Mandiant

CREATING SECURITY CONTENT OVERVIEW

To better support the Security Validation user community and to enhance the capabilities of the platform, you can create new Actions, Sequences, and Evaluations. You can create File Transfer and Email Actions from the File Library, but other Action types must be created from the Action Library. Sequences and Evaluations are often created by selecting Actions from the Action Library and adding them to the Action Queue. However, you can also clone existing security content and create Sequences & Evaluations from a file.

The Action Queue allows you to select a group of content from the library and then work with them to build Sequences, Evaluations, or just run the group immediately without saving it. The Action Queue is also used when you create a copy of an existing Sequence or Evaluation.

To support quick testing, after you save the new Action, the Action Library appears with the new Action selected. The Job results page for the Action also includes an edit option, letting you open the Action to make additional changes.

Actions that require approval will not be automatically selected after creating the Action.

Actions have versions and modified dates, which are updated differently based on the type of Action:

- User-created or imported Actions: The version and modified date updates when you modify the Action tags, dimensions, and Action details.
- Validation Platform Actions: The version and modified date only update when the Security Validation team provides a new version of the Action.

Everyone who has a Validation License and the correct user permissions can create the following Action Types:

- **Captive DNS Queries** (https://docs.mandiant.com/home/msv-adding-captive-dns-query-actions-2017)
- **Captive IOC - PCAP** (https://docs.mandiant.com/home/msv-adding-captive-ioc-pcap-actions)
- **Captive IOC - URL** (https://docs.mandiant.com/home/msv-adding-captive-ioc-url-actions)
- **Cloud** (https://docs.mandiant.com/home/msv-adding-cloud-actions)
- **Email** (https://docs.mandiant.com/home/msv-adding-email-actions)
- **From PCAP** (https://docs.mandiant.com/home/msv-adding-actions-from-packet-capture)
- **Host CLI** (https://docs.mandiant.com/home/msv-adding-host-command-line-interface-actions)
- **Protected Theater (a form of Host CLI Actions)** (https://docs.mandiant.com/home/msv-adding-protected-theater-actions)
- **Malicious DNS Query** (https://docs.mandiant.com/home/msv-adding-malicious-dns-query-actions)
- **Socket** (https://docs.mandiant.com/home/msv-adding-socket-based-actions)
- **TCP Port Scan** (https://docs.mandiant.com/home/msv-adding-tcp-port-scan-actions)
- **Web** (https://docs.mandiant.com/home/msv-adding-web-based-actions)
- **File Transfer** (https://docs.mandiant.com/home/msv-adding-file-transfer-actions)

Everyone can also create Sequences and Evaluations.

- **Sequences** (https://docs.mandiant.com/home/msv-creating-sequences-and-evaluations)
- **Evaluations** (https://docs.mandiant.com/home/msv-creating-sequences-and-evaluations)
- **Sequence or Evaluation from a File** (https://docs.mandiant.com/home/msv-creating-sequences-or-evaluations-from-a-file)

Host-Filled User Tags While Running Bulk Jobs

Security Validation includes host-filled user tags for Bulk Jobs, just like single Jobs. You can add user tags when running Actions, Sequences, or Evaluations in bulk.

> User tag inputs are only present if a group within a Bulk Job has a `host_cli_action` that needs these tags. Otherwise, the web interface displays **Actor Tags** as input.

The following screenshot shows user tags to **Run Bulk Evaluation**. *Host CLI - MIMIKATZ (2.1.1)*, *Variant #1* and *Host CLI - MIMIKATZ (2.1.1) W/ String Change and UPX* are the two user tags.

> All Actors sharing the specified tags receive the same user tag values. Separate Bulk Jobs with more refined tags are necessary if individual Actors require distinct user tag values.