MICROLAND
Connect with the best

CASE STUDY

Enhancing security operations with Microland's SOC services for a leading US-based branded payment solutions provider

Overview

A leading US-based branded payment solutions provider sought to enhance its security operations to manage the increasing complexity and volume of cyber threats. Recognizing the need for a robust and proactive approach, the company partnered with Microland to establish a dedicated 24x7 Security Operations Center (SOC). The goal was to ensure proactive threat management, rapid incident response, and overall improvement in the organization's security posture.

Scope and Business Challenge

Recognizing the need for a robust and proactive approach, the company partnered with Microland to establish a dedicated 24x7 Security Operations Center (SOC). The goal was to:

- Establish a 24x7 SOC to monitor and manage security incidents.
- Implement proactive threat hunting and SOAR automation.
- Develop comprehensive incident investigation and management processes.
- Create use cases for threat detection, policy violations, and anomaly detection.
- Integrate external threat intelligence feeds for enhanced threat management.
- Establish robust reporting and governance mechanisms.

The company faced a growing number of sophisticated cyber threats, necessitating a proactive and comprehensive security strategy. There was a need for streamlined incident management to ensure minimal disruption to business operations, but limited in-house expertise and resources hindered the establishment of a fully functional SOC. Additionally, compliance with industry regulations and effective risk management were critical, and the existing security operations were inefficient, leading to delayed response times and increased vulnerability.

Microland Solution

Microland established a dedicated **24x7 Security Operations Center (SOC)** staffed with experienced security professionals to provide continuous monitoring, threat detection, and incident response. The SOC was equipped with advanced threat hunting techniques to proactively identify potential threats before they could impact the organization. Additionally, Microland deployed SOAR (Security Orchestration, Automation, and Response) tools to automate repetitive tasks and enhance response times, ensuring a rapid and efficient response to security incidents.

To manage security incidents effectively, we developed robust processes for **alert monitoring and ongoing incident management.** These processes included the classification and prioritization of security incidents to ensure that critical issues were addressed promptly. The SOC also provided remediation recommendations and implemented corrective actions to prevent the recurrence of incidents, ensuring continuous improvement in security measures.

SOC engineering efforts focused on building use cases for threat detection, policy violation, and anomaly detection using three models: asset-based, business-based, and attack-based. This comprehensive approach ensured that all potential threat vectors were covered, enhancing the organization's ability to detect and respond to a wide range of security threats.

Microland also integrated external **threat intelligence** feeds into the SOC's operations to stay ahead of emerging threats. By continuously reviewing and analyzing these feeds, the SOC could proactively mitigate risks and operationalize threat detection and response based on the latest intelligence. This strategic approach to threat management ensured that the organization was always prepared to handle new and evolving cyber threats.

Furthermore, we developed **detailed SOC reporting** specifications to provide clear visibility into security operations. Performance scorecards and dashboard views were created to monitor SOC performance and effectiveness. A robust program governance framework was established to ensure seamless integration of security measures and continuous improvement, aligning with the company's strategic objectives.

Business Benefits

- **Increased Operational Efficiency:** The implementation of SOAR automation significantly improved operational efficiency by reducing manual intervention and streamlining incident response processes.

- **Improved Security Posture:** Proactive threat hunting and continuous monitoring enhanced the client's ability to detect and respond to threats quickly, thereby improving its overall security posture.

- **Better Compliance and Risk Management:** Continuous monitoring and adherence to regulatory requirements helped them improve its compliance and risk management practices, reducing the likelihood of non-compliance penalties.

- **Strategic Threat Management:** The integration of external threat intelligence feeds and proactive risk mitigation strategies enabled our client to stay ahead of emerging threats, ensuring a robust defense against potential attacks.