Course SC-5004: Defend against Cyberthreats with Microsoft Defender XDR

Level: Intermediate

Length: 1 day

Course Overview

About this course

This course teaches security operations analysts to defend against cyberthreats using Microsoft Defender XDR and Microsoft Defender for Endpoint.

Audience Profile: Security Operations Analysts, Security Engineers, SOC Teams, and Cybersecurity Professionals.

Course Details

Learning Path 2: Prepare data for analysis with Power BI

- Get data in Power BI
- Clean, transform, and load data in Power BI
- Choose a Power BI model framework

Learning Path 1: Mitigate incidents using Microsoft Defender

- Overview of Microsoft Defender XDR
- Incident management and investigation
- Alert correlation and attack investigation
- Incident response workflows

Learning Path 2: Deploy Microsoft Defender for Endpoint

- Architecture overview
- Onboard devices
- Configure endpoint protection
- Security policies

Learning Path 3: Configure alerts and detections

- Alert settings
- Indicators of compromise
- Detection configuration
- Threat detection strategies

Learning Path 4: Manage automation

- Automated investigation and remediation
- Automation policies
- Triggered actions

Learning Path 5: Perform device investigations

- Device timeline analysis
- Endpoint investigations
- Forensic evidence collection
- Threat hunting

Prerequisites

- Experience using Microsoft Defender portal
- Basic understanding of Defender for Endpoint
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL)