Managed Security Intelligence and Event Monitoring (SIEM) with Azure Sentinel

Comprehensive threat detection and security management across multiple attack surfaces

As organizations continue to invest in new technologies and enable remote working, the information security leaders face growing magnitude of alerts, diverse attack surfaces, and increasingly sophisticated cyber-attacks. In order to keep up, companies continue to add multiple third-party security tools, making security management even more inefficient at a time when their lean security teams are already outnumbered and overwhelmed.

31%
Increase in average attacks per company from 206 in 2020 to 270 in 2021[1]

15%
IT budget spent on security in 2021, up 5 percentage points from 2020[1]

49%
Respondents said keeping up with security requirements has gotten harder[2]

Get a standing watch by your side with our managed services

If your organization is struggling to keep up, we can be your cyber-security guards, helping you detect threats faster, reduce your security risks, and optimize your team to enhance operational efficiency.

Through an implementation of a baseline Azure Sentinel* solution, our managed SIEM services can help you simplify log aggregation, security analytics, and threat detection. We then provide you the flexibility to opt to address more in-depth investigations and remediation activities.

***Azure Sentinel** is a cloud-native intelligent security analytics and threat intelligence solution from Microsoft, providing a single platform for alert detection, threat visibility, proactive hunting, and threat response.

79%	Reduction in false-positive alerts
48%	Less expensive as compared to legacy SIEM solution
67%	Faster time-to-deployment with out-of-the box functionality

Source: The Total Economic Impact™ Of Microsoft Azure Sentinel, Forrester, 2020

Get in touch with us:

Bryan Kail
Practice Manager, Managed Services, Applied Information Sciences
bryan.kail@ais.com

Sources:
1. State of Cybersecurity Resiliency, Accenture, 2021
2. The State of Security, Splunk, 2021

Our process for threat monitoring and incident response with Azure Sentinel

Assess

Discover key business goals and challenges faced in the current scenario.

Understand existing IT architecture and key attack surfaces.

Understand existing security monitoring setup and security incident response plan.

Define

Provide an overview of how Azure Sentinel can help streamline security operations.

Design the reference architecture and define data connectors' mapping against log sources.

Establish baseline implementation

Connect log sources using in-built data connectors / develop custom data connectors (if required).

Set-up the required alerts and dashboards.

Our baseline of common log sources include:

- Azure Active Directory Identity Protection
- Azure Defender
- Microsoft 365 Defender
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- M365 Defender for Cloud (formerly known as Cloud App Security)

Ongoing management

Collect events from log sources and proactively monitor and hunt for threats within your environment.

Optimize threat detection rules from templates to detect risks and reduce false positives.

Investigate detected threats and work with your security team to mitigate legitimate threats.

AIS brings a rich legacy in the IT industry

For almost 40 years, AIS has delivered cloud transformation solutions to companies ranging from startups to Fortune 100, including government and security agencies.

Gold Microsoft Partner

Microsoft

Security
Cloud Platform
Datacenter
Application Integration
Data Platform

Microsoft

Advanced Specialization

Cloud Security

Microsoft

2018 Microsoft Partner of the Year for Azure Perfomance

Get in touch with us:

Bryan Kail
Practice Manager, Managed Services, Applied Information Sciences
bryan.kail@ais.com

ais APPLIED INFORMATION SCIENCES