SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Course description

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advise on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Audience prerequisites

Before attending this course, students must have:

- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Microsoft Windows
- Familiarity with the Microsoft Defender portal and services
- Familiarity with Microsoft Defender for Endpoint
- Basic understanding of Kusto Query Language (KQL).

Learning Path	Module
Course Introduction	N/A
Learning Path: Defend against cyber threats with Microsoft Defender XDR	**Module 1:** Mitigate incidents using Microsoft Defender
	Module 2: Deploy the Microsoft Defender for Endpoint environment
	Module 3: Configure for alerts and detections in Microsoft Defender for Endpoint
	Module 4: Configure and manage automation using Microsoft Defender for Endpoint
	Module 5: Perform device investigations in Microsoft Defender for Endpoint
	Module 6: Defend against Cyberthreats with Microsoft Defender XDR lab exercises

Labs

The labs must be completed within the lab environment provided by your lab hosting provider. Detailed step-by-step instructions are provided for each lab and presented as part of the UI experience within your lab environment.