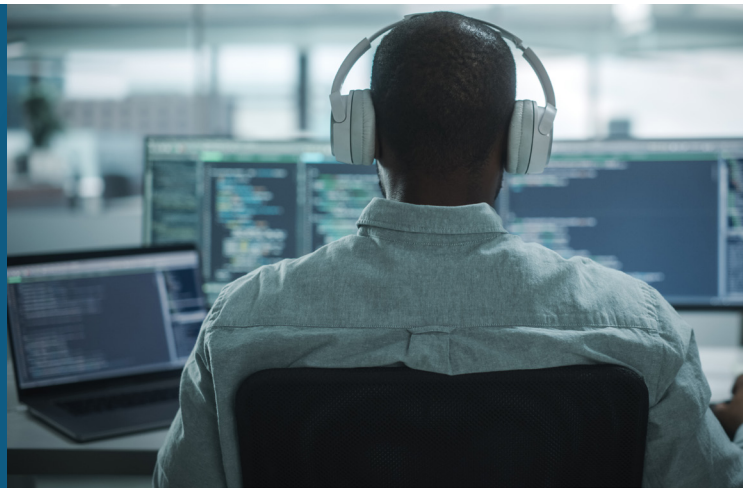
CYLERA | splunk>

SOLUTION BRIEF

Cylera and Splunk Integration

Full Healthcare IoT Visibility, Security, and Threat Detection

Superior NOC/SOC medical device cybersecurity monitoring and incident response



The Challenge

Many healthcare information technology (IT) departments and clinical engineering teams have little to no visibility into the healthcare IoT and connected medical devices on their networks. For these IT teams, securing medical devices presents a huge challenge. These devices can also give attackers a foothold they can then use to infiltrate healthcare networks, compromise patient data and privacy, and put healthcare service delivery at risk.

The Solution

Cylera and Splunk have partnered to deliver faster visibility, more complete threat detection and intelligence, and more accurate cyber risk correlation and analytics for connected medical devices.

Cylera discovers, identifies, and measures connected medical device vulnerabilities and risks, then shares this data with Splunk's Security Information Event Management (SIEM) solution. Splunk captures, indexes, and correlates real-time data, including data provided by Cylera, into a searchable repository network and security teams can use for operational intelligence and response.

Splunk's SIEM can use data from Cylera to help network operations center (NOC) and security operations center (SOC) teams to recognize data patterns, diagnose problems, produce metrics, and power IT to help ensure healthcare delivery organizations have a complete view of their healthcare networks and the devices on them. This also leads to faster mean-time-to-resolve (MTTR) for IT teams when investigating incidents or determining how to best resolve any cybersecurity-related incidents that may occur.

Benefits

- Improved healthcare connected medical device network visibility and security
- Faster **connected medical device threat detection and response**
- Maximization of current IT security investments with no additional cost
- Seamless integration with fast time to value

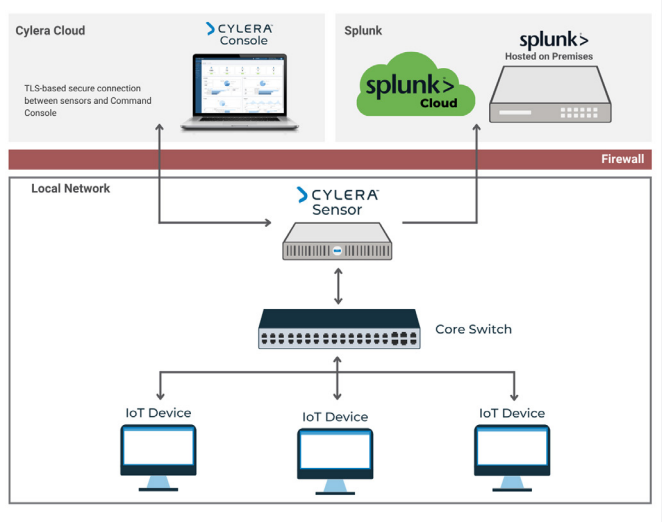
Fortify Care. Accelerate Cyber Resilience.

American Hospital Association™ Preferred Cybersecurity Service

Integration Highlights

- **Maximize existing IT investments:** Obtain real-time visibility into the health, performance, and security of connected medical devices on the network and identify and respond to threats more quickly.
- **Seamless integration and setup:** Configure alerting for anomalous activity on healthcare IoT and connected medical devices in minutes, without requiring extra services or back-end programming.
- **"Zero-touch" healthcare IoT inventory and risk profiling:** Collect detailed medical device information, with no disruption to physical devices or patient care services, using passive, patented Cylera device data collection techniques.
- **Speed response times:** Deliver the information IT teams need to quickly find and resolve incidents with no changes to current workflows.

How It Works



- Cylera's advanced healthcare IoT security and intelligence platform collects and forwards in-depth connected medical device information using patented, passive, zero-touch deep packet inspection technology, which includes vulnerability assessment and risk scoring, without ever touching the physical devices.
- Depending on the device type, Cylera can include over 30 granular device details that are matched with additional vulnerability and risk information from Cylera's proprietary threat intelligence database and threat researchers.
- Splunk then captures, indexes, and correlates the data Cylera provides into a real-time, searchable repository NOC and SOC teams can use for security and network operational intelligence and incident response.

Summary

The Cylera platform delivers an array of healthcare IoT device capabilities, including asset identification and management, network analysis, risk assessment, network segmentation, threat detection and intelligence, and fleet utilization and optimization. All of these capabilities are undergirded by unique, patented technologies - Adaptive Data Type Analysis™ and IoT Device Emulation Engine™, plus proprietary Cylera threat intelligence.

The Cylera and Splunk integration provides a resource-efficient, clinically-aware method for discovering and protecting healthcare IoT and connected medical devices against unauthorized access. It also ensures IT and NOC/SOC teams are fully aware of all of the healthcare IoT and connected medical devices on their network and have the information they need to rapidly respond to cyber incidents and ensure service delivery.

Cylera provides the easiest, most accurate and extensible platform for healthcare IoT intelligence and security to optimize patient care, service availability, and cyber defenses across diverse connected medical device and healthcare environments. The Cylera platform accurately discovers, categorizes, assesses, and monitors known and unknown assets with high fidelity to deliver unparalleled asset inventory, usage telemetry, risk prioritization, analytics, and guided threat remediation. Cylera integrates with popular IT and healthcare systems to allow organizations to advance cyber program maturity, increase operational efficiency,mitigate cyber threats, and enable compliance readiness.

CYLERA™

www.cylera.com