Mastering Microsoft 365 security administration with Microsoft Defender XDR Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

This three-day instructor led course will provide delegates with the knowledge and skills to deploy and administer Microsoft 365 Defender to protect against cyber threats. Delegates will learn how to configure security across messaging and collaboration tools, devices, identities and applications. They will also learn how to use the service to detect possible ongoing attacks and block them.

Prerequisites

Important This course may require the use of Multifactor Authentication (MFA). Please read this page and download the Microsoft Authenticator app (or similar app) prior to attending the course:

https://www.qa.com/resources/faqs/mfa-requirements/

Please see the below Microsoft article for further information on reasons for the MFA requirement:

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication

- An understanding of core technical concepts, including DNS, Networking, Identities, and software deployment methods
- An understanding of common security threats and attacks such as malware, phishing, ransomware and software exploits
- Experience with Microsoft 365 components including Azure Active Directory, Exchange, Teams, OneDrive and SharePoint
- Experience with managing Active Directory Domain Services, Group Policy and Windows clients

Instructors will demonstrate features throughout the event. Optional lab exercises are available for students to complete using a commercial Microsoft 365 tenancy provided for each student free of charge by QA. This tenancy lasts for 30 days.

Target Audience

This course was designed for people who work in a security administrator job role or a general purpose administrator role with a responsibility to ensure that their Microsoft 365 environment is secure.

Mastering Microsoft 365 security administration with Microsoft Defender XDR Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

What You Will Learn

- How to license the services and navigate the Microsoft 365 Defender portal
- How to configure Defender for Office 365 capabilities to protect messaging and collaboration services against threats such as malware or phishing
- How to deploy Defender for Endpoint to devices, and protect them against threats such as malware, ransomware and software exploits
- How to deploy Defender for Identity to an on-premises Active Directory to protect it from threats against identities, such as stealing credentials and gaining admin control of the domain
- How to implement threat detection policies in Defender for Cloud Apps to provide alerts on unusual application behaviours which are often indicators of an attack
- How to investigate security incidents using the Microsoft 365 Defender portal and use remediation actions to block the attack

Outline

LP1 - Overview of Microsoft 365 Defender

Cyber security attacks

- Zero Trust model
- MITRE ATT&CK framework
- Example attack chain

Microsoft 365 Defender services

- Services overview
- License requirements
- Administration
- Microsoft Secure Score

Labs

Review

LP2 - Configuring Defender for Office 365

Threats and protection

- Protection against known threats
- Email authentication to prevent spoofing
- Protection against unknown threats

Defender for Office 365 policies

- Policies and recommended settings
- Managing the quarantine
- Advanced delivery policies

Attack simulation training

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Types of simulation
- Create and run a simulation

Labs

Review

LP3 - Deploying and configuring Defender for Endpoint

Exploring the service

- Capabilities
- Defender Vulnerability Management

Deployment

- General settings
- Permissions
- Onboarding

Evaluation lab

Protecting endpoints

- Next-generation protection
- Attack surface reduction

Labs

Review

LP4 - Deploying Defender for Identity

Deploying the sensor

- Creating the service accounts
- Installing the sensor
- Entity tags

Identity security posture

- Assessments
- Securing accounts
- Securing authentication protocols

Lab

Review

LP5 - Configuring Defender for Cloud Apps

Connecting to apps and logs

- Connecting to Office 365
- Cloud Discovery

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Admin roles

Threat detection policies

- Importing user groups
- Creating policies

Labs

Review

LP6 - Investigating and responding to threats

Responding to incidents

- Managing incidents
- Remediate
- Automated investigation and response

Advanced hunting

- Creating queries
- Kusto query language (KQL)

Labs

Review