MICROLAND
Connect with the best

CASE STUDY

Microland enhanced cyber resiliency with an advanced Managed Detection and Response (MDR) solution for one for the world's largest petrochemicals producer

Overview

One of the world's largest petrochemicals producers partnered with Microland to enhance their cyber resiliency. The client sought to improve their cybersecurity posture and ensure comprehensive protection across their extensive infrastructure. This case study explores how Microland's Advanced Managed Detection and Response (MDR) solution and other proactive security measures transformed the client's security landscape.

Scope and Business Challenge

The client required a robust security solution to manage over 1,000 critical assets, including both on-premises and cloud environments. The primary goals were to enhance threat detection, improve incident response times, and ensure continuous compliance with industry regulations.

- **Complex Infrastructure:** The client's extensive and diverse infrastructure posed significant challenges for effective monitoring and threat management.
- **Threat Landscape:** The petrochemical industry is a prime target for cyberattacks, necessitating advanced measures for threat detection and prevention.
- **Resource Constraints:** Managing cybersecurity in-house was resource-intensive, requiring significant expertise and continuous monitoring.
- **Regulatory Compliance:** Ensuring compliance with stringent internal policies and external regulations required ongoing vulnerability assessments and risk mitigation.

Microland Solution

Microland designed a comprehensive **Managed Detection and Response (MDR)** solution tailored to the client's specific needs. This solution focused on enhancing cybersecurity posture through advanced threat detection, proactive threat management, and robust incident response capabilities.

A core component was the establishment of a **24/7 Security Operations Center (SOC)** to monitor over 1,000 critical assets. Leveraging a state-of-the-art Security Information and Event Management (SIEM) platform integrated with User and Entity Behavior Analytics (UEBA), Microland enabled advanced threat detection by identifying anomalous user and entity behavior patterns. To streamline incident response workflows and automate repetitive tasks, Security Automation and Orchestration (SOAR) capabilities were integrated.

Proactive threat management was ensured through regular vulnerability assessments, risk prioritization, and mitigation strategies. Additionally, Microland conducted proactive threat hunting to uncover hidden threats and implemented measures to safeguard the client's brand reputation through online threat and phishing monitoring. Rigorous controls were established for privileged access management to protect critical assets.

The MDR solution included advanced threat identification and prioritization using analytics and threat intelligence. A dedicated team of security experts was on hand for effective incident containment and response. Support was also provided to the incident forensics team during major attacks.

Proactive threat prevention was achieved through real-time threat intelligence gathering from the Dark Web and Indicator of Compromise (IOC) feeds. Vulnerability assessments were complemented by risk planning and mitigation strategies aligned with internal policies and external regulations.

To strengthen cloud security posture, Microland implemented robust access controls, permissions management, and configuration monitoring for cloud workloads. Automated remediation processes were established to address cloud misconfigurations promptly, and a centralized asset dashboard provided real-time insights into overall cloud security. Finally, the solution included a comprehensive library of automated actions to expedite incident response, standardized playbooks to streamline incident handling, and integration with the IT Service Management (ITSM) system for efficient ticket creation and automated remediation actions.

Business Benefits

- **Increased Threat Prevention:** Continuous vulnerability assessments and real-time threat intelligence enhanced the client's ability to proactively prevent potential threats.

- **Faster Detection and Response:** The advanced MDR solution improved Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), reducing the impact of security incidents.

- **Enhanced Cloud Security Posture:** The centralized asset dashboard provided comprehensive visibility and control over the cloud environment, ensuring prompt identification and remediation of security issues.