IBM

Product Name: QRadar

Main Website: http://www.ibm.com/us-en/

Product Website: http://www-03.ibm.com/software/products/en/qradar-siem

Product Integration Type

SIEM

Integration Objective

SmartCore can send syslogs to Qradar. Native LEEF is also supported. Log Event Extended Format (LEEF) is a customized event format for IBM® Security QRadar®

Customer Value Proposition

Customers can check alerts from SmartCore and other security devices on QRadar. Native support for LEEF ensures all data is correctly formatted, higher fidelity for alerts, and less false positives.

Tested Vendor Versions

QRadar Version 7.2.8 - Build 20160920132350

Integration Classification

SIEM

Integration Details

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

Integration Method

- Push: SmartCore sends syslogs to QRadar
- Vendor Pull: Qradar pulls data from SmartCore periodically to populate data

Integration Detail Summary (API, CLI)

- SmartCore can send alerts to QRadar via syslogs based on trigger or schedule
- Syslogs contain details such as filename, MD5, CNC server IP, and malware name

- LEEF allows for QRadar to poll SmartCore every few minutes to get alert details
- Qradar with LEEF can show threat category breakdown, top malware, and other statistics

Cyphort Manager GUI Component

- Yes
- Cyphort Manager configuration: SIEM alerts can be configured under Settings -> Environmental Settings

GUI Operational Use Case

Operational Use Case: QRadar UI is checked for threat alerts.

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

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