Secure cloud resources with Microsoft security technologies (AZ-500T00)

ID AZ-500T00 **Preis** CHF 3'380.– (exkl. MwSt.) **Dauer** 4 Tage

Zielgruppe

Dieser Kurs richtet sich an Azure Security Engineers, die die zugehörige Zertifizierungsprüfung ablegen möchten oder bei ihrer täglichen Arbeit Sicherheitsaufgaben ausführen. Dieser Kurs ist auch für Ingenieure hilfreich, die sich auf die Bereitstellung von Sicherheit für Azure-basierte digitale Plattformen spezialisieren und eine wichtige Rolle beim Schutz der Daten eines Unternehmens spielen möchten.

Empfohlenes Training für die Zertifizierung zum

Microsoft Certified: Azure Security Engineer Associate (MCASEA)

Voraussetzungen

Erfolgreiche Teilnehmer verfügen über Vorkenntnisse und Verständnis für:

- Verständnis bewährter Sicherheitsmethoden und Branchensicherheitsanforderungen, z. B. tiefgehende Verteidigung (Defense in Depth), Zugriff mit geringstmöglichen Berechtigungen, rollenbasierte Zugriffssteuerung, mehrstufige Authentifizierung, gemeinsame Verantwortung und Zero Trust-Modell
- Vertrautheit mit Sicherheitsprotokollen wie VPN (Virtual Private Networks), IPsec (Internet Security Protocol), SSL (Secure Socket Layer), Datenträger- und Datenverschlüsselungsmethoden
- Erfahrungen mit der Bereitstellung von Azure-Workloads. Dieser Kurs behandelt nicht die Grundlagen der Azure-Verwaltung, sondern der Kursinhalt baut auf diesem Wissen auf und vermittelt weitere sicherheitsspezifische Informationen.
- Erfahrung mit Windows- und Linux-Betriebssystemen und Skriptsprachen Kurslabs können PowerShell und die CLI verwenden.

Die vorherige Teilnahme am Kurs Microsoft Azure Administrator (AZ-104T00) wird empfohlen.

Kursziele

- Implementieren Sie Governance-Unternehmesstrategien, einschliesslich rollenbasierter Zugriffssteuerung, Azure-Richtlinien und Ressourcensperren.
- Implementieren Sie eine Azure AD-Infrastruktur mit Benutzern, Gruppen und Multi-Faktor-Authentifizierung.
- Implementieren Sie den Azure AD-Identitätsschutz, einschliesslich Risikorichtlinien, bedingtem Zugriff und Zugriffsüberprüfungen.
- Implementieren Sie die Verwaltung privilegierter Azure AD-Identitäten, einschliesslich Azure AD-Rollen und Azure-Ressourcen.
- Implementieren Sie Azure AD Connect einschliesslich Authentifizierungsmethoden und lokaler Verzeichnissynchronisierung.
- Implementieren Sie Perimeter-Sicherheitsstrategien, einschliesslich Azure Firewall.
- Implementieren Sie Netzwerksicherheitsstrategien, einschliesslich Netzwerksicherheitsgruppen und Anwendungssicherheitsgruppen.
- Implementieren Sie Host-Sicherheitsstrategien, einschliesslich Endpunktschutz, RAS-Verwaltung, Update-Verwaltung und Festplattenverschlüsselung.
- Implementieren Sie Containersicherheitsstrategien, einschliesslich Azure Container-Instanzen, Azure Container-Register und Azure Kubernetes.
- Implementieren Sie Azure Key Vault, einschliesslich Zertifikaten, Schlüsseln und Geheimnissen.
- Implementieren Sie Anwendungssicherheitsstrategien, einschliesslich App-Registrierung, verwaltete Identitäten und Service-Endpunkte.
- Implementieren Sie Speichersicherheitsstrategien, einschliesslich gemeinsam genutzter Zugriffssignaturen, Blob-Aufbewahrungsrichtlinien und Azure Dateien-Authentifizierung.
- Implementieren Sie Datenbanksicherheitsstrategien, einschliesslich Authentifizierung, Datenklassifizierung, dynamische Datenmaskierung, und das immer verschlüsselt.
- Implementieren Sie Azure Monitor, einschliesslich verbundener Quellen, Protokollanalysen und Warnungen.
- Implementieren Sie Azure Security Center. einschliesslich Richtlinien, Empfehlungen und Just-in-Time-Zugriff auf virtuelle Maschinen.

- Implementieren Sie Azure Sentinel, einschliesslich Arbeitsmappen, Ereignissen und Wiedergabebüchern.

Kursinhalt

Modul 1: Verwalten von Identität und Zugriff

Dieses Modul behandelt Azure Active Directory, Azure Identity Protection, Unternehmensverwaltung, Azure AD PIM und hybride Identität.

Lektionen

- Azure Active Directory
- Azure Identity Protection
- Governance in Unternehmen
- Azure AD Privileged Identity Management
- Hybrididentität
- Lab: Rollenbasierte Zugriffssteuerung
- Lab: Azure Policy
- Lab: Resource Manager-Sperren
- Lab: MFA, bedingter Zugriff und AAD-Identitätsschutz
- Lab: Azure AD Privileged Identity Management
- Lab: Implementieren der Verzeichnissynchronisierung

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Governance-Unternehmensstrategien, einschliesslich rollenbasierter Zugriffssteuerung, Azure-Richtlinien und Ressourcensperren.
- Implementieren Sie eine Azure AD-Infrastruktur mit Benutzern, Gruppen und Multi-Faktor-Authentifizierung.
- Implementieren Sie den Azure AD-Identitätsschutz, einschliesslich Risikorichtlinien, bedingtem Zugriff und Zugriffsüberprüfungen.
- Implementieren Sie die Verwaltung privilegierter Azure AD-Identitäten, einschliesslich Azure AD-Rollen und Azure-Ressourcen.
- Implementieren Sie Azure AD Connect einschliesslich Authentifizierungsmethoden und lokaler Verzeichnissynchronisierung.

Modul 2: Implementieren des Plattformschutzes

Dieses Modul behandelt die Perimeter-, Netzwerk-, Host- und Containersicherheit.

Lektionen

- Umgebungssicherheit
- Netzwerksicherheit
- Hostsicherheit
- Containersicherheit
- Lab: Netzwerksicherheitsgruppen und Anwendungssicherheitsgruppen
- Lab: Azure Firewall
- Lab: Konfigurieren und Schützen von ACR und AKS

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Perimeter-Sicherheitsstrategien, einschliesslich Azure Firewall.
- Implementieren Sie Netzwerksicherheitsstrategien, einschliesslich Netzwerksicherheitsgruppen und Anwendungssicherheitsgruppen.
- Implementieren Sie Host-Sicherheitsstrategien, einschliesslich Endpunktschutz, RAS-Verwaltung, Update-Verwaltung und Festplattenverschlüsselung.
- Implementieren Sie Containersicherheitsstrategien, einschliesslich Azure Container-Instanzen, Azure Container-Register und Azure Kubernetes.

Modul 3: Schützen von Daten und Anwendungen

Dieses Modul behandelt Azure Key Vault, Anwendungssicherheit, Speichersicherheit und SQL-Datenbanksicherheit.

Lektionen

- Azure-Schlüsseltresor
- Anwendungssicherheit
- Speichersicherheit
- SQL-Datenbank-Sicherheit
- Lab: Key Vault (Implementieren sicherer Daten durch Einrichten von „Always Encrypted“)
- Lab: Schützen von Azure SQL-Datenbank
- Lab: Dienstendpunkte und Schützen von Speicher

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Azure Key Vault, einschliesslich Zertifikaten, Schlüsseln und Geheimnissen.
- Implementieren Sie Anwendungssicherheitsstrategien, einschliesslich App-Registrierung, verwaltete Identitäten und Service-Endpunkte.
- Implementieren Sie Speichersicherheitsstrategien, einschliesslich gemeinsam genutzter Zugriffssignaturen, Blob-Aufbewahrungsrichtlinien und Azure Dateien-Authentifizierung.
- Implementieren Sie Datenbanksicherheitsstrategien, einschliesslich Authentifizierung, Datenklassifizierung, dynamische Datenmaskierung, und das immer verschlüsselt.

Modul 4: Verwalten von Sicherheitsvorgängen

Dieses Modul behandelt Azure Monitor, Azure Security Center und Azure Sentinel.

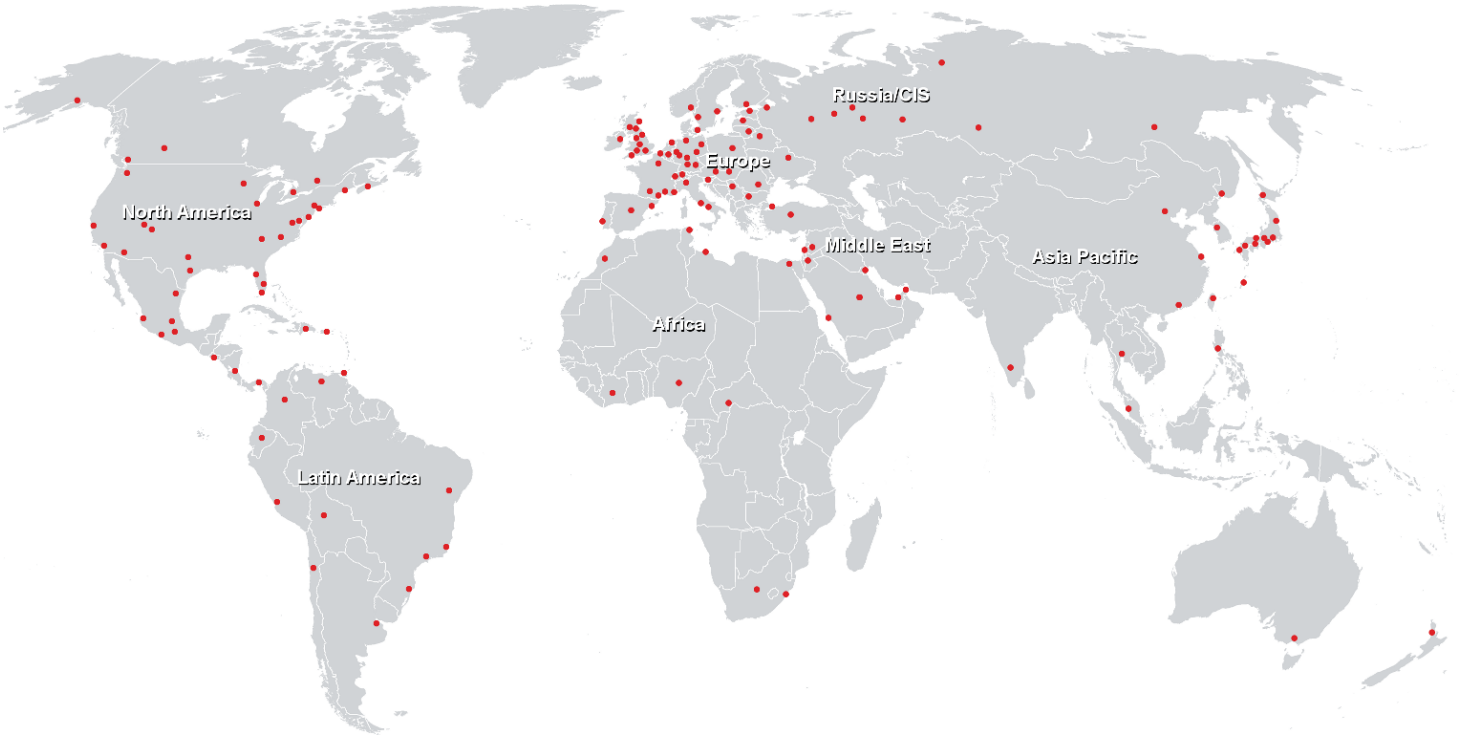
Lektionen

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

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Azure Monitor, einschliesslich verbundener Quellen, Protokollanalysen und Warnungen.
- Implementieren Sie Azure Security Center. einschliesslich Richtlinien, Empfehlungen und Just-in-Time-Zugriff auf virtuelle Maschinen.
- Implementieren Sie Azure Sentinel, einschliesslich Arbeitsmappen, Ereignissen und Wiedergabebüchern.

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch