AZ-500T00 Microsoft Azure Security Technologies

Summary

Length: 32 hours Level: Experienced

In this course students will gain the knowledge and skills needed to implement security controls, maintain the security posture, and identify and remediate vulnerabilities by using a variety of security tools. The course covers scripting and automation, virtualization, and cloud N-tier architecture. This course may earn a Credly Badge.

Learning Objectives

After completing this course, students will be able to:
Describe specialized data classifications on Azure
Identify Azure data protection mechanisms
Implement Azure data encryption methods
Secure Internet protocols and how to implement them on Azure
Describe Azure security services and features

Course Outline

1. Identity and Access

   Configure Azure Active Directory for Azure workloads and subscriptions
   Configure Azure AD Privileged Identity Management
   Configure security for an Azure subscription

2. Platform Protection

   Understand cloud security
   Build a network
   Secure network
   Implement host security
   Implement platform security
   Implement subscription security

3. Security Operations

   Configure security services
   Configure security policies by using Azure Security Center
   Manage security alerts
   Respond to and remediate security issues
   Create security baselines

4. Data and applications

   Configure security policies to manage data
   Configure security for data infrastructure
   Configure encryption for data at rest
   Understand application security
   Implement security for application lifecycle
   Secure applications
   Configure and manage Azure Key Vault

Audience

Students should have at least one year of hands-on experience securing Azure workloads and experience with security controls for workloads on Azure.

Prerequisites

Before attending this course, students must have knowledge of: Microsoft Azure Administrator Associate