TEACHME CYBERSECURITY

— LEARN. PRACTICE. SECURE. —

Microsoft Sentinel SIEM Engineer

Official Course Syllabus

Duration: 4 Weeks | Mode: Live Instructor-led | Practice: Hands-on Labs | Exit: Capstone Project

Course Overview: Master Security Information and Event Management (SIEM) and Security Orchestration, Automation & Response (SOAR) using Microsoft Sentinel. Learn log ingestion, Kusto Query Language (KQL), analytics rules, incident investigation, threat hunting, workbooks, automation, and Microsoft Defender XDR integration through real-world enterprise scenarios.

Course Modules

Module 1 – SIEM Fundamentals

- Introduction to SIEM
- SOC Architecture
- SIEM vs SOAR
- Security Monitoring
- MITRE ATT&CK Framework
- Incident Lifecycle

Module 2 – Microsoft Sentinel Fundamentals

- Sentinel Architecture
- Log Analytics Workspace
- Data Connectors
- Microsoft Sentinel Portal
- Cost Management
- Workspace Design

Module 5 – Analytics Rules & Incident Management

- Scheduled Analytics Rules
- Near Real-Time (NRT) Rules
- Fusion Detection
- Incident Queue
- Investigation Graph
- Entity Mapping
- Alert Tuning
- Hands-on Labs

Module 6 – Threat Hunting & Workbooks

- Hunting Queries
- MITRE ATT&CK Mapping
- Bookmarks
- Live Investigation
- Sentinel Workbooks
- Dashboards
- Executive Reporting
- Hands-on Labs

Course Modules (Continued)

Module 3 – Data Connectors & Log Ingestion

- Microsoft Defender XDR
- Microsoft Entra ID Logs
- Azure Activity Logs
- Office 365 Logs
- Syslog
- Windows Security Events
- Common Event Format (CEF)

Module 4 – Kusto Query Language (KQL)

- KQL Fundamentals
- Filtering
- Parsing
- Joins
- Aggregations
- Hunting Queries
- Workbook Queries
- Hands-on Labs

Module 7 – Automation & SOAR

- Automation Rules
- Logic Apps
- Playbooks
- Email Notifications
- Microsoft Teams Integration
- Incident Automation
- Response Workflows
- Hands-on Labs

Module 8 – Capstone Project

Deploy Microsoft Sentinel for an enterprise SOC environment. Students will:

- Connect multiple log sources
- Create Analytics Rules
- Build Hunting Queries
- Investigate Security Incidents
- Create Dashboards
- Build Automation Playbooks
- Generate Executive Security Reports

Tools Covered

Microsoft Sentinel • Log Analytics Workspace • Microsoft Defender XDR • Microsoft Entra ID • Microsoft Defender for Endpoint • Microsoft Defender for Office 365 • Azure Monitor • Logic Apps • Kusto Query Language (KQL)

Career Opportunities

Microsoft Sentinel Engineer • SIEM Engineer • SOC Analyst • Security Operations Engineer • Detection Engineer • Threat Hunter • Microsoft Security Engineer