



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



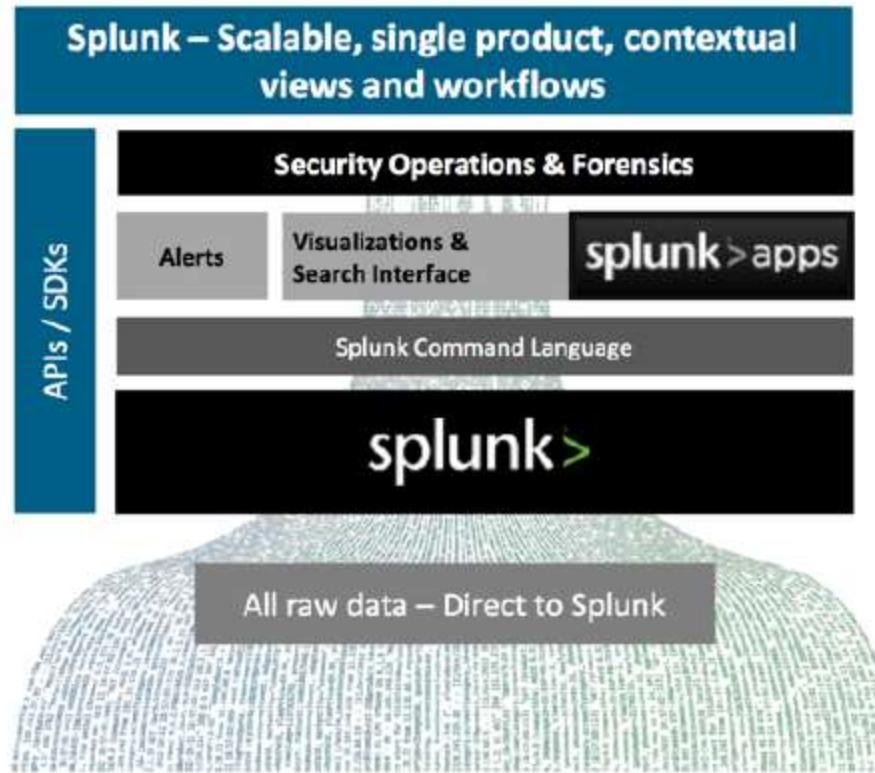
# ES Users



Security Analysts



SOC Staff



Security Execs/Mgrs



Security Auditors

# Advanced Persistent Threats (APT)

---

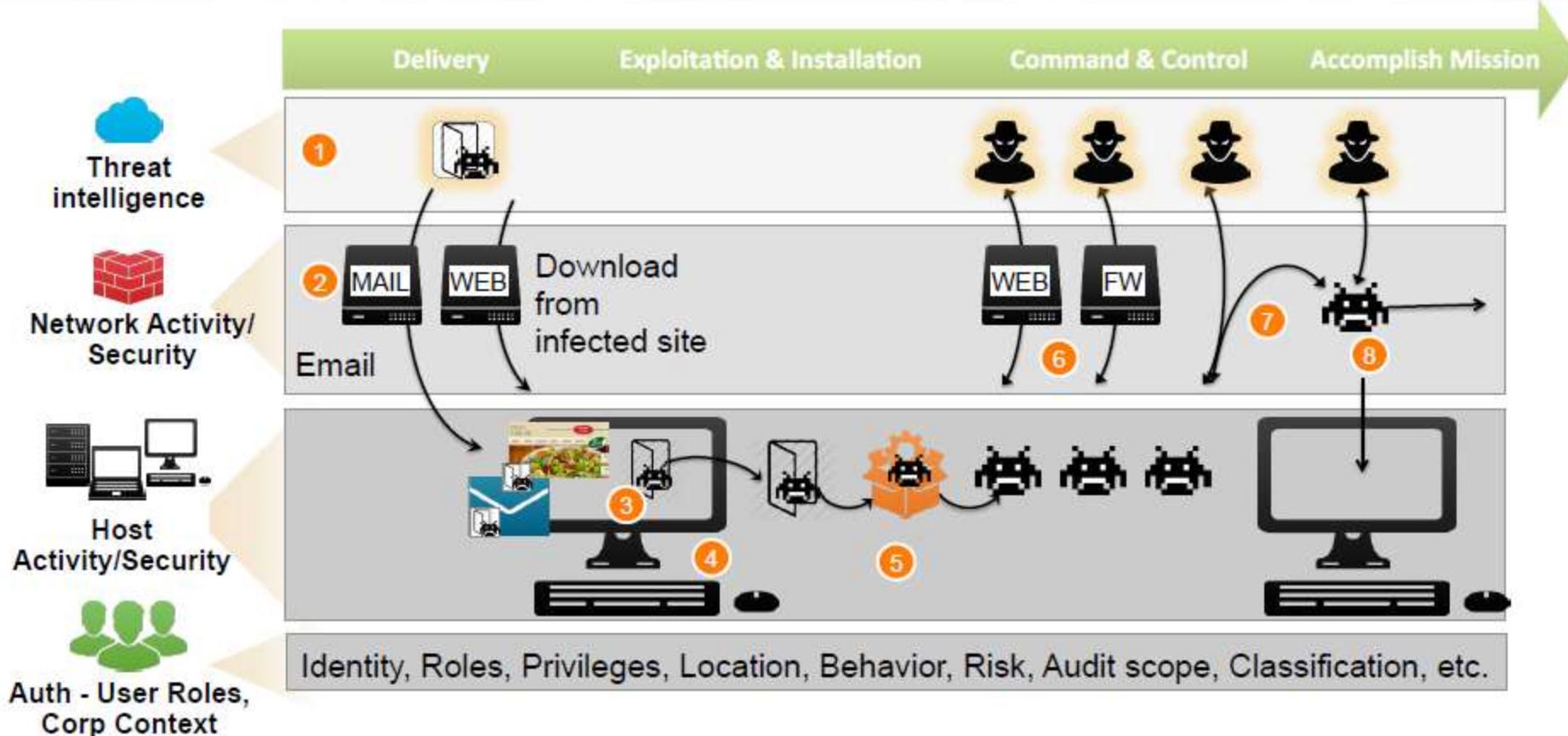
- A growing, global threat
- Focused attacks on specific systems
  - Recent examples: Yahoo, JPMorgan Chase, ...
- Goal: undetected insertion, long-term viability, extraction/delivery of valuable information
- Targets: business, government, individuals
- Many delivery methods
- Metamorphic/polymorphic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

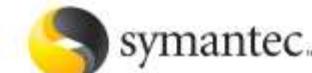
Both attacker and defender can use the kill chain methodology

# Anatomy of an APT Attack

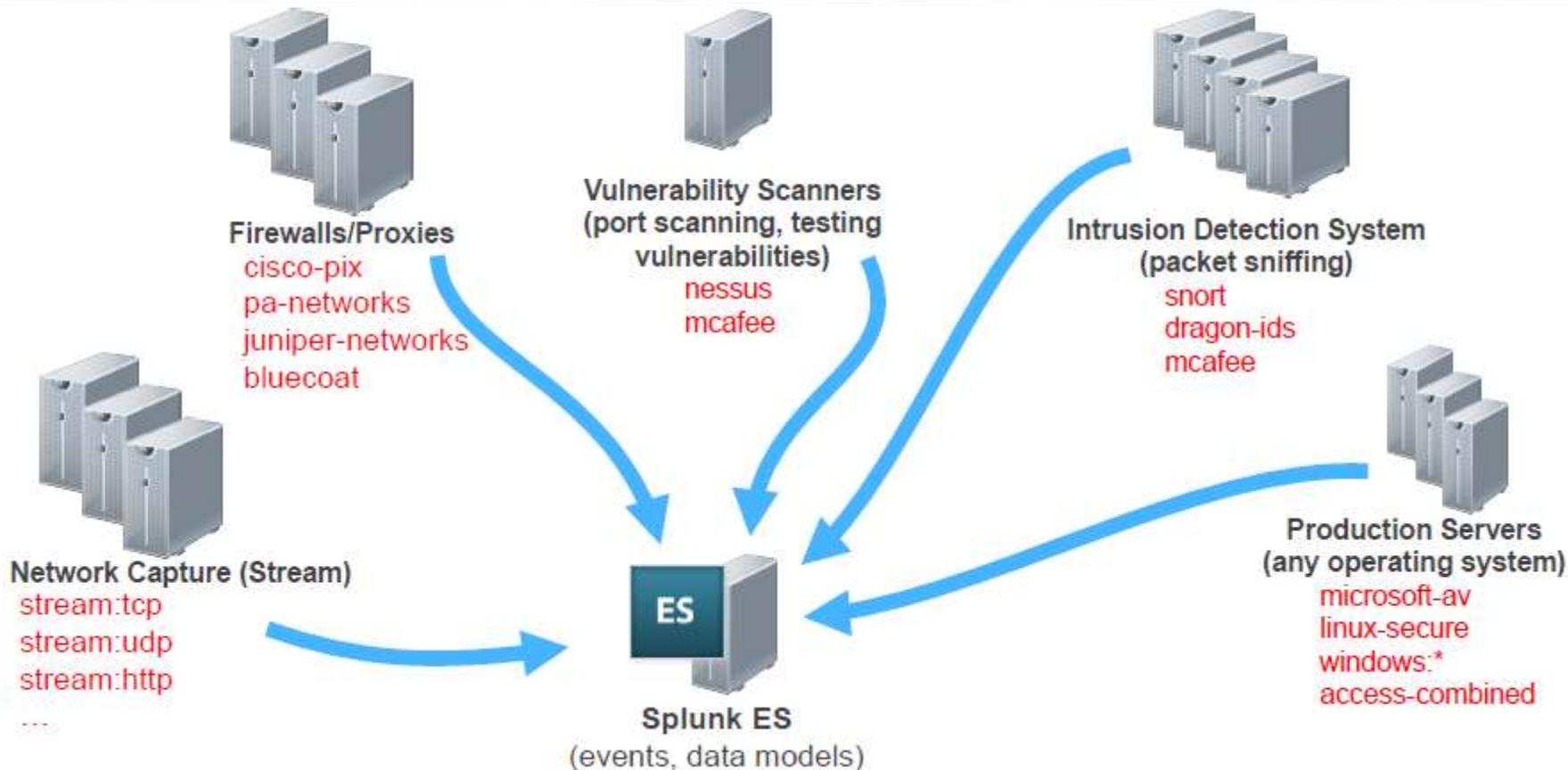


# How ES Works

- 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



## 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

---

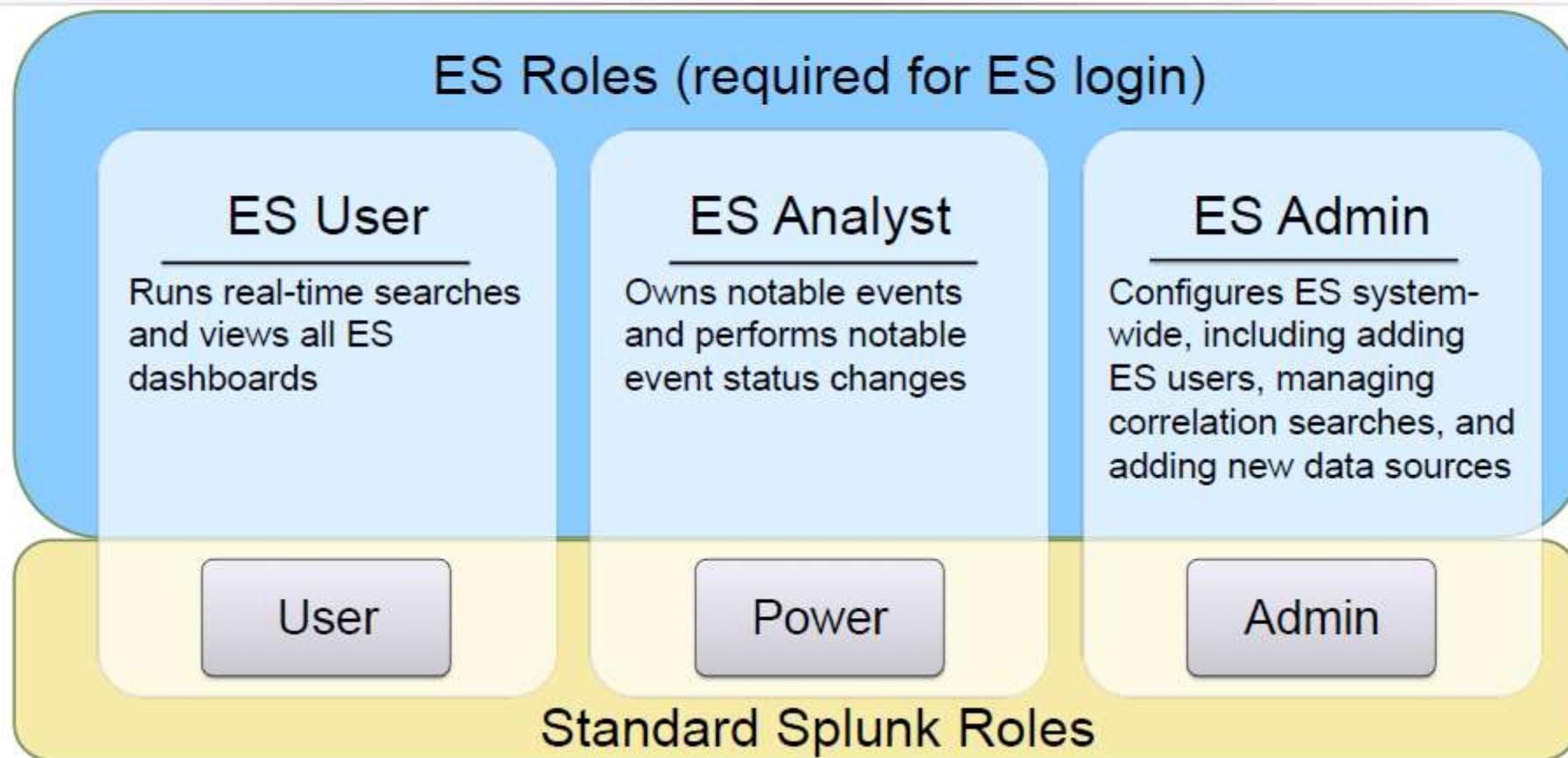
- Notable event urgency is based on the priority of the **assets** and **identities** in your environments
  - Assets are devices in your enterprise, such as routers and servers
  - Assets are identified by IP number or MAC address
  - Identities are people in your enterprise
  - Identities are identified 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

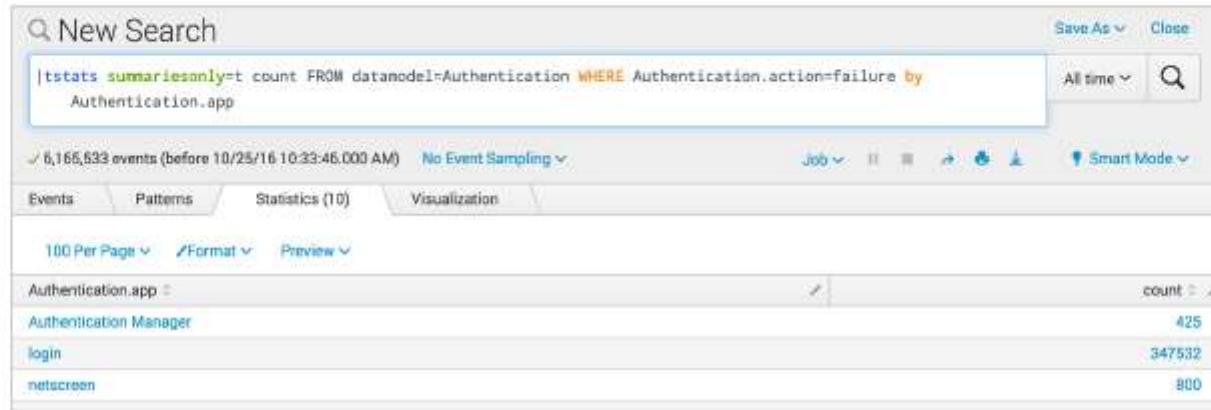
Content Management				
Manage application-specific search triggers, such as correlation searches, key indicators, reports, and other search types.				
I have to ES Configuration				
Edit Selection	Type: Correlation Search	View: All	Status: All	User
Items	Type	Actions	Next Scheduled Time	
Nonnormally High Number of Endpoint Changes By User	Correlation Search	SA-ESB-EndpointProtection	2019-10-27 18:00:00 UTC	Enabled   Disable
Abnormally High Number of HTTP Method Events By Src	Correlation Search	SA-ESB-NetworkProtection	2019-10-27 18:00:00 UTC	Enabled   Disable
Account Deleted	Correlation Search	SA-AccessProtection		Disabled   Enable
Activity From Expired User Identity	Correlation Search	SA-IdentityManagement	2019-10-27 18:20:00 UTC	Enabled   Disable   Change is scheduled
Anomalous Audit Trail Activity Detected	Correlation Search	SA-AuditAndDataProtection	2019-10-25 21:25:00 UTC	Enabled   Disable   Change is scheduled
Anomalous New Licensing Port	Correlation Search	SA-ESB-EndpointProtection		Disabled   Enable
Anomalous New Process	Correlation Search	SA-EndpointProtection		Disabled   Enable
Anomalous New Service	Correlation Search	SA-EndpointProtection		Disabled   Enable
Asset Ownership Unspecified	Correlation Search	SA-IdentityManagement		Disabled   Enable   Change is real-time
Bane Force Access Behavior Detected	Correlation Search	SA-AccessProtection	2019-10-25 21:25:00 UTC	Enabled   Disable   Change is scheduled
Bane Force Access Behavior Detected Over One Day	Correlation Search	SA-AccessProtection		Disabled   Enable
Clearance Password At Rest Detected	Correlation Search	SA-AccessProtection		Disabled   Enable   Change is scheduled
Completely Inactive Account	Correlation Search	SA-AccessProtection		Disabled   Enable
Concurrent Login Attempts Detected	Correlation Search	SA-ESB-AccessProtection		Disabled   Enable
Default Account Activity Detected	Correlation Search	SA-AccessProtection		Disabled   Enable   Change is scheduled
Default Account At Rest Detected	Correlation Search	SA-AccessProtection		Disabled   Enable   Change is scheduled
Excessive DNS Packets	Correlation Search	SA-ESB-NetworkProtection		Disabled   Enable   Change is real-time
Excessive DNS Queries	Correlation Search	SA-ESB-NetworkProtection		Disabled   Enable   Change is real-time
Excessive Failed Logins	Correlation Search	SA-AccessProtection		Disabled   Enable   Change is scheduled
Excessive HTTP Failure Responses	Correlation Search	SA-AccessProtection		Disabled   Enable   Change is real-time
Expected Host Not Reporting	Correlation Search	SA-AuditAndDataProtection		Disabled   Enable
Geographically Improbable Address Detected	Correlation Search	SA-ESB-AccessProtection		Disabled   Enable

# 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

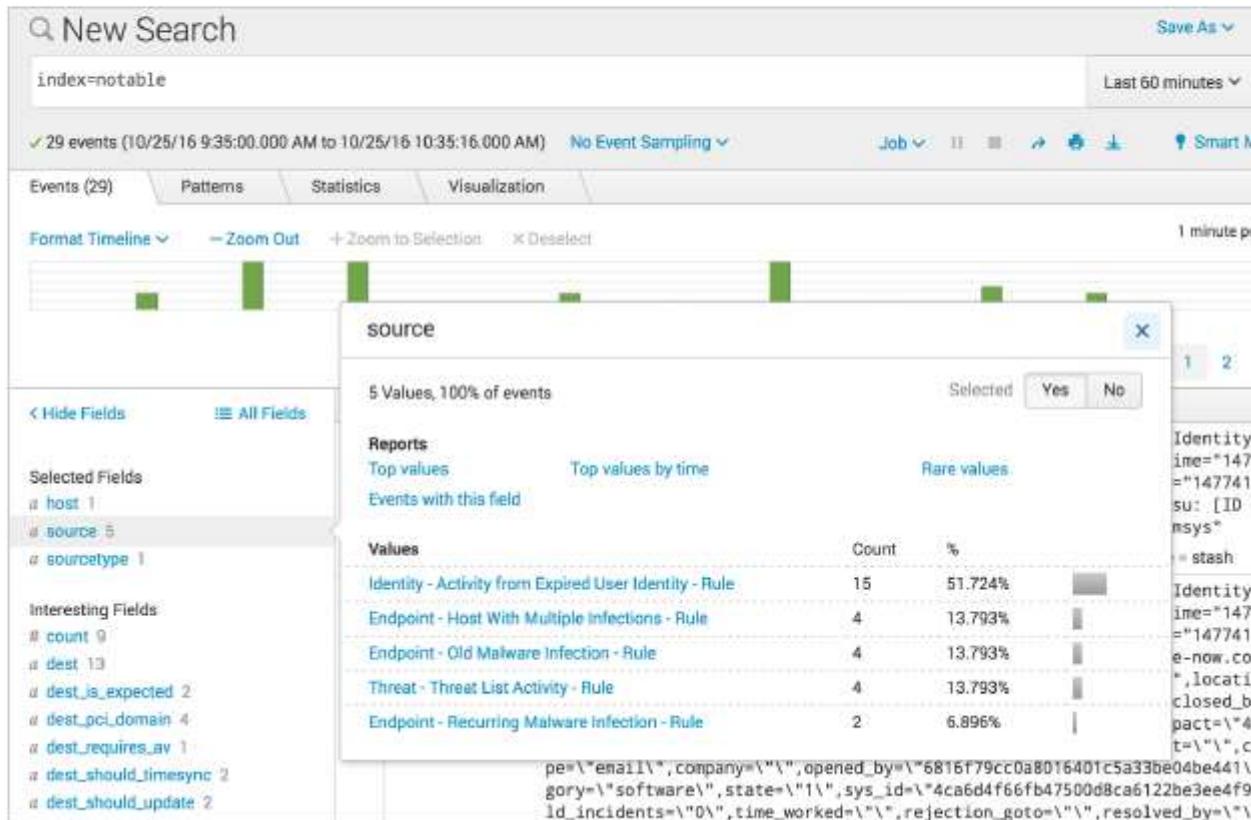
# ES Search Example



- 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

---

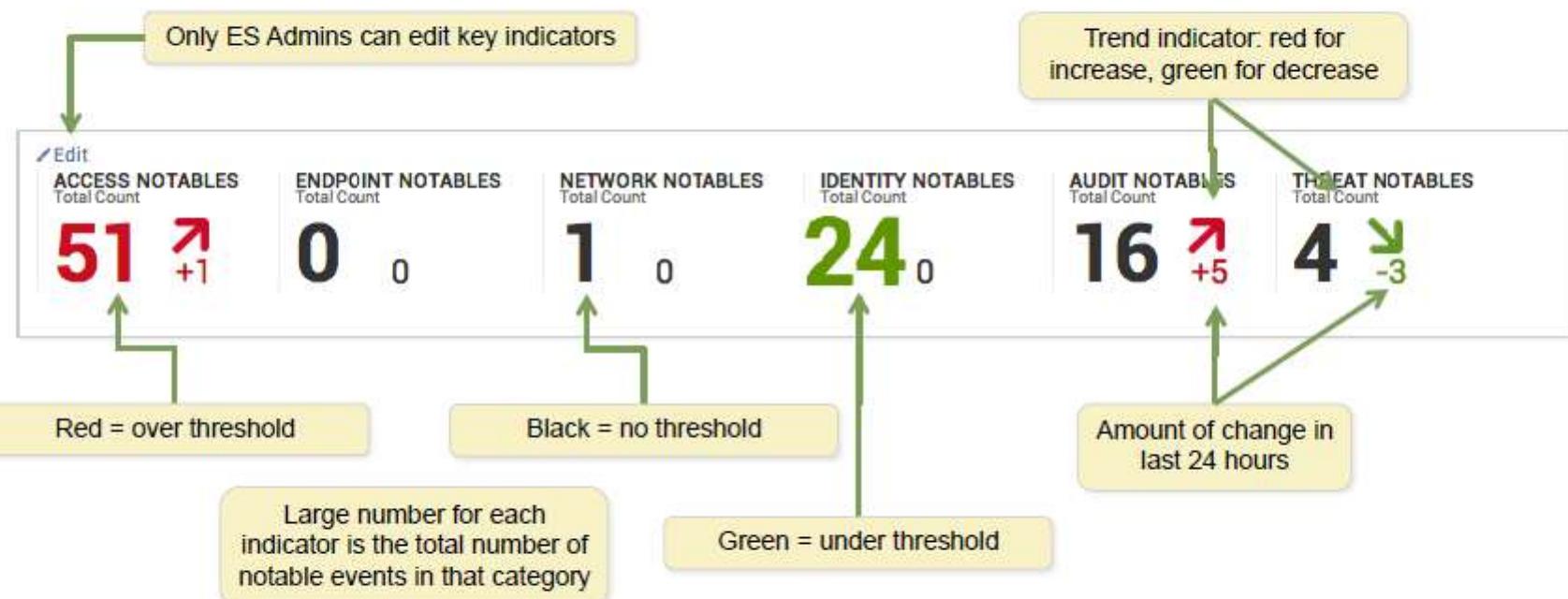
- ES continually runs correlation searches for known types of threats and vulnerabilities
  - There are currently over 60 different correlation search types built in to ES, and you can also create your own
- When a correlation search detects any indicators of compromise (IOC), a notable event is created
  - 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

Click a key indicator total value

A new window opens showing the source search that generates the key indicator values

ACCESS NOTABLES  
Total Count  
**8k** +8k

ENDPOINT NOTABLES  
Total Count  
**97** +97

NETWORK NOTABLES  
Total Count  
**3** +3

IDENTITY NOTABLES  
Total Count  
**3** +3

AUDIT NOTABLES  
Total Count  
**15** +15

THREAT NOTABLES  
Total Count  
**9** +9

New Search

```
| 'es_notable_events' | search security_domain=access | stats sum(count) as count by timeDiff_type | transpose | sort 1 -column | rename "row 1" as current_count,"row 2" as historical_count | 'get_delta' | table current_count,historical_count,delta
```

Events Patterns Statistics (1) Visualization

100 Per Page Formatted Preview

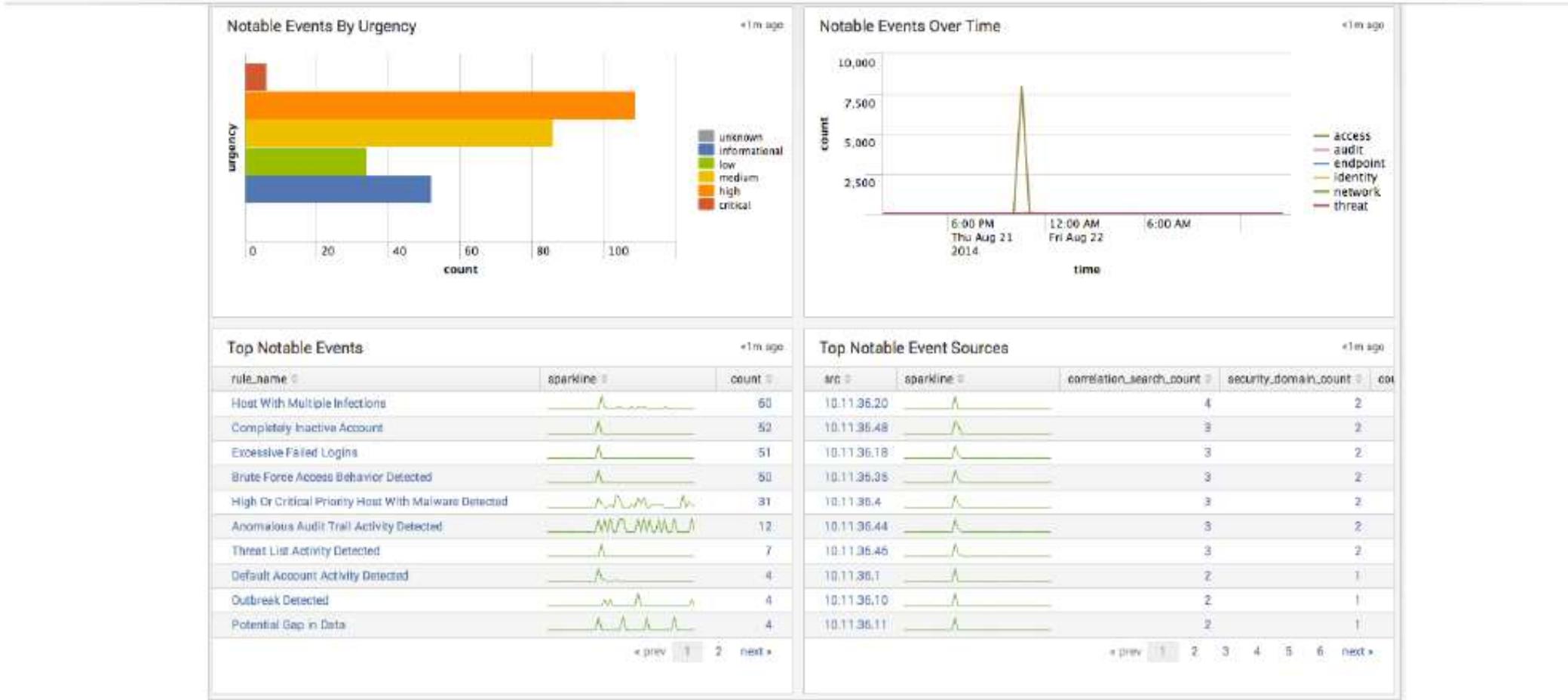
current\_count: 50

historical\_count: 50

delta: 0

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

# Security Posture Panels



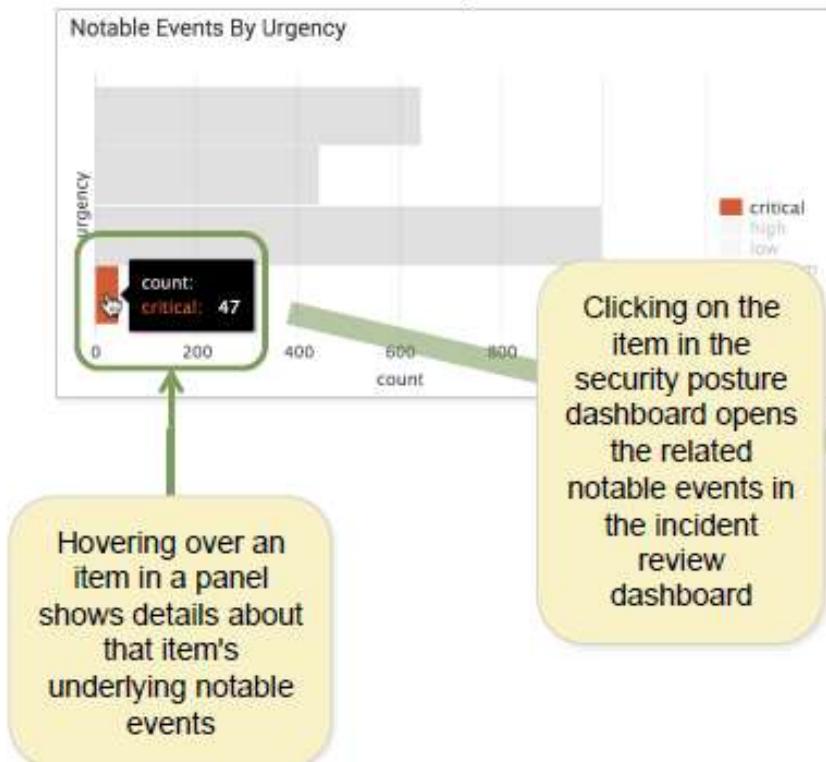
# Notable Event Urgency

---

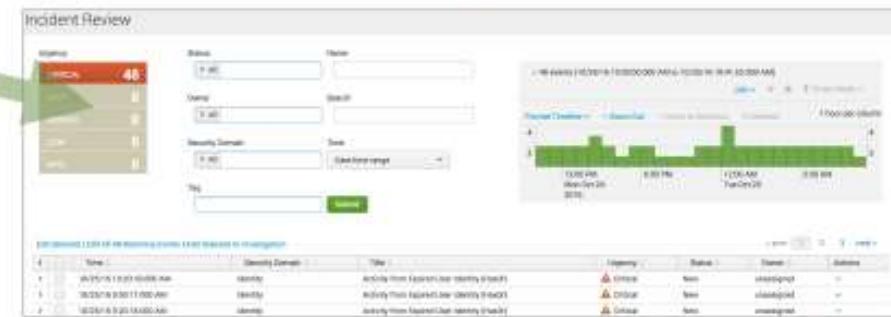
- Each notable event has an **urgency** field, ranging from informational to critical
- Urgency is a combination of two factors:
  - Severity of the incident, as determined by the correlation search
  - Priority of the associated assets or identities—i.e., the server or user
- Severity is based on the 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



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 options

Urgency	Count
Critical	48
High	1011
Medium	647
Low	446
Info	0

Urgency

Status  Name

Owner  Search

Security Domain  Time

Duration

Tag

Timeline & job controls  
✓ 2,152 events (1)  

Job Mode Smart Mode  
Format Timeline Zoom Out Zoom to Selection X Delete 1 hour per column  
450 250 450 250  
12:00 PM Mon Oct 24 6:00 PM 12:00 AM Tue Oct 25 6:00 AM

Sortable column headers

[Edit Selected](#) | [Edit All 2152 Matching Events](#) | [Add Selected to Investigation](#)

[prev](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

#	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	10/25/16 10:45:13.000 AM	Endpoint	Host With A Recurring Malware Infection (SENSITIVE-DATA Credit Card Numbers On 94.229.0.20)	Medium	New	unassigned	<input type="button" value="▼"/>
>	10/25/16 10:45:12.000 AM	Endpoint	Host With Old Infection Or Potential Re-Infection (JAVA_EXPL_AI On YEL-PC)	Medium	New	unassigned	<input type="button" value="▼"/>
>	10/25/16 10:45:10.000 AM	Endpoint	Host With A Recurring Malware Infection (SENSITIVE-DATA Credit Card Numbers On 201.3.120.132)	Medium	New	unassigned	<input type="button" value="▼"/>
>	10/25/16 10:45:09.000 AM	Endpoint	Host With Old Infection Or Potential Re-Infection (JAVA_EXPL_AI On YEL-PC)	High	New	unassigned	<input type="button" value="▼"/>
>	10/25/16 10:45:09.000 AM	Endpoint	Host With Old Infection Or Potential Re-Infection (JAVA_EXPL_AI On YEL-PC)	Medium	New	unassigned	<input type="button" value="▼"/>

Notable events

Click to expand details

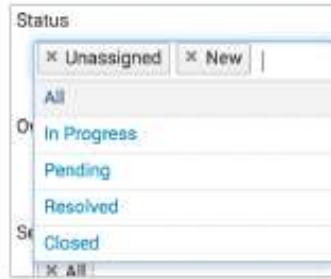
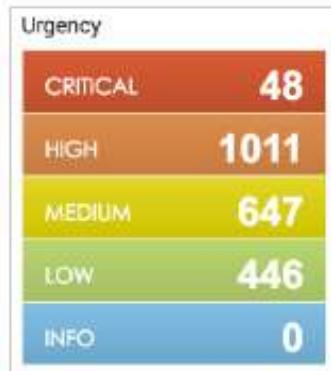
Actions menu

# 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 ORed 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 ANDed 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

10/25/16 10:45:13.000 AM Endpoint Host With A Recurring Malware Infection (SENSITIVE-DATA Credit Card Numbers On 94.229.0.20) Medium New unassigned

Description:  
The device 94.229.0.20 was detected with malware 'SENSITIVE-DATA Credit Card Numbers' that has been detected as active for 4 days in a row. AV has successfully removed the infection each time but the system is continually reinfected; this may indicate the presence of another form of malware is on the system that is prompting the download of 'SENSITIVE-DATA Credit Card Numbers'.

Additional Fields	Value	Action
Destination	94.229.0.20 <span style="background-color: red; color: white; padding: 2px 5px;">240</span>	▼
Destination Expected	false	▼
Destination PCI Domain	untrust	▼
Destination Requires Antivirus	false	▼
Destination Should Time	false	▼
Synchronize		▼
Destination S...		▼
Signature		▼

All fields for the notable event, with action menus for each field  
(pii)

Risk Score

Correlation Search:  
[Endpoint - Recurring Malware Infection - Rule](#)

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

Contributing Events:  
[View related 'SENSITIVE-DATA Credit Card Numbers' events](#)

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2016-10-25T10:45:10-0700	admin	✓ success
Risk Analysis	saved	2016-10-25T10:45:10-0700	admin	✓ success

[View Adaptive Response Invocations](#)

Next Steps:  
i No Next Steps defined.

Notes  
You can't expand an event until the search is complete. Not all incidents have all the same detail items.

Add Event to Investigation  
Create notable event  
Build Event 1  
Extract Fields  
Run Adaptive Response Actions  
Share Notable Event  
Suppress Notable Events  
Show Source

# 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

The screenshot shows a Splunk search results page. A specific field, 'Risk score', is highlighted with a yellow background and a red border. To the right of this field is a vertical action menu. The menu items are:

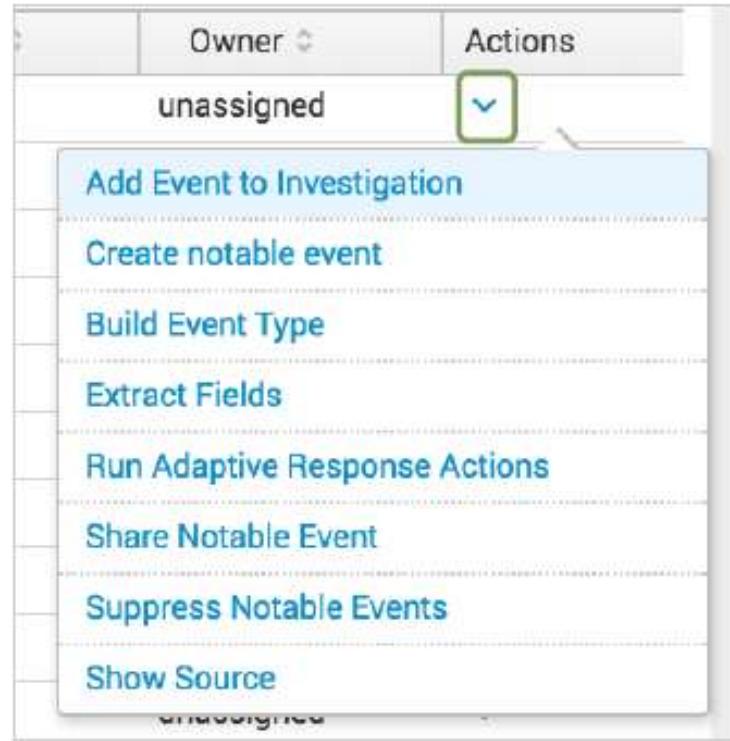
- Edit Tags
- Access Search (as destination)
- Access Search (as source)
- Asset Center** (highlighted with a mouse cursor)
- Asset Investigator
- Domain Dossier
- Map 25.246.33.128
- Google 25.246.33.128
- Intrusion Search (as destination)
- Intrusion Search (as source)

Below the action menu, there is a note box with the following text:

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



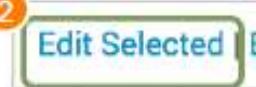
# Incident Workflow: Concepts

---

- 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

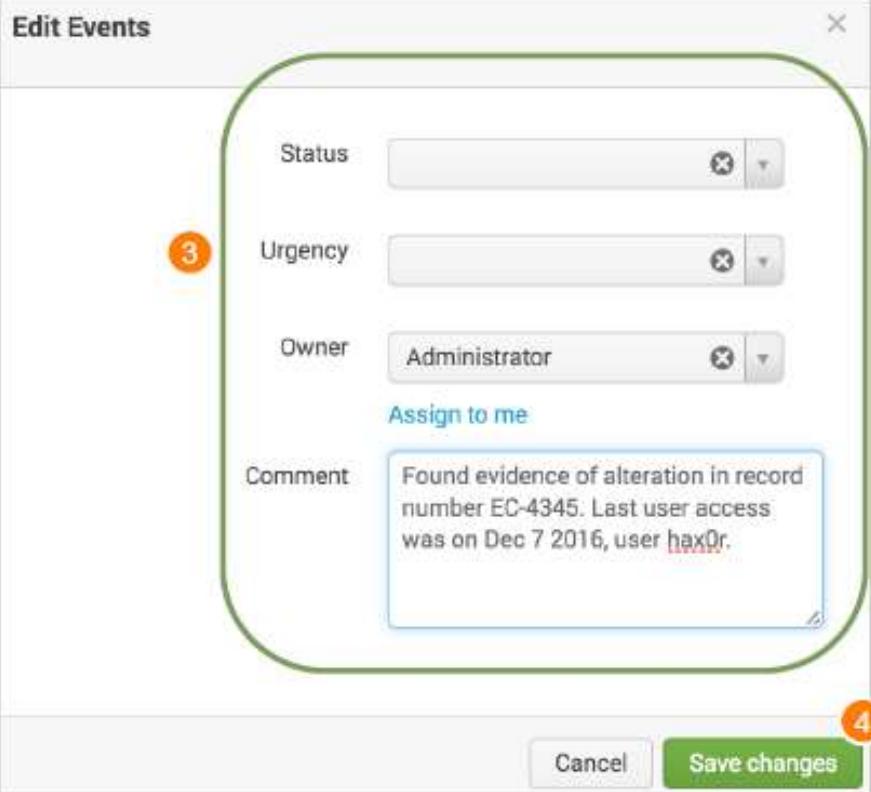
# Incident Workflow: Procedures

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



2

i	<input type="checkbox"/>	Time
1	<input checked="" type="checkbox"/>	10/27/15 3:10:28.000 PM
>	<input type="checkbox"/>	10/27/15 3:10:28.000 PM
>	<input type="checkbox"/>	10/27/15 3:10:28.000 PM



3

4

Cancel Save changes

Edit Events

Status

Urgency

Owner

Administrator

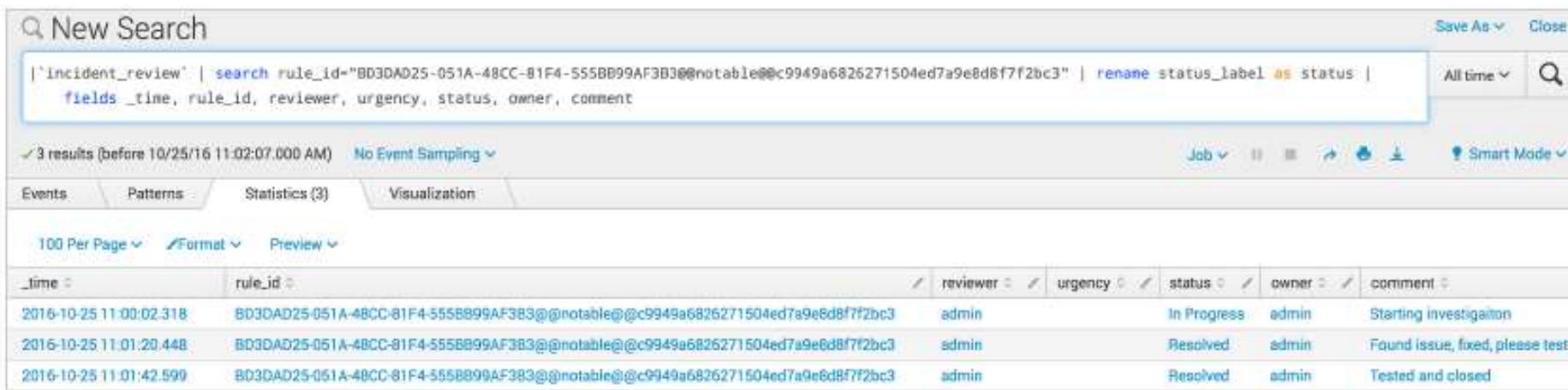
Assign to me

Comment

Found evidence of alteration in record number EC-4345. Last user access was on Dec 7 2016, user hax0r.

# 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



The screenshot shows a Splunk search interface titled "New Search". The search bar contains the query: `|`incident\_review` | search rule\_id="BD3DAD25-051A-48CC-81F4-555BB99AF3B3@notable@@c9949a6826271504ed7a9e8d8f7f2bc3" | rename status\_label as status | fields \_time, rule\_id, reviewer, urgency, status, owner, comment`. The results pane shows 3 results from before October 25, 2016, at 11:02:07 AM. The results are:

_time	rule_id	reviewer	urgency	status	owner	comment
2016-10-25 11:00:02.318	BD3DAD25-051A-48CC-81F4-555BB99AF3B3@notable@@c9949a6826271504ed7a9e8d8f7f2bc3	admin		In Progress	admin	Starting investigation
2016-10-25 11:01:20.448	BD3DAD25-051A-48CC-81F4-555BB99AF3B3@notable@@c9949a6826271504ed7a9e8d8f7f2bc3	admin		Resolved	admin	Found issue, fixed, please test
2016-10-25 11:01:42.599	BD3DAD25-051A-48CC-81F4-555BB99AF3B3@notable@@c9949a6826271504ed7a9e8d8f7f2bc3	admin		Resolved	admin	Tested and closed

# 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.

The screenshot shows a software interface for managing a notable event. At the top, there's a header with 'Urgency: Critical', 'Status: New', and 'Owner: Unassigned'. Below the header is a 'Actions' dropdown menu with several options: 'Add Event to Investigation', 'Create notable event', 'Build Event Type', 'Extract Fields', 'Run Adaptive Response Actions' (which is highlighted with a green box), 'Share Notable Event', 'Suppress Notable Events', and 'Show Source'. Underneath the menu, there's a section titled 'Adaptive Responses:' which contains a table with two rows. The table has columns for 'Response', 'Mode', 'Time', 'User', and 'Status'. The first row shows a 'Notable' response saved at 2016-10-26T13:55:16-0700 by 'admin' with a success status. The second row shows a 'Risk Analysis' response saved at the same time by 'admin' with a success status. Below the table is a link 'View Adaptive Response Invocations'. At the bottom, there's a 'Next Steps:' section with a button labeled 'risk ping'.

Response	Mode	Time	User	Status
Notable	saved	2016-10-26T13:55:16-0700	admin	✓ success
Risk Analysis	saved	2016-10-26T13:55:16-0700	admin	✓ success

# 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

Select actions to run.

+ Add New Response Action

Category All

Show only recommended actions

 Stream Capture	Creates stream capture	Category: Information Gathering   Task: create   Subject: network.capture   Vendor: Splunk
 Nbtstat	Runs the nbtstat command	Category: Information Gathering   Task: scan   Subject: device   Vendor: Operating System
 Nslookup	Runs the nslookup command	Category: Information Gathering   Task: scan   Subject: device   Vendor: Operating System
 Ping	Runs the ping command	Category: Information Gathering   Task: scan   Subject: device   Vendor: Operating System
 Risk Analysis	Creates risk modifier events in the risk index	

# 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

The screenshot shows the 'Select actions to run' interface. A 'Ping' action is selected, with the 'Host Field' set to 'dev'. Below it, a table lists three adaptive responses:

Response	Mode	Time	User	Status
Risk Analysis	saved	2016-10-27T10:55:17-0700	admin	✓ success
Notable	saved	2016-10-27T10:55:16-0700	admin	✓ success
Ping	adhoc	2016-10-27T04:01:57-0700	analyst	⚠ failure

# Tagging Incidents

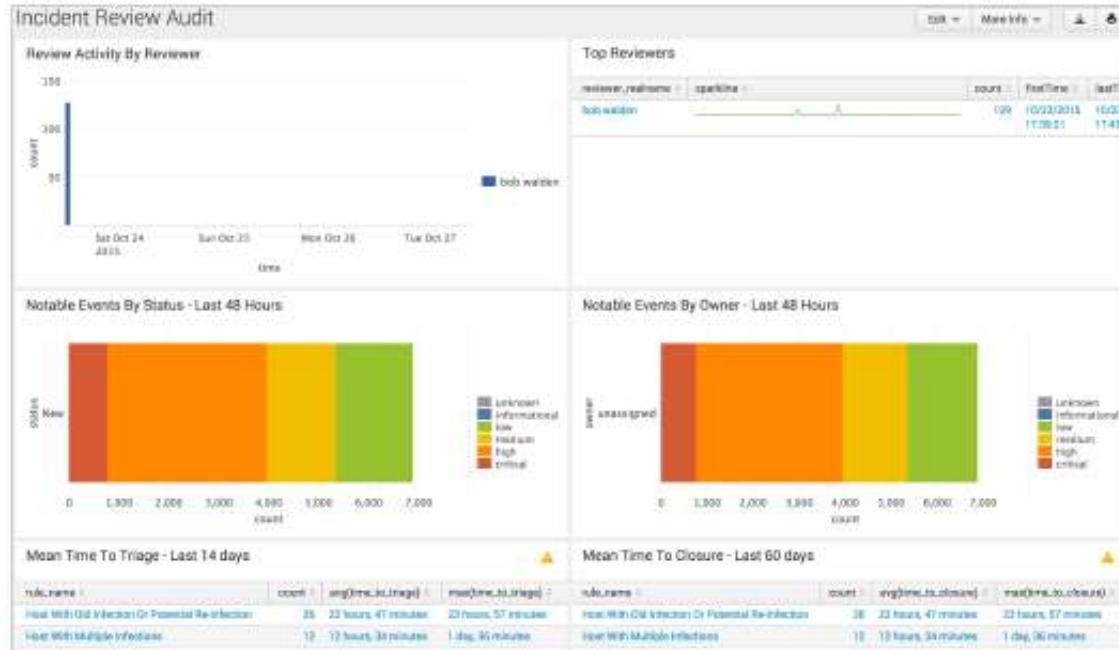
- You can use tags as a method to track significant incidents
  - Example: you want to be able to quickly find all the incidents related to servers being used by project “whammo”
- Add a tag to each server (using the action menu for the **dest**, **src** or **ip** fields in this example) and then search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

The screenshot shows a software interface for managing incidents. At the top, there is a table with columns for 'Description', 'Additional Fields', 'Value', and 'Action'. The 'Description' row contains the text: 'The device ACME-004 is accepting insecure or cleartext win:remote authentication'. The 'Additional Fields' section lists various destination-related fields like Destination Business Unit, Destination Category, Destination City, etc. A green box highlights the 'Edit Tags' button next to the 'Value' column for the 'win:remote (remote)' entry.

A modal dialog box titled 'Create Tags' is open in the foreground. It has two input fields: 'Field Value' containing 'dest=ACME-004' and 'Tag(s)' containing 'whammo'. A green arrow points from the 'Edit Tags' button in the main interface to the 'Tag(s)' input field in the dialog. Below the input fields is a placeholder text: 'Comma or space separated list of tags'. At the bottom of the dialog are 'Cancel' and 'Save' buttons.

# 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

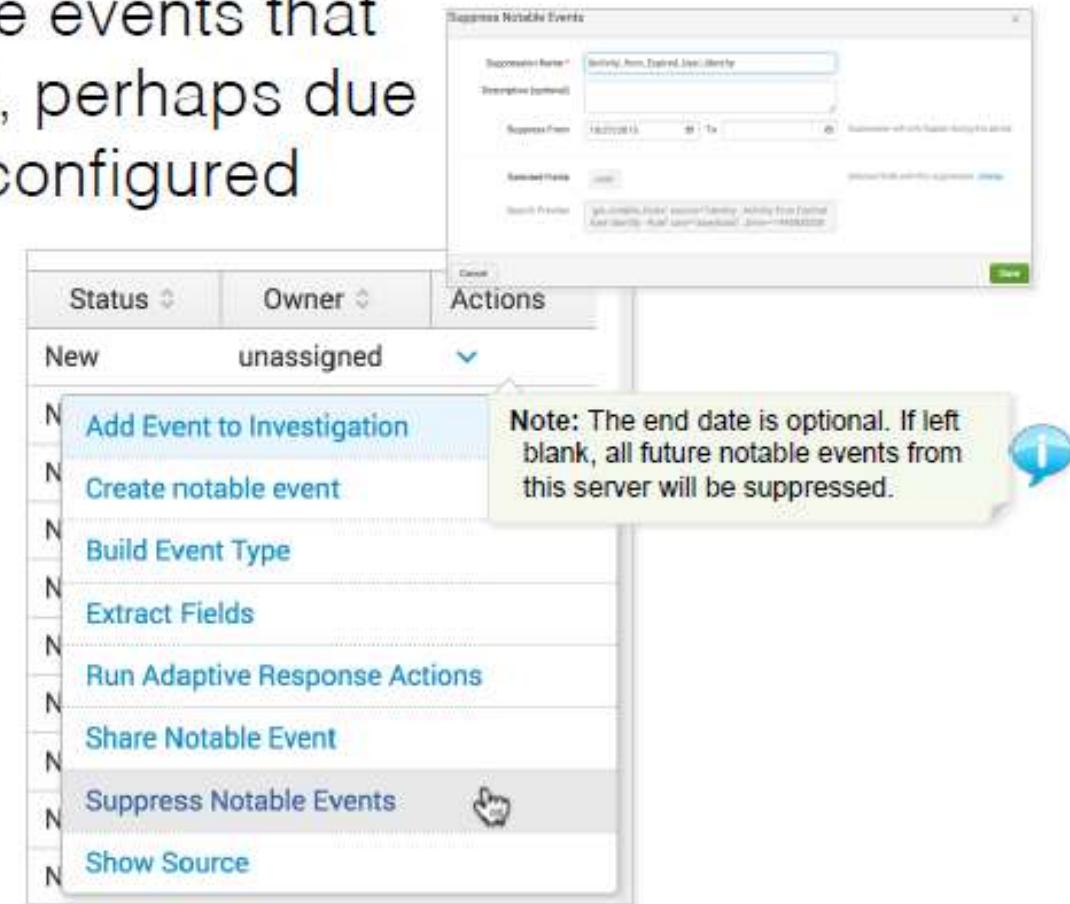
The screenshot shows a modal dialog box for creating a notable event. The fields are as follows:

- Title: Suspicious activity
- Domain: Access
- Urgency: Medium
- Owner: analyst
- Status: In Progress
- Description: Investigate!

At the bottom right are two buttons: "Cancel" and "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

Notable Event Suppressions					<a href="#">Create New Suppression</a>
<a href="#">Back to ES Configuration</a>		Description	Start Time	Expiration Time	Status
	Activity_from_Expired_User_Identity		Fri May 06 2016 00:00:00 GMT-0700 (PDT)		Enabled   Disable
	Host_With_Old_Infection_Or_Potential_Re-Infection		Fri May 13 2016 00:00:00 GMT-0700 (PDT)	Wed Nov 16 2016 00:00:00 GMT-0800 (PST)	Enable   Disabled
Showing 1 to 2 of 2 entries					
<a href="#">← Previous</a>		1	<a href="#">Next →</a>		



## 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

My Investigations

Track and manage investigations

Click to edit investigation name

Create New Investigation

1 Investigation Edit Selection Time: All Filter Filter by time or text Add investigations

<input type="checkbox"/>	Timeline	Last Modified Time:	Creation Time:	Actions
<input type="checkbox"/>	Breach in payment processing system	Oct 27, 2015 12:31 PM	Oct 27, 2015 12:23 PM	Edit   Remove

Click to edit

Lists all investigations

# Investigation List View

## Breach in payment processing system

Looks like some PII has been exfiltrated from the payment system.

[◀ Back to My Investigations](#)

Add items to the investigation timeline

Create New Entry ▾

Choose which items to view

Timeline

List

Type: All ▾

Filter

Add or remove collaborators



Edit Selection ▾

	Time	Title	Type	Actions
<input type="checkbox"/>	27 October 2015 12:21	Dashboard viewed: incident_review	Action History	<a href="#">View</a>   Remove
<input type="checkbox"/>	27 October 2015 12:24	Initial report	Note	<a href="#">Edit</a>   Remove
<input type="checkbox"/>	27 October 2015 12:26	Notable Event (Host:   Sourcetype: stash)	Notable Event	<a href="#">Remove</a>
<input type="checkbox"/>	27 October 2015 12:07	Search executed	Action History	<a href="#">Replay</a>   Remove
<input type="checkbox"/>	27 October 2015 12:30	Summary	Note	<a href="#">Edit</a>   Remove

Showing 1 to 5 of 5 entries

Items can be edited or removed

Previous 1 Next →

Toggle timeline or 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

The screenshot shows a digital investigation interface with the following elements:

- Title:** Breach in payment processing system
- Text:** Looks like some PII has been exfiltrated from th
- Backlink:** < Back to My Investigations
- Buttons:** Timeline, List, Type: All
- Section:** Edit Selection
- Table:** A table with columns for checkbox and Time, listing several entries from 27 October 2015.
- Modal:** Found data file collecting account numbers
  - Date: 9 May 2016 11:37
  - Attachment button
  - Description: on host PAYSYS25, /var/temp/accounts.txt, seems to be collecting account numbers from customer accounts and caching for later FTP to external sites.
  - Attached example. 2
  - A yellow callout bubble contains the text: Fill in fields; time defaults to now but can be modified; use attachment button to add attachments.
- Buttons at the bottom:** All Notes, Save for Later, Add to Investigation 3
- Right sidebar:**
  - Create New Entry
  - 1 Note
  - Action History
  - Actions:
    - View | Remove
    - Edit | Remove
    - Remove
    - Reply | Remove
    - Edit | Remove

# Example: Adding Action History Items

Breach in payment system

Looks like some PII has been exfiltrated.

< Back to My Investigations

Timeline List Type

Edit Selection

Time	Action	Type
27 October 2015 12:17	ssl_activity	Dashboard Viewed
27 October 2015 12:15	dns_activity	Dashboard Viewed
27 October 2015 12:14	generic_protocols	Dashboard Viewed
27 October 2015 12:10	predictive_analytics	Dashboard Viewed
27 October 2015 12:10	threat_artifacts	Dashboard Viewed
27 October 2015 12:09	threat_activity	Dashboard Viewed
27 October 2015 12:08	access_anomalies	Dashboard Viewed
27 October 2015 12:07	reverse_identity_lookup("Hax0r")	Search Run
27 October 2015 12:07	reverse_identity_lookup("Hax0r")	Search Run
27 October 2015 12:07	user_activity	Dashboard Viewed

Cancel

Create New Entry - Action History

Add action history entries to the investigation

Time: Last 24 hours Type: All Filter

Prev 1 2 3 4 5 Next >

Time	Action	Type
27 October 2015 12:17	ssl_activity	Dashboard Viewed
27 October 2015 12:15	dns_activity	Dashboard Viewed
27 October 2015 12:14	generic_protocols	Dashboard Viewed
27 October 2015 12:10	predictive_analytics	Dashboard Viewed
27 October 2015 12:10	threat_artifacts	Dashboard Viewed
27 October 2015 12:09	threat_activity	Dashboard Viewed
27 October 2015 12:08	access_anomalies	Dashboard Viewed
27 October 2015 12:07	reverse_identity_lookup("Hax0r")	Search Run
27 October 2015 12:07	reverse_identity_lookup("Hax0r")	Search Run
27 October 2015 12:07	user_activity	Dashboard Viewed

3 Add to Investigation

Create New Entry Note

1 Action History

+ bw A

Actions

View | Remove

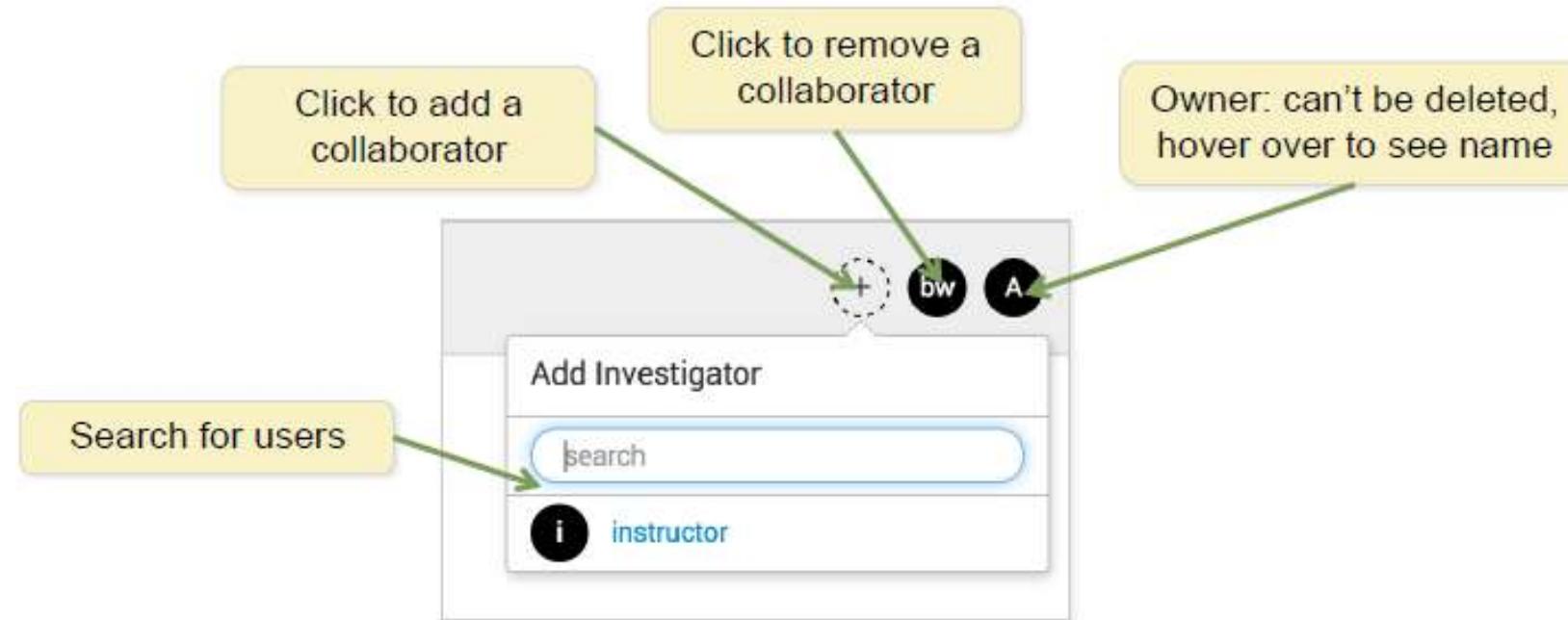
Edit | Remove

Remove

Replay | Remove

Edit | Remove

# Adding Collaborators



Only the owner and collaborators can work on an investigation

# Timeline View



# Investigation Bar

The screenshot shows the 'All Investigations' interface. A yellow box labeled 'Selector' highlights the investigation title 'POS breach'. A green arrow points from this title to a yellow button labeled 'Open investigation selector'. Another green arrow points from the 'POS breach' title to a yellow button labeled 'Create a new investigation'. A third green arrow points from the 'POS breach' title to a yellow button labeled 'Toggle timeline view'. In the top right corner of the interface, there are four small icons: a magnifying glass (Quick search), a plus sign (Add a note), a checkmark (Add action history items), and a circular arrow (refresh).

All Investigations

Events | Add Selected to Investigation

Security Domain	Title	Urgency	Status	Owner	Actions
Identity	Activity from Expired User Identity (Hax0r)	Critical	New	unassigned	▼
Endpoint	Host With Malware Detected	High	New	unassigned	▼
Identity	User Identity (aseykoski)	High	New	unassigned	▼
Identity	User Identity (aseykoski)	High	New	unassigned	▼
Identity	Activity from Expired User Identity (cargento)	High	New	unassigned	▼
Threat	Threat Activity Detected (25.108.23.204)	Low	New	unassigned	▼
Threat	Threat Activity Detected (25.22.163.129)	Low	New	unassigned	▼
Threat	Threat Activity Detected (25.252.15.82)	Low	New	unassigned	▼

POS breach

Open investigation selector

Create a new investigation

Toggle timeline view

Quick search

Add a note

Add action history items

# Inline Timeline View

Incident Review

Urgency

CRITICAL	398
HIGH	1390
MEDIUM	678
LOW	1056
INFO	0

Status

Name

Owner

Search

Security Domain

Time

Last 24 hours

Tag

Submit

3,522 events (10/26/15 10:00:00.000 PM to 10/27/15 10:19:36.000 PM)

Format Timeline ▾ Zoom Out +Zoom to Selection Deselect 1 hour per column

12:00 AM Tue Oct 27 2015

12:00 PM

5:00 PM

Edit Selected | Edit All 3522 Matching Events | Add Selected to Investigation

I	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	10/27/15 10:18:45.000 PM	Identity	Activity from Expired User Identity (joy_rence@bankofvulcan.com)	Medium	New	unassigned	...
>	10/27/15 10:18:04.000 PM	Identity	Activity from Expired User Identity (Hax0r)	Critical	New	unassigned	...
>	10/27/15 10:17:43.000 PM	Identity	Activity from Expired User Identity (breach@alarmatech.com)	Critical	New	unassigned	...

prev 1 2 3 4 5 6 7 8 9 10 next

Toggle timeline view

Dashboard viewed: Incident Review

12:18 PM 12:19 PM 12:20 PM 12:21 PM 12:22 PM 12:23 PM 12:24 PM

= + Breach in payment processing system

# Adding Events

The screenshot shows a web-based interface for managing security events. At the top, there are buttons for "Edit Selected", "Edit All 2105 Matching Events", and "Add Selected to Investigation". A green box highlights the "Add Selected to Investigation" button.

The main area displays a list of events with columns for ID, Time, Security Domain, Title, Urgency, Status, Owner, and Actions. The "Actions" column includes options like "Add Event to Investigation", "Create notable event", "Build Event Type", "Extract Fields", "Run Adaptive Response Actions", "Share Notable Event", "Suppress Notable Events", and "Show Source". A green arrow points from the "Add Selected to Investigation" button to the "Add Event to Investigation" option in the "Actions" column.

A yellow callout box contains the text "Add notable events from incident review..." and points to the "Create notable event" option in the "Event Actions" dropdown menu. Another yellow callout box contains the text "...or add source events from search result window" and points to the "Add Event to investigation" option in the same dropdown menu. The "Event Actions" dropdown also includes "Build Event Type", "Extract Fields", and "Show Source".

At the bottom left, there are two dropdown menus: "COMPID" and "DESTIP", each with a "Value" field containing "127.0.0.1". To the right of these dropdowns, there is some log-like text:

```
10/28/15 <msg time='2015-10-27T22:25:43.751-07:00' org_id='oracle' comp_id='tnslsnr' 1  
5:25:43.751 AM 1GR2-WIN host_addr='fe80::504d:ddb3:9bbb:18c2%12'><txt>29-OCT-2014 19:44:54  
T=__jdbc__(USER=ORACLE11GR2-WIN$)(SEP  
88) * establish * orcl.11g.win * 1251
```

# Quick Search

The screenshot shows the Splunk Quick Search interface. A yellow callout box labeled "Run search" points to the search bar where "snort" is typed. The search results table has columns for i, Time, and Event. Two events are listed:

i	Time	Event
>	May 06 21:25:30 2016 2:25:30.000 PM	snort.acmetech.com May 06 20:30:30 itsec snort[18774]: [1:3486:3] WEB-MISC SSLv3 invalid data version attempt [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} 10.150.20.61:45346 -> 192.168.1.12:443 host = ip-10-27-129-235 source = /opt/splunk/var/spool/splunk/sample.snort sourcetype = snort
>	May 06 21:25:23 2016 2:25:23.000 PM	snort.acmetech.com May 06 20:52:41 itsec snort[18774]: [1:882:6] WEB-CGI calendar access [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 10.157.120.61:55369 -> 192.168.1.101:80 host = ip-10-27-129-235

A green button labeled "Add to Investigation" is located at the bottom right of the results table. A yellow callout box labeled "Click quick search icon" points to the magnifying glass icon in the bottom right corner of the search bar. Another yellow callout box labeled "Add search to investigation" points to the "Add to Investigation" button.



## 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

---

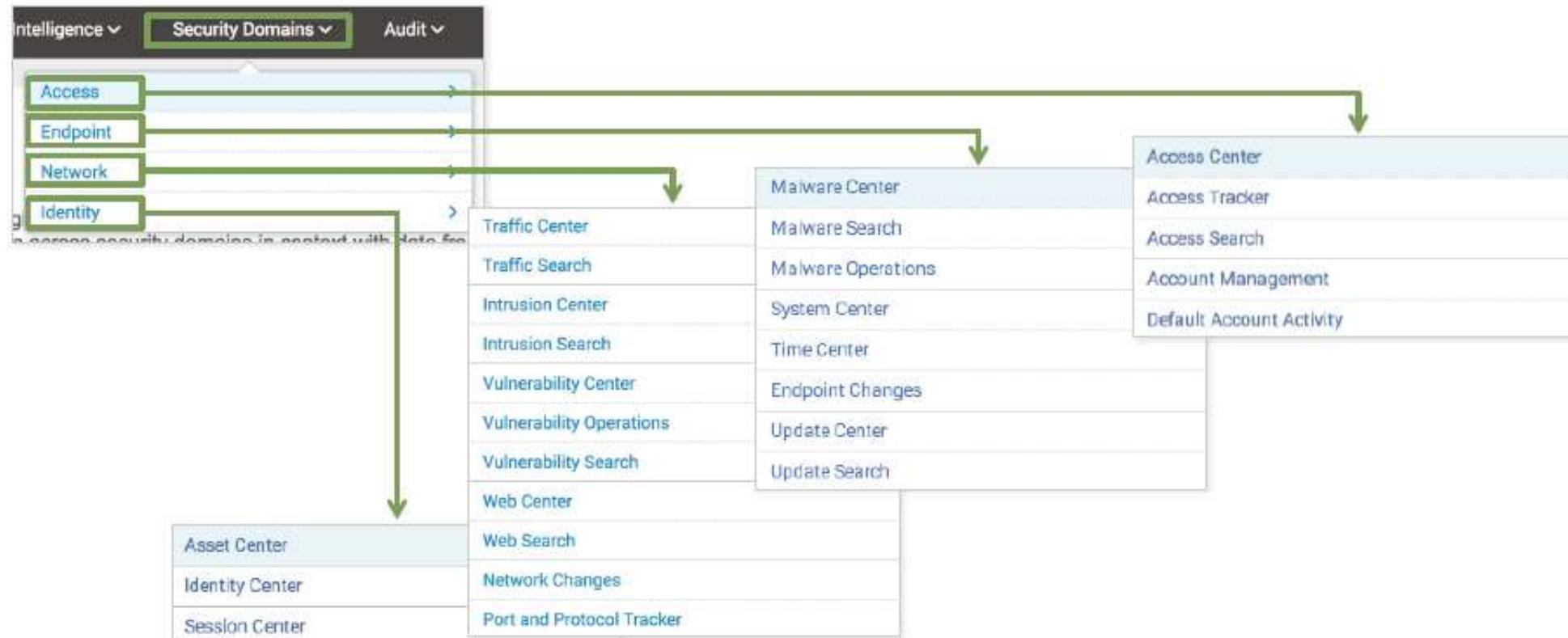
- When a breach occurs, you need to examine the details related to the incident to determine a root cause and eliminate the risk
- The domain dashboards in ES provide the necessary tools to examine related log and stream data in depth
- You can also use these dashboards as part of a periodic security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

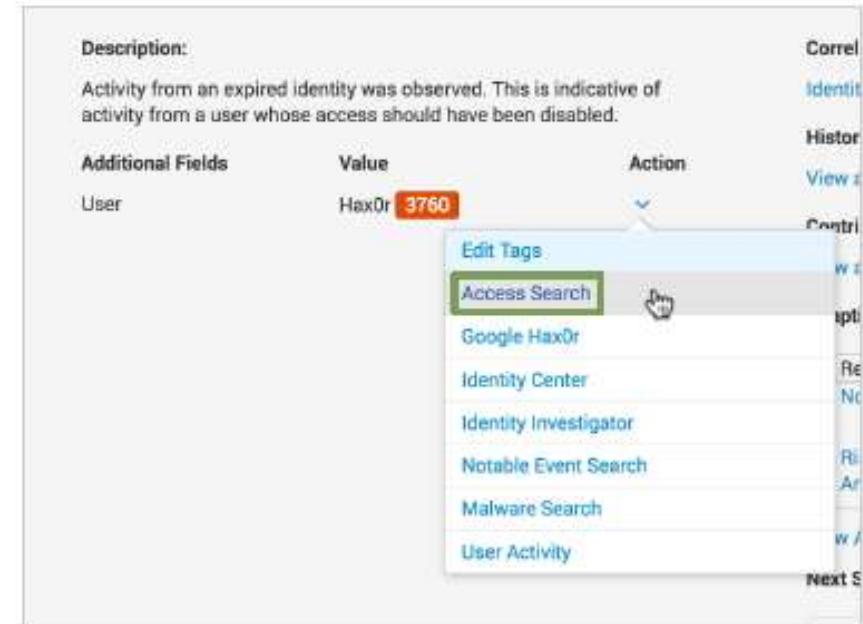
---

- 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 Search

Action: All App: All Source: Destination: User: Hax0r Last 7 days: Submit

Show Filters

time	action	app	src	src_user	dest	user	count
2016-10-28 10:24:59	failure	winlocal	10.11.36.20	ACMEDC018	HOST-001	Hax0r	6152

Time	Event
10/28/16 10:24:59 AM	10/28/2016 05:24:59 PM LogName=Security EventCode=529 EventType=16 Type=Failure Audit <a href="#">Show all 28 lines</a> action = failure failure app = winlocal local dest = HOST-001 src = 10.11.36.20 src_user = ACMEDC018 user = Hax0r
10/28/16 10:24:50.000 AM	10/28/2016 05:24:50 PM LogName=Security EventCode=529 EventType=16 Type=Failure Audit <a href="#">Show all 28 lines</a> action = failure failure app = winlocal local dest = HOST-001 src = 10.11.36.20 src_user = ACMEDC018 user = Hax0r

# 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

The screenshot displays the Access Center dashboard with various filtering and monitoring features.

**Top Filter Bar:** This bar contains five dropdown menus for filtering: Action (set to All), App (set to All), Business Unit (empty), Category (empty), and Special Access (empty). Below these is a time range selector set to "Last 24 hours" and a green "Submit" button.

**Main Dashboard Area:** The main area is titled "Access Center". It includes a toolbar with "Edit", "More Info", and other icons. Below the toolbar is another set of five dropdown menus for filtering: Action (All), App (All), Business Unit (empty), Category (empty), and Special Access (empty). A "Last 24 hours" time range selector and a "Submit" button are also present here.

**Metrics Section:** This section contains five cards with real-time data:

- AUTH. APPS**: Distinct Count: 12 (green arrow pointing up, -2)
- AUTH. SOURCES**: Distinct Count: 170 (red arrow pointing up, +39)
- AUTH. DEST'S**: Distinct Count: 5 (green arrow pointing up, -53)
- AUTH. USERS**: Distinct Count: 573 (green arrow pointing up, -139)
- AUTH. ATTEMPTS**: Total Count: extreme (red text, red arrow pointing up, increasing extremely. Currently is: 3W)

# 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

---

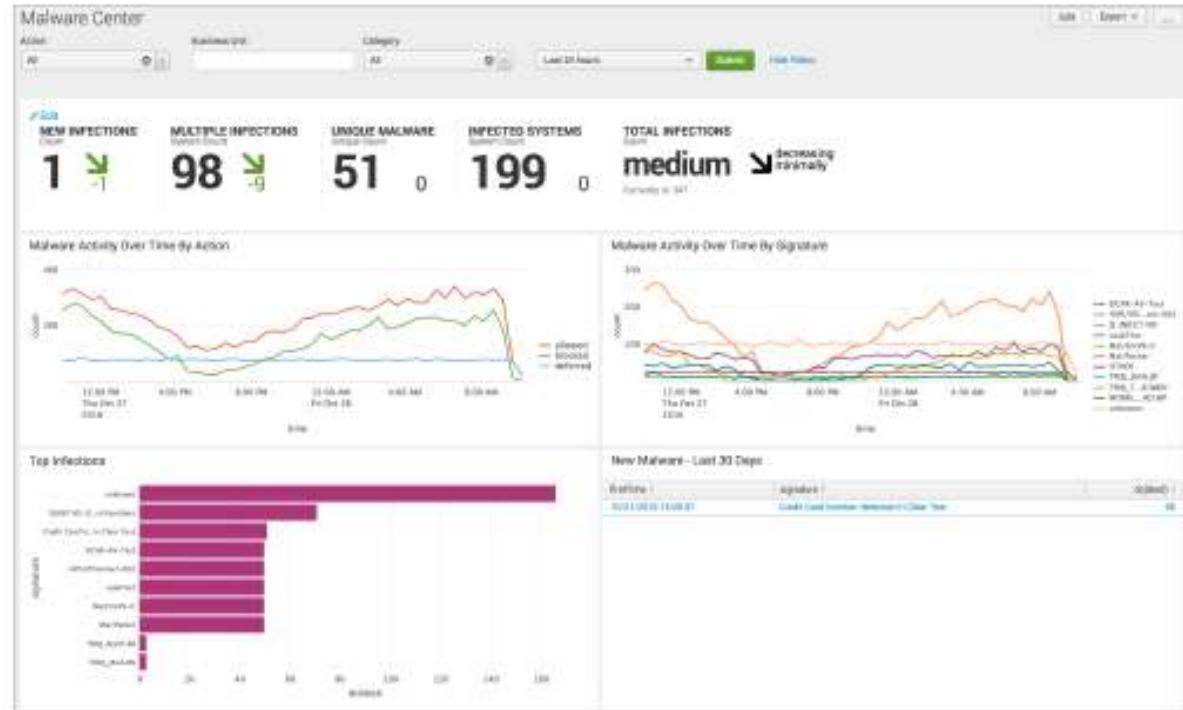
- The endpoint domain watches over your user systems:
  - Workstations, PCs, notebooks, handheld devices, and point-of-sale systems are examples
- Potential issues include:
  - Vulnerabilities: missing updates or patches
  - Malware: spyware, ransomware, or other malicious code
  - Unexpected running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

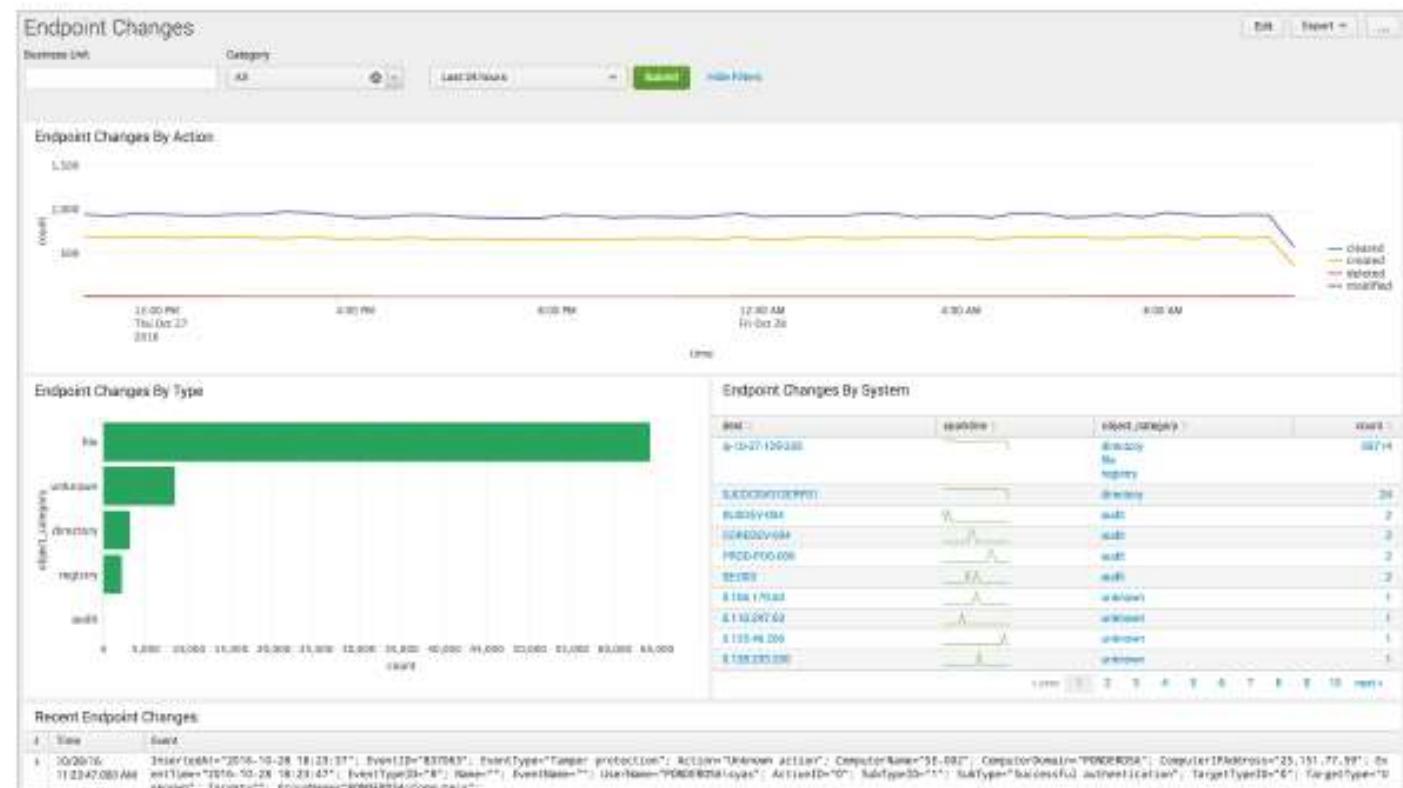
- Click a malware signature on the Malware Center dashboard to drill down to that malware type on the Malware Search dashboard
- This shows all infected systems, helping you identify the scope of the attack and also the origin
  - The first infection should be patient zero

Malware Search

Action	Signature	File	Destination	User	Date time range	Submit	Hide Filters
All	JS_INJECT.VB						
Time:	action:	signature:	file_name:	dest:	user:	count:	
2015-10-28 06:29:50	blocked	JS_INJECT.VB	30A70787d01 Ag4TvxNl.zip.part FedEx_Invoice.xlsx	ACME-12345	unknown	217	
Time	Event						
> 10/28/16 06:29:50 AM	10/28/2016 01:29:50 PM LogName=Application SourceName=Trend Micro OfficeScan Server EventCode=500 EventType=3 Show all 20 items						
action=blocked dest=ACME-12345 file_name=30A70787d01 signature=JS_INJECT.VB user=unknown vendor_product=Trend Micro OfficeScan							

# 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

The screenshot shows the Splunk Time Center interface with three main sections:

- Time Synchronization Failures:** A table showing failed synchronization attempts. One entry is visible: "2015-04-14 13:18:00" with status "Failure".
- Systems Not Syncing:** A table showing systems that are not synchronizing. One entry is visible: "2015-04-14 13:18:00" with status "NotSyncing".
- Indexing Time Delay:** A table showing indexing time delays. It includes columns for host, last\_indexed\_time, min\_difference, avg\_difference, and max\_difference. Several hosts are listed with their respective values.

# 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

---

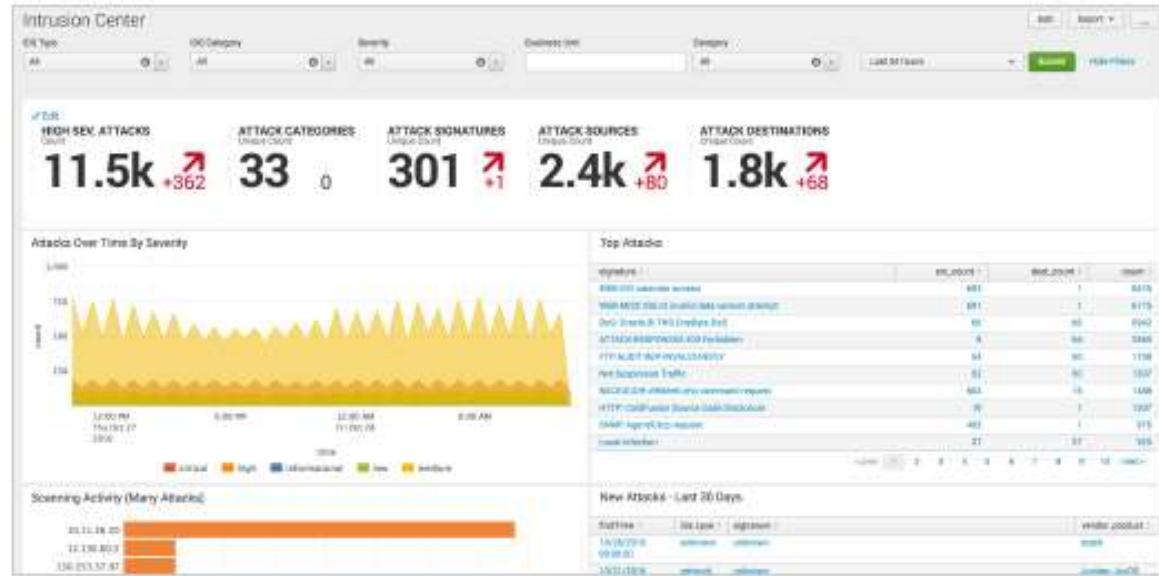
- Many network domain scenarios are preventative in nature:
  - Suspicious activity spotted by intrusion detection systems
  - Vulnerabilities
  - Unusual ports being opened
  - Suspicious DNS activity
  - Port scanning
- Other network analysis tools on the Security Intelligence menu:
  - Protocol Intelligence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

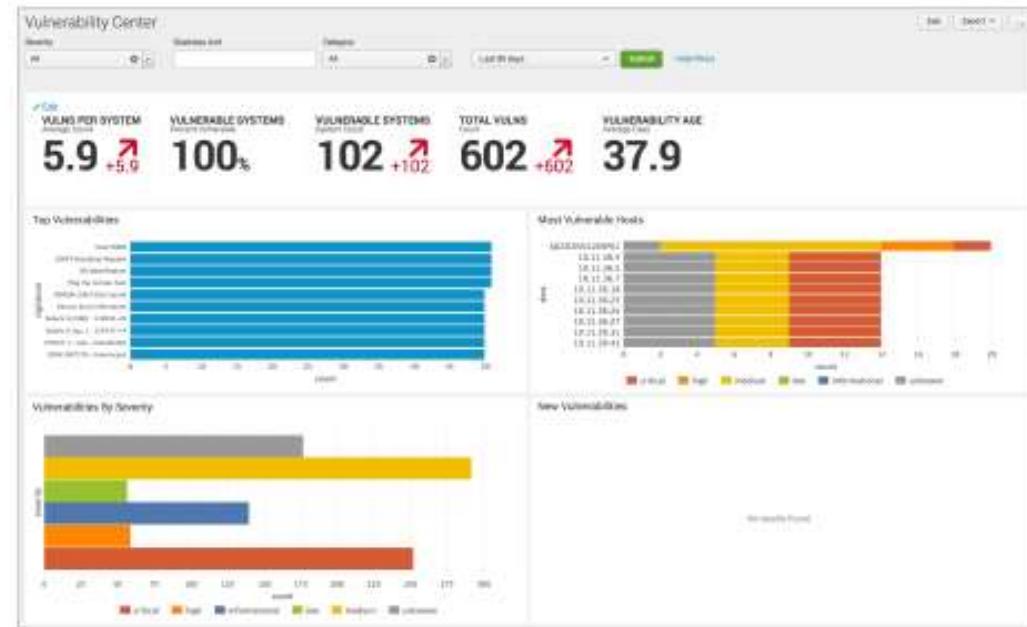
Intrusion Search

IDS Category	Severity	Signature	Source	Destination	Date/time range	Submit	Hide Filters
All	All	DoS: Oracle.9i.TNS.OneByte.DoS	12.130.60.5				
2016-10-28 11:53:02	critical	DoS		12.130.60.5	130.253.37.97	48	
2016-10-28 10:08:10	critical	DoS		12.130.60.5	12.130.60.5	46	
2016-10-28 11:34:43	critical	DoS		12.130.60.5	131.178.233.243	40	
2016-10-28 11:42:58	critical	DoS		12.130.60.5	125.17.14.100	38	
2016-10-28 11:37:59	critical	DoS		12.130.60.5	140.146.8.66	37	

I Time Event  
X 10/28/16 Oct 28 18:56:31 fortinet-01 date=2012-06-05,time=15:20:43,devname=FORTINET-01,device\_id=F6300B3909600791,log\_id=0419015384,type=Ips,subtype=signature,pri=alert,severity=medium,carrier\_ip="N/A",profilegroup="N/A",profiletype="N/A",profile="N/A",src=12.130.60.5,dst=217.132.169.69,src\_int="NON-PCI-MEB",dst\_int="PCI-APP-DB",policyid=302,identidx=0,serial=1260148874,status=detected,proto=6,service=1521/tcp,vd="root",count=1,attack\_name=Oracle.9i.TNS.OneByte.DoS,src\_port=13138,dst\_port=1521,attack\_id=10725,sensor="all\_default\_pass",ref="http://www.fortinet.com/ids/VID10725",user="N/A",group="N/A",incident\_serialno=651335754,msg="DoS: Oracle.9i.TNS.OneByte.DoS",category=DoS,dst\_int=217.132.169.69,dst\_port=1521,severity=critical,signature=DoS: Oracle.9i.TNS.OneByte.DoS,src\_ip=12.130.60.5,src\_port=13138,user=N/A,vendor\_product=Fortinet IPS  
X 10/28/16 Oct 28 18:53:02 fortinet-01 date=2012-06-05,time=21:47:45,devname=FORTINET-01,device\_id=F6300B3909600791,log\_id=0419015384,type=Ips,subtype=signature,pri=alert,severity=medium,carrier\_ip="N/A",profilegroup="N/A",profiletype="N/A",profile="N/A",src=12.130.60.5,dst=130.253.37.97,src\_int="NON-PCI-MEB",dst\_int="PCI-APP-DB",policyid=302,identidx=0,serial=1262157652,status=detected,proto=6,service=1521/tcp,vd="root",count=1,attack\_name=Oracle.9i.TNS.OneByte.DoS,src\_port=13138,dst\_port=1521,attack\_id=10725,sensor="all\_default\_pass",ref="http://www.fortinet.com/ids/VID10725",user="N/A",group="N/A",incident\_serialno=651335754,msg="DoS: Oracle.9i.TNS.OneByte.DoS",category=DoS,dst\_int=130.253.37.97,dst\_port=1521,severity=critical,signature=DoS: Oracle.9i.TNS.OneByte.DoS,src\_ip=12.130.60.5,src\_port=13138,user=N/A,vendor\_product=Fortinet IPS

# 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

Vulnerability Search

Vuln. Category	Severity	Signature	Reference (bugtraq, cert, cve, etc.)	Destination	Date/time range	Submit	Hide Filters
	medium			SJCDCSV012ERP01			
_time	category	severity	signature	cve	dest		count
2016-10-28 11:23:56	unknown	medium	SMB Detection		SJCDCSV012ERP01		638
2016-10-28 11:23:56	unknown	medium	Ping the remote host		SJCDCSV012ERP01		494
2016-10-28 11:23:56	unknown	medium	DCE Services Enumeration		SJCDCSV012ERP01		488
2016-10-28 11:23:56	unknown	medium	Host FQDN		SJCDCSV012ERP01		439
2016-10-28 11:23:56	unknown	medium	ICMP Timestamp Request		SJCDCSV012ERP01		420

< prev 1 2 3 next >

#	Time	Event
>	10/28/16 11:23:56.000 AM	start_time="Fri Oct 28 17:29:51 2016" end_time="Fri Oct 28 18:21:41 2016" dest_dns=SJCDCSV012ERP01 dest_nt_host=SJCDCSV012ERP01 dest_mac= dest_ip=10.12.34.56 os="Microsoft Windows 2008 Server R2" dest_port_proto="general" severity_id=2 signature_id=10180 signature="Ping the remote host" category="unknown" dest_n=SJCDCSV012ERP01 dev= unknown severity= medium signature= Ping the remote host
>	10/28/16 11:23:56.000 AM	start_time="Fri Oct 28 17:39:46 2016" end_time="Fri Oct 28 17:36:20 2016" dest_dns=SJCDCSV012ERP01 dest_nt_host=SJCDCSV012ERP01 dest_mac= dest_ip=10.12.34.56 os="Microsoft Windows 2008 Server R2" dest_port_proto="microsoft-ds(445/tcp)" severity_id=2 signature_id=11011 signature="SMB Detection"

# 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

<b>Vulnerability Operations</b>	Statistics on vulnerability aging and scan activity
<b>Network Changes</b>	Events recording changes to network configurations on routers, firewalls, etc.
<b>Port and Protocol Tracker</b>	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

**Risk Analysis**

Source: All Risk Object: All Last 24 hours Save Filters Edit

**Filters**

**Key Risk Indicators**

**Ad-hoc Risk**

**DISTINCT MODIFIER SOURCES** (Source Count) **11** 0

**DISTINCT RISK OBJECTS** (Object Count) **582** +12

**MEDIAN RISK SCORE** Overall Medium Risk **low** no change (delta is zero)  
Currently at 582

**AGGREGATED SYSTEM RISK** Total System Risk **increasing minimally**

**AGGREGATED USER RISK** Total User Risk **medium** no change (delta is zero)  
Currently at 581

**AGGREGATED OTHER RISK** Total Other Risk **medium** no change (delta is zero)  
Currently at 581

**Risk Modifiers Over Time**

Timeline shows most active risk-increasing events

**Risk Score By Object**

Objects with most associated risk

risk_object	risk_object_type	risk_score	events_count	count
00000000000000000000000000000000	User	13200	1	105
00000000000000000000000000000000	User	12900	1	107
00000000000000000000000000000000	Host	10000	1	42
00000000000000000000000000000000	Host	10000	1	10
00000000000000000000000000000000	Host	10000	1	16
00000000000000000000000000000000	System	1200	4	16
00000000000000000000000000000000	System	1100	3	18
00000000000000000000000000000000	System	1100	1	18
00000000000000000000000000000000	System	1100	6	16

**Most Active Sources**

Events causing the most risk

source	risk_score	risk_objects	count
Enforcement - Recurring Malware Infestation - Rule	43000	225	546
Rule - Abnormally High Number of HTTP Method Events By IP - Rule	35000	810	426
Device	1000	1	621
Ident	1000	1	371
Device	1000	1	101
Threat	1000	1	100
Geolocation - High Geolocation Suspicious Device - Rule	4000	31	61
Access - Data Flow Access Behavior Detected - Rule	4000	30	60
Device - High Priority Device With Malware - Rule	1000	10	17
ALARM - Application ALARM Threshold Exceeded - Rule	500	13	13

**Recent Risk Modifiers**

Events affecting risk scores

time	risk_object	risk_object_type	rule
2016-10-29 11:10:20	00000000000000000000000000000000	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).

# 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

Ad-Hoc Risk Score

Score	300
Description	I have a bad feeling about this server
Risk object	HOST-001
Risk object type	system



## 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

---

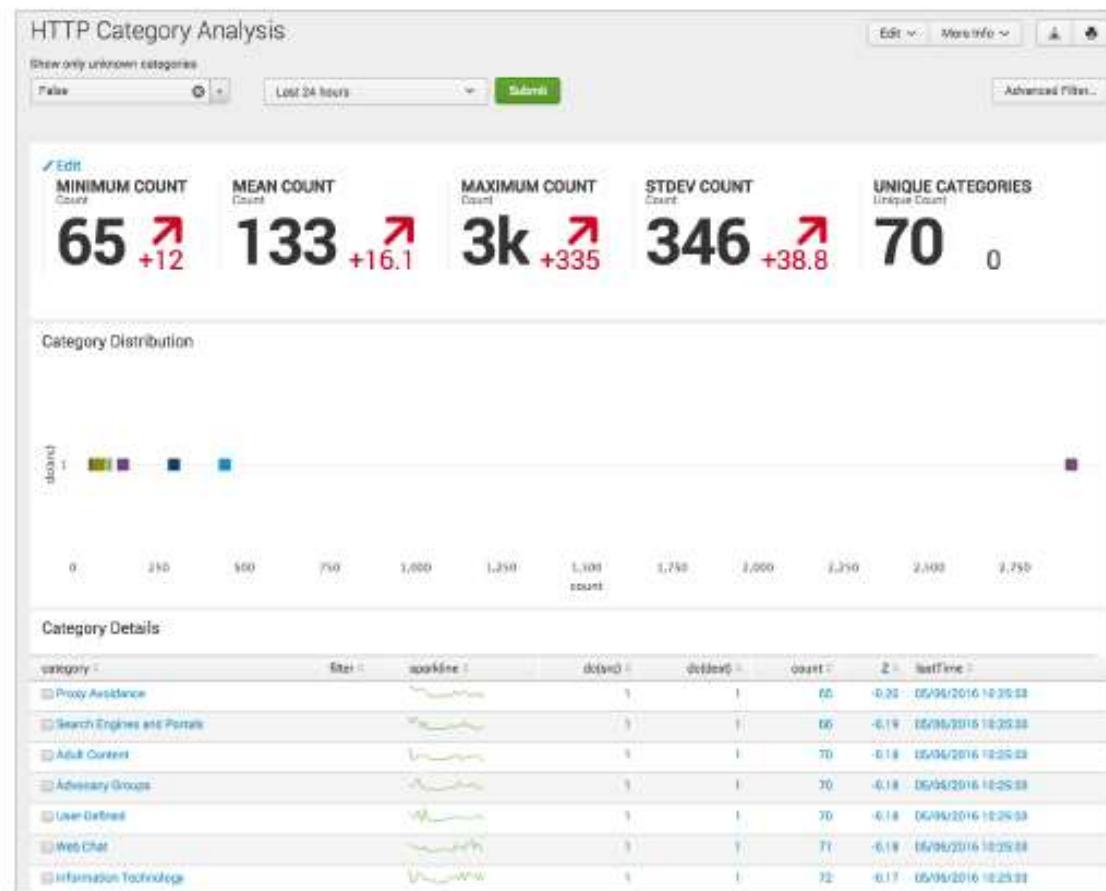
- **HTTP Category Analysis**: look for URLs associated with unwanted behavior
- **HTTP User Agent Analysis** : long or malformed user agent strings can be indicators of malicious activity
- **New Domain Analysis** : high count of new domains can indicate botnet or trojan attacks
- **URL Length Analysis**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

[docs.splunk.com/Documentation/ES/latest/User/  
ThreatListActivitydashboard](https://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](http://www.websense.com/content/support/library/web/v76/siem/siem.pdf)



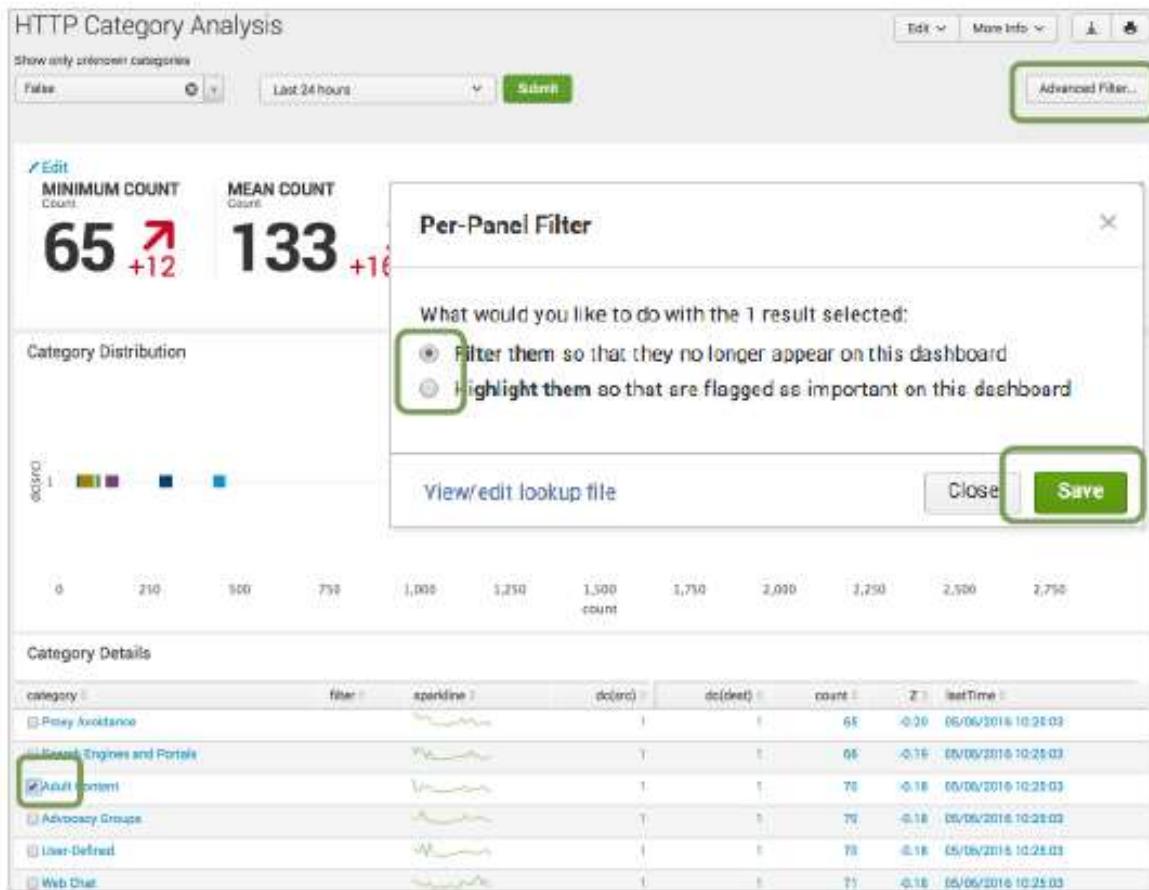
## Per Panel Filter

---

- 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

Category Details		
category	filter	sparkline
<input type="checkbox"/> Adult Content	!	
<input type="checkbox"/> Proxy Avoidance		
<input type="checkbox"/> Search Engines and Portals		
<input type="checkbox"/> Advocacy Groups		

# 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](https://docs.splunk.com/Documentation/ES/latest/User/AdvancedFilter)

The screenshot shows the Splunk 'ES Lookups' configuration page. On the left, a sidebar lists various lookups: Action History, Tracking Whitelist, Administrative Identities, Application Protocols, Asset/Identity Categories, Assets, Cloud Domains, Corporate Email Domains, Corporate Web Domains, Demonstration Assets, Demonstration Identities, ES Configuration Health Filter, Expected Views, and several others. The 'HTTP User Agent Analysis' item is highlighted with a green box and has a green arrow pointing to the 'Edit Lookup' modal.

The main area displays the 'Edit Lookup' modal for the 'ppf\_http\_user\_agent' file. The modal contains a table with five rows of data:

	start_time	end_time	http_user_agent
1	142921846		Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath 1; MS-RTC LM 8; .NET CLR 1.1.4322; .NET C
2	142921846		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
3	142921846		Windows NT 5.1; SV1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath 1; .NET CLR 3.0.4
4	142921846		Windows NT 5.1; SV1; FunWebProducts; .NET CLR 2.0.50727; InfoPath 1; MS-RTC LM 8
5	142921846		iOS X 10.0.3 AppleWebKit/600.1.17 (KHTML, like Gecko) Version/7.1 Safari/537.85.10

A context menu is open over the third row, listing options: Insert row above, Insert row below, Insert column on the left, Insert column on the right, Remove row, Remove column, Links, and Lists. At the bottom of the modal are 'Cancel' and 'Save' buttons.

# 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

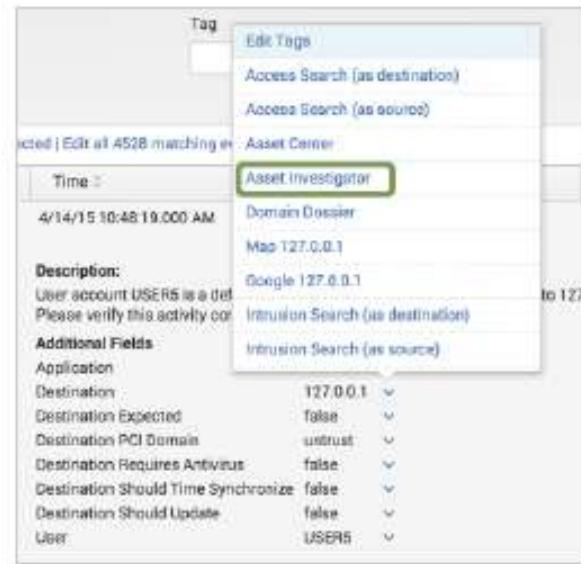
# Asset and Identity Investigators

---

- 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

Asset Investigator

Enter asset name here

acme-004

Search

Information about the asset

acme-004

time: 2016-11-11T12:47:47-0800  
country: UK  
lat: 50.84436  
should\_update: true

is\_expected: false  
nt\_host: ACME-004  
owner: taters  
long: -0.98461

city: Havant  
pol\_domain: wireless\_trust  
priority: high  
should\_timesync: true

category: pol  
requires\_av: true  
bunit: emea

● Edit

All Authentication

All Changes

Threat List Activity

IDS Attacks

Malware Attacks

Notable Events

Risk Modifiers

Today ▾

Swim lanes showing activity across areas

Search returned no results  
05:36:00 AM - 05:45:36 AM  
4 Events

action: allowed  
defect: ACME-004  
signature: EICAR-AV-Test  
Mal/Pecker  
+1 more  
per: PONDEROSA\\tater  
PONDEROSA\\tater  
+2 more

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

12:47:46

Choose time span for search

Area graph at bottom shows activity over time period

Selecting a bar (set of events) shows details at right

Details about the selected events in the swim lane

The screenshot displays the Asset Investigator interface. At the top, there's a search bar with 'Enter asset name here' placeholder text and a dropdown menu showing 'acme-004'. Below the search bar is a 'Search' button. To the right, a box titled 'Information about the asset' contains detailed information for 'acme-004', including its location (Havant, UK), priority (high), and category (pol). The main area features a timeline from 12:00 AM to 12:00 PM. On the left, a sidebar lists categories like All Authentication, All Changes, Threat List Activity, IDS Attacks, Malware Attacks, Notable Events, and Risk Modifiers. A 'Today ▾' button is highlighted with a green box. The timeline shows several colored bars representing different event types. A specific bar for 'Malware Attacks' is selected, and a tooltip shows '4 Events' from '05:36:00 AM - 05:45:36 AM'. To the right of the timeline, a detailed view of these 4 events is shown, listing their action (allowed), defect (ACME-004), signature (EICAR-AV-Test), and source (Mal/Pecker). A note indicates '+1 more' and '+2 more' events. At the bottom, an area graph shows activity over time.

# User Intelligence: Identity Investigator

Identity Investigator

Hax0r  Search Enter identity name here

bunit: americas phone: +1 (800)555-3039 endDate: 3/2/98 22:53	watchlist: true first: Hershel time: 2015-11-11T12:50:21-0800	last: Trapper email: htrapper@acmetech.com priority: critical	prefix: Mr. phone2: +1 (800)555-3154 startDate: 6/15/93 20:07
---	---	---	---

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

- All Authentication
- All Changes
- Threat List Activity
- IDS Attacks
- Malware Attacks
- Notable Events
- Risk Modifiers

Today ▾

Same tools and functionality as the Asset Investigator

All Authentication (25)

Fri Nov 11 Fri Nov 11  
06:36:18 06:50:19 GMT-08:00

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

# 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

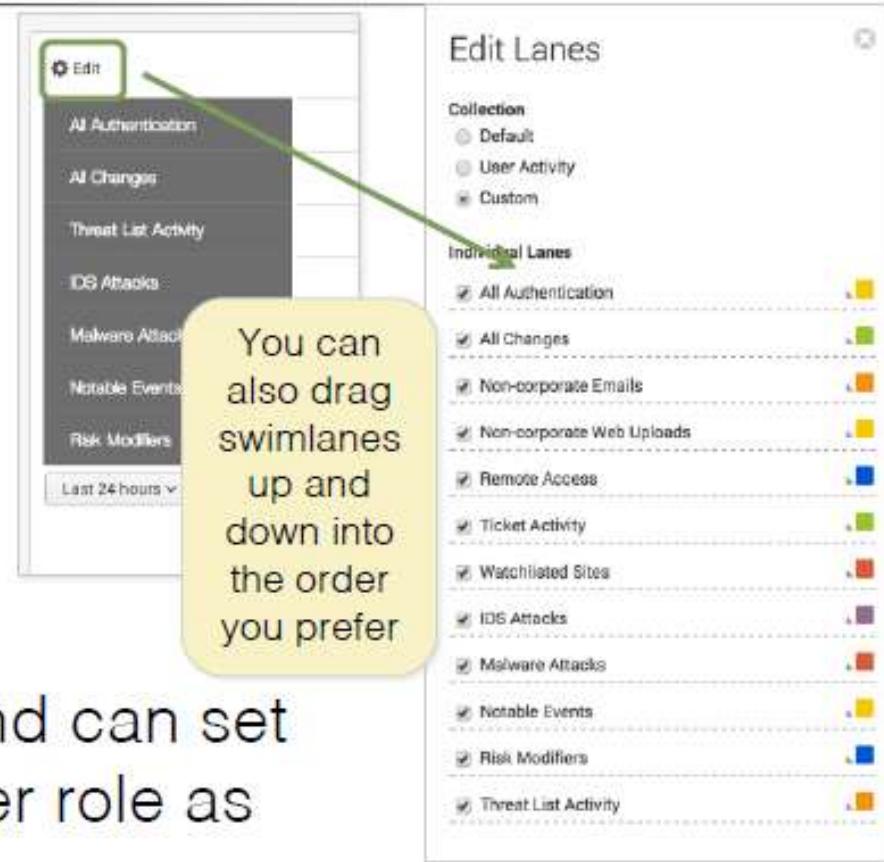
# Pan and Zoom



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

User Business Unit Watchlisted Users All Last 24 hours Submit Hide Filters

**TOTAL HIGH RISK USERS** Count: **6** 0 **TOTAL HIGH RISK USER EVENTS** Count: **376** +18 **NONCORP WEB VOLUME** bytes: **7.3b** +119.8m **NONCORP EMAIL VOLUME** bytes: **1.6m** +26.2k **WATCHLISTED WEBSITES** Access Count: **0** 0

**Users By Risk Scores**

user	user_first	user_last	user_email	user_bizunit	risk_score	watchlist	user	user_first	user_last	user_bizunit	user_email	size	watchlist
dmays	Don	Meyers	dmeyers@cometech.com	america	13040	false	unknown					729815421	false
waykoek	Allen	Reynold	waykoek@cometech.com	america	12323	true	-					4454522	false
Haider	Herzhal	Trapper	haider@cometech.com	america	3840	true	asdas					3844018	false
carpeno	Carmelo	Agents	carpeno@cometech.com	america	1048	false	1827109032					162576	false
markus@digitalsolutionsonline.net					48	false							
karsten@digitalsolutionsonline.net					48	false							

**Non-corporate Web Uploads**

user	user_first	user_last	user_bizunit	user_email	size	watchlist
unknown					729815421	false
4454522						
3844018						
162576						

**Non-corporate Email Activity**

user	user_email	volume_size	volume_count	volume_email	size	watchlist
cttivo@digita...	cttivo@digita...	236238	1	cttivo@digita...	629	false
jens_cottbeck@tntca.com	jens_cottbeck@tntca.com	230412	1			
akito.cong@gmail.com	akito.cong@gmail.com	237600	1			
ellen.mead7@gmail.com	ellen.mead7@gmail.com	227138	1			
arni@ctt...	arni@ctt...	223133	1			
inf.yapp@yappmedia.com	inf.yapp@yappmedia.com	223404	1			
mat.hope04@gmail.com	mat.hope04@gmail.com	218548	1			
						false

**Watchlisted Site Activity**

No results found.

**Remote Access**

**Ticket Activity**

CSV XLSX PDF Print Column Filter Reset search box

# 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

Identity Investigator

Hax0r

Hax0r hax0r;htrapper@acmetech.com,htrapper:  
bunit: americas  
endDate: 3/2/98 22:53  
prefix: Mr.

list: Trapper  
first: Hershel  
phone: +1 (800)555-3039

watchlist: true  
\_time: 2016-11-18T10:33:44-0800  
phone2: +1 (800)555-3154

email: htrapper@acmetech.com  
startDate: 6/15/93 20:07  
priority: critical

Edit

AI Authentication

AI Changes

Threat List Activity

IDS Attacks

Malware Attacks

Notable Events

Risk Modifiers

Today

Click a risk score event in investigator; see details (3) on right

02:00:00 AM

②

Users By Risk Scores

user_id	user_first	user_last	user_email
1	Hershel	Trapper	htrapper@acmetech.com
2	Allen	Savivski	aseykoski@acmetech.com
3	Ball	Bose	bball@acmetech.com
4	Wohler	Wong	wohler@acmetech.com
5	Agasiewski	Nowakowski	agasiewski@acmetech.com
6	Blase	Blase	blase@acmetech.com
7	Barack	Obama	barackobama@acmetech.com

①

Click a user in User Activity; Identity Investigator opens

③

Risk Modifiers (80)

Fri Nov 18 Fri Nov 18  
02:32:00 02:42:02  
GMT:0000

Q E A

risk\_object: Hax0r  
risk\_score: 80  
source: Identity - Activity from Expired User Identity - Rule

# 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

Access Anomalies

Action App User Business Unit

All All Last 60 minutes Submit

Geographically Improbable Accesses <Image>

user	user_bunit	sec	time	session_city	session_country	app	prev_sec	prev_time	prev_city	prev_country	prev_app	distance	speed
amanda		10.11.36.29	2015-04-17 09:46:00	Dallas	USA	sshd	10.11.36.10	04/17/2015 09:46:00	Havant	UK	sshd	4728.15	17021340.00
amenda		10.11.36.33	2015-04-17 09:46:00	Washington D.C.	USA	sshd	10.11.36.29	04/17/2015 09:46:00	Dallas	USA	sshd	416.53	1499608.00
netdump		10.11.36.4	2015-04-17 09:46:00	Havant	UK	sshd	10.11.36.23	04/17/2015 09:46:00	Dallas	USA	sshd	4728.15	17021340.00
root		10.11.36.47	2015-04-17 09:46:02	Mauritania	AF	sshd	10.11.36.16	04/17/2015 09:46:02	Havant	UK	sshd	2237.05	8063380.00
dennis		10.11.36.26	2015-04-17 09:46:03	Dallas	USA	sshd	10.11.36.18	04/17/2015 09:46:03	Havant	UK	sshd	4728.15	17021340.00

< prev 1 2 3 4 5 6 7 8 9 10 next >

<Image>



## Using the Access Anomaly Dashboard

---

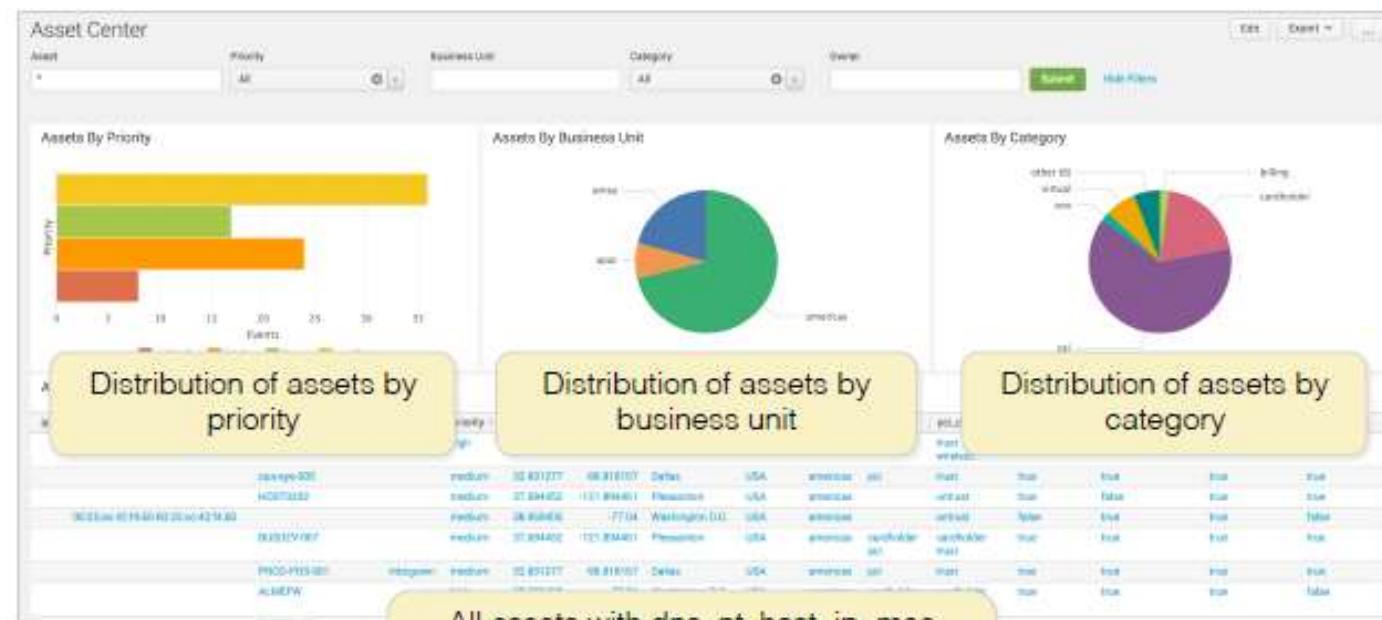
- Searches for user access during the requested time period, defaults to 60 minutes
- Displays user access events with locations more than 500 miles from their previous access location
- The distance (miles) and speed (miles per hour) between locations yields an indicator of improbability for a user 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



All assets with dns, nt\_host, ip, mac address, owner, priority, location, category, and PCI domain

# Identity Center

Security Domains Identity > Identity Center >

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



Identity information is shown with name, contact info, priority, business unit, watchlist (boolean: true or false), and start and end dates

## 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

Threat Activity

Threat Group: All Threat Category: All Search: Threat Match Value: Last 24 hours Submit Hide Filters Advanced Filter...

**THREAT MATCHES**: Unique Count: 190 +54 **THREAT COLLECTIONS**: Unique Count: 5 0 **THREAT CATEGORIES**: Unique Count: 5 0 **THREAT SOURCES**: Unique Count: 8 0 **THREAT ACTIVITY**: Total Count: 220 +64

Threat Activity Over Time

Most Active Threat Collections

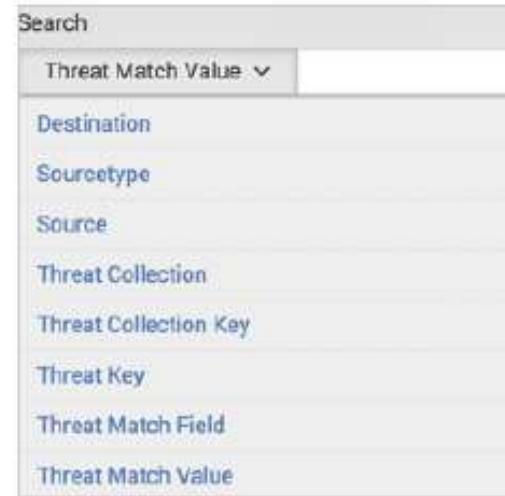
threat_collection	search	sparkline	definitive	count
ip_intel	Email Address Matches, Network Resolution Matches, Source And Destination Matches		58	176
file_intel	File Hash Matches, File Name Matches		22	37
certificate_intel	Certificate Common Name Matches, Certificate Organization Matches, Certificate Serial Matches, Certificate Uri Matches		4	8

Most Active Threat Sources

source_id	source_path	source_type	count
Injected_ip_addresses	/opt/spark/vt/apps/SA-ThreatIntelligence/default/data/threat_intel/Injected_ip_addresses.csv	CSV	85
brookej.ljgmcn	/opt/spark/vt/apps/SA-ThreatIntelligence/default/data/threat_intel/brookej_ljgmcn.csv	CSV	83
mandiant package 193593d6-1851-4cfe-b2f2-e016fae4200	/opt/spark/vt/apps/SA-EBP-ThreatIntelligence/default/data/threat_intel/Appendix_B_IGs_Nr_OpenOG.xml	XML	59
mandiant package 193591d6	/opt/spark/vt/apps/SA-EBP	XML	5

# 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	1	fortinet	130.253.37.97 132.239.106.34 141.146.8.66 94.229.0.20	111.118.177.101	ip_intel	iblacklist_proxy	threatlist	
2015-4-17 11:45:00	dest	111.118.177.101	1	fortinet	130.253.37.97 132.239.106.34 141.146.8.66 94.229.0.20	111.118.177.101	ip_intel	iblacklist_to	threatlist	
2015-4-17 11:45:00	dest	119.42.227.250	1	fortinet	106.70.143.150 109.232.224.91 122.228.206.87 138.246.7.1	119.42.227.250	ip_intel	iblacklist_spware	threatlist	
2015-4-17 10:45:00	dest	119.70.40.101	1	fortinet	110.196.218.200 116.183.62.226 139.130.49.4	119.70.40.101	ip_intel	iblacklist_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



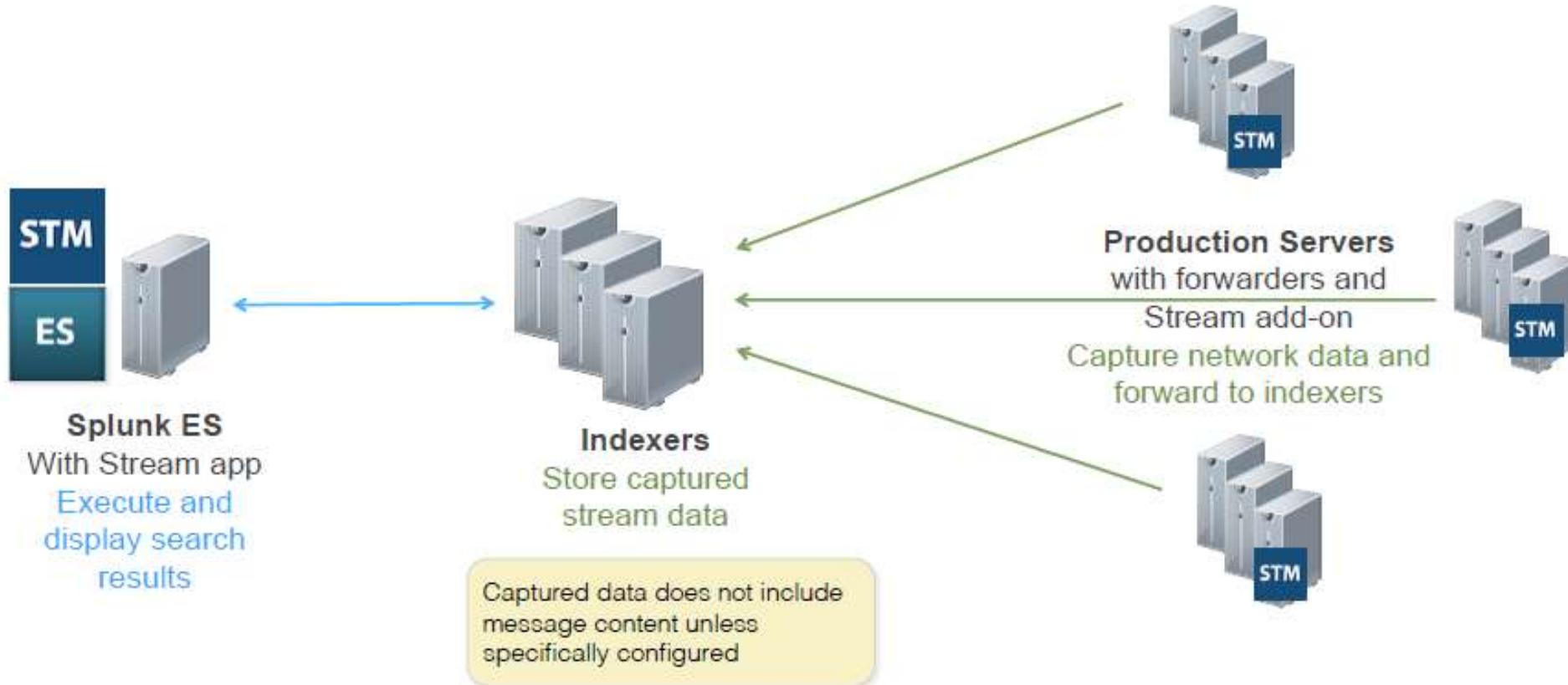
Protocol Center	An overview dashboard showing protocol activity across the network
Traffic Size	An analytical dashboard showing network traffic rates and trends
DNS	A pair of dashboards showing both an overview of activity of DNS queries as well as a search interface
SSL	A pair of dashboards for analyzing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

# Protocol Intelligence Use Cases

---

- Captures network traffic directly without 3<sup>rd</sup> 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

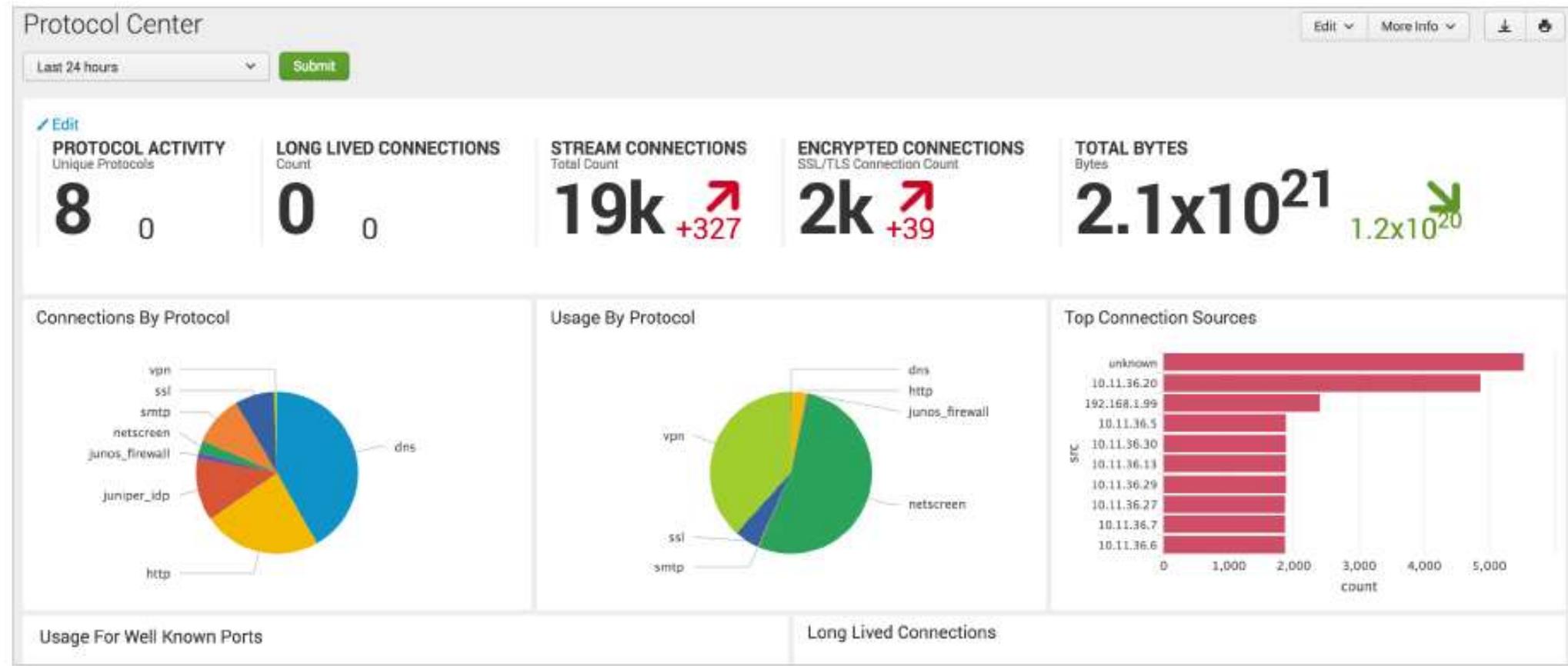


# Stream Events

---

- 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.

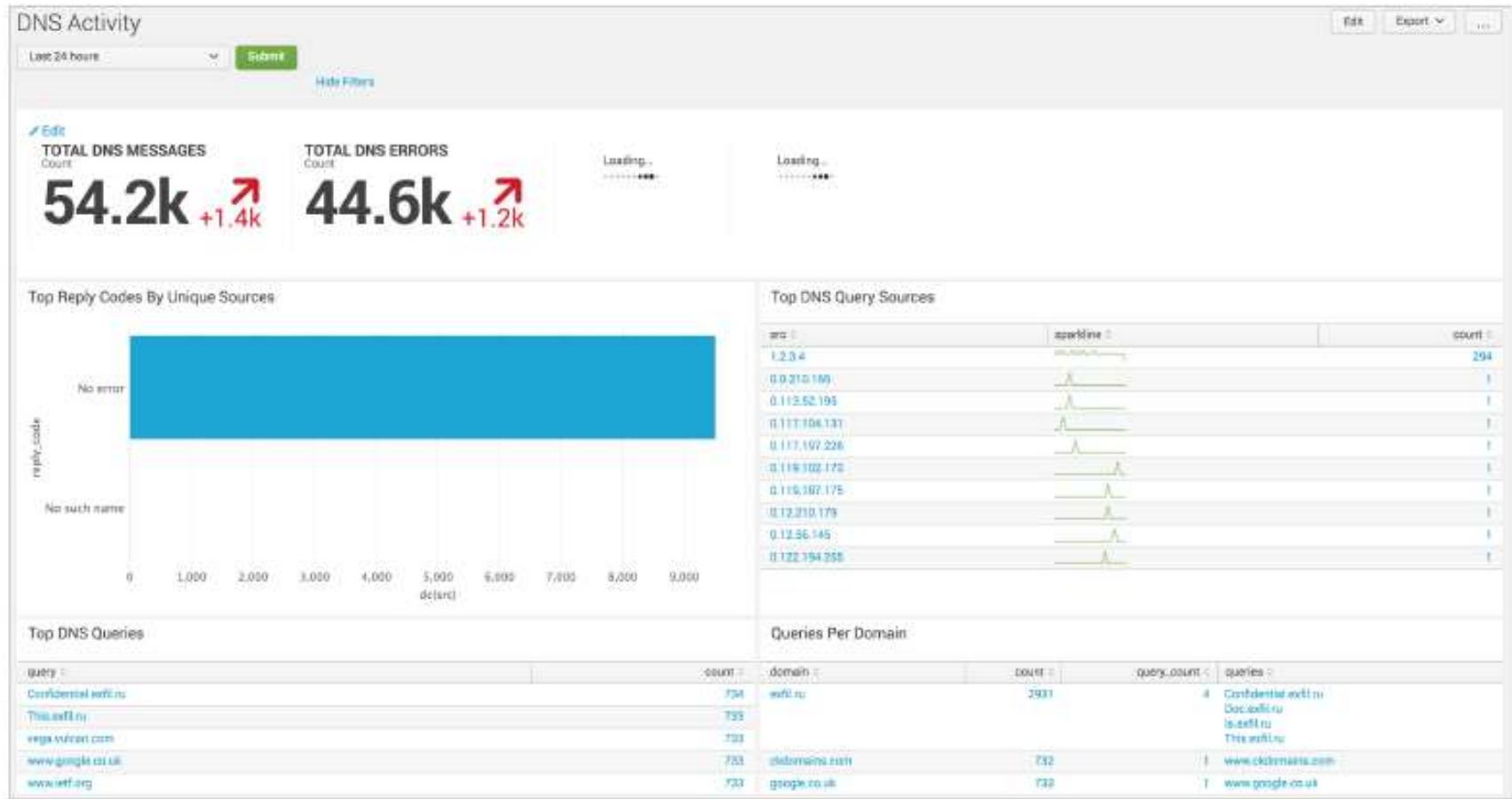
# Protocol Intelligence: Protocol Center



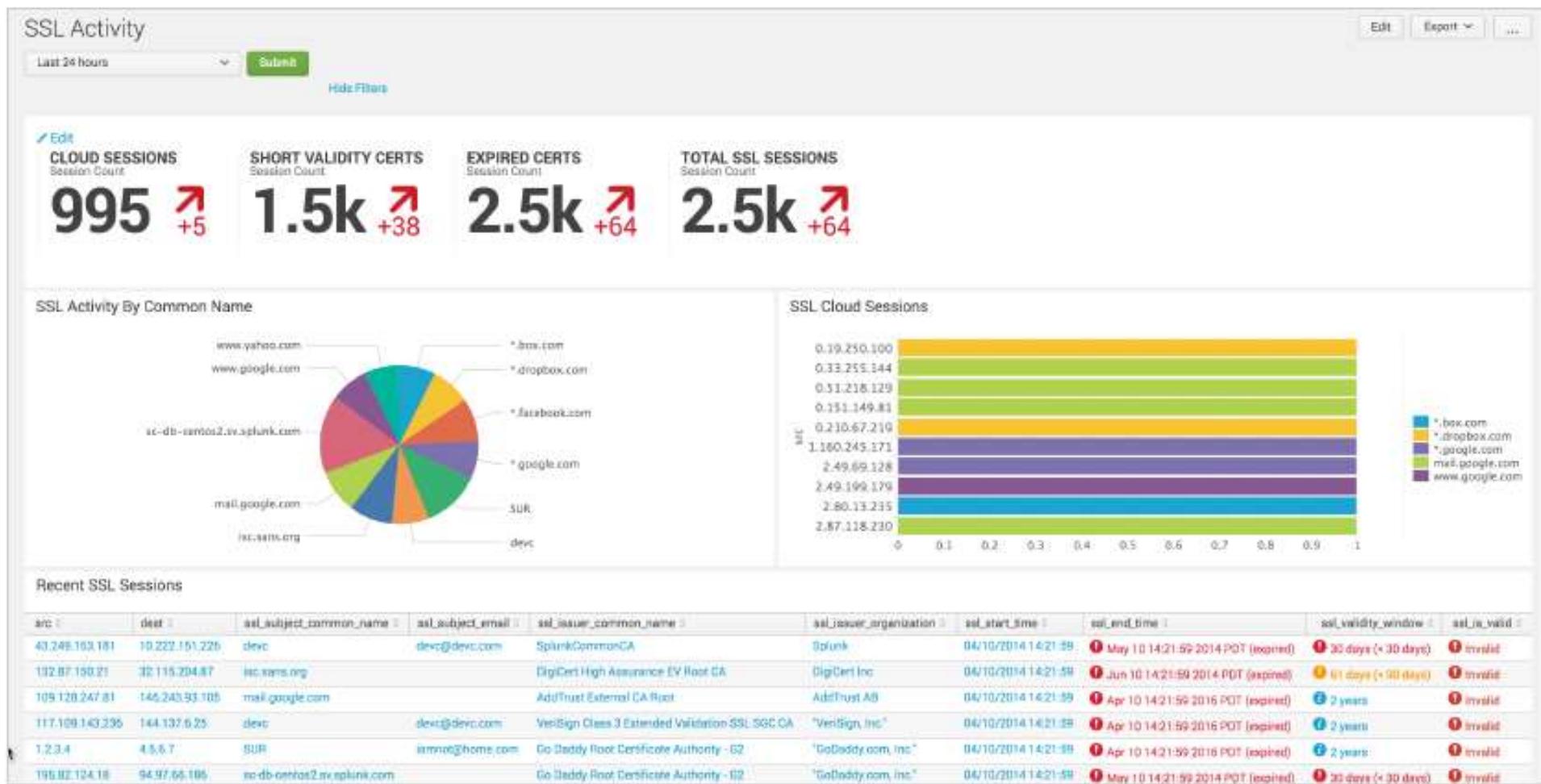
# Protocol Intelligence: Traffic Size Analysis



# Protocol Intelligence: DNS Activity



# Protocol Intelligence: SSL Activity



# Protocol Intelligence: Email Activity

Email Activity

Email Protocol:

Last 24 hours  Hide Filters.

**UNIQUE SENDERS** Sender Count: **10** 0   **UNIQUE RECEIVERS** Receiver Count: **11** 0   **CLOUD ACTIVITY** Email Count: **3.4k** +3.4k

**Top Email Sources**

src_ip	sparkline	count
123.4		593
10.11.36.44		587
10.11.36.17		529
10.11.36.76		524
10.11.36.9		522
10.11.36.11		521
10.11.36.48		519
10.11.36.19		514
10.11.36.26		514
10.11.36.30		514

**Large Emails**

No results found.

**Rarely Seen Senders**

src_user	protocol	src_count	recipient_count	count
evbender@update.defcononline.net	smtp	1	1	295
semon@home.com	smtp	1	1	295
hut_hope9@gmail.com	smtp	609	9	609
hal_yappyv@media.com	smtp	613	9	613
alzil@tux.net	smtp	617	9	617

**Rarely Seen Receivers**

recipient	protocol	src_count	src_user_count	count
nileg_gaphel@chaoomega.com	smtp	473	7	473
ccore@capcomscript.com	smtp	481	7	481
new_phing@ormula.com	smtp	481	7	481
bruce.jewachig@vixbox.com	smtp	487	7	487
resident_citizen@residents.com	smtp	488	7	488

# 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

The screenshot shows the Splunk interface with a context menu open over a correlation search result. The menu items are:

- Perform IPViking search for 10.11.36.20
- Malware Search
- Nbtstat 10.11.36.20
- Nslookup 10.11.36.20
- Ping 10.11.36.20
- Stream Capture** (highlighted with a green arrow)
- Traffic Search (as destination)
- Traffic Search (as source)
- Update Search

Below the menu, a modal window titled "Initiate a capture using the Splunk App for Stream" is displayed. It contains the following fields:

- Description: Stream to/from 10.11.36.20
- Protocols to capture: All
- Capture duration: 7 days
- Create capture button

## 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

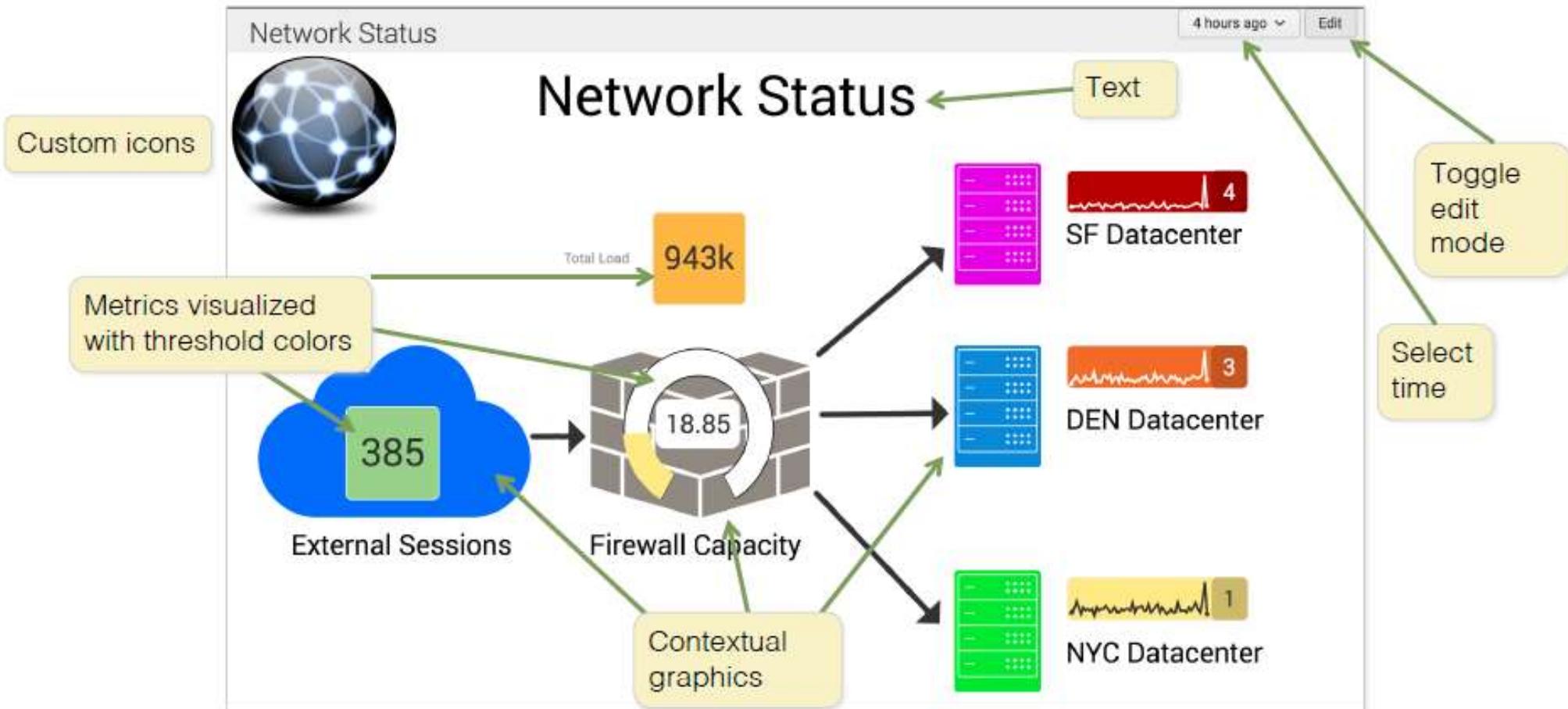
# Glass Table Management

- 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

The screenshot shows a user interface for managing glass tables. At the top, there is a header with a checkbox labeled "Saved Glass Tables", a "Create New Glass Table" button, and a "Viewer for all Glass Tables" link. Below the header, there is a summary section showing "3 Glass Tables". Underneath this, there is a table with the following data:

Title	Actions	Owner	App	Sharing
ES Deployment Template	Edit	admin	SplunkEnterpriseSecuritySuite	App
Network Diagram Templ...	Edit	admin	SplunkEnterpriseSecuritySuite	App
Network Status	Edit	analyst	SplunkEnterpriseSecuritySuite	App

# Glass Table: Standard View



# Glass Table: Edit Mode

Network Status

Tools

Controls

4 hours ago ▾ View Edit Clear Revert All Changes Save

Network Status

Work area

Total Load: 943k

External Sessions: 385

Firewall Capacity: 18.85

SF Datacenter: 4

DEN Datacenter: 3

NYC Datacenter: 1

Metrics

- > Access (7)
- > Change (1)
- > DNS (4)
- > Email (3)
- > Metrics
- > IDs (5)
- > Licensing (4)
- > Malware (13)
- > Modular Actions (6)
- > Network (1)
- > Notable (7)
- > Performance (3)
- > Risk (13)
- > SSL (4)
- > Threat Activity (5)
- > Traffic (12)
- > Updates (4)

Ad hoc Search

Position

Layer

Width: 156

Height: 37

Label Box: On

Label:

Label Location: Bottom ▾

Unit:

Search Type: Ad hoc Data Model

Search: acme-004 | timechart count

Run Search

Threshold Field:

Thresholds: On Off

Settings for selected widget

Delete Update

The screenshot shows a 'Network Status' dashboard in 'Edit Mode'. The left sidebar lists various metrics categories. The main area displays network components: a network icon, a blue cloud icon labeled 'External Sessions' (385), a grey firewall icon labeled 'Firewall Capacity' (18.85), and three datacenter icons labeled 'SF Datacenter' (4), 'DEN Datacenter' (3), and 'NYC Datacenter' (1). A callout bubble points to the 'SF Datacenter' settings, which include fields for Position, Layer, Width, Height, Label Box, Label, Label Location, Unit, Search Type, Search, Run Search, Threshold Field, Thresholds, Delete, and Update.

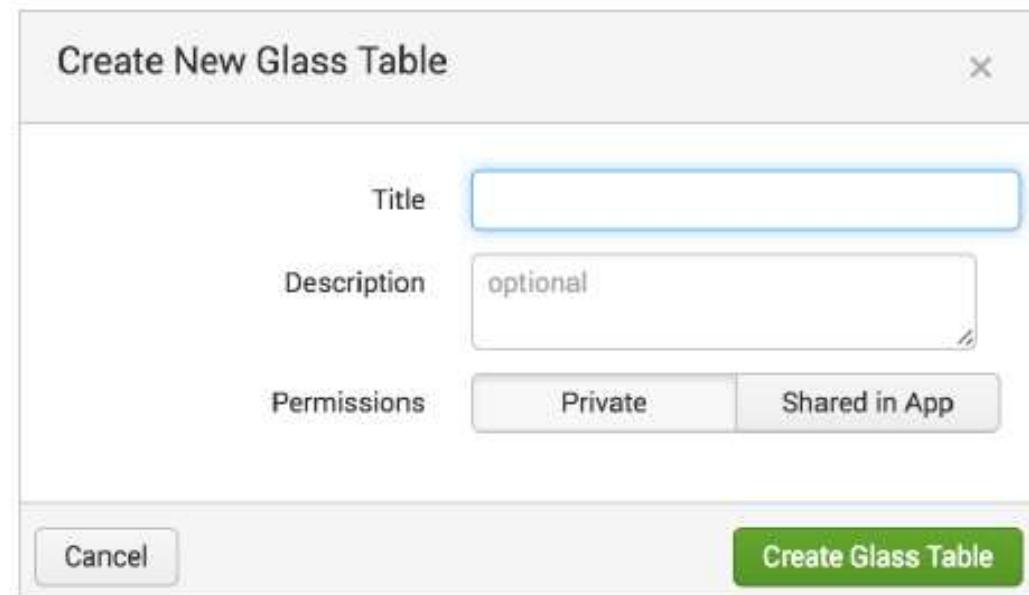
# Designing Glass Tables

---

- 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

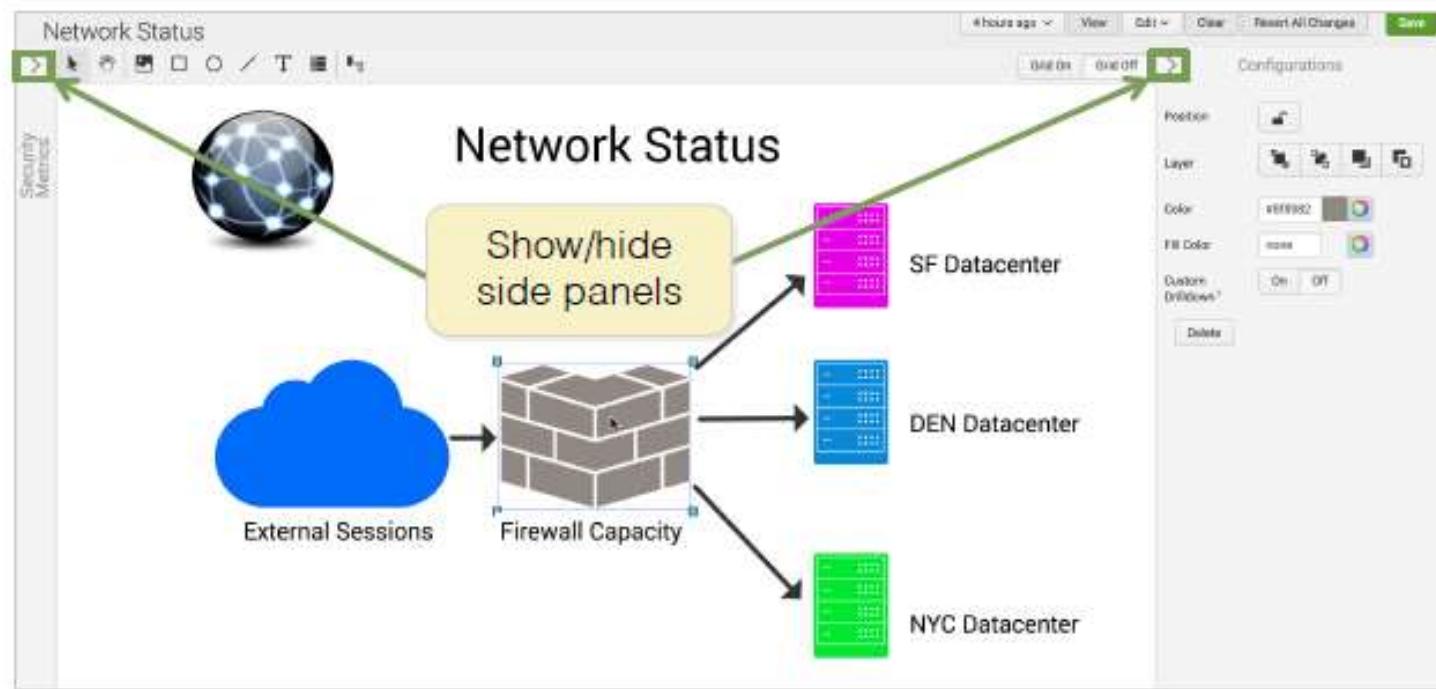
# Creating a Glass Table: 1

- 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



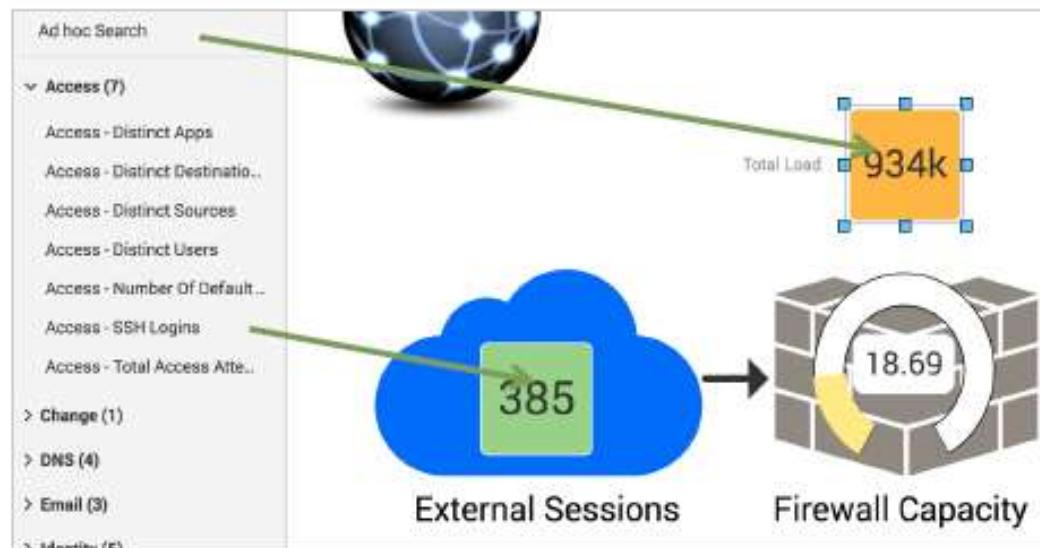
# Creating a Glass Table: 2

- 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



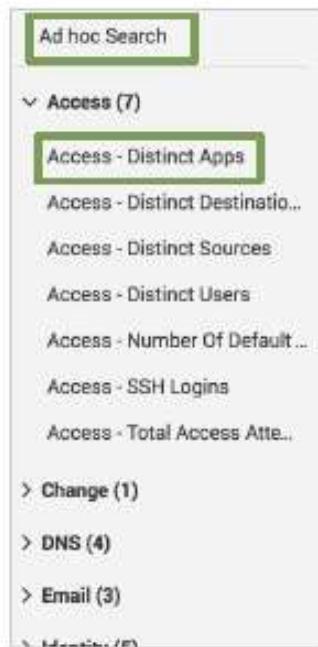
# Create a Glass Table: 3

- 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

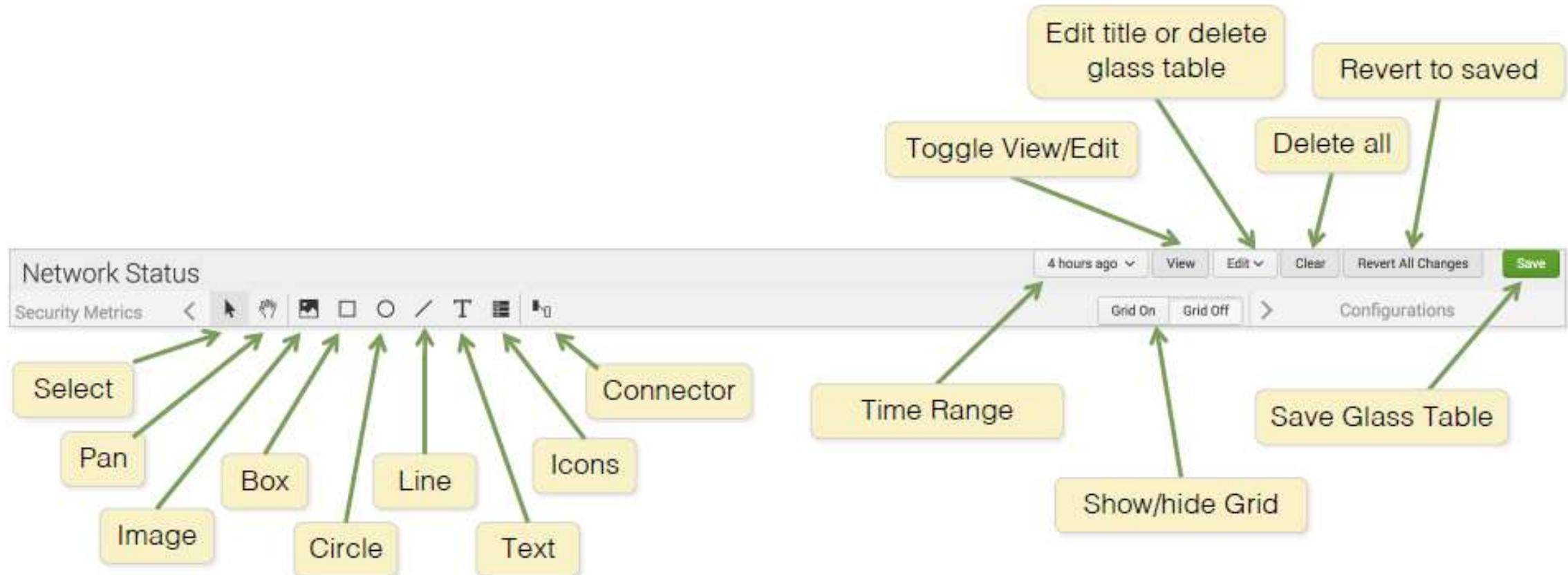


# Metrics

- 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

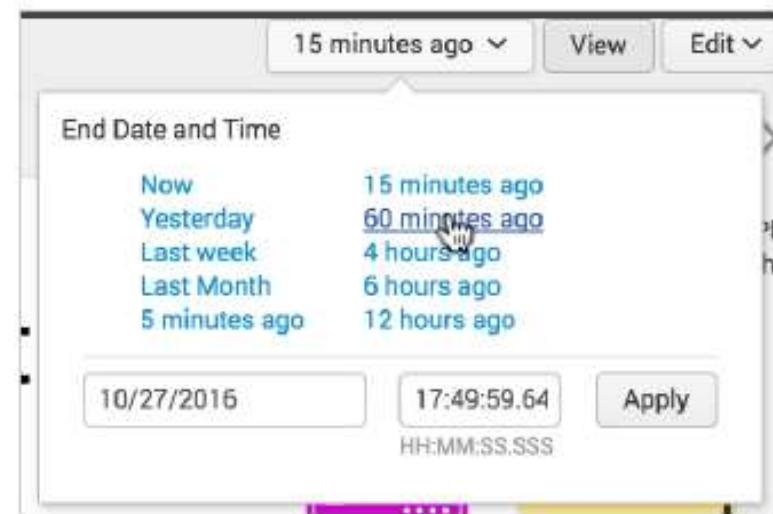
- You can add an ad-hoc search widget to display any search result without a key indicator
  - Drag an ad-hoc search widget onto the canvas
  - Select search type: **Ad-hoc** or **Data Model**
  - Enter search criteria
    - Use Run Search to test in a new window
    - The value to be displayed will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

The screenshot shows the configuration interface for an Ad-hoc search widget. It includes fields for 'Label Box' (On), 'Label' (empty), 'Label Location' (Bottom), 'Unit' (empty), 'Search Type' (Ad hoc selected), 'Search' (acme-002 | timechart count), 'Run Search' (button), and 'Threshold Field' (count).

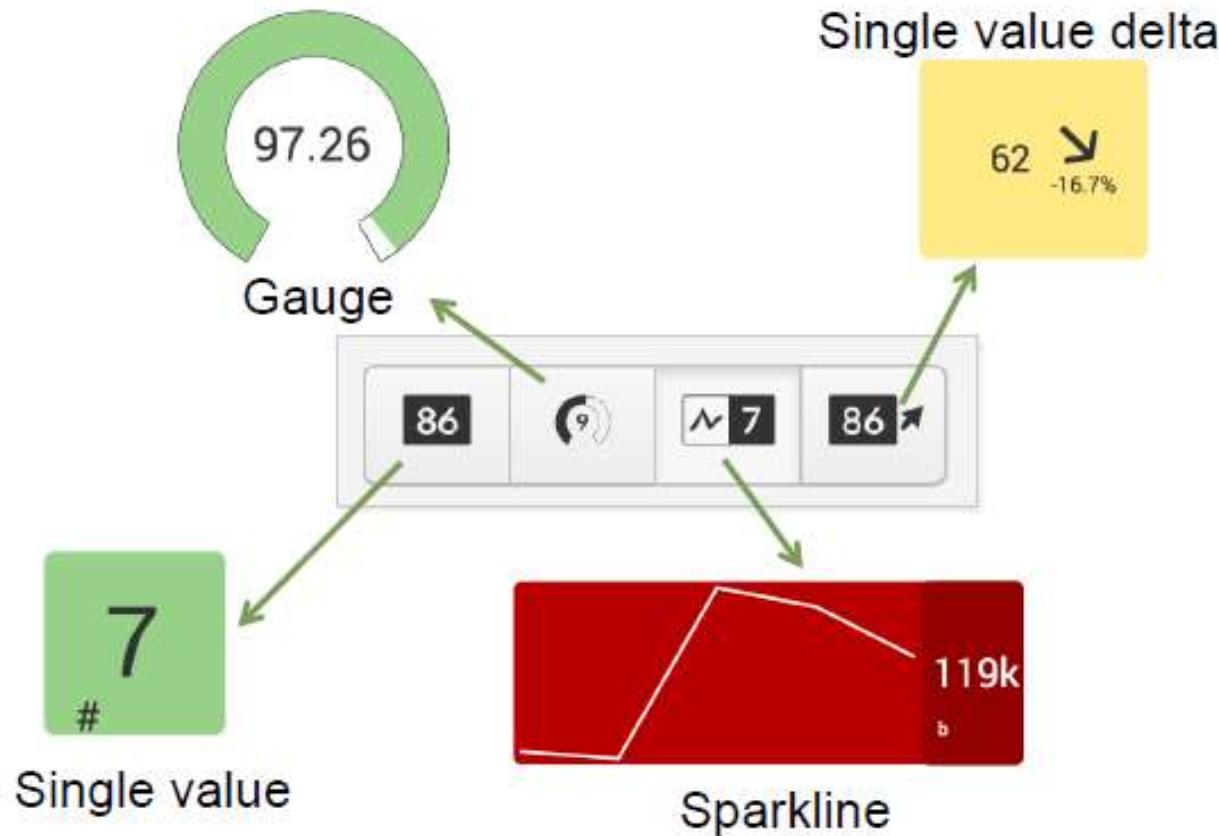
Label Box	<input checked="" type="radio"/> On <input type="radio"/> Off
Label	
Label Location	Bottom
Unit?	
Search Type	<input checked="" type="radio"/> Ad hoc <input type="radio"/> Data Model
Search?	acme-002   timechart count
Run Search	[button]
Threshold Field?	count

# 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**

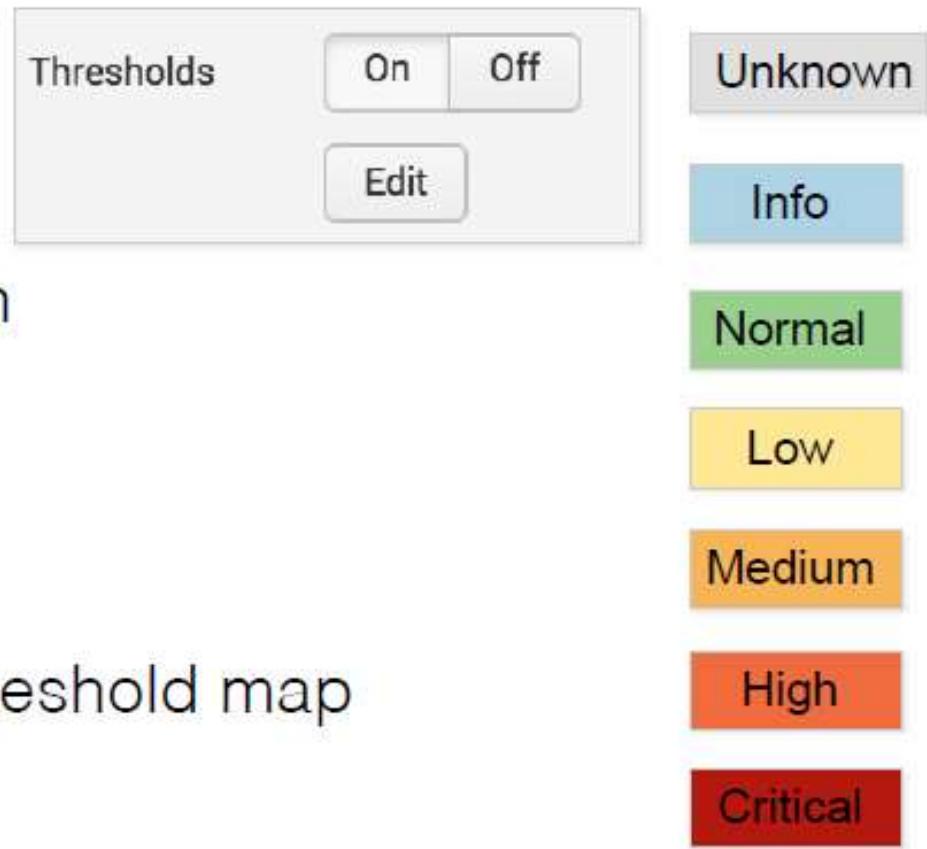


# Widget Visualization Types



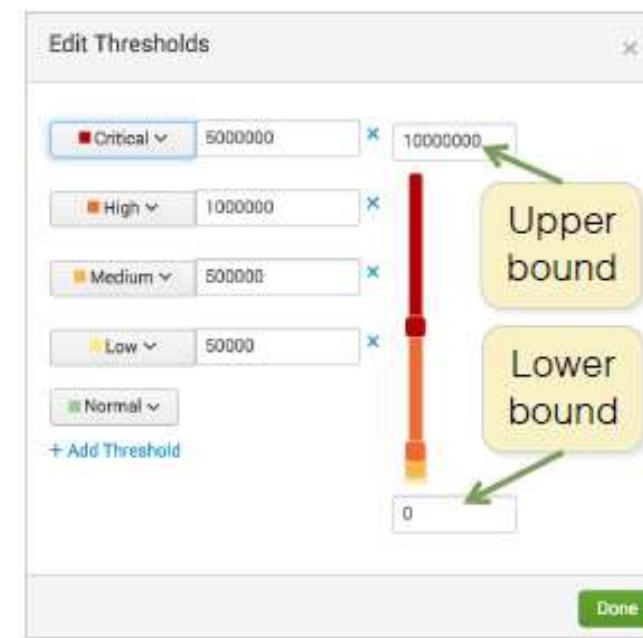
# Thresholds

- 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

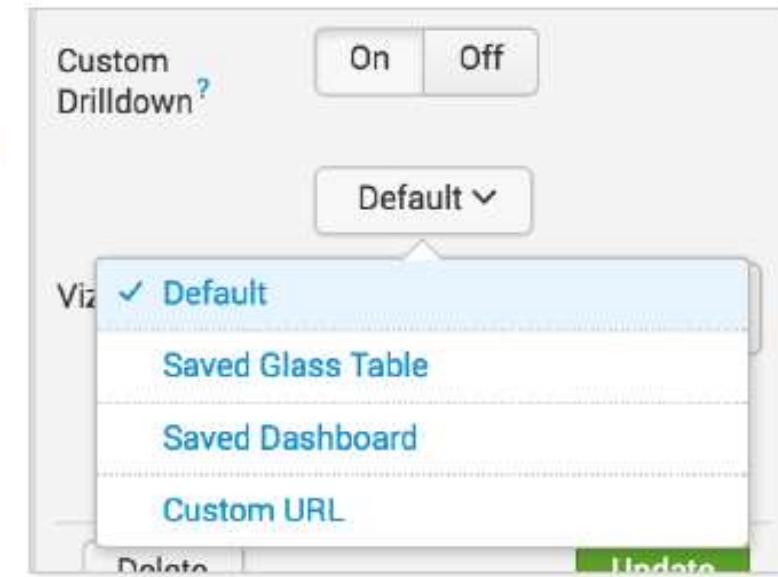
899k



17M ↑  
2.1%

# 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

Search Name *	Access - SSH Login
Destination App *	Enterprise Security
Title *	SSH Logins
Sub-title	Number of successful SSH logins

## 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

The screenshot shows a configuration panel for a Key Indicator named "Acceleration". It includes fields for "Drilldown URL", "Schedule" (set to "None"), "Value" (set to "current\_count"), and "Delta" (set to "delta"). Each field has a descriptive tooltip.

Drilldown URL	<input type="text"/>	Defines the view to redirect users to when they click the key indicator
Acceleration	Schedule <input checked="" type="radio"/> None	
Schedule	Scheduling a key indicator will make it load faster but may increase storage and processing costs	
Fields	Value* <input type="text" value="current_count"/> Specifies the name of the field that contains the current value of the key indicator	
	Delta <input type="text" value="delta"/> Specifies the name of the field that contains the change (delta) to the key indicator	

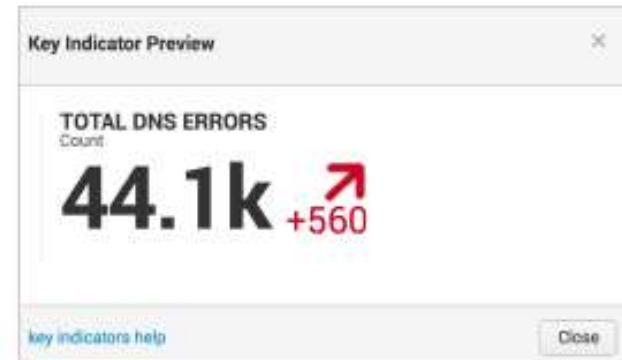
# Key Indicator: 5

- 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](https://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

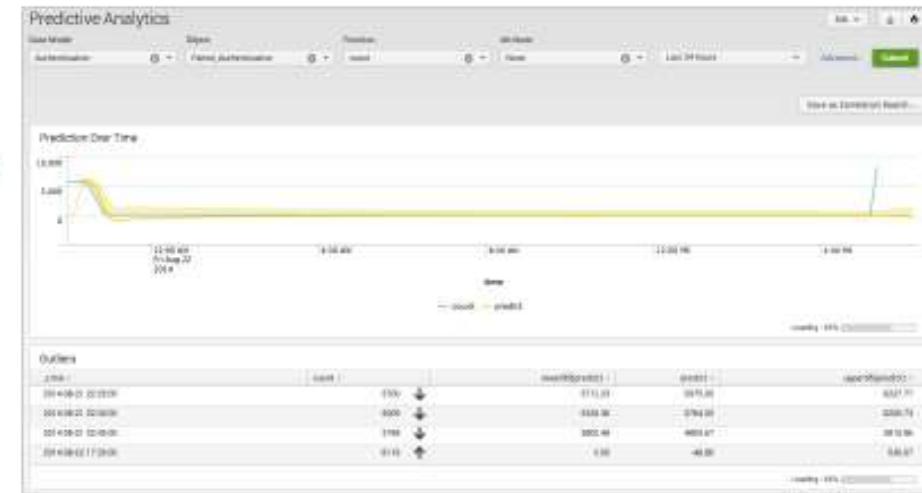
---

- 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



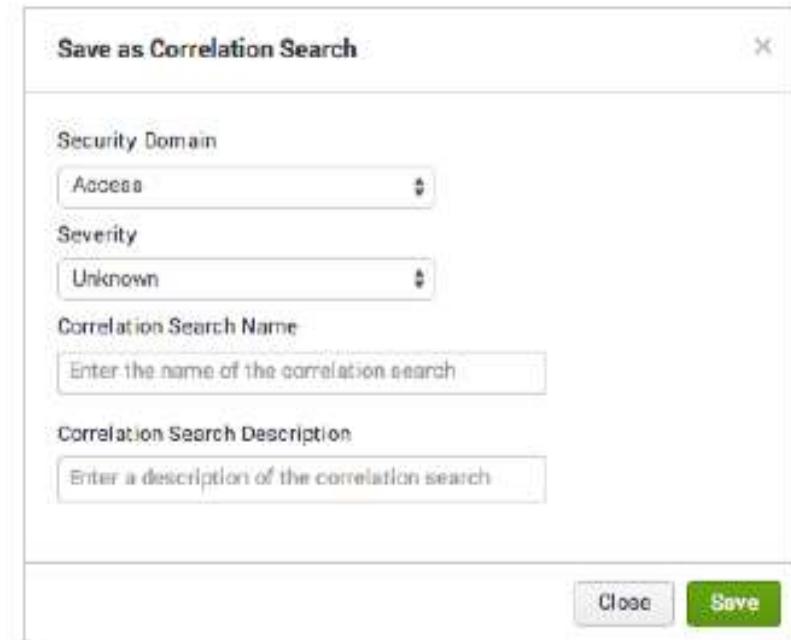
# Using Predictive Analytics

---

- 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

