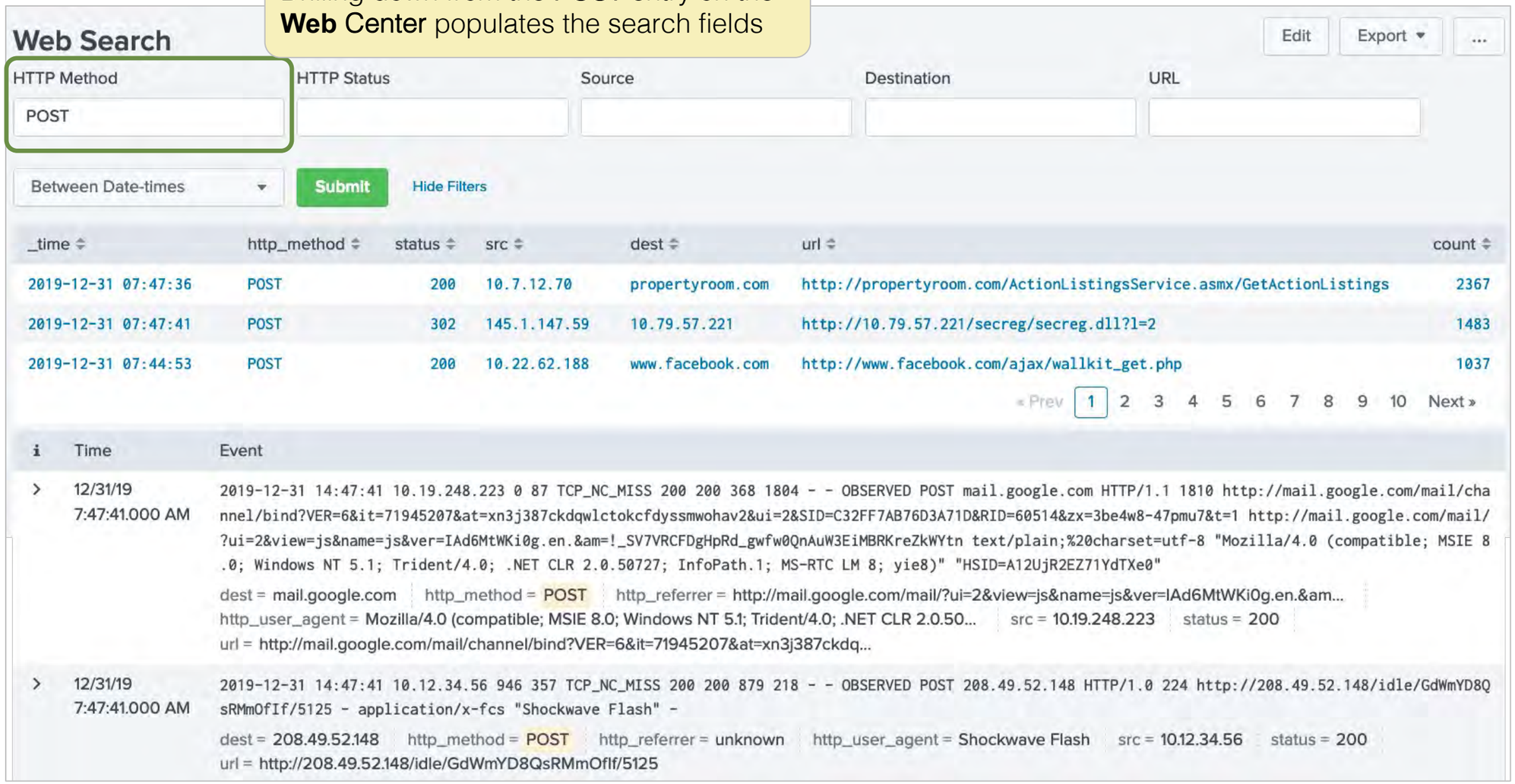
Focus in on a specific method like **POST**

Focus in on a specific status like **404 - Page Not Found** or **503 – Service Unavailable**

 | 25 May 2022

Network > Web Search

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



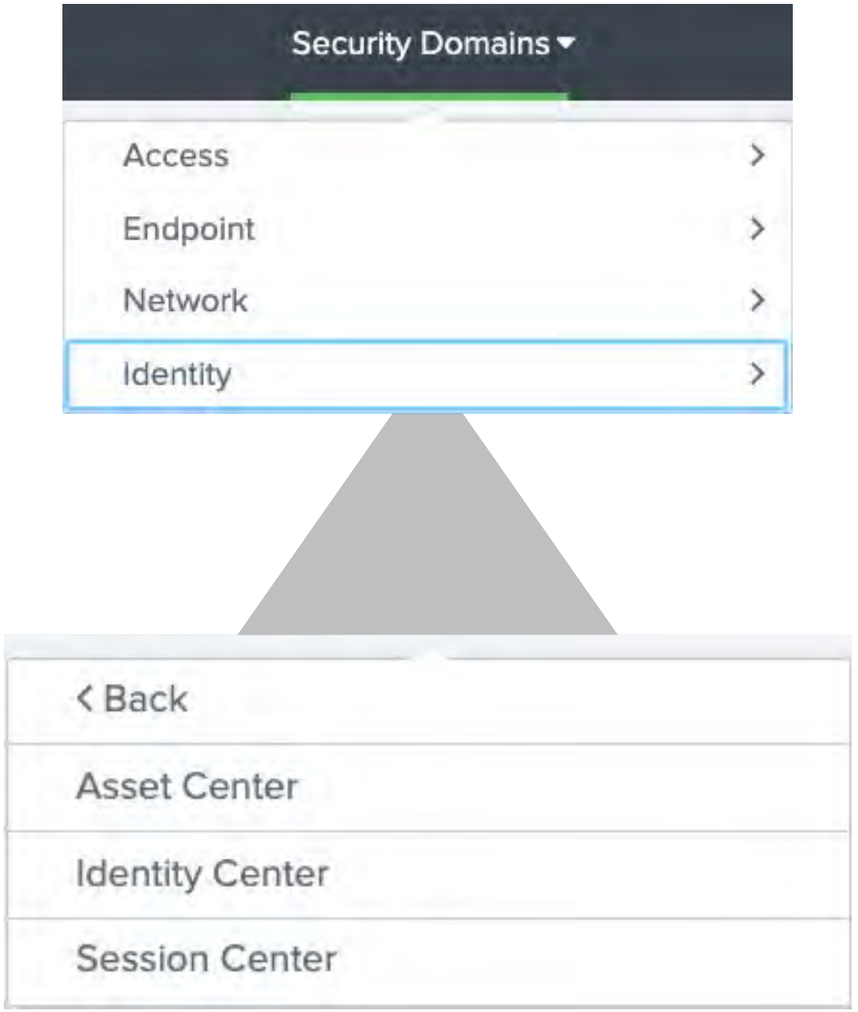
Other Network Domain Dashboards

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

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

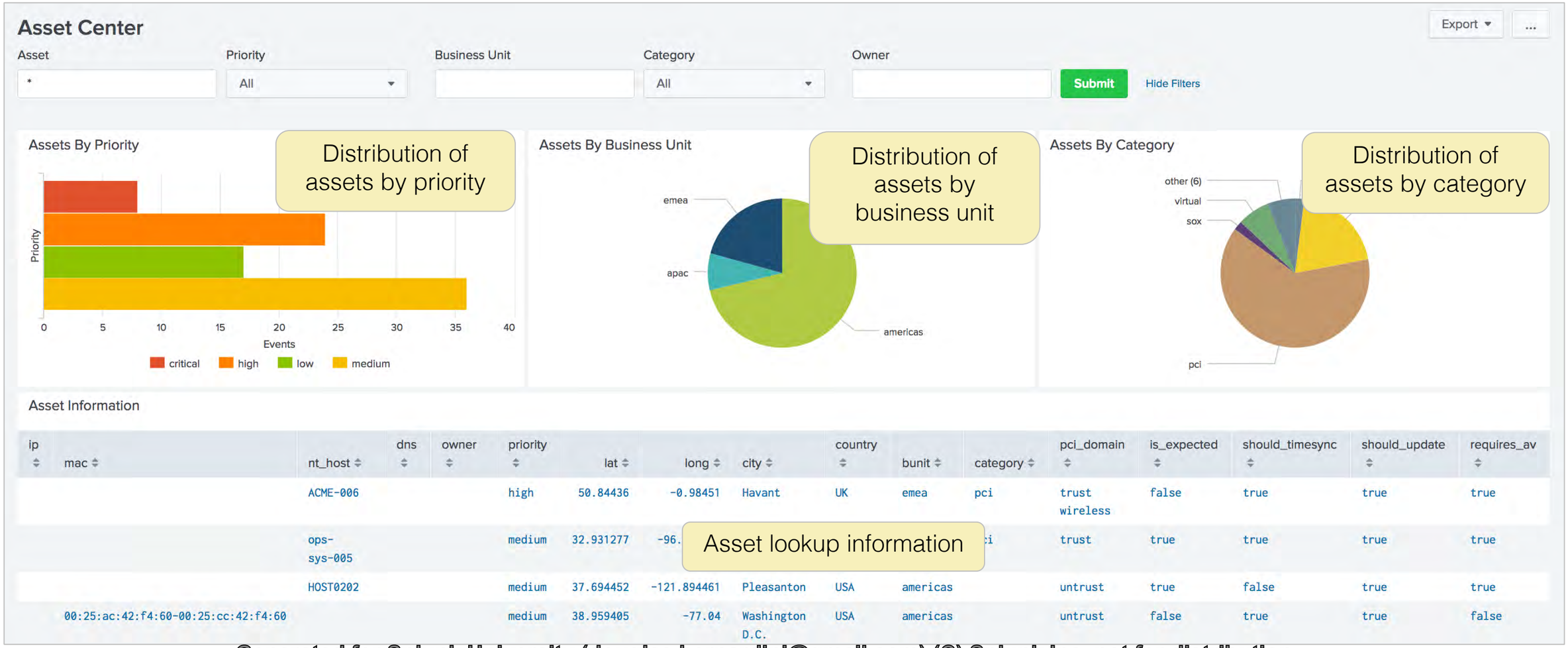
Identity Domain

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



Identity > Asset Center

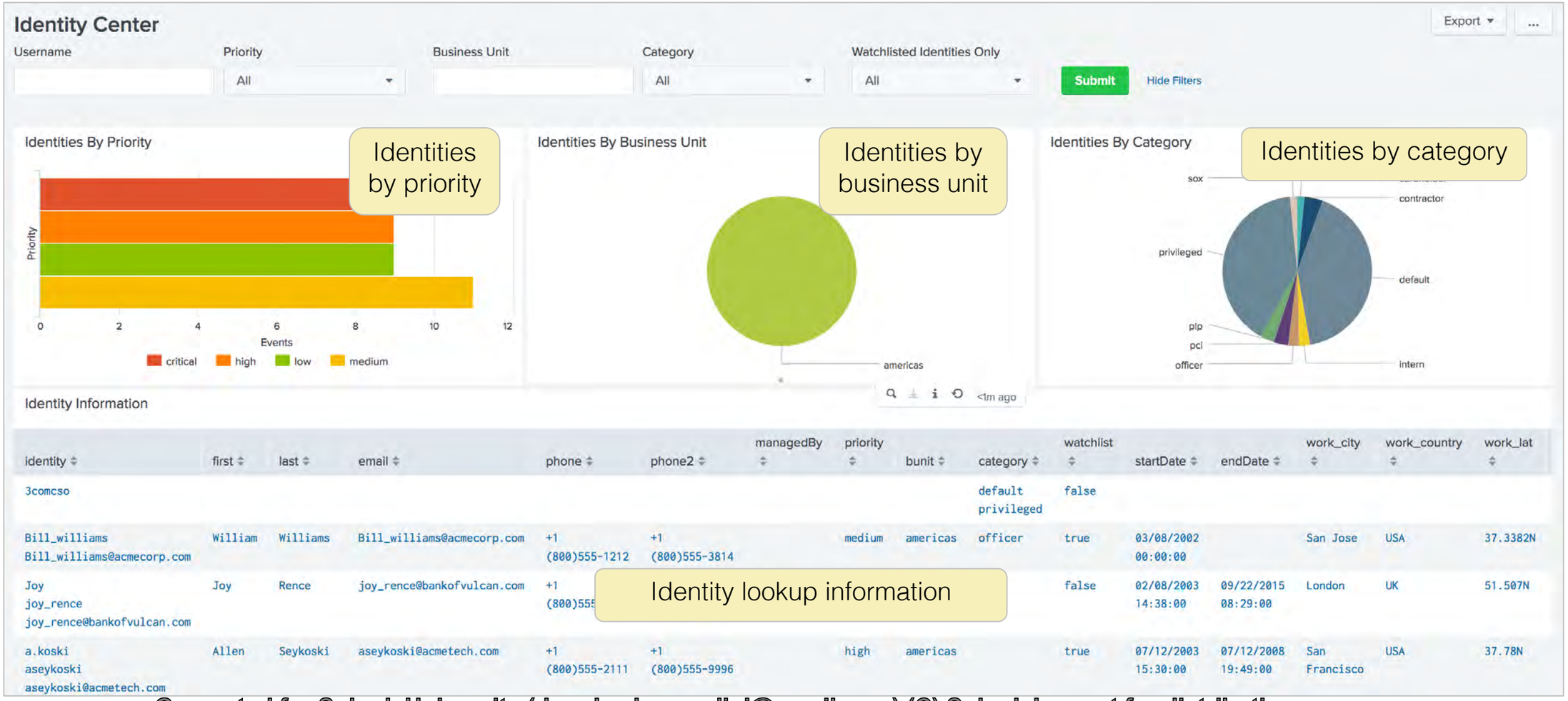
Security Domains > Identity > Asset Center



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

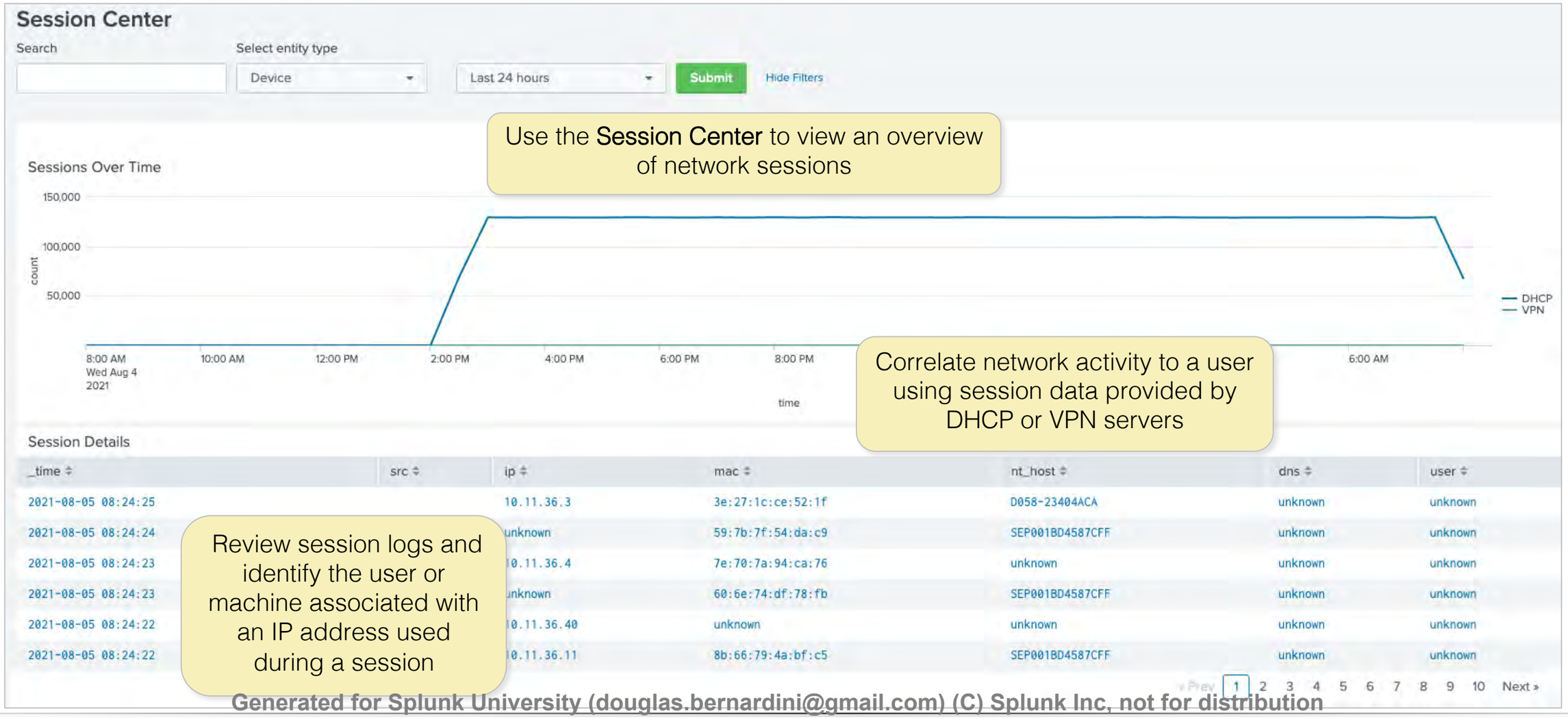
Identity > Identity Center

Security Domains > Identity > Identity Center



Identity > Session Center

Security Domains > Identity > Session Center



Use the **Session Center** to view an overview of network sessions

Correlate network activity to a user using session data provided by DHCP or VPN servers

Review session logs and identify the user or machine associated with an IP address used during a session

Module 6 Lab: Using Security Domain Dashboards

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

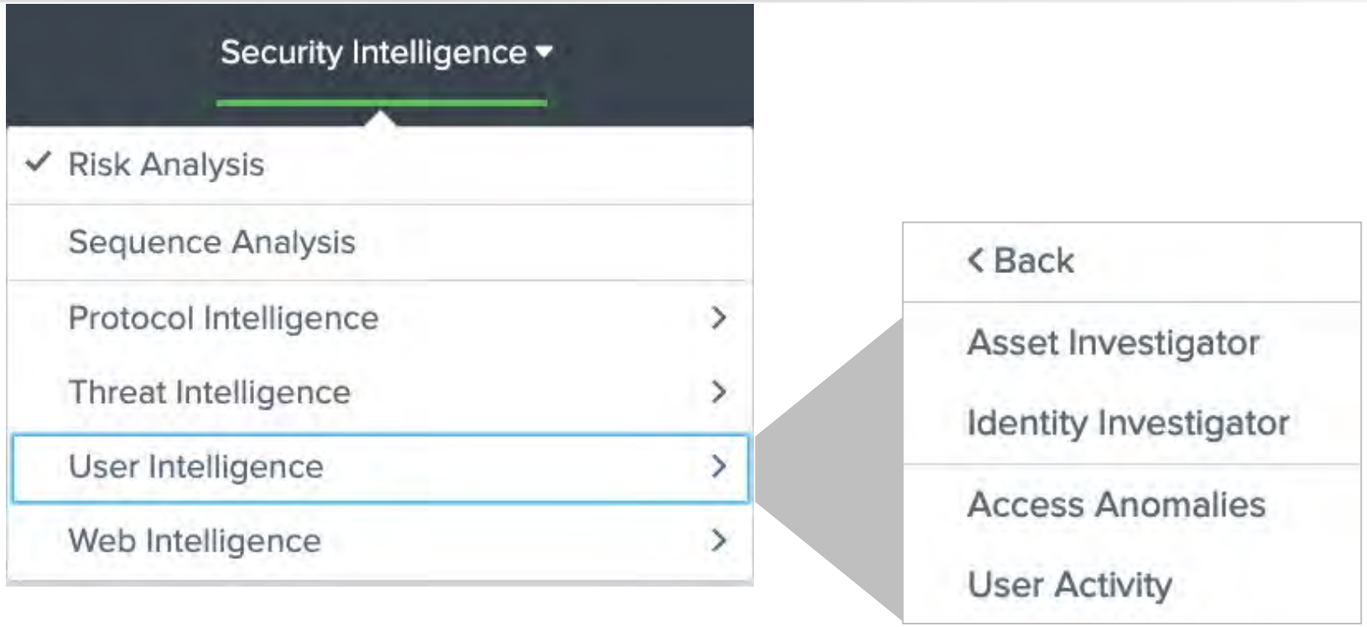
Module 7:
User Intelligence

Objectives

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

Security Intelligence > User Intelligence

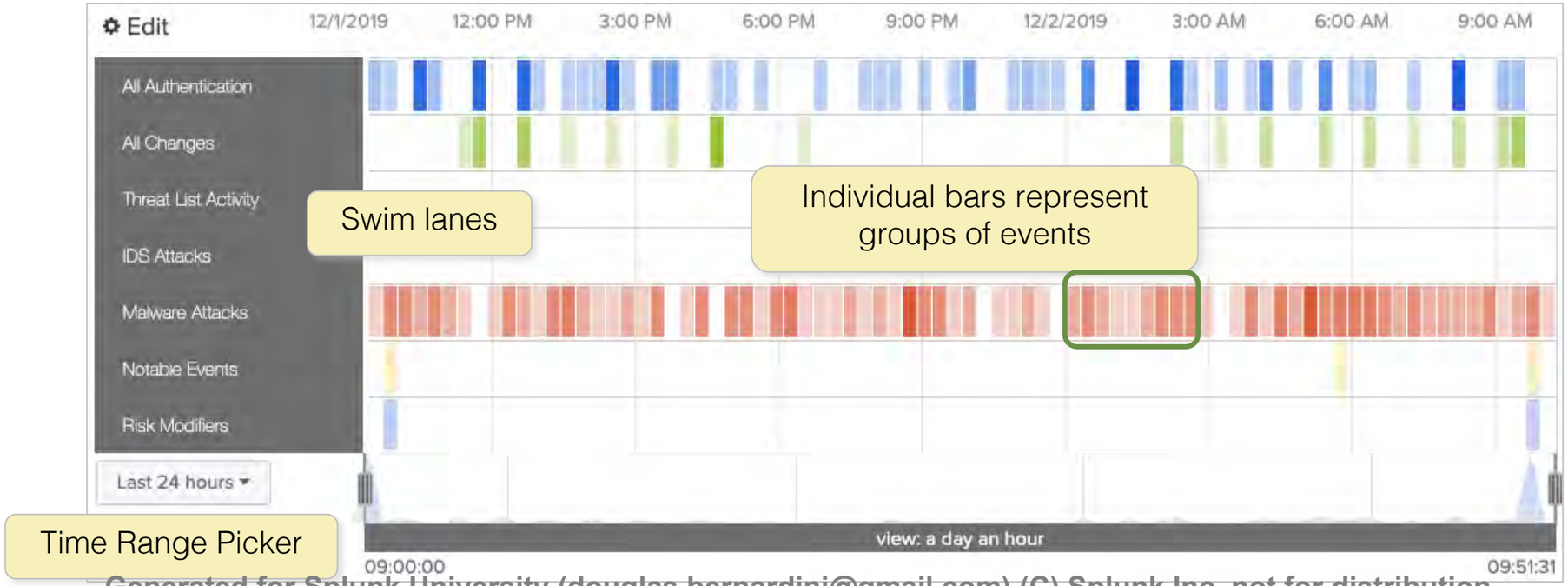
User intelligence tools provide the security practitioner with analytical tools to find potential internal threats



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

Asset and Identity Investigators

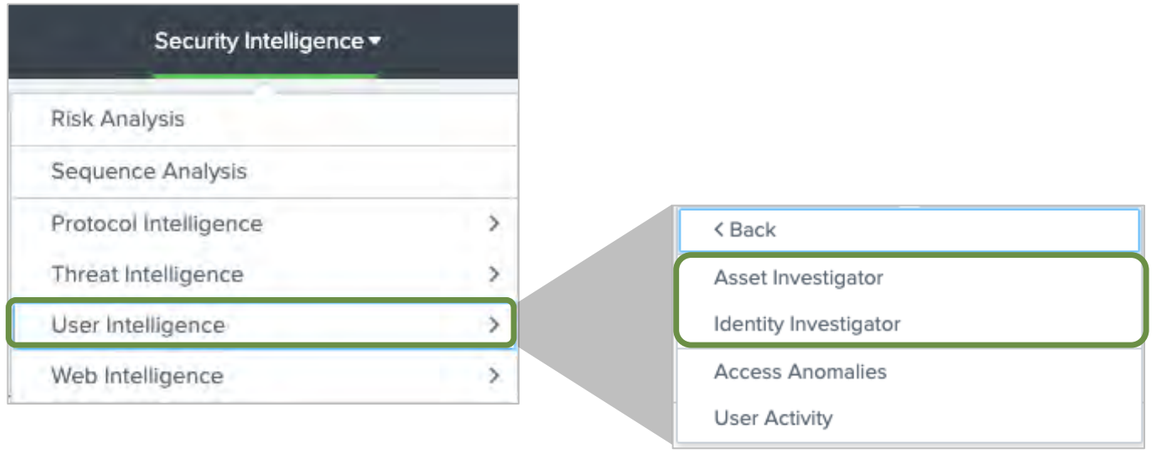
- Investigator dashboards allow you to search by an asset or identity for a specific time range
- Both return a time-sequenced set of **swim lanes** showing activity for that asset or identity

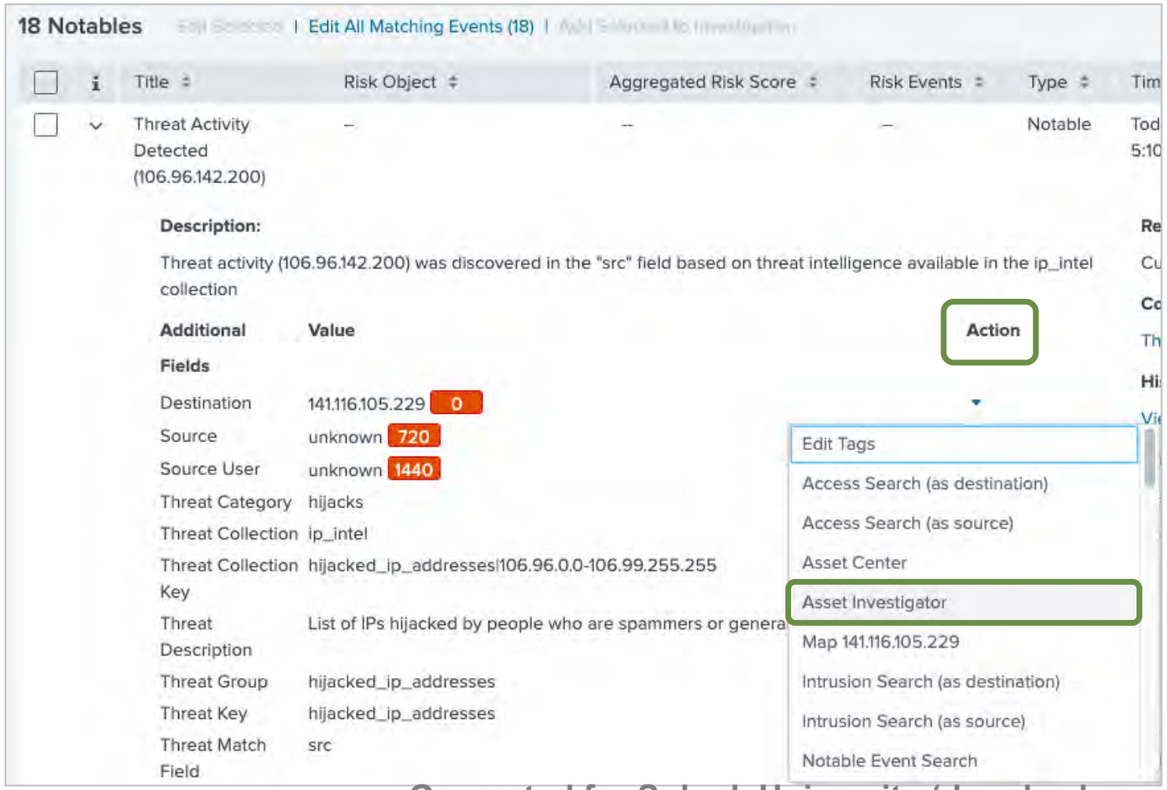


Accessing the Investigators

Access investigators

From the **User Intelligence** menu

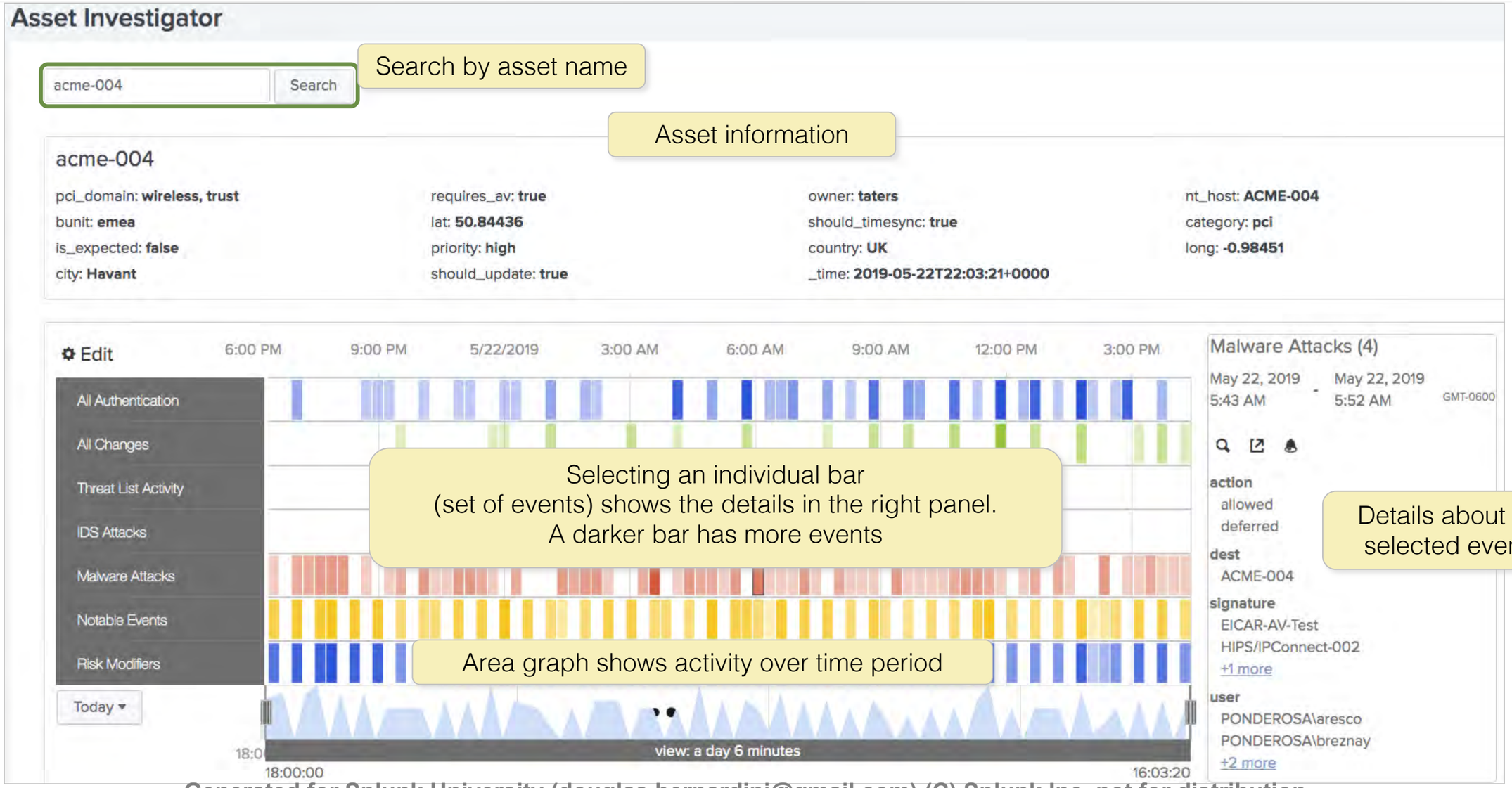




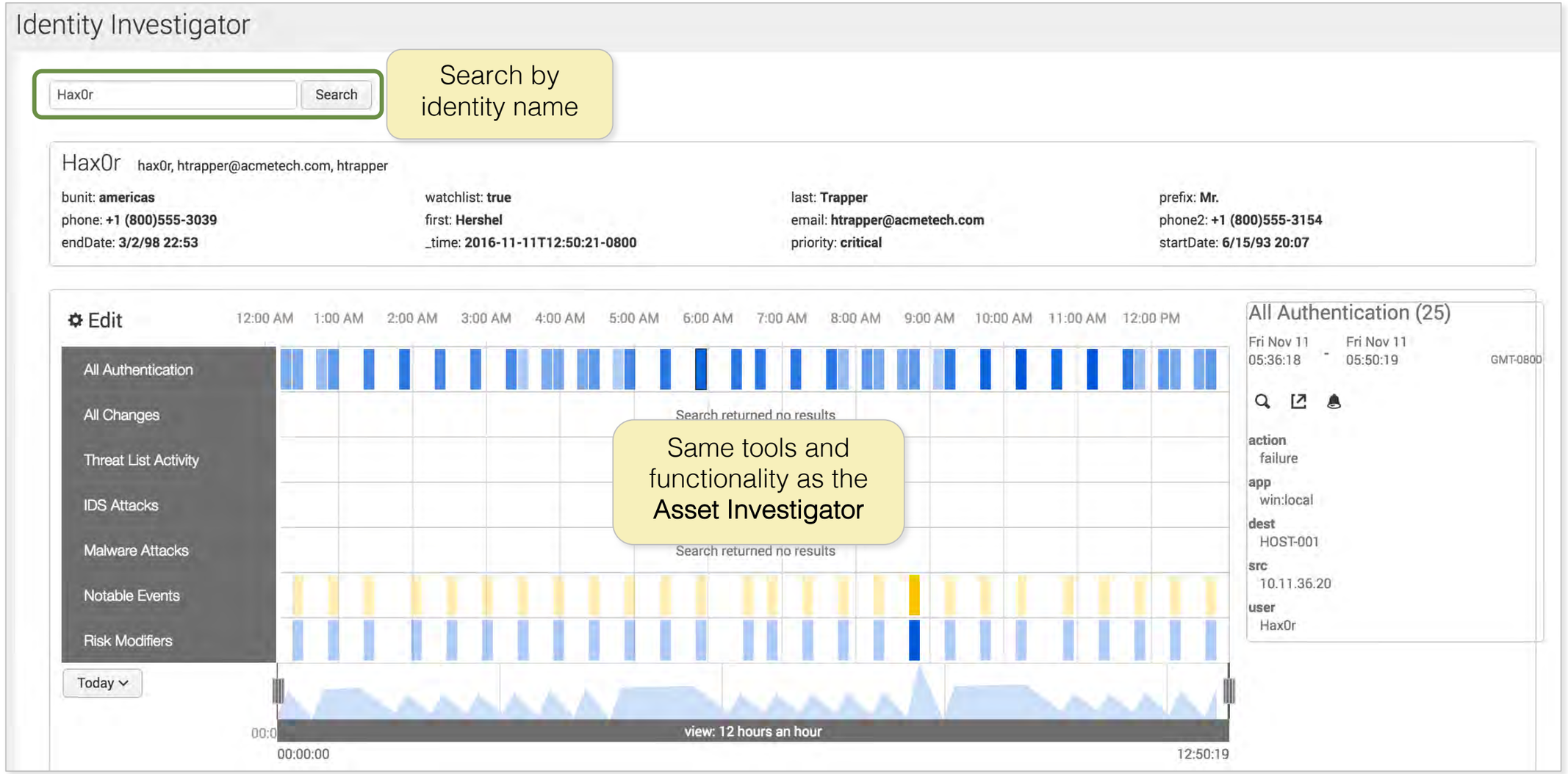
From a field **Action** menu in an **Incident Review** event

- Asset: `dest`, `src`, `ip`, `host`
- Identity: `user`, `src_user`

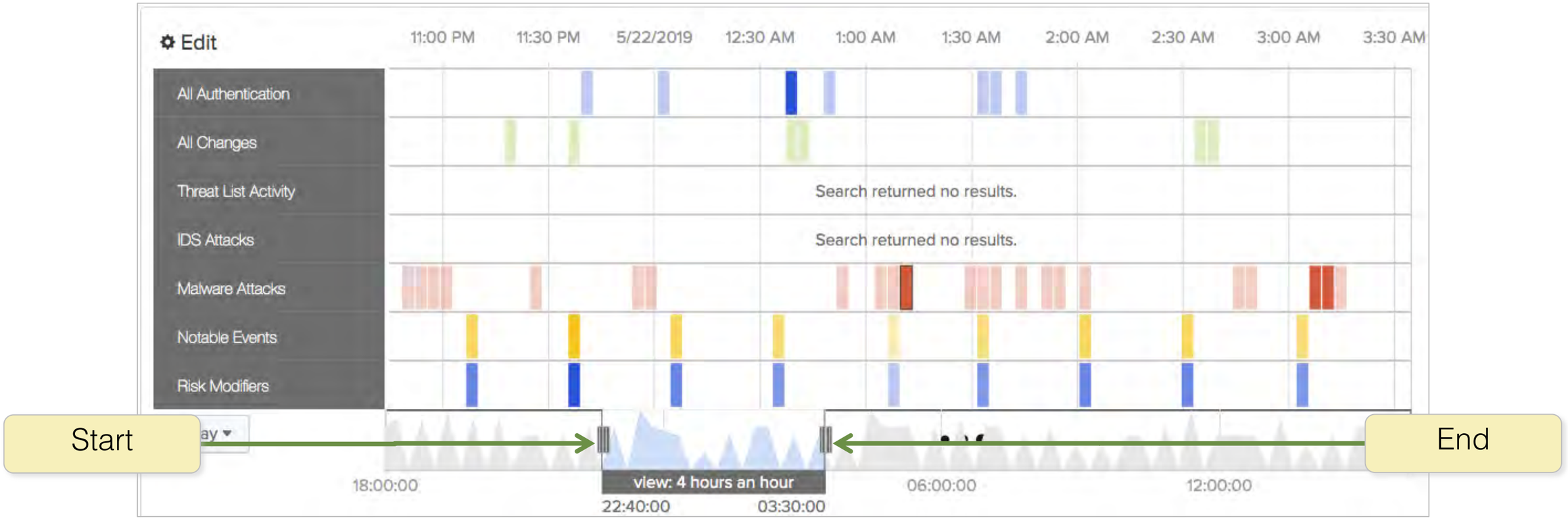
Asset Investigator



Identity Investigator



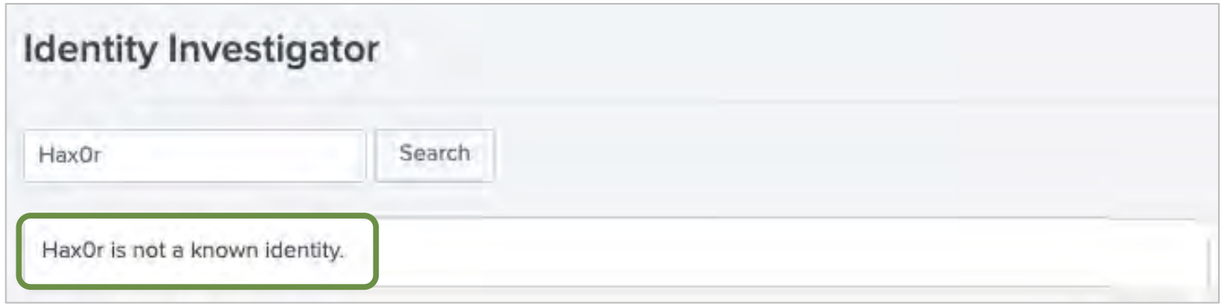
Pan and Zoom



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

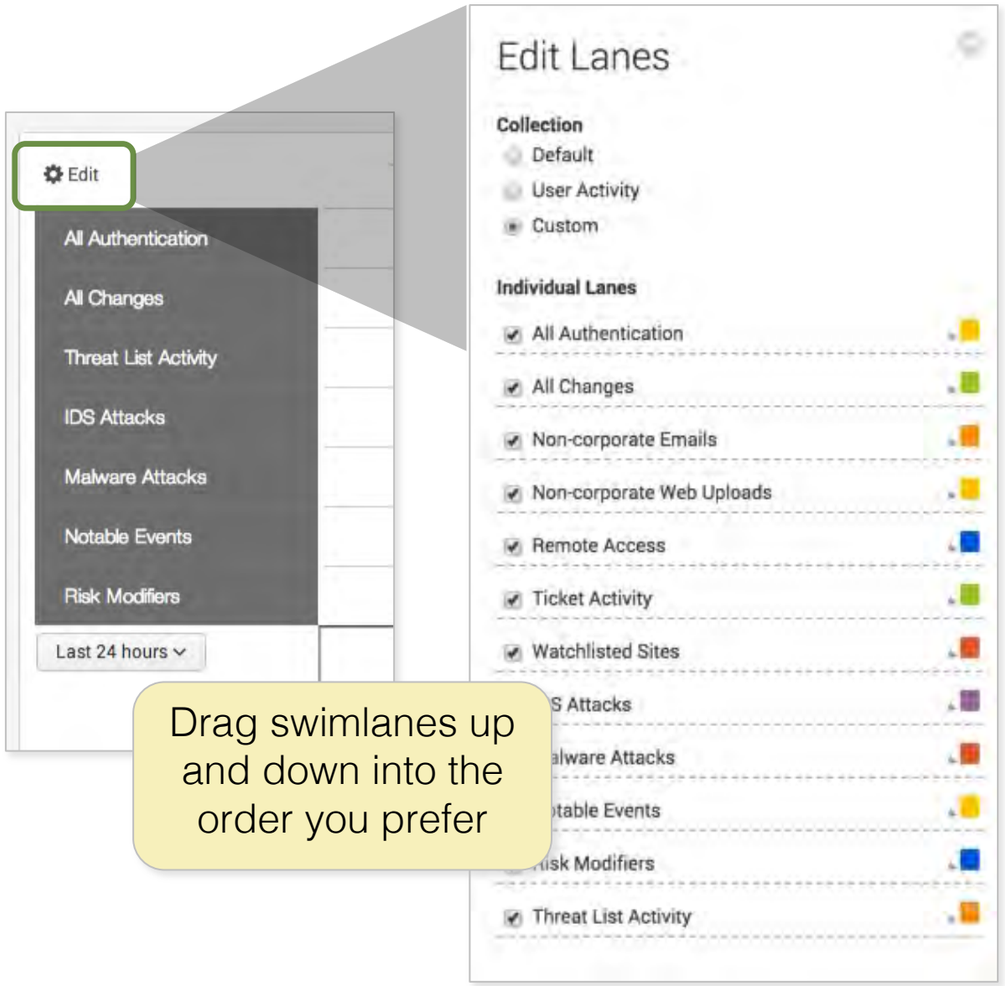
Missing Information

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

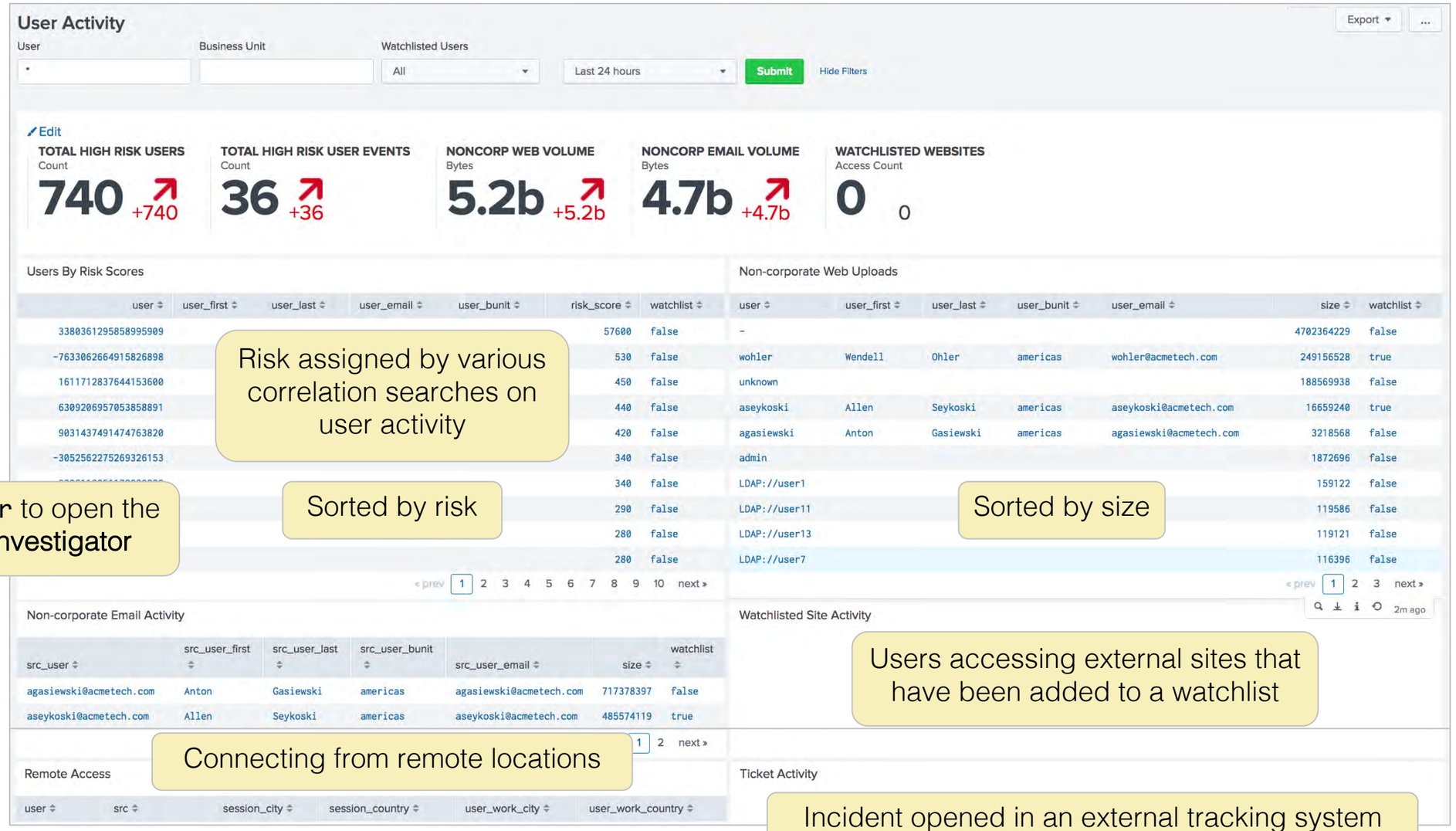


Configuring Swim Lanes

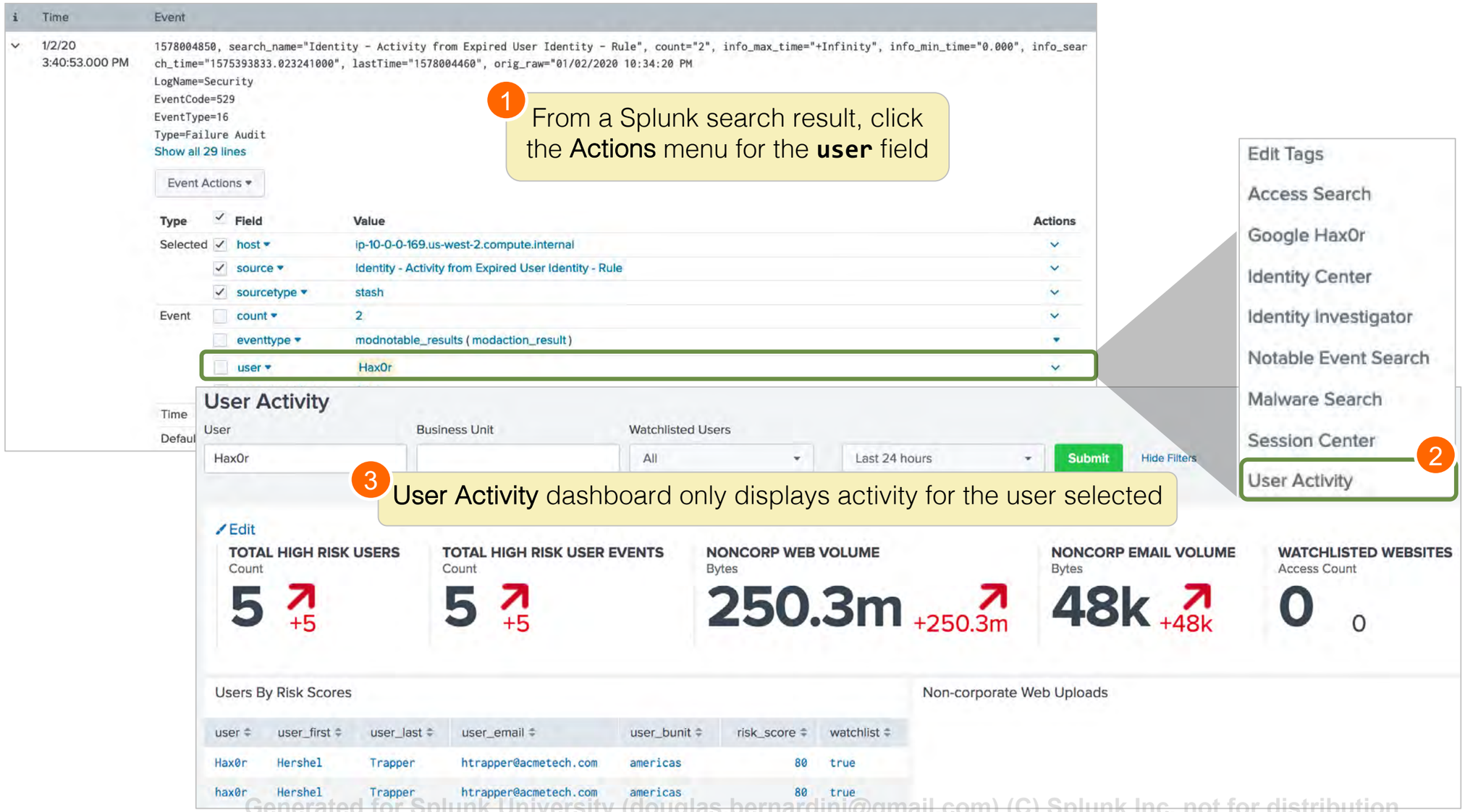
- Click **Edit** and select a collection of swim lanes
- Use the **Custom** collection to select specific swim lanes
- Customize swim lane colors
- ES Admins can add new swim lanes and set overall defaults and permissions per role
- Changes are not saved



User Intelligence > User Activity



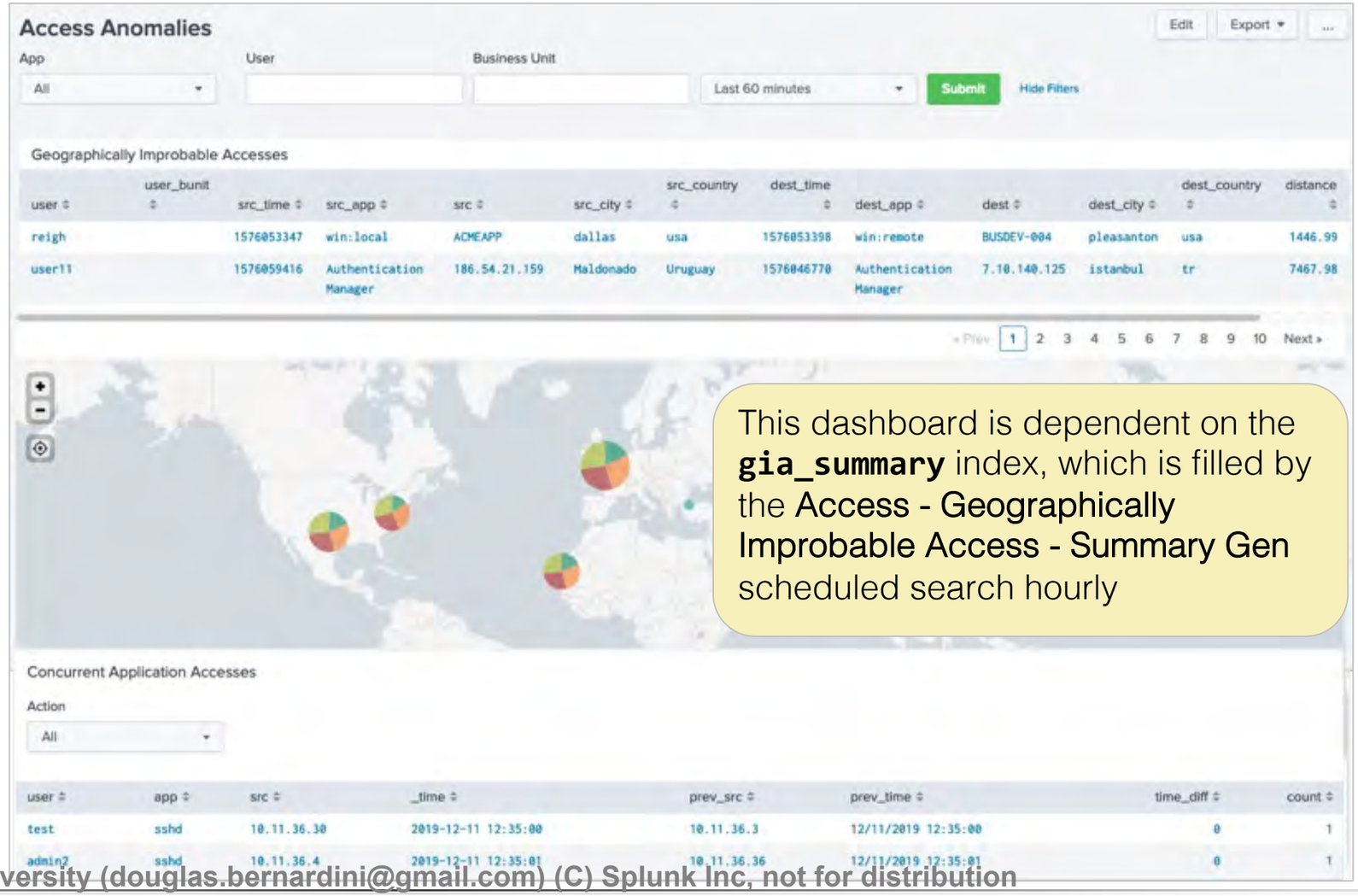
Access User Activity from a Source Event



Access Anomalies Dashboard

Security Intelligence > User Intelligence > Access Anomalies

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



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

Important!

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

Module 7 Lab: User Intelligence

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

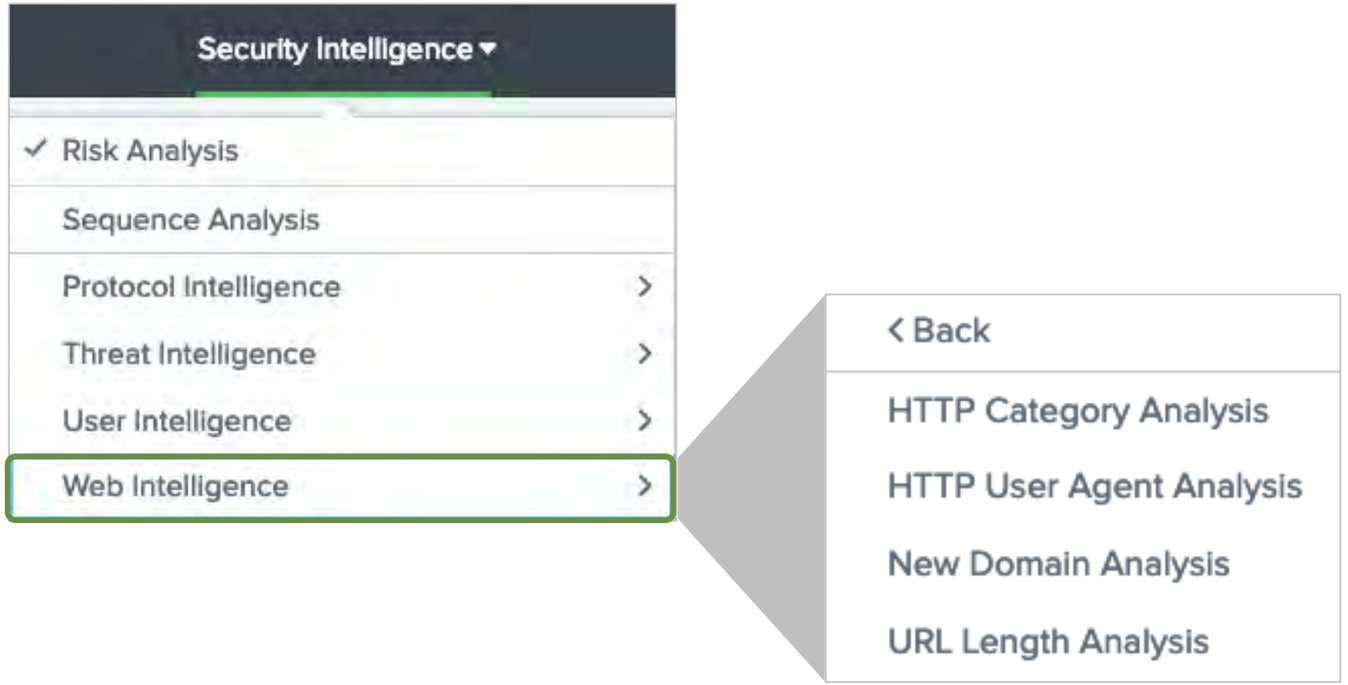
Module 8:
Web Intelligence

Objectives

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

Security Intelligence > Web Intelligence

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



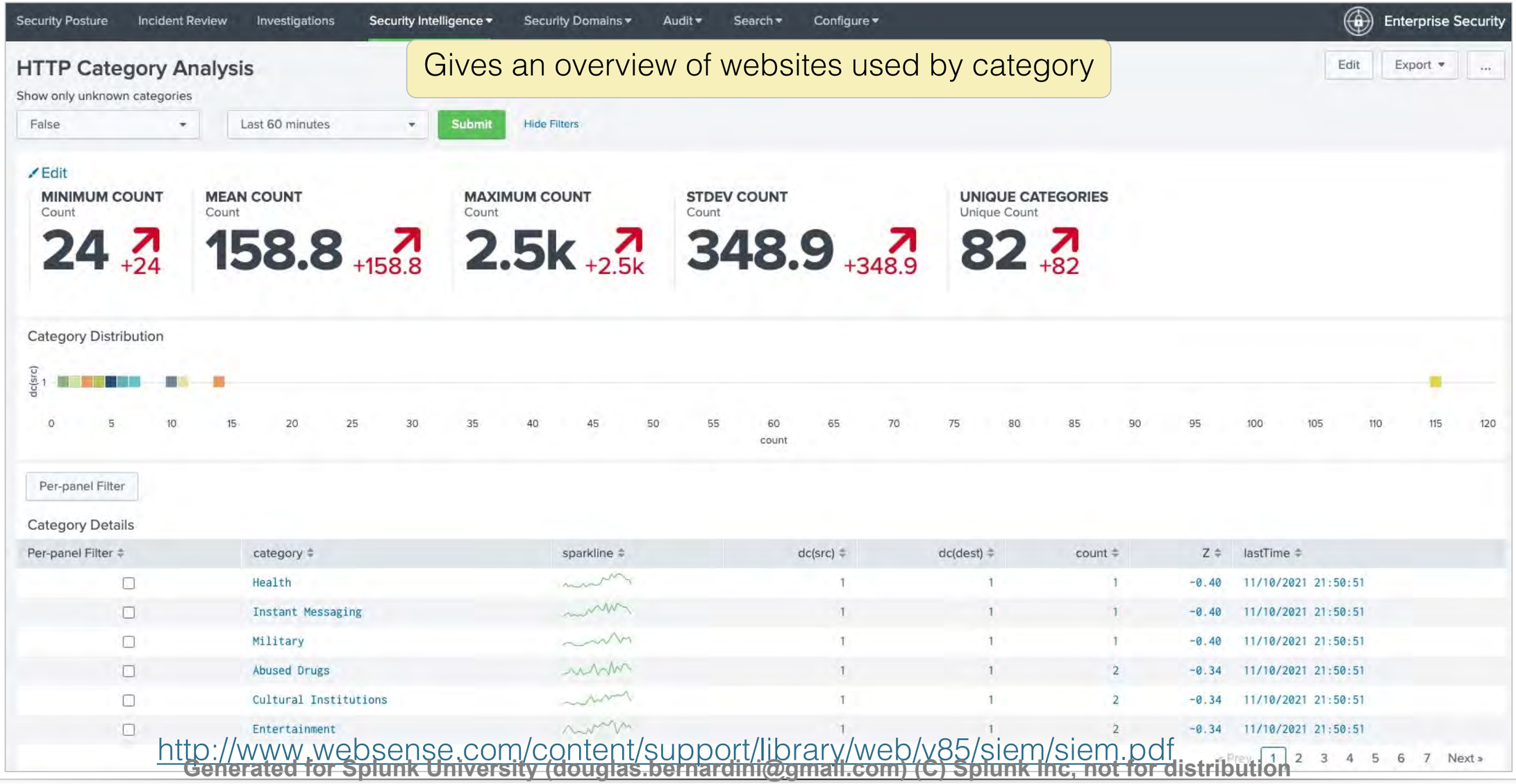
HTTP Category	Explore the types of websites being accessed in the network
HTTP User Agent	Examine the web user agents being used on the network
New Domain	See what external domains are being accessed
URL Length	Examine request URLs for unusual contents

Uses for Web Intelligence Dashboards

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

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

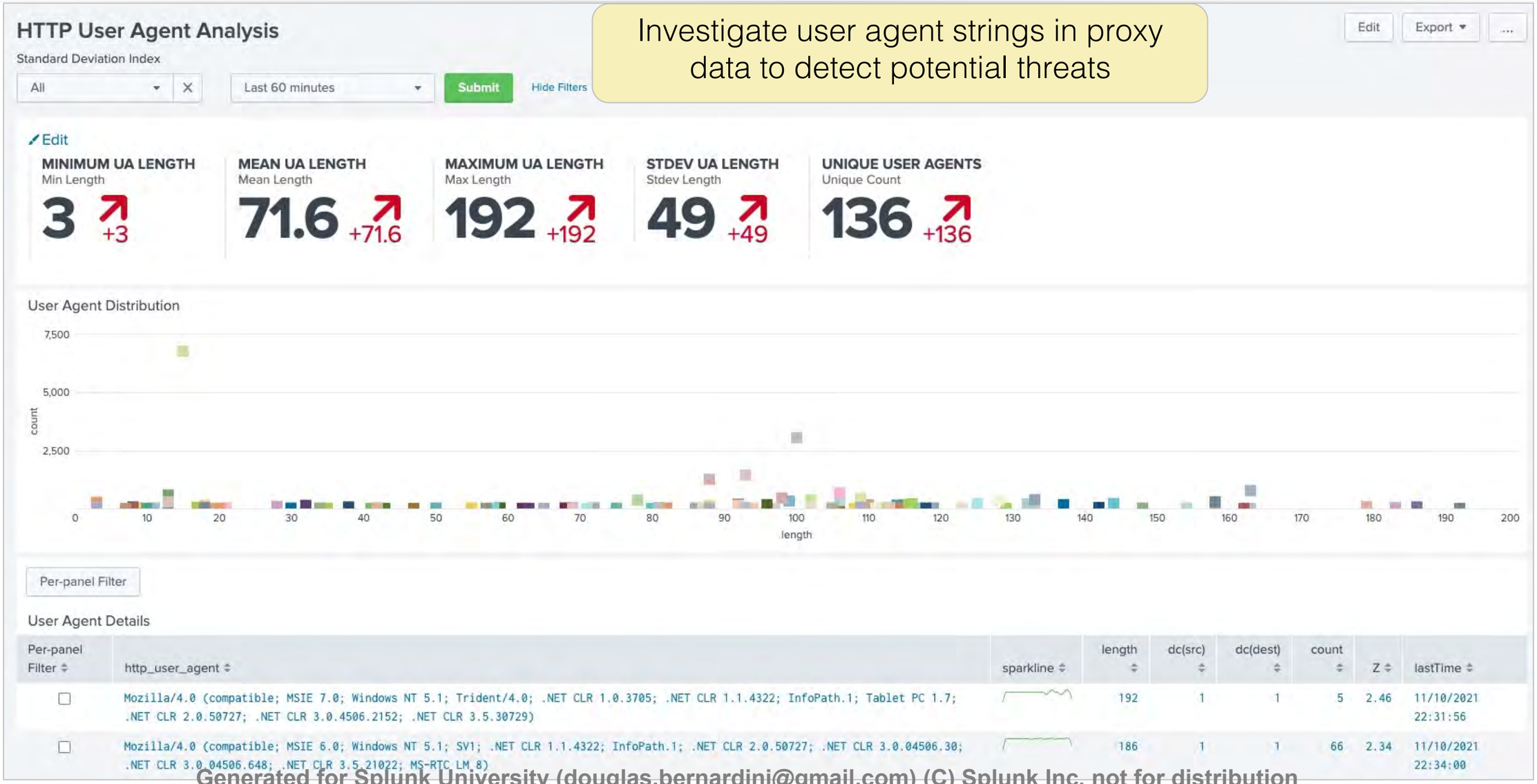
HTTP Category Analysis



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

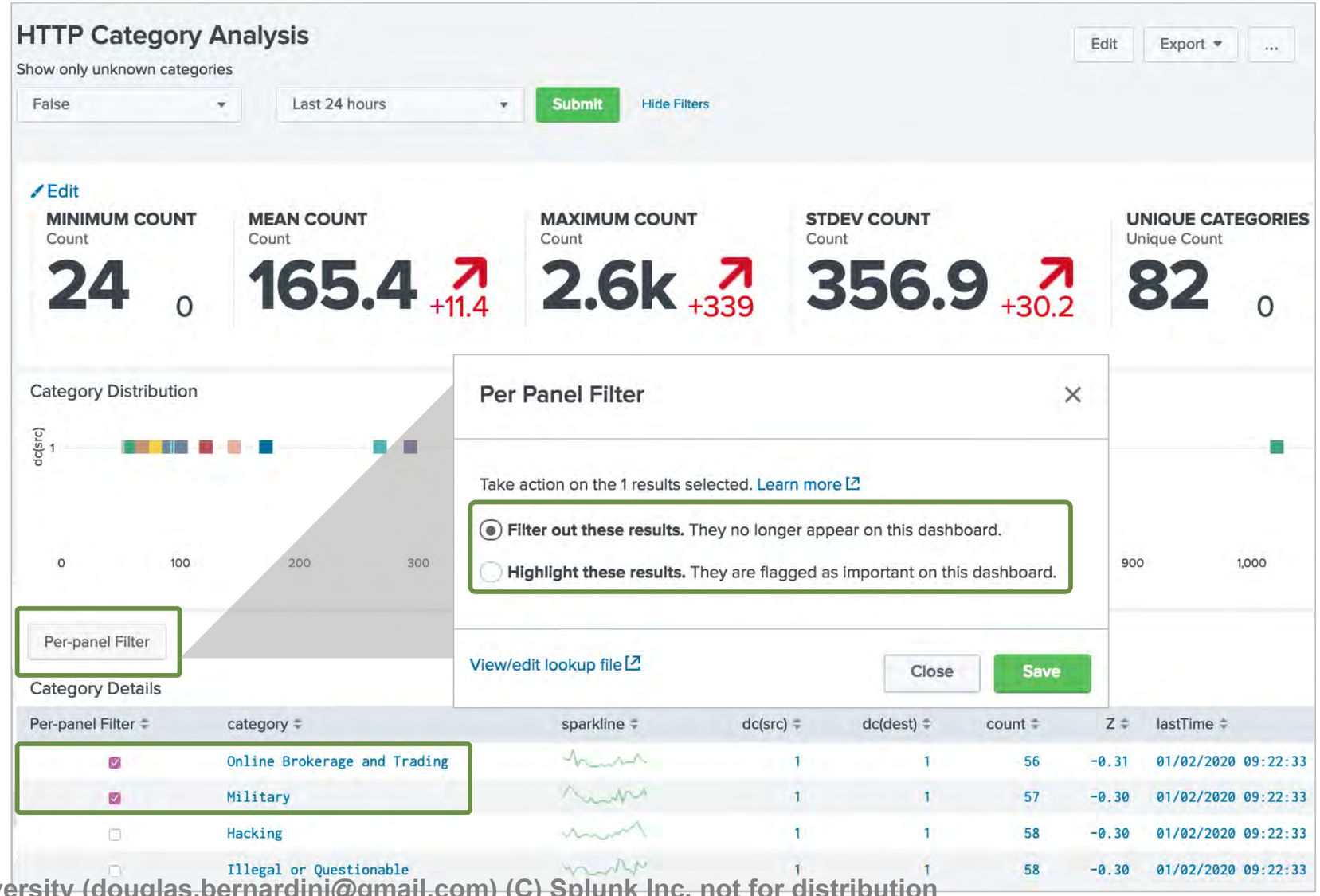
HTTP User Agent Analysis

Investigate user agent strings in proxy data to detect potential threats



Per Panel Filter

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



Note

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

Filtered vs. Highlighted Events

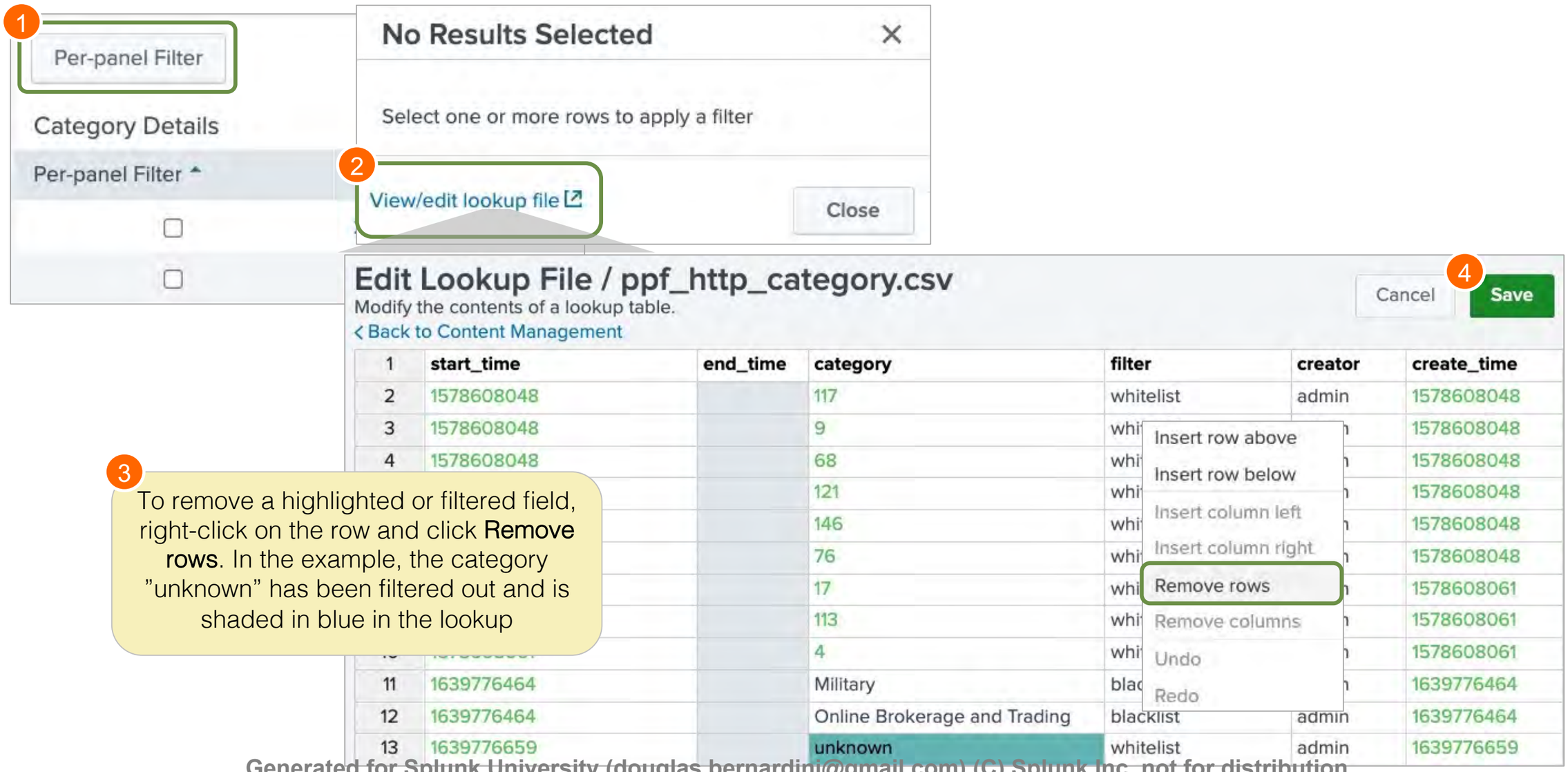
- Filtered events are no longer displayed
- Highlighted events are:
  - Highlighted in the Per-panel Filter column
  - Displayed at the top of the list by default

Per-panel Filter

Category Details

Per-panel Filter	category	sparkline	dc(src)	dc(dest)	count	Z	lastTime
☑	Online Brokerage and Trading		1	1	56	-0.31	01/02/2020 09:22:33
☑	Military		1	1	57	-0.30	01/02/2020 09:22:33
☐	Hacking		1	1	58	-0.30	01/02/2020 09:22:33
☐	Illegal or Questionable		1	1	58	-0.30	01/02/2020 09:22:33
☐	Traditional Religions		1	1	59	-0.30	01/02/2020 09:22:33
☐	Information Technology		1	1	60	-0.30	01/02/2020 09:22:33

Managing Per Panel Filtering Lookups

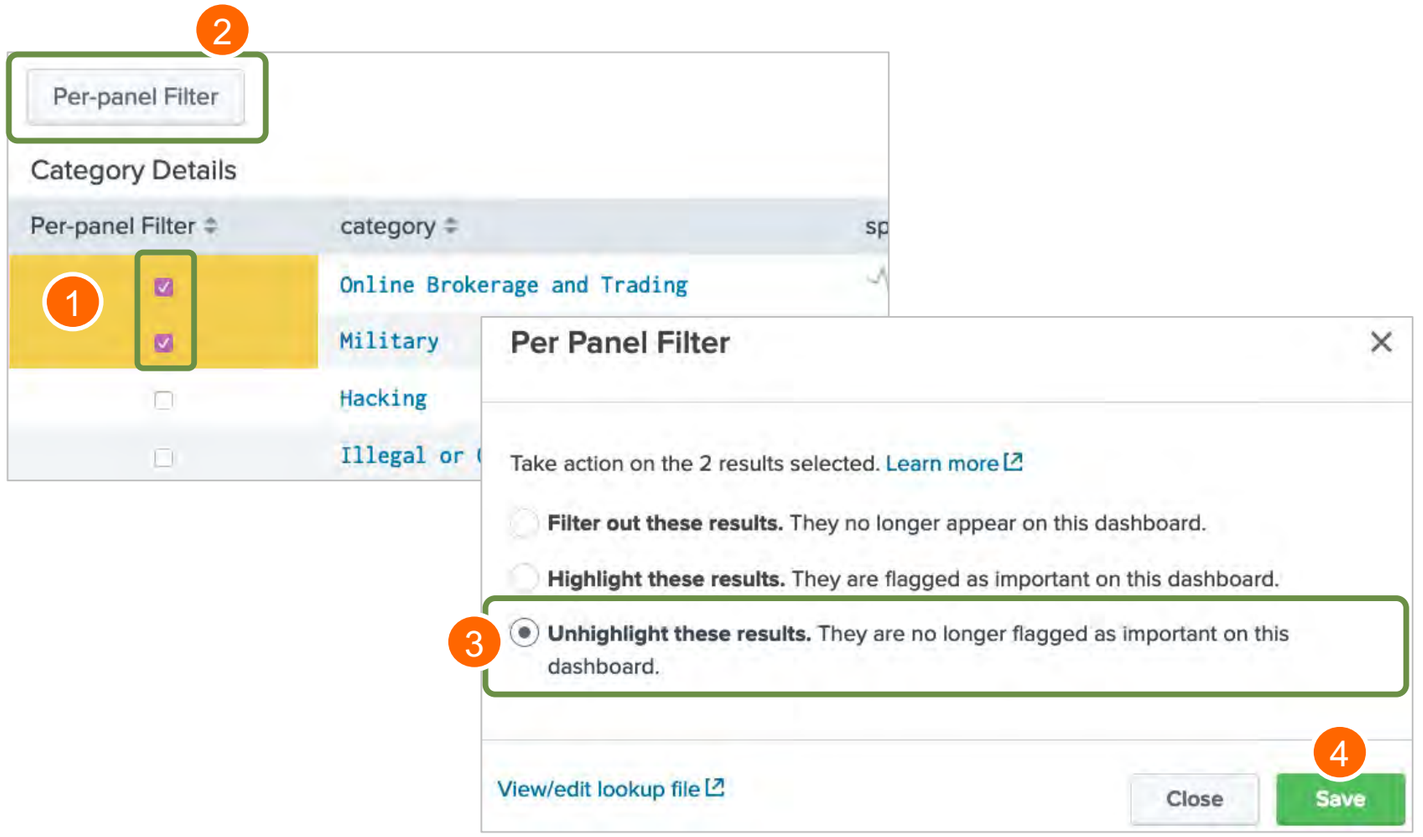


3 To remove a highlighted or filtered field, right-click on the row and click **Remove rows**. In the example, the category "unknown" has been filtered out and is shaded in blue in the lookup

Unhighlighting an Event

If an event is already highlighted

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



Note

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

Module 8 Lab: Web Intelligence

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

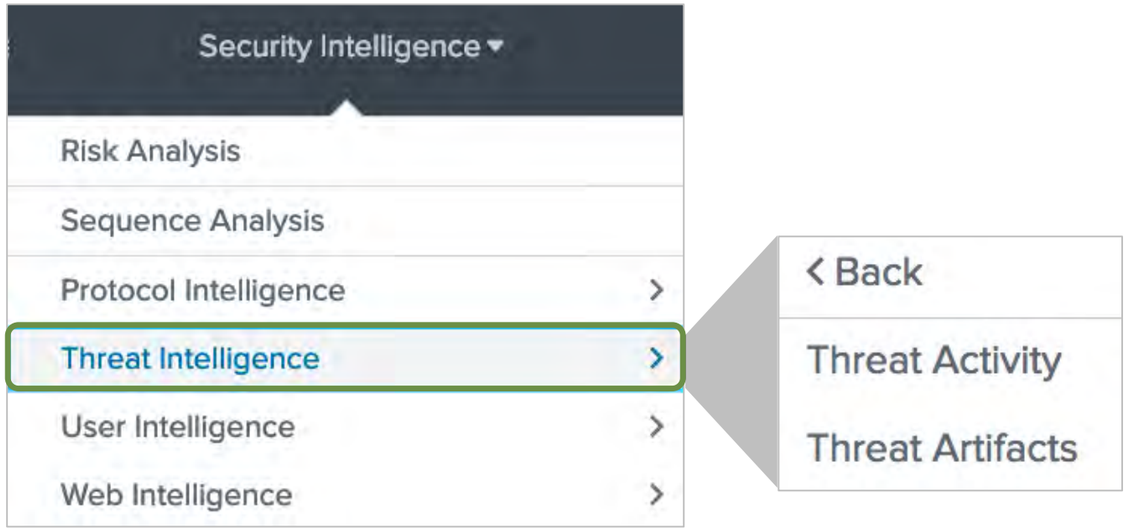
Module 9:
Threat Intelligence

Objectives

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

Security Intelligence > Threat Intelligence

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



Threat Activity	Examine activity from a threat perspective: • which threats have been identified • which systems or users are affected
Threat Artifacts	Examine the details of threat intel that has been downloaded from online threat libraries, or have been added locally

Threat Intelligence Framework

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

Threat Intelligence Administration

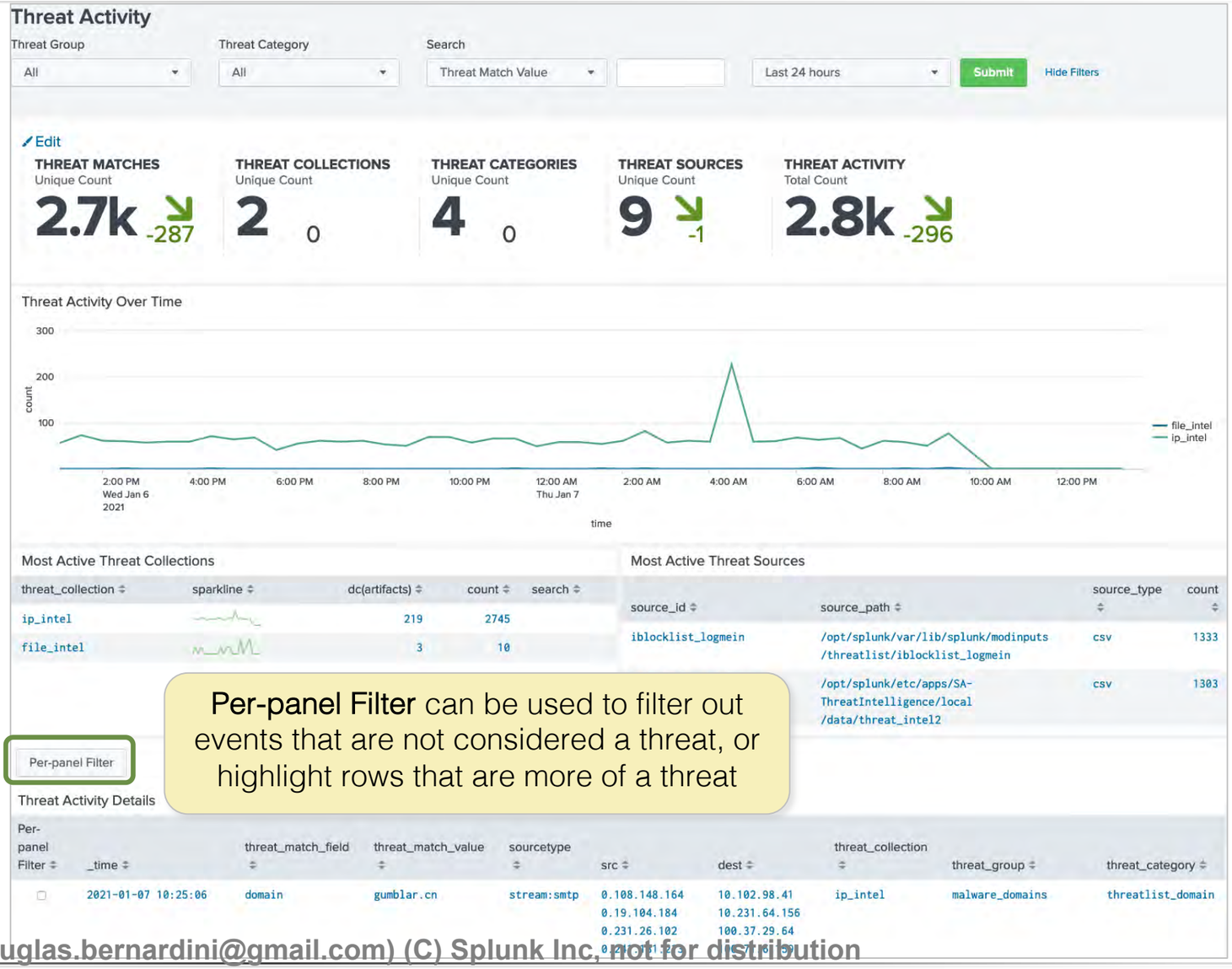
- ES Admins are tasked with managing ES threat intelligence
- Analysts and users can be given the **Edit Intelligence Downloads** permission to manage threat intelligence downloads
- Threat Intelligence can be added to ES by
  - downloading a feed from the Internet
  - uploading a structured file
  -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

Threat Intelligence Configuration

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

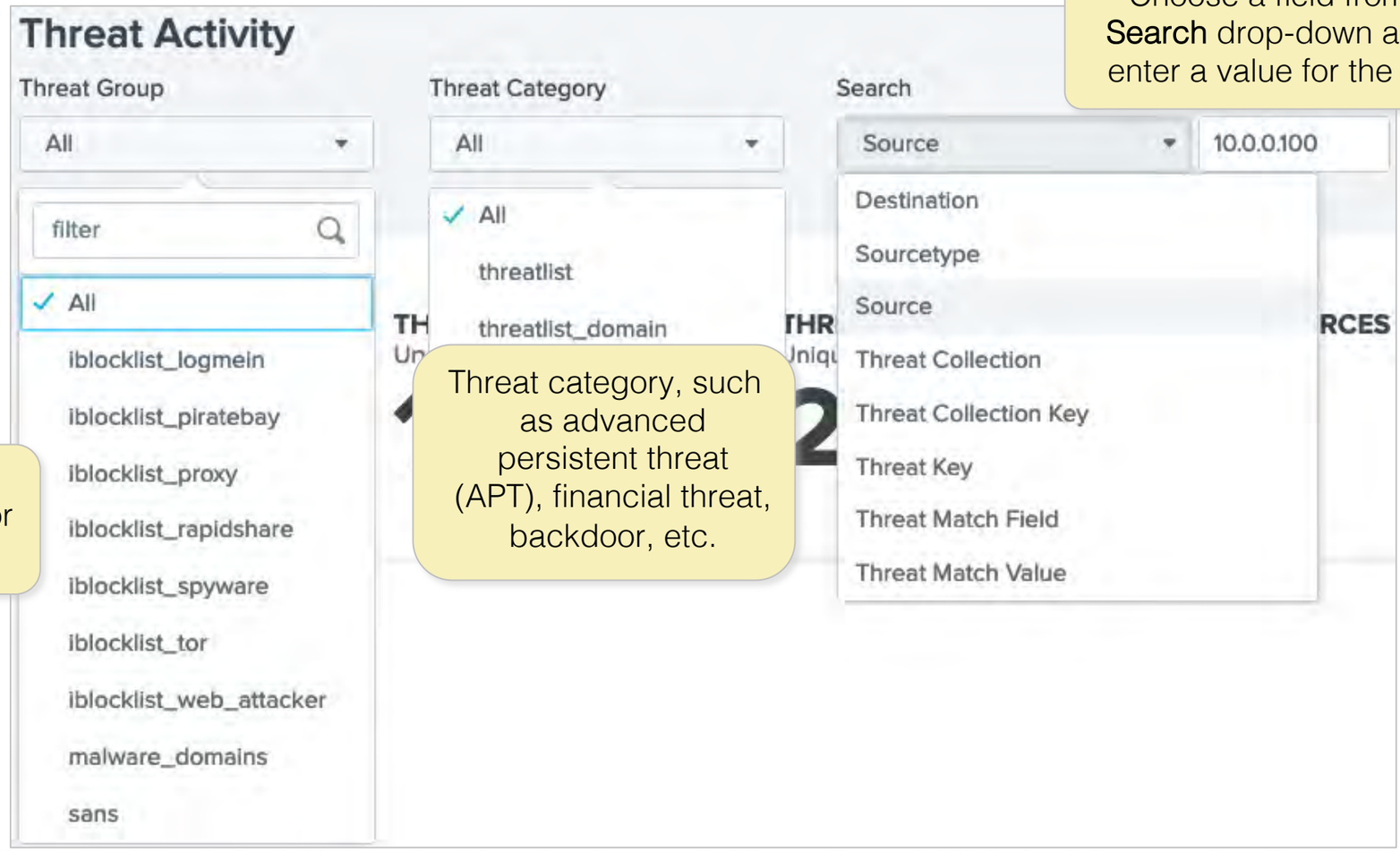
Threat Activity

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



Using the Threat Activity Dashboard

Filter the **Threat Activity** dashboard

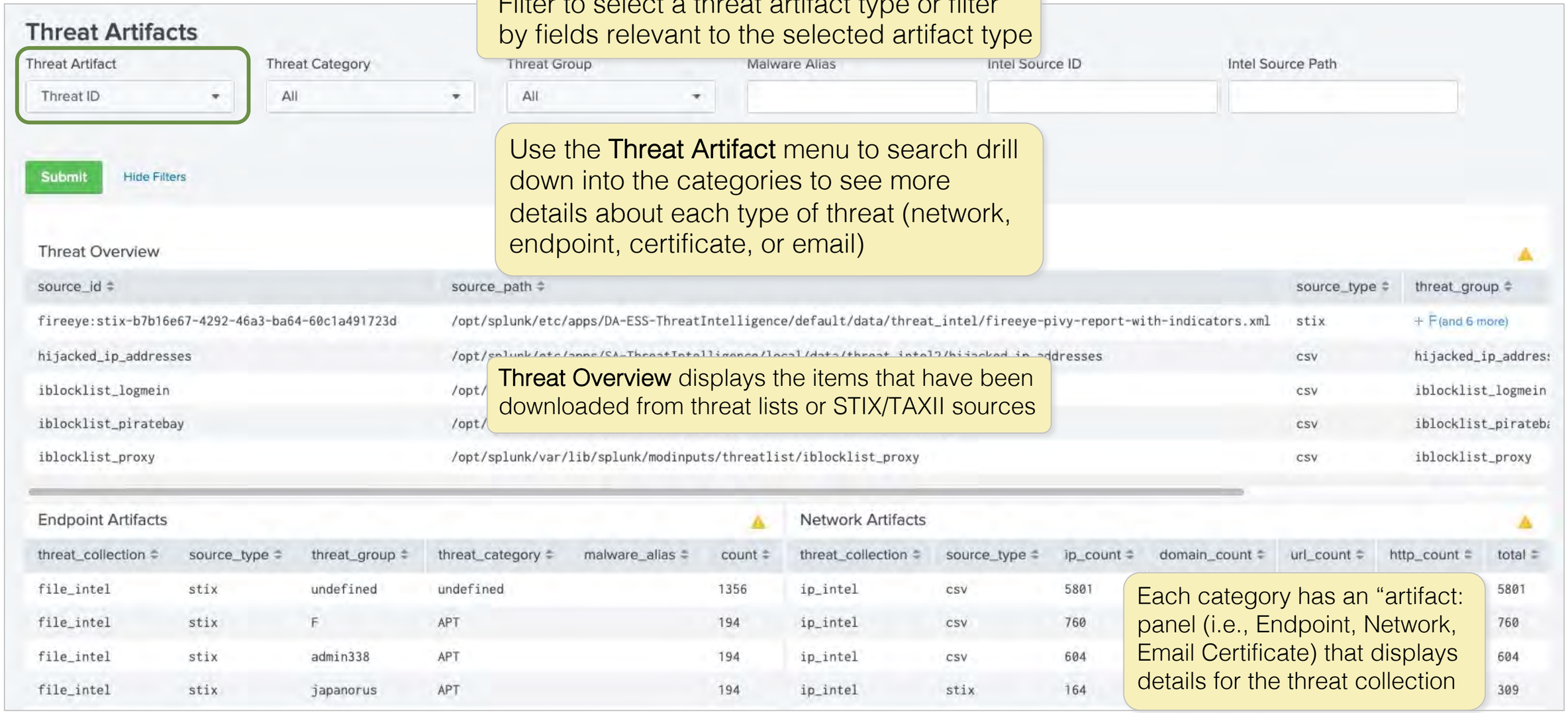


Choose a field from the **Search** drop-down and and enter a value for the search

Threat source: download feed or local file name

Threat category, such as advanced persistent threat (APT), financial threat, backdoor, etc.

Threat Artifacts



Using the Threat Artifacts Dashboard

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

Add Threat Intelligence from a Search

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

Module 9 Lab: Threat Intelligence

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

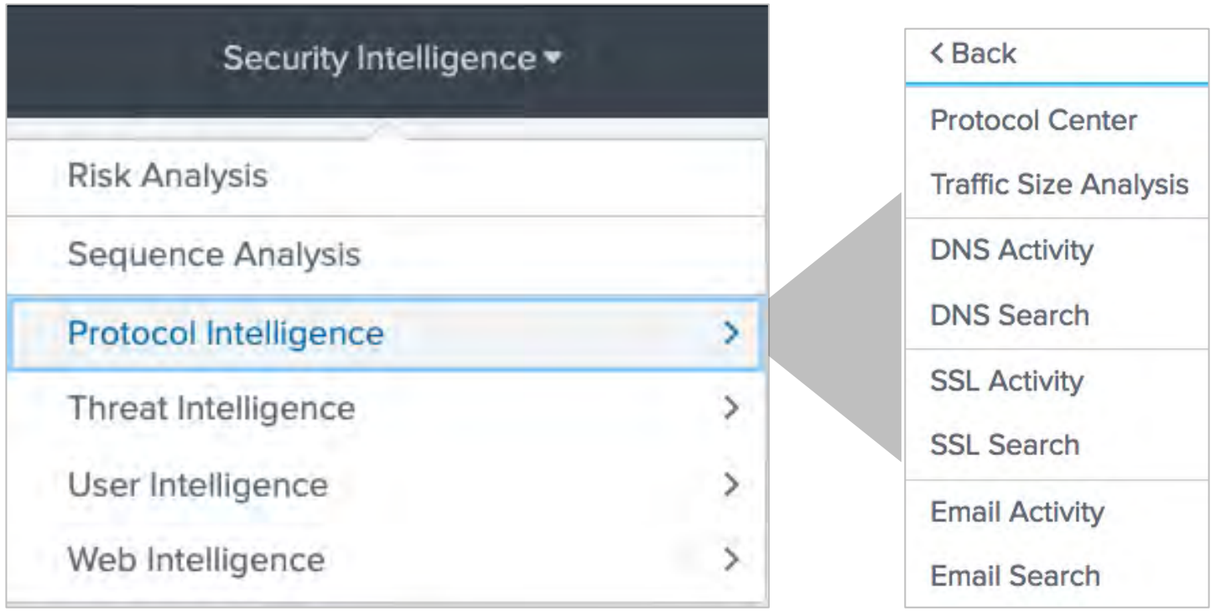
Module 10:
Protocol Intelligence

Objectives

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

Security Intelligence> Protocol Intelligence

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



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

Getting Data In

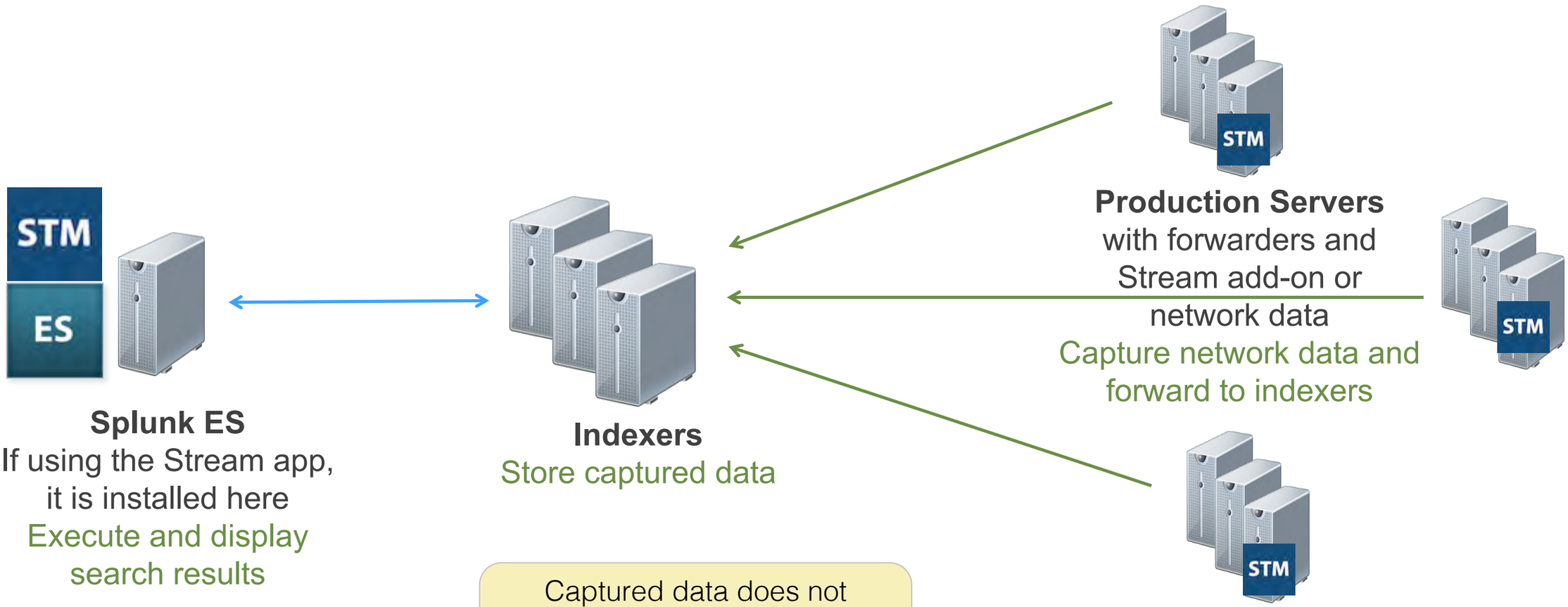
- Capture network traffic using the Splunk Stream app or by normalizing network log data (DNS, SSL, SMTP, HTTP)
- Uses Cases:
  - Monitor suspicious network traffic
  - Correlate logged vs. actual activity
  - Gain direct access to network traffic for SSL, HTTP, DNS, and SMTP
  - Configure correlation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

Splunk Stream

- Traffic can be captured using the **Splunk Stream** add-on
  docs.splunk.com/Documentation/StreamApp

- Deployed on forwarders and listens to traffic
- Traffic data is forwarded to indexers and made available to ES
- Additional captures can be set up within ES

Stream Data Flow



Splunk ES
If using the Stream app, it is installed here
Execute and display search results

Indexers
Store captured data

Production Servers
with forwarders and Stream add-on or network data
Capture network data and forward to indexers

Captured data does not include message content unless specifically configured

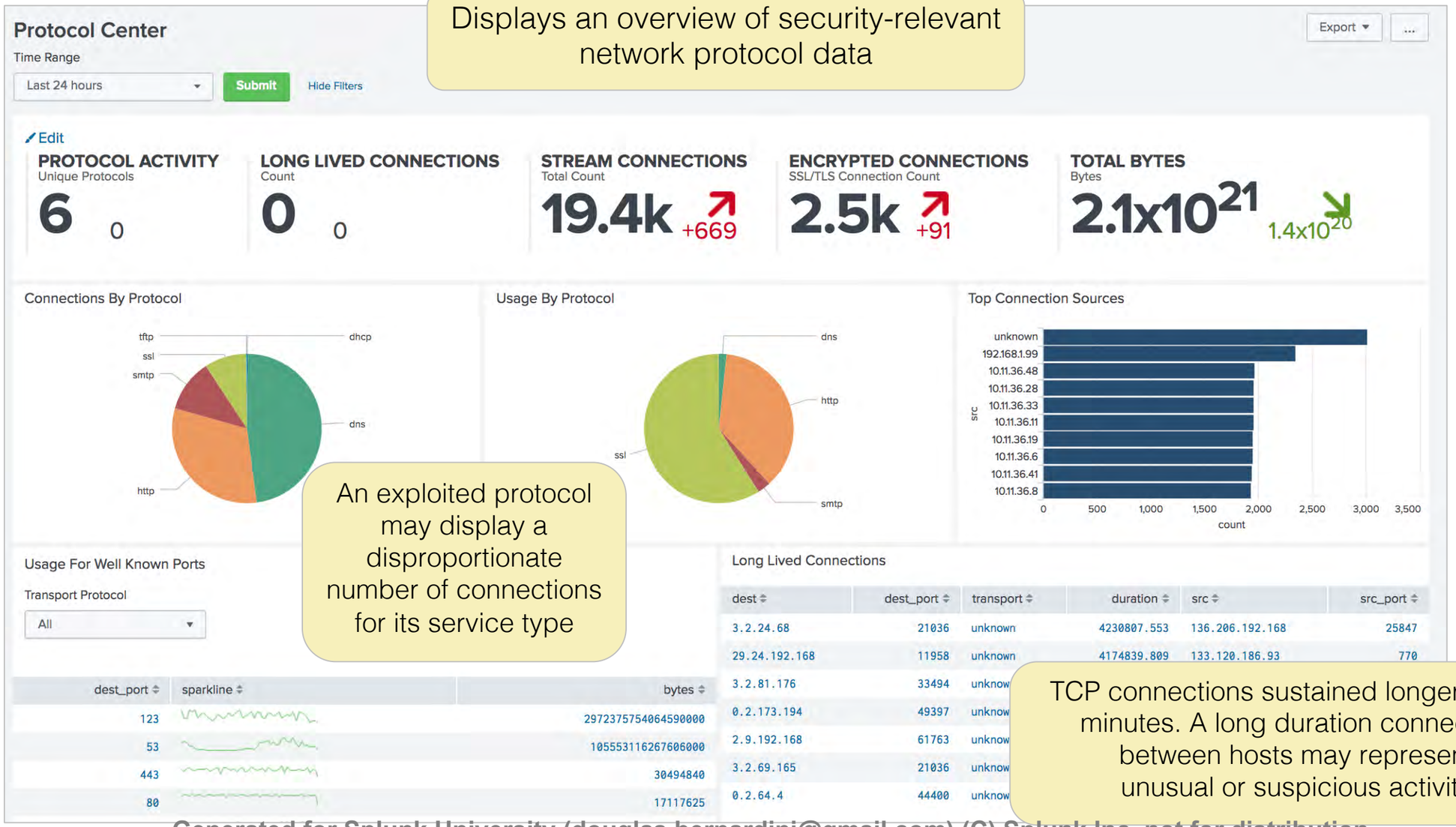
Stream Events

- Stream events are generated from the Splunk Stream app, or other streaming apps like Zeek (Bro) IDS
- Splunk Stream events in the **`notable`** index are stored with the **`orig_sourcetype`** field as **`stream:xxxx`** (**`stream:tcp`**, **`stream:http`** etc.)

- Standard fields are extracted, as well as additional fields for the specific source type
  - HTTP: cookies, request parameters, etc.
  - SMTP: sender, receiver, subject, summary of body
  - DNS: DNS query, query type, DNS host, etc.

Protocol Intelligence > Protocol Center

Displays an overview of security-relevant network protocol data

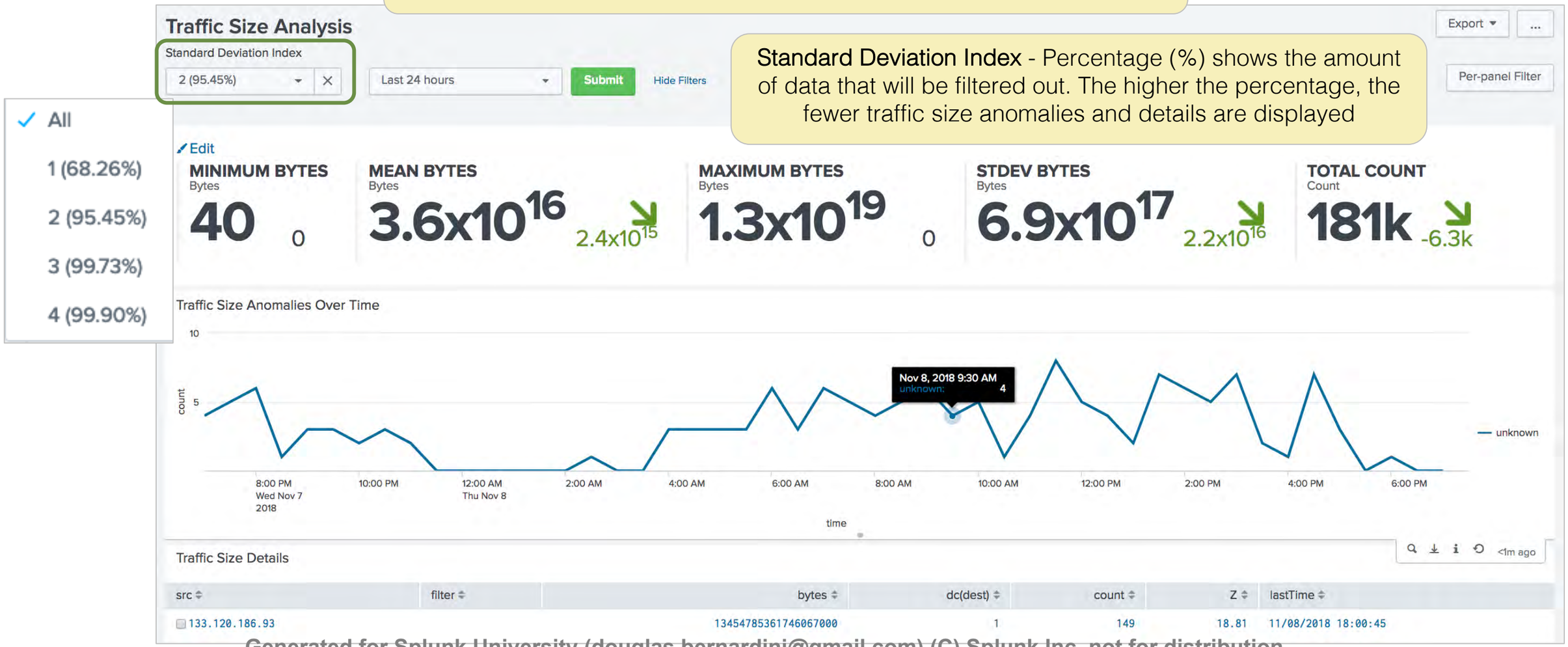


An exploited protocol may display a disproportionate number of connections for its service type

TCP connections sustained longer than 3 minutes. A long duration connection between hosts may represent unusual or suspicious activity

Protocol Intelligence > Traffic Size Analysis

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

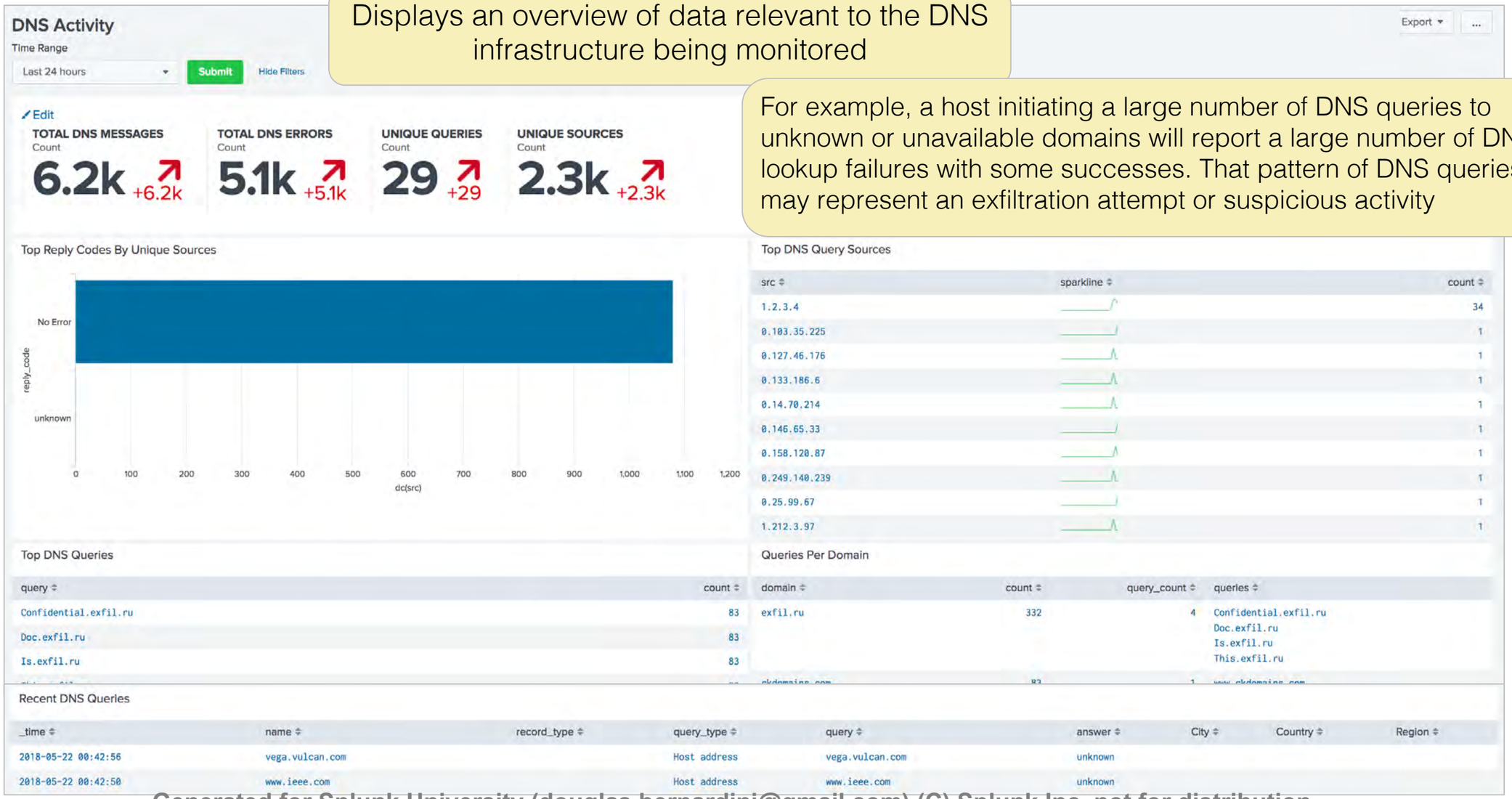


Standard Deviation Index - Percentage (%) shows the amount of data that will be filtered out. The higher the percentage, the fewer traffic size anomalies and details are displayed

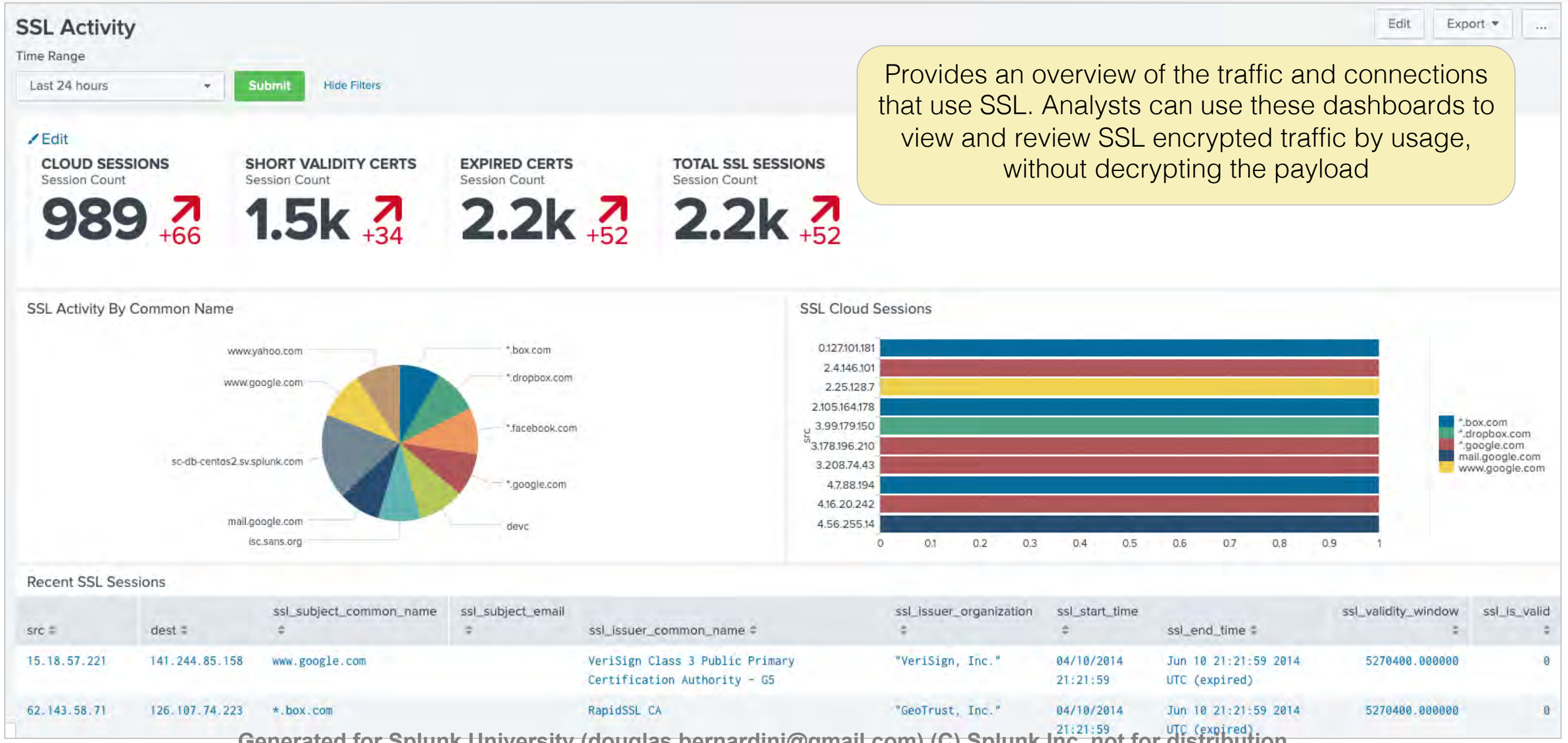
Protocol Intelligence > DNS Activity

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

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

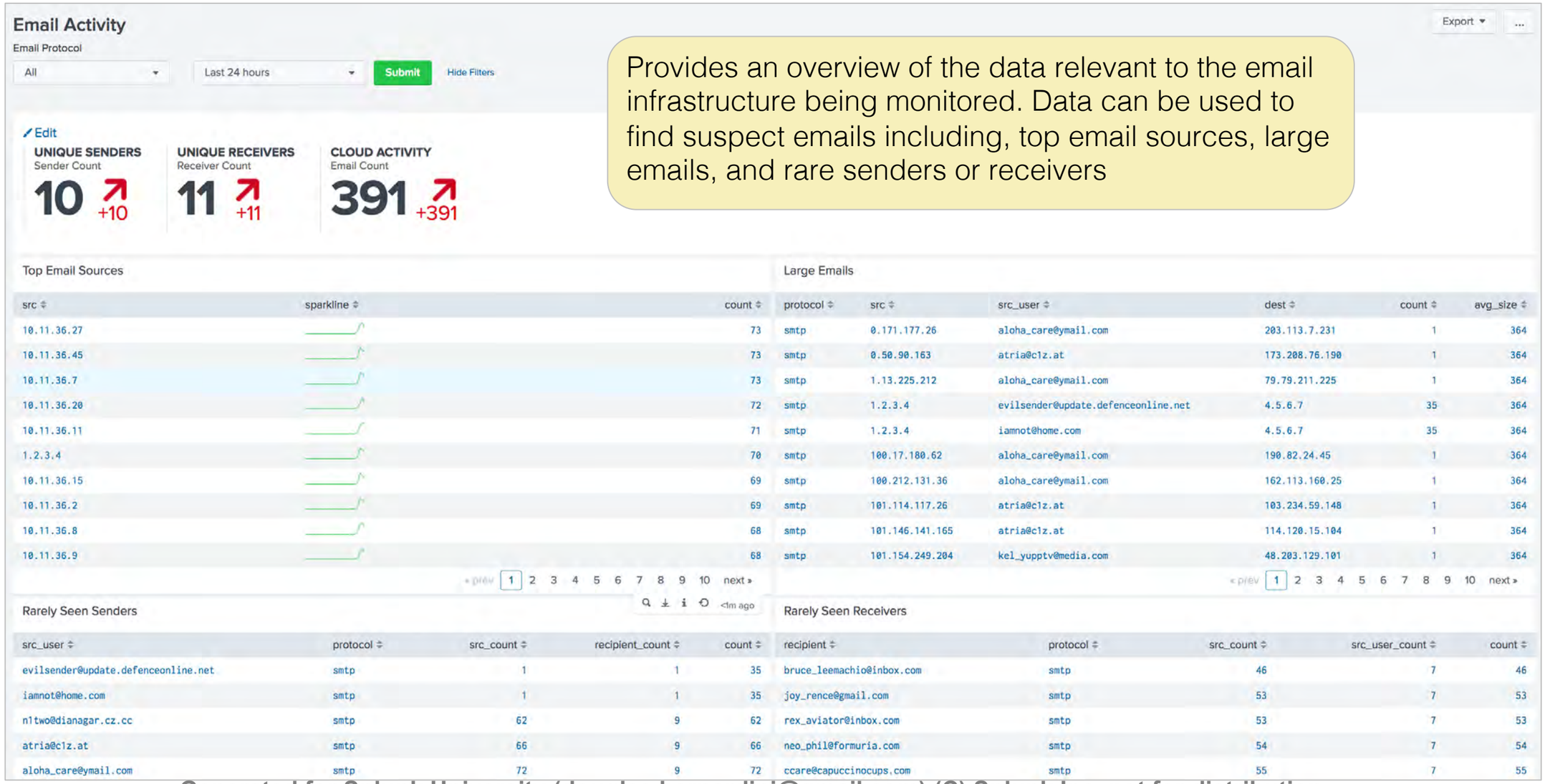


Protocol Intelligence > SSL Activity



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

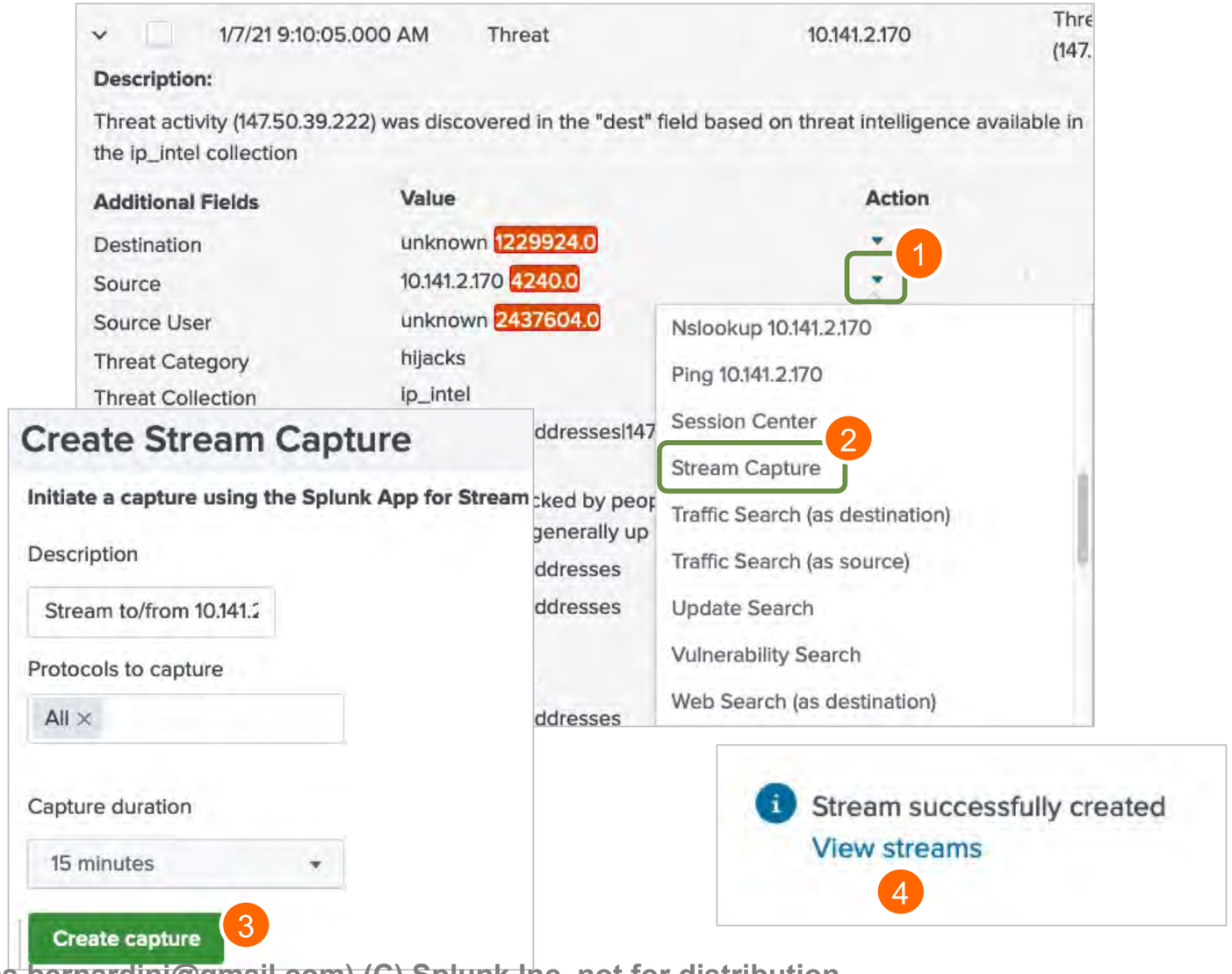
Protocol Intelligence > Email Activity



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

Creating a Stream Capture

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



Scenarios: Data Exfiltration

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

Module 10 Lab: Protocol Intelligence

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

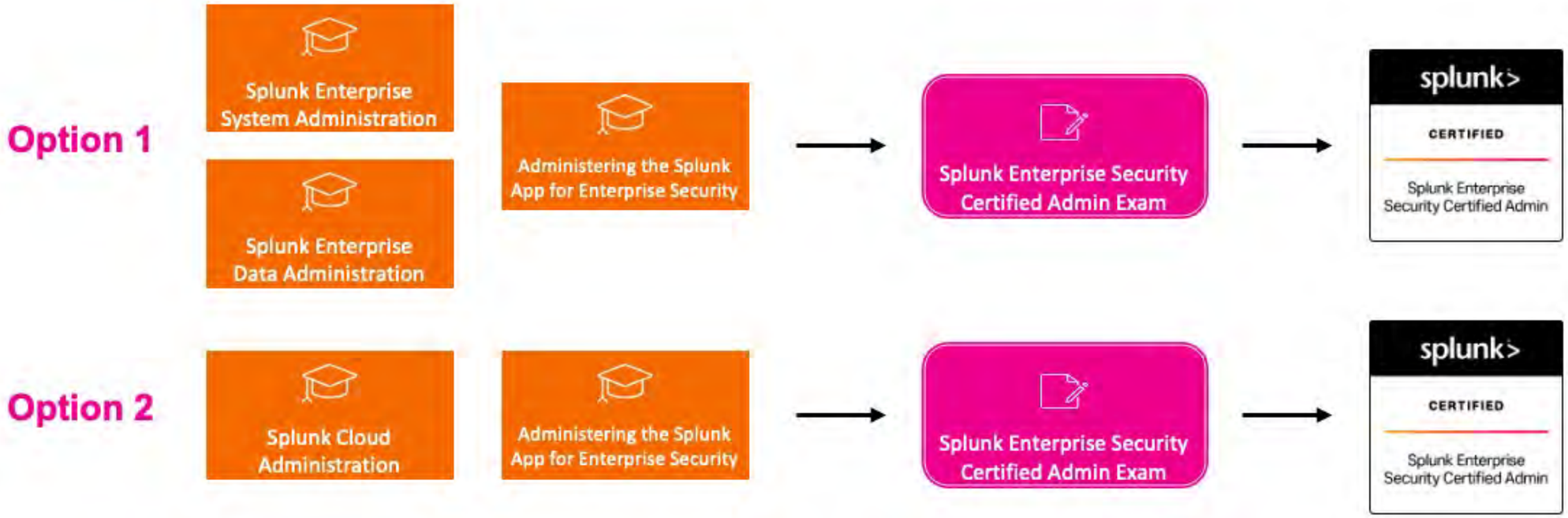
Wrap Up

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

What's Next?

Become a Splunk Enterprise Security Certified Admin

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



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

Exam registration assistance here. Study Guide here

 | 25 May 2022

Splunk Security Courses

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

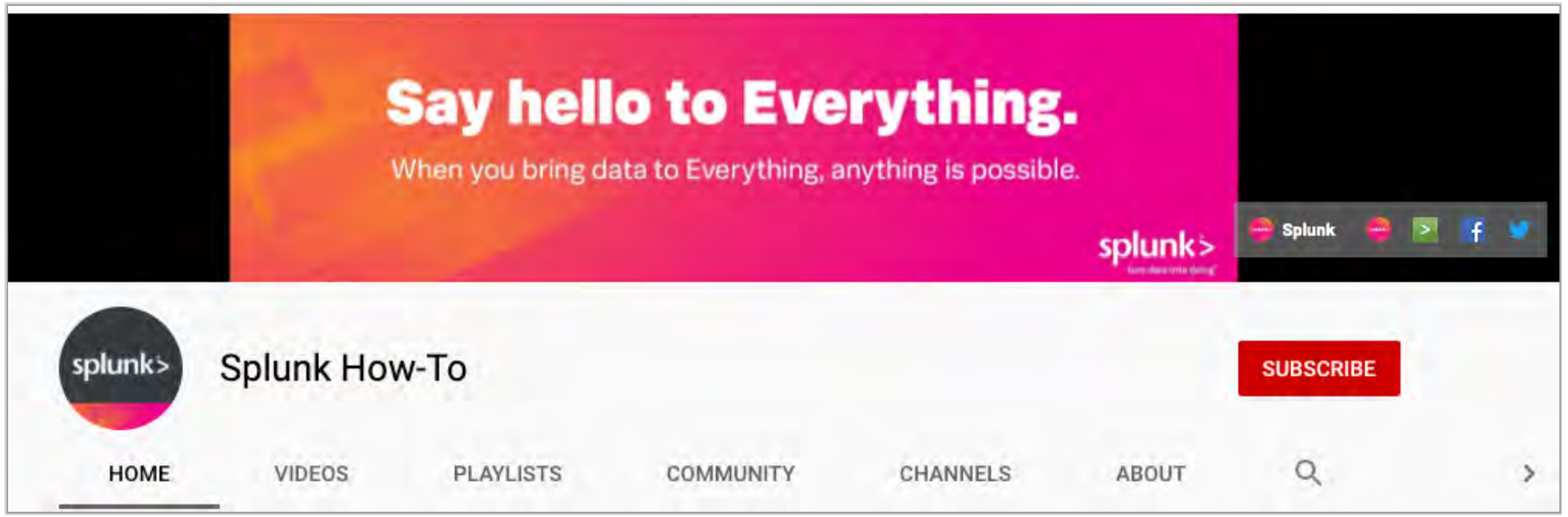
https://www.splunk.com/en_us/training.html

Community

- Splunk Community Portal
  splunk.com/en_us/community.html
  - Splunk Answers
    answers.splunk.com
  - Splunk Apps
    splunkbase.com
  - Splunk Blogs
    splunk.com/blog/
  - Splunk Live!
    splunklive.splunk.com
  - .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

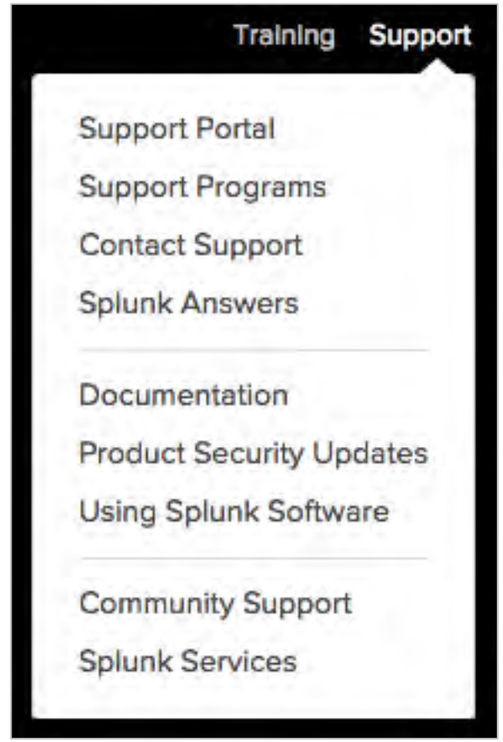
Splunk How-To Channel

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



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)



Thank You

splunk>

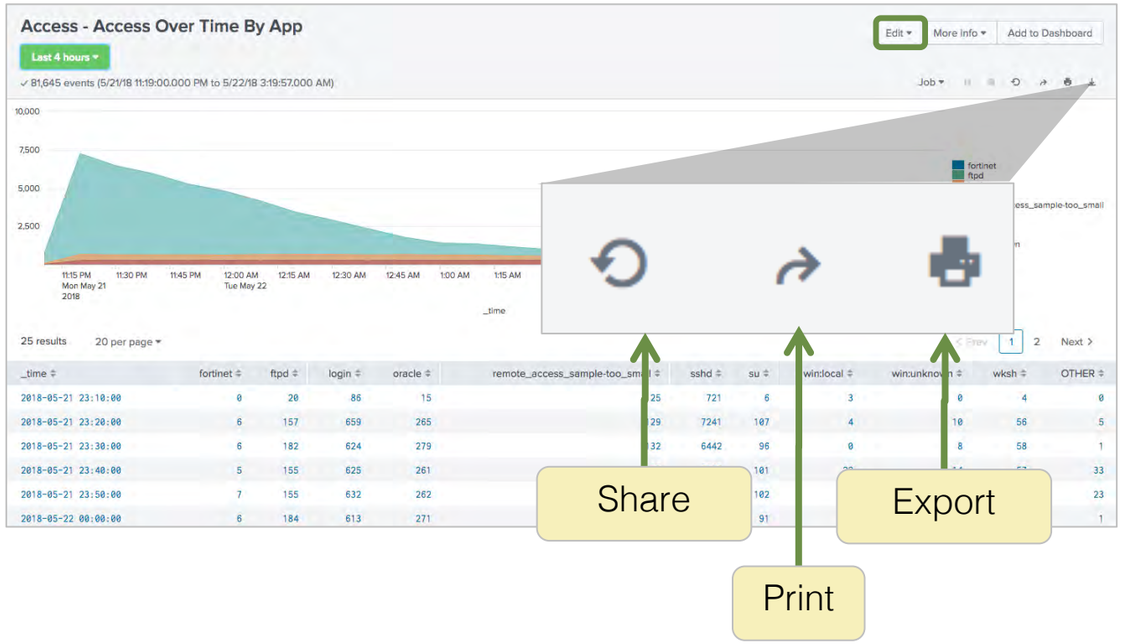
Appendix A: Reports, Dashboards, Data Models & Use Cases

Objectives

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

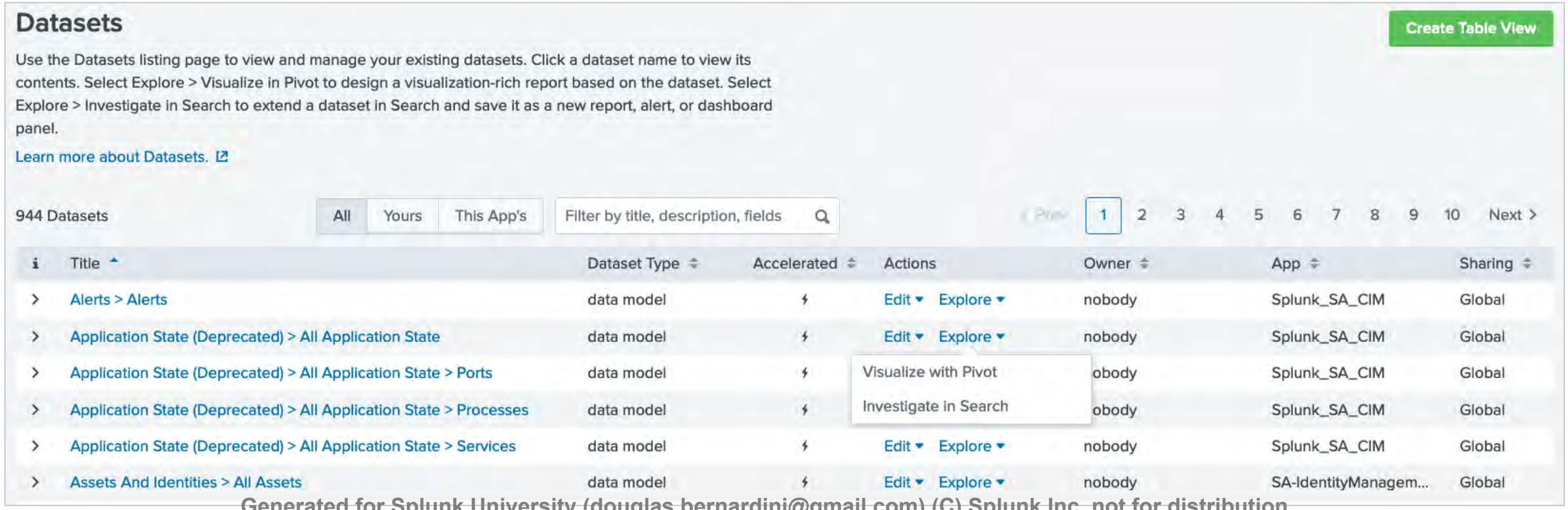
ES Reports

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



ES Datasets to Build New Reports

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



Lists of ES Correlation Searches

```
| rest splunk_server=local count=0 /services/saved/searches
| where match('action.correlationsearch.enabled', "1|[Tt]|[Tt][Rr][Uu][Ee]") | rename eai:acl.app as app, title as csearch_name, action.correlationsearch.label as csearch_label, action
    .notable.param.security_domain as security_domain | table csearch_name, csearch_label, app, security_domain, description
```

Last 24 hours

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

Events Patterns **Statistics (174)** Visualization

20 Per Page — Format — Preview — < Prev 1 2 3 4 5 6 7 8 9 Next >

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

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

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

Last 24 hours

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

Events Patterns **Statistics (11)** Visualization

20 Per Page — Format — Preview —

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

Enabled correlation searches and the adaptive response actions

Note

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

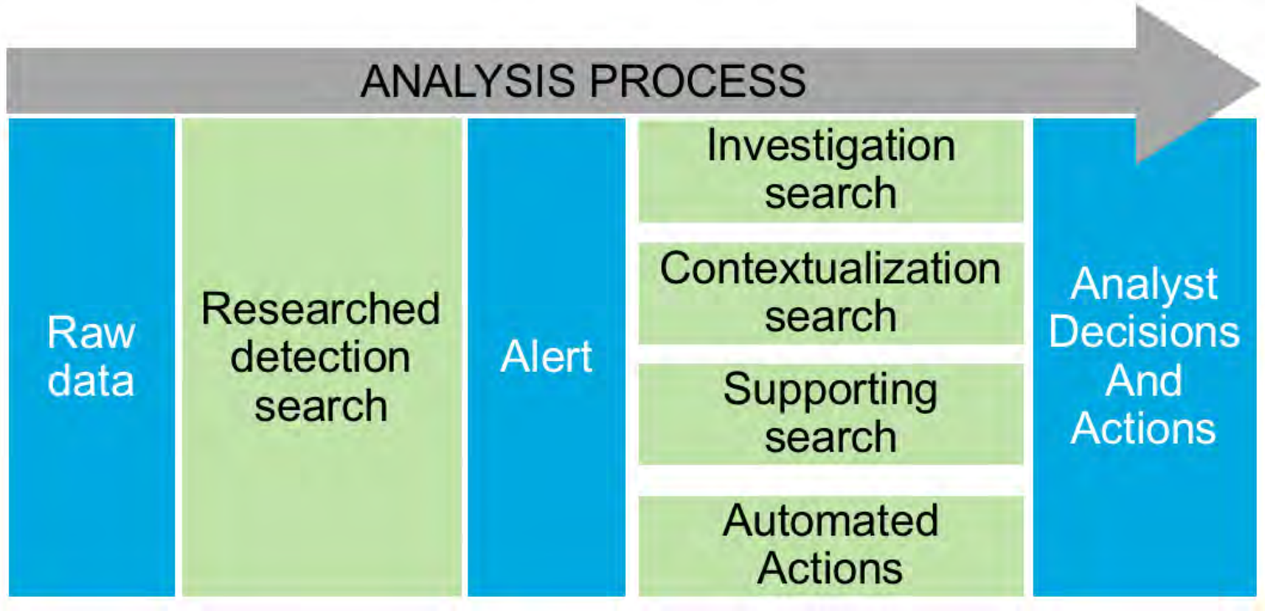
Common Information Model

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

docs.splunk.com/Documentation/CIM/latest/User/Overview

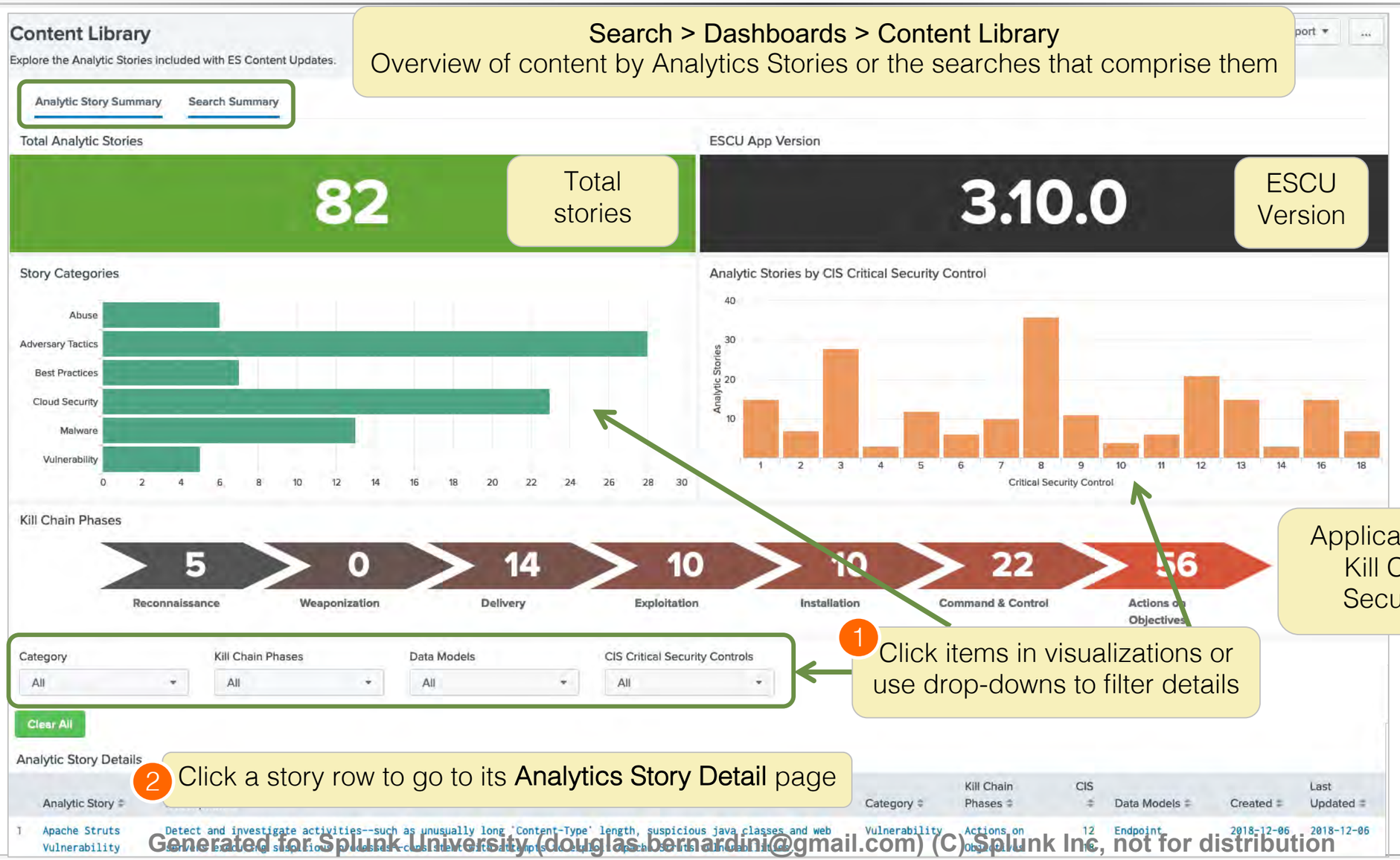
ES Content Updates: Analytic Stories

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

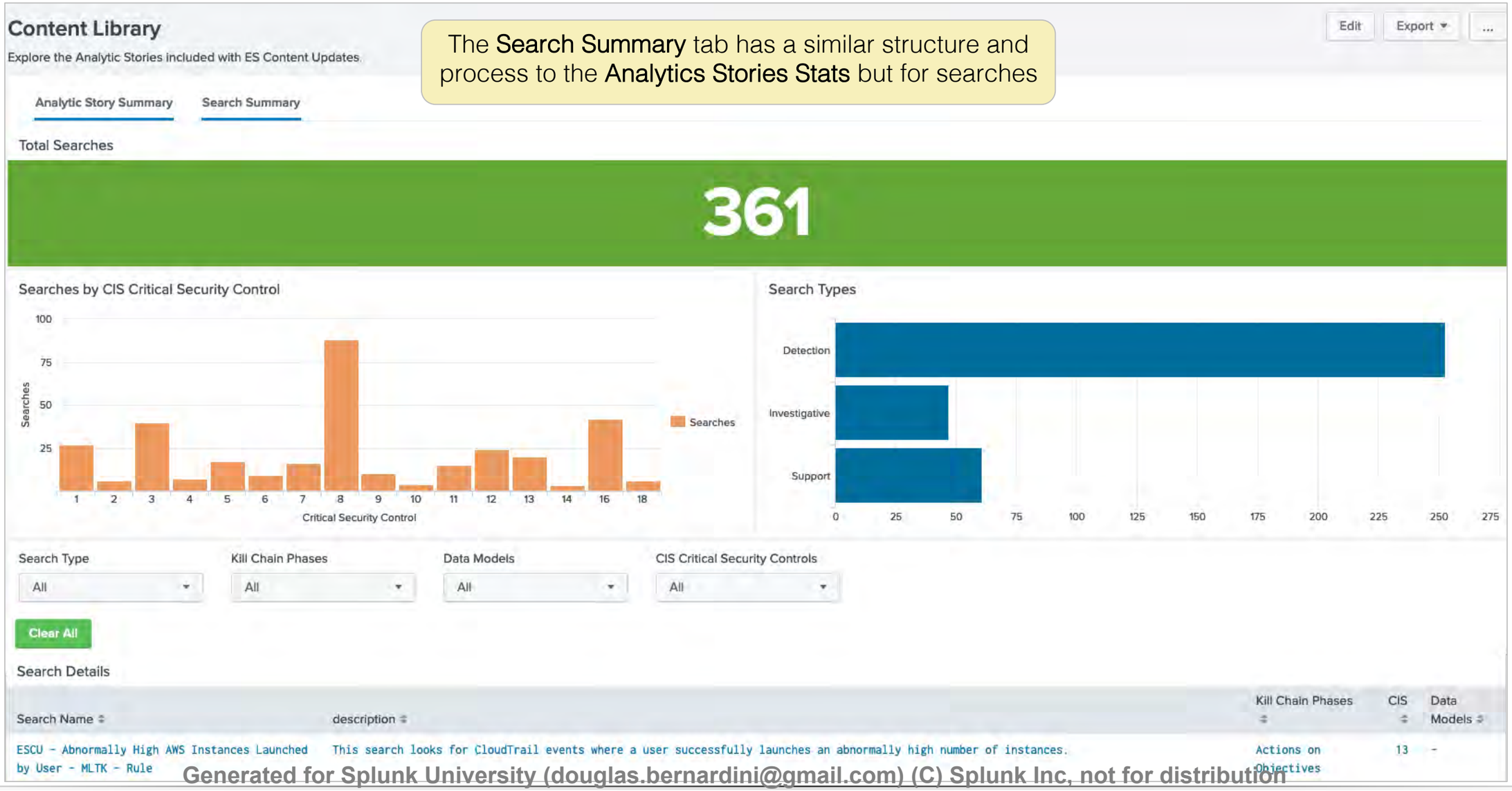


https://splunkbase.splunk.com/app/3449/

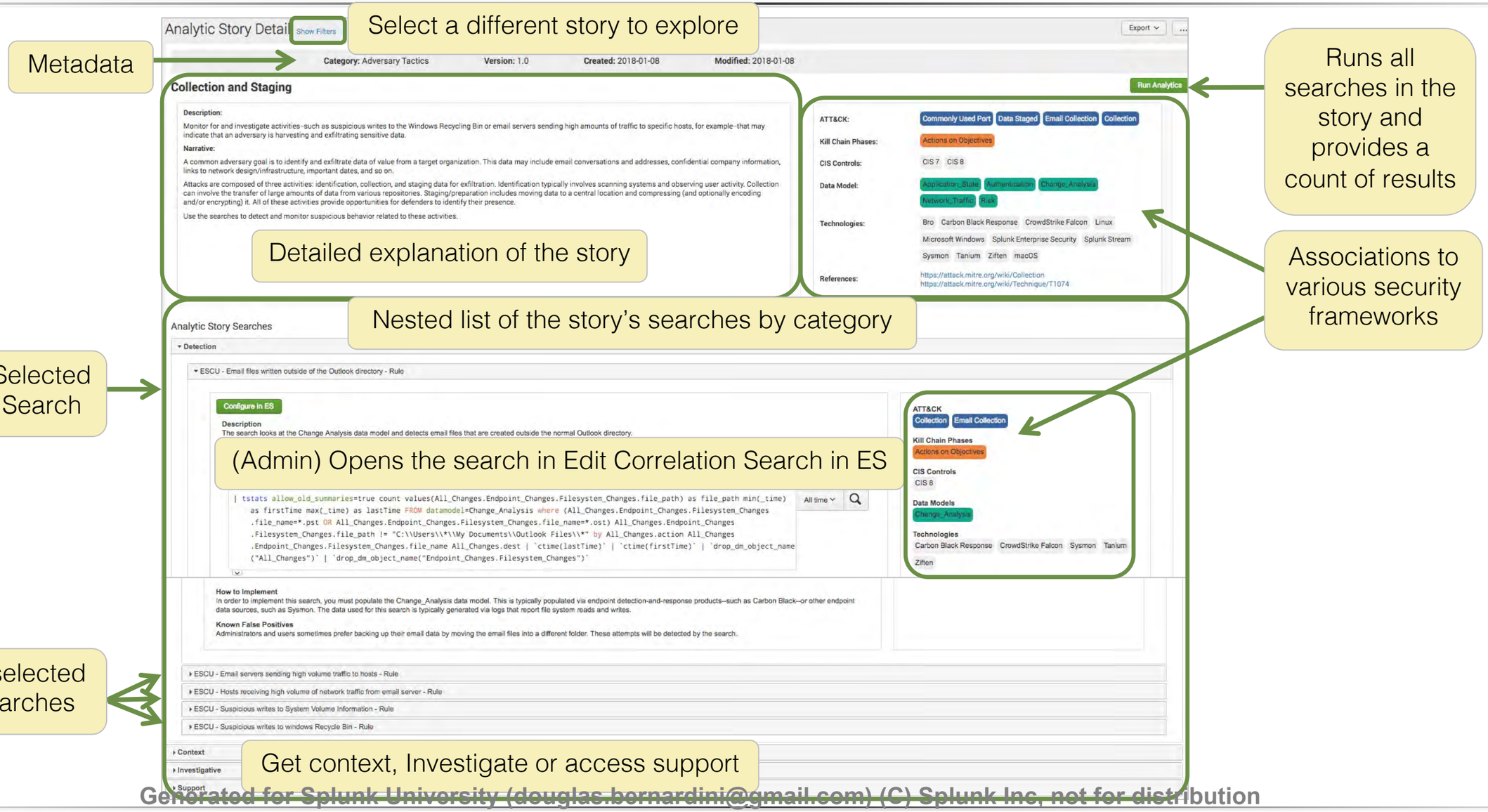
Content Library > Analytics Stories Stats



Content Library > Search Summary

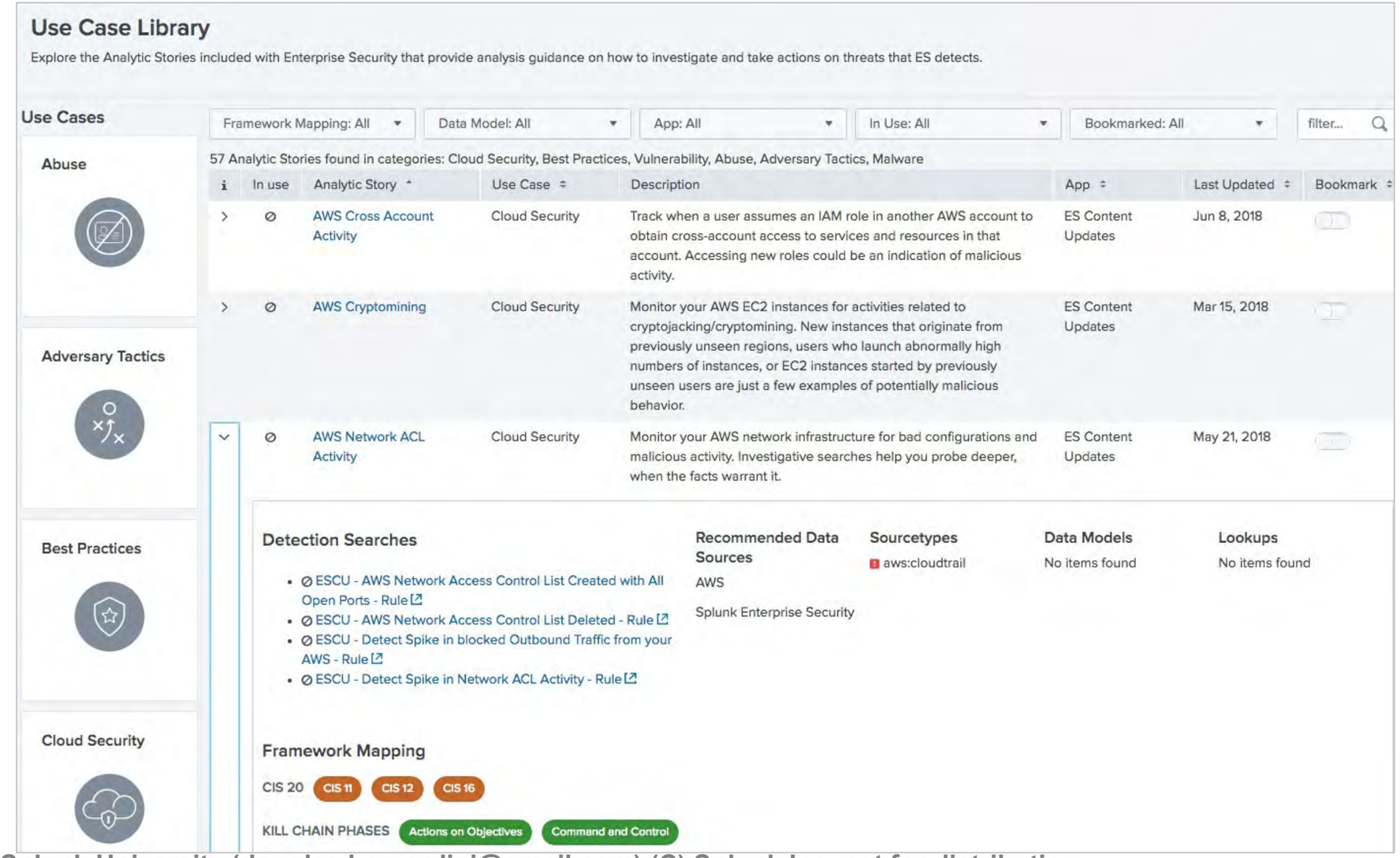


Analytic Story Detail

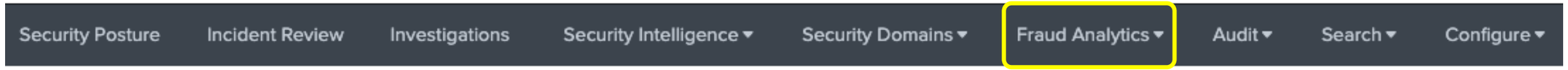


Configure > Content > Use Case Library

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



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)

Appendix B:
Event Sequence Engine

Event Sequencing Engine

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

Note

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

Example Use Case

Start (correlation search)

1. Brute Force Access Behavior Detected

Transitions (correlation searches)

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

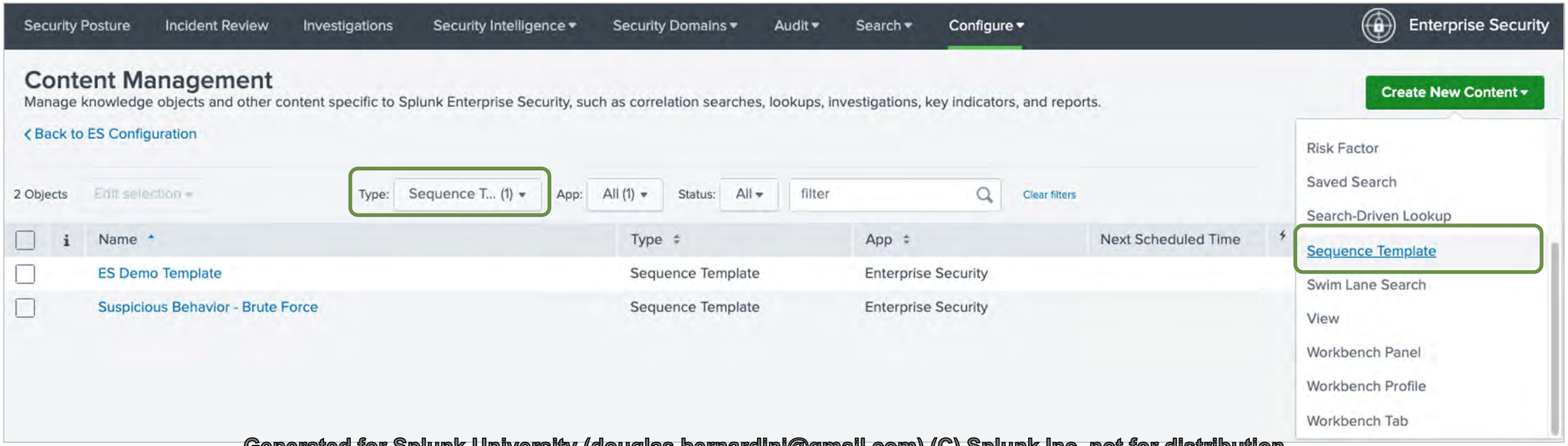
End (correlation search)

6. Abnormally High Number of Endpoint Changes by User

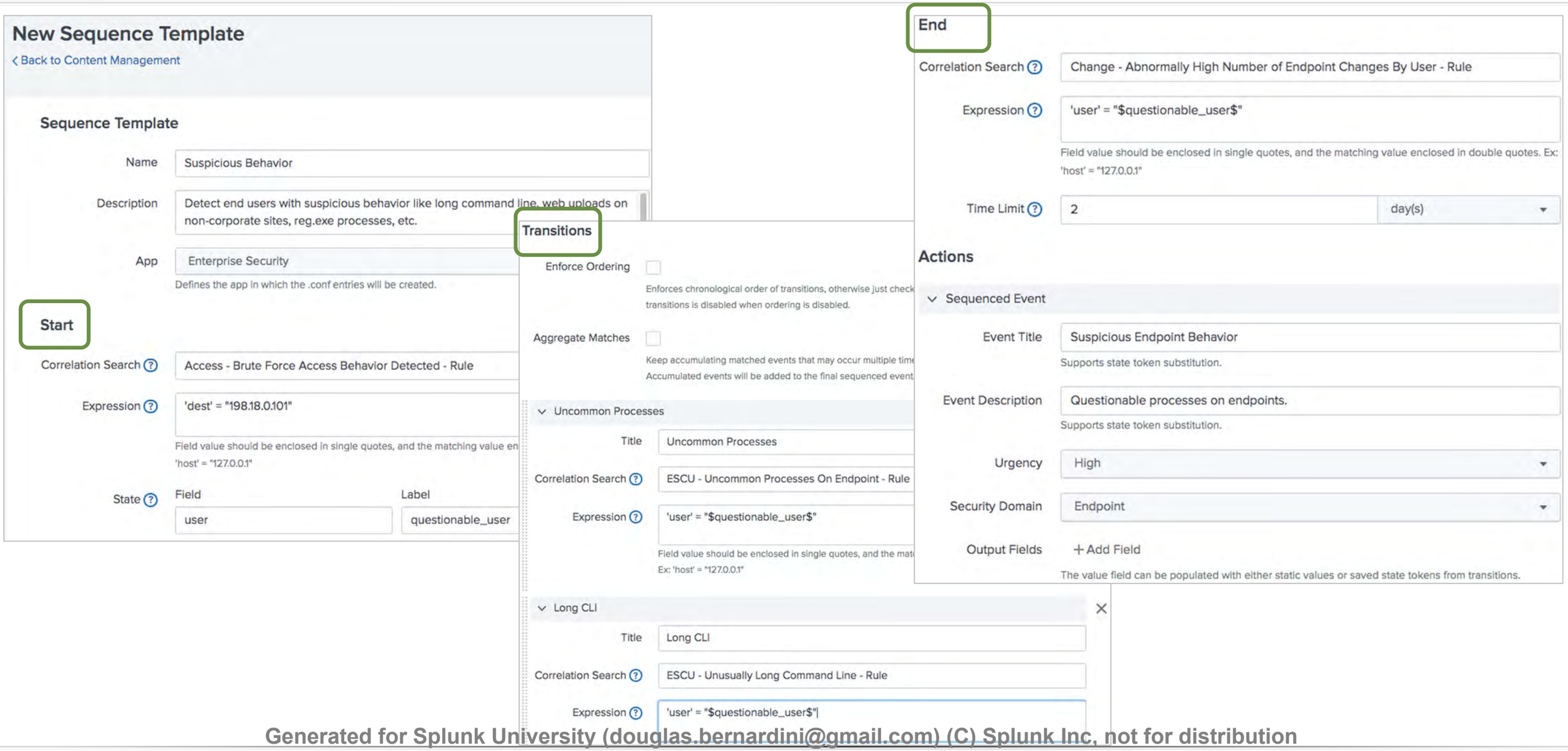
Example Configuration

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

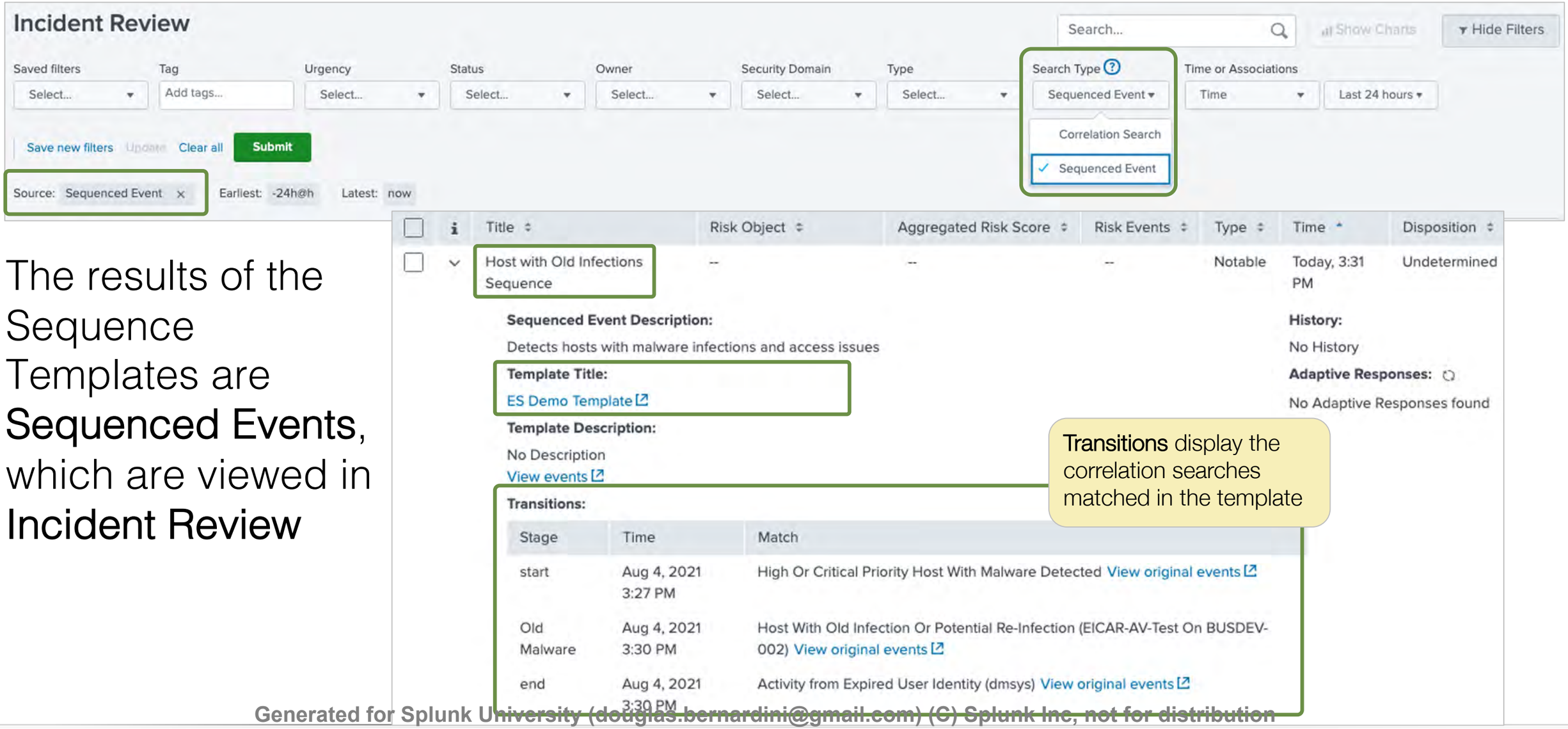
- The **Content Management** window has been filtered to show only Sequence Templates



Example Configuration (cont.)



Resulting Sequence Event



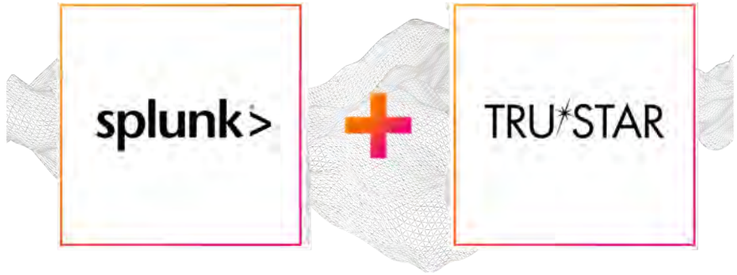
The results of the Sequence Templates are **Sequenced Events**, which are viewed in **Incident Review**

Transitions display the correlation searches matched in the template

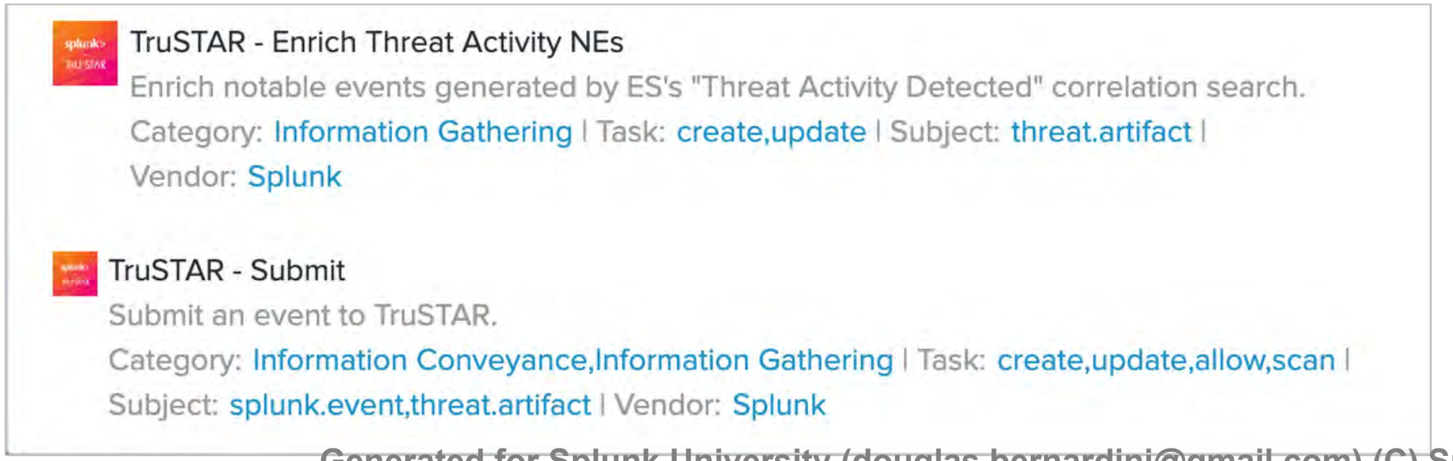
Appendix C: Interfacing with Splunk Intelligence Management (TrueSTAR)

Splunk Intelligence Management

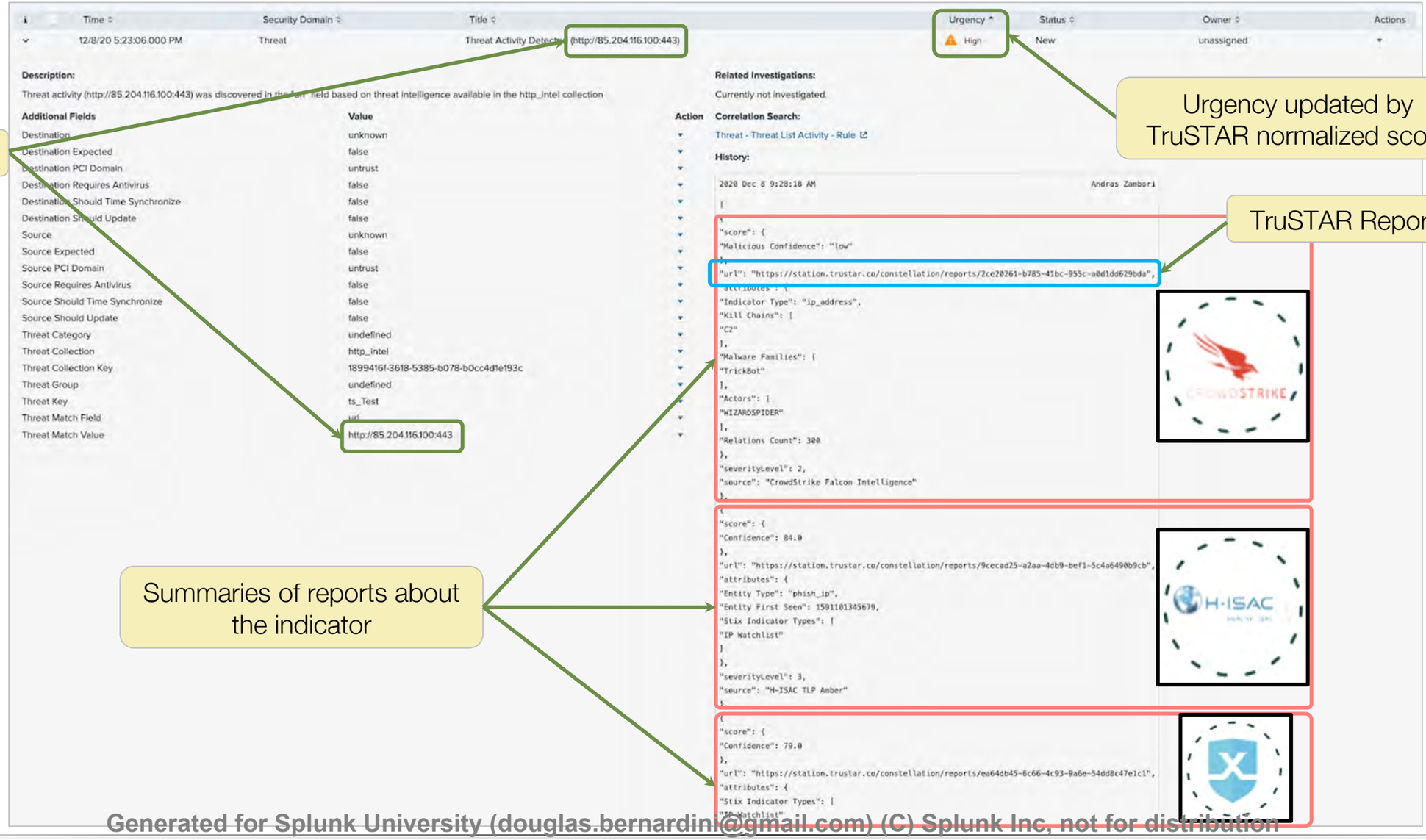
In addition to the Ingest of Indicators from multiple Intelligence Sources into Splunk KV stores for alerting, the TruSTAR Unified app enables two Adaptive Response actions:



- Enrich threat activity notable events
- Submit events to TruSTAR



Enrich Threat Activity Notable Events



The Indicator

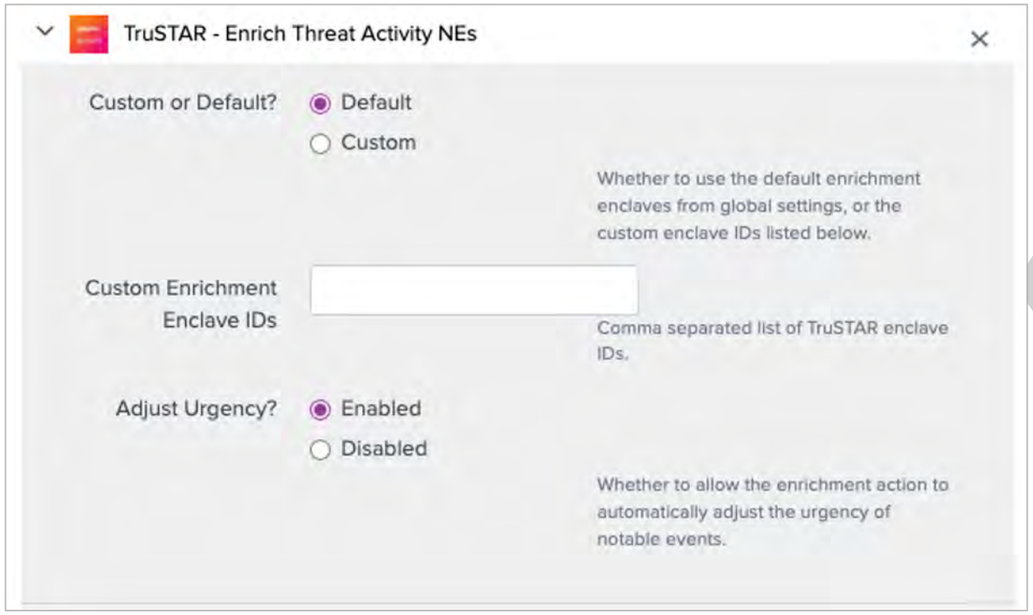
Urgency updated by TruSTAR normalized score

TruSTAR Report

Summaries of reports about the indicator

 |

Enrich Threat Activity Notable Events (cont.)




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


Pass-through/Original Score

Actor(s)

Malware Families

Normalized Score

 | 25 May 2022

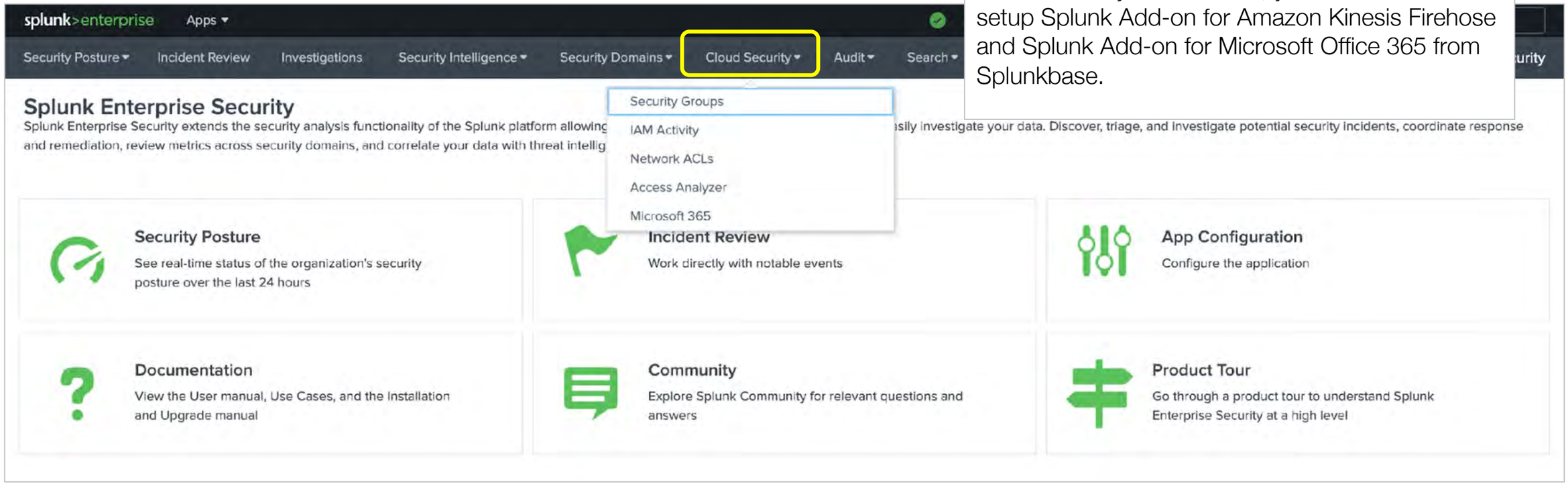
Appendix D:
Cloud Security Dashboards

Cloud Security Dashboards

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

Important!

To onboard Cloud data sources and examine your Cloud Security environment, you must install and setup Splunk Add-on for Amazon Kinesis Firehose and Splunk Add-on for Microsoft Office 365 from Splunkbase.



Prerequisites

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

Note

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

Available Dashboards

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