Property Management Organization Detects Unauthorized Insider Activity During MxDR Onboarding

How SilverSky Lightning MxDR correlated seemingly routine events to uncover unauthorized privileged activity, reduce organizational risk, and strengthen long-term security governance.

Operational Challenges

Limited User Visibility

User activity lacked centralized monitoring and context.

Insider Risk

Unauthorized activity required immediate investigation.

Early Threat Detection

Suspicious behavior needed to be identified from day one.

Onboarding Visibility

Security monitoring required a trusted operational baseline.

Lean Security Team

Internal resources couldn't continuously investigate every event.

Operational Confidence

The organization needed assurance that security events would be detected and acted upon quickly.

Overview

A property management organization partnered with SilverSky to deploy Lightning MxDR and improve visibility across its security environment.

Within the first 24 hours of onboarding, SilverSky Security Operations Center (SOC) analysts correlated thousands of low- and medium-severity events across firewall, DNS, and Active Directory telemetry. While each event appeared benign in isolation, together they revealed unauthorized privileged activity that created unnecessary organizational risk.

Working closely with the customer's IT leadership, SilverSky validated the findings, contained the activity, and helped establish stronger security governance to reduce future risk.

The Challenge

Organizations often generate thousands of routine security events every day. Without advanced analytics and continuous monitoring, unauthorized behavior can remain hidden because individual events appear low risk when viewed independently.

During onboarding, SilverSky detected suspicious activity associated with an administrator workstation. Investigation revealed unauthorized VPN and proxy services that bypassed established security controls and created unnecessary exposure across the organization's environment.

The SilverSky Response

SilverSky Lightning MxDR used behavioral analytics, machine learning, and cross-platform correlation to identify patterns that traditional monitoring had not recognized.

After confirming that the activity was unauthorized, SilverSky immediately notified the customer's IT leadership and coordinated containment efforts. The affected workstation was isolated while the organization investigated the employee's activity and removed the unauthorized services.

Following remediation, SilverSky worked with the customer to review existing security controls, identify governance improvements, and develop a prioritized roadmap for strengthening operational security.

The Outcome

Insider Activity Identified Early

SilverSky detected unauthorized behavior before it could develop into a larger security incident.

Reduced Organizational Risk

Unauthorized services were removed, reducing opportunities for misuse and unauthorized access.

Stronger Governance

The customer improved security policies, technical controls, and operational oversight.

Improved Security Maturity

The engagement provided a roadmap for strengthening security operations beyond the initial onboarding process.

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.

Security value should begin on day one. During onboarding, SilverSky identified unauthorized insider activity, demonstrating how continuous visibility and expert investigation can uncover meaningful risks before they become larger security incidents.

Why It Mattered

Not every security threat originates from external attackers.

Unauthorized privileged activity, policy violations, and insider risk can introduce significant exposure even when there is no malicious intent.

By combining advanced analytics, expert investigation, and continuous monitoring, SilverSky helped the customer identify hidden organizational risk and strengthen security governance before it could impact the business.

Talk to a Security Expert

Discover how SilverSky helps organizations identify insider threats, improve security visibility from day one, and reduce operational risk through continuous monitoring and expert investigation.

www.SilverSky.com | Learn@SilverSky.com