ZOOM
TECHNOLOGIES

Microsoft Sentinel Training

(Hands-On Cloud-Native SIEM & SOAR Operations)

The Microsoft Sentinel Training at Zoom Technologies is a complete, hands-on program that takes you from cloud computing fundamentals to confident operation of Microsoft Sentinel — Azure's cloud-native SIEM and SOAR platform. Starting with Azure essentials, networking, and Sentinel's data-flow architecture, you'll configure every major capability live in your own Azure tenant: Log Analytics workspaces, RBAC, data connectors, AMA and Data Collection Rules, on-premises onboarding through Azure Arc, Kusto Query Language, analytic rules across all five rule types, incident investigation, Logic Apps playbooks, workbooks, watchlists, and ingestion cost control. By the end, you'll be able to deploy, monitor, detect, automate, and optimise a production Microsoft Sentinel deployment in a real enterprise environment — with a curriculum closely mapped to the SC-200 certification exam objectives.

Key Topics:

- Cloud & Azure Fundamentals
- Sentinel Architecture & Data Flow
- Workspace Deployment & RBAC
- Data Connectors, AMA & DCR
- Azure Arc On-Premises Onboarding
- KQL Deep Dive
- Analytic Rules & Threat Detection
- Threat Hunting & Investigation
- SOAR Playbooks & Automation
- Workbooks & Watchlists
- AI Based SOC Operation
- Cost Optimisation

+91 7893399822 priya@zoomgroup.com www.zoomgroup.com

Microsoft Sentinel Training

Module 1: Cloud Computing Fundamentals
- What is cloud computing
- Cloud service models: IaaS, PaaS, SaaS
- Public, private, hybrid and community cloud
- Why cloud security matters
- Security challenges in cloud environments

Module 2: Azure Fundamentals
- What is Azure
- Shared responsibility model
- Azure subscription types
- Creating your Azure subscription
- Azure resource hierarchy
- Resources, resource groups and Role-Based Access Control (RBAC)
- Creating and managing Azure resource groups

Module 3: Azure Networking
- Overview of Azure networking and its components
- Implementing and managing Azure Virtual Networks (VNet)
- Configuring VNets, managing IP and subnets
- Creating and managing Azure Virtual Machines

Module 4: Microsoft Sentinel Architecture
- What is Microsoft Sentinel
- Sentinel as SaaS
- SIEM vs SOAR — understanding the differences
- Sentinel architecture and components
- How data flows in Microsoft Sentinel

Module 5: Deploying & Managing Sentinel
- Deployment prerequisites for Sentinel
- Creating a Log Analytics Workspace
- Creating a Sentinel workspace
- Azure RBAC and Sentinel RBAC
- Configuring Azure RBAC for Sentinel

Module 6: Data Connectors
- Overview of data connectors
- Typical data sources for a SIEM
- Working with the Content Hub
- Ingesting threat intelligence and verifying ingestion
- Ingesting Entra ID logs and verifying ingestion
- AMA and Data Collection Rules (DCR)
- Ingesting Windows Security Event logs with AMA and DCR
- Ingesting Linux Syslog logs with AMA and DCR

Module 7: On-Boarding On-Premises Machines
- What is Azure Arc
- Azure Arc roles
- Prerequisites for Azure Arc
- On-boarding on-premises Windows machines
- On-boarding on-premises Linux machines
- On-boarding on-premises virtual machines

Module 8: Ingesting On-Premises Logs
- Ingesting Windows Security Event logs with AMA
- Verifying Windows Security Event log ingestion
- Ingesting Linux Syslog logs with AMA
- Verifying Linux Syslog log ingestion

Module 9: Kusto Query Language (KQL)
- Introduction to KQL and Log Analytics
- Writing basic KQL queries
- Advanced KQL: joins, aggregations and time-series analysis
- Creating custom dashboards with KQL in Sentinel Logs
- Hands-on practice: KQL for threat investigation

Module 10: Threat Hunting & Investigation
- How Sentinel detects and correlates security incidents
- Investigating alerts and incidents in Sentinel
- Managing false positives and incident prioritisation
- Hands-on incident investigation walkthrough

Module 11: Analytic Rules & Threat Management

- Analytic rules — concepts and rule types
- Configuring analytic rules
- Scheduled analytic rules
- Scheduled analytic rules — Entra ID
- Scheduled analytic rules — Windows Security Events
- Near-Real-Time (NRT) rules
- NRT rules — Windows Security Events
- Fusion — multi-stage attack detection
- ML Behavior Analytics
- Threat Intelligence rules
- Microsoft Security rules

Module 12: Automation & SOAR

- Automation capabilities in Sentinel
- Automation rules and how to build them
- Playbooks
- Automation rules vs playbooks
- Azure Logic Apps
- Building playbooks with Azure Logic Apps

Module 13: Workbooks

- Workbooks in Sentinel
- Creating workbooks
- Creating a customised dashboard in Azure

Module 14: Watchlists

- Watchlists in Sentinel
- Creating watchlists
- Integrating watchlists with analytic rules

Module 15: Cost Optimisation

- Pricing models
- Commitment tiers
- Log types
- Archive and restore logs

Module 16: AI Based SOC Operation