SILVERSKY
Elevate your Cybersecurity

Case Study

Cyber Insurance Help

CASE STUDY

SilverSky Supported Cyber Insurance Application

Introduction: The Issue

A US manufacturing organization was seeking the required capabilities to meet the standards set forth by cybersecurity insurance policies from the insurance brokers.

Incident Identification and Classification

The company sought out SilverSky and our cybersecurity services to assist with meeting the required capabilities identified in their cyberinsurance policy by their insurance company. The company had implemented, but not operationalized, policies and technologies to the required standard. They also were missing key elements such as Endpoint Detection and Response (EDR), vulnerability management processes, security training and awareness, and Monitoring in the form of Managed Detection and Response (MDR). SilverSky was able to provide all of these services through our Lightning platform – Managed extended Detection & Response (MeDR), Managed Endpoint Detection & Response (MEDR), Insight Vulnerability Scanning and Attach Surface Management and our Aware – security training and phishing testing services.

Customer Details and Description

During the onboarding, SilverSky reviewed and improved multiple security policy elements, as required by the insurance carrier. Senior network engineers reviewed and reconfigured the firewalls to stop vulnerable services and ports like RDP. They implemented geographic blocks for domestic traffic and created zero-trust capabilities across the organizations' architectures.

SilverSky Lightning MEDR was deployed on the endpoints to enable advanced analytical capabilities. This was supported by the proactive blocking of applications and capabilities that hackers could use to gain a foothold within the organization. Profile groups were created to support key aspects of the business, such as the IT team, which still required these functions. Privileges were withdrawn from user accounts in Active Directory to prevent the unapproved installation of non-authorized services, programs, or applications. In addition, all privileged accounts and local accounts with access to critical infrastructure were enhanced with Multi-Factor Authentication (MFA).

MFA was also implemented on exchange email, as were key security services like URL rewrite, impersonation detections, and macro preventions.

A continuous vulnerability management agent was deployed into the network and to all endpoints to enable early detection.

Finally, the organization instituted a security training and phishing testing program to improve its awareness of hackers' techniques, tactics, and procedures.

Once all elements were implemented, feeds for each technology were forwarded to SilverSky's Lightning MxDR platform to enable 24/7 monitoring, response, and, if necessary, remediation.

linkedin.com/company/silversky
www.silversky.com

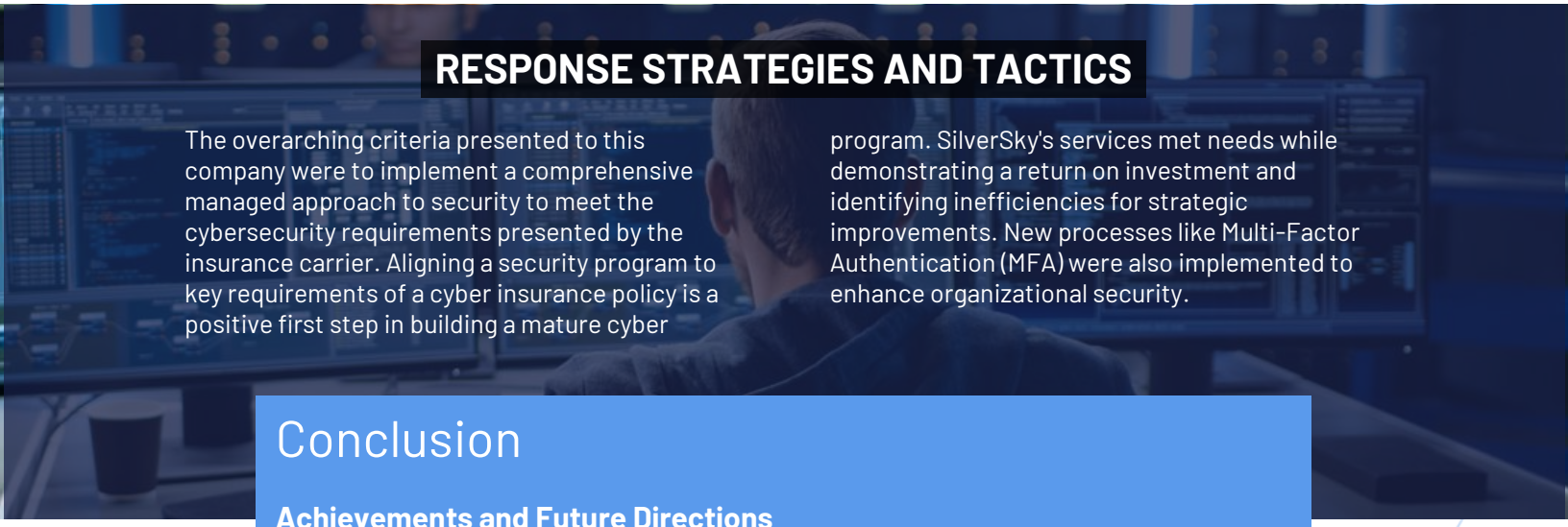
1-800-234-2175
learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560

CASE STUDY

Operational Response Framework

SilverSky's pre-sales team consulted the company on the meaning behind all requirements within the insurance policy presented to them by the insurance carrier. This enabled the organization to understand the services offered to them by SilverSky to ensure they understood the return on investment (ROI), as the security budget previously held by the organization underwhelmingly did not meet the needed amount to employ the services needed to meet the requirements of the insurance policy. Understandably, a manufacturing organization had key components such as next-generation firewalls and Microsoft services, but neither were configured, maintained, or monitored to the needed insurance standard. As stated, other services required per the insurance application were not implemented. This is a common finding for many organizations, as the traditional ideology is that technology should independently suffice the need to reduce threats. But based on the simplicity of how vulnerable an organization can be, simple tactics by hackers require consolidated approaches and consistency.



RESPONSE STRATEGIES AND TACTICS

The overarching criteria presented to this company were to implement a comprehensive managed approach to security to meet the cybersecurity requirements presented by the insurance carrier. Aligning a security program to key requirements of a cyber insurance policy is a positive first step in building a mature cyber program. SilverSky's services met needs while demonstrating a return on investment and identifying inefficiencies for strategic improvements. New processes like Multi-Factor Authentication (MFA) were also implemented to enhance organizational security.

Conclusion

Achievements and Future Directions

Upon the review with the insurance carrier, the organization was presented with an acceptance and reduction in rates due to the complete approach taken by SilverSky.

linkedin.com/company/silversky
www.silversky.com

1-800-234-2175
learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560