Mandiant

TAAM EVALUATIONS

A powerful functionality included with Security Validation's Threat Actor Assurance Module (TAAM) is the Evaluations it creates. After integrating with your TIP or TIF, you have Threat Actor information available in the Security Validation platform. These Threat Actors have different types of tags associated with them, and we use those tags to create two types of Threat Actor-specific Evaluations: General and Priority.

If you want a quick way to validate your environment is protected against a Threat Actor, use the Priority Evaluations.

General TAAM Evaluations have the following characteristics:

- Are based on the MITRE ATT&CK tags, with some exceptions:

  

  Since most our Actions have MITRE ATT&CK tags, these Evaluations can get very larger and include hundreds of Actions.

  - Threat Actors from Crowdstrike do not include MITRE ATT&CK Techniques so their Evaluations are based on the malware families.
  - Actions created by the Validation Research Team (VRT) that use the EICAR behaviors (which are not malicious and are used for testing and stability) are not included.

- May contain multiple groups
  - The groups are named according to the Actions' Source and Destination tags. These tags also account for the attributes on the Zones.
  - Groups will have 100 or fewer Actions. If more than 100 Actions meet the criteria for a group, multiple groups are added; they have **- Subset 1** added to the name of the first group, and increment for each group after.
- Separate Evaluations are created for Network Actions, Host CLI Actions, and Protected Theater Actions.
- VIDs start with S400.

Priority TAAM Evaluations have the following characteristics:

- Are based on the Threat Actor and Malware Family tags.

  

  The use of Threat Actor and Malware Family tags keeps these Evaluations focused.

- May contain multiple groups.
- Titles start with **Priority** to make them easy to identify.
- Separate Evaluations are created for Network Actions, Host CLI Actions, and Protected Theater Actions.
- VIDs start with S400.

When you modify your environment (add/remove Action tags, add/update Zones or Actors, add new content packs, and so on), Evaluations may be created or updated the next time the Threat Intelligence Integrations sync. If an Evaluation is updated, it has a new version number.

If you run two instances of the Validation Platform (a test and production environment, for example) the Evaluations that are created are different unless the instances are identical. This means the VIDs, groups, and Actions included could be different when looking at the same Actor.