SC-5001: Configure SIEM security operations using Microsoft Sentinel

Course Duration: 8 Hours **Course code: SC-5001**

1. Course Overview

The **SC-5001: Configure SIEM Security Operations using Microsoft Sentinel** course is designed to provide IT professionals and security operations teams with the knowledge and skills to configure, manage, and monitor security operations using Microsoft Sentinel. This course focuses on integrating Microsoft Sentinel with various data sources, creating detection rules, performing threat hunting, and responding to incidents effectively. By the end of this training, learners will be equipped with hands-on experience in leveraging Microsoft Sentinel for Security Information and Event Management (SIEM) solutions.

2. What You'll Learn?

- Understand the architecture and capabilities of Microsoft Sentinel.
- Configure and connect data sources to Microsoft Sentinel.
- Create and manage analytics rules to detect threats.
- Implement threat hunting queries using Kusto Query Language (KQL).
- Investigate and respond to security incidents.
- Automate security responses with playbooks.
- Manage workbooks and dashboards for security insights.

3. Target Audience

This course is intended for:

- Security Operations Center (SOC) Analysts.
- Security Engineers.
- IT Administrators and Security Professionals.
- Threat Hunters.

- Professionals preparing for Microsoft Security certifications.

4. Pre-Requisites

Before attending this course, learners should have:

- Basic understanding of Microsoft Azure services.
- Knowledge of security concepts such as SIEM, SOAR, and threat detection.
- Familiarity with networking and cloud fundamentals.
- Experience with Microsoft 365 Security and Azure Security tools is recommended.

5. Course Content

Module 1: Introduction to Microsoft Sentinel

- Overview of SIEM and SOAR
- Microsoft Sentinel architecture and capabilities
- Deployment and configuration basics

Module 2: Connecting Data Sources

- Integrating Microsoft 365 and Azure data sources
- Connecting on-premises and third-party sources
- Best practices for data ingestion

Module 3: Creating Detection Rules

- Configuring analytics rules
- Working with scheduled and near-real-time detections
- Managing alerts and incidents

Module 4: Threat Hunting with Microsoft Sentinel

- Introduction to Kusto Query Language (KQL)
- Building queries for hunting
- Using hunting workbooks and bookmarks

Module 5: Incident Investigation and Response

- Investigating alerts and incidents
- Using entity behavior analytics
- Incident response workflows

Module 6: Automating Security Operations

- Introduction to automation and playbooks

- Configuring Logic Apps for incident response
- Automating remediation processes

Module 7: Workbooks and Dashboards

- Creating and managing workbooks
- Visualizing security data
- Customizing dashboards for SOC operations