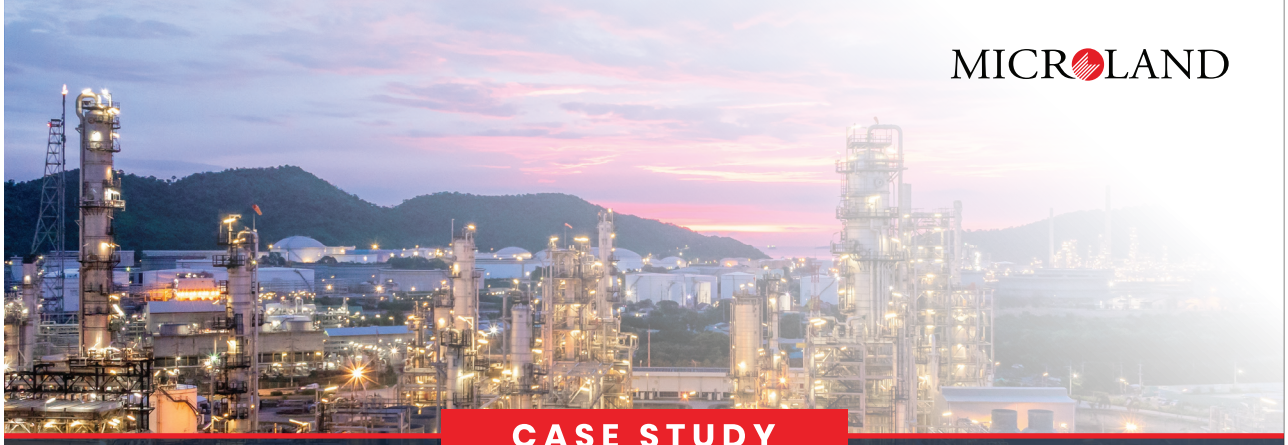

MICROLAND

CASE STUDY

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

Overview

One of the world's largest petrochemicals producers partnered with Microland to strengthen their cyber resiliency. The organization aimed to enhance its cybersecurity posture and ensure comprehensive protection across a vast and complex infrastructure. By deploying Microland's Advanced Managed Detection and Response (MDR) solution, supported by AI/ML-driven threat analytics and complemented by GenAI-assisted automation, the company successfully transformed its security landscape.

Client Challenges

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, including emerging **AI-driven threats and adversarial techniques**, necessitating advanced measures for threat detection and prevention.
- **Resource Constraints:** Managing cybersecurity in-house was resource-intensive, requiring significant expertise and continuous monitoring, and the ability to handle **high-volume AI-enabled attack attempts**.
- **Regulatory Compliance:** Ensuring compliance with stringent internal policies and external regulations required ongoing vulnerability assessments and risk mitigation.

Microland Solution

Here is the approach adopted by Microland to strengthen the customer's cybersecurity posture and ensure robust protection.

AI-Enabled MDR Solution

Microland designed a comprehensive AI-enabled MDR solution tailored to the client's specific needs. This solution focused on enhancing cybersecurity posture through AI-powered threat detection, GenAI-enabled triage, proactive threat management, and robust incident response capabilities.

24/7 Security Operations Center (SOC)

A core component was the establishment of a 24/7 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. AI/ML models continuously learned from activity baselines, while GenAI supported analysts by summarizing alerts and recommending next steps. To streamline incident response workflows and automate repetitive tasks, Security Automation and Orchestration (SOAR) capabilities were integrated. **These were enhanced with GenAI-driven playbooks**, which dynamically adapted response actions and generated contextual recommendations to accelerate triage.

Proactive Threat Management

Proactive threat management was ensured through regular vulnerability assessments, risk prioritization, and mitigation strategies. Additionally, Microland conducted proactive threat hunting to uncover hidden threats, using **AI-assisted hunting models to detect anomalies beyond signature-based rules**, 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 with **AI-based anomaly detection on privileged sessions** to flag insider risks.

The MDR solution included advanced threat identification and prioritization using analytics and threat intelligence. AI/ML-powered correlation engines enriched threat intelligence feeds, while GenAI auto-generated analyst-friendly intelligence briefs and plain-language executive summaries. 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, with **GenAI used to quickly reconstruct timelines and summarize forensic findings**.

Proactive Threat Prevention

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. AI/ML models continuously correlated dark web data with internal telemetry, while GenAI created risk advisories consumable by both technical and non-technical stakeholders.

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.

AI/ML-based misconfiguration detection ensured faster discovery, while GenAI-enabled compliance summaries simplified audit readiness.

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. AI/ML enrichment reduced false positives, and GenAI-driven advisories accelerated decision-making at both analyst and executive levels.
- **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. GenAI-assisted SOAR automation and AI anomaly detection enabled more accurate triage and quicker containment.
- **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. AI/ML-based detection of misconfigurations, coupled with GenAI compliance reports, strengthened audit readiness and reduced manual workload.
- **Operational Efficiency:** GenAI copilots reduced analyst fatigue by automating repetitive tasks such as incident summaries, ticket enrichment, and reporting, enabling the SOC to focus on high-value investigations.
- **Future-Ready Resilience:** By integrating AI/ML and GenAI throughout detection, response, and compliance, Microland positioned the client to defend against evolving, AI-driven cyber threats with adaptive, intelligent security operations.