Mandiant

SECURITY CONTENT OVERVIEW

The Validation Platform's Security Content can include files, applications, commands, network traffic samples, and other artifacts that can be malicious and/or represent real attacker behavior. New Baseline content packs are released each quarter. Headline content packs are released as needed.

Each Test can consist of a single Action, a Sequence, or an Evaluation.

- Actions are suspicious or malicious behaviors that are processed between, or on, Actors to mimic attacker behaviors.
- Sequences are saved groupings of Actions, frequently used to reflect advancing stages of attack (for example, reconnaissance Actions followed by exploitation Actions), and are further discussed in **Sequences & Evaluations (https://docs.mandiant.com/home/sequences-evaluations)**.

  If an Action in a Sequence results in an error when it is run, the Actions which follow it does not run.
- Evaluations are saved groupings of Actions used to test a specific use case or defense capability, such as data loss prevention or SQL injection defenses, and are further discussed in **Sequences & Evaluations (https://docs.mandiant.com/home/sequences-evaluations)**.

  All Actions in an Evaluation attempt to run, even if one of the Actions results in an error when it ran.

Each Action, Sequence, and Evaluation is assigned a Validation Identifier (VID). These have a standard format: (letter)###-###.

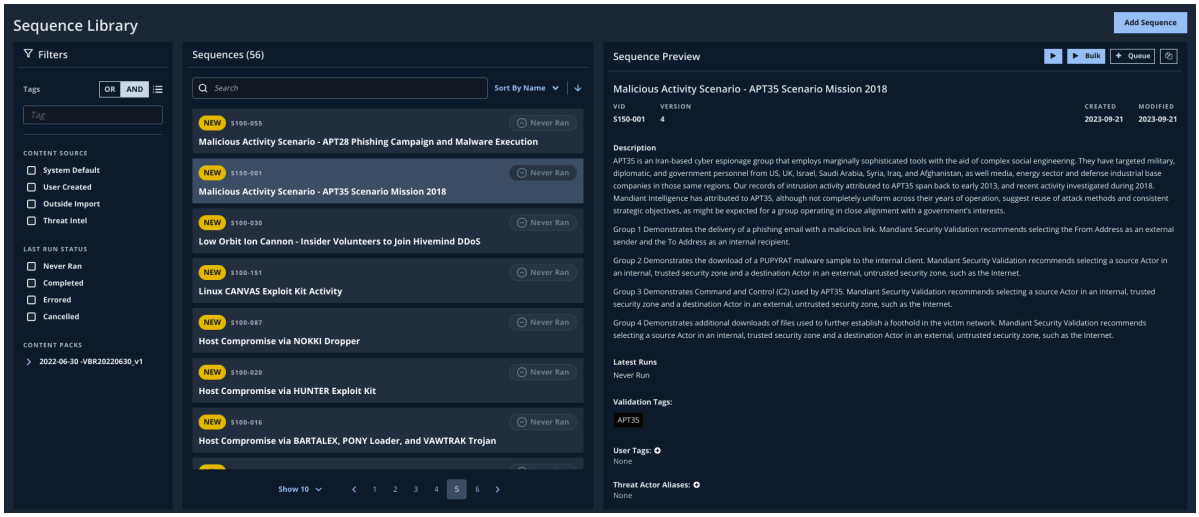
- A prefix: Actions
- S prefix: Sequences and Evaluation
- 10#-### range: Content that has been created by the Security Validation team
- 150-### range: Content created by Mandiant Intelligence, which is available in premium content packs
- 200-### range: User-created content
  For example, content with VID A200-123 represents the 123rd user-created Action.
- 300-### range: Content that has been imported from another source
- 400-### range: Evaluations automatically created based on Actions that include Threat Actor Tags

  These Evaluations are only seen if you have the TAAM module.

All Existing Actions, Sequence, and Evaluations, regardless of source, can be cloned to serve as the starting point for user-created content.

This video walks you through the Actions library for common use cases, such as how the Validation Platform can run a single attack behavior to test your environment's effectiveness against known threats.

To view security content, go to **Library**. Select **Actions**, **Sequences** (the default view in Security Validation), or **Evaluations** to preview, run, queue, clone, or create a Monitor from one of these content types.



The Sequence Library