Financial Services Organization Strengthens Security Through Threat-Led Defense

How SilverSky helped a nationwide mortgage lender align security operations to real-world attacker behavior, identify coverage gaps, and continuously improve cyber resilience.

Overview

A nationwide mortgage lender partnered with SilverSky to better understand how modern attackers target financial institutions and whether its existing security controls were aligned to those threats.

Using SilverSky's Threat-Led Defense methodology, the organization mapped industry-specific attacker tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK® framework and compared those threats against its existing security controls.

The result was a practical roadmap that helped the organization close detection gaps, prioritize security investments, and continuously improve its security posture through ongoing assessments and quarterly reviews.

Operational Challenges

Limited Threat Visibility

Security teams lacked context around sophisticated attack activity.

Reactive Security Operations

Earlier threat detection was needed to reduce organizational risk.

Detection Gaps

Existing controls required validation against real-world attack techniques.

Evolving Threat Landscape

Modern attackers demanded continuous detection improvements.

Lean Security Team

Limited resources made proactive threat hunting difficult.

Operational Resilience

Security needed to improve without disrupting financial operations.

The Challenge

Financial institutions face constant pressure from ransomware groups, credential theft campaigns, and financially motivated attackers. Although the customer had invested in multiple security technologies, it needed greater confidence that those tools were protecting against the techniques most commonly used within its industry.

The organization wanted to understand where detection gaps existed, prioritize improvements based on real-world risk, and build a security program that could adapt as attacker behavior evolved.

The SilverSky Response

SilverSky analyzed the organization's threat landscape using industry-specific intelligence and mapped relevant attacker behaviors to the MITRE ATT&CK framework.

The customer's existing security technologies, telemetry, and detection capabilities were then evaluated against those attack techniques to identify areas of strong coverage and opportunities for improvement.

SilverSky delivered prioritized recommendations that included expanding telemetry, improving log collection, refining detection logic, and addressing technology gaps. Quarterly reviews and validation exercises ensured the security program continued evolving alongside the changing threat landscape.

The Outcome

Improved Threat Visibility

The customer gained a clearer understanding of how attackers target organizations within the financial services industry.

Prioritized Security Investments

Threat intelligence helped focus resources on the security improvements with the greatest operational impact.

Stronger Detection Coverage

Security controls were aligned more closely with real-world attacker behavior and validated against evolving threats.

Continuous Security Improvement

Quarterly reviews and ongoing testing ensured the organization's security program adapted as new techniques emerged.

"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.

Modern financial organizations need more than reactive monitoring. By applying threat-led detection strategies and continuous security operations, SilverSky helped strengthen visibility, improve detection capabilities, and reduce operational risk.

Why It Mattered

Cybersecurity programs are most effective when they are aligned to the threats organizations are most likely to face.

By combining threat intelligence, MITRE ATT&CK mapping, and continuous validation, SilverSky helped the customer move beyond reactive security and build a program informed by real-world attacker behavior.

Rather than making technology decisions in isolation, the organization gained a repeatable process for evaluating coverage, reducing risk, and improving resilience over time.

Talk to a Security Expert

Learn how SilverSky helps financial organizations strengthen threat detection, improve operational resilience, and protect customer trust through intelligence-driven security operations and continuous monitoring.

www.SilverSky.com | Learn@SilverSky.com