Mandiant

RUN PROTECTED THEATER ACTIONS

Protected Theater (PT) Actions are run the same way as all other Actions. However, there are some limitations and additional steps that occur while they run/after they run.

- Network Actions should not be run from a PT Actor. Unless there are explicit Protected Rules defined, the PT network component will block any traffic.
- When you select a PT Action, only Protected Theaters or PT Actors can be selected.
- To run a PT Action with a User Profile, you can select the user profile from the **Run as User** drop-down for the Action. Depending on your global Actor settings, **Interactive Session** may be enabled or disabled by default. We recommend that you enable this setting as it is required for PT Actions. For more information in Actor settings, see **Actor Communication Settings** (https://docs.mandiant.com/home/msv-settings-actors).

  - 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.

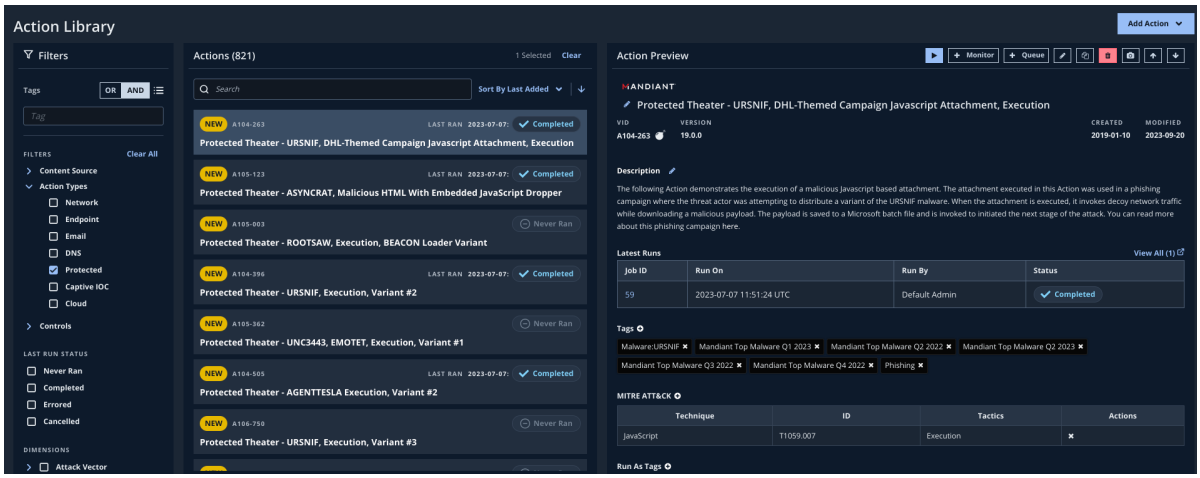
  - An interactive session signs out anyone else who is currently using the Windows Actor system.
  - On Windows Actors, non-System users may have insufficient privileges to run DNS tunneling actions.

- After running a Host CLI Action on its own, or a Malicious Files Action, the system rolls back to the most recent snapshot, removing any changes (file system & DNS entries for example) that were made. This also forces a time sync.
- After a Group containing a PT Host CLI Action completes, the system will roll back to the most recent snapshot. In reverting to a known good state in the Windows or Linux environment, any changes from running Host CLI Actions (such as file system and DNS entries) will no longer exist. It also means the Sequences and Evaluations could revert to the most recent snapshot multiple times and must include enough time to allow the rollback to complete.

For full information on how to run an Action, see **Running Actions** (https://docs.mandiant.com/home/msv-running-actions).

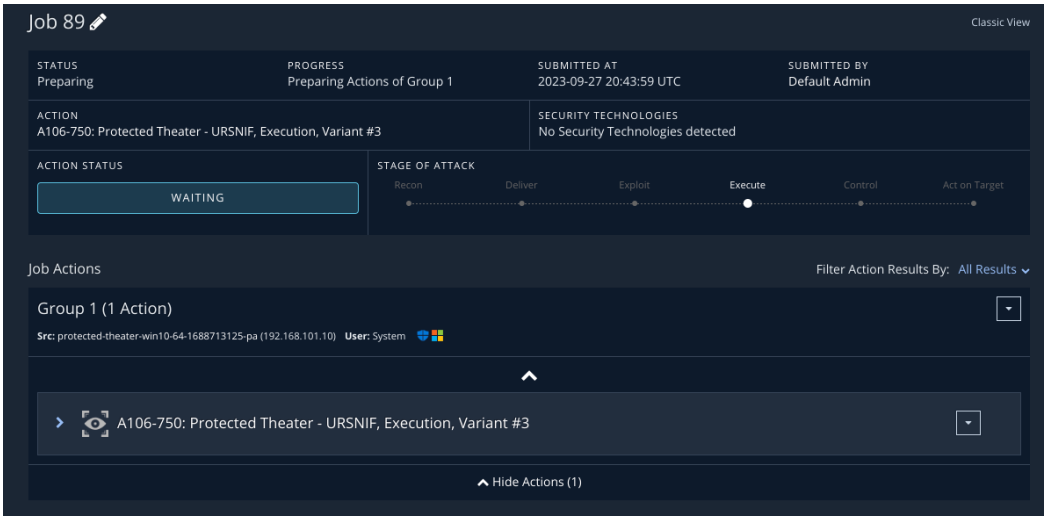
Identifying PT Actions

In the Action library, there is a dimension filter specifically for Protected Theater Actions. It is listed as **Protected**. When you select a PT Action, the Action Preview includes a  icon in the header to identify it as a PT Action.



Action library highlighting the Protected Action Type filter

When reviewing a Job, you can identify that it is a Protected Action by the icon next in the Group column next to the Action. You can view Screenshots and the CLI Log for Host CLI Protected Actions.



Job for a Protected Action