MICR🔴LAND®

NAVIGATE THE THREAT LANDSCAPE SEAMLESSLY WITH COMPREHENSIVE SIEM SERVICES

The expanding technology landscape has increased the risk of data breach and cyber attacks. To mitigate such events, businesses today are investing significantly in Security Information and Event Management (SIEM) products and solutions.

However, due to lack of skills and resource shortage, these security products are not used comprehensively and effectively. Use cases and rules are not updated in accordance with the existing threat trend which results in increased false positive events and wastage of time and effort.

HOW WE HELP

Microland offers end-to-end SIEM service for effective monitoring of security threats and events. The comprehensive solution elements of our SIEM services can be seen in Figure 1.
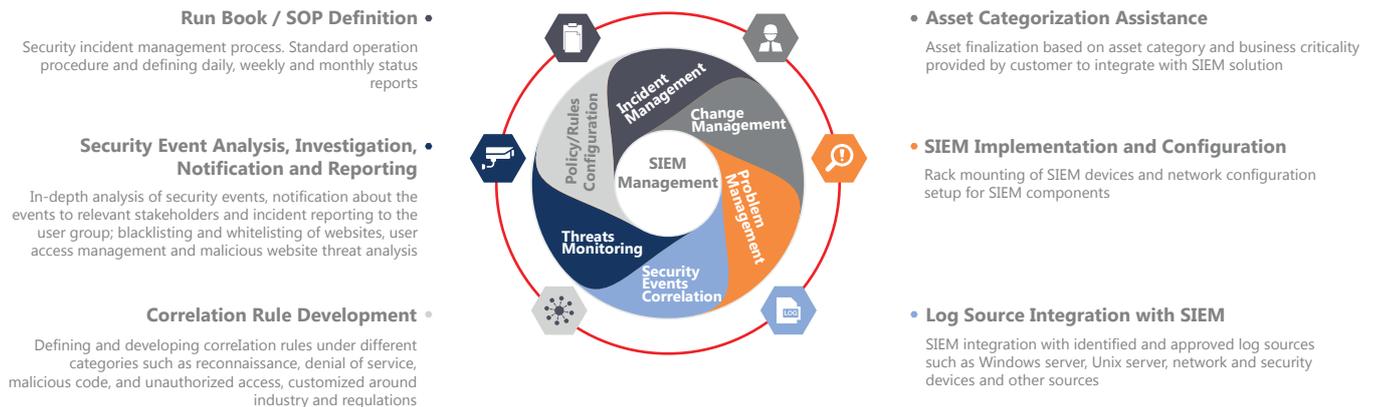
Run Book / SOP Definition •

Security incident management process. Standard operation procedure and defining daily, weekly and monthly status reports

Security Event Analysis, Investigation, Notification and Reporting •

In-depth analysis of security events, notification about the events to relevant stakeholders and incident reporting to the user group; blacklisting and whitelisting of websites, user access management and malicious website threat analysis

Correlation Rule Development •

Defining and developing correlation rules under different categories such as reconnaissance, denial of service, malicious code, and unauthorized access, customized around industry and regulations

• **Asset Categorization Assistance**

Asset finalization based on asset category and business criticality provided by customer to integrate with SIEM solution

• **SIEM Implementation and Configuration**

Rack mounting of SIEM devices and network configuration setup for SIEM components

• **Log Source Integration with SIEM**

SIEM integration with identified and approved log sources such as Windows server, Unix server, network and security devices and other sources

Figure 1: Microland's SIEM Service Components

WHAT YOU CAN EXPECT

Our comprehensive SIEM services help you mitigate threat and cyber attacks while ensuring data security. Key outcomes of our services include:

- Identification and elimination of advanced persistent threats through in-depth security analysis
- Content customization for accurate identification of business security issues
- Enabling live dashboards to provide leadership attention for security and compliance

- Cost optimization and increased operational efficiency
- Reduced noise of events for increased focus on real threats
- Reduced logging level resulting in storage, EPS licensing, and EPS saving

MICR🔴LAND®

WHAT SETS US APART

Some of our differentiators in the SIEM domain include:

Proprietary smartCenter Portal

- Microland's ITIL-based service management portal helps in reducing response and decision-making time to effectively mitigate security threats. Real-time, one-line dashboards improve visibility into operations

24/7 Security Monitoring

- We provide round-the-clock security management governed by industry standards and best practices

Mature Workflows

- Our well-defined processes help you respond quickly and effectively during an incident

Certified Security Experts

- We leverage the capabilities of certified and skilled security experts to deliver unmatched quality of service

For more information, log on to www.microland.com

About Microland

Microland is a leading Hybrid IT Infrastructure Service Provider and a trusted partner to enterprises in their IT-as-a-Service journey. Incorporated in 1989 and headquartered in Bangalore, India, Microland has more than 3,400 professionals across its offices in Europe, Middle East, North America and India. Microland enables global enterprises to become more agile and innovative through a comprehensive portfolio of services that addresses hybrid IT transformation, workspace transformation, service transformation and end-to-end IT infrastructure management.

MICROLAND®