MANAGED SENTINEL

AZURE Sentinel SIEM Management

Cloud-native SIEM for intelligent security analytics of the entire enterprise

Founded by senior cybersecurity architects, with extensive years of experience in deploying a wide range of network security controls, **Managed Sentinel** has identified Azure Sentinel as a game changer in the SIEM vendors marketplace.

The maturity of the cloud services offering combined with a realignment of the expectations of the ROI from the SIEM infrastructure make Azure Sentinel a perfect candidate for the next generation SIEM that combines the scalability of the cloud with a focus on effective threat hunting capabilities.

Scalability

Limitless cloud speed and scale – On demand capacity, no capital costs

Integration

Easy integration with existing monitoring and operations tools

Hybrid Infrastructure

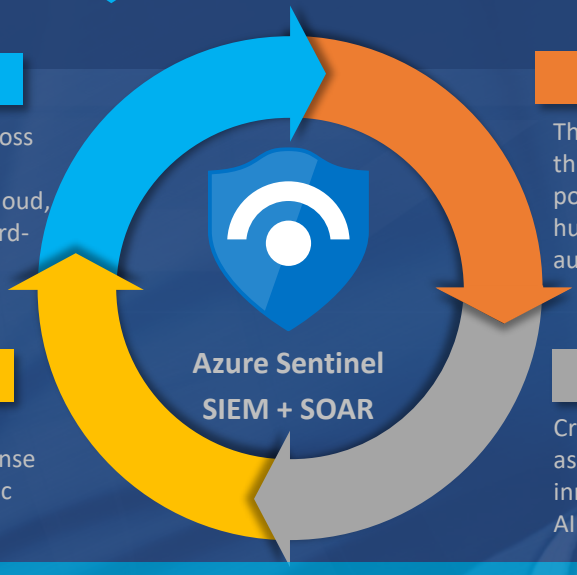
Collect logs from cloud, on-premises and 3rd party services

Collect

Logging data across the hybrid infrastructure: cloud, on-premises, third-party services

Detect

Threats with vast threat intelligence and powerful threat hunting tools, augmented by AI/ML



Respond

Rapidly and automate response using Azure Logic Apps

Investigate

Critical incidents assisted by innovative tools and AI

Managed Sentinel is purely focused on delivering the best in class SIEM management service. The SIEM functions of collecting logging data, detecting indicators of compromise, augmenting the investigation effort and being a critical component in the incident response process flow are reflected in how our service is designed: value, no-nonsense, efficiency and focus on actionable intelligence.

Premium Managed SIEM Services from Managed Sentinel Inc.

Support

Continuous monitoring of Azure Sentinel solution, log sources and deployed alerts and dashboards.

Support information security analysts during incident response.

Deployment

Design, deploy and configure Azure Sentinel SIEM. Configure data collection from cloud, on-premises and 3rd party sources.

Integration with IT operation tools and on-prem monitoring applications.

Alerts, Reports and Dashboards

Provide access to a large pool of use-cases applicable to endpoints, applications, network and security appliances, across the cloud and on-premises infrastructure.

Access to alert remediation knowledgebase.

Use-case Review /Tune-up

Regular review of deployed use-cases using. Tune-up alerts, reports and dashboards for maximum actionable intelligence.

Web: www.managedsentinel.com

Email: sales@managedsentinel.com

Microsoft Partner