How a Customer Incident Improved Every Future SilverSky MxDR Deployment

A real-world security incident led SilverSky to enhance its deployment methodology, adding proactive external attack surface validation that helps customers identify vulnerabilities before security monitoring begins.

Operational Challenges

Hidden External Exposure

Unknown internet-facing assets increased organizational risk.

Deployment Readiness

Greater validation was needed before security monitoring began.

Limited Attack Surface Visibility

External exposure required a more comprehensive assessment.

Continuous Improvement

Every customer engagement became an opportunity to strengthen future deployments.

Proactive Risk Reduction

Identifying vulnerabilities earlier helped improve security from day one.

Operational Excellence

The experience refined SilverSky's onboarding methodology for every future customer.

Overview

An educational institution with a small internal IT team partnered with SilverSky to deploy Lightning MxDR. During implementation, the customer experienced a security incident after attackers exploited internet-facing ports that had unintentionally remained open following a network change.

As part of the recovery effort, SilverSky performed a complimentary external perimeter assessment to identify additional exposed services and vulnerabilities. The assessment uncovered security gaps that, once remediated, significantly strengthened the customer's external security posture.

The engagement also prompted SilverSky to enhance its MxDR deployment methodology by incorporating proactive external attack surface validation into every new implementation.

The Challenge

The customer relied on outsourced IT and security resources while deploying SilverSky Lightning MxDR. During implementation, attackers exploited exposed perimeter services that had remained accessible after a routine infrastructure change.

Although incident response activities successfully restored operations, the event demonstrated that endpoint monitoring alone cannot identify every source of organizational risk. External exposure must also be validated to establish a strong security foundation.

The SilverSky Response

Following incident response, SilverSky conducted a comprehensive external perimeter assessment using its Attack Surface Management and vulnerability scanning capabilities.

The assessment identified additional exposed ports, vulnerable perimeter devices, and security improvements that reduced the organization's external attack surface before completing the MxDR deployment.

Based on the success of this engagement, SilverSky updated its implementation methodology so every new Lightning MxDR customer is offered a one-time external perimeter assessment during deployment. This provides valuable insight into externally visible risks before ongoing security operations begin.

The Outcome

Stronger External Security

The customer reduced unnecessary exposure by closing open ports and remediating identified vulnerabilities.

Improved Security Posture

External attack surface validation strengthened the customer's environment before full operational monitoring began.

Better Deployment Experience

SilverSky enhanced its deployment methodology using lessons learned from a real-world customer engagement.

Long-Term Customer Value

Every new Lightning MxDR deployment now benefits from proactive external perimeter validation, helping customers reduce risk before security operations begin.

Why It Mattered

Security operations are most effective when built on a secure foundation.

This engagement demonstrated that improving security isn't only about detecting threats—it's also about identifying and eliminating unnecessary exposure before attackers have an opportunity to exploit it.

The experience reinforced SilverSky's commitment to continuous improvement by transforming a single customer engagement into a deployment enhancement that now benefits future customers.

"Security Has To Be Operated."

Every customer engagement reinforces SilverSky's commitment to operational security, helping organizations reduce risk, strengthen resilience, and respond confidently to evolving cyber threats.

Every security event is an opportunity to improve. A real-world customer incident led SilverSky to enhance its onboarding methodology, adding proactive external attack surface validation that now helps every new customer reduce risk before monitoring begins.

Talk to a Security Expert

Discover how SilverSky helps organizations identify external exposures, validate attack surfaces, and strengthen security before monitoring even begins through a proactive, security-first deployment approach.

www.SilverSky.com | Learn@SilverSky.com