CISCO

Product Name: ASA

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

Product Website: http://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html

Product Integration Type

Firewall

Integration Objective

- Integrates with Cisco ASA to mitigate malicious IP addresses.
- SmartCore compiles the list of malicious IP addresses from CNC IP addresses seen in infections. To avoid false positives, SmartCore checks for the reputation of the CNC IP addresses.
- SmartCore pushes the CNC IP addresses automatically to ASA, without any need for manual intervention.

Customer Value Proposition

Integrates with existing third party infrastructure in the customer's environment to block calls to malicious CNC servers.

Tested Vendor Versions

Cisco's Winter 2014 ASA software release

Integration Classification

Blocking: Firewall and Web Proxy

Integration Details

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

Integration Method

Push: SmartCore pushes CNC IP addresses to ASA.

Integration Detail Summary (API, CLI)

- SmartCore uses ASA's JSON/REST API to push CNC IP addresses that need to be blocked
- REST API is not available along with base image. It needs to be downloaded separately
- The list of CNC IP addresses are pushed to a network object group which is used in a blocking policy
- SmartCore pushes the CNC IP addresses to an address book defined in SRX
- CNC IP addresses can be added or removed from the SRX using the Cyphort Manager UI
- User can also specify "expiry days" on Cyphort Manager's UI to automatically remove the CNC IP addresses from SRX after the specified number of days expire

Cyphort Manager GUI Component

- Yes
- Configuration: ASA settings can be configured under Settings -> Environmental Settings

GUI Operational Use Case

Operational Use Case: Under the Mitigation tab in the Cyphort Manager, the CNC IP addresses show up under Firewalls. The administrator can push or remove IP addresses from the ASA manually. From release 3.5 onwards, CNC IP addresses can be pushed automatically to ASA without the need for manual intervention

Threat Score Impact

No

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