24x7 SOC Services for Middle East based Roads & Transportation Governing Authority

Microland's customer is an independent government authority overseeing roads & transportation in UAE and is responsible for the planning & execution of transportation projects, legislation and strategic planning on transportation within the state. The mission of the customer is to develop integrated, sustainable and best-in-class public transportation for the residents & tourists.

The customer manages the entire public transportation system including metros, buses, ferries & taxies with ridership exceeding 500 million annually. With such a large customer base engaging the services through mobile applications and the customer venturing into automated metros rail system and other IoT based connected systems, ensuring security was a key concern for the customer.

With the threat landscape evolving, the customer was looking for Security solution which not only monitored the customer's infrastructure for attacks/ incidents but proactively identify and address advanced unknown threats and mitigate the risks associated with them. The security solution needed to address the challenges of people, process & technology and enable robust response to any incidents.

Microland's delivered a security infrastructure involving 24x7 SIEM monitoring, threat lifecycle management with incident response and security orchestration and automation. Microland took a phasewise approach to enhance the security posture for the organization including

- Improving overall Information security visibility of the organization
- Review, update, develop and enhance the security standard operating procedures
- Improve and measure the incident response capability of the organization
- Monitor contain and control the threat landscape to minimize the impacts of security events through early detection
- Engage with a third party to access and enhance the technology landscape in the event of a forensic investigation event

info@microland.com
www.microland.com

A snapshot of Microland's SOC operations for the customer is provided below:

- Microland's SOC processes 430 Million events each day from the internal logs and threat intelligence portals by employing business contextualized use-cases.
- Round the cloud monitoring of 4,000+users (employees) through UEBA & Endpoint security solutions
- Implementing Fortinet SOAR solution for alert automation & improve Mean Time to Detect (MTTD), Mean Time to Response (MTTR) and Mean Time to Recover (MTTR)
- Identified & contained multiple attack patterns of SQL Injection, PHP based attacks etc. through vulnerability scanning & proactive threat hunting.

About Microland

Microland's delivery of digital is all about making technology do more and intrude less. As we help enterprises move to nextGen technologies, we make sure this embrace of brilliance is predictable, reliable and stable. Incorporated in 1989 and headquartered in Bengaluru, India, Microland comprises more than 4,500+ digital specialists across offices and delivery centers in Asia, Australia, Europe, Middle East and North America.

info@microland.com
www.microland.com