



Microsoft Defender for Endpoint (Client Security) AD483

Durch den aktuell stattfindenden Wandel hin zum mobilen Arbeiten, wird es immer wichtiger mobile Geräte effektiv gegen Angriffe und andere Bedrohungen zu schützen. Dieser Schutz muss jederzeit gewährleistet, überwacht und konfiguriert werden können. Der Microsoft Defender for Endpoint bietet Ihnen die Möglichkeit all diese Funktionen innerhalb einer Lösung zusammenzufassen. Durch die in Windows 10/11 enthaltenen Endpunktverhaltenssensoren, wird das Verhalten des Betriebssystems analysiert und die gesammelten Daten automatisiert an eine private, isolierte Cloud-Instanz von Microsoft Defender for Endpoint übermittelt. In dieser werden die Daten durch die Cloud-Sicherheitsanalyse verarbeitet. Hierfür kommen Konzepte wie Big Data und sogenanntes Geräte-Learning zum Einsatz. Aus diesen Analysen lassen sich dann mögliche Bedrohungen und Reaktionen auf diese ableiten. Ein weiterer wichtiger Bestandteil ist die integrierte Threat Intelligence. Welche gefüllt durch Microsofts Sicherheitsteams und Partner eine schnellstmögliche Identifizierung von Angriffen ermöglicht. Zudem besteht die Möglichkeit Defender for Endpoint in weitere Microsoft-Lösungen wie Intune oder Microsoft Sentinel zu integrieren und über eine zentrale Oberfläche zu verwalten.

Listenpreis

1.750,00 € exkl. MwSt

2.082,50 € inkl. MwSt

Dauer

2 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

- **Microsoft Defender for Endpoint im Überblick**
 - Was ist MS Defender for Endpoint
 - Datenspeicherung und Datenschutz
 - Defender Security Center
 - Endpunktverhaltenssensoren
 - Cloud-Sicherheitsanalyse
 - Threat Intelligence
- **Kernfunktionen**
 - Bedrohungs- und Sicherheitsrisikomanagement
 - Angriffsflächen reduzieren
 - Next generation protection
 - Endpunkterkennung und -reaktion
 - Microsoft Threat Experts
 - Verwaltung & APIs
- **Administrierung**
 - Onboarding
 - Zugriffsverwaltung
 - Sicherheitskonfiguration
 - Reporting
 - SIEM Integration
- **Erkennen von Bedrohungen**
 - Bedrohungsanalyse
 - Erkennung am Endpunkt



- Sicherheits Dashboard
- Erweiterte Suche (Kusto-Abfragen)
- Möglichkeiten zur Automatisierung
- **Umgang mit Bedrohungen**
 - Reaktion auf Geräten
 - Reaktion auf Dateien
 - Verwalten von Alarmen
- **Integration anderer Microsoft-Lösungen**
 - Microsoft Defender for Cloud
 - Intune
 - Microsoft Sentinel
 - Configuration Manager

Ziele

In diesem Seminar lernen Sie den Windows Defender im Detail kennen und lernen, wie Sie diesen in der Praxis effektiv und zielgerichtet einsetzen können. Im Seminar arbeiten Sie gemeinsam mit unserem projekterfahrenen Trainer in einer Test-Umgebung um das erlernte Wissen sofort in der Praxis anwenden zu können.

Zielgruppe

Dieses Training richtet sich an Administratoren und IT-Professionals, die Windows Defender im Detail kennenlernen und ihr KnowHow vertiefen möchten, um eine Implementierung durchzuführen und die Administration übernehmen zu können.