Using Splunk Enterprise Security

Course Goals

- Use Splunk Enterprise Security (ES) to detect, identify, and investigate security-related threats
- Determine root causes of malicious or anomalous events
- Use ES to discover previously unknown types of potential threats
- Create reports that meet security requirements

Course Outline

Module 1: Getting Started with Enterprise Security

Module 2: Security Monitoring and Incident Investigation

Module 3: Investigations

Module 4: Forensic Investigation with ES

Module 5: Risk Analysis

Module 6: Web Intelligence

Module 7: User Intelligence

Module 8: Threat Intelligence

Module 9: Protocol Intelligence

Module 10: Glass Tables

Appendix: Reports, Dashboards, Data Models, and Predictive Analysis

Module 1:
Getting Started With Enterprise Security

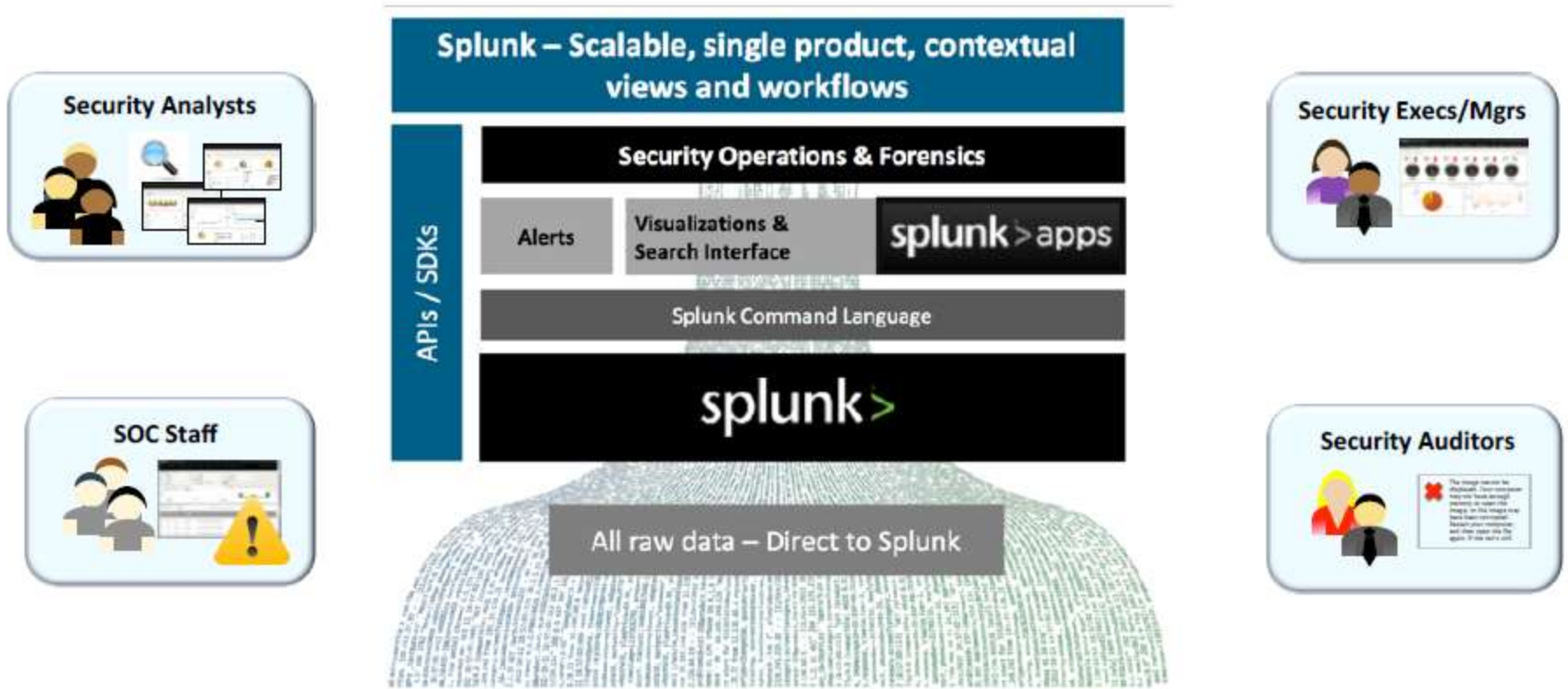
Objectives

- Describe the features and capabilities of Splunk Enterprise Security (ES)
- Explain how ES helps security practitioners detect, prevent, and respond to threats
- Describe correlation searches and notable events
- Describe user roles in ES
- Log on to ES

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, prevent, 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 Users


Splunk – Scalable, single product, contextual views and workflows
Security Analysts
Security Execs/Mgrs
SOC Staff
Security Auditors
APIs / SDKs
Security Operations & Forensics
Alerts
Visualizations & Search Interface
splunk>apps
Splunk Command Language
splunk>
All raw data – Direct to Splunk

Advanced Persistent Threats (APT)

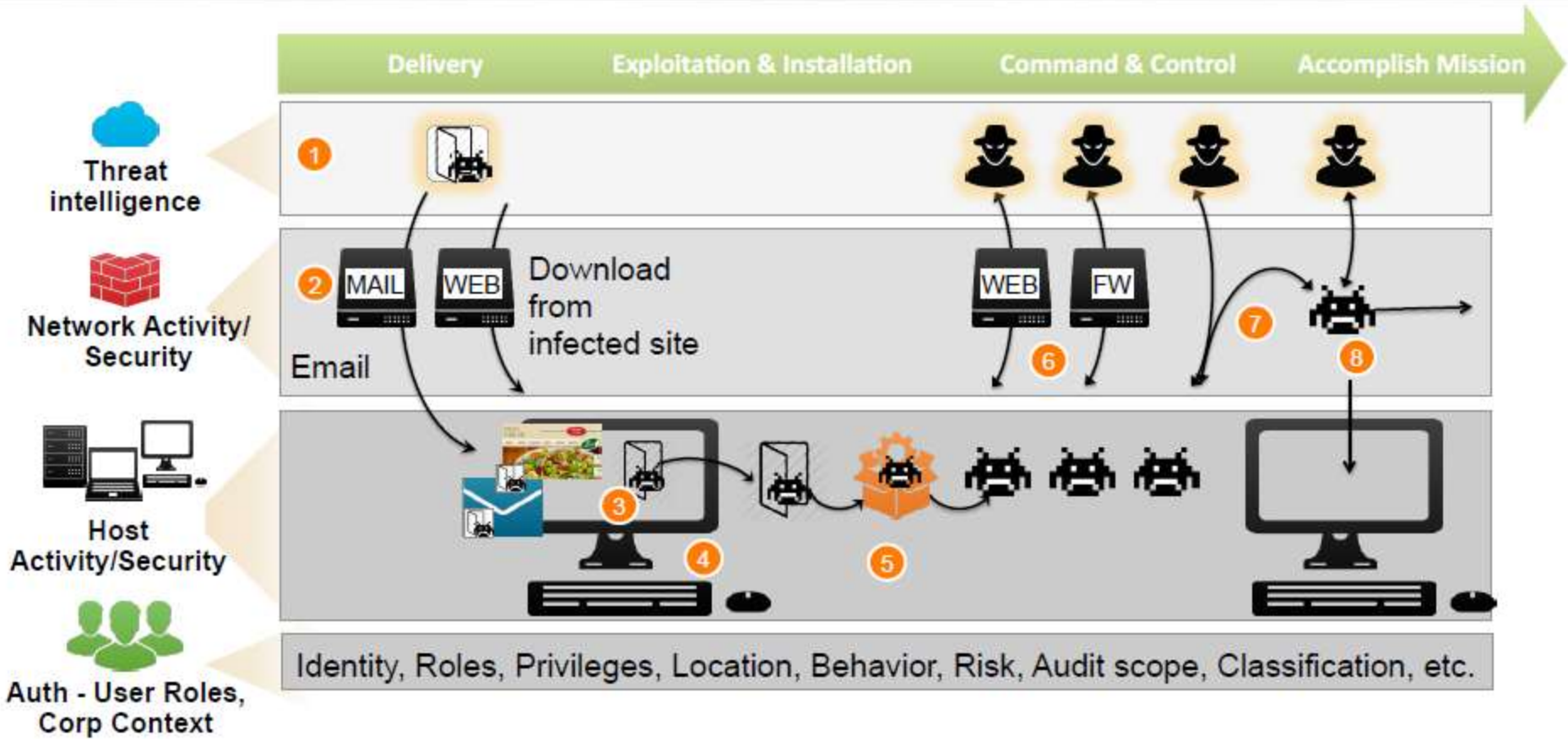
- A growing, global threat
- Focused attacks on specific systems
  - Recent examples: Yahoo, JPMorgan Chase, …
- Goal: undetected insertion, long-term viability, extraction/delivery of valuable information
- Targets: business, government, individuals
- Many delivery methods
- Metamorphic/polymorphic coding
- Constantly changing and adapting

The Kill Chain

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

Both attacker **and** defender can use the kill chain methodology

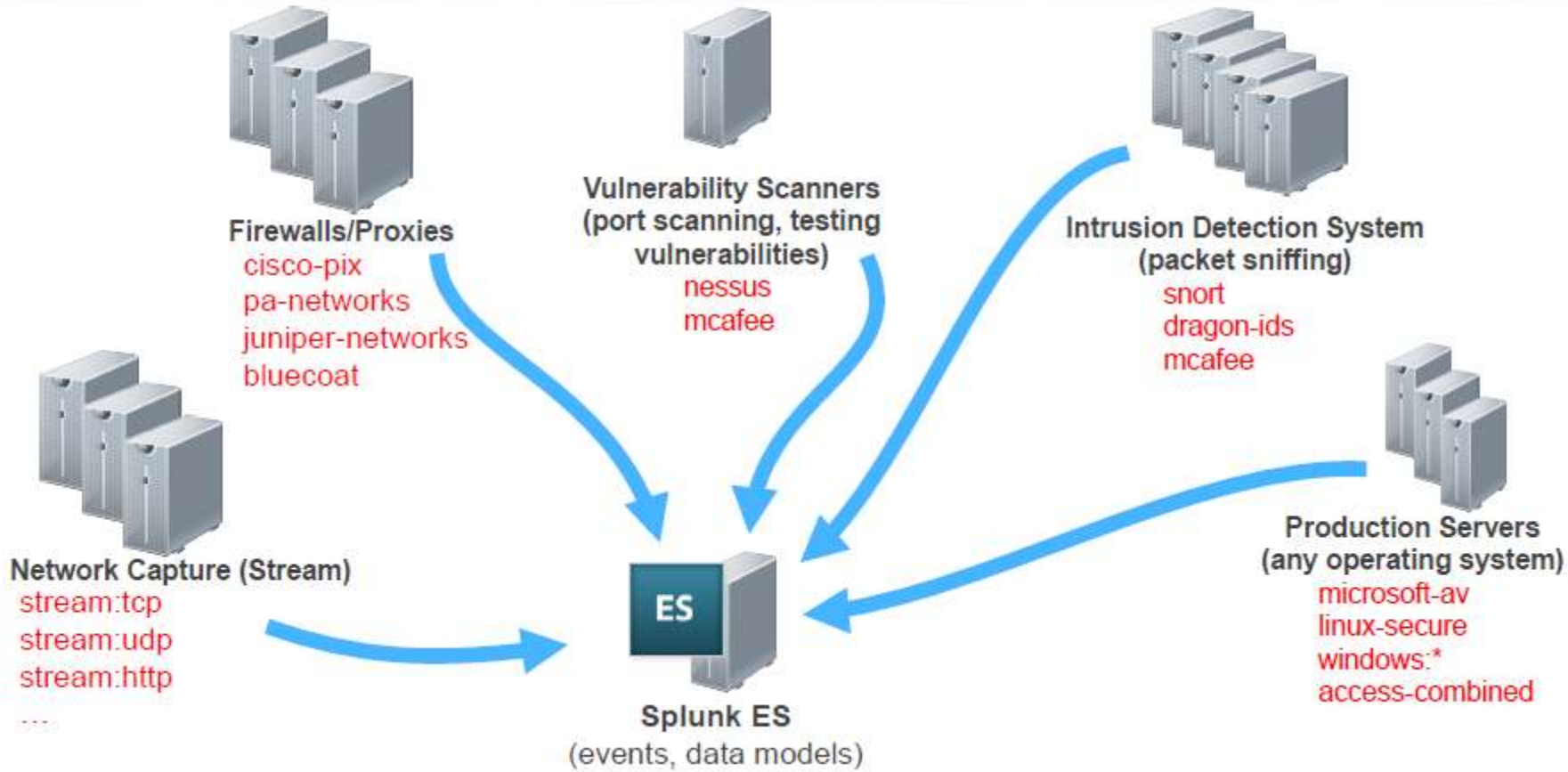
Anatomy of an APT Attack



How ES Works

- 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 real-time searches, looking 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


Firewalls/Proxies
cisco-pix
pa-networks
juniper-networks
bluecoat
Vulnerability Scanners
(port scanning, testing vulnerabilities)
nessus
mcafee
Intrusion Detection System
(packet sniffing)
snort
dragon-ids
mcafee
Network Capture (Stream)
stream:tcp
stream:udp
stream:http
...
ES
Splunk ES
(events, data models)
Production Servers
(any operating system)
microsoft-av
linux-secure
windows:*
access-combined

Correlation Searches

- **Correlation searches** run in the background to detect evidence of attacks, known threats, or vulnerabilities
  - These searches run either in real-time or on a schedule
- ES ships with many correlation searches, which can be modified or extended as needed
- Each correlation search is looking for one specific type of threat, vulnerability, or sign of malicious attack
- If a correlation search finds something that requires attention, an alert is triggered which creates a **notable event**
  - Can also send emails, run scripts, update risk scores, etc.

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** fields show the correlation search that created the notable event

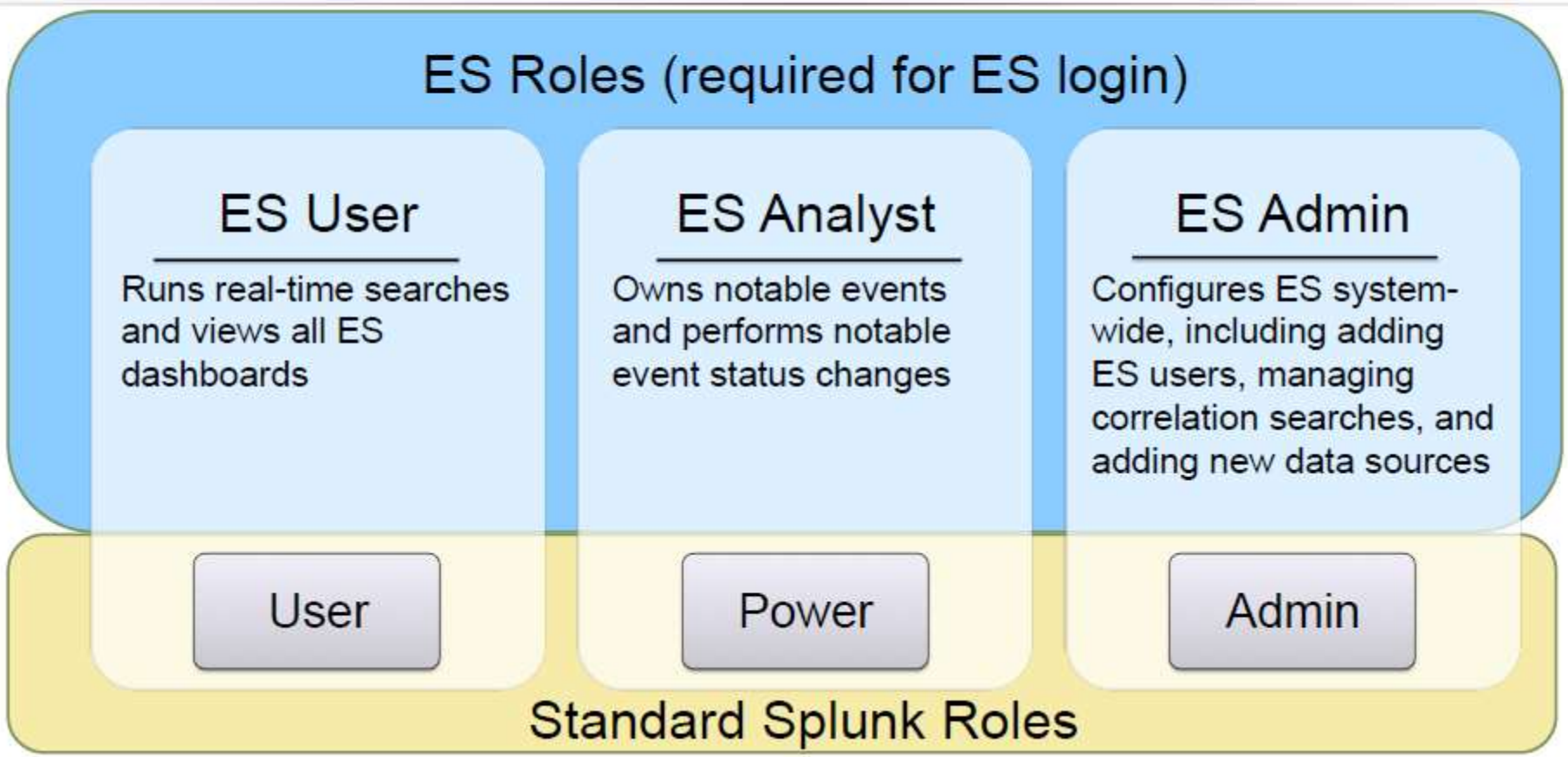
Assets and Identities

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

Beyond Notable Events

- ES provides many advanced tools you can use to examine security data in detail, such as:
  - Risk and threat analysis
  - Web and user intelligence
  - Protocol (stream) intelligence
  - Adaptive response
- These tools will help you:
  - During forensic investigation of existing breaches
  - Analyze your environment for new threats
  - Examine the history of old breaches to understand how they happened and prevent them in the future

ES Role Overview



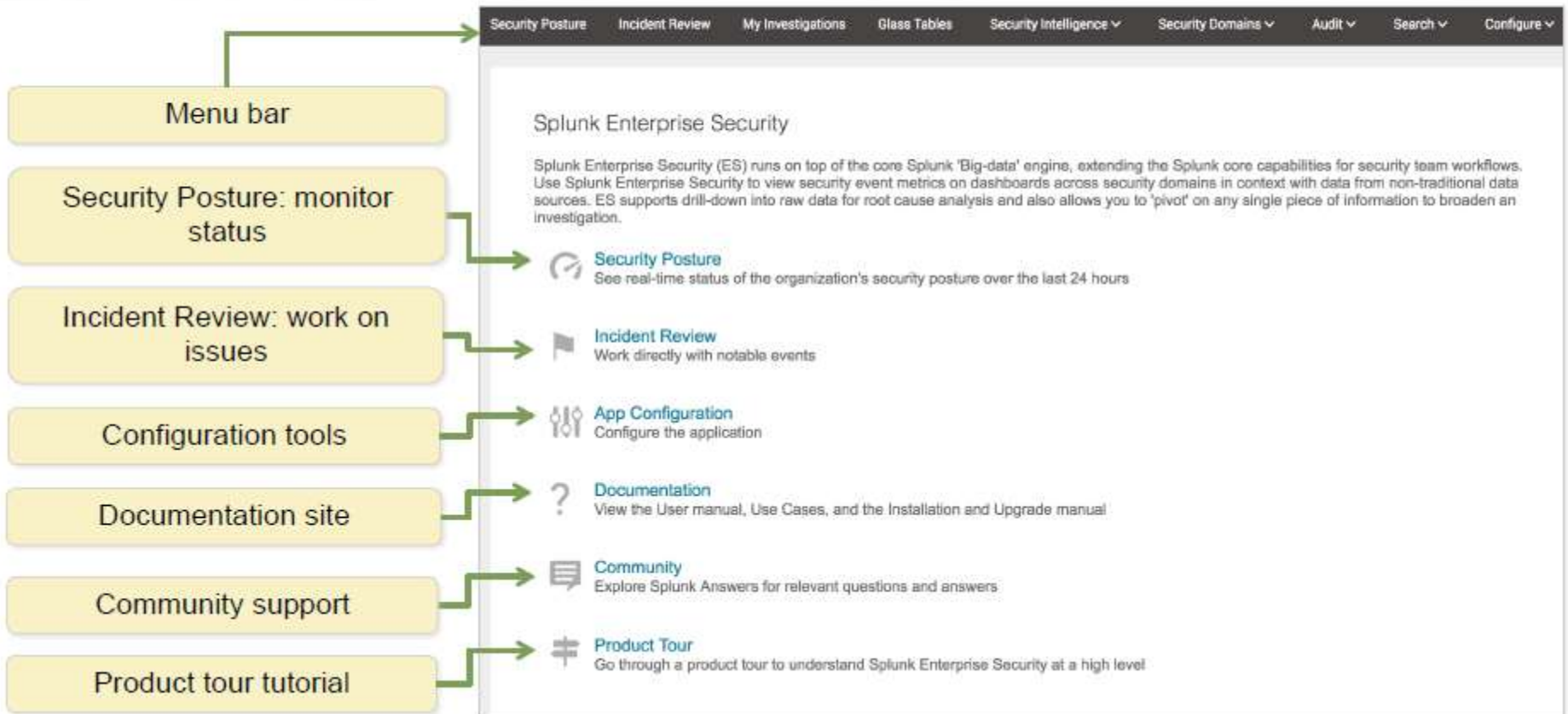
Accessing ES

- Typically, ES runs on a secure (HTTPS) port, so the URL for the server will look something like this:

  `https://eshostname:8000`

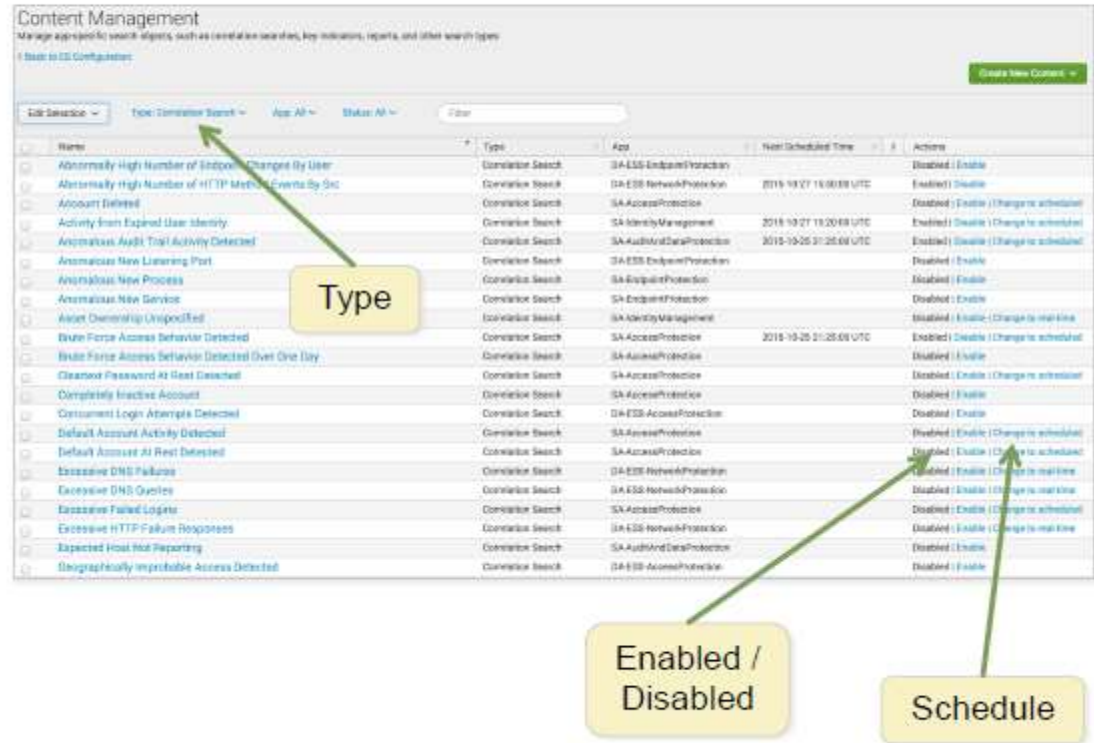
- You must have an assigned role on the ES server
- Once you log on, you see the ES app in the list of apps on the Splunk home page
- You can configure ES to be your default app in your user preferences
  - Click your user name on the top menu bar

The ES Home Page



Active Correlation Searches

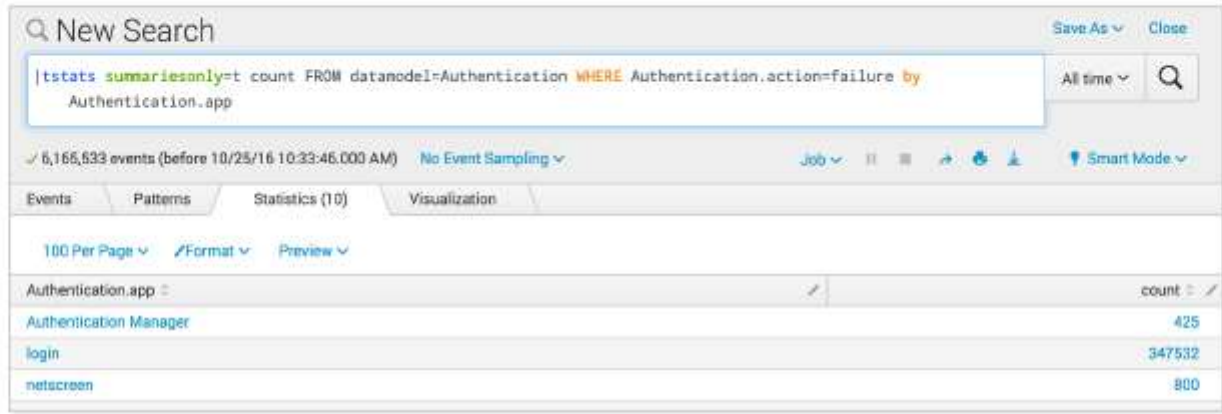
- Select **Configure > Content Management** and choose **Correlation** in the **Type** drop-down
- Note which searches are enabled or disabled
- By default, only ES Admins can enable, disable, modify, or add new correlation searches



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 the Splunk Common Information Model (CIM)
  3. Events are referenced by the accelerated CIM **data models**
- All ES correlation searches, dashboards, and reports use these accelerated data models in their searches
- You can create your own custom searches based on the events in **main** or the data models as needed
  - Use **Search > Search** to begin creating a new search
  - Use **Search > Pivot** to create pivots using ES data models

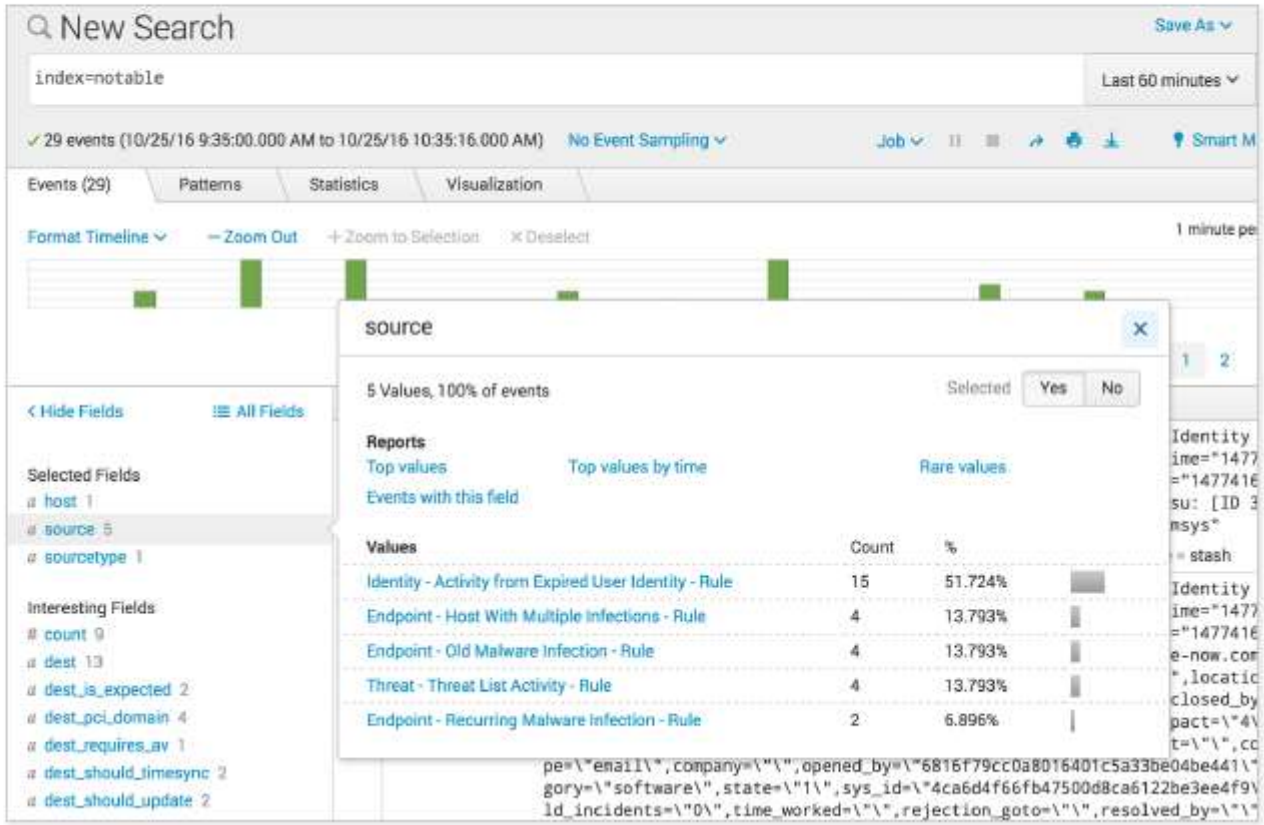
ES Search Example



- Use **tstats** or **datamodel** to create reports based on accelerated data models
  - With **tstats**, use **summariesonly=t** to restrict results to accelerated data for performance improvement
- Use **Search > Pivot** to build pivot reports using ES data models

Notable Events Example

- Select **Search > Search** and run a search in the **notable** index
- Note the list of sources found over the last 24 hours, indicating which correlation searches have generated notable events



Module 2:
Security Monitoring and Incident Investigation

Objectives

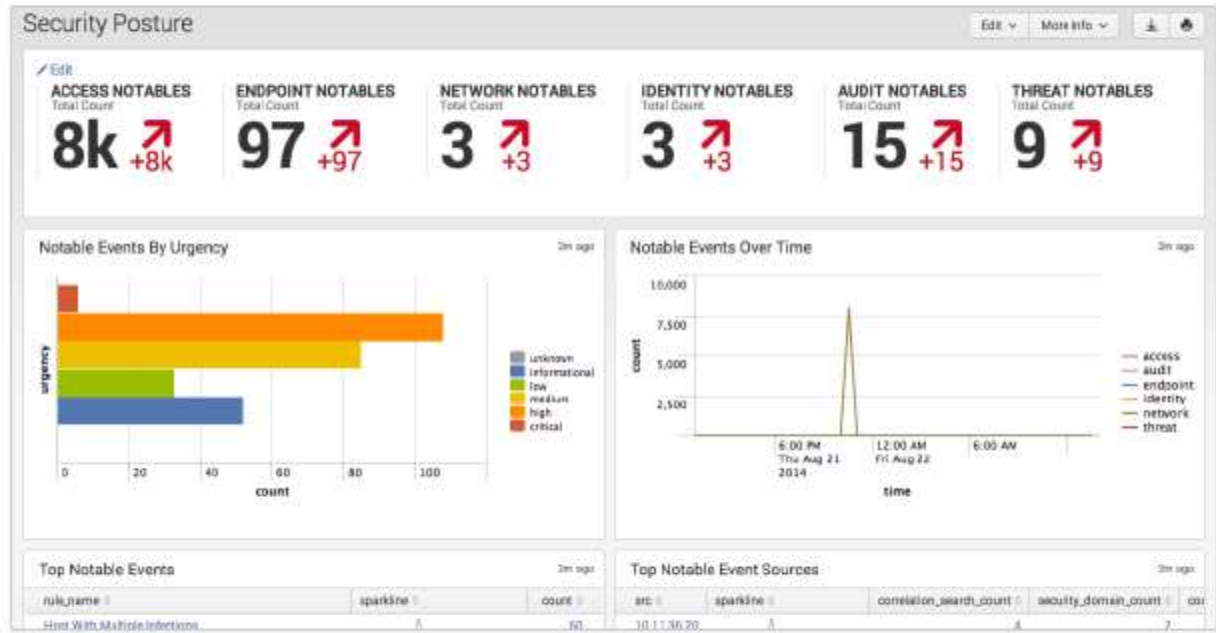
- Use the Security Posture dashboard to monitor enterprise security status
- Use the Incident Review dashboard to investigate notable events
- Take ownership of an incident and move it through the investigation workflow
- Create notable events
- Suppress notable events

Monitoring and Response

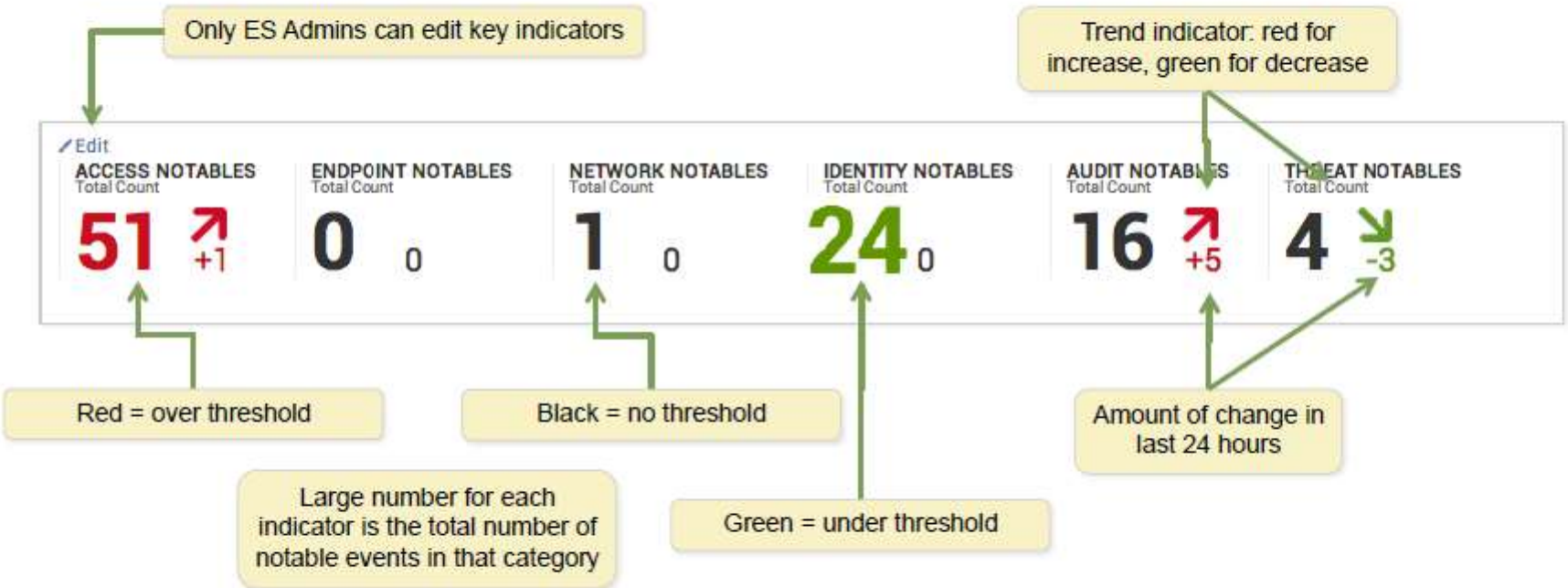
- ES continually runs correlation searches for known types of threats and vulnerabilities
  - There are currently over 60 different correlation search types built in to ES, and you can also create your own
- When a correlation search detects any indicators of compromise (IOC), a notable event is created
  - Notable events are referred to as **incidents**, which can be tracked, updated, and resolved
- Use the **Security Posture** dashboard for an overview of recent notable events, and **Incident Review** to inspect and manage notable event incidents

The Security Posture Dashboard

- An overview of your Enterprise Security condition
- **Key indicators** at the top provide an at-a-glance view of notable event status over the last 24 hours
- Four panels below provide additional summary information categorized by urgency, time, and most common notable event types and sources

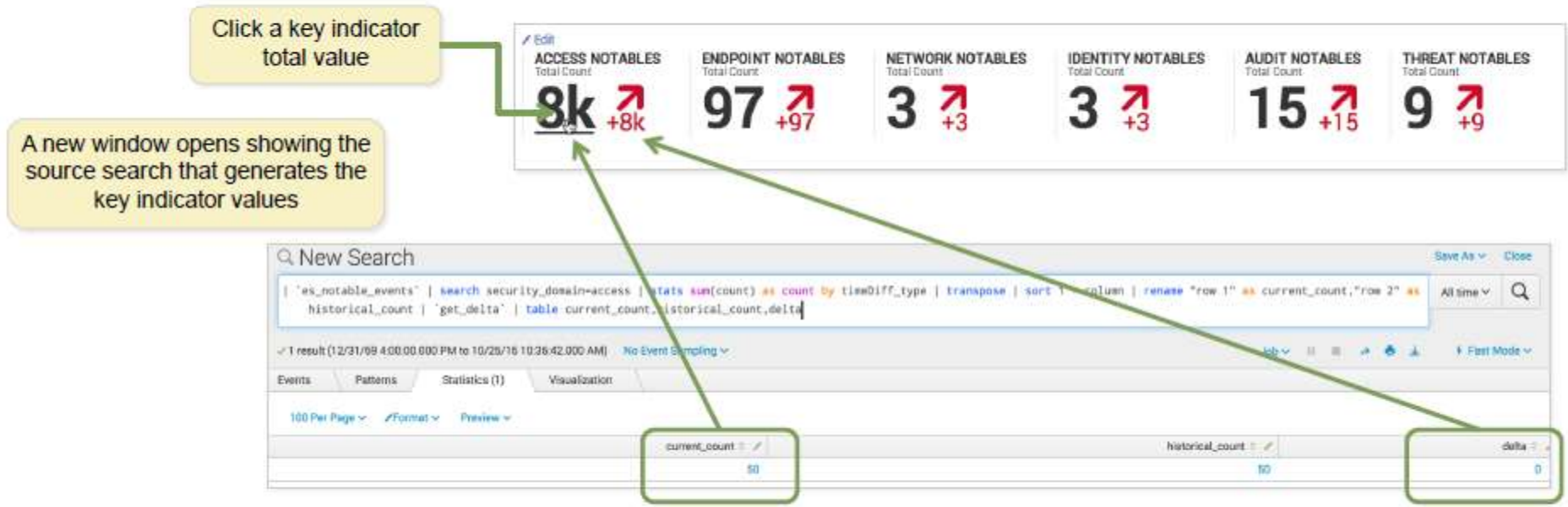


Key Indicators



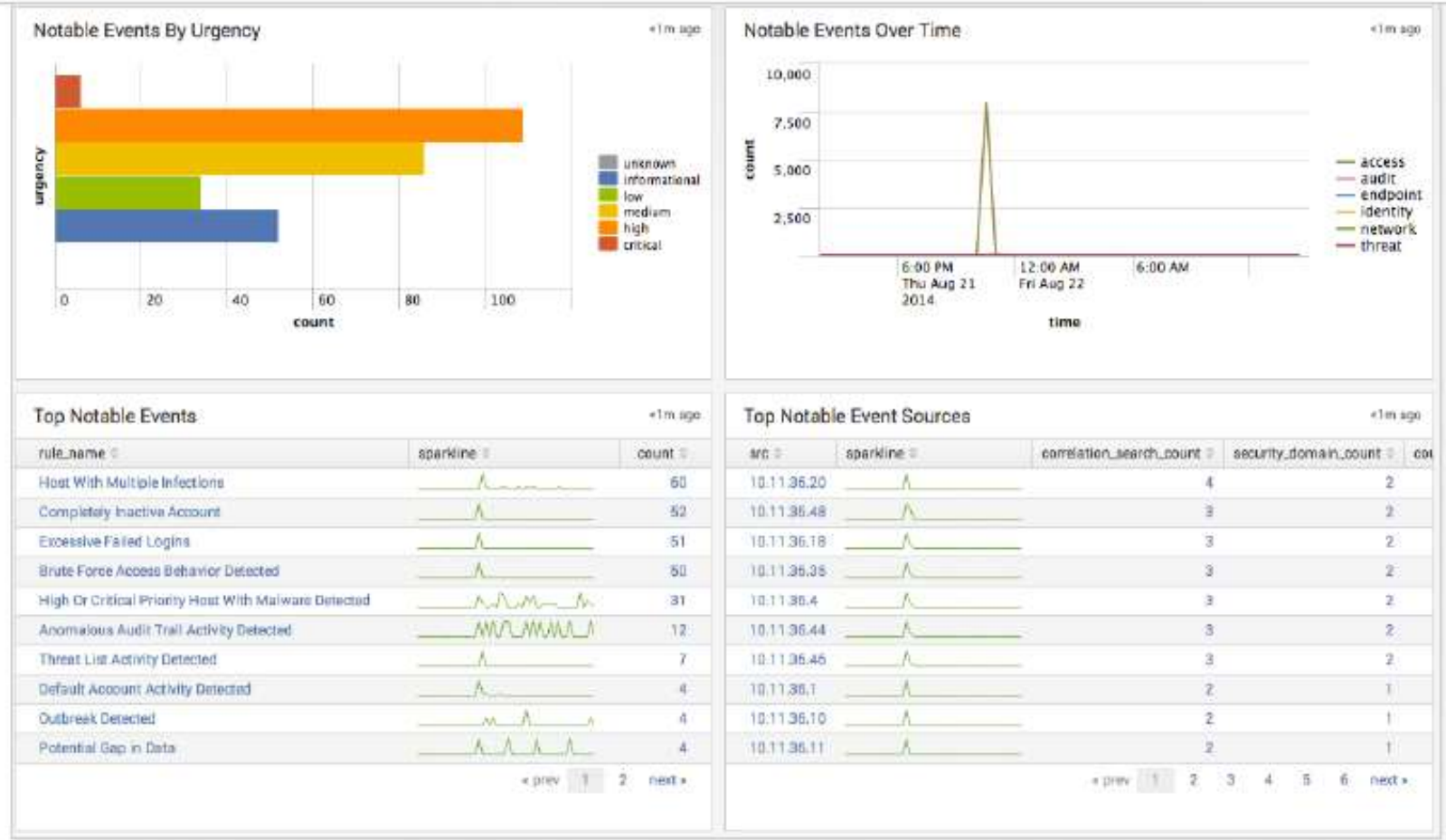
Current total count of events, trend of events, and total increase or decrease over the past 48 hours (from previous 24-hr period to last 24-hr period)

Key Indicator Drilldown



Clicking a key indicator total count displays the search that populates the key indicator values

Security Posture Panels

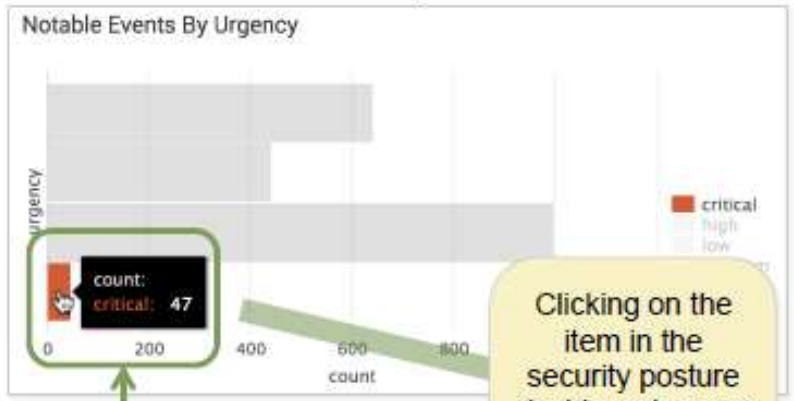


Notable Event Urgency

- Each notable event has an **urgency** field, ranging from informational to critical
- Urgency is a combination of two factors:
  - **Severity** of the incident, as determined by the correlation search
  - **Priority** of the associated assets or identities—i.e., the server or user
- Severity is based on the raw event(s) found by the correlation search
- Priority is assigned to each asset or identity in ES
- If more than one asset or identity is involved in a single notable event, the one with the highest priority determines the urgency

Drilldown Support

Panel in Security Posture



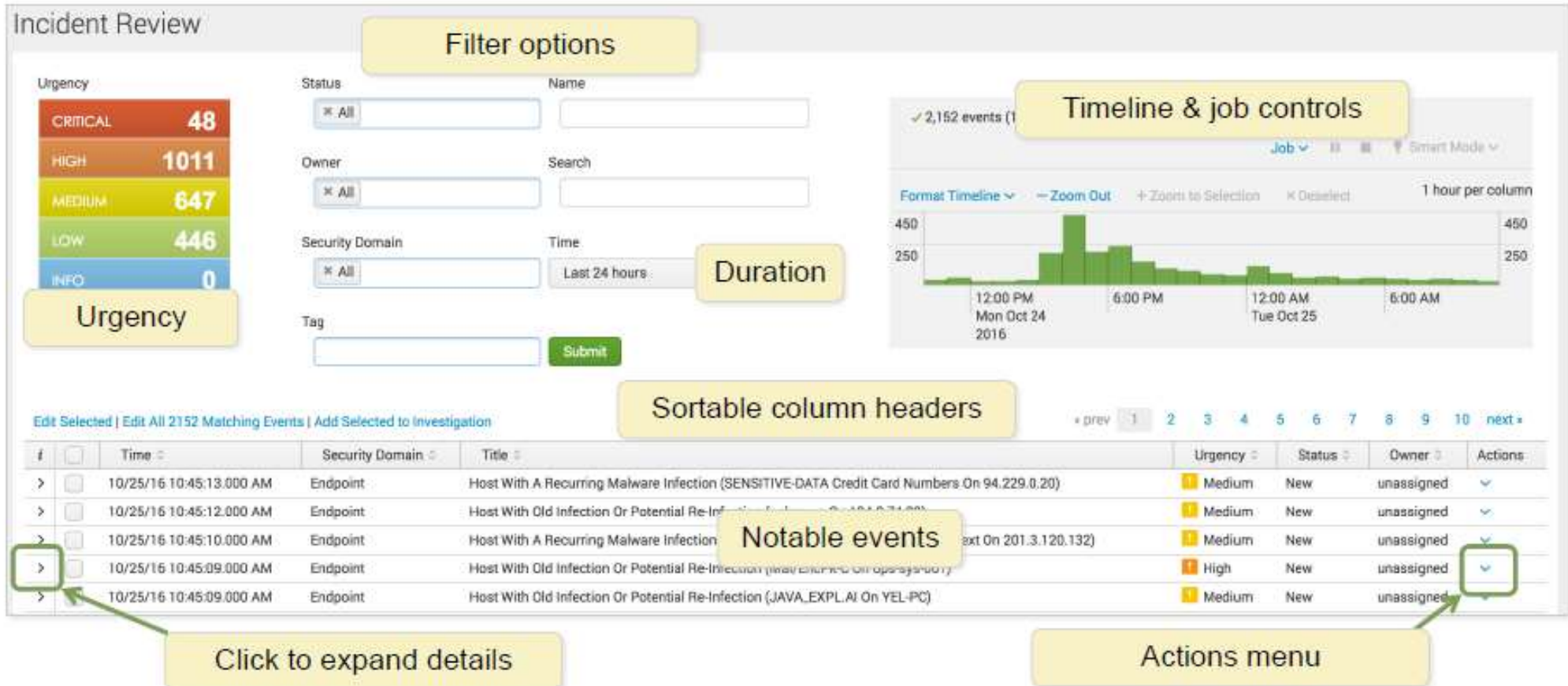
Hovering over an item in a panel shows details about that item's underlying notable events

Clicking on the item in the security posture dashboard opens the related notable events in the incident review dashboard

Once opened in the incident review dashboard, you can drill down into the details of each notable event, take ownership, and "work" the issue

Incident Review Dashboard

The Incident Review Dashboard

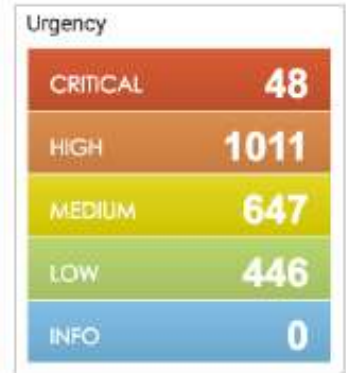


Incident Review Filter Fields

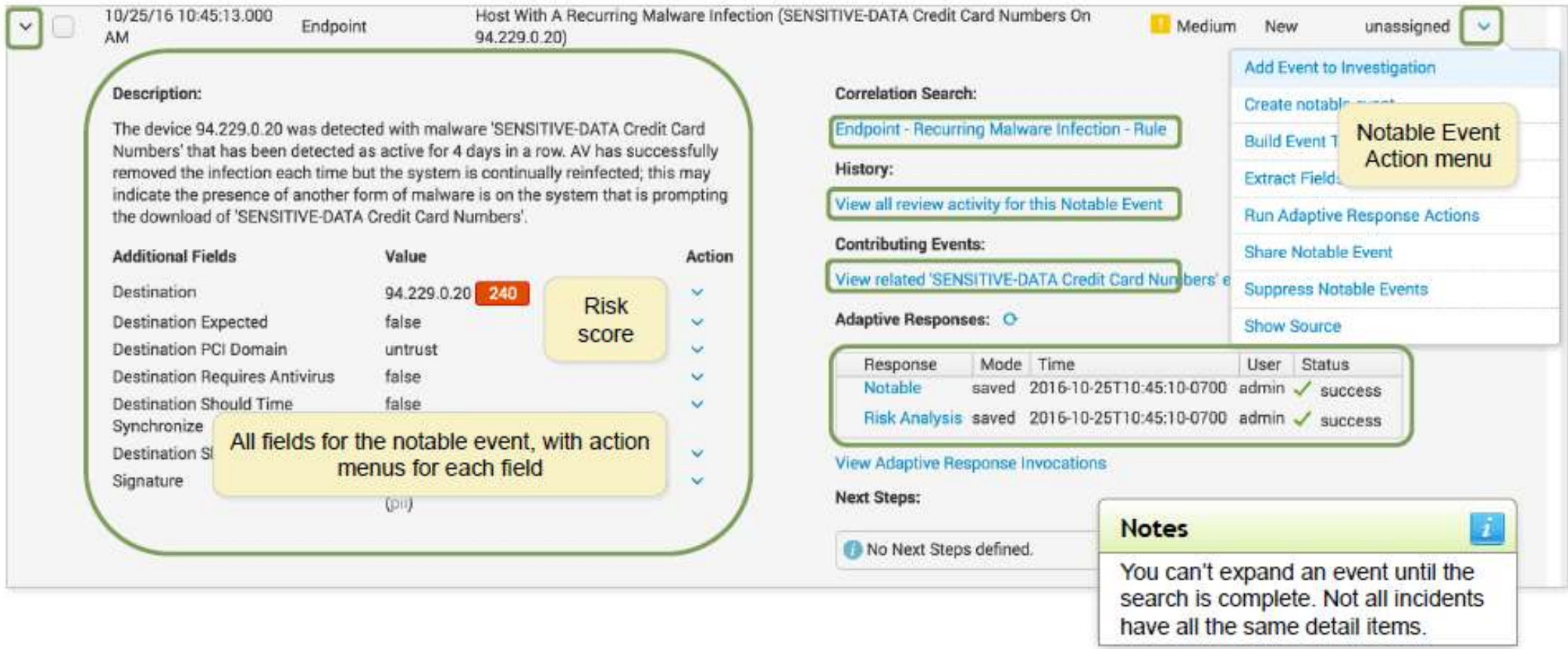
- **Status**: New, In Progress, Pending, Resolved, Closed
  - Along with Owner, use to track status of an incident
- **Urgency**: info, low, medium, high, critical
- **Security Domain**: Access, Endpoint, Identity, Network, Threat, Audit
- **Owner**: The user assigned to investigate and resolve an incident
- **Name**: The title of a correlation search—wildcards (*) supported
- **Search**: Splunk search language expressions
- **Tag**: a list of tag names

Using the Incident Review Dashboard

- Select one or more values per field
  - More than one value per field are **OR**ed together
- Urgency values can be toggled on and off
  - Grey values are "off" and will not be displayed
- If values are set for more than one field, the fields are **AND**ed together
- **Status**, **owner**, **domain** and **tag** support multiple **OR** values
  - The default **And** is ignored if other values are selected
- **Name** supports wildcards, **Search** supports full SPL

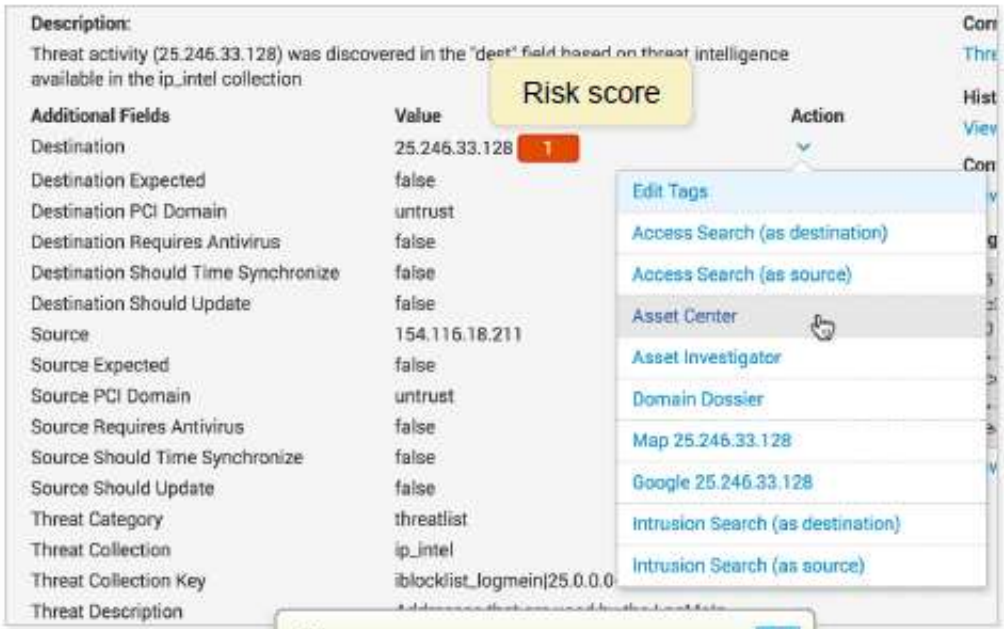


Notable Event Details



Field Action Menus

- Each notable event field has an action menu allowing you to set tags, access other ES dashboards to view events or analyze the data in the field, and more
- Risk scores for hosts or users are displayed next to fields
  - Clicking a risk score opens the Risk Analysis dashboard for that asset or identity

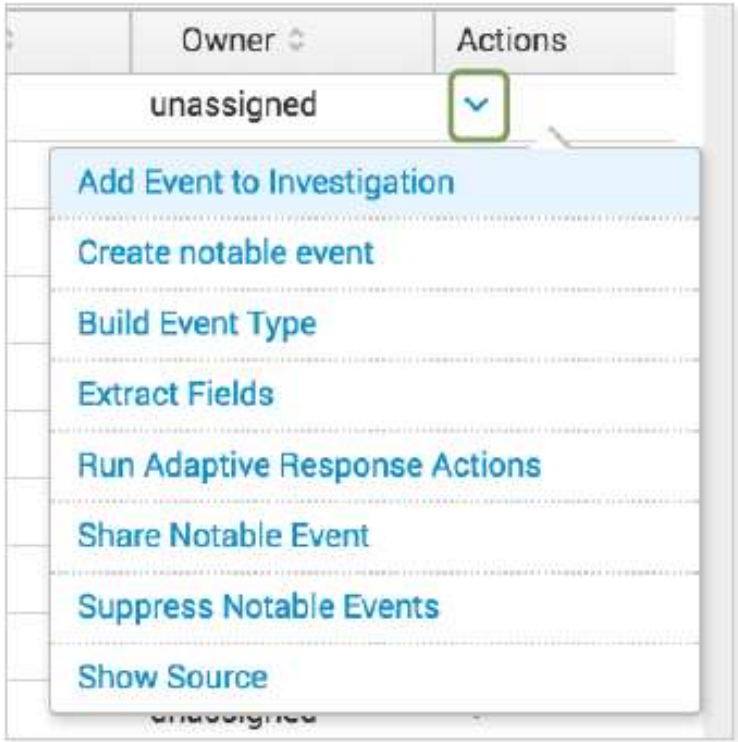


Notes

Action menus only display 10 items at a time. Scroll the menu to make sure you see all the items.

Notable Event Actions Menu

- Each notable event also 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 adaptive response actions

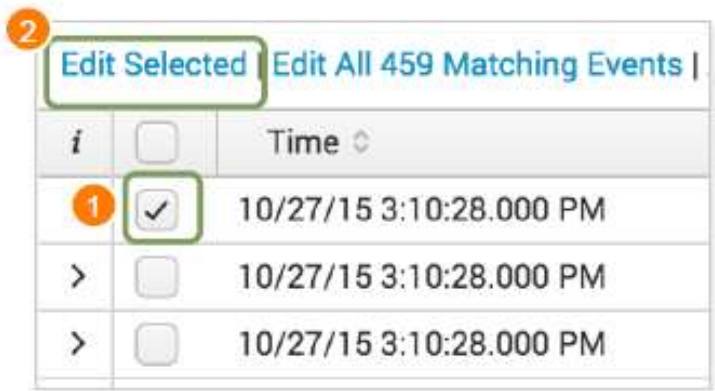


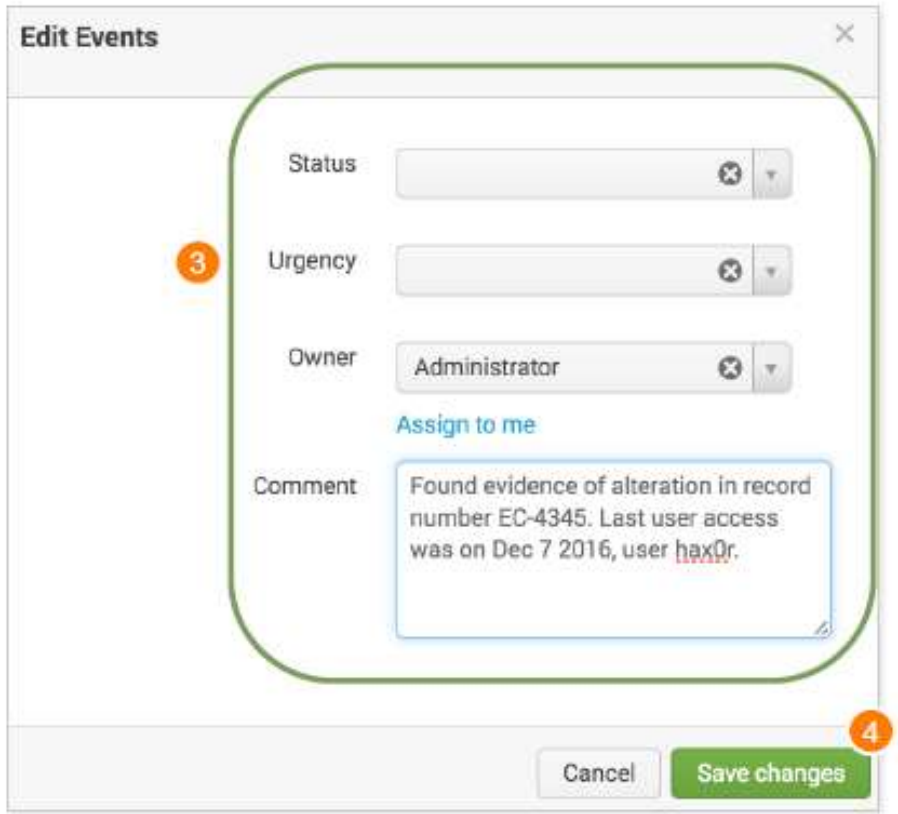
Incident Workflow: Concepts

- Working an incident consists of assigning the incident to an owner, investigating, and implementing corrective measures
- Change the status as you progress from investigation to resolution
- How you use these status flags is up to you--ideas:
  - New = not yet being worked
  - In progress = investigation under way, no resolution determined
  - Pending = various: work in progress, awaiting action, etc.
  - Resolved = fixed, awaiting verification
  - Closed = fix verified
- ES Admins can add new status values as necessary

Incident Workflow: Procedures

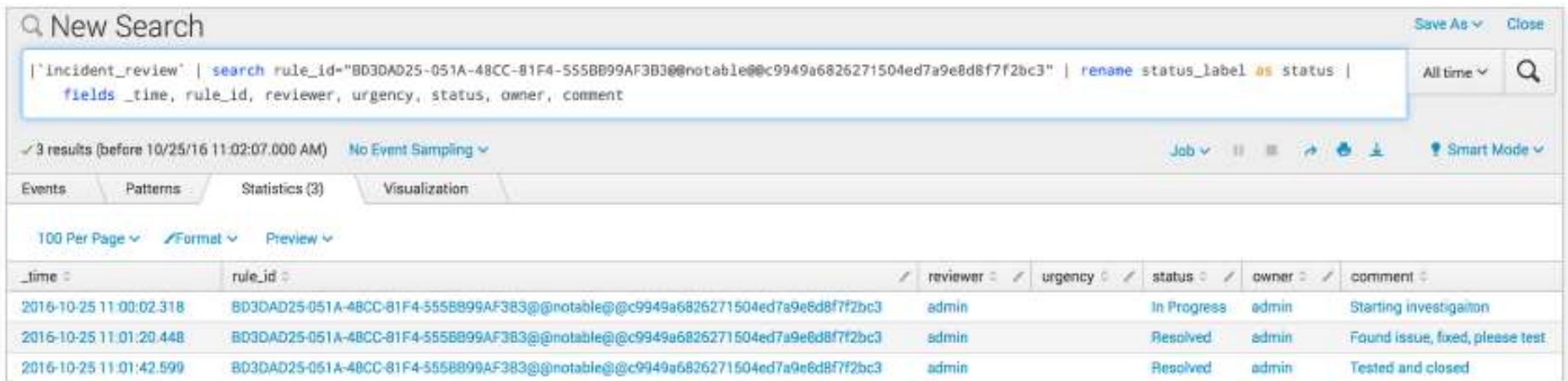
1. Select one or more events
2. Click **Edit Selected**
3. Set Status, Urgency, Owner, and Comment
4. Click **Save changes**





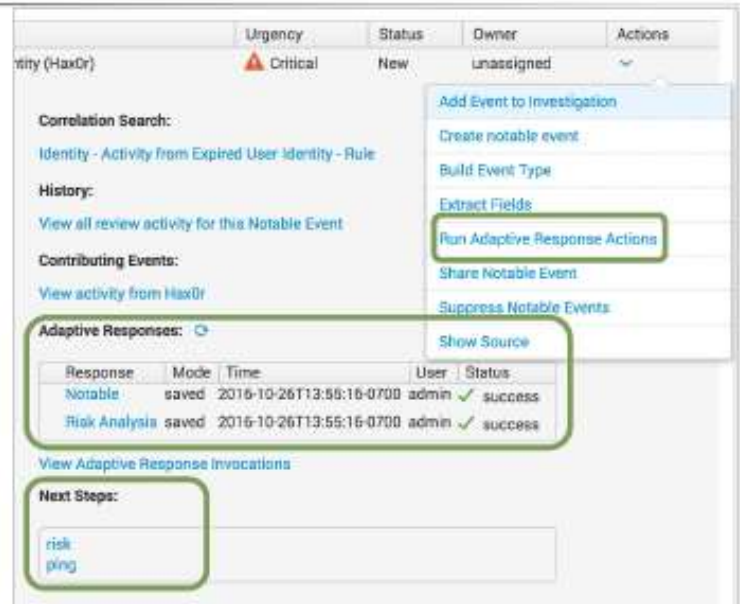
Incident Review History

- Selecting **View all review history for this Notable Event** opens a new search showing all review events for the current issue
- The **`incident_review`** macro can be used in your own custom searches and reports for incident status tracking



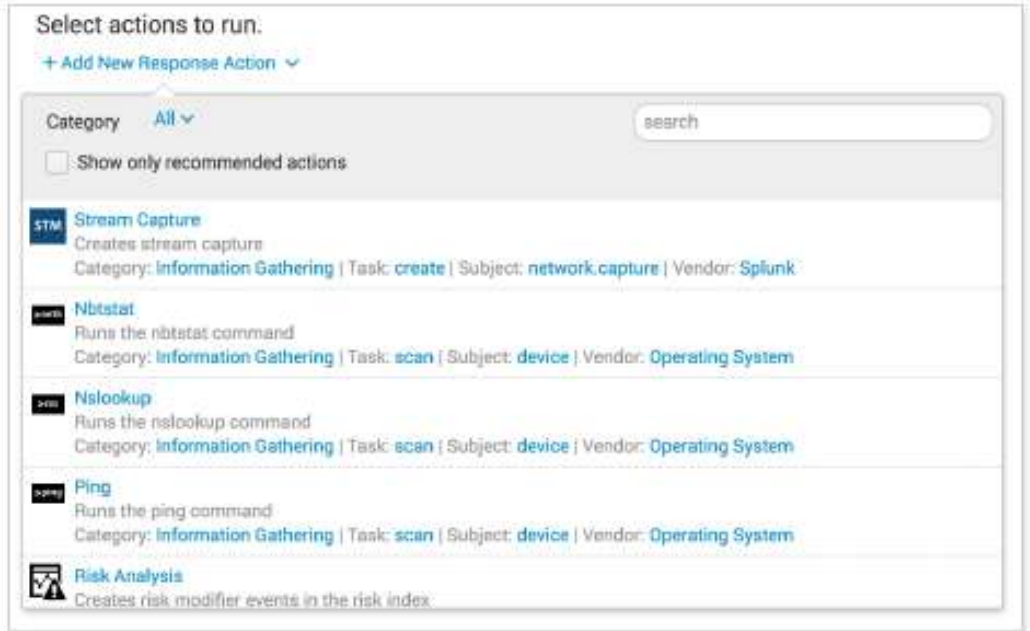
Adaptive Response

- A notable event may contain **adaptive responses** the analyst can initiate
  - Actions menu: Select other adaptive responses to execute
  - Adaptive Responses: See a list of previously executed responses
  - Next Steps: Click a suggested response
- Depending on the type of notable event, different adaptive responses are available
  - Examples: ping host, change risk, run a script, send to UBA, etc.



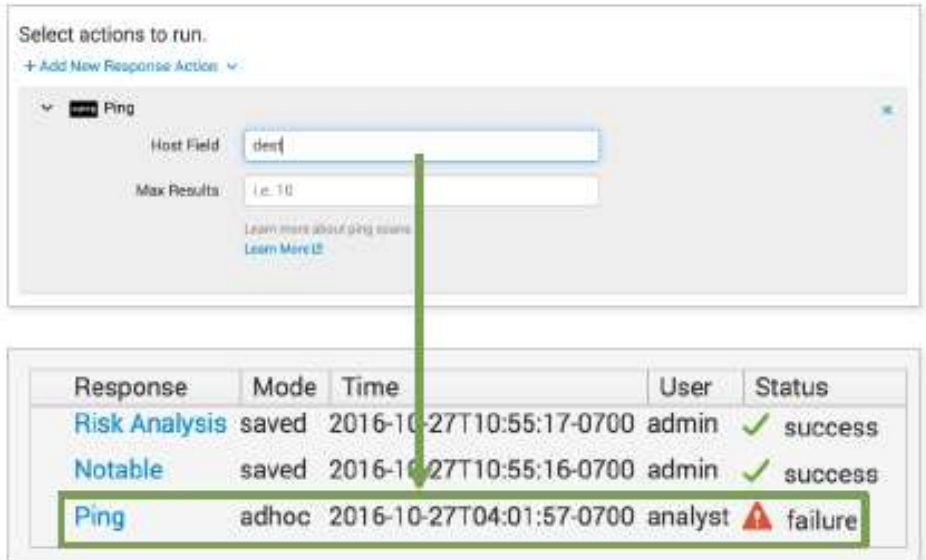
Adaptive Response Actions

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



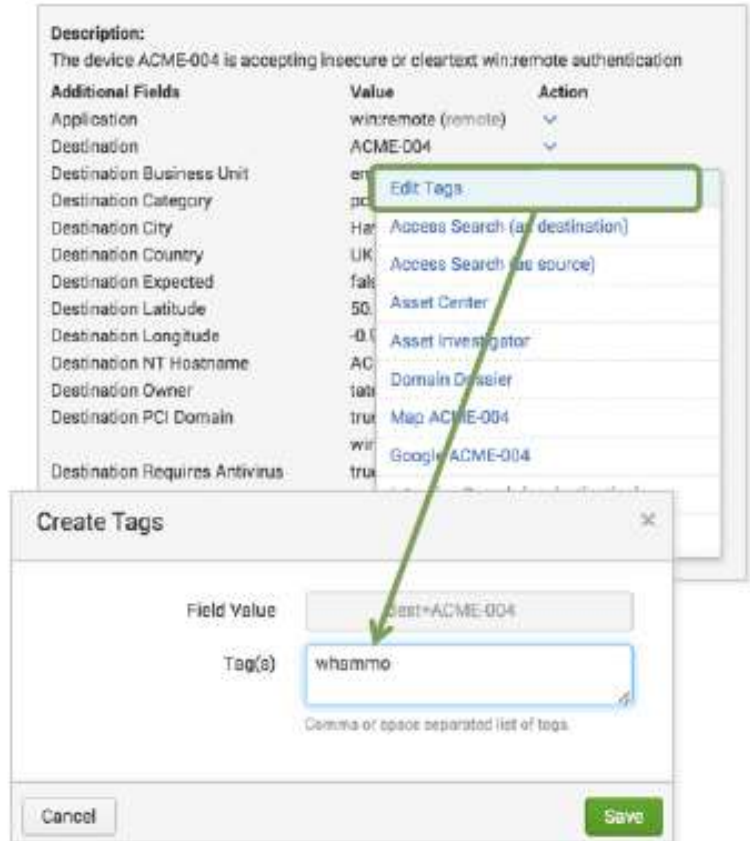
Adaptive Response Example: Ping

- As you investigate an incident, you may need to determine if the affected server is up
- From the list of adaptive response actions, select **Ping**, and fill in the host field
  - You can use a static value or the name of a field in the notable event containing the server's IP address or host name
- After the action executes, the results are displayed in the notable event's list of adaptive responses



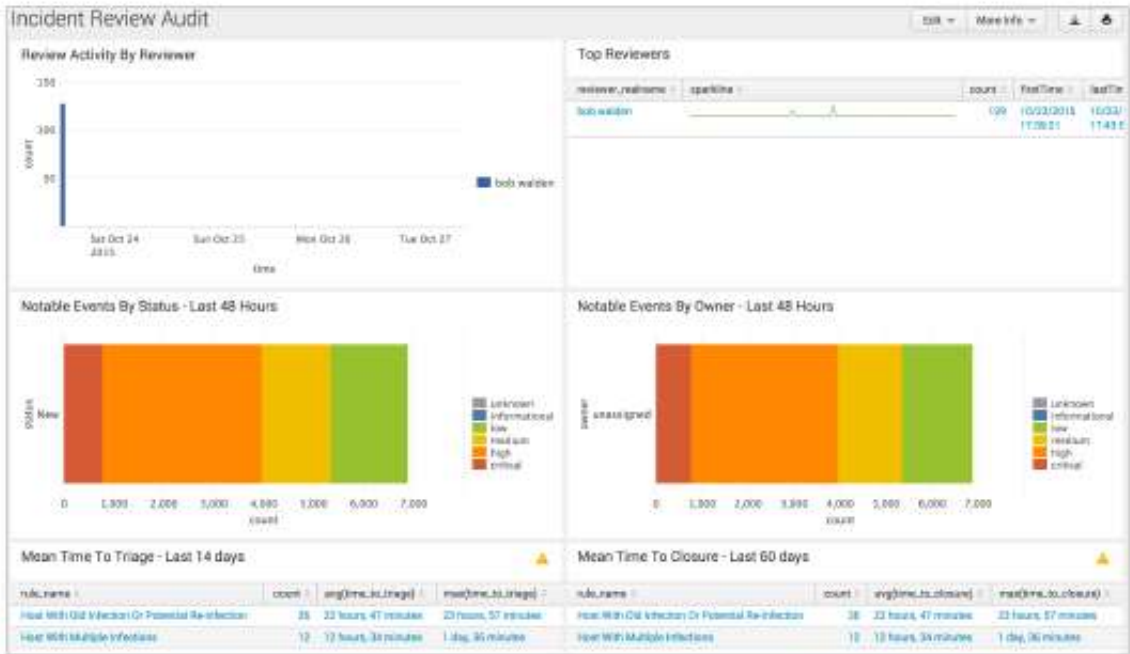
Tagging Incidents

- You can use tags as a method to track significant incidents
  - Example: you want to be able to quickly find all the incidents related to servers being used by project "whammo"
- Add a tag to each server (using the action menu for the **dest**, **src** or **ip** fields in this example) and then search for the tag name in the **Tag** filter field
- Now only notable events/incidents with this tag value are displayed



Incident Review Audit

- **Audit > Incident Review Audit**
- Provides an overview of incident review activity
- Shows how many incidents are being reviewed and by whom
- Displays incident aging over last 48 hours, broken down by status and by reviewer
- Statistics on triage time and closure time

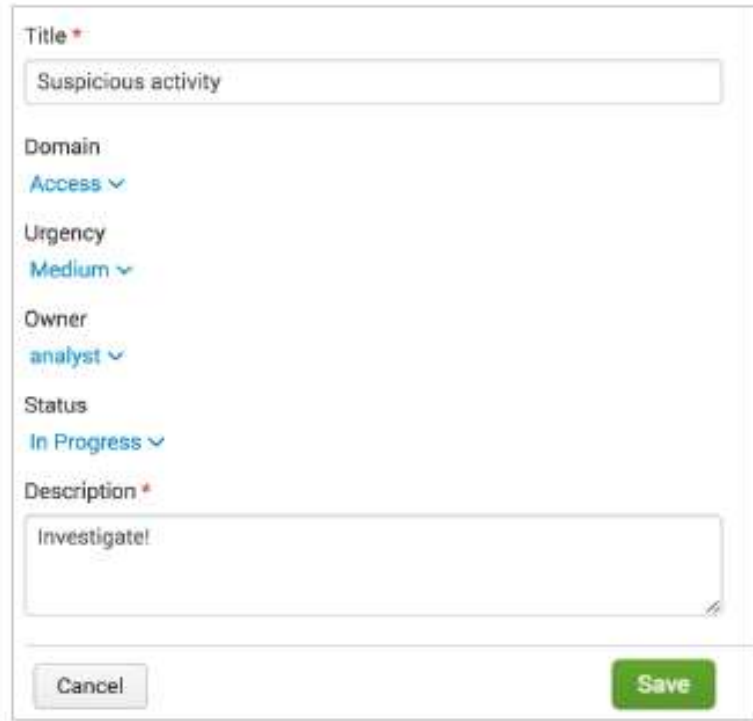


Creating and Suppressing Notable Events

- **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
- By default, ES Analysts do not have permission to perform these actions
  - An ES Admin must enable these capabilities for ES Analysts if desired

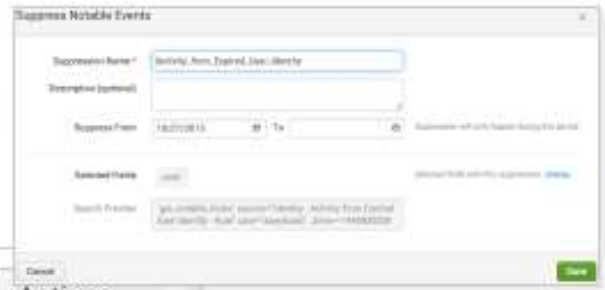
Creating Notable Events

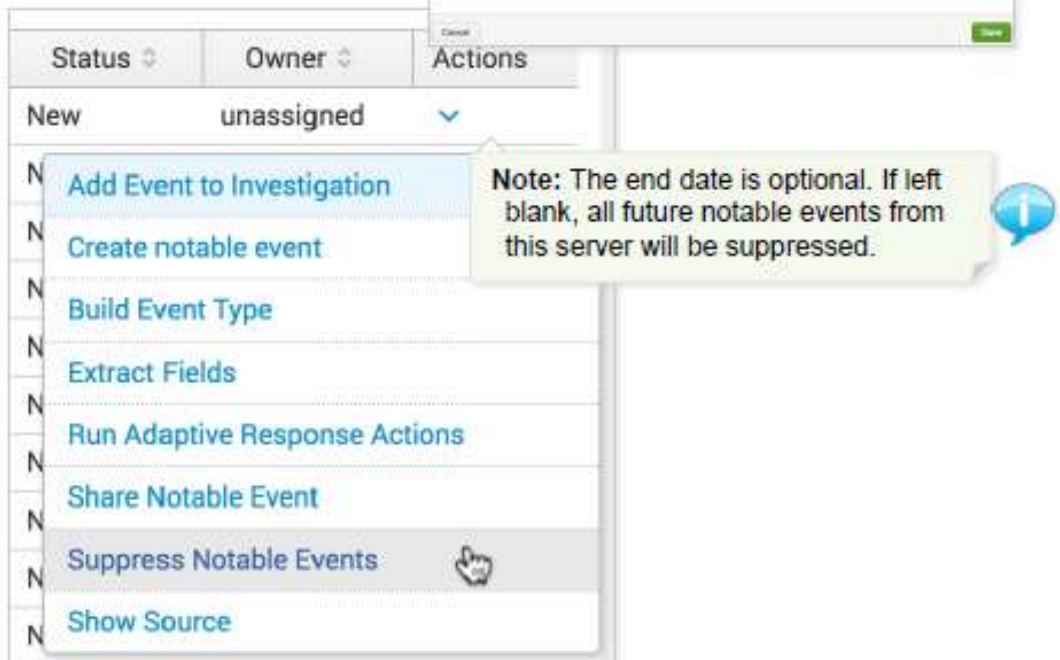
- You can create ad-hoc notable events
  - For instance: if you find an event in Splunk that has not triggered a correlation search's parameters, but you feel it should be investigated
- Steps:
  1. Run a search on the source events
  2. Expand an event and select **Event Actions**
  3. Select **Create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



Suppressing Notable Events

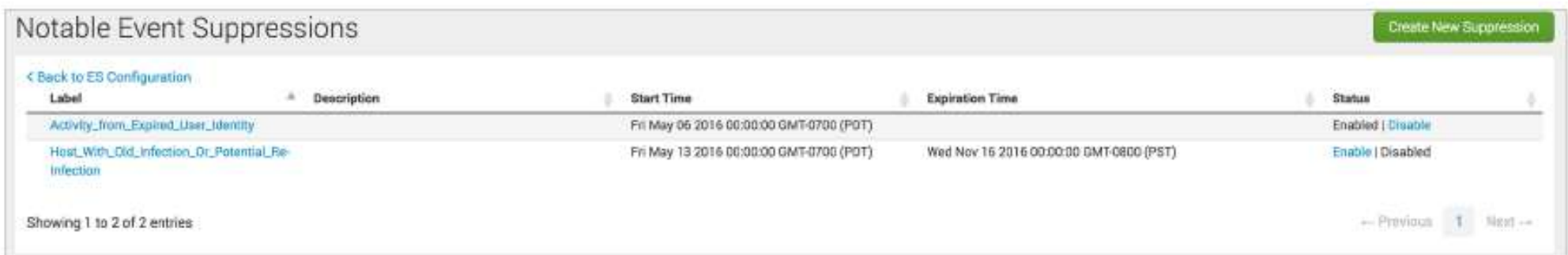
- You may want to suppress notable events that are deemed to be a false positive, perhaps due to a server being temporarily misconfigured
- To do so, start from **Incident Review**:
  1. Expand the notable event's **Actions** menu
  2. Select **Suppress Notable Events**
  3. Set description and dates
  4. Click **Save**





Managing Notable Event Suppressions

- After you create a new notable event suppression, you will see the list of suppressions as a confirmation
  - You can access this list via **Configure > Incident Management > Notable Event Suppressions**
- Only ES admins can edit these suppressions by default
  - While editing, you can modify the suppression search criteria if desired



Module 3:
Investigations

Objectives

- Use investigations to manage incident response activity
- Use the investigation timeline
- Add items to investigations

Investigations

- An **investigation** is a collection of activities and notes related to work done on a specific issue, such as a breach or other incident
- Investigations are organized chronologically into **timelines**
- Investigations can be managed by one or more analysts
- Use investigations to:
  - Visualize progress
  - Document work
  - Share information

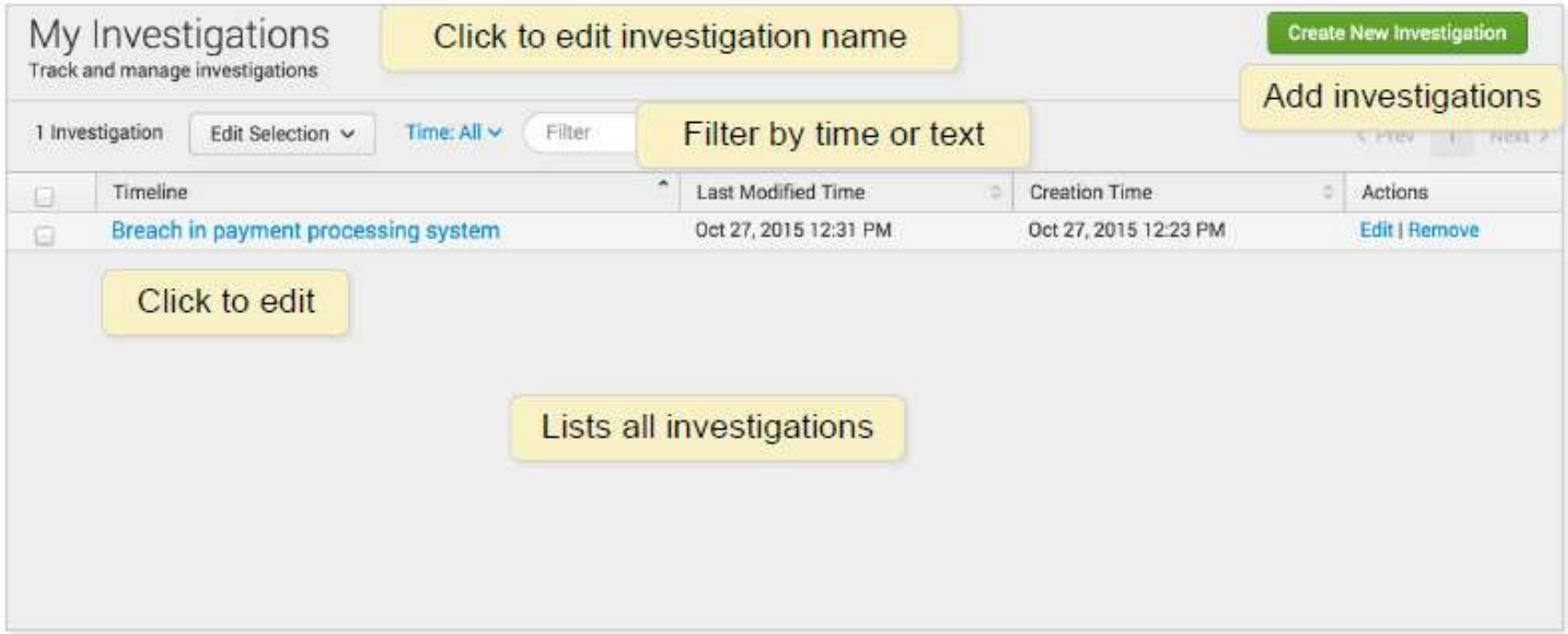
Starting an Investigation

- You can create a new investigation:
  - From the Incident Review dashboard's Actions menu
  - On the **My Investigations** dashboard
  - From any ES dashboard using the Investigation Bar at the bottom of the ES window
  - When searching raw events, from the Event Actions menu
- By default, only ess_admin and ess_analyst users can create investigations
- Each investigation has one owner and can have any number of additional collaborators
  - Only owners and collaborators can modify the investigation

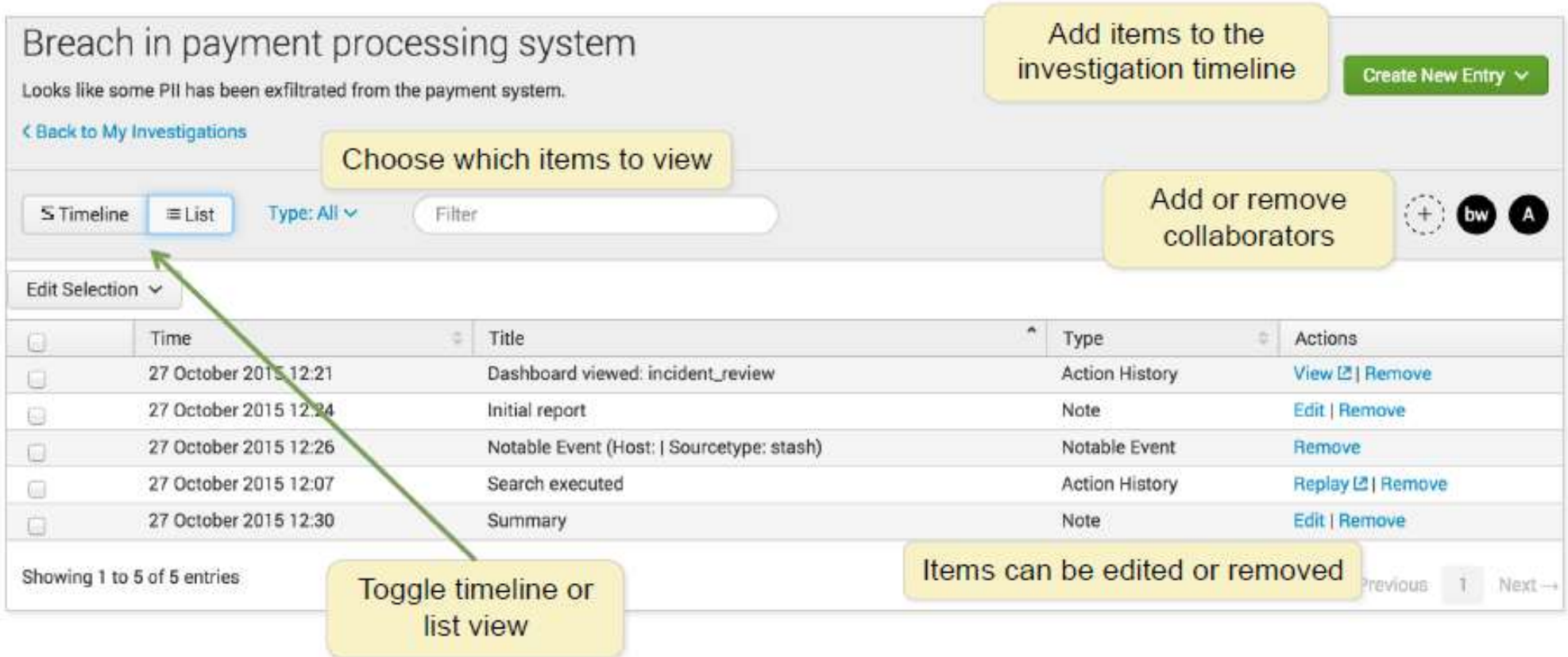
Scenario: Data Exfiltration

- Customers have reported unauthorized use of their account numbers (from your store)
- Start an investigation, and begin researching the issue
  1. Create a note describing the situation and how you were notified
  2. Examine notable events related to the payment processing system and add them to the investigation
  3. Run ad-hoc searches and add the results to the timeline
  4. Add notes periodically to explain why you ran searches and what you found in the results
  5. Add notes detailing actions taken to mitigate the breach and close the vulnerability

My Investigations Dashboard



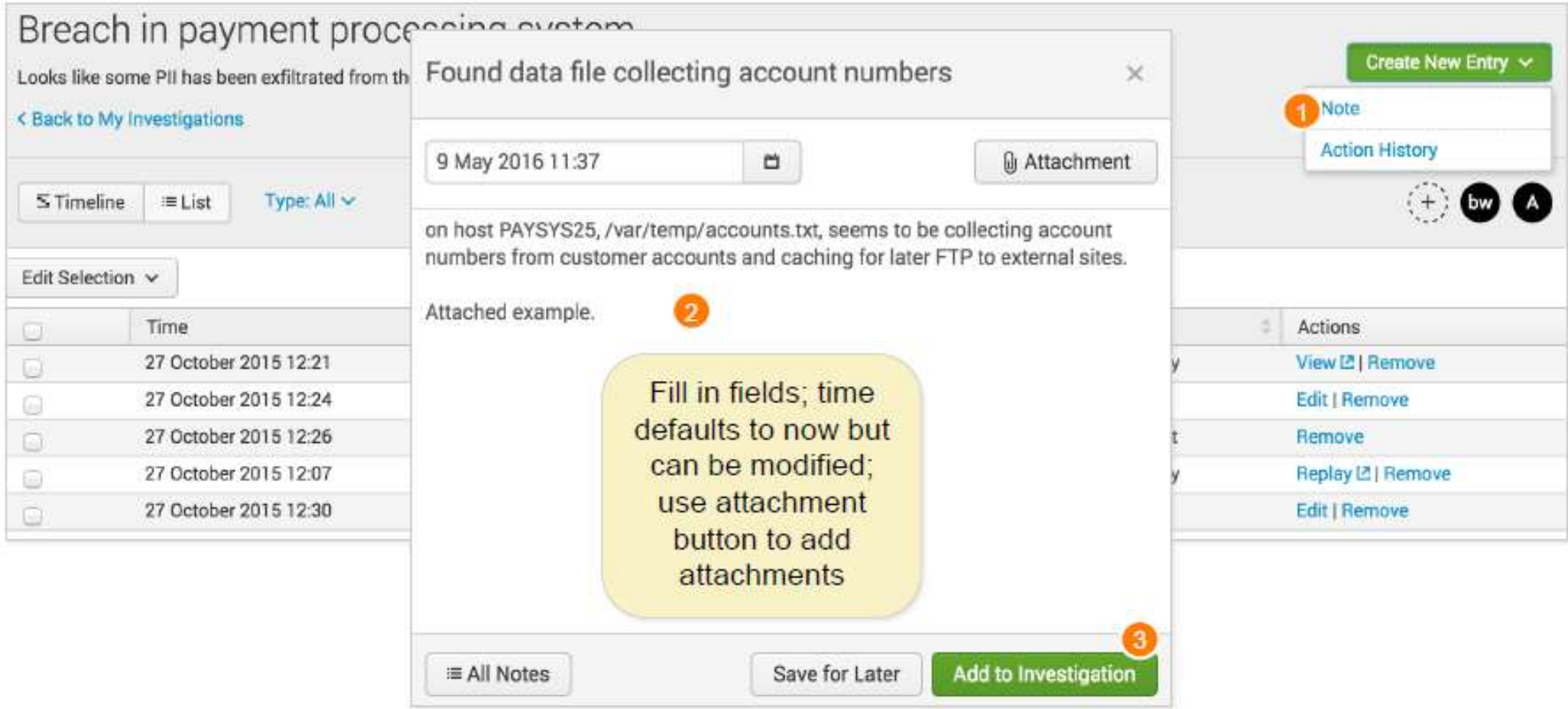
Investigation List View



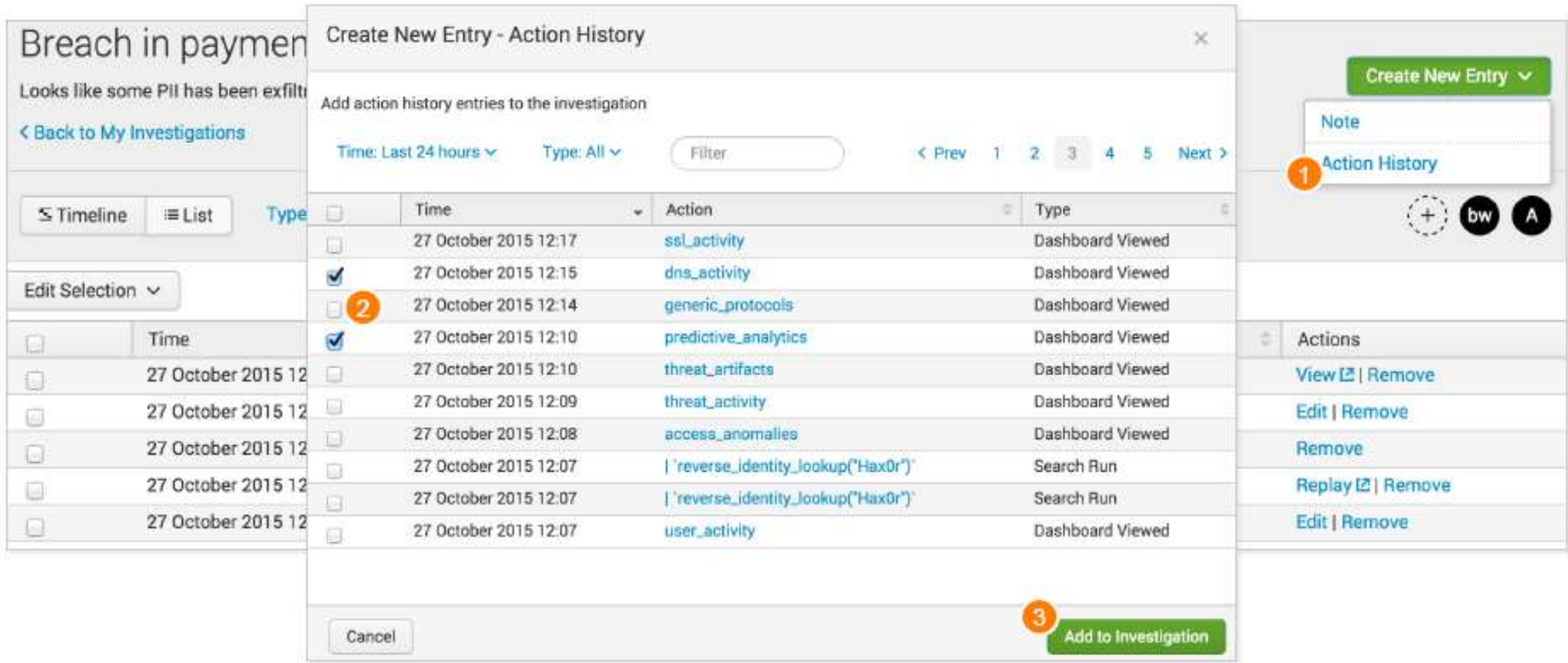
Adding Items to the Investigation

- Use the **Create New Entry** drop-down to add new items
- **Note**
  - Generic text items used to add information relevant to the investigation
- **Action History**
  - A reverse chronological list of all of your activities in ES: searches run, dashboards used, etc.
  - Add these to your investigation to document the steps you've taken to research the issue
  - Adding notes can clarify why you ran the search and what the results mean for your investigation

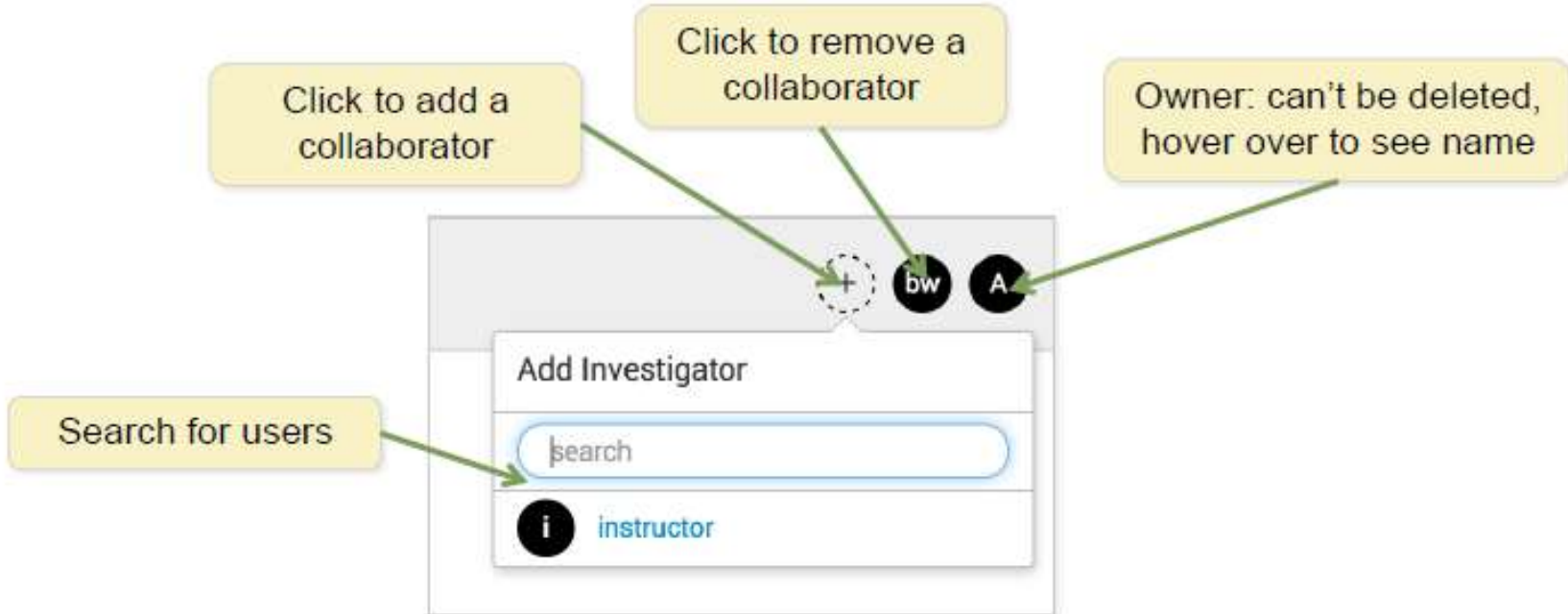
Example: Adding a Note



Example: Adding Action History Items

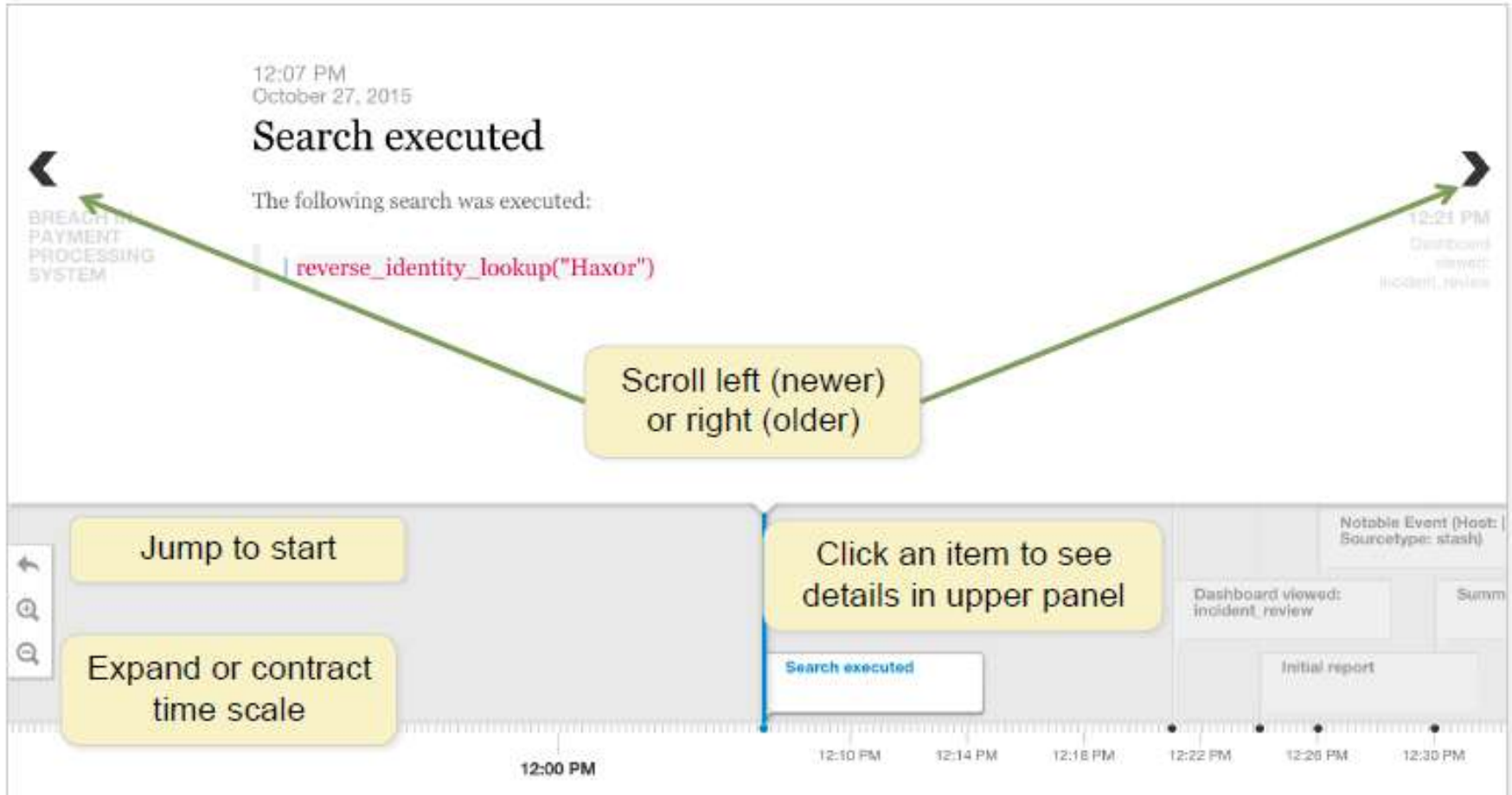


Adding Collaborators

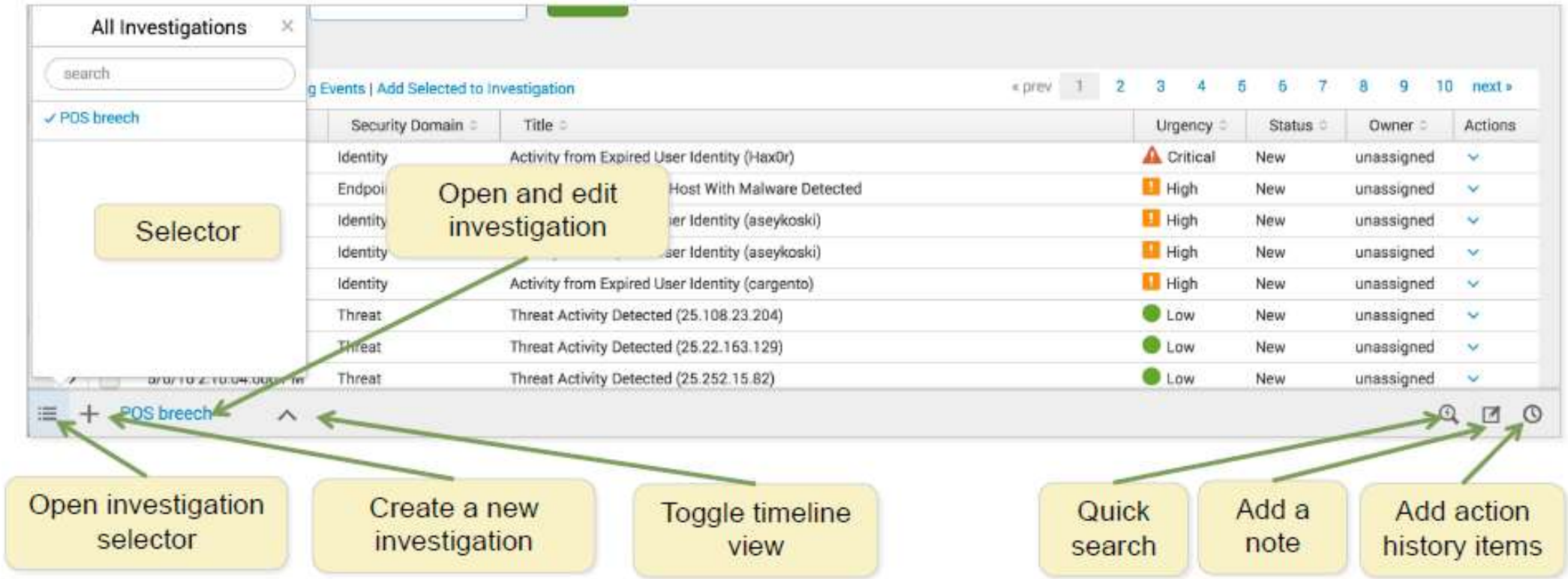


Only the owner and collaborators can work on an investigation

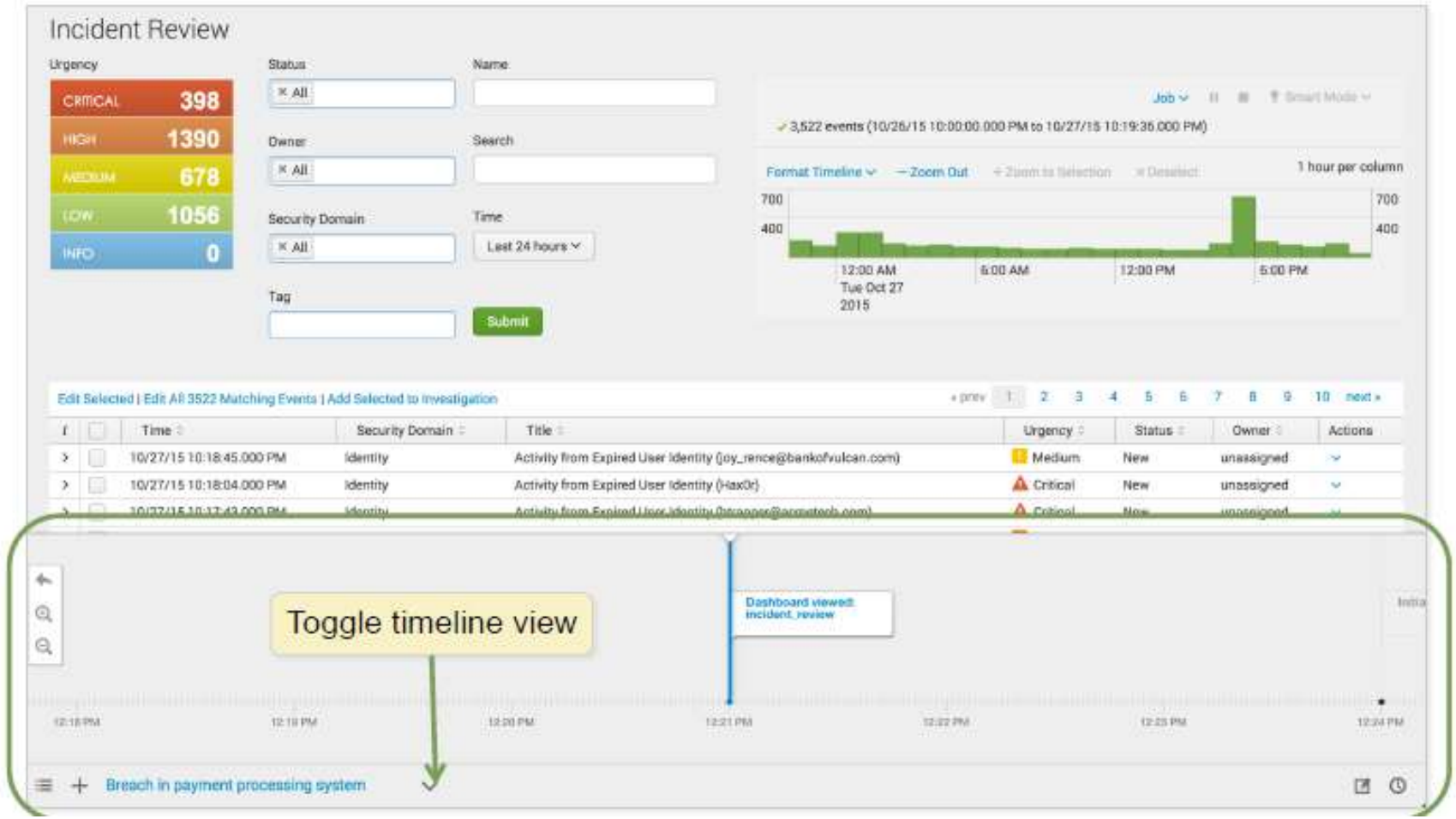
Timeline View



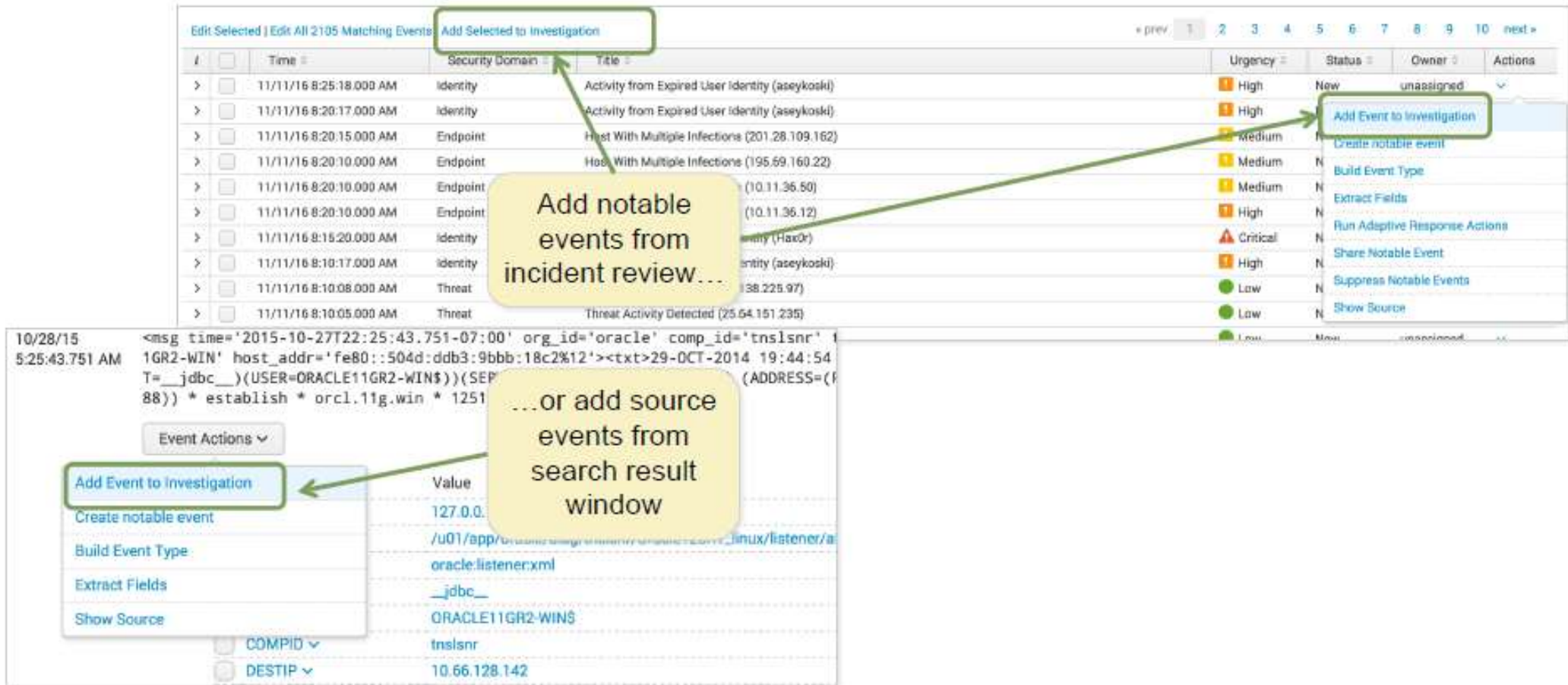
Investigation Bar



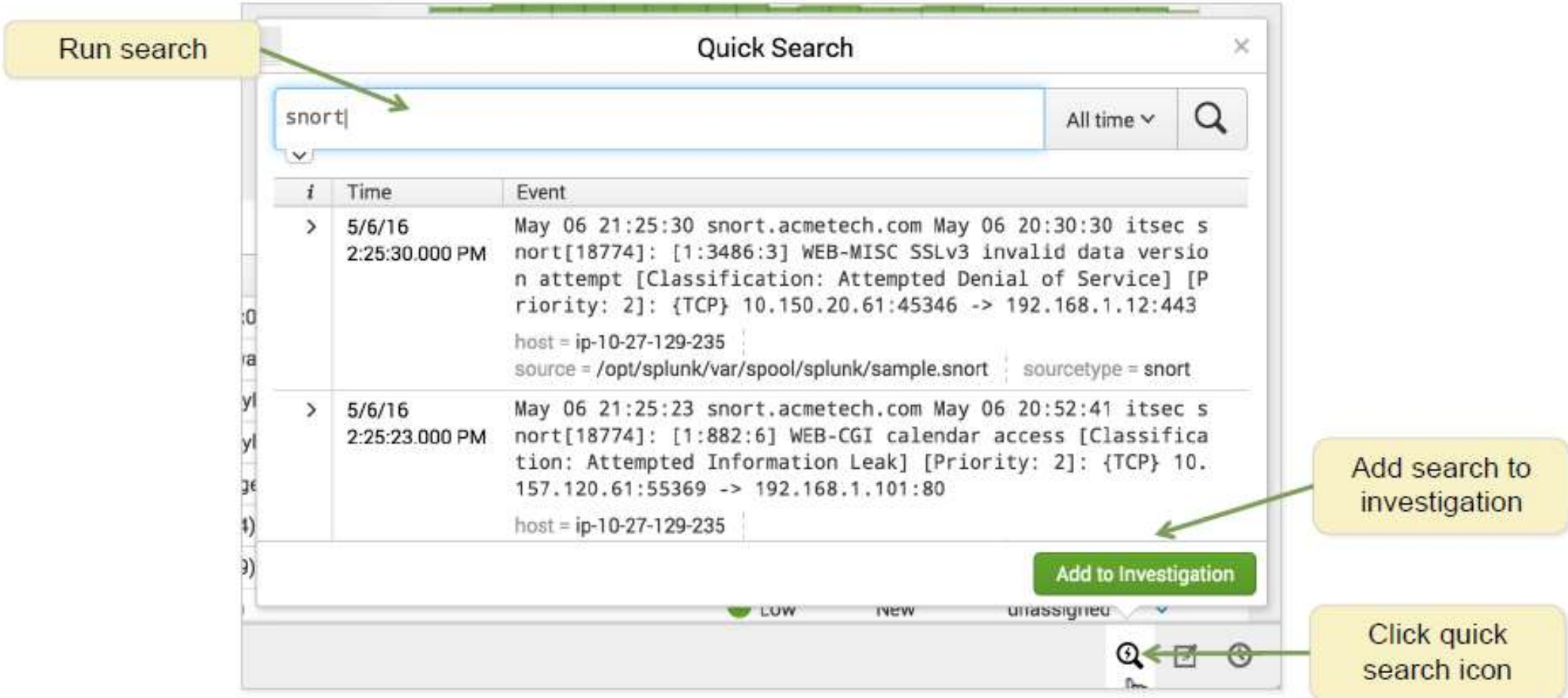
Inline Timeline View



Adding Events



Quick Search



Module 4:
Forensic Investigation with ES

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

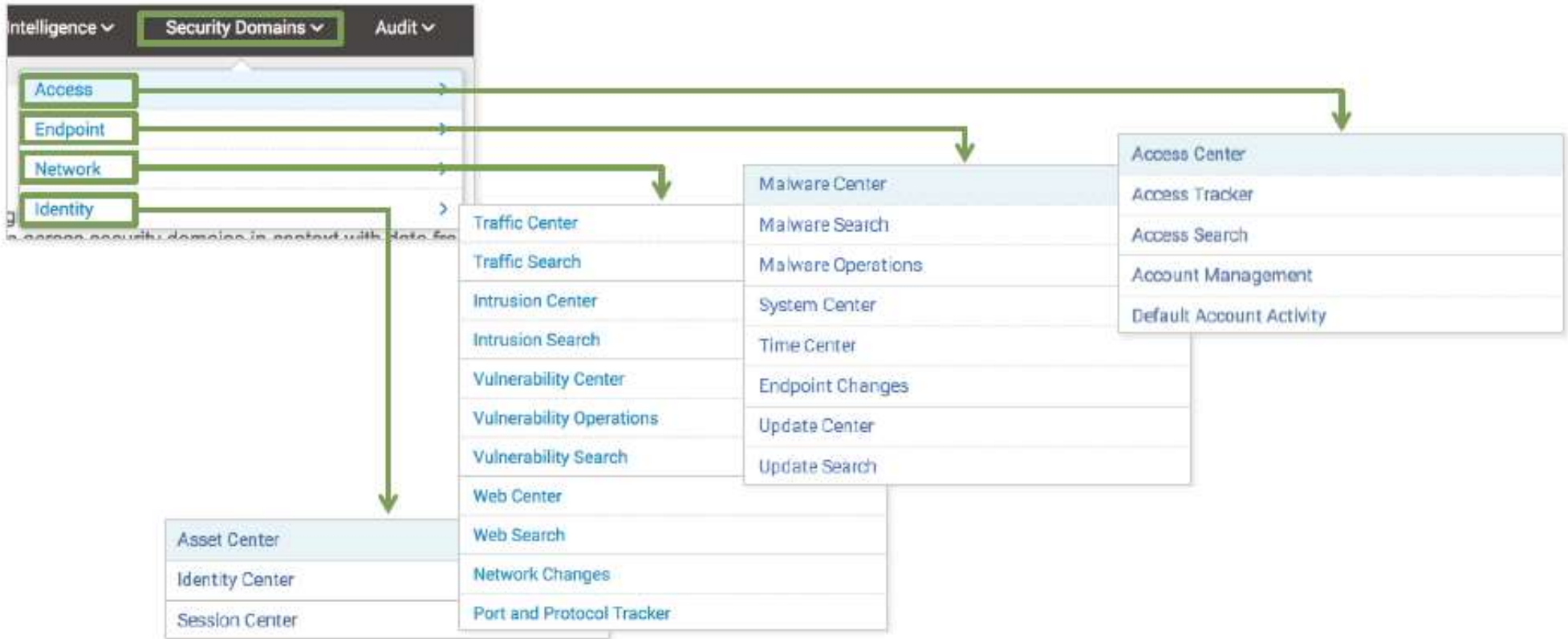
ES and Forensic Investigation

- When a breach occurs, you need to examine the details related to the incident to determine a root cause and eliminate the risk
- The domain dashboards in ES 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

Identifying Primary Domains

- **Access**: authentication attempts and access control related events (login, logout, 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, network vulnerability scanners, proxy servers, and hosts
- **Identity**: examine identity and asset lookup data

Domain Dashboard Navigation



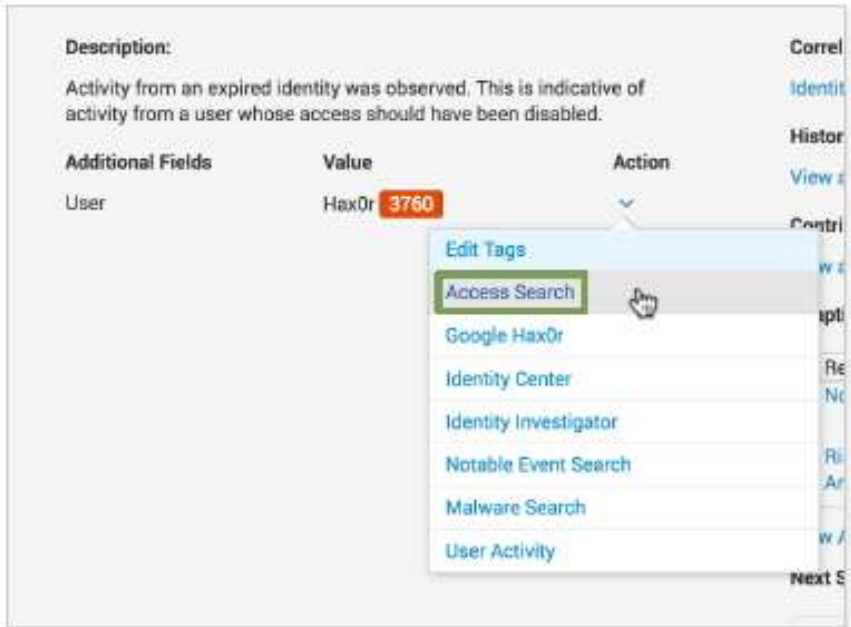
How to Use Domain Dashboards

- 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 domain dashboards from:
  - The **Security Domains** menu
  - Actions menu in Incident Review
  - Field action menus in search results

Accessing Forensics Dashboards

When expanding a notable event on the Incident Review dashboard, a field's Action menu contains links to relevant security domain dashboards

- Example: while investigating the user **Hax0r**, click **Access Search** to navigate directly to the Access Search dashboard



Access Domain: Investigation Scenarios

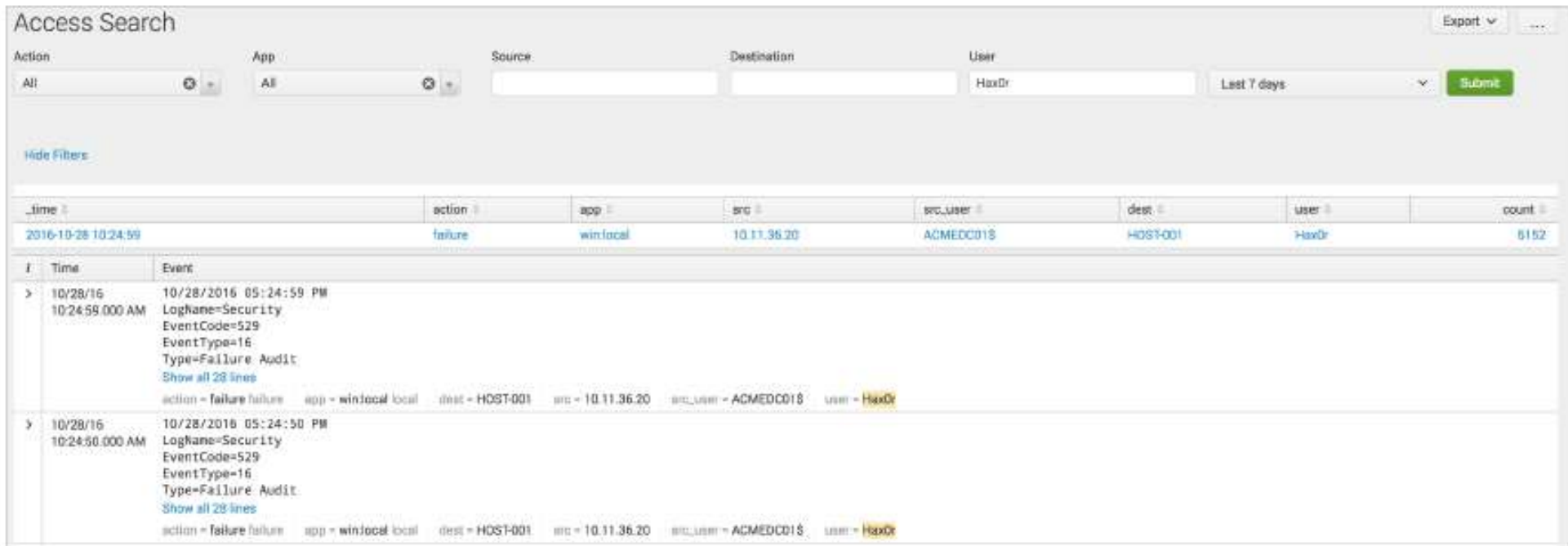
- The access domain is focused on user identity and authentication
- These dashboards provide tools to research:
  - Brute force attacks
  - Privileged account (i.e., root) misuse
  - Access by rare or new accounts
  - Access by expired or disabled accounts
  - Access via unusual applications (i.e., SSH, VNC, etc.)
- The **User Intelligence** dashboards on the **Security Intelligence** menu provide more tools for access domain investigation

Access Domain Correlation Searches

Account Deleted	Geographically Improbable Access Detected
Brute Force Access Behavior Detected	High or Critical Priority Individual Logging into Infected Machine
Brute Force Access Behavior Detected Over 1d	Inactive Account Usage
Cleartext Password At Rest	Insecure Or Cleartext Authentication
Completely Inactive Account	Short-lived Account Detected
Concurrent App Accesses	Asset - Asset Ownership Unspecified
Default Account Usage	Activity from Expired User Identity
Default Accounts At Rest	High Volume Email Activity with Non-corporate Domains
Excessive Failed Logins	Web Uploads to Non-corporate Domains

Access Search

After selecting **Access Search** for **Hax0r** from incident review, the Access Search dashboard is automatically populated with Hax0r's login attempts

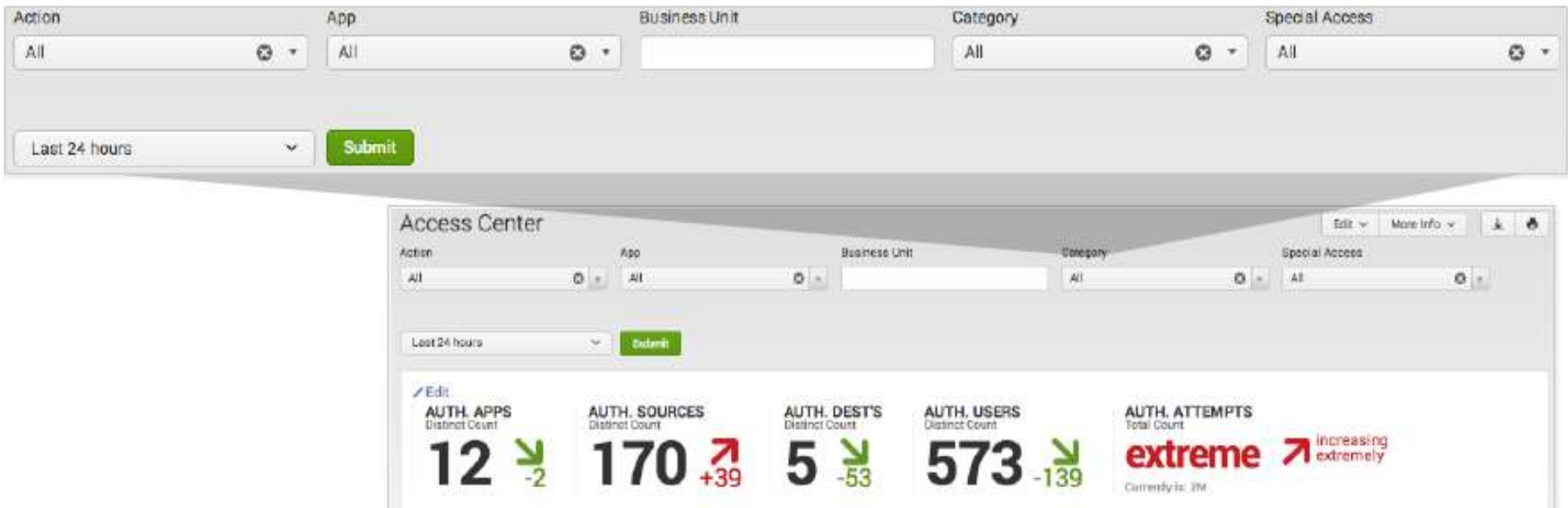


Access Center

- Examine access apps, by success vs. failure and by time
  - Large failure rates indicate brute force probing
- Examine access by source
  - High access rates from a single source can be malicious
- Examine access by unique users
  - User accounts with high rates of login activity may be compromised

Dashboard Filtering

- All of the dashboards support some form of filtering
- For instance, the Access Center has filter options for action, app, business unit, category, and special access



Other Access Domain Dashboards

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

Endpoint Domain Investigation Scenarios

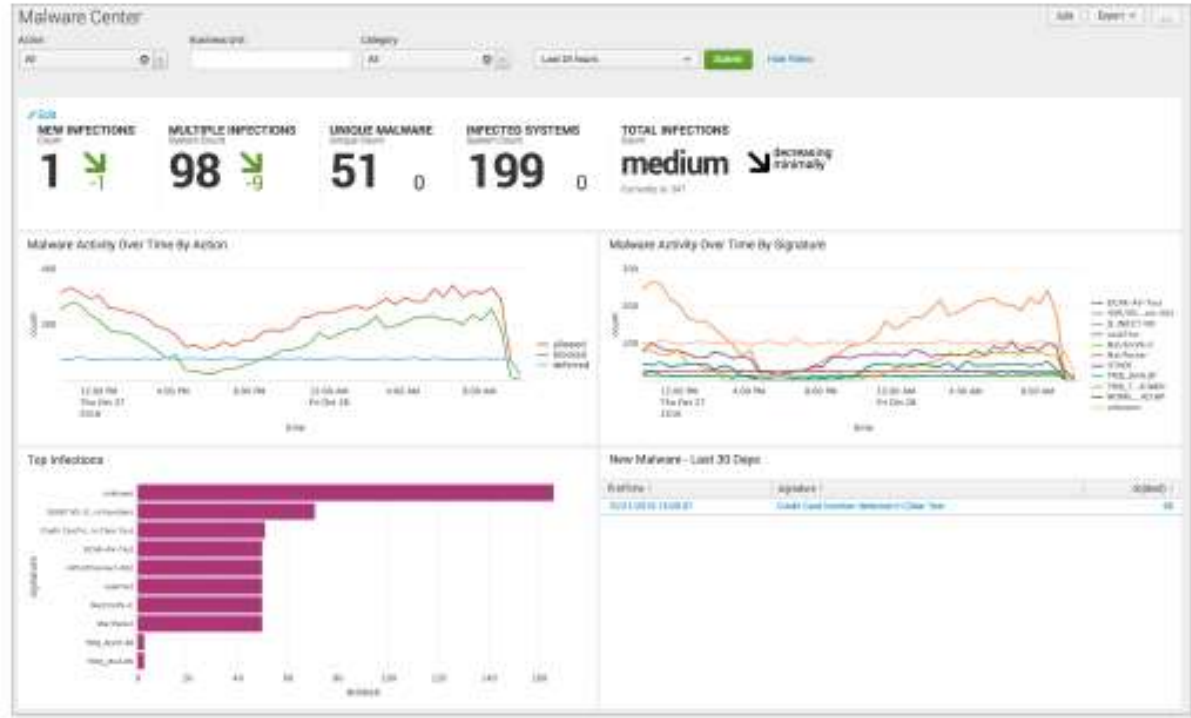
- The endpoint domain watches over your user systems:
  - Workstations, PCs, notebooks, handheld devices, and point-of-sale systems are examples
- Potential issues include:
  - Vulnerabilities: missing updates or patches
  - Malware: spyware, ransomware, or other malicious code
  - Unexpected running processes or services
  - Unexpected registry changes

Endpoint Domain Correlation Searches

Abnormally High Number of Endpoint Changes By User	Host With Excessive Number Of Processes
Anomalous New Listening Port	Host With Excessive Number Of Services
Anomalous New Processes	Host With Multiple Infections
Anomalous New Services	Multiple Primary Functions Detected
Anomalous User Account Creation	Old Malware Infection
High Number of Hosts Not Updating Malware Signatures	Outbreak Observed
High Number Of Infected Hosts	Prohibited Process Detection
High Or Critical Priority Host With Malware	Prohibited Service Detection
Host Sending Excessive Email	Recurring Malware Infection
Host With Excessive Number Of Listening Ports	Should Timesync Host Not Syncing

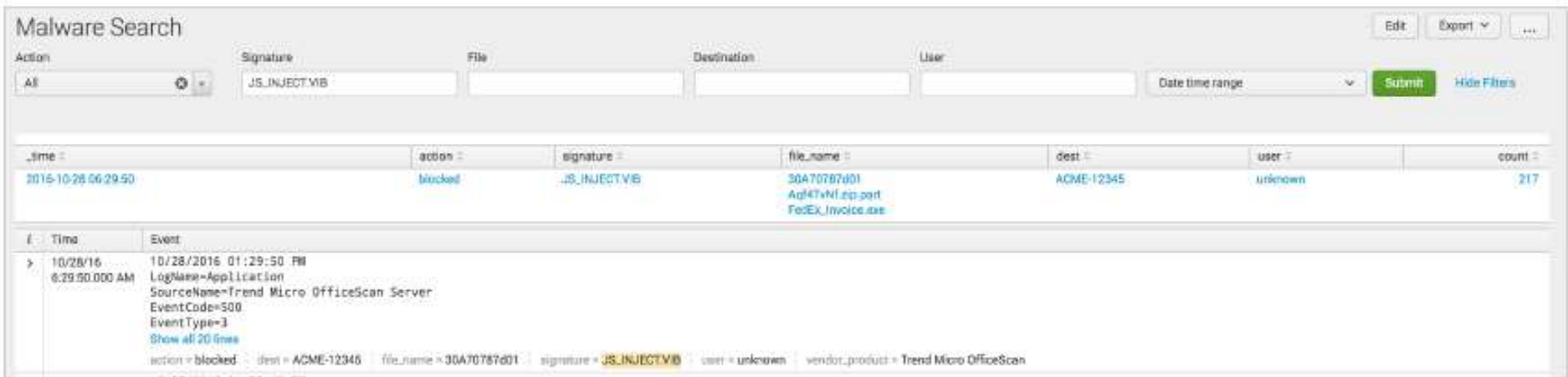
Malware Center

- Overview of malware in your environment
  - Allowed vs. blocked
  - Types of infections
  - Statistics on most common infection types
  - New malware identification
- This dashboard can help you prioritize investigations based on infection scope and type



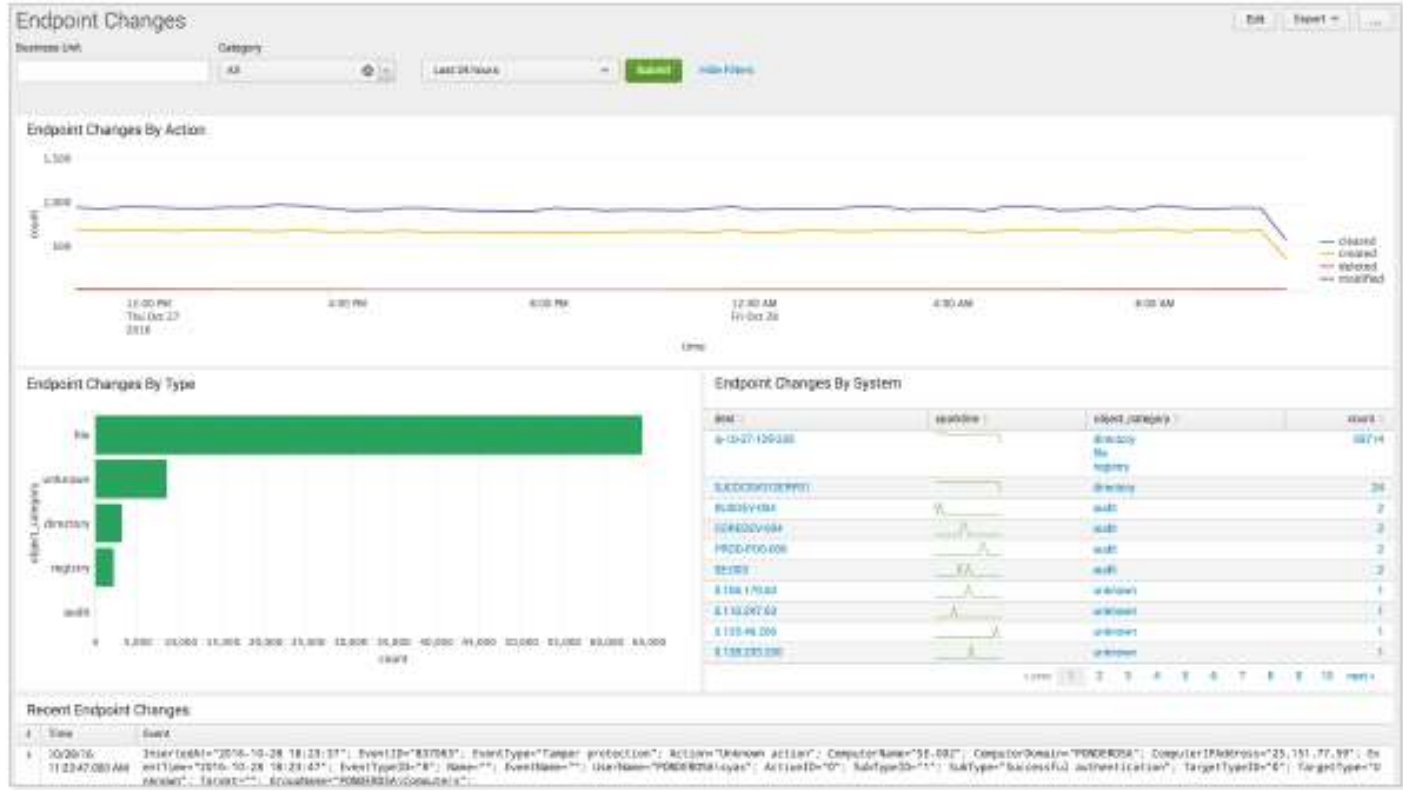
Malware Search

- Click a malware signature on the Malware Center dashboard to drill down to that malware type on the Malware Search dashboard
- This shows all infected systems, helping you identify the scope of the attack and also the origin
  - The first infection should be patient zero



Endpoint Changes

- Track changes on your systems
  - By type: file, registry, etc.
  - By system
  - List of change details

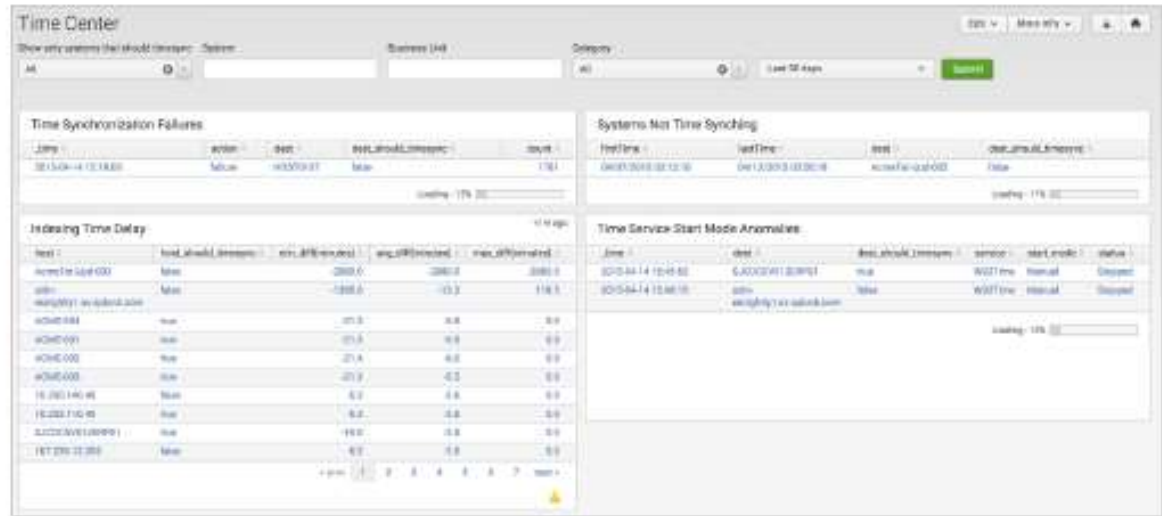


Malware Operations

- An overview of malware status, including:
  - Infected systems
  - Infection duration statistics
  - Malware client (i.e., antivirus) information
  - Statistics on repeat and aging infections

Time Center

- Reports the status of time synchronization in your environment
- Systems not properly synchronizing will not send correct time-stamped data to Splunk
  - This in turn can lead to search failure and false negatives in ES



Other Endpoint Domain Dashboards

System Center	Statistics about the operating systems and versions in use in your environment
Update Center	Statistics about the status of patches and other software updates
Update Search	Search interface for update events

Network Domain Investigation Scenarios

- Many network domain scenarios are preventative in nature:
  - Suspicious activity spotted by intrusion detection systems
  - Vulnerabilities
  - Unusual ports being opened
  - Suspicious DNS activity
  - Port scanning
- Other network analysis tools on the **Security Intelligence** menu:
  - **Protocol Intelligence**
  - **Web Intelligence**

Network Domain Correlation Searches

Excessive DNS Failures	Substantial Increase in Port Activity (By Destination)
Excessive DNS Queries	Unapproved Port Activity Detected
Excessive HTTP Failure Responses	Unroutable Host Activity
High Volume of Traffic from High or Critical Host	Unusual Volume of Network Activity
Network Device Rebooted	Vulnerability Scanner Detection (by event)
Policy Or Configuration Change	Vulnerability Scanner Detection (by targets)
Substantial Increase in an Event	Abnormally High Number of HTTP Method Events By Src

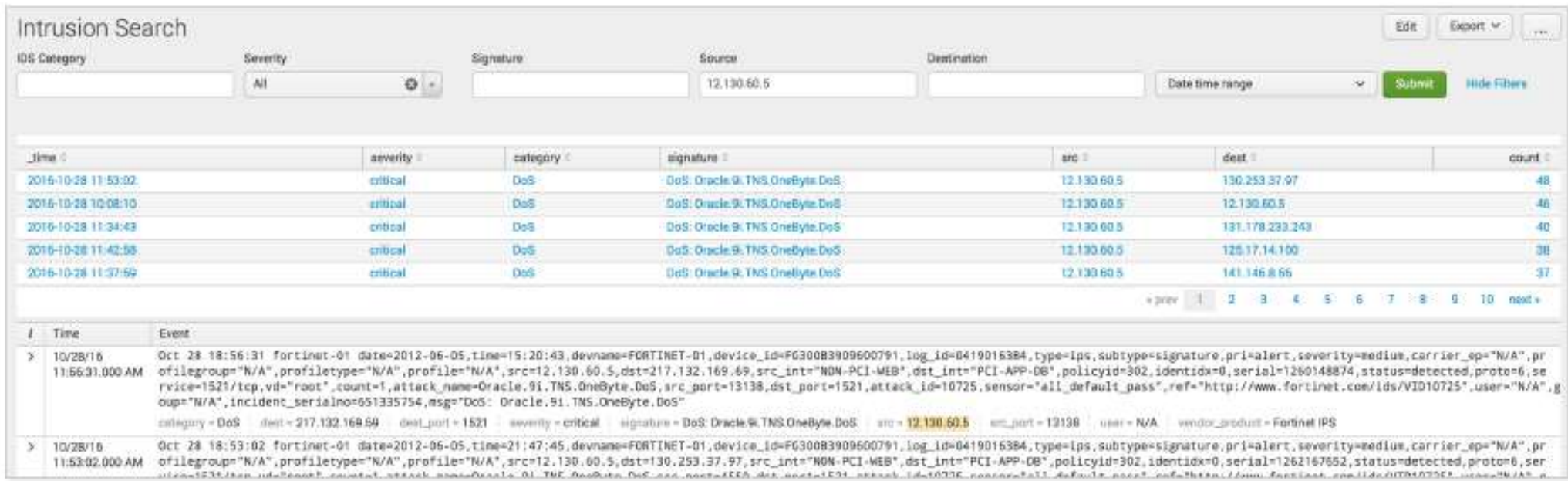
Intrusion Center

- This dashboard displays events logged from intrusion detection systems (IDS)
  - Sourcefire, Cisco, McAfee, etc.
- Use filters to focus on types of attacks, severity, or business units

- Click in any panel to drill down to the Intrusion Search dashboard

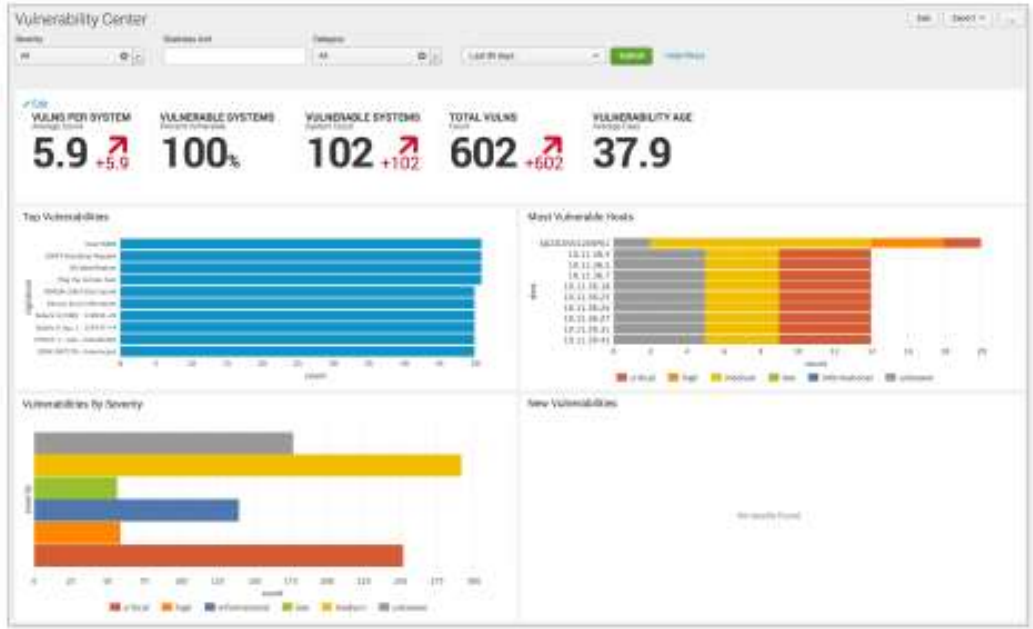
Intrusion Search

As an example, clicking on a system in the Scanning Attacks panel displays the specific type of attack (in this case, a denial of service on an Oracle system)



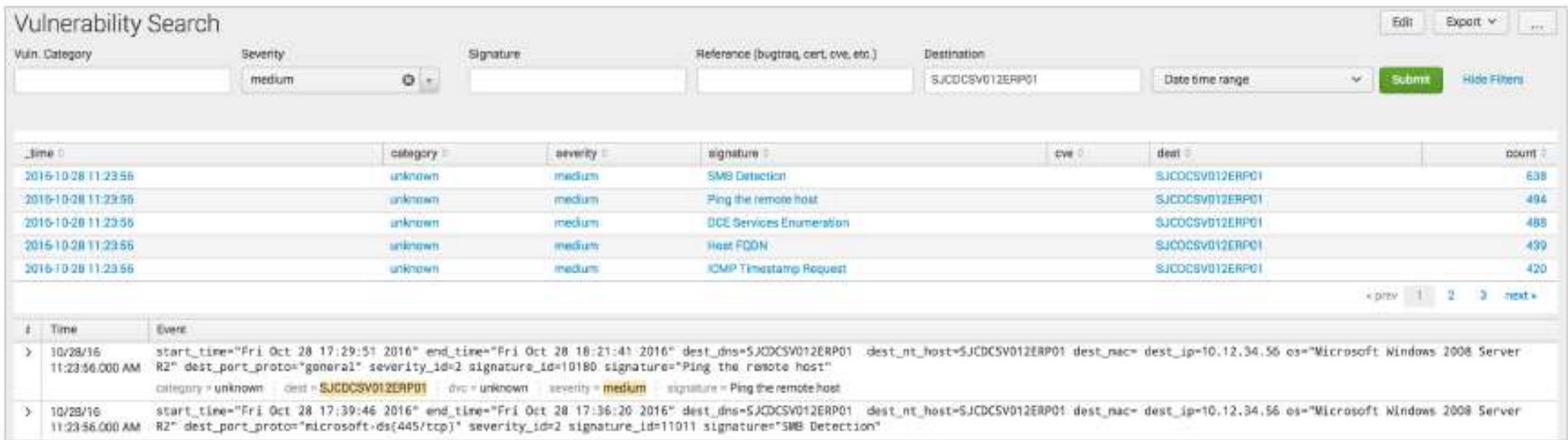
Vulnerability Center

- Displays statistics on system security settings from vulnerability scanners
  - Such as Tenable, Nessus, etc.
- Click in any panel to drill down to the Vulnerability Search dashboard



Vulnerability Search

For example, clicking a host bar in the Most Vulnerable Hosts panel displays events containing that host name in the Vulnerability Search dashboard



Web Center

Provides insights into HTTP activity in your environment

- This information comes from your web server, proxy and firewall logs
- Examine web activity by type,status, source and destination

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 and protocol type

Module 5:
Risk Analysis

Objectives

- Understand risk analysis concepts
- Use the Risk Analysis dashboard to monitor activity related to risk
- Manage risk scores for objects or users

Security Intelligence: Risk Analysis

- Risk Analysis is a dashboard on the **Security Intelligence** menu
- Along with the other dashboards on this menu, Risk Analysis is a tool that enables you to examine events in your ES indexes in detail

- These tools give security practitioners an ability to proactively analyze their environment to detect potential problems before they become issues

Risk Analysis

- Correlation searches can add a numeric risk value to objects
  - Systems or users
- Risk can be increased by any event that occurs to an object
- The amount of risk assigned can be configured per-object and per-event
- This is different than priority, severity, or urgency
  - Allows you to see cumulative risk caused by multiple events over time
  - Allows you to fine-tune the way you interpret threats or vulnerabilities to your enterprise
- Admins configure risk values to correlation searches and objects

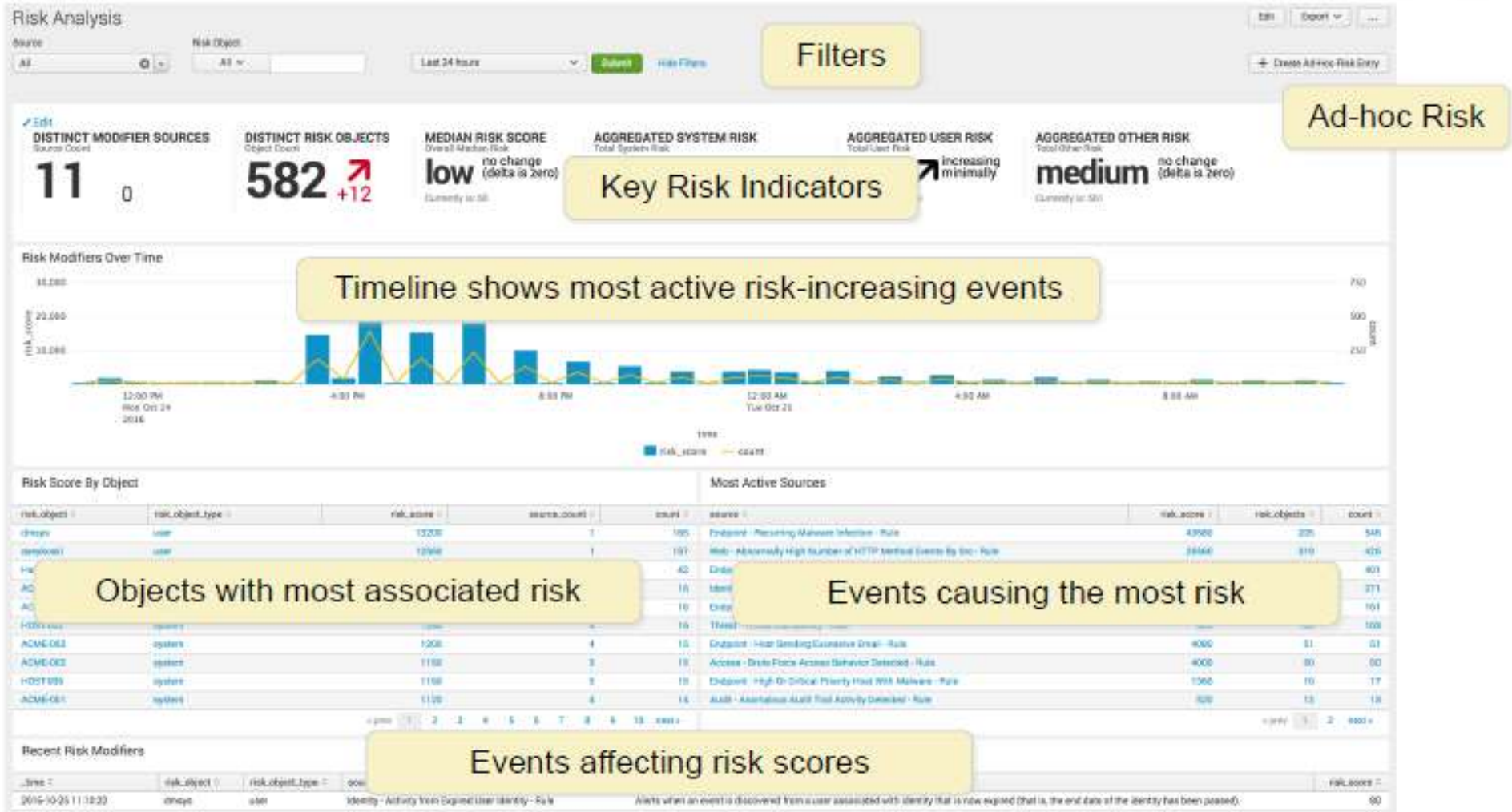
Risk Analysis Example

- A high priority firewall server is attacked periodically over time
  - A few such attacks are expected, but as they accumulate over weeks, the risk score for that server will increase
- If other low priority events are also accumulating for that server, like minor vulnerabilities and low-grade anomalous network activity, they will also contribute to the risk score for the server
- If the risk for that server increases more than other servers due to this continuing activity, you can be alerted and investigate
- This activity might otherwise be difficult to detect without this cumulative approach

Risk Activity Examples

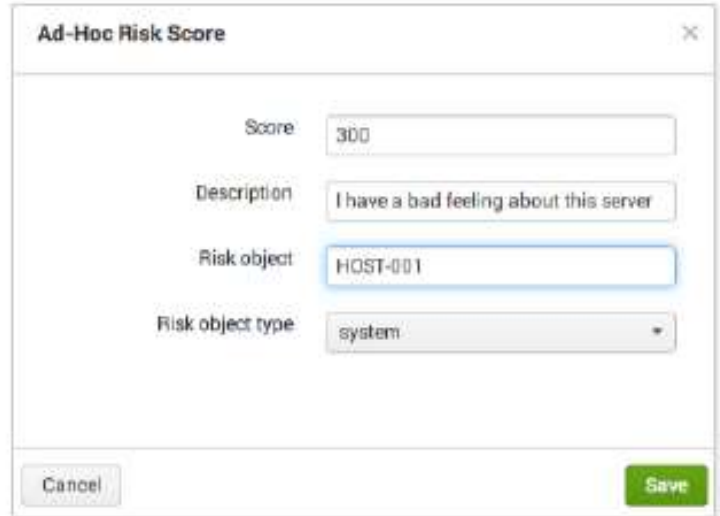
- User risk
  - An employee who begins moving files to a local workstation and emailing attachments to external sites
  - A contractor who begins logging on from many different geographically remote systems throughout the organization
- Asset risk
  - A restricted system (like a point-of-sale station)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

Risk Analysis Dashboard



Ad-hoc Risk Entry

- Use this tool to add or subtract risk for any object
- Add a score (positive or negative), a description, and the risk object name (an asset or identity)
- Select the object type and click Save
- The risk value you entered is added (or subtracted) to/from the object's overall risk score
- Useful if you want to promote or demote an object's risk based on your own investigation



Module 6:
Web Intelligence

Objectives

- Use the web intelligence dashboards to analyze your network environment
- Filter and highlight events

Security Intelligence: Web Intelligence

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

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

Using the Web Intelligence Dashboards

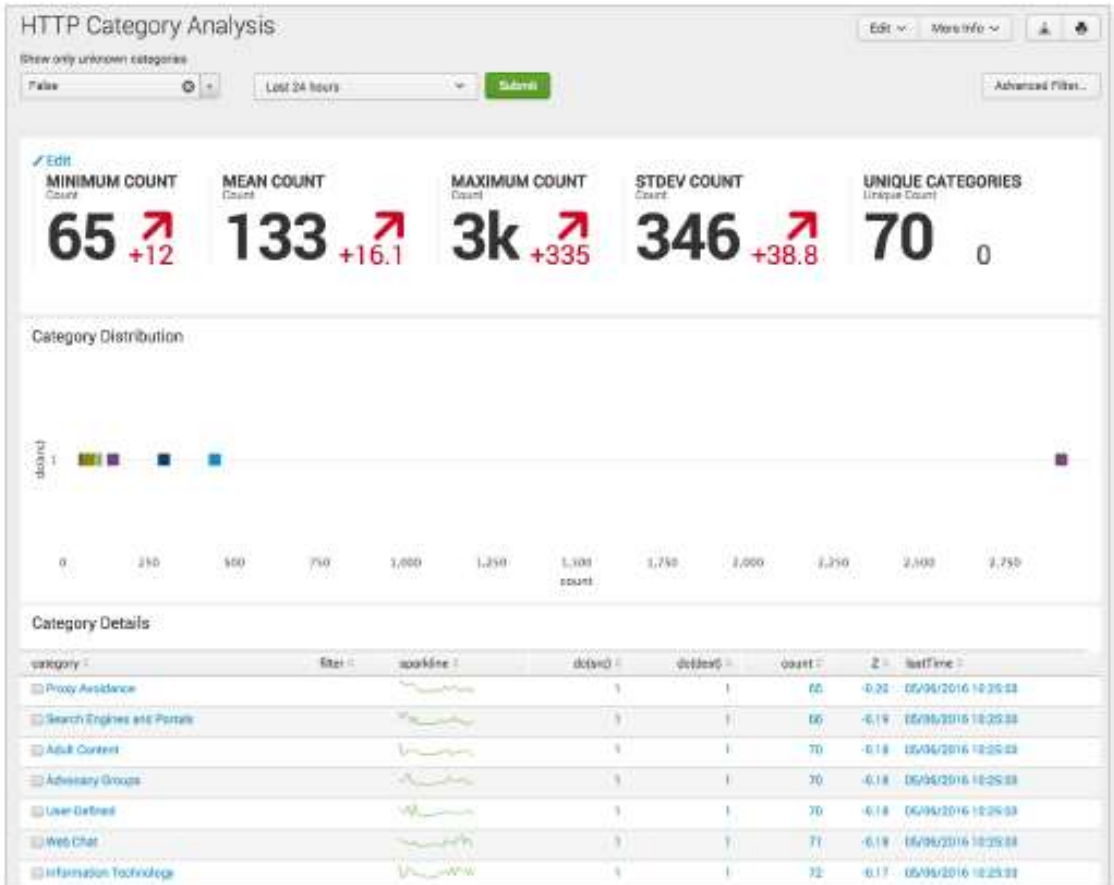
- **HTTP Category Analysis**: look for URLs associated with unwanted behavior
- **HTTP User Agent Analysis** : long or malformed user agent strings can be indicators of malicious activity
- **New Domain Analysis** : high count of new domains can indicate botnet or trojan attacks
- **URL Length Analysis** : look for embedded SQL, cross-site scripting, etc.

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

Example: HTTP Category Analysis

- Overview of website use in your organization by category
- Categories are published and defined by Websense

  www.websense.com/content/support/library/web/v76/siem/siem.pdf

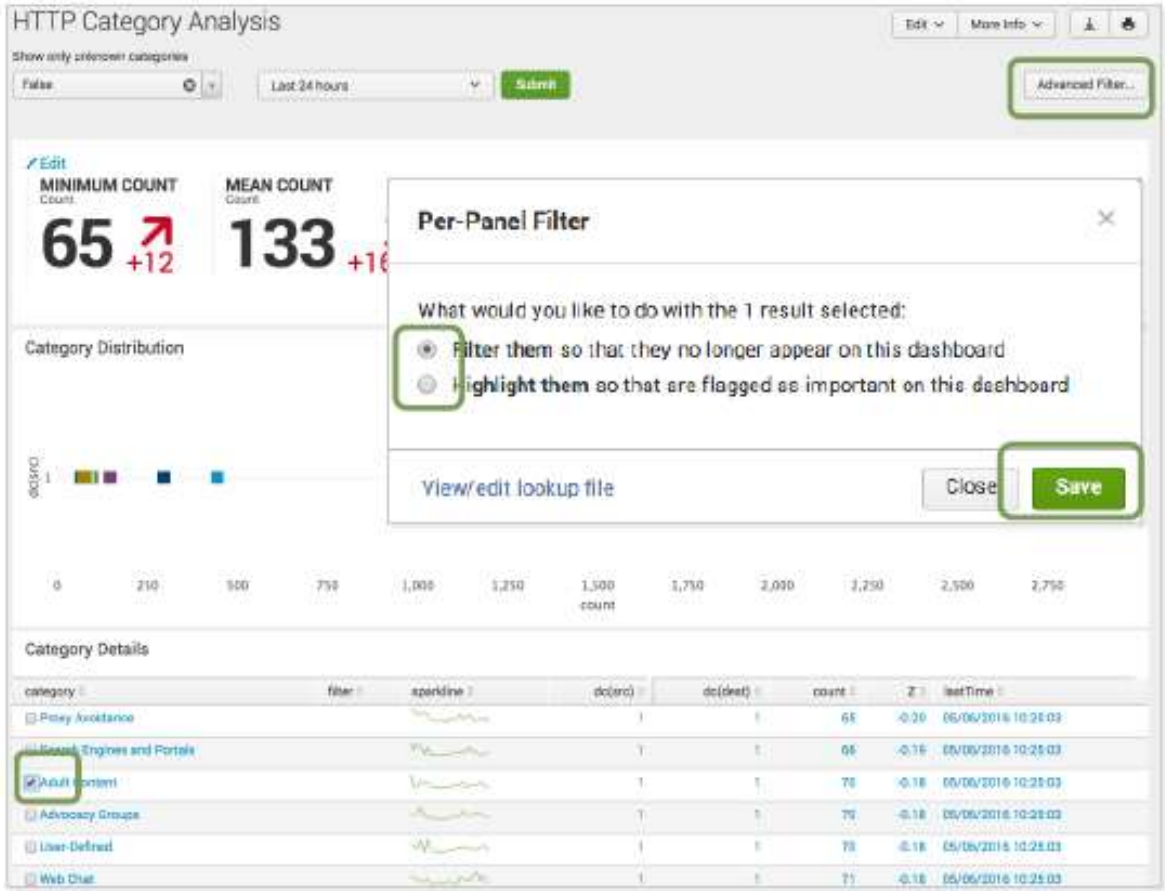


Per Panel Filter

- Analysis dashboards enable analysts to highlight or filter items out of dashboard views that are deemed unimportant or a non-issue
  - After it is determined that an event is not a threat, it can be added to your whitelist to remove from the dashboard view
  - If an event is determined to be a threat, use the Advanced Filter editor to add the item to your blacklist of known threats
- This feature is unavailable by default for ES Analysts
  - Can be enabled by an ES Admin
- For instance, for HTTP Category Analysis you may want to filter out expected categories and highlight unwanted categories

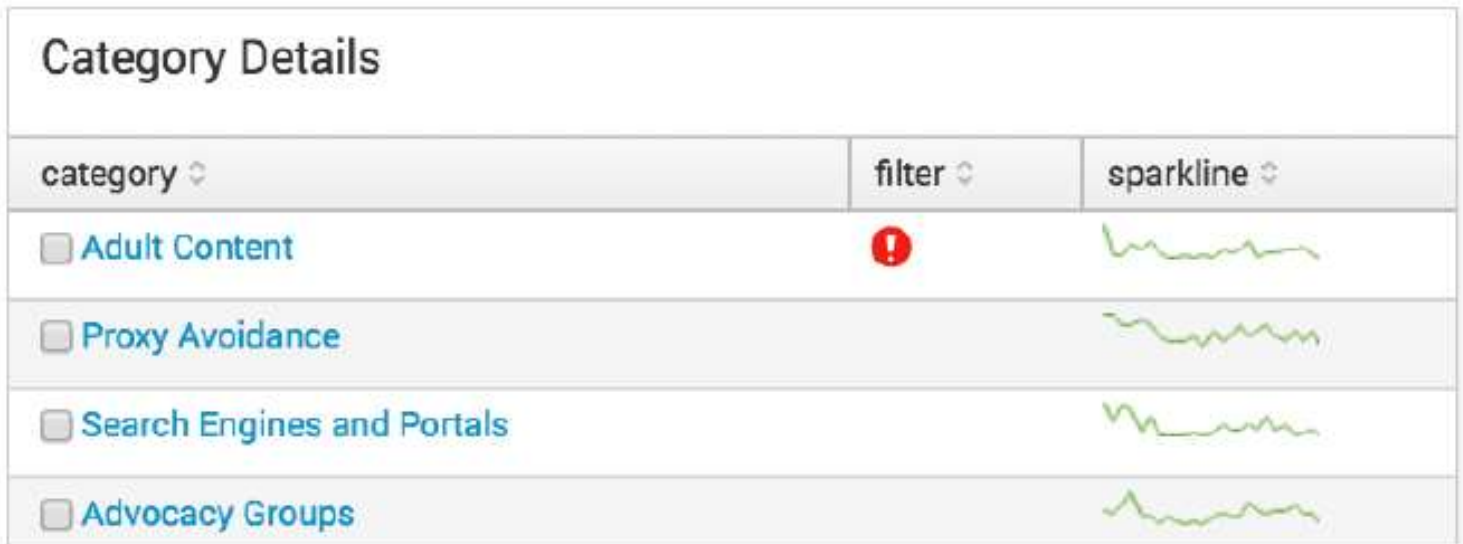
Creating Per Panel Filters

- Select one or more events in the dashboard
- Select **Advanced Filter**
- Choose between filtering or highlighting
- Click Save



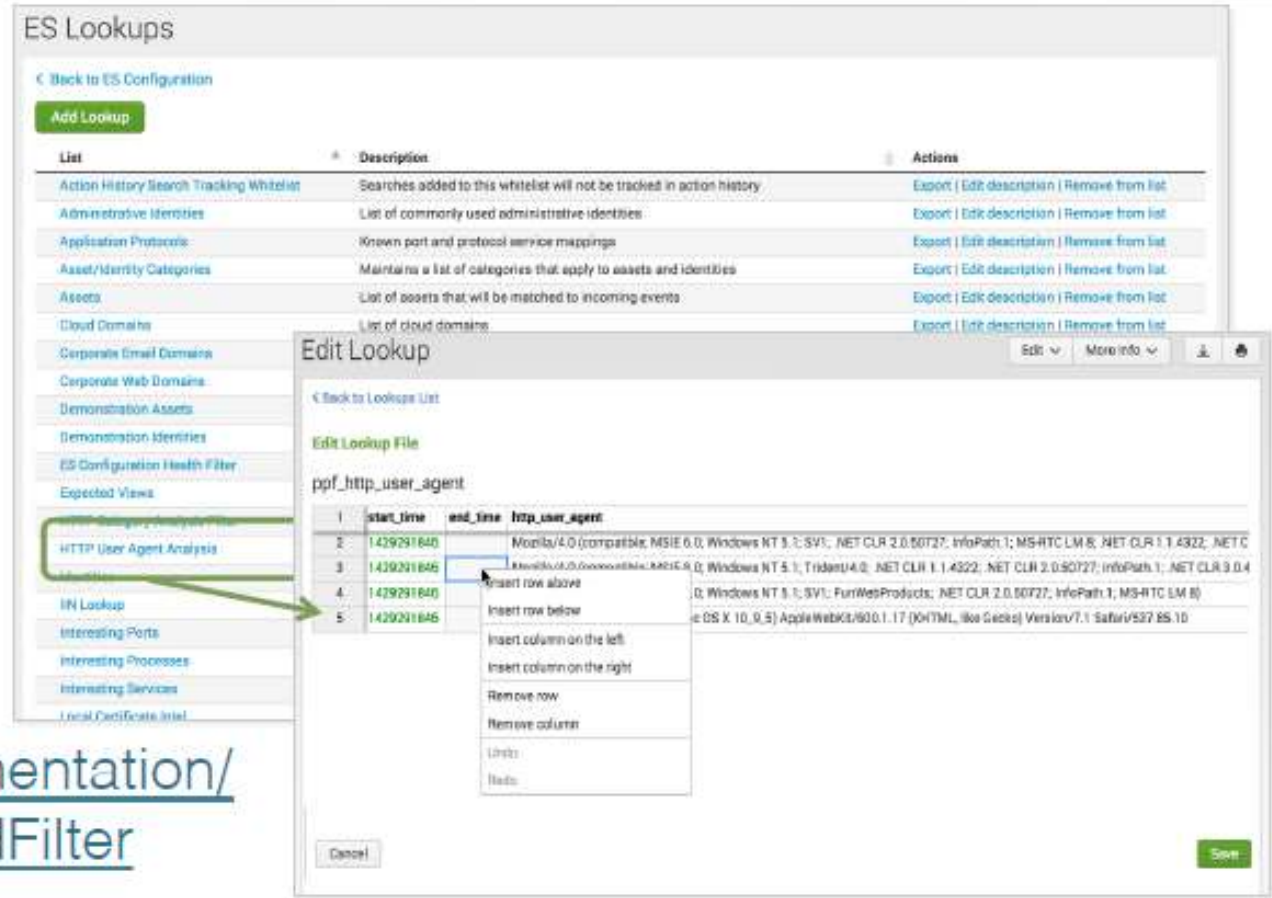
Filtered vs. Highlighted Events

- Filtered events are no longer displayed
- Highlighted events are marked with a red icon in the filter column and are displayed at the top of the list by default



Managing Per Panel Filtering Lookups

- Select **Configure > Data Enrichment > Lists and Lookups**
- Click an analysis dashboard name to edit
- Click Save



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

Unhighlighting an Event

- If an event is already highlighted, you can select it and select **Advanced Filter**
- You can then remove the highlight or change to filtering

Module 7:
User Intelligence

Objectives

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

Insider Threats

- Some threats originate from inside your organization
  - Social engineering can compromise employee accounts
  - Disloyal employees or contractors may engage in unwanted activities
- ES contains many tools to investigate and analyze user activity:
  - What user accounts are active and what are they doing?
  - What equipment (servers, etc) are they accessing?
  - Where are they logging on?
  - How much risk has been accumulated by each user or device?

Security Intelligence: User Intelligence

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

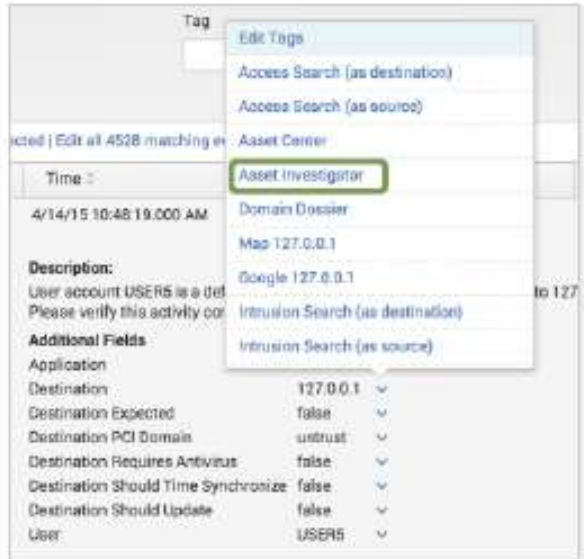
Asset Investigator	Examine a specific asset, such as a server or workstation, and compare events over time in parallel lanes showing different types of activity
Identity Investigator	Examine a specific identity and compare events over time in parallel lanes showing different types of activity
Access 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

- Both investigator dashboards allow you to enter an asset or identity name and a search range
- Both return a time-sequenced set of **swim lanes** showing activity for that asset or identity over time, comparing activity between:
  - Threats
  - IDS attacks
  - Authentication activity
  - Malware attacks
  - Notable events
  - Changes (such as firmware or software upgrades, etc.)

Accessing the Investigators

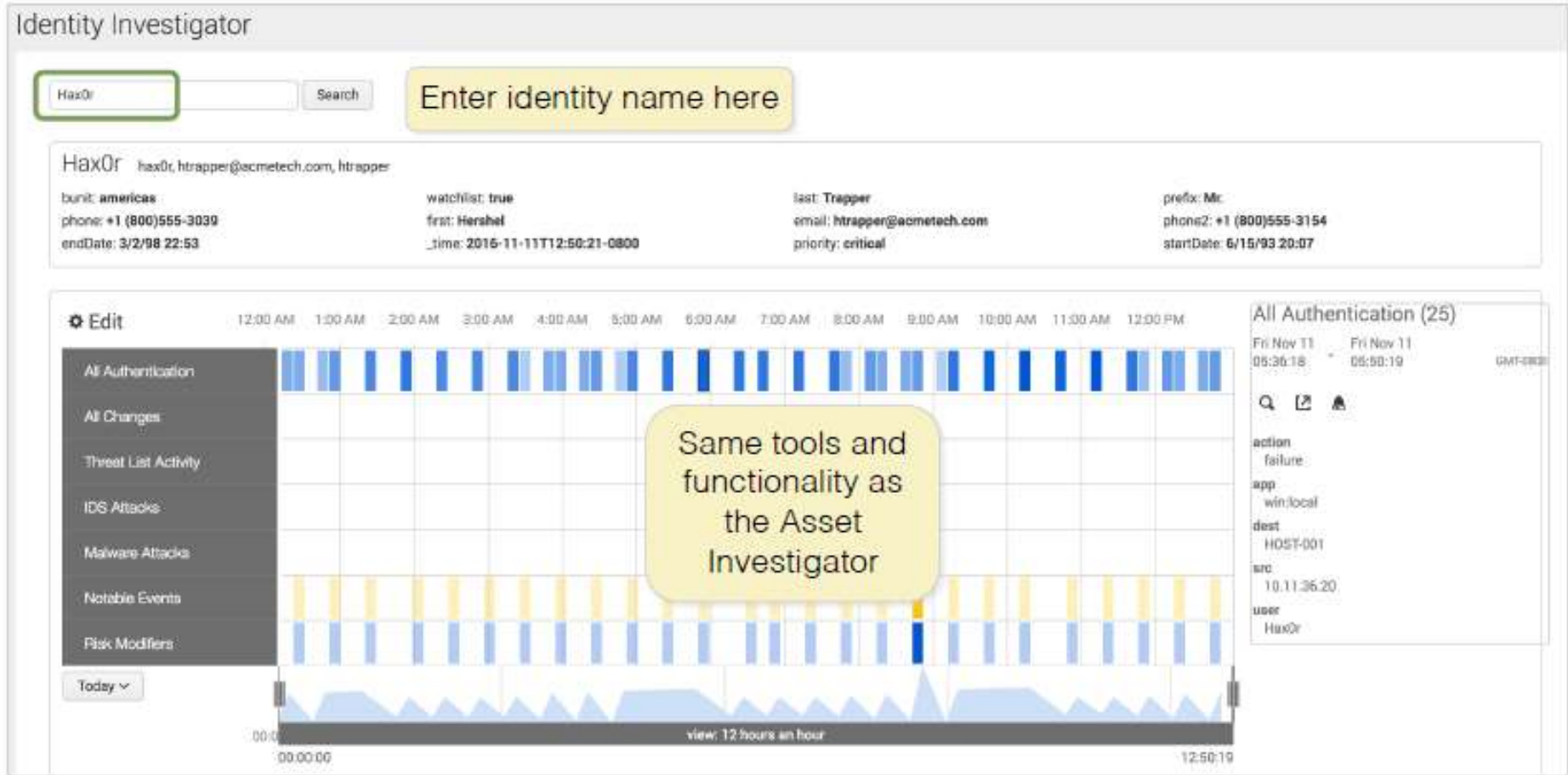
- Asset Investigator:
  - Select **Security Intelligence > User Intelligence >** and enter an asset name or IP address, or
  - In a search result or details in Incident Review, use an asset field's action menu to select **Asset Investigator**



- Asset fields: destination, src, ip, host, etc. (fields that identify a server)
- Identity Investigator: Per above, either use the main menu **Security Intelligence > User Intelligence >** or use an identity field's (user, src_user, etc.) action menu

User Intelligence: Asset Investigator

User Intelligence: Identity Investigator



How to Interpret Investigators

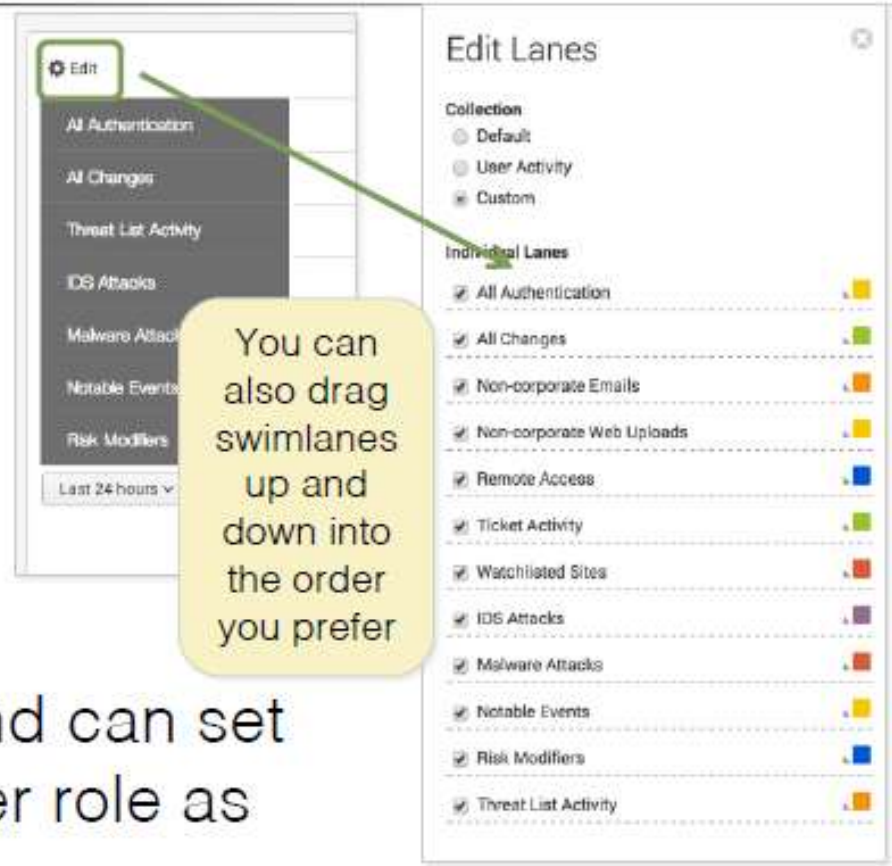
- The swim lanes visually show activity in various areas in time sequence, making it easy to see incidents that are simultaneous or sequential
- Activities that coincide in time may have a cause-effect relationship
- For example:
  - A server shows a burst of authentications at 1:15 am
  - At 1:17 am, a malware attack notable event is triggered for that server
  - The asset investigator makes it apparent that there is a possible cause-effect relationship spanning across two (or more) swim lanes

Pan and Zoom

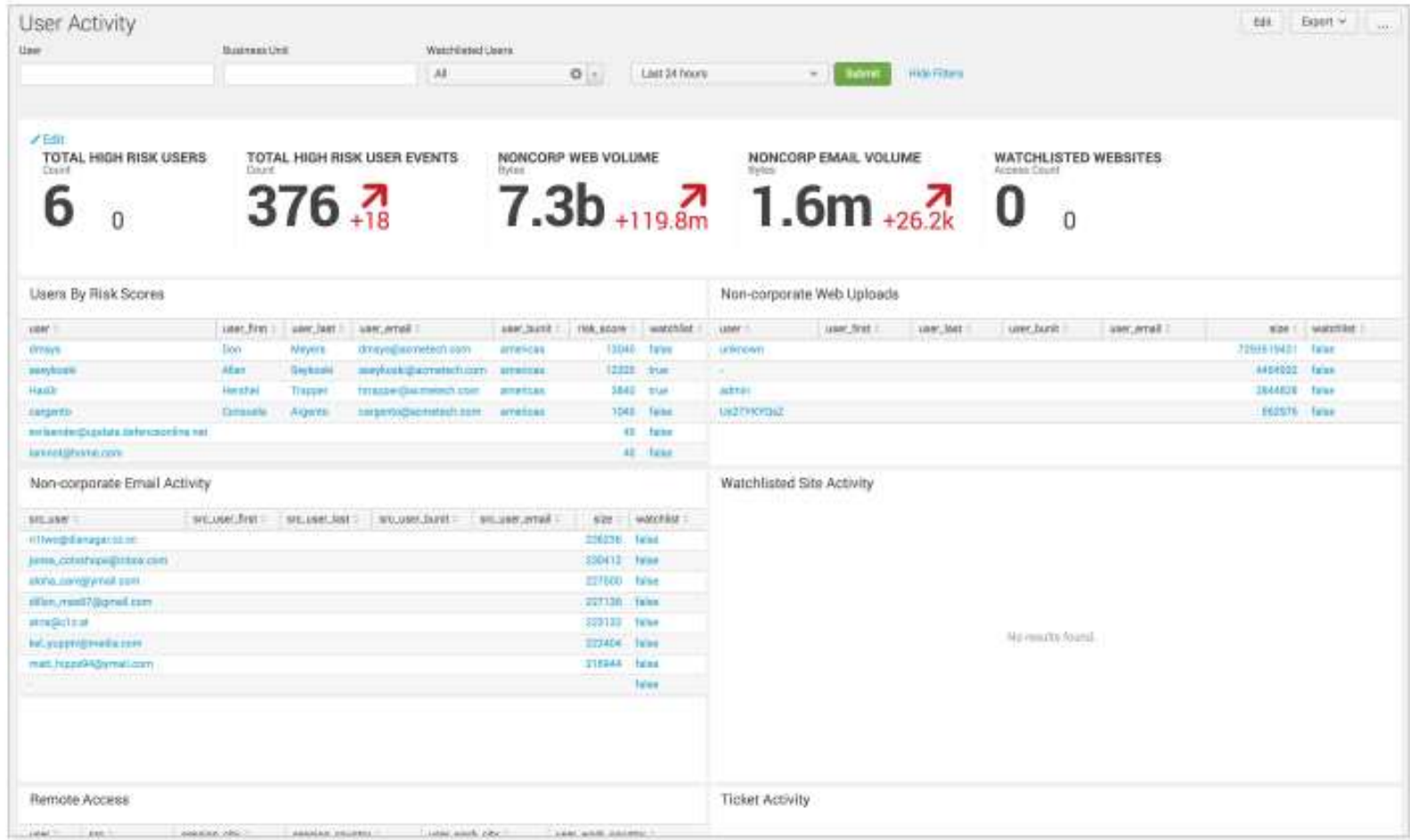
Dragging the pan/zoom controls changes the time frame for the search and re-executes the search, showing only the activity in the selected range

Configuring Swimlanes

- Click **Edit** and select a collection of swimlanes
- Use the **Custom** collection to select specific swimlanes
- Customize swimlane colors
- All changes are saved as preferences for the current user
- Admins can add new swimlanes and can set overall defaults and permissions per role as needed



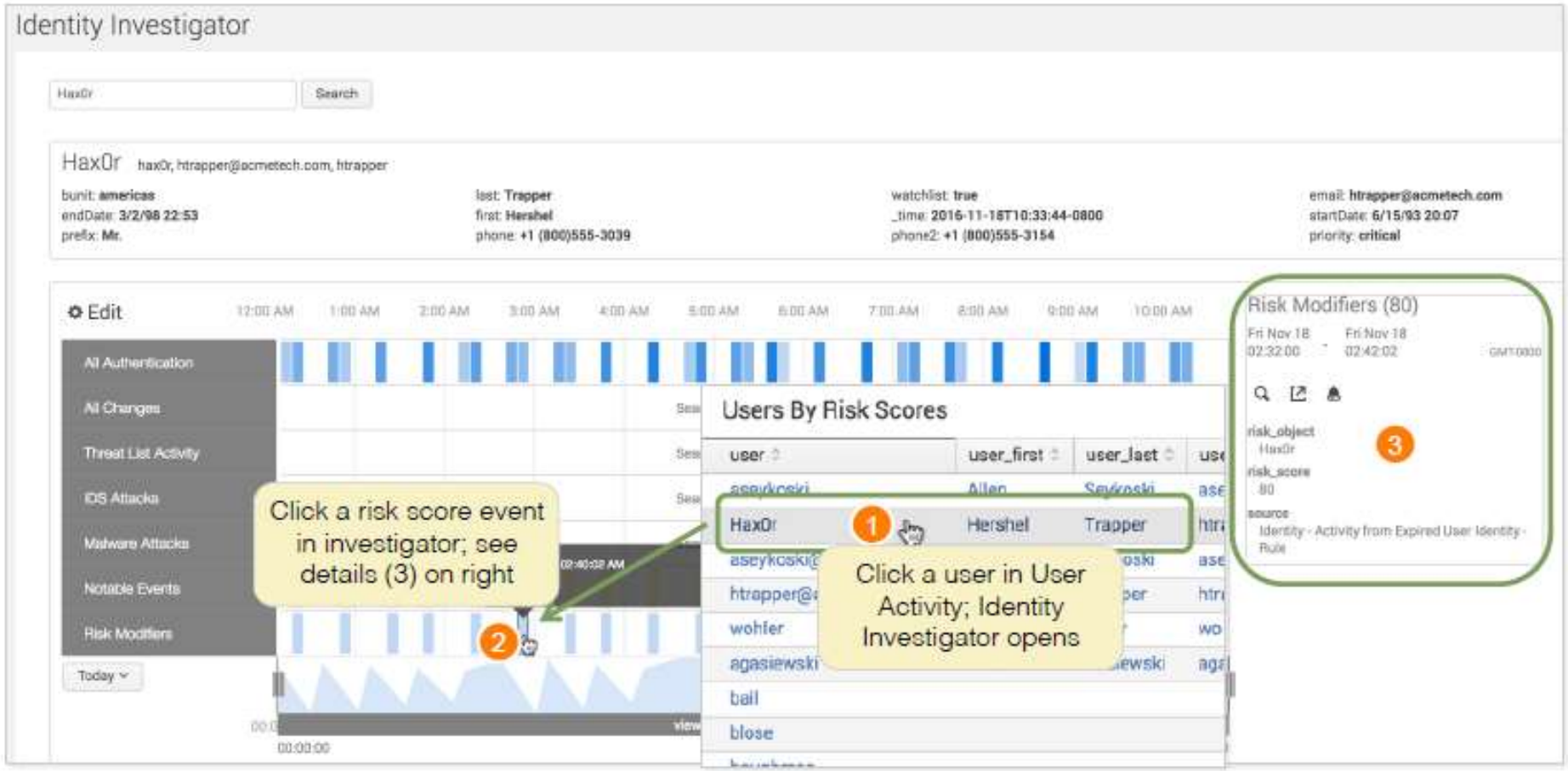
User Intelligence: User Activity



User Activity Panels

Users by risk scores	Risk assigned by various correlation searches related to user activity
Non-corporate web uploads and email activity	Sorted by size
Watchlisted sites	Users accessing external sites that have been added to a watchlist
Remote access	Users connecting to their accounts from geographically remote locations
Ticket activity	Users identified in an open incident in an external tracking system

Drilldown for More Details



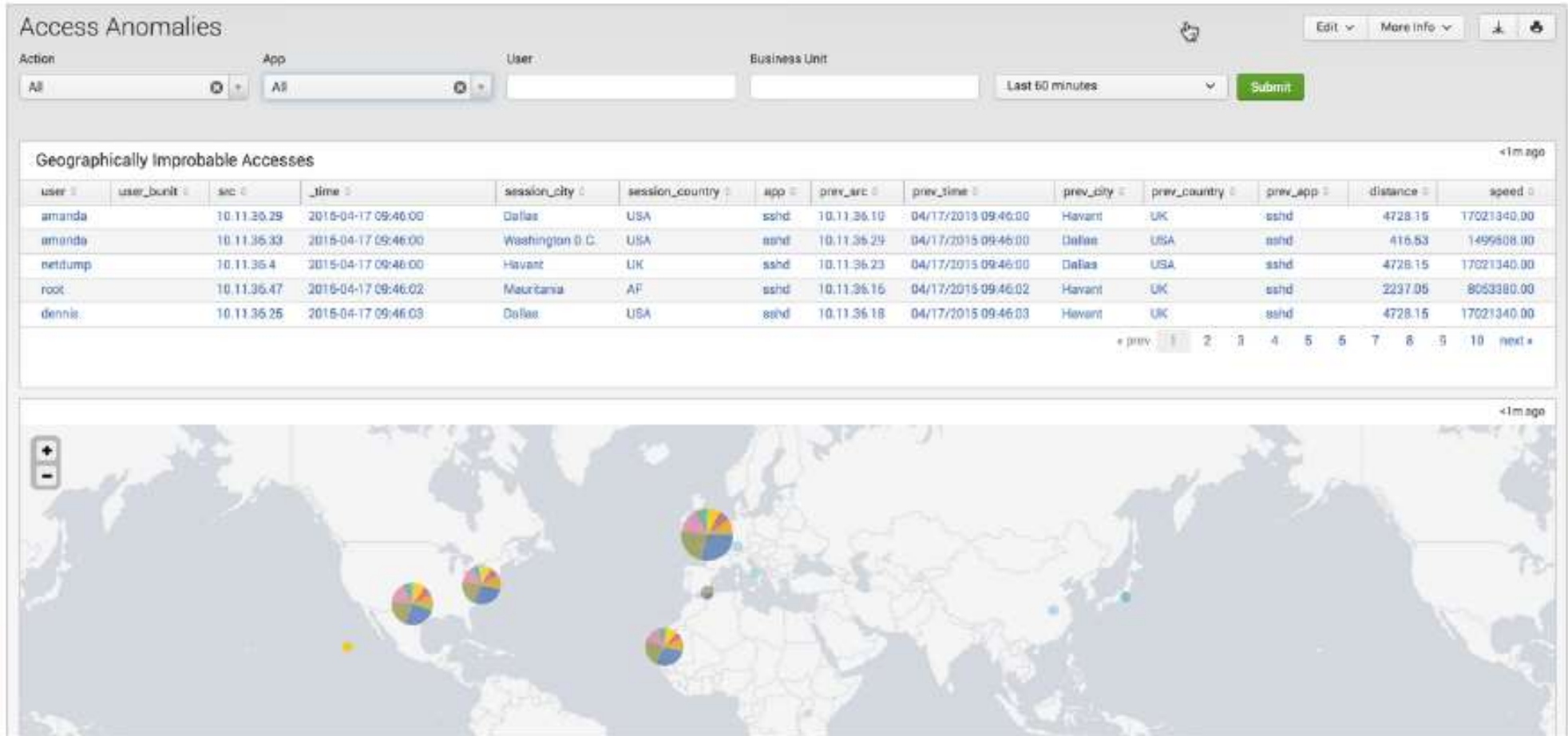
Watchlisted Users and Sites

- Users and sites can be added to watchlists by your ES admins
- Users can be added to the watchlist for various reasons:
  - Short term or new contractors
  - Under investigation
- Sites can be watchlisted to track access
- The correlation search **Watchlisted Event Observed** creates a notable event if a watchlisted user or site is involved in an event
- Optional swimlanes on the identity and asset investigators also display watchlisted activity

Access User Activity from Action Menus

- After running a search, you can open the **action** menu for the **user** field and select **User Activity**
  - Opens the User Activity dashboard displaying only that user's account activity

Access Anomalies



Using the Access Anomaly Dashboard

- Searches for user access during the requested time period, defaults to 60 minutes
- Displays user access events with locations more than 500 miles from their previous access location
- The distance (miles) and speed (miles per hour) between locations yields an indicator of improbability for a user to actually log in from both locations
- Many access events spanning a short time from many geographically remote locations is suspicious

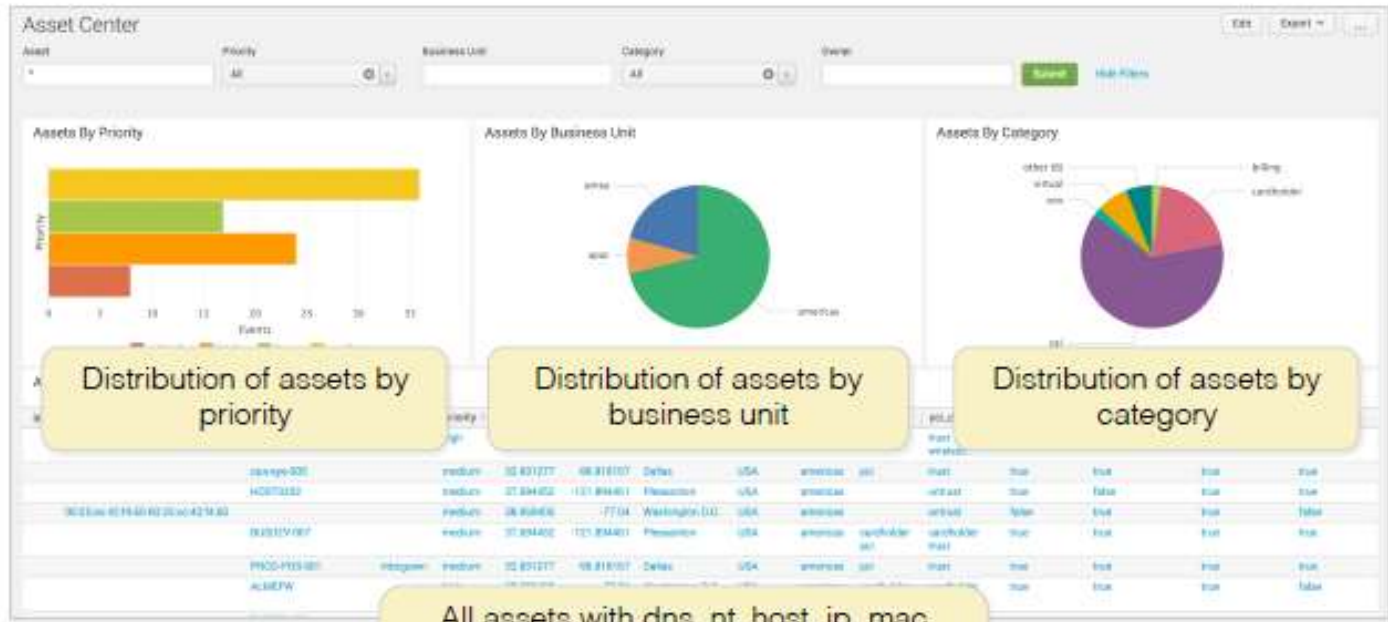
Splunk UBA Integration

- Splunk User Behavior Analysis (UBA) is a separate solution that extends your ability to detect insider threats
  - UBA can be integrated with ES
  - After integration, UBA can forward insider threat intelligence to ES, and ES can forward notable events to UBA
- ES can use the insider threat intelligence to generate notable events for insider threat events
  - These can be viewed on the Incident Review dashboard
  - UBA threats also appear on the asset and identity investigators

http://docs.splunk.com/Documentation/UBA/latest/User/ES

Asset Center

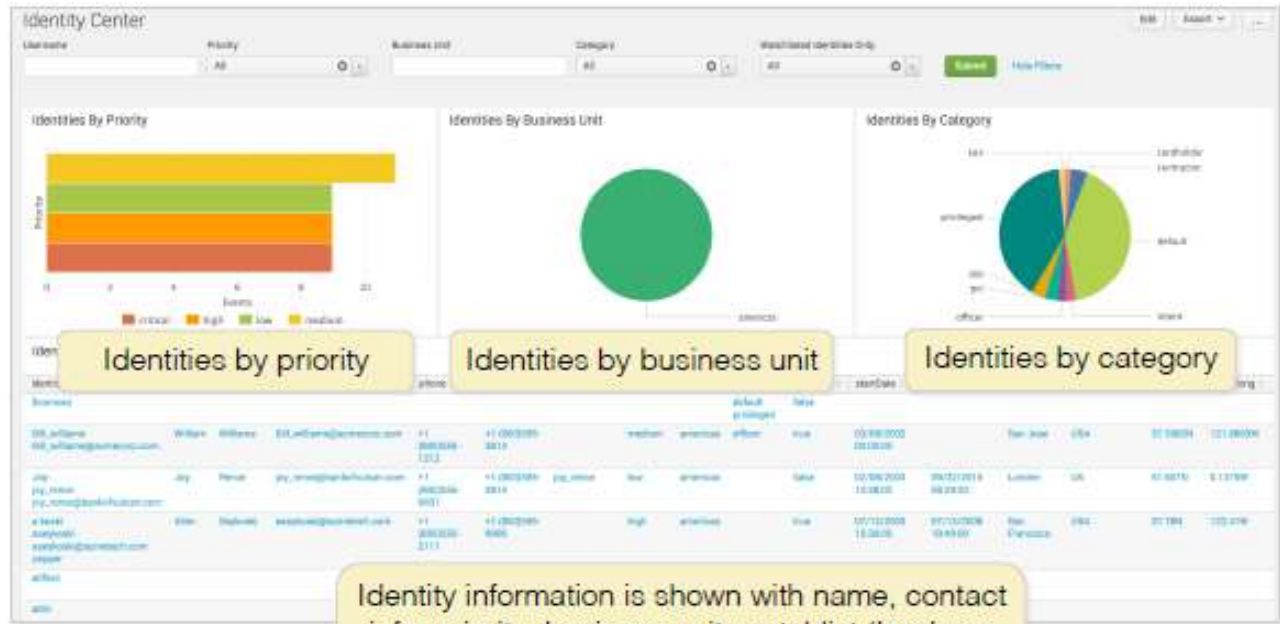
- Security Domains > Identity > Asset Center
- Overview of assets
- Visualizations by priority, business unit, and category
- Table at bottom shows all asset lookup columns



Identity Center

Security Domains Identity > Identity Center >

- Overview of identities
- Bottom table shows all identity lookup columns



Related Correlation Searches

- Correlation searches related to insider (user) threat:
  - Abnormally High Number of Endpoint Changes By User
  - Activity from Expired User Identity
  - High Volume Email Activity to Non-corporate Domains by User
  - New User Account Created On Multiple Hosts
  - Web Uploads to Non-corporate Sites by Users
  - Watchlisted Event Observed

Module 8:
Threat Intelligence

Objectives

- 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

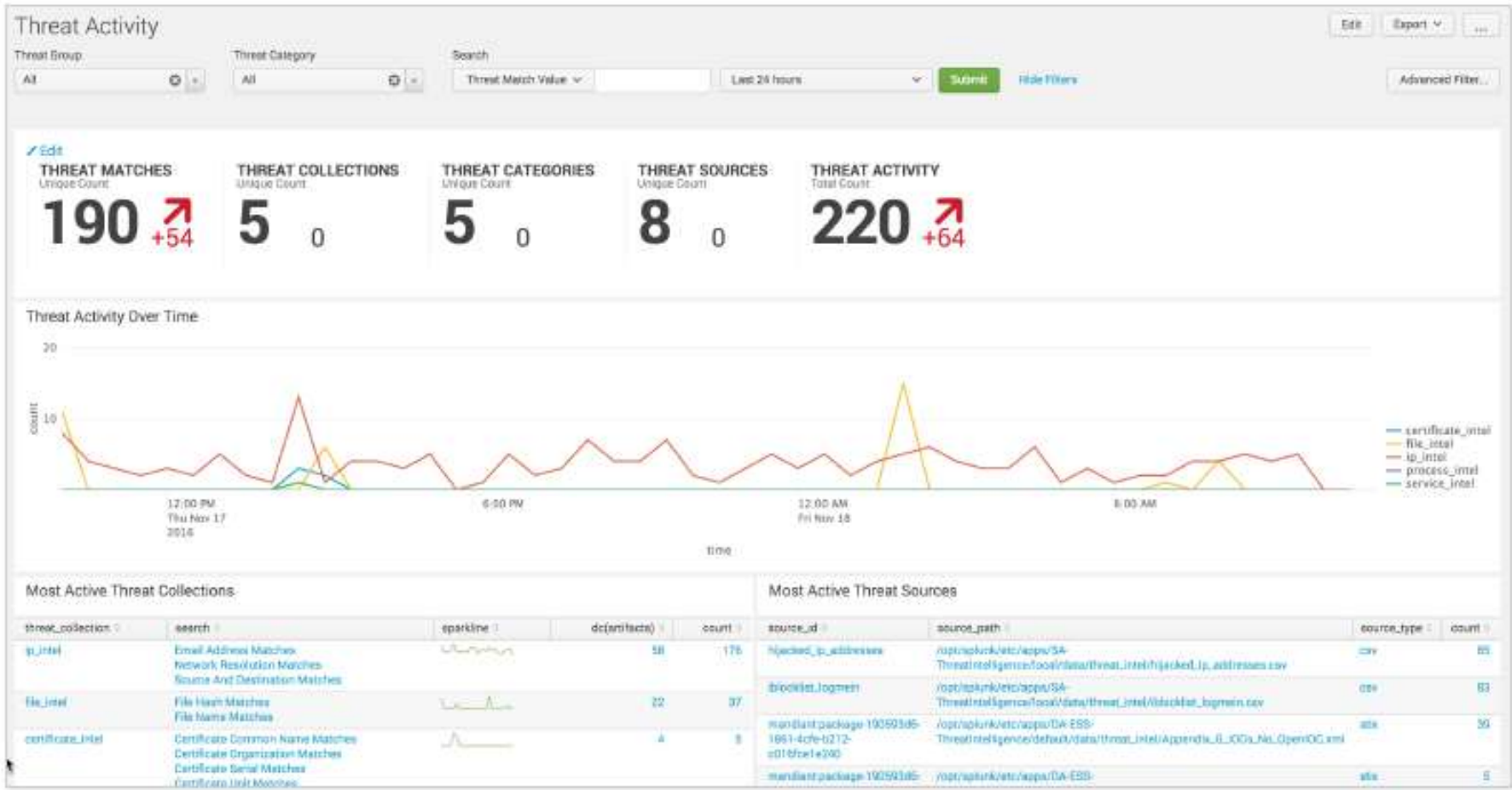
Threat intelligence provides tools to help security practitioners find and prevent potential external threats in your environment

Threat Activity	Examine activity in your organization from a threat perspective: what threats have been identified, what systems or users are affected, etc.
Threat Artifacts	Examine the details of threat intel that has been downloaded from online threat libraries

The Threat Intelligence Framework

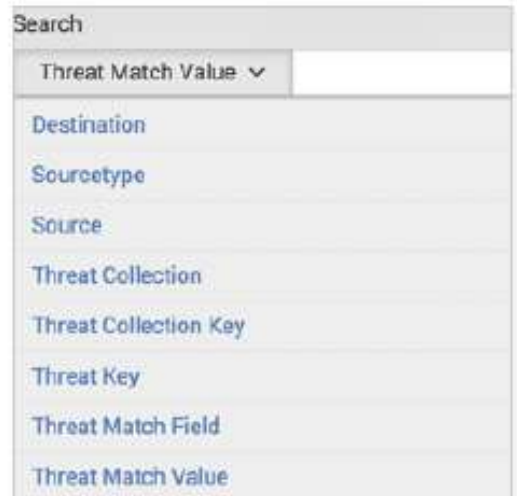
- The **Threat Activity Detected** correlation search creates a notable event if an indicator of compromise (IOC) is detected from a threat intelligence collection
- The threat intel collections are populated automatically by downloads from external threat libraries
- Threats are categorized by:
  - Group: the source or entity originating the threat
  - Category: the type of threat, like backdoor, APT, financial, etc.
  - Collection: organized by threat method or routing, such as email, file, process, user, etc.

Threat Intelligence: Threat Activity



Using Threat Activity

- Displays events related to known threat sites over the desired time period
- Panels
  - Threat activity over time by threat collection
  - Most active threat collections and sources
  - Threat activity detail
- Filters
  - **Threat group**: a known threat source—i.e., "who"
  - **Threat category**: threat type, such as APT, backdoor, etc.
  - **Threat Match Value**: choose a filter from a list of fields



Threat Activity Details

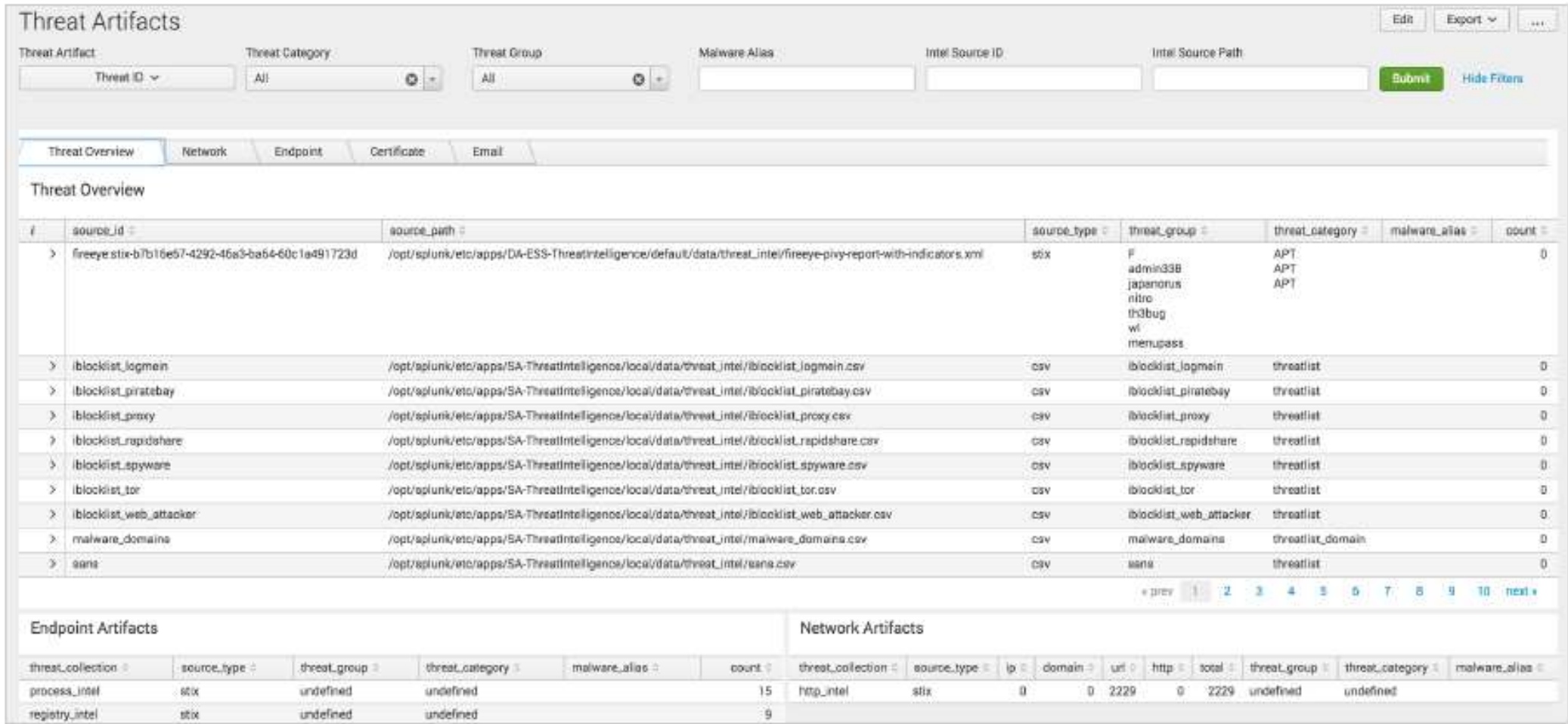
Threat Activity Details

12m ago

_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
2015-4-17 11:45:00	dest	111.118.177.101		fortinet	130.253.37.97 132.239.106.34 141.146.8.66 94.229.0.20	111.118.177.101	ip_intel	iblocklist_proxy	threatlist
2015-4-17 11:45:00	dest	111.118.177.101		fortinet	130.253.37.97 132.239.106.34 141.146.8.66 94.229.0.20	111.118.177.101	ip_intel	iblocklist_tor	threatlist
2015-4-17 11:45:00	dest	119.42.227.250		fortinet	108.70.143.150 109.232.224.91 122.228.206.87 138.246.7.1	119.42.227.250	ip_intel	iblocklist_spyware	threatlist
2015-4-17 10:45:00	dest	119.70.40.101		fortinet	110.136.218.200 115.163.62.226	119.70.40.101	ip_intel	iblocklist_web_attacker	threatlist

- Use threat details to examine the most recent threat events, including source, destination, sourcetype (i.e., how was it detected), threat collection, group, and category
- You can also filter or highlight rows (similar to the Web Intelligence dashboards)
  - Select one or more rows, then click **Advanced Filter**

Threat Artifacts



Using Threat Artifacts

- Threat Artifacts displays the current content of the threat intelligence data that ES has downloaded
- You can use the filters at the top to select a threat artifact type, and then filter by fields relevant to the selected artifact type
- The threat overview panel displays the items that have been downloaded from threat lists or STIX/TAXII sources
- The sub-panels display statistics on the threat intelligence data by endpoint, email, network and certificate
- The tabs allow you to drill down into the categories to see more details about each type of threat

Integrating Artifacts During Investigation

- Use the Threat Artifacts dashboard to get more information about an active threat
- For instance:
  - On the Threat Activity dashboard's **Most Active Threat Source** panel, you see that **iblocklist_proxy** is the most common threat source, and you want to learn more
    - 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, and in the Network tab you can inspect the full list of known IP addresses from this threat list, including locations when known

Module 9:
Protocol Intelligence

Objectives

- Describe how stream data is input into Splunk events
- List the types of stream events
- Use ES protocol intelligence to analyze captured stream data

Security Intelligence: Protocol Intelligence

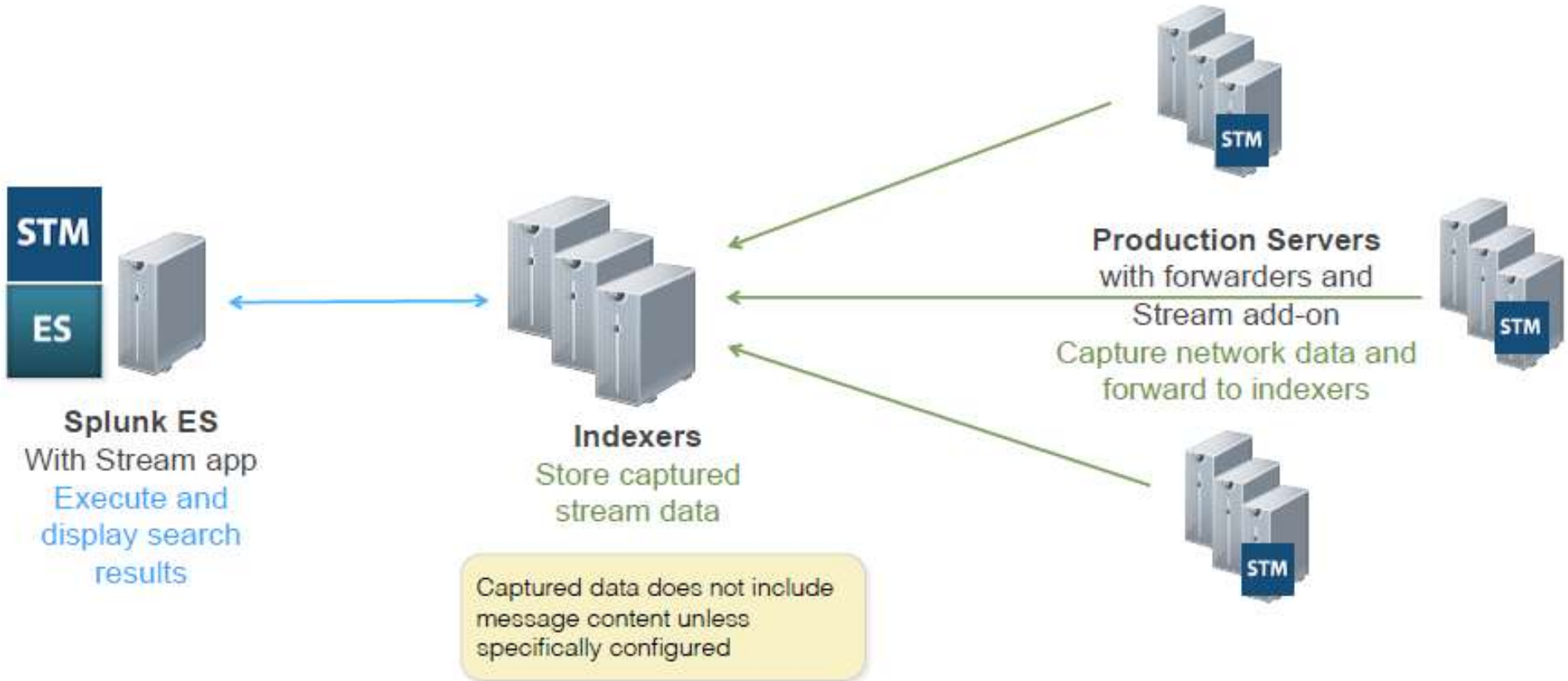
Protocol intelligence is ES's set of tools for analyzing network traffic

Protocol Center	An overview dashboard showing protocol activity across the network
Traffic Size	An analytical dashboard showing network traffic rates and trends
DNS	A pair of dashboards showing both an overview of activity of DNS queries as well as a search interface
SSL	A pair of dashboards for analyzing SSL certificate activity
Email	A pair of dashboards for analyzing email activity

Protocol Intelligence Use Cases

- Captures network traffic directly without 3rd party vendor software or log data
- Use it to:
  - Monitor suspicious network traffic
  - Correlate logged vs. actual activity
  - Gain direct access to network traffic for SSL, HTTP, DNS, and SMTP activity
  - Configure correlation searches that can monitor network traffic

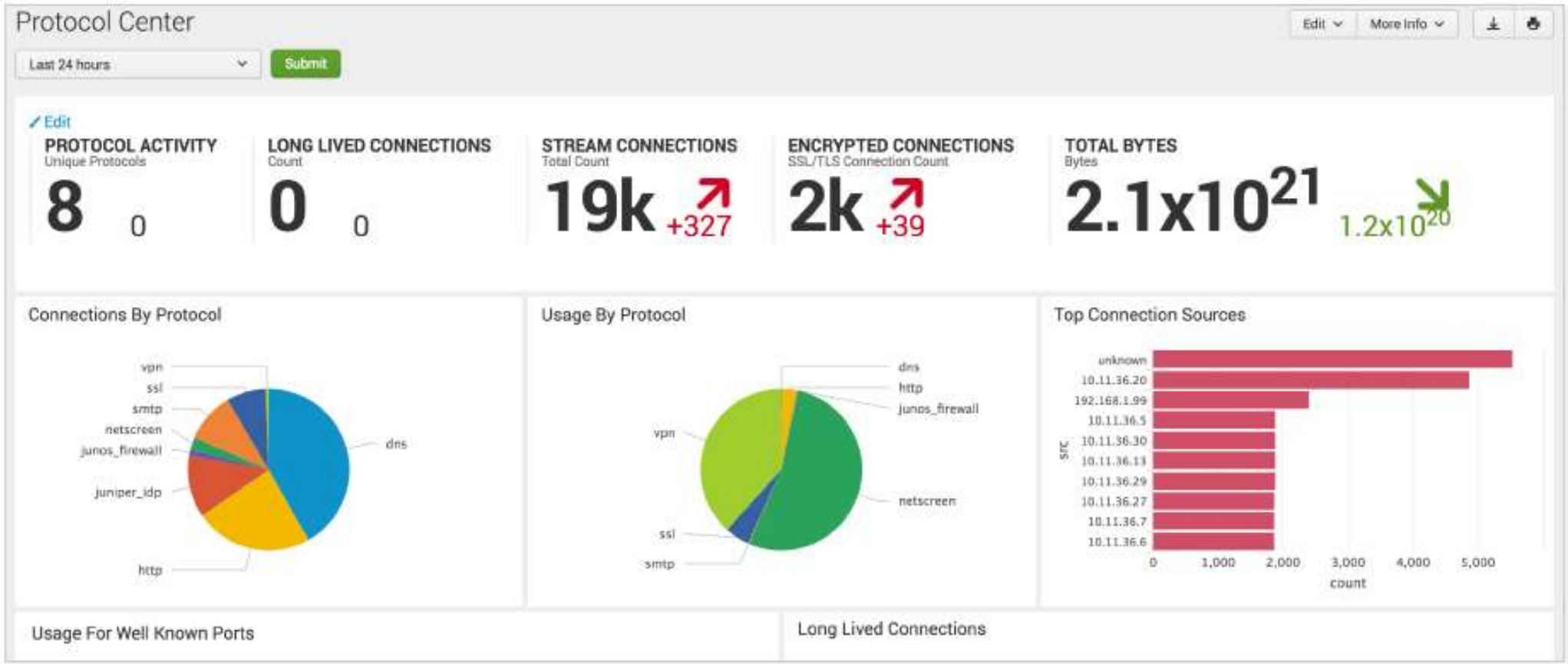
Stream Data Flow



Stream Events

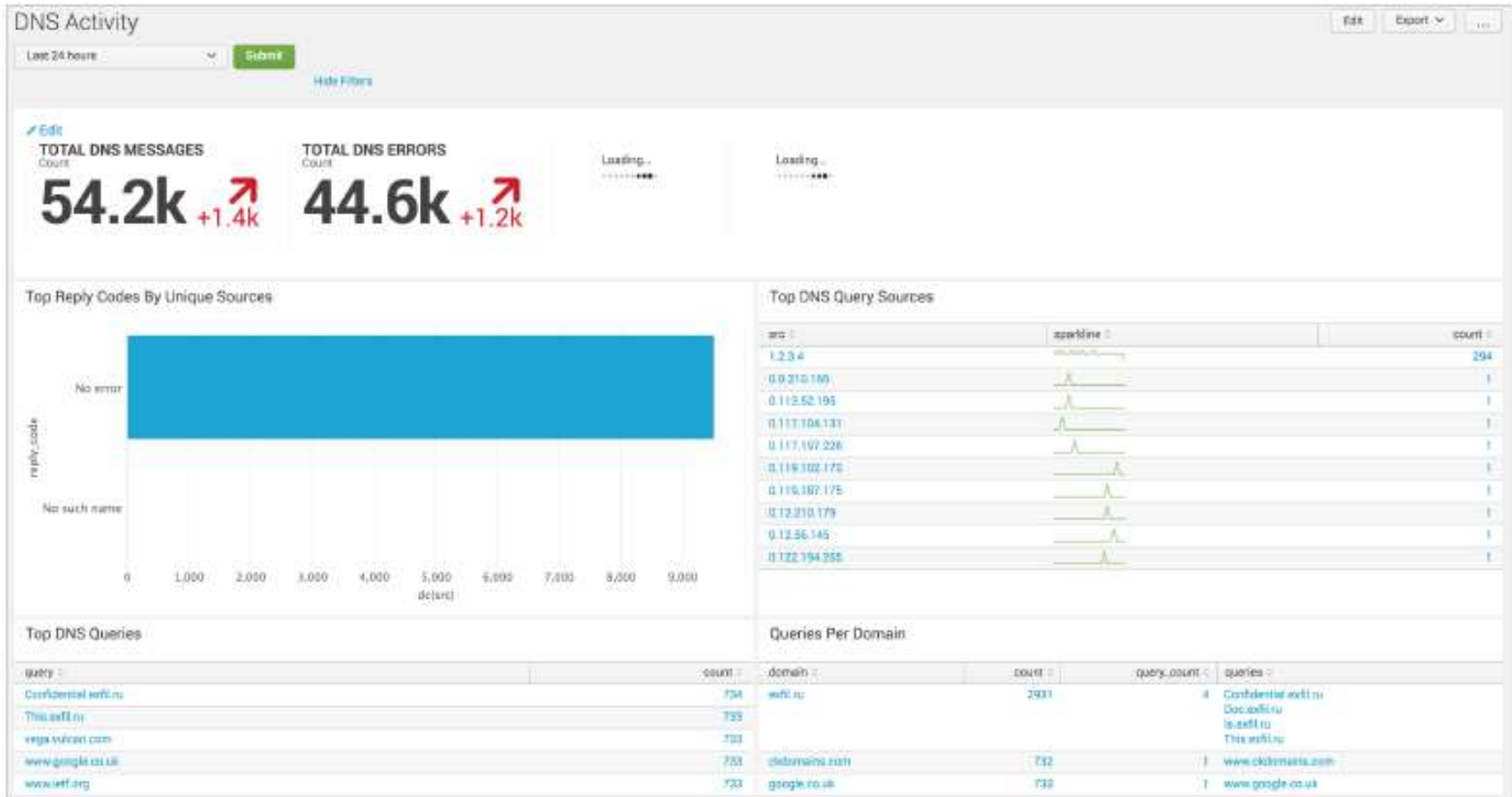
- Stream events are stored with **`stream:xxxx`** source types
  - Examples: `tcp`, `udp`, `dns`, `smtp`, `http`
- Standard field extractions:
  - Capture time, type, size, source/dest info
- Depending on specific source type, additional fields are extracted
  - HTTP: cookies, request parameters, etc.
  - SMTP: sender, receiver, subject, summary of body
  - DNS: DNS query, query type, DNS host, etc.

Protocol Intelligence: Protocol Center

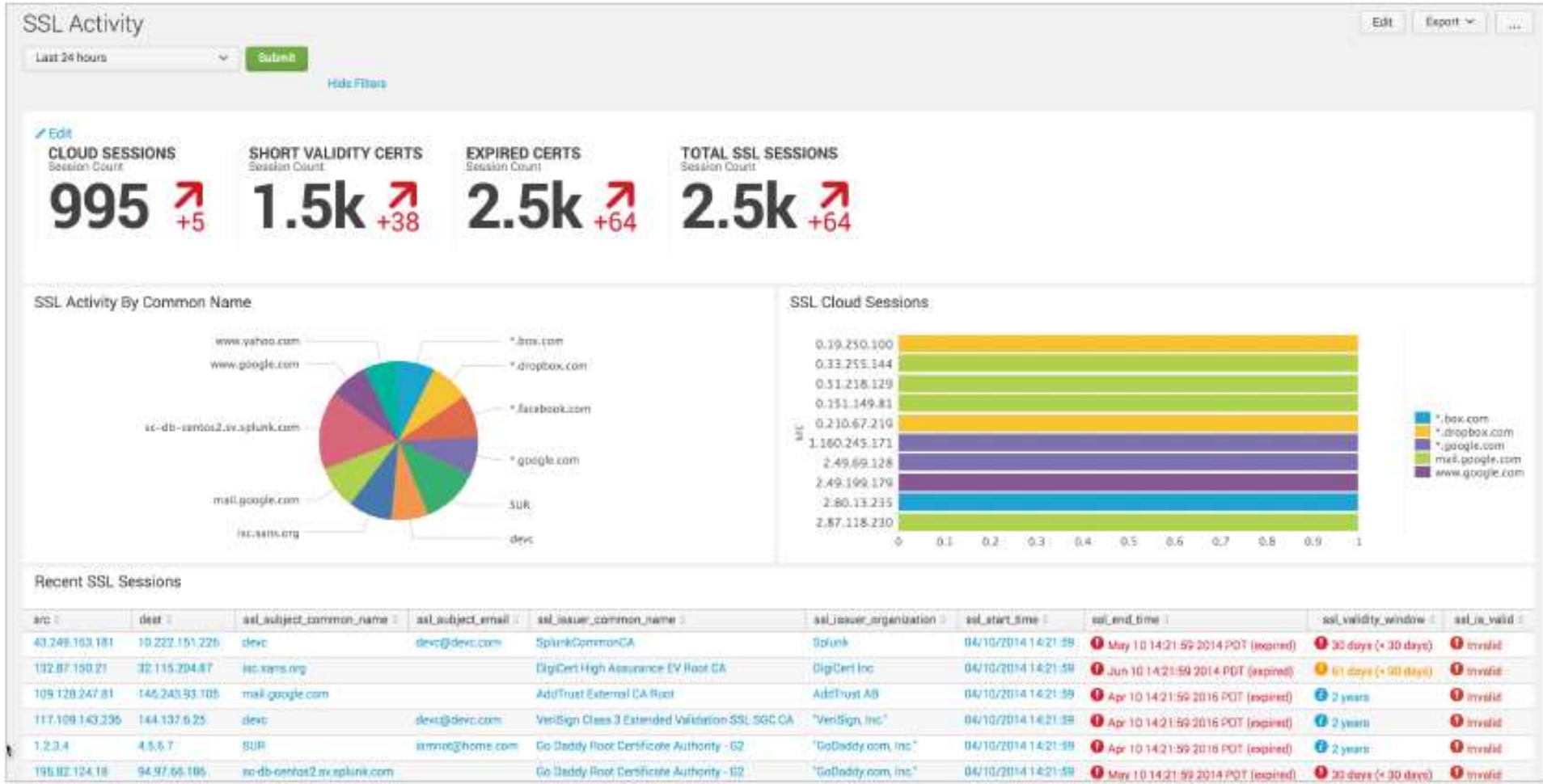


Protocol Intelligence: Traffic Size Analysis

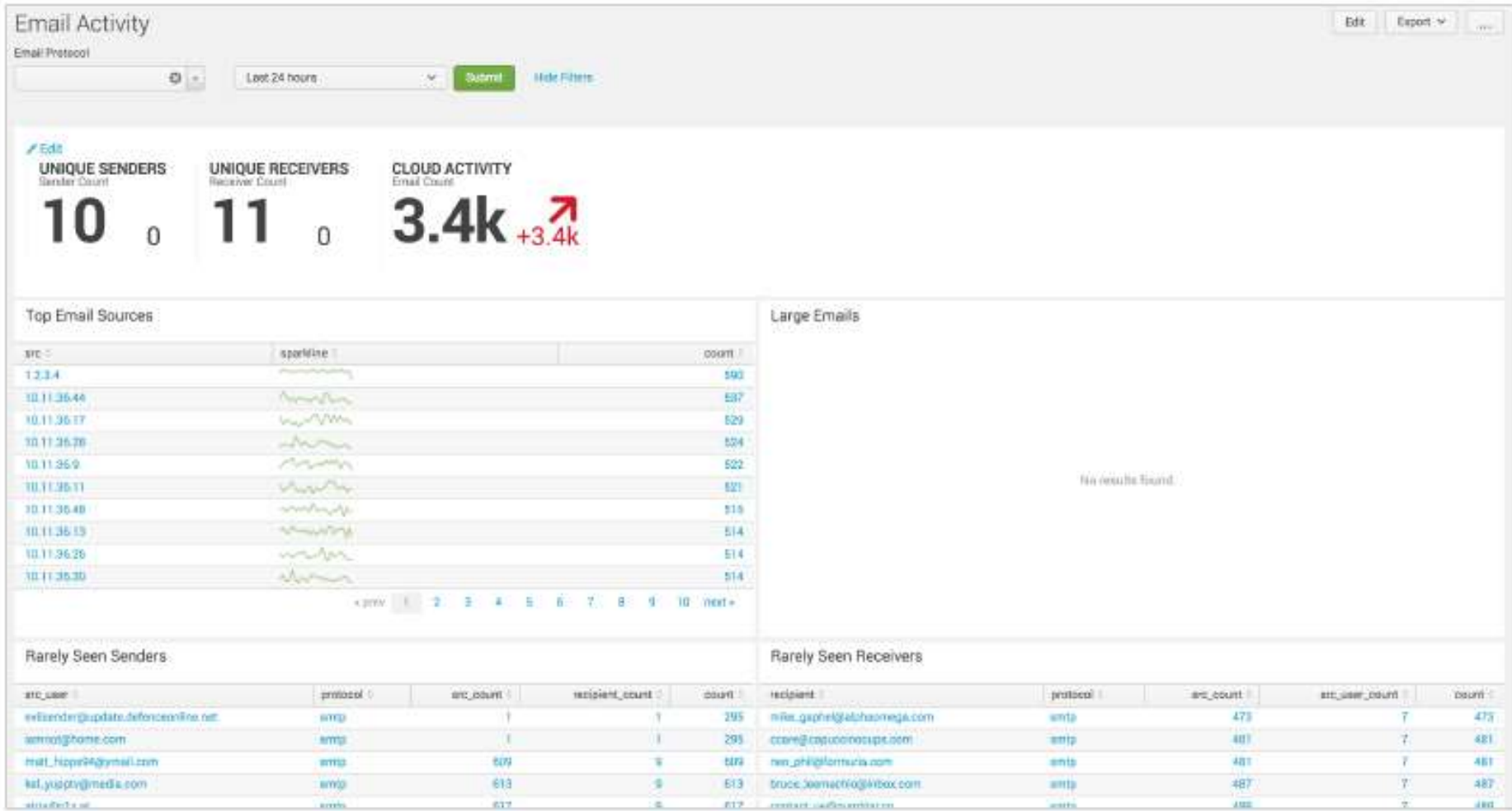
Protocol Intelligence: DNS Activity



Protocol Intelligence: SSL Activity

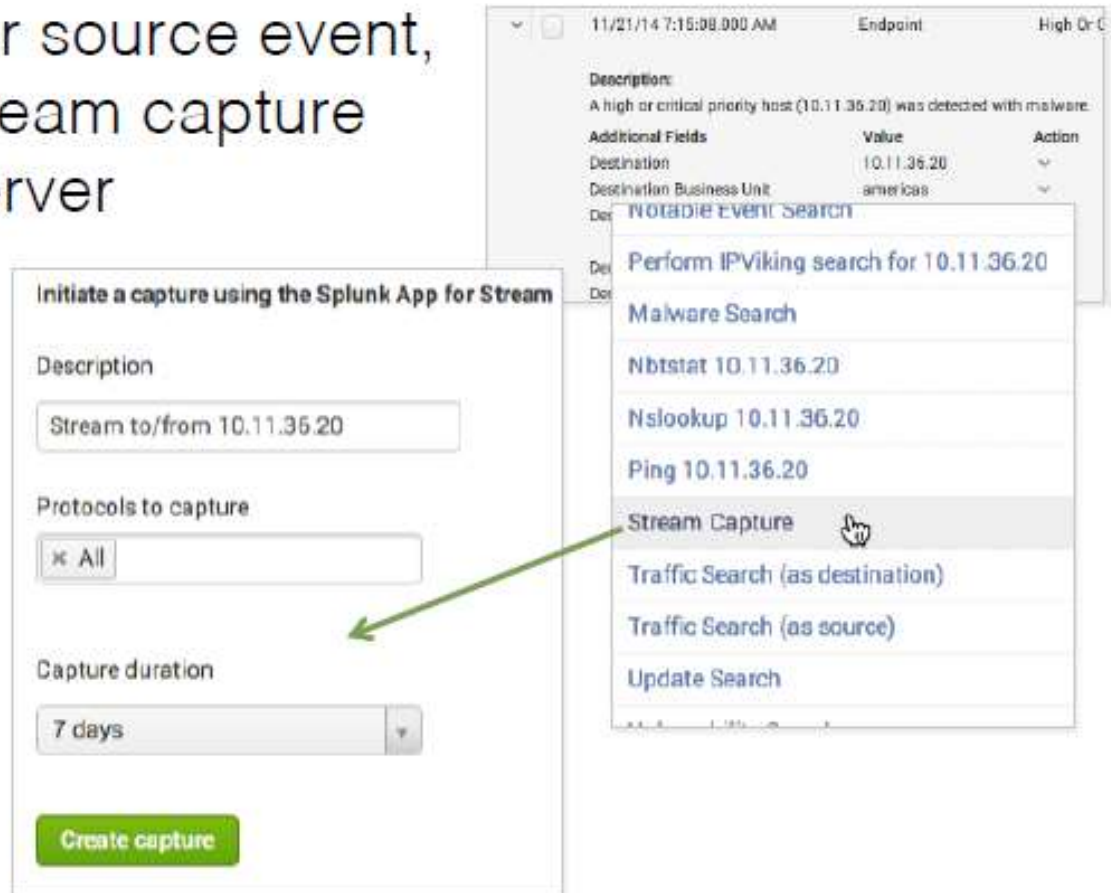


Protocol Intelligence: Email Activity



Creating a Stream Capture

- When investigating a notable or source event, you can create a temporary stream capture for the source or destination server
- You can then investigate the stream data associated with that server as part of your analysis
- Stream capture can also be started from a correlation search or by an adaptive response action



Scenario: Data Exfiltration

- Some of the protocol intelligence dashboards are very useful for investigating data exfiltration events:
  - **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**: look in **Queries per Domain** for unfamiliar domains getting large numbers of lookups
- If you find an endpoint or server that you think is involved in data exfiltration, create a stream capture for it and analyze the data
  - Look for sensitive information, intellectual property, etc.

Module 10:
Glass Tables

Objectives

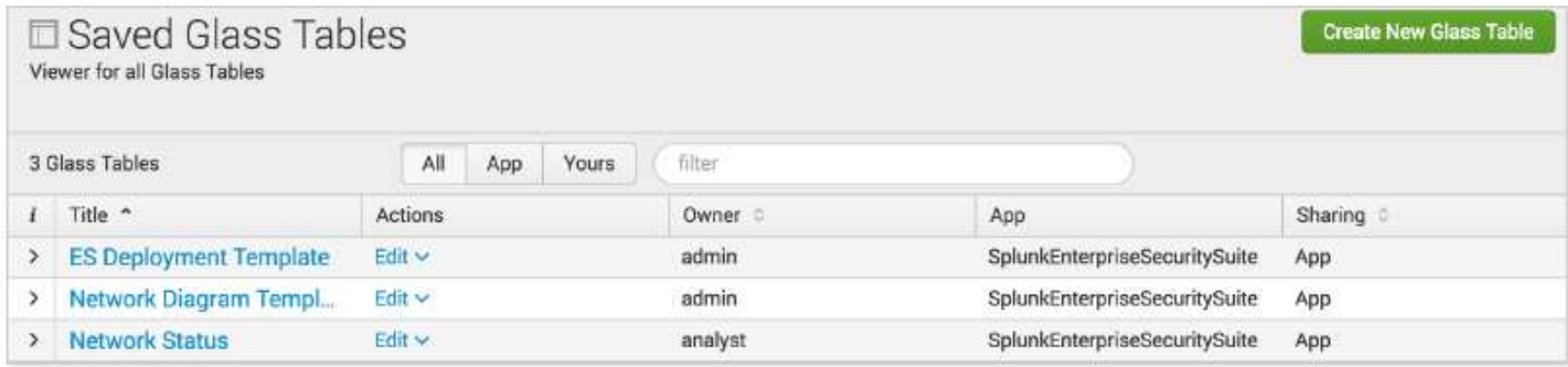
- Design glass tables to display security status information
- Use the glass table editor to create and edit glass tables
- Use key indicators and ad-hoc searches on glass tables
- Add glass table drilldown options
- Create new key indicators

Glass Tables

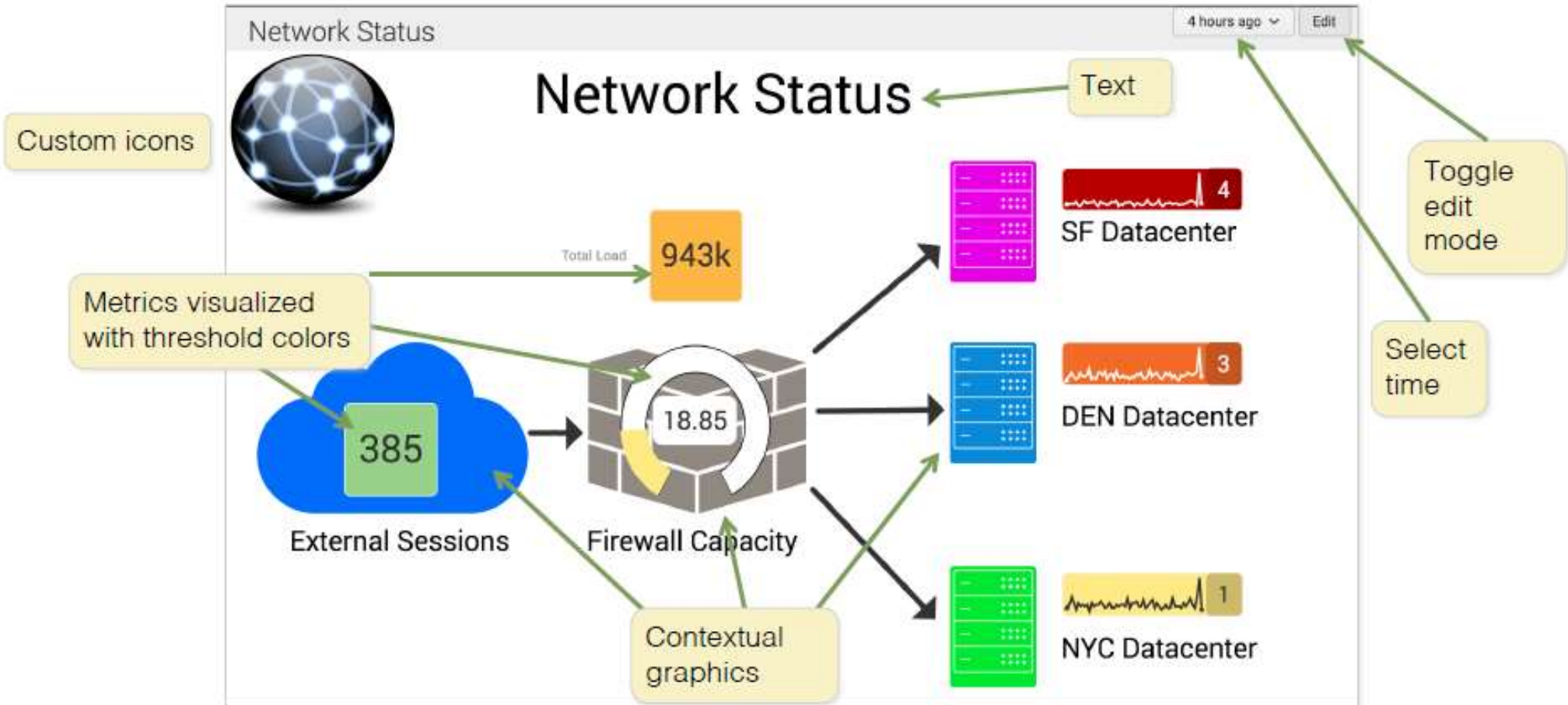
- Glass tables are visualization tools for ES
- Use the time picker to display key indicators and ad-hoc values at a specific time
  - These values are called **metrics** on a glass table
  - Metrics are displayed in visual widgets
- Use glass tables to:
  - Create security operations center displays
  - Show the status of critical metrics
  - Display key indicators in a variety of visual styles
  - Use custom icons and graphics to enhance the display

Glass Table Management

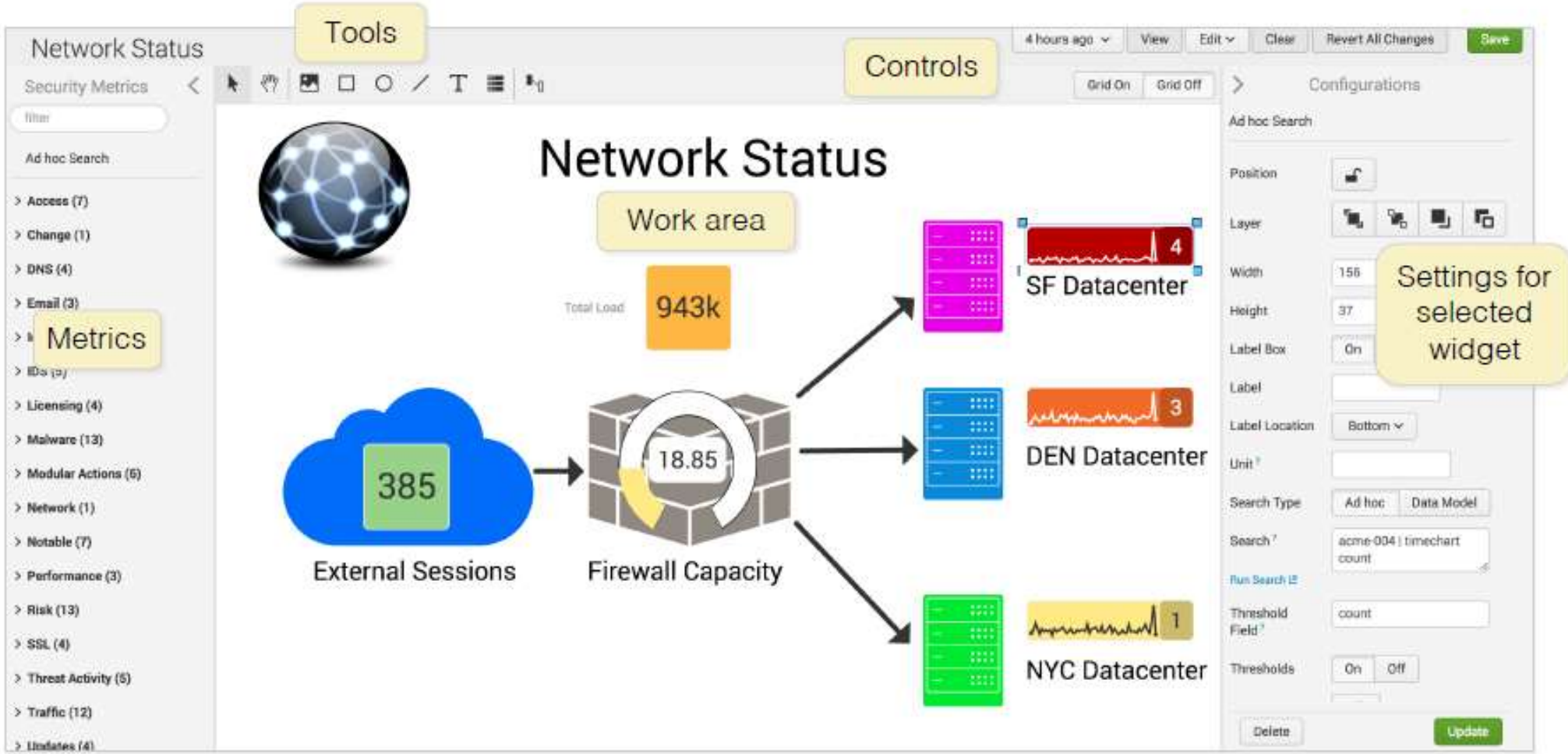
- Navigate to the **Glass Tables** menu
- Select a glass table name to view
  - Analysts or administrators can also edit, delete, or create new glass tables
- Each glass table can be private or shared



Glass Table: Standard View



Glass Table: Edit Mode

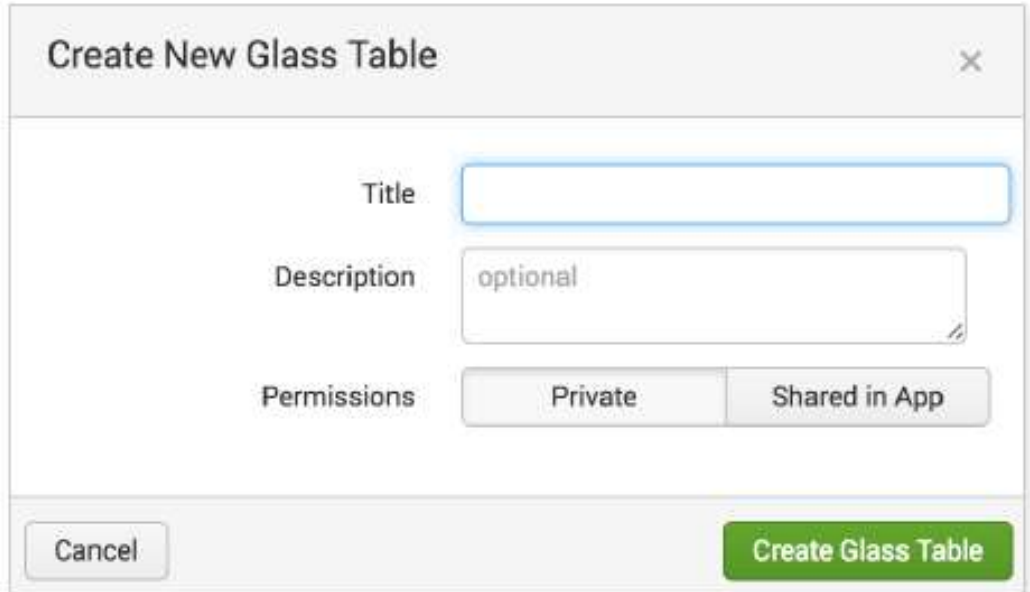


Designing Glass Tables

- Determine which views are needed at the site based on workflow, operations center display requirements, etc.
- Plan the visualization ahead of time
  - Use site graphics and icons if possible to enhance conceptual understanding
- Examine existing documentation for design elements
  - Flow charts, schematics, overview diagrams, etc.
- Plan the overall structure of the visualization and identify required metrics

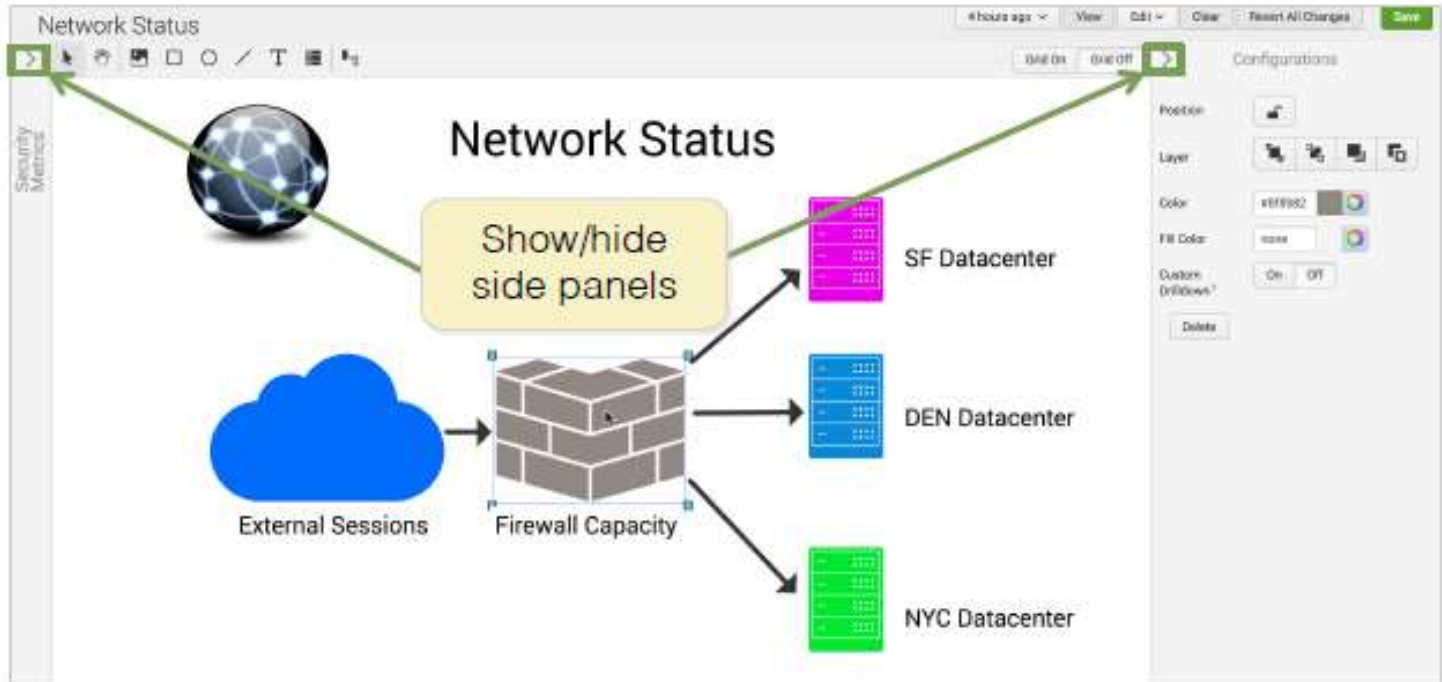
Creating a Glass Table: 1

- Select **Glass Tables > Create New Glass Table**
- Enter the title (will be visible)
- Add a description (optional)
- Select the sharing mode:
  - Private or shared in app
- Click **Create Glass Table**
  - The new glass table now displays in the list
  - Click the title to open the glass table editor



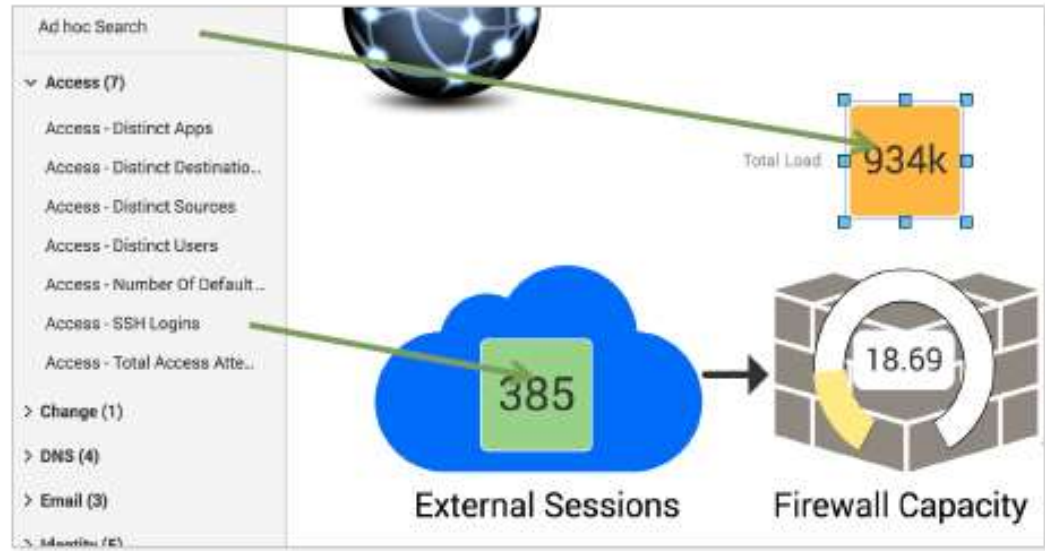
Creating a Glass Table: 2

- Add conceptual graphics and lay out overall visual structure
- Use image tool to add custom graphics
- Selected widget properties can be modified on the right side
- You can hide side panels when not in use



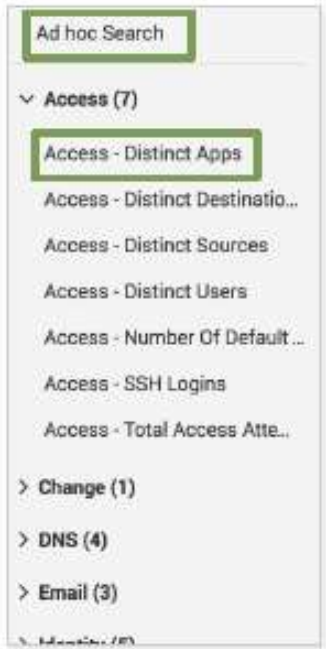
Create a Glass Table: 3

- Use drag and drop to add metrics to the canvas
  - Pre-existing key indicators
  - Ad hoc searches
- Select a visualization type
- Set label and threshold values as needed
- Click **Update**

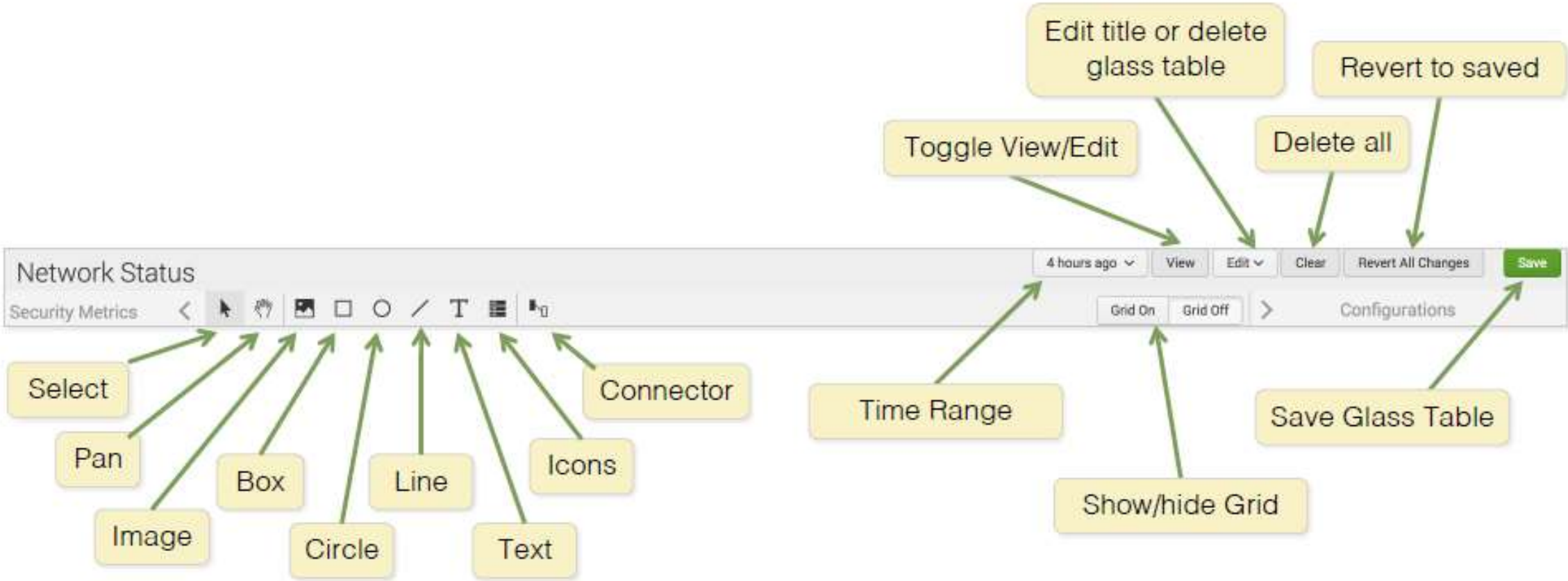


Metrics

- Metrics are based on searches, which generate a display value
  - Normally numeric but can display text
  - Can also display current vs. historic value or a sparkline
- Use an ad hoc search to display a new metric value
  - You write the search when you add the widget
- Use key indicators to display standardized values
  - Key indicators are categorized by type: Access, DNS, etc.



Top Bar Controls



Configuration Bar: General

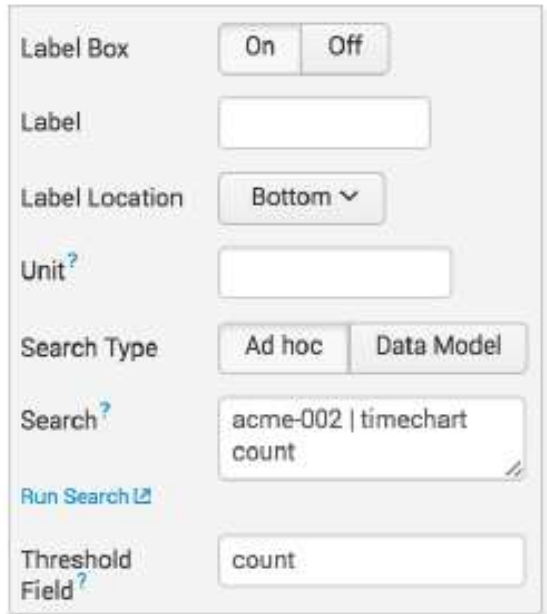
- Most widgets have controls for:
  - Position locking
  - Layer control (bring forward/back)
  - Object color (fore color)
  - Fill color
  - Deletion
    - Or, use the delete key

Configuration Bar: Metrics

- Metric widgets have additional controls:
  - Width and height
  - Label and unit controls
  - Search information (disabled for key indicators)
  - Threshold on/off
  - Custom drilldown
  - Visualization type
- Use the **Update** button to refresh the glass table with any changes you make to a widget before selecting a different widget

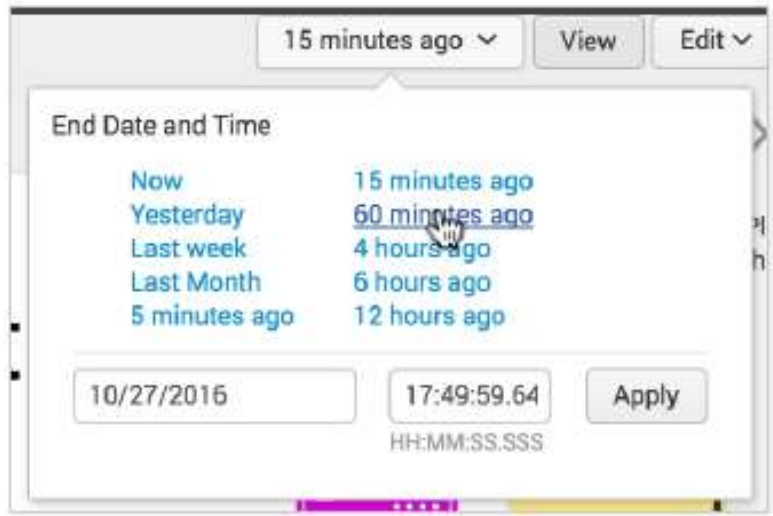
Configuration Bar: Ad-hoc Search

- You can add an ad-hoc search widget to display any search result without a key indicator
  - Drag an ad-hoc search widget onto the canvas
  - Select search type: **Ad-hoc** or **Data Model**
  - Enter search criteria
    - Use **Run Search** to test in a new window
    - The value to be displayed will be one of the result fields
  - Add the field name containing the value to be displayed in the **Threshold Field**
  - Click Update



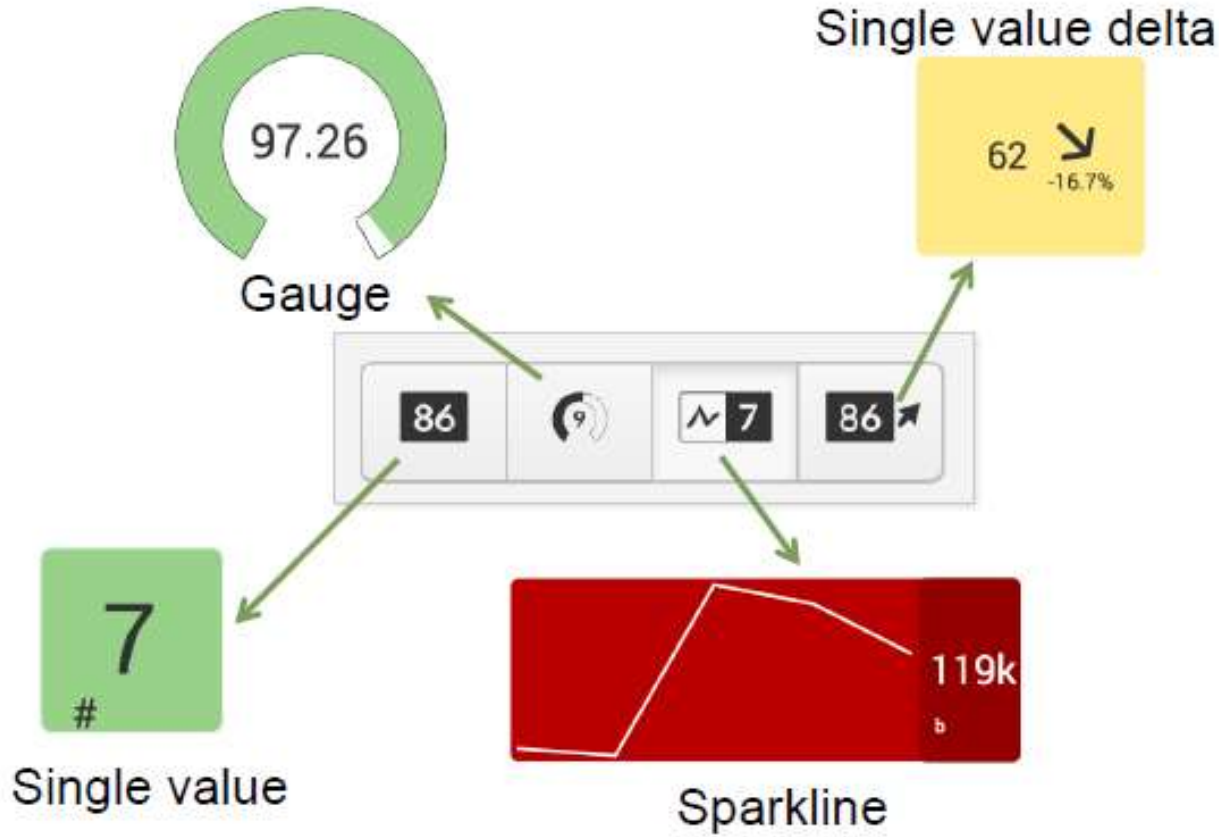
Metric Time Ranges

- Your search should set relative time ranges using the **earliest** and **latest** commands
  - Generally, set **latest=+0s**
  - Set **earliest** to determine the window size, such as **-60m**



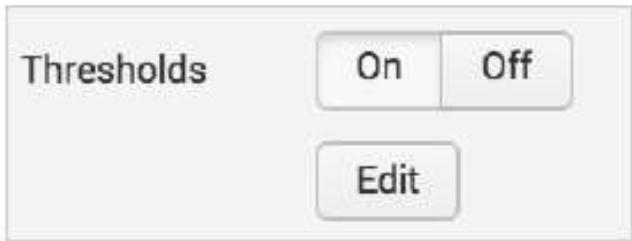
- The search range is relative to the time the user selects
  - Given the example above, if the user selects **60 minutes ago**, the metric displays results from **-60m** to **-120m**

Widget Visualization Types



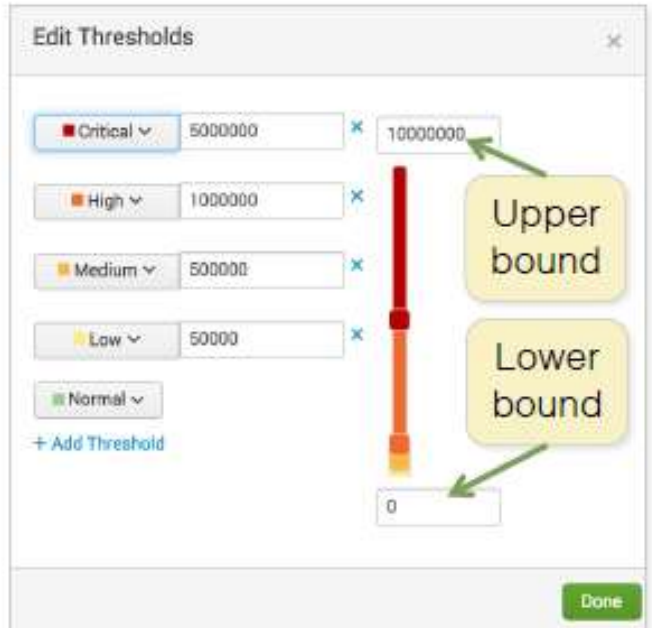
Thresholds

- Metric widgets can display colors to indicate severity
- The scale runs from **Normal** (green) to **Critical** (red), plus Info and Unknown
  - **Info**: a value that has no severity
  - **Unknown**: the value does not exist
- To display threshold colors, click **On**
- Use the **Edit** button to configure the threshold map



Threshold Mapping

- Add as many threshold levels as you need
  - Enter a value for each level
  - Use Info for values that don't have a logical severity
- Levels can be in any order
  - Normal high
  - Normal low
  - Normal middle
- Fill in the upper and lower bound if applicable
- Click Done

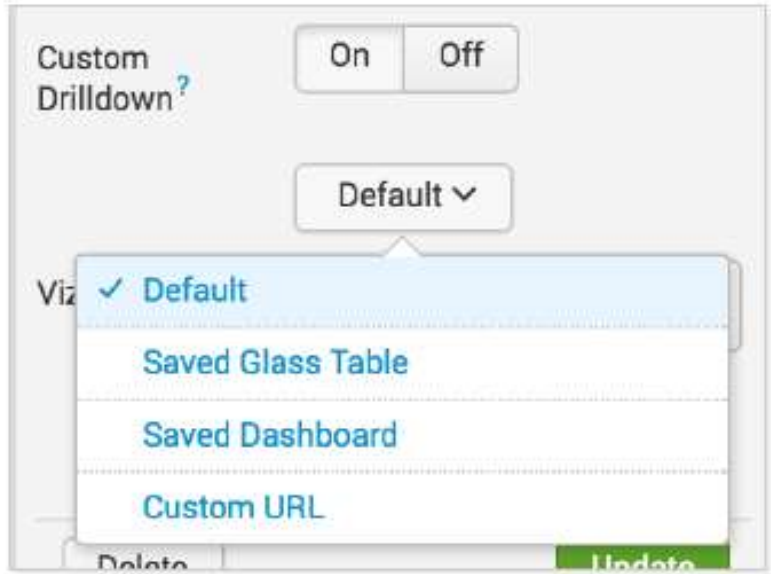


Visualization Requirements

- Single value visualization
  - Just needs a single output value
  - The value can be text—but then it can't use thresholding
- Gauge
  - Requires an upper and lower bound setting
- Sparkline
  - Requires a search using **timechart**
  - Supports mouse-over for details
- Delta
  - Requires count and delta fields

Glass Table Drilldown

- By default, clicking a metric widget opens a new window and runs the search for that metric
- Alternatively, you can enable a custom drilldown to open:
  - A saved glass table
  - A dashboard in Splunk
  - Any accessible URL



Glass Table Storage

- Each glass table is managed in the KV store and is contained within the ES app context
- Each glass table can be either:
  - Private, only accessible by the owner
  - Shared with all users who have access to the ITSI app

Creating New Key Indicators

- If you have the same metric to display on multiple glass tables, you may want to define it as a new key indicator
  - This will also make it available as a key indicator on other ES dashboards
- You must be an analyst or administrator to create or edit key indicator searches
- Start by selecting **Configure > Content Management**, and then selecting **Create New Content > Key Indicator Search**

Key Indicator: 1

- Enter a name for the search
  - This will not be displayed
  - Must start with a capitalized security domain, such as “Access – “ or “Network – “
  - Cannot be changed
- Select an app to store the search in
- Enter a title and sub-title
  - These will be displayed

Key Indicator: 2

- Your search should produce the following:
  - A **current_count** field
  - A **historical_count** field
  - A **delta** field (the difference between current and historical)
- Key indicators need a current value for the past 24 hour period and a historical value for the 24 hour period before that
  - Use the **earliest** and **latest** terms to set the time range
- You can use the `**get_delta**` macro to generate the delta field

Key Indicator: 3

- If possible use the **tstats** command and **summariesonly**
  - This provides faster results by searching only accelerated events
  - The **`tstats`** macro automatically sets this option
- Use **appendcols** to run two searches to create both the current and historic counts

```
| `tstats` count as current_count from datamodel =
Authentication.Authentication where earliest=-24h@h latest=+0s
(Authentication.app=sshd)
| appendcols [| `tstats` count as historical_count from datamodel =
Authentication.Authentication where earliest=-48h@h latest=-24h@h
(Authentication.app=sshd)]
| `get_delta`
```

Key Indicator: 4

- Drilldown URL: optional
  - A URL to any dashboard or external page
  - Defaults to opening the KI search
- Schedule
  - Accelerates the results
- Fields:
  - Value (required): the current field
  - Delta (optional): the delta field; without delta, the KI will only show the current value—no trend indicator or change value

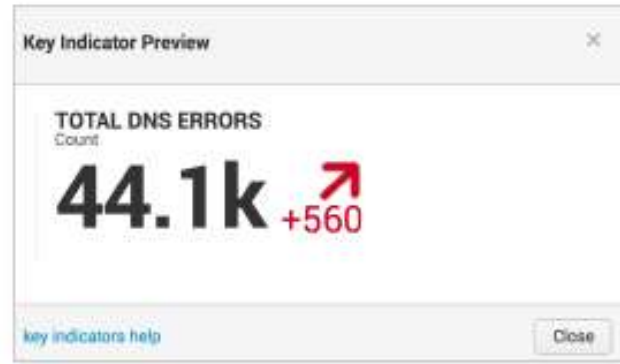
Key Indicator: 5

- Threshold: optional; the KI value will be displayed in green if it is below the threshold and red if it is above
  - Invert swaps this
- Value suffix: optional; for instance “%” or “kb/sec”

Key Indicator: 6

- You can preview your key indicator
  - Click the **Preview** button
- Also provides a link to key indicator documentation

  docs.splunk.com/Documentation/ES/latest/User/KeyIndicators
- Click Save when finished
- The key indicator can now be added to dashboards or glass tables
  - Only administrators can edit dashboards by default

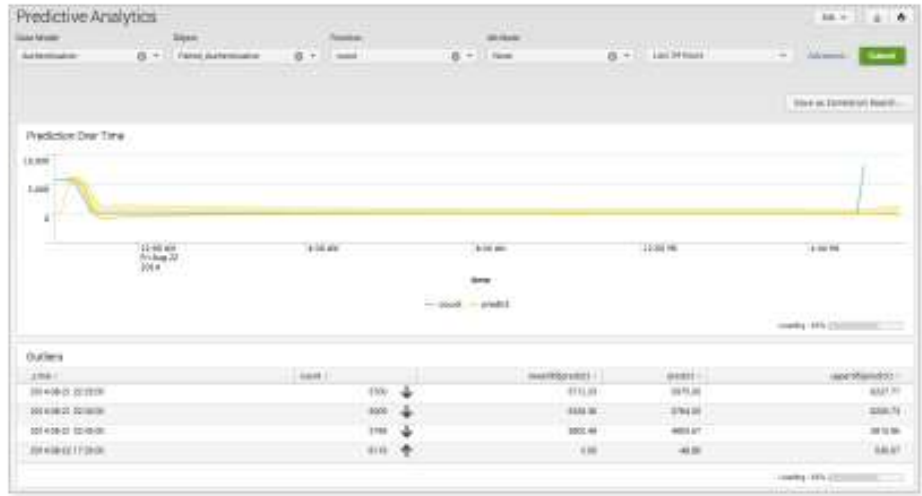


Glass Table Role Capabilities

- By default, both ES **administrators** and **analysts** can create, edit and delete glass tables and key indicators
- Only ES administrators can add key indicators to dashboards they don't own
- Related capabilities:
  - `delete_glass_table`
  - `read_glass_table`
  - `write_glass_table`

Predictive Analytics

- Search > Predictive Analytics
- Displays the actual values over time (blue line) vs. predicted values (yellow line) and the possible range of values for the selected object over time (shaded area), within two standard deviations



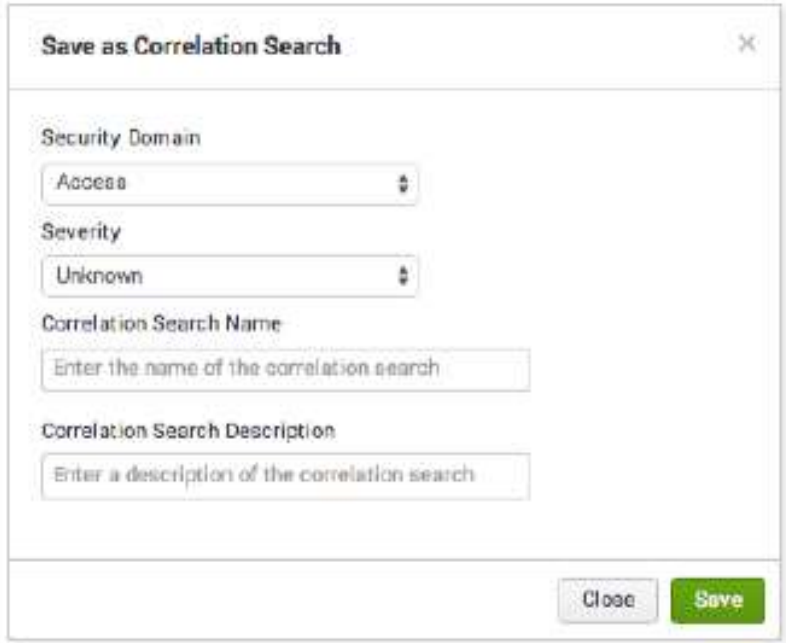
- Outlier data (outside 2 standard deviations) displays in the table below
- Use fields at top of page to select data model, object, and optional settings for function, attribute, and time range

Using Predictive Analytics

- Scenario: There seems to be a lot of failed login attempts—is it outside of what you should expect?
  - In Predictive Analytics, select the **Authentication** data model and **Failed Authentication** data set
  - Select the **Count** function and leave **Attribute** set to **None**
  - Select the appropriate time range for your investigation and run the search
- Examine the time graph for time segments where the blue line is outside the shaded area
  - The **Outliers** table identifies these segments
- The outliers represent anomalous trends

Predictive Analytics Correlation Searches

- Only ES Admins can use this command
- After configuring the Predictive Analytics dashboard, it can be saved as a new correlation search
- Select **Save as Correlation Search...**
- Set the fields in the dialog as appropriate
- Click **Save**
- Now ES will automatically search for outliers from this predictive analysis and create notable events when they occur in the future to alert you to investigate



How to Set Advanced Predict Options

- Select the **Advanced**… link
  - You can change the timespan, algorithm, future timespan, holdback, and lower and higher confidence intervals
  - These normally can be left defaulted