Infosys®
Navigate your next

MICROSOFT AZURE SENTINEL-BASED MANAGED THREAT, DETECTION AND RESPONSE (SOC SERVICES)

Accelerate your digitization and cloud journey, manage cyber security risks and improve your overall security posture

With a strong strategic and technical partnership with Microsoft, Infosys Cyber Security offers a full spectrum of security service for the Azure environment. Our services provide security and maturity assessment, security architecture design, implementation of security controls, monitoring, management, and operations of not only the Azure environment but also the hybrid cloud and O365 platforms.

Microsoft Azure Sentinel offers below controls and services:

- Security monitoring and architecture design
- SIEM solution implementation using Microsoft Sentinel
- Integration with Infosys shared security monitoring infrastructure
- Custom data source integrations
- Custom threat scenario monitoring
- Custom log data retention solution

Comprehensive SOC operations

Triage, analysis and response integrated into a comprehensive SOC operating model reducing time and improving effectiveness. Integrated threat and risk modelling with security analysis and reporting for private cloud, public cloud, and hybrid configurations.

Respond quickly and effectively

To any security incidents to protect your data, staff and organization. Removes the noise of event logs and time-consuming task of event analysis, allowing your IT team to better focus their time. Ensures any security incidents are thoroughly investigated and can be quickly acted upon to mitigate damage and remove threats.

Visibility and Compliance

Provide holistic visibility into your complete asset and environment through collaboration, automation and tools with business partners and IT stakeholders within the organization. This will help in identifying threats and provide a complete view of vulnerabilities in real time, correlate and analyze them.

Optimize

Delivering flexible and adaptive security solution for securing the Azure environment through a simple engagement model with commercial flexibility to streamline the cost of managed security threat detection, response and SoC services

Manage Risk

Single holistic view of risk and threat across the enterprise including private and public clouds with centralized integrated security knowledge repository with enhanced anomaly detection