Designing Cisco Security Infrastructure (SDSI)

ID SDSI **Preis** auf Anfrage **Dauer** 5 Tage

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

Kursüberblick

Die Schulung Designing Cisco Security Infrastructure (SDSI) vermittelt Ihnen Kenntnisse über das Design von Sicherheitsarchitekturen, einschließlich sicherer Infrastrukturen, Anwendungen, Risiken, Ereignisse, Anforderungen, künstliche Intelligenz (AI), Automatisierung und DevSecOps.

Dieses Training bereitet Sie auf die Prüfung 300-745 SDSI v1.0 vor. Bei Bestehen erhalten Sie die Cisco Certified Specialist - Designing Cisco Security Infrastructure Zertifizierung und erfüllen die Anforderung der Konzentrationsprüfung für die Cisco Certified Network Professional (CCNP) Security Zertifizierung.

Wie Sie davon profitieren

Diese Schulung wird Ihnen helfen:

- Praktische Erfahrung mit dem Entwurf von Sicherheitsarchitekturen sammeln
- Qualifizieren Sie sich für Sicherheitsberufe auf Fach- und Expertenebene
- Vorbereitung auf die Prüfung 300-745 SDSI v1.0
- Erwerben Sie 41 CE-Punkte für die Rezertifizierung

Was Sie bei der Prüfung erwartet

Designing Cisco Security Infrastructure (300-745 SDSI) v1.0 ist eine 90-minütige Prüfung, die mit der Cisco Certified Specialist - Designing Cisco Security Infrastructure Zertifizierung verbunden ist und die Kernprüfungsanforderungen für die CCNP Security Zertifizierung erfüllt.

Diese Prüfung prüft Ihr Wissen über den Entwurf von Sicherheitsarchitekturen, einschließlich:

- Sichere Infrastruktur
- Anwendungen
- Risiko
- Veranstaltungen
- Requirements
- Künstliche Intelligenz und Automatisierung
- DevSecOps

Zielgruppe

- Systemingenieure von Cisco und Partnern
- Kunden-Netzwerk- und Infrastruktur-Ingenieure
- Kunden-Sicherheit/NOC-Ingenieure

Voraussetzungen

Für diese Schulung gibt es keine Voraussetzungen. Es wird jedoch empfohlen, dass Sie vor der Teilnahme an dieser Schulung folgende Kenntnisse und Fähigkeiten besitzen:

- Cisco CCNP Security oder gleichwertige Kenntnisse
- Vertrautheit mit Microsoft Windows-Betriebssystemen
- Vertrautheit mit dem Cisco Security Portfolio

Diese Fähigkeiten können in den folgenden Cisco-Lernangeboten erworben werden:

- Implementing and Operating Cisco Security Core Technologies (SCOR)
- Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)
- Implementing and Configuring Cisco Identity Services Engine (SISE)
- Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)
- Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA)
- !Implementing Automation for Cisco Security Solutions (SAUI)
- Implementing Secure Solutions with Virtual Private Networks (SVPN)
- Introducing Automation for Cisco Solutions (CSAU)
- Securing Email with Cisco Email Security Appliance (SESA)

- Securing the Web with Cisco Web Security Appliance (SWSA)

Kursziele

- Identifizierung und Erläuterung der grundlegenden Konzepte der Sicherheitsarchitektur und wie sie den Entwurf, den Aufbau und die Wartung einer sicheren Infrastruktur unterstützen
- Identifizierung der Schichten der Sicherheitsinfrastruktur, der wichtigsten Sicherheitstechnologien und der Infrastrukturkonzepte
- Erläutern, wie die Grundsätze des Sicherheitsdesigns zu einer sicheren Infrastruktur beitragen
- Identifizierung und Erörterung von Rahmenwerken für die Sicherheitsgestaltung und -verwaltung, die für die Gestaltung der Infrastruktursicherheit verwendet werden können
- Erläuterung der Bedeutung und der Methoden zur Durchsetzung der Einhaltung von Vorschriften bei der Sicherheitsgestaltung
- Identifizierung von Tools, die die Erkennung von und Reaktion auf Sicherheitsvorfälle in der Infrastruktur ermöglichen
- Erläuterung verschiedener Strategien, die zur Anpassung traditioneller Sicherheitsarchitekturen an die technischen Anforderungen moderner Unternehmensnetze eingesetzt werden können
- Implementierung sicherer Netzwerkzugriffsmethoden, wie 802.1X, MAC Authentication Bypass (MAB) und webbasierte Authentifizierung
- Beschreibung von Sicherheitstechnologien, die auf WAN-Verbindungen (Wide Area Network) von Unternehmen angewendet werden können
- Vergleich von Methoden zur Sicherung des Netzwerkmanagements und des Datenverkehrs auf der Steuerungsebene
- Vergleich der Unterschiede zwischen herkömmlichen Firewalls und Next-Gen-Firewalls (NGFWs) und Identifizierung der erweiterten Funktionen, die NGFWs bieten
- Erklären, wie Web Application Firewalls (WAFs) Webanwendungen vor Bedrohungen schützen
- Beschreibung der wichtigsten Merkmale und bewährten Verfahren für den Einsatz von Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) als Teil des Sicherheitsdesigns der Unternehmensinfrastruktur
- Erklären Sie, wie Endpunkte und Dienste in Cloud-nativen oder Microservice-Umgebungen mit Host-basierten oder verteilten Firewalls geschützt werden können.
- Erörterung von Sicherheitstechnologien für Anwendungsdaten und Daten, die sich im Transit befinden
- Identifizierung verschiedener Sicherheitslösungen für Cloud-native Anwendungen, Microservices und Container
- Erläutern Sie, wie der technologische Fortschritt die Sicherheit der heutigen Infrastrukturen verbessern kann.
- Identifizierung von Tools, die die Erkennung von und Reaktion auf Sicherheitsvorfälle in der Infrastruktur ermöglichen
- Beschreibung von Rahmenwerken und Kontrollen für den Zugang zu und die Minderung von Sicherheitsrisiken für Infrastrukturen
- Erläutern, wie nach einem Sicherheitsvorfall Sicherheitsanpassungen vorgenommen werden können
- Identifizierung von DevSecOps-Integrationen, die das Sicherheitsmanagement und die Reaktion verbessern
- Erörterung der Frage, wie die Sicherheit automatisierter Dienste gewährleistet werden kann
- Erörterung der Frage, wie KI bei der Erkennung von und Reaktion auf Bedrohungen helfen kann

Detaillierter Kursinhalt

- Definition und Zweck der Sicherheitsarchitektur
- Komponenten der Sicherheitsinfrastruktur
- Grundsätze des Sicherheitsdesigns
- Sicherheit und Design Frameworks
- Konformitäts- und Regulierungsanforderungen
- Sicherheitsansätze zum Schutz vor Bedrohungen
- Modifizierung der Sicherheitsarchitektur zur Erfüllung der technischen Anforderungen
- Sicherheit beim Netzzugang
- VPN- und Tunneling-Lösungen
- Sichere Infrastrukturverwaltung und Kontrollpläne
- Nextgen Firewalls
- Web-Anwendungs-Firewall (WAF)
- IPS/IDS-Bereitstellung
- Host-basierte Firewalls und verteilte Firewalls
- Sicherheitslösungen auf der Grundlage von Anwendungs- und Flussdaten
- Sicherheit für Cloud-native Anwendungen, Microservices und Container
- Aufstrebende Technologien für die Anwendungssicherheit
- SOC-Tools für die Behandlung von und Reaktion auf Vorfälle
- Design ändern, um das Risiko zu mindern
- Ereignisabhängige Sicherheitsanpassungen
- DevSecOps-Integration
- Sichere automatisierte Arbeitsabläufe und Pipelines
- Die Rolle der KI bei der Sicherung der Infrastruktur

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