Azure Sentinel Course

Course Duration: 24 Hours **Course code: AZ-SEN-01**

1. Course Overview

Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) solution that helps organizations detect, investigate, and respond to cyber threats. This course provides hands-on training to monitor security events, analyze threats, and automate responses using Azure Sentinel.

2. What You'll Learn

- Introduction to Microsoft Azure and Azure Sentinel
- Setting up Azure Sentinel workspace
- Data connectors and log integration
- Threat detection using analytics rules
- Incident investigation and response
- Automation using playbooks and Logic Apps
- KQL (Kusto Query Language) basics
- Security monitoring and threat hunting techniques

3. Target Audience

- Security Analysts
- IT Professionals
- Cloud Engineers
- SOC Team Members
- Cybersecurity Enthusiasts
- System Administrators

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

4. Pre-Requisites

- Basic knowledge of cloud computing
- Understanding of networking concepts
- Familiarity with cybersecurity fundamentals
- Basic knowledge of Microsoft Azure portal (recommended but not mandatory)

5. Course Content

Module 1: Introduction to Azure Sentinel

- Overview of SIEM & SOAR
- Benefits of Azure Sentinel

Module 2: Azure Fundamentals for Security

- Azure architecture basics
- Resource groups and subscriptions

Module 3: Setting Up Azure Sentinel

- Creating Log Analytics Workspace
- Enabling Azure Sentinel

Module 4: Data Connectors

- Azure services integration
- Third-party data connectors
- Log ingestion

Module 5: Analytics & Detection

- Creating analytics rules
- Alert configuration
- Threat intelligence integration

Module 6: Incident Management

- Investigating incidents
- Incident response workflows

Module 7: Threat Hunting

- Using KQL queries
- Hunting queries and notebooks

Module 8: Automation & Response

- Creating playbooks
- Integrating with Logic Apps

Module 9: Workbooks & Visualization

- Creating dashboards
- Monitoring reports

Module 10: Best Practices & Real-World Use Cases

- Security optimization
- Case studies

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com