Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Configure correlation searches in Splunk Enterprise Security

Generated: 6/12/2022 11:14 am

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 most correlation searches disabled so that you can choose the searches that are most relevant to your security use cases.

However, the following risk and UEBA correlation searches may be enabled by default in Splunk Enterprise Security:

- `ATT&CK Tactic Threshold Exceeded for Object Over Previous 7 days`
- `Risk Threshold Exceeded for Object Over 24 Hour Period`
- `UEBA Threat Detected`
- `UEBA Threat Detected (Risk)`
- `UEBA Anomaly Detected (Risk)`

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

You can change the default search type of a correlation search from real-time to scheduled. In general, real-time searches have more impact on your overall cluster performance than scheduled searches. Splunk Enterprise Security uses indexed real-time searches by default for some correlation searches.

To change from real-time to scheduled, complete the following steps.

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** ~ **+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 Platform, see Prioritize concurrently scheduled reports in Splunk Web in the Splunk Cloud Platform *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.

Use security framework annotations in correlation searches

Use annotations to enrich your correlation search results with security framework mappings. You also see these annotations as field labels in Incident Review and Risk Analysis.

1. Select **Configure > Content > Content Management**.
2. Click the title of the correlation search you want to edit.
3. You can use annotations for industry-standard mappings or unmanaged annotations for custom mappings.

The annotations are stored in `action.correlationsearch.annotations` in JSON format in the savedsearches.conf file. MITRE ATT&CK definitions are pre-populated in the security_framework_annotations.csv file. You don't need to revise this unless you want to display non-default info in the annotations dropdown field.

When annotated, the correlation searches do not automatically display in the use case library for use with the Framework Mapping filter. To add correlation searches to analytic stories, see Edit or add Analytic Story details.

Annotations

Use annotations to enrich your correlation search results with the context from industry-standard mappings.

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

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

3. (Conditional) If you are using the adaptive response action of **Notable** because you want see annotations as field labels in Incident Review, and if you are editing a correlation search that does not use the Risk data model, then you need to append an eval statement for the `annotations.mitre_attack` field to end of the correlation search, such as:

```
| from datamodel:"Identity_Management"."Expired_Identity_Activity" | stats max("_time") as
"lastTime",latest("_raw") as "orig_raw",count by "expired_user" | rename "expired_user" as "user" |
eval annotations.mitre_attack="T1027"
```
4. (Conditional) If you are using the adaptive response action of **Risk Analysis** because you want see annotations as field labels in the Risk Analysis Dashboard, the annotations show up automatically. For more information about creating risk factors to adjust risk scores for risk objects, see Create risk factors in Splunk Enterprise Security.
5. Click **Save**.
6. Search your MITRE ATT&CK intelligence download data to verify the annotation details as follows:

```
| inputintelligence mitre_attack
```

Consider MITRE ATT&CK annotations as an example. At search time, the **mitre_attack_enrichment** automatic lookup uses the mitre technique id that you selected, and it outputs additional industry-standard context as event fields. Some examples include, but are not limited to, the following: `annotations.mitre_attack.mitre_description`, `annotations.mitre_attack.mitre_detection`, `annotations.mitre_attack.mitre_platform`, `annotations.mitre_attack.mitre_software_name`, `annotations.mitre_attack.mitre_software_platform`, `annotations.mitre_attack.mitre_tactic`, `annotations.mitre_attack.mitre_technique`, `annotations.mitre_attack.mitre_technique_id`, `annotations.mitre_attack.mitre_url`.

Unmanaged Annotations

Unmanaged annotations won't be enriched with any industry-standard context.

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

Consider an unmanaged annotation as an example. In your events, you will see `annotations.<unmanaged_framework_name>=<unmanaged_tactic_id_value>`.

Add additional security frameworks to your annotations

While the MITRE ATT&CK framework annotations are available by default, you can also add other industry-standard frameworks. You can add them from scratch, but clone the existing mitre_attack for convenience.

Add the intelligence download by completing the following steps:

1. From the Splunk Enterprise menu bar, select **Settings > Data inputs > Intelligence Downloads**.
2. Filter on **mitre**.
3. Click the **Clone** action for **mitre_attack**.
4. Type a name for the industry-standard framework.
5. Revise the description.
6. Leave **Is Threat Intelligence** unchecked.
7. Revise the type.
8. Revise the URL.
9. Click **Save**.

Add the lookup definition by completing the following steps:

1. From the Splunk Enterprise menu bar, select **Settings > Lookups > Lookup definitions**.
2. Filter on **mitre**.
3. Click the **Clone** action for **mitre_attack_lookup**.
4. Leave **Type** as-is.
5. Type a name for the industry-standard framework.
6. Revise the **Supported fields**.
7. Click **Save**.

Add the automatic lookup by completing the following steps:

1. From the Splunk Enterprise menu bar, select **Settings > Lookups > Automatic lookups**.
2. Filter on **mitre**.
3. Click the **Clone** action for **source::...- Rule : LOOKUP-mitre_attack_enrichment**.
4. Leave **Destination app** as-is.

5. Leave **Apply to** as-is. The named* **source::...- Rule** is necessary.
6. Type a name for the industry-standard framework.
7. Revise all the fields.
8. Click **Save**.

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 Platform, see Configure alert trigger conditions in the Splunk Cloud Platform *Alerting Manual*.

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.

If you have throttling set for an existing alert action, editing the details of the alert or the throttle configuration causes the throttling to be disregarded. This includes any changes to fields you throttle on, the SPL in the correlation search, the cron schedule, and so on. The change causes the throttle file, which notes how long to ignore events, to be removed. Therefore the throttling does not occur until the next event is triggered based on the new parameters.

Clone a correlation search

You can clone correlation searches to create your own, rather than starting from scratch.

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. Scroll to find the name of the correlation search to clone.
4. In the Actions column of the correlation search, click **Clone**.
5. Type a unique name for the New Search Label. This field is case sensitive, so a name of **Account Deleted CLONE** is different than **Account Deleted Clone**.
6. (Optional) Chose an App from the drop-down list.
7. Click **Save**.
8. To edit the cloned correlation search immediately, click the link in the success message pop-up window. Alternately, you can close the pop-up window and edit the clone later.
9. Your cloned correlation search appears in **Content > Content Management** within a few minutes. The status is disabled by default.
10. Click **Enable** when you're ready to use it.

See also

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