Legal Firm Prevents Wire Fraud Through Early Phishing Detection

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 law firm partnered with SilverSky Lightning MxDR to strengthen visibility across its security environment. During routine monitoring, SilverSky Security Operations Center (SOC) analysts detected unusual email traffic and suspicious DNS activity associated with a phishing campaign targeting real estate transactions.

By rapidly investigating the activity, validating compromised communications, and working alongside the firm's IT team, SilverSky helped stop a wire fraud attempt before financial transactions were redirected, protecting both the firm and its clients.

Operational Challenges

Phishing Threats

Sophisticated email attacks targeted employees and client communications.

Wire Fraud Risk

Fraudulent payment requests created significant financial risk.

Email Security Visibility

Greater insight into suspicious email activity was needed.

Early Threat Detection

Rapid identification helped stop attacks before funds were compromised.

Lean Security Team

Limited internal resources made continuous investigation difficult.

Protecting Client Trust

Preventing fraud was critical to maintaining client confidence and business reputation.

The Challenge

Legal organizations frequently exchange sensitive financial information, making them attractive targets for phishing campaigns and business email compromise (BEC).

SilverSky detected suspicious email behavior involving display-name spoofing, unusual DNS activity, and unauthorized communications associated with real estate closing transactions. Individually, these events appeared routine, but together they indicated a coordinated phishing attack targeting financial transfers.

The SilverSky Response

SilverSky Lightning MxDR correlated activity across multiple telemetry sources and escalated the investigation to the SOC.

Working directly with the customer's IT leadership, analysts identified malicious emails, confirmed the attempted attack, and coordinated immediate removal before fraudulent wire transfer instructions could be acted upon.

Following the incident, SilverSky helped the organization strengthen email security by implementing multi-factor authentication (MFA), improving email protections, introducing phishing awareness training, and recommending stronger password hygiene and monitoring practices.

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.

Business email compromise remains one of the most effective attack methods targeting professional services. Early detection and expert investigation helped identify suspicious activity before fraudulent wire transfers could impact the organization.

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.

Why It Mattered

Business email compromise remains one of the most effective attack methods against professional services organizations.

By combining continuous monitoring, expert investigation, and operational guidance, SilverSky helped the customer prevent financial fraud while strengthening long-term email security.

Talk to a Security Expert

Learn how SilverSky helps organizations detect phishing attacks earlier, reduce wire fraud risk, and protect sensitive communications through continuous threat monitoring and rapid response.