

Trend Micro Vision One XDR Training for Certified Professionals

Die Teilnehmer lernen, wie sie die Funktionen von Trend Micro Vision One für erweiterte Detection Response (XDR) Aktivitäten nutzen können. Dieser Kurs beschreibt einige der Konzepte im Zusammenhang mit erweiterter Erkennung und Reaktion. In den Lektionen des Kurses wird erläutert, wie Trend Micro und Produkte von Drittanbietern mit Trend Micro Vision One verbunden werden, wie XDR-Sensoren auf Geräten in der Infrastruktur installiert werden, wie Workbenches navigiert und interpretiert werden, wie Bedrohungsdaten von Drittanbietern eingebunden werden, wie nach Informationen im Trend Micro Vision One Data Lake gesucht wird und wie Reaktionen mit Security Playbooks automatisiert werden.

Dieser Kurs wird von Trend Micro-zertifizierten Trainern unterrichtet und beinhaltet eine Vielzahl praktischer Laborübungen, die es den Teilnehmern ermöglichen, die Lerninhalte in die Praxis umzusetzen.

Kursinhalt

- XDR Concepts
- Trend Micro Vision One
- Connecting Trend Micro Products
- Enabling XDR Sensors
- Integrating with Third-Party Products
- Using the XDR Apps
- Sharing Threat Intelligence
- Searching the Data Lake
- Responding to Incidents Using Security Playbooks

E-Book Sie erhalten ausführliche Kursunterlagen von Trend Micro in englischer Sprache. Wahlweise stellen wir die Printversion oder ein Trend Micro e-Kit zur Verfügung.

Zielgruppe

Dieser Kurs richtet sich an Mitglieder der Security Operations Teams eines Unternehmens, die für die Erkennung, Untersuchung, Priorisierung und Reaktion auf Bedrohungen zuständig sind und die Trend Micro Vision One noch nicht oder nur wenig kennen. Dieser Kurs richtet sich auch an Administratoren, die für die Ersteinrichtung zuständig sind, z. B. für die Verbindung von Produkten mit Trend Micro Vision One und die Aktivierung von XDR-Sensoren auf Geräten.

Voraussetzungen

Zu den Voraussetzungen für die Teilnahme an diesem Kurs gehören:

- Gute Kenntnisse der Trend Micro Endpoint- und Network Protection Lösungen und Services
- Ein Verständnis für grundlegende Netzwerkkonzepte und -prinzipien ist hilfreich

Die Teilnehmer müssen außerdem den E-Learning-Kurs Trend Micro Vision One Fundamentals auf dem Trend Micro Education Portal erfolgreich abgeschlossen haben.

Kursziel

Nach Abschluss des Kurses können die Teilnehmer die Zertifizierungsprüfung zum Trend Micro Certified Professional for Vision One XDR ablegen. Die Prüfung ist im Kurspreis inkludiert. Für die Registrierung zum Examen wird ein Account im Trend Micro Education Portal benötigt.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/TMXD

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.	
Termine in Österreich	3 Tage	€ 1.995,-
Online Training	3 Tage	€ 1.995,-
Termine auf Anfrage		

Stand 24.01.2025



Inhaltsverzeichnis

Trend Micro Vision One XDR Training for Certified Professionals

XDR Concepts

- Collecting telemetry
- Data correlation
- MITRE ATT&CK

Trend Micro Vision One

- How Trend Micro Vision One fits into the Trend Micro One platform
- Trend Micro Vision One core capabilities
- Trend Micro Vision One features for XDR
- Trend Micro Vision One apps

Connecting Trend Micro Products

- Collecting security events
- Connecting Trend Micro Apex One™ as a Service
- Connecting Deep Security™ Software
- Connecting Trend Micro Cloud One™ – Endpoint &

Workload Security

- Connecting Cloud App Security
- Connecting the Service Gateway
- Connecting Web Security™
- Connecting Deep Discovery™ Inspector
- Connecting TippingPoint™ SMS

Enabling XDR Sensors

- Installing Endpoint Basecamp
- Creating Endpoint Groups and Security Policies
- Enabling endpoint sensors
- Enabling email sensors
- Enabling network sensors
- Enabling web sensors

Integrating with Third-Party Products

- Integration purposes

Using the XDR Apps

- XDR apps
- Viewing raw security event and activity data
- Filtering security event and activity data
- Workbenches
- Workbench actions
- Execution profiles
- Network analytics
- Automating responses
- Targeted attack detection
- Response management

- Managed XDR service

Sharing Threat Intelligence

- Curated and custom intelligence reports
- Suspicious object management
- Sandbox analysis

Searching the Data Lake

- Simple and complex search syntax
- Search tips
- Watchlists

Responding to Incidents Using Security Playbooks

- Playbook templates
- Playbook triggers
- Playbook conditions
- Playbook actions

