Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)

ID SCAZT **Preis** 3.595,– € (exkl. MwSt.) **Dauer** 5 Tage

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

Kursüberblick

Die Schulung **Designing and Implementing Secure Cloud Access for Users and Endpoints** vermittelt Ihnen die Fähigkeiten, eine Cloud-Sicherheitsarchitektur zu entwerfen und zu implementieren, Benutzer- und Gerätesicherheit, Netzwerk- und Cloud-Sicherheit, Cloud-Anwendungs- und Datensicherheit, Cloud-Transparenz und -Gewährleistung sowie die Reaktion auf Cloud-Bedrohungen.

Dieses Training bereitet Sie auf die Prüfung 300-740 SCAZT v1.0 vor. Bei Bestehen erhalten Sie die Zertifizierung Cisco Certified Specialist - Security Secure Cloud Access und erfüllen die Anforderung der Konzentrationsprüfung für das Cisco Certified Network Professional Security (CCNP SECURITY).

Wie Sie davon profitieren

Diese Schulung wird Ihnen helfen:

Erlangung von Fähigkeiten für die Entwicklung und Implementierung von Cloud-Sicherheitsarchitekturen, Benutzer- und Gerätesicherheit, Netzwerk- und Cloud-Sicherheit, Cloud-Anwendungs- und Datensicherheit, Cloud-Sichtbarkeit und -Sicherheit sowie Reaktion auf Cloud-Bedrohungen Erwerb von Kenntnissen über Protokolle, Lösungen und Entwürfe, um eine professionelle und fachkundige Rolle bei der Entwicklung und Implementierung von Clouds zu übernehmen

Was Sie bei der Prüfung erwartet

300-740 SCAZT v1.0: Designing and Implementing Secure Cloud Access for Users and Endpoints ist eine 90-minütige Prüfung, die mit der Cisco Certified Specialist - Secure Cloud Access Zertifizierung verbunden ist und die Anforderung der Konzentrationsprüfung für die Cisco Certified Network Professional Security (CCNP SECURITY) erfüllt.

In der Prüfung werden die Kenntnisse in den Bereichen Konzeption und Umsetzung geprüft:

- Architektur der Cloud-Sicherheit
- Benutzer- und Gerätesicherheit
- Netz- und Cloud-Sicherheit
- Anwendungs- und Datensicherheit
- Sichtbarkeit und Sicherheit
- Reaktion auf Bedrohungen

Zielgruppe

- Netzwerk-Ingenieure
- Netzwerksicherheitsingenieure
- Netzwerk-Architekten
- Vertrieb/Verkaufsingenieure

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

Die Kenntnisse und Fähigkeiten, die Sie vor der Teilnahme an dieser Schulung haben sollten, sind

- Grundlegendes Verständnis von Enterprise Routing
- Grundlegendes Verständnis von WAN-Netzwerken
- Grundlegendes Verständnis von Cisco SD-WAN
- Grundlegendes Verständnis von Public Cloud-Diensten

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

- Implementing and Administering Cisco Solutions (CCNA) v2.1

- Implementing Cisco SD-WAN Solutions (ENSDWI)
- Cisco SD-WAN Operation and Deployment (SDWFND)

Kursziele

- Vergleich und Gegenüberstellung der Sicherheitsrahmenwerke des National Institute of Standards and Technology (NIST), der Cybersecurity and Infrastructure Security Agency (CISA) und der Defense Information Systems Agency (DISA) sowie Verständnis für die Bedeutung der Übernahme standardisierter Rahmenwerke für die Cybersicherheit zur Verbesserung der Sicherheitslage eines Unternehmens
- Beschreiben Sie die Cisco Security Reference Architecture und ihre fünf Hauptkomponenten
- Beschreibung gängiger Anwendungsfälle und Empfehlung der erforderlichen Fähigkeiten innerhalb einer integrierten Sicherheitsarchitektur, um diese effektiv zu bewältigen
- Beschreiben Sie die Cisco Secure Architecture for Everyone (SAFE) Architektur
- Überprüfung der Vorteile, Komponenten und Verfahren der zertifikatsbasierten Authentifizierung für Benutzer und Geräte
- Aktivieren Sie die Duo-Multifaktor-Authentifizierung (MFA), um eine Anwendung vom Duo-Administrationsportal aus zu schützen, und konfigurieren Sie dann die Anwendung so, dass sie Duo MFA für die Authentifizierung der Benutzeranmeldung verwendet
- Installieren Sie Cisco Duo und implementieren Sie die Multifaktor-Authentifizierung im virtuellen privaten Netzwerk (VPN) für den Fernzugriff.
- Konfigurieren der Endpunktkonformität
- Überprüfung und Nachweis der Fähigkeit, Stateful Switchover (SSO) unter Verwendung der Security Assertion Markup Language (SAML) oder OpenID Connect in Verbindung mit Cisco Duo zu verstehen
- Beschreiben Sie die Cisco Software-defined Wide-Area Network (SD-WAN) On-Box- und integrierten Threat Prevention Security Services
- Beschreiben Sie die SD-WAN On-Box- und integrierten Content-Filtering-Sicherheitsdienste
- Beschreiben Sie die Funktionen und Möglichkeiten von Cisco Umbrella Secure Internet Gateway (SIG), wie DNS-Sicherheit, Cloud-Delivered Firewall (CDFW), Intrusion Prevention Systems (IPS) und Interaktion mit Cisco SD-WAN
- Einführung des Reverse-Proxys für den Schutz von Anwendungen mit Internetzugang
- Erkunden Sie den Anwendungsfall von Cisco Umbrella SIG zur Sicherung des Zugriffs auf Cloud-Anwendungen, die Einschränkungen und Vorteile der Lösung sowie die verfügbaren Funktionen zur Erkennung und Kontrolle des Zugriffs auf Cloud-Anwendungen
- Entdecken Sie die Cisco ThousandEyes-Funktionen zur Überwachung der Cisco SD-WAN-Bereitstellung
- Beschreiben Sie die Herausforderungen beim Zugriff auf SaaS-Anwendungen in modernen Geschäftsumgebungen und lernen Sie die Cisco SD-WAN Cloud OnRamp for SaaS-Lösung mit direktem oder zentralisiertem Internetzugang kennen
- Einführung in die Cisco Secure Firewall-Plattformen, Anwendungsfälle und Sicherheitsfunktionen
- ein umfassendes Verständnis von Web Application Firewalls nachweisen
- Demonstration eines umfassenden Verständnisses der Funktionen, Bereitstellungsoptionen, Agenten und Konnektoren von Cisco Secure Workload
- Demonstration eines umfassenden Verständnisses von Cisco Secure Workload Application Dependency Mapping und Policy Discovery
- Demonstration eines umfassenden Verständnisses gängiger Cloud-Angriffstaktiken und Abhilfestrategien
- Demonstration eines umfassenden Verständnisses der Multi-Cloud-Sicherheitsanforderungen und -richtlinienfunktionen
- Einführung in die Sicherheitsprobleme bei der Einführung von öffentlichen Clouds und in die gemeinsamen Fähigkeiten von Cloud-Tools zur Sichtbarkeit und Sicherheit, um diese Probleme zu entschärfen
- Einführung in Cisco Secure Network Analytics und Cisco Security Analytics and Logging
- Beschreiben Sie das Cisco Attack Surface Management
- Beschreiben Sie, wie Anwendungsprogrammschnittstellen (APIs) und Automatisierung bei der Fehlersuche in der Cloud-Richtlinie helfen können, insbesondere im Zusammenhang mit Fehlkonfigurationen
- Demonstration umfassender Kenntnisse über die angemessenen Reaktionen auf Cloud-Bedrohungen in spezifischen Szenarien
- Demonstration der umfassenden Kenntnisse, die erforderlich sind, um die Automatisierung für die Erkennung von und Reaktion auf Cloud-Bedrohungen zu nutzen

Detaillierter Kursinhalt

- Sicherheitsrahmen für die Industrie
- Grundlagen der Cisco-Sicherheitsreferenzarchitektur
- Gemeinsame Anwendungsfälle der Cisco-Sicherheitsreferenzarchitektur
- Cisco SAFE-Architektur
- Zertifikatsbasierte Benutzer- und Geräteauthentifizierung
- Cisco Duo Multifaktor-Authentifizierung für Anwendungsschutz
- Cisco Duo mit AnyConnect VPN für Fernzugriff
- Einführung in die Cisco ISE Endpoint Compliance Services
- SSO mit SAML oder OpenID Connect

- Vor-Ort-Bedrohungsschutz bereitstellen
- Prüfung der Inhaltsfilterung
- Erkundung der Cisco Umbrella SIG
- Umgekehrter Proxy
- Absicherung von Cloud-Anwendungen mit Cisco Umbrella SIG
- Erkundung von Cisco SD-WAN ThousandEyes
- Optimierung von SaaS-Anwendungen
- Sicherheitsrichtlinien für Remote Access VPN
- Cisco Sicherer Zugang
- Cisco Sichere Firewall
- Web-Anwendungs-Firewall
- Cisco Secure Workload-Implementierungen, Agenten und Konnektoren
- Cisco Secure Workload Struktur und Richtlinie
- Angriffe auf die Cloud-Sicherheit und Abhilfemaßnahmen
- Multicloud-Sicherheitsrichtlinien
- Cloud-Transparenz und -Gewährleistung
- Cisco Secure Network Analytics und Cisco Secure Analytics und Logging
- Cisco XDR
- Cisco Angriffsflächen-Management
- Überprüfungen von Cloud-Anwendungen und Datenzugriff
- Automatisierung der Cloud-Politik
- Reaktion auf Cloud-Bedrohungen
- Automatisierung von Erkennung und Reaktion auf Cloud-Bedrohungen

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