


## 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) (<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) (<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 123<sup>rd</sup> 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.

Sequence Library
Add Sequence

**Filters**

Tags: OK AND

**CONTENT SOURCE**

System Default

User Created

Outside Import

Threat Intel

**LAST RUN STATUS**

Never Ran

Completed

Errored

Cancelled

**CONTENT PACKS**

> 2022-06-30 - IPR20220630\_v1

Sequences (56)

Sort By Name v

NEW S100-055 Never Ran

**Malicious Activity Scenario - APT28 Phishing Campaign and Malware Execution**

NEW S100-001 Never Ran

**Malicious Activity Scenario - APT35 Scenario Mission 2018**

NEW S100-030 Never Ran

**Low Orbit Ion Cannon - Insider Volunteers to Join Hivemind DDoS**

NEW S100-151 Never Ran

**Linux CANVAS Exploit Kit Activity**

NEW S100-087 Never Ran

**Host Compromise via NOKKI Dropper**

NEW S100-020 Never Ran

**Host Compromise via HUNTER Exploit Kit**

NEW S100-016 Never Ran

**Host Compromise via BARTALEX, PONY Loader, and VAWTRAK Trojan**

Show 10 < 1 2 3 4 5 6 >

**Sequence Preview** ▶ Back + Queue 🔍

**Malicious Activity Scenario - APT35 Scenario Mission 2018**

VID: S150-001 | VERSION: 4 | CREATED: 2023-09-21 | MODIFIED: 2023-09-21

**Description**

APT35 is an Iran-based cyber espionage group that employs marginally sophisticated tools with the aid of complex social engineering. They have targeted military, diplomatic, and government personnel from US, UK, Israel, Saudi Arabia, Syria, Iraq, and Afghanistan, as well as media, energy sector and defense industrial base companies in those same regions. Our records of intrusion activity attributed to APT35 span back to early 2013, and recent activity investigated during 2018. Mandiant Intelligence has attributed to APT35, although not completely uniform across their years of operation, suggest reuse of attack methods and consistent strategic objectives, as might be expected for a group operating in close alignment with a government's interests.

Group 1 Demonstrates the delivery of a phishing email with a malicious link. Mandiant Security Validation recommends selecting the From Address as an external sender and the To Address as an internal recipient.

Group 2 Demonstrates the download of a PUJWRAT malware sample to the internal client. Mandiant Security Validation recommends selecting a source Actor in an internal, trusted security zone and a destination Actor in an external, untrusted security zone, such as the Internet.

Group 3 Demonstrates Command and Control (C2) used by APT35. Mandiant Security Validation recommends selecting a source Actor in an internal, trusted security zone and a destination Actor in an external, untrusted security zone, such as the Internet.

Group 4 Demonstrates additional downloads of files used to further establish a foothold in the victim network. Mandiant Security Validation recommends selecting a source Actor in an internal, trusted security zone and a destination Actor in an external, untrusted security zone, such as the Internet.

**Latest Runs**

Never Run

**Validation Tags:**

APT35

**User Tags:**

None

**Threat Actor Aliases:**

None

The Sequence Library