Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

ID CCNACBR **Prix** CHF 4 495,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

- Analystes en cybersécurité de niveau Associate

Cette formation prépare à la/aux certifications

Cisco Certified Cybersecurity Associate (CCNA CYBERSECURITY)

Pré-requis

Aucun prérequis formel n'est requis pour cette formation. Toutefois, il est recommandé de posséder les connaissances et compétences suivantes avant d'y participer :

- Connaissance des réseaux Ethernet et TCP/IP
- Maîtrise opérationnelle des systèmes d'exploitation Windows et Linux
- Connaissance des concepts fondamentaux de sécurité des réseaux

Ces compétences peuvent être acquises grâce à l'offre de formation Cisco suivante :

- Implementing and Administering Cisco Solutions (CCNA)

Objectifs

A l'issue de la formation, vous serez en mesure de :

- Expliquer les principes fondamentaux des SOC, notamment leurs différents types, les rôles clés et les indicateurs essentiels permettant de mesurer leur efficacité
- Appliquer les principes fondamentaux de sécurité et les concepts de gestion des risques afin d'évaluer et protéger les actifs de l'organisation
- Comparer et appliquer différents modèles de contrôle d'accès pour sécuriser les ressources réseau et faire respecter les politiques de l'organisation
- Différencier les différents modèles de déploiement et de services cloud et expliquer le modèle de responsabilité partagée en matière de sécurité dans les environnements cloud
- Expliquer les concepts fondamentaux de la cryptographie, différencier les divers algorithmes cryptographiques et expliquer comment les principes cryptographiques sont appliqués dans les protocoles et systèmes du monde réel, notamment l'échange de clés, les signatures numériques et SSL/TLS
- Identifier et décrire les composants fondamentaux et les aspects opérationnels du système d'exploitation Windows dans le cadre de l'analyse de sécurité
- Identifier et décrire les composants fondamentaux et les aspects opérationnels du système d'exploitation Linux dans le cadre de l'analyse de sécurité
- Utiliser les interfaces en ligne de commande (CLI) pour les interactions système de base, la gestion des fichiers et les tâches liées à la sécurité dans les environnements Windows et Linux
- Expliquer le fonctionnement des protocoles réseau fondamentaux et identifier leurs implications en matière de sécurité
- Décrire et différencier les différents contrôles de sécurité réseau ainsi que leur rôle dans la protection des infrastructures réseau
- Différencier les différents systèmes de détection et de prévention d'intrusion (IDS/IPS) et interpréter leurs résultats dans le cadre de la supervision de la sécurité
- Décrire et comparer diverses solutions de sécurité des terminaux et leur efficacité face aux menaces courantes
- Identifier et catégoriser les différents acteurs de la menace cyber en fonction de leurs motivations, capacités et tactiques habituelles
- Expliquer les différentes phases du modèle classique Cyber Kill Chain et identifier les actions des attaquants à chaque étape
- Appliquer le cadre MITRE ATT&CK pour analyser et cartographier les cybermenaces, expliquer sa structure et son utilisation, et l'exploiter afin d'améliorer la détection des menaces, la réponse aux incidents et la communication au sein d'un environnement SOC
- Identifier et décrire les différents vecteurs d'attaque d'ingénierie sociale, y compris ceux renforcés par l'IA générative
- Décrire les techniques fondamentales d'attaque réseau exploitant les vulnérabilités des protocoles
- Décrire les vecteurs d'attaque avancés et les menaces

émergentes du paysage actuel de la cybersécurité
- Identifier et expliquer les différents types de données de Network Security Monitoring (NSM) et leur rôle dans les enquêtes sur les incidents
- Identifier et interpréter les différentes sources de journaux issues des systèmes d'exploitation, des équipements réseau et des outils de sécurité
- Expliquer le fonctionnement de NetFlow et son utilisation comme outil de sécurité pour la supervision réseau et la détection d'anomalies
- Décrire les attaques courantes contre les applications web et leurs méthodes d'exploitation
- Appliquer des techniques avancées d'analyse des journaux afin d'interpréter les données de sécurité et d'identifier des schémas de comportement suspects
- Réaliser des analyses de captures réseau et appliquer les processus d'investigation numérique (forensics) lors d'incidents de sécurité. L'accent est mis sur les 5 tuples et les horodatages pour la corrélation avec d'autres journaux, principal outil de l'investigation réseau
- Expliquer les résultats de l'analyse de logiciels malveillants et appliquer les cadres de renseignement sur les menaces dans les enquêtes de sécurité
- Expliquer l'architecture, les fonctions principales et les bonnes pratiques de mise en œuvre des solutions SIEM pour une supervision efficace de la sécurité
- Expliquer les fonctionnalités et les cas d'usage courants des plateformes SOAR pour automatiser et rationaliser la réponse aux incidents
- Expliquer la plateforme Cisco XDR, ses fonctions principales, ses fonctionnalités et ses composants pour une détection et une réponse unifiées aux menaces
- Différencier les recommandations historiques et modernes du NIST en matière de réponse aux incidents (NIST SP 800-61 Rev 2 et Rev 3), décrire les composants clés de la réponse aux incidents alignés sur le cadre NIST CSF 2.0 et identifier comment ces pratiques répondent aux exigences CMMC pour la Defense Industrial Base (DIB)
- Décrire les rôles, les catégories et les services opérationnels des équipes de réponse aux incidents de sécurité informatique (CSIRT)
- Expliquer le concept des playbooks de supervision de la sécurité et leurs composants pour standardiser la réponse aux incidents
- Appliquer différentes méthodologies de chasse aux menaces (threat hunting) afin d'identifier et de réduire de manière proactive les menaces cachées au sein d'un réseau

- Modèles de contrôle d'accès
- Modèles de sécurité cloud
- Cryptographie pour les opérations de sécurité
- Fondamentaux du système Windows
- Fondamentaux du système Linux
- Utilisation des CLI en sécurité
- Protocoles réseau
- Contrôles de sécurité réseau
- IDS et IPS
- Sécurité des terminaux
- Acteurs de la menace
- Modèle Cyber Kill Chain
- Cadre MITRE ATT&CK
- Attaques d'ingénierie sociale
- Fondamentaux des attaques réseau
- Paysage avancé des menaces
- Données de supervision réseau (NSM)
- Sources de données de journaux
- NetFlow pour la supervision de la sécurité
- Attaques des applications web
- Analyse avancée des journaux
- Capture de paquets et investigation numérique (forensics)
- Logiciels malveillants et renseignement sur les menaces
- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation and Response)
- XDR (Extended Detection and Response)
- Planification de la réponse aux incidents
- Rôles et opérations des CSIRT
- Playbooks de supervision de la sécurité
- Méthodologies de Threat Hunting

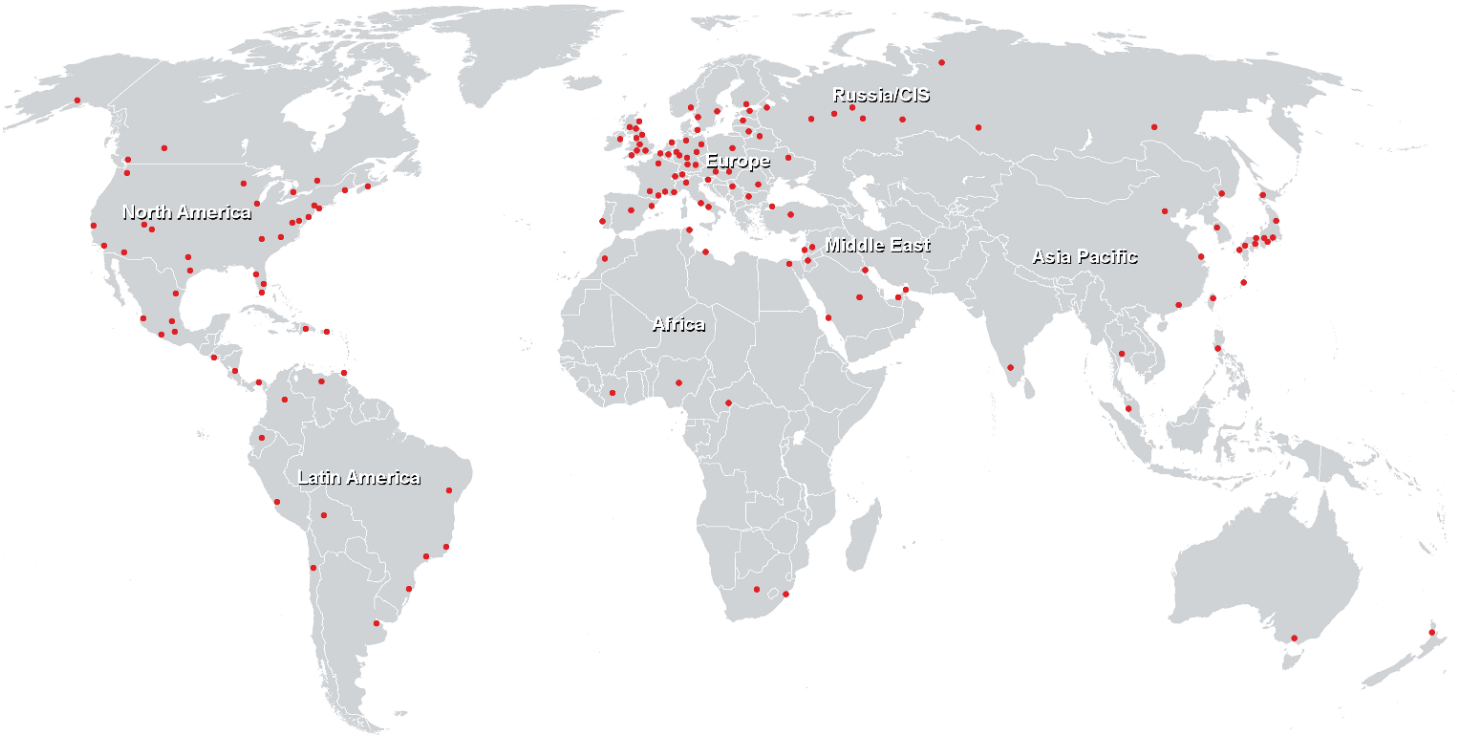
Labs

- Découvrir les technologies cryptographiques
- Découvrir le système d'exploitation Windows
- Découvrir le système d'exploitation Linux
- Découvrir la sécurité des terminaux
- Étudier la méthodologie des hackers
- Découvrir les attaques TCP/IP
- Étudier les menaces persistantes avancées (APT)
- Utiliser les outils NSM pour analyser les catégories de données
- Analyser une activité DNS suspecte
- Étudier les attaques basées sur le navigateur
- Corréler les journaux d'événements, fichiers PCAP et alertes liés à une attaque
- Découvrir les playbooks SOC
- Rechercher du trafic malveillant

Contenu

- Opérations de sécurité
- Principes de sécurité

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