DW-360: Threat Protection and Incident Response with Microsoft Sentinel within Unified Platform

Threat Intelligence and Investigation in Microsoft Sentinel

Module 1: Designing and Configuring Microsoft Sentinel

- Introduction to Microsoft Sentinel
- Designing Microsoft Sentinel Workspace Architecture
- Managing Roles and Permissions in Microsoft Sentinel
- Enabling Data Connectors using Content Hub
- Deploying a Log Forwarder for Syslog and CEF Ingestion
- Understanding Security Coverage with the MITRE ATT&CK;® Framework
- Integrating Microsoft Sentinel with Amazon Web Services (AWS)
- AWS Service Log Ingestion
- AWS S3 Connector – Architecture Overview

Identify Advanced Threats in Microsoft Sentinel

Module 2: Threat Intelligence and Investigation

- Introduction to Microsoft Content Hub Solutions
- Overview of Threat Intelligence in Microsoft Sentinel
- Connecting Third-Party Threat Intelligence Platforms
- Working with Threat Indicators
- Detecting Threats and Analyzing Security Data
- Investigating Incidents in Microsoft Sentinel
- Using Workbooks for Threat Investigation and Analysis

Automating Responses and Advanced Analytics in Microsoft Sentinel

Module 3: User and Entity Behavior Analytics (UEBA)

- Introduction to User and Entity Behavior Analytics (UEBA)
- UEBA Analytics Architecture
- Enabling UEBA in Microsoft Sentinel
- Understanding Anomalies Detected by UEBA
- Querying UEBA Data

- Investigating Security Events Using UEBA

Integration and Automation with Microsoft Sentinel

Module 4: SOAR and Platform Integrations

- Introduction to SOAR in Microsoft Sentinel
- Creating and Managing Automation Rules
- Automating Incident Response with Playbooks
- Overview of Azure Logic Apps
- Customizing Microsoft Sentinel Playbooks from Templates
- Bring Your Own Machine Learning (BYOML) Platform
- Integration with Microsoft 365 Defender
- Integration with Microsoft Defender for Cloud

Security Copilot and Unified SOC

Module 5: AI-Driven Security Operations

- Introduction to Microsoft Security Copilot
- Enhancing Threat Detection with AI-Driven Insights
- Integrating Security Copilot into SOC Workflows
- Unified SOC Operations with Microsoft Defender and Sentinel
- Improving Analyst Efficiency and Decision-Making with Security Copilot