BUILD A PERSONALIZED THREAT LANDSCAPE WITH THREAT PROFILES

Mandiant Advantage Threat Intelligence (MATI) lets you build a personalized Threat Landscape by creating customizable Threat Profiles. Threat Profiles filter all of Mandiant's threat intelligence so you can focus only on the threats that matter most to your organization. **Your Threat Profile** also lets you follow selected threats over time so you can easily operationalize their associated threat intelligence within your existing workflows.

Create Threat Profiles

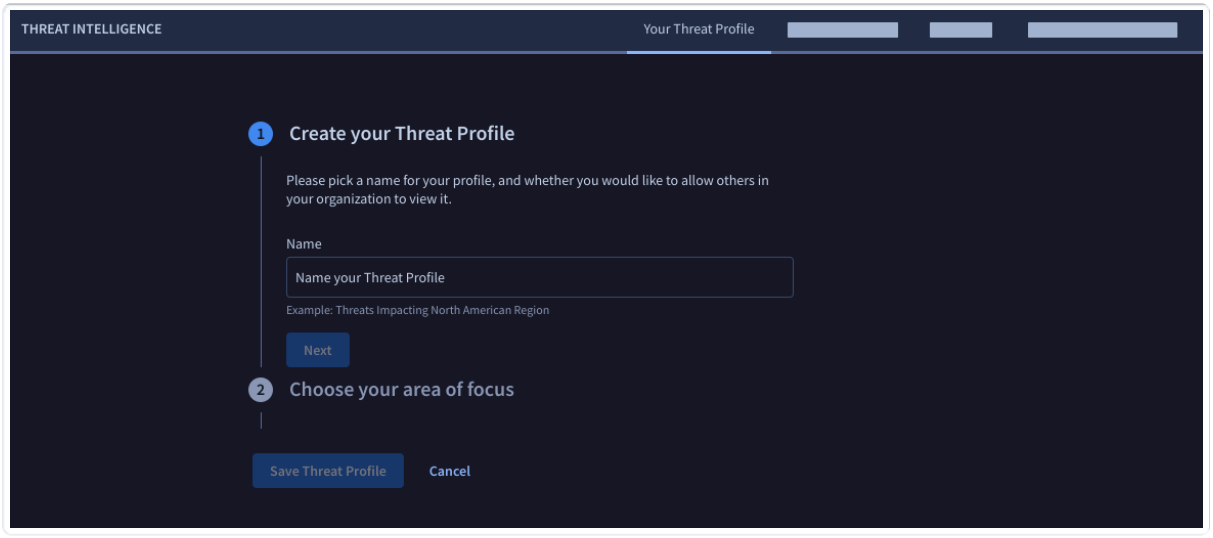
Perform the following steps to create your first threat Profile and then add additional Threat Profiles.

- **Create a Threat Profile**
- **Create additional Threat Profiles**

Create a Threat Profile

Threat Profiles let you apply top-level filters for **Target Industries** and **Target Regions** to immediately provide a more focused view of relevant threats. Complete the following steps to create a Threat Profile.

1. Sign into the **Mandiant Advantage Threat Intelligence (MATI) platform** **(https://advantage.mandiant.com/)**.
2. Click **Your Threat Profile**, then click **Create Threat Profile**. The guided steps appear to help you create your first Threat Profile.



Guided steps for creating your first Threat Profile

3. For **Create Your Threat Profile**, enter a meaningful **Name** and then click **Next**.
4. For **Choose your area of focus**, select at least one value for the **Industry** and one value for the **Target Region**.

   - For Target Region, you can select a whole region (for example, Americas) or specific subregions (for example, North America or United States of America).
   - If you make any mistakes in your selections, you can remove them by clicking ✕ next to the entry you want to remove.

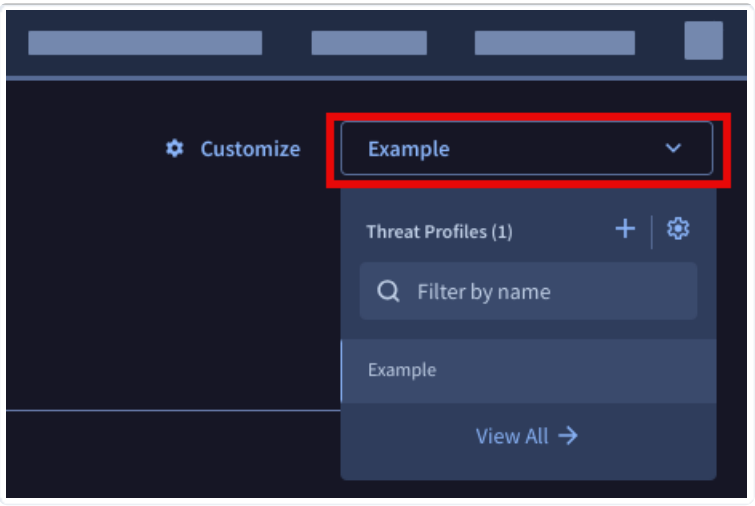
5. Click **Save Threat Profile**. A message appears confirming that your profile is created. You can either confirm with **Okay, Got It** or repeat the steps with **Create Another Threat Profile**.

- Threats that match your Threat Profile filters for Industries and Target Regions are populated within their respective threat type category.
- Once saved, the name of the Threat Profile you're viewing appears in the Profile Switcher next to your user profile in the browser header. The Profile Switcher includes an **Expand More** drop-down that lets you add and manage Threat Profiles.

Create additional Threat Profiles

MATI lets you add and easily switch between multiple Threat Profiles to support your various roles, responsibilities, and workflows:

1. Click the Profile Switcher drop-down.



2. Select + **Create Threat Profile** to add a new Threat Profile.
3. Complete Step 1 (**Name**) and 2 (**Choose area of focus**), as shown in the preceding procedure.
4. For **Continue following existing threats**, choose an option:
   - Click **Yes, continue to follow existing threats from** and then choose the threats you want to continue to follow in the new profile.
   - Click **No, I'd like to create a new profile with no existing follows**.

Any threat listed in your Threat Profile as **Mandiant Recommended** includes the option to click thumb up or thumb down to indicate its relevancy. This feedback mechanism aids in improving the accuracy and applicability of our proprietary ML model.

Manage Threat Profiles

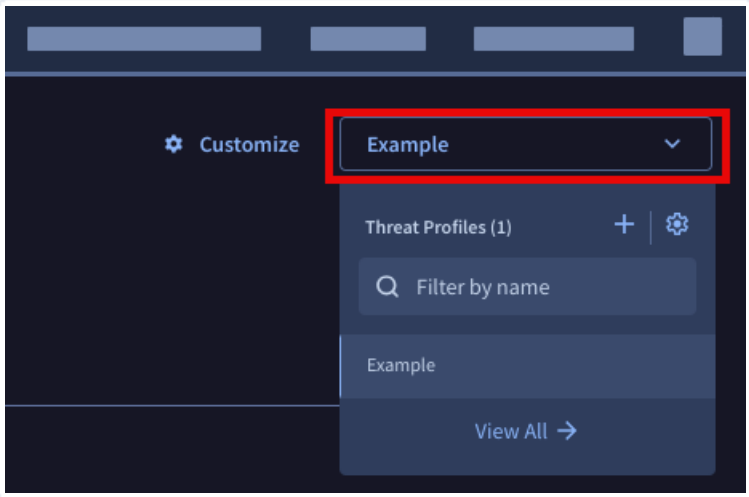
Perform the following steps to manage your Threat Profiles and customize them further:

- **Manage Threat Profiles**
- **Customize Threat Profiles**

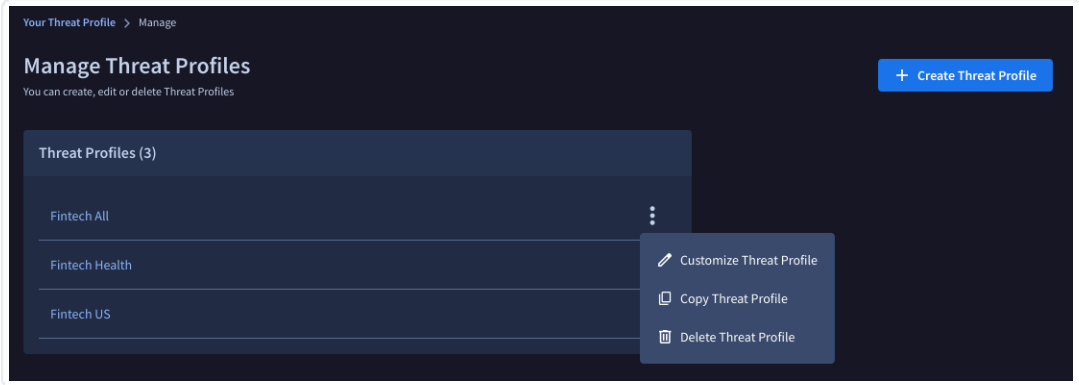
Manage Threat Profiles

Easily manage your Threat Profiles by clicking **Manage Threat Profiles** in the Profile Switcher.

1. Click the Profile Switcher drop-down.



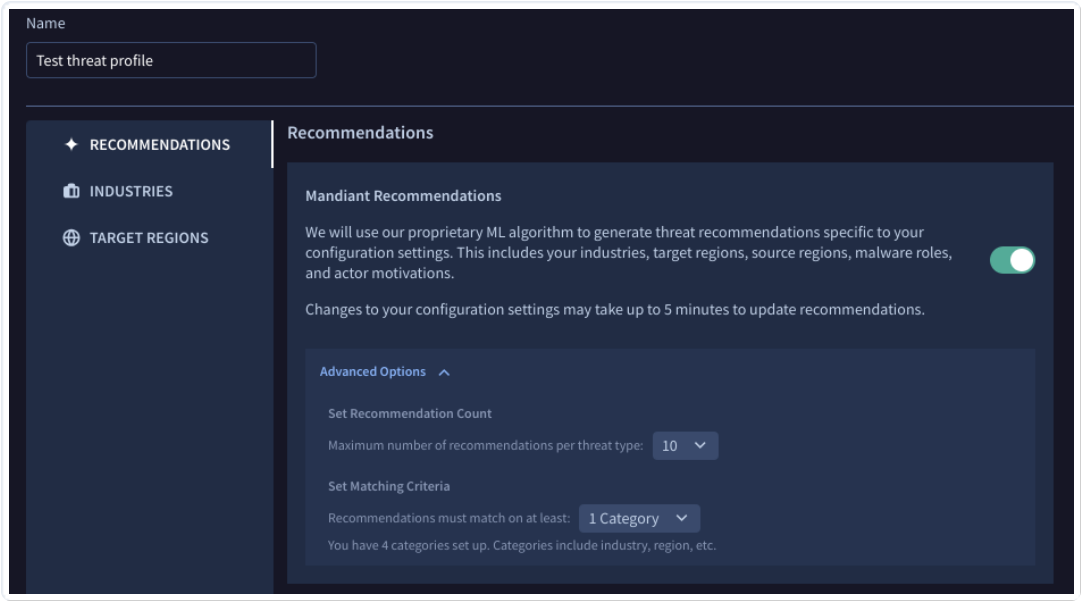
2. Perform one of the following steps:
    - Select + **Create Threat Profile** to add a new Threat Profile.
    - Select ⚙ **Manage Threat Profiles** to create a new Threat Profile or manage existing Threat Profiles.
        - Click ⋮ **More** to customize, copy, or delete the selected Threat Profile.



Customize Threat Profiles

Once Threat Profiles are created, you can make changes to suit your needs. For example, if too many recommendations appear, you can modify that.

1. From the Profile Switcher drop-down, choose an existing Threat Profile.
2. Click ⚙ **Customize**.
3. Verify or change any settings, as needed:
    - **Recommendations**:
        - **Mandiant Recommends:** Change this setting, as needed. **On** is the default and recommended setting.



Mandiant Recommendations settings for machine learning (ML)-based threat recommendations

- Changes for this setting can take up to five minutes to update your recommendations.
- Actors, Campaigns, and Malware are supported with this setting.

- **Advanced Options**: Set these preferences if you want to fine tune what gets matched in your Threat Profiles:
  - **Set Recommendation Count:** Set the maximum number of recommendations per threat type. For example, selecting **10** (the default) surfaces up to 10 actors, malware, and campaign recommendations to the user based on category matching criteria.
  - **Set Matching Criteria**: Select how many categories that recommendations must match. Categories include industries and target regions.

- **Industries**: Change any selected industries, as needed.
- **Target Regions**: Change any selected target regions, as needed.

4. Save your changes.

Explore Threats

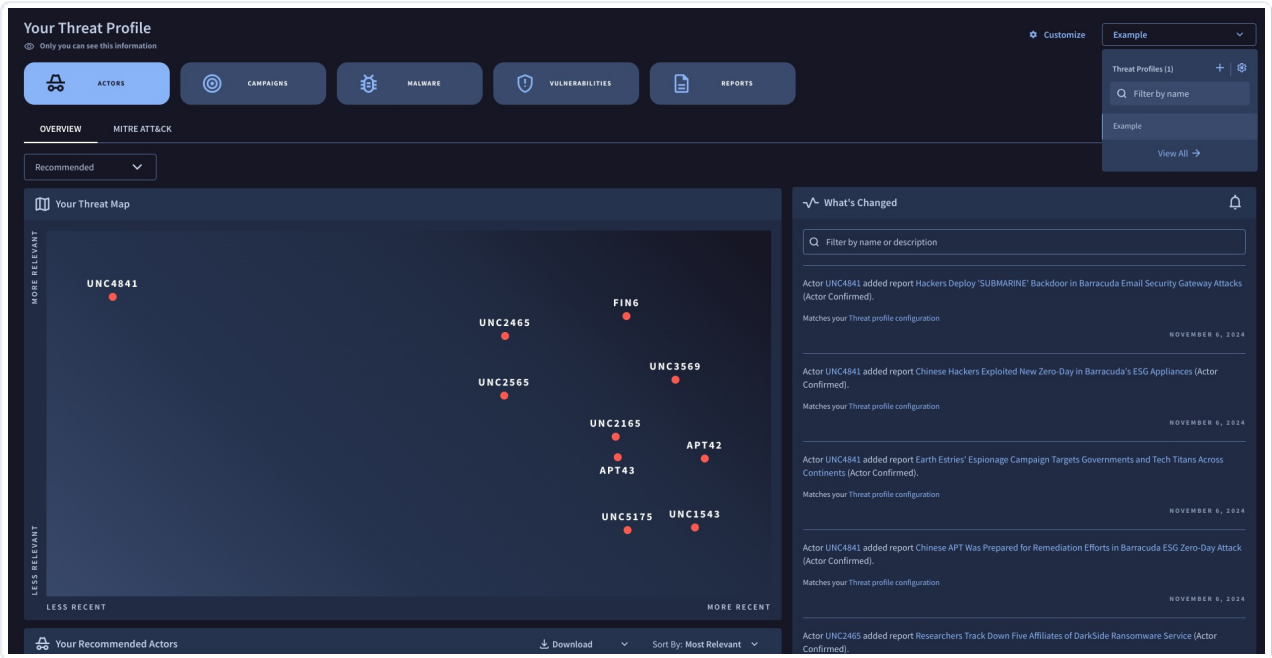
Perform the following steps to explore threats and access recommendations about them:

- **Explore your Threat Landscape**
- **Access recommendations to understand Threat Landscape**

Explore your Threat Landscape

Your Threat Profile lets you easily pivot between filtered threat types by selecting from the displayed threat type categories **Actors**, **Campaigns**, **Malware**, and **Vulnerabilities**, while also providing **Reports**. You can also view any threats you've added to the selected Threat Profile in the ✓ **Added to Threat Profile** category.

You can modify your Threat Profile filters at any time by clicking **Customize**.



Your Threat Profile landing page

- The **Overview** tab provides a summary of threats within the selected threat type that match the filters for the active Threat Profile. Information in this tab depends on the threat object that you choose:
  - **Your Threat Map** (Actors only): Displays all threats within the selected threat type that match your Threat Profile configuration.

    - Relevance of threats is set by the number of criteria that are matched: the more matches, the higher up in the map.
    - The Recent level for threats is based on the Last Seen date.

  - **Your Recommended [Actors | Campaigns | Malware]** : Displays recommended threat types for you to be aware of that match your Threat Profile configuration.
    - Click + **Add** to follow a threat for changes over time by adding it to a Threat Profile.

      All threats you add to the selected Threat Profile appear in the ✓ **Added to Threat Profile** threat type category.

    - The **Take Action** drop-down lets you perform the following:
      - **View Details**: Pivot directly to the detailed profile of the threat.
      - **Download Indicators (CSV)**: Download all associated indicators in CSV format for further analysis. The following fields are included in the exported CSV file when you download indicators:
        - Indicator Value
        - Indicator Type
        - IC Score
        - Associated Actors
        - Associated Malware
        - Associated Tools
        - Associated Campaigns
        - Exclusive

        - First Seen
        - Last Seen

    - **Download MITRE TTPs (CSV)**: Download a CSV file of all tactics, techniques, and procedures (TTPs) associated with the indicator.

      > The option to **Download MITRE TTPs (CSV)** is only available for **Actors** and **Campaigns**.

      The following fields are included in the exported CSV file:
        - MITRE Category Name
        - Technique ID
        - Technique Name
        - Sub-Technique IDs
        - Sub-Technique Names
        - Actor usage count
        - Actor 1
        - Actor 2
        - Actor 3

  - **Your Added Vulnerabilities** (Vulnerabilities only): Any vulnerability entries that you added to the selected Threat Profile.
  - **Reports**: It lists all of Mandiant's latest reports related to Actor and Malware threats.

    > For more information about reports, see **Threat Intelligence Reports (https://docs.mandiant.com/home/mati-reports)**.

  - **What's Changed**: Lists updates to any of **Your Threats** in this Threat Profile over time.

- The **MITRE ATT&CK** tab is available for **Actors**, **Campaigns**, and **Malware**. It displays all the tactics, techniques, and procedures (TTPs) observed to be used by the selected threat type. TTPs are displayed as a heat map that highlights the number of threats within the selected threat type that your Threat Profile.

  > TTPs can also be downloaded directly from this tab by clicking **Download TTPs**.

Access recommendations to understand Threat Landscape

1. From the Profile Switcher drop-down, choose an existing Threat Profile.
2. From **Your Threat Profile**, click **Actors**, **Campaigns**, or **Malware.**
3. In the **Recommended** view on the **Overview**, note the data that appears in the Threat Map (supported for Actors only). In the following example, the Actors Overview shows a mapping of Threat Actors based on relevance (from **Less Relevant** to **More Relevant** on the y-axis) and recency (**Less Recent** to **More Recent** on the x-axis).

Example of the Threat Actor Overview page, showing Threat Actors mapped by recency and relevance

4. Scroll to **Your Recommended Threats** to see a list of prioritized threats based on the ML recommendations. You can also sort the results or click **Download** to get a copy of the list of **Indicators** or **MITRE TTPs** in CSV format.
5. Click **MITRE ATT&CK** to access the MITRE heatmap, which plots the count of Actors using particular TTPs and color-codes them accordingly on the heatmap. You can click **Download TTPs** to get a copy of the list of TTPs in CSV format.
6. Click **Relevant Reports** to access reports that are associated with the Actors that are listed as recommended threats. You can filter the results by any combination of **Report Title**, **Report Type**, **Associated Actors**, **Associated Malware**, and **Published Date**.
7. Repeat any steps for Campaigns and Malware.

- Overviews are available for Actors, Campaigns, or Malware, but only Actors provide the Heat Map view at this time.
- Campaigns do not currently support Relevant Reporting.
- In addition to Indicators and MITRE TTPs, the Malware section lets you download YARA rules.

Track changes

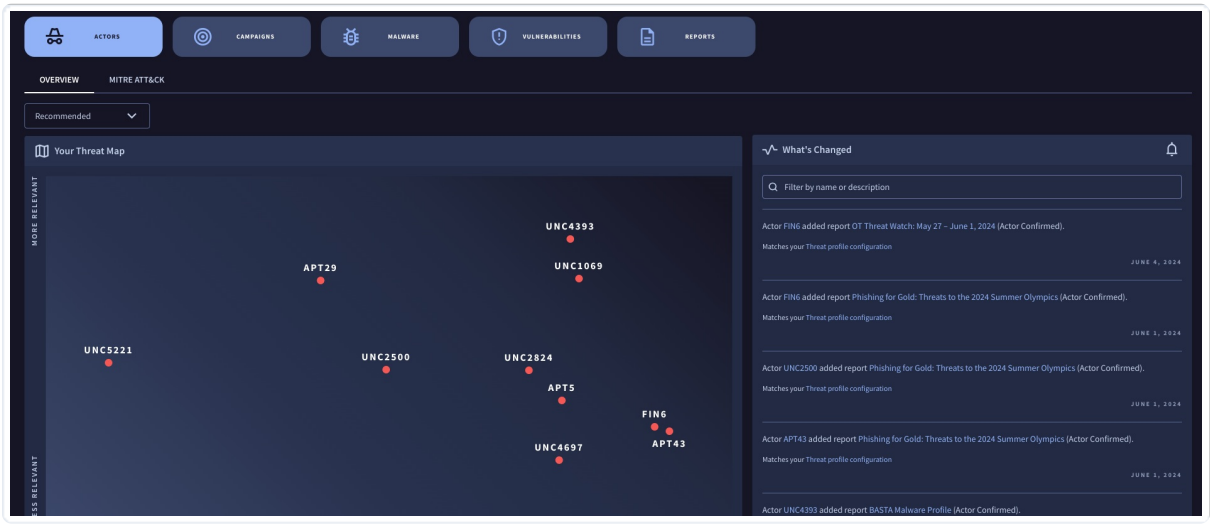
Perform the following steps to track changes to threat objects through the web interface or by email notifications:

- **Track changes to objects in Threat Profile**
- **Subscribe to email notifications**

Track changes to objects in Threat Profile

As items are added to your Threat Profile, any changes are tracked and identified for you so you can stay up to date.

1. From the Profile Switcher drop-down, choose an existing Threat Profile.
2. Study the **What's Changed** section for any object in the profile and identify any events that are of interest to you. For example, a new report or TTP that is added to a Threat Actor you're following or that matches your Threat Profile configuration.
3. Click any links that are provided (reports, malware families, TTPs, and so on) if you want to see more details on the change.



List of What's Changed for events related to Threat Actors in Your Threat Profile

The following events may appear in the What's Changed section:

Type	Change event
Actor	New targeted country
	New targeted industry
	New TTP added
	New malware/tool added
	New vulnerability exploited
	Suspected group association added
	New report published
Campaign	New actor added
	New vulnerability exploited
	New targeted country
	New targeted industry
	New TTP added
	New malware / tool added
	New report published
	New key event
	New key x509 certificate created
Malware	New actor added
	New vulnerability exploited
	New targeted industry
	New TTP added
	New detection rule added
	New report published
Vulnerability	Severity score upgraded to high or critical
	New publicly available exploit
	Exploitation state changes to actively exploited

Subscribe to email notifications

You can configure email notifications to easily track changes to your threat profile when they happen and get the latest, personalized threat updates in your inbox.

At least one Threat Profile must be established before setting up email notifications.

1. From the **What's changed** table, click **Setup email notifications**. This takes you to the **Email Notifications** page.

   For more information on setting up email notifications, see **Email Notifications (https://docs.mandiant.com/home/mati-manage-account-settings#email-notifications)** in the "Manage Threat Intelligence Account Settings" documentation.

How to use an email notification

Once you start receiving email notifications, you can pivot to the appropriate area of the product and see if the threat is something you are following or that is recommended by the AI model. For example, you get an email notification when a new YARA rule is published for one of the Malware groups you're tracking in your Threat Profile. You can immediately export that YARA rule in MATI.

Example email notification