CompTIA Security+ (SECURITY+)

ID SECURITY+ **Prix** CHF 2 860,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

Ce cours s'adresse aux professionnels de l'informatique, notamment les :

- Administrateurs de sécurité
- Spécialistes de la sécurité
- Administrateurs de systèmes
- Analystes du service d'assistance
- Ingénieurs sécurité
- Analystes de sécurité

Pré-requis

Avant de suivre ce cours accéléré, vous devriez avoir :

- 2 ans d'expérience en administration informatique avec un accent sur la sécurité
- Une compréhension des systèmes d'exploitation et des connaissances sur les systèmes basés sur Windows
- La capacité d'identifier les composants réseau de base et leurs rôles, y compris les routeurs, les commutateurs, les pare-feux et les rôles des serveurs
- Quelques connaissances en configuration de pare-feux
- Une compréhension des réseaux sans fil
- Une compréhension du modèle OSI et du TCP/IP, y compris le sous-réseautage IPv4

Nous vous recommandons également d'avoir suivi le cours CompTIA A+ et/ou CompTIA Network+ (NETWORK+).

Objectifs

À l'issue de la formation, vous devrez être en mesure de :

- Identifier et comparer les contrôles de sécurité, et mettre en œuvre des solutions cryptographiques adaptées (PKI, chiffrement, hachage, signatures numériques)
- Caractériser les acteurs des menaces, leurs motivations et les vecteurs d'attaque, et appliquer les techniques d'atténuation appropriées (segmentation, durcissement, isolation, correctifs)
- Analyser les vulnérabilités applicatives, cloud, mobiles et liées à la chaîne d'approvisionnement, et reconnaître les principales activités malveillantes
- Concevoir et évaluer des architectures de sécurité adaptées aux environnements on-premises, cloud, IoT et ICS, en assurant la protection des données et la continuité des opérations
- Sécuriser les ressources informatiques et administrer les outils de sécurité d'entreprise : pare-feu, IDS/IPS, DLP, NAC et EDR/XDR
- Mettre en œuvre une gestion des identités et des accès (provisionnement, SSO, MFA, accès privilégiés) et conduire une réponse aux incidents incluant le threat hunting et le forensics
- Appliquer les principes de gouvernance de la sécurité : politiques, gestion des risques, conformité réglementaire et gestion des risques tiers
- Planifier et interpréter les résultats d'audits et de tests d'intrusion, et mettre en œuvre un programme de sensibilisation à la sécurité

Contenu

CONCEPTS GÉNÉRAUX DE SÉCURITÉ

- Contrôles de sécurité : comparaison des contrôles techniques, préventifs, managériaux, dissuasifs, opérationnels, détectifs, physiques, correctifs, compensatoires et directifs
- Concepts fondamentaux : confidentialité, intégrité et disponibilité (CIA) ; non-répudiation ; authentification, autorisation et traçabilité (AAA) ; zero trust ; technologies de leurre et de perturbation
- Gestion du changement : processus métier, implications techniques, documentation et contrôle de version
- Solutions cryptographiques : infrastructure à clé publique (PKI), chiffrement, obfuscation, hachage, signatures numériques et blockchain

MENACES, VULNÉRABILITÉS ET ATTÉNUATIONS

- Acteurs et motivations des menaces : États-nations, attaquants non qualifiés, hacktivistes, menaces internes, crime organisé, shadow IT — motivations : exfiltration de données, espionnage, gain financier
- Vecteurs de menaces et surfaces d'attaque : messages, réseaux non sécurisés, ingénierie sociale, fichiers, appels

vocaux, chaîne d'approvisionnement, logiciels vulnérables
- Vulnérabilités : applications, matériel, appareils mobiles, virtualisation, systèmes d'exploitation, cloud, web, chaîne d'approvisionnement
- Activités malveillantes : attaques par malware, attaques sur les mots de passe, attaques applicatives, attaques physiques, attaques réseau, attaques cryptographiques
- Techniques d'atténuation : segmentation, contrôle d'accès, application des configurations, durcissement, isolation et correctifs

ARCHITECTURE DE SÉCURITÉ

- Modèles d'architecture : on-premises, cloud, virtualisation, IoT, systèmes de contrôle industriel (ICS), infrastructure as code (IaC)
- Infrastructure d'entreprise : application des principes de sécurité aux considérations d'infrastructure, sélection des contrôles, communications et accès sécurisés
- Protection des données : types de données, méthodes de sécurisation, considérations générales et classifications
- Résilience et reprise : haute disponibilité, choix de site, tests, alimentation électrique, diversité des plateformes, sauvegardes et continuité des opérations

OPÉRATIONS DE SÉCURITÉ

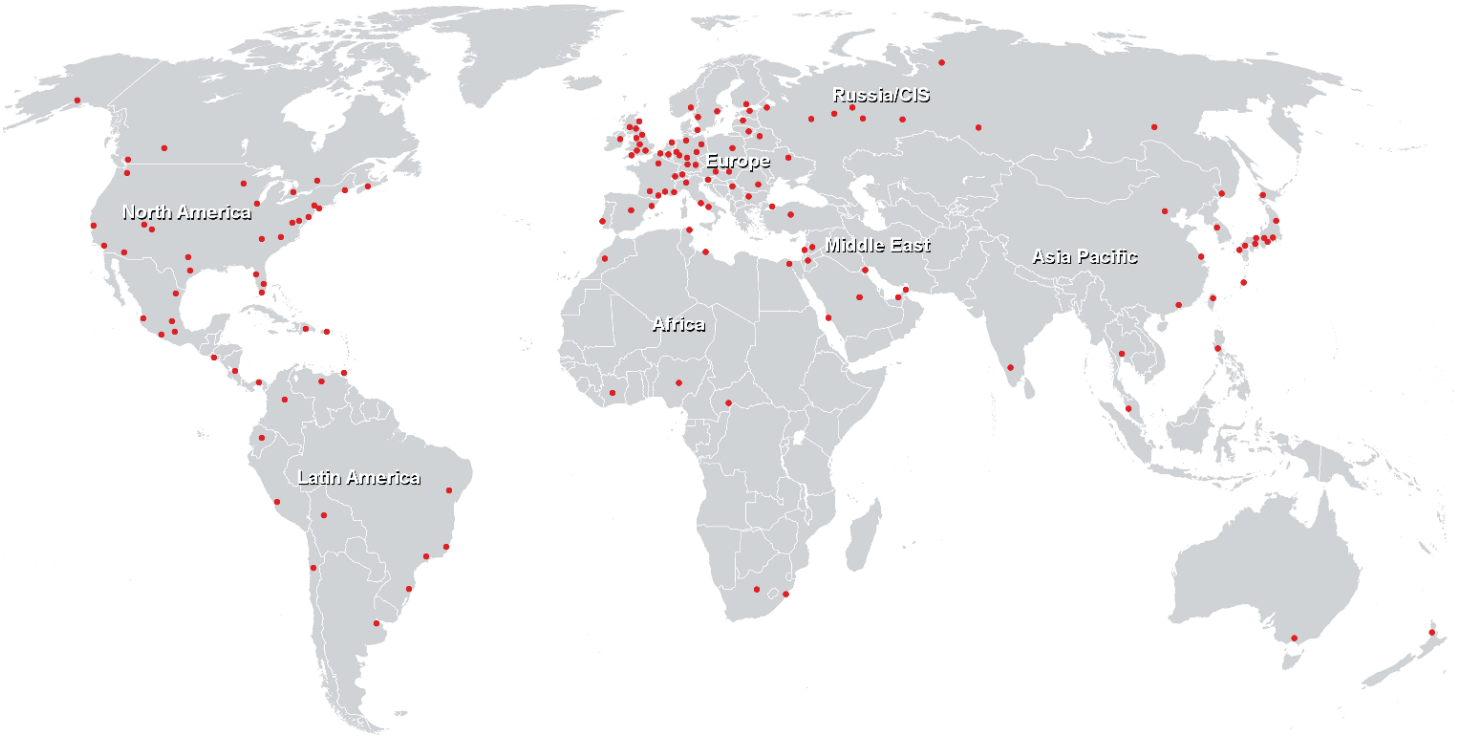
- Ressources informatiques : baselines sécurisées, solutions mobiles, durcissement, sécurité sans fil, sécurité applicative, sandboxing et supervision
- Gestion des actifs : acquisition, cession, attribution et suivi des actifs matériels, logiciels et données
- Gestion des vulnérabilités : identification, analyse, remédiation, validation et reporting des vulnérabilités
- Alertes et supervision : outils de monitoring et activités des ressources informatiques
- Sécurité d'entreprise : pare-feu, IDS/IPS, filtrage DNS, DLP (prévention des pertes de données), NAC (contrôle d'accès réseau), EDR/XDR (détection et réponse sur les endpoints)
- Gestion des identités et des accès : provisionnement, SSO (authentification unique), MFA (authentification multifacteur), outils de gestion des accès privilégiés
- Automatisation et orchestration : cas d'usage de l'automatisation, bénéfices des scripts et points de vigilance
- Réponse aux incidents : processus, formation, tests, analyse des causes racines, threat hunting et investigation numérique (forensics)
- Sources de données : utilisation des journaux d'événements et autres sources pour les investigations

GOUVERNANCE ET SUPERVISION DU PROGRAMME DE SÉCURITÉ

- Gouvernance de la sécurité : directives, politiques, standards, procédures, considérations externes, supervision, structures de gouvernance, rôles et responsabilités
- Gestion des risques : identification, évaluation, analyse, registre des risques, tolérance, appétit, stratégies, reporting et analyse d'impact métier (BIA)
- Risques tiers : évaluation et sélection des fournisseurs, accords, supervision, questionnaires et règles d'engagement
- Conformité : reporting de conformité, conséquences de la non-conformité, supervision et protection de la vie privée
- Audits et évaluations : attestation, audits internes/externes et tests d'intrusion (penetration testing)
- Sensibilisation à la sécurité : formation anti-phishing, reconnaissance des comportements anormaux, guides utilisateurs, reporting et supervision

CompTIA Security+ (SECURITY+)

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