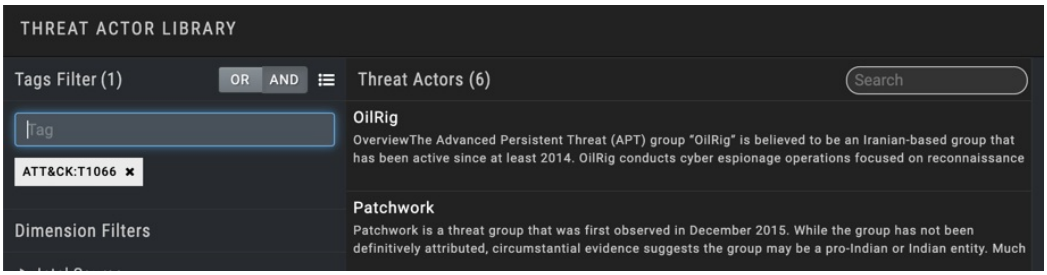
# MANAGING THREAT ACTORS IN SECURITY VALIDATION

## Locating a Threat Actor

The Threat Actor Library has three features to help you locate a specific Threat Actor: Tags, Dimension Filters, and a text-based search. These can be used separately or together.

### To filter the list using Tags

1. Go to **Library > Threat Actors**.
2. Click in the **Tags** field and select a tag from the list. You can also click in the **Tag** field and enter a full or partial tag name. The list is updated automatically as you type.




Threat Actor Library Tags filter

3. Repeat step 2 until you have selected all Tags that you want.
4. Click **OR** to filter the list with a logical OR of the selected Tags (displays Threat Actors with any of the selected Tags); Click **AND** to filter the list with a logical AND of the selected Tags (displays Threat Actors with ALL of the selected Tags).

### To use text search to locate a specific Threat Actor

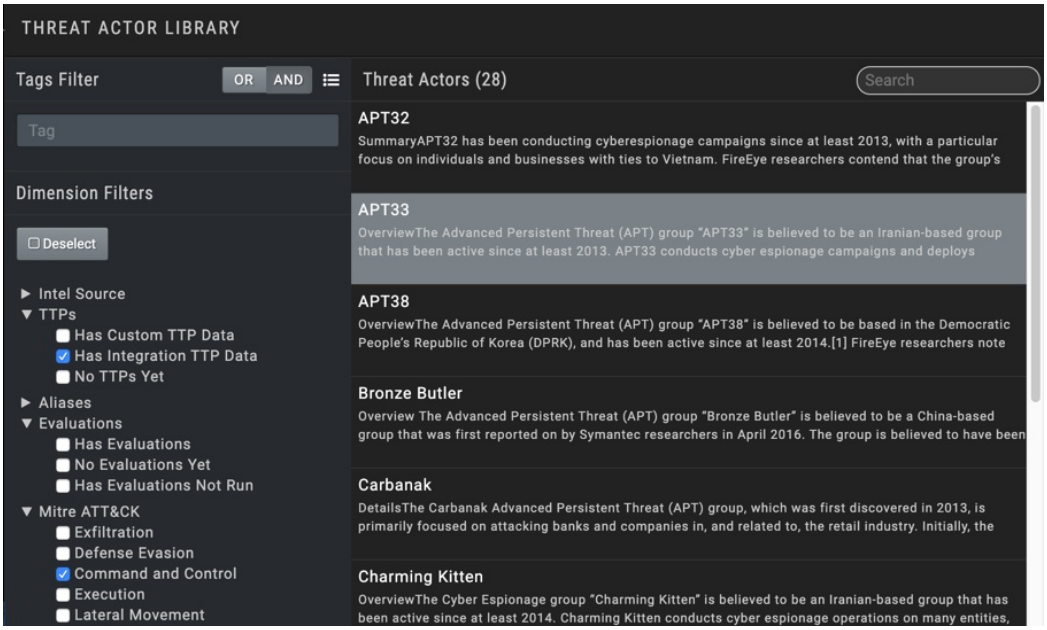
The Threat Actor search field looks for matches everywhere in the profile, including the Name, Overview, TTP Tags, and Aliases.

1. Go to **Library > Threat Actors**.
2. Click in the **Search** field and enter full or partial search text. The list is updated automatically as you type.

### To use dimension filters to locate a specific Threat Actor

For a full list of the available dimensions, see **Understanding Threat Actor Information in Security Validation (https://docs.mandiant.com/home/msv-threat-actor-library)**.

1. Go to **Library > Threat Actors**.
2. In the **Dimension Filters** section, expand a Dimension Category and select one or more Dimensions. The list of Threat Actors automatically filter to include only the Threat Actors that match the selected Dimension.
3. You can filter the list further by selecting another Dimension for the same Dimension Category or from another Dimension Category.
    - If you select two Dimensions from the same category, the Threat Actors must match one of the Dimensions selected, not both, to be included in the filtered list.
    - If you select two Dimensions from different categories, the Threat Actors must match both the Dimensions to be included in the filtered list.



Threat Actor Library Dimension Filter

If an Evaluation runs but finishes with a status of Errored, the system still counts it as an Evaluation that has run. This means Threat Actors that only have Evaluations in this state are not included when you use the Dimension Filter Has Evaluation Not Run.

## Adding a Threat Actor

When you manually add a new Threat Actor, its Information is saved under the Custom tabs of the Threat Actor.

Evaluations are not automatically generated for manually added Threat Actors. However, you can associate an Evaluation with a Threat Actor by adding one or more of its Alias tags to the Evaluation in the Evaluations Library.

## To Add A Threat Actor

1. Go to **Library > Threat Actors**.
2. Click **Add Threat Actor**.
3. Enter the Name.
4. Optional: Select the Country.
5. Click **Save**.
6. In the **Overview** section, click **Add Now**.
    a. Add text as desired. Information can be entered in plain text, markdown syntax, and HTML markup syntax.
    b. Click **Save**.
7. In the **Tactics, Techniques, and Procedures** section, click **Add Now**.
    a. Select a Tag from the list. You can also click in the enter Tag field and type a full or partial tag to limit the list of available tags. If the tag you want to add doesn't exist, type it and then click **New TTP: <tag>**.
    b. Repeat the process until you've added all your tags.
8. In the **Aliases** section, click **Add Now**. The list of existing Aliases displays.
    a. Select an Alias from the list. You can also click in the enter Alias field and type a full or partial Alias to limit the list of available options. If the Alias you want to add doesn't exist, type it and then click **New Alias:** <alias>.

b. Repeat the process to add additional aliases.

### Editing a Threat Actor

In addition to information provided from your Threat Intelligence Integrations, you can change the display name and country of the Threat Actor as well as add information to any of the Threat Actors. This includes adding Overviews, TTPs, and Aliases. Information that you enter is saved under a tab in each section labeled Custom.

> Evaluations will be generated automatically by the system based on the Threat Intelligence Integration-provided ATT&CK tags in the TTP section. These will be listed at the end of each Threat Actor Profile and in the Evaluation Library. Threat Actor Evaluations will all begin with S400.

### To Edit a Threat Actor

1. Go to **Library > Threat Actors**.
2. Locate the Threat Actor you want to edit and click on it to bring up the Threat Actor Profile.
3. To update the Name or Country:
   a. Click the Flag icon or Edit next to the Threat Actor name.
   b. Optional: Update the Name.
   c. Optional: Select the Country.
   d. Click **Save**.
4. To mark the Threat Actor as important, click the star so it turns orange .

   > When the star is orange, the Threat Actor is marked as important, which is used on the TAAM dashboard.
5. To add a custom Overview:

   > Your Overview information will be used in the Threat Actor list

   a. In the **Overview** section, click **Add Now**.

      > The **Add Now** link is only available if the section is empty.

   b. Add text as desired. Information can be entered in plain text, markdown syntax, and HTML markup syntax.
   c. Click **Save**.
6. To update a custom overview:
   a. Click Edit in the Custom overview section.
   b. Add text as desired. Information can be entered in plain text, markdown syntax, and HTML markup syntax.
   c. Click **Save**.
7. To add TTPs, including MITRE ATT&CK tags:
   a. In the **Tactics, Techniques, and Procedures** section, click the **Add Now** link or click **Add Tag**.

      > The **Add Now** link is only available if the section is empty.

   b. The list of existing Tags is displayed. Select a Tag from the list. You can also click in the enter **Tag** field and type a full or partial Tag to limit the list of available Tags. If the Tag you want to add doesn't exist, type it and then click **New TTP:** <tag>.
   c. Repeat the process until you've added all your tags.
   d. If you need to remove a Tag, click Remove on the tag.

8. To add Aliases:
    a. In the **Aliases** section, click **Add Now** .

    > The **Add Now** link is only available if the section is empty.

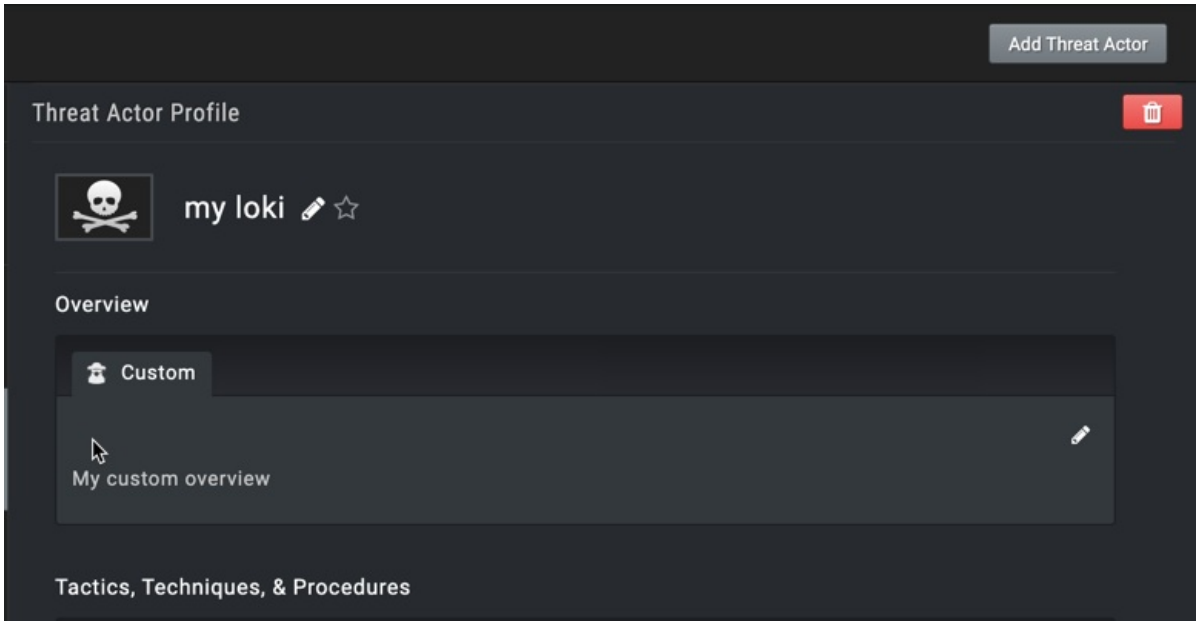
    b. The list of existing Aliases is displayed. Select an Alias from the list. You can also click in the enter **Alias** field and type a full or partial tag to limit the list of available options. If the Alias you want to add doesn't exist, type it and then click **New Alias:** <alias>.
    c. Repeat the process to add additional aliases.
    d. If you need to remove an Alias, click Remove.

### Deleting a Threat Actor

You can delete any custom (user-created) Threat Actors.

### To Delete a Threat Actor

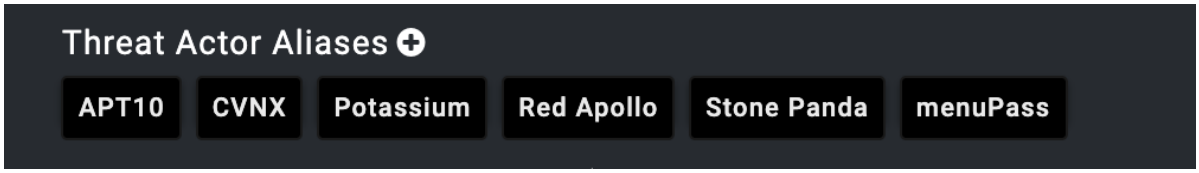
1. Go to **Library > Threat Actors**.
2. Locate the Threat Actor you want to delete.
   The easiest ways to do this is to use the Dimension filter **Intel Source > Custom Dimension** Filter or to search for the Threat Actor using the text search.
3. Click Delete and then click Delete on the confirmation window.




Delete a Threat Actor

### Associating an Evaluation or Sequence to a Threat Actor

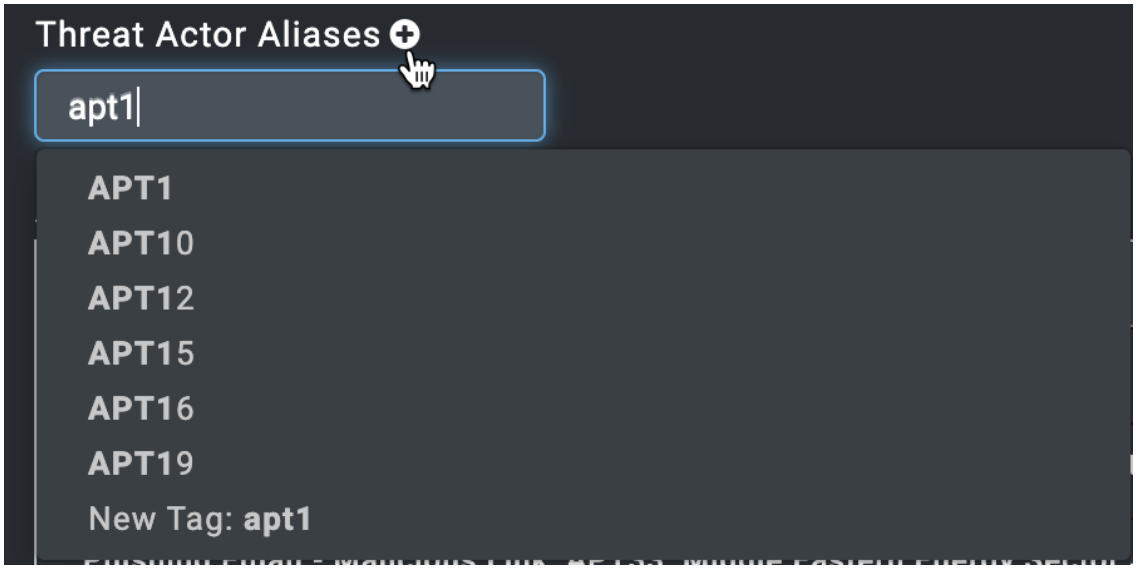
When you have the Threat Actor Assurance Module (TAAM), you can associate any existing Evaluation and Sequence to a Threat Actor by adding its Threat Actor Alias tag. When you do this, the Evaluation or Sequence appears in the Sequences and Evaluations section of the Threat Actor's profile.




Threat Actor Aliases on a Sequence or Evaluation

### To Associate an Evaluation with a Threat Actor

1. Click **Library > Evaluations**.
2. Select the *Evaluation* so you see the Evaluation Preview.
3. In the Threat Actor Aliases section, click **Add**. The list of existing Tags is displayed.
4. Select a Tag from the list. You can also click in the enter Tag field and type a full or partial tag to limit the list of available tags. If the tag you want to add doesn't exist, type it and then click **New Tag: *tag***.




Add Threat Actor Alias to a Sequence or Evaluation

> If you create a new Tag, you will need to edit the Threat Actor to include that tag as well.

5. Repeat until you've added all the aliases you want.

### To Associate a Sequence with a Threat Actor

1. Click **Library > Sequences**.
2. Select the *Sequence* so you see the Sequence Preview.
3. In the Threat Actor Aliases section, click **Add**. The list of existing Tags is displayed.
4. Select a Tag from the list. You can also click in the enter Tag field and type a full or partial tag to limit the list of available tags. If the tag you want to add doesn't exist, type it and then click **New Tag: <tag>**.

> If you create a new Tag, you will need to edit the Threat Actor to include that tag as well

5. Repeat until you've added all the aliases you want