Manufacturing Organization Uncovers Hidden Threats with SilverSky Lightning MxDR

How SilverSky combined continuous monitoring, expert investigation, and enhanced endpoint visibility to identify malicious activity that had gone undetected and help strengthen the organization's security posture.

Overview

A manufacturing organization partnered with SilverSky to implement Lightning MxDR while continuing to use its existing endpoint protection platform. Shortly after deployment, SilverSky Security Operations Center (SOC) analysts detected suspicious network activity that could not be validated by the customer's existing endpoint security tools.

By enabling additional Managed Endpoint Detection & Response (MEDR) capabilities within the SilverSky platform, analysts identified active attacker behavior, confirmed malicious activity, and worked alongside the customer to contain the threat and strengthen endpoint protection across the environment.

Operational Challenges

Limited Security Visibility

Disconnected tools reduced visibility across the environment.

Manufacturing Uptime

Production systems required continuous protection and availability.

Alert Fatigue

Too many alerts made it difficult to identify real threats.

Lean Security Team

Limited resources made 24×7 monitoring difficult.

Evolving Threats

Modern attacks demanded faster detection and response.

Operational Resilience

Security needed to improve without disrupting production.

The Challenge

The organization relied on business-critical production systems that demanded continuous uptime. Even a minor security incident had the potential to interrupt manufacturing operations, delay production schedules, impact supplier commitments, and create costly operational downtime.

Leadership recognized that simply deploying additional security tools would not solve the problem. They needed experienced analysts, continuous monitoring, and a mature security operations capability that could quickly identify real threats while reducing unnecessary alert noise.

SilverSky Lightning MxDR provided the organization with continuous threat detection, expert investigation, and operational visibility across its environment, helping transform fragmented security data into actionable intelligence.

The SilverSky Response

To increase visibility, SilverSky enabled Managed Endpoint Detection & Response capabilities through the SilverSky Security Agent already deployed within the customer's environment.

Almost immediately, SilverSky analysts identified evidence of malicious activity, including attacker tools commonly associated with credential theft and lateral movement. The SOC confirmed the compromise, notified the customer, and coordinated remediation efforts.

Following incident response activities, the customer expanded MEDR protection across all endpoints.

Continued monitoring identified additional malicious activity that was isolated and removed before further damage could occur.

The Outcome

Active Threat Identified

SilverSky uncovered malicious activity that had not been detected through the customer's existing endpoint monitoring.

Improved Endpoint Visibility

Additional endpoint telemetry provided the context needed to investigate and validate suspicious behavior.

Stronger Security Operations

Continuous monitoring and analyst-led investigation enabled faster detection and more confident response decisions.

Increased Protection

Expanded MEDR capabilities strengthened endpoint security and improved resilience against future attacks.

"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.

Hidden threats often exist long before they trigger an alert. Through continuous monitoring and expert investigation, SilverSky helped uncover suspicious activity that improved visibility across the environment and strengthened the organization's overall security posture."

Why It Mattered

Security visibility is only as effective as the quality of the data available for investigation.

By combining continuous monitoring, endpoint telemetry, and expert-led threat analysis, SilverSky helped the customer identify malicious activity that might otherwise have remained hidden.

The engagement reinforced an important principle: effective security operations rely on integrated visibility, experienced analysts, and continuous execution—not on any single security product alone.

Talk to a Security Expert

Learn how SilverSky can help improve threat visibility, uncover hidden risks, and strengthen security operations through continuous monitoring and expert-led detection and response.

www.SilverSky.com | Learn@SilverSky.com