

## Enhanced Security with Microsoft Sentinel

Member of  
Microsoft Intelligent  
Security Association



### BUSINESS CHALLENGES:

As businesses grow, managing security across their enterprise environments becomes increasingly complex. Many organizations find it challenging to monitor potential threats, secure their infrastructure, and respond promptly to security incidents. Legacy security tools often lack the necessary integration, automation, and advanced analytics to address evolving cyber threats. The transition to hybrid and multi-cloud environments further complicates these issues, necessitating a unified and intelligent approach to protect against increasingly sophisticated attacks.

### SOLUTION OVERVIEW:

Zones address security challenges by utilizing Microsoft Azure Sentinel, a cloud-native SIEM (Security Information and Event Management) solution. Microsoft Sentinel offers centralized security analytics, real-time threat detection, and automated response capabilities across your IT infrastructure.

Our solution seamlessly integrates with your existing systems, utilizing advanced AI and machines, learning to detect anomalies and respond to threats before they escalate. With Azure Log Analytics and Logic Apps, we enable automated workflows, while customizable dashboards and actionable insights provide security teams with complete control over their environments. By implementing proactive monitoring and a comprehensive threat intelligence stream, Sentinel enhances your capability to defend against attacks and minimize risk.

### KEY BENEFITS INCLUDE:

**Centralized Threat Detection:** Unify security monitoring across multi-cloud environments & on-premises systems.

**AI-Enhanced Monitoring:** Utilize AI to identify threats more quickly and efficiently than traditional tools.

**Automated Response:** Implement automated threat responses to reduce human intervention & speed up remediation.

**Customizable Dashboards:** Gain real-time visibility & detailed insights with customizable, role-based dashboards.

### DEMO OVERVIEW:

This demo showcases the power of Microsoft Sentinel in a real-world environment. You'll see how to configure Microsoft Sentinel, set up data ingestion, and leverage AI-driven threat detection to enhance your security posture. The demo covers the end-to-end process, from setting up a sample environment to creating security alerts and automated workflows for threat remediation. You'll also explore how Sentinel integrates with existing security tools and uses multi-cloud data to provide full visibility into your infrastructure.

**For more details or to schedule a demo, contact your Zones Account Executive.**

MDM Lab Environment  
Powered By ManageEngine

