CROWDSTRIKE: EXCLUSIONS & LOCAL LOGS

Security Validation validates the effectiveness of your security technologies. This is done by installing Actors in locations around your network. Endpoint security technologies running on the Actor may flag Mandiant services that are required to run Actions. In order for these Actors to be effective and carry out Actions, certain endpoint files pertaining to the execution of these Actors must be added to the allowlist with the security technologies installed on the host.

> The following information is based on the security technology manufacturer's documentation. If the steps do not match your UI, consult the technology's documentation directly.

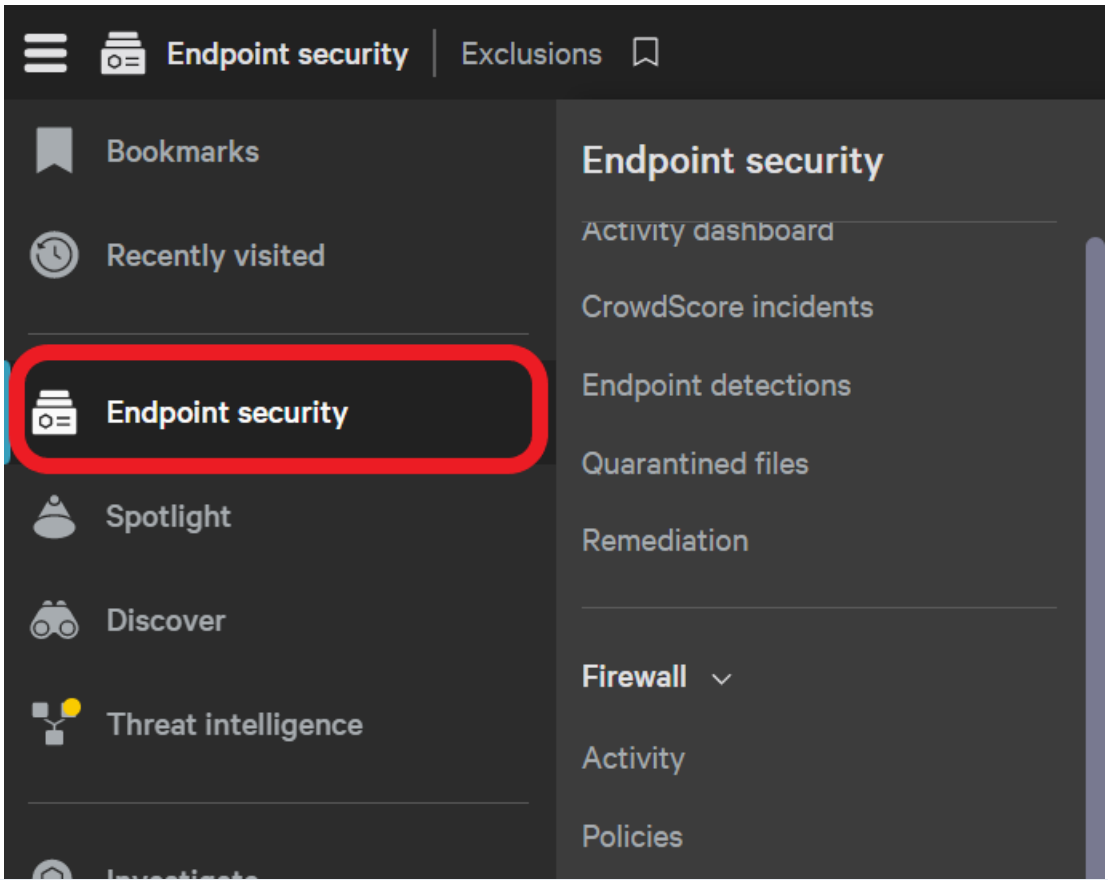
When using Security Validation on a network that includes CrowdStrike, the Mandiant Advantage team recommends completing the following two processes:

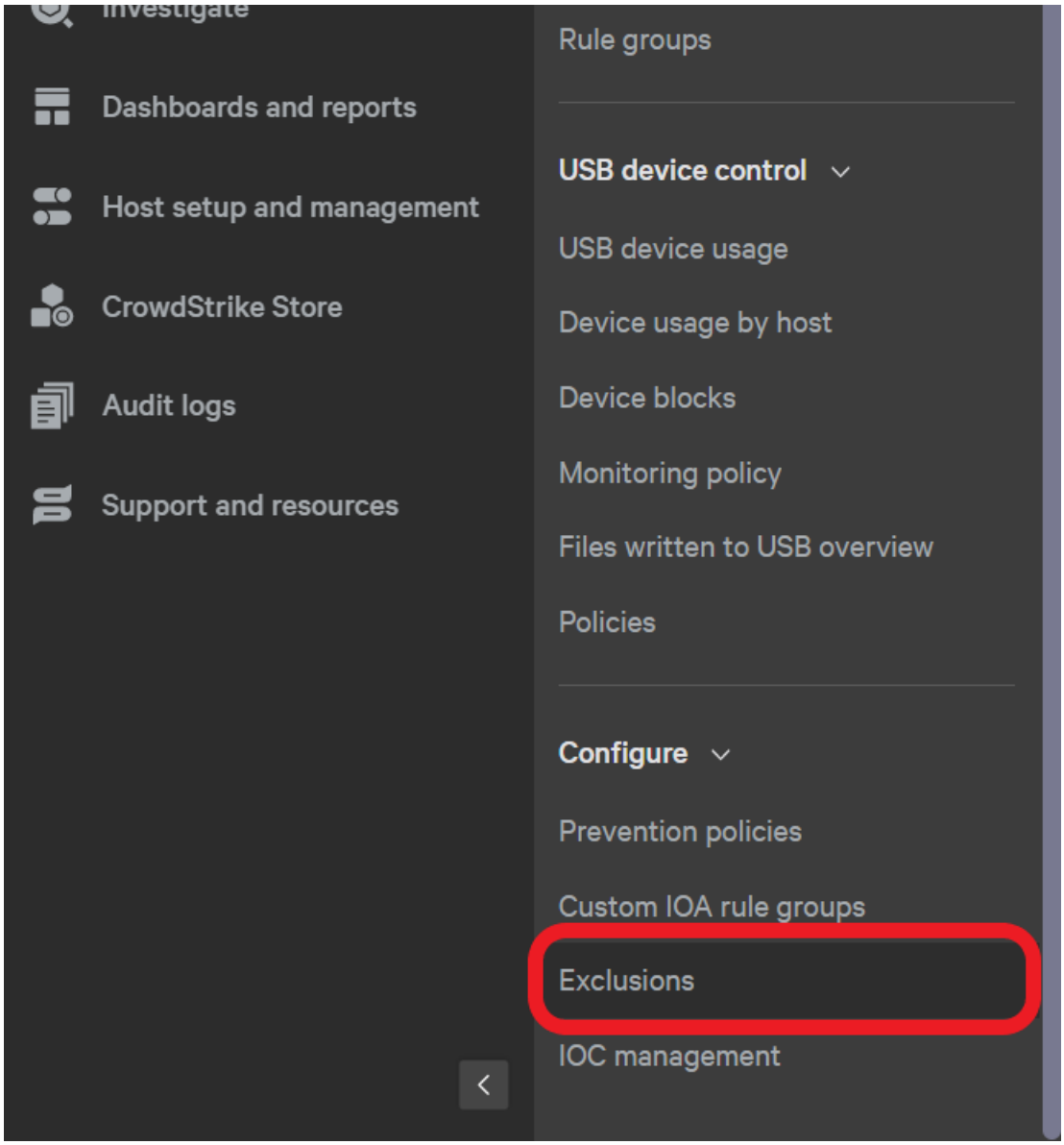
- **Establish Exclusions in CrowdStrike:** Instructions on how to create exclusions within CrowdStrike to quiet detections for known file paths and allow trusted processes to run.
- **Enable Local Logs** in **CrowdStrike:** Instructions on how to set-up local logging for CrowdStrike on Windows endpoints.

CrowdStrike: Establish Exclusions

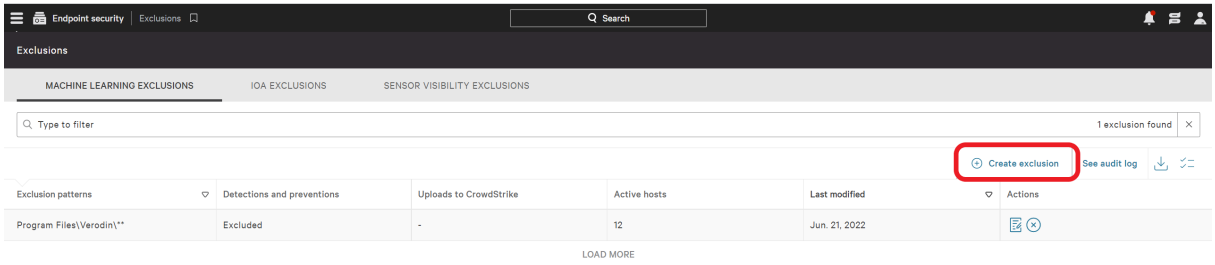
These are instructions on how to create exclusions within CrowdStrike to quiet detections for known file paths and allow trusted processes to run.

1. Navigate to Exclusions menu item: **Configuration > Endpoint security > Exclusions**.

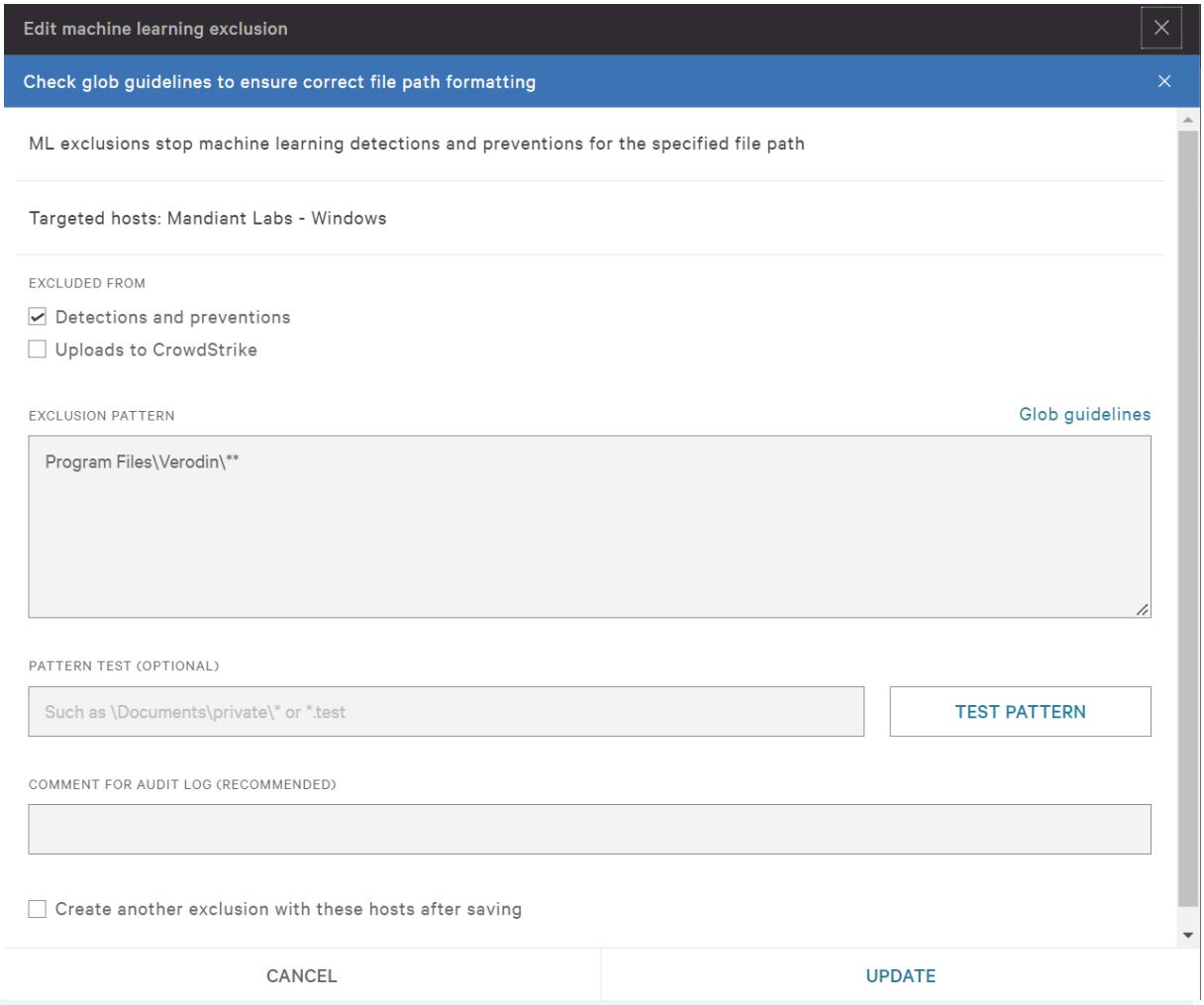




2. Select **Create exclusion** under the MACHINE LEARNING EXCLUSIONS tab.



3. Select the group you would like to apply the exclusions to.
4. Add *Program Files/Verodin/*** to exclude all subfolders and processes within that folder, which is the Security Validation directory.



NOTE: If your security controls prevent you from using wildcards, you can use the full file names or hashes instead. If you choose to use the hashes, CrowdStrike will need to be updated each Validation release. A list of the file names and their hashes (for the current version) is located in the Windows Actor Install QS Guide.

5. Click **Update** to apply the exclusion.

CrowdStrike: Enable Local Logs

These are instructions on how to set-up local logging for CrowdStrike on Windows endpoints.

1. Create a file with the extension .reg titled *crowdstrike_local_log_enable.reg*.
2. Copy and paste the following into your file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default]
"AFLAGS"=hex:03,00,00,00
```

3. Open a command prompt and run the following command to enable logging:

```
regedit crowdstrike_local_log_enable.reg
```

4. The logs can be found at `Falcon Sensor-CSFalconService/Operational`.