

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 solution combined SIEM and SOAR with advanced AI/ML-driven threat analytics and GenAI-assisted workflows, ensuring proactive threat management, rapid incident response, and overall improvement in the organization's security posture.

Client Challenges

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

- Establish a 24x7 SOC for continuous monitoring and incident response, leveraging AI/ML-powered anomaly detection to identify subtle deviations and reduce false positives.
- Implement proactive threat hunting and SOAR automation.
- Develop comprehensive incident investigation and management processes augmented with GenAI-driven playbooks that recommend next-best actions and accelerate triage.
- Create use cases for threat detection, policy violations, and anomaly detection enhanced by adaptive AI models that evolve with new attack techniques and adversarial behaviours.
- Integrate external threat intelligence feeds for enhanced threat management with AI/ML correlation engines enriching and prioritizing threat data for faster analyst decision-making.
- 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 supported by GenAI-generated executive summaries and AI-driven predictive analytics to forecast potential escalation 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.

©2025 Microland Limited

The company was particularly concerned about the rise of AI-driven attacks and adversarial techniques, which required specialized skills and continuous training. With limited resources available, combating these evolving AI-powered threats became even more challenging, adding urgency to the need for an advanced SOC.

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 combining traditional methods with **AI/ML-based anomaly detection** to proactively identify potential threats before they could impact the organization. Additionally, Microland deployed SOAR tools to automate repetitive tasks and enhance response times, ensuring a rapid and efficient response, enriched with GenAI-driven playbooks that recommended next-best actions, reducing analyst workload and accelerating decision-making.

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. AI-powered prioritization models were introduced to forecast escalation likelihood, while GenAI-generated incident briefs provided concise, plain-language updates for business stakeholders 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 was further strengthened by **adaptive AI models that continuously learn from evolving attack patterns** 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. AI/ML correlation engines were used to enrich these feeds, while GenAI summarized insights into analyst-ready advisories, making threat intelligence both actionable and easy to consume. 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. **AI-powered dashboards enabled predictive analytics on SOC efficiency, and GenAI was used to generate executive-level summaries automatically, reducing manual reporting effort.** 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 Outcomes

- **Increased Operational Efficiency:** The implementation of SOAR automation significantly

©2025 Microland Limited

improved operational efficiency by reducing manual intervention and streamlining incident response processes. AI/ML-based noise reduction further lowered false positives, allowing analysts to focus on high-priority alerts.

- **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. **Adaptive AI models strengthened this by learning from evolving attack patterns, making detection more precise.**
- **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. **GenAI-assisted threat summaries made intelligence easier to operationalize across SOC teams.**

Microland is a leading AI-first, platform-led, technology infrastructure services company. We have enabled enterprises to build intelligent, resilient, and future-ready operations and are a trusted partner to global enterprises. We bring over 35 years of expertise in digital networks, cloud, data centers, workplaces, and cybersecurity, and combine it with our commitment to customer centricity, delivery excellence, and continuous innovation. Our operations, currently in more than 100 countries, are supported by a strong global delivery model and our AIOps platform, intelligeni, powered by Agentic AI, which is shaping the future of autonomous technology operations across enterprises.

For more information visit **www.microland.com** or email us at info@microland.com

©2025 Microland Limited