Symantec Endpoint Protection 14.2 Configure and Protect (SEPCP42)

ID SEPCP42 **Preis** 1.990,– € (exkl. MwSt.) **Dauer** 3 Tage

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Der Kurs Symantec Endpoint Protection 14.2: Configure and Protect" richtet sich an Netzwerk-, IT-Sicherheits- und Systemadministrationsexperten in einer Security Operations-Position, die mit der Konfiguration der optimalen Sicherheitseinstellungen für Endgeräte betraut sind, die durch Symantec Endpoint Protection 14.2 geschützt werden. Dieser Kurs liefert Kontext und Beispiele für Angriffe und Tools, die von Cyberkriminellen verwendet werden.

Zielgruppe

Der Kurs "Endpoint Protection 14.2 Configure and Protect" richtet sich an Netzwerk-, IT-Sicherheits- und Systemadministrationsexperten, die mit der Konfiguration optimaler Sicherheitseinstellungen für die von Symantec Endpoint Protection 14.2 geschützten Endgeräte betraut sind.

Voraussetzungen

In diesem Kurs wird vorausgesetzt, dass die Teilnehmer über ein grundlegendes Verständnis der Computerterminologie verfügen, einschließlich der Begriffe TCP/IP-Netzwerke und Internet, sowie über Kenntnisse auf Administratorebene der Microsoft Windows-Betriebssysteme.

Kursziele

Nach Abschluss dieses Kurses werden Sie in der Lage sein:

- Schutz von Endgeräten vor netzwerk- und dateibasierten Bedrohungen
- Kontrolle der Integrität und Konformität von Endpunkten
- Durchsetzung einer anpassungsfähigen Sicherheitsposition

Kursinhalt

- Einführung von Netzwerk-Bedrohungen
- Schutz vor Netzwerkangriffen und Durchsetzung von Unternehmensrichtlinien mithilfe der Firewall-Richtlinie
- Blockieren von Bedrohungen mit Intrusion Prevention
- Einführung von dateibasierten Bedrohungen
- Verhinderung von Angriffen mit SEP Layered Security
- Absicherung von Windows-Clients
- Absicherung von Linux-Clients
- Absicherung von Mac-Clients
- Granulare Kontrolle mit Host-Integrität bereitstellen
- Kontrolle des Anwendungs- und Dateizugriffs
- Einschränkung des Gerätezugriffs für Windows- und Mac-Clients
- Härtung von Clients mit System Lockdown
- Anpassen von Richtlinien basierend auf dem Standort
- Verwaltung von Sicherheitsausnahmen

Detaillierter Kursinhalt

Modul 1: Einführung in Netzwerkbedrohungen

- Beschreibt, wie Symantec Endpoint Protection jede Schicht des Netzwerkstapels schützt
- Entdeckung der von Angreifern verwendeten Tools und Methoden
- Beschreibung der Phasen eines Angriffs

Modul 2: Schutz vor Netzwerkangriffen und Durchsetzung von Unternehmensrichtlinien mithilfe der Firewall-Richtlinie

- Verhinderung von Netzwerkangriffen
- Prüfung der Elemente der Firewall-Richtlinie
- Benutzerdefinierte Firewall-Regeln erstellen
- Durchsetzung der Sicherheitsrichtlinien des Unternehmens mit Firewall-Regeln
- Konfigurieren der erweiterten Firewall-Funktion

Modul 3: Blockieren von Bedrohungen mit Intrusion Prevention

- Einführung von Intrusion Prevention-Technologien
- Konfigurieren der Richtlinie zur Eindämmung von Speicherausnutzungsproblemen
- Konfigurieren der Intrusion Prevention-Richtlinie
- Verwalten von benutzerdefinierten Signaturen
- Überwachung von Intrusion Prevention-Ereignissen

Modul 4: Einführung in dateibasierte Bedrohungen

- Beschreiben von Bedrohungsarten
- Aufdecken, wie Angreifer ihre bösartigen Anwendungen tarnen
- Beschreiben von Bedrohungsvektoren
- Beschreibung von Advanced Persistent Threats und eines typischen Angriffsszenarios
- Befolgung bewährter Sicherheitsverfahren zur Risikominderung

Modul 5: Verhinderung von Angriffen mit SEP Layered Security

- Viren- und Spyware-Schutzbedarf und Lösungen
- Prüfung der Bewertung der Dateireputation
- Beschreibung des Schutzes von Endpunkten mit dem Intelligent Threat Cloud Service
- Beschreibung der Art und Weise, wie der Emulator eine Datei in einer Sandbox ausführt, und der Rolle und Funktion des maschinellen Lernsystems
- Beschreibung des Download-Schutzes mit Download Insight.
- Beschreibung von Dateisystem und E-Mail-Autoprotect sowie verschiedener Überlegungen zu Auto-Protect.
- Beschreibung des SONAR-Echtzeitschutzes.
- Beschreibung der verschiedenen Scantypen und Überlegungen zu Scans.

Modul 6: Absicherung von Windows-Clients

- Überblick über die Richtlinien zum Schutz von Plattformen und Viren und Spyware
- Maßgeschneiderte Scans für die Bedürfnisse einer Umgebung
- Gewährleistung des Echtzeitschutzes für Kunden
- Erkennung und Beseitigung von Risiken in heruntergeladenen Dateien
- Identifizierung von Zero-Day- und unbekannten Bedrohungen
- Verhindern des Herunterladens von Malware per E-Mail
- Konfigurieren der erweiterten Optionen
- Überwachung von Viren- und Spyware-Aktivitäten

Modul 7: Absicherung von Linux-Clients

- Navigieren auf dem Linux-Client
- Maßgeschneiderte Viren- und Spyware-Einstellungen für Linux-Clients
- Überwachung von Linux-Clients
- SEP für Linux-Protokolle

Modul 8: Absicherung von Mac-Clients

- Rundgang durch den SEP für Mac-Client
- Absicherung von Mac-Clients
- Überwachung von Mac-Clients
- SEP Logs auf Mac Klienten

Modul 9: Granulare Kontrolle mit Host-Integrität bereitstellen

- Sicherstellung der Einhaltung der Host Integrity durch den Kunden
- Host-Integritätskonzepte
- Konfigurieren der Host-Integrität
- Fehlerbehebung bei der Host-Integrität
- Überwachung der Host-Integrität

Modul 10: Kontrolle des Anwendungs- und Dateizugriffs

- Überblick über die Anwendungskontrolle
- Beschreibung der Anwendungskontrolle und der Konzepte
- Erstellen von Anwendungsregelsätzen zur Einschränkung der Ausführung von Anwendungen
- Überwachung von Ereignissen der Anwendungskontrolle

Modul 11: Einschränkung des Gerätezugriffs für Windows- und Mac-Clients

- Einführung von Device Cotrol
- Beschreibung der Funktionen und Konzepte der Gerätesteuerung für Windows
- Beschreiben der Funktionen und Konzepte der Gerätesteuerung für Mac-Clients
- Erkennen von Verstößen gegen die Hardware-Zugriffsrichtlinie mit Berichten, Protokollen und Benachrichtigungen

Modul 12: Härtung von Clients mit System Lockdown

- Was ist eine Systemabschaltung?
- Erstellen und Verwalten der Datei-Fingerprint-Liste
- System Lockdown Anwendungsfälle

Modul 13: Anpassen von Richtlinien basierend auf dem Standort

- Schaffung von Standorten zur Gewährleistung eines angemessenen Sicherheitsniveaus bei der Fernanmeldung
- Zuweisung von Richtlinien zu Standorten

- Überwachungsstandorte auf dem SEPM und SEP-Client

Modul 14: Verwaltung von Sicherheitsausnahmen

- Beschreibung von Sicherheitsausnahmen
- Beschreibung des automatischen Ausschlusses, der während der Installation erstellt wird
- Verwaltung von Windows- und Mac-Ausschlüssen
- Überwachung von Sicherheitsausnahmen

Über Fast Lane

Die weltweite Fast Lane-Gruppe ist Spezialist für Technologie- und Business-Training und Beratung im Highend-Bereich. Fast Lane ist autorisierter Trainingspartner führender Hersteller und bietet zudem eigene IT-Trainingsprogramme zu aktuellen Technologien und den wesentlichen Trends an. Herstellerübergreifende Beratungsleistungen reichen von vorbereitenden Analysen und Evaluierungen über die Konzipierung zukunftsweisender IT-Lösungen bis zum Projektmanagement und zur Umsetzung der Konzepte im Unternehmen Training-on-the-Job und Weiterqualifizierung der zuständigen Spezialisten bei den Kunden verbinden die Kernbereiche der Fast Lane Dienstleistungen Training und Consulting.

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 in 60 Ländern 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