Splunk® Enterprise Security
Use Splunk Enterprise Security 7.0.2

Generated: 11/02/2022 9:38 am

Table of Contents

Table of Contents

Dashboard Reference

Introduction

About Splunk Enterprise Security

Splunk Enterprise Security provides the security practitioner with visibility into security-relevant threats found in today's enterprise infrastructure. Splunk Enterprise Security is built on the Splunk operational intelligence platform and uses the search and correlation capabilities, allowing users to capture, monitor, and report on data from security devices, systems, and applications. As issues are identified, security analysts can quickly investigate and resolve the security threats across the access, endpoint, and network protection domains.

Access Splunk Enterprise Security

1. Open a web browser and navigate to Splunk Web.
2. Log in with your username and password.
3. From the **Apps** list, click **Enterprise Security**.

Get started

Get started with common analyst workflows in Splunk Enterprise Security.

- See Introduction to the dashboards available in Splunk Enterprise Security for an overview of the dashboards available and how to use them for your use cases.
- See Overview of Incident Review in Splunk Enterprise Security to learn how to work with notable events.
- See Investigations in Splunk Enterprise Security for an introduction to tracking your work in an investigation.
- See Use Analytic Stories for actionable guidance in Splunk Enterprise Security for using the use case library to help with detecting, analyzing, and addressing security threats.
- See Analyze risk in Splunk Enterprise Security to learn how Splunk Enterprise Security assigns risk to objects.

If you are a Splunk Enterprise Security administrator, see *Administer Splunk Enterprise Security* to access documentation specific to your administrator workflows.

Incident Review

Overview of Incident Review in Splunk Enterprise Security

The Incident Review dashboard displays notable events and their current status. You can also filter notable events based on specific fields and accelerate the triage of notable events through an investigation workflow.

A notable event represents one or more anomalous incidents detected by a correlation search across data sources. For example, a notable event can represent:

- The repeated occurrence of an abnormal spike in network usage over a period of time
- A single occurrence of unauthorized access to a system
- A host communicating with a server on a known threat list

As an analyst, you can use the dashboard to gain insight into the severity of events occurring in your system or network. You can use the dashboard to triage new notable events, assign events to analysts for review, and examine notable event details for investigative leads.

As an administrator, you can manage and customize Incident Review and notable event settings. See Managing Incident Review in Splunk Enterprise Security for more information about administrator activities.

> The option to run a real time search is no longer available on the Incident Review page from release 6.6.2 or higher.

How Splunk Enterprise Security identifies notable events

Splunk Enterprise Security detects patterns in your data and automatically reviews events for security-relevant incidents using **correlation searches**. When a correlation search detects a suspicious pattern, the correlation search creates a new notable event.

The Incident Review dashboard surfaces all notable events, and categorizes them by potential severity so you can quickly triage, assign, and track issues.

Incident review workflow

You can use this example workflow to triage and work notable events on the **Incident Review** dashboard.

1. An administrative analyst monitors the **Incident Review** dashboard, sorting and performing high-level triage on newly-created notable events.
2. When a notable event warrants investigation, the administrative analyst assigns the event to a reviewing analyst to start investigating the incident.
3. The reviewing analyst updates the status of the event from **New** to **In Progress**, and begins investigating the cause of the notable event.
4. The reviewing analyst researches and collects information on the event using the fields and field actions in the notable event. The analyst records the details of their research in the **Comments** field of the notable event. As part of the research, the analyst might run adaptive response actions. If the research proves that the notable event needs more lengthy investigation, the analyst can assign the notable event to an investigation.
5. After the reviewing analyst addresses the cause of the notable event and any remediation tasks have been escalated or solved, the analyst sets the notable event status to **Resolved**.

6. The analyst assigns the notable event to a final analyst for verification.
7. The final analyst reviews and validates the changes made to resolve the issue, and sets the status to **Closed**.

Change the UI theme of Splunk Enterprise Security

Splunk Enterprise Security provides the option of switching between light and dark UI themes, when using Splunk Enterprise Security version 7.0.2 or lower and Splunk Cloud Platform version 9.0.2205 or lower. The default setting for the UI theme in Splunk Enterprise Security is the dark theme.

Follow these steps to select the UI theme in Splunk Enterprise Security if you are using Splunk Enterprise Security version 7.0.2 or lower and Splunk Cloud Platform version 9.0.2205 or lower:

1. From the Splunk Enterprise Security menu bar, select **Configure > All Configurations**.
2. Click **General > General Settings**.
3. Scroll to **ES Theme** and select mode.

> When using Splunk Enterprise Security version 7.0.2 or higher and Splunk Cloud Platform version 9.0.2208 or higher, you cannot switch between the dark and light UI themes using the Splunk Enterprise Security app. However, you can switch UI themes using the Splunk Enterprise search app.

Follow these steps to select the UI theme using the Splunk Enterprise search app:

1. In the Splunk Enterprise Search app, navigate to **Administrator > Preferences**.
2. Scroll to **Theme** and select from the following options to set a theme for your ES app:
    - **Light**
    - **Dark**

    > The Splunk Search app offers three UI theme options, including '''Light''', '''Dark''', and '''Default System Theme''' options. However, Splunk Enterprise Security supports only the '''Dark''' and '''Light''' themes for both Cloud and on-prem.

For more information on selecting the UI theme in the Splunk search app, see Change the UI theme of Splunk Cloud Platform. Currently, not all apps used with Splunk Enterprise support the dark theme. If the dark theme is not supported, the default theme, "Enterprise", is applied.

When you load the Common Information Model (CIM) app within the ES context using **Configure > CIM Setup**, the mode displayed for CIM is the same as set for Enterprise Security. However, when you load the CIM app independently of Splunk Enterprise Security, Enterprise mode is displayed by default.

Users such as `ess_analyst` or `ess_user` cannot switch between dark or Enterprise modes. However, as an administrator, you might grant access to other users and override the dark mode upon request by making edits to the `user-prefs.conf` configuration file.
To enable specific users to access the Enterprise mode, add `theme = enterprise` in the `[general]` stanza of the `user-prefs.conf` configuration file located at `./etc/users/<userid>/user-prefs/local/user-prefs.conf`.
To enable all other users to access the Enterprise mode at a system level, add `theme = enterprise` in the `[general]` stanza of the `user-prefs.conf` configuration file located at `./etc/apps/user-prefs/local/user-prefs.conf`.

Triage notables on Incident Review in Splunk Enterprise Security

You can monitor notables, assign notables to specific owners, and prioritize actions that analysts take to resolve security events on the Incident review page. You can also accelerate the triage of notables by using filters or tags and by adding dispositions.

Ways to triage notables faster

Drill down on specific notables or groups of notables that pose the highest threat to accelerate the triage of notables during an investigation. Triaging notables helps to respond to security threats faster. You can triage notables by sorting notables, grouping notables using filters, or adding dispositions to the notables.

Sort notables

You can sort notables on the Incident Review page to triage notables faster. Notables contain **Urgency**, **Status**, **Security Domain**, **Owner**, and **Type** filters to help you categorize, track, and assign events.

You can further speed up the triage of your notable event through the investigation workflow by creating filters. Using filters helps you to drill down on specific and detailed information about the notable events and identify potential threats faster. Toggle **Show Charts** or **Hide Charts** to display visualizations for the notable events based on **Urgency**, **Status**, **Owner**, and **Domain**. You can hide the filters feature used for grouping notable events by clicking **Close Filters**.

You can also customize the fields or add additional fields to display your notable events. For more information on customizing notable event fields, see Change notable event fields.

Filter notable events using the following fields that appear on the Incident Review page:

Field	Description
Urgency	Importance of the notable event, such as, **Medium**, **Low**, **High**, **Critical**, **Informational**, and **Unknown**
Status	Status of the notable, such as, **New**, **In-progress**, **Pending**, **Resolved**, and **Closed**
Owner	Name of the owner.
Security Domain	Domain from which the notable is generated, such as, **Access**, **Endpoint**, **Network**, **Threat**, **Identity**, and **Audit**
Type	Option to select all notables or specific notables based on risk events Options include: **All Notables**, **Notables** (that don't use risk based alerting), and **Risk Notables**
Search type	Correlation search or sequenced search You can also filter notables using specific correlation searches
Time or	Time span during which notables are created, such as **Last 24 hours**, **Last 30 days**, and so on.
Associations	Specific investigations, short IDs, or running attack templates that are associated with the notables.

You can filter for notable events created by the same correlation search using the **Correlation Search Name** filter to type the name of the correlation search that created a notable event. As you type, the correlation search names appear for you to select.

Type a Search Processing Language (SPL) string into the **Search** filter to search within the notable event details of notable events on Incident Review.

If you added notable events to investigations, or generated short IDs for notable events to share them with other analysts, you can filter by the **Associations** filter to quickly view the notable events associated with a specific investigation or the notable event represented by a short identifier. However, the short ID filter dropdown lists all short IDs, including notable events that are suppressed. If the notable event is suppressed, you will not be able to see it on the Incident Review page when filtering on short ID.

Additionally, you can simplify searching and add identifiers to notable events using tags. Click **Edit Tags** in the field actions menu for a notable event field such as **Title**, **Status**, or **Owner** to add new tags or modify existing ones. After you create a tag, you can use it to filter the notable events on the page.

If you want to see a filtered view of Incident Review by default, ask your ES admin to modify the navigation menu in Enterprise Security to link directly to a filtered view. See Add a link to a filtered view of Incident Review in *Administer Splunk Enterprise Security*.

Group notables

Reuse the grouping of notable events by specific fields during an investigation by saving filters. You can reuse saved filters or make edits to existing filters based on specific fields. Additionally, you can also save a filter as a default.

1. From the Splunk Enterprise Security menu bar, click the Incident Review page.
2. Select the fields that you want to use to group the notables.
   For example, **Urgency: Critical**; **Status: New**; **Owner: Carl**; **Time: Last 24 hours**; **Security Domain: Endpoint**
3. Click **Save New Filters**.
4. Enter a name for the filter.
5. Check **Save as Default Filter** if you want to add it as a default filter.
6. Click **Save** to save the filters.
   All active filters are listed in the **Save Filters** dialog box.
7. Verify that the filter is in the **Saved Filters** drop down menu on the Incident Review page.

Manage filters for notables

Edit, delete, or select specific filters to group notable events based on specific fields for easier triage during an investigation.

1. From the Splunk Enterprise Security menu bar, click the Incident Review page.
2. Click **Manage Filters** from the **Saved Filters drop down menu.**
3. Click **Open** under the **Default** column to change the default filters.
4. Click the pencil icon to edit the filter name.
5. Click the trash icon to delete a filter.

Add dispositions to notables

Add a disposition to any notable on the Incident Review page to identify the threat level associated with the notable accurately. Dispositions help classify the notables and separate the false positives without impacting the status of the notable event, such as **New**, **In-progress**, **Closed**, and so on.

1. From the Splunk Enterprise Security menu bar, click the Incident Review page.
2. Scroll down to the table that lists the notables.
3. Select the notable to which you want to add a disposition.
4. Click **Edit Selected** to edit the selected notable event.
5. Select one of the following options from the **Disposition** drop down menu:
   - **Undetermined**
   - **True Positive - Suspicious Activity**
   - **Benign Positive - Suspicious But Expected**

- ♦ **False Positive - Incorrect Analytic Logic**
- ♦ **False Positive - Inaccurate Data**

The default option for the **Disposition** field is "Undetermined". You can also add a custom disposition to the notable.

6. Click **Save Changes**.

Add custom dispositions to a notable

Follow these steps to create a custom disposition for notables:

1. From the Splunk Enterprise Security menu bar, select **Configure>Incident Management>Incident Review Settings**.
2. Scroll down to **Incident Review-Dispositions**.
3. Click **New**.
4. In the **New Disposition** dialog, add a label and description for the new disposition.
5. Click **Save**.

Follow these steps to add the custom disposition to any notable:

1. From the Splunk Enterprise Security menu bar, click the Incident Review page.
2. From the list of notables, select the notables to which you want to add the custom disposition.
3. Click **Edit Selected**.
4. In the **Edit Events** dialog, select the custom disposition from the drop down menu.
5. Click **Save Changes**.
6. Click **Close**.

Assign notables to owners

You can assign one event at a time or several at once.

1. Select a notable.
2. Click **Edit selected**.
3. Select an **Owner** to assign the notable. Or, click **Assign to me** to assign the event or events to yourself.
4. Save your changes.

Owners are unassigned by default, and you can assign notables to any user with an **administrator**, **ess_admin**, or **ess_analyst** role. For more on user roles, see Configure users and roles in the *Installation and Upgrade Manual*.

If you use SAML authentication, it might take up to 10 minutes to update the list of users that you can assign notables to.

Update the status of a notable

New notables have the **New** status. As analysts triage and move a notable through the incident review workflow, the owner of the investigation can update the status of the notable to reflect the actions they take to address the event.

1. Select one or more events, then click **Edit all selected**. To take action on all displayed events, click **Edit all ## matching events**.
2. In the **Edit Events** window, update the fields to reflect your actions.

3. (Optional) Add a **Comment** to describe the actions you took.
4. Save changes.

If your Enterprise Security (ES) administrator customized the Incident Review page, you might need to enter comments when updating a notable. See Customize Incident Review in Splunk Enterprise Security for more information about how ES admins can customize the ways that analysts view and interact with notables.

> If your changes are not immediately visible, check the filters. For example, if the filter is set to "New" after you changed an event to "In Progress", your updated event will not display.

You can choose from the following notable statuses.

Status	Description
Unassigned	Used by Enterprise Security when an error prevents the notable from having a valid status assignment.
New	Default status. The event has not been reviewed.
In Progress	An owner is investigating the event.
Pending	The assignee must take an action.
Resolved	The owner has addressed the cause of the event and is waiting for verification.
Closed	The resolution of the event has been verified.

You can customize the notable status names and workflow progression to match your process. For more information, see Manage notable statuses.

Prioritize notables by urgency

Use the urgency level of a notable event to prioritize incident review. Every notable is assigned an urgency. Urgency levels can be **Unknown**, **Low**, **Medium**, **Informational**, **High**, or **Critical**.

Enterprise Security calculates the urgency level using the severity of the correlation search event and the priority of the asset or identity involved in the event. See How urgency is assigned to notable events in Splunk Enterprise Security.

By default, security analysts can change the urgency of a notable. See Customize Incident Review in Splunk Enterprise Security to learn how to change the default value for urgency of a notable.

Analyze risk event notables to identify threat

Use the Incident Review page to investigate the contributing risk events that created a notable. You can quickly identify the risk events that might be a threat to your security environment by analyzing the timeline of the risk events with their associated risk score.

1. From the Splunk Enterprise Security menu bar, click the Incident Review page.
2. From the **Type** filter dropdown, select **Risk Notable** to display the notables that have associated risk events. You can expand the notable on the Incident Review page to launch the risk event timeline and further investigate the risk events associated with the notable.
3. Review the following two fields for the risk notables:

Field	Description
Risk Events	Events that created the notable alert

Field	Description
Aggregated Risk Score	Sum of all the scores associated with each of the contributing risk events For example, if there are five risk events and each risk event is assigned a score of 10, 20, 30, 40, and 50 respectively, then the aggregated risk score is 150.

4. Click the value in the **Risk Events** field for the notable that you want to investigate.
   This opens a window that contains two panels. The top panel displays a timeline visualization of the contributing risk events that created the notable. The bottom panel includes a table with detailed information on the contributing risk events.
5. Sort the contributing risk events in the table based on any of the following fields:
   - **Time**
   - **Risk Rule**
   - **Risk Score**
6. Expand the risk notable in the **Contributing Risk Events** table for more details to further analyze the risk objects in your security environment.
   This includes information on the following fields:
   - **Risk Object**
   - **Source**
   - **Risk Score**
   - **Risk Message**
   - **Saved Search Description**
   - **Threat Object**
   - **Threat Object Type**
7. Click **View Contributing Events** for information on the contributing events that triggered the risk event.
   You can also search for specific contributing risk events that created the notables through the filter.
8. Correlate the risk events with dates and severity of the risk scores in the timeline visualization to identify threats.
   You can zoom in and out to narrow down the time of occurrence since the timeline visualization plots of the contributing risk events using time on the x-axis and the risk score on the y-axis.
   The timeline visualization also uses color codes on the icons that indicate the severity of the risk scores. The color coding of risk score icons is consistent across the **Contributing Risk Events** table and the timeline visualization of the risk events. A lighter color icon corresponds to a lower risk score.
   You can view a maximum of 100 risk events on the **Contributing Risk Events** table and the timeline visualization. If you have more than 100 risk events, the event count displays as `100+` on the header and includes a link to the search page that displays the complete list of risk events. If the number of risk events is less than 100, the event count is displayed as is.
   The risk score in the **Contributing Risk Events** table and the timeline visualization is the calculated risk score of all events.
9. Hover over the color coded icons in the timeline visualization to view more information on the risk event within a tooltip. The following additional details about the risk event are displayed in the tooltip:
   - **Risk Score**
   - **Event Name**
   - **Description**
   - **Time**
   - **MITRE Tactic**
   - **MITRE Technique**
10. Click a notable on the timeline to highlight the associated row in the **Contributing Risk Events** table.
11. Identify the risk object type through the icons displayed in the header of the timeline visualization from the following icons:
    - User
    - System
    - Network Artifacts

- Other

You might see a small discrepancy between the event count on the Incident Review page and the event count on the risk window because a new search is launched when you click the notable on the Incident Review page.

Use custom risk notables to identify threats

Use the timeline visualizations for custom risk notables to search the risk index and identify threats. You can use custom risk notables in addition to using default risk notables to identify threats that are specific to your security environment. Following are examples of the default risk notables that are packaged with Splunk Enterprise Security:

- `24 hour risk threshold`
- `ATT&CK Tactic Threshold Exceeded over previous 7 days`

The risk timeline modal cannot be selected unless all required fields are present within the risk notable event and the contributing risk events.

To create a custom risk notable, define the following fields in your risk notable. The following fields are common to the risk index and risk data model:

Field	Description
`risk_object`	The risk event identifier
`risk_object_type`	The risk event identifier type
`risk_score`	A number that represents the risk level of a specific risk object.
`risk_event_count`	The total number of risk events associated with the notable event. This value is calculated using the notable search.
`drilldown_earliest`	The start time used to identify the contributing events for the risk notable. This value is automatically populated using the `info_min_time` in the notable framework.
`drilldown_latest`	The end time used to identify the contributing events for the risk notable. This value is automatically populated using the `info_max_time` in the notable framework.
`drilldown_search`	The search used to identify the contributing events for the risk notable. This SPL must return a `calculated_risk_score` field with a non-null value. The `calculated_risk_score` field is common to the Risk data model.

Example: How to create custom risk notables

Following is an example of creating a risk notable. You must follow this format to use the Risk Timeline visualization.

Say, you have the following events in the Risk data model:

Risk object	Risk object type	Risk score
foo	user	30
bar	user	50
foo	user	30

The underlying notable search must contain the following required fields:

- `risk_object`

- `risk_object_type`
- `risk_score`
- `risk_event_count`
- `drilldown_earliest`
- `drilldown_latest`
- `drilldown_search`

Following is an example of the search for the risk notables with associated results:

> Required fields that are not part of the Risk data model are calculated.

```
| tstats `summariesonly` sum(All_Risk.calculated_risk_score) as risk_score,
count(All_Risk.calculated_risk_score) as risk_event_count from datamodel=Risk.All_Risk by
All_Risk.risk_object, All_Risk.risk_object_type
```

Results:

Risk object	Risk object type	Risk score	Risk event count
foo	user	60	2
bar	user	50	1

Though search results add the `drilldown` fields automatically, you must specify a `drilldown_search` when you configure the risk notable on the Correlation Search editor. Additionally, the notable `drilldown_search` must contain the field `calculated_risk_score`.

Following is an example of the `drilldown_search`:

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

As shown in this example, the `calculated_risk_score` already exists in the Risk data model and is calculated automatically.

For more information on accessing the Risk Timeline visualization to analyze risk event notables and identify threat, see Analyze risk event notables to identify threat.

Investigate a notable on Incident Review in Splunk Enterprise Security

After you finish triaging notable events, begin your investigation. Use the available fields on a notable event to assess the urgency, contributing events, and risk scores associated with the notable event.

Open the event details to learn more about a notable event.

- Review the **History** to see the recent investigation activity on the notable event. Click **View all recent activity for this Notable Event** to see analyst comments, status changes, and other activities for the event.
- Determine if the notable event is part of an existing investigation by reviewing the **Related Investigations** section. Click the name of the investigation to open it.
- See which correlation search generated the notable event. Click the name of the correlation search to make changes to or review the correlation search to understand why the notable event was created.
- View the **Contributing Events** that caused the notable event to be created.
- Review the risk scores listed for assets and identities involved in a notable event. Click a risk score to open the

Risk Analysis dashboard filtered on that asset or identity.

- If one original event created a notable event, you can see the full details of the original event.
- Review the **Adaptive Responses** to see which adaptive response actions have been performed for this notable event, whether the actions were successfully performed, and drill down for more details. Click the name of the response action to see potential results generated by this action's invocation. Click **View Adaptive Response Invocations** to see the raw audit events for the response actions associated with this correlation search. It takes up to five minutes for updates to appear on this table.
- Review the **Next Steps** to see if any next steps for notable event triage are defined.
- Click **Create Short ID** to create a short ID to share with other analysts. You can also share a notable event with a link. See Take action on a notable event on Incident Review in Splunk Enterprise Security.

Why are some of my contributing events missing?

There are some correlation searches that detect a lack of something. For example, the "Endpoint - Should Timesync Host Not Syncing - Rule" detects a lack of successful time synchronization events for a particular host. Another example is the "Audit - Expected Host Not Reporting - Rule" that detects a lack of data from a host.

When notable events are created for these hosts, it is possible that clicking the **view all contributing events** link from Incident Review will result in "No results found". You can use the time range picker to expand the time range for identifying when the lack of events occurred, but it's possible that "No results found" will persist because the host never did the thing it was supposed to do.

Find the sequenced events generated by the event sequence template

Once you have created a sequence template, and it has reached the end state, the output is listed as a sequenced event in the Incident Review dashboard. See Find the sequenced events generated by the event sequence template.

Take action on a notable on Incident Review in Splunk Enterprise Security

From Incident Review, you can suppress or share a notable event, add an event or multiple events to an investigation, analyze the risk that an asset or identity poses to your environment, or investigate a field in more detail on another dashboard.

Run an adaptive response action

Based on the details in a notable event, you may want to run a response action to gather more information, take an action in another system, send information to another system, modify a risk score, or something else.

Prerequisite
Some custom adaptive response actions use the credential store to connect to a third-party system or app. To run these actions successfully, you must have the `list_storage_passwords` capability.

Steps

1. From a notable event, select the arrow to expand the **Actions** column.
2. Click **Run Adaptive Response Actions**.
3. Click **Add New Response Action** and select an adaptive response action from the list. You can use the category filter or search to reduce the number of actions that you can select.
4. Fill out the form fields for the response action. Use the field name to specify a field, rather than the name that shows on Incident Review.

For example, type "src" instead of "Source" to specify the source field for an action.
5. Click **Run**.

You can check the status of the response action in the notable event details. View the original field names of fields displayed on Incident Review on the Incident Review - Event Attributes panel of the Incident Review Settings dashboard.

> Adblock extensions in your browser can cause response actions to fail. Add the host name of your Splunk Enterprise Security host to the site whitelist for the adblock extension.

See Included adaptive response actions with Splunk Enterprise Security for more about the different adaptive response actions included with Splunk Enterprise Security.

Share or bookmark a notable event

You can share a notable event with another analyst using a short ID or a link.

1. From the event actions, click **Share Notable Event**.
   Enterprise Security creates a short ID for the notable event and displays a link that you can copy to share with an analyst. You can also save the link as a bookmark by dragging the bookmark icon to the bookmarks toolbar in your web browser.

You cannot share a notable event from the Search dashboard.

Analyze risk of an asset or identity

You can analyze the risk that an asset or identity poses to your environment in the Incident Review dashboard.

1. Open the event details.
2. Review the risk score next to asset or identity fields such as **src** or **host**.
3. Click the risk score to open the **Risk Analysis** dashboard filtered on the asset or identity.

Not all assets and identities display a risk score. Risk scores that display for an asset or identity in Incident Review may not match the risk score on the Risk Analysis dashboard for that risk object. For more information, see How risk scores display in Incident Review in *Administer Splunk Enterprise Security*.

Add a notable event to an investigation

Investigate notable events that could be a part of a security incident by adding them to an investigation.

Add a notable event to an existing investigation

1. Add one or more notable events to an investigation.
   1. Add a single notable event by selecting **Add Event to Investigation** from the **Event Actions**.
   2. Add multiple notable events by selecting the check boxes next to the notable events and click **Add Selected to Investigation**.
2. Select an investigation to add the notable events to. If you selected an investigation in the investigation bar, that investigation is selected by default.
3. Click Save.
4. After the event or events are successfully added to the investigation, click **Close**.

Add a notable event to a new investigation

1. Select one or several notable events and click **Add Selected to Investigation**.
2. Click **Create Investigation** to start a new investigation.
3. Type a title for the investigation.
4. (Optional) Change the default status.
5. (Optional) Type a description.
6. Click **Save** to save the investigation and add the notable event or notable events to the investigation. Clicking Cancel does not add the selected notable events, but the new investigation is still created. You can click **Start Investigation** to add the notable events to the investigation and open the investigation.
7. After the event or events are successfully added to the investigation, click **Close** or click **Open <Investigation name>** to open the investigation.

See Investigations in Splunk Enterprise Security for more.

After you add a notable event to an investigation, you can filter by notable events on that investigation on the Incident Review dashboard using the Associations filter, or view the investigation in the notable event details.

When adding a sequenced event to an investigation, the contributing notable events will be added instead. For more information about creating sequenced events, see Create sequence templates in Splunk Enterprise Security.

Get notified about incoming related notable events

While you are investigating an event, you can get notified about incoming notable events that are related to the investigation via the investigation toolbar. The investigation toolbar is available on all ES dashboards. Settings enabled for an investigation in one dashboard are carried over to that investigation in other dashboards automatically.

Enable the related notable event livefeed.

1. Click the bell icon on the investigation toolbar at the bottom-right side of the Incident Review page, the Investigation Workbench, or any ES dashboard.
2. Toggle the switch to enable notification for the livefeed.
3. Click **Close**.

While you are investigating, you will get a visual notification if any related notable events occur. The bell icon color will change to orange within five minutes of the occurrence.

Acknowledge the livefeed notification or add notable events to the investigation.

1. Hover over the orange bell icon on the investigation bar at the bottom-right side of the Incident Review page or the Investigation Workbench. This tells you how many notable events are available.
2. Click the orange bell icon.
3. The related notable event livefeed window appears, containing events from the last 48 hours.
4. (Optional) Click **+** to add a notable event to the investigation.
5. Click **Mark All as Seen** to clear the livefeed when you no longer want to see the related events. This will also reset the notification, so that these no longer count against the notification number mentioned in step 1.
6. Click **Close**.

Investigate a field in more detail

Take action on a specific field, such as `host`, `src`, `src_ip`, `dest`, or `dest_ip`. Different actions are available to take depending on the field you select.

- Tag fields by selecting **Edit tags**.
- Investigate an asset by selecting **Asset Investigator** to open the Asset Investigator dashboard filtered on the asset.
- Search for access-related events for a specific destination IP address by selecting **Access Search (as destination)**.
- Investigate a domain by selecting **Domain Dossier**.
- Find other notable events with matching malware signatures by selecting **Notable Event Search**.
- Use the embedded workbench to get more context about specific field values.

Example of using the embedded workbench

The embedded workbench provides a simplified drill-down experience, reduces the number of open tabs, and makes it easier to determine notable event trends.

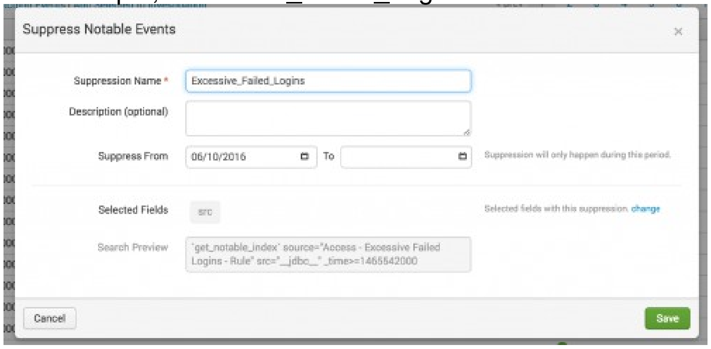
Using the source field as an example, consider a value where you want more context about an asset. From the Enterprise Security menu bar, perform the following steps:

1. Go to **Incident Review**.
2. From a notable event that contains a **Source** (src) value:
3. Click the source field actions menu.
4. Scroll down to the menu items that start with "workbench" and select one such as **Workbench - Authentication (src)**.
5. View source analysis related to investigated assets or identities. The data source is the Authentication data model. Results include events that contain artifacts in the `src, dest, user, user_id, user_role, src_user, src_user_id, src_user_role, or vendor_account` fields.

Suppress a notable event

Hide notable events from the Incident Review dashboard by suppressing them. Creating a notable event suppression does not change the counts of notable events on the posture or auditing dashboards. See Create and manage notable event suppressions for more details.

1. Select a notable event on the Incident Review dashboard.
2. From the **Actions** menu, select **Suppress Notable Events**.
3. Type a **Suppression Name**.
   For example, Excessive_Failed_Logins.



Suppression Name * Excessive_Failed_Logins

Description (optional)

Suppress From 06/10/2016 To

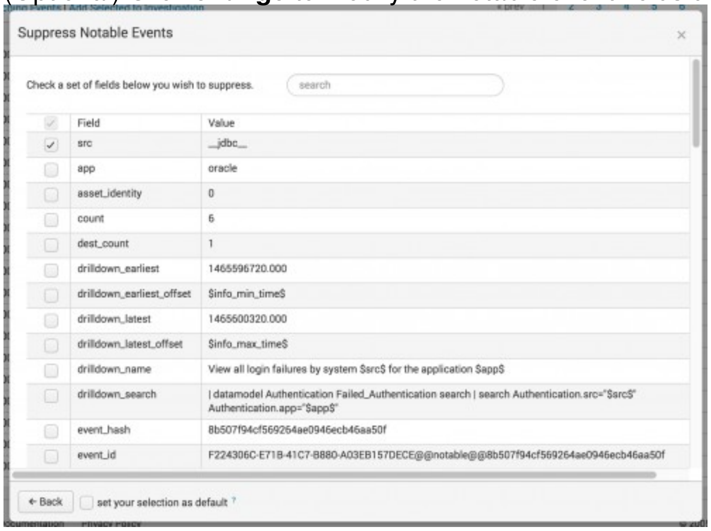
Suppression will only happen during this period.

Selected Fields src

Selected fields with this suppression. change

Search Preview `get_notable_index` source="Access - Excessive Failed Logins - Rule" src="__jdbc__" _time>=1465542000

4. (Optional) Provide a reason for the suppression using the **Description** field.
5. (Optional) Set a date range. After the time limit ends, the suppression filter expires and stops hiding events.
6. Review the **Selected Fields** to validate the fields that you want to suppress notable events from. For example, the `src` field
7. (Optional) Click **change** to modify the notable event fields used for the suppression.



Suppress Notable Events

Check a set of fields below you wish to suppress.

☑	Field	Value
☑	src	__jdbc__
□	app	oracle
□	asset_identity	0
□	count	6
□	dest_count	1
□	drilldown_earliest	1465596720.000
□	drilldown_earliest_offset	$info_min_time$
□	drilldown_latest	1465600320.000
□	drilldown_latest_offset	$info_max_time$
□	drilldown_name	View all login failures by system src for the application app
□	drilldown_search	| datamodel Authentication Failed_Authentication search | search Authentication.src="src" Authentication.app="app"
□	event_hash	8b507f94cf569264ae0946ecb46aa50f
□	event_id	F224306C-E71B-41C7-8880-A03EB157DECE@@notable@@8b507f94cf569264ae0946ecb46aa50f

8. Save changes.

This example notable event suppression hides all notable events created after June 10, 2016 that contain a `src=_jdbc_` field from Incident Review.

You cannot suppress notable events from the **Search** dashboard.

Included adaptive response actions with Splunk Enterprise Security

Splunk Enterprise Security includes several adaptive response actions that you can run on a notable event from Incident Review.

- Analyze the risk from assets and identities
- Modify a risk score with a risk modifier
- Start a stream capture with Splunk Stream
- Ping a host
- Run nbtstat
- Run nslookup
- Add threat intelligence

Note: ES administrators can configure these and additional adaptive response actions to be triggered by correlation searches. See Configure adaptive response actions for a correlation search in Splunk Enterprise Security in Administer Splunk Enterprise Security.

> Search commands and adaptive response actions such as ping, nbtstat, and nslookup can no longer send results to customized indexes. Results from search commands and adaptive response actions such as ping, nbtstat, and nslookup are written to the default index.

Analyze the risk from assets and identities

Analyze the risk posed by assets and identities by adding adaptive response actions to correlation searches. You can assign risk as an adaptive response action by adding a risk message, modifying risk scores, and assigning potential sources of threat.

1. Click **Add New Response Action** and select **Risk Analysis**.
2. Type a **Risk Message**. For example: `Flag users based on command line usage.`
3. Add risk modifiers to the notable by assigning values for the following fields:

Field	Description	Example
Risk score	Positive or negative integer or a decimal number to assign a value to the risk object, which is any asset or identity.	`10`
Risk Object Field	Name of a field that exists in the correlation search so that the risk score can be applied to that field.	`dest` (destination) or `src` (source)
Risk Object Type	\`risk_object_types\` macro.	system, user, other

4. Click **+** to add additional risk modifiers.
5. Add values for objects that may be potential sources of threat. For example, if you want to flag users based on their command line usage, enter `command line` for **Threat Object Field** and `Command` for **Threat Object Type**.
6. Click **Save**.

Modify a risk score with a risk modifier

Modify a risk score as a result of a correlation search or in response to notable event details with the **Risk Analysis** adaptive response action. The risk adaptive response action creates a risk modifier event. You can view the risk modifier events on the Risk Analysis dashboard in Enterprise Security.

1. Click **Add New Response Action** and select **Risk Analysis**.
2. Type the score to assign to the risk object.
3. Select a field from the notable event to apply the risk score to for the **Risk Object Field**.
4. Select the **Risk Object Type** to apply the risk score to.

Run a script

Run a script stored in `$SPLUNK_HOME/bin/scripts`.

1. Click **Add New Response Action** and select **Run a script**.
2. Type the filename of the script.

More information about scripted alerts can be found in the Splunk platform documentation.

- For Splunk Enterprise, see Configure scripted alerts in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud Platform, see Configure scripted alerts in the Splunk Cloud Platform *Alerting Manual*.

Start a stream capture with Splunk Stream

Start a Stream capture to capture packets on the IP addresses of the selected protocols over the time period that you select. You can view the results of the capture session on the Protocol Intelligence dashboards.

A stream capture will not work unless you integrate Splunk Stream with Splunk Enterprise Security. See Splunk Stream integration.

1. Click **Add New Response Action** and select **Stream Capture** to start a packet capture in response to a correlation search match.
2. Type a **Description** to describe the stream created in response to the correlation search match.
3. Type a **Category** to define the type of stream capture. You can view streams by category in Splunk Stream.
4. Type the comma-separated event fields to search for IP addresses for the Stream capture. The first non-null field is used for the capture.
5. Type the comma-separated list of protocols to capture.
6. Select a **Capture duration** to define the length of the packet capture.
7. Type a **Stream capture limit** to limit the number of stream captures started by the correlation search.

Ping a host

Determine whether a host is still active on the network by pinging the host.

1. Click **Add New Response Action** and select **Ping**.
2. Select the field that contains the host that you want to ping in the **Host Field**.
3. Type the number of maximum results that the ping returns. Defaults to 1.

Run nbtstat

Learn more about a host and the services that the host runs by running nbtstat. You must have nbtstat installed on the search head for this to run successfully.

1. Click **Add New Response Action** and select **Nbtstat**.
2. Select the field that contains the host that you want to run the nbtstat for in the **Host Field**.
3. Type the number of maximum results that the nbtstat returns. Defaults to 1.

Run nslookup

Look up the domain name of an IP address, or the IP address of a domain name, by running nslookup. You must have nslookup installed on the search head for this to run.

1. Click **Add New Response Action** and select **Nslookup**.
2. Select the field that contains the host that you want to run the nslookup for in the **Host Field**.
3. Type the number of maximum results that the nslookup returns. Defaults to 1.

Add threat intelligence

Create threat artifacts in a threat collection.

1. Click **Add New Response Action** and select **Add Threat Intelligence**.
2. Select the **Threat Group** to attribute this artifact to.
3. Select the **Threat Collection** to add the threat artifact to.
4. Select the **Field from event** that contains the value to add as a threat artifact to the threat intelligence collection.

5. Type a **Description** for the threat artifact.
6. Type a **Weight** associated with the threat list. Defaults to 1.
7. Type a number of **Max Results** to specify the number of results to process as threat artifacts. Each unique search field value counts as a result. Defaults to 100.

How urgency is assigned to notable events in Splunk Enterprise Security

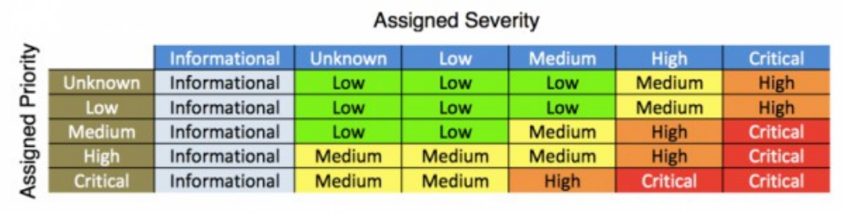
The urgency_lookup determines the urgency level by using both the severity and priority value assigned to the notable that is generated from the correlation search and the priority assigned to specific fields in the assets and identities.

The following fields are used to determine priority when priority is assigned through an asset and identity lookup:

- For identities: `user` or `src_user`
- For assets: `dest`, `src`, or `dvc`

The severity value is set directly on the notable that is generated by the correlation search. If both the asset and identity in the notable event have an assigned priority, the higher priority is used to calculate the urgency. You may use the **Urgency** field to prioritize the investigation of notable events.

This table provides an example of how the urgency values are calculated in notable events by default. The default results can be overwritten by modifying priority and rank, search syntax, or urgency lookups.



Assigned Priority	Assigned Severity					
	Informational	Unknown	Low	Medium	High	Critical
Unknown	Informational	Low	Low	Low	Medium	High
Low	Informational	Low	Low	Low	Medium	High
Medium	Informational	Low	Low	Medium	High	Critical
High	Informational	Medium	Medium	Medium	High	Critical
Critical	Informational	Medium	Medium	High	Critical	Critical

- If event severity is informational, the event urgency is informational, regardless of asset priority.
- If asset priority is unknown or low and event severity is unknown, low, or medium, the event urgency is low.
- If asset priority is unknown or low and event severity is high, the event urgency is medium.
- If asset priority is unknown or low and event severity is critical, the event urgency is high.
- If asset priority is unknown or low and event severity is critical, the event urgency is high.
- If asset priority is medium and event severity is unknown or low, the event urgency is low.
- If asset priority is medium and event severity is medium, the event urgency is medium.
- If asset priority is medium and event severity is high, the event urgency is high.
- If asset priority is medium and event severity is critical, the event urgency is critical.
- If asset priority is high and event severity is unknown, low, or medium, the event urgency is medium.
- If asset priority is medium and event severity is high, the event urgency is high.
- If asset priority is medium and event severity is critical, the event urgency is critical.
- If asset priority is critical and event severity is unknown or low, the event urgency is medium.
- If asset priority is critical and event severity is medium, the event urgency is high.
- If asset priority is critical and event severity is high or critical, the event urgency is critical.

A notable event can be assigned an "unknown" urgency level if the priority value from the asset and identity lookups or the severity value assigned by the correlation search or in a triggering event is not recognized by Enterprise Security.

Incident Review filters on the urgencies of "high", "medium", "low", "critical", "informational", or "unknown." Any value that is not one of the filtered urgencies also defaults to "unknown". This ensures that all notable events are displayed in

Incident Review.

You may also modify the urgency level once the notable is created and this modified value for urgency is then used by the incident review lookup.

Modify notable event urgency

Use one of the following methods to modify the urgency assigned to notable events:

- Modify priority and rank in the Asset and Identity Framework
- Modify notable event severity in correlation search syntax
- Modify the urgency lookup directly

Modify priority and rank in the Asset and Identity Framework

When asset and identity correlation is enabled, if you have made your lookups automatic, the Asset and Identity Framework helps to calculate the event urgency. When a correlation search runs, the results are enriched with the data from these automatic lookups. The priority field in an automatic lookup table affects notable event urgency. See Correlation Setup for enabling correlation and making lookups automatic.

You can rank the order of your asset and identity lists to determine priority for merging assets and identities. For example, if you have identity lists called source A and source B:

Source A	Source B
• identity=foo • priority=low • rank=1	• identity=foo • priority=high • rank=2

These merge on the matching key identity fields, and the priority is set to low. Source A is the higher rank, therefore takes higher precedence when merging single valued fields. If two or more sources have the same rank, then the last nonempty value is the priority. See Rank the order for merging assets and Rank the order for merging identities for merge ranking.

See Search preview for testing the merge to collections.

The data is merged into three different collections: asset_lookup_by_str, asset_lookup_by_cidr, and identities_lookup_expanded. Lookups on these collections are based on a primary key. Therefore, an event is typically not enriched by both an asset and an identity collection. However, if it does happen, then a field such as priority would be displayed depending on its alias as defined in `props.conf`. If there is an event that is enriched by both asset and identity lookups, then the event has the fields `dest_priority`, `dvc_priority`, and `src_priority` (coming from asset enrichment) and `src_user_priority` and `user_priority` (coming from identity enrichment).

See Reset collections to reset the collections.

Modify notable event severity in correlation search syntax

Potentially modify the urgency of a notable event by defining severity in the correlation search syntax. You must have access to edit correlation searches to make these changes.

For example, if you want to change the severity of a correlation search according to the number of failures in the search results. To set a "critical" severity when there are more than 100 failures, a high severity when there are more than 50 failures, and a medium severity for the rest of the results, add search syntax like the following example to the end of the correlation search:

```
... | eval severity=case(failure>100,"critical",failure>50,"high",failure<=50,"medium")
```

Severity defined in the search syntax results in an event where severity takes precedence over the severity defined in the notable event adaptive response action.

Modify the urgency lookup directly

You can change which severity and priority values result in which calculated urgency values for notable events in Splunk Enterprise Security.

Only specific values are valid for severity or priority values. Use only those values when modifying the lookup. Do not modify the names of the notable event urgency values.

- Valid severity values: unknown, informational, low, medium, high, critical.
- Valid priority values: unknown, low, medium, high, critical.
- Valid urgency values: informational, low, medium, high, critical.

1. On the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Choose the **Urgency Levels** lookup. An editable, color coded table representing the urgency lookup file displays.
3. In any row where the **priority** or **severity** is listed as **unknown**, review the assigned **urgency**.
4. (Optional) Edit the table and change the **urgency** to another one of the accepted values. All urgency values must be lower case.
5. Click **Save**.

Investigations

Investigations in Splunk Enterprise Security

Visualize and document the steps you take during an investigation by creating and adding details to an investigation in Splunk Enterprise Security.

- Start an investigation in Splunk Enterprise Security.
- Investigate a potential security incident on the investigation workbench in Splunk Enterprise Security
- Add details to an investigation in Splunk Enterprise Security.
- Make changes to an investigation in Splunk Enterprise Security.
- Collaborate on an investigation in Splunk Enterprise Security.
- Review an investigation in Splunk Enterprise Security.
- Share or print an investigation in Splunk Enterprise Security.
- Review the summary of an investigation in Splunk Enterprise Security.

You can start, manage, and add details to investigations on the Investigations page. View or filter the investigations assigned to you, or create one. You can view all investigations that you collaborate on using the Investigations page. Enterprise Security admins can also view and manage all investigations that exist in Splunk Enterprise Security. For information for admins, see Manage investigations in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

As an analyst, you only see investigations assigned to you unless you also have been granted the capability to manage all investigations.

Manage your investigations

Manage ongoing investigations from the Investigations page. You can see the titles, descriptions, time created, last modified time, and collaborators on the investigations assigned to you. If you have the capability to manage all investigations, you can see all the same details for all investigations, not just the investigations that you collaborate on.

Find an investigation or refine the list of investigations by filtering. Type in the **Filter** box to search the title and description fields of investigations.

Example investigation workflow

1. You are notified of a security incident that needs investigation through a notable event, an alert action, or an email, ticket from the help desk, or a phone call.
2. Create an investigation in Splunk Enterprise Security.
3. Add colleagues to the investigation as collaborators.
4. Open the investigation and start investigating on the workbench.
5. Add artifacts to the investigation scope, in addition to those added automatically from notable events.
6. Review the tabs and panels for information relevant to your investigation, such as additional affected assets or details about the affected assets that can accelerate your investigation.
7. As you investigate, add helpful or insightful events, actions, and artifacts to the investigation to record the steps you took in your investigation.
    1. Run searches, adding useful searches to the investigation from your action history with the investigation bar or relevant events using event actions. This makes it easy to replicate your work for future, similar investigations, and to make a comprehensive record of your investigation process.

    2. Filter dashboards to focus on specific elements, like narrowing down a swim lane search to focus on a specific asset or identity on the asset or identity investigator dashboards. Add insightful filtering actions from your action history to the investigation using the investigation bar.
    3. Triage and investigate potentially-related notable events. Add relevant notable events to the investigation.
    4. Add notes to record other investigation steps, such as notes from a phone call, email or chat conversations, links to press coverage or social media posts. Upload files like screenshots or forensic investigation files.
8. Complete the investigation and close the investigation and optionally, close associated notable events.
9. Review the investigation summary and share it with others as needed.

Start an investigation in Splunk Enterprise Security

You can start an investigation in several ways in Splunk Enterprise Security.

- Start an investigation from Incident Review while triaging notable events. See Add a notable event to an investigation.
- Start an investigation with an event workflow action. See Add a Splunk event to an investigation.
- Start an investigation from the Investigations page.
- Start an investigation when viewing a dashboard using the investigation bar.

After you start an investigation, you can investigate assets and identities using the investigation workbench, and start adding details to the investigation.

By default, users with the **ess_admin** and **ess_analyst** roles can start an investigation.

Start an investigation from the Investigations page

Start an investigation from the Investigations page.

1. Click **Create New Investigation**.
2. Type a title.
3. Select a status.
4. (Optional) Type a description.
5. Click **Save**.

Start an investigation from the investigation bar

When viewing dashboards in Splunk Enterprise Security, you can see an investigation bar at the bottom of the page. You can use the investigation bar to track your investigation progress from any page in Splunk Enterprise Security.

1. Click the + icon to create an investigation.
2. Type a title.
3. Select a status.
4. (Optional) Type a description.
5. Click **Save**.

The investigation is loaded in the investigation bar.

Investigate a potential security incident on the investigation workbench in Splunk Enterprise Security

Investigate assets and identities, or artifacts, involved in a potential security incident on the investigation workbench. After you create an investigation in Splunk Enterprise Security, you can start using the workbench for that investigation. Each investigation has a separate workbench.

When you investigate artifacts on an investigation workbench, by default you see Context, Endpoint Data, and Network Data tabs. Those tabs contain panels that help you gain context into the assets and identities you investigate, endpoint-related data such as file system activity, and network data such as network traffic.

Add artifacts to the scope of your investigation

As part of your investigation on the workbench, you can add assets, identities, files, and URLs as artifacts to the scope of your investigation so that you can verify whether or not they are affected by, or participants in, the overall security incident.

- Add artifacts automatically from a notable event. See Set up artifact extraction for notable events in *Administer Splunk Enterprise Security*.
- Add artifacts manually. See Manually add artifacts to the scope of your investigation in this topic.
- Add artifacts from a workbench panel. See Add artifacts from a workbench panel in this topic.
- Add artifacts from an event on the investigation. See Add artifacts from a raw event on the investigation in this topic.

For example, if you're investigating a malware outbreak at your organization, you can add hosts to the scope that you suspect are infected with malware without adding the associated events to the timeline and recording them as verifiably compromised. Add them to the scope first and review the relevant panels for additional context. If you discover that an artifact is part of the security incident you are investigating, you can add the event or detail that revealed that insight to the investigation to record that information for later.

> You can add any value as an artifact on the workbench. Assets and identities added as artifacts to the scope are not limited to the assets and identities in the asset and identity framework in Splunk Enterprise Security.

Manually add artifacts to the scope of your investigation

When artifacts are extracted, duplicates are not created if they already exist in the investigation. You will see a notification that "the following artifacts already exist and have not been added." The existing artifact is not linked against the new notable event that would have caused the duplicate artifact to be created. This does not prevent you from manually adding a duplicate artifact.

You can manually add artifacts such as assets, identities, files, or URLs to the scope of your investigation on the workbench.

1. From the ES menu bar, select **Investigations**.
2. Open an investigation to view the workbench for that investigation.
3. On the Artifacts panel, click **Add Artifact**.
    - ♦ To add one artifact, use the default **Add artifact** tab:
        1. For **Artifact**, type the value of the artifact.
        2. For **Type**, select the type of the artifact: Identity, Asset, File, or URL.
           The file artifact is a filename, file hash, or file path.

3. (Optional) Type a description.
   For example, Personal computer infected by ransomware.
4. (Optional) Type one or more labels to contextualize the entity. Press **enter** to add a label, or use a comma-separated entry for multiple labels.
   For example, ransomware, laptop, mac.
5. (Optional) Click **Expand Artifacts** to look up the asset or identity in the asset or identity lookups and add the correlated artifacts to the investigation scope.

   > Only assets and identities can be expanded.

- To add multiple artifacts:
   1. Select the **Add multiple artifacts** tab.
   2. Select the **Type**: Identity, Asset, File or URL. All artifacts that you add must be the same type. The file artifact is a filename, file hash, or file path.
   3. You can use a comma or a line break as a delimiter. Select a **Separator** that delimits the list of assets or identities.
   4. Type or paste the values for the assets or identities, using the separator specified in the previous step.
   5. (Optional) Type a description to apply to all artifacts that you are adding.
      For example, Potentially-infected computers in the HR department.
   6. (Optional) Type one or more labels to apply to all artifacts that you are adding. Press **enter** to add a label, or use a comma-separated entry for multiple labels.
      For example, ransomware, laptop, mac.

4. Click **Add to Scope** to add the artifacts to your investigation scope.

The artifacts that you add to your investigation scope manually are automatically selected so that you can click **Explore** and continue your investigation with the new artifacts.

The labels can be seen under the workbench tab if you hover over the artifact and select the information icon (**i**). Labels can also be seen under the summary tab.

Add artifacts from a workbench panel

If a workbench panel has drilldown enabled, you can add field values as artifacts from the panel.

1. Open the investigation and view the workbench.
2. Select artifacts and click **Explore**.
3. In a panel, click a field value.
   The Add Artifact dialog box appears with the value already added.
4. Select a **Type** for the artifact. Some types, such as IP addresses, are automatically detected.
5. (Optional) Add a description for the artifact.
6. (Optional) Add labels for the artifact.
7. (Optional) Click **Expand Artifacts** to look up the asset or identity in the asset or identity lookups and add the correlated artifacts to the investigation scope.
8. Click **Add to Scope** to add the artifact to your investigation scope.

The ability to add artifacts replaces any other drilldown that might exist on the panel. See Administer and customize the investigation workbench in *Administer Splunk Enterprise Security*.

Add artifacts from a raw event on the investigation

After you add an event to the investigation, you can add field values from the event as artifacts to your investigation scope.

1. Open the investigation and view the **Timeline** of the investigation.
2. Locate the event in the **Slide View**.
3. Click **Details** to view a table of fields and values in the event.
4. Click the value that you want to add to the investigation scope.
   The Add Artifact dialog box appears with the value already added.
5. Select a **Type** for the artifact. Some types, such as IP addresses, are automatically detected.
6. (Optional) Add a description for the artifact.
7. (Optional) Add labels for the artifact.
8. (Optional) Click **Expand Artifacts** to look up the asset or identity in the asset or identity lookups and add the correlated artifacts to the investigation scope.
9. Click **Add to Scope**.

Adjust the time range of your investigation

If there are notable events on the investigation, the workbench searches over a suggested time range based on the times of the notable events on the investigation. Time analysis suggests a time range based on the `_time` value of the earliest and latest notable events on the investigation.

If there are no notable events on an investigation, the workbench uses your default time range settings. See Change the default time range in the *Search Manual*.

If a time range is defined in the XML or in the search of a prebuilt panel, that time range takes precedence over the time range that you choose on the workbench.

Add new tabs and profiles to the workbench

Your administrator can develop additional panels, tabs, and profiles, which you can then add to the workbench to further simplify your investigation process. See Administer and customize the investigation workbench.

Add the new profiles and tabs to an investigation workbench.

1. Open an investigation and click **Explore** to explore artifacts on the workbench.
2. Click **Add Content**.
3. To load a profile on the workbench, click **Load profile**.
    1. Select a profile.
    2. Click **Save**.
4. To add a tab to the workbench, click **Add single tab**.
5. Select a profile or a tab.
    1. Click **Save**.

Tabs and profiles that you add to the investigation workbench disappear when you refresh the workbench. Only the default tabs display.

Cloud alerts use case

Add a single tab to the investigation workbench for importing cloud-alerts-related notable events into an investigation and getting context about what you are investigating.

See the previous add new tabs to the workbench section. Select the **Alerts** tab from the drop-down menu.

The pre-built panels in the Alerts tab reference investigative searches from the existing analytic stories that are related to infrastructure as a service, and they leverage the cloud-related fields in the Alerts data model. See Alerts.

You can see alert events over time by source, destination, user, and signature id. You can also see alert events over time by app for severity and by app for MITRE technique ID.

Cloud authentication use case

Add a single tab to the investigation workbench for importing cloud-authentication-related notable events into an investigation and getting context about what you are investigating.

See the previous add new tabs to the workbench section. Select the **Authentication** tab from the drop-down menu.

The pre-built panels in the Authentication tab reference investigative searches from the existing analytic stories that are related to infrastructure as a service, and they leverage the cloud-related fields in the Authentication data model. See Authentication.

The panels also support the concept of filtering based on the account ID. Expand the panels to full size, so that you can load all user activity across all your cloud vendor accounts, filter down to a specific account and specific user, or see which apps and agents are involved in privilege escalations (such as `sudo su -` or short-lived credentials for service accounts).

Cloud network traffic use case

Add a single tab to the investigation workbench for importing cloud-network-traffic-related notable events into an investigation and getting context about what you are investigating.

See the previous add new tabs to the workbench section. Select the **Network Traffic** tab from the drop-down menu.

The pre-built panels in the Network Traffic tab reference investigative searches from the existing analytic stories that are related to infrastructure as a service, and they leverage the cloud-related fields in the Network Traffic data model. See Network Traffic.

You can see network traffic details by source, destination, or device. Examples include: the top ports and protocols; accepted traffic over time; rejected traffic per source, destination, or device. The panels also support the concept of filtering based on the vendor account.

Add details to an investigation in Splunk Enterprise Security

As an analyst working on an investigation, add details and evidence to your investigation by adding events, actions, and notes. While you conduct your investigation using Splunk Enterprise Security, you can add notable events or Splunk events that add insight to the investigation. Add searches, suppression filters, and dashboard views to the investigation from your action history. Record important investigation steps that you take, such as phone, email, or chat conversations as notes on the investigation. You can use notes to add relevant information like links to online press coverage, tweets, or upload screenshots and files.

Run a quick search from the investigation bar

Run a search without opening the search dashboard by clicking **Quick Search** 🔍 on the investigation bar. The investigation bar is found at the bottom-right side of the Incident Review page or the Investigation Workbench.

- Add the search to the investigation in the investigation bar by clicking **Add to Investigation**.
- Use the **Event Actions** to add specific events in the search results to an investigation.
- To save the search results at investigation time, click **Export** to export the search results as a CSV file. Add the search results as an attachment to a note on the investigation.
- Click **Open in Search** to view the search results on the Search dashboard.
- Enlarge or shrink your view of the search results by clicking and dragging the corner of the window. Double click to expand the search view to cover most of your screen, or double click again to shrink it.

Add a notable event to an investigation

You can add a notable event to an investigation from the Incident Review dashboard. See Add a notable event to an investigation.

If the status of a notable event changes, or if an adaptive response action is run from the notable event, the investigation is updated with that information.

Add a Splunk event to an investigation

Add an event from the Splunk search page to an investigation. You can only add an event to an investigation from the search page in the Splunk Enterprise Security context.

1. Expand the event details to see the **Event Actions** menu and other information.
2. Click **Event Actions** and select **Add to Investigation**.
3. A dialog box opens.
    1. Select an assignee.
       If you have the manage_all_investigations capability, you can select **User** to see investigations where you are a collaborator or you can select **All** to see all the investigations in the system. If you don't have manage_all_investigations, then the assignee dropdown menu does not appear.
    2. Select from existing investigations, or create one.
       If you have the manage_all_investigations capability, and All selected as an assignee, you can add events to investigations where you are not a collaborator. This is used, for example, when a senior analyst is triaging and assigning events to the investigations of junior analysts.
4. Click **Save**.

See Capabilities specific to Splunk Enterprise Security in the *Installation and Upgrade Manual*.

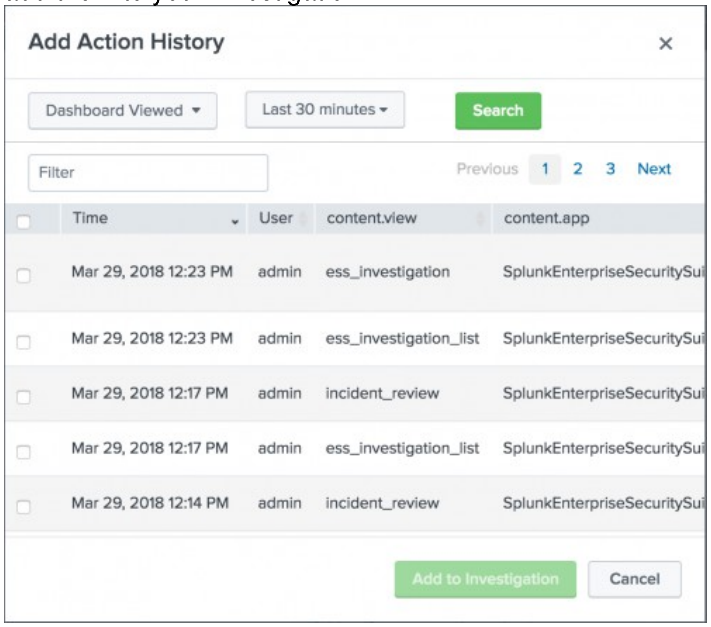
Add an entry from your action history to an investigation

The action history stores a history of the actions that you have performed in Splunk Enterprise Security, such as searches that you have run, dashboards you have viewed, and per-panel filtering actions that you have performed.

Add an entry to an investigation from your action history with the investigation bar. Search for specific types of action history items over time to find the action history items that you want to add to your investigation.

1. From the investigation bar, click the 🕓 icon.
2. Select an action history type and optionally change the time range.

3. Click **Search** to retrieve a list of action history items.
4. Find the actions that you want to add to the investigation. For example, view the dashboards that you viewed to add them to your investigation.



□	Time	User	content.view	content.app
□	Mar 29, 2018 12:23 PM	admin	ess_investigation	SplunkEnterpriseSecuritySui
□	Mar 29, 2018 12:23 PM	admin	ess_investigation_list	SplunkEnterpriseSecuritySui
□	Mar 29, 2018 12:17 PM	admin	incident_review	SplunkEnterpriseSecuritySui
□	Mar 29, 2018 12:17 PM	admin	ess_investigation_list	SplunkEnterpriseSecuritySui
□	Mar 29, 2018 12:14 PM	admin	incident_review	SplunkEnterpriseSecuritySui

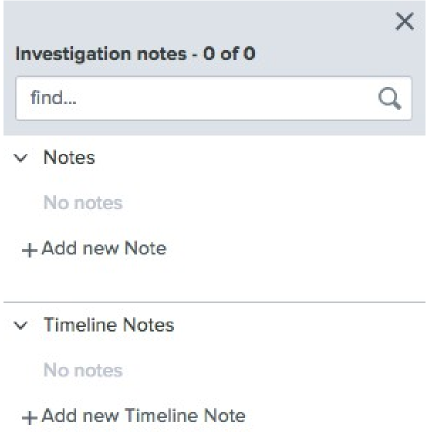
5. The actions that you've taken display in the action history dialog box. You can only add actions from your own action history.
6. Locate the action you want to add and select the check box next to the action or actions that you want to add to the investigation timeline.
7. Click **Add to Investigation**.
   The actions are added to the investigation that you are viewing or that is selected in the investigation bar.

See Refer to your action history.

Add a note to an investigation

Add a note to an investigation to record investigation details or add attachments. You can add a note from dashboards in Splunk Enterprise Security.

1. From the investigation bar, click the ✎ icon.
2. In the investigation notes window, click **Add new Note** or **Add new Timeline Note**.



Timeline notes show up in the timeline slide view, while standard notes do not.

3. Type a title for the note.
   For example, "Phone conversation with police."
4. Select a date and time. The default is the current date and time.
   For example, select the time of the phone call.
5. (Optional) Click the check box to show or hide the note on the timeline.
6. (Optional) Type a description.
   For example, a note to record a phone conversation might include the description: Called the police. Spoke with Detective Reggie Martin. Discussed an employee stealing identities from other employees.
7. (Optional): Attach a file to the note.
    1. In the attachments section, drag the file onto the note or click browse to find the file.
    2. Select a file to add from your computer.
       The maximum file size is 4 MB. You can add multiple files to a note. The first file you add to the note previews on the investigation timeline.
    3. If the filename contains unsupported characters, click the **Replace not supported characters with '-'** and then click **Change**.
       Alternately, you can remove and replace the unsupported characters manually.
8. Click **Add to Investigation** to add the note to the open investigation.

Make changes to an investigation in Splunk Enterprise Security

Make changes to the entries on an investigation from the timeline list or slide view.

Change the title and description of an investigation

Change the title and description of an investigation from the investigation bar. For example, change the name of the investigation as your investigation progresses to more accurately describe the security incident you are investigating.

1. From the investigation bar, click the ✎ icon. From the investigation view, click **Edit**.
2. Change the title or description.
3. Click **Save**.

Update the status of an investigation

Update the status of an investigation from the workbench, summary, or timeline view.

1. While viewing the investigation, click **Edit > Edit title, description, and status**.
2. Select a new status.
3. Click **Save**.

You can also update the status of an investigation from the investigation bar.

1. Click the ☰ icon and select your investigation.
2. After loading your investigation into the investigation bar, click the ✎ icon and select a status.
3. Click **Save**.

Similar to notable events, administrators can customize the statuses available to select, and restrict the status workflow. Because of this, you might not be able to transition from some statuses to other statuses. See Manage and customize investigation statuses in *Administer Splunk Enterprise Security*.

Delete investigation entries

You can delete investigation entries when viewing the investigation timeline list or slide views.

1. Find the entry on the investigation.
2. Click **Action > Delete Entry**.
3. Click **Delete** to confirm deleting the entry.

To delete multiple entries:

1. Click **List** to view the investigation as a list of entries.
2. Select the check box next to the investigation entries that you want to delete.
3. Click **Action** and select **Delete**.
4. Click **Delete** to confirm deleting the entry.

Edit or delete a note

Edit a note by clicking on it in the investigation notes window.

1. From the investigation bar, click the 📝 icon.
2. Select the note.
3. Edit the title, date, timeline display, the note itself, and add or delete attachments.

Alternately, go to the timeline list view to edit or delete the note entry.

1. From the timeline tab, click **List View**.
2. From the actions column, you will see both notes and timeline notes.
3. Select **Edit Entry** to edit it or **Delete Entry** to delete it.

Change the title of an entry

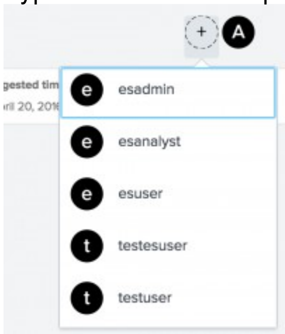
You can change the title of an entry to make it more clear.

1. Locate the notable event, Splunk event, action history item, or other entry on the investigation.
2. From the **Actions** menu, click **Edit**.
3. Change the title.

Collaborate on an investigation in Splunk Enterprise Security

You can collaborate with other analysts on an investigation.

Add a collaborator to an investigation

1. Open the investigation that you want to add a collaborator to.
2. Click the ⊕ icon.
3. Type the name of the person you want to add and select their name from the list to add them to the investigation.


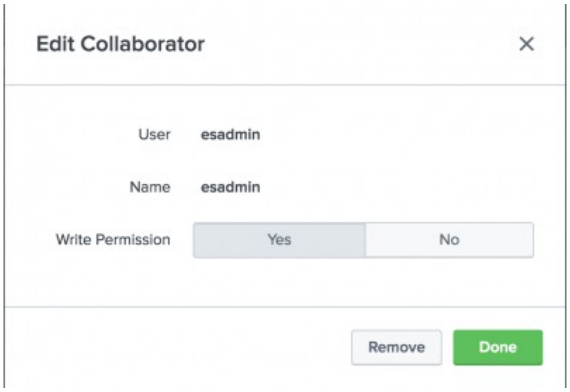
4. Their initials appear in a circle to confirm that they were added.

You can add any Splunk user in your deployment as a collaborator. By default, a collaborator has write permissions on the investigation. The option to add more collaborators to an investigation disappears if all available users have been added to the investigation.

View the collaborators assigned to an investigation

You can view the collaborators assigned to an investigation from an individual investigation or from the Investigations dashboard.

- Hover over the collaborator icons to see the names of the collaborators on your investigation.
- If a collaborator does not have write permissions for an investigation, the icon is gray and **(read-only)** is appended to their name.
- Click the icon of a collaborator to see information about them. See their name and the permissions that the user has for the investigation.



Edit Collaborator

User esadmin

Name esadmin

Write Permission Yes No

Make changes to the collaborators on an investigation

If you are a collaborator on an investigation with write permissions, you can change the permissions of other collaborators on the investigation.

1. Click the icon of a collaborator.
2. Change the **Write permissions**. By default, all collaborators have **Yes** for **Write permissions**. All investigations must have at least one collaborator with write permissions.

You can remove a collaborator if they are not the only collaborator on the investigation with write permissions.

1. Click the icon of a collaborator.
2. Click **Remove**.

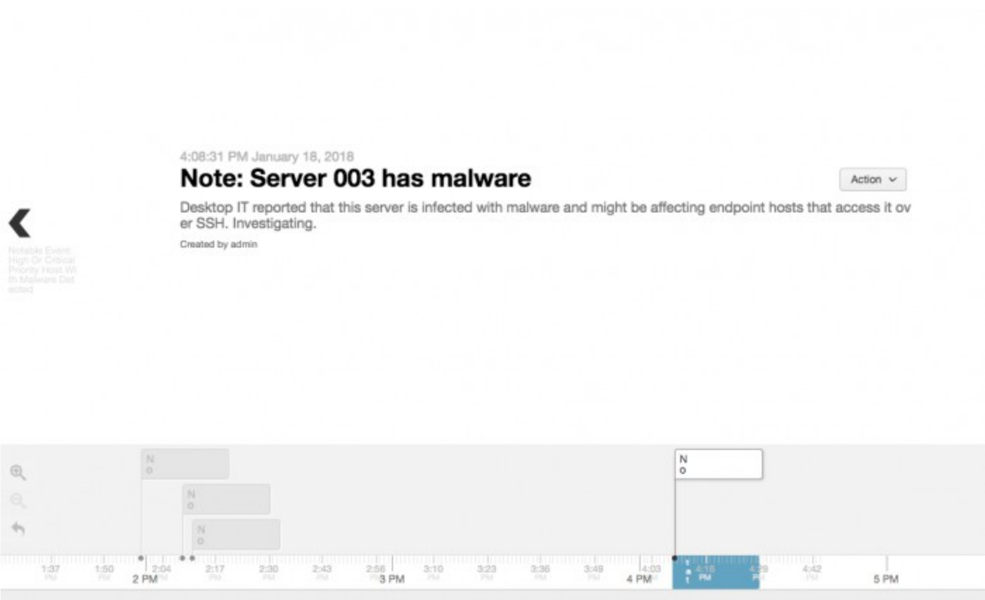
Review an investigation in Splunk Enterprise Security

Revisit past investigations, or view a current investigation by clicking the title from the investigation bar or from the Investigations page. Users with the capability to manage all investigations can view all investigations. Only collaborators on an investigation with write permissions can edit an investigation. See Manage access to investigations in *Administer Splunk Enterprise Security*.

You can also review the summary of an investigation. See Review the summary of an investigation in Splunk Enterprise Security.

Review an entry's investigation for training or research purposes. Click an entry on an investigation to see all details associated with it.

- For notes with file attachments, click the file name to download the file attachment.
- For notable events, click **View on Incident Review** to open the Incident Review dashboard filtered on that specific notable event.
- For action history entries, you can repeat the previously-performed action. For a search action history entry, click the search string to open it in search. For a dashboard action history entry, click the dashboard name to view the dashboard.



4:08:31 PM January 18, 2018

Note: Server 003 has malware

Desktop IT reported that this server is infected with malware and might be affecting endpoint hosts that access it ov er SSH. Investigating.

Created by admin

Gain insight into an attack or investigation by viewing the entire investigation timeline or view only part of it by expanding or contracting the timeline.

Click the timeline to move it and scan the entries. View a chronological list of all timeline entries by clicking the list icon, or refine your view of the timeline using filters. You can filter by type or use the **Filter** box to filter by title.

Review the status history of an investigation

You can review the status history of an investigation visually on the investigation timeline. The timeline changes color to reflect changes in status assignments. The color does not relate directly to the status of the investigation, and is automatically assigned. The colors cannot be changed, customized, or removed.

Share or print an investigation in Splunk Enterprise Security

To share an investigation with someone that does not use Splunk Enterprise Security, such as for auditing purposes, you can print any investigation or save any investigation as a PDF.

1. From the investigation, click the 🖶 icon. Splunk Enterprise Security generates a formatted version of the investigation timeline with entries in chronological order. The order of the entries in the printout remains in the original order, even if you manually edit the times so that they show up differently in the user interface.
2. Print the investigation or save it as a PDF using the print dialog box options.

Refer to your action history in Splunk Enterprise Security

While you investigate an attack or other security incident, actions that you take in Splunk Enterprise Security are recorded in your action history. You can only view your own entries in your action history. After you add an item to an investigation, all collaborators on the investigation can view that entry.

Your action history tracks the following types of actions using searches:

- Dashboards you visit
- Searches you run
- Per-panel filtering actions you take
- Changes you make to a notable event
- Changes you make to the suppression filters of a notable event

When you select a type of action history to add an investigation, the corresponding search runs to retrieve results. Splunk Enterprise Security tracks these actions to help you add context to an investigation, audit an investigation, and give a complete history of actions taken during an investigation that resulted in relevant findings.

For example, if you run a search that gives helpful information for an investigation, you can add that search to the investigation. You can then find that search string in the investigation, run the search again, or revisit a search to save it as a report when the investigation is over. See Add an entry from your action history to an investigation for more about using your action history when investigating in Splunk Enterprise Security.

Review the summary of an investigation in Splunk Enterprise Security

Every investigation in Splunk Enterprise Security includes a summary. From an investigation, click **Summary** to view the summary. The summary provides an overview of the notable events and the artifacts, or investigated assets and identities, that are associated with your investigation.

You can use the summary to provide an overview of an investigation to a SOC manager or to get an overview of the current state of an investigation before you continue working on it.

The summary reflects a point in time of the investigation, rather than the overall progress of an investigation. Therefore, the artifacts listed on the summary page reflect the artifacts present at the end of the investigation, rather than all artifacts that you investigated on the workbench.

Analytic Stories

Use Analytic Stories for actionable guidance in Splunk Enterprise Security

The Splunk Security Research team writes Analytic Stories that provide actionable guidance for detecting, analyzing, and addressing security threats. An Analytic Story contains the searches you need to implement the story in your own environment. It also provides an explanation of what the search achieves and how to convert a search into adaptive response actions, where appropriate.

By default, the `ess_admin` and `ess_analyst` roles can configure the use case library with relevant Analytic Stories. See Manage Analytic Stories through the use case library in Splunk Enterprise Security in the *Administer Splunk Enterprise Security* manual.

Determine which Analytic Stories to use

You can use common industry use cases to determine which Analytic Stories and searches are useful to you. There are a variety of ways to determine if an Analytic Story contains the searches you need:

- by industry use case
- by framework
- by data

In the following scenario, you know that you're interested in common AWS-related security issues, so you start by filtering on known use cases for cloud security.

1. From the Splunk ES menu bar, select **Configure > Content > Use Case Library**.
2. From the use cases filters on the left, click **Cloud Security**.
3. From an Analytic Story, such as Suspicious AWS EC2 Activities, click the greater than (>) symbol to expand the display.
4. You see the detection searches that are related to this use case.
5. You also see your data sources, data models, and lookups that these searches use.

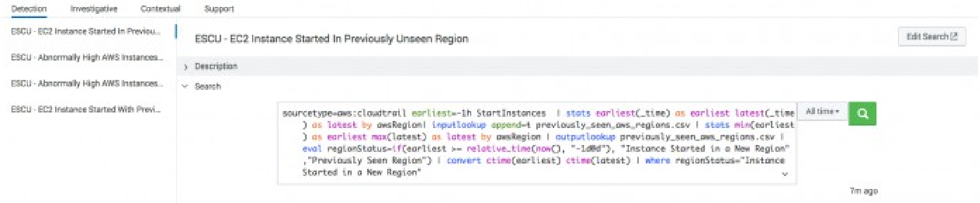
Data Sources	Description
Recommended Data Sources	The type of data sources that are likely to provide valuable data.
Sourcetypes	Your sourcetypes that are in use by the detection searches for this Analytic Story. If the status icon shows a red exclamation mark, hover over the icon to see the reason.
Data Models	Your data that is in use by the detection searches for this Analytic Story as mapped to the Splunk data models via the CIM add-on. If the status icon shows a red exclamation mark, hover over the icon to see the reason.
Lookups	Your lookups that are in use by the detection searches for this Analytic Story. If the status icon shows a red exclamation mark, hover over the icon to see the reason.

You can use an Analytic Story if the recommended data sources, sourcetypes, data models, and lookups do not have red exclamation marks. However, even though green checkmarks indicate that sources are available, they don't always mean that the searches return results based on the ingested data.

Use Analytic Stories to search for results and get guidance

In the following scenario, you know that you're interested in EC2 instances that originate from unusual locations or those launched by previously unseen users, so you start by filtering on known use cases for cloud security.

1. From the Splunk ES menu bar, select **Configure** > **Content** > **Use Case Library**.
2. From the use cases filters on the left, click **Cloud Security**.
3. Click the name of the Analytic Story. In this case, click **Suspicious AWS EC2 Activities**.
   The Analytic Story Details page opens for the story.
    1. From the References section, see any links, white papers, or PDFs provided.
    2. From the Detection section, select a search, such as **ESCU - EC2 Instance Started In Previously Unseen Region**.
    3. From the Search section, click the greater than (>) symbol to expand the display.
    4. Revise the time picker and click **Search** to manually run the search and see the results.

       
       Detection
       Investigative
       Contextual
       Support
       ESCU - EC2 Instance Started In Previou...
       ESCU - Abnormally High AWS Instances...
       ESCU - Abnormally High AWS Instances...
       ESCU - EC2 Instance Started With Previ...
       ESCU - EC2 Instance Started In Previously Unseen Region
       Edit Search
       Description
       Search
       All time
       7m ago

       ```
       sourcetype=aws:cloudtrail earliest=-1h StartInstances  | stats earliest(_time) as earliest latest(_time
           ) as latest by awsRegion| inputlookup append=t previously_seen_aws_regions.csv | stats min(earliest
           ) as earliest max(latest) as latest by awsRegion | outputlookup previously_seen_aws_regions.csv |
           eval regionStatus=if(earliest >= relative_time(now(), "-1d@d"), "Instance Started in a New Region"
           ,"Previously Seen Region") | convert ctime(earliest) ctime(latest) | where regionStatus="Instance
           Started in a New Region"
       ```

    5. From the Known False Positives section, click the greater than (>) symbol to expand the display for tips on when the results might not indicate a problem.

By default, the `ess_admin` and `ess_analyst` roles can enable and schedule to run this search automatically on a regular basis. See Enable and schedule the Analytic Story in the *Administer Splunk Enterprise Security* manual.

Bookmark the Analytic Story

Bookmarks persist per user, so you can bookmark the Analytic Stories that are specific to your duties.

1. From the Splunk ES menu bar, select **Configure** > **Content** > **Use Case Library**.
2. Find the name of the Analytic Story.
3. Toggle the **Bookmark** switch to enable it.
4. From the drop-down filters, select **Bookmarked** > **True** to find your bookmarked stories.

Risk Analysis

Analyze risk in Splunk Enterprise Security

A risk score is a single metric that shows the relative risk of a device or user in the network environment over time. Splunk Enterprise Security classifies a device as a system, a user as a user, and unrecognized devices or users as other.

Enterprise Security uses risk analysis to take note of and calculate the risk of small events and suspicious behavior over time to your environment. The Risk Analysis dashboard displays these risk scores and other risk-related information. Enterprise Security indexes all risk as events in the `risk` index.

How Splunk Enterprise Security assigns risk scores

A risk score is a single metric that shows the relative risk of a device or user object in the network environment over time. An object represents a **system**, a **user**, or an unspecified **other**.

Enterprise Security uses correlation searches to correlate machine data with asset and identity data, which comprises the devices and user objects in a network environment. Correlation searches search for a conditional match to a question. When a match is found, an alert is generated as a notable event, a risk modifier, or both.

- A notable event becomes a task. It is an event that must be assigned, reviewed, and closed.
- A risk modifier becomes a number. It is an event that will add to the risk score of a device or user object.

Risk scoring example

Host 192.0.2.2 is a system that is generating several notable events. The correlation search for **Personally Identifiable Information Detected** is creating five notable events per day for that system.

Using the Risk Analysis dashboard to view the risk for this host shows a risk score of 480.0 in the **Risk Score by Object** and **Most Active Sources** panels for the last seven days by default.

Risk Score by Object				
risk_object	risk_object_type	risk_score	source_count	count
192.0.2.2	system	480.0	1	6

Most Active Sources			
source	risk_score	risk_objects	count
Audit - Personally Identifiable Information Detection - Rule	480.0	1	6

Perhaps 192.0.2.2 is a test server, so this behavior is less interesting than if the same behavior is observed in the production environment. Rather than ignoring or suppressing notable events generated by test servers, you can create specific rules to monitor those servers differently.

You can do this by creating a correlation search that assigns a risk modifier instead of creating a notable event, when the correlation matches hosts that serve as test servers.

1. Isolate test servers from the existing correlation searches using a whitelist. See Whitelist events in *Administer Splunk Enterprise Security* for more information.

2. Create and schedule a new correlation search based on **Personally Identifiable Information Detected**, but isolate the search to the test server hosts and assign a risk modifier alert type only.
3. Verify the risk modifiers are applied to the test server hosts by raising their risk score incrementally. With the new correlation search, no notable events will be created for those hosts based on personally identifiable information.

As the relative risk score goes up, 192.0.2.2 can be compared to similar test servers. If the relative risk score for 192.0.2.2 exceeds its peers, that host would be investigated by an analyst. If the risk scores of some similar test servers are higher relative to others, an internal security policy may need to be reviewed or implemented differently. See the Risk Analysis With Enterprise Security 3.1 blog post for additional examples.

It is also worth noting that risk modifiers cannot be suppressed in the same manner as notable events. Instead, the following options are available:

Correlation Search Aggregation

> You can aggregate multiple firings of a correlation search based on fields and duration via `savedsearches.conf` in the alert.suppress settings. See Savedsearchesconf.

Correlation Search Modification

> To prevent further false positives, you can edit the correlation search syntax to filter events or results.

Assign risk to an object

Create a risk analysis response action, or risk modifier, to assign risk to an object. You can assign risk to objects in several ways.

- Assign risk automatically as part of a correlation search. See Modify a risk score with a risk modifier in *Administer Splunk Enterprise Security*.
- Assign risk on as an ad hoc adaptive response action from Incident Review. See Modify a risk score with a risk modifier in this manual.
- Create an ad hoc risk entry from the Risk Analyis dashboard. See Create an ad hoc risk entry in Splunk Enterprise Security in this manual.
- Assign risk through a search. See Assign risk through a search.

Assign risk through a search

You can assign risk using search rather than an alert. You can do this to modify risk on multiple risk objects, or to alter the risk score of an object based on the results of a search.

Use these search examples to assign risk to a user, system, or other risk object in a custom correlation search. To assign risk to just one field, or on an ad hoc basis, use the risk adaptive response action instead.

Each example uses `...` to indicate a search that includes the field to which you want to assign risk in the results.

Assign risk with the appendpipe command

Use `appendpipe` to add risk to multiple objects. Replace `<your_risk_score_integer>` with the risk score that you want to apply to the fields.

```
... | eval risk_score=<your_risk_score_integer> | eval
risk_object=if(isnotnull(dest),dest,null()),risk_object_type=if(isnotnull(dest),"system",null()) |
appendpipe [| eval
risk_object=if(isnotnull(user),user,null()),risk_object_type=if(isnotnull(user),"user",null())] | sendalert
risk param._risk_score=<your_risk_score_integer>
```

For example, run this search to assign a risk score of 15 to `mysystem` and `myuser`.

```
| makeresults | eval dest="mysystem", user="myuser" | eval
risk_object=if(isnotnull(dest),dest,null()),risk_object_type=if(isnotnull(dest),"system",null()) |
appendpipe [| eval
risk_object=if(isnotnull(user),user,null()),risk_object_type=if(isnotnull(user),"user",null())] | sendalert
risk param._risk_score=15
```

Assign risk with sendalert

You can use `sendalert` without `appendpipe` to assign risk directly to field values, without performing conditional evaluations of the field values.

```
... | sendalert risk param._risk_object_type="system" param._risk_score=<your_risk_score_integer> | eval
risk_object=user | sendalert risk param._risk_object_type="user"
param._risk_score=<your_risk_score_integer>
```

For example:

```
| makeresults | eval dest="mysystem", user="myuser" | sendalert risk param._risk_object="dest"
param._risk_object_type="system" param._risk_score=15 | sendalert risk param._risk_object="user"
param._risk_object_type="user" param._risk_score=20
```

Compute and assign a risk score

You can also set a risk score based on a calculation performed in the search, rather than setting it to a static integer.

For example, if you want to set a higher risk score for users that log into multiple infected assets, write a search that collects the users that logged in to infected assets, then does a count of the users in the results, split by user so that you see how many login attempts there are by each user.

```
... | stats count by user | eval risk_score=(count*2) | sendalert risk param._risk_object="user"
param._risk_object_type="user" param._risk_score="risk_score"
```

For example, the **Threat Activity Detected** correlation search uses search-assigned risk in addition to an alert-type risk modifier. When the search finds an asset or identity communicating with a host that matches a configured threat list, the search modifies the risk score accordingly. In this case, the risk modifier reflects the number of times the system or user communicated with the threat list, multiplied by the weight of the threat list. As a formula, risk score of a system or user + (threat list weight x event count) = additional risk.

```
... | eval risk_score=case(isnum(record_weight), record_weight, isnum(weight), weight, 1=1, null()) |
fields - *time | eval risk_object_type=case(threat_match_field="query" OR threat_match_field=="src" OR
threat_match_field=="dest","system",threat_match_field=="src_user" OR
threat_match_field=="user","user",1=1,"other") | eval risk_object=threat_match_value
```

See the risk score in search

See the changes that you made by searching the data model or the risk correlation lookups:

```
| from datamodel:Risk.All_Risk | search (risk_object=myuser OR risk_object=mysystem)
```

or

```
| makeresults | eval dest="mysystem" | `risk_correlation`
```

Score ranges for risk

Risk scoring offers a way to capture and aggregate the activities of an asset or identity into a single metric using risk modifiers.

The correlation searches included in Enterprise Security assign a risk score between **20** and **100** depending on the relative severity of the activity found in the correlation search. The searches scope the default scores to a practical range. This range does not represent an industry standard. Enterprise Security does not define an upper limit for the total risk score of an identity or asset, but operating systems can impose a limit. For example, 32-bit operating systems limit a risk score to two million.

Risk score levels use the same naming convention as event severity. You can assess relative risk scores by comparing hosts with similar roles and asset priority.

- 20 - Info
- 40 - Low
- 60 - Medium
- 80 - High
- 100 - Critical

ES Admins can edit correlation searches to modify the risk score that the risk analysis response action assigns to an object. See Included adaptive response actions with Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Managing risk objects

Enterprise Security associates risk modifiers with risk objects.

Risk object field

The risk object field is a reference to a search field returned by a correlation search. Correlation searches use fields such as `src` and `dest` to report on matching results. The risk object field represents a system, host, device, user, role, credential, or any object that the correlation search is designed to report on. Review any correlation search that assigns a risk score for examples of fields that receive a risk score.

Risk object types

Splunk Enterprise Security defines three risk object types.

Object type	Description
System	Network device or technology. Can represent a device in the asset lookup.
User	Network user, credential, or role. Can represent an identity in the identity lookup.
Other	Any undefined object that is represented as a field in a data source.

If a risk object matches an object in the asset or identity table, Enterprise Security maps the object as the associated type. For example, an object that matches an asset in the asset lookup is mapped to a risk object type of system. However, devices and users do not need to be represented in the corresponding asset and identity tables to be identified as system or user risk objects. ES categorizes undefined or experimental object types with a risk object type of **Other**.

Resetting a risk score

There is a limitation with completely resetting a risk score for an object. Consider a scenario where a system is infected, the correlation searches generate many notable events for it, which leads to a high risk score. This system is re-imaged, but still has the same IP address or hostname, and you want to reset the risk score to zero as if it's new.

Using the previous example host again of 192.0.2.2 with a 480.0 risk score, you have few options for changing the score to zero because risk scores contain a time component:

- Change the time range picker from the default, and the risk score changes. You might see no results for this host if you change the time range to **Last 15 minutes**. The score is zero if no events are created in that timeframe. This does not reset the score, but helps you verify the new risk score, if you know the timeframe when the system is re-imaged.
- Create an ad-hoc risk entry with a risk score of -480. However, this is very dependent on the timeframe. This also does not actually reset the score. If your ad-hoc risk entry is outside the time window of the event, then the negative offset does not apply, and the object has a score of -480. See Create an ad hoc risk entry in Splunk Enterprise Security.

Create an ad hoc risk entry in Splunk Enterprise Security

Creating an ad-hoc risk entry allows you to make a manual, one-time adjustment to an object's risk score. You can use it to add a positive or negative number to the risk score of an object.

1. Select **Security Intelligence** > **Risk Analysis**.
2. Click **Create Ad-hoc Risk Entry**.
3. Complete the form.
4. Click **Save**.

Risk Modifiers	Description
Risk Score	The number added to a **Risk object**. Can be a positive or negative integer.
Risk object	Text field. Wildcard with an asterisk (*)
Risk object type	Drop-down: select to filter by.

Add a threat object to an ad hoc risk entry in Splunk Enterprise Security

You may add threat objects to an adhoc risk entry to correlate threat objects with risk events and make adjustments to the risk score.

1. Select **Security Intelligence** > **Risk Analysis**.
2. Click **Create Ad-hoc Risk Entry**.
3. Make adjustments to the form as required.
4. Populate the **Threat Object** and the **Threat Object Type** fields.
5. Click **Save**.

Threat Objects	Description
Threat Object	Specify a threat object that poses a threat to the environment, including a command or a script that you must run. For example: `payload`

Threat Objects	Description
Threat Object Type	Type of the threat object. For example: `file_hash`

Use security framework annotations in an ad-hoc risk entry

Use annotations to add context from industry-standard mappings to your ad-hoc risk entry results. Only MITRE ATT&CK definitions are pre-populated for enrichment.

Annotations
Annotations are enriched with industry-standard context.

1. Scroll to **Annotations**.
2. Add annotations for the common framework names listed. These fields are for use with industry-standard mappings, but also allow custom values. Industry-standard mappings include values such as the following:

Security Framework	Five Random Mapping Examples
CIS 20	CIS 3, CIS 9, CIS 11, CIS 7, CIS 12
Kill Chain	Reconnaissance, Actions on Objectives, Exploitation, Delivery, Lateral Movement
MITRE ATT&CK	T1015, T1138, T1084, T1068, T1085 This field also contains mitre technique names for you to select because they are pre-populated for enrichment.
NIST	PR.IP, PR.PT, PR.AC, PR.DS, DE.AE

3. Click **Save**.

Dashboard example
Consider MITRE ATT&CK annotations as an example. You see them in dashboards by ID, such as T1015, rather than by the technique name.

Unmanaged Annotations
Unmanaged annotations are not enriched with any industry-standard context.

1. Scroll to **Unmanaged Annotations**.
2. Click **+ Framework** to add your own framework names and their mapping categories. These are free-form fields.
3. Click **Save**.

Search example
Consider unmanaged annotations as an example. If you search the risk index directly, you see your unmanaged annotations.

```
index=risk
```

Search results
Unmanaged annotations display results as `annotations._all` with your `<unmanaged_attribute_value>`, and `annotations._frameworks` with your `<unmanaged_framework_value>`.

i	Time	Event
>	7/22/20 5:34:09.000 PM	1595453646, search_name="AdHoc Risk Score", annotations="{\"example_attack\":[],\"example-net\":[\"nim\",\"butler\",\"koko\"]}", annotations._all="butler", annotations._all="nim", annotations._all="koko", annotations._frameworks="example-net", annotations.example-net="nim", annotations.example-net="butler", annotations.example-net="koko", creator="admin", description="test", info_max_time="+Infinity", info_min_time="0.000", risk_object="testuser", risk_object_type="user", risk_score="10.0"

Dashboard Overview

Introduction to the dashboards available in Splunk Enterprise Security

Splunk Enterprise Security includes more than 100 dashboards to identify and investigate security incidents, reveal insights in your events, accelerate incident investigations, monitor the status of various security domains, and audit your incident investigations and your ES deployment.

The specific dashboards that will be most useful to you depend on how you plan to use Splunk Enterprise Security.

Identify and investigate security incidents

You can identify and investigate security incidents with a suite of dashboards and workflows. Splunk Enterprise Security uses **correlation searches** to identify **notable events** in your environment that represent security incidents.

- Security Posture provides a high-level overview of the notable events in your environment over the last 24 hours. Identify the security domains with the most incidents, and the most recent activity. See Security Posture dashboard.
- Incident Review shows the details of all notable events identified in your environment. Triage, assign, and review the details of notable events from this dashboard. See Incident Review.
- My Investigations shows all investigations in your environment. Open and work investigations to track your progress and activity while investigating multiple related security incidents. See My Investigations.

Accelerate your investigations with security intelligence

A set of security intelligence dashboards allow you to investigate incidents with specific types of intelligence.

- Risk analysis allows you to assess the risk scores of systems and users across your network and identify particularly risky devices and users posing a threat to your environment. See Risk Analysis.
- Protocol intelligence dashboards use packet capture data from stream capture apps to provide network insights that are relevant to your security investigations. Identify suspicious traffic, DNS activity, email activity, and review the connections and protocols in use in your network traffic. See Protocol Intelligence dashboards.
- Threat intelligence dashboards use the threat intelligence sources included in Splunk Enterprise Security and custom sources that you configure to provide context to your security incidents and identify known malicious actors in your environment. See Threat Intelligence dashboards.
- User intelligence dashboards allow you to investigate and monitor the activity of users and assets in your environment. See Asset and Identity Investigator dashboards and User Activity Monitoring.
- Web intelligence dashboards help you analyze web traffic in your network and identify notable HTTP categories, user agents, new domains, and long URLs. See Web Intelligence dashboards.

Monitor security domain activity

Domain dashboards provided with Splunk Enterprise Security allow you to monitor the events and status of important security domains. You can review the data summarized on the main dashboards, and use the search dashboards for specific domains to investigate the raw events.

- Access domain dashboards display authentication and access-related data, such as login attempts, access control events, and default account activity. See Access dashboards.

- Endpoint domain dashboards display endpoint data relating to malware infections, patch history, system configurations, and time synchronization information. See Endpoint dashboards.
- Network domain dashboards display network traffic data provided by devices such as firewalls, routers, network intrusion detection systems, network vulnerability scanners, proxy servers, and hosts. See Network dashboards and Web Center and Network Changes dashboards and Port & Protocol Tracker dashboard.
- Identity domain dashboards display data from your asset and identity lists, as well as the types of sessions in use. See Asset and Identity dashboards.

Audit activity in Splunk Enterprise Security

The audit dashboards provide insight into background processes and tasks performed by Splunk Enterprise Security. Some audit dashboards allow you to review actions taken by users in Splunk Enterprise Security, while others provide insight into your deployment and the status of your data models and content use. See Audit dashboards.

Display visualizations of your Cloud Security environment

You can explore your Cloud Security environment by displaying visualizations of your Amazon Web Services (AWS) and Microsoft 365 environments using the Cloud Security dashboards. You can access the dashboards through the Cloud Security menu and use them for insights into potential security issues such as errors, unusual events, unintended access, and suspicious activity.

- Security Groups for your VPC in Splunk Enterprise Security
- User and Authentication Activity in Splunk Enterprise Security
- Network ACL Analytics in Splunk Enterprise Security
- AWS Access Analyzer in Splunk Enterprise Security
- Microsoft 365 Security in Splunk Enterprise Security

Prerequisites to use Cloud Security dashboards

To onboard Cloud data sources and explore your Cloud Security environment by displaying visualizations of your Amazon Web Services (AWS) and Microsoft 365 environments using the Cloud Security dashboards, you must meet the following prerequisites:

> If you are currently using the Amazon Web Services (AWS) and Microsoft 365 TAs, you can configure your existing indexes following these steps, instead of creating a new index.

1. Create indexes to populate the Cloud Security dashboards. For more information on creating custom indexes, see Create custom indexes.
2. Provide the index name in the Enterprise Security app settings following these steps:
   1. From the Splunk Enterprise Security menu, select **Configure > General > General Settings**. This displays the configuration settings of Splunk Enterprise Security by applications.
   2. Navigate to **AWS Index** or **Microsoft 365**. The default index value for the **AWS Index** is: `aws_security` and the default index value for the **Microsoft 365** is `o365_security`.

> No indexes exist with the default names. You must create your own indexes to populate the Cloud Security dashboards and provide the name of the index field for both AWS Index and the MS 365 Index.

    3. Populate the index name in the app settings for **AWS Index** and **Microsoft 365** Index.
3. Install the Splunk Add-on for Amazon Kinesis Firehose and Splunk Add-on for Microsoft Office 365 from Splunkbase.
    - For more information on installing the add-on, see Splunk Add-on for Amazon Kinesis Firehose
    - For more information on installing the add-on, see Splunk Add-on for Microsoft Office 365

   Installing these add-ons helps to populate the Cloud Security dashboards and use them for insights into potential security issues such as errors, unusual events, unintended access, and suspicious activity.
4. Configure the add-ons to send data to the Splunk platform and prepare the Splunk platform to receive the data.
    - For more information on configuring Splunk Add-on for Amazon Kinesis Firehose, see Configure Firehose.
    - For more information on configuring Splunk Add-on for Microsoft 365, see Configure Microsoft 365

Now you can use the visualizations on the following Cloud Security dashboards to explore your Amazon Web Services (AWS) and Microsoft 365 environments.

Risk factors enabled by default

> You can modify the calculated score for AWS GuardDuty and Security Hub alert risk events.

The following risk factors are enabled by default:

- The Critical Severity Alert risk factor increases the risk when the alert is critical severity.
- The High Severity Alert risk factor increases the risk when the alert is high severity.
- The Medium Severity Alert risk factor does not increase or decrease the risk when the alert is medium severity.
- The Informational Severity Alert risk factor decreases the risk when the alert is informational severity.
- The Low Severity Alert risk factor decreases the risk when the alert is low severity.

Learn more

Security Groups for your VPC in Splunk Enterprise Security

User and Authentication Activity in Splunk Enterprise Security

Network ACL Analytics in Splunk Enterprise Security

AWS Access Analyzer in Splunk Enterprise Security

Microsoft 365 Security in Splunk Enterprise Security

Customize Splunk Enterprise Security dashboards to fit your use case

You can make changes to dashboards and the searches behind dashboard panels to make them more relevant to your organization, environment, or security use cases. View the search behind a dashboard panel with the panel editor to see where the data is coming from. Edit the title of a panel, the search behind a panel, and even the visualization.

- For Splunk Enterprise, see Edit dashboards with the Dashboard Editor in Splunk Enterprise *Dashboards and Visualizations*.
- For Splunk Cloud Platform, see Edit dashboards with the Dashboard Editor in Splunk Cloud Platform *Dashboards and Visualizations*.

Drill down to raw events

Dig deeper into data on dashboards by drilling down to raw events, and use workflow actions to move from raw events to investigating specific fields on dashboards, or performing other actions outside of the Splunk platform.

You can drill down to raw events from charts and tables in dashboards. You can find information about the drilldown behavior in the Splunk platform documentation.

- For Splunk Enterprise, see Use drilldown for dashboard interactivity in Splunk Enterprise *Dashboards and Visualizations*.
- For Splunk Cloud Platform, see Use drilldown for dashboard interactivity in Splunk Cloud Platform *Dashboards and Visualizations*.

Create custom workflow actions

You can take action on raw events with workflow actions. You can also create custom workflow actions. You can find information about workflow actions in the Splunk platform documentation.

- For Splunk Enterprise, see Control workflow action appearance in field and event menus in the Splunk Enterprise *Knowledge Manager Manual*.
- For Splunk Cloud Platform, see Control workflow action appearance in field and event menus in the Splunk Cloud Platform *Knowledge Manager Manual*.

Key indicators in Splunk Enterprise Security

Splunk Enterprise Security includes predefined key indicators that identify key security metrics for the security domains covered by Splunk Enterprise Security. You can view the key indicators on dashboards in Splunk Enterprise Security.

Key indicators provide a visual reference for several security metrics. Key indicator searches populate the security metrics of key indicators.The key indicator searches run against the **data models** defined in Enterprise Security, or the data models defined in the Common Information Model app. Some key indicator searches run against the count of **notable events**.

Interpreting key indicators on dashboards

On dashboards, each key indicator includes a value indicator, a trend amount, a trend indicator, and a threshold value used to indicate the importance or priority of the indicator. The key indicator searches default to running over a **relative time** span of 48 hours.

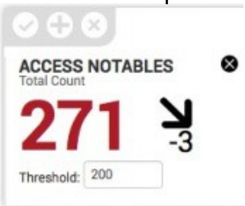
Field	Description
Description	Brief description of the security-related metrics: Access Notables

Field	Description
	The total count and trend of notable events from the Access security domain in incident review. These notable events include titles such as Excessive Failed Logins. Endpoint Notables The total count and trend of notable events from the Endpoint security domain in incident review. These notable events include titles such as Host With A Recurring Malware Infection. Network Notables The total count and trend of notable events from the Network security domain in incident review. These notable events include titles such as Network Change Detected. Identity Notables The total count and trend of notable events from the Identity security domain in incident review. These notable events include titles such as Activity from Expired User Identity. Audit Notables The total count and trend of notable events from the Audit security domain in incident review. These notable events include titles such as Personally Identifiable Information Detected. Threat Notables The total count and trend of notable events from the Threat security domain in incident review. These notable events include titles such as ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days. UBA Notables The total count and trend of notable events from filtering on UBA in incident review, if you're sending threat data from Splunk UBA to Splunk Enterprise Security (ES). See Investigate threats from Splunk UBA using Splunk Enterprise Security in the *Splunk Add-on for Splunk UBA* manual.
Value indicator	Current count of events. If a threshold is set, the numbers will change color as they cross thresholds. Click the value indicator to drill down into the key indicator search and view the raw events. If the value indicator is wrong, such as a percentage value greater than 100%, there could be missing or wrong data in the data model dataset used by the key indicator search to calculate a value.
Trend amount	Displays the change in event count over the time period defined in the key indicator search.
Trend indicator	Displays a directional arrow to indicate the direction of the trend. The arrow changes color and direction over time.

Edit key indicators on dashboards

Enterprise Security includes preconfigured key indicators. Each dashboard key indicator row includes an editor that allows simple, visual changes to be made directly to the key indicators without leaving the dashboard. You can make changes to the search generating the key indicator on the **Content Management** dashboard. See Edit a key indicator search in *Administer Splunk Enterprise Security*.

1. Click the **Edit** pencil icon to the top left of the indicator bar. The editing tools display above the indicators.



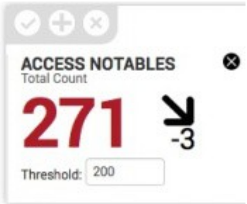
Threshold: 200

2. Drag and drop the indicators to rearrange them. There can be 5 indicators per row, and multiple indicator rows.
3. Click the checkmark icon to save.

Remove key indicators from a dashboard

Remove a key indicator from a dashboard.

1. Click the **Edit** pencil icon to the top left of the indicator bar. The editing tools display above the indicators.



ACCESS NOTABLES
Total Count
271 -3
Threshold: 200

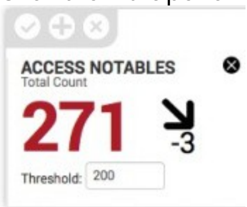
2. Click the **X** to the top right of the indicator.
3. Click the checkmark icon to save.

Removing the indicator from a dashboard does not remove the key indicator from Enterprise Security.

Add key indicators to a dashboard

Add key indicators to a dashboard.

1. Click the **Edit** pencil icon to the top left of the indicator bar. The editing tools display above the indicators.



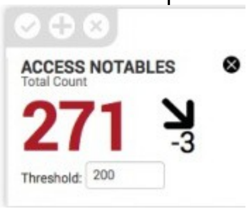
ACCESS NOTABLES
Total Count
271 -3
Threshold: 200

2. Click the plus icon to open the **Add indicators** panel.
3. Click the checkmark icon to save.

Set a threshold for a key indicator on a dashboard

You can set a threshold for a key indicator on a dashboard to change the color of the key indicator. A threshold defines an acceptable value for the event count of an indicator. An event count above the threshold causes the key indicator to display as red, while an event count below the threshold causes the key indicator to display as green. If the threshold is **undefined**, the event count remains black.

1. Click the **Edit** pencil icon to the top left of the indicator bar. The editing tools display above the indicators.



ACCESS NOTABLES
Total Count
271 -3
Threshold: 200

2. Type a **Threshold** for the key indicator.
3. Click the checkmark icon to save.

Dashboard Reference

Security Posture dashboard

The **Security Posture** dashboard is designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a Security Operations Center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.

Dashboard panels

Panel	Description
Key Indicators	Displays the count of notable events by security domain over the past 24 hours. For more information, see Key indicators in Splunk Enterprise Security.
Notable Events by Urgency	Displays the notable events by Urgency for the last 24 hours. Notable Events by Urgency uses an urgency calculation based on the priority assigned to the asset and the severity assigned to the correlation search. The drilldown opens the **Incident Review** dashboard showing all notable events with the selected urgency in the last 24 hours.
Notable Events Over Time	Displays a timeline of notable events by security domain. The drilldown opens the **Incident Review** dashboard showing all notable events in the selected security domain and time frame.
Top Notable Events	Displays the top notable events by rule name, including a total count and a sparkline to represent activity spikes over time. The drilldown opens the **Incident Review** dashboard scoped to the selected notable event rule.
Top Notable Event Sources	Displays the top 10 notable event by `src`, including a total count, a count per correlation and domain, and a sparkline to represent activity spikes over time. The drilldown opens the **Incident Review** dashboard scoped to the selected notable event source.

Executive Summary dashboard

The Executive Summary dashboard is designed to provide a high level insight into security operations so that executives can evaluate security trends over time based on key metrics, notables, risk, and other additional metrics. Use the Executive Summary dashboard to prioritize security operations, monitor the overall health and evaluate the risk to your organization.

Dashboard panels

Key metrics

Panel	Description and default search
Mean Time to Triage	Displays the average time (in minutes) to triage or prioritize the investigation of a notable over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean time taken to triage the notable compares to the previous mean time taken to triage the notable over the same time period. For example, the trendline may display that the mean time to triage a notable over the last 7 days is 0.5% up or down over the mean time taken to triage the notable during the previous 7 day time period. For more information, see Triage notable events in Splunk Enterprise Security.

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | lookup update=true incident_updates_lookup rule_id OUTPUTNEW time | search time=* | stats earliest(_time) as create_time, earliest(time) as triage_time by rule_id | eval diff=triage_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_triage_time | fillnull value=0 mean_triage_time</td></tr>
<tr><td>Mean Time to Resolution</td><td>Displays the average time (in minutes) taken by the notable to reach its configured end status over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean time taken by the notable to reach its configured end status compares to the previous mean time taken by the notable to reach its configured end status over the same time period. For more information, see Take action on notable events in Splunk Enterprise Security.
| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | eval temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUTNEW time, status | `get_reviewstatuses` | search time=* AND status_end=true | stats first(_time) as create_time, last(time) as resolve_time by rule_id | eval diff=resolve_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_resolution_time | fillnull value=0 mean_resolution_time</td></tr>
<tr><td>Investigations Created</td><td>Displays the number of investigations created in the SOC over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean number of investigations created compares to the previous mean number of investigations created over the same time period. For more information, see Start an investigation in Splunk Enterprise Security.
| inputlookup investigation_lookup | where create_time > relative_time(now(), "-14d@d") | stats count(eval(create_time < relative_time(now(), "-7d@d"))) AS past, count(eval(create_time >= relative_time(now(), "-7d@d"))) AS current | transpose | rename "column" as count_type, "row 1" as count</td></tr>
</table>

You can access the Key Performance Indicator (KPI) panel for **Investigations Created** on the Executive Summary Dashboard. Only the admin and the ess_admin roles have the manage_all_investigations capability by default. For all other roles such as ess_analystor ess_user, you see an error message on the **Investigations Created** KPI panel. An administrator can add the manage_all_investigations capability for users that allows other users to access the **Investigations Created** KPI panel on the Executive Summary dashboard. For more information on adding capabilities to a specific role, see Specify role capabilities.

Notables

Panel	Description and default search
Distribution by Urgency	

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>Displays the distribution of the urgency level that is calculated based on the severity and priority level of a notable over the duration of a specified time period. The distribution is based on the following categories: **Critical**, **High**, **Medium**, **Low**, **Information**, and **Unknown**. For more information, see How urgency is assigned to a notable event in Splunk Enterprise Security.
|`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW severity | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT urgency as new_urgency | eval urgency=if(isnotnull(new_urgency),new_urgency,urgency) | `get_urgency` | eval urgency = upper(substr(urgency,1,1)).lower(substr(urgency,2)) | timechart span=1d count by urgency</td></tr>
<tr><td>Notables by Domain</td><td>Displays the classification of the notables by security domains, such as **Access**, **Endpoint**, **Network**, **Threat**, **Identity**, and **Audit** over the duration of a specified time period.
| tstats summariesonly=true earliest(_time) as _time, first(source) as source FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW security_domain | fillnull value="threat" security_domain | lookup update=true security_domain_lookup security_domain OUTPUTNEW label as security_domain_label | timechart span=1d count by security_domain_label</td></tr>
<tr><td>Untriaged Notables by Domain</td><td>Displays the classification the untriaged notables by security domain, such as **Access**, **Endpoint**, **Network**, **Threat**, **Identity**, and **Audit** over the duration of a specified time period.
| tstats summariesonly=true earliest(_time) as _time, first(source) as source FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | eval temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT time as triage_time | where isnull(triage_time) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW security_domain | fillnull value="threat" security_domain | lookup update=true security_domain_lookup security_domain OUTPUTNEW label as security_domain_label | timechart span=1d count by security_domain_label</td></tr>
<tr><td>Top 10 Untriaged Notables by Source</td><td>Displays the top 10 untriaged notables by their sources over the duration of a specified time period.
`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT time as triage_time | where isnull(triage_time) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW rule_name | eval rule_name=if(isnull(rule_name),source,rule_name) | stats count by rule_name | sort - count | head 10</td></tr>
<tr><td>Untriaged Notables by Type</td><td>Displays the classification of notables based on whether they are risk notables or regular notables over the duration of a specified time period.
`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT time as triage_time | where isnull(triage_time) | eval type=if(isnotnull(risk_object), "Risk Notable", "Notable") | timechart span=1d count by type</td></tr>
<tr><td>Frequent Notables Event Sources</td><td>Displays the sources that generate the most number of notables over the duration of a specified time period.</td></tr>
</table>

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>`get_notable_index` | eval source=case(isNotNull(orig_source), orig_source, isNotNull(source_correlation_search), source_correlation_search, 1=1, source) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW rule_name | eval rule_name=if(isnull(rule_name),source,rule_name) | stats count by rule_name | sort - count | head 10</td></tr>
<tr><td></td><td>Displays the sources that generate the least number of notables over the duration of a specified time period.

`get_notable_index` | eval source=case(isNotNull(orig_source), orig_source, isNotNull(source_correlation_search), source_correlation_search, 1=1, source) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW rule_name | eval rule_name=if(isnull(rule_name),source,rule_name) | stats count by rule_name | sort + count | head 10|}</td></tr>
</table>

Risk

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td>Risk Notables vs Notable Events</td><td>Displays a comparison graph of regular notables versus risk notables in the SOC over the duration of a specified time period.

`get_notable_index` | eval notable_type=if(isnotnull(risk_object) AND isnotnull(risk_object_type), "Risk Notable", "Notable") | fields notable_type, count | timechart span=1d count by notable_type</td></tr>
<tr><td>Risk Events Contributing to Risk Notables</td><td>Displays a comparison graph of risk events that generated risk notables versus the risk events that did not generate risk notables over the duration of a specified time period.

(index=risk) OR (`get_notable_index` risk_object=*) | eval source=case(index="risk",source,isnull(orig_source),source_correlation_search,1=1,orig_source),search_time=if(index="notable",mvzip(info_min_time,mvsort(info_max_time)),null()),risk_id=if(index="risk",replace(_bkt,".*~(.+)","\1")."@@".index."@@".md5(_time._raw),null()), risk_id_time=if(index="risk",mvzip(risk_id,_time),null()) | stats values(index) AS index, values(risk_id_time) AS risk_id_time, values(search_time) AS search_time by source, risk_object, risk_object_type | mvexpand risk_id_time | mvexpand search_time | eval risk_id=if(isnull(risk_id_time),null(),mvindex(split(risk_id_time,","),0)),risk_time=if(isnull(risk_id_time),null(),mvindex(split(risk_id_time,","),1)),search_earliest=if(isnull(search_time),null(),mvindex(split(search_time,","),0)), search_latest=if(isnull(search_time),null(),mvindex(split(search_time,","),1)),contributing=if(isnull(search_earliest) OR isnull(search_latest) OR risk_time <= search_earliest OR risk_time >= search_latest,"false","true") | stats values(contributing) as contributing, values(risk_time) as _time by risk_id | eval contributed=if(contributing="true", "Contributed", "Not Contributed") | timechart span=1d count by contributed</td></tr>
<tr><td>Risk Event Types Not Contributing to Risk Notables</td><td>Displays a list in descending order of frequency of the type of risk events that did not generate risk notables over the duration of a specified time period.

(index=risk) OR (`get_notable_index` risk_object=*) | eval source=if(index="notable",if(isnull(orig_source),source_correlation_search, orig_source), source) | stats count, values(index) as index by source | where index != "notable" | `get_correlations` | table rule_name, count | sort - count</td></tr>
</table>

Additional Metrics

Panel	Description and default search
Adaptive Response Actions Triggered	Displays a graph indicating the type and frequency of the adaptive response actions that were triggered over the duration of a specified time period.

Panel	Description and default search
	`| tstats summariesonly=true count from datamodel=Splunk_Audit.Modular_Actions where Modular_Actions.is_Modular_Action_Invocations=1 by _time, Modular_Actions.action_mode, Modular_Actions.action_name | `drop_dm_object_name("Modular_Actions")` | eval action_mode=if(action_mode="saved","automated", action_mode), action_name=action_mode+"-"+action_name | fields - action_mode | timechart span=1d sum(count) as count by action_name`
Sources with Notable Action vs Risk Action Enabled	Displays a graph indicating how many enabled sources have risk actions versus notables actions over the duration of a specified time period. `| inputlookup correlationsearch_changes_lookup | where _time > relative_time(now(),"-7d@d") | sort -_time | bin _time span=1d | dedup label, _time | where (disabled == 0) | mvexpand actions | where actions="notable" OR actions="risk" | eval actions=if(actions="notable", "Notable Action", "Risk Action") | timechart span=1d count by actions`
Correlation Searches Enabled vs Disabled	Displays a bar chart that provides a distribution of the correlation searches enabled versus correlation searches disabled in the SOC over the duration of a specified time period. `| inputlookup correlationsearch_changes_lookup | where _time > relative_time(now(),"-7d@d") | sort -_time | bin _time span=1d | dedup label, _time | timechart span=1d count by disabled | rename 0 as Enabled, 1 as Disabled`

For key indicator panels and time chart visualizations on the Executive Summary dashboard, some arguments in the underlying SPL searches may be dynamically updated based on the time range selected on the dashboard UI.

SOC Operations dashboard

The SOC Operations dashboard is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you can monitor the efficiency of the SOC and ensure that all security operations (detections, analysis, and responses) are on track.

Dashboard panels

Key metrics

Panel	Description and default search
Mean Time to Triage	Displays the average time (in minutes) to triage or prioritize the investigation of a notable over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean time taken to triage the notable compares to the previous mean time taken to triage the notable over the same time period. For example, the trendline may display that the mean time to triage a notable over the last 7 days is 0.5% up or down over the mean time taken to triage the

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>notable during the previous 7 day time period. For more information, see Triage notable events in Splunk Enterprise Security.

| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | lookup update=true incident_updates_lookup rule_id OUTPUTNEW time | search time=* | stats earliest(_time) as create_time, earliest(time) as triage_time by rule_id | eval diff=triage_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_triage_time | fillnull value=0 mean_triage_time</td></tr>
<tr><td>Mean Time to Resolution</td><td>Displays the average time (in minutes) taken by the notable to reach its configured end status over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean time taken by the notable to reach its configured end status compares to the previous mean time taken by the notable to reach its configured end status over the same time period. For more information, see Take action on notable events in Splunk Enterprise Security.

| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | eval temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUTNEW time, status | `get_reviewstatuses` | search time=* AND status_end=true | stats first(_time) as create_time, last(time) as resolve_time by rule_id | eval diff=resolve_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_resolution_time | fillnull value=0 mean_resolution_time</td></tr>
<tr><td>Investigations Created</td><td>Displays the number of investigations created in the SOC over the duration of a specified time period. Also, displays a trendline (in absolute</td></tr>
</table>

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>value) that indicates how the mean number of investigations created compares to the previous mean number of investigations created over the same time period. For more information, see Start an investigation in Splunk Enterprise Security.

| `investigations` all=true strict=true | where create_time > relative_time(now(), "-14d@d") | stats count(eval(create_time < relative_time(now(), "-7d@d"))) AS past, count(eval(create_time >= relative_time(now(), "-7d@d"))) AS current | transpose | rename "column" as count_type, "row 1" as count</td></tr>
</table>

Workflow

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td>Assigned Notables Over Time</td><td>Displays a comparison graph of assigned versus unassigned notables over the duration of a specified time period.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id | `get_current_status` | `get_owner` | timechart span=1d count(eval(owner!="unassigned")) AS "Assigned Notables", count(eval(owner="unassigned")) AS "Unassigned Notables"</td></tr>
<tr><td>Notables in End State by Time</td><td>Displays a comparison graph for notables that are assigned versus the notables that have been resolved i.e. reached the configured end state over the duration of a specified time period.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id | `get_current_status` | `get_owner` | where owner != "unassigned" | timechart span=1d count(eval(status_end="true")) AS "In End State", count AS "Total Assigned"</td></tr>
<tr><td>Analyst Close Rate Over Time</td><td>Displays a comparison graph for assigned open versus assigned closed notables by an analyst over the duration of a specified time period.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id | `get_current_status` | `get_owner` | where owner != "unassigned" | stats count(eval(status_end = "true")) AS "Notables Closed", count(eval(status_end = "false")) AS "Notables Open" by owner_realname | rename owner_realname AS "Analyst"</td></tr>
</table>

Dispositions

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td>Dispositions Over Time</td><td>Displays a distribution of the various dispositions that are assigned to notables over the duration of a specified time period. This visualization provides insight into the number of notables that are false positives versus notables that are true positives. For more information on assigning dispositions to notables, see Add dispositions to notables.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as</td></tr>
</table>

Panel	Description and default search
	source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition) | `get_notable_disposition` | timechart span=1d count by disposition_label
Sources Contributing to False Positive - Incorrect Analytic Logic	Displays a list of sources, which generated notables that have the disposition **False Positive - Incorrect Analytic Logic** over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition) | `get_notable_disposition` | where disposition="disposition:3" | stats count by source | sort - count
Sources Contributing to False Positive - Inaccurate Data	Displays a list of sources, which generated notables that have the disposition **False Positive - Inaccurate Data** over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition) | `get_notable_disposition` | where disposition="disposition:4" | stats count by source | sort - count
Sources Contributing to True Positive - Suspicious Activity	Displays a list of sources, which generated notables that have the disposition **True Positive - Suspicious** over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition) | `get_notable_disposition` | where disposition="disposition:1" | stats count by source | sort - count
Sources Contributing to True Positive - Suspicious but Expected	Displays a list of sources, which generated notables that have the disposition **True Positives - Suspicious, but Expected** over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition) | `get_notable_disposition` | where disposition="disposition:2" | stats count by source | sort - count

For key indicator panels and time chart visualizations on the SOC Operations dashboard, some arguments in the underlying SPL searches may be dynamically updated based on the time range selected on the dashboard UI.

Audit dashboards

Use the audit dashboards to validate the security and integrity of the data in Enterprise Security. Ensure that forwarders are functioning, that data has not been tampered with and is secured in transmission, and that analysts are reviewing the notable events detected by correlation searches.

Incident Review Audit

The **Incident Review Audit** dashboard provides an overview of incident review activity. The panels display how many incidents are being reviewed and by which user, along with a list of the most recently reviewed events. The metrics on this dashboard allow security managers to review the activities of analysts.

Panel	Description
Review Activity by Reviewer	Displays the numbers of events reviewed by each user. This panel is useful for determining which user is performing the incident reviews and if the total number of incidents reviewed is changing over time. The drilldown opens a search with all activity by the selected reviewer.
Top Reviewers	Displays the top users that have performed incident reviews. The panel includes details for each user, including the date they first performed an incident review, the date they last performed a review, and the total number of incidents reviewed. The drilldown opens a search with all activity by the selected reviewer.
Notable Events By Status - Last 48 Hours	Displays the status, count, and urgency for all notable events in the last 48 hours. This panel is useful for determining if the incident review users are keeping up with incidents, or whether a backlog of unreviewed incidents is forming. The drilldown opens the Incident Review dashboard and searches on the selected urgency and status over the lat 48 hours.
Notable Events By Owner - Last 48 Hours	Displays the owner, count, and urgency for all notable events in the last 48 hours. This panel is useful for determining how many events are assigned to a user and the urgency of the events. The drilldown opens the Incident Review dashboard and searches on the selected urgency over the lat 48 hours.
Mean Time to Triage - Last 14 days	Displays the average time it took for a notable event to be triaged after it was created over the last 14 days, split by the name of the notable event. This panel is useful for determining how quickly analysts are triaging notable events, or whether certain types of events take longer to triage than others. The drilldown opens the Incident Review dashboard and searches on the matching notable event names over the last 14 days.
Mean Time to Closure - Last 60 days	Displays the average time it took for a notable event to be closed after it was created over the last 60 days, split by the name of the notable event. This panel is useful for determining how long it takes to close certain types of notable event investigations. The drilldown opens the Incident Review dashboard and searches on the matching notable event names that have a status of closed from the last 60 days.
Recent Review Activity	Displays the 10 most recent changes on the incident review dashboard, such as triage actions. The drilldown opens a search with the selected rule ID.

To audit data from Incident Review from Enterprise Security prior to version 3.2, you must perform an ad hoc search like this example.

```
index=_audit sourcetype=incident_review | rex field=_raw "^(?<end_time>[^,]*),(?<rule
_id>[^,]*),(?<owner>[^,]*),(?<urgency>[^,]*),(?<status>[^,]*),(?<comment>[^,]*),(?<user>[^,]*),(?<rule_name>[^,]*)"
```

Data sources

The reports in the **Incident Review Audit** dashboard reference fields in the notable index and the incident review objects in a KVStore collection. See Notable index on the Splunk dev portal for more on the notable index.

Investigation Overview

The **Investigation Overview** dashboard gives insight into investigations, including monitoring open investigations, time to completion, and number of collaborators. You can filter by investigations where you're a collaborator or by investigations that exist on the system. you can use the **All** filter only if you have the "manage_all_investigations" capability.

In the descriptions that follow, there are references to "progress state" and "end state." Depending on your configuration, progress states can include statuses such as new, pending, and resolved. These states are considered unclosed because there is more work to do on the investigations. Also depending on your configuration, end states can include statuses such as closed, withdrawn, and fixed. These states are considered closed because there is no more work to do on the investigations.

Panel	Description
Unclosed Investigations	Displays the number of investigations in a progress state during the time set in the time range picker. This includes investigations that were closed yesterday but are reopened today, as the only states that are included in this panel are progress states.
Investigations Created	Displays the number of investigations created in the time set in the time range picker.
Investigations Closed	Displays the number of investigations that have reached an end state during the time set in the time range picker. This does not include investigations that were closed yesterday but are reopened today, as the only states that are included in this panel are current end states.
Oldest Unclosed Investigations	Displays the age of the investigations in a progress state during the time set in the time range picker. The investigations are sorted by create time. This is the list of investigations that corresponds to the number shown in the Unclosed Investigations panel.
Total Time Spent On Investigations	Displays the investigations, which were created in the time set in the time range picker, that spent the most cumulative time in a progress state.
Time Unclosed (In Days)	Displays the average and median number of days that investigations spent in a progress state during the time set in the time range picker.
Time To Complete (In Days)	Displays the average and median number of days for investigations to reach an end state during the time set in the time range picker. This includes the total lifetime from when the investigation started, went through states of progress, and even if it reached an end state, then was opened and completed again.
Investigations Unclosed Per Collaborator	Displays the number of investigations in a progress state for each collaborator during the time set in the time range picker, and the status of the investigations.
Investigations Unclosed Per Creator	Displays the number of investigations in a progress state for each person who created an investigation during the time set in the time range picker.
Investigations Unclosed Per Status	Displays the number of investigations in a progress state for each status during the time set in the time range picker.
Number of Collaborators Per Unclosed Investigation	Displays the number of people working on investigations in a progress state during the time set in the time range picker.
Longest Inactive Investigation (Unclosed)	Displays the investigations in a progress state that haven't been modified during the time set in the time range picker. These are investigations that are underway, but are not being actively worked on.
Most Often Reopened	Displays the investigations that have been completed and reopened the most amount of times during the time set in the time range picker.
Investigations Created Per Day	Displays the investigations created each day during the time set in the time range picker.

Suppression Audit

The **Suppression Audit** dashboard provides an overview of notable event suppression activity. This dashboard shows how many events are being suppressed, and by whom, so that notable event suppression can be audited and reported on.

The metrics on this dashboard allow security managers to review the activities of analysts, which is useful for tuning correlation searches. You can identify correlation search rules that are generating more events than your analysts are capable of looking at, and tune them accordingly.

Panel	Description
Suppressed Events Over Time - Last 24 Hours	Displays notable events suppressed in the last 24 hours.
Suppression History Over Time - Last 30 Days	Displays the history of suppressed notable events.
Suppression Management Activity	Displays suppression management activity for the time period.
Expired Suppressions	Displays expired suppressions.

Data sources

The reports in the **Suppression Audit** dashboard reference events in the Notable index.

Per-Panel Filter Audit

The **Per-Panel Filter Audit** dashboard provides information about the filters currently in use in your deployment.

The following table describes the panels for this dashboard.

Panel	Description
Per-Panel By Reviewer	Displays the count of updates to per-panel filters by user
Top Users	Shows users, sparkline for trends, number of views, and first and last time viewed.
Recent Filter Activity	Activity by time, user, action, and filename

Adaptive Response Action Center

The Adaptive Response Action Center dashboard provides an overview of the response actions initiated by adaptive response actions, including notable event creation and risk scoring.

Panel	Description
Action Invocations Over Time By Name	Displays a time chart of the adaptive response actions triggered by name.
Top Actions By Name	Displays the top adaptive response actions by name.
Top Actions By Search	Displays the top adaptive response actions by search.
Recent Response Actions	Displays the most recent adaptive response actions.

Data sources

The reports in the Adaptive Response Action Center dashboard reference fields in the Audit data model. For a list of data model objects and constraints, see Splunk Audit Logs in the *Common Information Model Add-on* manual.

Threat Intelligence Audit

The **Threat Intelligence Audit** dashboard tracks and displays the current status of all threat and generic intelligence sources. As an analyst, you can review this dashboard to determine if threat and generic intelligence sources are current, and troubleshoot issues connecting to threat and generic intelligence sources.

Panel	Description

Intelligence Downloads	Displays the status of all intelligence sources defined on the **Intelligence Downloads** configuration page. Use the filters to sort by status or download location.
Intelligence Audit Events	Displays log events related to intelligence downloads configured on the **Intelligence Downloads** configuration page and modular inputs configured on the **Threat Intelligence Manager** configuration page. Use the filters to sort and filter the events displayed.

If an intelligence download fails, a search automatically creates a system message. See Troubleshoot intelligence downloads in Splunk Enterprise Security.

Data sources

The reports in the **Threat Intelligence Audit** dashboard reference events in the `_internal` index and state information from the `/services/data/inputs/threatlist` REST endpoint.

Machine Learning Audit

The **Machine Learning Audit** dashboard displays information related to usage of the Machine Learning Toolkit (MLTK).

Panel	Description
Machine Learning Toolkit Errors and Failed Fit and Apply Searches - Last 7 days	The `mlspl.log` log file itself doesn't contain a lot of details about specific models and when they ran as part of a search or a rule. As an analyst, you can review this chart to help determine where MLTK errors are happening. It shows all the MLTK errors over the last 7 days. If you click on the chart to drill-down into the details, you can see the audits of failed searches that contain the `fit` or `apply` commands, which can help you correlate errors with the actual searches that produced the issues.
Machine Learning Models	The list shows the names of the MLTK models. If you click on a model name to drill-down into the details, it opens a custom search that helps audit your model generating searches and the corresponding rules that apply them. See Audit searches using an MLTK Model.
List of Model Generating Searches	The button shows all the MLTK model generating searches and their statuses.

ES Configuration Health

Use the ES Configuration Health dashboard to compare the latest installed version of Enterprise Security to prior releases and identify configuration anomalies. The dashboard does not report changes to add-ons (TA.) Select the previous version of Enterprise Security installed in your environment using the Previous ES Version filter.

Mode	Description
Unshipped	The Unshipped setting compares the latest installed version of Enterprise Security with the content in the ES installation package. Any item that was not provided as part of the Enterprise Security installation, such as files or scripts used for customization, is labeled as an Unshipped item. Review Unshipped items to evaluate their use, determine if they are still needed, and reconcile if necessary. The Unshipped setting ignores the Previous ES Version filter.
Removed Stanzas	The Removed Stanzas setting compares the latest installed version of Enterprise Security with the version that you select in the filter. Removed Stanzas are configuration stanzas that changed between versions, such as a deprecated threat list or input. Review Removed Stanzas to evaluate their use, determine if they are still needed, and reconcile if necessary.
Local Overrides	The Local Overrides setting compares the installed version of Enterprise Security with the version that you select in the filter. A setting that conflicts with or overrides the installed version of Enterprise Security is labeled as a Local Override. Review any Local Override settings to evaluate their use, determine if they are still needed, and reconcile if necessary.

Data Model Audit

The **Data Model Audit** dashboard displays information about the state of data model accelerations in your environment.

Field Name Panel	Description
Top Accelerations By Size	Displays the accelerated data models sorted in descending order by MB on disk
Top Accelerations By Run Duration	Displays the accelerated data models sorted in descending order by the time spent on running acceleration tasks.
Accelerations Details	Displays a table of the accelerated data models with additional information.

Data model acceleration can be in progress and 100% complete at the same time. The process running and the status completing are not directly tied together.

Data sources

The reports in the **Data Model Audit** dashboard reference fields in the Splunk Audit data model. For a list of data model objects and constraints, see Splunk Audit Logs in the *Common Information Model Add-on Manual*.

Forwarder Audit

The **Forwarder Audit** dashboard reports on hosts forwarding data to Splunk Enterprise.

Use the search filters and time range selector to focus on groups of forwarders or an individual forwarder.

Filter by	Description	Action
Show only expected hosts	An expected host is a host defined in ES by the expected host field `is_expected` in the Asset table.	Drop-down, select to filter by
Host	Filter by the host field in the Asset table.	Text field. Wildcard with an asterisk (*)
Business Unit	Filter by the business unit `bunit` field in the Asset table.	Text field. Wildcard with an asterisk (*)
Category	Filter by the category field in the Asset table.	Drop-down, select to filter by

Panel	Description
Event Count Over Time By Host	Displays the number of events reported over the time period selected in the filter. The events are split by host.
Hosts By Last Report Time	Displays a list of hosts, ordered by the last time they reported an event.
Splunkd Process Utilization	Displays the resource utilization of the forwarder's Splunk daemon `splunkd`.
Splunk Service Start Mode	Displays the host names that are forwarding events, but are not configured to have `splunkd` start on boot.

Data sources

Relevant data sources for the Forwarder Audit dashboard include data from all forwarders in your Splunk environment and the Application_State data model. See the Common Information Model Add-on Manual for more information. The Common Information Model fields `bunit` and `category` are derived by automatic identity lookup, and do not need to be mapped directly.

Indexing Audit

The **Indexing Audit** dashboard is designed to help administrators estimate the volume of event data being indexed by Splunk Enterprise. The dashboard displays use EPD (Events Per Day) as a metric to track the event volume per index, and the rate of change in the total event counts per index over time. The EPD applies only to event counts, and is unrelated to the Volume Per Day metric used for licensing.

Panel	Description
Key Indicators	The key indicators on this dashboard are scoped to "All Time," not the "Last 24 hours".
Events Per Day Over Time	Displays a column chart representing the event counts per day.
Events Per Day	Displays a table representing event counts per day and the average eps.
Events Per Index (Last Day)	Displays a table of event counts per index for the last day.

Data sources

The reports in the **Indexing Audit** dashboard reference data generated by the `Audit - Events Per Day - Lookup Gen` saved search and are stored within a KVStore collection.

Search Audit

The **Search Audit** dashboard provides information about the searches being executed in Splunk Enterprise. This dashboard is useful for identifying long running searches, and tracking search activity by user.

Panel	Description
Searches Over Time by Type	Shows the number of searches executed over time by type, such as ad-hoc, scheduled, or real-time. Helps determine whether Splunk's performance is being affected by excessive numbers of searches.
Searches Over Time by User	Shows the number of searches executed by each user. Helps determine when a particular user is executing an excessive number of searches. The `splunk-system-user` is the name of the account used to execute scheduled searches in Splunk Enterprise.
Top Searches by Run Time	Lists the most expensive searches in terms of duration. Helps to identify specific searches that may be adversely affecting Splunk performance.

Data sources

The reports in the **Search Audit** dashboard reference scheduled search auditing events from the `audit` index.

View Audit

The **View Audit** dashboard reports on the most active views in Enterprise Security. View Audit enables tracking of views that are being accessed on a daily basis and helps to identify any errors triggered when users review dashboard panels.

Panel	Description
View Activity Over Time	Displays the Enterprise Security views that have the greatest access counts over time. The drilldown opens a search view of all page activity for the time selected.
Expected View Activity	Lists the views set up in the Expected View lookup. You want to review these views on a daily basis for your deployment. Select a dashboard to see details in the Expected View Scorecard panel below. See Manage internal lookups in Splunk Enterprise Security.

Panel	Description
Web Service Errors	Displays errors that occurred while loading the web interface. Helps identify custom views that contain errors or an underlying issue that need to be escalated to Splunk.

Data sources

The reports in the **View Audit** dashboard reference fields in the Splunk Audit data model. For a list of data model objects and constraints, see Splunk Audit Logs in the *Common Information Model Add-on Manual*.

Managed Lookups Audit

The **Managed Lookups Audit** dashboard reports on managed lookups and collections such as services, data, transforms, KV Store lookups, and CSV lookups in Enterprise Security. Managed Lookups Audit shows the growth of lookups over time and the markers for anomalous growth. You can use this to help determine if any managed lookups are growing too large for your particular environment's performance and need to be pruned.

Field	Description
Name	Displays the name of the Enterprise Security lookup. The drill-down takes you to all the contributing events for this particular lookup name from the audit_summary index.
Growth	Lists the lookup size over time as measured via a saved search that writes to the audit_summary index, running every 24 hours, displayed as a sparkline.
Count	Displays the estimated number of rows in the lookup file.
Size	Displays the size of the file in megabytes, sorted by the largest first.

Data Protection

The **Data Protection** dashboard reports on the the status of the data integrity controls.

Panel	Description
Data Integrity Control By Index	Displays a view of all indexes with data protection enabled, sorted by search peer. For more information on configuring and validating data integrity, see Manage data integrity in *Securing Splunk Enterprise*. If you use Splunk Cloud Platform, file a support case to request enablement of data integrity control.
Sensitive Data	Displays the count of events with sensitive data. This panel requires enabling the **Personally Identifiable Information Detected** correlation search. For more information on how the IIN and the LUHN lookups are leveraged by correlation searches and displayed on the Data Protection dashboard, see Internal lookups that you can modify.

Predictive Analytics dashboard

> With Common Information Model Add-on 4.15.0 and later, the Predictive Analytics dashboard is removed. Machine Learning Toolkit functionality can be leveraged instead. MLTK is more robust for finding different varieties of anomalous events in your data than the | predict command used by the Predictive Analytics dashboard. See Machine Learning Toolkit Overview in Splunk Enterprise Security and see Release Notes in the Common Information Model Add-on Manual.

Use the **Predictive Analytics** dashboard to search for different varieties of anomalous events in your data. **Predictive Analytics** uses the predictive analysis functionality in Splunk to provide statistical information about the results, and identify outliers in your data. The predict command can take some time to generate results.

To analyze data with predictive analytics, choose a data model, then an object, a function, an attribute, and a time range, and click **Search**.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The **Predictive Analytics** dashboard filters are implemented in a series from left to right. For example, the **Object** filter is populated based on the **Data Model** selection.

Filter by	Description
Data Model	Specifies the data model for the search. Available data models are shown in the drop-down list.
Object	Specifies the object within the data model for the search. You must select a **Data Model** to apply an **Object**.
Function	Specifies the function within the object for the search. Functions specify the type of analysis to perform on the search results. For example, choose "`avg`" to analyze the average of search results. Choose "`dc`" to create a distinct count of the results.
Attribute	Specifies the constraint attributes within the object for the search. Attributes are constraints on the search results. For example, choose "`src`" to view results from sources. You must select an **Object** to apply an **Attribute**.
Time Range	Select the time range to represent.
Advanced	Access to the options for the predict command.

You can find information about the predict command options in the Splunk platform documentation.

- For Splunk Enterprise, see predict options in the Splunk Enterprise *Search Reference*.
- For Splunk Cloud Platform, see predict options in the Splunk Cloud Platform *Search Reference*.

Dashboard Panels

Panel	Description
Prediction Over Time	The Prediction Over Time panel shows a predictive analysis of the results over time, based on the time range you chose. The shaded area shows results that fall within two standard deviations of the mean value of the total search results.
Outliers	The Outliers panel shows those results that fall outside of two standard deviations of the search results.

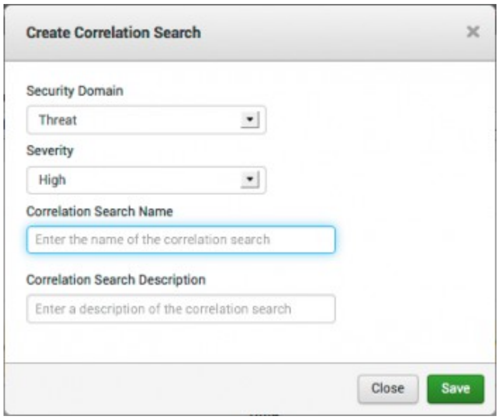
Data sources

The Predictive Analytics dashboard references data in any user selected data model. If the data model accelerations are unavailable or incomplete for the chosen time range, the dashboard reverts to searching unaccelerated, raw data.

Create a correlation search

From this dashboard, create a correlation search based on the search parameters for your current predictive analytics search. This correlation search will create an alert when the correlation search returns an event.

1. Click **Save as Correlation Search...** to open the Create Correlation Search dialog.
2. Select the Security domain and Severity for the notable event created by this search.
3. Add a search name and description.
4. Click **Save**.


Create Correlation Search

Security Domain: Threat

Severity: High

Correlation Search Name: Enter the name of the correlation search

Correlation Search Description: Enter a description of the correlation search

To view and edit correlation searches, go to **Configure** > **Content** > **Content Management**. See Configure correlation searches in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Troubleshooting

This dashboard references data from various data models. Without the applicable data, the panels will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Access dashboards

The Access Protection domain monitors authentication attempts to network devices, endpoints, and applications within the organization. Access Protection is useful for detecting malicious authentication attempts, as well as identifying systems users have accessed in either an authorized or unauthorized manner.

Access Center dashboard

Access Center provides a summary of all authentication events. This summary is useful for identifying security incidents involving authentication attempts such as brute-force attacks or use of clear text passwords, or for identifying authentications to certain systems outside of work hours.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Action	Filter based on authentication success or failure.	Drop-down: select to filter by
App	Filter based on authentication application.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by

Filter by	Description	Action
Special Access	Restricts the view to events related to privileged access. See Administrative Identities in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Time Range	Select the time range to view.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Access Over Time By Action	Displays the count of authentication events over time by action.
Access Over Time By App	Displays the count of authentication events over time by app. For example, "win:local" refers to the local authentication performed on a Windows system and "win:remote" refers to remote API access.
Top Access By Source	Displays a table of highest access counts by source. This table is useful for detecting brute force attacks, since aggressive authentication attempts display a disproportionate number of auth requests.
Top Access By Unique Users	Displays a table of the sources generating the highest number of unique user authentication events.

Access Tracker dashboard

The **Access Tracker** dashboard gives an overview of account statuses. Use it to track newly active or inactive accounts, as well as those that have been inactive for a period of time but recently became active. Discover accounts that are not properly de-provisioned or inactivated when a person leaves the organization.

As inactive accounts or improperly active accounts are vulnerable to attackers, it is a good idea to check this dashboard on a regular basis. You can also use this dashboard during an investigation to identify suspicious accounts and closely examine user access activity.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
First Time Access - Last 7 days	Displays new account access by user and destination.
Inactive Account Usage - Last 90 days	Displays accounts that were inactive for a period of time, but that have shown recent activity.

Panel	Description
Completely Inactive Accounts - Last 90 days	Displays accounts that have shown no activity. Use this panel to identify accounts that should be suspended or removed. If the organization has a policy that requires password change after a specified interval, then accounts that have shown no activity for more than that interval are known to be inactive. This panel also indicates the effectiveness of the enterprise's policy for closing or de-provisioning accounts. If a large number of accounts display here, the process may need to be reviewed.
Account Usage For Expired Identities - Last 7 days	Displays activity for accounts that are suspended within the specified time frame. Use this panel to verify that accounts that should be inactive are not in use.

Access Search dashboard

Use the **Access Search** dashboard to find specific authentication events. The dashboard is used in ad-hoc searching of authentication data, but is also the primary destination for drilldown searches used in the Access Anomalies dashboard panels.

The **Access Search** page displays no results unless it is opened in response to a drilldown action, or you set a filter and/or time range and click Submit.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Action	Filter based on authentication success or failure.	Drop-down: select to filter by
App	Filter based on authentication application.	Drop-down: select to filter by
Source	A string that the source field `src` must match.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	A string that the destination field `dest` must match.	Text field. Empty by default. Wildcard strings with an asterisk (*)
User	A string that the user field `user` must match.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Account Management dashboard

The **Account Management** dashboard shows changes to user accounts, such as account lockouts, newly created accounts, disabled accounts, and password resets. Use this dashboard to verify that accounts are being correctly administered and account administration privileges are being properly restricted. A sudden increase in the number of accounts created, modified, or deleted can indicate malicious behavior or a rogue system. A high number of account lockouts could indicate an attack.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action

Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Special Accounts	Restricts the view to events related to privileged access. See Administrative identities in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Time Range	Select the time range to view.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Account Management Over Time	Displays all account management events over time.
Account Lockouts	Displays all account lockouts, including the number of authentication attempts per account.
Account Management by Source User	Tracks the total account management activity by source user, and shows the source users with the most account management events. The source user is the user that performed the account management event, rather than the user that was affected by the event. For example, if user "Friday.Adams" creates an account "Martha.Washington", then "Friday.Adams" is the source user. This panel helps identify accounts that should not be managing other accounts and shows spikes in account management events, such as the deletion of a large number of accounts.
Top Account Management Events	Shows the most frequent management events in the specified time period.

Default Account Activity dashboard

The **Default Account Activity** dashboard shows activity on "default accounts", or accounts enabled by default on various systems such as network infrastructure devices, databases, and applications. Default accounts have well-known passwords and are often not disabled properly when a system is deployed.

Many security policies require that default accounts be disabled. In some cases, you may need to monitor or investigate authorized use of a default account. It is important to confirm that the passwords on default accounts are changed before use. Abnormal or deviant user behavior from a default account can indicate a security threat or policy violation. Use this dashboard to ensure that security policies regarding default accounts are properly followed.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by

Filter by	Description	Action
Time Range	Select the time range to view.	Drop-down: select to filter by

Dashboard panels

Panel	Description
Default Account Usage Over Time by App	Shows default account activity on all systems and applications during the selected time frame, split by application. For example, sshd or ftpd. Application accounts are shown by the number of successful login attempts and when the last attempt was made. Use this chart to identify spikes in default account login activity by application, which may indicate a security incident, as well as to determine whether default account use is common (for example, a daily event) or rare for a certain application.
Default Accounts in Use	Shows all default user accounts with a high number of login attempts on different hosts, including the last attempt made. Abnormal default user account activity that could indicate a security threat. Also helps ensure that default account behavior matches the security policy.
Default Local Accounts	Lists all default accounts that are active on enterprise systems, including accounts "at rest". Any available default accounts are listed, regardless of whether the account is actually in use. Only accounts detected on a local system, for example by examining the users list on a host, are included in this list.

Troubleshooting Access dashboards

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Endpoint dashboards

The Endpoint Protection domain provides insight into malware events including viruses, worms, spyware, attack tools, adware, and PUPs (Potentially Unwanted Programs), as well as your endpoint protection deployment.

Malware Center dashboard

Malware Center is useful to identify possible malware outbreaks in your environment. It displays the status of malware events in your environment, and how that status changes over time based on data gathered by Splunk.

Search malware events directly using Malware Search, or click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. Configure new data inputs through the Settings menu.

You can use the filters to refine which events are shown.

Filter by	Description	Action
Action	All, allowed, blocked, or deferred.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Malware Activity Over Time By Action	Shows all malware detected over the specified time period, split by action (allowed, blocked, deferred). Use this chart to detect whether too many malware infections are allowed.
Malware Activity Over Time By Signature	Shows all malware detected over the specified time period, split by signature. Example signatures are Mal/Packer, LeakTest, EICAR-AV-Test, TROJ_JAVA.BY. Use this chart to detect which infections are dominant in your environment.
Top Infections	Shows a bar chart of the top infections in your environment, split by signature. This panel helps identify outbreaks related to a specific type of malware.
New Malware - Last 30 Days	Shows new malware detected on the network over the last 30 days. For each malware signature identified, the date and time it was first detected and the total number of infections are shown. First-time infections are the most likely to cause outbreaks.

Malware Search dashboard

The Malware Search dashboard assists in searching malware-related events based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of malware data, but is also the primary destination for drilldown searches used in the Malware Center dashboard panels.

The Malware Search dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Action	Filter by the action taken on the malware (allowed, blocked, or deferred).	Drop-down: select to filter by
Signature	Filter on malware with matching signatures.	Text field. Empty by default. Wildcard strings with an asterisk (*)
File	Filter on file name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter on endpoint systems.	Text field. Empty by default. Wildcard strings with an asterisk (*)
User	Filter based on username.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Malware Operations dashboard

The Malware Operations dashboard tracks the status of endpoint protection products deployed in your environment. Use this dashboard to see the overall health of systems and identify systems that need updates or modifications made to their endpoint protection software. This dashboard can also be used to see how the endpoint protection infrastructure is being administered.

You can click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. Configure new data inputs through the Settings menu.

Use the filters to refine which events are shown.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Clients by Product Version	Shows a bar chart of the number of clients with a certain version of the endpoint protection product installed.
Clients by Signature Version	Shows a bar chart of the number of clients with a certain signature version.
Repeat Infections	Shows repeated malware infections. Sort by signature, destination, action, or number of days.
Oldest Infections	Shows the oldest malware infections in your environment. Sort by date that the infection was detected (first or last time), the signature, destination host (affected system), or days the infection has been active.

System Center dashboard

The System Center dashboard shows information related to endpoints beyond the information reported by deployed anti-virus or host-based IDS systems. It reports endpoint statistics and information gathered by the Splunk platform. System configuration and performance metrics for hosts, such as memory usage, CPU usage, or disk usage, can be displayed on this dashboard.

Click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. Configure new data inputs through the Settings menu.

Use the filters to refine which events are shown.

Filter by	Description	Action
Destination	Host name of the affected endpoint system.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Operating Systems	Shows the operating systems deployed on the network. Use this chart to detect operating systems that should not be present in your environment.

Panel	Description
Top-Average CPU Load by System	Shows the systems on the network with the top average CPU load.
Services by System Count	Shows services ordered by the number of systems on which they are present.
Ports By System Count	Shows the transport method (e.g., tcp) and destination ports, ordered by the number of systems.

Note: If incorrect or missing data is showing up in the System Center dashboard, be sure that the technology add-ons that supply the data for this dashboard are installed on the full forwarders in the deployment. Technology add-ons containing knowledge needed for parsing of data need to be installed on the full forwarders.

Time Center dashboard

The Time Center dashboard helps ensure data integrity by identifying hosts that are not correctly synchronizing their clocks.

Splunk will create an alert when it discovers a system with time out of sync. When you receive an alert, you can drill down to the raw data and investigate further by clicking any of the chart elements or table rows on the dashboard. See Drill down to raw events for more information on this feature.

Use the filters to refine which events are shown.

Filter by	Description	Action
Show only systems that should timesync	Select true to filter by systems categorized as `should_timesync=true` in the Asset table or false to filter by systems categorized as `should_timesync=false` in the Asset table. See Configure the new asset or identity list in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for more about asset configuration.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Time Synchronization Failures	A list of systems where time synchronization has failed.
Systems Not Time Synching	Shows a list of systems that have not synchronized their clocks in the specified time frame.
Indexing Time Delay	Shows hosts with significant discrepancies between the timestamp the host places on the event and the time that the event appears in the Splunk platform. For example, if the timestamp on an event is later than the time that Splunk indexes the event, the host is timestamping events as future events. A large difference (on the order of hours) indicates improper time zone recognition.
Time Service Start Mode Anomalies	Shows hosts that have a time service start mode, such as `Manual` that others do not.

Endpoint Changes dashboard

The Endpoint Changes dashboard uses the Splunk change monitoring system, which detects file-system and registry changes, to illustrate changes and highlight trends in the endpoints in your environment. For example, Endpoint Changes can help discover and identify a sudden increase in changes that may be indicative of a security incident.

You can click chart elements or table rows on this dashboard to display raw events. See Drill down to raw events for more information on this feature.

Use the filters to refine which events are shown.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Endpoint Changes by Action	Summarizes changes over time. A substantial increase in changes may indicate the presence of an incident that is causing changes on the endpoints such as a virus or worm.
Endpoint Changes by Type	Summarizes the type of changes observed on the endpoints, such as file or registry changes.
Changes by System	Summarizes changes by system
Recent Endpoint Changes	Shows the most recent endpoint changes observed.

Update Center dashboard

The Update Center dashboard provides additional insight into systems by showing systems that are not updated. It is a good idea to look at this dashboard on a monthly basis to ensure systems are updating properly.

You can click any of the chart elements or table rows on the dashboard to see raw events. See Drill down to raw events for more information on this feature.

Use the filters to refine which events are shown.

Filter by	Description	Action
Show only systems that should update	Select true to filter by systems categorized as `should_update=true` in the Asset table or false to filter by systems categorized as `should_update=false` in the Asset table. See Configure the new asset or identity list in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for more about asset configuration.	Drop-down: select to filter by
Destination	Host name of the system.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)

Filter by	Description	Action
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Top Systems Needing Updates	A bar chart of the top systems that need updates installed.
Top Updates Needed	A bar chart of the top updates needed across the environment, sorted by signature, such as the KB number.
Systems Not Updating - Greater Than 30 Days	Systems that have not been updated, sorted by the number of days for which they have not been updated.
Update Service Start Mode Anomalies	Shows all systems where the update startup task or service is disabled. Administrators sometimes disable automatic updates to expedite a restart and can forget to re-enable the process.

Update Search dashboard

The Update Search dashboard shows patches and updates by package and/or device. This dashboard helps identify which devices have a specific patch installed. This is useful when, for example, there is a problem caused by a patch and you need to determine exactly which systems have that patch installed.

The Update Search dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Show only systems that should update	Select true to filter by systems categorized as `should_update=true` in the Asset table or false to filter by systems categorized as `should_update=false` in the Asset table. See Configure the new asset or identity list in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for more about asset configuration.	Drop-down: select to filter by
Update Status	Filter by the status of the update on a machine.	Drop-down: select to filter by
Signature	Filter by the signature, for example the KB number, of a particular update.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter on affected endpoint systems.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Asset and Identity dashboards

The Identity domain dashboards provide information about the assets and identities defined in Splunk Enterprise Security. See Add asset and identity data to Splunk Enterprise Security in *Administer Splunk Enterprise Security* for instructions on defining assets and identities.

Asset Center dashboard

Use the **Asset Center** dashboard to review and search for objects in the asset data added to Enterprise Security. The asset data represents a list of hosts, IP addresses, and subnets within the organization, along with information about each asset. The asset list correlates asset properties to indexed events, providing context such as asset location and the priority level of an asset.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels.

Filter by	Description
Asset	A known or unknown asset
Priority	Filter by the Priority field in the Asset table.
Business Unit	A group or department classification for the asset.
Category	Filter by the Category field in the Asset table.
Owner	Filter by the Owner field in the Asset table.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Assets by Priority	Displays the number of assets by priority level. The drilldown opens a search with the selected priority level.
Assets by Business Unit	Displays the relative amount of assets by business unit. The drilldown opens a search with the selected business unit.
Assets by Category	Displays the relative amount of assets by category. The drilldown opens a search with the selected category.
Asset Information	Shows all assets that match the current dashboard filters. The drilldown opens the Asset Investigator dashboard if the "`ip`", "`nt_host`", "`mac`", or "`dns`" fields are selected. Any other field will open a search with the selected field.

Data sources

The reports in the **Asset Center** dashboard reference fields in the Asset and Identities data model. Relevant data sources include lists of assets and identities collected and loaded as lookups, scripted inputs, or search-extracted data.

Identity Center dashboard

Use the **Identity Center** dashboard to review and search for objects in the identity data added to Enterprise Security. Identity data represents a list of account names, legal names, nicknames, and alternate names, along with other associated information about each identity. The identity data is used to correlate user information to indexed events, providing additional context.

Filtering Identities in Identity Center

The filter for the Identity Center dashboard uses a key=value pair search field. To filter identities, enter a key=value pair instead of a name or text string.

Some sample key=value pairs are email=*acmetech.com or nick=a_nickname.

Use the available dashboard filters to refine the results displayed on the dashboard panels.

Filter by	Description
Username	A known or unknown user
Priority	Filter by the Priority field in the Identities table
Business Unit	A group or department classification for the identity.
Category	Filter by the Category field in the Identities table.
Watchlisted Identities Only	Filter by the identities tagged as "watchlist" in the Identities table.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Identities by Priority	Displays the count of Identities by priority level. The drilldown opens a search with the selected priority level.
Identities by Business Unit	Displays the relative number of Identities by business unit. The drilldown opens a search with the selected business unit.
Identities by Category	Displays the relative number of Identities by category. The drilldown opens a search with the selected category.
Identity Information	Shows all assets that match the current dashboard filters. The drilldown opens the Identity Investigator dashboard if you select the `identity` field. Any other field opens a search with the selected field.

Data sources

The reports in the **Identity Center** dashboard reference fields in the Asset and Identities data model. Relevant data sources include lists of assets and identities collected and loaded as lookups, scripted inputs, or search extracted data.

Session Center dashboard

The **Session Center** dashboard provides an overview of network sessions. Network sessions are used to correlate network activity to a user using session data provided by DHCP or VPN servers. Use the Session Center to review the session logs and identify the user or machine associated with an IP address used during a session. You can review network session information from the Network Sessions data model, or user and device association data from Splunk UBA.

Dashboard Panels

Network Sessions tab:

Panel	Description
Sessions Over Time	Displays the total count of network sessions over time. The drilldown opens a search with the selected session and time range.
Session Details	Displays the top 1000 network sessions that have been most recently opened, based on the session start time. The drilldown opens a search with the selected session details.

User Behavior Analytics tab:

Panel	Description
Sessions of Associated Entities	Based on the search filter, displays the sessions of users and devices associated with a device that you search, or devices associated with a user that you search. Hover over a session to learn more about the session activity.
Session Details	Shows the entity ID from Splunk UBA, the name of the entity, the type of entity, the start and end times of the session, and event data from Splunk UBA. Expand a row to view more details.

For more about viewing data from Splunk UBA, see Viewing data from Splunk UBA in Enterprise Security.

Troubleshooting Identity dashboards

The dashboards reference data from various data models. Without the applicable data, the panels will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Asset and Identity Investigator dashboards

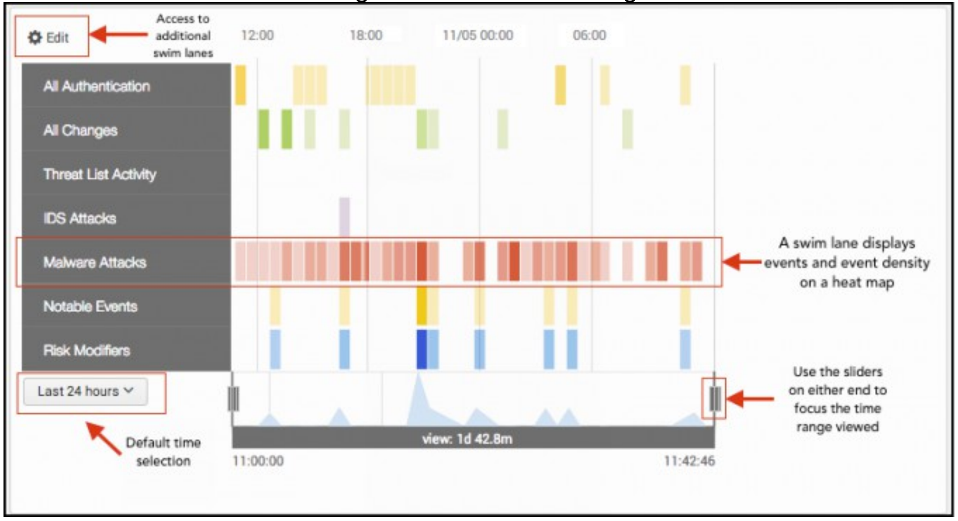
The Asset and Identity Investigator dashboards visually aggregate security-related events over time using category-defined swim lanes. Each swim lane represents an event category, such as authentication, malware, or notable events. The swim lane uses a heat map to display periods of high and low activity. The color saturation on the swim lane corresponds to the event density for a given time. For example, high activity periods display a darker color. An analyst can visually link activity across the event categories and form a complete view of a host or user's interactions in the environment.

Asset Investigator

The Asset Investigator dashboard displays information about known or unknown assets across a pre-defined set of event categories, such as malware and notable events.

Use the Asset Investigator dashboard

You can use the Asset Investigator dashboard to triage an asset's interactions with the environment.



Access to additional swim lanes

A swim lane displays events and event density on a heat map

Use the sliders on either end to focus the time range viewed

Default time selection

The dashboard contains multiple event categories, with each one represented by its own swim lane. Each event category contains relevant events that correspond to a data model. For example, the Malware Attacks swim lane displays events from an anti-virus management or other malware data source, limited to the asset searched. Multiple swim lanes are displayed at once to make it easier for you to track the actions of an asset across event categories.

Additionally, you can use this dashboard for ad hoc searching.

1. Browse to **Security Intelligence > User Intelligence > Asset Investigator**.
2. Type the host name or IP address in the search bar with an optional wildcard.
3. Set a time range and click **Search**.

A workflow for asset investigation

To initiate the asset investigation workflow, perform a workflow action from any dashboard that displays events with network source or destination addresses.

1. Look at the asset description at the top of the dashboard to confirm that you are viewing the asset you would like to investigate. All events displayed in the swim lanes are limited to the selected asset.
2. Use the time range picker to narrow down the general time range you are interested in. Use the time sliders to isolate periods of interesting events or peak event counts.
3. Add or change the swim lanes using the edit menu. For example, to display data collected on an asset from packet analysis tools, change the selected collection from Default to Protocol Intelligence, which represents packet capture data. See Edit the swim lanes.
4. Review individual and grouped events. After selecting an event, you can use the Event Panel to examine common fields represented in the individual or grouped events.
5. If there is an event or pattern that you want to share or investigate further, you can do this using the Event Panel.
    1. Click **Go to Search** to view a drilldown of the selected events.
    2. Click **Share** for a shortened link to the current view.
    3. Click **Create Notable Event** to open a dialog box to create an ad-hoc notable event. See Manually create a notable event in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Data sources

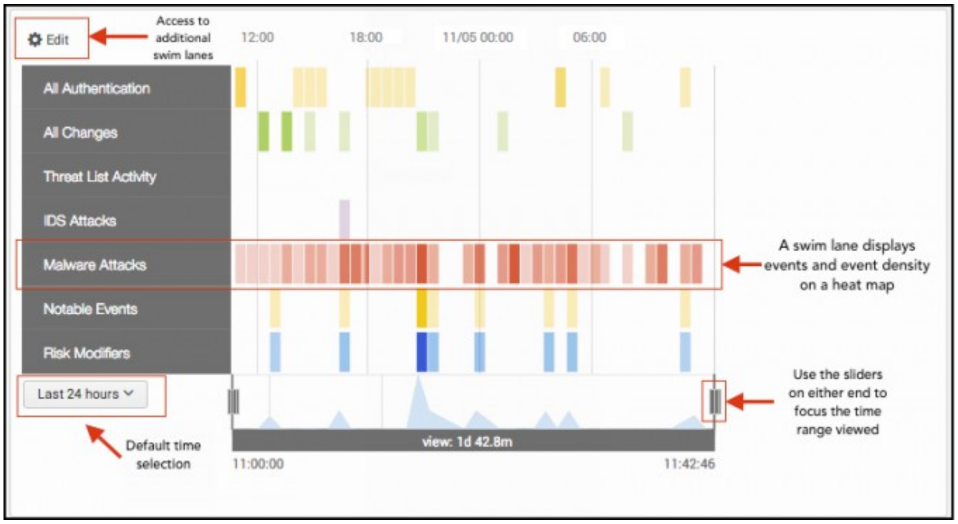
The event categories in the Asset Investigator dashboard display events from a number of data models containing an asset or host field. In any given time selection, a selected asset may not have data to display in one or more event categories. When a data model search returns no matching events, the swim lane displays "Search returned no results." See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Identity Investigator

The Identity Investigator dashboard displays information about known or unknown user identities across a predefined set of event categories, such as change analysis or malware.

Use the Identity Investigator dashboard

You can use the Identity Investigator dashboard to triage a user identity's interactions with the environment.



The dashboard contains multiple event categories, with each one represented by its own swim lane. Each event category contains relevant events that correspond to a data model. For example, the Malware Attacks swim lane displays events from an anti-virus management or other malware data source, limited to the user identity or credential searched. Multiple swim lanes are displayed at once to make it easier for you to track the actions of a user across event categories.

Additionally, you can use this dashboard for ad-hoc searching.

1. Browse to **Security Intelligence > User Intelligence > Identity Investigator**.
2. Type a user credential in the search bar. Optionally, include a wildcard.
3. Set a time range and click Search.

A workflow for identity investigation

The identity investigation workflow is initiated through a workflow action from any dashboard that displays events with network source or destination address.

1. Look at the identity description at the top of the dashboard to confirm that you are viewing the identity you would like to investigate. All events displayed in the swim lanes are limited to the selected identity.
2. Use the time range picker to narrow down the general time range you are interested in. Use the time sliders to isolate periods of interesting events or peak event counts.
3. Add or change swim lanes by using the edit menu. For example, to display identity information collected for user activity monitoring, change the selected collection from Default to User Activity. See Edit the swim lanes.
4. Review individual and grouped events. After selecting an event, you can use the Event Panel to examine common fields represented in the individual or grouped events.
5. If there is an event or pattern that you would like to share or investigate further, you can do this using the Event Panel.
   1. Click **Go to Search** to view a drilldown of the selected events.
   2. Click **Share** for a shortened link to the current view.
   3. Click **Create Notable Event** to open a dialog box to create an ad-hoc notable event. See Manually create a notable event in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Data sources

The event categories in the Identity Investigator dashboard display events from a number of data models containing an identity or a user field. In any given time selection, an identity may not display data in one or more event categories. When a data model search returns no matching events, the swim lane displays "Search returned no results." See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Edit the swim lanes

You can add or remove swim lanes from the Entity Investigator dashboards by opening the Edit Lanes customization menu. The Entity Investigator dashboards support the addition of custom swim lanes bundled with add-ons or created using ES Content Management. For more information, see Managing content in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

1. Choose **Edit** at the top of the dashboard.
2. Select the radio button for a Custom collection.
3. Select a checkbox to add a swim lane to the dashboard.
4. Deselect a checkbox to remove a swim lane from the dashboard.
5. Click the color next to a swim lane to change it.
6. Click the **X** to close the edit menu.

The order of swim lanes can be changed on the dashboard and does not require the Edit Lanes menu.

1. Select a swim lane category.
2. Drag and drop the swim lane where you would like it.

The Asset Investigator has additional, optional swim lanes in the collection Protocol intelligence to display data collected about an asset using packet analysis tools. The Identity Investigator has additional, optional swim lanes in the collection User Activity to display data collected about an identity for user activity monitoring.

Swimlane Name	Asset or Identity dashboard	Description
All Authentication	Both	Matches events in the Authentication data model.
All Changes	Both	Matches events in the Change Analysis data model.
Threat List Activity	Both	Matches events in the Threat Lists data model.
IDS Attacks	Both	Matches events in the Intrusion Detection data model.
Malware Attacks	Both	Matches events in the Malware data model.
Notable Events	Both	Matches events in the Notable index.
Risk Modifiers	Both	Matches events in the Risk Analysis data model.
DNS Errors	Asset only	Matches events in the Network Resolution DNS data model.
Cloud Emails	Asset only	Matches events in the Email data model.
SSL Expired Certs	Asset only	Matches events in the Certificates data model.
HTTP Errors	Asset only	Matches events in the Web data model.
Non-corporate Emails	Identity only	Matches events in the Email data model.
Non-corporate Web Uploads	Identity only	Matches events in the Web data model.
Remote Access	Identity only	Matches events in the Authentication data model.
Ticket Activity	Identity only	Matches events in the Ticket Management data model.
Watchlisted Sites	Identity only	Matches events in the Web data model.

Troubleshooting Asset and Identity Investigator dashboards

The Asset and Identity Investigator dashboards display events from the data model named in each swim lane. When a data model search returns no matching events, the swim lane displays "Search returned no results." See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

User Activity Monitoring

User Activity

The **User Activity** dashboard displays panels representing common risk-generating user activities such as suspicious website activity. For more information about risk scoring, see How Splunk Enterprise Security assigns risk scores.

Dashboard filters

You can use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description
User	A known or unknown identity
Business Unit	A group or department classification for the identity.
Watchlisted Users	Designates a monitored identity.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Users By Risk Scores	Displays the top 100 highest risk users. As an insider threat can represent subtle and indirect changes in behavior, this panels assists an analyst in focusing on the riskiest users in the organization. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Non-corporate Web Uploads	Displays high volume upload and download activity by user. An irregular pattern of upload or download activity can be an indicator of data exfiltration. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Non-corporate Email Activity	Displays the top 100 users performing high volume email activity to non-corporate domains. A pattern of large or high volume email activity can be an indicator of data exfiltration. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Watchlisted Site Activity	Displays web access by user. Accessing specific categories of web sites while using workplace resources and assets can be an indicator of insider threat activity. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Remote Access	Displays remote access authentication by user. A user performing risky web or email activity while using remote access services can be an indicator of data exfiltration, or exploited credentials. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Ticket Activity	Displays ticketing activity by user. A user performing risky web or email activity while filing tickets to provide additional services or internal access can be an indicator of data exfiltration, or exploited credentials. The drilldown opens the Identity Investigator dashboard and searches on the selected user.

Data sources

The reports in the **User Activity** dashboard reference data fields in multiple sources. Relevant data sources include proxy servers, gateways and firewalls, or other sources that reference a distinct user. In order for the dashboards to populate, new lookup content and fields in the identities list must be added. For a list of additional data sources, see Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Access Anomalies

The **Access Anomalies** dashboard displays concurrent authentication attempts from different IP addresses and improbable travel anomalies using internal user credentials and location-relevant data.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels.

Filter by	Description
Action	A successful or failed authentication attempt.
App	The application field in the authentication data model.
User	A known or unknown identity.
Business Unit	A group or department classification for the identity.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Geographically Improbable Accesses	Displays users that initiated multiple authentication attempts separated by an improbable time and distance. Authenticating from two geographically distant locations in a time frame lower than typical transportation methods provide can be an indicator of exploited credentials. The drilldown opens the Access Search dashboard and searches on the selected user.
Concurrent Application Accesses	Displays users that initiated multiple authentication attempts from unique IP addresses within a short time span. This pattern of authentication can be an indicator of shared or stolen credentials. The drilldown redirects the page to the Access Search dashboard and searches on the selected user.

Data sources

The reports in the **Access Anomalies** dashboard reference data fields in the Authentication data model. Relevant data sources include proxy servers, gateways and firewalls, or other sources that reference a distinct user. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Troubleshooting

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Risk Analysis

The **Risk Analysis** dashboard displays recent changes to risk scores and objects that have the highest risk scores. As an analyst, you can use this dashboard to assess relative changes in risk scores and examine the events that contribute to an object's risk score.

You can use the Risk Analysis dashboard to review changes to an object's risk score, determine the source of a risk increase, and decide if additional action is needed.

Dashboard filters

Use any of the available filters on the **Risk Analysis** dashboard to search and filter the results. A filter is applied to all panels in the dashboard, but not the key security indicators.

Filter by	Description
Source	Filter by the correlation search that has risk modifiers
Risk Object	Select a risk object type and type a string to filter by risk object. Risk object type defaults to **All**.

The **Risk Object** filter works by performing a reverse lookup against the asset and identity tables to find all fields that have been associated with the specified **Risk Object**. All associated objects found by the reverse lookup then display on the dashboard. For example, if you select a risk object type of **system** and type a **Risk Object** of 10.10.1.100, the reverse lookup against the assets table could return a MAC address. The **Risk Analysis** dashboard will update to display any risk score applied to the 10.10.1.100 address and a MAC address. If no match to another object was found in the asset table, only the IP address matches from the Risk Analysis data model will be displayed.

Dashboard panels

The Risk Analysis dashboard offers additional views to help analyze risk scoring changes and what caused the changes. Use the filters to refine the view to a specific object or group of objects. Use the drilldown to explore the data as events.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Risk Modifiers Over Time	Displays the changes made to risk modifiers over time. Use the dashboard filters to scope the view to a specific object or group of objects. The drilldown opens a search on all events in the Risk data model scoped to the selected time frame.
Risk Modifiers by Annotations	Displays the changes made to risk modifiers by annotations.
Risk Score by Annotations	Displays the risk score by annotations.
Risk Modifiers by Threat Object	Displays the risk modifiers by threat objects.
Risk Score By Object	Displays the objects with the highest risk score. The drilldown opens a search with the selected risk object and scoped to the selected time frame.
Most Active Sources	Displays the correlation searches that contribute the highest amount of risk to any object. The drilldown opens a search with the selected source.
Recent Risk Modifiers	Displays a table of the most recent changes in a risk score, the source of the change, and the object.

Network dashboards

The Network Protection domain provides insight into the network and network-based devices, including routers, switches, firewalls, and IDS devices. This domain aggregates all the traffic on the network, including overall volume, specific patterns of traffic, what devices or users are generating traffic, and per-port traffic. It also shows results from the vulnerability scanners on the network.

Traffic Center dashboard

The **Traffic Center** dashboard profiles overall network traffic, helps detect trends in type and changes in volume of traffic, and helps to isolate the cause (for example, a particular device or source) of those changes. This helps determine when a traffic increase is a security issue and when it is due to an unrelated problem with a server or other device on the network.

You can use the filters to limit which items are shown. Configure new data inputs through the **Settings** menu, or search for particular network intrusion events directly through **Incident Review**.

Filter by	Description	Action
Action	Filter based on firewall rule actions.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Traffic Over Time by Action	Displays network traffic by action. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected action and time range.
Traffic Over Time By Protocol	Displays the number of events per day for a specified protocol. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected protocol and time range.
Top Sources	Displays the top sources of total traffic volume over the given time frame with a sparkline representing peak event matches. The drilldown opens the Traffic Search dashboard and searches on the selected source IP and time range.
Scanning Activity (Many Systems)	Displays network activity from port scanners or vulnerability scanners and helps identify unauthorized instances of these scanners. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected source IP and time range.

Traffic Search dashboard

The **Traffic Search** dashboard assists in searching network protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of network data, but is also the primary destination for drilldown searches used in the Traffic Center dashboard panels.

The **Traffic Search** dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Action	Filter based on firewall rule actions.	Drop-down: select to filter by
Source	Filter based on source IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Transport Protocol	Filter based on transport protocol.	Drop-down: select to filter by
Destination port	Filter based on destination host port.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Intrusion Center dashboard

The **Intrusion Center** provides an overview of all network intrusion events from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) device data. This dashboard assists in reporting on IDS activity to display trends in severity and in volume of IDS events.

Filter by	Description	Action
IDS Type	Filter based on events matching a specified type of IDS.	Drop-down: select to filter by
IDS Category	Filter based on events matching vendor-defined categories.	Drop-down: select to filter by
Severity	Filter based on event severity.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to view.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Attacks Over Time By Severity	Displays the top attacks over time by severity. The drilldown opens the Intrusion Search dashboard and searches on the selected severity and time range.
Top Attacks	Displays the top attacks by count and signature. The drilldown opens the Intrusion Search dashboard and searches on the selected signature.
Scanning Activity (Many Attacks)	Displays source IP's showing a pattern of attacks. The drilldown opens the Intrusion Search dashboard and searches on the selected source IP and time range.
New Attacks - Last 30 Days	Displays attacks that have been identified for the first time. New attack vectors indicate that a change has occurred on the network, potentially due to the presence of a new threat, such as a new malware infection. The drilldown opens the Intrusion Search dashboard and searches on the selected signature and time range.

Intrusion Search dashboard

The **Intrusion Search** dashboard assists in searching IDS-related events such as attacks or reconnaissance-related activity, based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of network data, but is also the primary destination for drilldown searches used in the Intrusion Center dashboard panels.

The **Intrusion Search** dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
IDS Category	Filter based on events matching vendor-defined categories.	Drop-down: select to filter by
Severity	Filter based on event severity.	Drop-down: select to filter by
Signature	Filter based on IDS signature name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Source	Filter based on source IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Vulnerability Center dashboard

The **Vulnerability Center** provides an overview of vulnerability events from device data.

Filter by	Description	Action
Severity	Filter based on event severity.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 60 days. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Top Vulnerabilities	Displays the most common issues reported by the vulnerability scanners. The reported issues are aggregated by host so that the chart represents the number of unique occurrences of the issue as opposed to the number of times the issue was detected (since scanning a single host multiple times will likely reveal the same vulnerabilities each time). The drilldown opens the Vulnerability Search dashboard and searches on the selected signature and time range.
Most Vulnerable Hosts	Displays the hosts with the highest number of reported issues. The drilldown opens the Vulnerability Search dashboard and searches on the selected severity, host, and time range.
Vulnerabilities by Severity	Displays issues by the severity assigned by the vulnerability scanner. Helps identify trends that are not visible when looking at vulnerabilities individually. The drilldown opens the Vulnerability Search dashboard and searches on the selected severity and time range.
New Vulnerabilities	Displays the most recent new vulnerabilities detected as well as the date each one was first observed. Helps identify new issues appearing on the network that need to be investigated as potential new attack vectors. The drilldown opens the Vulnerability Search dashboard and searches on the selected signature and time range.

Vulnerability Operations dashboard

The Vulnerability Operations dashboard tracks the status and activity of the vulnerability detection products deployed in your environment. Use this dashboard to see the overall health of your scanning systems, identify long-term issues, and see systems that are no longer being scanned for vulnerabilities.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Scan Activity Over Time	Displays vulnerability scan activity by systems over time. Hover over item for details. The drilldown opens the Vulnerability Search dashboard and searches on the selected time range.
Vulnerabilities by Age	Displays detected vulnerabilities by age, with signature, destination, and event time. Click an item to view in the Vulnerability Profiler for more detail. The drilldown opens the Vulnerability Search dashboard and searches on the selected signature or destination host, and time range.
Delinquent Scanning	Displays vulnerability scans with a severity of "high". Includes signature. The drilldown opens the Vulnerability Search dashboard and searches on the selected destination host and time range.

Vulnerability Search dashboard

The **Vulnerability Search** dashboard displays a list of all vulnerability-related events based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of vulnerability data, but is also the primary destination for drilldown searches used in the Vulnerability Center dashboard panels.

The **Vulnerability Search** dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Vuln. category	Filter based on events matching vendor-defined categories.	Drop-down: select to filter by
Severity	Filter based on event severity.	Drop-down: select to filter by
Signature	Filter based on vendor signature name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Reference (bugtraq, cert, cve, etc.)	Filter based on common reference standards.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to represent.	Drop-down: select to filter by

Troubleshooting Network Dashboards

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Web Center and Network Changes dashboards

Web Center

You can use the Web Center dashboard to profile web traffic events in your deployment. This dashboard reports on web traffic gathered by Splunk from proxy servers. It is useful for troubleshooting potential issues such as excessive bandwidth usage, or proxies that are no longer serving content for proxy clients. You can also use the Web Center to profile the type of content that clients are requesting, and how much bandwidth is being used by each client.

You can configure new data inputs through Splunk Settings, or search for particular traffic events directly through Incident Review. Use the filters at the top of the screen to limit which items are shown. Filters do not apply to Key Indicators.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Events Over Time by Method	Shows the total number of proxy events over time, aggregated by Method, or the HTTP method requested by the client (POST, GET, CONNECT, etc.).
Events Over Time by Status	Shows the total number of proxy events, aggregated by Status, or the HTTP status of the response.
Top Sources	Sources associated with the highest volume of network traffic. This is useful for identifying sources that are using an excessive amount of network traffic (for example, file-sharing hosts), or frequently-requested destinations generating large amounts of network traffic (for example, YouTube or Pandora).
Top Destinations	Destinations associated with the highest volume of network traffic. This is useful for identifying sources that are using an excessive amount of network traffic (for example, file-sharing hosts), or frequently-requested destinations generating large amounts of network traffic (for example, YouTube or Pandora).

Web Search

The **Web Search** dashboard assists in searching for web events that are of interest based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of web data, but is also the primary destination for drilldown searches used in the Web Search dashboard panels.

The Web Search dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
HTTP Method	Filter based on HTTP Method.	Text field. Empty by default. Wildcard strings with an asterisk (*)
HTTP Status	Filter based on HTTP Status code.	Text field. Empty by default. Wildcard strings with an asterisk (*)

Filter by	Description	Action
Source	Filter based on source IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
URL	Filter based on URL details.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Network Changes

Use the Network Changes dashboard to track configuration changes to firewalls and other network devices in your environment. This dashboard helps to troubleshoot device problems; frequently, when firewalls or other devices go down, this is due to a recent configuration change.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Network Changes by Action	Shows all changes to the devices by the type of change, or whether a device was added, deleted, modified, or changed. The drilldown opens the "New Search" dashboard and searches on the selected action and time range.
Network Changes by Device	Shows all devices that have been changed as well as the number of the changes, sorted by the devices with the highest number of changes. The drilldown opens the "New Search" dashboard and searches on the selected device and time range.
Recent Network Changes	Shows a table of the most recent changes to network devices in the last day.

Troubleshooting

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Port and Protocol Tracker dashboard

The Port and Protocol Tracker tracks port and protocol activity, based on the rules set up in **Configure > Content > Content Management** in Enterprise Security. To edit, search for interesting_ports_lookup or use the Type dropdown menu to filter on **Managed Lookup** and scroll to **Interesting Ports**.

The lookup table specifies the network ports that the enterprise allows. From this dashboard, you can view new activity by port to identify devices that are not in compliance with corporate policy, as well as detect prohibited traffic.

Filter by	Description	Action

Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Port/Protocol Profiler	Displays the volume network transport and port activity over time, to evaluate if port activity is trending upwards or downwards. Sudden increases in unapproved port activity may indicate a change on the networked devices, such as an infection. The drilldown opens the "New Search" dashboard and searches on the selected transport destination port and time range.
New Port Activity - Last 7 Days	Displays a table of transport and port traffic communication over time. The drilldown opens the Traffic Search dashboard and searches on the selected transport and time range.
Prohibited Or Insecure Traffic Over Time - Last 24 Hours	Displays the volume of prohibited network port activity over time, and helps determine if unapproved port activity is trending upwards or downwards. The drilldown opens the "New Search" dashboard and searches on the selected transport destination port and time range.
Prohibited Traffic Details - Last 24 Hours	Displays a table of the number of prohibited network traffic events. The drilldown opens the "New Search" dashboard and searches on the selected source IP, destination IP, transport, port, and time range.

Troubleshooting

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Protocol Intelligence dashboards

Protocol Intelligence is a collection of dashboards and searches that report on the information collected from common network protocols. As an analyst, you can use these dashboards to gain insight into HTTP, DNS, TCP/UDP, TLS/SSL, and common email protocols across your system or network.

The Protocol Intelligence dashboards use packet capture data. Packet capture data contains security-relevant information not typically collected in log files. Integrating network protocol data provides a rich source of additional context when detecting, monitoring, and responding to security related threats.

Obtain packet capture data from apps such as Splunk Stream and the Splunk Add-on for Bro IDS. The dashboards will be empty without applicable data.

- For information about integrating Splunk Stream with Splunk Enterprise Security, see Splunk Stream integration in the Enterprise Security *Installation and Upgrade Manual*.
- For information about the protocols supported in Splunk Stream, see Supported protocols in the Splunk Stream *User Manual*.

Protocol Center

The Protocol Center dashboard provides an overview of security-relevant network protocol data. The dashboard searches display results based on the time period selected using the dashboard time picker.

Dashboard Panels

Panel	Description
Key Indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security. Key indicators displayed include **Protocol Activity**, **Long Lived Connections**, **Stream Connections**, **Encrypted Connections**, and **Total Bytes**.
Connections By Protocol	Displays the sum of all protocol connections, sorted by protocol over time. The connection distribution by protocol shows the most common protocols used in an environment, such as email protocols and HTTP/SSL. An exploited protocol may display a disproportionate number of connections for its service type.
Usage By Protocol	Displays the sum of all protocol traffic in bytes, sorted by protocol over time. The bandwidth used per protocol will show consistency relative to the total network traffic. An exploited protocol may display a traffic increase disproportionate to its use.
Top Connection Sources	Displays the top 10 hosts by total protocol traffic sent and received over time. A host displaying a large amount of connection activity may be heavily loaded, experiencing issues, or represent suspicious activity. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected source IP.
Usage For Well Known Ports	Displays the sum of protocol traffic, sorted by ports under 1024 over time. The bandwidth used per port will show consistency relative to the total network traffic. An exploited port may display an increase in bandwidth disproportionate to its use. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected port.
Long Lived Connections	Displays TCP connections sustained longer than 3 minutes. A long duration connection between hosts may represent unusual or suspicious activity. The drilldown opens the Traffic Search dashboard and searches on the selected event.

Data sources

The reports in the **Protocol Center** dashboard use fields in the Network Traffic data model. Relevant data sources include all devices or users generating TCP and UDP protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

Traffic Size Analysis

Use the **Traffic Size Analysis** dashboard to compare traffic data with statistical data to find outliers, traffic that differs from what is normal in your environment. Any traffic data, such as firewall, router, switch, or network flows, can be summarized and viewed on this dashboard.

- Investigate traffic data byte lengths to find connections with large byte counts per request, or that are making a high number of connection attempts with small byte count sizes.
- Use the graph to spot suspicious patterns of data being sent.
- Drill down into the summarized data to look for anomalous source/destination traffic.

Dashboard filters

Use the filters to refine the traffic size events list on the dashboard.

Filter by	Description
Standard Deviation Index	The percentage (%) shows the amount of data that will be filtered out if that number of standard deviations is selected. Choose a higher number of deviations to see fewer traffic size anomalies and details, or choose a lower number of deviations to see a greater number of traffic size anomalies and details.
Time Range	Select the time range to represent.
Advanced Filter	Click to see the list of category events that can be filtered for this dashboard. See Configure per-panel filtering in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for information.

Dashboard panels

Click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Traffic Size Anomalies Over Time	The chart displays a count of anomalous traffic size in your environment over time. It displays traffic volume greater than the number of standard deviations selected in the filter (2 by default) displayed in a line graph with time as the x-axis and count as the y-axis.
Traffic Size Details	Table that displays each of the traffic events and related details such as the size of the traffic event in bytes. If there is more that one event from a source IP address, the `count` column shows how many events are seen. In the `bytes` column, the minimum, maximum, and average number of bytes for the traffic event are shown. Z indicates the standard deviations for the traffic event.

DNS Activity

The DNS Activity dashboard displays an overview of data relevant to the DNS infrastructure being monitored. The dashboard searches display results based on the time period selected using the dashboard time picker.

Dashboard Panels

Panel	Description
Key Indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Top Reply Codes By Unique Sources	Displays the top DNS Reply codes observed across hosts. A host initiating a large number of DNS queries to unknown or unavailable domains will report a large number of DNS lookup failures with some successes. That pattern of DNS queries may represent an exfiltration attempt or suspicious activity. The drilldown opens the DNS Search dashboard and searches on the selected Reply Code.
Top DNS Query Sources	Displays the top DNS query sources on the network. A host sending a large amount of DNS queries may be improperly configured, experiencing technical issues, or represent suspicious activity. The drilldown opens the DNS Search dashboard and searches on the selected source IP address.
Top DNS Queries	Displays the top 10 DNS **QUERY** requests over time. The drilldown opens the DNS Search dashboard and searches on the queried host address.
Queries Per Domain	Displays the most common queries grouped by domain. An unfamiliar domain receiving a large number of queries from hosts on the network may represent an exfiltration attempt or suspicious activity. The drilldown opens the DNS Search dashboard and searches on the queried domain address.
Recent DNS Queries	Displays the 50 most recent DNS Response queries with added detail. The drilldown opens the DNS Search dashboard and searches on the selected queried address.

Data sources

The reports in the DNS dashboard use fields in the Network Resolution data model. Relevant data sources include all devices or users generating DNS protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

DNS Search

The DNS Search dashboard assists in searching DNS protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of DNS data, but is also the primary destination for drilldown searches in the DNS dashboard panels.

The **DNS Search** page displays no results unless it is opened in response to a drilldown action, or you set a filter and/or time range and click Submit.

Filter by	Description
Source	Source IP address
Destination	Destination IP address
Query	DNS Query
Message Type	DNS Message type: Query, Response, or All.
Reply Code	DNS Reply type: All, All Errors, and a list of common Reply Codes

SSL Activity

The **SSL Activity** dashboard displays an overview of the traffic and connections that use SSL. As an analyst, you can use these dashboards to view and review SSL encrypted traffic by usage, without decrypting the payload. The dashboard searches display results based on the time period selected using the dashboard time picker.

Dashboard Panels

Panel	Description
Key Indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
SSL Activity By Common Name	Displays outbound SSL connections by common name (CN) of the SSL certificate used. An unfamiliar domain receiving a large number of SSL connections from hosts on the network may represent unusual or suspicious activity. The drilldown redirects the page to the SSL Search dashboard, and searches on the selected common name.
SSL Cloud Sessions	Displays the count of active sessions by CN that represents a known cloud service. The CN is compared to a list of cloud service domains pre-configured in the Cloud Domains lookup file. For more information about editing lookups in ES, see Create and manage lookups in Splunk Enterprise Security in *Administer Splunk Enterprise Security*. The drilldown opens the SSL Search dashboard and searches on the selected source IP and common name.
Recent SSL Sessions	Displays the 50 most recent SSL sessions in a table with additional information about SSL key. The fields `ssl_end_time`, `ssl_validity_window`, and `ssl_is_valid` use color-coded text for fast identification of expired, short lived, or invalid certificates. The drilldown redirects the page to the SSL Search dashboard and displays the full details of the selected event.

Data sources

The reports in the SSL Activity dashboard use fields in the Certificates data model. Relevant data sources include all devices or users generating SSL protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

SSL Search

The SSL Search dashboard assists in searching SSL protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of SSL protocol data, but is also the primary destination for drilldown searches in the SSL Activity dashboard panels.

The **SSL Search** page displays no results unless it is opened in response to a drilldown action, or you set a filter and/or time range and click Submit.

Filter by	Description

Filter by	Description
Source	Source IP address.
Destination	Destination IP address.
Subject/Issuer	Subject or Issuer fields.
Subject/Issuer Common Name	Common name retrieved from the x.509 certificate Subject or Issuer fields.
Certificate Serial Number	The x.509 certificate Serial Number field.
Certificate Hash	The x.509 certificate Signature field.

Email Activity

The **Email Activity** dashboard displays an overview of data relevant to the email infrastructure being monitored. The dashboard searches displays result based on the time period selected using the dashboard time picker.

Dashboard Panels

Panel	Description
Key Indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Top Email Sources	Displays the hosts generating the most email protocol traffic. A host sending excessive amounts of email on the network may represent unusual or suspicious activity. Periodicity displayed across hosts viewed on the sparklines may be an indicator of a scripted action. The drilldown opens the Email Search dashboard and searches on the selected source IP.
Large Emails	Displays the hosts sending emails larger than 2MB. A host that repeatedly sends large emails may represent suspicious activity or data exfiltration. The drilldown opens the Email Search dashboard and searches on the selected source IP.
Rarely Seen Senders	Displays Sender email addresses that infrequently send email. An address that represents a service account or non-user sending email may indicate suspicious activity or a phishing attempt. The drilldown opens the Email Search dashboard and searches on the selected Sender.
Rarely Seen Receivers	Displays Receiver email addresses that infrequently receive email. An address that represents a service account or non-user receiving email may indicate suspicious activity or a phishing attempt. The drilldown opens the Email Search dashboard and searches on the selected Recipient.

Data sources

The reports in the Email dashboard use fields in the Email data model. Relevant data sources include all the devices or users generating email protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

Email Search

The Email Search dashboard assists in searching email protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of email protocol data, but is also the primary destination for drilldown searches used in the Email Activity dashboard panels.

The **Email Search** page displays no results unless it is opened in response to a drilldown action, or you set a filter and/or time range and click Submit.

Filter by	Description
Email Protocol	The email communication protocol.

Filter by	Description
Source	Source IP address
Sender	The sender's email address.
Destination	Destination IP address
Recipient	The recipient's email address.

Troubleshooting Protocol Intelligence dashboards

The Protocol Intelligence dashboards use packet capture data from apps such as Splunk Stream and the Splunk Add-on for Bro IDS. Without applicable data, the dashboards remain empty. For an overview of Splunk Stream Integration with ES, see Splunk Stream integration in the Enterprise Security *Installation and Upgrade Manual*. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Threat Intelligence dashboards

Threat Activity

The **Threat Activity** dashboard provides information on threat activity by matching threat intelligence source content to events in Splunk Enterprise.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description
Threat Group	A named group or entity representing a known threat, such as a malware domain.
Threat Category	A category of threat, such as advanced persistent threat, financial threat, or backdoor.
Search	Used for searching on a value related to fields: Destination, Sourcetype, Source, Threat Collection, Threat Collection Key, Threat Key, Threat Match Field, and Threat Match Value.
Time Range	Select the time range to represent.

Dashboard panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information, and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Threat Activity Over Time	Displays the count of events by all threat collections over the selected time. The drilldown opens a search with the selected threat collection and scoped to the selected time frame. To review the threat collections, see Supported types of threat intelligence in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.
Most Active Threat Collections	Displays the top threat collections by event matches over the selected time, with a sparkline representing peak event matches. The drilldown opens a search with the selected threat collection.
Most Active Threat Sources	Displays the top threat sources over the selected time by event count matches. The drilldown opens a search with the selected threat source.

Panel	Description
Threat Activity Details	Displays a breakout of the most recent threat matches. Use the event selection box **Threat Activity Details** with the **Advanced Filter** option to: • Whitelist by `threat_match_value` to remove matches. • Highlight specific `threat_match_value` matches and place them at the top of the table.

Data sources

The reports in the **Threat Activity** dashboard use fields in the Threat_Intelligence data model. Relevant data sources include threat source event matches in the `threat_activity` index along with the associated threat artifacts. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Threat Artifacts

The **Threat Artifacts** dashboard provides a single location to explore and review threat content sourced from all configured threat download sources. It provides additional context by showing all threat artifacts related to a user-specified threat source or artifact.

The dashboard offers multiple selection filters and tabs to isolate the threat content.

Begin by changing the **Threat Artifact** to select from available threat artifact types.

Filter by	Description
Threat Artifact	A collection of objects grouped by the threat collection, such as network, file, and service.

Other available filters will change depending on your selection.

Threat Artifact selection	Filter by Text: (*) wildcard defaulted	Filter by Drop-down
Threat ID	Malware Alias, Intel Source ID, and Intel Source Path	Threat Category, Threat Group
Network	IP, Domain	HTTP. Select from: Referrer: User Agent, Cookie, Header, Data, or URL and add a string to search.
File	File Name, File Extension, File Path, and File Hash	
Registry	Hive, Path, Key Name, Value Name, Value Type, and Value Text	
Service	Name, Descriptive Name:, Description:, and Type	
User	User, Full Name, Group Name, and Description	
Process	Process, Process Arguments, Handle Names, and Handle Type	
Certificate	Serial Number, Subject, Issuer, Validity Not After, and Validity Not Before	
Email	Address, Subject, and Body	

Use the tabs to review threat source context:

Tab	Panels
Threat Overview	Endpoint Artifacts, Network Artifacts, Email Artifacts, Certificate Artifacts

Tab	Panels
Network	HTTP Intelligence, IP Intelligence, Domain Intelligence
Endpoint	File Intelligence, Registry Intelligence, Process Intelligence, Service Intelligence, User Intelligence
Certificate	Certificate Intelligence
Email	Email Intelligence

Data sources

The **Threat Artifacts** dashboard references fields in the threat collection KVStore. Relevant data sources include threat sources such as STIX and OpenIOC documents.

Troubleshooting

This dashboard references data from the Threat Intelligence KVStore collections. Without the applicable data, the dashboard panels will remain empty. To determine why data is not displaying in the dashboard, follow these troubleshooting steps.

1. Confirm that the inputs are properly configured in the **Threat Intelligence Downloads** and **Threat Intelligence Manager** pages. Those inputs are responsible for ingesting data from the threat sources and placing it into the KVStore collections.
2. Use the **Threat Intelligence Audit** dashboard panel Threat Intelligence Audit Events to review log entries created by the modular inputs.

For more, see Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Web Intelligence dashboards

Use the **Web Intelligence** dashboards to identify potential and persistent threats in your environment.

HTTP Category Analysis dashboard

The **HTTP Category Analysis** dashboard looks at categories of traffic data. Any traffic data, such as firewall, router, switch, or network flows, can be summarized and viewed in this dashboard.

- Compare statistical data to identify traffic outliers, or traffic different from what is typically found in your environment.
- Look for category counts that fall outside of the norm (small or large) that may indicate a possible threat.
- Find low volume traffic activity and drill down from the summarized data to investigate events.
- Use sparklines to identify suspicious patterns of activity by category.

Unknown traffic categories

Use the "Show only unknown categories" filter on the **HTTP Category Analysis** dashboard to filter and view unknown categories of web traffic.

Before you can filter unknown traffic, define which categories are unknown.

1. Select **Settings** > **Tags**.

2. Click **List by tag name**.
3. Select an **App context** of DA-ESS-NetworkProtection or a related network add-on, such as TA-websense.
4. Click **New**.
5. Type a **Tag name** of `unknown`.
6. Type a **Field-value pair** to define as unknown traffic.
   For example, `category=undetected`.
7. Click **Save**.

Dashboard filters

Filters can help refine the HTTP category list.

Filter by	Description
Time Range	Select the time range to represent.
Advanced Filter	Click to see the list of category events that can be filtered for this dashboard. See Configure per-panel filtering in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for information.

Dashboard panels

Click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Category Distribution	Displays category counts as a scatter plot, with `count` as the x-axis and `src_count` as the y-axis. The chart updates when you change filters or the time range. Hover over an item to see details.
Category Details	Displays details of the HTTP categories, including a sparkline that represents the activity for that HTTP category over the last 24 hours.

HTTP User Agent Analysis dashboard

Use the **HTTP User Agent Analysis** dashboard to investigate user agent strings in your proxy data and determine if there is a possible threat to your environment.

- A bad user agent string, where the browser name is misspelled (like Mozzila) or the version number is completely wrong (v666), can indicate an attacker or threat.
- Long user agent strings are often an indicator of malicious access.
- User agent strings that fall outside of the normal size (small or large) may indicate a possible threat that should be looked at and evaluated.

The Advanced Filter can be used to include or exclude specific user agents. Use the statistical information to visually identify outliers. In the summarized data, you can evaluate user agents for command and control (C&C) activity, and find unexpected HTTP communication activity.

Dashboard filters

The dashboard includes a number of filters that can help refine the user agent list.

Filter by	Description

Standard Deviation Index	The percentage (%) shows the amount of data that will be filtered out if that number of standard deviations is selected. Choose a higher number of deviations to see fewer user agent strings, or choose a lower number of deviations to see a greater number of user agent strings.
Time Range	Select the time range to represent.
Advanced Filter	Click to see the list of category events that can be filtered for this dashboard. See Configure per-panel filtering in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for information.

Dashboard panels

Click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
User Agent Distribution	Displays user agent strings as a scatter plot, with `length` as the x-axis and `count` as the y-axis. The chart updates when you change the filters or the time range. Hover over an item to see details about the raw data.
User Agent Details	Displays details of the user agents in your environment, including the string value of the user agent and a sparkline that represents the activity for that user agent string over the last 24 hours.

New Domain Analysis dashboard

The **New Domain Analysis** dashboard shows any new domains that appear in your environment. These domains can be newly registered, or simply newly seen by ES. Panels display New Domain Activity events, New Domain Activity by Age, New Domain Activity by Top Level Domain (TLD), and Registration Details for these domains.

- View hosts talking to recently registered domains.
- Discover outlier activity directed to newly registered domains in the New Domain Activity by Age panel.
- Identify unexpected top level domain activity in the New Domain Activity by TLD panel.
- Investigate high counts of new domains to find out if your network has an active Trojan, botnet, or other malicious entity.

Dashboard filters

The dashboard includes a number of filters to refine the list of domains displayed.

Filter by	Description
Domain	Enter the domain (Access, Endpoint, Network).
New Domain Type	Select **Newly Registered** or **Newly Seen** to filter the types of domains to be viewed.
Maximum Age (days)	The time range for the newly seen or newly registered domains. The default is 30 days.
Time Range	Select the time range to represent.
Advanced Filter	Click to see the list of category events that can be filtered for this dashboard. See Configure per-panel filtering in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for information.

Dashboard panels

Click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. The following table describes the panels for this dashboard.

Panel	Description
New Domain Activity	Table view of information about new domain activity
New Domain Activity by Age	Scatter plot that displays `Age` as the x-axis and `Count` as the y-axis. Hover over a square for the exact age and number of new domains.
New Domain Activity by TLD (Top Level Domain)	A bar chart with `Count` as the x-axis and `TLD` as the y-axis. Hover over a bar for the current number of events for a top level domain.
Registration Details	A table view of information about new domain registrations. Click a domain in the table to open a search on that domain and view the raw events.

Configure the external API for WHOIS data

To see data in the **New Domain Analysis** dashboard, you must configure a connection to an external domain lookup data source. You can use the example domain lookup data source provided in ES or you can use one of your choice. The dashboard will only report whether or not a domain is newly seen until this modular input is configured and enabled.

The example uses the external domain source domaintools.com, which provides a paid API for WHOIS data.

1. Sign up for a domaintools.com account.
2. Collect the API host name and your API access credentials from the site. Note that the API access credentials are different from your account email address.

Use the API information to set up a modular input in Splunk Enterprise Security.

1. From the ES menu bar, Select **Configure** > **Data Enrichment** > **WHOIS Management**.
2. Click **Enable** next to **whois_domaintools**.
3. Click the name of the modular input to add the API hostname and username used to access the domaintools API.
4. Save the API credentials on the Credential Management view. See Manage input credentials in Splunk Enterprise Security.

If you choose to use a different domain source, complete the following steps.

1. From the ES menu bar, Select **Configure** > **Data Enrichment** > **WHOIS Management**.
2. Click **New**.
3. Enter the name of the modular input to add the API hostname and username used to access the API.
4. Save the API credentials on the Credential Management view. See Manage input credentials in Splunk Enterprise Security.
5. Click **Enable** next to the name of the modular input you just created.

Until you enable the modular input, domains processed by the input will not be queued. This prevents the checkpoint directory from filling up with files.

After enabling the modular input, enable the `outputcheckpoint_whois` macro to create checkpoint data.

1. Select **Configure** > **General** > **General Settings**.
2. Select **Enable** for the **Domain Analysis** setting to enable WHOIS tracking.

The modular input stores information in the `whois_tracker.csv` lookup file. After a file exists in the `$SPLUNK_HOME/var/lib/splunk/modinputs/whois` directory, the `whois` index will begin to populate with data. After they are processed, checkpoint files will be deleted.

Errors versus normal behavior

- If you see `404` errors in the logs, this is normal behavior when querying domains that don't exist.
- If you see `400` errors in the logs returned from the domaintools API, this is normal behavior when querying domains with invalid top level domains.
- If you don't see new events in the whois index, this might be normal behavior if using `HTTP://` the api_url when it should be `HTTPS://`. You can use either `HTTP://` or `HTTPS://` in the url. However, if you don't pick `HTTP://` or `HTTPS://`, then `HTTP://` is prepended to the api_url by default .

URL Length Analysis dashboard

The **URL Length Analysis** dashboard looks at any proxy or HTTP data that includes URL string information. Any traffic data containing URL string or path information, such as firewall, router, switch, or network flows, can be summarized and viewed in this dashboard.

- Compare each URL statistically to identify outliers.
- Investigate long URLs that have no referrer.
- Look for abnormal length URLs that contain embedded SQL commands for SQL injections, cross-site scripting (XSS), embedded command and control (C&C) instructions, or other malicious content.
- Use the details table to see how many assets are communicating with the URL.

Use the key indicators to compare each new URL and to identify outlier URL strings, ones that are different from what is typically found in your environment. URLs that fall outside of the normal size (small or large) may indicate a possible threat. Unusually long URL paths from unfamiliar sources and/or to unfamiliar destinations are often indicators of malicious access and should be examined.

Dashboard filters

Use the filters to refine the URL length events represented on the dashboard.

Filter by	Description
Standard Deviation Index	The percentage (%) shows the amount of data that will be filtered out if that number of standard deviations is selected. Choose a higher number of deviations to see fewer user agent strings, or choose a lower number of deviations to see a greater number of user agent strings.
Time Range	Select the time range to represent.
Advanced Filter	Click to see the list of category events that can be filtered for this dashboard. See Configure per-panel filtering in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for information.

Dashboard panels

Click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. The following table describes the panels for this dashboard.

Panel	Description

Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security in this manual.
URL Length Anomalies Over Time	The chart displays a count of URL length anomalies across time. It displays URL lengths greater than the number of standard deviations selected in the filter (2 by default) displayed in a line graph with time as the x-axis and count as the y-axis.
URL Length Details	Table that displays the URL strings and details such as the full URI string. If there is more that one event from a source IP address, the `count` column shows how many events are seen. Z indicates the standard deviations for the URL length.

Security Groups for your VPC in Splunk Enterprise Security

Monitor security groups in your Amazon Web Services (AWS) environment so that you have visibility into your virtual firewalls and can manually detect any suspicious activity.

Security Group Dashboard

Use the Security Group Dashboard to monitor security group activity in the AWS environment, including error events, number of security groups and rules, any unused security groups, activity over time, and the detailed list of error activities.

> The Security Groups and Security Group Rules panels are snapshots based on the AWS lambda ingestion interval of three hours. If no events occur during that interval, your dashboards continue to show data based on the last snapshot from three hours ago. Also, if no events occur during the time you've chosen in the time range picker, such as one hour, your dashboards still show data based on the last snapshot from three hours ago. See Data Ingestion Mechanisms and Intervals in Data Manager in the Data Manager User Manual.

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **Security Groups**.

The Security Group Dashboard includes the following panels:

Panel	Source Type	Datamodel

Error Events	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Security Group Actions	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Security Group Activity Over Time	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Most Recent Security Group Activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`
Most Recent Authorize and Revoke Activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`
Security Group Error Activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`

User and Authentication Activity in Splunk Enterprise Security

Monitor your Amazon Web Services (AWS) user activity to uncover suspicious behaviors that may be associated with malicious activity, such as activity spikes or unusual events.

Use the IAM Activity Dashboard

Use the IAM Activity Dashboard to monitor user activity in your environment, including the error events, which users have the most activity, activity over time, and the detailed list of error activities.

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **IAM Activity**.

The IAM Activity Dashboard includes the following panels:

Panel	Source Type	Datamodel

Error Events	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

Activity by User	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

IAM Actions	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

IAM Actions Over Time	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

Success vs. Failure Activity	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

Most Recent IAM Activity	`aws:cloudtrail`	`datamodel:"Change.Account_Management"`
IAM Error Activity	`aws:cloudtrail`	`datamodel:"Change.Account_Management"`

Filter your panel results

You can filter the results that you see in the dashboard panels.

Filter	Description
Account ID	Specify one or more of the data account IDs that you chose during onboarding.
Regions	Specify one or more of the data source regions that you chose during onboarding.
Status	Choose from the following statuses: • All - All event statuses, including both successes and errors. • Error - Only error event statuses. Some panels are based on error trends, so there is no difference in the results if you select All or if you select Error.

Filter	Description
Action	Choose from the following actions: • All - All event actions. • Each action - You can filter on each action individually or a combination of actions.
Time Range	Define the time range of a search with the **time range picker**.

Network ACL Analytics in Splunk Enterprise Security

Monitor your Amazon Web Services (AWS) network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper, when the facts warrant it.

Network ACLs Dashboard

Use the Network ACLs Dashboard to monitor the network ACL activity in your AWS environment, including error events, the number of Network ACLs, activity over time, and the detailed list of error activities.

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **Network ACLs**.

The Network Dashboard includes the following panels:

Panel	Source Type	Datamodel

Error Events	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Network ACL Actions	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Network ACL Activity Over Time	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Most Recent Network ACLs Activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`
Network ACL Error Activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`

AWS Access Analyzer in Splunk Enterprise Security

Monitor your Amazon Web Services (AWS) shared resources to identify potential unintended access.

Access Analyzer Dashboard

Use the Access Analyzer Dashboard to Monitor your AWS public facing queues, lambdas, and S3 Buckets.

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **Access Analyzer**.

The Access Analyzer Dashboard includes the following panels:

Panel	Source Type	Datamodel
Number of Public Facing Queues	aws:accessanalyzer:finding	n/a
Number of Public Facing AWS Lambda	aws:accessanalyzer:finding	n/a
Number of Public Facing S3 Buckets	aws:accessanalyzer:finding	n/a
Access Analyzer Trend	aws:accessanalyzer:finding	n/a

Microsoft 365 Security in Splunk Enterprise Security

Get a summary of relevant Microsoft 365 security data to monitor your Microsoft 365 applications such as Active Directory, Exchange, Security and Compliance, Teams, and so on. Investigative searches help you probe deeper, when the facts warrant it.

Microsoft 365 Security Dashboards

Use the Microsoft 365 Security Dashboard to monitor security activity in your Microsoft 365 applications.

Active Directory

To access the Active Directory dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **Microsoft 365**.
3. Click **Active Directory**.

The Active Directory Dashboard includes the following panels:

Panel	Source Type	Datamodel
Password Account Lockouts	o365:management:activity	n/a
Users with Enable vs. Disable MFA	o365:management:activity	n/a
Failed User Logins	o365:management:activity	n/a
Impossible Travel	o365:management:activity	n/a
Non-existent Accounts - Login Attempts	o365:management:activity	n/a
Added/Removed Members from Group	o365:management:activity	n/a

Exchange

To access the Exchange dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **Microsoft 365**.
3. Click **Exchange**.

The Exchange Dashboard includes the following panels:

Panel	Source Type	Datamodel
Exchange Operations by Location	o365:management:activity	n/a

Panel	Source Type	Datamodel
External Domain with Forwarding Policy	`o365:management:activity`	n/a
Mailbox Exports	`o365:management:activity`	n/a
Mailbox Forwarding Rules	`o365:management:activity`	n/a
FullAccess Permission changes	`o365:management:activity`	n/a

OneDrive and SharePoint

To access the OneDrive and SharePoint dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **Microsoft 365**.
3. Click **OneDrive and SharePoint**.

The OneDrive and SharePoint Dashboard includes the following panels:

Panel	Source Type	Datamodel
Activity by Location	`o365:management:activity`	n/a
Operations over Time	`o365:management:activity`	n/a
Activity by User	`o365:management:activity`	n/a
Items Shared with External Users	`o365:management:activity`	n/a
Risky Downloads over Time	`o365:management:activity`	n/a
Permission Changes	`o365:management:activity`	n/a
Top SharePoint Sites Accessed	`o365:management:activity`	n/a

Security and Compliance

To access the Security and Compliance dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Cloud Security**.
2. Click **Microsoft 365**.
3. Click **Security and Compliance**.

The Security and Compliance Dashboard includes the following panels:

Panel	Source Type	Datamodel
Alerts over Time	`o365:management:activity`	n/a
Alerts by User	`o365:management:activity`	n/a
Alerts by Name	`o365:management:activity`	n/a
Alert Details	`o365:management:activity`	n/a

Filter your panel results

You can filter the results that you see in the dashboard panels.

Filter	Description
Time Range	Define the time range of a search with the **time range picker**. Even though you can change the time range for all the panels, the behavior is different for the **Password Account Lockouts** panel. Changing the time range only changes the trend line in the panel. It doesn't change the number that displays in the panel. The time range for the number is hardcoded to 24 hours.

Included Add-ons

Viewing data from Splunk UBA in Enterprise Security

After you integrate Splunk Enterprise Security and Splunk User Behavior Analytics (UBA), the apps can share information and allow you to identify different types of security threats in your environment and facing your organization.

- Send threats and anomalies from Splunk UBA to Splunk Enterprise Security to adjust risk scores and create notable events.
- Send correlation search results from Splunk Enterprise Security to Splunk UBA to be processed for anomalies.
- Retrieve user and device association data from Splunk UBA to view it in Splunk Enterprise Security. Identify user accounts and devices associated with devices during specific sessions, and devices associated with users during specific sessions.

In Enterprise Security, you can see data from Splunk UBA In several places.

- View anomalies on the UBA Anomalies dashboard.
- View threat and anomaly swim lanes on the Asset and Identity Investigator dashboards.

See Integrate Splunk Enterprise Security and Splunk UBA with the Splunk add-on for Splunk UBA in the *Send and Receive Data from the Splunk Platform* manual.

View threats on Security Posture and Incident Review

Threats sent from Splunk UBA to Splunk Enterprise Security appear as notable events on the Incident Review and Security Posture dashboards. You can see the count of notable events created from threats on the Security Posture dashboard as a Key Security Indicator (KSI).

On Incident Review, you can expand the event details to see the description, threat category, correlation search referencing Splunk UBA, and more details. Use the workflow actions on the event to **View Contributing Anomalies** and open the Threat Details page in Splunk UBA. See Threat Details in *Use Splunk User Behavior Analytics*.

View anomalies on the UBA Anomalies dashboard

You can use the UBA Anomalies dashboard to view anomalies from Splunk UBA in Enterprise Security and understand anomalous activity in your environment. Select **Security Intelligence > User Intelligence > UBA Anomalies** to view the dashboard.

- See how the count of various metrics have changed over the past 48 hours in your environment with the key indicators. Review the count of UBA notables, UBA anomaly actors, UBA anomaly signatures, UBA anomalies per threat, and the total count of UBA anomalies.
- Investigate spikes in anomalous activity and compare the number of actors with the number of anomalies over time on the **Anomalies Over Time** panel.
- Identify the most common types of anomalous activity on the **Most Active Signatures** panel.
- Determine which users, devices, apps, and other actors are responsible for the most anomalous activity on the **Most Active Actors** panel.
- See the latest anomalous activity on the **Recent UBA Anomalies** panel.

View an anomaly in Splunk UBA by clicking on a value on the dashboard to drill down to the search. Use the event actions on a specific anomaly event to **View Contributing Anomalies** and open Splunk UBA to view the **Anomaly Details** view. See Anomaly Details in *Use Splunk User Behavior Analytics*.

View threat and anomaly swim lanes on the Asset and Identity Investigator dashboards

You can use swim lanes on the Asset and Identity Investigator dashboards to correlate counts of UBA threats and anomalies with other notable events in ES.

To see anomaly and threat information associated with each asset or identity that you search, add the UEBA Threats and UBA Anomalies swim lanes to the Asset Investigator and Identity Investigator dashboards. See Edit the swim lanes.

View an anomaly in Splunk UBA by clicking the swim lane to open a search with additional details. Use the event actions to **View Contributing Anomalies** and open Splunk UBA to view the **Anomaly Details** or **Threat Details**. See Review current threats for more.

Anomalies and threats modify risk scores

Enterprise Security uses the risk score of anomalies and threats from Splunk UBA to modify risk for the assets and identities associated with the threats and anomalies. The risk score modifier is 10 times the risk score of the anomaly or threat in Splunk UBA.

For example:

1. Splunk UBA sends Enterprise Security an anomaly that applies to the host `10.11.12.123`. The anomaly has a risk score of 8.
2. Enterprise Security modifies the risk for the host `10.11.12.123` in response to the anomaly. A risk modifier of 10 * UBA risk score results in a risk modifier of 80.

You can see the source of increased risk when analyzing risk scores on the Risk Analysis dashboard.

Send correlation search results to Splunk UBA

After you set up Enterprise Security and Splunk UBA, you can start sending correlation search results to Splunk UBA. You can send correlation search results automatically, or you can send correlation search results in an ad-hoc manner by sending notable events from the Incident Review dashboard.

Automatically send correlation search results to Splunk UBA

Edit an existing correlation search or create a new correlation search to add a response action of **Send to UBA** to automatically send correlation search results to Splunk UBA.

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click the name of a correlation search or click **Create New** to create a new correlation search.
3. Click **Add New Response Action** and select **Send to UBA**.
4. Type a **Severity** to set the score in Splunk UBA for an anomaly that might be created from the correlation search result.
   For example, type 7 to represent a high severity.
5. Save the correlation search.

Send correlation search results ad-hoc from Incident Review

Send notable events created by correlation search results to Splunk UBA in an ad-hoc manner from the Incident Review dashboard.

1. On the Incident Review dashboard, locate the notable event that you want to send to Splunk UBA.
2. From the **Actions** column, select **Run Adaptive Response Actions**.
3. Click **Add New Response Action** and select **Send to UBA**.
4. (Optional) Type a **Severity** to set the score in Splunk UBA for the anomaly that might be created from the notable event. The severity that you type takes precedence over the default severity of the notable event.
5. Click **Run** to run the response action and send the notable event details to Splunk UBA.

Types of results to send to Splunk UBA

Only some correlation search results create anomalies in Splunk UBA. Splunk UBA parses the correlation search results as external alarms, and correlation searches with a source, destination, or user in the results are most likely to produce anomalies in Splunk UBA. Not all correlation search results sent from Enterprise Security appear as anomalies in Splunk UBA. Splunk UBA only creates anomalies for the correlation search results with relevant data, and ignores other correlation search results.