MICROLAND
Connect with the best

CASE STUDY

Microland employs a Cyber Resiliency First approach to secure operations globally for a middle-east based retail conglomerate

Overview

A Middle East-based retail conglomerate, with operations spanning over 70 stores globally, faced the increasing complexity of securing its vast IT infrastructure and protecting sensitive customer data. As the digital landscape evolved, the threat landscape expanded, necessitating a proactive and comprehensive approach to cybersecurity. The company sought a strategic partner to bolster its security posture, ensuring business continuity and customer trust. Partnering with Microland, the conglomerate adopted a "Cyber Resiliency First" approach to ensure robust security across its operations.

Scope and Business Challenge

The primary focus was on securing a large user base of over 15,000 employees and more than 2,200 devices. This comprehensive cybersecurity program aimed to implement 24x7 Security Operations Center (SOC) services to ensure continuous monitoring and incident response. Additionally, the initiative sought to establish robust Governance, Risk, and Compliance (GRC) frameworks to meet various industry-specific and regional regulations. Enhancing endpoint, email, and data security was a crucial component, ensuring that all aspects of the IT environment were protected. The adoption of an Open XDR architecture was also within the scope, aimed at unifying and simplifying the security operations to improve threat detection and response capabilities.

The client's primary concerns included:

- **Protection of sensitive customer data:** Safeguarding personal information and financial transactions was paramount.
- **Securing a sprawling IT infrastructure:** Managing endpoints, networks, and applications across multiple locations posed significant challenges.
- **Compliance with industry regulations:** Adhering to stringent data privacy and security standards was mandatory.
- **Minimizing business disruptions:** Ensuring uninterrupted operations and mitigating the impact of cyber incidents was crucial.
- **Building a robust security culture:** Developing security awareness among employees was essential.

Microland Solution

24x7 SOC Services

Microland established a 24x7 Security Operations Center (SOC) to monitor the entire IT ecosystem, including endpoints, networks, and applications. This continuous vigilance enabled real-time threat detection and swift incident response. The SOC utilized advanced alert triaging to quickly identify and prioritize threats. Microland also focused on continuous service improvements, fine-tuning processes, and standardizing policies to maintain a robust and adaptive security posture.

Securing Endpoints & Employees

To protect over 15,000 devices and users, Microland deployed advanced endpoint security solutions and comprehensive email and data security measures. This initiative included continuous policy improvements, configuration adjustments, and access control enhancements to adapt to new threats. Additionally, periodic user awareness training sessions were conducted to educate employees on preventing social engineering attacks and maintaining security vigilance.

Transforming to Open XDR

The conglomerate transitioned to an Open Extended Detection and Response (XDR) architecture, unifying the entire security stack to simplify operations and increase resilience. This integration improved data and alert correlation, leading to faster and more accurate threat detection and response. By adopting next-generation tools within the Open XDR framework, the organization enhanced its ability to manage and mitigate cybersecurity risks effectively.

Risk Management & Compliance

Microland conducted continuous risk assessments, incorporating probability and impact analysis to identify and address critical risks. Detailed response plans were developed to mitigate high-impact risks, ensuring business continuity. Regular compliance audits were performed to meet industry-specific and regional regulations, maintaining high governance standards and reinforcing the company's commitment to legal and regulatory adherence.

Business Benefits

Microland's cybersecurity solutions delivered significant benefits:

- **Increased compliance:** Adherence to industry regulations and internal policies.
- **Improved security posture:** Strengthened defenses against cyber threats.
- **Enhanced risk management:** Proactive identification and mitigation of risks.
- **Faster incident response:** Reduced mean time to detect (MTTD) and mean time to respond (MTTR).
- **Business continuity:** Minimized disruptions to operations.
- **Cost optimization:** Efficient use of security resources.
- **Data privacy:** Protection of sensitive customer information.