DW-301 - Migrating your SIEM Solution to Microsoft Sentinel Deployment Workshop

Duration : 8 hrs

Module 1 Microsoft Sentinel basic concepts

- Microsoft Cloud Fundamentals
- Log Analytics Fundamentals
- High level Architecture Design
- Sizing and Cost Components
- Data Collection
- Multi-cloud Environment
- Automation /SOAR with Microsoft Sentinel
- Threat Intelligence
- MITRE Att&ck
- Analytical Rules
- Sentinel Workbooks
- DevOps – CI/CD Automation

Module 2 Planning the migration

- Planning your Migration
- Designing your Microsoft Sentinel workspace architecture
- Microsoft Sentinel content and solutions
- Writing Queries using Kusto Query language
- Creating Threat detection rules

Module 3 Migrating to Microsoft Sentinel from the Legacy SIEMs

- Migrating Detection rules
- Migrating SOAR Automation
- Migrating historical data
- Converting dashboards to workbooks
- Updating SOC Processes

Module 4 Post-migration optimization

- Permissions in Microsoft Sentinel
- Integrating Threat Detection
- Hunt for threats
- User Entity Behaviour Analytics
- Creating Automation rules
- Using Playbooks for Automation
- Investigating incidents
- Multi-customer Management after Migration