Hexadigitall Technologies

https://hexadigitall.com

Scan to open this course page, enroll, and access live updates.

Course Snapshot

Secure Azure infrastructure with hands-on labs, identity protection, and real-world SOC automation projects.

Azure Security Technologies

Microsoft Certified: Azure Security Engineer Associate (AZ-500)

Duration: 16 Weeks

Level: Advanced

Study Time: 2 hours/week + Labs

School: Cybersecurity

Welcome to Your Azure Security Journey! 🎓

Congratulations on taking the first step towards becoming a Microsoft Certified Azure Security Engineer! This comprehensive 16-week program is designed to equip you with the essential skills and knowledge needed to secure Azure cloud infrastructure, implement security controls, and prepare for the AZ-500 certification exam.

Throughout this course, you'll master identity and access management, platform protection, security operations, and data & application security in Azure. You'll gain hands-on experience with real-world scenarios, lab exercises, and industry-standard security practices.

Your success is our priority. We've carefully structured this curriculum to balance theoretical knowledge with practical application, ensuring you're not just exam-ready, but career-ready.

Prerequisites & What You Should Know

Before Starting This Course

- ✓ Basic understanding of Azure fundamentals (compute, storage, networking)
- ✓ Familiarity with Azure portal and Azure CLI
- ✓ Understanding of networking concepts (DNS, VPN, firewalls)
- ✓ Basic knowledge of Windows Server and Linux administration
- ✓ Understanding of identity concepts (authentication, authorization)
- ✓ Familiarity with PowerShell and basic scripting
- ✓ Understanding of encryption and cryptography basics

💡 Recommended Foundation:

If you're new to Azure, we strongly recommend completing "Azure Fundamentals (AZ-900)" or having 6-12 months of hands-on experience with Azure before starting this advanced security course.

Recommended Complementary Courses

Cybersecurity Fundamentals

Strengthen your security foundation with network and systems defense fundamentals.

DevSecOps Engineering

Learn to automate security in CI/CD pipelines and integrate security into DevOps workflows.

Enterprise Cloud Solutions Architect

Understand enterprise architecture patterns and cloud solution design.

Network Security Administration

Deepen your network security knowledge with advanced administration techniques.

Essential Learning Resources

📚 Free Resources

Microsoft Learn - AZ-500

learn.microsoft.com/certifications/az-500 FREE

Azure Security Documentation

learn.microsoft.com/azure/security FREE

Azure Security Benchmark

learn.microsoft.com/security/benchmark/azure FREE

Azure Architecture Center

learn.microsoft.com/azure/architecture FREE

💎 Recommended Paid Resources

Pluralsight - Azure Security Path

pluralsight.com/paths/az-500 PAID

A Cloud Guru - AZ-500 Course

acloudguru.com/az-500 PAID

Udemy - AZ-500 Complete Course

udemy.com/topic/az-500 PAID

MeasureUp Practice Tests

measureup.com/az-500 PAID

Your Learning Roadmap

Phase 1: Foundation (Weeks 1-4)

Build your security foundation with Azure AD, RBAC, and identity management essentials.

Phase 2: Platform Security (Weeks 5-8)

Master network security, perimeter protection, and compute/container security.

Phase 3: Security Operations (Weeks 9-12)

Learn monitoring, threat detection, incident response, and Azure security tools.

Phase 4: Data & Apps (Weeks 13-14)

Secure data at rest and in transit, implement application security, and manage Key Vault.

Phase 5: Exam Prep (Weeks 15-16)

Review, practice exams, hands-on labs, and final certification preparation.

Detailed Weekly Curriculum

Week 1

2 hours

Azure Active Directory & Identity Management Fundamentals

→ Azure AD architecture and components

→ User and group management

→ Azure AD Connect and hybrid identity

→ Self-service password reset (SSPR)

→ Azure AD Domain Services

🔬 **Lab Exercise**

→ Create and configure Azure AD tenant

→ Manage users, groups, and administrative units

→ Configure SSPR and password policies

Week 2

2 hours

Advanced Identity Protection & Multi-Factor Authentication

→ Azure AD Multi-Factor Authentication (MFA)

→ Conditional Access policies

→ Azure AD Identity Protection

→ Risk-based authentication

→ Privileged Identity Management (PIM) introduction

🔬 **Lab Exercise**

→ Configure and test Azure MFA

→ Create Conditional Access policies

→ Enable and configure Identity Protection

Week 3

2 hours

Role-Based Access Control (RBAC) & Access Management

→ Azure RBAC fundamentals and best practices

→ Built-in and custom roles

→ Resource and management group scopes

→ Azure role assignments and inheritance

→ Deny assignments and ABAC (Attribute-Based Access Control)

🔬 Lab Exercise

→ Assign built-in RBAC roles

→ Create custom RBAC roles

→ Audit and review role assignments

Week 4

2 hours

Privileged Identity Management (PIM) & Governance

→ PIM for Azure AD roles

→ PIM for Azure resources

→ Just-in-time (JIT) access

→ Access reviews and approvals

→ PIM alerts and notifications

🔬 Lab Exercise

→ Configure PIM for privileged roles

→ Request and approve JIT access

→ Conduct access reviews

Week 5

2 hours

Azure Network Security Fundamentals

→ Virtual Network (VNet) security

→ Network Security Groups (NSGs)

→ Application Security Groups (ASGs)

→ Azure Bastion for secure VM access

→ Network segmentation strategies

🔬 Lab Exercise

→ Create and configure NSGs

→ Implement ASGs for application tiers

→ Deploy Azure Bastion

Week 6

2 hours

Perimeter Security & Azure Firewall

→ Azure Firewall architecture and features

→ Firewall rules and policies

→ Application and network rules

→ Azure DDoS Protection

→ Azure Front Door and Web Application Firewall (WAF)

🔬 Lab Exercise

→ Deploy and configure Azure Firewall

→ Create firewall rules and policies

→ Enable Azure DDoS Protection

Week 7

2 hours

Compute & Container Security

- → Azure VM security best practices
- → VM disk encryption and secure boot
- → Update management and patch compliance
- → Azure Kubernetes Service (AKS) security
- → Container security and Azure Container Registry

🔬 Lab Exercise

- → Enable disk encryption on VMs
- → Configure Azure Update Management
- → Secure AKS cluster and implement pod security

Week 8

2 hours

Azure Security Center & Defender for Cloud

- → Microsoft Defender for Cloud overview
- → Secure Score and recommendations
- → Regulatory compliance dashboard
- → Defender plans (Servers, Storage, SQL, etc.)
- → Adaptive application controls and network hardening

🔬 Lab Exercise

- → Enable Defender for Cloud
- → Review and remediate Secure Score recommendations
- → Configure adaptive controls

Week 9

2 hours

Azure Monitor & Log Analytics

→ Azure Monitor architecture

→ Log Analytics workspace configuration

→ KQL (Kusto Query Language) fundamentals

→ Diagnostic settings and data collection

→ Activity logs and resource logs

🔬 Lab Exercise

→ Create Log Analytics workspace

→ Write KQL queries for security analysis

→ Configure diagnostic settings

Week 10

2 hours

Azure Sentinel (Microsoft Sentinel)

→ Microsoft Sentinel overview and architecture

→ Data connectors and ingestion

→ Analytics rules and threat detection

→ Workbooks and visualization

→ Investigation and hunting queries

🔬 Lab Exercise

→ Deploy Microsoft Sentinel

→ Configure data connectors

→ Create analytics rules and incidents

Week 11

2 hours

Threat Detection & Incident Response

→ Security incidents and alerts

→ Incident response workflow

→ Automation and playbooks (Logic Apps)

→ SOAR (Security Orchestration, Automation, and Response)

→ Threat intelligence integration

🔬 Lab Exercise

→ Investigate security incidents

→ Create automation playbooks

→ Implement threat intelligence feeds

Week 12

2 hours

Compliance & Governance

→ Azure Policy and initiatives

→ Compliance standards (ISO, GDPR, HIPAA, etc.)

→ Azure Blueprints

→ Resource locks and tags

→ Audit and compliance reporting

🔬 Lab Exercise

→ Create and assign Azure Policies

→ Deploy Azure Blueprints

→ Generate compliance reports

Week 13

2 hours

Azure Key Vault & Secrets Management

- Key Vault architecture and access models
- Keys, secrets, and certificates management
- Managed identities for Azure resources
- Key rotation and lifecycle management
- Key Vault monitoring and logging

🔬 Lab Exercise

- Create and configure Azure Key Vault
- Store and retrieve secrets
- Implement managed identities

Week 14

2 hours

Data Security & Application Protection

- Azure Storage security (encryption at rest and in transit)
- Azure SQL Database security features
- Data classification and Azure Information Protection
- Application security best practices
- API security and Azure API Management

🔬 Lab Exercise

- Configure storage encryption and access policies
- Implement SQL Database security features
- Set up Azure Information Protection

Week 15

2 hours

Comprehensive Review & Practice Scenarios

→ Review all exam objectives and domains

→ Practice exam questions and scenarios

→ Common exam topics and patterns

→ Hands-on scenario walkthroughs

→ Identifying knowledge gaps

🔬 Lab Exercise

→ Complete full-length practice exam

→ Hands-on troubleshooting scenarios

→ Review incorrect answers and concepts

Week 16

2 hours

Final Preparation & Exam Readiness

→ Final practice exams and scoring analysis

→ Exam day strategies and tips

→ Time management techniques

→ Final Q&A and doubt clarification

→ Certification registration and scheduling

🔬 Lab Exercise

→ Take final full-length practice exam

→ Review performance analytics

→ Schedule your AZ-500 certification exam

Capstone Projects

Project 1: Enterprise Azure Security Architecture

Design and implement a comprehensive security architecture for a fictional enterprise migrating to Azure. This includes identity management, network security, monitoring, and compliance controls.

Objectives:

- Design multi-region Azure AD architecture
- Implement Conditional Access and PIM
- Configure network security with Azure Firewall
- Set up Microsoft Sentinel for monitoring
- Ensure compliance with industry standards

Project 2: Security Operations Center (SOC) Automation

Build an automated security operations workflow using Microsoft Sentinel, Logic Apps, and Azure Automation to detect, respond, and remediate security incidents.

Objectives:

- Configure Sentinel data connectors and analytics rules
- Create automated incident response playbooks
- Implement threat hunting queries
- Build custom workbooks for visualization
- Document incident response procedures

Project 3: Zero Trust Security Implementation

Implement a Zero Trust security model for an Azure environment, focusing on identity verification, least privilege access, and continuous validation.

Objectives:

- Design Zero Trust network architecture
- Implement identity-driven security controls
- Configure JIT VM access and Bastion
- Set up continuous monitoring and validation
- Document security policies and procedures

Study Tips for Success

- ✓ Dedicate consistent study time (minimum 2 hours/week + lab practice)
- ✓ Use Microsoft Learn modules to supplement each week's topics
- ✓ Practice with Azure free tier and trial accounts for hands-on experience
- ✓ Join Azure community forums and study groups
- ✓ Take notes and create your own reference documentation
- ✓ Focus on understanding concepts, not just memorizing answers
- ✓ Review exam skills outline regularly
- ✓ Schedule your exam 2-3 weeks in advance to create accountability
- ✓ Take at least 3 full-length practice exams before the real exam
- ✓ Get adequate rest before exam day

About the AZ-500 Certification

Exam Details

Exam Code AZ-500	**Duration** 100 minutes
Question Format 40-60 questions (Multiple choice, case studies, labs)	**Passing Score** 700/1000
Cost $165 USD	**Validity** 1 year (requires renewal)

📝 Exam Domains Distribution:

- Manage Identity and Access (30-35%)
- Secure Networking (20-25%)
- Secure Compute, Storage, and Databases (20-25%)
- Manage Security Operations (25-30%)

Ready to Begin Your Journey?

We're excited to be part of your Azure Security certification journey!

Remember: Consistency is key. Stay committed, practice regularly, and don't hesitate to reach out for support.

Best of luck! 🚀