

Dieses Training zeigt Ihnen, wie Sie die Cisco® Email Security Appliance einsetzen und verwenden, um Ihre E-Mail-Systeme vor Phishing, E-Mail-Kompromittierungen und Ransomware zu schützen und die Verwaltung von E-Mail-Sicherheitsrichtlinien zu optimieren.

Dieser praxisorientierte Kurs vermittelt Ihnen die Kenntnisse und Fähigkeiten zur Implementierung, Fehlerbehebung und Verwaltung der Cisco Email Security Appliance, einschließlich wichtiger Funktionen wie erweiterter Malware-Schutz, Spam-Blockierung, Virenschutz, Filterung von Ausbrüchen, Verschlüsselung, Quarantänen und Verhinderung von Datenverlusten.

Kursinhalt

- Describe and administer the Cisco Email Security Appliance
- Control sender and recipient domains
- Control spam with Talos SenderBase and anti-spam
- Use anti-virus and outbreak filters
- Use mail policies
- Use content filters
- Use message filters
- Prevent data loss
- Perform lightweight directory access protocol (LDAP) queries
- Authenticate simple mail transfer protocol (SMTP) sessions
- Authenticate email
- Encrypt email
- Use system quarantines and delivery methods
- Perform centralized management using clusters
- Test and troubleshoot

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlage stattdessen in die Lernerfläche integriert.

Zielgruppe

- Security Engineers
- Security Administrators
- Security Architects
- Operations Engineers
- Network Engineers
- Network Administrators
- Network or Security Technicians
- Network Managers
- System Designers
- Cisco Integrators and Partners

Voraussetzungen

Sie sollten Sie über eine oder mehrere der folgenden technischen Grundkenntnisse verfügen:

- Cisco-Zertifizierung (Cisco CCENT®-Zertifizierung oder höher)
- Relevante Branchenzertifizierungen wie (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC) und ISACA
- Abschluss der Cisco Networking Academy (CCNA® 1 und CCNA® 2)
- Windows-Know-how: Microsoft (Microsoft Spezialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE), CompTIA (A+, Network+, Server+)

Zudem folgende Kenntnisse und Fähigkeiten:

TCP/IP-Dienste, einschließlich Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP und HTTPS; Erfahrung mit IP-Routing.

Kursziel

Dieser Kurs bereitet Sie auf die Prüfung Securing Email with Cisco Email Security Appliance innerhalb der CCNP® Security Zertifizierung vor und zudem auf den Certified Specialist – Email Content Security.

Bearbeitungszeit

ca. 24 Stunden

Dieser Kurs im Web



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

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.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzgeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.

6 Monate Freischaltung **CHF 885,-**

Training Preise zzgl. MwSt.

Termine in Deutschland 4 Tage CHF 3.515,-

Termine in Österreich 4 Tage CHF 3.515,-

Online Training 4 Tage CHF 3.515,-

Termin/Kursort **Kurssprache Deutsch**

28.07.-31.07.25 Online 03.11.-06.11.25 Frankfurt

28.07.-31.07.25 Wien 03.11.-06.11.25 Online

Inhaltsverzeichnis

SESA – Securing Email with Cisco Email Security Appliance

Course Outline

- Describing the Cisco Email Security Appliance
- Controlling Sender and Recipient Domains
- Controlling Spam with Talos SenderBase and Anti-Spam
- Using Anti-Virus and Outbreak Filters
- Using Mail Polices
- Using Content Filters
- Using Message Filters
- Preventing Data Loss
- Using LDAP
- Describing SMTP Session Authentication
- Using Email Authentication
- Using Email Encryption
- Administering the Cisco Email Security Appliance
- Using System Quarantines and Delivery Methods
- Centralizing Management Using Clusters
- Testing and Troubleshooting

Lab Outline

- Verify and Test Cisco ESA Configuration
- Advanced Malware in Attachments (Macro Detection)
- Protect Against Malicious or Undesirable URLs
- Beneath Shortened URLs
- Protect Against Malicious or Undesirable URLs Inside Attachments
- Intelligently Handle Unscannable Messages
- Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
- Integrate Cisco ESA with AMP Console
- Prevent Threats with Anti-Virus Protection
- Applying Outbreak Filters
- Configure Attachment Scanning
- Configure Outbound Data Loss Prevention
- Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Forged Email Detection
- Perform Basic Administration
- Configure the Cisco Secure Email and Web Manager for Tracking and Reporting

