



CT-500 Microsoft 365 Security für Administratoren

In diesem Kurs (früher MS-500) erfahren Sie, wie Sie den Benutzerzugriff auf die Ressourcen Ihrer Organisation sichern können. Der Kurs behandelt den Schutz von Benutzerpasswörtern, Multi-Faktor-Authentifizierung, die Aktivierung von Azure Identity Protection, die Einrichtung und Verwendung von Azure AD Connect und führt Sie in die Zugangskontrolle in Microsoft 365 ein.

Sie lernen die Technologien zum Schutz vor Bedrohungen kennen, die zum Schutz Ihrer Microsoft 365-Umgebung beitragen. Insbesondere erfahren Sie etwas über Bedrohungsvektoren und die Sicherheitslösungen von Microsoft zur Eindämmung von Bedrohungen. Sie erfahren mehr über Secure Score, Exchange-Online-Schutz, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection und Bedrohungsverwaltung.

Listenpreis

2.190,00 € exkl. MwSt

2.606,10 € inkl. MwSt

Dauer

4 Tage

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin



Gabriela Bücherl
Geschäftsführung
Vertrieb

Kontakt/Fragen:

g.buecherl@cbt-training.de

Telefon: +49 (0)89-4576918-16

Inhalte

- **Benutzer- und Gruppenverwaltung**
 - Identitäts- und Zugriffsmanagementkonzepte
 - Das Zero Trust-Modell
 - Identitäts- und Authentifizierungslösungen planen
 - Benutzerkonten und Rollen
 - Passwort-Verwaltung
- **Synchronisation und Schutz von Identitäten**
 - Planen der Verzeichnissynchronisierung
 - Konfigurieren und verwalten von synchronisierten Identitäten
 - Azure AD-Identitätsschutz
- **Identitäts- und Zugriffsverwaltung**
 - Anwendungsmanagement
 - Identitätsmanagement
 - Verwalten des Gerätezugriffs
 - Rollenbasierte Zugriffskontrolle (RBAC)
 - Lösungen für den externen Zugriff
 - Privilegierte Identitätsverwaltung
- **Sicherheit in Microsoft 365**
 - Bedrohungsvektoren und Datenverletzungen
 - Sicherheitsstrategie und -prinzipien
 - Microsoft Sicherheitslösungen
 - Secure Score
- **Threat Protection (ATP)**
 - Exchange-Online-Protection
 - Microsoft Defender für Office 365
 - Verwalten sicherer Anhänge

Kursinformationen



- Verwalten sicherer Links
- Microsoft Defender für Identität
- Microsoft Defender für Endpoint
- **Threat Management**
 - Microsoft Sentinel
 - Security Dashboard
 - Threat investigation and response
 - Advanced Threat Analytics
- **Microsoft Cloud Application Security**
 - Bereitstellen der Cloud-Anwendungssicherheit
 - Verwenden Sie Sicherheitsinformationen für Cloud-Anwendungen
- **Mobile Geräteverwaltung (MDM)**
 - Mobile Application Management (MAM)
 - Mobile Device Management (MDM)
 - Bereitstellen von Services für mobile Geräte
 - Registrieren von Geräten für die Verwaltung mobiler Geräte
- **Informationsschutz und Governance**
 - Konzepte zum Informationsschutz
 - Governance und Records Management
 - Sensibilitätskennzeichnungen
 - Archivierung in Microsoft 365
 - Aufbewahrung in Microsoft 365
 - Aufbewahrungsrichtlinien im Microsoft 365 Compliance Center
 - Archivierung und Aufbewahrung in Exchange
 - In-Place Records Management in SharePoint
- **Rechteverwaltung und Verschlüsselung**
 - Secure Multipurpose Internet Mail Extension (S-MIME)
 - Office 365 Message Encryption
- **Verhinderung von Datenverlust**
 - Information Rights Management (IRM)
 - Secure Multipurpose Internet Mail Extension (S-MIME)
 - Office 365 Message Encryption
- **Verhinderung von Datenverlust**
 - Richtlinien zum Schutz vor Datenverlust
 - Erstellen einer DLP-Richtlinie
 - Anpassen einer DLP-Richtlinie
 - Erstellen einer DLP-Richtlinie zum Schutz von Dokumenten
- **Compliance Management**
 - Compliance Center
- **Insider -Risikomanagement**
 - Insider Risk
 - Privileged Access
 - Informationsbarrieren
 - Aufbau von Ethical-Walls in Exchange Online
- **Verwalten der elektronischen Suche und Recherche**
 - Audit Log Untersuchungen



Ziele

Weiterhin erfahren Sie in diesem Kurs mehr über Informationsschutztechnologien, mit denen Sie Ihre Microsoft 365-Umgebung schützen können. Insbesondere lernen Sie Bedrohungsvektoren und die Sicherheitslösungen von Microsoft kennen, um Bedrohungen zu mindern.

Sie erhalten Informationen zu Secure Score, Exchange Online-Schutz, Azure Advanced Threat Protection und Windows Defender Advanced Threat Protection sowie zur Verwendung von Threat Management.

In diesem Kurs werden speziell mit Informationsrechten verwaltete Inhalte, Nachrichtenverschlüsselung sowie Beschriftungen, Richtlinien und Regeln behandelt, die die Verhinderung von Datenverlust und den Schutz von Informationen unterstützen. Sie lernen die Archivierung und Aufbewahrung in Microsoft 365 sowie die Datenverwaltung und das Durchführen von Inhaltssuchen und -untersuchungen. Dieser Kurs behandelt Richtlinien und Tags zur Vorratsdatenspeicherung, die direkte Verwaltung von Datensätzen für SharePoint, die Aufbewahrung von E-Mails und die Durchführung von Inhaltssuchen, die eDiscovery-Untersuchungen unterstützen.

Zielgruppe

Sicherheitsexperte und Netzwerk-Administratoren, die Sicherheits- und Compliance-Lösungen für Microsoft 365 und hybride Umgebungen implementieren, verwalten und überwachen.

Voraussetzungen

- Grundlegendes konzeptionelles Verständnis von Microsoft Azure.
- Erfahrung mit Windows 10/11-Geräten.
- Erfahrung mit Microsoft 365.
- Grundlegendes Verständnis von Autorisierung und Authentifizierung.
- Grundlegendes Verständnis von Computernetzwerken.
- Grundkenntnisse in der Verwaltung mobiler Geräte.