NETCAMPUS GROUP

unlocking potential

COURSE OUTLINE

Microsoft Solutions Partner
Security
Training Services

Course Code: AZ-500T00

Course Name: Microsoft Azure Security Technologies

DURATION	SKILL LEVEL	DELIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
4 days	Intermediate	VILT/ILT	N/A	Azure

Course Overview

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization’s security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications, and security operations.

Target Audience

This course is for Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

Job role:

Security Engineer

Exam Requirements

AZ-500

Prerequisites

- None

.

Topics

Module 1

Secure Azure solutions with Microsoft Entra ID

- 1 hr 12 min
- Module
- 15 Units

Feedback

Intermediate

Security Engineer

Azure

Microsoft Entra ID

Microsoft Entra External ID

Explore how to securely configure and administer your Microsoft Entra instance.

Learning objectives

By the end of this module, you will be able to:

- Configure Microsoft Entra ID and Microsoft Entra Domain Services for security
- Create users and groups that enable secure usage of your tenant
- Use MFA to protect user's identities
- Configure passwordless security options

Module 2:

Implement Hybrid identity

- 1 hr
- Module
- 10 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Microsoft Entra ID

Active Directory Federation Services

Microsoft Entra

Explore how to deploy and configure Microsoft Entra Connect to create a hybrid identity solution for your company.

Learning objectives

By the end of this module, you'll be able to:

- Deploy Microsoft Entra Connect
- Pick and configure that best authentication option for your security needs
- Configure password writeback

Module 3:

Deploy Microsoft Entra ID Protection

- 1 hr 40 min
- Module
- 14 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Microsoft Entra ID

Protect identities in Microsoft Entra ID using Conditional Access, MFA, access reviews, and other capabilities.

Learning objectives

By the end of this module, you will be able to:

- Deploy and configure Identity Protection

- Configure MFA for users, groups, and applications
- Create Conditional Access policies to ensure your security
- Create and follow an access review process

Module 4:

Configure Microsoft Entra Privileged Identity Management

- 11 min
- Module
- 11 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Microsoft Entra ID

Microsoft Entra

Ensure that your privileged identities have extra protection and are accessed only with the least amount of access needed to do the job.

Learning objectives

By the end of this module, you'll be able to:

- Describe Zero Trust and how it impacts security
- Configure and deploy roles using Privileged Identity Management (PIM)
- Evaluate the usefulness of each PIM setting as it relates to your security goals

Module 5:

Design an enterprise governance strategy

- 1 hr 37 min
- Module
- 14 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Microsoft Entra ID

Azure Blueprints

Azure Policy

Azure Role-based access control

Learn to use RBAC and Azure Policy to limit access to your Azure solutions, and determine which method is right for your security goals.

Learning objectives

By the end of this module, you will be able to:

- Explain the shared responsibility model and how it impacts your security configuration
- Create Azure policies to protect your solutions
- Configure and deploy access to services using RBAC

Module 6:

Implement perimeter security

- 1 hr 22 min
- Module
- 13 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure DDos Protection

Azure Firewall

Azure Firewall Manager

Azure Virtual Network

Azure VPN Gateway

Prevent attacks before they get to your Azure solutions. Use the concepts of defense in depth and zero trust to secure Azure perimeter.

Learning objectives

By the end of this module, you will be able to:

- Define defense in depth
- Protect your environment from denial-of-service attacks
- Secure your solutions using firewalls and VPNs
- Explore your end-to-end perimeter security configuration based on your security posture

Module 7:

Configure network security

- 1 hr 33 min
- Module
- 14 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure Application Gateway

Azure ExpressRoute

Azure Firewall

Azure Firewall Manager

Azure Front Door

Azure Web Application Firewall

Use Azure network capabilities to secure your network and applications from external and internal attacks.

Learning objectives

By the end of this module, you will be able to:

- Deploy and configure network security groups to protect your Azure solutions
- Configure and lockdown service endpoints and private links
- Secure your applications with Application Gateway, Web App Firewall, and Front Door
- Configure ExpressRoute to help protect your network traffic

Module 8:

Configure and manage host security

- 1 hr 53 min
- Module
- 15 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure Disk Encryption

Azure Virtual Machines

Microsoft Defender for Cloud

Microsoft Defender

Azure Update Manager

Learn to lock down the devices, virtual machines, and other components that run your applications in Azure.

Learning objectives

By the end of this module, you will be able to:

- Configure and deploy Endpoint Protection
- Deploy a privileged access strategy for devices and privileged workstations
- Secure your virtual machines and access to them
- Deploy Windows Defender
- Practice layered security by reviewing and implementing Security Center and Security Benchmarks

Module 9:

Enable Containers security

- 1 hr 23 min
- Module
- 14 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Microsoft Entra ID

Azure Container Instances

Azure Container Registry

Azure Kubernetes Service (AKS)

Microsoft Defender for Cloud

Explore how to secure your applications running within containers and how to securely connect to them.

Learning objectives

By the end of this module, you will be able to:

- Define the available security tools for containers in Azure
- Configure security settings for containers and Kubernetes services
- Lock down network, storage, and identity resources connected to your containers
- Deploy RBAC to control access to containers

Module 10:

Deploy and secure Azure Key Vault

- 1 hr 31 min
- Module
- 14 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure Key Vault

Protect your keys, certificates, and secrets in Azure Key Vault. Learn to configure key vault for the most secure deployment.

Learning objectives

By the end of this module, you will be able to:

- Define what a key vault is and how it protects certificates and secrets
- Deploy and configure Azure Key Vault
- Secure access and administration of your key vault
- Store keys and secrets in your key vault
- Explore key security considers like key rotation and backup / recovery

Module 11

Configure application security features

- 1 hr 56 min
- Module
- 15 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure App Configuration

Azure App Service

Microsoft Graph

Register your company applications then use Azure security features to configure and monitor secure access to the application.

Learning objectives

By the end of this module, you will be able to:

- Register an application in Azure using app registration
- Select and configure which Microsoft Entra users can access each application
- Configure and deploy web app certificates

Module 12

Implement storage security

- 1 hr 22 min
- Module
- 12 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure Blob Storage

Azure Disk Storage

Azure Files

Azure Storage

Azure Storage Accounts

Ensure your data is stored, transferred, and accessed in a secure way using Azure storage and file security features.

Learning objectives

By the end of this module, you will be able to:

- Define data sovereignty and how that is achieved in Azure
- Configure Azure Storage access in a secure and managed way
- Encrypt your data while it is at rest and in transit
- Apply rules for data retention

Module 13

Configure and manage SQL database security

- 2 hr
- Module
- 17 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure SQL Database

Azure SQL Managed Instance

Configure and lock down your SQL database on Azure to protect your corporate data while it's stored.

Learning objectives

By the end of this module, you'll be able to:

- Configure which users and applications have access to your SQL databases
- Block access to your servers using firewalls
- Discover, classify, and audit the use of your data
- Encrypt and protect your data while is it stored in the database.

Module 14

Configure and manage Azure Monitor

- 1 hr 3 min
- Module
- 10 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Azure Log Analytics

Azure Monitor

Use Azure Monitor, Log Analytics, and other Azure tools to monitor the secure operation of your Azure solutions.

Learning objectives

By the end of this module, you will be able to:

- Configure and monitor Azure Monitor
- Define metrics and logs you want to track for your Azure applications
- Connect data sources to and configure Log Analytics
- Create and monitor alerts associated with your solutions security

Module 15

Enable and manage Microsoft Defender for Cloud

- 2 hr 23 min
- Module
- 19 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Microsoft Defender for Cloud

Use Microsoft Defender for Cloud to strengthen security posture and protect workloads against modern threats in Azure.

Learning objectives

By the end of this module, you're able to:

- Define the most common types of cyber-attacks
- Configure Microsoft Defender for cloud based on your security posture
- Review Secure Score and raise it
- Lock down your solutions using Microsoft Defender for Cloud's workload protection
- Enable Just-in-Time access and other security features

Module 16

Configure and monitor Microsoft Sentinel

- 45 min
- Module
- 9 Units

Feedback

Intermediate

Administrator

Security Engineer

Azure

Microsoft Sentinel

Use Microsoft Sentinel to discover, track, and respond to security breaches within your Azure environment.

Learning objectives

By the end of this module, you'll be able to:

- Explain what Microsoft Sentinel is and how it is used

- Deploy Microsoft Sentinel
- Connect data to Microsoft Sentinel, like Azure Logs, Microsoft Entra ID, and others
- Track incidents using workbooks, playbooks, and hunting techniques

Exams and Certifications

A Certificate of completion is issued at the end of the Course.

Schedule your Microsoft exam here: Microsoft :: Pearson VUE

Follow on Course

Schedules | Netcampus Group