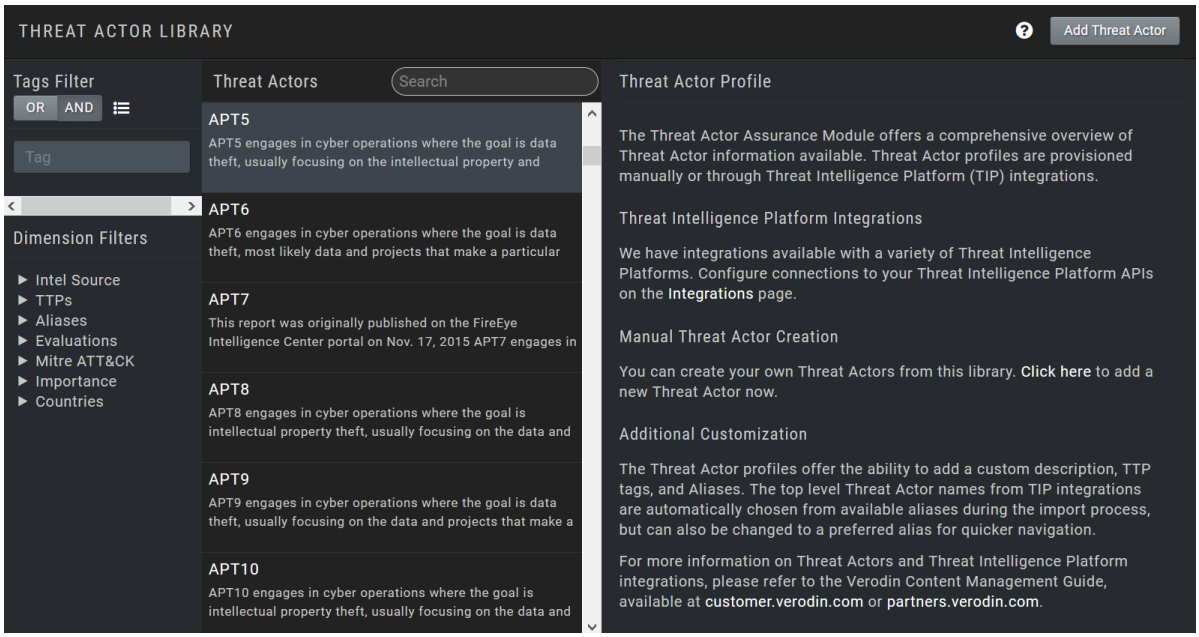
UNDERSTANDING THREAT ACTOR INFORMATION IN SECURITY VALIDATION

Threat Actor Library

The Threat Actor Library is included when you have Threat Actor Assurance Module (TAAM) and shows a comprehensive overview of Threat Actor information. Threat Actor profiles can be created manually from the Threat Actor Library page, or automatically through **Threat Intelligence Integrations** (https://docs.mandiant.com/home/threatintelligence-integrations). From a Threat Actor Profile, you can also run Evaluations and Sequences that are related to that Threat Actor, and jump to the most recent Job results.



Threat Actor Library Page

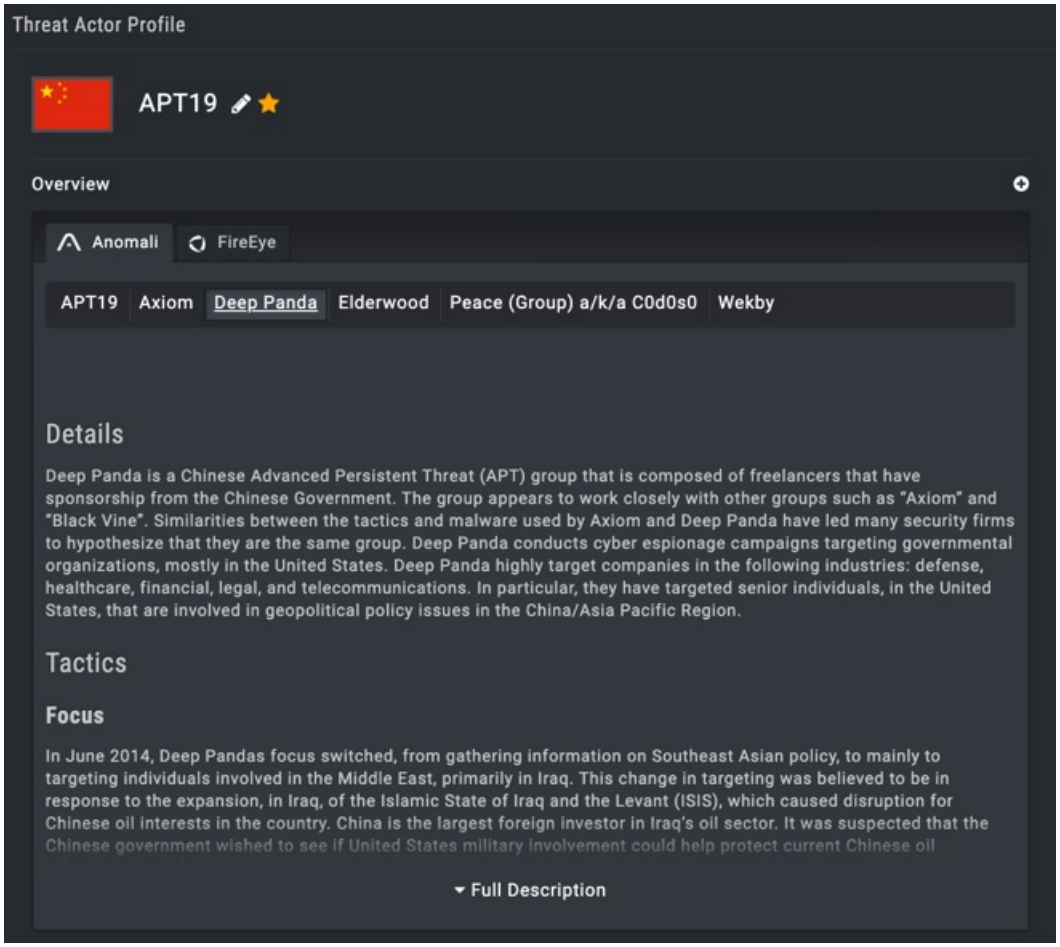
Threat Actor Profiles

When you select a Threat Actor from the Security Validation Threat Library, it displays a profile for that Threat Actor, based on information pulled in from your Threat Intelligence Integration and information you have entered. The profile has five sections: General, Overview, Tactics Techniques & Procedures, Aliases, and Evaluations & Sequences.

The first part of the profile is the associated country, the name, and importance level. The Overview includes a tab for each Threat Intelligence Integration. If the Threat Intelligence Integration includes separate write ups for the Aliases, they are included as sub-tabs in the Threat Intelligence Integration's tab. If you've added information, that will be in its own tab.

The top-level Threat Actor name for Threat Actors from Threat Intelligence Integration is automatically chosen during the import process. The country of origin information does not populate and will be unknown  until you select it. However, both the name and country of origin can be changed to a preferred alias for quicker navigation. If you have Anomali and have marked the Threat Actor as important in the Threat Intelligence Integration, that will also carry over and appear in the Threat Actor Profile.

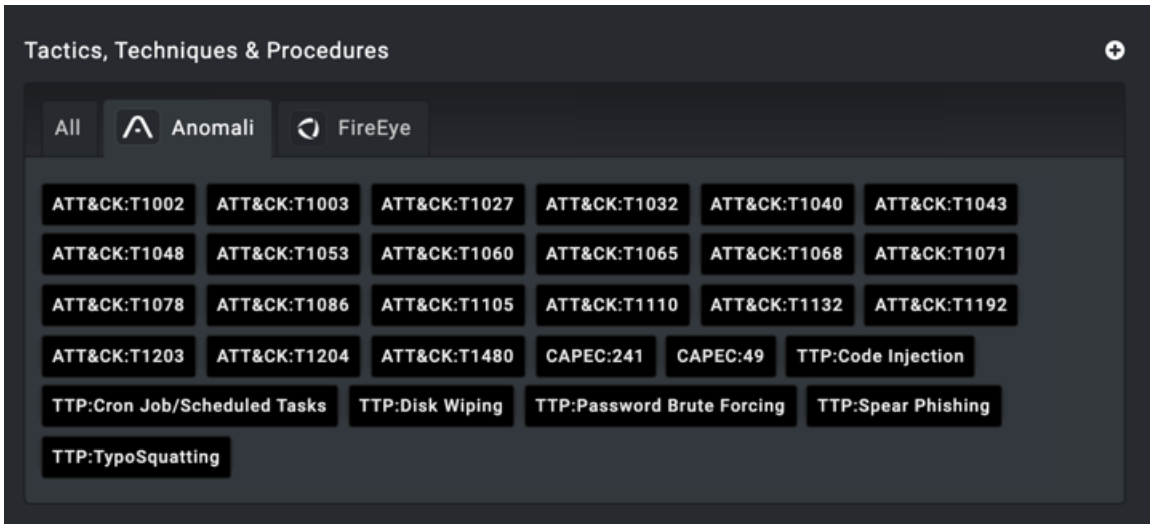
NOTE: If country data is only included in the descriptive information for a Threat Actor and is not pulled in separately, you will not see the flag in the Threat Intelligence Integration's tab.



Threat Actor Profile - General & Overview sections

Tactics, Techniques, & Procedures (TTP)

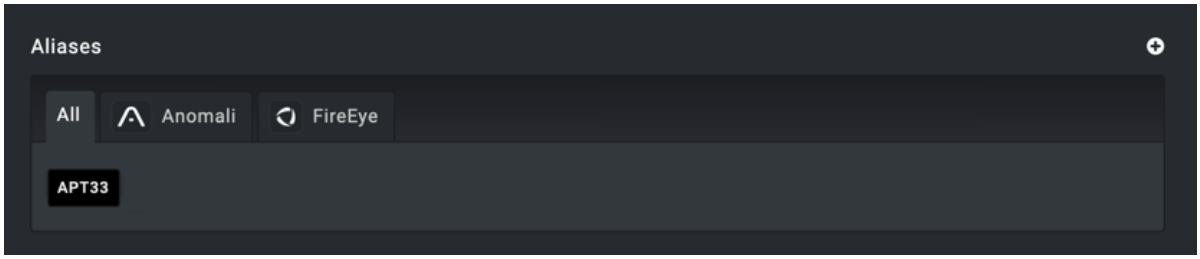
TTP information from the Threat Intelligence Integration is added as tags and maintained in its own section of the profile. Based on your Threat Intelligence Integration, you could see MITRE ATT&CK tags, TTP tags, Malware, and CAPEC (Common Attack Pattern Enumeration and Classification) tags. You can also add your own tags. Information is maintained in tabs: an **All** tab that shows all TTPs, individual tabs for each Threat Intelligence Integration, and a custom tab if you've added information. Tags that come from the Threat Intelligence Integration have a black background with white letters. User-created tags have a white background with black letters.



Threat Actor Profile - TTP section

Aliases

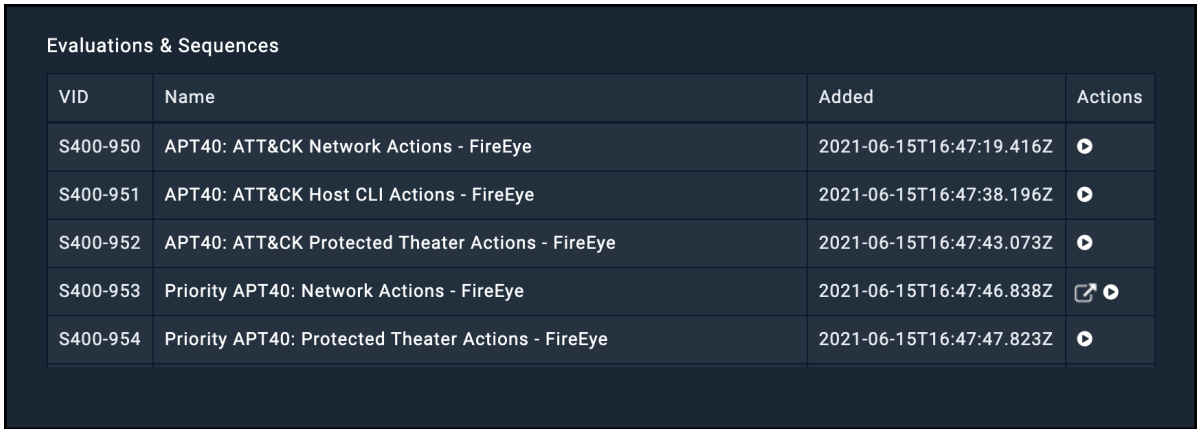
The Aliases section has tags for any names the Threat Actor uses. Information is maintained in tabs: an **All** tab that shows all Aliases, individual tabs for each Threat Intelligence Integration, and a custom tab if you've added information. The Aliases tags have the same color scheme as the Threat Intelligence Integration tags.



Threat Actor Profile - Aliases section

Evaluations & Sequences

The last section shows Evaluations and Sequences that are related to the Threat Actor. Here you can click on the Name to view the details and clone the Evaluation, jump to the most recent Job for the Evaluation or Sequence, and run the Evaluation or Sequence.



There are two ways an Evaluation or Sequence appear in this table:

- You add a Threat Actor tag to a Sequence or Evaluation
- The Validation Platform created an Evaluation when the Threat Intelligence Integration syncs. See **TAAM Evaluations (https://docs.mandiant.com/home/msv-taam-evaluations)** for more information about these Evaluations.

Threat Actor Dimensions

These Dimensions are found in the Threat Actor Library and can be used to help identify specific Threat Actors you are interested in.

Intel Source

- Your Threat Intelligence Integration will be listed here
- Custom
  This option filters the list to show any Threat Actors that include user-added content.

TTPs

- Has Custom TTP Data
- Has Integration TTP Data
- No TTPs

Aliases

- Has Custom Aliases
- Has Integration Aliases
- No Aliases

Evaluations

- Has Evaluations
- No Evaluations Yet
- Has Evaluations Not Run
  This option filters the lists to show Threat Actors that have one or more associated Evaluations that have not yet been run.

MITRE ATT&CK

Selecting a MITRE ATT&CK Tactic filters the list to show all Threat Actors that are tagged with one or more of the Tactic's Techniques or Sub-Techniques (ATT&CK:T1002, etc).

Both User and Threat Intelligence Integration tags are considered when using this filter.

- Collection
- Command and Control
- Credential Access
- Defense Evasion
- Discovery
- Execution
- Exfiltration
- Impact
- Initial Access

- Lateral Movement
- Persistence
- Privilege Escalation
- Reconnaissance
- Resource Development

Importance

- Important
- Standard

Countries

This section displays when one or more Threat Actor profiles has the Country information defined. This means the flag must appear in either the general or Overview section. If the country is listed only in the body of the Overview, it is not included.