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

ID SCAZT **Prix** CHF 3 595,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

- Ingénieurs réseaux
- Ingénieurs en sécurité des réseaux
- Architectes réseaux
- Ingénieurs commerciaux/avant-vente

Cette formation prépare à la/aux certifications

Cisco Certified Network Professional Security (CCNP SECURITY)

Pré-requis

Les connaissances et les compétences que vous êtes censé posséder avant de participer à cette formation sont les suivantes :

- Compréhension de base du routage d'entreprise
- Compréhension de base des réseaux WAN
- Compréhension de base de Cisco SD-WAN
- Compréhension de base des services de Cloud public

Ces compétences peuvent être trouvées dans les offres de formation Cisco suivantes :

- Implementing and Administering Cisco Solutions (CCNA)
- Implementing Cisco SD-WAN Solutions (ENSDWI)
- Cisco SDWAN Fundamentals (SDWFND)

Objectifs

A l'issue de ce cours, vous serez en mesure de :

- Comparer les cadres de sécurité du National Institute of Standards and Technology (NIST), de la Cybersecurity and Infrastructure Security Agency (CISA) et de la Defense Information Systems Agency (DISA), et comprendre l'importance de l'adoption de cadres normalisés pour la cybersécurité dans l'amélioration de la posture de sécurité d'une organisation.
- Décrire l'architecture de référence de sécurité de Cisco et ses cinq principaux composants
- Décrire les cas d'utilisation couramment déployés et recommander les capacités nécessaires au sein d'une architecture de sécurité intégrée pour les traiter efficacement.
- Décrire l'architecture SAFE (Secure Architecture for Everyone) de Cisco.
- Examiner les avantages, les composants et le processus d'authentification par certificat pour les utilisateurs et les appareils.
- Activer l'authentification multifactorielle Duo (MFA) pour protéger une application à partir du portail d'administration Duo, puis configurer l'application pour utiliser Duo MFA pour l'authentification de la connexion de l'utilisateur
- Installer Cisco Duo et mettre en œuvre l'authentification multifactorielle sur le réseau privé virtuel (VPN) d'accès à distance
- Configurer la conformité des terminaux
- Examiner et démontrer la capacité à comprendre le Stateful Switchover (SSO) en utilisant le langage de balisage d'assertion de sécurité (SAML) ou OpenID Connect avec Cisco Duo
- Décrire les services de sécurité de prévention des menaces intégrés et intégrés au réseau étendu défini par logiciel (SD-WAN) de Cisco.
- Décrire les services de sécurité SD-WAN on-box et de filtrage de contenu intégré
- Décrire les caractéristiques et les capacités de Cisco Umbrella Secure Internet Gateway (SIG), telles que la sécurité DNS, le Cloud-Delivered Firewall (CDFW), les systèmes de prévention des intrusions (IPS) et l'interaction avec Cisco SD-WAN.
- Présenter le proxy inverse pour les protections des applications tournées vers l'internet
- Explorer le cas d'utilisation de Cisco Umbrella SIG pour sécuriser l'accès aux applications sur cloud, les limites et les avantages de la solution, et les fonctionnalités disponibles pour découvrir et contrôler l'accès aux applications sur cloud.
- Explorer les capacités de Cisco ThousandEyes pour surveiller le déploiement du SD-WAN de Cisco.
- Décrire les défis liés à l'accès aux applications SaaS dans les environnements professionnels modernes et explorer la solution Cisco SD-WAN Cloud OnRamp for SaaS avec un accès direct ou centralisé à Internet.
- Présenter les plateformes, les cas d'utilisation et les capacités de sécurité de Cisco Secure Firewall

- Démontrer une compréhension globale des pare-feu d'application web
- Démontrer une compréhension complète des capacités de Cisco Secure Workload, des options de déploiement, des agents et des connecteurs.
- Démontrer une compréhension complète du mappage des dépendances des applications et de la découverte des politiques de Cisco Secure Workload
- Démontrer une compréhension complète des tactiques d'attaque courantes du cloud et des stratégies d'atténuation.
- Démontrer une compréhension globale des exigences et des capacités de politique de sécurité multicloud.
- Présenter les problèmes de sécurité liés à l'adoption des clouds publics et les capacités communes des outils de visibilité et d'assurance du cloud pour atténuer ces problèmes.
- Présenter Cisco Secure Network Analytics et Cisco Security Analytics and Logging
- Décrire la gestion de la surface d'attaque de Cisco
- Décrire comment les interfaces de programme d'application (API) et l'automatisation peuvent contribuer au dépannage de la politique du cloud, en particulier dans le contexte de configurations erronées.
- Démontrer une connaissance approfondie des réponses appropriées aux menaces liées au cloud dans des scénarios spécifiques
- Démontrer les connaissances complètes nécessaires à l'utilisation de l'automatisation pour la détection et la réponse aux menaces liées au cloud.

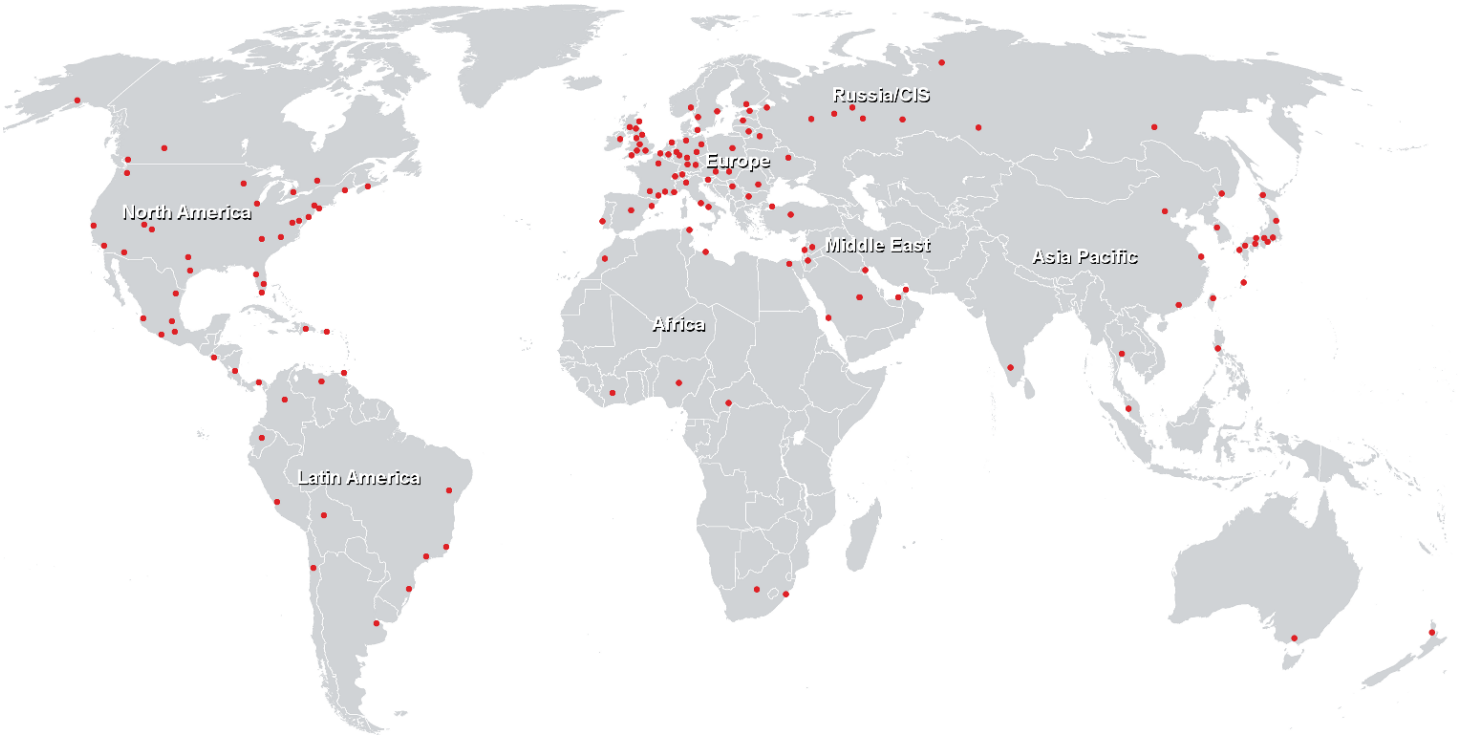
Contenu

- Cadres de sécurité sectoriels
- Principes fondamentaux de l'architecture de référence de sécurité de Cisco
- Cas d'utilisation courants de l'architecture de référence de sécurité de Cisco
- Architecture SAFE de Cisco
- Authentification des utilisateurs et des appareils basée sur des certificats
- Authentification multifactorielle Cisco Duo pour la protection des applications
- Cisco Duo avec AnyConnect VPN pour l'accès à distance
- Présentation de Cisco ISE Endpoint Compliance Services
- SSO à l'aide de SAML ou OpenID Connect
- Déploiement de la prévention des menaces sur site
- Examen du filtrage de contenu
- Exploration de Cisco Umbrella SIG
- Reverse Proxy
- Sécuriser les applications cloud avec Cisco Umbrella SIG
- Explorer Cisco SD-WAN ThousandEyes
- Optimiser les applications SaaS
- Politiques de sécurité pour l'accès à distance VPN
- Accès sécurisé Cisco
- Pare-feu sécurisé de Cisco
- Web Application Firewall
- Déploiements, agents et connecteurs Cisco Secure Workload
- Structure et politique de la charge de travail sécurisée de Cisco
- Attaques de sécurité dans le cloud et atténuations
- Politiques de sécurité multicloud
- Visibilité et assurance du nuage
- Cisco Secure Network Analytics et Cisco Secure Analytics and Logging
- Cisco XDR
- Gestion de la surface d'attaque Cisco
- Vérifications des applications dans le cloud et de l'accès aux données
- Automatisation de la politique du cloud
- Réponse aux menaces du cloud
- Automatisation de la détection et de la réponse aux menaces dans le cloud

Labs

- Explorer Cisco SecureX
- Activité interactive Windows Client BYOD Onboarding
- Utiliser Cisco Duo MFA pour protéger l'application Splunk
- Intégrer le proxy d'authentification Cisco Duo pour mettre en œuvre le MFA pour le pare-feu sécurisé de Cisco AnyConnect Remote Access VPN
- Configurer les services de conformité Cisco ISE
- Configurer la prévention des menaces
- Mettre en œuvre la sécurité Web
- Déployer la sécurité DIA avec la politique de sécurité unifiée
- Configurer les politiques DNS de Cisco Umbrella
- Déployer la passerelle Internet sécurisée Cisco Umbrella
- Mettre en œuvre la sécurité CASB
- Test de Microsoft 365 SaaS à l'aide de Cisco ThousandEyes
- Configurer l'accès à distance VPN sur le Cisco Secure Firewall Threat Defense
- Configurer les politiques de Cisco Secure Firewall
- Explorer la charge de travail Cisco Secure
- Explorer les techniques basées sur le cloud de la matrice ATT&CK
- Explorer Cisco Secure Network Analytics
- Explorer les tâches de réponse aux incidents de Cisco XDR

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch