CROWDSTRIKE

Product Name: Falcon Prevent

Main Website: http://www.crowdstrike.com

Product Website: https://www.crowdstrike.com/products/falcon-prevent/

Product Integration Type

Endpoint

Integration Objective

Verifies if a binary file was executed on an endpoint after SmartCore logs a network download event.

Customer Value Proposition

- Incident Response teams do not have sufficient information to determine if an endpoint is infected with malware after an endpoint downloads a binary file.
- SmartCore polls the CrowdStrike server to verify if any binary was executed on an endpoint.
- If the binary file was executed, there is a high probability of infection, and the endpoint will require reimaging.
- If the binary file was not executed, the file only requires removal of the malicious file.

Tested Vendor Versions

Falcon - Windows Sensor 2.28.502

Integration Classification

Other: Incident Response

Integration Details

Enterprise. Can work in large environments with a variety of integration points.

Integration Method

Pull: CrowdStrike file execution. SmartCore polls the CrowdStrike server to verify if a file was executed on an endpoint. The polling uses a hostname. For optimum CrowdStrike integration, SmartCore requires integration with Active Directory to know the hostname of the endpoint and its IP address information.

Integration Detail Summary (API, CLI)

- SmartCore uses the CrowdStrike API to verify if a binary file was executed on an endpoint.
- There are no APIs in CrowdStrike to query based on endpoint IP address. The query to CrowdStrike is based on hostname information. SmartCore requires integration with Active Directory to obtain the endpoint hostname information.
- CrowdStrike + AD Integration + CrowdStrike Endpoint Integration would be total solution for CrowdStrike Integration to work.

Cyphort Manager GUI Component

- Yes
- Cyphort Manager Configuration requires Active Directory integration. This is configured under Settings -> Environmental Settings
- CrowdStrike Integration: This is configured under Settings -> Environmental Settings -> Endpoint Integration Settings

GUI Operational Use Case

If a file was executed at the endpoint, the relevance increases thus increasing the threat score. The progression is appended with the keywords EX—meaning the binary was executed.

Threat Score Impact

Yes

Integration Documentation

N/A

Integration Demo

No

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com

Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com