Document Generated: 12/17/2025

Learning Style: Virtual Classroom

Technology: Microsoft

Difficulty: Intermediate

Course Duration: 1 Day

Configure SIEM security operations using Microsoft Sentinel (SC-5001)

About This Course:

Start your journey with Microsoft Sentinel security operations by setting up and configuring the Microsoft Sentinel workspace to serve as the central hub for monitoring and managing security events. Connect various Microsoft services, such

as Azure and Microsoft 365, along with Windows security event logs, to ensure comprehensive data collection and visibility across your environment. Configure advanced analytics rules to detect potential threats, streamline threat detection processes, and identify anomalous activities. Enhance your security posture by implementing automated response mechanisms that allow for swift and efficient threat mitigation, reducing response times and minimizing risk

Course Objectives:

- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs
- Plan for Microsoft services connectors
- Connect the Microsoft Office 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector
- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs
- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules
- Understand automation options

- Create automation rules

Audience:

- Security Operations Analysts
- Security Engineers
- IT Administrators

Prerequisites:

- Fundamental understanding of Microsoft Azure
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in Microsoft Sentinel

Course Outline:

- Create and manage Microsoft Sentinel workspaces
- Connect Microsoft services to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- **Configure SIEM security operations using Microsoft Sentinel**