Schutz vor Cyberbedrohungen mit Microsoft Defender XDR (SC-5004)

ID SC-5004 **Preis** 690,– € (exkl. MwSt.) **Dauer** 1 Tag

Kursüberblick

Implementieren Sie die Microsoft Defender for Endpoint-Umgebung zum Verwalten von Geräten, führen Sie Untersuchungen zu Endpunkten durch, verwalten Sie Vorfälle in Defender XDR, und nutzen Sie die erweiterte Bedrohungssuche mit KQL (Kusto-Abfragesprache), um einzelne Bedrohungen zu erkennen.

Voraussetzungen

- Erfahrung mit der Verwendung des Microsoft Defender-Portals
- Grundlegendes Verständnis von Microsoft Defender for Endpoint
- Grundlegende Microsoft Sentinel-Kenntnisse
- Erfahrung mit der Kusto-Abfragesprache (KQL) in Microsoft Sentinel

Sie benötigen Zugriff auf einen Microsoft 365 E5-Mandanten mit einer P2-Lizenz für Microsoft Defender for Endpoint, um die Übungen durchzuführen.

Kursinhalt

Abmildern von Incidents mit Microsoft Defender

Erfahren Sie, wie das Microsoft Defender-Portal eine einheitliche Ansicht von Vorfällen in der Microsoft Defender-Produktfamilie bereitstellt.

- Einführung
- Verwenden des Microsoft Defender-Portals
- Verwalten von Incidents
- Untersuchen von Incidents
- Verwalten und Untersuchen von Warnungen
- Verwalten von automatisierten Untersuchungen
- Verwenden des Info-Centers
- Erkunden der erweiterten Bedrohungssuche
- Untersuchen von Microsoft Entra-Anmeldeprotokollen
- Grundlegendes zur Microsoft-Sicherheitsbewertung
- Analysieren der Bedrohungsanalyse
- Berichte analysieren
- Konfigurieren des Microsoft Defender-Portals
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Bereitstellen der Microsoft Defender für Endpunkt-Umgebung

Hier erfahren Sie, wie Sie die Microsoft Defender für Endpunkt-Umgebung bereitstellen, einschließlich des Onboardings von Geräten und der Sicherheitskonfiguration.

- Einführung
- Erstellen der Umgebung
- Grundlegendes zu Kompatibilität und Features von Betriebssystemen
- Integrieren von Geräten
- Verwalten des Zugriffs
- Erstellen und Verwalten von Rollen für die rollenbasierte Zugriffssteuerung
- Konfigurieren von Gerätegruppen
- Konfigurieren erweiterter Umgebungsfeatures
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt

Erfahren Sie, wie Sie Einstellungen zur Verwaltung von Warnungen und Benachrichtigungen konfigurieren. Außerdem erfahren Sie, wie Sie Indikatoren im Rahmen des Erkennungsprozesses aktivieren.

- Einführung
- Konfigurieren erweiterter Features
- Konfigurieren von Warnungsbenachrichtigungen
- Verwalten der Warnungsunterdrückung
- Verwalten von Indikatoren
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt

Erfahren Sie, wie Sie die Automatisierung in Microsoft Defender für Endpunkt durch Verwalten der Umgebungseinstellungen konfigurieren.

- Einführung
- Konfigurieren erweiterter Features
- Verwalten von Einstellungen für automatisierte Uploads und Ordner
- Konfigurieren der Funktionen für die automatisierte Untersuchung und Wartung
- Blockieren auf Risikogeräten
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt

Microsoft Defender für Endpunkt bietet umfassende Geräteinformationen, einschließlich forensischer Informationen. Hier erfahren Sie mehr über die Informationen, die Ihnen über Microsoft Defender für Endpunkt zur Verfügung stehen und bei Untersuchungen hilfreich sind.

- Einführung
- Verwenden der Geräteinventarliste
- Untersuchen des Geräts
- Verwenden des verhaltensbasierten Blockierens
- Erkennen von Geräten mit Geräteermittlung
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Labübungen zum Schutz vor Cyberbedrohungen mit Microsoft Defender XDR

In diesem Modul haben Sie erfahren, wie Sie Microsoft Defender XDR konfigurieren, Microsoft Defender for Endpoint bereitstellen und Geräte onboarden. Sie haben auch Richtlinien konfiguriert, Bedrohungen entschärft und mit Defender XDR auf Vorfälle reagiert.

- Einführung
- Konfigurieren der Microsoft Defender XDR-Umgebung
- Bereitstellen von Microsoft Defender für Endpunkt
- Entschärfung von Angriffen mit Microsoft Defender for Endpoint
- Zusammenfassung

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch