Healthcare Organization Protects Critical Medical Devices Through Continuous Detection and Response

How SilverSky identified vulnerable medical devices, detected signs of active exploitation, and helped a healthcare provider reduce risk while maintaining critical patient services.

Overview

A healthcare provider partnered with SilverSky to strengthen security operations across its clinical environment using Lightning MxDR and continuous vulnerability validation.

During routine monitoring, SilverSky identified vulnerable medical devices communicating in ways that suggested potential malicious activity.

Although a vendor patch was not immediately available, SilverSky worked closely with the hospital's IT team to implement compensating controls, increase monitoring, and reduce the organization's exposure until remediation could be completed.

The result was improved visibility, reduced operational risk, and uninterrupted support for critical patient care systems.

Operational Challenges

Medical Device Visibility

Connected clinical devices increased the organization's attack surface.

Protecting Patient Care

Security incidents could impact critical healthcare operations.

Legacy Medical Systems

Older technologies required additional monitoring and protection.

Continuous Threat Detection

The organization needed 24×7 visibility across its environment.

Lean Security Team

Limited internal resources made rapid investigation and response difficult.

Operational Resilience

Security needed to improve without disrupting patient care.

The Challenge

Healthcare organizations depend on connected medical devices that often cannot be taken offline for immediate patching or replacement. In this environment, balancing cybersecurity with patient care requires continuous visibility and carefully planned response strategies.

SilverSky identified vulnerable medical devices affected by a newly discovered security issue. Additional analysis revealed suspicious DNS communications and behavioral indicators suggesting the vulnerability could be actively exploited.

Because the devices remained essential to patient care, immediate replacement or patching was not an option.

The SilverSky Response

SilverSky combined vulnerability intelligence, continuous monitoring, behavioral analytics, and Security Operations Center expertise to investigate the activity.

Working directly with the hospital, analysts confirmed the affected devices, identified suspicious communications, and developed compensating controls that reduced the likelihood of attacker movement while maintaining operational availability.

The team also helped fingerprint device communications, supported secure vendor access for future maintenance, and assisted the organization in implementing a Zero Trust network strategy while waiting for the manufacturer to release a permanent patch.

The Outcome

Critical Devices Protected

The healthcare provider reduced operational risk without disrupting essential clinical services.

Improved Visibility

Continuous monitoring provided greater insight into vulnerable devices and suspicious activity.

Faster Decision-Making

Security and IT teams gained the information needed to respond confidently despite limited remediation options.

Stronger Security Posture

Compensating controls and Zero Trust principles strengthened protection while permanent remediation was planned.

Security Has To Be Operated.

Cybersecurity isn't defined by the tools an organization owns—it's defined by how effectively those tools are monitored, managed, and continuously improved. Every customer engagement reinforces SilverSky's commitment to operational security, helping organizations reduce risk, strengthen resilience, and respond confidently to evolving cyber threats.

Healthcare depends on technology that must remain available around the clock. SilverSky helped deliver continuous visibility across connected medical devices and clinical systems, supporting stronger security while helping protect uninterrupted patient care.

Why It Mattered

This engagement demonstrated how continuous monitoring, vulnerability intelligence, and expert-led security operations can help organizations reduce risk—even when vulnerabilities cannot be immediately patched.

Rather than waiting for a vendor update, the healthcare provider implemented practical security controls that protected critical medical devices while maintaining uninterrupted patient care.

Talk to a Security Expert

See how SilverSky helps healthcare organizations protect connected medical devices, strengthen clinical security, and reduce cyber risk while supporting uninterrupted patient care.

www.SilverSky.com | Learn@SilverSky.com