CASE STUDY

Microland Delivers Enhanced Security Posture with MDRaaS for the World's Largest and Oldest University Press

Overview

The client is renowned for their commitment to excellence in research, scholarship, and education through global publishing. To safeguard their extensive digital estate spanning on-premises infrastructure and cloud environments, the client sought a Managed Security Services (MSS) provider to enhance their cybersecurity posture. Microland stepped in to deliver comprehensive Managed Detection and Response (MDR) services, including threat intelligence, vulnerability management, user entity behavior analytics, and automation.

Scope and Business Challenge

The client has increasingly relied on digital technology to gather, store, and distribute information, making a reliable cybersecurity solution a critical concern. Cybersecurity breaches can have severe consequences for publishers, such as stealing or compromising sensitive information, including concepts, content, and confidential data. Such a breach can damage the reputation and credibility of our client, leading to significant financial losses due to hefty fines and legal action. Protecting sensitive information and maintaining the trust of readers is essential for the client. Cybersecurity plays a vital role in ensuring **information integrity and privacy**. In addition, our client is responsible for protecting the privacy and security of their subscribers & readers.

To address these challenges, Microland aimed to provide a robust **MDR-as-a-Service (MDRaaS)** offering, ensuring quick detection and response to cyber threats, improved incident response capabilities, enhanced visibility and proactive defense measures, simplified and cost-effective security management, and comprehensive coverage and automation to support the client's critical systems.

Microland Solution

We delivered the MDRaaS on our Cyber Resiliency First – 'SMART' framework which is based on a flexible architecture that aligns with industry standards, with assured service quality and visualization of security posture. It assures transformation to next-gen SOC capabilities with accelerated detection and response, along with reduced costs of operations.

❑ **Standardize & Simplify:**

- A flexible and simplified architecture aligned with NIST standards, enabling continuous refinement
- A lightweight yet effective management layer to drive intended benefits without complexity

❑ **Measure & Mitigate:**

- Metrics and KPIs to measure service quality and take corrective actions
- Comprehensive visualization of the security posture to manage defenses effectively

- Advanced threat-hunting capabilities to detect undetected cyber threats

❑ **Automate & Accelerate:**

- Near real-time visibility into anomalies

- Core automation for efficiency, better insights, and quick response

- Fast implementation and onboarding of data sources with seamless risk-optimized transition

❑ **Refine & Reduce:**

- Identifying opportunities to streamline operations and reduce costs

- Optimized technology solutions and integrated service consumption for cost-efficiency

- Common service management framework across delivery centers, governance, and ITSM

❑ **Transform & Transparency:**

- Framework to baseline current operations and mitigate risks with next-gen technology

- Leveraging AI for data protection and compliance, bringing best practices and industry knowledge

- Simplified billing methodology with service consumption reports

Business Benefits

- Microland enabled real-time threat detection, SOAR-based automated incident response, and proactive threat-hunting, significantly enhancing incident detection and response.

- Central control of distributed security resources

- Advanced analytics and risk quantification provided better security visibility through centralized dashboards and persona-based reports.

- Transformation of cyber security capabilities to a high level of maturity

- Threat-hunting capabilities help identify and neutralize threats before they cause substantial damage to the client.