Mandiant

ADDING PROTECTED THEATER ACTIONS

Protected Theater Actions are a special type of Host CLI Action that includes destructive behaviors. These Actions can include malicious files or be completely based on code, using one of the following shells: cmd.exe, PowerShell 2.0+, Python, and Bash.

In general, the overall process to create a Protected Theater Action includes the following steps:

1. Determine if the Action uses a file and if that file is already in the File Library.
2. If necessary, go to the File Library and add the file.
3. Approve the file / have your Security Validation admin approve the file.
4. From the Action Library, select the option to create a Host CLI Action.
5. Create and save (save and Require Protected if you have the permissions) the Host CLI Action.
6. If necessary, have your Security Validation admin review and save as a Protected Theater Action.

As with standard Host CLI Actions, there are **several options and limitations** **(https://docs.mandiant.com/home/msv-adding-host-command-line-interface-actions#Options_and_Limitations)** you need to be aware of.

For adding and approving files, see:

- **Adding Files to the File Library** **(https://docs.mandiant.com/home/msv-adding-files-to-the-file-library)**
- **Approving Files for Use in the File Library** **(https://docs.mandiant.com/home/msv-approving-files-for-use)**

For creating and approving the Host CLI Action, see:

- **Create a Host CLI Action** **(https://docs.mandiant.com/home/msv-adding-host-command-line-interface-actions#To_Create_a_Host_CLI_Action)**
- **Approve a Host CLI Action** **(https://docs.mandiant.com/home/msv-adding-host-command-line-interface-actions#To_Approve_a_Host_CLI_Action)**