CHECK POINT

Product Name: Next-Generation Firewall

Main Website: https://www.checkpoint.com/

Product Website: https://www.checkpoint.com/products-solutions/next-generation-firewalls/

Product Integration Type

Firewall

Integration Objective

- Integrates with Check Point 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
- As of version 3.5, SmartCore pushes the CNC IP addresses automatically to Check Point, 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

- R77.30
- Note: Only the Check Point GAiA operating system release R76, R77, or later is supported. Check Point's IPSO and Secure Platform (SPLAT) are **not supported.**

Integration Classification

Blocking: Firewall, 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 Check Point

Integration Detail Summary (API, CLI)

- SmartCore uses Check Point's SAM (Suspicious Activity Monitor) feature to push CNC IP addresses that need to be blocked.
- SmartCore logs into Check Point using the SSH interface.
- The list of CNC IP addresses are pushed to a network object group which is used in a blocking policy.
- SmartCore uses the "fw sam" commands to configure SAM rules on Check Point. Basic and advanced modes are available.
- CNC IP addresses can be added or removed from Check Point using the Cyphort Manager UI
- Users can specify "expiry days" on the Cyphort Manager's UI to automatically remove the CNC IP addresses from Check Point after the specified number of days expire.

Cyphort Manager GUI Component

- Yes
- Cyphort Configuration: Check Point settings can be configured under Settings -> Environmental Settings.

GUI Operational Use Case

Under the Mitigation tab in Cyphort Manager, the CNC IP addresses show up under firewalls. The administrator can push or remove IP addresses from Check Point manually. From release 3.5 onwards, CNC IP addresses can be pushed automatically to Check Point 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

Copyright 2017 Cyphort, Inc. All rights reserved. Part#TP3004-001US