Mandiant

VIEW INDIVIDUAL JOBS

When Actions, Sequences, Evaluations, or Monitors are run, they become Jobs. You can view Jobs and their results in a number of ways.

You can also generate HTTP/HTTPS or syslog notifications to send to a specified destination that ingests machine data, such as Splunk or Elasticsearch, by selecting the Notification Formats menu option.

You can access these Job features by going to the Jobs menu on the navigation bar.

The Validation Platform supports parallel Job execution, with the following limitation:

- When an Actor is involved in multiple Jobs, the Jobs will be queued in the order they are received.

This limitation means any Actors queued for Job one will be unavailable to Job two until Job one is complete, therefore queuing all Job two Actions. Jobs may contain one or more Job Actions, which involve up to two Actors.

For each ad hoc, scheduled, or Monitor-related Job processed, a Job Results page is created. This page displays the Job details, including

- Overall status of the Job
- Feedback on if Actions were detected, blocked, or had an alert generated by the Integration (alerted)
- Groups of Actions, including:
    - The security technologies involved
    - Start and end times (when the group starts and completes running a job)
- Detailed information for each Action that runs, including:
    - Group it's part of
    - Source and Destination Actors
    - Began at and ended at times (when the individual action started and completed)
    - Runtime parameters configured
    - Security Technologies involved in the Job
    - Events that fired when the Action ran
    - General details for the Action (Description, Tags, Dimensions, Common Detection Alerts)
    - The json for the Job Action

From this page you can

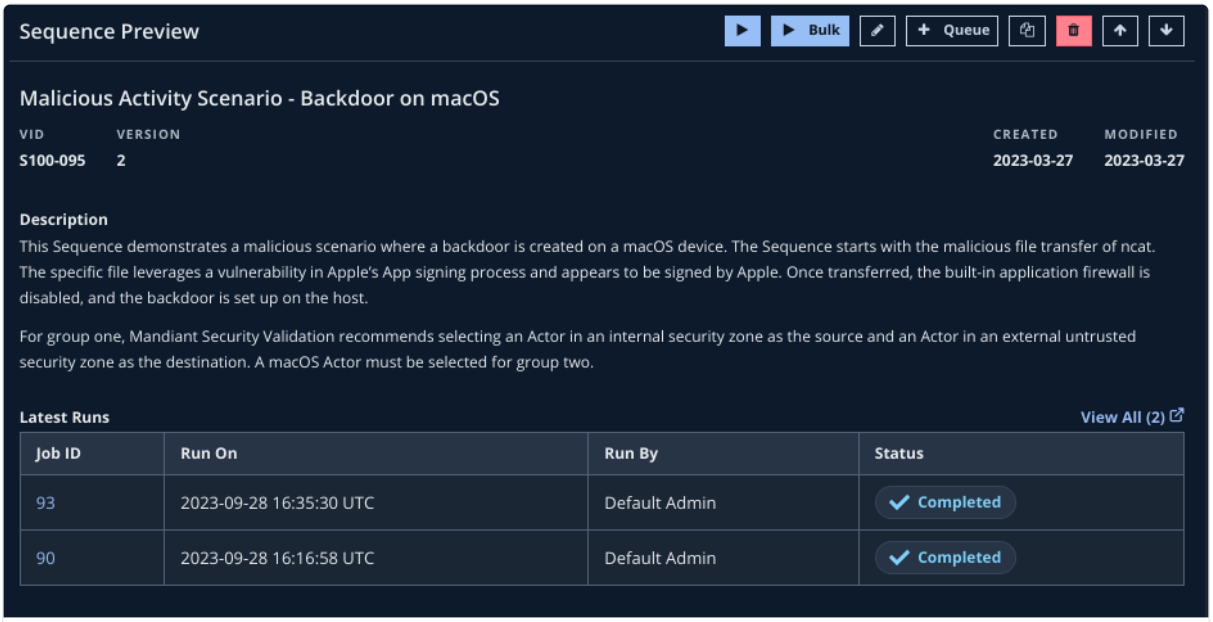
- Create Monitors
- Clone Actions
- View Actions
- Export the Job
- Edit the Job name
- Edit Group or Action notes
- Add Group or Action attachments

There are two versions of the page, one for Actions and one for Sequences and Evaluations. The majority of the page is the same, but the Job Overview is different, with the later including interactive charts.

View an individual Job's page

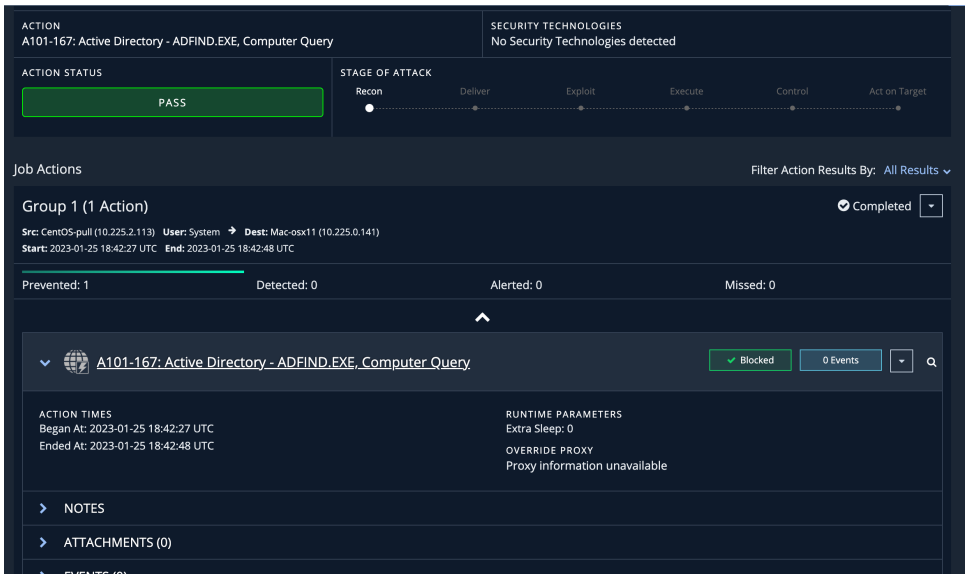
To view an individual Job's page, use one of these options.

- On the content Preview pane, click the **Job ID** value from the **Latest Runs** table.



Latest Runs on a Sequence Preview

- On the Job Status page, click on the **Job Name**.
  The standard keyboard and mouse shortcuts open the Job in a new tab or window.
- On the Job Status page, click **View** next to the Job you want to see.
  This replaces the Job Status page unless you use the standard OS keyboard shortcuts to open the page in a new tab or window.
- If you know the Job ID number, you can enter it in the URL, as shown:
  https://*[Director_address]*/jobs/*[Job ID]*



Job Results - Action

Job Results - Sequence Overview