SPLUNK

Product Name: Splunk Enterprise

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

Product Website: http://www.splunk.com/en_us/products/splunk-enterprise.html

Product Integration Type

SIEM

Integration Objective

Send syslogs to Splunk Enterprise. Splunk App is also supported.

Customer Value Proposition

Customers can check SmartCore alerts and other security devices on Splunk. The Splunk app shows detailed alert statistics in the form of charts and graphs.

Tested Vendor Versions

Splunk 6.1

Integration Classification

SIEM: ArcSight, Splunk

Integration Details

- Basic. Typically works with a single server in small environments
- Enterprise. Can work in large environments with a variety of integration points

Integration Method

- Push: SmartCore sends syslogs to Splunk
- Vendor Pull: Splunk app pulls data from SmartCore periodically to populate data

Integration Detail Summary (API, CLI)

- SmartCore can send alerts to Splunk via syslogs based on trigger or schedule
- Syslogs contain details such as filename, MD5, CNC server IP, and malware name
- Splunk app uses REST API to poll SmartCore every few minutes to get alert details
- Splunk app can show threat category breakdown, top malware, and other statistics

Cyphort Manager GUI Component

Yes

GUI Operational Use Case

- Cyphort Manager configuration: SIEM alerts can be configured under Settings -> Environmental Settings
- Operational Use Case: Splunk UI is checked for threat alerts

Threat Score Impact

No

Integration Documentation

- https://splunkbase.splunk.com/app/3061/#/details
- Cyphort Operators Guide

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