# Defend against cyberthreats with Microsoft Defender XDR (SC-5004) Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **1 Day**

This course equips security operations professionals with the skills to detect, investigate, and respond to cyberthreats using Microsoft Defender XDR. Learners will explore how Microsoft Defender technologies work together to improve visibility, accelerate response times, and reduce organisational risk through integrated threat protection workflows.

The course focuses on incident mitigation, Microsoft Defender for Endpoint deployment, alert and detection configuration, automation, and advanced device investigations. Through hands-on labs and real-world threat scenarios, learners will build practical experience using Microsoft Defender XDR to strengthen security operations and improve cyber resilience.

We believe organisations of the future need security teams that can rapidly adapt, collaborate, and apply defensive skills in real-world environments. This course supports that goal by combining technical knowledge with applied learning experiences aligned to modern security operations practices.

## Prerequisites

Participants should have:

- A fundamental understanding of Microsoft security, compliance, and identity technologies
- Intermediate knowledge of Microsoft Windows environments
- Familiarity with the Microsoft Defender portal and Microsoft Defender for Endpoint
- Basic understanding of Kusto Query Language (KQL)
- Experience with security operations or threat monitoring concepts is recommended

Learners preparing for the associated Microsoft Applied Skills assessment or working in a Security Operations Analyst role will benefit most from this course.

### Target audience

This course is designed for:

- Security Operations Analysts responsible for threat monitoring and incident response
- Cybersecurity professionals working with Microsoft Defender technologies
- SOC teams looking to improve threat investigation and remediation capabilities
- IT professionals supporting endpoint protection and organisational security operations
- Organisations seeking to strengthen cyber resilience through applied Microsoft security skills

This course is particularly valuable for teams responsible for reducing organisational risk through faster threat detection, response, and remediation.

# Defend against cyberthreats with Microsoft Defender XDR (SC-5004) Training

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## What You Will Learn

By the end of this course, learners will be able to:

- Mitigate security incidents using Microsoft Defender XDR tools and workflows
- Deploy and configure Microsoft Defender for Endpoint environments
- Configure alerts and detections to improve visibility into security threats
- Automate security operations tasks using Microsoft Defender for Endpoint capabilities
- Perform device investigations to identify suspicious activity and support remediation efforts
- Investigate and respond to cyberthreats using integrated Microsoft Defender XDR tools
- Apply practical threat response techniques through guided lab exercises and scenario-based learning

These learning outcomes align to the Microsoft Applied Skills assessment objectives for SC-5004 and reflect modern security operations analyst responsibilities.