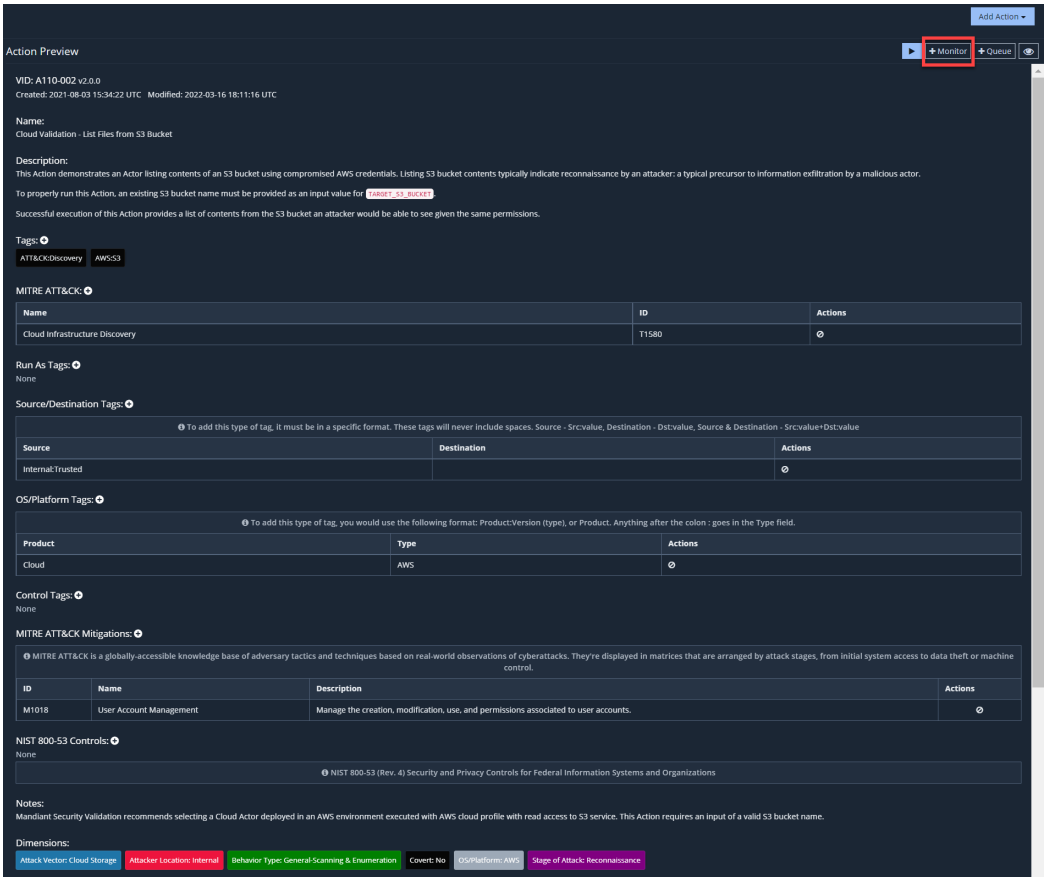
CREATE AND EDIT MONITORS

You can add a Monitor from several places:

- From an Action in the Action Library: Go to **Library > Actions** then click **Monitor**.
- From a Sequence or Evaluation: after you click **Run**, click **Monitor**.
- From a Job: click the Job's **Monitor** or from a single Action in a Job by clicking **Creating Monitor from Action** from its **Action** menu.

- If you create a monitor from the Action Library, you see all events from any Job. If you create a monitor from a Job, you see only the events from that specific Job.
- If a security technology was deleted from the environment and the security stack, those events are still shown.
- You cannot create a monitor for a Job or Job Action if an Action was deleted or if the Evaluation or Sequence was modified.



Add a Monitor from an Action definition

Before you begin

For Email Actions only: to avoid receiving duplicate email notifications for each failed Email Action within an evaluation, the **Timeout for Monitor Event Detection** must be a larger value than the settings for **Initial Period** and **Long Period** checks. For more information, see **Advanced Settings for Security Validation** **(https://docs.mandiant.com/home/msv-**

advanced-settings).

Add a monitor

1. From any point mentioned above, click **+Monitor** or **+** next to an Action on a Job page.
   The **Create Monitor** wizard opens. The steps required for a Monitor depend on the Monitor type.

   Creating a Monitor from a Job pre-populates the configuration for you.

   a. Enter a Monitor *name.*
   b. Optional: Enter a Monitor *description*.
   c. Optional: Add *Tags*.
   d. Add a *Monitor Group* by selecting an existing Monitor or adding a new group from this field.

      Typeahead search is enabled for searching existing Monitors.

   e. Enter the *Initial Runtime* for the Monitor (default is current time).
   f. Enter the repeat interval (in seconds, minutes, hours, or days).

      A Monitor is always set to repeat until you pause or cancel it.

   g. Enter *Extra Sleep* (in seconds).

      This field only applies to Host CLI Actions and should be used when either of the following applies:
      - Environments running the Actions are slow and need extra time for events to be generated and pulled on the host system.
      - Security technologies on the host OS take some time to generate events and the action needs extra time to wait for the events to be generated

   h. Click **Next**.

2. Complete the runtime parameters for each Action in the Monitor. Each Action will have its own Action Run Configuration page in the wizard.
   a. Configure **Run Group Between** by selecting **Actors** or **Zones** from the drop-down menu.

      For Cloud Actions, you can select a Cloud Profile from the Cloud Profiles drop-down menu or select No Cloud Profile.

   b. Complete the Group configuration. The configuration fields are presented based on your choice in the previous step.

      - For Port Scan Actions, you can specify the Interfaces you want to use, and define the expected Open Ports and Closed Ports. Port numbers can be entered as a comma-separated list, a range of ports, or a combination of the two methods. If you have a Monitor interface configured, you can specify that interface for running the Monitor.
      - If you create a Monitor from the Action Library (**Library > Actions**), the input values for the Action are pre-populated. If you create a Monitor from a previous Job, the Cloud Action inputs / Cloud Profile values are prepopulated. If you edit an existing Monitor, saved input values display.

- Certain Actions (Network, DNS, Host CLI) can be run as a specified user, rather than the default system user. If you choose a Windows Actor as a source and run one of these Actions, you can choose a different user account under **Run as User** and specify whether this user should sign in using an **Interactive Session**.
- The Interactive Session setting may already be checked by default, depending on the Action being run and your global Actor settings. When enabled, the selected user account can sign into the Windows Actor so that supported Actions can run. See **Actor Communication Settings** (https://docs.mandiant.com/home/msv-settings-actors) for more information on global default settings for Actors.
- An interactive session supports certain Host CLI commands that won't run successfully without a desktop. This session is needed for Host CLI commands that need to get window titles.
- An interactive session is required for testing certain security controls.

- An interactive session signs out anyone else who is currently using the Windows Actor system.
- On Windows Actors, non-System users may have insufficient privileges to run DNS tunneling actions.

c. Define the expected result for the Group. Set each of the following fields to **Yes**, **No**, or **Does Not Matter**.
   - **Expected Blocked**: Set to Yes if you expect this Action to be blocked by security technologies.
   - **Expected Detected**: Set to Yes if you want this Action to pass when it is detected.

     You cannot set both Expected Blocked and Expected Detected to "Does Not Matter" or the Monitor will not run.

3. If **Expected Detected** is **Yes**, select the events required for the Monitor to pass.
   - If you are creating the Monitor from a Job that has been run, the wizard will pull in events for the Job and will display them as a list, sorted by the integration they came from.

     Only selected events will be used for matching when the Monitor runs. If no events are selected, any event that fires will meet the Pass requirements for Expected Detected.
   - When you select an event, you can then edit the text description of the event, if desired. The event will be matched if the string is matched. The string is case-insensitive.
   - Events can also be edited for a partial string match.

4. When an event includes dynamic data that is not repeatable, that exact event will never occur again and, therefore, AEDA is rendered inoperable.
   For example, you create a monitor and select a Palo Alto Firewall event, which generates the following message name:

   ```
   trojan.alert blocked 29JAN2022-15:05:03 UTC
   ```

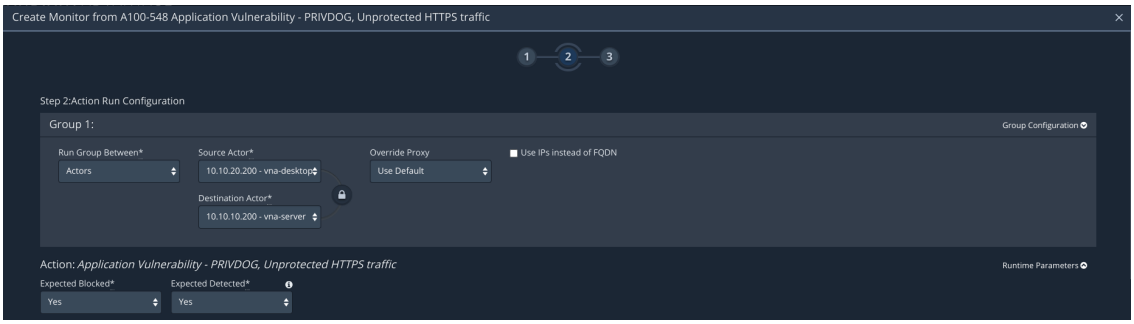
   This event will never occur again because of the date/time stamp. To edit for a partial string match, you can select the message name with a left-click and access a cursor; then, delete the date/time stamp so that the event now reads:

   ```
   trojan.alert blocked
   ```

So now, when a future event comes in as

```
trojan.alert blocked 03FEB2022-11:20:09UTC
```

the string matches.



HTTPS Monitor with Events

5. Click **Next**.
   Continue to complete configuration for all Actions. The numbers at the top of the wizard indicate screens within the current Monitor configuration. You can click on a wizard page to return to a given Action.
6. Review the **Summary** and then click **Save Monitor**.

Edit a monitor

1. Go to **AEDA > Configuration**.
2. Click **Edit** next to the Monitor you want to edit in the Monitors table.
3. Edit the Monitor Definition and Actions, as needed.

   When you edit a Monitor configuration, you will see all events from any of an Action's Jobs.
4. Review the Summary.
5. Click **Update Monitor**.