happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Azure Sentinel

Introduction

Security has become a fundamental part of IT Infrastructure, and you require a better Security Information and Event Management (SIEM) tool to analyze today's advance threat. Azure Sentinel, an SIEM Microsoft Product, is a perfect cloud-native solution that provides intelligent security analytics at cloud scale for your entire organization. It effectively uses the power of Artificial Intelligence to detects the actual threats within no time.

Centralized Log Management

Security Threat Detection

Proactive Threat Hunting

Service Needs and Challenges

Defending organization against the ever-growing Cyber Security Threats

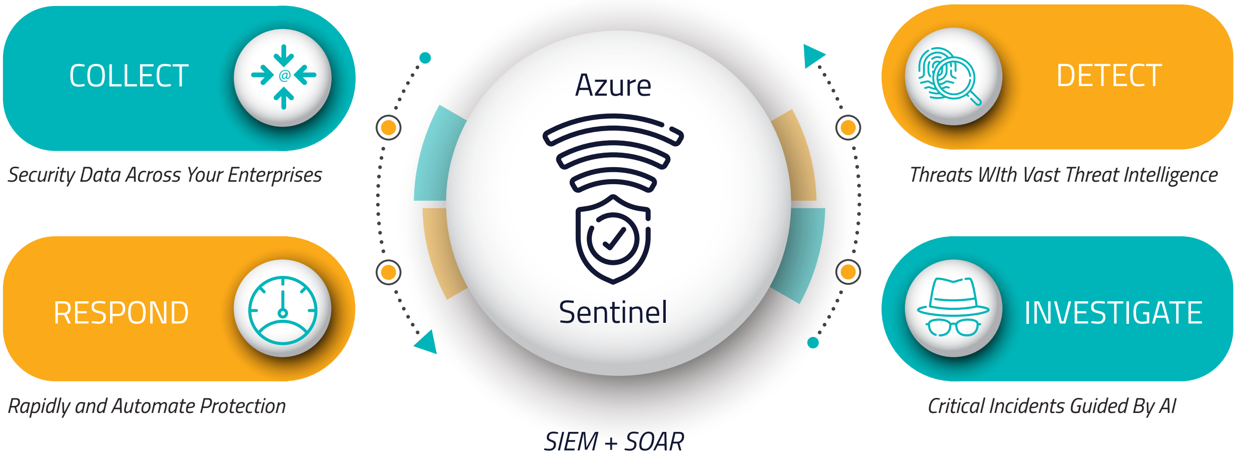
Identity, Credential, Access Management

Malicious Inbound Communications

Lack of Visibility, Control and Monitoring Suspicious Activities

Automated playbooks that increase the productivity of IT and support personnel by reducing the amount of trivial and time-consuming remediation tasks required.

Key Features



COLLECT

Security Data Across Your Enterprises

DETECT

Threats WIth Vast Threat Intelligence

Azure Sentinel

RESPOND

Rapidly and Automate Protection

INVESTIGATE

Critical Incidents Guided By AI

SIEM + SOAR

Key Benefits

01 Enterprise Integration, Assimilates with other Azure Services

02 Advance AI, uses ML & AI to hunt network threats

03 Eradicates Security Infra, reduced the maintenance cost

04 Collect data at cloud scale both on-premises & multiple clouds

05 Use workbooks to power interactive dashboards, rich visualization and gain more insights

06 Correlate events with Microsoft URL intelligence and with your own threat intelligence

07 Analysis of multistage attack: Start and track investigations from prioritized, actionable security incidents

08 SOAR scalability: Playbooks can be attached to the alerts and a pre-determined response can be initiated

09 Detect previously undetected threats, and minimize false positives using Microsoft's in-built analytics rules and unparalleled threat intelligence

Service offering suite for Azure Sentinel as a Service

Azure Sentinel as a Service

Consulting

Consulting package which covers POC with use case customizations, two out of the box integration and recommendations

System Integration Services

System Integration Services package encompasses Design and Access, Implementations

Azure Manage Services

Manage Services would comprise of Basic and Platinum packages which includes monitoring and few additional customizations based on requirements

Build and Implement

Requirement Gathering and Planning

Gathering technical objectives and requirements

Architecture Designing

Designing the Azure Sentinel Architecture as per the requirements

Integration and Implementation

Integration and of in-scope devices, develop and enable the relevant use cases (feeds, rules, dashboards, playbooks)

Manage and Operate

Operations and Support

Definition and management of the scope, processes and SLA. Fine-tuning for continuous improvement

Incident Response

Playbooks to ensure streamlined incident identification, analysis and remediation

Proactive Threat Hunting

Hunting for threat behaviors proactively and automate investigations using playbooks

Service Packages

Services	Silver	Gold	Platinum
Service Window	8*5	24*7	24*7
Environment Assessment	✓	✓	✓
Design and Implementation	✓	✓	✓
Out-of-Box Integration and Analytics Rules	✓	✓	✓
Enabling Default Analytics and Playbooks	✓	✓	✓
Out of the box Automation use cases	✓	✓	✓
Out of the box Dashboards	✓	✓	✓
Recommendations to Remediate	✓	✓	✓
Out of the box reports	✓	✓	✓
Custom Log Sources integration	Up to 2	Up to 3	Up to 5
Custom Workbooks and Automation use cases	None	Upto 5	Upto 10
Weekly / Monthly Service review	✓	✓	✓
Quarterly Governance review with leadership	X	X	✓
Customized Reports	X	X	✓
Threat Hunting with In-Built Queries and HM Native Tools	X	X	✓
Custom Analytics Rules based on MITRE Framework	X	X	✓
Remediation support	X	✓	✓

Our Value and differentiator

Collaboration & Coordination-Integrated across enterprise ecosystem, enables seamless services experience

Agility & Value Realization-Drive value for Business, enhance user experience and brings business aligned agility

Simple & Sustainable-Focus on building fundamental capabilities, efficient approach to meeting objectives

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

www.happiestminds.com

Business Contact **business@happiestminds.com**

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, Blockchain, Automation including RPA, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

A Great Place to Work-Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, The Netherlands, Australia and Middle East.