



## Overview

In the digital age, public service organizations face increasing threats from cybercriminals. A leading UK-based public services provider, responsible for critical infrastructure and sensitive citizen data, recognized the need to enhance its cybersecurity posture. To address these challenges, the organization partnered with Microland to implement an end-to-end managed Security Operations Center (SOC) service. This collaboration aimed to improve the visibility of cyber threats, monitor and manage risks across critical systems, and ensure the security of endpoints and servers distributed across Europe, the Middle East, and ASPAC.

## Scope and Business Challenge

The primary objectives of the engagement included:

- **Designing, Deploying, and Monitoring Critical Systems:** Establishing robust security measures to safeguard critical systems while enhancing visibility into cyber threats.
- **Developing Use Cases for Risk Management:** Crafting comprehensive use cases for the monitoring, detection, and management of risks associated with critical systems.
- **Managing a Diverse IT Environment:** Addressing the complexities associated with a distributed infrastructure encompassing thousands of endpoints and servers across multiple regions.

The organization faced several challenges:

- **Inadequate Threat Visibility:** Existing security measures did not provide sufficient visibility into potential cyber threats, leading to delayed incident detection.
- **Resource Constraints:** Limited in-house expertise and resources hampered the ability to respond effectively to security incidents.
- **Compliance Requirements:** The organization was under increasing pressure to meet compliance and regulatory requirements, necessitating a robust security framework.

## Microland Solution

To address the organization's challenges, Microland implemented a comprehensive suite of managed SOC services:

## 1. Endpoint Security:

- Microland deployed Microsoft Defender Endpoint to provide next-generation protection and attack surface reduction. This included continuous monitoring, real-time protection against malware, centralized management, and vulnerability management.

## 2. 24/7 Monitoring & Incident Response:

- A dedicated team of L1, L2, and L3 analysts provided round-the-clock monitoring and prompt investigation of security alerts and incidents. The tiered approach ensured swift containment actions were coordinated effectively to minimize the impact of security breaches.

## 3. Continuous Improvement & Innovation:

- The transition to Microland's SOC involved thorough planning, due diligence, and knowledge management. Continuous improvement was achieved through regular health checks, configuration backups, sensor health reviews, and tuning based on threat intelligence.

## 4. Threat Hunting & Intelligence:

- Microland implemented continuous threat intelligence updates and proactive threat hunting activities. Threat hunters employed advanced methodologies, including event-based Kusto Query hunting and IOC-based hunting, to investigate security incidents and identify potential threats.

## Business Benefits

The partnership between the UK-based public services provider and Microland yielded significant benefits:

- **Reduced Mean Time to Detect (MTTD) & Mean Time to Respond (MTTR):** Enhanced monitoring capabilities and a tiered incident response approach led to a significant reduction in the time taken to detect and respond to security incidents.
- **Improved & Secure End-User Experience:** With robust endpoint security measures and real-time threat detection, end users experienced fewer disruptions and enhanced security, fostering trust in the organization's digital services.
- **Improved Compliance and Audit Success:** The comprehensive security framework established by Microland ensured adherence to compliance requirements, resulting in improved audit success rates and a stronger overall security posture.

Microland is a pioneering IT Infrastructure services and consulting company headquartered in Bengaluru, India, with a proven track record of delivering tangible business outcomes for 35 years. Today, as enterprises recognize that networks underpin the functionality and efficiency of modern digital systems and support innovation, we provide next-generation technologies such as AI, automated operations, and platform-driven solutions – which drive operational excellence, agility, and productivity for organizations worldwide. Our team of over 4,600 experts delivers services in over 100 countries across Asia, Australia, Europe, the Middle East, and North America, offering cutting-edge solutions in networks, cloud, data centers, cybersecurity, services management, applications, and automation. Recognized by leading industry analysts for our innovative strategies, Microland is committed to strong governance, environmental sustainability, and fostering an inclusive workplace where diverse talent thrives. When businesses work with Microland, they connect with the best talent, technologies, and solutions to create unparalleled value. For more information, visit [www.microland.com](http://www.microland.com)