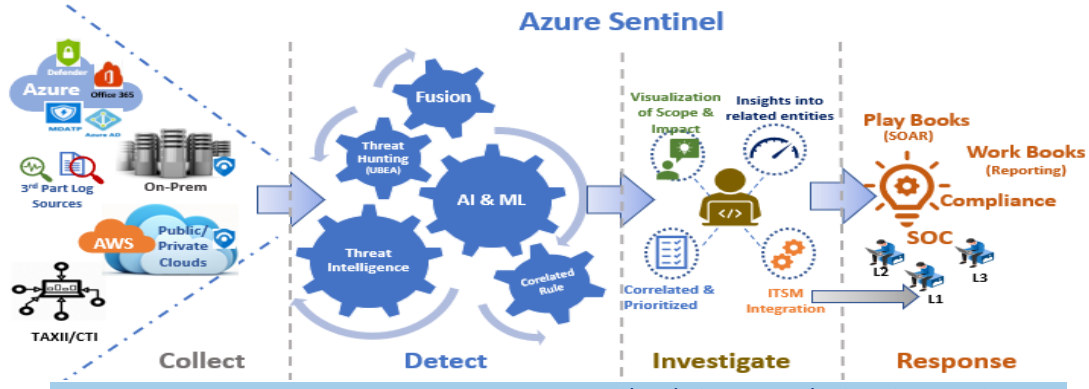
ZenSOC Security Solution with Azure Sentinel

TRANSFORM | AUTOMATE | SECURE

It's time for organizations to say no to the complexities of legacy SIEM products and yes to a holistic approach for protecting environments using modern technology. Zensar, in partnership with Microsoft, offers free assessment of 2 weeks that helps building a robust business case for technical deployments of cloud native SIEM solution using Azure Sentinel. Zensar is a Managed Security Service Provider, specializing in industry-leading solutions, technologies and expertise to secure cloud and non-cloud



- Proactive Threat hunting and detection
- MITRE Framework
- Automate alerting using AI/ML
- SOAR Incident Management
- Cloud, On-prem devices integration at Scale and Speed.
- Fusion Technology
- Threat Intelligence and User Behavior Analytics (UBA)
- 90% reduction on Alert Fatigue.

- Offers 2 weeks of free assessment.
- Providing continuous real-time threat detection, threat hunting and SOAR response to cyber attacks for cloud and on-premises IT resources.
- Increasing visibility into security posture and responding timely to security incidents across client's global locations.
- Incorporated solutions having AI/ML/Fusion, SOAR etc. that makes it scalable and cost-effective
- Recommendation plan for Seamless operations for deploying Azure Sentinel, considering cost, sizing, and other factors.
- Agility and flexibility

Service Features

- **24x7 Alerting & Incident response:** Operational support delivered from SOC that covers 24x7x365 service window, to provide information on qualified security incidents and response to reduce attack surface.
- **Cloud Monitoring & Costs Optimization:** Our SOC analysts know that Cloud consumption is a key metric and optimizing cost is a critical component for our customers.
- **Enterprise grade solution:** Helps establish a non-intrusive log collection and storage mechanism across Enterprise IT infrastructure and applications, results in capability to correlate millions of independent events from heterogeneous sources to detect and report actual security incidents to our clients.
- **Continuous Use Case Finetuning:** Our Security Engineering Team continuously do research on current state and do tune-up the alert rules and playbooks in order to reduce the volume of false positives.

Free 2 Weeks of Assessment Offer!

- **Week 0: Kick off, o**bject setting and scope, Plan the PoV and define Outcome.
- **Week 1:** Assess current Network and Infra architectural details, Tools and Technology, existing challenges and future requirements.
- **Week 2:** We will identify & analyze the average consumption, based on key log sources types. Recommendation on best use cases using power of AI/ML. suggest Playbook and Dashboards for organization as per the client specific industry and best practices.
- **Conclusion:** We will deliver high level design of 'To Be Architecture'(HLD), help building a business case for technical deployment of True cloud native SIEM. Provide recommended approach leveraging the Advance ZenSOC SIEM Services.

Advancements

- **AI/ML :** Security expertise in deploying Azure Sentinel SIEM that includes custom Use cases with the Power of AI/ML, automated playbooks and dashboard to help Client, by detecting and responding real time threats quickly.
- **Framework and compliance :** Continuous Fine-tuning of use cases based on MITRE ATT&CK framework and industry specific to clients User, cloud/ Hybrid Infrastructure and compliance policies.
- **MTTD/MTTR :** Perform Incident management with detailed Root Cause Analysis and Mitigation. Decreases Mean time to Detection, prevent and remediation threats through automation.
- **Speed and Scale:** Continuous improvement to reduce false positives and improve outcomes with offering limitless cloud scale and speed, scaling automatically to address your needs.

Zensar Modernizes your Security Operations Center (SOC) with an Intelligent SIEM + SOAR solution - Azure Sentinel

Provisioning

- Azure Sentinel setup
- Onboarding Log Sources
- Usage Reports
- Threat Intelligence Feed
- Resilient Log Monitoring

Use Case Configuration

- Deploy Sentinel alert rules
- Configure Playbooks(SOAR)
- Configure Workbooks(Dashboard)
- Create Log Parsers
- Add additional Log Sources

Analysis

- Reduce 90% of false positive
- Experienced Data Scientist, Analysts and Threat Hunter.
- Correlated and prioritized incidents using AI/ML.
- Decrease Mean Time to Remediation (MTTR).
- Central place for security operations well-established best practices for Cyber Resiliency.

SOAR

- Create Custom Playbooks
- Condition with K-Query
- Creation of Alert Rules and Triggers
- Advance Fusion and Jupyter notebooks
- Managed Action with Managed Action groups
- Integrate alerts/notifications with Email/ ITSM tools

Tune-Up

- Sentinel alert rules tune-up
- Additional optimization of log ingestion
- Regular meetings with customer
- Executive Dashboard

Implementation & Engineering Services

24 x 7 Managed Services

Advisory and Consulting

Security OPEX Reduction

Productivity Improvement

Speed and scale

Compliances

Reduce Risk Exposure

central place for security operations

SOAR/ Proactive Threat Hunting

Why Zensar? Fortune 2000 companies are using Zensar's Digital Infrastructure Services.

We are a Gold Certified, Globally Managed, Microsoft Cloud Solution Provider.

DXP

Microsoft

Magento

sitecore Own the experience

CISCO

Adobe Experience Manager

Microsoft Azure