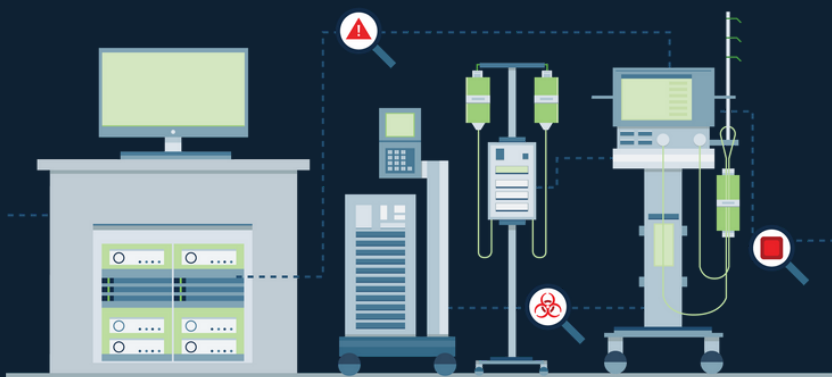
Cynerio | splunk>

Splunk and Cynerio: Optimizing Healthcare IoT Cybersecurity with a Clinical SIEM



Unleashing Powerful Integration

Patients have more control over their data and treatment plans than ever, thanks to connected medical and IoT devices. These devices have transformed the healthcare industry and provided greater accessibility to treatment for patients and streamlined workflows for healthcare professionals, but they have also broadened the attack surface and exposed healthcare facilities to myriad threat actors and cyber exploitation.

The Growing Threat to Healthcare IoT

As healthcare suffers relentless barrages of cyber attacks, identifying at-risk devices and vulnerabilities, managing risk, and remediating threats have become progressively more difficult. Weak security and widespread use of devices running legacy firmware/OS combined with medical and IoT devices' inherent vulnerabilities (e.g. open services and ports, TCP/IP stack vulnerabilities), unique communications patterns, and traditional IT tools' inability to recognize medical/IoMT devices have made healthcare facilities easy and lucrative targets for threat actors.

Executing clinically-blind risk management and incident response risks compromising device functionality, disrupting medical workflows and services, and even network slowdown or total shutdown. Patient safety and data confidentiality are paramount, meaning none of these scenarios is ever an option.

How It Works

The integration between Splunk's SIEM solutions and Cynerio's Healthcare IoT Cybersecurity Platform provides a suite of scalable healthcare-specific solutions developed to address the increasing cyber threats to healthcare.

Cynerio-Splunk integration expedites healthcare-safe Zero Trust risk management and security incident response

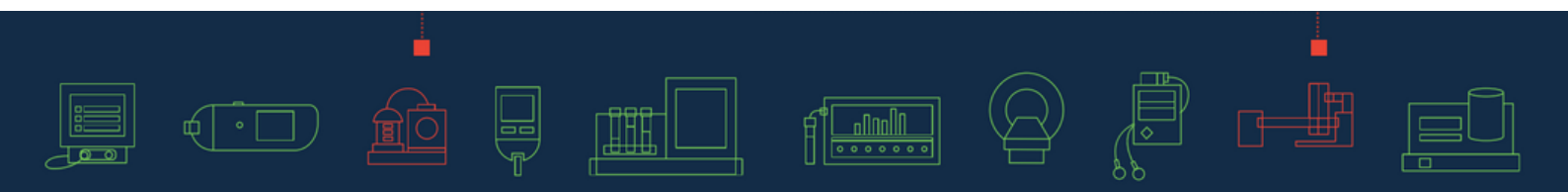
Solution Components

- Cynerio Healthcare IoT Cybersecurity Platform
- Splunk® Enterprise
- Splunk Cloud™
- Splunk® Phantom
- Splunkbase's Data-to-Everything® Platform

The Benefits of Integration

- Real-time risk detection with alerts sent to relevant team members
- Ongoing monitoring of device behavior enriched with clinical context
- Easy incident detection, investigation, and diagnosis with end-to-end observability with Splunkbase's Data-to-Everything® Platform
- Frictionless multi-site deployment, and agentless, network-based monitoring

A centralized view into clinically-contextualized security events, vulnerabilities, and policy violations streamlines risk management and incident response and offers SOC and IT security teams the ability to easily monitor and enforce healthcare-safe policies on medical and IoT devices with the ease of enforcing them on standard IT assets.



1. **Cynerio's device discovery** inventories every connected device, whether it's a medical/IoMT device, Enterprise IoT device, or OT system, and automates ongoing inventory. Every asset is fingerprinted using deep packet inspection (DPI), and Cynerio provides granular, clinically-contextualized information on device communications, vendor, model, OS/firmware, version, MAC address, serial number, utilization patterns, VLANs, and more.

2. The **combined power of Cynerio's AI and in-house threat intelligence research team and Splunk's SIEM solutions,** pinpoints every at-risk Healthcare IoT device, identifies vulnerabilities (i.e. legacy firmware/OS, CVEs, open services, etc.), monitors for threats, and calculates device risk impact according to clinical context and mission criticality.

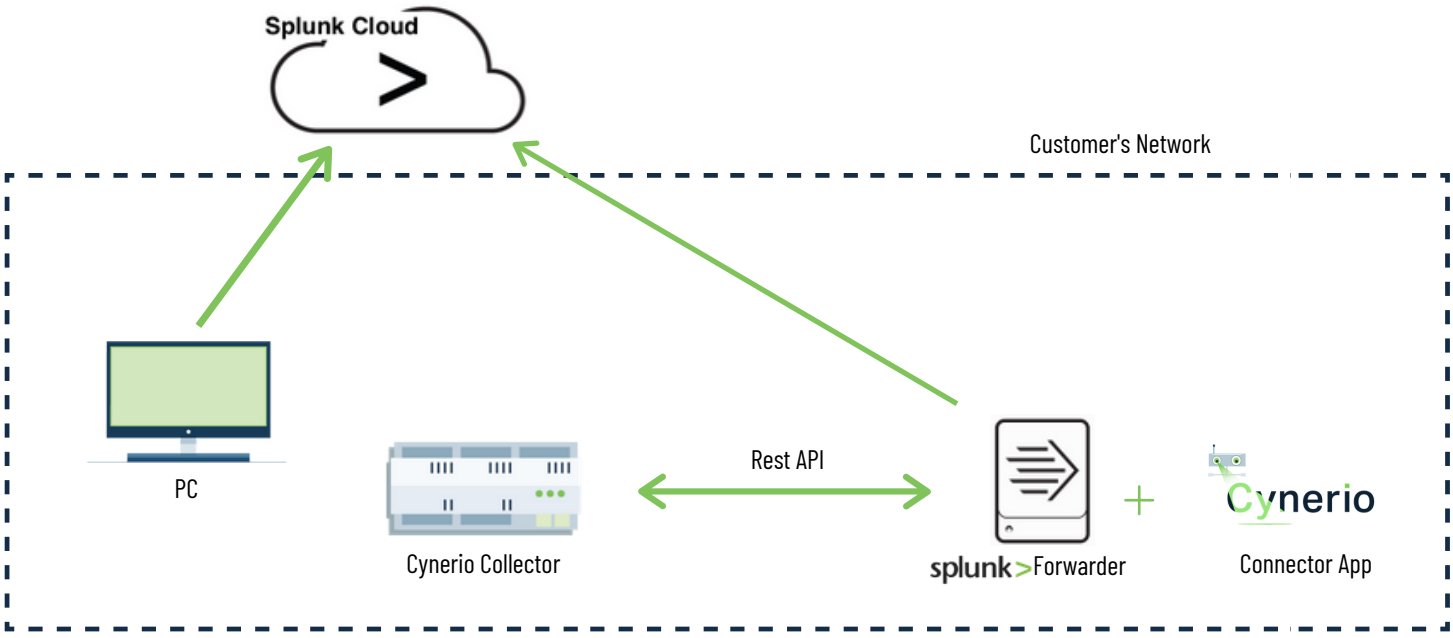
3. **Splunk ingests Cynerio's clinically-enriched data** and integrates it with its proprietary risk management solutions, alerts teams in real time to any suspicious/anomalous activity, unmanaged devices, and newly discovered vulnerabilities.

4. Cynerio provides **step-by-step remediation paths** built on Zero Trust policies optimized for hospital-specific workflows and network topologies for every device, vulnerability, and risk.

5. Cynerio's **Virtual Segmentation capability** auto-configures robust, **healthcare-safe Zero Trust security policies** in seconds and allows them to be tested for violations and edited before they're enforced. The combination of Virtual Segmentation with the Splunk SIEM's powerful violation monitoring facilitates **streamlined risk management and automated incident response** while ensuring the preservation of clinical workflows and patient safety.

The Benefits of Integration (cont'd.)

- Automated and continuous, real-time Healthcare IoT asset (medical/IoMT, Enterprise IoT, and OT) discovery and fingerprinting data is passed to Splunk
- Clinically enriched risk scores calculated according to device risk impact
- Automated mitigation executes actions across security infrastructure in seconds
- Automation enables offloading of repetitive security tasks and enables staff to focus on mission-critical projects
- Frictionless and automated sync of complex workflows across every team and security tool facilitates a unified defense strategy with Splunk® Phantom
- Healthcare-safe Zero Trust mitigation and incident response strategies infused with clinical context
- Ability to configure and test mitigating segmentation policies for violations before enforcing them with Cynerio's **Virtual Segmentation** capability



Integration Components

Cynerio

Cynerio's clinical security intelligence on every Healthcare IoT device can be easily consumed by Splunkbase products to streamline clinical risk management and automate incident response. The platform's healthcare-focused solutions adapt to rapidly evolving threats, technological advancements, and healthcare industry standards. Its AI-powered, full-suite Healthcare IoT cybersecurity platform empowers hospitals with the ability to act fast, ensure compliance, and achieve sustainable and robust security posture with foresight and easily deployable, scalable, and adaptable IT solutions tailored to healthcare.

Splunk

Splunk® Enterprise

Splunk Enterprise Security is the analytics-driven SIEM solution that gives you the ability to quickly detect and respond to internal and external attacks. It makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results. Identify, prioritize and manage security events with event sequencing, alert management, risk scores, and customizable dashboards and visualizations. Gather all the context you need in one view to perform rapid investigations and response. Take care of existing and newly discovered threats fast with contextual threat detection and incident response.

Splunk Cloud™

Splunk Cloud is the industry's only enterprise-ready cloud service for machine data, offering a 100% uptime SLA and standard plans from 5GB/day to 5TB/day. From infrastructure management to data compliance, Splunk Cloud is built to scale to your data analytics needs, ranging from GBs to PBs and beyond. Architected to facilitate sudden bursts in data volume, Splunk Cloud allows you to incrementally upgrade capacity white retaining security by design.

Splunk® Phantom

Splunk® Phantom provides security orchestration, automation and response (SOAR) capabilities that allow analysts to improve efficiency and shorten incident response times. Phantom supercharges the scalability, performance and speed of your security automation with the ability to process 50,000 security events per hour. With Phantom, organizations are able to improve security and better manage risk by integrating teams, processes and tools together. Security teams can automate tasks, orchestrate workflows and support a broad range of security operations center (SOC) functions including event and case management, collaboration and reporting.