301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

MICROSOFT

MS-500T00: Microsoft 365 Security Administration

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Course Overview

Phoenix TS' 4-day instructor-led Microsoft 365 Security Administration training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online you will learn how to secure user access to your organization's resources. The course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to setup and use Azure AD Connect, and introduces you to conditional access in Microsoft 365. 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 to mitigate threats. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. In the course you will learn about information protection technologies that help secure your Microsoft 365 environment. The course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. This course covers data retention policies and tags, in-place records management for SharePoint, email retention, and how to conduct content searches that support eDiscovery investigations.

What You'll Learn

- Administer user and group access in Microsoft 365.
- Describe and manage Azure Identity Protection features.
- Plan and implement Azure AD Connect.
- Manage synchronized identities.
- Describe and use conditional access.
- Describe cyber-attack threat vectors.
- Describe security solutions for Microsoft 365.

- Use Microsoft Secure Score to evaluate your security posture.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Plan and deploy secure mobile devices.
- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Windows information protection for devices.
- Plan and deploy a data archiving and retention system.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.

Schedule

Currently, there are no public classes scheduled. Please contact a Phoenix TS Training Consultant to discuss hosting a private class at 301-258-8200.

Program Level

Intermediate

Training Delivery Methods

Group Live

Duration

4 Days / 32 hours Training

CPE credits

20 NASBA CPE Credits

Field of Study

Information Technology

Advanced Prep

N/A

Course Registration

Candidates can choose to register for the course by via any of the below methods:

- Email: Sales@phoenixts.com
- Phone: 301-582-8200
- Website: www.phoenixts.com

Upon registration completion candidates are sent an automated course registration email that includes attachments with specific information on the class and location as well as pre-course study and test preparation material approved by the course vendor. The text of the email contains a registration confirmation as well as the location, date, time and contact person of the class.

Online enrolment closes three days before course start date.

On the first day of class, candidates are provided with instructions to register with the exam provider before the exam date.

Complaint Resolution Policy

To view our complete Complaint Resolution Policy policy please click here: Complaint Resolution Policy

Refunds and Cancellations

To view our complete Refund and Cancellation policy please click here: Refund and Cancellation Policy

Who Should Attend

The Microsoft 365 Security administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and to 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 hybrid environments. This role has strong skills and experience with identity protection, information protection, threat

protection, security management and data governance.

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.

Exam Information

MS-500: Microsoft 365 Security Administration

Note: The content of this exam was updated on June 8, 2020.

Implement and manage identity and access	30-35%
Implement and manage threat protection	20-25%
Implement and manage information protection	15-20%
Manage governance and compliance features in Microsoft 365	20-25%

You can purchase the exam voucher separately through Phoenix TS. Phoenix TS is an authorized testing center for Pearson VUE and Prometric websites. Register for exams by calling us or visiting the Pearson VUE and Prometric websites.

Duration

4 Days

Price

$2,585

Course Outline

Module 1: User and Group Protection

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to Privileged Identity Management in Azure AD as well as Identity Protection. The module sets the foundation for the remainder of the course.

Lessons

- Identity and Access Management Concepts
- Zero Trust Security
- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365
- Azure AD Identity Protection

Lab : Initialize your trial tenant

- Set up your Microsoft 365 tenant

Lab : Configure Privileged Identity Management

- Discover and Manage Azure Resources
- Assign Directory Roles
- Activate and Deactivate PIM Roles
- Directory Roles (General)
- PIM Resource Workflows
- View audit history for Azure AD roles in PIM

After completing this module, students will be able to:

- Create and manage user accounts.
- Describe and use Microsoft 365 admin roles.
- Plan for password policies and authentication.
- Describe the concepts of Zero Trust security
- Implement multi-factor authentication in Office 365.
- Enable Azure Identity Protection

Module 2: Identity Synchronization

This module explains concepts related to synchronizing identities for Microsoft 365. Specifically, it focuses on Azure AD Connect and managing directory synchronization to ensure the right people are connecting to your Microsoft 365 system.

Lessons

- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities
- Introduction to Federated Identities

Lab : Implement Identity Synchronization

- Set up your organization for identity synchronization

After completing this module, students will be able to:

- Describe authentication options for Microsoft 365.
- Explain directory synchronization.
- Plan directory synchronization.
- Describe and use Azure AD Connect.
- Configure Azure AD Connect Prerequisites.
- Manage users and groups with directory synchronization.
- Describe Active Directory federation.

Module 3: Access Management

This module explains conditional access for Microsoft 365 and how it can be used to control access to resources in your organization. The module also explains Role Based Access Control (RBAC) and solutions for external access.

Lessons

- Conditional access
- Manage device access
- Role Based Access Control (RBAC)
- Solutions for external access

Lab : Use Conditional Access to enable MFA

- MFA Authentication Pilot (require MFA for specific apps)
- MFA Conditional Access (complete an MFA roll out)

After completing this module, students will be able to:

- Describe the concept of conditional access.
- Describe and use conditional access policies.
- Plan for device compliance.
- Configure conditional users and groups.
- Configure role based access control

Module 4: Security in Microsoft 365

This module explains the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions used to mitigate 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 strategy and principles
- Security solutions in Microsoft 365
- Microsoft Secure Score

Lab : Use Microsoft Secure Score

- Improve your secure score in the Microsoft 365 Security Center

After completing this module, students will be able to:

- Describe several techniques attackers use to compromise user accounts through email.
- Describe techniques attackers 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 the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to use Secure Score to identify gaps in your current Microsoft 365 security posture.

Module 5: Advanced Threat Protection

This module explains the various threat protection technologies and services available for Microsoft 365. 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
- Manage Safe Attachments
- Manage Safe Links

- Azure Advanced Threat Protection
- Microsoft Defender Advanced Threat Protection

Lab : Manage Microsoft 365 Security Services

- Implement ATP Policies

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
- Configure Azure Advanced Threat Protection.
- Configure Windows Defender ATP.

Module 6: Threat Management

This module explains Microsoft Threat Management which provides you with the tools to evaluate and address cyber threats and formulate responses. You will learn how to use the Security dashboard and Azure Sentinel for Microsoft 365. The module also explains and configures Microsoft Advanced Threat Analytics.

Lessons

- Use the Security dashboard
- Microsoft 365 threat investigation and response
- Azure Sentinel for Microsoft 365
- Configuring Advanced Threat Analytics

Lab : Using Attack Simulator

- Conduct a simulated Spear phishing attack
- Conduct simulated password attacks

After completing this module, students will be able to:

- 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 and trends.
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it.
- Configure Advanced Threat Analytics.
- Use the attack simulator in Microsoft 365.
- Describe how Azure Sentinel can used for Microsoft 365.

Module 7: Mobility

This module focuses on securing mobile devices and applications. You will learn about Mobile Device Management and how it works with Microsoft 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

Lab : Configure Azure AD for Intune

- Enable Device Management
- Configure Azure AD for Intune
- Create Intune Policies

After completing this module, students will be able to:

- Describe mobile application considerations.
- Use Intune to manage mobile applications.
- Manage devices with MDM.
- Configure Domains for MDM.
- Manage Device Security Policies.
- Enroll devices to MDM.
- Configure a Device Enrollment Manager Role.

Module 8: Information Protection

The module explains how to implement Azure Information Protection and Windows Information Protection.

Lessons

- Information Protection Concepts
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection

Lab : Implement Azure Information Protection and Windows Information Protection

- Implement Azure Information Protection
- Implement Windows Information Protection

After completing this module, students will be able to:

- Configure labels and policies for Azure Information Protection.
- Configure the advance AIP service settings for Rights Management Services (RMS) templates.
- Plan a deployment of Windows Information Protection policies.

Module 9: Rights Management and Encryption

This module explains information rights management in Exchange and SharePoint. The module also describes encryption technologies used to secure messages.

Lessons

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption

Lab : Configure Office 365 Message Encryption

- Configure Office 365 Message Encryption
- Validate Information Rights Management

After completing this module, students will be able to:

- Describe the various Microsoft 365 Encryption Options.
- Describe the use of S/MIME.
- Describe and enable Office 365 Message Encryption.

Module 10: Data Loss Prevention

This module focuses on data loss prevention in Microsoft 365. You will learn about how to create policies, edit rules, and customize user notifications to protect your data.

Lessons

- Data Loss Prevention Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents
- Policy Tips

Lab : Implement Data Loss Prevention policies

- Manage DLP Policies
- Test MRM and DLP Policies

After completing this module, students will be able to:

- Describe Data Loss Prevention (DLP).
- Use policy templates to implement DLP policies for commonly used information.
- Configure the correct rules for protecting content.
- Describe how to modify existing rules of DLP policies.
- Configure the user override option to a DLP rule.
- Explain how SharePoint Online creates crawled properties from documents.

Module 11: Cloud Application Security

This module focuses on cloud application security in Microsoft 365. The module will explain cloud discovery, app connectors, policies, and alerts. You will learn how these features work to secure you cloud applications.

Lessons

- Cloud App Security Explained
- Using Cloud Application Security Information

After completing this module, students will be able to:

- Describe Cloud App Security.
- Explain how to deploy Cloud App Security.
- Control your Cloud Apps with Policies.
- Use the Cloud App Catalog.
- Use the Cloud Discovery dashboard.
- Manage cloud app permissions.

Module 12: Compliance in Microsoft 365

This module focuses on data governance in Microsoft 365. The module will introduce you to Compliance Manager and discuss Global Data Protection Regulations (GDPR).

Lessons

- Plan for compliance requirements
- Build ethical walls in Exchange Online
- Manage Retention in Email
- Troubleshoot Data Governance

After completing this module, students will be able to:

- Plan security and compliance roles.
- Describe what you need to consider for GDPR.
- Describe what an ethical wall in Exchange is and how it works.
- Work with retention tags in mailboxes.

- Describe retention policies with email messages and email folders.
- Explain how the retention age of elements are calculated.
- Repair retention policies that do not operate as expected.

Module 13: Archiving and Retention

This module explains concepts related to retention and archiving of data for Microsoft 365 including Exchange and SharePoint.

Lessons

- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention policies in the Microsoft 365 Compliance Center
- Archiving and Retention in Exchange
- In-place Records Management in SharePoint

Lab : Compliance and Retention

- Initialize Compliance
- Configure retention tags and policies

After completing this module, students will be able to:

- Describe the difference between In-Place Archive and Records Management.
- Explain how data is archived in Exchange.
- Explain how a retention policy functions.
- Create a retention policy.
- Enable and disable in-place archiving.
- Create useful retention tags.

Module 14: Content Search and Investigation

This module focuses on content search and investigations. The module covers how to use eDiscovery to conduct advanced investigations of Microsoft 365 data. It also covers audit logs and discusses GDPR data subject requests.

Lessons

- Content Search
- Audit Log Investigations
- Advanced eDiscovery

Lab : Manage Search and Investigation

- Investigate your Microsoft 365 Data
- Conduct a Data Subject Request

After completing this module, students will be able to:

- Describe how to use content search.
- Design a content search.
- Configure search permission filtering.
- Configure Audit Policies.
- Enter criteria for searching the audit log.
- Describe advanced eDiscovery in Microsoft 365.
- View the advanced eDiscovery event log.

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Phoenix TS is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints re-garding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.