Table of Contents

Overview.................................................................................................................................1
Administering Splunk Enterprise Security...........................................................................1

Incident Review and Investigations.........................................................................................3
Managing Incident Review in Splunk Enterprise Security....................................................3
Customize Incident Review in Splunk Enterprise Security.......................................................4
Manually create a notable event in Splunk Enterprise Security..............................................7
Customize notable event settings in Splunk Enterprise Security............................................9
Expand tokens in notable events using the expandtoken command......................................17
Manage investigations in Splunk Enterprise Security..............................................................19
Administer and customize the investigation workbench......................................................20
Manage and customize investigation statuses in Splunk Enterprise Security..........................28

Correlation Searches..............................................................................................................32
Correlation search overview for Splunk Enterprise Security................................................32
Create correlation searches in Splunk Enterprise Security....................................................32
Configure correlation searches in Splunk Enterprise Security................................................33
List correlation searches in Splunk Enterprise Security..........................................................37
Upgrade correlation searches in Splunk Enterprise Security..................................................38
Create sequence templates in Splunk Enterprise Security.....................................................43
Set up adaptive response actions in Splunk Enterprise Security............................................43
Set up an adaptive response relay from a Splunk Cloud Enterprise Security search head to an on-premises device.................................................................57
Configure adaptive response actions for a correlation search in Splunk Enterprise Security..............................................................................................................61

Assets and Identities..............................................................................................................68
Add asset and identity data to Splunk Enterprise Security.....................................................68
Collect and extract asset and identity data in Splunk Enterprise Security.............................68
Define identity formats in Splunk Enterprise Security............................................................70
Format an asset or identity list as a lookup in Splunk Enterprise Security...............................70
Configure a new asset or identity list in Splunk Enterprise Security.......................................79
Verify that your asset and identity data was added to Splunk Enterprise Security....................82
Configure asset and identity correlation in Splunk Enterprise Security.................................83
How Splunk Enterprise Security processes and merges asset and
Table of Contents

Assets and Identities

  identity data .......................................................................................................................... 85
  Lookups that store merged asset and identity data in Splunk Enterprise Security .......................................................... 86
  Asset and identity fields after processing in Splunk Enterprise Security ................................................................. 87
  Test the asset and identity merge process in Splunk Enterprise Security ................................................................. 90
  Customize the asset and identity merge process in Splunk Enterprise Security .............................................................. 90
  Modify asset and identity lookups in Splunk Enterprise Security ...................................................................................... 90
  Example methods of adding asset and identity data in Splunk Enterprise Security .......................................................... 93

Threat Intelligence ............................................................................................................................... 96

  Add threat intelligence to Splunk Enterprise Security ......................................................................................... 96
  Supported types of threat intelligence in Splunk Enterprise Security ............................................................................. 97
  Configure the intelligence sources included with Splunk Enterprise Security ............................................................. 98
  Download a threat intelligence feed from the Internet in Splunk Enterprise Security ......................................................... 101
  Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security ................................................ 108
  Upload a custom CSV file of threat intelligence in Splunk Enterprise Security ............................................................... 108
  Add threat intelligence from Splunk events in Splunk Enterprise Security ........................................................................ 111
  Add and maintain threat intelligence locally in Splunk Enterprise Security ................................................................. 112
  Add threat intelligence with a custom lookup file in Splunk Enterprise Security .............................................................. 113
  Verify that you have added intelligence successfully to Splunk Enterprise Security .......................................................... 113
  Change existing intelligence in Splunk Enterprise Security ............................................................................................... 115
  Example: Add a ransomware threat feed to Splunk Enterprise Security ............................................................................. 117

Generic Intelligence ........................................................................................................................................ 122

  Add intelligence to Splunk Enterprise Security ................................................................................................. 122
  Download an intelligence feed from the Internet in Splunk Enterprise Security .............................................................. 122
# Table of Contents

## Generic Intelligence
- Security.................................................................................................. 122
- Use generic intelligence in search with inputintelligence.................. 125
- Example: Add a generic intelligence source to Splunk Enterprise Security.................................................................................................. 128

## Managing Content.................................................................................. 131
- Managing content in Splunk Enterprise Security.................................... 131
- Create and manage data models in Splunk Enterprise Security............. 131
- Create and manage key indicator searches in Splunk Enterprise Security.................................................................................................. 132
- Create and manage saved searches in Splunk Enterprise Security.......... 134
- Create and manage search-driven lookups in Splunk Enterprise Security.................................................................................................. 135
- Create and manage swim lane searches in Splunk Enterprise Security.................................................................................................. 139
- Create and manage views in Splunk Enterprise Security....................... 140
- Export content from Splunk Enterprise Security as an app..................... 141
- Create and manage lookups in Splunk Enterprise Security.................... 143
- Manage internal lookups in Splunk Enterprise Security.......................... 145
- Create risk and edit risk objects in Splunk Enterprise Security............... 156
- Expand Content Management searches to view dependency and usage information in Splunk Enterprise Security................................... 156
- Use analytic stories through the use case library in Splunk Enterprise Security.................................................................................................. 158

## Configuration and Troubleshooting....................................................... 165
- Configure general settings for Splunk Enterprise Security...................... 165
- Manage credentials in Splunk Enterprise Security.................................. 167
- Manage permissions in Splunk Enterprise Security.................................. 169
- Customize the menu bar in Splunk Enterprise Security......................... 170
- Configure per-panel filtering in Splunk Enterprise Security..................... 177
- Create a Splunk Web message in Splunk Enterprise Security............... 179
- Troubleshoot script errors in Splunk Enterprise Security...................... 181
- Troubleshoot messages about default indexes searched by the admin role.................................................................................................. 182
- Troubleshoot messages about unnecessary read or write access to investigation KV store collections........................................................... 184
- Troubleshoot failed intelligence downloads in Splunk Enterprise
# Table of Contents

**Configuration and Troubleshooting**
- Security......................................................................................................................... 185
- Troubleshoot dashboards in Splunk Enterprise Security.............................................. 185
- Dashboard requirements matrix for Splunk Enterprise Security.............................. 187

**Extreme Search............................................................................................................**
- How Splunk Enterprise Security uses extreme search................................................. 203
- Extreme search example in Splunk Enterprise Security............................................. 209
- Extreme search commands....................................................................................... 215
Overview

Administering Splunk Enterprise Security

Splunk Enterprise Security administrators are responsible for configuring, maintaining, auditing, and customizing an instance of Splunk Enterprise Security. If you are not administering Splunk Enterprise Security, see *Use Splunk Enterprise Security* for an introduction to using this app as a security analyst.

Use the links below to learn more about administrative tasks in Splunk Enterprise Security.

Manage and support analyst workflows

To enable and customize the workflows for analysts in your organization, see:

- Managing Incident Review in Splunk Enterprise Security
- Customize Incident Review in Splunk Enterprise Security
- Customize notable event settings in Splunk Enterprise Security
- Manage investigations in Splunk Enterprise Security

Enrich data for Enterprise Security

Enrich Splunk Enterprise Security with data about the assets and identities in your environment and with additional data about known threats.

- See *Add asset and identity data to Splunk Enterprise Security* for a full list of tasks related to adding and managing asset and identity data in Splunk Enterprise Security.
- See *Add threat intelligence to Splunk Enterprise Security* for information on all tasks related to managing threat intelligence sources in Splunk Enterprise Security.

Manage and customize configurations

To perform ongoing configuration in Splunk Enterprise Security, see:

- Configure general settings for Splunk Enterprise Security
- Manage input credentials in Splunk Enterprise Security
- Manage permissions in Splunk Enterprise Security
• Customize the menu bar in Splunk Enterprise Security
• Configure advanced filtering in Splunk Enterprise Security

You can find additional configuration information in the *Install and Upgrade Manual*.

• Configure and deploy indexes
• Configure users and roles
• Configure data models for Splunk Enterprise Security

**Create, manage, and export content**

To create new content or manage and customize existing content, see:

• Create correlation searches in Splunk Enterprise Security
• Create and manage key indicator searches in Splunk Enterprise Security
• Create and manage saved searches in Splunk Enterprise Security
• Create and manage search-driven lookups in Splunk Enterprise Security
• Create and manage swim lane searches in Splunk Enterprise Security
• Create and manage views in Splunk Enterprise Security
• Create and manage lookups in Splunk Enterprise Security
• Create risk and edit risk objects in Splunk Enterprise Security

To share custom content with other ES instances, see Export content from Splunk Enterprise Security as an app.

**Troubleshoot dashboards**

• For tips and best practices useful for troubleshooting dashboards in Enterprise Security, see Troubleshoot dashboards in Splunk Enterprise Security.
• For information about data model datasets that populate Enterprise Security dashboards, see Dashboard requirements matrix for Splunk Enterprise Security.
• For an overview of all dashboards in Splunk Enterprise Security, see Introduction to the dashboards available in Splunk Enterprise Security in Use Splunk Enterprise Security.
Incident Review and Investigations

Managing Incident Review in Splunk Enterprise Security

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 an alert called a notable event.

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

- For information about how analysts use the Incident Review dashboard, see Incident Review overview in Use Splunk Enterprise Security.
- To audit and review analyst activity on the Incident Review dashboard, see Incident Review Audit in Use Splunk Enterprise Security.
- To customize the display of the Incident Review dashboard, and also modify analyst capabilities and permissions, see Customize Incident Review in Splunk Enterprise Security.
- To manually create notable events, see Manually create a notable event in Splunk Enterprise Security.
- To customize settings for notable events, see Customize notable event settings in Splunk Enterprise Security.
- For more information about how notable events are populated and managed by the notable event framework, see Notable Event framework in Splunk Enterprise Security on the Splunk developer portal.

How risk scores display in Incident Review

Risk scores do not display in Incident Review for every asset or identity. Only assets or identities (risk objects) that have a risk score and a risk object type of "system" or "user" display in Incident Review. Risk scores only show for the following fields: orig_host, dvc, src, dest, src_user, and user. The risk score for an asset or identity might not match the score on the Risk Analysis dashboard. The risk score is a cumulative score for an asset or identity, rather than a score specific to an exact username.
For example, if a person has a username of "buttercup" that has a risk score of 40, and an email address of "buttercup@splunk.com" with a risk score of 60, and the identity lookup identifies that "buttercup" and "buttercup@splunk.com" belong to the same person, a risk score of 100 displays on Incident Review for both "buttercup" and "buttercup@splunk.com" accounts.

As another example, if an IP of 10.11.36.1 has a risk score of 80 and an IP of 10.11.36.19 has a risk score of 30, and the asset lookup identifies that a range of IPs "10.11.36.1 - 10.11.36.19" belong to the same asset, a risk score of 110 displays on Incident Review for both "10.11.36.1" and "10.11.36.19" IP addresses.

Risk scores are calculated for Incident Review using the Threat - Risk Correlation - Lookup Gen lookup generation search. The search runs every 30 minutes and updates the risk_correlation_lookup lookup file. To see more frequent updates to the risk scores in Incident Review, update the cron_schedule of the saved search.

**Notify an analyst of untriaged notable events**

You can use a correlation search to notify an analyst if a notable event has not been triaged.

1. Select Configure > Content > Content Management.
2. Locate the Untriaged Notable Events correlation search using the filters.
3. Modify the search, changing the notable event owner or status fields as desired.
4. Set the desired alert action.
5. Save the changes.
6. Enable the Untriaged Notable Events correlation search.

**Customize Incident Review in Splunk Enterprise Security**

As a Splunk Enterprise Security administrator, you can customize the way that analysts view and interact with notable events on the Incident Review dashboard.

**Modify analyst capabilities and permissions**

Configure whether analysts can override the calculated urgency of a notable event and choose whether to require an analyst to add a comment when
updating a notable event on the **Incident Review Settings** page.

1. Select **Configure > Incident Management > Incident Review Settings** to view the Incident Review settings.
2. Allow or prevent analysts from overriding the calculated urgency of a notable event with the **Allow Overriding of Urgency** checkbox. Analysts are allowed to override urgency by default.
3. Require analysts to add a comment when updating a notable event by checking the **Required** checkbox under **Comments**.
4. If you require analysts to add a comment, enter the minimum character length for required comments. The default character length is 20 characters.

**Configure the recommended capacity for analysts**

Configure the recommended maximum number of notable events that should be assigned per security analyst on the **General Settings** page.

1. Select **Configure > General > General Settings** to view the General Settings.
2. Enter a preferred number of notable events that should be assigned to an analyst with the **Incident Review Analyst Capacity** setting. The default is 12.

This value is used for audit purposes, and does not prevent more than the default number of notable events from being assigned to an analyst.

**Change Incident Review columns**

You can change the columns displayed on the Incident Review dashboard.

1. Review the existing columns in **Incident Review - Table Attributes**.
2. Use the action column to edit, remove, or change the order of the available columns.
3. Add custom columns by selecting **Insert below** or selecting **More...**, then **Insert above**.

**Troubleshoot an issue where analysts cannot edit notable events successfully on Incident Review**

If analysts cannot edit notable events successfully on Incident Review, several issues could be the cause.
The analyst might not have permission to make status transitions. See Manage notable event statuses.
The analyst might be attempting to edit a notable event that is visible, but cannot be edited successfully due to the limited number of events that can be retrieved from a bucket.

If a correlation search creates a high number of notable events in a short period of time, such as 1000 in less than five minutes, the Incident Review dashboard can hit the max_events_per_bucket limit when attempting to retrieve notable events for display from the notable index.

If analysts are unable to edit a notable event for this reason, the analyst can use a smaller time range when reviewing notable events on Incident Review. For example, a time range that reduces the number of events on the Incident Review dashboard to less than 1000. 1000 is the default value of max_events_per_bucket, so search that produces less than 1000 events cannot produce this error.

To prevent this from happening at any time, you can modify the maximum number of events that can be returned from a bucket. However, modifying this setting can negatively affect the performance of your Splunk software deployment.

If you are running Splunk Enterprise Security on Splunk Cloud, file a support ticket for assistance with this setting.

2. Set max_events_per_bucket to a number above 1000.
3. Save.

See limits.conf for more about the max_events_per_bucket setting.

Add a navigation link to a filtered view of Incident Review

To help ES analysts with their workflows, you can add a link in the app navigation that loads a version of Incident Review with filters applied. See Add a link to a filtered view of Incident Review.
Manually create a notable event in Splunk Enterprise Security

You can manually create a notable event from an indexed event, or create one from scratch.

**Note:** By default, only administrators with the edit_reviewstatus capability can manually create notable events. To grant other users this capability, see Configure users and roles in the *Installation and Upgrade Manual*.

**Create a notable event from an existing event**

You can create a notable event from any indexed event using the *Event Actions* menu. Do not create a notable event from notable events on the Incident Review dashboard.

1. From an event, view the event details and click *Event Actions*.
2. Select **Create notable event**.
3. Enter a **Title** for the event.
4. (Optional) Select a security **Domain**.
5. (Optional) Select an **Urgency** level.
6. (Optional) Select an **Owner**.
7. (Optional) Select a **Status**.
8. Enter a **Description** for the event that describes why you created the notable event or what needs to be investigated.
9. Save the new notable event. The *Incident Review* dashboard displays with your new notable event.

**Note:** A notable event created in this way includes tracking fields such as **Owner** and **Status**, but does not include the unique fields or links created when a notable event is generated by a correlation search alert action.

**Create a notable event from scratch**

Create a notable event based on observations, a finding from a security system outside Splunk, or something else.

1. Select **Configure > Incident Management > New Notable Event**.
2. Enter a **Title** for the event.
3. (Optional) Select a security **Domain**.
4. (Optional) Select an **Urgency** level.
5. (Optional) Select an **Owner**.
6. (Optional) Select a **Status**.
7. Enter a **Description** for the event that describes why you created the notable event or what needs to be investigated.
8. Save the new notable event. The **Incident Review** dashboard displays with your new notable event.

**Use the owner field in a Splunk event to create a notable event with said owner**

Normally in a correlation search, the **owner** field automatically maps to **orig_owner**. If you have some Splunk events, doesn't matter where they came from, and you want the owner field of the Splunk event to be the owner of the notable event, it is crucial that the value of the **owner** field is a Splunk username. To use the owner field in a Splunk event to create a notable event with said owner, remove the **owner** field from the list of notable mapfields.

Your correlation rule will look similar to the following in

$SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/local/savedsearches.conf:

```
# savedsearches.conf
[Threat ? My Correlation ? Rule]
? action.notable.param.mapfields = rule_id,rule_name,rule_title,rule_description,security_domain,nes_fields,drilldown_name,drilldown_search,governance,contro...rule_description,security_domain,nes_fields,drilldown_name,drilldown_search,governance,contro...
?
```

For example, if you have a CSV lookup that contains the "owner" field for assigning the new owners, then you can dynamically update the owner of an event in incident review by updating the lookup using a search similar to this one:

```
| inputlookup es_notable_events | search owner=gleb | eval owner="george"| outputlookup es_notable_events append=true key_field=owner
```

**Pinpoint the original event via drill-down**

If you are creating a notable event from a raw event, you can pinpoint the specific raw event that contributed to the notable event.

When certain fields exist such as **orig_event_hash**, a secondary drill-down link is automatically constructed for you called "View original event." If the correct fields are passed with the notable event you can construct a very performant search for getting back to the original event.
The following fields come into play:

- `orig_time` (optional)
- `orig_index` (optional)
- `orig_indexer_guid` (optional)
- `orig_event_hash` (required)

The `orig_time` and `orig_index` are automatically created if you pass `_time` and `index` respectively. This is because `_time` and `index` are included in the default set of `mapfields`. For `indexer_guid` and `event_hash` you will either need to manually rename to `orig_<field>` or add them to `mapfields` as appropriate.

Your correlation rule will look similar to the following in

```
[SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/local/savedsearches.conf]

# savedsearches.conf
[Threat: My Correlation: Rule]

action.notable.param.mapfields = rule_id,rule_name,rule_title,rule_description,security_domain,nes_fields,drilldown_name,drilldown_search,governance,contro
```

Customize notable event settings in Splunk Enterprise Security

As a Splunk Enterprise Security administrator, you can make configuration changes to notable events.

- Change notable event fields.
- Manage notable event statuses.
- Create and manage notable event suppressions.

Change notable event fields

Make changes to the fields displayed on the Incident Review dashboard for notable events on the Incident Review Settings dashboard. For example, change the label of a field in the notable event details, remove a field, or add a field to the Additional Fields section of the notable event details. Changes that you make to notable event fields affect all notable events.

1. From the Splunk Enterprise Security menu bar, select **Configure > Incident Management > Incident Review Settings.**
2. Review the **Incident Review - Event Attributes**.
3. Click **Edit** to change a field or the label for a specific field that appears on Incident Review.
4. Click **Remove** to remove a field from the notable event details on the Incident Review dashboard.
5. Click **Save** to save your changes.

**Add a field to the notable event details**

A field appears in the **Additional fields** of the notable event details if the field exists in the correlation search results and Incident Review can display the field. To add a field to the notable event details, first make sure that the correlation search results include the field and then make sure that Incident Review can display the field.

1. Determine if the field you want to see is included in the correlation search results. Run the correlation search on the Search page to review the output or the search syntax.
   - If the field exists in the search results, go to step four.
   - If the field does not exist in the search results, go to step two.
2. Modify the correlation search to include the field.
   - If you can edit the search with the guided search editor, add the field as an aggregate function with an alias. Use the **values** function to return all possible values of a given field, or the **latest** function to return the most recent value for the field.
   - If you created the search manually, modify the search to extract the fields. Make sure that you do not modify the correlation criteria when you modify the search.
     - If the search does not include statistical transformations, add `| fields + newfieldname` to the end of the search, where `newfieldname` is the name of the new field you want to see in the additional details.
     - If the search does include statistical transformations, extract the fields when you perform the statistical transformation. For example, if your search includes a stats search `| stats count by src | where count>5`, the `src` and `count` fields appear in the notable event details. To add the `dest` field to the notable event details, you might change the search to the following: `| stats values(dest) as dest, count by src`.
3. Verify changes to correlation searches on the Search page before saving them.
4. Add the field to the list of additional fields.
1. From the Splunk Enterprise Security menu bar, select **Configure > Incident Management > Incident Review Settings**.
2. Click **Add new entry** to add the new field to the **Additional Fields** section of the notable event details.
3. Type a **Label** to use as the display name of the field in the notable event details.
4. Type a **Field** to match the field that you want to appear in the notable event details.
5. Click **Done**.
6. Click **Save**.

**Manage notable event statuses**

An analyst assigns a status to a notable event in the investigation workflow. The status aligns with the stages of an investigation, and can be used to review and report on the progress of a notable event investigation on the Incident Review Audit dashboard.

To see the available statuses for notable events, select **Configure > Incident Management > Status Configuration**.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Can be edited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unassigned</td>
<td>Used by Enterprise Security when an error prevents the notable event from having a valid status assignment.</td>
<td>No</td>
</tr>
<tr>
<td>New (default)</td>
<td>The notable event has not been reviewed.</td>
<td>No</td>
</tr>
<tr>
<td>In Progress</td>
<td>An investigation or response to the notable event is in progress.</td>
<td>Yes</td>
</tr>
<tr>
<td>Pending</td>
<td>Closure of the notable event is pending some action.</td>
<td>Yes</td>
</tr>
<tr>
<td>Resolved</td>
<td>The notable event has been resolved and awaits verification.</td>
<td>Yes</td>
</tr>
<tr>
<td>Closed</td>
<td>The notable event has been resolved and verified.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Every notable event is assigned a status of **New** by default when it is created by a correlation search. You can customize notable event statuses to match an existing workflow at your organization.
**Edit notable event statuses**

Change the available statuses for notable events on the **Edit Notable Event Status** page.

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. Select a notable event status to open the **Edit Notable Event Status** page.
3. (Optional) Change the **Label** or **Description**.

You cannot edit the **Unassigned** and **New** statuses because they are defaults used when creating notable events.

**Manage notable event status history**

Notable events are associated with users, statuses, and comments. Changes made to status names only affect the name of a status, not the status ID assigned to the notable event in the notable index.

If you change the name of a default notable event status, the name changes for both past and future notable events. For example, if you rename "pending" to "waiting for customer", all notable events with a status of "pending" will then have a status of "waiting for customer". The status ID assigned to the notable events remains the same.

**Notable event status transitions**

Statuses represent the steps in investigating a notable event. Status transitions define the path of a notable event investigation.

An analyst changes the status of the notable event as the investigation progresses. To change the status of a notable event:

- The analyst must be a member of a role that has permission to change a status. The ability to change notable event statuses is available to the **ess_analyst** and **ess_admin** roles by default.
- The follow-on status must allow a transition from the current status. By default, every status can transition to any other status. For example, an analyst can change the status of a notable event with the **New** status to any other status, such as **Closed**.
Restrict notable event status transitions

You can define a status workflow and limit which statuses analysts can transition to other statuses, creating a path for a notable event investigation. By default, a notable event in any status can be changed to any other status.

Prerequisites

- You must have the ess_admin role or your role must be assigned the Edit Statuses capability. For more information about user roles and capabilities, see Configure users and roles in the Installation and Upgrade Manual.
- Define a status workflow for notable event investigations. Determine which statuses to require, and whether analysts must follow a specific sequence of statuses before completing the workflow. Determine whether any roles can bypass the full workflow.

Steps

2. Select a notable event status to open the Edit Notable Event Status page.
3. In Status Transitions, modify the To Status fields. These fields control which statuses analysts can transition a notable event to if it is in the status that you are editing.
   1. To define which roles are allowed to transition a notable event to the selected status, choose the Authorization field and add or remove roles.
   2. To remove a transition for an event to the selected status, choose Unselect All.
4. Click Save.

Example of restricting notable event status transitions

This example walks you through setting up restricting status transitions for analysts. Restrict status transitions so that analysts must follow a path from New, to In Progress or Pending, to Resolved, then to Closed.

2. Restrict the transitions from the New status. Select the New status to open the Edit Investigation Status page.
3. In **Status Transitions**, select the roles for the **Resolved** status and
deselect the check box for the ess_analyst role.
4. Select the roles for the **Closed** status and deselect the check box for the
ess_analyst role.
5. Click **Save** to save the changes to the **New** status.
6. Restrict the transitions on the **In Progress** and **Pending** statuses to
prevent the ess_analyst role from transitioning to **New** or to **Closed**.
7. Select the **In Progress** status.
8. In **Status Transition**, select the roles for the **New** status and deselect the
check box for the ess_analyst role. Repeat for the **Closed** status.
9. Click **Save** to save the changes to the **In Progress** status.
10. Repeat steps 8 and 9 for the **Pending** status.
11. Restrict the **Resolved** status. Click the **Investigation** tab and select the
**Resolved** status.
12. In **Status Transition**, select the roles for the **New** status and deselect the
check box for the ess_analyst role. Repeat for the **In Progress** and
**Pending** statuses.
13. Click **Save** to save the changes to the **Resolved** status.
14. Restrict the transitions for the **Closed** status. Select the **Closed** status.
15. In **Status Transition**, select the roles for the **New** status and deselect the
check box for the ess_analyst role. Repeat for the **In Progress, Pending,**
and **Resolved** statuses.
16. Click **Save** to save the changes for the **Closed** status.

**Create a status**

Create a status for the notable event investigation workflow.

**Prerequisites**

If you restrict status transitions, determine where the new status is needed in the
workflow and whether any roles can bypass the new status in the workflow.

**Steps**

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident
Management > Status Configuration**.
2. Select **Create New Status > Notable**.
3. Type a **Label** that represents the status on the Incident Review
dashboard.
   For example, Waiting on ITOps.
4. (Optional) Type a description that appears on the Status Configuration
   page.
For example, Waiting on the IT operations department.

5. (Optional) Select the check box for Default Status. Select this check box if you want to replace the New status as the default status for newly-created notable events.

6. (Optional) Select the check box for End Status. Select this check box if you are adding an additional Closed status for notable events, such as False Positive.

7. (Optional) Deselect the check box for Enabled. Deselect this check box if you want to create this status without using it.

8. Update the status transitions by modifying the To Status fields. If you do not select any roles that can transition from this status to another one, no one will be able to move the notable event to a different status after transitioning the notable event to this status. If you do not restrict status transitions, select all roles for each status.

9. Click Save.

If you restrict status transitions based on user roles, modify the status transitions for each status that can transition to this new status.

**Create and manage notable event suppressions**

You can hide notable events from the Incident Review dashboard by creating a notable event suppression.

A suppression is a search filter that hides additional notable events from view, and is used to stop excessive or unwanted numbers of notable events from appearing on the Incident Review dashboard. Notable events that meet the search conditions are still created and added to the notable index. Suppressed notable events continue to contribute to notable event counts on the Security Posture and auditing dashboards.

To prevent notable events that meet certain conditions from being created, see Throttle the number of response actions generated by a correlation search.

You can create a suppression filter in two ways.

- Create a suppression from Incident Review. See Suppress a notable event.
- Create a suppression from the Configure menu. See Create a suppression from Notable Event Suppressions.
Create a suppression from Notable Event Suppressions

1. Select Configure > Incident Management > Notable Event Suppressions.
2. Click Create New Suppression.
3. Enter a Name and Description for the suppression filter.
4. Enter a Search to use to find notable events to be suppressed. The search goes directly into the eventtype stanza, so the use of pipes is limited. See eventtypes.conf in the Splunk Enterprise Admin Manual.
5. Set the Expiration Time. This defines a time limit for the suppression filter. The expiration time does not prevent the suppression from working, so events within the specified time range will continue to be suppressed until you disable the suppression. Notable events that fall outside the expiration time are not suppressed.

Edit notable event suppressions

1. Select Configure > Incident Management > Notable Event Suppressions.
2. Select a notable event suppression to open the Edit Notable Event Suppression page.
3. Edit the Description and Search fields used for the suppression filter.
4. Click Save.

Disable notable event suppressions

1. Select Configure > Incident Management > Notable Event Suppressions.
2. Select Disable in the Status column for the notable event suppression.

Remove a notable event suppression

1. From the Splunk platform toolbar, select Settings > Event types.
2. Search for the the suppression event: notable_suppression-<suppression_name>.
3. Select delete in the Actions column for the notable event suppression.

Audit notable event suppressions

Audit notable event suppressions with the Suppression Audit dashboard. See Suppression Audit in Use Splunk Enterprise Security.
Expand tokens in notable events using the expandtoken command

Tokens in notable event titles and descriptions automatically get expanded to include the values of the tokens on the Incident Review dashboard. With the `expandtoken` search command, you can expand the tokens in so that token replacement happens in your search results. The `expandtoken` search command is intended for use in Splunk Web.

**Description**

Expand the fields in notable events that contain tokens in the values, such as the title (`rule_name`) or description (`rule_description`) of a notable event. Tokens are automatically expanded on the Incident Review dashboard, but not within search.

**Syntax**

```plaintext
... | expandtoken [field],[field1],[field2]...
```

**Optional argument**

`field`

**Description:** The name of a field in the notable event that contains a token to expand. Do not specify the name of the token. Specify additional fields separated by commas. If you do not specify a field, all fields are processed for tokens to expand. For a list of example fields in notable events, see Using notable events in search in the Splunk developer portal.

**Usage**

The `expandtoken` command is a **streaming command**.

**Limitations**

The search command does not support token delimiters in the middle of a field name.

If you have tokens dependent on the expansion of other tokens, those tokens might not be reliably expanded because you cannot specify the order in which
tokens are expanded. For example, if you have a rule_description: "Brute force access behavior detected from $src$." and a drilldown_name: "See contributing events for $rule_description$", the following search might expand the $src$ token without expanding the $rule_description$ token.

`
`notable` | expandtoken

For more information about tokens, see Token usage in dashboards in the Splunk Enterprise *Dashboards and Visualizations Manual*.

**Examples**

The following examples show usage of the `expandtoken` search command in Splunk Web.

**Expand tokens for all notable events**

`
`notable` | expandtoken
rule_title,rule_description,drilldown_name,drilldown_search

**Expand tokens for a specific notable event**

Expand tokens for a specific notable event based on the event_id field.

`
`notable` | where event_id="<event_id>" | expandtoken
rule_title,rule_description

Expand tokens for a specific notable event based on the short ID field.

`
`notable` | where notable_xref_id="<short ID>" | expandtoken
rule_title,rule_description

**See also**

For a list of example fields in notable events, see Using notable events in search in the Splunk developer portal.

For more information about tokens, see Token usage in dashboards in the Splunk Enterprise *Dashboards and Visualizations Manual*. 
Manage investigations in Splunk Enterprise Security

As an Enterprise Security administrator, you can manage access to security investigations, and support analysts by troubleshooting problems with their action history.

For more information about the analyst investigation workflow, see Investigations in Splunk Enterprise Security in *Use Splunk Enterprise Security*.

Manage access to investigations

Users with the *ess_admin* role can create, view, and manage investigations by default. Users with the *ess_analyst* role can create and edit investigations. Make changes to capabilities with the Permissions dashboard.

- To allow other users to create or edit an investigation, add the *Manage Your Investigations* capability to their role. Users can only make changes on investigations on which they are a collaborator.
- To allow other users to manage, view, and delete all investigations, add the *Manage All Investigations* capability to their role.

See Configure users and and roles in the *Installation and Upgrade Manual*.

You can manage who can make changes to an investigation by setting write permissions for collaborators on a specific investigation. By default, all collaborators have write permissions for the investigations to which they are added, but other collaborators on the timeline can change those permissions to read-only. See Make changes to the collaborators on an investigation in *Use Splunk Enterprise Security*.

After a user creates an investigation, any user with the *Manage All Investigations* capability can view the investigation, but only the collaborators on the investigation can edit the investigation. You cannot view the investigation KV Store collections as lookups. Only users with the admin role can view or modify the KV store collections using the KV Store API endpoint. For details about using the KV Store API endpoint, see KV Store endpoint descriptions in the Splunk Enterprise REST API Reference Manual.

Data sources for investigations

Splunk Enterprise Security stores investigation information in several KV Store collections. The investigations on the Investigations page, items added to the
investigation, attachments added to notes on the investigation, and artifacts added to the investigation workbench each have their own collection. See Investigations in the Dashboard requirements matrix for Splunk Enterprise Security.

Investigation details from investigations created in versions earlier than 4.6.0 of Splunk Enterprise Security are stored in two KV Store collections, investigative_canvas and investigative_canvas_entries. Those collections are preserved in version 4.6.0 but the contents are added to the new investigation KV Store collections. So to restore, you may need to restore investigation, investigation_attachment, investigation_event, investigation_lead, investigative_canvas, and investigative_canvas_leads.

Troubleshoot investigation action history items

When an analyst selects a type of action history to add to an investigation, one of five searches run over the selected time range.

- Dashboard Views - Action History
- Search Tracking - Action History
- Per-Panel Filtering - Action History
- Notable Suppression - Action History
- Notable Status - Action History

View the searches by navigating to Configure > Content > Content Management and using the filters on the page. If you change these saved searches, action history items might fail to appear in your action history. To exclude a search from your action history, use the Action History Search Tracking Whitelist lookup. See Create and manage lookups in Splunk Enterprise Security.

Administer and customize the investigation workbench

The workbench extends existing investigation functionality in Splunk Enterprise Security by allowing analysts to perform investigative actions in one location. Analysts investigate artifacts, or assets and identities, using panels, tabs, and profiles on the workbench. You can customize the workbench by creating panels, tabs, and profiles to help analysts. You can also set up artifact extraction from notable events to accelerate investigations that start from notable events.
The workbench introduces a configuration file, `es_investigations.conf`, that is used to manage the metadata for panels, tabs, and profiles. You can make changes in the file system by adding stanzas to the `es_investigations.conf` file. Refer to `es_investigations.conf.spec` and `es_investigations.conf.example` for details.

**Create panels and tabs for the investigation workbench**

The investigation workbench can display any prebuilt panel that has a workbench panel reference and has been added to a workbench tab.

1. Create or modify a prebuilt panel. See Create or modify a prebuilt panel for the investigation workbench in this topic.
2. Create a workbench panel that references the prebuilt panel. See Create a tab for the investigation workbench in this topic.
3. Create a workbench tab that includes the workbench panel. See Create a tab for the investigation workbench in this topic.

For an example of this entire process, see Example panel conversion and workbench panel creation in this topic.

**Create or modify a prebuilt panel for the investigation workbench**

You can use any prebuilt panel on the investigation workbench. You can create one specifically for the workbench, or you can modify an existing panel. You can create or modify a prebuilt panel with Splunk Enterprise Security in several ways:

- Create a panel from Content Management.
  1. From the ES menu bar, select **Configure > Content > Content Management**.
  2. Select **Create New Content > Panel**.
  3. Type a **Prebuilt panel ID**.
  4. Select a **Destination App**.
  5. Type **Prebuilt panel XML**.
  6. Click **Save**.

- Convert a dashboard panel to a prebuilt panel. See Convert an existing panel to a prebuilt panel in *Dashboards and Visualizations*.

- Modify a panel in Splunk Settings.
  1. From the Splunk menu bar, select **Settings > User Interface**.
  2. Click **Prebuilt Panels** and click **Edit > Edit Panel** for the panel that you want to modify.
If you modify an existing prebuilt panel, consider cloning it before you modify it. If you clone the panel, change the panel ID so that you remember which one is specific to the workbench.

• Create a panel in Splunk Settings. See Add panels to dashboards in Dashboards and Visualizations.

When creating or modifying a prebuilt panel for the workbench, follow these guidelines for the best user experience:

• Add one or more tokens to the panel search to limit your search results to the artifacts investigated on the workbench. Use multiple tokens to substitute more than one type of artifact. Define your token using the syntax $\text{token}\$. You set up the format of the token when you create the workbench panel.

• Remove the panel name from the panel XML. If you do not do this, two panel titles appear on the workbench. Workbench panels get the title from the Label field when you create a workbench panel.

• Add a drilldown to the panel so that analysts can add artifacts from the panel. Add a drilldown using the syntax <option name="drilldown">cell</option> in the panel XML. The workbench replaces existing panel drilldowns, such as custom searches, with this ability to add artifacts to the workbench scope from the panel.

• Update the permissions on the panel to be shared with Splunk Enterprise Security. Confirm that the panel is Shared in App or set to Display For: All Apps.

• If you save your panel in a dedicated app, make sure that the objects in the app are set to export globally. See Set permissions for objects in a Splunk app in the Splunk dev portal.

• To make your panel use a different time range than the one set by the workbench, set a time range in the panel search or panel XML.

Then, follow the steps to create a panel for the investigation workbench. See Create a panel for the investigation workbench in this topic.

**Create or modify a panel for the investigation workbench**

Create a workbench panel.

1. Select Configure > Content > Content Management.
2. Select Create New Content > Workbench Panel.
3. Select the prebuilt panel that you want to use on workbench from the drop-down list.
4. (Optional) Type a **Label** to replace the default panel title on the workbench.

5. (Optional) Type a **Description** to provide information about the panel.

6. Add a token to replace the token in the panel search. See Example panel conversion and workbench panel creation in this topic or see Define tokens for multiselect inputs in the Splunk Enterprise *Dashboards and Visualizations Manual*.

   1. Select the type of artifact from the **Type** drop-down menu: Identity, Asset, File, or URL.
   2. Click **Apply**.

7. Click **Save**.

8. Click **Save**.

Then add the panel to a tab so that it is visible on the workbench.

**Modify a workbench panel.**

1. Select **Configure > Content > Content Management**.
2. From the Type filter, select **Workbench Panel**.
3. Click the name of the panel.
4. Edit something, such as a token.

Tokens are now displayed in summary view instead of list view. The summary view displays each token name, type of artifact, and a preview of the token text that is generated out of the artifacts and put into place to run the search.
When you click the pencil to edit a token in the summary view, it will slide open into edit mode. In the preview section at the bottom of the edit window, you can see how the token value changes as you edit the token parameters. This helps to simulate what you will see in the search under certain situations.

Create a tab for the investigation workbench

Create a tab to display information specific to a particular data type, use case, or something else.

1. Select **Configure > Content > Content Management**.
2. Select **Create New Content > Workbench Tab**.
3. Type a **Tab Name**. This name becomes part of the stanza name in `es_investigations.conf` and is used as the label if you do not specify a label.
4. (Optional) Type a **Label** to provide a user-facing name for the workbench tab.
5. In **Workbench Panels**, select the panels that you want to appear on this tab. The order in which you select the panels is the order in which they appear on this tab on the workbench.
6. (Optional) Select a workbench profile to associate with this tab. You can only associate a tab with one profile. Profiles allow analysts to load multiple tabs that relate to a use case on the workbench.
7. (Optional) Change the **Load by default** selection. Select **True** if you want this tab to load for all workbench investigations.
8. (Optional) Type a **Description** for the tab. This helps analysts determine what types of information and context they can gather using the panels on the tab.
9. Click **Save**.

**Example panel conversion and workbench panel creation**

**Prerequisite**

You must have the Splunk Add-on for Blue Coat ProxySG installed, and data from the add-on in your Splunk Enterprise Security deployment. You can download the Splunk Add-on for Blue Coat ProxySG from Splunkbase.

1. Clone a panel and modify the search to use an input token with the workbench.
   1. Select **Settings > User Interface**.
   2. Click **Prebuilt panels**.
   3. Click **Edit > Clone** for the `actions_by_destination_ip` for the Splunk_TA_bluecoat-proxysg.
   4. Type a Prebuilt panel ID: `workbench_actions_by_dest_ip`.
   5. Remove the title from the XML, unless you want two titles to appear on the workbench.
   6. Modify the query in the XML to include a token that limits the results to the investigated asset artifacts.
      ```xml
      sourcetype="bluecoat:proxysg:access*" $dest_token$ | iplocation dest | geostats count by action
      ```
   7. Decide whether to remove the `<earliest>` and `<latest>` time range for the panel. This time range takes precedence over the time range set on the workbench, so you likely want to remove it so that analysts can perform context-sensitive searches.
   8. Click **Save**.

2. Modify the permissions of the panel.
   1. Locate the panel that you just created, `workbench_actions_by_dest_ip`.
   2. Select **Edit > Edit Permissions**.
   3. For **Display for**, select **All apps**.
   4. Click **Save**.

3. Return to Splunk Enterprise Security and set up the panel to be used on the workbench.
   1. Select **Configure > Content > Content Management**.
   2. Select **Create New Content > Workbench Panel**.
   3. Select a **Panel Name** of `workbench_actions_by_dest_ip`.
   4. (Optional) Type a user-facing **Label** that appears on the workbench: **Proxy Actions by Destination**.
   5. (Optional) Type a user-facing description that appears on the workbench: **Displays a map that graphs the actions by**
destination IP, when possible, specific to the investigated assets.

6. Click Add a Token to add a token for the $dest_token$ from the search.

7. Type a Token Name that corresponds to the token name. 
   dest_token

8. Type a Prefix of (. 

9. Type a Suffix of ).

10. Type a Value Prefix of dest=". 

11. Type a Value Suffix of ".

12. Unselect the check box for Is Null for the Delimiter and type or in the text box. Include the spaces on either side of the OR.

13. Leave the check box for Is Null for the Default field selected. If this check box is selected, the search runs only when an artifact of the relevant type is selected on the workbench. In this case, the search runs only if you are exploring assets on the workbench.

14. Select a Type of Asset, because the destination is an asset, not an identity or file or URL.

15. Click the Available Artifacts buttons to see what the token value will look like if there are 0, 1, or 2 artifacts. For an example of two assets:

   (dest="<Asset_Value_1>" OR dest="<Asset_Value_2>")

16. Click Apply.

17. Click Save.

   This panel now contains a search that would be constructed as follows for two assets investigated on the workbench:

   sourcetype="bluecoat:proxysg:access*"
   (dest="<investigated_asset_1>" OR dest="<investigated_asset_2>") | iplocation dest | geostats count by action

4. Add the new panel to a new tab.

   1. On Content Management, select Create New Content > Workbench Tab.

   2. Type a Tab Name of proxy_data. This name becomes the stanza name in es_investigations.conf and is used as the label if the label is not specified.

   3. (Optional) Type a Label of Proxy Data.

   4. In Workbench Panels, type and select the Proxy Actions by Destination IP panel.

   5. For Load by default, leave it as False. Select True if you want this tab to load for all workbench investigations.

   6. (Optional) Type a Description for the tab. Proxy data related to investigated assets and identities.
7. Click **Save**.

Analysts can then open a workbench and add the new tab to start investigating proxy data in the workbench.

**Create a workbench profile**

You can use profiles on the workbench to associate several tabs together that all fit a specific use case. For example, a DDoS Investigation profile might include a Firewall data tab and a general Network data tab. An analyst can then add the DDoS Investigation profile to an investigation to add both of those tabs to the workbench, rather than having to individually add tabs that fit the investigation.

1. Select **Configure > Content > Content Management**.
2. Select **Create New Content > Workbench Profile**.
3. Type a **Profile Name**. This name becomes the stanza name in `es_investigations.conf` and is used as the label if the label is not specified.
4. (Optional) Type a **Label** to provide a user-facing name for the workbench profile.
5. (Optional) Type a **Description** for the profile. This helps analysts determine what types of information and context they can gather by adding the profile to their investigation.
6. Click **Save**.

After creating a profile, update the tabs with the profile that you created. For the DDoS investigation example, edit the Firewall data and Network data tabs and select the new DDoS Investigation profile.

**Set up artifact extraction for notable events**

You can define the fields that are automatically extracted as identities or assets on the workbench when a notable event is added to an investigation. By default, the same fields that are used for asset and identity correlation are the fields extracted from the notable events created by included correlation searches. You must add fields to be extracted for any custom correlation searches.

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.
<table>
<thead>
<tr>
<th>Type of investigation artifact</th>
<th>Fields extracted for investigation scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>dest, src, dvc, orig_host</td>
</tr>
<tr>
<td>Identity</td>
<td>user, src_user</td>
</tr>
</tbody>
</table>

If your correlation search does not use data models, or the search results contain different fields that you want to extract, you can specify the fields to extract into the investigation scope.

1. Select **Configure > Content > Content Management**.
2. Click the correlation search that you want to customize to open it for editing.
3. Select the notable event adaptive response action.
4. For **Asset Extraction**, type a field name from the correlation search results that identifies an asset. Press Enter to add the field name.
5. For **Identity Extraction**, type a field name from the correlation search results that identifies an identity. Press Enter to add the field name.
6. Click **Save**.

## Manage and customize investigation statuses in Splunk Enterprise Security

Starting in version 5.0.0, you can add statuses to investigations. After upgrading to this version, investigations that did not have a status are assigned the **New** status.

To change the status of an investigation, an analyst must have the `transition_reviewstatus-<x>_to_<y>` capability for the statuses that they want to transition between. The `ess_analyst` role and the `ess_admin` role have those capabilities for all statuses by default. Modifying status transitions for investigations modifies these capabilities.

To make changes to statuses as an analyst, you must have the `edit_reviewstatuses` capability. The `ess_admin` role has this capability by default. See Configure users and roles in the *Installation and Upgrade Manual*.

## Create an investigation status

Create a status for analysts to select when performing an investigation.

If you restrict status transitions, update status transitions after creating a status, otherwise analysts will be unable to select the new status. See **Restrict status**
transitions for investigations in this topic.

1. From the Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. (Optional) Select the **Investigation** tab to review existing investigation statuses.
3. Select **Create New Status > Investigation**.
4. Type a **Label** that appears as the name of the status on the investigation. For example, Waiting on Desktop IT.
5. (Optional) Type a **Description** that appears on the **Status Configuration** page to describe the status. For example, Investigation is waiting for desktop IT to perform additional remediation or forensics steps.
6. (Optional) Select the check box for **Default Status** to set this status as the default for newly-created investigations.
7. (Optional) Select the check box for **End Status** to set this status as a possible last status for an investigation.
8. (Optional) Deselect the check box for **Enabled** to create the status without allowing anyone to use it yet.
9. Update the user roles that are able to transition an investigation from this new status, for example Waiting on Desktop IT, to another status, such as Closed. If you do not select any roles that can transition from this status to another one, no one will be able to move the investigation to a different status after transitioning the investigation to this status.
10. Click **Save**.

**Restrict status transitions for investigations**

The status transitions that can be made on an investigation define the path of an investigation. By default, an investigation in any status can be changed to any other status. For example, someone can change the status of an investigation in the **New** status to any other status, such as **Closed**.

You can restrict the statuses that analysts can choose when investigating. Determine which statuses to require, and whether analysts must follow a specific sequence of statuses before completing an investigation. Determine whether any roles can bypass the full sequence of statuses.

This example walks you through setting up restricting status transitions for analysts. Restrict status transitions so that analysts must follow a path from **New**, to **In Progress** or **Pending**, to **Resolved**, then to **Closed**.
Prerequisites

- You must have the `ess_admin` role or your role must be assigned the `Edit Statuses` capability. For more information about user roles and capabilities, see Configure users and roles in the *Installation and Upgrade Manual*.

1. On the Splunk Enterprise Security toolbar, select **Configure > Incident Management > Status Configuration**.
2. Click the **Investigation** tab.
3. Restrict the transitions from the **New** status. Select the **New** status to open the Edit Investigation Status page.
4. In **Status Transitions**, select the roles for the **Resolved** status and deselect the check box for the `ess_analyst` role.
5. Select the roles for the **Closed** status and deselect the check box for the `ess_analyst` role.
6. Click **Save** to save the changes to the **New** status.
7. Restrict the transitions on the **In Progress** and **Pending** statuses to prevent the `ess_analyst` role from transitioning to **New** or to **Closed**.
8. Click the **Investigation** tab and select the **In Progress** status.
9. In **Status Transition**, select the roles for the **New** status and deselect the check box for the `ess_analyst` role. Repeat for the **Closed** status.
10. Click **Save** to save the changes to the **In Progress** status. Repeat those steps for the **Pending** status.
11. Restrict the **Resolved** status. Click the **Investigation** tab and select the **Resolved** status.
12. In **Status Transition**, select the roles for the **New** status and deselect the check box for the `ess_analyst` role. Repeat for the **In Progress** and **Pending** statuses.
13. Click **Save** to save the changes to the **Resolved** status.
14. Restrict the transitions for the **Closed** status. Click the **Investigations** tab and select the **Closed** status.
15. In **Status Transition**, select the roles for the **New** status and deselect the check box for the `ess_analyst` role. Repeat for the **In Progress**, **Pending**, and **Resolved** statuses.
16. Click **Save** to save the changes for the **Closed** status.
Correlation Searches

Correlation search overview for Splunk Enterprise Security

A correlation search scans multiple data sources for defined patterns. When the search finds a pattern, it performs an adaptive response action.

Correlation searches can search many types of data sources, including events from any security domain (access, identity, endpoint, network), asset lists, identity lists, threat intelligence, and other data in Splunk platform. The searches then aggregate the results of an initial search with functions in SPL, and take action in response to events that match the search conditions with an adaptive response action.

- To create a correlation search, see Create a correlation search in Splunk Enterprise Security Tutorials.
- To set up or modify correlation searches in your environment, see Configuring correlation searches.

Examples of correlation searches

- Identify an access attempt from an expired account by correlating a list of identities and an attempt to authenticate into a host or device.
- Identify a high number of hosts with a specific malware infection, or a single host with a high number of malware infections by correlating an asset list with events from an endpoint protection system.
- Identify a pattern of high numbers of authentication failures on a single host, followed by a successful authentication by correlating a list of identities and attempts to authenticate into a host or device. Then, apply a threshold in the search to count the number of authentication attempts.

Create correlation searches in Splunk Enterprise Security

You can create your own correlation searches to create notable events, modify risk scores, and perform other adaptive response actions automatically based on a correlation in events. There are two ways to create correlation searches in
Splunk Enterprise Security.

- Create a correlation search manually if you are an expert with SPL. You can review the included correlation searches for examples of the search methodology and available options. Test your correlation search ideas on the Search page before implementing them.
- For more assistance with the syntax of correlation searches, use the guided search creation wizard to create a correlation search. The guided search creation wizard allows you to create a correlation search that uses data models or lookups as the data source. The wizard takes your choices about the data source, time range, filtering, aggregate functions, split-by fields, and other conditions and builds the syntax of the search for you. See Create a correlation search in Splunk Enterprise Security Tutorials for a step-by-step tutorial of creating a correlation search.

For details about how to make sure that additional fields appear in the notable event details for a custom correlation search, see Change notable event fields.

See also

- Configure correlation searches in Splunk Enterprise Security
- List correlation searches in Splunk Enterprise Security

Configure correlation searches in Splunk Enterprise Security

Configure correlation searches to enable or disable them, update the settings associated with how they run, change the search logic, and throttle their resulting adaptive response actions. See Correlation search overview for Splunk Enterprise Security to learn more about correlation searches.

Enable correlation searches

Enable correlation searches to start running adaptive response actions and receiving notable events. Splunk Enterprise Security installs with all correlation searches disabled so that you can choose the searches that are most relevant to your security use cases.

1. From the Splunk ES menu bar, select Configure > Content > Content Management.
2. Filter the **Content Management** page by a **Type** of **Correlation Search** to view only correlation searches.

3. Review the names and descriptions of the correlation searches to determine which ones to enable to support your security use cases. For example, if compromised accounts are a concern, consider enabling the **Concurrent Login Attempts Detected** and **Brute Force Access Behavior Detected** correlation searches.

4. In the **Actions** column, click **Enable** to enable the searches that you want to enable.

Only enable correlation searches that you use. For example, don’t enable **Untriaged Notable Events** in an unattended production environment.

After you enable correlation searches, dashboards start to display notable events, risk scores, and other data.

**Change correlation search scheduling**

Change the default search type of a correlation search from real-time to scheduled. Splunk Enterprise Security uses indexed real-time searches by default.

1. From the **Content Management** page, locate the correlation search you want to change.
2. In the **Actions** column, click **Change to scheduled**.

After changing a search to be scheduled, you can modify the schedule settings of the search.

1. From the **Content Management** page, click the name of the correlation search you want to change.
2. (Optional) Modify the search schedule.
   Correlation searches can run with a real-time or continuous schedule. Use a real-time schedule to prioritize current data and performance. Searches with a real-time schedule are skipped if the search cannot be run at the scheduled time. Searches with a real-time schedule do not backfill gaps in data that occur if the search is skipped. Use a continuous schedule to prioritize data completion, as searches with a continuous schedule are never skipped.
3. (Optional) Modify the cron schedule to control how frequently the search runs.
4. (Optional) Specify a schedule window for the search. Type **0** to not use a schedule window, type **auto** to use the automatic schedule window set by
the scheduler, or type a number that corresponds with the number of minutes that you want the schedule window to last. When there are many scheduled reports set to run at the same time, specify a schedule window to allow the search scheduler to delay running this search in favor of higher-priority searches.

5. (Optional) Specify a schedule priority for the search. Change the default to Higher or Highest depending on how important it is that this search runs, and that it runs at a specific time. The schedule priority setting overrides the schedule window setting, so you do not need to set both.

If you manually convert a real-time search to a scheduled search, this does not automatically adjust the earliest or latest dispatch times. The time range default remains the same as the original real-time search, such as \(-5m@m \sim +5m@m\) which does discard events based on the extracted time being slightly in the future versus in the past. You will also need to evaluate the syntax of the converted search. This is because | datamodel is in use for real-time searches. However, if you are moving to a scheduled search, you can use | tstats for efficiency. If you use guided mode to convert the search, it can automatically switch the syntax from | datamodel to | tstats for you.

For information on search schedule priority, see the Splunk platform documentation.

- For tstats syntax, see Tstats in the Splunk Enterprise Search Reference.
- For Splunk Enterprise, see Prioritize concurrently scheduled reports in Splunk Web in the Splunk Enterprise Reporting Manual.
- For Splunk Cloud, see Prioritize concurrently scheduled reports in Splunk Web in the Splunk Cloud Reporting Manual.

**Edit a correlation search**

You can make changes to correlation searches to fit your environment. For example, modify the thresholds used in the search, change the response actions that result from a successful correlation, or change how often the search runs. Modifying a correlation search does not affect existing notable events.

1. From the Content Management page, locate the correlation search you want to edit.
2. Click the name of a correlation search on the Content Management page to edit it.
3. Modify the parameters of the search, then click Save.
If you modify the start time and end time for the correlation search, use relative time modifiers. See Specify time modifiers in your search in the Splunk Enterprise Search Manual.

**Edit the correlation search in guided mode**

You can edit some correlation searches in guided mode. Not all correlation searches support guided search editing. If a search appears grayed-out and has the option to **Edit search in guided mode**, the search was built in guided mode and can be edited in guided mode. If a search can be edited in the search box, you cannot edit it in guided mode. Attempting to switch to guided mode overwrites your existing search with a new search.

1. Click **Edit search in guided mode** to open the guided search creation wizard.
2. Review the search elements in the correlation search, making changes if you want.
3. Save the search.

**Throttle the number of response actions generated by a correlation search**

Set up throttling to limit the number of response actions generated by a correlation search. When a correlation search matches an event, it triggers a response action.

By default, every result returned by the correlation search generates a response action. Typically, you may only want one alert of a certain type. You can use throttling to prevent a correlation search from creating more than one alert within a set period. To change the types of results that generate a response action, define trigger conditions. Some response actions allow you to specify a maximum number of results in addition to throttling. See Set up adaptive response actions in Splunk Enterprise Security.

1. Select **Configure > Content > Content Management**.
2. Click the title of the correlation search you want to edit.
3. Type a **Window duration**. During this window, any additional event that matches any of the **Fields to group by** will not create a new alert. After the window ends, the next matching event will create a new alert and apply the throttle conditions again.
4. Type the **Fields to group by** to specify which fields to use when matching similar events. If a field listed here matches a generated alert, the correlation search will not create a new alert. You can define multiple
fields. Available fields depend on the search fields that the correlation search returns.
5. Save the correlation search.

Throttling applies to any type of correlation search response action and occurs before notable event suppression. See Create and manage notable event suppressions for more on notable event suppression.

**Define trigger conditions for adaptive response actions generated by a correlation search**

You can modify the conditions that control when an adaptive response action is generated by a correlation search. Throttling is different from defining trigger conditions and happens after search results meet the trigger conditions. When you define trigger conditions, the correlation search results are evaluated to check if they match the conditions. If the search results match the conditions, throttling rules control whether an adaptive response action is generated.

You can set up trigger conditions to generate response actions per-result, based on the number of results returned by the correlation search, based on the number of hosts, number of sources, or based on custom criteria. For custom criteria, type a custom search string to create a condition. Trigger conditions act as a secondary search against the results of the correlation search.

For information on trigger conditions and configuring those conditions for a search, see the Splunk platform documentation.

- For Splunk Enterprise, see Configure alert trigger conditions in the Splunk Enterprise Alerting Manual.
- For Splunk Cloud, see Configure alert trigger conditions in the Splunk Cloud Alerting Manual.

**See also**

- List correlation searches in Splunk Enterprise Security
- Set up adaptive response actions in Splunk Enterprise Security

**List correlation searches in Splunk Enterprise Security**
To obtain a list of correlation searches enabled in Splunk Enterprise Security, use a REST search to extract the information that you want in a table.

For example, create a table with the app, security domain, name, and description of all correlation searches in your environment.

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

As another example, create a table with only the enabled correlation searches and the adaptive response actions associated with those searches in your environment. To see the adaptive response actions for all correlation searches, remove | where disabled=0.

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

**Upgrade correlation searches in Splunk Enterprise Security**

Starting in Splunk Enterprise Security version 4.6.0, correlationsearches.conf is no longer used to define correlation searches. Instead, savedsearches.conf uniquely identifies correlation searches using the action.correlationsearch.enabled=1 parameter. The correlationsearches.conf file is deprecated.

**Changes Splunk Enterprise Security makes at upgrade**

When you upgrade to Splunk Enterprise Security 4.6.0, Splunk Enterprise Security migrates all correlation searches in your environment from correlationsearches.conf to savedsearches.conf using the confcheck_es_correlationmigration.py script. The migration can take up to five minutes to complete after the upgrade. In a search head cluster, the captain performs the migration.
During the upgrade, Splunk Enterprise Security continues to create notable events without interruption. This change does not prevent or delay notable events from appearing on Incident Review because the Threat - Correlation Searches - Lookup Gen saved search continues to use the contents of both correlationsearches.conf and savedsearches.conf to populate the correlationsearches KV Store collection used by Incident Review.

**Changes you have to make after upgrade**

After upgrading to Splunk Enterprise Security 4.6.0 or later, you have to make additional changes.

- Check correlationsearches.conf for search definitions that would indicate that a search did not migrate successfully. Migrated searches only exist in savedsearches.conf. If a search did not get migrated, migrate the correlationsearches.conf entries manually to savedsearches.conf using the parameter definitions below.
- Update searches that call the correlationsearches REST endpoint.
  - For example, a search that displays a list of correlation searches in your environment would change from
    
    ```bash
    | rest splunk_server=local
    /services/alerts/correlationsearches | rename eai:acl.app as app, title as csearch_name | table app security_domain csearch_name description
    ```

    to

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

  ♦ See List correlation searches in Splunk Enterprise Security for more examples of updated searches.

Custom search macros that reference the correlationsearches KV Store collection continue to work as before, but consider updating them anyway.

**correlationsearches.conf parameter translation to savedsearches.conf**

All correlationsearches.conf parameters now exist in savedsearches.conf and the correlationsearches.conf file has been deprecated. Do not update it directly
except to manually migrate correlation search definitions.

**Identification parameters for correlation searches**

New parameters identify whether a saved search is a correlation search and the name of the correlation search.

<table>
<thead>
<tr>
<th>correlationsearches.conf parameter in pre-4.6.0 versions</th>
<th>savedsearches.conf parameter starting in 4.6.0</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>action.correlationsearch=0</td>
<td>This is an internal parameter and can be ignored.</td>
</tr>
<tr>
<td>A stanza for the search exists</td>
<td>action.correlationsearch.enabled=1</td>
<td>This parameter identifies a saved search as a correlation search.</td>
</tr>
<tr>
<td>rule_name</td>
<td>action.correlationsearch.label</td>
<td>This parameter provides the name of the correlation search.</td>
</tr>
<tr>
<td>description</td>
<td>description</td>
<td>This parameter provides the description of the correlation search.</td>
</tr>
</tbody>
</table>
Notable event parameters for correlation searches

The `action.notable` parameter identifies a notable event associated with a correlation search. The parameters that describe additional details associated with the notable event now exist in the `savedsearches.conf` file.

<table>
<thead>
<tr>
<th>correlationsearches.conf parameter in pre-4.6.0 versions</th>
<th>savedsearches.conf parameter starting in 4.6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>security_domain</td>
<td>action.notable.param.security_domain</td>
</tr>
<tr>
<td>severity</td>
<td>action.notable.param.severity</td>
</tr>
<tr>
<td>rule_title</td>
<td>action.notable.param.rule_title</td>
</tr>
<tr>
<td>rule_description</td>
<td>action.notable.param.rule_description</td>
</tr>
<tr>
<td>nes_fields</td>
<td>action.notable.param.nes_fields</td>
</tr>
<tr>
<td>drilldown_name</td>
<td>action.notable.param.drilldown_name</td>
</tr>
<tr>
<td>drilldown_search</td>
<td>action.notable.param.drilldown_search</td>
</tr>
<tr>
<td>default_status</td>
<td>action.notable.param.default_status</td>
</tr>
<tr>
<td>default_owner</td>
<td>action.notable.param.default_owner</td>
</tr>
</tbody>
</table>

Related search parameters for correlation searches

Searches related to a correlation search, such as the context-generating searches associated with a correlation search that uses extreme search, are now part of a JSON blob `action.correlationsearch.related_searches` parameter.

<table>
<thead>
<tr>
<th>correlationsearches.conf parameter in pre-4.6.0 versions</th>
<th>savedsearches.conf parameter starting in 4.6.0</th>
</tr>
</thead>
</table>
| related_search_name = Endpoint - Emails By Source - Context Gen | action.correlationsearch.related_searches = [
| related_search_name.0 = Endpoint - Emails By Destination Count - Context Gen |

Example correlation search stanzas from this version and previous versions

The `savedsearches.conf` stanza for a correlation search looks as follows starting in 4.6.0.
In previous versions of Splunk Enterprise Security, the `savedsearches.conf` and `correlationsearches.conf` definitions for the same correlation search would look as follows. `savedsearches.conf`
Create sequence templates in Splunk Enterprise Security
The Event Sequencing Engine provides capabilities for threat detection that allow you to group correlation searches into batches of events, either in a specific sequence, by specific attributes, or both.

You create batches of events by defining a workflow to run correlation searches in an order of your choice, specifying what notable events would need to occur in order to advance to the next step.

The concept is similar to writing a script to automate the things that you might otherwise have to do manually when tracking a variety of notable events and variables through a variety of correlation searches. The concept is also similar to that of meta notable events or named multi-vector notables, which are alerts that are generated by correlation searches monitoring for multiple specific conditions prior to raising the alert.

**How sequence templates work**

The Event Sequencing Engine runs as a real-time search and listens for incoming notable events and risk modifiers that are triggered by correlation searches. Security analysts can provide specifications on how sequenced events are constructed by using sequence templates. Once you have created a sequence template, it is available for execution within 5 minutes.

Sequence templates are stored in the `sequence_templates.conf` file.

The Event Sequencing Engine periodically stores information regarding the currently running sequence templates. This information can be viewed from the sequence lister page. See the status of a template.

**Sequence template details**

A sequence template defines the various constraints of constructing a sequence. It has three main components: start, transitions, and end. You can construct a sequence template using the editor.

The following diagram shows an example of the way that you can start with one correlation search (1), flow through any number of correlation searches in the transitions (2 through 5), and end with a final search (6).
Start

The start section defines match conditions for starting the execution of a template. Optionally, the start section can define state variables to store field values for the purpose of matching further notables or risk modifiers. State variables can also be used as outputs in the final sequenced event. Once the start condition is met, the event sequencing engine will start the execution of the corresponding sequence template.

Match conditions

The match condition defines the criteria for considering notable events or risk modifiers for transitioning through the phases in a template. The match condition has two parts that are evaluated successively, correlation search and expression.

<table>
<thead>
<tr>
<th>Match Conditions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correlation Search</td>
<td>The correlation search to match the source of the incoming notable or risk modifier. Wildcard matching (*) is supported on this field.</td>
</tr>
</tbody>
</table>
| Expression | The expression allows you to compare any field from an incoming event with a static value or a state variable (see state for further information). Expressions follow Splunk style syntax in the format of `<field> <comparator> <value>`. Note that while similar to SPL syntax, expressions in the event sequencing engine are more restricted than in standard SPL syntax. For example, SPL doesn't enforce AND/OR operators for field searches, but the event sequencing engine does. Wildcard matching (*) and regular expressions are not supported in the expression section. You can also use brackets for grouping. You must use the logical operators of AND or OR in your grouping, such as: `'host' = "127.0.0.1" AND ('dest' = "example.com" OR
The expression is made up of field, comparison function, and value.

**Field**
The name of any SPL field in single quotes, such as: 'host', 'source', 'sourcetype', etc. Multivalue fields are supported, and an event is considered a match as long as one value matches.

**Comparison function**
The comparison function can be any of the following: =, !=, >, <, >=, <=. The following comparison functions force numeric comparisons: >=, <=, >, <.

**Value**
The field value in double quotes, which can be in string format or in state_variable notation, such as: 'host' = "127.0.0.1" or 'host' = "$host$".

Based on an example event in .csv format such as the following:

<table>
<thead>
<tr>
<th>host, source, sourcetype</th>
<th>&quot;127.0.0.1&quot;, &quot;Threat Detected&quot;, &quot;nginx&quot;</th>
</tr>
</thead>
</table>

- An expression for matching on the host is 'host' = "127.0.0.1".
- An expression for matching on any other source is 'source' != "Threat Detected".

If you want to use assets and identities in expressions, configure asset and identity correlation with the **enable for all sourcetypes** option selected. This makes sure that identity and asset information is enriched during search time when receiving contents from the risk or notable index. See Configure asset and identity correlation in Splunk Enterprise Security.
State

The state provides a way to store values from matched events for the lifetime of a sequence. State can be stored at the start section and at each transition if the enforce ordering check box is unchecked. You cannot save a new state at the end step. These values can then be used for matching expressions in consecutive transitions. State can also be an output in the final sequenced event. If a multivalue is the output in the final sequenced event, it will be returned in a comma separated format. Once stored, state variables can be referenced using $variable_name$ syntax. State allows you to store important pieces of information for future matching. The state contains two parts, the field and the label.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>The name of any SPL field that you want to capture for later use. State fields defined in the start section can be used in all transitions. But state fields defined in the transitions section will be available only to expressions in subsequent transitions.</td>
</tr>
<tr>
<td>Label</td>
<td>The label is the variable name for referring to the state field in a later search. The state_variable notation for referring to the label is similar to an SPL token in the way it is used to capture and pass values. The label is available only for use while the template is running. It does not persist when the template terminates or completes. The label cannot contain a dollar sign ($).</td>
</tr>
</tbody>
</table>

Transitions

The transitions section defines the sequence, either chronologically or in an order-independent way. You can define a series of match conditions to find the sequence. Each transition defines a title and a match condition.

Chronological

Transitions are matched chronologically by default. With the enforce order check box checked, the Event Sequencing Engine will check if notable events or risk modifiers match the completed transitions in the order specified. A transition is completed by matching an incoming event with a match condition. Given a sequence of correlation searches in the following order, with the enforce order check box checked for example, the notable events will be matched in order:

Start
  1. Brute Force Access Behavior Detected

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

End

6. Abnormally High Number of Endpoint Changes By User

Transitions can only define state variables if the **enforce order** check box is checked. Enforcing the order provides a way to chronologically build a sequence. A state stored in an earlier transition is available for matching in later ones.

**Not chronological**

You can turn off chronological matching by unchecking the enforce order checkbox. With enforce order unchecked, the Event Sequencing Engine will check if notable events or risk modifiers match any of the incomplete transitions. Once matched, corresponding transitions will be considered complete. The order of events will not be considered. For example, given a sequence of correlation searches with the enforce order check box unchecked, you'll notice that notable events can match in any order:

Start

1. Brute Force Access Behavior Detected

Transitions

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

End

6. Abnormally High Number of Endpoint Changes By User
Wildcard

Transitions also support the same constructs for match conditions as in the start section. Since the correlation search field in the match condition allows wildcard match, it is possible to construct sequences that require forks. Transitions can define more than one next possible notable event or risk modifier. Given a wildcard correlation search sequence, for example:

The sequence can go in the following patterns:

Start

1. Brute Force Access Behavior Detected

Transitions

2. Option A or Option B, using a wildcard for two correlation searches. For example, a search of step_one or step_two by matching either one using the wildcard, such as step*.

4. Suspicious Reg.exe Process

5. Web Uploads to Non-corporate Sites by Users

End

6. Abnormally High Number of Endpoint Changes By User
Aggregate

Transitions can also be configured to aggregate notable events or risk modifiers that may happen after a transition match is found. If the **aggregate matches** check box is checked, the Event Sequencing Engine will add any notable events or risk modifiers that satisfy the match condition for one of the completed transitions. This can be used to add more context to the final sequenced event.

Consider a sequence of correlation searches like the following, where we have one correlation search that fires multiple notable events (Uncommon Processes On Endpoint) during the lifetime of our sequence:

**Start**

1. Brute Force Access Behavior Detected

**Transitions**

2. Uncommon Processes On Endpoint
3. Unusually Long Command Line
2. Uncommon Processes On Endpoint
4. Suspicious Reg.exe Process

**End**

6. Abnormally High Number of Endpoint Changes By User

If aggregate matches is unchecked, then there will only be one match for Uncommon Processes On Endpoint in the final sequenced event, even though it matched multiple times. If **aggregate matches** is checked, the event sequencing engine will try to match all new incoming notables and risk modifiers with completed transitions. In this case, after finding the first Uncommon Processes On Endpoint, the sequencing engine re-evaluates the next two Uncommon Processes On Endpoint notable events with match conditions and adds them to the final sequenced event if true.

**End**

The end section defines the termination criteria for a sequence template. A template can terminate if either of these two conditions are true:

- All transitions are complete and the event satisfying match condition is found. The event sequencing engine will consider this outcome as a
successful run of a template and will trigger the sequenced event creation.
• The template has reached the configured max time to live (max_ttl). As the template has not reached its end state in the desired time, the event sequencing engine will discard this run and no sequenced event will be created.

Sequenced event

After the successful termination of a template, the output is a sequenced event. This sequenced event is the result of a template run and holds the necessary information for identifying a sequence. Sequenced events are written to the sequenced_events index. Sequence templates can be configured to use any of the state variables or statically configured values as output in the final sequenced events. The variables are stored and available for use only during the runtime of a template.

Create a template

You can create a template to run any number of searches that match your criteria.

The sequence template does not require any special capability to view, but requires the edit_sequence_template capability to manage sequence templates. By default, ES assigns the edit_sequence_template capability to the ess_admin role. An admin can assign it to other roles from the Permissions setting.

In the following scenario, you know that you’re interested in detecting a prohibited application spawning the cmd.exe process. Once you’ve detected the process, you’re interested in knowing if it's happening on your favorite computer, particularly if it starts creating new local admin accounts. Finally, you want to know if the user is making an abnormally high number of changes elsewhere. Because each system involved is set for logging at a different time interval, you are not necessarily interested in chronological order.

1. From the Splunk ES menu bar, select Configure > Content > Content Management > Create New Content > Sequence Template.
2. In the Sequence Template section, type a Name for your template, a Description for it, and select an App with which to run the search.
3. In the Start section, add the following:
   1. Select the Correlation Search to begin with, such as Detect Prohibited Applications Spawning cmd.exe.
   2. Type the Expression to match on, such as 'dest' = "198.18.0.101"
3. Type a State to store for use in a later correlation search, such as:
   ◊ Field: user
   ◊ Label: questionable_user
4. In the Transition section, do the following:
   1. Uncheck the Enforce Ordering check box.
   2. Type a Title for this section, such as: new local admin
   3. Select the Correlation Search to run next, such as: ESCU - Detect New Local Admin account - Rule.
   4. Type the Expression to match on, such as the state you saved earlier: 'user' = "$questionable_user$".
5. In the End section, add the following:
   1. Select the Correlation Search to end with, such as Change - Abnormally High Number of Endpoint Changes By User - Rule.
   2. Type the Expression to match on, such as the state you saved earlier: 'user' = "$questionable_user$".
   3. Select the Time Limit when the search should expire, such as 2 days.
6. In the Actions section, add the following:
   1. Type the Event Title that you want to see in the Incident Review, such as Prohibited cmd, new local account, high endpoint changes.
   2. Type the Description that you want to see in the Incident Review, such as The questionable user on my favorite computer is $questionable_user$.
   3. Select the Urgency that you want to see in the Incident Review, such as High.
   4. Select a Security Domain that you want to see in the Incident Review, such as Access.
7. Click Save.

Enable or Disable a template

Manage sequence templates individually by enabling or disabling each one. Enable or disable the template by performing the following steps:

1. From the Splunk ES menu bar, select Configure > Content > Content Management.
2. From the Type filter, select the Sequence Template option.
3. Check the check box for your Sequence Template.
4. Click Edit selection > Enable or Edit selection > Disable.
Enable event sequencing

Manage sequence templates as a whole by enabling or disabling the Event Event Sequencing Engine. The sequence templates will run only if the Event Sequencing Engine is enabled. The Event Sequencing Engine is disabled by default.

Enable the Event Sequencing Engine by performing the following steps:

1. From the Splunk ES menu bar, select Configure > General > General Settings.
2. (Optional) Type Event Sequencing Engine in the filter field.
3. Click Enable to enable the Event Sequencing Engine.

Edit an existing template

The sequence template does not require any special capability to view, but requires edit_sequence_template to manage sequence templates. By default, ES assigns the edit_sequence_template capability to the ess_admin role. An admin can always assign it to other roles from the Permissions setting.

You can edit all templates, whether they’re enabled or disabled.

1. From the Splunk ES menu bar, select Configure > Content > Content Management.
2. From the Type filter, select the Sequence Template option.
3. (Optional) Click Disable to disable an enabled template.
4. Click the name of the search to edit the template parameters.

See the status of a template

You can see which sequences are running or completed.

1. From the Splunk ES menu bar, select Security Intelligence > Sequence Analysis.
2. From the Showing filter, select the Running Templates or Completed Templates.
3. From the event information column, click the greater than (>) symbol to expand the display.

You can see which templates are running and their current status in terms of which events have been matched and how many transitions have been
Find the sequenced events generated by the event sequence template

Once you create a sequence template and it reaches the end state, the output displays as a sequenced event in the Incident Review dashboard. See Incident Review overview for information about using the dashboard.

To find the output from the sequence template search, do the following:

1. From the Splunk ES menu bar, select Incident Review.
2. Click the Sequenced Event filter to show only sequenced events.
3. (Optional) Sort by Title.
4. You will see the Event Title that you typed in the editor as the title of your sequenced event.
5. From the event information column, click the greater than (>) symbol to expand the display.

ES displays information specific to that sequence of events, such as the name and description, the state of each transition in the sequence, and the sequence expiration date. For example when we see Rare Process, then DDNS Activity, then Web Traffic, then a UBA-triggered DGA alert.
Execute the Event Sequencing Engine in an ad-hoc manner

When you create a template, the Event Sequencing Engine starts executing it within 5 minutes. Alternately, you can run the helper macro, `execute_sequence_template`. This macro takes two parameters: the template name and a Boolean expression indicating if a sequenced event is created or not. For example:

```
'execute_sequence_template(template_name, false)'
```

In this case, `false` means that the sequenced event will not be created.

This macro can be run over historical data, so you can find sequenced events in past notable events and risk modifiers. After running the macro, the Event Sequencing Engine returns sequenced events if any are found. You can only execute one template at a time. This macro is intended for explorations and fine tuning to manage sequence templates.

Set up adaptive response actions in Splunk Enterprise Security

Adaptive response actions allow you to gather information or take other action in response to the results of a correlation search or the details of a notable event. Splunk Enterprise Security includes several adaptive response actions. See Included adaptive response actions.

You can add adaptive response actions and alert actions to correlation searches, or run adaptive response actions from notable events on the Incident Review dashboard. Collect information before you start your investigation to save time at triage by adding adaptive response actions to correlation searches. Take action at triage time by running adaptive response actions from the Incident Review dashboard.

The adaptive response actions that ship out of the box for ping, nbtstat, and nslookup are modified to support Splunk Cloud. Additional setup is required before configuring adaptive response actions from Splunk Cloud to on-premises infrastructure and services. See Set up an adaptive response relay from Splunk Cloud to an on-premises device.
Add new adaptive response actions


Audit adaptive response actions

Audit all adaptive response actions on the Adaptive Response Action Center.

Configure permissions for adaptive response actions

Restrict certain adaptive response actions to certain roles by adjusting the permissions for adaptive response actions in the alert actions manager. You can find information about the alert actions manager in the Splunk platform documentation.

- For Splunk Enterprise, see Using the alert actions manager in the Splunk Enterprise Alerting Manual.
- For Splunk Cloud, see Using the alert actions manager in the Splunk Cloud Alerting Manual.

In order to run adaptive response actions from the Incident Review dashboard that have credentials stored in the credential manager, you must have the appropriate capability.

- For Splunk platform version 6.5.0 and later, list_storage_passwords.
- For earlier Splunk platform versions, admin_all_objects.

Add an adaptive response action to a correlation search

1. On the Splunk Enterprise Security menu bar, click Configure > Content > Content Management.
2. Click an existing correlation search, or click Create New > Correlation Search.
3. Click Add New Response Action and select the response action you want to add.
4. Complete the fields for the action. If you want, add another response action.
5. Click Save to save all changes to the correlation search.
For instructions on configuring each of the adaptive response actions included with Splunk Enterprise Security, see Configure adaptive response actions for a correlation search in Splunk Enterprise Security. For instructions on configuring a custom adaptive response action, see the documentation for the app or add-on that supplied the adaptive response action.

**Troubleshoot why an adaptive response action is not available to select**

If an adaptive response action is not available to select on the correlation search editor or Incident Review, several things could be the cause.

- Your role may not have permissions to view and use the adaptive response action. See Using the alert actions manager in the Alerting Manual.
- Check the alert actions manager to determine if the adaptive response actions exist in Splunk platform. See Using the alert actions manager in the Alerting Manual.
- If the adaptive response actions from an add-on do not appear in Splunk Enterprise Security, but do appear in the alert actions manager, make sure that the add-on is being exported globally. See Make Splunk knowledge objects globally available in the Splunk Enterprise Admin Manual.
- If you can select the adaptive response action on the correlation search editor, but not on Incident Review, the adaptive response action might be an ordinary alert action, or the response action does not support ad hoc invocation. See Determine whether your action supports ad hoc invocation on the Splunk developer portal.

**Set up an adaptive response relay from a Splunk Cloud Enterprise Security search head to an on-premises device**

Splunk Cloud customers can utilize adaptive response actions in Splunk Enterprise Security (ES) without exposing infrastructure controls and administration to the open internet. Adaptive response relay allows adaptive response actions to queue on the Splunk Cloud ES search head. These queued actions store metadata and search results that allow a separate proxy component to execute those adaptive response actions from within the on-premises environment.
You need to perform the following steps to set up adaptive response actions:

1. **Install the technical add-on for adaptive response on your heavy forwarder.**
2. **Configure your Splunk Cloud ES search head with an API key.**
3. **Configure your on-premises heavy forwarder with an API key.**
4. **Configure your on-premises heavy forwarder with a modular action relay.**
5. **Configure your Splunk Cloud ES search head with a modular action worker.**
6. **Configure adaptive response actions for your Splunk Cloud ES search head.**

### Install the technical add-on for adaptive response on your heavy forwarder

For an on-premises heavy forwarder to perform adaptive response actions, you must install the actions on both the Splunk Cloud ES search head and the heavy forwarder. These actions are installed by default with ES in $SPLUNK_HOME/etc/apps/SA-ThreatIntelligence, but you need to install them manually on your heavy forwarder.

1. From the Splunk ES menu bar of the Splunk Cloud ES search head, select **Configure > General > Distributed Configuration Management.**
2. Click *Splunk_TA_AROnPrem* to download the app.
3. Install the app on the heavy forwarder.

### Configure your Splunk Cloud ES search head with an API key

The API key allows you to authenticate from the KV Store collection and CAM queue. You must create and manage your own API key. The API key follows a specific format, and it does not support two-factor authentication. For a Splunk Cloud environment that requires two-factor authentication, turn off this feature by not setting an API key.

1. Retrieve the heavy forwarder's `serverName` value by running the following search on the heavy forwarder:

   ```
   | rest /services/server/info | table serverName
   ```

   Take note of this name because you will need it when you set up your heavy forwarder. In this example the `serverName` value is `hf1`.
2. Install the Common Information Model version 4.12 or higher on the Splunk Cloud ES search head, if you haven't done so already.
3. Generate an API key on the Splunk Cloud ES search head.
   1. From the Splunk ES menu bar, select **Configure > CIM Setup**, and then click **Manage API Key**.
   2. In the **Key Name** field, type the `servername` value that you retrieved: in this case, `hf1`.
   3. To generate the API key value, type the following URI into a browser window of your Splunk Cloud ES search head:
      ```
      ```
      This will return a random 128-character string in the valid format.
   4. Copy and paste the string into the **API Key** field.
      Take note of this string because you will use it when you configure your heavy forwarder.

**Configure your on-premises heavy forwarder with an API key**

An API key allows the heavy forwarder to authenticate against the Splunk Cloud ES search head. The API key on the heavy forwarder must match the API key on the Splunk Cloud ES search head.

1. Install the Common Information Model version 4.12 or higher on the heavy forwarder, if you haven't done so already.
2. From the Splunk ES menu bar, select **Configure > CIM Setup**, and then click **Manage API Key**
   1. On the key management page, in the **Key Name** field, type the `servername` value that you took note of in the Configure your Splunk Cloud ES search head with an API key section.
   2. On the key management page, in the **API Key** field, paste the string that you took note of in the Configure your Splunk Cloud ES search head with an API key section.

**Configure your on-premises heavy forwarder with a modular action relay**

The modular action relay is where you set the heavy forwarder to retrieve queued search results from a Splunk Cloud correlation search so that it can execute adaptive response actions on premises.

1. From the Splunk ES menu bar, select **Settings > Data inputs**.
2. Scroll down to Modular Action Relay and click + Add new.
   1. Type a **Name** for the relay, such as `relay1`.
   2. Type the **Remote Search Head URI** in the format of `protocol://servername:port`, such as:
8089 is the default port for Splunk Cloud.

3. Type a **Description** for the relay, such as `remote search head`.
4. Type the **Api Key Name** (the `serverName` value that you took note of in the Configure your Splunk Cloud ES search head with an API key section), such as `hf1`.
5. Type **True** in the **Verify** field to verify the certificates between the worker and the Splunk Cloud ES search head.
6. (Optional) If your ES search head is using a privately signed SSL certificate, add your root CA certificate chain file to the `Splunk_SA_CIM/auth` directory on the heavy forwarder and provide its file name to this input in the **Client Certificate** field. If your search head is in Splunk Cloud, this is not an issue.

### Configure your Splunk Cloud ES search head with a modular action worker

The modular action worker is where you specify the `serverName` value of the heavy forwarder that the Splunk Cloud ES search head will queue search results for.

1. From the Splunk ES menu bar of the Splunk Cloud ES search head, select **Configure > Content > Content Management**.
2. Type **Modular Action Workers** in the search filter.
3. Click the name of the **Modular Action Workers** lookup.
4. Add a worker set and the name of the worker. The `worker_set` value is used when running adaptive response actions from ES. The `cam_worker` is the actual name of the heavy forwarder that will execute the actions.
   1. Leave the row with **local** as-is because it allows for local execution of actions on the Splunk Cloud ES search head.
   2. In the **worker_set** column, type a descriptive name for the heavy forwarder: `onprem`.
   3. In the **cam_workers** column, type the `serverName` value that you took note of in the Configure your Splunk Cloud ES search head with an API key section, such as `"["hf1"]"`. The format requires array-style notation of `"["nameofworker"]"` with each worker name in quotes and separated with commas in CSV encoded JSON. An example of multiple workers is `"["hf1","hf2"]"`. 

60
Configure adaptive response actions for your Splunk Cloud ES search head

See Configure adaptive response actions for a correlation search in Splunk Enterprise Security for information about configuring adaptive response actions in general.

The Worker Set drop-down menu is specific to adaptive response actions on a Splunk Cloud ES search head. After completing the in the Configure your Splunk Cloud ES search head with a modular action worker section, when you create or edit a correlation search to add an adaptive response action, the drop-down menu includes the worker_set that you created.

Select the worker_set to use for executing those adaptive response actions from within the on-premises environment.

Troubleshoot adaptive response relay from Splunk Cloud ES search head to an on-premises device

The adaptive response modular input runs on a default interval of 2 minutes. You can adjust this based on your needs. A more frequent execution time will place additional load on the Splunk Cloud ES search head. To avoid performance problems with the CAM queue, adjust the interval to run less frequently, and do not set it below 10 seconds.

Ensure that your heavy forwarder is configured to forward its data to your indexers. This includes forwarding data from the relayed modular actions. You can run a search similar to the following search on your ES search head to verify that data is forwarding, where hf1 is the name of your heavy forwarder:

   index="cim_modactions" host=hf1

If this search never returns results, then your heavy forwarder is experiencing issues connecting to the ES search head.

Configure adaptive response actions for a correlation search in Splunk Enterprise Security

As a Splunk Enterprise Security admin, you can configure which adaptive response actions that a correlation search triggers.
Analysts can run some adaptive response actions on an ad hoc basis from Incident Review. See Included adaptive response actions with Splunk Enterprise Security in Use Splunk Enterprise Security.

Splunk Enterprise Security includes several adaptive response actions, and you can obtain additional ones from add-ons available on Splunkbase.

Included adaptive response actions

Splunk Enterprise Security includes several adaptive response actions.

- Create a notable event.
- Modify a risk score with a risk modifier.
- Send an email.
- Run a script.
- Start a stream capture with Splunk Stream.
- Ping a host.
- Run Nbtstat.
- Run Nslookup.
- Add threat intelligence.
- Create a Splunk Web message.

Create a notable event

Create a notable event when the conditions of a correlation search are met.

1. On the Splunk Enterprise Security menu bar, click Configure > Content > Content Management.
2. Click an existing correlation search, or click Create New > Correlation Search.
3. Click Add New Response Action and select Notable to add a notable event.
4. Type a Title of the notable event on the Incident Review dashboard. Supports variable substitution from the fields in the matching event.
5. Type a Description of the notable event. Supports variable substitution from the fields in the matching event.
6. Select the Security Domain of the notable event from the drop-down list.
7. Select the Severity of the notable event from the drop-down list. The severity is used to calculate the Urgency of a notable event.
8. (Optional) Change the default owner of the notable event from the system default, unassigned.
9. (Optional) Change the default status of the notable event from the system default, New.
10. Type a drill-down name for the Contributing Events link in the notable event.
11. Type a drill-down search for the Contributing Events link in the notable event.
12. In the Drill-down earliest offset field, type the amount of time before the time of the triggering event to look for related events for the Contributing Events link in the notable event.
   For example, 2h to look for contributing events 2 hours before the triggering event.
13. In the Drill-down latest offset field, type the amount of time after the time of the triggering event to look for related events for the Contributing Events link in the notable event.
   For example, 1h to look for contributing events 1 hour after the triggering event.
14. (Optional) Add Investigation Profiles that apply to the notable event.
   For example, add an investigation profile that fits a use case of "Malware" to malware-related notable events.
15. (Optional) Add fields that contain assets in Asset Extraction to extract the field values and add them to the investigation workbench as artifacts when the notable event is added to an investigation.
16. (Optional) Add fields that contain identities in Identity Extraction to extract the field values and add them to the investigation workbench as an artifact when the notable event is added to an investigation.
17. Type Next Steps for an analyst to take after triaging a notable event. Type text or click Insert Adaptive Response Action to reference a response action in the text of the next steps. You can only type plain text and links to response actions in the next steps field. Use next steps if you want to recommend response actions that should be taken in a specific order.
   For example, ping a host to determine if it is active on the network. If the host is active, increase the risk score by 100, otherwise, increase the risk score by 50.
18. Select Recommended Actions to complement the next steps. From the list of all adaptive response actions, click the name of an action that you recommend as a triage or investigation step for this notable event to add it to the list of recommended actions that analysts can take for this notable event. You can add as many recommended actions as you like. Use recommended actions to recommend response actions that do not need to be taken in a specific order.
   For example, increase the risk score on a host and perform an nslookup on a domain name.
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. Type a field in the search to apply the risk score to for the Risk Object Field.
   For example, type "src" to specify the source field.
4. Select the Risk Object Type to apply the risk score to.

See Assign risk to an object in Use Splunk Enterprise Security for other ways to modify risk scores.

Send an email

Send an email as a result of a correlation search match.

Prerequisite

Make sure that the mail server is configured in the Splunk platform before setting up this response action.

- For Splunk Enterprise, see Configure email notification settings in the Splunk Enterprise Alerting Manual.
- For Splunk Cloud, see Configure email notification settings in the Splunk Cloud Alerting Manual.

Steps

1. Click Add New Response Action and select Send email.
2. In the To field, type a comma-separated list of email addresses to send the email to.
3. (Optional) Change the priority of the email. Defaults to Lowest.
4. Type a subject for the email. The email subject defaults to "Splunk Alert: $name$", where $name$ is the correlation search Search Name.
5. Type a message to include as the body of the email. Defaults to "The scheduled report '$name$' has run."
6. Select the check boxes of the information you want the email message to include.
7. Select whether to send a plain-text or HTML and plain-text email message.

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, see Configure scripted alerts in the Splunk Cloud 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.


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. Type the event 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.

1. Click Add New Response Action and select Nbtstat.
2. Type the event 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.

1. Click Add New Response Action and select Nslookup.
2. Type the event 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 insert the threat artifact into.
4. Type the Search Field that contains the value to insert into the threat artifact.
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.
Assets and Identities

Add asset and identity data to Splunk Enterprise Security

Splunk Enterprise Security uses an asset and identity system to correlate asset and identity information with events to enrich and provide context to your data. This system takes information from external data sources to populate lookups, which Enterprise Security correlates with events at search time.

Add asset and identity data to Splunk Enterprise Security to take advantage of asset and identity correlation.

3. Format the asset or identity list as a lookup in Splunk Enterprise Security.
5. Verify that your asset or identity data was added to Splunk Enterprise Security.

See also

How Splunk Enterprise Security correlates, processes, and merges asset and identity data

Lookups that store merged asset and identity data

Collect and extract asset and identity data inSplunk Enterprise Security

Collect and extract your asset and identity data in order to add it to Splunk Enterprise Security. In a Splunk Cloud deployment, work with Splunk Professional Services to design and implement an asset and identity collection solution. For examples of adding asset and identity data, see Example methods of adding asset and identity data to Splunk Enterprise Security.
1. Determine where the asset and identity data in your environment is stored.
2. Collect and update your asset and identity data automatically to reduce the overhead and maintenance that manual updating requires and improve data integrity.

   - Use Splunk DB Connect or another Splunk platform add-on to connect to an external database or repository.
   - Use scripted inputs to import and format the lists.
   - Use events indexed in the Splunk platform with a search to collect, sort, and export the data to a list.

Suggested collection methods for assets and identities.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Asset or Identity data</th>
<th>Collection methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Both</td>
<td>SA-Idapsearch and a custom search. See <a href="#">Example methods of adding asset and identity data</a>.</td>
</tr>
<tr>
<td></td>
<td>Both</td>
<td>SecKit Windows Add On for ES Asset and Identities</td>
</tr>
<tr>
<td>LDAP</td>
<td>Both</td>
<td>SA-Idapsearch and a custom search.</td>
</tr>
<tr>
<td>CMDB</td>
<td>Asset</td>
<td>DB Connect for integrating with 3rd Party structured data sources, and a custom search.</td>
</tr>
<tr>
<td>ServiceNow</td>
<td>Both</td>
<td>Splunk Add-on for ServiceNow</td>
</tr>
<tr>
<td>Asset Discovery</td>
<td>Asset</td>
<td>Splunk for Asset Discovery</td>
</tr>
<tr>
<td>Bit9</td>
<td>Asset</td>
<td>Splunk Add-on for Bit9 and a custom search.</td>
</tr>
<tr>
<td>Cisco ISE</td>
<td>Both</td>
<td>Splunk Add-on for Cisco ISE and a custom search.</td>
</tr>
<tr>
<td>Microsoft SCOM</td>
<td>Asset</td>
<td>Splunk Add-on for Microsoft SCOM and a custom search.</td>
</tr>
<tr>
<td>Okta</td>
<td>Identity</td>
<td>Splunk Add-on for Okta and a custom search.</td>
</tr>
<tr>
<td>Sophos</td>
<td>Asset</td>
<td>Splunk Add-on for Sophos and a custom search.</td>
</tr>
<tr>
<td>Symantec Endpoint Protection</td>
<td>Asset</td>
<td>Splunk Add-on for Symantec Endpoint Protection and a custom search.</td>
</tr>
<tr>
<td>Technology</td>
<td>Asset or Identity data</td>
<td>Collection methods</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Splunk platform</td>
<td>Asset</td>
<td>Add asset data from indexed events in Splunk platform.</td>
</tr>
<tr>
<td>Amazon Web Services (AWS)</td>
<td>Asset</td>
<td>SecKit AWS Add On for ES Asset and Identities</td>
</tr>
<tr>
<td>Configuration Management Database (CMDB)</td>
<td>Asset</td>
<td>SecKit SA Common tools for populating assets and identities in Enterprise Security and PCI apps</td>
</tr>
</tbody>
</table>

Next step

(Optional) Define identity formats in Splunk Enterprise Security

Format an asset or identity list as a lookup in Splunk Enterprise Security

Define identity formats in Splunk Enterprise Security


Prerequisite

Collect and extract asset and identity data in Splunk Enterprise Security

Steps

1. From the Splunk ES menu bar, select **Configure > Data Enrichment > Identity Lookup Configuration.**
2. (Optional) Deselect the check box for **Email** if email addresses do not identify users in your environment.
3. (Optional) Deselect the check box for **Email short** if the username of an email address does not identify users in your environment.
4. (Optional) Select the check box for **Convention** if you want to define custom conventions to use to identify users.
   1. Click **Add a new convention** to add a custom convention.
   2. You can identify users by the first few letters of their first name and the first few letters of their last name, based on the columns in the
Identities Table. Use the convention of 
\text{identity\_first}(n)\text{middle}(n)\text{last}(n) where \text{identity}, \text{first}, and \text{last} are any columns from the Identities Table, and where \text{n} is a number starting with 0. For example:

\begin{itemize}
  \item "Jane Marie Johnson" using the convention \text{first}(3)\text{last}(3)
    is janjoh
  \item "John Michael Smith" using the convention 
    \text{first}(1)\text{middle}(1)\text{last}() is jm.smith
  \item "John Doe" using the convention \text{ADMIN\_first}(1)\text{last}() is 
    ADMIN_jdoe
  \item Multiple matches are resolved automatically by taking the first match in the table or manually by specifying \text{identity} values.
\end{itemize}

5. (Optional) Select the check box for \textbf{Case Sensitive} to require case sensitive identity matching. Case sensitive identity matching produces fewer matches.

6. Click \textbf{Save}.

\textbf{Next step}

\textbf{Format the asset or identity list as a lookup in Splunk Enterprise Security}

\textbf{Format an asset or identity list as a lookup in Splunk Enterprise Security}

Format your collected asset or identity data into a lookup file so that it can be processed by Splunk Enterprise Security.

\textbf{Prerequisites}

- Collect and extract asset and identity data for Splunk Enterprise Security
- (Optional) Define identity formats in Splunk Enterprise Security

\textbf{Steps}

1. Create a plain text, CSV-formatted file with Unix line endings and a .csv file extension.
2. Use the correct headers for the CSV file. See \texttt{Asset lookup header} or \texttt{Identity lookup header} for the headers expected by Splunk Enterprise Security.
3. Populate the rows of the CSV with the asset or identity fields. See Asset lookup fields or Identity lookup fields for reference.

For an example asset list, review the Demonstration Assets lookup.

- Locate the list in Splunk Web by navigating to Configure > Content > Content Management.
- Locate the list in the file system, the demo_assets.csv file is located in the SA-IdentityManagement/lookups/ directory.

If you use a custom search to generate a lookup, make sure that the lookup produced by the search results contains fields that match the headers.

Next step

Configure the new asset or identity list in Splunk Enterprise Security

Asset lookup header

ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should_timesync,should_update,requires_av

Asset lookup fields

Populate the following fields in an asset lookup.

To add multi-homed hosts or devices to the asset list, add each IP address to the ip field for the host, pipe-delimited. Multi-homed support is limited, and having multiple hosts with the same IP address on different network segments can cause conflicts in the merge process.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
<th>Example values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>pipe-delimited numbers</td>
<td>A pipe-delimited list of single IP address or IP ranges. An asset is required to have an entry in the ip, mac, nt_host, or dns fields. Do not use pipe-delimiting for more than</td>
<td>2.0.0.0/8</td>
</tr>
<tr>
<td>Field</td>
<td>Data type</td>
<td>Description</td>
<td>Example values</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mac</td>
<td>pipe-delimited</td>
<td>A pipe-delimited list of MAC address. An asset is required to have an entry in the <code>ip</code>, <code>mac</code>, <code>nt_host</code>, or <code>dns</code> fields. Do not use pipe-delimiting for more than one of these fields per asset.</td>
<td>00:25:bc:42:f4:60</td>
</tr>
<tr>
<td>nt_host</td>
<td>pipe-delimited</td>
<td>A pipe-delimited list of Windows machine names. An asset is required to have an entry in the <code>ip</code>, <code>mac</code>, <code>nt_host</code>, or <code>dns</code> fields. Do not use pipe-delimiting for more than one of these fields per asset.</td>
<td>ACME-0005</td>
</tr>
<tr>
<td>dns</td>
<td>pipe-delimited</td>
<td>A pipe-delimited list of DNS names. An asset is required to have an entry in the <code>ip</code>, <code>mac</code>, <code>nt_host</code>, or <code>dns</code> fields. Do not use pipe-delimiting for more than one of these fields per asset.</td>
<td>acme-0005.corp1.acmetech.org</td>
</tr>
<tr>
<td>owner</td>
<td>string</td>
<td></td>
<td><a href="mailto:f.prefect@acmetech.org">f.prefect@acmetech.org</a>, DevOps, Bill</td>
</tr>
<tr>
<td>Field</td>
<td>Data type</td>
<td>Description</td>
<td>Example values</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>priority</td>
<td>string</td>
<td><strong>Recommended.</strong> The priority assigned to the device for calculating the Urgency field for notable events on Incident Review. An &quot;unknown&quot; priority reduces the assigned Urgency by default. For more information, see How urgency is assigned to notable events in Splunk Enterprise Security.</td>
<td>unknown, low, medium, high or critical.</td>
</tr>
<tr>
<td>lat</td>
<td>string</td>
<td>The latitude of the asset</td>
<td>41.040855</td>
</tr>
<tr>
<td>long</td>
<td>string</td>
<td>The longitude of the asset</td>
<td>28.986183</td>
</tr>
<tr>
<td>city</td>
<td>string</td>
<td>The city in which the asset is located</td>
<td>Chicago</td>
</tr>
<tr>
<td>country</td>
<td>string</td>
<td>The country in which the asset is located</td>
<td>USA</td>
</tr>
<tr>
<td>bunit</td>
<td>string</td>
<td><strong>Recommended.</strong> The business unit of the asset. Used for filtering</td>
<td>EMEA, NorCal</td>
</tr>
<tr>
<td>Field</td>
<td>Data type</td>
<td>Description</td>
<td>Example values</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>category</td>
<td>pipe-delimited strings</td>
<td><strong>Recommended.</strong> A pipe-delimited list of logical classifications for assets. Used for asset and identity correlation and categorization. See <a href="#">Asset/Identity Categories.</a></td>
<td>server</td>
</tr>
<tr>
<td>pci_domain</td>
<td>pipe-delimited strings</td>
<td>A pipe-delimited list of PCI domains. See Configure assets in the Splunk App for PCI Compliance <a href="#">Installation and Configuration Manual.</a></td>
<td>cardholder, trust</td>
</tr>
<tr>
<td>is_expected</td>
<td>boolean</td>
<td>Indicates whether events from this asset should always be expected. If set to true, the Expected Host Not Reporting correlation search performs an adaptive response action when this asset stops reporting events.</td>
<td>&quot;true&quot;, or blank to indicate &quot;false&quot;</td>
</tr>
<tr>
<td>Field</td>
<td>Data type</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>should_timesync</td>
<td>boolean</td>
<td>Indicates whether this asset must be monitored for time-sync events. It set to true, the Should Timesync Host Not Syncing correlation search performs an adaptive response action if this asset does not report any time-sync events from the past 24 hours.</td>
<td>&quot;true&quot;, or blank to indicate &quot;false&quot;</td>
</tr>
<tr>
<td>should_update</td>
<td>boolean</td>
<td>Indicates whether this asset must be monitored for system update events.</td>
<td>&quot;true&quot;, or blank to indicate &quot;false&quot;</td>
</tr>
<tr>
<td>requires_av</td>
<td>boolean</td>
<td>Indicates whether this asset must have anti-virus software installed.</td>
<td>&quot;true&quot;, or blank to indicate &quot;false&quot;</td>
</tr>
</tbody>
</table>

**Identity lookup header**

identity,prefix,nick,first,last,suffix,email,phone,phone2,managedBy,priority,bunit,category,watchlist,startDate,endDate,work_city,work_country,work_lat,work_long

**Identity lookup fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity</td>
<td>pipe-delimited strings</td>
<td>Required. A pipe-delimited list of username</td>
<td>a.vanhelsing</td>
</tr>
<tr>
<td>Field</td>
<td>Data type</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>prefix</td>
<td>string</td>
<td>Prefix of the identity.</td>
<td>Ms., Mr.</td>
</tr>
<tr>
<td>nick</td>
<td>string</td>
<td>Nickname of an identity.</td>
<td>Van Helsing</td>
</tr>
<tr>
<td>first</td>
<td>string</td>
<td>First name of an identity.</td>
<td>Abraham</td>
</tr>
<tr>
<td>last</td>
<td>string</td>
<td>Last name of an identity.</td>
<td>Van Helsing</td>
</tr>
<tr>
<td>suffix</td>
<td>string</td>
<td>Suffix of the identity.</td>
<td>M.D., Ph.D</td>
</tr>
<tr>
<td>email</td>
<td>string</td>
<td>Email address of an identity.</td>
<td><a href="mailto:a.vanhelsing@acmetech.org">a.vanhelsing@acmetech.org</a></td>
</tr>
<tr>
<td>phone</td>
<td>string</td>
<td>A telephone number of an identity.</td>
<td>123-456-7890</td>
</tr>
<tr>
<td>phone2</td>
<td>string</td>
<td>A secondary telephone number of an identity.</td>
<td>012-345-6789</td>
</tr>
<tr>
<td>managedBy</td>
<td>string</td>
<td>A username representing the manager of an identity.</td>
<td><a href="mailto:phb@acmetech.org">phb@acmetech.org</a></td>
</tr>
<tr>
<td>priority</td>
<td>string</td>
<td><strong>Recommended.</strong> The priority assigned to the</td>
<td>unknown, low, medium, high or critical.</td>
</tr>
</tbody>
</table>

Strings representing the identity. After the merge process completes, this field includes generated values based on the identity lookup configuration settings.
<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>identity for calculating the <strong>Urgency</strong> field for notable events on Incident Review. An &quot;unknown&quot; priority reduces the assigned <strong>Urgency</strong> by default. For more information, see How urgency is assigned to notable events in Splunk Enterprise Security.</td>
<td></td>
</tr>
<tr>
<td>bunit</td>
<td>string</td>
<td><strong>Recommended.</strong> A group or department classification for identities. Used for filtering by dashboards in Splunk Enterprise Security.</td>
<td>Field Reps, ITS, Products, HR</td>
</tr>
<tr>
<td>category</td>
<td>pipe-delimited strings</td>
<td><strong>Recommended.</strong> A pipe-delimited list of logical classifications for identities. Used for asset and identity correlation and categorization. See Asset/Identity Categories.</td>
<td>Privileged</td>
</tr>
<tr>
<td>Field</td>
<td>Data type</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>watchlist</td>
<td>boolean</td>
<td>Marks the identity for activity monitoring.</td>
<td>Accepted values: &quot;true&quot; or empty. See User Activity Monitoring in this manual.</td>
</tr>
<tr>
<td>startDate</td>
<td>string</td>
<td>The start or hire date of an identity.</td>
<td>Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:%M</td>
</tr>
<tr>
<td>endDate</td>
<td>string</td>
<td>The end or termination date of an identity.</td>
<td>Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:%M</td>
</tr>
<tr>
<td>work_city</td>
<td>string</td>
<td>The primary work site City for an identity.</td>
<td></td>
</tr>
<tr>
<td>work_country</td>
<td>string</td>
<td>The primary work site Country for an identity.</td>
<td></td>
</tr>
<tr>
<td>work_lat</td>
<td>string</td>
<td>The latitude of primary work site City in DD with compass direction.</td>
<td>37.78N</td>
</tr>
<tr>
<td>work_long</td>
<td>string</td>
<td>The longitude of primary work site City in DD with compass direction.</td>
<td>122.41W</td>
</tr>
</tbody>
</table>

**Configure a new asset or identity list in Splunk Enterprise Security**

Configure a new asset or identity lookup in Splunk Enterprise Security. This multistep process adds the lookup in Splunk Enterprise Security and defines the lookup for the merge process.

**Prerequisite** Format an asset or identity list as a lookup in Splunk Enterprise Security.
Steps

1. Add the new lookup table file
2. Set permissions on the lookup table file to share it with Splunk Enterprise Security
3. Add a new lookup definition
4. Set permissions on the lookup definition to share it with Splunk Enterprise Security
5. Add an input stanza for the lookup source
6. (Optional) Force a merge

Add the new lookup table file

1. From the Splunk menu bar, select Settings > Lookups > Lookup table files.
2. Click New.
4. Select the lookup file to upload.
5. Type the Destination filename that the lookup table file should have on the search head. The name should include the filename extension. For example, network_assets_from_CMDB.csv
6. Click Save to save the lookup table file and return to the list of lookup table files.

Set permissions on the lookup table file to share it with Splunk Enterprise Security

1. From Lookup table files, locate the new lookup table file and select Permissions.
2. Set Object should appear in to All apps.
3. Set Read access for Everyone.
4. Set Write access for admin or other roles.
5. Click Save.

Add a new lookup definition

1. From the Splunk menu bar, select Settings > Lookups > Lookup definitions.
2. Click New.
4. Type a name for the lookup source. This name must match the name defined later in the input stanza definition on the Identity Management
Select a Type of File based. For example, select network_assets_from_CMDB.csv.

Set permissions on the lookup definition to share it with Splunk Enterprise Security

1. From Lookup definitions, locate the new lookup definition and select Permissions.
2. Set Object should appear in to All apps.
3. Set Read access for Everyone.
4. Set Write access for admin or other roles.
5. Click Save.

Add an input stanza for the lookup source

2. From the Splunk ES menu bar, select Configure > Data Enrichment > Identity Management.
3. Click New.
4. Type the name of the lookup.
   For example, network_assets_from_CMDB.
5. Type a Category to describe the new asset or identity list.
   For example, CMDB_network_assets.
6. Type a Description of the contents of the list.
   For example, network assets from the CMDB.
7. Type asset or identity to define the type of list.
8. Type a Source that refers to the lookup definition name.
   For example, lookup://network_assets_from_CMDB.
9. Click Save.
10. Wait five minutes. Splunk Enterprise Security merges the asset and identity lists every five minutes with a saved search. For an explanation of this process, see How Splunk Enterprise Security processes and merges asset and identity data.

Force a merge

You can also run the primary saved searches directly to force a merge immediately without waiting the five minutes for the scheduled search to run.
1. Open the Search page.
2. Run the primary saved searches.

| from savedsearch:"Identity - Asset String Matches - Lookup Gen"
| from savedsearch:"Identity - Asset CIDR Matches - Lookup Gen"
| from savedsearch:"Identity - Identity Matches - Lookup Gen"

**Next step**

Verify that your asset and identity data was added to Splunk Enterprise Security

**Verify that your asset and identity data was added to Splunk Enterprise Security**

Verify that your asset or identity data was added to Splunk Enterprise Security by searching and viewing dashboards.

**Prerequisite**

Configure the new asset or identity list in Splunk Enterprise Security

**Steps**

Verify asset lookup data.

1. Verify that a specific asset record exists in the asset lookup.
   1. Choose an asset record with data in the `ip`, `mac`, `nt_host`, or `dns` fields from an asset list.
   2. Search for it in Splunk Web.

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

   • View all available assets in your instance using one of the following methods. Compare the number of rows with your asset data sources to verify the number of asset records matches your expectations, or spot check specific records.

   • View the Asset Center dashboard. See Asset Center dashboard in *Use Splunk Enterprise Security*.
• Use the assets macro.

    | `assets`

• Search the data model.

    | `datamodel("Identity_Management", "All_Assets")`
    | `drop_dm_object_name("All_Assets")`

Verify identity lookup data.

1. Verify that a specific identity record exists in the identity lookup.
   1. Choose an identity record with data in the `identity` field.
   2. Search for it in Splunk Web.

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

• View all available identities in your instance using one of the following methods. Compare the number of rows with your identity data sources to verify the number of identity records matches your expectations, or spot check specific records.

• View the Identity Center dashboard. See Identity Center dashboard in Use Splunk Enterprise Security.

• Use the identities macro.

    | `identities`

• Search the data model.

    | `datamodel("Identity_Management", "All_Identities")`
    | `drop_dm_object_name("All_Identities")`

Next step

Configure asset and identity correlation in Splunk Enterprise Security

Configure asset and identity correlation in Splunk Enterprise Security

After you add your asset and identity data to Splunk Enterprise Security, configure asset and identity correlation in Splunk Enterprise Security.
Prerequisite

Verify that your asset and identity data was added to Splunk Enterprise Security

Steps

1. Choose whether to enable asset and identity correlation, disable it, or restrict correlation to occur only for select source types. If in doubt, keep asset and identity correlation enabled. See How asset and identity correlation works for more information about how the correlation enriches events at search time.
2. From the Splunk ES menu bar, select Configure > Data Enrichment > Identity Correlation.
3. Enable correlation is selected by default. You can change this to Disable correlation (not recommended) or Enable selectively by sourcetype.
4. If you choose Enable selectively by sourcetype, type a source type and select the check box for asset and/or identity.
5. Click Save.

Disabling asset and identity correlation completely prevents events from being enriched with asset and identity data from the asset and identity lookups. This might prevent correlation searches, dashboards, and other functionality from working as expected. Consult with Splunk Professional Services or Splunk Support before disabling asset and identity correlation.

How asset and identity correlation works

To effectively detect security intrusions, an organization must be able to correlate events in log data with specific assets and identities that may be responsible for, or affected by the intrusion. When asset and identity correlation is enabled, Splunk Enterprise Security compares indexed events with asset and identity data in the asset and identity lists to provide data enrichment and context. The comparison process uses automatic lookups. You can find information about automatic lookups in the Splunk platform documentation.

- For Splunk Enterprise, see Make your lookup automatic in the Splunk Enterprise Knowledge Manager Manual.
- For Splunk Cloud, see Make your lookup automatic in the Splunk Cloud Knowledge Manager Manual.

Asset and identity correlation enriches events with asset and identity data at search time.
Asset correlation compares events that contain data in any of the src, dest, or dvc fields against the merged asset lists for matching IP address, MAC address, DNS name, or Windows NetBIOS names. Asset correlation no longer occurs automatically against the host or orig_host fields.

Identity correlation compares events that contain data in any of the user or src_user fields against the merged identity lists for a matching user or session.

Enterprise Security adds the matching output fields to the event. For example, correlation on the asset src field results in additional fields such as src_is_expected and src_should_timesync.

Asset and identity correlation allows you to determine whether multiple events can relate to the same asset or identity. You can also perform actions on the identity and asset fields added to events to open additional searches or dashboards scoped to the specific asset or identity. For example, open the Asset Investigator dashboard on a src field.

### How Splunk Enterprise Security processes and merges asset and identity data

Splunk Enterprise Security takes the asset and identity data that you add as lookups and generates combined lookup files. Splunk Enterprise Security uses the generated lookup files to correlate asset and identity data with events using automatic lookups. The following steps describe this process at a high level.

1. You collect asset and identity data from data sources using an add-on and a custom search or manually with a CSV file. See Collect and extract asset and identity data.
2. You configure any settings in the identity lookup configuration setup. See Define identity formats on the identity configuration page.
4. You format the data as a lookup, using a search or manually with a CSV file. See Format the asset or identity list as a lookup.
5. You configure the list as a lookup table, definition, and input. See Configure a new asset or identity list.
6. The Splunk Enterprise Security identity manager modular input detects two things:
   - Changed content in the identity_manager://<input_name>.
   - Changes to stanzas in the input.
7. The Splunk Enterprise Security identity manager modular input updates the macros used to identify the input sources based on the currently enabled stanzas in inputs.conf. For example, the `generate_identities` macro dynamically updates based on the conventions specified on the Identity Lookup Configuration page.

8. The Splunk Enterprise Security identity manager modular input dispatches lookup generating saved searches if it identifies changes that require the asset and identity lists to be merged.

9. The lookup generating saved searches merge all configured and enabled asset and identity lists.
   - The primary saved searches concatenate the lookup tables referenced by the identity manager input, generate new fields, and output the concatenated asset and identity lists into target lookup table files.
   - Secondary saved searches generate lookup tables for asset categories, identity categories, and asset PCI domains (in the Splunk App for PCI Compliance).

10. You verify that the data looks as expected. See Verify that your asset or identity data was added to Splunk Enterprise Security.

The merging of identity and asset lookups does not validate or de-duplicate input. Errors from the identity manager modular input are logged in identity_manager.log. This log does not show data errors.

### Lookups that store merged asset and identity data in Splunk Enterprise Security

After the asset and identity merging process completes, four lookups store your asset and identity data.

<table>
<thead>
<tr>
<th>Function</th>
<th>Table name</th>
<th>Saved search</th>
<th>Lookup name</th>
</tr>
</thead>
<tbody>
<tr>
<td>String-based asset correlation</td>
<td>assets_by_str.csv</td>
<td>Identity - Asset String Matches - Lookup Gen</td>
<td>LOOKUP-zu-asset_lookup_by_str-dvc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LOOKUP-zu-asset_lookup_by_str-dvc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LOOKUP-zu-asset_lookup_by_str-src</td>
</tr>
<tr>
<td>CIDR subnet-based</td>
<td>assets_by_cidr.csv</td>
<td>Identity - Asset</td>
<td>LOOKUP-zv-asset_lookup_by_cidr-dvc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LOOKUP-zv-asset_lookup_by_cidr-dvc</td>
</tr>
</tbody>
</table>
### Asset and identity fields after processing in Splunk Enterprise Security

The following tables describe the fields that exist in the asset and identity lookups after Splunk Enterprise Security finishes processing the source lookup files. These fields are the fields present in the lookups that store merged asset and identity data. See Lookups that store merged asset and identity data in Splunk Enterprise Security.

For more information about the merge process, see How Splunk Enterprise Security processes and merges asset and identity data.

#### Asset fields after processing

Asset fields of the asset lookup after the saved searches perform the merge process.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action taken by ETL</th>
</tr>
</thead>
<tbody>
<tr>
<td>bunit</td>
<td>unchanged</td>
</tr>
</tbody>
</table>

For more information about the asset and identity merge process, see How Splunk Enterprise Security processes and merges asset and identity data.
<table>
<thead>
<tr>
<th>Field</th>
<th>Action taken by ETL</th>
</tr>
</thead>
<tbody>
<tr>
<td>city</td>
<td>unchanged</td>
</tr>
<tr>
<td>country</td>
<td>unchanged</td>
</tr>
<tr>
<td>dns</td>
<td>Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>lat</td>
<td>unchanged</td>
</tr>
<tr>
<td>long</td>
<td>unchanged</td>
</tr>
<tr>
<td>mac</td>
<td>Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>nt_host</td>
<td>Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>owner</td>
<td>unchanged</td>
</tr>
<tr>
<td>priority</td>
<td>unchanged</td>
</tr>
<tr>
<td>asset_id</td>
<td>Generated from the values of dns, ip, mac, and nt_host fields.</td>
</tr>
<tr>
<td>asset_tag</td>
<td>Generated from the values of category, pci_domain, is_expected, should_timesync, should_update, requires_av, and bunit fields.</td>
</tr>
<tr>
<td>category</td>
<td>Appends &quot;pci&quot; if the value contains &quot;cardholder&quot;. Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>ip</td>
<td>Validates and splits the field into CIDR subnets as necessary. Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>pci_domain</td>
<td>Appends &quot;trust&quot; or &quot;untrust&quot; based on certain field values. Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>is_expected</td>
<td>Normalized to a boolean.</td>
</tr>
<tr>
<td>should_timesync</td>
<td>Normalized to a boolean.</td>
</tr>
<tr>
<td>should_update</td>
<td>Normalized to a boolean.</td>
</tr>
<tr>
<td>requires_av</td>
<td>Normalized to a boolean.</td>
</tr>
<tr>
<td>key</td>
<td>Generated by the ip, mac, nt_host, and dns fields after the original fields are transformed.</td>
</tr>
</tbody>
</table>
Identity fields after processing

Identity fields of the identity lookup after the saved searches perform the merge process.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action taken by ETL</th>
</tr>
</thead>
<tbody>
<tr>
<td>bunit</td>
<td>unchanged</td>
</tr>
<tr>
<td>email</td>
<td>unchanged</td>
</tr>
<tr>
<td>endDate</td>
<td>unchanged</td>
</tr>
<tr>
<td>first</td>
<td>unchanged</td>
</tr>
<tr>
<td>last</td>
<td>unchanged</td>
</tr>
<tr>
<td>managedBy</td>
<td>unchanged</td>
</tr>
<tr>
<td>nick</td>
<td>unchanged</td>
</tr>
<tr>
<td>phone</td>
<td>unchanged</td>
</tr>
<tr>
<td>phone2</td>
<td>unchanged</td>
</tr>
<tr>
<td>prefix</td>
<td>unchanged</td>
</tr>
<tr>
<td>priority</td>
<td>unchanged</td>
</tr>
<tr>
<td>startDate</td>
<td>unchanged</td>
</tr>
<tr>
<td>suffix</td>
<td>unchanged</td>
</tr>
<tr>
<td>work_city</td>
<td>unchanged</td>
</tr>
<tr>
<td>work_country</td>
<td>unchanged</td>
</tr>
<tr>
<td>work_lat</td>
<td>unchanged</td>
</tr>
<tr>
<td>work_long</td>
<td>unchanged</td>
</tr>
<tr>
<td>watchlist</td>
<td>Normalized to a boolean.</td>
</tr>
<tr>
<td>category</td>
<td>Appends &quot;pci&quot; if the value contains &quot;cardholder&quot;. Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>identity</td>
<td>Generated based on values in the input row and conventions specified in the Identity Lookup Configuration. Accepts pipe-delimited values and converts them to a multi-value field.</td>
</tr>
<tr>
<td>identity_id</td>
<td>Generated from the values of identity, first, last, and email.</td>
</tr>
<tr>
<td>identity_tag</td>
<td>Generated from the values of bunit, category, and watchlist.</td>
</tr>
</tbody>
</table>
Test the asset and identity merge process in Splunk Enterprise Security

You can test the asset and identity merge process if you want to confirm that the data produced by the merge process is expected and accurate. Run the saved searches that perform the merge process without outputting the data to the merged lookups to determine what the merge will do with your data without actually performing the merge. These steps are not required, but can be performed to validate the merge works as expected.

Test the merge process without performing a merge and outputting the data to a lookup.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. Locate the first of the three primary saved searches **Identity - Asset CIDR Matches - Lookup Gen**.
3. Click the search name to open it.
4. Copy the search from the **Search** field.
5. Open the **Search** page.
6. Paste the search and remove the `output_*` macro. For example, change
   | `asset_sources` | `make_assets_cidr` |
   `output_assets("SA-IdentityManagement", "assets_by_cidr.csv")` to |
   | `asset_sources` | `make_assets_cidr`.
7. Run the search.
8. Repeat steps 2-7 for the other two searches, **Identity - Asset String Matches - Lookup Gen** and **Identity - Identity Matches - Lookup Gen**.

Customize the asset and identity merge process in Splunk Enterprise Security

You can modify the saved searches that perform the asset and identity merge process to perform additional field transformations or data sanitization. Add any operations that you want to change in the merge process to the search before the `output_*` macro.

Certain modifications to the saved searches are unsupported and could break the merge process or asset and identity correlation.

- Do not add or delete fields from the output.
Do not change the output location to a different lookup table or a KV store collection.
Do not replace the `output_*` macros with the `outputlookup` command.

Modify asset and identity lookups in Splunk Enterprise Security

Make changes to the asset and identity lookups in Splunk Enterprise Security to add new assets or identities, or change existing values in the lookup tables. You can also disable or enable existing lookups.

Edit asset and identity lookups

Edit an asset or identity lookup in the Identity Management dashboard.

1. In Enterprise Security, select **Configure > Data Enrichment > Identity Management**.
2. Find the name of the asset or identity list you want to edit, and select Source. The list opens in an interactive editor.
3. Use the scroll bars to view the columns and rows in the table. Double click a cell to add, change, or remove content.
4. Click Save when you are finished.

Changes made to an asset or identity list will be reflected in search results after the next scheduled merge. See How Splunk Enterprise Security processes and merges asset and identity data.

Disable or enable asset and identity lookups

Disable or enable an asset or identity lookup input. Disable an input to prevent the contents of the corresponding list from being included in the merge process. Enable a disabled input to allow the associated list to be merged at the next scheduled merge of the asset or identity data. Disabling an input does not delete the data from the associated lookup from Splunk Enterprise Security.

1. In Enterprise Security, select **Configure > Data Enrichment > Identity Management**.
2. Locate the asset or identity lookup you want to disable.
3. Click Disable or Enable.
Starting with version 5.0.0, asset and identity lookup inputs are disabled by default after installation. Local settings are respected after an upgrade.

**Disable the demo asset and identity lookups**

The demo asset and identity lookups are disabled by default. Disable the demo asset and identity lookups to prevent the demo data from being added to the primary asset and identity lookups used by Splunk Enterprise Security for asset and identity correlation. After you disable the demo data lookups, saved searches update the primary asset and identity lookups and removes the data from the disabled lookups from the primary lookups.

1. In Enterprise Security, select **Configure > Data Enrichment > Identity Management**.
2. Locate the demo_assets and demo_identities lookups.
3. Click **Disable** for each.

**Include or exclude asset or identity lookups from bundle replication**

Starting in version 4.7.0, the asset and identity source lookup files are excluded from bundle replication in an indexer cluster by default. The merged lookup files are still included in bundle replication to support asset and identity correlation. See [Lookups that store merged asset and identity data in Splunk Enterprise Security](#) for the lookup files that continue to be included in bundle replication.

Changing the default to include asset and identity lookup files in bundle replication might reduce system performance.

1. In Enterprise Security, select **Configure > Data Enrichment > Identity Management**.
2. Click the lookup that you want to include or exclude from bundle replication.
3. Select or deselect the check box for **Blacklist**. If selected, the lookup file is excluded from bundle replication.

You can only make this change if the "Enable Identity Generation Autoupdate" setting is set to "true". See [Configure general settings for Splunk Enterprise Security](#).
Example methods of adding asset and identity data in Splunk Enterprise Security

These example methods cover some common ways to add asset and identity data to Splunk Enterprise Security. You can work with Splunk Professional Services to find the best solution for your environment.

Add asset and identity data from Active Directory

This example describes how to add asset and identity data from Active Directory.

Set up the Splunk Support for Active Directory app

Collect asset and identity data with the Splunk Support for Active Directory app. For information about installing and configuring the app, see Install the Splunk Supporting Add-on for Active Directory.

Collect asset and identity data from Active Directory

Collect asset and identity data from Active Directory by searching the data in SA-ldapsearch.

1. Follow the steps to configure a new asset or identity list. See Configure a new asset or identity list in Splunk Enterprise Security.
2. Disable the lookup file you created until you finish setting up the saved search to prevent the asset or identity data from merging with incomplete or inaccurate data. See Disable or enable asset and identity lookups.
3. Create a saved search in SA-IdentityManagement to populate the lookup table file with the ldapsearch command. The exact syntax of this search varies depending on your AD configuration. See Example search for collecting identity data from Active Directory and Example search for collecting asset data from Active Directory for two examples.

Example search for collecting identity data from Active Directory

This example search assigns static values for suffix, endDate, category, watchlist, and priority. Use it as a guide to construct and test a working search, then replace the static values with information from your AD environment. Rename the lookup my_identity_lookup to something appropriate for your environment.
Example search for collecting asset data from Active Directory

This example search assigns static values for several fields. Use it as a guide to construct and test a working search, then replace the static values with information from your AD environment. Rename the lookup my_asset_lookup to something appropriate for your environment.

Add asset data from indexed events in the Splunk platform

This example demonstrates how to identify hosts that appear in indexed events that are not currently associated with existing asset data and add those hosts to your asset lookup.

Use this example search to compare hosts communicating with the Splunk platform to the set of existing asset information and review the table of
unmatched hosts. You can then export the table as an asset list.

```
| `host_eventcount`
| search host_is_expected=false NOT host_asset_id=*
| fields - firstTime, recentTime, lastTime, _time,
host_owner_*, host_asset_tag, host_asset_id
| sort -totalCount, dayDiff
| table
host, ip, mac, nt_host, dns, owner, priority, lat, long, city, country, bunit, category, pci_domain,
```

Manually add new asset or identity data

Manually add new asset or identity data to Splunk Enterprise Security by editing
the Assets or Identities lookups. For example, add internal subnets, IP addresses
to be whitelisted, and other static asset and identity data.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. To add asset data, click the **Assets** lookup to edit it. To add identity data,
click the **Identities** list to edit it.
3. Use the scroll bars to view the columns and rows in the table. Double click
in a cell to add, change, or remove content.
4. Save your changes.
Threat Intelligence

Add threat intelligence to Splunk Enterprise Security

As an ES administrator, you can correlate indicators of suspicious activity, known threats, or potential threats with your events by adding threat intelligence to Splunk Enterprise Security. Adding threat intelligence enhances your analysts’ security monitoring capabilities and adds context to their investigations.

Splunk Enterprise Security includes a selection of threat intelligence sources. Splunk Enterprise Security also supports multiple types of threat intelligence so that you can add your own threat intelligence.

ES administrators can add threat intelligence to Splunk Enterprise Security by downloading a feed from the Internet, uploading a structured file, or inserting the threat intelligence directly from events in Splunk Enterprise Security.

Prerequisite


Steps

1. Configure the threat intelligence sources included with Splunk Enterprise Security.
2. For each additional threat intelligence source not already included with Splunk Enterprise Security, follow the procedure to add threat intelligence that matches the source and format of the intelligence that you want to add.
   - Download a threat intelligence feed from the Internet
   - Upload a STIX or OpenIOC structured threat intelligence file
   - Upload a custom CSV file of threat intelligence
   - Add threat intelligence from Splunk events in Splunk Enterprise Security
   - Add and maintain threat intelligence locally in Splunk Enterprise Security
   - Add threat intelligence with a custom lookup file in Splunk Enterprise Security
3. Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

See also

Change existing threat intelligence in Splunk Enterprise Security

Add threat intelligence with an adaptive response action.

Threat Intelligence API reference in REST API Reference.

Threat Intelligence framework in Splunk ES on the Splunk developer portal

**Supported types of threat intelligence in Splunk Enterprise Security**

Splunk Enterprise Security supports several types of threat intelligence. The supported types of threat intelligence correspond to the KV Store collections in which the threat intelligence is stored.

The threat intelligence manager modular input parses downloaded and uploaded files and adds indicators to these collections. Files can contain any combination of indicators.

<table>
<thead>
<tr>
<th>Threat collection in KV Store</th>
<th>Supported IOC data types</th>
<th>Local lookup file</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate_intel</td>
<td>X509 Certificates</td>
<td>Local Certificate Intel certificate_issuer,certificate_subject,certificate_issuer_organization,certificate_subject_organization,certificate_serial,certificate_issuer_unit,certificate_subject_unit,description,weight</td>
</tr>
<tr>
<td>email_intel</td>
<td>Email</td>
<td>Local Email Intel description,src_user,subject,weight</td>
</tr>
<tr>
<td>file_intel</td>
<td>File names or hashes</td>
<td>Local File Intel description,file_hash,file_name,weight</td>
</tr>
<tr>
<td>http_intel</td>
<td>URLs</td>
<td>Local HTTP Intel description,http_referrer,http_user_agent,url,weight</td>
</tr>
<tr>
<td>ip_intel</td>
<td>IP addresses</td>
<td>Local IP Intel description,ip,weight</td>
</tr>
<tr>
<td>Threat collection in KV Store</td>
<td>Supported IOC data types</td>
<td>Local lookup file</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>domains</td>
<td>Local Domain Intel</td>
<td>description, domain, weight</td>
</tr>
<tr>
<td>process_intel</td>
<td>Local Process Intel</td>
<td>description, process, process_file_name, weight</td>
</tr>
<tr>
<td>registry_intel</td>
<td>Local Registry Intel</td>
<td>description, registry_path, registry_value_name, registry_value_text, weight</td>
</tr>
<tr>
<td>service_intel</td>
<td>Local Service Intel</td>
<td>description, service, service_file_hash, service_dll_file_hash, weight</td>
</tr>
<tr>
<td>user_intel</td>
<td>Local User Intel</td>
<td>description, user, weight</td>
</tr>
</tbody>
</table>

The `collections.conf` file in the `DA-ESS-ThreatIntelligence` subdirectory lists these KV Store collections.

**Configure the intelligence sources included with Splunk Enterprise Security**

Splunk Enterprise Security includes several intelligence sources that retrieve information across the Internet.

None of these intelligence sources are enabled by default. Review the types of intelligence provided by the sources, and determine if the included intelligence is useful to your team before enabling specific sources.

**Prerequisites**

- Your Splunk Enterprise deployment must be connected to the Internet. If your deployment is not connected to the Internet, disable these sources or source them in an alternate way.
- To set up firewall rules for these sources, you might want to use a proxy server to collect the intelligence before forwarding it to Splunk Enterprise Security and allow the IP address for the proxy server to access Splunk.
Enterprise Security. The IP addresses for these sources can change.

Steps

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
2. Review the **Description** field for all defined intelligence sources to learn more about the types of information or threat indicators that can be correlated with your events.
3. Enable the intelligence sources that fit your security use cases.
4. Configure the enabled intelligence sources that fit your security use cases, using the links to the source websites to review the source provider’s documentation. Each source website provides suggestions for polling intervals and other configuration requirements separate from Splunk Enterprise Security.

Splunk Enterprise Security expects all intelligence sources to send properly-formatted data and valuable intelligence information. Feed providers are responsible for malformed data or false positives that might be identified in your environment as a result.

If you determine that your Splunk Enterprise Security installation is retrieving data from unexpected IP addresses, perform a WHOIS or nslookup to determine if the IP address matches that of one of the intelligence sources configured in your environment.

Next step

To add a custom threat source, see **Add threat intelligence to Splunk Enterprise Security** and follow the link that matches the source that you want to add.

If you are finished adding intelligence sources, see **Verify that you have added intelligence successfully in Splunk Enterprise Security**.

### Included threat intelligence sources

The threat intelligence sources are parsed for threat indicators and added to the relevant KV Store collections.

<table>
<thead>
<tr>
<th>Threat source</th>
<th>Threat list</th>
<th>Website for the threat source</th>
</tr>
</thead>
</table>

99
<table>
<thead>
<tr>
<th>Table</th>
<th>Data list</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>provider</strong></td>
<td><strong>Data provider</strong></td>
</tr>
<tr>
<td>Emerging Threats compromised IPs blocklist</td>
<td>Emerging Threats</td>
</tr>
<tr>
<td>Emerging Threats firewall IP rules</td>
<td>Emerging Threats</td>
</tr>
<tr>
<td>Malware domain host list</td>
<td>Hail a TAXII.com</td>
</tr>
<tr>
<td>iblocklist Logmein</td>
<td>I-Blocklist</td>
</tr>
<tr>
<td>iblocklist Piratebay</td>
<td>I-Blocklist</td>
</tr>
<tr>
<td>iblocklist Proxy</td>
<td>I-Blocklist</td>
</tr>
<tr>
<td>iblocklist Rapidshare</td>
<td>I-Blocklist</td>
</tr>
<tr>
<td>iblocklist Spyware</td>
<td>I-Blocklist</td>
</tr>
<tr>
<td>iblocklist Tor</td>
<td>I-Blocklist</td>
</tr>
<tr>
<td>iblocklist Web attacker</td>
<td>I-Blocklist</td>
</tr>
<tr>
<td>Malware Domain Blocklist</td>
<td>Malware Domains</td>
</tr>
<tr>
<td>abuse.ch Palevo C&amp;C IP Blocklist</td>
<td>abuse.ch</td>
</tr>
<tr>
<td>Phishtank Database</td>
<td>Phishtank</td>
</tr>
<tr>
<td>SANS blocklist</td>
<td>SANS</td>
</tr>
<tr>
<td>abuse.ch ZeuS blocklist (bad IPs only)</td>
<td>abuse.ch</td>
</tr>
<tr>
<td>abuse.ch ZeuS blocklist (standard)</td>
<td>abuse.ch</td>
</tr>
</tbody>
</table>

**Included generic intelligence sources**

Splunk Enterprise Security also includes generic intelligence that is not added to the threat intelligence KV Store collections and are instead used to enrich data in Splunk Enterprise Security.
You can configure the generic intelligence source to use for top one million sites:

1. From the Splunk ES menu bar, select **Configure > General > General Settings**
2. Scroll down to Top 1M Site Source and select **Cisco**.

## Download a threat intelligence feed from the Internet in Splunk Enterprise Security

Splunk Enterprise Security can periodically download a threat intelligence feed available from the Internet, parse it, and add it to the relevant KV Store collections.

1. (Optional) **Configure a proxy for retrieving threat intelligence.**
2. Follow the procedure that matches the format of the threat source:
   - Add a URL-based threat source
   - Add a TAXII feed
If you manually disable a threat artifact in a collection, but the threat intelligence source provides the same indicator in a download again, then the entry in KVStore gets overwritten, and does not preserve your flag.

**Configure a proxy for retrieving threat intelligence**

If you use a proxy server to send threat intelligence to Splunk Enterprise Security, configure the proxy options for the threat source.

The user must correspond to the name of a Splunk secure stored credential in Credential Management. If you remove an existing proxy user and password in the Intelligence Download Setting editor, the download process no longer references the stored credentials. Removing the reference to the credential does not delete the stored credentials from Credential Management. See Manage credentials in Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select Configure > Data Enrichment > Intelligence Downloads.
2. Select the threat download source or add a new threat download source. See Add a URL-based threat source or Add a TAXII feed.
3. Configure the proxy options.
   1. Type a proxy server address. The Proxy Server cannot be a URL. For example, 10.10.10.10 or server.example.com.
   2. Type a proxy server port to use to access the proxy server address.
   3. Type a proxy user credential for the proxy server. Only basic and digest authentication methods are supported. The user must correspond to the name of a credential stored in Credential Management.
   4. (Optional) Type a proxy user realm for the proxy user credential. Use this to specify a proxy user realm for the user credential.
4. Save your changes.

**Add a URL-based threat source**

Add a non-TAXII source of intelligence that is available from a URL on the Internet. For an example of adding a URL-based threat intelligence source, see Example: Add a ransomware threat feed to Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select Configure > Data Enrichment > Intelligence Downloads.
2. Click New to add a new intelligence source.
3. Type a Name for the threat download. The name can only contain alphanumeric characters, hyphens, and underscores. The name cannot
contain spaces.

4. Select or deselect the check box for Is Threat Intelligence.
5. (Optional) Select or deselect the check box for Sinkhole. Select the check box to delete the downloaded file after processing.
6. Type a Type for the threat download. The type identifies the type of threat indicator that the feed contains.
7. Type a Description. Describe the indicators in the threat feed.
8. Type an integer to use as the Weight for the threat indicators. Enterprise Security uses the weight of a threat feed to calculate the risk score of an asset or identity associated with an indicator on the threat feed. A higher weight indicates an increased relevance or an increased risk to your environment.
9. (Optional) Change the default download Interval for the threat feed. Defaults to 43200 seconds, or every 12 hours.
10. (Optional) Type POST arguments for the threat feed. You can use POST arguments to retrieve user credentials from Credential Management. Use the format key=$user:<username>$ or key=$user:<username>,realm:<realm>$ to specify a username and realm.

11. (Optional) Type a Maximum age to define the retention period for this threat source, defined in relative time. Enable the corresponding saved searches for this setting to take effect. See Configure threat source retention.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delimiting regular expression</td>
<td>A regular expression string used to split, or delimit, lines in an intelligence source. For complex delimiters, use an extracting regular expression.</td>
<td>^\S+</td>
</tr>
<tr>
<td>Extracting regular expression</td>
<td>A regular expression used to extract fields from individual lines of a threat source document.</td>
<td>^\S+</td>
</tr>
</tbody>
</table>

12. (Optional) If you need to specify a custom User agent string to bypass network security controls in your environment, type it in the format <user-agent>/<version>. For example, Mozilla/5.0 or AppleWebKit/602.3.12. The value in this field must match this regex: ([A-Za-z0-9_.-]+)/([A-Za-z0-9_.-]+). Check with your security device administrator to ensure the string you type here is accepted by your network security controls.

13. Fill out the Parsing Options fields to make sure that your threat list parses successfully. You must fill out either a delimiting regular expression or an extracting regular expression. You cannot leave both fields blank.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>expression</td>
<td>Use to extract values in the threat source.</td>
<td></td>
</tr>
<tr>
<td>Fields</td>
<td>Required if your document is line-delimited. Comma-separated list of fields to be extracted from the threat list. Can also be used to rename or combine fields. Description is a required field. Additional acceptable fields are the fields in the corresponding KV Store collection for the threat intelligence, visible in the local lookup files or the DA-ESS-ThreatIntelligence/collections.conf file. Defaults to description:$1,ip:$2.</td>
<td>&lt;fieldname&gt;:&lt;$number&gt;,&lt;fieldname&gt;.$&lt;number&gt;,ip:$1,description:domain_blocklist</td>
</tr>
<tr>
<td>Ignoring regular expression</td>
<td>A regular expression used to ignore lines in a threat source. Defaults to ignoring blank lines and comments beginning with #.</td>
<td>^\s*$)</td>
</tr>
<tr>
<td>Skip header lines</td>
<td>The number of header lines to skip when processing the threat source.</td>
<td>0</td>
</tr>
<tr>
<td>Intelligence file encoding</td>
<td>If the file encoding is something other than ASCII or UTF8, specify the encoding here. Leave blank otherwise.</td>
<td>latin1</td>
</tr>
</tbody>
</table>

14. (Optional) Change the **Download Options** fields to make sure that your threat list downloads successfully.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry interval</td>
<td>Number of seconds to wait between download retry attempts. Review the recommended poll interval of the threat source provider before changing the retry interval.</td>
<td>60</td>
</tr>
<tr>
<td>Remote site user</td>
<td>If the threat feed requires authentication, type the user name to use in remote authentication, if required. The user name you add in this field must match the name of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.</td>
<td>buttercup</td>
</tr>
<tr>
<td>Remote site user realm</td>
<td>If the threat feed requires authentication, type the user name to use in remote authentication, if required. The realm you add in this field must match the realm of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.</td>
<td>paddock</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Retries</td>
<td>The maximum number of retry attempts.</td>
<td>3</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds to wait before marking a download attempt as failed.</td>
<td>30</td>
</tr>
</tbody>
</table>

15. (Optional) If you are using a proxy server, fill out the **Proxy Options** for the threat feed. See Configure a proxy for retrieving threat intelligence.

16. Save your changes.

**Next step**

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

**Add a TAXII feed**

Add threat intelligence provided as a TAXII feed to Splunk Enterprise Security.

**Prerequisite**

Determine whether the TAXII feed requires certificate authentication. If it does, add the certificate and keys to the same app directory in which you define the TAXII feed. For example, DA-ESS-ThreatIntelligence.

1. Follow the steps to add a new certificate to Splunk Enterprise Security to add both the certificate and the private key files. See Manage credentials in Splunk Enterprise Security.

2. Follow the steps for adding a TAXII feed to Splunk Enterprise Security, using the `cert_file` and `key_file` POST arguments to specify the file names of the certificate and private key file.

**Steps**

1. On the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
2. Click **New** to add a new TAXII feed.
3. Type a **Name** for the threat intelligence feed.
4. Select the check box for **Is Threat Intelligence**.
5. (Optional) Select or deselect the check box for **Sinkhole**. Select the check box to delete the downloaded file after processing.

6. Type a **Type** of **taxii**.

7. Type a **Description** for the threat intelligence feed.

8. Type a URL to use to download the TAXII feed.

9. (Optional) Change the default **Weight** for the threat intelligence feed.
   
   Increase the weight if the threats on the threat feed are high-confidence and malicious threats that should increase the risk score for assets and identities that interact with the indicators from the threat source.

10. (Optional) Adjust the interval at which to download the threat intelligence. Defaults to 43200 seconds, or twice a day.

11. Type TAXII-specific space-delimited **POST arguments** for the threat intelligence feed.

\[<\text{POST argument}>="<\text{POST argument value}>"\]

<table>
<thead>
<tr>
<th>Example POST argument</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>collection</td>
<td>Name of the data collection from a TAXII feed.</td>
<td>(\text{collection} = \text{&quot;A_TAXII_Feed_Name&quot;})</td>
</tr>
<tr>
<td>earliest</td>
<td>The earliest threat data to pull from the TAXII feed.</td>
<td>(\text{earliest} = \text{&quot;-1y&quot;})</td>
</tr>
<tr>
<td>taxii_username</td>
<td>An optional method to provide a TAXII feed username.</td>
<td>(\text{taxii_username} = \text{&quot;user&quot;})</td>
</tr>
<tr>
<td>taxii_password</td>
<td>An optional method to provide a TAXII feed password. If you provide a username without providing a password, the threat intelligence modular input attempts to find</td>
<td>(\text{taxii_password} = \text{&quot;password&quot;})</td>
</tr>
<tr>
<td>Example POST argument</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>taxii_username_realm</td>
<td>An optional method to provide a realm for the TAXII feed username. Used with the taxii_username to locate the user credential password in Credential Management.</td>
<td>taxii_username_realm=&quot;realm&quot;</td>
</tr>
<tr>
<td>cert_file</td>
<td>Add the certificate file name if the TAXII feed uses certificate authentication. The file name must match exactly and is case sensitive.</td>
<td>cert_file=&quot;cert.crt&quot;</td>
</tr>
<tr>
<td>key_file</td>
<td>Add the key file name for the certificate if the TAXII feed uses certificate authentication. The file name must match exactly and is</td>
<td>key_file=&quot;cert.key&quot;</td>
</tr>
<tr>
<td>Example POST argument</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>case sensitive.</td>
<td></td>
</tr>
</tbody>
</table>

12. TAXII feeds do not use the **Maximum age** setting. To configure file retention for TAXII files, see Configure intelligence file retention.

13. TAXII feeds do not use the **User agent** setting.

14. TAXII feeds do not use the **Parsing Options** settings.

15. (Optional) Change the **Download Options**.

16. (Optional) Change the **Proxy Options**. See Configure a proxy for retrieving threat intelligence.

17. Save the changes.

You cannot use an authenticated proxy with a TAXII feed because the libtaxii library used by Enterprise Security does not support authenticated proxies. If possible, use an unauthenticated proxy instead.

**Next step**

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

**Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security**

Upload threat intelligence in a STIX or OpenIOC file to Splunk Enterprise Security using one of the following methods:

- Upload a STIX or OpenIOC file using the Splunk Enterprise Security interface
- Add STIX or OpenIOC files using the REST API
- Add STIX or OpenIOC files using the file system

**Upload a STIX or OpenIOC file using the Splunk Enterprise Security interface**
Splunk Enterprise Security supports adding OpenIOC, STIX, and CSV file types directly in the Splunk Enterprise Security interface.

1. On the Enterprise Security menu bar, select Configure > Data Enrichment > Threat Intelligence Uploads.
2. Type a file name for the file you want to upload. The file name you type becomes the name of the file saved to $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel. The file name cannot include spaces or special characters.
3. Upload an OpenIOC or STIX-formatted file.
4. Type a Weight for the threat intelligence file. The weight of a threat intelligence file increases the risk score of objects associated with threat intelligence on this list.
5. (Optional) Type a Threat Category. If you leave this field blank and a category is specified in the OpenIOC or STIX file, Splunk Enterprise Security uses the threat category specified in the file.
6. (Optional) Type a Threat Group. If you leave this field blank and a group is specified in the OpenIOC or STIX file, Splunk Enterprise Security uses the threat group specified in the file.
7. (Optional) Select the Overwrite check box. If you have previously uploaded a file with the same file name, select this check box to overwrite the previous version of the file.
8. (Optional) Select the Sinkhole check box. This deletes the file after the intelligence from the file is processed.
9. Click Save.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add STIX or OpenIOC files using the REST API

The Splunk Enterprise Security REST API supports uploading threat intelligence files in OpenIOC, STIX, or CSV format. See Threat Intelligence API reference.

Next step
To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add STIX or OpenIOC files using the file system

You can also add threat intelligence to Splunk Enterprise Security by adding a properly-formatted file to a file system folder.

1. Add a STIX-formatted file with a .xml file extension or an OpenIOC file with a .ioc file extension to the $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel folder on your Splunk Enterprise Security search head or make it available to that file directory on a mounted local network share.
2. By default, the da_ess_threat_local modular input processes those files and places the threat intelligence found in the relevant KV Store collections.
3. By default, after processing the intelligence in the files, the modular input deletes the files because the sinkhole setting is enabled by default.

Change the da_ess_threat_local inputs settings

1. On the Enterprise Security menu bar, select Configure > Data Enrichment > Threat Intelligence Management.
2. Click the da_ess_threat_local modular input.
3. Review or change the settings as required.

Do not change the default da_ess_threat_default input.

Configure a custom folder and input monitor for threat sources

You can also add threat intelligence to Splunk Enterprise Security by adding a properly-formatted file to a custom file directory. The file directory must match the pattern $SPLUNK_HOME/etc/apps/<app_name>/local/data/<directory_name>, and you must create an input monitor to monitor that file directory for threat intelligence.

Create an input monitor for threat sources to add threat intelligence to a different folder than the one monitored by the da_ess_threat_local modular input.
1. From the Enterprise Security menu bar, select Configure > Data Enrichment > Threat Intelligence Management.

2. Click New

3. Type a descriptive name for the modular input. The name cannot include spaces.

4. Type a path to the file repository. The file repository must be
   \$SPLUNK_HOME/etc/apps/<app_name>/local/data/<directory_name>

5. (Optional) Type a maximum file size in bytes.

6. (Optional) Select the Sinkhole check box. If selected, the modular input deletes each file in the directory after processing the file.

7. (Optional) Select the Remove Unusable check box. If selected, the modular input deletes a file after processing it if it has no actionable threat intelligence.

8. (Optional) Type a number to use as the default weight for all threat intelligence documents consumed from this directory.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Upload a custom CSV file of threat intelligence in Splunk Enterprise Security

You can add a custom file of threat intelligence to Splunk Enterprise Security.

Prerequisite

Format the custom CSV file by adding headers for each type of intelligence in the file. The custom file can contain multiple types of intelligence, but you must include headers for each column in the CSV file. See Supported types of threat intelligence in Splunk Enterprise Security for the headers relevant for each type of threat intelligence.

Add the custom file to Splunk Enterprise Security.
1. On the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Uploads**.

2. Type a file name for the file you want to upload. The file name you type becomes the name of the file saved to

   
   $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel.

   The file name cannot include spaces or special characters.

3. Upload the CSV-formatted file.

4. Type a **Weight** for the threat list. The weight of a threat file increases the risk score of objects associated with threat intelligence on this list.

5. (Optional) Type a **Threat Category**.

6. (Optional) Type a **Threat Group**.

7. (Optional) Select the **Overwrite** check box. If you have previously uploaded a file with the same file name, select this check box to overwrite the previous version of the file.

8. (Optional) Select the **Sinkhole** check box. This deletes the file after the intelligence from the file is processed.

9. Click **Save**.

**Next step**

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

**Add threat intelligence from Splunk events in Splunk Enterprise Security**

You can add threat intelligence from Splunk events to the local threat intelligence lookups.

1. Write a search that produces threat indicators.

2. Add `| outputlookup local_<threat intelligence type>_intel append=t` to the end of the search.

For example, write a search that produces a list of IP addresses that are testing a web server for vulnerabilities and add them to the `local_ip_intel` lookup to be processed by the modular input and added to the `ip_intel` KV Store collection.
Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add and maintain threat intelligence locally in Splunk Enterprise Security

Each threat collection has a local lookup file that you can use to manually add threat intelligence.

1. On the Enterprise Security menu bar, select Configure > Content > Content Management.
2. Find the local lookup that matches the type of threat indicator you want to add. For example, Local Certificate intel to add information about malicious or spoofed certificates.
3. Click the lookup name to edit the lookup.
4. Add indicators to the lookup. Right-click and select Insert Row Below to add new rows as needed.
5. (Optional) Type a numeric Weight to change the risk score for objects associated with indicators on this threat intelligence source.
6. Click Save.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add threat intelligence with a custom lookup file in Splunk Enterprise Security
You can add threat intelligence to Splunk Enterprise Security as a custom lookup file. Add a custom lookup file in this way if you want to edit the lookup file in Splunk Enterprise Security. If you want to add a lookup file to have the intelligence in it extracted once, upload the CSV file instead. See Upload a custom CSV file of threat intelligence in Splunk Enterprise Security.

A lookup-based threat source can add data to any of the supported threat intelligence types, such as file or IP intelligence. See Supported types of threat intelligence in Splunk Enterprise Security.

Prerequisite

Create the custom CSV file. The custom file can contain multiple types of intelligence, but you must include headers for each column in the CSV file. See Supported types of threat intelligence in Splunk Enterprise Security for the headers relevant for each type of threat intelligence.

Steps

First, add the lookup to Splunk Enterprise Security.

1. Select Configure > Content > Content Management.
2. Select Create New Content > Lookup.
3. Click Create New.
4. Select the lookup file to upload.
5. Select an App of SA-ThreatIntelligence.
6. (Optional) Modify the file name. For example, type threatindicatorszerodayattack.csv.
7. (Optional) Modify the definition name. For example, zero_day_attack_threat_indicators_list.
8. Leave the default lookup type of Manual editing.
9. Type a label for the lookup. The label appears as the name for the lookup on the Content Management page. For example, Zero Day Threat Indicators.
10. Type a description for the lookup. For example, File-based threat indicators from zero day malware.
11. Save.

Next, add a threat source input stanza that corresponds to the lookup file so that ES can parse the threat intelligence.

1. Select Configure > Data Enrichment > Intelligence Downloads.
2. Click **New**.
3. Type a **Name**. The name cannot include spaces. For example, `zero_day_attack_threat_indicators`
4. Type a **Type**. For example, `zero_day_IOC`
5. Type a **Description**. For example, `File-based threat indicators from zero day malware`
6. Type a **URL** that references the lookup definition you created. For example, `lookup://zero_day_attack_threat_indicators_list`
7. (Optional) Change the default **Weight** for the threat data.
8. (Optional) Change the default **Retry interval** for the lookup.
9. If your lookup contains multiple types of threat intelligence, type the headers in the **Fields** section.
10. Save.

**Next step**

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

**Verify that you have added intelligence successfully to Splunk Enterprise Security**

After you add new intelligence sources or configure included intelligence sources, verify that the intelligence is being parsed successfully and that threat indicators are being added to the threat intelligence KV Store collections. The modular input responsible for parsing intelligence runs every 60 seconds.

**Verify that the intelligence source is being downloaded**

This verification procedure is relevant only for URL-based sources and TAXII feeds.

1. From the Enterprise Security menu bar, select **Audit > Threat Intelligence Audit**.
2. Find the intelligence source and confirm that the `download_status` column states **threat list downloaded**.
3. Review the **Intelligence Audit Events** to see if there are errors associated with the lookup name.

If the download fails, attempt the download directly from the terminal of the Splunk server using a curl or wget utility. If the intelligence source can be successfully downloaded using one of these utilities, but is not being downloaded successfully in Splunk Enterprise Security, ask your system administrator whether you need to specify a custom user-agent string to bypass network security controls in your environment. See step 10 in Add a URL-based threat source.

**Verify that threat indicators exist in the threat collections**

For threat intelligence sources, verify that the threat intelligence was successfully parsed and threat indicators exist in the threat collections.

1. Select **Security Intelligence > Threat Intelligence > Threat Artifacts**.
2. Search for the threat source name in the **Intel Source ID** field.
3. Confirm that threat indicators exist for the threat source.

**Troubleshoot parsing errors**

Review the following log files to troubleshoot errors that can occur when parsing intelligence sources in order to add them to Enterprise Security.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Suggestion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issues related to downloading intelligence sources.</td>
<td>Look at the Intelligence Audit Events panel on the Threat Intelligence Audit dashboard. Look for events from the threatlist.log file with the threatintel:download sourcetype.</td>
</tr>
<tr>
<td>Issues related to parsing or processing.</td>
<td>Look at the Intelligence Audit Events panel on the Threat Intelligence Audit dashboard. Look for events from the threat_intelligence_manager.log file with the threatintel:manager sourcetype.</td>
</tr>
<tr>
<td>Errors result from uploading a file.</td>
<td>Review the threat_intel_file_upload_rest_handler.log file.</td>
</tr>
<tr>
<td>Other parsing errors.</td>
<td>Verify that the modular inputs are running as expected. See python_modular_input.log for errors associated with modular input failures.</td>
</tr>
</tbody>
</table>
Change existing intelligence in Splunk Enterprise Security

After you add intelligence to Splunk Enterprise Security, you can make changes to the settings to make sure the intelligence you correlate with events is useful.

Disable an intelligence source

Disable an intelligence source to stop downloading information from the source. This also prevents new threat indicators from the disabled source from being added to the threat intelligence collections.

1. From the Enterprise Security menu bar, select Configure > Data Enrichment > Intelligence Downloads.
2. Find the intelligence source.
3. Under Status, click Disable.

Disable individual threat artifacts

To prevent individual threat artifacts on a threat list from creating notable events if they match events in your environment, disable individual threat artifacts. If you have command line access to the Enterprise Security search head, you can disable individual threat artifacts using the REST API. See Threat Intelligence API reference in Splunk Enterprise Security REST API Reference.

Edit an intelligence source

Change information about an existing intelligence source, such as the retention period or the download interval for the source.

1. From the Enterprise Security menu bar, select Configure > Data Enrichment > Intelligence Downloads.
2. Click the name of the intelligence source you want to edit.
3. Make changes to the fields as needed.
4. Save your changes.

By default, only administrators can edit intelligence sources. To allow non-admin users to edit intelligence sources, see Adding capabilities to a role in the Installation and Upgrade Manual.
Configure threat source retention

Remove threat intelligence from the KV Store collections in Splunk Enterprise Security based on the date that the threat intelligence was added to Enterprise Security.

The default maximum age is \(-30d\) for 30 days of retention in the KV Store. To remove the data more often, use a smaller number such as \(-7d\) for one week of retention. To keep the data indefinitely, use a blank field. However, if the KV Store collection is stored indefinitely, the .csv files that result from lookup-generating searches can grow large enough to impact search head cluster replication performance. If you manually delete the data from the .csv file, the maximum age timer does not reset based on the edit date, and the data is still removed from the KV Store after the maximum age expires.

1. If the threat intelligence source is not a TAXII feed, define the maximum age of the threat intelligence. This field is not used for TAXII feeds.
   1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
   2. Select an intelligence source.
   3. Change the **Maximum age** setting using a relative time specifier.
2. Enable the retention search for the collection.
   1. From the Splunk platform menu bar, select **Settings** and click **Searches, reports, and alerts**.
   2. Search for "retention" using the search filter.
   3. Enable the retention search for the collection that hosts the threat source. All retention searches are disabled by default.

Configure threat intelligence file retention

Configure how long files are stored by Splunk Enterprise Security after processing. Modular inputs managed on the Threat Intelligence Management page handle file parsing of intelligence sources. Modify the settings of the local modular inputs to manage global file retention for intelligence sources, or modify individual settings for each download or upload to more granularly control file retention.

Use the following table to determine the conditions under which Splunk Enterprise Security deletes a file after processing. For files placed into a directory by a script, for example, use the modular input sinkhole.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Sinkhole set for modular input</td>
<td>Sinkhole set for individual file</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>

*Remove files managed by a specific modular input*

Use the sinkhole or the remove unusable settings to selectively remove files managed by a modular input.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Select the modular input for the file retention settings that you want to modify.
   1. For downloaded files, select the `sa_threat_local` modular input.
   2. For uploaded files, select the `da_ess_threat_local` modular input.
3. Select the **Sinkhole** check box so that the modular input deletes each file in the directory after processing.
4. Select the **Remove Unusuable** check box so that the modular input deletes a file after processing if it has no actionable intelligence.
5. Save your changes.

*Remove files associated with a specific download*

Use the sinkhole check box to remove files associated with a threat intelligence download.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Intelligence Downloads**.
2. Locate the threat intelligence download.
3. Select the **Sinkhole** check box.
4. Save your changes.

*Remove files associated with a specific upload*

When you upload the file, select the sinkhole check box to delete the file after processing.

- See Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security.
See Upload a custom CSV file of threat intelligence in Splunk Enterprise Security.

Example: Add a ransomware threat feed to Splunk Enterprise Security

This example describes how to add a list of blocked domains that could host ransomware to Splunk Enterprise Security to better prepare your organization for a ransomware attack. The feed used in this example is from abuse.ch.

1. On the Enterprise Security menu bar, select Configure > Data Enrichment > Intelligence Downloads.
2. Click New to add a new threat intelligence source.
3. Type a Name of ransomware_tracker to describe the threat download source.
4. Type a Type of domain to identify the type of threat intelligence contained in the threat source.
5. Type a Description of Blocked domains that could host ransomware.
7. (Optional) Change the default Weight of 1 to 2 because ransomware is a severe threat and you want an extra risk score multiplier for assets or identities associated with blocked ransomware domains.
8. Leave the default Interval of 43200 seconds, or every 12 hours.
9. Leave the POST arguments field blank because this type of feed does not accept POST arguments.
10. Decide whether to define a Maximum age for the threat intelligence. According to the ransomware tracker website, items on the blocklist stay on the blocklist for 30 days. To drop items off the blocklist in Enterprise Security sooner than that, set a maximum age of less than 30 days. Type a maximum age of −7d.
11. Determine whether you need to specify a User agent string due to security controls in your environment. If not, leave this field blank.
12. Type a default Delimiting regular expression of : so that you can enrich the threat indicators by adding fields.
13. Leave the Extracting regular expression field blank because the domain names do not need to be extracted because they are line-delimited.
14. Type Fields of domain:$1,description:ransomware_domain_blocklist to define the fields in this blocklist.
15. (Optional) Leave the default Ignoring regular expressions field.
16. Change the **Skip header lines** field to 0 because the ignoring regular expression ignores the comments at the top of the feed.
17. Leave the **Retry interval** at the default of 60 seconds.
18. (Optional) Leave the **Remote site user** and **Remote site user realm** fields blank because this feed does not require any form of authentication.
19. Leave the **Retries** field at the default of 3.
20. Leave the **Timeout** field at the default of 30 seconds.
21. Ignore the **Proxy Options** section unless you are using a proxy server to add threat intelligence to Splunk Enterprise Security.
22. Click **Save**.
23. From the Splunk platform menu bar, select **Apps > Enterprise Security** to return to Splunk Enterprise Security.
24. From the Enterprise Security menu bar, select **Audit > Threat Intelligence Audit**.
25. Find the **ransomware_tracker** stanza in the **Threat Intelligence Downloads** panel and verify that the **status** is **threat list downloaded**.
26. From the Enterprise Security menu bar, select **Security Intelligence > Threat Intelligence > Threat Artifacts**.
27. Type an **Intel Source ID** of **ransomware_tracker** to search for domains added to Splunk Enterprise Security from the new threat feed.
28. Click **Submit** to search.
29. Click the **Network** tab and review the **Domain Intelligence** panel to verify that threat intelligence from the **ransomware_tracker** threat source appears.
Generic Intelligence

Add intelligence to Splunk Enterprise Security

As an ES administrator, you can use the threat intelligence framework in Splunk Enterprise Security to download and parse other forms of intelligence that you can use to correlate with events or enrich dashboards using search. Adding these generic forms of intelligence enhances your analysts’ security monitoring capabilities and adds context to their investigations.

Splunk Enterprise Security includes a few intelligence sources. Splunk Enterprise Security also supports adding other generic intelligence sources.

ES administrators can add generic intelligence to Splunk Enterprise Security by downloading a feed from the Internet.

1. Configure the intelligence sources included with Splunk Enterprise Security.
2. Download an intelligence feed from the Internet.
3. Verify that you have added intelligence successfully in Splunk Enterprise Security.
4. Use generic intelligence in search with inputintelligence.

Download an intelligence feed from the Internet in Splunk Enterprise Security

Splunk Enterprise Security can periodically download an intelligence feed available from the Internet and store it in the $SPLUNK_DB/modinput/threatlist directory. You can then use the inputintelligence search command to use the intelligence in reports, searches, or dashboards. See Example: Add a generic intelligence source to Splunk Enterprise Security.

1. (Optional) Configure a proxy for retrieving intelligence.
2. Add a URL-based intelligence source.

Configure a proxy for retrieving intelligence

If you use a proxy server to send intelligence to Splunk Enterprise Security, configure the proxy options for the intelligence source.
The user must correspond to the name of a Splunk secure stored credential in Credential Management. If you remove an existing proxy user and password in the Intelligence Download Setting editor, the download process no longer references the stored credentials. Removing the reference to the credential does not delete the stored credentials from Credential Management. For more information, see Manage credentials in Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select Configure > Data Enrichment > Intelligence Downloads.
2. Select the download source.
3. Configure the proxy options.
   1. Type a proxy server address. The Proxy Server cannot be a URL. For example, 10.10.10.10 or server.example.com.
   2. Type a proxy server port to use to access the proxy server address.
   3. Type a proxy user credential for the proxy server. Only basic and digest authentication methods are supported. The user must correspond to the name of a credential stored in Credential Management.
   4. (Optional) Type a proxy user realm for the proxy user credential. Use this to specify a proxy user realm for the user credential.
4. Save your changes.

Add a URL-based intelligence source

Add a non-TAXII source of intelligence that is available from a URL on the Internet. For an example of adding a URL-based generic intelligence source, see Example: Add a generic intelligence source to Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select Configure > Data Enrichment > Intelligence Downloads.
2. Type a Name for the download. The name can only contain alphanumeric characters, hyphens, and underscores. The name cannot contain spaces.
3. Click New to add a new intelligence source.
4. Do not select the check box for Sinkhole.
5. Deselect the check box for Is Threat Intelligence.
6. Type a Type for the download. The type identifies the type of information that the feed contains.
7. Type a Description. Describe the information in the feed.
8. Leave the default Weight because the field does not matter for the generic intelligence source.
9. (Optional) Change the default download Interval for the feed. Defaults to 43200 seconds, or every 12 hours.
10. (Optional) Type POST arguments for the feed. You can use POST arguments to retrieve user credentials from Credential Management. Use the format  
key=$user:<username>$ or  
key=$user:<username>,realm:<realm>$ to specify a username and realm.

11. Do not use the Maximum age setting.

12. (Optional) If you need to specify a custom User agent string to bypass network security controls in your environment, type it in the format  
$user-agent>/<version>$. For example, Mozilla/5.0 or AppleWebKit/602.3.12. The value in this field must match this regex:  
([A-Za-z0-9_.-]+)/([A-Za-z0-9_.-]+). Check with your security device administrator to ensure the string you type here is accepted by your network security controls.

13. Fill out the Parsing Options fields to make sure that your list parses successfully. You must fill out either a delimiting regular expression or an extracting regular expression. You cannot leave both fields blank.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delimiting regular expression</td>
<td>A regular expression string used to split, or delimit, lines in an intelligence source. For complex delimiters, use an extracting regular expression.</td>
<td>, or : or \t</td>
</tr>
<tr>
<td>Extracting regular expression</td>
<td>A regular expression used to extract fields from individual lines of an intelligence source document. Use to extract values in the intelligence source.</td>
<td>^(\S+)\t+(\S+)\t+S+\t+S+\t+S+</td>
</tr>
<tr>
<td>Fields</td>
<td>Required if your document is line-delimited. Comma-separated list of fields to be extracted from the intelligence list. Can also be used to rename or combine fields. Description is a required field. Additional acceptable fields are the fields in the corresponding KV Store collection for the threat intelligence, visible in the local lookup files or the DA-ESS-ThreatIntelligence/collections.conf file. Defaults to description:$1,ip:$2.</td>
<td>&lt;fieldname&gt;:$&lt;number&gt;,&lt;fieldname&gt;$&lt;number&gt; ip:$1,description:domain_blocklist</td>
</tr>
<tr>
<td>Ignoring regular expression</td>
<td>A regular expression used to ignore lines in an intelligence source. Defaults to ignoring blank lines and comments that begin with #.</td>
<td>^\s*$)</td>
</tr>
<tr>
<td>Skip header lines</td>
<td>The number of header lines to skip when processing the intelligence source.</td>
<td>0</td>
</tr>
</tbody>
</table>

latin1
### Field Description Example

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence file encoding</td>
<td>If the file encoding is something other than ASCII or UTF8, specify the encoding here. Leave blank otherwise.</td>
<td></td>
</tr>
</tbody>
</table>

14. (Optional) Change the **Download Options** fields to make sure that your list downloads successfully.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry interval</td>
<td>Number of seconds to wait between download retry attempts. Review the recommended poll interval of the intelligence source provider before changing the retry interval.</td>
<td>60</td>
</tr>
<tr>
<td>Remote site user</td>
<td>If the threat feed requires authentication, type the user name to use in remote authentication, if required. The user name you add in this field must match the name of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.</td>
<td>buttercup</td>
</tr>
<tr>
<td>Remote site user realm</td>
<td>If the threat feed requires authentication, type the user name to use in remote authentication, if required. The realm you add in this field must match the realm of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.</td>
<td>paddock</td>
</tr>
<tr>
<td>Retries</td>
<td>The maximum number of retry attempts.</td>
<td>3</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds to wait before marking a download attempt as failed.</td>
<td>30</td>
</tr>
</tbody>
</table>

15. (Optional) If you are using a proxy server, fill out the **Proxy Options** for the feed. See Configure a proxy for retrieving intelligence.

16. Save your changes.

If you are finished adding intelligence sources, see Verify that you have added intelligence successfully in Splunk Enterprise Security.

### Use generic intelligence in search with inputintelligence

After you add generic intelligence to Splunk Enterprise Security, you can use the `inputintelligence` command to make use of the intelligence. See Add generic
Use the `inputintelligence` command to add intelligence from the threatlist directory to your search results. When downloaded, generic intelligence is parsed and stored in the `$SPLUNK_DB/modinputs/threatlist$` directory.

**Syntax**

```
| inputintelligence <threatlist_stanza_name> [fields=<string>] [delim_regex=<string>] [extract_regex=<string>] [ignore_regex=<string>] [skip_header_lines=<int>] [include_raw=<bool>] [append=<bool>] [no_parse=<bool>]
```

**Required arguments**

**threatlist_stanza_name**

Syntax: `<string>`
Description: The stanza of the intelligence download. Matches the **Name** field on the Intelligence Downloads page. You can include multiple stanza names in your search. See Download an intelligence feed from the Internet in Splunk Enterprise Security.

**Optional arguments**

**fields**

Syntax: `<string>`
Description: Overrides the default fields setting for the intelligence download defined in the Intelligence Download page. Required if your document is line-delimited. Comma-separated list of fields to be extracted from the intelligence list. Can also be used to rename or combine fields. Description is a required field. Additional acceptable fields are the fields in the corresponding KV Store collection for the threat intelligence, visible in the local lookup files or the DA-ESS-ThreatIntelligence/collections.conf file. Defaults to `description:$1,ip:$2`.

**delim_regex**

Syntax: `<string>`
**Description**: Overrides the default delimiting regular expression setting for the intelligence download defined in the Intelligence Download page. A regular expression string used to split, or delimit, lines in an intelligence source. For complex delimiters, use an extracting regular expression.

**extract_regex**

**Syntax**: <string>

**Description**: Overrides the default extracting regular expression setting for the intelligence download defined in the Intelligence Download page. A regular expression used to extract fields from individual lines of an intelligence source document. Use to extract values in the intelligence source.

**ignore_regex**

**Syntax**: <string>

**Description**: Overrides the default ignore regular expression setting for the intelligence download defined in the Intelligence Download page. A regular expression used to ignore lines in an intelligence source. Defaults to ignoring blank lines and comments that begin with #.

**skip_header_lines**

**Syntax**: <int>

**Description**: Overrides the default skip header lines setting for the intelligence download defined in the Intelligence Download page. The number of header lines to skip when processing the intelligence source. 
**Default**: 0

**include_raw**

**Syntax**: <bool>

**Description**: If 1, t, or true, adds the original line content to an additional column called raw. 
**Default**: 0

**append**

**Syntax**: <bool>

**Description**: If 1, t, or true, appends the results of the inputintelligence command to an existing set of search results instead of replacing it. 
**Default**: 0
no_parse

Syntax: <bool>
Description: If 1, t, or true all other options are ignored and the raw contents of the intelligence file is returned one line per row.
Default: 0

Usage

The inputintelligenc e command is a transforming command.

Examples

1. View the top one million sites

View the top one million sites according to Cisco.

inputintelligence cisco_top_one_million_sites

2. Further examples

See Example: Add a generic intelligence source to Splunk Enterprise Security.

See also

inputlookup

Example: Add a generic intelligence source to Splunk Enterprise Security

As a security analyst, you want to compare hosts seen in your network with the hosts associated with Spotify advertisements so that you can assess the risk that listening to Spotify Free during the work day poses to your network. The hosts associated with Spotify ads are not malicious, and you do not want to add them to Splunk Enterprise Security as threat intelligence. Instead, you can add them as generic intelligence.

Download the generic intelligence

First, create a download configuration for the list.
1. Select **Configure > Data Enrichment > Intelligence Downloads.**
2. Click **New.**
3. Type a **Name** of **spotify_ads.**
4. Deselect the check box for **Is Threat Intelligence.**
5. Type a **Type** of **spotify_ads.**
6. Type a **Description** of Hostnames of machines hosting Spotify ads.
7. Type a URL of **https://raw.githubusercontent.com/FadeMind/hosts.extras/master/StreamingAds/hosts.**
8. (Optional) Change the default **Weight.**
9. (Optional) Change the default **Interval.**
10. Type a delimiting regular expression of **\s.**
11. Type **Fields** of **url:$2.**
12. Type an **Ignoring regular expression** of (**^#|^\s*$).**
13. Save.

**Verify that the intelligence downloads successfully**

Using search, verify that the modular input is downloading information from the source.

```
| inputintelligence no_parse=1 spotify_ads
```

**Verify that the intelligence parses correctly**

Use the custom search command **inputintelligence** to verify that the intelligence parses correctly.

```
| inputintelligence spotify_ads
```

If the intelligence does not seem to be parsing correctly, review **search.log** for any error messages. In addition, you can change the parsing settings for the download using the optional arguments for the **inputintelligence** command to determine the correct settings. See **Use generic intelligence in search with inputintelligence.**

**Use the new intelligence source in a search**

You can use the new intelligence source in many ways in searches.

**Use Spotify ads in a subsearch**

To return 100 URLs used by Spotify ads in a list with the following subsearch:
| search [ | inputintelligence spotify_ads | return 100 url |

**Use Spotify ads in join**

Join the hosts in the Spotify ads intelligence source with another set of data with `join`:

```plaintext
... | join url [ | inputintelligence spotify_ads | eval spotify_ad="true"] | search spotify_ad="true"
```

**Add Spotify ads to a lookup table file**

Add the hosts from Spotify ads to a lookup table file using a lookup generating search:

```plaintext
| inputintelligence spotify_ads | eval spotify_ad="true" | outputlookup spotify_ads.csv
```

After creating the lookup, use it in search with the following example search:

```plaintext
... | lookup spotify_ads.csv url OUTPUT spotify_ad | search spotify_ad="true"
```
Managing Content

Managing content in Splunk Enterprise Security

As a Splunk Enterprise Security administrator, you can use the Content Management page to display, create, configure, and edit content that is unique to Splunk Enterprise Security, such as correlation searches, key indicators, saved searches, and swim lane searches.

- Create correlation searches in Splunk Enterprise Security
- Create and manage data models in Splunk Enterprise Security
- Create and manage key indicator searches in Splunk Enterprise Security
- Create and manage lookups in Splunk Enterprise Security
- Create and manage saved searches in Splunk Enterprise Security
- Create and manage search-driven lookups in Splunk Enterprise Security
- Create and manage swim lane searches in Splunk Enterprise Security
- Create and manage views in Splunk Enterprise Security
- Export content from Splunk Enterprise Security as an app

See also

- Create and edit risk objects in Splunk Enterprise Security

Create and manage data models in Splunk Enterprise Security

Create and manage data models using the Content Management page in Splunk Enterprise Security.

- Review the list of data models in Splunk Enterprise Security.
- Review the next scheduled time, acceleration status, and choose whether or not to accelerate a data model.
- Click a data model name to edit the data model.

Create a data model

1. From the Enterprise Security menu bar, select Configure > Content > Content Management.
2. Click Create New Content and select Data Model.
3. Create a data model following the instructions in the Splunk platform documentation.
   ♦ For Splunk Enterprise, see Create a data model in the Splunk Enterprise Knowledge Manager Manual.
   ♦ For Splunk Cloud, see Create a data model in the Splunk Cloud Knowledge Manager Manual.

Create and manage key indicator searches in Splunk Enterprise Security

Configure key indicator searches on Content Management in Splunk Enterprise Security. Use the filters to select a type of key indicator to view only key indicator searches.

Create a custom key indicator search

Create a key indicator search to create a key indicator that you can add to a dashboard or glass table as a security metric.

1. From the Enterprise Security menu bar, select Configure > Content > Content Management.
2. Click Create New Content and select Key Indicator Search.
3. Type a key indicator name.
   In order for the key indicator to show up in the list of security metrics on glass table, type a category or security domain at the beginning of the key indicator name followed by a hyphen. For example, APT - Example Key Indicator or Access - Sample Key Indicator.
4. Type a search, and other details.
   The key indicators that come with Enterprise Security use data models to accelerate the return of results.
5. (Optional) Select Schedule to use data model acceleration for your custom key indicator.
6. Type the name of the field that corresponds to the value of the key indicator in the Value field.
7. Type the name of the field that corresponds to the change in the key indicator in the Delta field.
8. (Optional) Type a Threshold for the key indicator. The threshold controls whether the key indicator changes color. You can also set the threshold in dashboards and on glass tables.
9. Type a Value Suffix to indicate units or another word to follow the key indicator.
10. Select the Invert check box to invert the colors of the key indicator. Select this check box to indicate that a high value is good and a low value is bad.

11. Click Save.

**Schedule a key indicator search**

Key indicators included with Splunk Enterprise Security use data model acceleration. Enable acceleration and schedule the search to run as a scheduled report. Scheduled report results are cached, allowing the indicator to display results on the dashboard more quickly.

1. Select Configure > Content > Content Management.
2. Locate the key indicator search that you want to accelerate.
3. Click Accelerate in the Actions column.
4. In the Edit Acceleration window, select the Accelerate check box.
5. Select a Refresh Frequency for how often Enterprise Security should update the cached results.
6. Click Save.

After a key indicator is accelerated, the Next Scheduled Time populates on the Content Management page and the lightning bolt for that indicator changes from grey to yellow.

**Edit a key indicator search**

Make changes to a key indicator search.

1. From the ES menu bar, select Configure > Content > Content Management
2. Select a key indicator search.
3. (Optional) Change the search name.
4. (Optional) Change the destination app where the search is stored.
5. (Optional) Change the title of the key indicator. The title appears above the key indicator on a dashboard, or next to the security metric on a glass table.
6. (Optional) Change the sub-title of the key indicator that is used to describe the type of the key indicator function on dashboards.
7. (Optional) Change the search string that populates the key indicator.
8. (Optional) Add a drilldown URL such as a custom search or dashboard link to override the default drilldown behavior. By default, the key indicator drilldown opens the search results that produced the key indicator value. For key indicators on glass tables, you can set a custom drilldown when you add the key indicator to the glass table.
9. (Optional) Select the **Schedule** check box to enable acceleration for a key indicator and allow it to load faster on a dashboard.

10. (Optional) Change the **Cron Schedule** frequency using standard cron notation.

11. (Optional) Change the **Threshold** behavior to determine the color assigned to the value indicator. By default, no threshold produces a black value indicator, a threshold number higher than the count of a value indicator produces a green value indicator, and a threshold number lower than the count of a value indicator produces a red value indicator.

12. (Optional) Add a **Value suffix** to describe the value indicator. For example, specify units. On dashboards, the value suffix appears between the value indicator and the trend indicator.

13. (Optional) Select the **Invert** check box to change the default colors of the trend indicator threshold. If this check box is selected, a threshold number higher than the count of a value indicator produces a red value indicator, and a threshold number lower than the count of a value indicator produces a green value indicator.

14. Click **Save**.

### Create and manage saved searches in Splunk Enterprise Security

Create a saved search, also called a scheduled report, in Splunk Enterprise Security.

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **Saved Search**.
3. Create a saved search, also called a scheduled report, following the instructions in the Splunk platform documentation.
   - For Splunk Enterprise, see Create a new report in the Splunk Enterprise Reporting Manual.
   - For Splunk Cloud, see Create a new report in the Splunk Cloud Reporting Manual.
4. Modify the permissions of the report to share it with Enterprise Security so that you can view and manage the search in Enterprise Security, following the instructions in the Splunk platform documentation.
   - For Splunk Enterprise, see Set report permissions in the Splunk Enterprise Reporting Manual.
   - For Splunk Cloud, see Set report permissions in the Splunk Cloud Reporting Manual.
Create and manage search-driven lookups in Splunk Enterprise Security

A search-driven lookup lets you create a lookup based on the results of a search that runs at regular scheduled intervals. The search can run only against data stored in data models or in an existing lookup. Lookups created as search-driven lookups are excluded from bundle replication and are not sent to the indexers.

When to use search-driven lookups

Create a search-driven lookup if you want to know when something new happens in your environment, or need to consistently update a lookup based on changing information from a data model or another lookup.

The search-driven lookup collects and stores information from data models or other lookups. The data stored in the lookup represents a historical summary of selected fields gathered from events. You can view changes on a dashboard or use a correlation search to compare data from the search-driven lookup with new events, and alert if there is a match. For example, to find out when a new user logs in to a web server.

1. Search for user data in the Authentication data model and filter by the web server host name with the where command.
2. Verify the search results match the known hosts and users in your environment.
3. Create a guided search-driven lookup to collect and store information on a recurring schedule about users logging in to the web servers.
4. Create a correlation search that alerts you when a user logs in to one of the web servers that he or she has not accessed in the past, based on the historical information in the search-driven lookup.

Create a search-driven lookup

When you create a search-driven lookup, two knowledge objects are created. One knowledge object is the lookup that is generated by the search, while the other knowledge object is the search that drives the lookup.

Create a search-driven lookup as follows:

1. From the Splunk Enterprise Security menu bar, select Configure > Content > Content Management.
2. Click Create New Content and select Search-Driven Lookup.
3. (Optional) Select an App. The default app is SplunkEnterpriseSecuritySuite. You can create the lookup in a specific app, such as SA-NetworkProtection, or a custom app. You cannot change the app after you save the search-driven lookup.

4. (Optional) Type a description for the search.

5. Type a label for the lookup. This is the name of the search-driven lookup that appears on Content Management.

6. Type a name for the lookup. After you save the lookup, the name cannot be changed.

7. Type a cron schedule to define how often you want the search to run.

8. Select real-time or continuous scheduling for the search. Real-time scheduling prioritizes search performance, while continuous scheduling prioritizes data integrity.

9. Type a Search Name to define the name of the saved search. After you save the lookup, the name cannot be changed.

10. Select a mode of Guided to create a search without having to write the search syntax yourself, or select Manual to write your own search. See the example for help building a search with the guided search editor.

11. If you create a search in manual mode, type a search.

12. Click Save to save the search.

Example search-driven lookup

In this example search-driven lookup included with Splunk Enterprise Security, you want to track attacks identified by your intrusion detection system (IDS). You can then be notified of new attacks with a correlation search, or determine whether an attack is new to your environment or not. The Intrusion Center dashboard uses this search-driven lookup for the New Attacks - Last 30 Days panel. See Intrusion Center dashboard.

1. From the Splunk Enterprise Security menu bar, select Configure > Content > Content Management.

2. Click Create New Content and select Search-Driven Lookup.

3. (Optional) Select an App of SA-NetworkProtection. You cannot change the app after you save the search-driven lookup.

4. Type a description of "Maintains a list of attacks identified by an IDS and the first and last time that the attacks were seen."

5. Type a label of IDS Attack Tracker Example for the lookup. This is the name of the search-driven lookup that appears on Content Management.

6. Type a unique and descriptive name for the lookup of ids_attack_tracker_example. After you save the lookup, the name cannot be changed.
7. Type a cron schedule to define how often you want the search to run. If your IDS collects data often, type a cron schedule of 25 * * * * to run the search at 25 minutes every hour every day.
8. Select a Continuous Schedule because the lookup must track all data points.
9. Type a **Search Name** of *Network - IDS Attack Tracker - Example Lookup Gen*.
10. Select guided mode to use the guided search editor to create the search.
11. Click **Open guided search editor** to start creating the search.
12. Select a data source of **Data Model** because the IDS Attack data is stored in a data model.
13. Select a data model of *Intrusion_Detection* and a data model dataset of *IDS_Attacks*.
14. Select **Yes** for the summaries only field to run the search against only the data in the accelerated data model.
15. Select a time range that uses Relative time that begins with an earliest time of 70 minutes ago, starting at the beginning of the minute, and ends now. Click **Apply** to save the time range.
16. Click **Next**.
17. (Optional) Type a where clause to filter the data from the data model to only the data from a specific IDS vendor and click **Next**.
18. Add aggregate values to track specific statistics about the data and store that information in the lookup. At least one aggregate is required.
   1. To track the first time that an IDS attack was seen in your environment, add a new aggregate with a function of **min** and a field of _time and save it as **firstTime**.
   2. Track the last time an attack was seen by adding another aggregate with a **max** function and a field of _time and saving it as **lastTime**. This creates two columns in the lookup, firstTime and lastTime.
19. Add split-by clauses to track more data points in the lookup. All split-by clauses appear as columns in the lookup.
   1. Add a split-by clause of **IDS_Attacks.ids_type** and rename it as **ids_type** to monitor the IDS type in the lookup.
   2. Add a split-by clause to rename IDS_Attacks.signature as **signature**.
   3. Add a split-by clause to rename IDS_Attacks.vendor_product as **vendor_product**.
20. Click **Next**.
21. Select a retention period that defines the age of the data to be stored in the lookup. For example, you want to keep 5 years of IDS attack evidence stored in this lookup. Select a time field of **lastTime** to base the retention on the last time an attack was identified by the IDS. Type an earliest time
of -5y and indicate the format of the time value that you entered: %s. You can find guidance on the time format in the Splunk platform documentation.

- For Splunk Enterprise, see Date and time format variables in the Splunk Enterprise Search Reference manual.
- For Splunk Cloud, see Date and time format variables in the Splunk Cloud Search Reference manual.

22. Click Next.
23. Review the search created by the wizard and click Done to finish using the guided search editor.
24. Click Save to save the search.

Modify a search-driven lookup

Since a search-driven lookup contains the two knowledge objects of search and lookup, there are two ways to modify it. Both ways will open the search-driven lookup editor.

Modify the search-driven lookup as follows:

1. From the Splunk Enterprise Security menu bar, select Configure > Content > Content Management.
2. Select a Type of Search-Driven Lookup.
3. Click the lookup that you want to edit.
4. Make changes and click Save.

Modify the lookup generating search as follows:

1. From the Splunk Enterprise Security menu bar, select Configure > Content > Content Management.
2. Select a Type of Lookup Generating Search.
3. Click the lookup that you want to edit.
4. Make changes and click Save.

Enable or disable the search populating a search-driven lookup

You can enable or disable the search of a search-driven lookup to prevent the search from updating the lookup. If you disable the search that populates a search-driven lookup, the search stops updating the lookup and the data in the
lookup will stop being updated. Correlation searches or dashboards that rely on the data inside the lookup will be out-of-date.

1. Select Configure > Content > Content Management.
2. Filter on a type of search-driven lookup and open the search-driven lookup that you want to enable or disable.
3. Find the Search name of the search-driven lookup.
4. From the Splunk platform menu bar, select Settings > Searches, reports, alerts.
5. (Optional) Filter by Type and App of All.
6. Find the search and enable or disable it.

Create and manage swim lane searches in Splunk Enterprise Security

Create a swim lane search to create a swim lane that you can add to the Asset Investigator or Identity Investigator dashboard. Swim lanes on the investigator dashboards help you profile activity by a specific asset or identity over time.

1. From the Enterprise Security menu bar, select Configure > Content > Content Management.
2. Click Create New Content and select Swim Lane Search.
3. Type a Search Name.
4. Select a Destination App.
5. Type a Title for the swim lane that appears on the dashboard.
6. Type a Search that populates the swim lane.
7. Type a Drilldown Search that runs when a user clicks a swim lane item. By default, the swim lane item drilldown shows the raw events.
8. Select a color.
9. Select an Entity Type of Asset or Identity.
10. Type Constraint Fields. Type a field to specify constraints on the search. Your search must contain where $constraints$ to use these constraint fields in the search. Only specific constraints are valid for each type of swim lane search. For example, an Asset Investigator swim lane search using the Malware data model and the Malware_Attacks data model dataset could specify the Malware_Attacks.user field as a constraint.
11. Click Save.
Example

For example, create a swim lane to identify all authentication events involving a specific asset.

1. Type a **Search Name** of *Authentication by Asset - Example*
2. Select a **Destination App** of *DA-ESS-AccessProtection.*
3. Type a **Title** for the swim lane that appears on the dashboard. *All Authentication.*
4. Type a **Search** that populates the swim lane.

   ```
   | tstats `summariesonly` values(Authentication.action) as action,values(Authentication.app) as app,values(Authentication.src) as src,values(Authentication.dest) as dest,values(Authentication.user) as user,count from datamodel=Authentication.Authentication where $constraints$ by _time span=$span$
   ```
5. Type a **Drilldown Search.**

   ```
   | `datamodel("Authentication","Authentication")` | search $constraints$
   ```
6. **Select the color Purple.**
7. **Select an entity type of Asset** because you want to investigate all authentication events by asset and be able to add this swim lane to the Asset Investigator dashboard. With this specified, all constraints specified as constraint fields perform a reverse lookup against the other fields that identify an asset.
8. **Type constraint fields of Authentication.src and Authentication.dest to identify authentications originating from or targeting a specific asset.**

Assuming an asset lookup entry with an IP address of 1.2.3.4, dns of server.example.com, and nt_host of server1, the search for this swim lane searches for all authentication events where the source or destination of the authentication event is 1.2.3.4, server.example.com, or server1.

   ```
   ... Authentication.src=1.2.3.4 OR Authentication.src=server.example.com OR Authentication.src=server1 OR Authentication.dest=1.2.3.4 OR Authentication.dest=server.example.com OR Authentication.dest=server1
   ```

Create and manage views in Splunk Enterprise Security

Create a new view or dashboard using Simple XML from Content Management.
**Prerequisite**

Creating new views and dashboards from Content Management requires familiarity with Simple XML. For an overview of building and editing dashboards, including working with Simple XML, see the Splunk platform documentation.

- For Splunk Enterprise, see Dashboard overview in Splunk Enterprise *Dashboards and Visualizations*.
- For Splunk Enterprise, see Dashboard overview in Splunk Enterprise *Dashboards and Visualizations*.

**Task**

1. From the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content** and select **View**.
3. Create a new dashboard with Simple XML.
4. Modify the permissions to share the new view with Enterprise Security so that you can view and manage it in Enterprise Security.
   1. From the Splunk bar, select **Settings > User interface > Views**.
   2. Locate the **View name** that you created.
   3. Click **Permissions** and modify the permissions to share the view with Enterprise Security.
   4. Click **Save**.

You can also create a new dashboard with the interactive dashboard editor. Select **Search > Dashboards** to open the Dashboards page. You can find information about the Dashboard Editor in the Splunk platform documentation.

- For Splunk Enterprise, see Open the Dashboard Editor in Splunk Enterprise *Dashboards and Visualizations*.
- For Splunk Cloud, see Open the Dashboard Editor in Splunk Cloud *Dashboards and Visualizations*.

Use the Navigation editor to change which dashboards are visible on the menu in your deployment. For more information, see Customize the menu bar in Splunk Enterprise Security.

**Export content from Splunk Enterprise Security as an app**
Export content from Splunk Enterprise Security as an app from the Content Management page. Use the export option to share custom content with other ES instances, such as migrating customized searches from a development or testing environment into production. You can export any type of content on the Content Management page, such as correlation searches, glass tables, data models, and views.

By default, only admin users can export content. To add the export capability to another role, see Adding capabilities to a role in the Installation and Upgrade Manual.

1. From the ES menu bar, select Configure > Content > Content Management.
2. Select the check boxes of the content you want to export.
3. Click Edit Selection and select Export.
4. Type an App name. This will be the name of the app in the file system. For example, SOC_custom.
5. Select an App name prefix. If you want to import the content back into Splunk Enterprise Security without modifying the default app import conventions, select DA-ESS-. Otherwise, select No Prefix.
6. Type a Label. This is the name of the app. For example, Custom SOC app.
7. Type a Version and Build number for your app.
8. Click Export.
9. Click Download app now to download the app package to the search head at the location $SPLUNK_HOME/etc/apps/SA-Utils/local/data/appmaker/*.
10. Click Close to return to Content Management.

Limitations to exported content

Exported content may not work on older versions of Enterprise Security. The following items are included or not included in exported content.

<table>
<thead>
<tr>
<th>Exported item</th>
<th>Included in export</th>
<th>Not included in export</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data models</td>
<td>datamodels.conf and data model JSON definition.</td>
<td>N/A</td>
</tr>
<tr>
<td>Saved searches, including correlation, key indicator, and swim lane</td>
<td>savedsearches.conf governance.conf Alert actions and response actions, including risk assignments, script names, and</td>
<td>Macros, script files, lookups, or any binary files referenced by the search object. Extreme Search objects, such as</td>
</tr>
</tbody>
</table>
Create and manage lookups in Splunk Enterprise Security

Splunk Enterprise Security provides lookups to manage asset and identity correlation with events, match threat indicators with events, and enrich dashboards and panels with information.

As an administrator, you can add lookups to Splunk Enterprise Security. After you add lookups to Splunk Enterprise Security, you can use the lookups in searches, edit them, add descriptions, and export them.

Add a lookup to Splunk Enterprise Security

Upload and create a lookup in Splunk Enterprise Security.

1. Select Configure > Content > Content Management.
2. Click Create New Content > Managed Lookup.
3. Click Create New.
4. Select a lookup file to upload.

<table>
<thead>
<tr>
<th>Exported item</th>
<th>Included in export</th>
<th>Not included in export</th>
</tr>
</thead>
<tbody>
<tr>
<td>searches</td>
<td>email addresses.</td>
<td>the context generating search, the contexts, or the concepts referenced by the search object.</td>
</tr>
<tr>
<td>Search-driven lookups</td>
<td>savedsearches.conf</td>
<td>Macros, script files, lookups, or any binary files referenced by the search object.</td>
</tr>
<tr>
<td></td>
<td>governance.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>managed_configurations.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>collections.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transforms.conf</td>
<td></td>
</tr>
<tr>
<td>Managed lookups</td>
<td>The lookup CSV file.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>managed_configurations.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>collections.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transforms.conf</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Views</td>
<td>The XML or HTML, CSS, and JS files for the view.</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Sequence Template</td>
<td>app.conf and sequence_templates.conf for all the selected templates.</td>
<td>The sequenced events themselves are not exported, but saved in the sequenced_events index.</td>
</tr>
</tbody>
</table>
5. (Optional) Change the default App for the file.
6. (Optional) Modify the file name.
7. (Optional) Modify the definition name.
8. (Optional) Change the default lookup type.
9. Type a label for the lookup. The label appears as the name for the lookup on the Content Management page.
10. Type a description for the lookup.
11. (Optional) Change the option to allow editing of the lookup file.
12. Click Save.

Add an existing lookup to Splunk Enterprise Security

If the lookup file and definition already exists in the Splunk platform, you can add it to Splunk Enterprise Security so that you can edit it.

1. Select Configure > Content > Content Management.
2. Click Create New Content > Managed Lookup.
3. Click Select Existing.
4. Select the lookup definition from the drop-down list.
5. (Optional) Modify the lookup type.
6. Type a label for the lookup. The label appears as the name for the lookup on the Content Management page.
7. Type a description for the lookup.
8. (Optional) Change the option to allow editing of the lookup file.
9. Click Save.

Verify that you added a lookup successfully

Confirm that you added a lookup file successfully by using the inputlookup search command to display the list. For example, to review the application protocols lookup:

```
| inputlookup append=T application_protocol_lookup
```

Edit a lookup in Splunk Enterprise Security

Only users with appropriate permissions can edit lookups. See Manage permissions in Splunk Enterprise Security. Lookups do not accept regular expressions, and the lookup editor does not validate the accuracy of your entries. You cannot save a lookup file with empty header fields.
Stop managing a lookup

You can stop managing a lookup on the Content Management page by clicking **Stop managing**. When you stop managing a lookup, you can no longer edit the lookup from Splunk Web but the lookup is not deleted.

Export a lookup in Splunk Enterprise Security

1. On Content Management, locate the lookup that you want to export.
2. Under the Actions column, click **Export** to export a copy of the file in CSV format.

You can export multiple lookup files and other knowledge objects as part of an app. See Export content from Splunk Enterprise Security as an app in *Administer Splunk Enterprise Security*.

Audit changes made to lookup files

To review the last time a lookup file was edited and by whom, use a search. For example:

```
index=_internal
```

Manage internal lookups in Splunk Enterprise Security

Splunk Enterprise Security provides and maintains internal lookups to support dashboards, searches, and other internal processes.

These lookups are created in several ways.

- Populated by a static lookup table
- Populated internally by search commands, called a search-driven lookup
- Populated with information from the Internet

The internal lookups populated with information from the Internet are used by some correlation searches to identify hosts that are recognized as malicious or suspicious according to various online sources, such as the SANS Institute. If Splunk Enterprise Security is not connected to the Internet, these lookup files are not updated and the correlation searches that rely on the lookups might not
function correctly. Most of the internal lookups populated by the Internet are threat intelligence sources. See Configure the threat intelligence sources included with Splunk Enterprise Security in this manual.

Select Configure > Content > Content Management to view the existing lookups that you can edit in Splunk Enterprise Security.

Splunk Enterprise Security uses the internal lookups in different ways.

<table>
<thead>
<tr>
<th>Lookup type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td>Small, relatively static lists used to enrich dashboards.</td>
<td>Categories</td>
</tr>
<tr>
<td>Asset or identity list</td>
<td>Maintained by a modular input and searches. See How Splunk Enterprise Security processes and merges asset and identity data.</td>
<td>Assets</td>
</tr>
<tr>
<td>Threat intelligence collections</td>
<td>Maintained by several modular inputs. See Threat intelligence framework in Splunk ES on the Splunk developer portal.</td>
<td>Local Certificate Intel</td>
</tr>
<tr>
<td>Tracker</td>
<td>Search-driven lookups used to supply data to dashboard panels.</td>
<td>Malware Tracker</td>
</tr>
<tr>
<td>Per-panel filter lookup</td>
<td>Used to maintain a list of per-panel filters on specific dashboards.</td>
<td>HTTP Category Analysis Filter</td>
</tr>
</tbody>
</table>

**Internal lookups that you can modify**

Some lookups are managed by searches (search-driven lookups), and others you update manually. This table lists the lookups that you might need to modify in Splunk Enterprise Security.

<table>
<thead>
<tr>
<th>Lookup name</th>
<th>Type</th>
<th>Description</th>
<th>Usage details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action History Search Tracking Whitelist</td>
<td>List</td>
<td>Add searches to this whitelist to prevent them from creating action history items for investigations.</td>
<td>Type a start_time of 1 to whitelist the search. Type a start_time and an end_time to whitelist the search for a specific period of time.</td>
</tr>
<tr>
<td>Administrative Identities</td>
<td>List</td>
<td>You can use this lookup to identify</td>
<td>Modify the category column to indicate the</td>
</tr>
</tbody>
</table>
privileged or administrative identities on relevant dashboards such as the Access Center and Account Management dashboards.

<table>
<thead>
<tr>
<th>Lookup name</th>
<th>Type</th>
<th>Description</th>
<th>Usage details</th>
</tr>
</thead>
<tbody>
<tr>
<td>privileged status of an account. Specify privileged default accounts with `default</td>
<td>privileged<code>, or </code>type privileged<code>for privileged accounts that are not default accounts, or</code>default` for default accounts that are not privileged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Protocols</td>
<td>List</td>
<td>Used by the Port and Protocol dashboard.</td>
<td>See Application Protocols.</td>
</tr>
<tr>
<td>Asset/Identity Categories</td>
<td>List</td>
<td>You can use this to set up categories to use to organize an asset or identity. Common categories for assets include compliance and security standards such as PCI or functional categories such as server and web_farm. Common categories for identities include titles and roles.</td>
<td>See Asset/Identity Categories.</td>
</tr>
<tr>
<td>Assets</td>
<td>Asset list</td>
<td>You can manually add assets in your environment to this lookup to be included in the asset lookups used for asset correlation.</td>
<td>See Manually add new asset or identity data.</td>
</tr>
<tr>
<td>Demonstration Assets</td>
<td>Asset list</td>
<td>Provides sample asset data for demonstrations or examples.</td>
<td>Disable the lookup for use in production environments. See Disable the demo asset and identity lookups.</td>
</tr>
<tr>
<td>Lookup name</td>
<td>Type</td>
<td>Description</td>
<td>Usage details</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Demonstration Identities</td>
<td>Identity list</td>
<td>Provides sample identity data for demonstrations or examples.</td>
<td>Disable the lookup for use in production environments. See Disable the demo asset and identity lookups.</td>
</tr>
<tr>
<td>ES Configuration Health Filter</td>
<td>Per-panel filter lookup</td>
<td>Per-panel filtering for the ES Configuration Health dashboard.</td>
<td>See Configure per-panel filtering in Splunk Enterprise Security.</td>
</tr>
<tr>
<td>Expected Views</td>
<td>List</td>
<td>Lists Enterprise Security views for analysts to monitor regularly.</td>
<td>See Expected Views.</td>
</tr>
<tr>
<td>HTTP Category Analysis Filter</td>
<td>Per-panel filter lookup</td>
<td>Per-panel filtering for the HTTP Category Analysis dashboard</td>
<td>See Configure per-panel filtering in Splunk Enterprise Security.</td>
</tr>
<tr>
<td>HTTP User Agent Analysis</td>
<td>Per-panel filter lookup</td>
<td>Per-panel filtering for the HTTP User Agent Analysis dashboard</td>
<td>See Configure per-panel filtering in Splunk Enterprise Security.</td>
</tr>
<tr>
<td>Identities</td>
<td>Identity list</td>
<td>You can manually edit this lookup to add identities to the identity lookup used for identity correlation.</td>
<td>See Manually add new asset or identity data.</td>
</tr>
<tr>
<td>IIN Lookup</td>
<td>List</td>
<td>Static list of Issuer Identification Numbers (IIN) used to identify likely credit card numbers in event data.</td>
<td>Used to detect Personally-Identifiable Information (PII) in your events.</td>
</tr>
<tr>
<td>Interesting Ports</td>
<td>List</td>
<td>Used by correlation searches to identify ports that are relevant to your network security policy.</td>
<td>See Interesting Ports.</td>
</tr>
<tr>
<td>Lookup name</td>
<td>Type</td>
<td>Description</td>
<td>Usage details</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interesting Processes</td>
<td>List</td>
<td>Used by a correlation search to identify processes running on hosts relevant to your security policy.</td>
<td>See Interesting Processes.</td>
</tr>
<tr>
<td>Interesting Services</td>
<td>List</td>
<td>Used by a correlation search to identify services running on hosts relevant to your security policy.</td>
<td>See Interesting Services.</td>
</tr>
<tr>
<td>Local * Intel</td>
<td>Threat intelligence lookup</td>
<td>Used to manually add threat intelligence.</td>
<td>See Add and maintain threat intelligence locally in Splunk Enterprise Security.</td>
</tr>
<tr>
<td>Modular Action Categories</td>
<td>List</td>
<td>Used to categorize the types of adaptive response actions available to select.</td>
<td>Add a custom category to categorize a custom adaptive response action on Incident Review or the correlation search editor.</td>
</tr>
<tr>
<td>New Domain Analysis</td>
<td>Per-panel filter lookup</td>
<td>Per-panel filtering for the New Domain Analysis dashboard.</td>
<td>See Configure per-panel filtering in Splunk Enterprise Security.</td>
</tr>
<tr>
<td>PCI Domain Lookup</td>
<td>Identity list</td>
<td>Used by the Splunk App for PCI Compliance to enrich the pci_domain field. Contains the PCI domains relevant to the PCI standard.</td>
<td>See Set up asset categories.</td>
</tr>
<tr>
<td>Primary Functions</td>
<td>List</td>
<td>Identifies the primary process or service running on a host. Used by a correlation search.</td>
<td>See Primary Functions.</td>
</tr>
<tr>
<td>Prohibited Traffic</td>
<td>List</td>
<td></td>
<td>See Prohibited Traffic.</td>
</tr>
<tr>
<td>Lookup name</td>
<td>Type</td>
<td>Description</td>
<td>Usage details</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk Object Types</td>
<td>List</td>
<td>The types of risk objects available.</td>
<td>Edit the lookup to create a custom risk object type. You can then filter on the new risk object type or add a new risk entry on the Risk Analysis dashboard. See Create risk and edit risk objects in Splunk Enterprise Security.</td>
</tr>
<tr>
<td>Security Domains</td>
<td>List</td>
<td>Lists the security domains that you can use to categorize notable events when created and on Incident Review.</td>
<td>Edit the lookup and add a custom security domain.</td>
</tr>
<tr>
<td>Threat Activity Filter</td>
<td>Per-panel filter lookup</td>
<td>Per-panel filtering for the Threat Activity dashboard.</td>
<td>See Configure per-panel filtering in Splunk Enterprise Security.</td>
</tr>
<tr>
<td>Urgency Levels</td>
<td>List</td>
<td>Urgency Levels contains the combinations of priority and severity that dictate the urgency of notable events.</td>
<td>See How urgency is assigned to notable events in Splunk Enterprise Security in Use Splunk Enterprise Security.</td>
</tr>
<tr>
<td>URL Length Analysis</td>
<td>Per-panel filter lookup</td>
<td>Per-panel filtering for the URL Length</td>
<td>See Configure per-panel filtering in</td>
</tr>
</tbody>
</table>
### Application Protocols

The Application Protocols list is a list of port and protocol combinations and their approval status in your organization. This list is used by the Port & Protocol Tracker dashboard. See Port & Protocol Tracker dashboard.

The following fields are available in this file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dest_port</td>
<td>The destination port number. Must be a number from 0 to 65535.</td>
</tr>
<tr>
<td>transport</td>
<td>The protocol of the network traffic. For example, icmp, tcp, or udp.</td>
</tr>
<tr>
<td>app</td>
<td>The name of the application using the port.</td>
</tr>
</tbody>
</table>

### Asset/Identity Categories

The category list can contain any set of categories you choose for organizing an asset or an identity. A category is logical classification or grouping used for assets and identities. Common choices for assets include compliance and security standards such as PCI, or functional categories such as server and web_farm. Common choices for identities include titles and roles. For more examples, see Format an asset or identity list as a lookup in Splunk Enterprise Security.

To enrich events with category information in asset and identity correlation, you must maintain the category field in the asset and identity lists instead of in the Asset/Identity Categories list. See Format an asset or identity list as a lookup in Splunk Enterprise Security.

There are two ways to maintain the Asset/Identity Categories list.

**Run a saved search to maintain a list of categories**

Splunk Enterprise Security includes a saved search that takes categories defined in the asset and identity lists and adds them to the Asset/Identity Categories list. The search is not scheduled by default.
1. From the Splunk platform menu bar, select **Settings > Searches, reports, alerts**.
2. Locate the **Identity - Make Categories - Lookup Gen** search-driven lookup or lookup generating search.
3. Click **Edit > Enable**.

**Manually maintain a list of categories**

Maintain the Categories list manually by adding categories to the lookup directly. By default, you must maintain the list manually.

1. Select **Configure > Content > Content Management**.
2. Click the **Asset/Identity Categories** list.
3. Add new categories to the list.
4. Click **Save**.

**Expected Views**

The Expected Views list specifies Splunk Enterprise Security views that are monitored on a regular basis. The View Audit dashboard uses this lookup. See **View Audit** for more about the dashboard.

The following table describes the fields in this file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>The application that contains the view. This is usually set to SplunkEnterpriseSecuritySuite.</td>
</tr>
<tr>
<td>is_expected</td>
<td>Either &quot;true&quot; or &quot;false&quot;. If not specified, Splunk Enterprise Security assumes by default that the view is not expected to be monitored.</td>
</tr>
<tr>
<td>view</td>
<td>The name of the view. Available in the URL or on the Content Management dashboard.</td>
</tr>
</tbody>
</table>

To find the name of a view:

1. Navigate to the view in Enterprise Security.
2. Look at the last segment of the URL to find the view name.

For example, the view in the following URL below is named **incident_review**:

Interesting Ports

Interesting Ports contains a list of TCP and UDP ports determined to be required, prohibited, or insecure in your deployment. Administrators can set a policy defining the allowed and disallowed ports and modify the lookup to match that policy. To get alerts when those ports are seen in your environment, enable the correlation search that triggers an alert for those ports, such as Prohibited Port Activity Detected.

The following table describes the fields in this file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>The application or service name using the port.</td>
<td>Win32Time</td>
</tr>
<tr>
<td>dest</td>
<td>The destination host for the network service. Use a wildcard * to match all hosts.</td>
<td>DARTH*, 10.10.1.100, my_host.</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>An optional PCI domain. Accepts a wildcard.</td>
<td>trust, untrust</td>
</tr>
<tr>
<td>dest_port</td>
<td>The destination port number. Accepts a wildcard.</td>
<td>443, 3389, 5900</td>
</tr>
<tr>
<td>transport</td>
<td>The transport protocol. Accepts a wildcard.</td>
<td>tcp or udp</td>
</tr>
<tr>
<td>is_required</td>
<td>If you require the service to be running, and want the correlation search to create an alert if it is not running, set to true.</td>
<td>true or false</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>If you do not want the port to be used in your network, and want the correlation search to create an alert if it is in use, set to true.</td>
<td>true or false</td>
</tr>
<tr>
<td>is_secure</td>
<td>If the traffic sent through the port is secure, set to true.</td>
<td>true or false</td>
</tr>
<tr>
<td>note</td>
<td>Describe the service using the port and the explanation for the port policy.</td>
<td>Unencrypted telnet services are insecure.</td>
</tr>
</tbody>
</table>
Interesting Processes

Interesting Processes contains a list of processes and whether you consider the processes required, prohibited, or secure to be running in your environment. Splunk Enterprise Security uses this list in the Prohibited Process Detected correlation search.

The following table describes the fields in this file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>Application name</td>
</tr>
<tr>
<td>dest</td>
<td>Destination of the process</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>PCI domain, if available</td>
</tr>
<tr>
<td>is_required</td>
<td>If the process is required to be running on the destination host, set to true. Possible values are true or false.</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>If the process is prohibited on the destination host, set to true. Possible values are true or false.</td>
</tr>
<tr>
<td>is_secure</td>
<td>If the process is secure, set to true. Possible values are true or false.</td>
</tr>
<tr>
<td>note</td>
<td>Describe any additional information about this process. For example, The telnet application is prohibited due to insecure authentication.</td>
</tr>
</tbody>
</table>

Interesting Services

Interesting Services contains a list of services in your deployment. The correlation search Prohibited Service Detected uses this lookup to determine whether a service is required, prohibited, and/or secure.

The following table describes the fields in this file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>Application name</td>
</tr>
<tr>
<td>dest</td>
<td>Destination host that the service is running on.</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>PCI domain of the host, if available</td>
</tr>
<tr>
<td>is_required</td>
<td>If the service is required to be running on the host, set to true. Possible values are true or false.</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>If the service is prohibited on the host, set to true. Possible values are true or false.</td>
</tr>
</tbody>
</table>
If the service is prohibited from running on the host, set to true. Possible values are true or false.

**is_secure**
If the service is secure, set to true. Possible values are true or false.

**note**
Any additional information about this service.

### Primary Functions

Primary Functions contains a list of primary processes and services and their function in your deployment. Use this list to define which services are primary and the port and transport to be used by the services. This lookup is used by the Multiple Primary Functions Detected correlation search.

The following table describes the fields in this file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Name of the process</td>
</tr>
<tr>
<td>service</td>
<td>Name of the service</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>PCI domain of the destination host, if available</td>
</tr>
<tr>
<td>transport</td>
<td>Protocol used for transport by the process. Possible values are tcp or udp.</td>
</tr>
<tr>
<td>port</td>
<td>The port number used by the process.</td>
</tr>
<tr>
<td>is_primary</td>
<td>If the process is the primary process on the host, set to true. Possible values are true or false.</td>
</tr>
<tr>
<td>function</td>
<td>The function that the process performs. For example, proxy, authentication, database, Domain Name Service (DNS), web, or mail.</td>
</tr>
</tbody>
</table>

### Prohibited Traffic

Prohibited Traffic lists processes that, if seen in your network traffic, could indicate malicious behavior. This list is used by the System Center dashboard and is useful for detecting software that is prohibited by your security policy, such as IRC, data destruction tools, file transfer software, or known malicious software, such as malware that was recently implicated in an outbreak.

The following table describes the fields in this file.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>The name of the process (such as echo, chargen, etc.)</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>If the process is prohibited in your environment, set to true. Possible values are true or false.</td>
</tr>
<tr>
<td>note</td>
<td>Add a description about why the process is prohibited.</td>
</tr>
</tbody>
</table>

**Create risk and edit risk objects in Splunk Enterprise Security**

As an ES Admin, you can create and edit risk objects.

**Create a new risk object**

1. From the Enterprise Security menu, select Configure > Content > Content Management.
2. From the Type drop-down filter, select Lookup.
3. (Optional) In the Search filter, type risk object types.
4. Select the Risk Object Types list.
5. Highlight the last risk_object_type cell in the table and right-click to see the table editor.
6. Insert a new row into the table.
7. Double-click in the new row to edit it, then add the new object type name.
8. Save the changes.

**Edit an existing risk object**

1. From the Enterprise Security menu, select Configure > Content > Content Management.
2. From the Type drop-down filter, select Lookup.
3. (Optional) In the Search filter, type risk object types.
4. Select the Risk Object Types list.
5. Highlight the risk object type and change the name.
6. Save the changes.

**Expand Content Management searches to view dependency and usage information in Splunk Enterprise Security**
In Content Management, it is possible to see more details about the knowledge objects such as data models, correlation searches, lookups, investigations, key indicators, glass tables, and reports.

**Additional details**

With these additional details, you can verify health status, statistics, associated knowledge objects, and that the proper technical add-ons are populating within each of objects.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. (Optional) From the Type filter, select a type such as **Search** or **Data Model**.
3. From the event information column of a search or data model, click the greater than (>) symbol to expand the display.

Not every Type will include the greater than (>) symbol, and each different Type will show different details.

The following table describes the additional usage details and dependencies:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Icon to show the overall health. If the icon is not a green checkmark, then you are not ingesting enough data for this content to report accurately.</td>
</tr>
<tr>
<td>Statistics</td>
<td>For searches, if the saved search is scheduled, this shows execution statistics from the _audit index. For data models, if the data model is accelerated, the execution statistics are also returned for the acceleration search.</td>
</tr>
<tr>
<td>Associated Searches</td>
<td>The saved searches that use this object or dataset.</td>
</tr>
<tr>
<td>Associated Panels</td>
<td>The panels that use this object or dataset.</td>
</tr>
<tr>
<td>Indexes</td>
<td>The indexes that this object or dataset uses. If the icon is a green checkmark, then the index has events for the past 24 hours.</td>
</tr>
<tr>
<td>Lookups</td>
<td>The lookups that this object or dataset uses. If the icon is a green checkmark, then the row counts for the csv or kvstore lookup files are not empty.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sourcetypes</td>
<td>The sourcetypes that this object or dataset uses. For example, if you have Unix in your environment and you would expect to see that sourcetype listed here, but you don't see it, then you would know that you need to revise the way you're getting that data into Splunk. If the icon is a green checkmark, then the index has events for the past 24 hours.</td>
</tr>
<tr>
<td>Tags</td>
<td>The tags that this object or dataset uses.</td>
</tr>
</tbody>
</table>

Associated objects are only visible if there is data to populate them. If there is no data to populate them, then you will see a message such as "No associated objects or datasets found."

**Use analytic stories through the use case library 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 Splunk Enterprise Security (ES) environment. An analytic story also provides an explanation of what the search achieves and how to convert a search into adaptive response actions, where appropriate.

The Splunk Enterprise Security Content Update (ESCU) delivers analytic stories to customers as part of a content subscription service. Analytic stories give you advice on how to use Splunk ES to investigate and take action on new threats that Splunk ES detects in your environment.

The ESCU analytic story content is available directly in Splunk ES through the use case library. If you do not have ESCU installed, you will see some analytic stories by default as well as a message prompting you to download and install the ESCU add-on for access to common security analytic stories.

Prerequisites for using the use case library include the following:

- Data is ingested via your forwarders and technical add-ons.
- The CIM add-on is installed.
- (Optional) The ESCU add-on is installed so you can access more analytic stories.
You can explore, activate, bookmark, and configure common searches in the use case library.

**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 will see the detection searches that are related to this use case.
5. You will also see your data sources, data models, and lookups that these searches use.

<table>
<thead>
<tr>
<th>Data Sources</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Data Sources</td>
<td>The type of data sources that are likely to provide valuable data.</td>
</tr>
<tr>
<td>Sourcetypes</td>
<td>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.</td>
</tr>
<tr>
<td>Data Models</td>
<td>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.</td>
</tr>
<tr>
<td>Lookups</td>
<td>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.</td>
</tr>
</tbody>
</table>
Data Sources | Description
--- | ---

6. Click the name of the analytic story. In this case, click **Suspicious AWS EC2 Activities**. The Analytic Story Details page opens for the story.

7. You will see the searches related to the stages of detecting, investigating, assessing, and mitigating issues.

   1. From the Detection section, select a search, such as **ESCU - EC2 Instance Started In Previously Unseen Region**.
   2. From the Search section, click the greater than (>) symbol to expand the display.
   3. Revise the time picker and click **Search**.

   4. From the How to Implement section, click the greater than (>) symbol to expand the display for tips on implementation.

   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.

If you want to run this search automatically on a regular basis, see **Enable and schedule the analytic story**.

### Enable and schedule the analytic story

Once you determine that an analytic story will help you detect, investigate, assess, or mitigate an issue, you can enable and schedule it. An analytic story is considered "in use" when at least one search is enabled and scheduled. By default, all stories are disabled. If a search is enabled but not scheduled, or if it is run manually, then it is not considered in use.

1. From the Splunk ES menu bar, select **Configure > Content > Use Case Library**.

2. From the event information column, click the greater than (>) symbol to expand the display.

   1. Click the name of an ESCU detection search.
      A new content management window opens.
   2. Click **Enable**.

3. To edit the correlation search schedule, click the name of the search.

4. Click **Save**.
To modify correlation searches in your environment, see Create correlation searches in Splunk Enterprise Security.

**Bookmark the analytic story**

Bookmarks persist per user, so individual analysts can bookmark the analytic stories that are specific to their 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.

**Configure the library**

You can revise how the preconfigured use case library displays your most frequently used analytic stories and searches.

The use case library does not require any special capability to view analytic stories, but it does require the edit_analyticstories capability to edit and add them. By default, ES assigns the edit_analyticstories capability to the ess_admin and ess_analyst roles. An admin can assign other roles from the Permissions setting.

**Edit or add analytic story details**

To edit the displayed descriptions, narratives, references, or searches:

1. From the Splunk ES menu bar, select Configure > Content > Use Case Library.
2. From the use case library, click the name of an analytic story to see the Analytic Story Details page, which contains all the default information that is provided by the ESCU content.
3. From the top-right of the Analytic Story Details page, click Edit.
4. A new browser window opens so you can change the story descriptions, narratives, or references to fit your specific usage. These changes are global, not per user, so everyone sees the same updates.
5. You can also add existing searches that do not display by default in this analytic story.
   1. Scroll to the Searches section.
   2. Click Add Search.
3. Select the search to include in this story.

6. Click **Save**.

**Search types**

When you add a search in the Edit Analytic Stories window, the type of search appears to the right of the search name. By default you will see detection, investigative, contextual, support, or select to annotate.

Only annotated searches are associated with an analytic story. When you add an annotated search, the search is immediately added to the analytic story. In those added searches, you can click **Edit Search** to revise the annotations of that search.

If the search is not annotated, do the following to annotate it:

1. From the right side of the search name, click **Select to annotate**.
2. In the annotation editor, type the name of an existing search type or type the name a new search type in the Type field. This is the only mandatory field.
3. (Optional) If you want analysts to see information when deciding which stories and searches to use, fill in information for Description, How to Implement, Known False Positives, Providing Technologies (also known as data sources or technology add-ons).
4. (Optional) In the Annotations field, click **Add row** to add Framework names and their Mapping categories. These are free-form fields. You can use them for either industry-standard frameworks, such as National Institute of Standards and Technology issues for detecting and continuous monitoring of vulnerabilities (NIST + DE.CM), or you can use them for frameworks of your own.
You can find these later from the Framework Mapping filter.
1. From the Splunk ES menu bar, select **Configure > Content > Use Case Library**.
2. From the drop-down filters, click **Framework Mapping**.
3. Type the name of a Framework or scroll to find it.
4. Click the check box to select a Framework. The filter is using OR logic, so the more check boxes you select, the more results you will see.

The `savedsearches.conf` file is used to annotate existing saved searches.

**Create an analytic story**

You can create your own analytic story and map it to the searches of your choice.

The use case library does not require any special capability to view analytic stories, but requires the `edit_analyticstories` capability to edit and create new ones. By default, ES assigns the `edit_analyticstories` capability to the `ess_admin` and `ess_analyst` roles. An admin can assign it to other roles from the Permissions setting.

1. From the Splunk ES menu bar, select **Configure > Content > Content Management**.
2. Click **Create New Content > Analytic Story**.
3. Fill in the required fields to create your analytics story.
4. Scroll down to the **Searches** field.
5. From the Add Search drop-down menu, you can select any of the searches that have been annotated.
6. Click **Save**.

**Install analytic stories from other apps**

While ESCU content is imported automatically, you can also import analytic stories from apps other than ESCU into the use case library.

Install the app to see the analytic stories in the use case library.

1. Install the app onto the same search head as Splunk ES.
2. Export the app to other apps or globally.
3. Review the new knowledge objects. If the analytic stories are visible in the use case library, the export is successful.
4. Use the new analytic stories.
If you do not see the new analytic stories in the use case library, it's because of one of the following reasons:

- Make sure that the app is being exported globally. See Make Splunk knowledge objects globally available in the Splunk Enterprise *Admin Manual*.
- If the app does not contain compatible use cases, it does not contain an analyticstory.conf file.
Configuration and Troubleshooting

Configure general settings for Splunk Enterprise Security

As a Splunk Enterprise administrator, you can make configuration changes to your Splunk Enterprise Security installation. Change threshold values, macro definitions, search filters, and other commonly changed values on the General Settings page.

On the Enterprise Security menu bar, select **Configure > General > General Settings**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Sources</td>
<td>A search macro that enumerates the lookup tables that contain asset information used for asset correlation.</td>
</tr>
<tr>
<td>Auto Pause</td>
<td>Type the time in seconds before a drilldown search will pause.</td>
</tr>
<tr>
<td>Default Watchlist Search</td>
<td>Define the watchlisted events for the 'Watchlisted Events' correlation search</td>
</tr>
<tr>
<td>Domain Analysis</td>
<td>Enable or disable WHOIS tracking for Web domains.</td>
</tr>
<tr>
<td>Domain From URL Extraction Regex</td>
<td>A regular expression used to extract domain (url_domain) from a URL.</td>
</tr>
<tr>
<td>Enable Identity Generation</td>
<td>If true, permit the Identity Manager to auto-update asset_sources, identity_sources, and generate_identities macros. True by default.</td>
</tr>
<tr>
<td>Autoupdate</td>
<td></td>
</tr>
<tr>
<td>Generic Error Search</td>
<td>A search filter for defining events that indicate an error has occurred.</td>
</tr>
<tr>
<td>HTTP Category Analysis Sparkline Earliest</td>
<td>Set the start time for sparklines displayed on the <a href="#">HTTP User Category Analysis</a> dashboard.</td>
</tr>
<tr>
<td>HTTP Category Analysis Sparkline Span</td>
<td>Set the time span for sparklines displayed on the <a href="#">HTTP User Category Analysis</a> dashboard.</td>
</tr>
<tr>
<td>HTTP User Agent Analysis Sparkline</td>
<td>Set the start time for sparklines displayed on the <a href="#">HTTP User Agent Analysis</a> dashboard.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Earliest</td>
<td></td>
</tr>
<tr>
<td>HTTP User Agent Analysis Sparkline Span</td>
<td>Set the time span for sparklines displayed on the HTTP User Agent Analysis dashboard.</td>
</tr>
<tr>
<td>IRT Disk Sync Delay</td>
<td>Set the number of seconds for Enterprise Security to wait for a disk flush to finish. Relevant to indexed real time searches.</td>
</tr>
<tr>
<td>Identity Generation</td>
<td>Defines the transformations used to normalize identity information. See How Splunk Enterprise Security processes and merges asset and identity data</td>
</tr>
<tr>
<td>Identity Generation Timeout</td>
<td>Number of seconds the Identity Manager waits before warning of slow search completion in identity_manager.log.</td>
</tr>
<tr>
<td>Identity Sources</td>
<td>Enumerates the source lookup tables that contain identity information.</td>
</tr>
<tr>
<td>Incident Review Analyst Capacity</td>
<td>Estimated maximum capacity of notable events assigned to an analyst. Relative measure of analyst workload.</td>
</tr>
<tr>
<td>Indexed Realtime</td>
<td>Enable or disable indexed real-time mode for searches.</td>
</tr>
<tr>
<td>Large Email Threshold</td>
<td>An email that exceeds this size in bytes is considered large.</td>
</tr>
<tr>
<td>Licensing Event Count Filter</td>
<td>Define the list of indexes to exclude from the &quot;Events Per Day&quot; summarization.</td>
</tr>
<tr>
<td>Maximum Documents Per Batch Save (kvstore)</td>
<td>The maximum number of documents that can be saved in a single batch to a KV Store collection.</td>
</tr>
<tr>
<td>New Domain Analysis Sparkline Span</td>
<td>Set the time span for sparklines displayed in the New Domain Analysis dashboard.</td>
</tr>
<tr>
<td>Notable Modalert Pipeline</td>
<td>SPL for the notable event adaptive response action.</td>
</tr>
<tr>
<td>Override Email Alert Action</td>
<td>Override the email alert action settings to allow users to send notable events via email through adaptive response actions on the Incident Review dashboard.</td>
</tr>
<tr>
<td>Risk Modalert Pipeline</td>
<td>SPL for the risk modifier adaptive response action.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search Disk Quota (admin)</td>
<td>Set the maximum amount of disk space in MB that an admin user can use to store search job results.</td>
</tr>
<tr>
<td>Search Jobs Quota (admin)</td>
<td>Set the maximum number of concurrent searches allowed for admin users.</td>
</tr>
<tr>
<td>Search Jobs Quota (power)</td>
<td>Set the maximum number of concurrent searches for power users.</td>
</tr>
<tr>
<td>Short Lived Account Length</td>
<td>An account creation and deletion record that exceeds this threshold is anomalous.</td>
</tr>
<tr>
<td>TSTATS Allow Old Summaries</td>
<td>Enable or disable searching of data model accelerations containing fields that do not match the current data model configuration.</td>
</tr>
<tr>
<td>TSTATS Local</td>
<td>Determine whether or not the TSTATS macro will be distributed.</td>
</tr>
<tr>
<td>TSTATS Summaries Only</td>
<td>Determine whether or not the TSTATS or summariesonly macro will only search accelerated events.</td>
</tr>
<tr>
<td>Use Other</td>
<td>Enable or disable the term OTHER on charts that exceed default series limits.</td>
</tr>
<tr>
<td>Website Watchlist Search</td>
<td>A list of watchlisted websites used by the &quot;Watchlisted Events&quot; correlation search.</td>
</tr>
</tbody>
</table>

**See also**

- Manage input credentials in Splunk Enterprise Security
- Manage permissions in Splunk Enterprise Security
- Customize the menu bar in Splunk Enterprise Security
- Configure per-panel filtering in Splunk Enterprise Security

**Manage credentials in Splunk Enterprise Security**

Use the Credential Management page to store credentials for scripted or modular inputs. Input configurations that reference credentials use the credentials stored in Credential Management. You can store credentials such as usernames and passwords, or certificates used for authentication with third-party systems. Do not use this page to manage certificates used to encrypt
server-to-server communications.

Your role must have the appropriate capabilities to add, modify, and view credentials and certificates. See Configure users and roles in the Installation and Upgrade Manual.

Add a new credential for an input

1. On the Enterprise Security menu bar, select Configure > General > Credential Management.
2. Click New Credential to add a new user credential.
3. Type a Username.
4. (Optional) Type a Realm field to differentiate between multiple credentials that have the same username.
5. Type the Password for the credential, and type it again in Confirm password.
6. Select the App for the credential.
7. Click Save.

Edit an existing input credential

You can edit passwords of existing input credentials.

1. On the Enterprise Security menu bar, select Configure > General > Credential Management.
2. In the Action column of a credential, click Edit.
3. Type a new Password for the credential, and type it again in Confirm password.
4. Click Save.

Add a new certificate

You cannot add a new certificate using Credential Management on a search head cluster (SHC). To add a new certificate to Splunk Enterprise Security on a SHC, add the certificate to $SPLUNK_HOME/etc/shcluster/apps/<app_name>/auth on the deployer and deploy the certificate to the SHC members.

1. On the Enterprise Security menu bar, select Configure > General > Credential Management.
2. Click New Certificate to add a new certificate.
3. Type a File name for the certificate. This is the file name that the certificate is saved as in the $SPLUNK_HOME/etc/apps/<app_name>/auth
directory.
4. Add **Certificate text** for the certificate. Paste the contents of an existing certificate file here to add the certificate to Splunk Enterprise Security.
5. Select an **App** to save the certificate in.
6. Click **Save**.

**Edit an existing certificate**

You can edit the certificate text of existing certificates in Credential Management. You cannot edit certificates on a search head cluster.

1. On the Enterprise Security menu bar, select **Configure > General > Credential Management**.
2. In the **Action** column of a certificate, click **Edit**.
3. Type a new **Certificate text** for the certificate.
4. Click **Save**.

**Delete an existing input credential or certificate**

You cannot delete certificates on a search head cluster.

1. On the Enterprise Security menu bar, select **Configure > General > Credential Management**.
2. In the **Action** column of a credential or certificate, click **Delete**.
3. Click **OK** to confirm.

**Manage permissions in Splunk Enterprise Security**

Use the Permissions page to view and assign Enterprise Security capabilities to non-admin roles.

1. On the Enterprise Security menu bar, select **Configure > General > Permissions**.
2. Select the checkbox for the role and permissions for that role.
3. Click **Save**.

For more information about ES capabilities, see Configure users and roles in the *Installation and Upgrade Manual*. 
Customize the menu bar in Splunk Enterprise Security

Customize the menu bar in Splunk Enterprise Security with the Edit Navigation view. Add new **dashboards**, reports, **views**, links to filtered dashboards, or links to the web to your menu bar. You must have Enterprise Security administrator privileges to make changes to the menu bar navigation.

You can add views to the menu bar as part of a collection that groups several views together or as an individual item on the menu bar. For example, Incident Review is an individual dashboard in the menu bar, and Audit is a collection of the audit dashboards.

Splunk Enterprise Security persists customizations you made to the navigation from previous versions.

Check for updated views

Views and collections that are new, updated, or deprecated in the version of the app that you have installed are highlighted with small icons that indicate the relevant changes.

After installing a new version of Splunk Enterprise Security or a new version of an app that provides views and collections for use in Enterprise Security, visit the Edit Navigation view to check for updates in those views and collections.

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. If any content has been updated, the message "Some content updates available" appears at the top of the navigation editor.
3. Look for icons on the views on the editor pane to find content that has been added, updated, or deprecated. These same icons also appear in the **Add a New View** and **Add a New Collection** menus.

Set a default view for Splunk Enterprise Security

To see a specific view when you or other users open Splunk Enterprise Security, set a default view.

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Locate the view that you want to be the default view.
3. Click the checkmark icon that appears when you mouse over the view to **Set this as the default view**.

4. Click **Save** to save your changes
5. Click **OK** to refresh the page and view your changes.

Only views can be selected as default views.

**Edit the existing menu bar navigation**

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Click and drag views or collections of views to change the location of the views or collections of views in the menu.
3. Click the **X** next to a view or collection to remove it from the menu.
4. Click the **»** icon to edit the name of a collection.
5. Click the **«** icon to add a divider and visually separate items in a collection.
6. Click **Save** to save your changes
7. Click **OK** to refresh the page and view your changes.

**Add a single view to the menu bar**

You can add a new view to the menu bar without adding it to a collection.

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. Click **Add a New View**.
3. Leave **View Options** set to the default of **View**.
4. Click **Select a View** from **Unused Views**.
5. Select a dashboard or view from the list.
6. Click **Save**. The dashboard appears on the navigation editor.
7. If you are finished adding items to the menu, click **Save** to save your changes
8. Click **OK** to refresh the page and view your changes.

**Add a collection to the menu bar**

Use a collection to organize several views or links together in the menu bar.

1. On the Enterprise Security menu bar, select **Configure > General >**
You must add a view or link to the collection before it appears in the menu navigation.

**Add a view to an existing collection**

Add views to an existing collection.

2. Locate the collection that you want to add views to.
3. Click the icon.
4. Leave View Options set to the default of View.
5. Click Select a View from Unused Views.
6. Select a view from the list.
7. Click Save. The view appears on the navigation editor.
8. If you are finished adding items to the menu, click Save to save your changes.
9. Click OK to refresh the page and view your changes.

**Add a link to the menu bar**

You can add a link to the menu bar of Splunk Enterprise Security. For example, add a link to a specifically-filtered view of Incident Review or to an external ticketing system.

**Create a link in the menu to an external system or webpage**

2. Click Add a New View to add it to the menu, or locate an existing collection and click the icon to add the link to an existing collection of views.
3. Select Link from View Options.
4. Type a Name to appear on the Splunk Enterprise Security menu. For example, Splunk Answers.
5. Type a link. For example, https://answers.splunk.com/
6. Click Save.
7. If you are finished adding items to the menu, click **Save** to save your changes.
8. Click **OK** to refresh the page and view your changes.

**Add a link to a filtered view of Incident Review**

A common link to add to the menu bar is a filtered view of Incident Review.

1. Filter Incident Review with your desired filters. When you filter the dashboard, the URL updates with query string parameters matching your filters.
2. In the web browser address bar, copy the part of the URL that starts with `/app/SplunkEnterpriseSecuritySuite/` and paste it in a plain text file for reference.
   For example, if you filtered the dashboard to show only critical notable events, the part of the URL that you copy looks like `/app/SplunkEnterpriseSecuritySuite/incident_review?form.selected_urgency=critical`.
3. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
4. Click **Add a New View** to add it to the menu, or locate an existing collection and click the **Add View** icon to add the link to an existing collection of views.
5. Select **Link** from **View Options**.
6. Type a **Name** to appear on the Splunk Enterprise Security menu. For example, **IR - Critical**.
7. In the **Link** field, paste the URL section. For example, `/app/SplunkEnterpriseSecuritySuite/incident_review?form.selected_urgency=critical`
8. Click **Save**.
9. If you are finished adding items to the menu, click **Save** to save your changes.
10. Click **OK** to refresh the page and view your changes.

If you add a link with multiple parameters you must modify the query string parameters by adding &. For example, type the link for a filtered view of Incident Review that shows new and unassigned notable events as `app/SplunkEnterpriseSecuritySuite/incident_review?form.status_form=1&form.owner_form=unassigned`.

You can also construct a URL manually using the parameters in the following table. Use an asterisk to show all results for a specific parameter. Not all parameters are required.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
</table>

173
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>form.selected_urgency</td>
<td>Display notable events with the urgency specified by this parameter.</td>
<td>critical, high, medium, low, informational</td>
</tr>
<tr>
<td>form.status_form</td>
<td>Display notable events with the status specified by this parameter.</td>
<td>0 for unassigned, 1 for new, 2 for in progress, 3 for pending, 4 for resolved, 5 for closed</td>
</tr>
<tr>
<td>form.owner_form</td>
<td>Display notable events owned by the user specified by this parameter.</td>
<td>usernames</td>
</tr>
<tr>
<td>form.source</td>
<td>Display notable events created by the correlation search specified by this parameter. HTML-encode spaces in the correlation search name and use the name that appears in the notable event rather than the name that appears on Content</td>
<td>Endpoint - Host With Multiple Infections - Rule</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Possible values</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>form.rule_name</td>
<td>Display notable events created by the correlation search specified by this parameter. HTML-encode spaces in the correlation search name. Use the name that appears on Content Management.</td>
<td>Host With Multiple Infections</td>
</tr>
<tr>
<td>form.tag</td>
<td>Displays notable events with the tag specified by this parameter.</td>
<td>malware, any custom tag value</td>
</tr>
<tr>
<td>form.srch</td>
<td>Displays notable events that match the SPL specified in this parameter. HTML-encode special characters such as = for key-value pairs.</td>
<td>dest=127.0.0.1</td>
</tr>
<tr>
<td>form.security_domain_form</td>
<td>Displays notable events in the security domain specified by this parameter.</td>
<td>access, endpoint, network, threat, identity, audit</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Possible Values</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>earliest= and latest=</td>
<td>Displays notable events in the time range specified by these parameters. Specify a relative time range. HTML-encode special characters such as @.</td>
<td>-24h@h, now</td>
</tr>
<tr>
<td>form.new_urgency_count_form</td>
<td>Displays notable events that do not have the urgency specified by this parameter.</td>
<td>critical, high, medium, low, informational</td>
</tr>
<tr>
<td>form.selected_urgency</td>
<td>Displays notable events that have the urgency specified by this parameter. Use multiple instances of this parameter to select multiple urgency settings.</td>
<td>critical, high, medium, low, informational</td>
</tr>
<tr>
<td>event_id</td>
<td>Displays the notable event that matches the specified event_id.</td>
<td>3C84A9D8-87F6-4066-8659-C7DD680F98E6@@notable@@80e0f89da83cad6665dd1de7447cedb4</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Possible values</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>form.association_type</td>
<td>Used together, displays the notable events associated with a short ID or an investigation.</td>
<td>short_id, investigation EYIYNW, 5a4be2b8cdc9736b2352c7c3</td>
</tr>
<tr>
<td>form.association_id</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Restore the default navigation

To restore the default navigation of the Splunk Enterprise Security menu bar:

1. On the Enterprise Security menu bar, select **Configure > General > Navigation**.
2. In the upper right corner, click **Restore Default Configuration**.
3. Click **OK** to confirm.
4. Scroll to the bottom of page and click **Save**.

### Configure per-panel filtering in Splunk Enterprise Security

Some dashboards in Splunk Enterprise Security include the per-panel filter option, which can filter items out of dashboard views, making it easier to find those events that require investigation.

- If you determine that an event is a threat, use the per-panel filter to add the item to your **blacklist** of known threats.
- If you determine that an event is not a threat, you can add it to your **whitelist** to remove it from the dashboard view.

The per-panel filter button appears only if the user has permission. To configure this permission, see Configure users and roles in the *Installation and Configuration* manual.

### Whitelist events

After you determine that an event is not a threat, you can whitelist the event to hide it from the dashboard view. After you whitelist an event, the summary statistics continue to calculate whitelisted items, but the whitelisted items are not displayed in the dashboard.
**Whitelist an event**

Use the per-panel filter to whitelist, or filter, events on a dashboard.

For example, to whitelist traffic events on the **Traffic Size Analysis** dashboard:

1. Use the checkboxes to select the items to filter.
2. Click **Per-panel Filter** in the top right corner to display options for events that can be filtered in this dashboard.
3. Select the radio button to filter events on this dashboard.
   - For example, on the **Traffic Size Analysis** dashboard, you can either filter events so that they no longer appear or highlight them so that they are flagged as important.
4. Click **Save** when you are done.

In this example, after an item is added to the whitelist, it is no longer considered a threat and no longer appears on the **Traffic Size Analysis** dashboard.

**Remove an item from the whitelist**

1. Click **Per-panel Filter**, then **View/edit lookup file** to see the list of entries currently being filtered.
2. Right-click a cell in the table to view the context menu.
3. Select **Remove row** to remove the row containing the whitelisted item.
4. Click **Save**.

**Blacklist events**

An event can also be blacklisted. Blacklisting an item means that you have identified an event that is known to be malicious, or thought to communicate with a command and control server that is known to be malicious. Anytime the event or string shows up in the data, you will want to investigate the system, the user associated with the system, and the web activity to understand the nature and possible proliferation of the threat.

Blacklisting an event or string is similar to whitelisting. Events can only be blacklisted after they have been filtered from the dashboard.

To blacklist a traffic event on, for example, the **Traffic Size Analysis** dashboard, do the following:

1. Click **Per-panel Filter**, then **View/edit lookup file** to see the list of entries currently being filtered.
2. Locate the entry you want to add to the blacklist. Under the filter column, double-click the word whitelist to edit the cell. Delete "whitelist" and type "blacklist".
3. Click Save.

Edit the per-panel filter list

To see a current list of per-panel filters by dashboard, select Configure > Content > Content Management. Lookups with a description indicating that they are a per-panel filter show the current per-panel filters for the dashboard in the lookup name. Events added to the whitelist for a dashboard are listed in that lookup.

For example, the Threat Activity Filter lookup displays the filters for the Threat Activity dashboard.

Edit the per-panel filter lookup.

1. Open the filter list for the relevant dashboard. The name of the filter, for example ppf_threat_activity, shows in the upper left-hand corner.
2. To edit a field, select a cell and begin typing.
3. To insert or remove a row or column in the filter, right-click the field for edit options. Removing a row adds that item back to the dashboard panel view and removes it from the whitelist.
4. To "blacklist" an item, use the editor to add a new row to the table and use "blacklist" in the "filter" column.
5. Click Save to save your changes.

Audit per-panel filters

Changes made to the per-panel filters are logged in the per-panel filtering audit logs. The lookup editor and the per-panel filter module modify per-panel filters. Use the Per-Panel Filter Audit dashboard to audit per-panel filters.

Create a Splunk Web message in Splunk Enterprise Security

Create a message in Splunk Web based on the results of a search using the Create Splunk messages alert action. Only administrators can create messages using this alert action.
The message that you create with this alert action must already exist in messages.conf. See Customize Splunk Web messages in the Splunk Enterprise Admin Manual for more about creating messages.

1. You can create Splunk Web messages from a search or from a correlation search:

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new alert</td>
<td>From the Search page in the Search and Reporting app, select Save As &gt; Alert. Type and select alert details and configure triggering and throttling as needed.</td>
</tr>
<tr>
<td>Create or edit a correlation search</td>
<td>From the ES menu bar, select Configure &gt; Content &gt; Content Management. Select Create New Content &gt; Correlation Search. Type and select correlation search configurations as needed.</td>
</tr>
<tr>
<td>Edit a correlation search</td>
<td>From the ES menu bar, select Configure &gt; Content &gt; Content Management. Select the correlation search.</td>
</tr>
</tbody>
</table>

2. Click Add Actions and select Create Splunk messages.
3. Select a Name. The name corresponds to a stanza in messages.conf of an existing message.
   For example, DISK_MON:INSUFFICIENT_DISK_SPACE_ERROR.
4. (Optional) Type a Message ID that identifies the message.
   For example, insufficient_diskspace.
5. (Optional) If a message uses field substitution, type the Fields to use. The fields used for argument substitution must be returned in the search results to be included in the message. Type the fields in the order that they must be substituted in the message.
   For example, for a message Host %s has free disk space %d, below the minimum 5GB., type the fields src,FreeMBytes.
6. (Optional) Select Yes for Keep Only Latest and keep only the latest message produced by a search.
   For example, if the host has low disk space for three days, rather than get daily messages for three days, select Yes for this setting to only see one message.
7. Click Save.
Troubleshoot script errors in Splunk Enterprise Security

Troubleshoot script errors from modular inputs in Splunk Enterprise Security. If you see a message about a script exiting abnormally or a script that is in an unknown state, investigate the script and stanza that produced the error.

The Audit - Script Errors search replaces a configuration check script and creates Splunk messages to warn about non-zero exit codes that result from scripts in your Splunk deployment.

<table>
<thead>
<tr>
<th>Possible root cause</th>
<th>Verification</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The script did not run successfully.</td>
<td>Review the log files for the script. Run the script manually to see if it runs successfully, and review the exit code that results.</td>
<td>Address the reasons why the script exited with a non-zero exit code.</td>
</tr>
<tr>
<td>The script ran successfully with a non-zero exit code.</td>
<td>Run the script manually to see if it runs successfully, and review the exit code that results.</td>
<td>Include the script in the suppression for the search so that it does not display messages for this script.</td>
</tr>
<tr>
<td>The script is in an unknown state. There is a stop time for the script, but no exit status or start time.</td>
<td>Check the modular input settings to confirm they are correct.</td>
<td>Correct the modular input settings.</td>
</tr>
</tbody>
</table>


Prevent messages about specific scripts

If needed, you can prevent messages about specific scripts by modifying the match syntax in the `script_error_msg_ignore` macro.

If you had locally-defined script suppression regex in the [configuration_check://confcheck_script_errors] stanza, you can replicate it in the macro. For example, the suppression stanza includes the following regular expression:
suppress = 
((streamfwd|splunk-(wmi\.path|MonitorNoHandle\.exe|winevtlog\.exe|netmon\.exe|perfmon\.
   with code 1)

The macro replicates this suppression with the following definition:

match(script,
   "(streamfwd|splunk-(wmi\.path|MonitorNoHandle\.exe|winevtlog\.exe|netmon\.exe|perfmon\.
   AND exit_status=1

To reduce the frequency of messages about specific scripts rather than prevent
them from appearing, throttle the alerts. Set up alert throttling for the Audit -
Script Errors search based on the necessary values, such as the script field.

- For Splunk Enterprise, see Throttle alerts in the Alerting Manual.
- For Splunk Cloud, see Throttle alerts in the Alerting Manual.

Disable the configuration checker

To stop the messages by disabling the configuration checks, such as
confcheck_app_exports\.py, do the following:

1. On the Enterprise Security menu bar, select Configure > General >
   Configuration Checker.
2. Find the name of the script and click Disable.

Though in the case of confcheck_app_exports\.py specifically, also check the
5.3.0 Release notes regarding Improved App Import and Export Support to verify
if you want to export the apps or disable the configuration checker. See What's
New.

Troubleshoot messages about default indexes
searched by the admin role

Troubleshoot Splunk messages about default indexes searched by the admin
role in the Splunk platform.
Default admin searches include summary indexes

When the admin role searches summary indexes by default, you can see decreased performance. You can stop seeing messages about this setting by limiting the indexes searched by the admin role or by disabling the search.

Limit the indexes searched by the admin role

Prevent the admin role from searching summary indexes. You can identify summary index names because the index names end in _summary, such as endpoint_summary.

1. Select Settings > Access controls.
2. Click Roles.
3. Click admin.
4. From Indexes click any summary index to remove it from the selected indexes.
5. Click Save.

Disable the search to prevent messages

If you do not want to limit the indexes searched by the admin role, but you want to stop seeing messages, disable the search.

1. Select Settings > Searches, reports, and alerts.
2. Locate the Audit - Default Admin Search Indexes search.
3. Select Edit > Disable.
4. Click Disable.

Default admin searches include all non-internal indexes

When the admin role searches all non-internal indexes by default, you can see decreased performance. You can stop seeing messages about this setting by limiting the indexes searched by the admin role or disabling the search.

Limit the indexes searched by the admin role

Prevent the admin role from searching all non-internal indexes.

1. Select Settings > Access controls.
2. Click Roles.
3. Click **admin**.
4. From **Indexes** click **All non-internal indexes** to remove it from the selected indexes.
5. Click **Save**.

**Disable the search to prevent messages**

If you do not want to limit the indexes searched by the admin role, but you want to stop seeing messages, disable the search.

1. Select **Settings > Searches, reports, and alerts**.
2. Locate the **Audit - Default Admin Search All Non-Internal** search.
3. Select **Edit > Disable**.
4. Click **Disable**.

**Troubleshoot messages about unnecessary read or write access to investigation KV store collections**

Troubleshoot Splunk Web messages about roles that have unnecessary read or write access to the investigation KV store collections.

You might see the following error messages in Splunk Web:

Health Check: Review roles for unnecessary read or write access to the investigation_attachment collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigation_event collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigative_canvas_entries collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the files collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigation collection and remove access if possible
Health Check: Review roles for unnecessary read or write access to the investigative_canvas collection and remove access if possible

These messages are produced by the **Audit - Investigation Collection ACLs** saved search. The search looks for non-admin permissions to the investigation KV store collections.
**Remove the unnecessary read or write access from the collections**

If you see these messages, remove the corresponding `collections/<stanza_name>`, collections from `$SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/metadata/local.meta`. Access to these collections by non-admin roles is not recommended. After making the changes, refresh the file cache from Splunk Web: `http://<yoursplunkserver>:8000/en-us/debug/refresh?`.

In a search head cluster environment, make these changes to the `local.meta` file on each member in the cluster, via the deployer if applicable. Then refresh the file cache from Splunk Web for each search head: `http://<yoursplunkserver>:8000/en-us/debug/refresh?`. Alternately, if there are more than a few members in the cluster, a rolling restart can be used instead of the debug/refresh command.

**Troubleshoot failed intelligence downloads in Splunk Enterprise Security**

If you receive the message that a threat list failed to download, there are several possible root causes.

<table>
<thead>
<tr>
<th>Possible root cause</th>
<th>Verification</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The threat or intelligence source is no longer available at the IP address or URL.</td>
<td>Attempt to visit the URL or curl the threat source manually.</td>
<td>Disable the intelligence source if it is no longer available to download.</td>
</tr>
<tr>
<td>Firewall or proxy settings are preventing the intelligence source from being accessed.</td>
<td>Test if you can visit the URL or curl the intelligence source manually on a different machine.</td>
<td>Modify the firewall or proxy settings to allow access to the intelligence source.</td>
</tr>
</tbody>
</table>

**Troubleshoot dashboards in Splunk Enterprise Security**

Each dashboard in Enterprise Security references data from various data models. Without the relevant data, the dashboards will remain empty. If you expect data to appear, or if the data appearing is older than you expect, follow
these troubleshooting steps.

1. Perform a search against the data model. Click **Open in Search** in the lower left corner of a dashboard view to perform a direct search against the data model. The **New Search** dashboard also exposes the search commands and objects used to populate a particular view.

2. If the search yields no results, determine if any data required for a dashboard is available in the data model.
   1. See the **Dashboard requirements matrix** in this manual to determine the data model datasets used by a dashboard.
   2. Use the data model and data model dataset to search for events in the data model.

<table>
<thead>
<tr>
<th>Action</th>
<th>Search</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the data is normalized to the Common Information Model</td>
<td>`</td>
<td>datamodel data_model_name root_object_name search</td>
</tr>
</tbody>
</table>

3. If no data is available, confirm the data model is being accelerated.
   1. In Enterprise Security, browse to **Audit > Data Model Audit**.
   2. Review the **Acceleration Details** panel for information about the data model acceleration status, such as when the latest data model acceleration occurred, or whether it is 100% complete. See Configure data models for Splunk Enterprise Security in the *Installation and Upgrade Manual*.

4. If the data model acceleration status is as expected, validate that additional required data sources are available. For example, the **User Activity** dashboard uses additional data sources.

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Data type</th>
<th>Data source</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Activity</td>
<td>Lookups</td>
<td>The <strong>Cloud Domains</strong>, <strong>Corporate Email Domains</strong>, and <strong>Corporate Web Domains</strong> lookup files.</td>
</tr>
<tr>
<td></td>
<td>Identities</td>
<td>The <strong>Identity fields</strong>: bunit, email, watchlist, work_city, work_country,</td>
</tr>
</tbody>
</table>
work_lat, and work_long. For more details, see Identity lookup fields in this manual.

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Data type</th>
<th>Data source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>* High Volume Email Activity with Non-corporate Domains</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Watchlisted Event Observed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Web Uploads to Non-corporate Sites by Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Impossible Travel Events Detected For Users</td>
</tr>
</tbody>
</table>

Access Anomalies

**Dashboard requirements matrix for Splunk Enterprise Security**

The Enterprise Security dashboards rely on events that conform to the Common Information Model (CIM), and are populated from data model accelerations unless otherwise noted.

**Dashboard panel to data model**

*A - E*

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Anomalies</td>
<td>Geographically Improbable Accesses Relies on the gia_summary summary index, which is populated by the Access - Geographically Improbable Access - Summary Gen search. That search references the Authentication.app, .src, .user</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Authentication data model.</td>
</tr>
<tr>
<td>Concurrent Application Accesses</td>
<td>Authentication.app, .src, .user</td>
</tr>
<tr>
<td>Access Center</td>
<td>Access Over Time By Action</td>
</tr>
<tr>
<td></td>
<td>Access Over Time By App</td>
</tr>
<tr>
<td></td>
<td>Top Access By Source</td>
</tr>
<tr>
<td></td>
<td>Top Access By Unique User</td>
</tr>
<tr>
<td>Access Search</td>
<td>First Time Access - Last 7 days</td>
</tr>
<tr>
<td></td>
<td>Inactive Account Usage - Last 90 days</td>
</tr>
<tr>
<td></td>
<td>Completely Inactive Accounts - Last 90 days</td>
</tr>
<tr>
<td></td>
<td>Account Usage For Expired Identities - Last 7 days</td>
</tr>
<tr>
<td>Account Management</td>
<td>Account Management Over Time</td>
</tr>
<tr>
<td></td>
<td>Account Lockouts</td>
</tr>
</tbody>
</table>

188
<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Center</td>
<td>All_Changes.Account_Management,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>.src_user</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All_Changes.Account_Management,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>.action</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assets By Priority</td>
<td>Assets And Identities</td>
<td>All_Assets.priority, .bunit, .category,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.owner</td>
</tr>
<tr>
<td></td>
<td>Asset Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset</td>
<td>Asset Investigator</td>
<td>Based on swim lane selection</td>
<td></td>
</tr>
<tr>
<td>Investigator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dashboard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Integrity Control By Index</td>
<td>Incident Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sensitive Data</td>
<td>None. Calls a REST search</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>on indexes checking for</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>data integrity controls.</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Default Account Usage Over Time</td>
<td>Authentication</td>
<td>Authentication.Default_Authentication,</td>
</tr>
<tr>
<td>Account</td>
<td>By App</td>
<td></td>
<td>.action, .app</td>
</tr>
<tr>
<td>Activity</td>
<td>Default Accounts In Use</td>
<td></td>
<td>Authentication.user_category, .dest, .user</td>
</tr>
<tr>
<td></td>
<td>Default Local</td>
<td>None. Calls useraccounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tracker lookup</td>
<td></td>
</tr>
</tbody>
</table>

189
<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Activity</td>
<td>Top DNS Query Sources</td>
<td>Network Resolution DNS</td>
<td>DNS.message_type, DNS.src</td>
</tr>
<tr>
<td></td>
<td>Top DNS Queries</td>
<td></td>
<td>DNS.message_type, DNS.query</td>
</tr>
<tr>
<td></td>
<td>Queries Per Domain</td>
<td></td>
<td>DNS.message_type, DNS.query</td>
</tr>
<tr>
<td></td>
<td>Recent DNS Queries</td>
<td></td>
<td>DNS.message_type</td>
</tr>
<tr>
<td></td>
<td>DNS Search</td>
<td></td>
<td>DNS.message_type, DNS.reply_code, DNS.dest, DNS.src,DNS.query_type, DNS.query, DNS.answer</td>
</tr>
<tr>
<td>Email Activity</td>
<td>Top Email Sources</td>
<td>Email</td>
<td>All_Email.src</td>
</tr>
<tr>
<td></td>
<td>Large Emails</td>
<td></td>
<td>All_Email.size, src, .src_user, .dest</td>
</tr>
<tr>
<td></td>
<td>Rarely Seen Senders</td>
<td></td>
<td>All_Email.protocol, .src, .src_user, .recipient</td>
</tr>
<tr>
<td></td>
<td>Rarely Seen Receivers</td>
<td></td>
<td>All_Email.protocol, .src, .recipient</td>
</tr>
<tr>
<td>Email Search</td>
<td></td>
<td></td>
<td>All_Email.protocol, .recipient, .src, .src_user, .dest</td>
</tr>
<tr>
<td>Endpoint Changes</td>
<td>Endpoint Changes By Action</td>
<td>Change</td>
<td>All_Changes.Endpoint_Changes, .action</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>Endpoint Changes By Type</td>
<td>Data Model</td>
<td>All_Changes.Endpoint_Changes, .object_category</td>
</tr>
<tr>
<td></td>
<td>Endpoint Changes By System</td>
<td>Data Model</td>
<td>All_Changes.Endpoint_Changes, .object_category, .dest</td>
</tr>
</tbody>
</table>

**F - M**

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarder Audit</td>
<td>Event Count Over Time By Host</td>
<td>None. Calls host_eventcount macro and search.</td>
<td></td>
</tr>
<tr>
<td>Forwarder Audit</td>
<td>Hosts By Last Report Time</td>
<td>Endpoint.Processes.cpu_load_percent, .mem_used, .process_exec, Endpoint_Ports_.fillnull_dest.dest</td>
<td></td>
</tr>
<tr>
<td>Forwarder Audit</td>
<td>Splunkd Process Utilization</td>
<td>Endpoint</td>
<td>All_Application_State.Services.start_mode, .status, .service</td>
</tr>
<tr>
<td>HTTP Category Analysis</td>
<td>Category Distribution</td>
<td>Web.src, .category</td>
<td></td>
</tr>
<tr>
<td>HTTP Category Analysis</td>
<td>Category Details</td>
<td>Web.src, .dest, .category,</td>
<td></td>
</tr>
<tr>
<td>HTTP User Agent Analysis</td>
<td>User Agent Distribution</td>
<td>Web.http_user_agent_length, .http_user_agent</td>
<td></td>
</tr>
<tr>
<td>HTTP User Agent Analysis</td>
<td>User Agent Details</td>
<td>Web.http_user_agent_length, .src, .dest, .http_user_agent</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>All_Identities.priority, .bunit, .category</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Identity Center</td>
<td>Identities By Priority</td>
<td>Assets and Identities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identities By Business Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identities By Category</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Investigator</td>
<td>Identity Information</td>
<td>Based on swim lane selection</td>
<td></td>
</tr>
<tr>
<td>Incident Review Audit</td>
<td>Review Activity By Reviewer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Reviewers</td>
<td>None. Calls a search over the es_notable_events KV Store collection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notable Events By Status - Last 48 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notable Events By Owner - Last 24 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recent Review Activity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indexing Audit</td>
<td>Events Per Day Over Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events Per Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Center</td>
<td>Events Per Index (Last Day)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attacks Over Time By</td>
<td>Intrusion Detection</td>
<td>IDS_Attacks.severity</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Attacks</td>
<td>IDS_Attacks.dest, .src, .signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scanning Activity (Many Attacks)</td>
<td>IDS_Attacks.signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New Attacks</td>
<td>IDS_Attacks.ids_type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IDS_Attacks.severity, .category, .signature, .src, .dest</td>
<td></td>
</tr>
<tr>
<td>Intrusion Search</td>
<td>Investigations</td>
<td>None. Calls a search over the investigation_event KV Store collection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Investigation timelines</td>
<td>None. Calls a search over the investigation KV Store collection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Investigation note attachments</td>
<td>None. Calls a search over the investigation_attachment KV Store collection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action history</td>
<td>None. Calls one of five different searches. See Manage investigations in Splunk Enterprise Security.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Investigation workbench artifacts</td>
<td>None. Calls a search over the investigation_leads KV Store collection.</td>
<td></td>
</tr>
<tr>
<td>Investigation workbench</td>
<td>Authentication Data</td>
<td>Authentication.app, .action, .src, .src_user, .dest, .dest_port, .ssl_is_valid, .ssl_validity_window, .ssl_hash, .ssl_serial, .ssl_subject, .ssl_start_time, .ssl_end_time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Certificate Activity</td>
<td>Certificates.SSL, .src, .src_port, .dest, .dest_port, .ssl_is_valid, .ssl_validity_window, .ssl_hash, .ssl_serial, .ssl_subject, .ssl_start_time, .ssl_end_time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Computer Inventory</td>
<td>Compute_Inventory.All_Inventory, .os, .vendor_product, .user, .dest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Data</td>
<td>Network_Resolution.DNS, DNS.dest, .query, .query_count, .message_type, .answer, .reply_code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email Data</td>
<td>Email.All_Email, .src, .dest, .src_user, .action, .recipient, .recipient_count, .subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Filesystem Changes</td>
<td>Change.All_Changes, .user, .dest, .action, .status, Change.All_Changes.Endpoint_Changes.Filesystem_Changes.All_Changes.Filesystem_Changes.Filesystem_Changes.file_name, .file_hash, .file_path, .file_size, .file_create_time, .file_modify_time, .file_access_time</td>
<td></td>
</tr>
<tr>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>IDS Alerts</td>
<td>Intrusion Detection</td>
<td>Intrusion_Detection.IDS_Attacks, .user, .src, .dest, .severity, .category, .signature, .ids_type, .vendor_product, .dvc</td>
<td></td>
</tr>
<tr>
<td>Latest OS Updates</td>
<td>Updates</td>
<td>Updates.status, .user, .dest, .signature_id, .signature, .vendor_product</td>
<td></td>
</tr>
<tr>
<td>Network Session Data</td>
<td>Network Sessions</td>
<td>Network_Sessions.All_Sessions, .src_ip, .dest_ip, .dest_nt_host, .tag, .action, .vendor_product</td>
<td></td>
</tr>
<tr>
<td>Network Traffic Data</td>
<td>Network Traffic</td>
<td>Network_Traffic.All_Traffic, .packets, .src_ip, .dest_ip, .user, .transport, .action, .src, .src_port, .dest, .dest_port</td>
<td></td>
</tr>
<tr>
<td>Notable Events</td>
<td>Incident Management</td>
<td>Incident_Management.Notable_Events, .user, .src, .dest, .rule_name, .severity, .urgency, .security_domain, .status_label, .owner, .savedsearch_description</td>
<td></td>
</tr>
<tr>
<td>Port Activity</td>
<td>Endpoint</td>
<td>Endpoint.Ports, .dest_port, .transport, .process_id</td>
<td></td>
</tr>
<tr>
<td>Process Activity</td>
<td>Endpoint</td>
<td>Endpoint_Application_State, .dest, .user, .process_name, .process</td>
<td></td>
</tr>
<tr>
<td>Registry Activity</td>
<td>Change</td>
<td>Change.All_Changes, .user, .dest, .action, .status, .object, .object_path, .object_attrs, .object_id, .Endpoint_Changes.Registry_Changes</td>
<td></td>
</tr>
<tr>
<td>Risk Scores</td>
<td>Risk Analysis</td>
<td>Risk.All_Risk, .risk_score, .risk_object_type, .risk_object</td>
<td></td>
</tr>
<tr>
<td>Service Activity</td>
<td>Endpoint</td>
<td>Endpoint.Processes, .user_id, .process_exec, .process_id</td>
<td></td>
</tr>
<tr>
<td>System Vulnerabilities</td>
<td>Vulnerabilities</td>
<td>Vulnerabilities.Vulnerabilities, .user, .dest, .severity, .signature, .category, .vendor_product</td>
<td></td>
</tr>
<tr>
<td>User Account Changes</td>
<td>Change</td>
<td>Change.All_Changes, .user, .dest, .action, .status, .object, .object_path, .object_attrs, .object_id, .Account_Management</td>
<td></td>
</tr>
<tr>
<td>Malware Center</td>
<td>Malware Activity Over Time By Action</td>
<td>Malware Attacks.action</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malware Activity Over Time By Signature</td>
<td>Malware Attacks.signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Infections</td>
<td>Malware Attacks.signature, .dest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New Malware - Last 30 Days</td>
<td>None. Calls malware_tracker lookup.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malware Operations</th>
<th>Clients By Product Version</th>
<th>None. Calls malware_operations_tracker lookup.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clients By Signature Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oldest Infections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeat Infections</td>
<td>Malware Attacks.action, .signature, .dest</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malware Search</th>
<th>Malware Attacks.action, .file_name, .user, .signature, .dest</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Managed Lookups Audit</th>
<th>Lookups</th>
<th>None. Calls</th>
<th>rest/services/data/transforms/managed_lookups</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Modular Action Center</th>
<th>Action Invocations Over Time By Name</th>
<th>Splunk Audit Logs</th>
<th>Modular_Actions.Modular_Action_Invocations, .action_name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Top Actions By Name</td>
<td></td>
<td>Modular_Actions.Modular_Action_Invocations, .action_mode, .user, .duration, .search_name, .rid, .sid</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Top Actions By Search</td>
<td>Modular_Actions.Modular_Action_Invocations, .action_name, .action_mode, .user, .search_name, .rid, .sid</td>
<td></td>
</tr>
</tbody>
</table>

### N - S

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Changes</td>
<td>Network Changes By Action</td>
<td>Change</td>
<td>All_Changes.Network_Changes, .action</td>
</tr>
<tr>
<td></td>
<td>Network Changes By Device</td>
<td></td>
<td>All_Changes.Network_Changes, .dvc</td>
</tr>
<tr>
<td>New Domain Analysis</td>
<td>New Domain Activity</td>
<td>Web</td>
<td>Web.dest</td>
</tr>
<tr>
<td></td>
<td>New Domain Activity By Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New Domain Activity By TLD</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Registration Details</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port &amp; Protocol Tracker</td>
<td>Port/Protocol Profiler</td>
<td>Network Traffic</td>
<td>All_Traffic.transport, .dest_port</td>
</tr>
<tr>
<td></td>
<td>Prohibited Or Insecure Traffic Over Time - Last 24 Hours</td>
<td>Network Traffic</td>
<td>All_Traffic.src_category, .dest_category, .src, .dest, .transport, .dest_port</td>
</tr>
<tr>
<td></td>
<td>Prohibited Traffic Details - Last 24 Hours</td>
<td>Network Traffic</td>
<td>All_Traffic.src_category, .dest_category, .src, .dest, .transport, .dest_port</td>
</tr>
<tr>
<td>Protocol Center</td>
<td>New Port Activity - Last 7 Days</td>
<td>None. Calls the application protocols lookup.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connections By Protocol</td>
<td>Network Traffic</td>
<td>All_Traffic.app</td>
</tr>
<tr>
<td></td>
<td>Usage By Protocol</td>
<td></td>
<td>All_Traffic.app, .bytes</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------</td>
<td>------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Top Connection Sources</td>
<td>Data Model</td>
<td>All_Traffic.src</td>
</tr>
<tr>
<td></td>
<td>Usage For Well Known Ports</td>
<td></td>
<td>All_Traffic.bytes, .dest_port</td>
</tr>
<tr>
<td></td>
<td>Long Lived Connections</td>
<td></td>
<td>All_Traffic.src, .src_port, .duration, .dest, .dest_port, .transport</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Analysis</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Risk Modifiers Over Time</td>
<td></td>
<td>All_Risk.risk_score</td>
</tr>
<tr>
<td></td>
<td>Risk Score By Object</td>
<td></td>
<td>All_Risk.risk_score</td>
</tr>
<tr>
<td></td>
<td>Most Active Sources</td>
<td>Risk Analysis</td>
<td>All_Risk.risk_score, .risk_object</td>
</tr>
<tr>
<td></td>
<td>Recent Risk Modifiers</td>
<td></td>
<td>All_Risk.*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Posture</td>
<td>Notable Events By Urgency</td>
<td></td>
<td>None. Calls a search over the es_notable_events KVStore collection.</td>
</tr>
<tr>
<td>Security Posture</td>
<td>Notable Events Over Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Posture</td>
<td>Top Notable Events</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Posture</td>
<td>Top Notable Event Sources</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Session Center</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sessions Over Time</td>
<td>Network Sessions</td>
<td>All_Sessions.Session_*</td>
</tr>
<tr>
<td></td>
<td>Session Details</td>
<td></td>
<td>All_Sessions.*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSL Activity</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SSL Activity By Common Name</td>
<td>Certificates</td>
<td>All_Certificates.SSL.ssl_subject_common_name</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>SSL Cloud Sessions</td>
<td><strong>Data Model</strong></td>
<td>All_Certificates.SSL.ssl_subject_common_name, .src,</td>
<td></td>
</tr>
<tr>
<td>Recent SSL Sessions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Search</td>
<td></td>
<td>All_Certificates.src, .dest, .ssl_subject_common_name, .ssl_subject_email, .ssl_issuer_common_name, .ssl_issuer_organization, .ssl_start_time, .ssl_end_time, .ssl_validity_window, .ssl_is_valid</td>
<td></td>
</tr>
<tr>
<td>Suppressed Events Over Time - Last 24 Hours</td>
<td></td>
<td></td>
<td>Calls a macro to search on notable events.</td>
</tr>
<tr>
<td>Suppression Audit</td>
<td>Suppression History Over Time - Last 30 Days</td>
<td>None</td>
<td>Calls a macro and a search on Summary Gen information.</td>
</tr>
<tr>
<td></td>
<td>Suppression Management Activity</td>
<td></td>
<td>Calls a search by eventtype.</td>
</tr>
<tr>
<td></td>
<td>Expired Suppressions</td>
<td></td>
<td>Calls a search by eventtype.</td>
</tr>
<tr>
<td></td>
<td>Operating Systems</td>
<td>None. Calls system_version_tracker lookup.</td>
<td></td>
</tr>
<tr>
<td>System Center</td>
<td>Top-Average CPU Load By System</td>
<td>Performance</td>
<td>All_Performance.CPU.cpu_load_percent, All_Performance.dest</td>
</tr>
<tr>
<td></td>
<td>Services By System Count</td>
<td></td>
<td>Endpoint.Services</td>
</tr>
<tr>
<td></td>
<td>Ports By System Count</td>
<td></td>
<td>Endpoint.Ports</td>
</tr>
<tr>
<td><strong>T - Z</strong></td>
<td><strong>Endpoint</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

198
<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Activity</strong></td>
<td>Threat Activity Over Time</td>
<td>Intrusion Detection, Network Traffic, and Web. For more details, see Threat Activity Data Sources.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Most Active Threat Collections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Most Active Threat Sources</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Activity Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Artifacts</strong></td>
<td>Threat Overview</td>
<td>None. Calls the threat intelligence KV Store collections. For a list of threat intelligence collections, see Supported types of threat intelligence in Splunk Enterprise Security.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Endpoint Artifacts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Artifacts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email Artifacts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Certificate Artifacts</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Intelligence Audit</strong></td>
<td>Threat Intelligence Downloads</td>
<td>None. Calls a search by REST endpoint.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Intelligence Audit Events</td>
<td>None. Calls a search by eventtype.</td>
<td></td>
</tr>
<tr>
<td><strong>Time Center</strong></td>
<td>Time Synchronization Failures</td>
<td>All_Performance.OS.Timesync, All_Performance.dest, .dest_should_timesync, OS.Timesync.action</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Systems Not Time Synching</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indexing Time Delay</td>
<td>None. Calls the results of a Summary Gen search.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time Service Start Mode Anomalies</td>
<td>Endpoint_Status, Endpoint_Services_fillnull_start_mode, Endpoint_Services_fillnull_status, Endpoint_Services_fillnull_dest .dest_should_timesync, .tag</td>
<td></td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Traffic Center</td>
<td>Traffic Over Time By Action</td>
<td>Network Traffic</td>
<td>All_Traffic.action</td>
</tr>
<tr>
<td>Traffic Center</td>
<td>Traffic Over Time By Protocol</td>
<td>Network Traffic</td>
<td>All_Traffic.transport</td>
</tr>
<tr>
<td>Traffic Center</td>
<td>Scanning Activity (Many Systems)</td>
<td></td>
<td>All_Traffic.dest, .src</td>
</tr>
<tr>
<td>Traffic Center</td>
<td>Top Sources</td>
<td></td>
<td>All_Traffic.src</td>
</tr>
<tr>
<td>Traffic Search</td>
<td>Traffic Size Anomalies Over Time</td>
<td>Network Traffic</td>
<td>All_Traffic.transport, .src</td>
</tr>
<tr>
<td>Traffic Search</td>
<td>Traffic Size Details</td>
<td></td>
<td>All_Traffic.bytes, .dest, .src</td>
</tr>
<tr>
<td>Update Center</td>
<td>Top Systems Needing Updates</td>
<td>Updates</td>
<td>Updates.status, .dest, .signature_id, .vendor_product</td>
</tr>
<tr>
<td>Update Center</td>
<td>Top Updates Needed</td>
<td>Updates</td>
<td>Updates.status, .dest, .signature_id, .vendor_product</td>
</tr>
<tr>
<td>Update Center</td>
<td>Systems Not Updating - Greater Than 30 Days</td>
<td></td>
<td>Updates.dest_should_update, .dest, .signature_id, .vendor_product, .status</td>
</tr>
<tr>
<td>Update Center</td>
<td>Update Service Start Mode Anomalies</td>
<td>Endpoint</td>
<td>Endpoint_Services_fillnull_start_mode, Endpoint_Services_fillnull_status, .Services.service_exec, .tag</td>
</tr>
<tr>
<td>Update Search</td>
<td>Update Search</td>
<td>Updates</td>
<td>Updates.dest_should_update, .status, .dest, .signature_id, .vendor_product</td>
</tr>
<tr>
<td>URL Length</td>
<td>URL Length</td>
<td>Web</td>
<td>Web.http_method, .url</td>
</tr>
<tr>
<td>Dashboard Name</td>
<td>Panel Title</td>
<td>Data Model</td>
<td>Data Model Dataset</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Analysis</td>
<td>Anomalies Over Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL Length Details</td>
<td></td>
<td>Web.url_length, .src, .dest, .url</td>
</tr>
<tr>
<td>User Activity</td>
<td>Users By Risk Scores</td>
<td>Risk Analysis</td>
<td>All_Risk.risk_object</td>
</tr>
<tr>
<td></td>
<td>Non-corporate Web Uploads</td>
<td>Web</td>
<td>Web.bytes, .user, .http_method, .url</td>
</tr>
<tr>
<td></td>
<td>Non-corporate Email Activity</td>
<td>Email</td>
<td>All_Email.size, .recipient, .src_user,</td>
</tr>
<tr>
<td></td>
<td>Watchlisted Site Activity</td>
<td>Web</td>
<td>Web.src, .url</td>
</tr>
<tr>
<td></td>
<td>Remote Access</td>
<td>Authentication</td>
<td>Authentication.src, .user</td>
</tr>
<tr>
<td></td>
<td>Ticket Activity</td>
<td>Ticket Management</td>
<td>All_Ticket_Management.description, .priority, .severity, .src_user</td>
</tr>
<tr>
<td>View Audit</td>
<td>View Activity Over Time</td>
<td>Splunk Audit Logs</td>
<td>View_Activity.app, .view, .user</td>
</tr>
<tr>
<td>Vulnerability Center</td>
<td>Top Vulnerabilities</td>
<td>Vulnerabilities</td>
<td>Vulnerabilities.signature, .dest</td>
</tr>
<tr>
<td></td>
<td>Most Vulnerable Hosts</td>
<td>Vulnerabilities</td>
<td>Vulnerabilities.signature, .severity, .dest</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities By Severity</td>
<td>Vulnerabilities</td>
<td>Vulnerabilities.signature, .severity, .dest</td>
</tr>
<tr>
<td></td>
<td>New Vulnerabilities</td>
<td>Calls vuln_signature_reference lookup.</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Operations</td>
<td>Scan Activity Over Time</td>
<td>Vulnerabilities</td>
<td>Vulnerabilities.dest</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities By Age</td>
<td>Calls vulnerability_tracker lookup.</td>
<td></td>
</tr>
</tbody>
</table>
### Dashboards to Add-on

Add-on dashboards are included in Splunk Enterprise Security. Use the navigation editor to add or rearrange dashboards on the menu bar. For more information about using the navigation editor, see Customize the menu bar in Splunk Enterprise Security.

To view the entire list of dashboards in Enterprise Security, select **Search > Dashboards**.

To review the list of dashboards in Enterprise Security by add-on, use Content Management and filter by app or data model. See Expand Content Management searches to view dependency and usage information in Splunk Enterprise Security.

<table>
<thead>
<tr>
<th>Dashboard Name</th>
<th>Panel Title</th>
<th>Data Model</th>
<th>Data Model Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Search</td>
<td>Delinquent Scanning</td>
<td>Vulnernabilities</td>
<td>Vulnerabilities.dest</td>
</tr>
<tr>
<td>Web Center</td>
<td>Events Over Time By Method</td>
<td>Web</td>
<td>Web.http_method</td>
</tr>
<tr>
<td></td>
<td>Events Over Time By Status</td>
<td>Web</td>
<td>Web.status</td>
</tr>
<tr>
<td></td>
<td>Top Sources</td>
<td>Web.dest, .src</td>
<td>Web.dest, .src</td>
</tr>
<tr>
<td></td>
<td>Top Destinations</td>
<td>Web.dest, .src</td>
<td>Web.http_method, .status, .src, .dest, .url</td>
</tr>
</tbody>
</table>
Extreme Search

How Splunk Enterprise Security uses extreme search

Extreme search enhances the Splunk platform search language with a set of commands. For a list of extreme search commands, see Extreme search commands.

As implemented in Splunk Enterprise Security, you can use the extreme search commands to:

- Build dynamic thresholds based on event data.
- Provide context awareness by replacing event counts with natural language.

For example, in the Enterprise Security Malware Center dashboard, the Key Security Indicator Total Infections displays the total number of systems with malware infections over the last 48 hours.

Splunk ES determines the displayed rate of change by comparing the current count of infections against the count of infected systems from the day before. There is no automatic determination of a normal daily range for infected systems in your environment. The threshold is entirely user-configured. Infections have increased by three, but the value has no context to indicate whether it is a notable increase.

The same indicator using extreme search displays the relevant information, but includes a depth of information that was not available with the default Total Infections indicator.
Using extreme search, Splunk ES calculates the infection count and rate of new infections using a dynamically-updating model. The key security indicator uses contextual and easy-to-understand language. In this case, you know that the total malware infection count is not higher than it would be any other day, and the rate of change in infections is not alarming.

The use of context and concept in extreme search

The core ideas of context and concept are critical to the understanding of extreme search. These ideas are responsible for the data model used for dynamic thresholds by an extreme search command.

1. **Context**: A context defines a relationship to a field or data in numerical terms. The data to be modeled must be represented by numerical values as the result of a search. Example contexts include total network throughput over the last 24 hours or network latency over the last 24 hours.

2. **Concept**: A term that applies to data, representing a qualitative rather than quantitative description. Example concepts include the terms "extreme," "high," "medium," "low," and "minimal".

By combining context and concept, extreme search adds meaning and value to the data.

- The total network throughput over the last 24 hours was Extreme, high, medium, low, or minimal.
- The network latency over the last 24 hours was extreme, high, medium, low, or minimal.

The concept terms describe network activity in both examples, but have different meanings based on the context they are applied to. If your environment reports that total network throughput is minimal, it is a warning. If the environment reports that network latency is minimal, the network is operating normally.

Data models and extreme search

After you choose a context and concept to represent your data, Splunk ES creates a data model. Using the extreme search commands, the data model maps the context and event statistics by concept. Extreme search commands refer to this combined model as a context.

Saved searches update contexts, such as the dynamic threshold context. The saved search searches event data for statistics to update the context. For a list of
the saved searches that update contexts, see Containers, contexts, and saved searches in this topic.

Configuring extreme search for Enterprise Security

The use of extreme search commands in Enterprise Security requires no additional configuration. The default installation of ES provides all contexts used by the extreme search commands and enables the saved searches that maintain them.

- For a list of the contexts and saved searches implemented in Enterprise Security, see Containers, contexts, and saved searches in this topic.
- For a list of the key security indicators that use extreme search, see Extreme search key security indicators in this topic.
- For a list of the correlation searches that use extreme search, see Correlation searches that use extreme search in this topic. All correlation searches are disabled by default.

Correlation searches that use extreme search

All correlation searches in Enterprise Security are disabled by default. See Enable correlation searches in this manual.

Guided Search Creation is not available for correlation searches that use extreme search commands. These correlation searches use extreme search.

<table>
<thead>
<tr>
<th>Search Name</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brute Force Access Behavior Detected</td>
<td>failures_by_src_count_1h</td>
</tr>
<tr>
<td>Brute Force Access Behavior Detected Over One Day</td>
<td>failures_by_src_count_1d</td>
</tr>
<tr>
<td>Abnormally High Number of Endpoint Changes By User</td>
<td>change_count_by_user_by_change_type_1d</td>
</tr>
<tr>
<td>Host Sending Excessive Email</td>
<td>recipients_by_src_1h</td>
</tr>
<tr>
<td>Substantial Increase in Intrusion Events</td>
<td>count_by_signature_1h</td>
</tr>
<tr>
<td>Substantial Increase in Port Activity</td>
<td>count_by_dest_port_1d</td>
</tr>
<tr>
<td>Unusual Volume of Network</td>
<td>count_30m</td>
</tr>
</tbody>
</table>
### Extreme search key security indicators

You can easily identify the key indicators that use extreme search by their use of semantic language instead of numerical values. The key security indicators on each dashboard are enabled by default.

<table>
<thead>
<tr>
<th>Search Name</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access - Total Access Attempts</td>
<td>authentication: count_1d, percentile</td>
</tr>
<tr>
<td>Malware - Total Infection Count</td>
<td>malware: count_1d, percentile</td>
</tr>
<tr>
<td>Risk - Median Risk Score</td>
<td>median_object_risk_by_object_type_1d, percentile</td>
</tr>
<tr>
<td>Risk - Median Risk Score By System</td>
<td>median_object_risk_by_object_type_1d, percentile</td>
</tr>
<tr>
<td>Risk - Median Risk Score By User</td>
<td>median_object_risk_by_object_type_1d, percentile</td>
</tr>
<tr>
<td>Risk - Median Risk Score By Other</td>
<td>median_object_risk_by_object_type_1d, percentile</td>
</tr>
<tr>
<td>Risk - Aggregated Risk</td>
<td>total_risk_by_object_type_1d, percentile</td>
</tr>
<tr>
<td>Risk - Aggregated System Risk</td>
<td>total_risk_by_object_type_1d, percentile</td>
</tr>
<tr>
<td>Risk - Aggregated User Risk</td>
<td>total_risk_by_object_type_1d, percentile</td>
</tr>
<tr>
<td>Risk - Aggregated Other Risk</td>
<td>total_risk_by_object_type_1d, percentile</td>
</tr>
</tbody>
</table>

### Containers, contexts, and saved searches

Enterprise Security stores contexts in objects called containers. A container is both an object in the file system and a logical configuration used to classify contexts. In Enterprise Security, the containers are files with the `.context` extension. A container can contain multiple contexts. You can view the saved searches that generate contexts on the Content Management view in Enterprise Security. See [Create and manage saved searches in Splunk Enterprise Security](https://docs.splunk.com/Documentation/Splunk/9.0.0/EnterpriseSecurity/ESAdministrator/ESAdmin_CreateManageSavedSearches) for more information.
**Note:** Enterprise Security enables the dynamic context saved searches by default.

<table>
<thead>
<tr>
<th>Container name</th>
<th>Context name</th>
<th>App location</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>failures_by_src_count_1h</td>
<td>SA-AccessProtection</td>
</tr>
<tr>
<td></td>
<td>failures_by_src_count_1d</td>
<td></td>
</tr>
<tr>
<td></td>
<td>count_1d</td>
<td></td>
</tr>
<tr>
<td>change_analysis</td>
<td>change_count_by_user_by_change_type_1d</td>
<td>SA-EndpointProtection</td>
</tr>
<tr>
<td>email</td>
<td>destinations_by_src_1h</td>
<td>SA-EndpointProtection</td>
</tr>
<tr>
<td></td>
<td>recipients_by_src_1h</td>
<td></td>
</tr>
<tr>
<td>malware</td>
<td>count_1d</td>
<td>SA-NetworkProtection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Container name</td>
<td>Context name</td>
<td>App location</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>ids_attacks</td>
<td>count_by_signature_1h</td>
<td>SA-NetworkProtection</td>
</tr>
<tr>
<td></td>
<td>count_by_dest_port_1d</td>
<td></td>
</tr>
<tr>
<td>network_traffic</td>
<td>src_count_30m</td>
<td>SA-NetworkProtection</td>
</tr>
<tr>
<td></td>
<td>count_30m</td>
<td></td>
</tr>
<tr>
<td>web</td>
<td>count_by_http_method_by_src_1d</td>
<td>SA-NetworkProtection</td>
</tr>
<tr>
<td>risk</td>
<td>median_object_risk_by_object_type_1d</td>
<td>SA-ThreatIntelligence</td>
</tr>
<tr>
<td></td>
<td>total_risk_by_object_type_1d</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>percentile</td>
<td>SA-Utils</td>
</tr>
</tbody>
</table>
Extreme search example in Splunk Enterprise Security

You can convert existing correlation searches to use extreme search commands. You do not need to make any configuration changes or modifications to use searches converted to use extreme search commands. For a list of extreme search commands, see Extreme search commands.

This example demonstrates how to convert the existing "Brute Force Access Behavior Detected" correlation search to use extreme search commands.

This example is for illustration purposes only. The "Brute Force Access Behavior Detected" correlation search included in Splunk Enterprise Security has already been converted to use extreme search commands.

The Brute Force Access Behavior Detected search

The correlation search "Brute Force Access Behavior Detected" searches for an excessive number of failed login attempts, followed by a successful attempt. The base search finds relevant events, counts the events by type "failure" and looks for a trailing "success" event for every host authentication over the last hour. If the identified events meet a threshold, the search triggers an alert action to create a notable event or other alert types.

"Brute Force Access Behavior Detected" correlation search without extreme search commands:

```
| `datamodel("Authentication","Authentication")` | stats values(Authentication.tag) as tag,count(eval('Authentication.action'=='"failure")) as failure,count(eval('Authentication.action'=='"success")) as success by
```
Without extreme search commands, the search defines a static threshold for the "success" events with the string | search failure>6. The Enterprise Security administrator has to select a threshold value, or accept the default value. If the administrator sets the threshold too low, the search creates a storm of notable events. If they set the threshold too high, the search could miss notable events, creating a potential blind spot to a security threat.

A search that implements extreme search removes the static value and uses, in this example, the authentication data ingested by Splunk Enterprise to determine a notable level of authentication failures in your environment.

1. Examine the data

To use extreme search, you must build a data model for the commands to rely on. To build the data model, you must understand what the data represents and what question you are trying to answer.

In this example, the "Brute Force Access Behavior Detected" correlation search, you know that the count of authentication failures will not go below zero, and may range much higher. A scale of magnitude represents the authentication values being searched.

2. Choose a context

You can choose one of three types of contexts, each requiring three data points.

- Mean average: requires a mean value, a standard deviation, and a total count of events.
- Median average: requires a median value, a standard deviation, and a total count of events.
- Domain: requires a minimum, a maximum, and a total count of events.

In this example, the count of authentication events does not include a negative value and is progressive, so a domain is the best fit for the authentication data.

3. Choose a concept

A concept represents a qualitative description of the data. Splunk Enterprise Security includes predefined concepts for interpreting change, direction, and magnitude as a qualitative value. Concepts are differentiated by the terms used.
• Change uses the terms: "minimally, slightly, moderately, greatly, extremely."
• Direction uses the terms: "decreasing, unchanged, increasing"
• Magnitude uses the terms: "minimal, low, medium, high, extreme"

In this case, the magnitude concept best represents the behavior of authentication failures.

4. Create the context

As described in How Splunk Enterprise Security uses extreme search in this manual, a context has both a name and a container, with the container residing in an app. The "Brute Force Access Behavior Detected" search runs against authentication events, so the context container is called "authentication." The "authentication" container is located in the "SA-AccessProtection" app along with the authentication searches and other objects.

ES includes a pre-initialized authentication context. This context will not represent your environment unless a saved search updates it with events. Splunk Enterprise Security contains this context so that updates will carry a greater weight than the values used during the creation of the context. The domain for this authentication context is defined with a min=0, max=10, and count=0.

For the "Brute Force Access Behavior Detected" search, the context name is chosen to facilitate quick identification: failures_by_src_count_1h.

Create the initial context using example data.

```
| xsCreateUDContext app="SA-AccessProtection" name=failures_by_src_count_1h container=authentication scope=app terms=`xs_default_magnitude_concepts` min=0 max=10 count=0 type=domain
```

This context is a user-defined context because you are specifying the data in the search to make sure that the context works. In the final search, the context is data-defined because it relies on data from the search results of the earlier search.

Display the context, once created:

```
| xsdisplaycontext failures_by_src_count_1h in authentication
```
Before implementing extreme search, the static threshold for authentication failures was six. Using the context `failures_by_src_count_1h`, a count of six is modeled at the end of the term "medium". The model will change after the updated "Brute Force Access Behavior Detected" search searches the authentication data and the saved search that updates the `failures_by_src_count_1h` runs.

List the terms used in a context:

| xslistconcepts failures_by_src_count_1h in authentication

5. Apply the context in the search

You can use the search command `xsWhere` to evaluate a data value against a context. This correlation search uses `xsWhere` to compare the count of authentication failures against the context `failures_by_src_count_1h` to determine if the count represents a value above "medium."

In this example, a concept of medium represents the range of values that change after the context is updated with data. A saved search updates the context. If the count of events identified by the saved search is greater than medium, the correlation search using extreme search will trigger an alert action and create a notable event.

"Brute Force Access Behavior Detected" with extreme search capabilities

| `datamodel("Authentication","Authentication")` | `stats values(Authentication.tag) as tag,count(eval('Authentication.action'=='failure')) as failure,count(eval('Authentication.action'=='success')) as success by Authentication.src | `drop_dm_object_name("Authentication")` | `search success>0 | xswhere failure from failures_by_src_count_1h in authentication is above medium | `settags("access")` |
6. Update the context

A search threshold can be dynamic because it uses a saved search to update a context. The saved searches included with ES that generate context information for extreme search end with "Context Gen" to provide easy identification.

The domain context used by the "Brute Force Access Behavior" correlation search requires values for minimum, maximum, and count. Those values are drawn from the authentication data model. The "Access - Authentication Failures By Source - Context Gen" saved search that generates the failures_by_src_count_1h context for the "Brute Force Access Behavior" correlation search.

For the failures_by_src_count_1h context, the results of the context generating search change the maximum value to a multiple of the median to prevent outliers from skewing the underlying context and potentially introducing oversights.

"Access - Authentication Failures By Source - Context Gen" saved search

```bash
| tstats `summariesonly` count as failures from datamodel=Authentication where Authentication.action="failure" by Authentication.src, _time span=1h | stats median(failures) as median, min(failures) as min, count as count | eval max = median*2 | xsUpdateDDContext app="SA-AccessProtection" name=failures_by_src_count_1h container=authentication scope=app
```

This search updates the failures_by_src_count_1h context with xsUpdateDDContext. In this case, the data from the search is added to the context, creating a historical trend that informs the context. This is different from the context search in step 4 that used xsUpdateUDContext, because the first part of the search supplies the data used by the context, rather than being supplied by the user.

The saved search, "Access - Authentication Failures By Source - Context Gen," is scheduled to run once per day by default. The correlation search, "Access - Brute Force Access Behavior Detected - Rule," is a real-time search only.

- See Tstat for further information about tstats syntax.
- See Stats for further information about stats syntax.
- See Eval for further information about eval syntax.
7. Use hedges to modify the results

Hedges are semantic terms that modify the range represented by a concept. Use a hedge to limit, shrink, or modify the shape of the curve that a concept term uses to model the data. The hedges "above" and "below" are useful for alerting searches as they redefine the range of values that will match.

The "Brute Force Access Behavior Detected" correlation search using extreme search applies a hedge so an alert action triggers only when the count of failures is "above medium."

Examples of a concept with various hedges applied:

<table>
<thead>
<tr>
<th>Hedge example</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>xsDisplayConcept medium from failures_by_src_count_1h in authentication</td>
</tr>
<tr>
<td></td>
<td>xsDisplayConcept very medium from failures_by_src_count_1h in authentication</td>
</tr>
<tr>
<td></td>
<td>xsDisplayConcept above medium from failures_by_src_count_1h in authentication</td>
</tr>
<tr>
<td></td>
<td>xsDisplayConcept below medium from failures_by_src_count_1h in authentication</td>
</tr>
<tr>
<td></td>
<td>xsDisplayConcept around medium from failures_by_src_count_1h in authentication</td>
</tr>
</tbody>
</table>

The synonyms.csv lookup file in the Splunk_SA_ExtremeSearch app contains the extreme search hedges.

Summary

The "Brute Force Access Behavior Detected" correlation search using extreme search is included with Splunk Enterprise Security. The context generation search runs and updates the context on a recurring interval. The correlation search references the context, and the concept within the context sets the threshold. The concept is hedged to "above medium" so that the correlation search will only create a notable event when the count of failed authentications followed by a successful authentication is "high" or "extreme."

In plain language, extreme search transformed the "Brute Force Access Behavior Detected" correlation search from "find all authentication attempts where X count of failed authentications are followed by a successful authentication" to "find all
authentication attempts where a high or extreme number of failed authentications are followed by a successful authentication."

**Extreme search commands**

<table>
<thead>
<tr>
<th>Search command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xsWhere</td>
<td>Used to match a concept within a specified context, and determine compatibility.</td>
</tr>
<tr>
<td>xsFindBestConcept</td>
<td>Used when evaluating a search count and comparing the count to a context. The closest match returns the term used by the concept. The key security indicators use this command.</td>
</tr>
<tr>
<td>xsUpdateDDContext</td>
<td>Used to update a data-defined context. A scheduled report that calls &quot;xsUpdateDDContext&quot; builds a context that represents a historical view.</td>
</tr>
<tr>
<td>xsListContexts</td>
<td>Used to list all contexts in a container</td>
</tr>
<tr>
<td>xsListConcepts</td>
<td>Used to list all concepts in a context</td>
</tr>
<tr>
<td>xsDisplayContext</td>
<td>Used to display the range of values in a context, including the terms used in the concept.</td>
</tr>
<tr>
<td>xsDisplayConcept</td>
<td>Used to display the range of values used for a concept.</td>
</tr>
</tbody>
</table>