Module Title : MS-500T02-A: Implementing Microsoft 365 Threat Protection
Duration : 1 day

About this course

Threat protection helps stop damaging attacks with integrated and automated security. In this course you will learn about threat protection technologies that help protect your Microsoft 365 environment. Specifically, you will learn about threat vectors and Microsoft's security solutions for them. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and how to use Microsoft 365 Threat Intelligence. It also discusses securing mobile devices and applications. The goal of this course is to help you configure your Microsoft 365 deployment to achieve your desired security posture.

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and ensures that the solutions comply with the policies and regulations of the organization.

This role proactively secures Microsoft 365 enterprise environments. Responsibilities include responding to threats, implementing, managing and monitoring security and compliance solutions for the Microsoft 365 environment. They respond to incidents, investigations and enforcement of data governance.

The Microsoft 365 Security administrator is familiar with Microsoft 365 workloads and has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, students will be able to:

- Describe cyber-attack threat vectors.
- Describe security solutions for Microsoft 365
- Use Microsoft Secure Score to evaluate your security posture.
- Use the Security Dashboard in the Microsoft Security & Compliance center.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Plan and deploy Mobile Device Management.

Course Outline

Module 1: Security in Microsoft 365

This module starts by explaining the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions to thwart those threats. The module finishes with an explanation of Microsoft Secure Score and how it can be used to evaluate and report your organizations security posture.

Lessons

- Threat Vectors and Data Breaches
- Security Solutions for Microsoft 365
- Microsoft Secure Score

After completing this module, students will be able to:

- Describe several techniques hackers use to compromise user accounts through email.
- Describe techniques hackers use to gain control over resources.
- List the types of threats that can be avoided by using Exhange Online Protection and Office 365 ATP.
- Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization's security officers and administrators.
- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to use the tool to identify gaps between your current state and where you would like to be with regards to security.

Module 2: Advanced Threat Protection

This module explains the various threat protection technologies and services available in Microsoft 365. Specifically, the module covers message protection through Exchange Online Protection, Azure Advanced Threat Protection and Windows Defender Advanced Threat Protection.

Lessons

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection

Lab : Advanced Threat Protection

- Setting up your lab environment
- Editing an ATP Safe Links policy and creating a Safe Attachment policy

After completing this module, students will be able to:

- Describe the anti-malware pipeline as email is analyzed by Exchange Online Protection.
- Describe how Safe Attachments is used to block zero-day malware in email attachments and documents.
- Describe how Safe Links protect users from malicious URLs embedded in email and documents that point to malicious websites.
- Configure Azure Advanced Threat Protection.
- Configure Windows Defender ATP.
- Integrate Windows Defender ATP with Azure ATP.

Module 3: Threat Intelligence

This module explains Microsoft Threat Intelligence which provides you with the tools to evaluate and address cyber threats. You will learn how to use the Security Dashboard in the Microsoft 365 Security and Compliance Center. It also explains and configures Microsoft Advanced Threat Analytics.

Lessons

- Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics

Lab : Advanced Threat Analytics

- Enabling and installing the ATA Center

After completing this module, students will be able to:

- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- Describe how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe how the Security Dashboard gives C-level executives insight into top risks, global trends, protection quality, and the organization's exposure to threats.
- Describe how the Security dashboard can be used as a launching point to enable security analysts to drill down for more details by using Threat Explorer.
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it.
- Configure Advanced Threat Analytics.

Module 4: Mobility

This module is all about securing mobile devices and applications. You will learn about Mobile Device Management and how it works with Intune. You will also learn about how Intune and Azure AD can be used to secure mobile applications.

Lessons

- Plan for Mobile Application Management
- Plan for Mobile Device Management
- Deploy Mobile Device Management
- Enroll Devices to Mobile Device Management

After completing this module, students will be able to:

- Describe mobile application considerations.
- Use Intune to manage mobile applications.
- Manage devices with MDM.
- Compare MDM for Office 365 and Intune.
- Configure Domains for MDM.
- Manage Device Security Policies.
- Define Corporate Device Enrollment Policy.
- Enroll devices to MDM.
- Configure a Device Enrollment Manager Role.

Prerequisites

Learners should start this course already having the following skills:

- Basic conceptual understanding of Microsoft Azure.
- Experience with Windows 10 devices.
- Experience with Office 365.
- Basic understanding of authorization and authentication.
- Basic understanding of computer networks.
- Working knowledge of managing mobile devices.