SILVERSKY
Elevate your Cybersecurity

Case Study

Insider Threats

CASE STUDY

SilverSky Discovered Insider Threats

Introduction: The Incident

A property management company experienced a surge in unusual communications from external IP addresses, targeting ports irrelevant to its operations, raising concerns about their nature and potential malicious intent.

Incident Identification and Classification

A new customer subscribed to SilverSky's Lighting Managed extended Detection & Response (MxDR). During normal operations, events were generated over three main areas within the business (Firewall, DNS, and Active Directory). The local technology classified all events generated as information, low, and some medium in severity. It wasn't until the analytics within the Lightning MxDR platform correlated them together based on common indicators that they were classified correctly as a high severity classification and the SilverSky Security Operations Center (SOC) took action.

It was determined that this was a high-severity event. The event generated several thousand alerts creating 4 incidents and 1 case.

Incident Details and Description

Using the Machine Learning (ML) and Artificial Intelligence (AI) engines within the Lightning MxDR platform, the log data from the customer's firewall, DNS, and Active Directory logs were analyzed to detect and correlate evidence suggesting an insider threat.

The SilverSky SOC analyst working with the onboarding team communicated to the customer that a system administrator had installed an unauthorized VPN and proxy server on their laptop.

Upon agreement between the SilverSky SOC analyst and the IT manager for the customer that these services were not permitted, the SilverSky SOC was able to lock down the device until the laptop could be located. Locating the laptop and the employee in question, it was determined that the employee was using the laptop to conduct a secondary business. The same employee had also configured local security running on his device to allow the activity without creating alerts to the IT team; in doing so, the employee created a means by which, if exploited, the whole business could have been subjected to a larger attack.

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

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

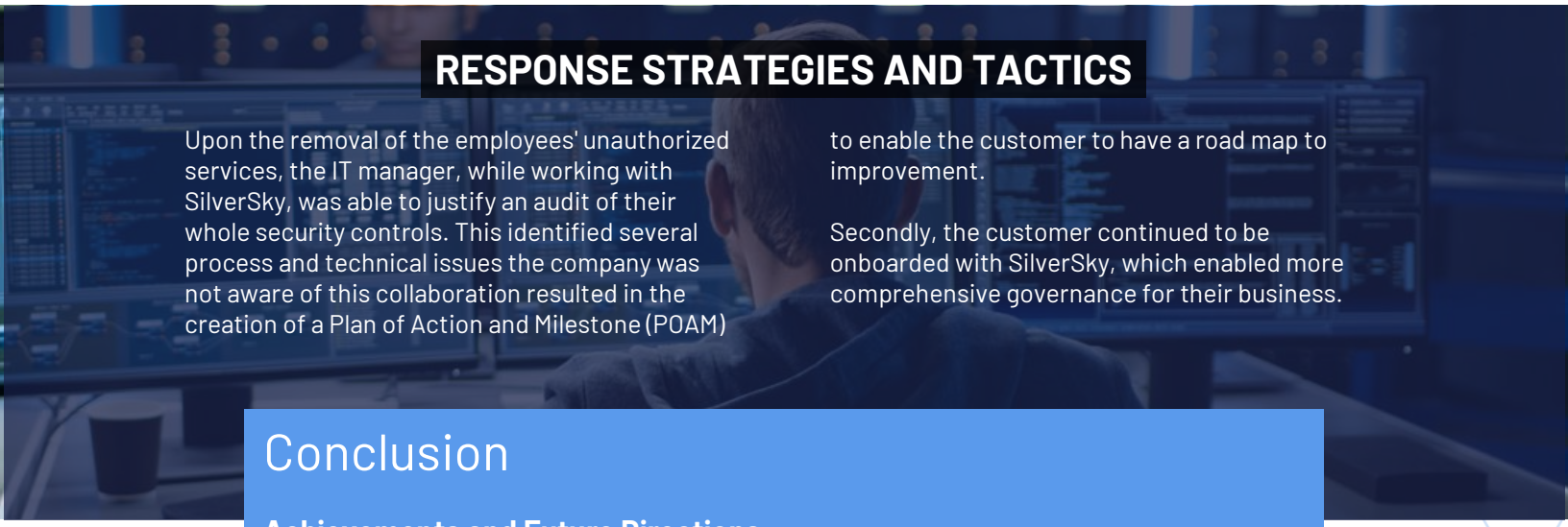
3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560

CASE STUDY

Operational Response Framework

The events detected by the Lightning MxDR platform were identified within 24 hours of starting onboarding and receiving their log data. Therefore, the customer was still classified as being within the onboarding stage. However, due to the volume of the events seen, the SilverSky onboarding lead escalated one of the data review calls with the primary contact to ensure what was being seen was aligned with the analyst's review.

- Initial communications were sent out within 15 minutes of the case being generated, and the analysis confirmed the potential insider threat.
- Email communications enabled a meeting to be scheduled the next day due to the severity.
- The event was mitigated a few hours after the meeting.



RESPONSE STRATEGIES AND TACTICS

Upon the removal of the employees' unauthorized services, the IT manager, while working with SilverSky, was able to justify an audit of their whole security controls. This identified several process and technical issues the company was not aware of this collaboration resulted in the creation of a Plan of Action and Milestone (POAM) to enable the customer to have a road map to improvement.

Secondly, the customer continued to be onboarded with SilverSky, which enabled more comprehensive governance for their business.

Conclusion

Achievements and Future Directions

During the onboarding of the SilverSky Lightning MxDR services, unusual events were detected by the analytics used in the Lightning MxDR platform. These events escalated communications with the customer to determine the legitimacy of these events, which, although not malicious, were unauthorized.

These findings and actions allowed for a more comprehensive approach, expanding the opportunity scope due to the customer's need to review security controls. Additionally, the onboarding timing improved due to the commitment of both organizations.

The outcome for the customer was better technical policies preventing unauthorized activities, updated written policies and education for the organization, and ultimately 24/7 monitoring and response from SilverSky for all ongoing inquiries.

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

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

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560