Crowdstrike - Cheatsheet

- Create Test Detections

Create Test Detections

Original Article

We have several test detections that can be run to verify the Falcon sensor is sending detections back to the cloud and that they are being received in a timely manner.

If you have a SOC that receives and responds to alerts, it would be advisable to alert them before testing, as it will set off notifications and possibly wake up your on-call. (Don’t wake up your on call, they won’t be happy for a test!)

The following are test detections that can be used on your host:

Windows

```
cmd crowdstrike_test_critical
```

```
cmd crowdstrike_test_high
```

```
cmd crowdstrike_test_medium
```

```
cmd crowdstrike_test_low
```

```
cmd crowdstrike_test_informational
```

Steps:

1. Open a command shell with admin privileges.
2. You have the option of running the commands above either all at once, or one at a time.
3. Running all commands at once will result in one detection, with multiple processes seen as they were all run together. This will also generate an incident as well.
4. Make sure you hit Enter after running the command in order to complete it.