# Managed Security Services 🔍

MANAGED SENTINEL

Managed Azure Sentinel SIEM (MAS³)

Managed Sentinel Inc., a Microsoft solution partner, has been recognized as one of the world's most innovative cybersecurity firms with a focus on Cloud domain.

Managing and monitoring a Security Information and Event Management (SIEM) device can quickly become costly and inefficient. Instead of allowing internal security engineers to focus on new projects and core business needs, they may be stuck reviewing logs, monitoring alerts for possible issues, performing device upgrades and providing remediation. By outsourcing the monitoring and management aspect of this important part of your security program, you can reallocate internal resources and receive peace of mind that your environment is efficiently managed and constantly monitored for infection or compromise.

Our core managed service is Managed Azure Sentinel SIEM Service, service offering tailored to help enterprises and SMB globally to increase visibility into their security posture and to better respond to cybersecurity incident. Our Managed Azure Sentinel SIEM Service (MAS3) includes:

❖ **Incident Response Support:** Managed Sentinel Inc. has extensive hands-on experience managing complex security breaches.

❖ **Cloud Costs Monitoring and Optimization:** Our analysts know that Cloud consumption is a key metric and optimizing this for our customers is a critical component.

❖ **Continuous Use Case Tuning:** The value of a managed SIEM service stays in service provider capabilities to continuously tune-up the alert rules and playbooks in order to reduce the volume of false positives.

❖ **Embedded Threat Intelligence:** Our proprietary, machine learning algorithm, and dark web discovery are leveraged to expedite triage and enrich cybersecurity investigations.

❖ **Regular Service Review:** Managed Sentinel Inc. SOC team meets regularly the customer to review and collect feedback and new requirements on alerts, playbooks and workbooks.

❖ **Access to largest Azure Sentinel alert rule database:** Managed Sentinel Inc. engineers has developed a large repository of alert rules which has been deployed and tested in many Azure Sentinel instances.
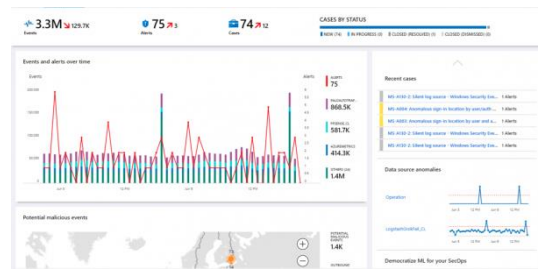
Why Choose MAS3 service ?

❖ No capital expenses

❖ Service backed by best of bread Cloud SIEM technology

❖ Short implementation timelines

❖ No additional software or hardware to deploy

❖ Reduced Alert Fatigue

❖ Our pool of experts eliminates your staffing headaches

❖ Meet security compliance

❖ Pay-as-you-go model

| Managed Sentinel SIEM Service | Azure Sentinel Consulting Services | Cloud Security Professional Services | O365 Security Monitoring | Firegen Threat Intelligence Feeds |

MANAGED SENTINEL

Managed Azure Sentinel SIEM (MAS³)

It's time for organizations to say no to the complexities of legacy SIEM products and yes to a simpler approach to protecting their environments. With the **MAS³** managed service you don't need to be an expert to take your security and compliance posture to the next level.

Service Elements

❖ SIEM Capabilities delivered from the Azure Cloud

❖ No additional software or hardware to deploy

❖ Support for on-premises log sources (>30 log parsers available)

❖ Security Monitoring of Cloud services (Azure, AWS, Google)

❖ Continuous alerts and playbooks tuning and optimization

❖ Performance and availability monitoring and notification

❖ Access to Managed Sentinel Alert Rules Service Catalogue

❖ Compliance aware monitoring

❖ Daily Log Analysis

❖ Support during security incidents

❖ SOAR support and integration

❖ Cloud costs alerting & reporting

❖ Threat intelligence service integration

❖ On-demand APT IoC lookups

❖ Online access MS-Alert knowledgebase

❖ Monthly service review

❖ Azure Sentinel SIEM runs in customer Azure subscription
❖ Service is priced based on the number and type of log sources

MAS³ offers the intelligence and automation to correlate and analyze high volumes of log and audit events from across disparate systems and applications. Powerful Cloud SIEM platform and big data enabled intelligence systems cover nine core correlation dimensions including:

❖ Asset based

❖ Behavior based

❖ Heuristic based

❖ Historical based

❖ Risk based

❖ Rule based

❖ Statistical based

❖ Threat based

❖ Vulnerability based

About Managed Sentinel Inc.

Managed Sentinel, a Microsoft solution partner provides cybersecurity products and services to SMB and enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity organizations, and excel in complex, multi-technology environments. Our service expertise includes Azure Sentinel SIEM, Advisory Services, Technology Architecture & Implementation, Managed Security Services, Threat Intelligence Management, and Incident Response. Managed Sentinel Inc. has customers all over the world. For more information, visit www.managedsentinel.com or contact us at sales@managedsentinel.com