Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Customize threat match searches using Splunk Enterprise Security

Generated: 6/13/2022 9:46 am

Customize threat match searches using Splunk Enterprise Security

Use the Splunk Enterprise Security UI to edit threat match searches that are available in the app to enrich the incoming data in your deployment with threat intelligence.

Configuring the threat match specifications in the UI automatically populates the settings in the `[threat match]` stanza for the DSS Threat intelligence module in the `inputs.conf` configuration file. The threat match settings are used by the custom search builder to construct the SPL for the threat match searches.

The events generated by these threat match searches are tagged for the Threat intelligence data model and populate the `threat_activity` index. As a security analyst, you may review the items in the `threat_activity` index on the Threat Activity dashboard to investigate threats.

You can customize the threat match searches by making the following changes:

- Add or remove extra data models
- Change the time interval
- Change the earliest or latest time
- Add or remove aggregates
- Add or remove datasets

If you upgrade your instance of Splunk Enterprise Security app to version 6.4.0, you may see a conflict between the previous threat gen searches that you had defined in the savedsearches.conf and the new dynamically generated threat gen searches by the custom search builder. If this occurs, you may receive a health check warning "Threat gen searches may cause conflicts with default threat gen searches". You must delete the existing threat gen searches in the savedsearches.conf file to remove this conflict.

Edit threat match settings to customize threat match searches

Edit the threat match settings to generate the SPL for threat match searches and enrich your data with threat intelligence.

Prerequisite
You have an administrator role with `edit_modinput_threatmatch` capabilities to edit the threat match settings.

Steps

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**. This displays the list of downloaded intelligence documents in the app that are sorted by Interval, Type, URL, Weight, and Status.
2. Click on the **Threat Matching** tab.
   Use the following table to identify the available threat match sources and the associated configuration settings for the threat match searches:

Setting	Description	Example
Source	Type of threat match sources in your deployment.	`certificate_common_name`, `certificate_serial`, `certificate_unit`, `dest`, `certificate_organization`, `domain`
Interval	The cron interval at which the search runs.	`0,30***` For more information on cron formats, see Commonly used cron field formats.
Earliest Time	Time when the search starts.	`-45m@m`

Setting	Description	Example
Latest Time	Time when the search completes.	`+0s`
Match Fields	Fields to match against to generate threats.	`All_Certificates.SSL.ssl_issuer_common_name` `All_Certificates.SSL.ssl_subject_common_name`
Status	Enable or disable the threat match search	`Enable`, `Disable`

You can expand the threat match source to view the SPL generated for the threat match search.

3. Click on the threat match source to edit the threat match settings.
   This opens the **Edit Threat Match Configuration** dialog.

   You may only enable, disable, or edit existing threat match sources using this UI. You may not use the editor to create new threat match sources.

   Use the following table to edit the specific configuration settings for your threat match search:

Setting	Description
Name	Name of the threat match stanza.
Source	Name of the threat match source or the threat artifact.
Earliest Time	Time when the threat match search starts.
Latest time	Time when the threat match search completes.
Interval	Cron interval at which the threat match search runs.
Max Aggregate values	Maximum number of aggregate values for the threat match search.
Datasets	Datasets currently included in the threat match search.

   You may delete any existing dataset from the threat match search by clicking on the **X** button next to the specific dataset. You may also edit any existing dataset included in the threat match search by clicking the pencil icon next to the specific dataset. You may enable or disable an existing dataset by clicking on the `Enable` or `Disable` button for the dataset. You may also remove specific fields against which you want to match in the threat match searches.

To add a new dataset to the threat match search

1. Click on the **Add Dataset** to add more datasets to the threat match search.
   This opens the **Add a Dataset** dialog.
2. Select the data model for the dataset from the **Datamodel** drop down to specify the source of the dataset.
   For example: Alerts, Authentication, Certificates, Change Analysis, Inventory, Database, and so on.
3. Select the object using the **Object** drop down menu to specify the type of object used from the datamodel.
   For example: If you selected **Authentication** as the datamodel type, you can select various objects like: Failed_Authentication, Default_Authentication, Successful_Authentication, Insecure_Authentication, and so on.
4. Specify the boolean clause to filter out events for the threat match search in the **Event Filter** field. The Boolean clause translated to the where clause within the search SPL.
5. Specify the **Match field** field to select the fields to match on and generate threats. For example: source, sourcetype, and so on.
6. Click **Add Aggregate** to identify the datasets that the search may retrieve from the datamodel.
7. Specify the **alias** for the **field** to rename the aggregate.
   For example, you may rename the aggregate `All_Certificates.src` to the alias `src`; or, you may rename the

aggregate `All_Certificates.dest` to the alias `dest` while specifying the settings for the threat match search.

8. Click **Save Dataset** to build the threat match search.