Secure cloud resources with Microsoft security technologies

Category: Networking & Security | **Vendor:** Microsoft

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Related Exam: AZ-500

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.

You could also consider the below Applied Skills courses to provide real-world experience for security tasks covered in the AZ-500 course:

- Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls (SC-5002)
- Secure storage for Azure Files and Azure Blob Storage (AZ-1003)

About This Course

Module 1: Manage Identity and Access

This module covers Azure Active Directory, Azure Identity Protection, Enterprise Governance, Azure AD PIM, and Hybrid Identity.

Lessons

- Azure Active Directory
- Azure Identity Protection
- Enterprise Governance
- Azure AD Privileged Identity Management
- Hybrid Identity
- Lab: Role-Based Access Control
- Lab: Azure Policy
- Lab: Resource Manager Locks
- Lab: MFA, Conditional Access and AAD Identity Protection
- Lab: Azure AD Privileged Identity Management
- Lab: Implement Directory Synchronization

After completing this module, students will be able to:

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.

Module 2: Implement Platform Protection

This module covers perimeter, network, host, and container security.

Lessons

- Perimeter Security
- Network Security
- Host Security
- Container Security
- Lab: Network Security Groups and Application Security Groups
- Lab: Azure Firewall
- Lab: Configuring and Securing ACR and AKS

After completing this module, students will be able to:

- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.

Module 3: Secure Data and Applications

This module covers Azure Key Vault, application security, storage security, and SQL database security.

Lessons

- Azure Key Vault
- Application Security
- Storage Security
- SQL Database Security
- Lab: Key Vault (Implementing Secure Data by setting up Always Encrypted)
- Lab: Securing Azure SQL Database
- Lab: Service Endpoints and Securing Storage

After completing this module, students will be able to:

- Implement Azure Key Vault including certificates, keys, and secretes.

- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.

Module 4: Manage Security Operations

This module covers Azure Monitor, Azure Security Center, and Azure Sentinel.

Lessons

- Azure Monitor
- Azure Security Center
- Azure Sentinel
- Lab: Azure Monitor
- Lab: Azure Security Center
- Lab: Azure Sentinel

After completing this module, students will be able to:

- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

Who Should Attend

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.

Prerequisites & Entry Requirements

General Prerequisites:

Successful learners will have prior knowledge and understanding of:

- Security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model.
- Be familiar with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
- Have experience with Windows and Linux operating systems and scripting languages. Course labs may use PowerShell and the CLI.

Prior attendance of the course Microsoft Azure Administrator (AZ-104T00) is recommended.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.
- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.
- Implement Azure Key Vault including certificates, keys, and secretes.
- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.
- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

Detailed Course Outline

Protect identity and access in Azure: Manage security controls for identity and access; Manage Microsoft Entra application access | Protect network infrastructure in Azure: Plan and implement

security for virtual networks; Plan and implement security for private access to Azure resources; Plan and implement security for public access to Azure resources | Protect compute, storage, and databases: Plan and implement advanced security for compute; Plan and implement security for storage; Plan and implement security for Azure SQL Database and Azure SQL Managed Instance | Strengthen security posture using Microsoft Defender for Cloud and Microsoft Sentinel: Implement and manage enforcement of cloud governance policies; Manage security posture by using Microsoft Defender for Cloud; Configure and manage threat protection by using Microsoft Defender for Cloud; Configure and manage security monitoring and automation solutions

Skills You Will Learn:

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.
- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.
- Implement Azure Key Vault including certificates, keys, and secretes.
- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.
- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

Frequently Asked Questions

Q: What delivery options are available for Secure cloud resources with Microsoft security technologies?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: Which exam does this course prepare me for?

This course prepares you for the AZ-500 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 4-day Secure cloud resources with Microsoft security technologies course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Secure cloud resources with Microsoft security technologies training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Secure cloud resources with Microsoft security technologies?

Yes, we provide corporate training, dedicated training, and closed classes for Secure cloud resources with Microsoft security technologies. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Secure cloud resources with Microsoft security technologies, Security, AZ-500T00

Q: Why choose Nexus Human for Secure cloud resources with Microsoft security technologies?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Secure cloud resources with Microsoft security technologies training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)