Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

ID CBROPS **Prix** CHF 4 670,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

- Analystes en cybersécurité de niveau associé qui travaillent dans des centres d'opérations de sécurité.

Cette formation prépare à la/aux certifications

Cisco Certified CyberOps Associate (CCCA)

Pré-requis

Avant de suivre ce cours, vous devez posséder les connaissances et compétences suivantes :

- Compétences et connaissances équivalentes à celles acquises dans le Implementing and Administering Cisco Solutions (CCNA).
- Familiarité avec les réseaux Ethernet et TCP/IP.
- Connaissance pratique des systèmes d'exploitation Windows et Linux.
- Familiarité avec les concepts de base de la sécurité des réseaux.

Le cours Cisco suivant peut vous aider à acquérir les connaissances nécessaires à la préparation de ce cours :

Implementing and Administering Cisco Solutions (CCNA)

Objectifs

À l'issue de ce cours, vous serez capable de :

- Expliquer le fonctionnement d'un SOC et décrire les différents types de services qui sont effectués du point de vue d'un analyste SOC de niveau 1.
- Expliquer les outils de surveillance de la sécurité des réseaux (Network Security Monitoring - NSM) qui sont disponibles pour l'analyste de la sécurité des réseaux.
- Expliquer les données qui sont disponibles pour l'analyste de la sécurité des réseaux.
- Décrire les concepts de base et les utilisations de la cryptographie.
- Décrire les failles de sécurité dans le protocole TCP/IP et comment elles peuvent être utilisées pour attaquer les réseaux et les hôtes.
- Comprendre les technologies courantes de sécurité des terminaux.
- Comprendre la chaîne d'élimination et les modèles de diamant pour les enquêtes sur les incidents, et l'utilisation de kits d'exploitation par les acteurs de la menace.
- Identifier les ressources pour la chasse aux cybermenaces.
- Expliquer la nécessité de la normalisation des données d'événements et la corrélation des événements.
- Identifier les vecteurs d'attaque courants.
- Identifier les activités malveillantes.
- Identifier les modèles de comportements suspects.
- Mener des enquêtes sur les incidents de sécurité.
- Expliquer l'utilisation d'un playbook typique dans le SOC.
- Expliquer l'utilisation des métriques SOC pour mesurer l'efficacité du SOC.
- Expliquer l'utilisation d'un système de gestion des flux de travail et l'automatisation pour améliorer l'efficacité du SOC.
- Décrire un plan typique de réponse aux incidents et les fonctions d'un CSIRT typique.
- Expliquer l'utilisation de VERIS pour documenter les incidents de sécurité dans un format standard.
- Décrire les caractéristiques et les fonctionnalités du système d'exploitation Windows.
- Décrire les caractéristiques et les fonctionnalités du système d'exploitation Linux.

Ce cours vous aidera à :

- Acquérir les connaissances et les compétences pour mettre en œuvre un protocole qui modernise et adapte votre infrastructure réseau.
- Apprendre une formation pratique pour rationaliser, concevoir et configurer des mesures de sécurité pour fortifier vos réseaux contre les attaques de cybersécurité.

Contenu

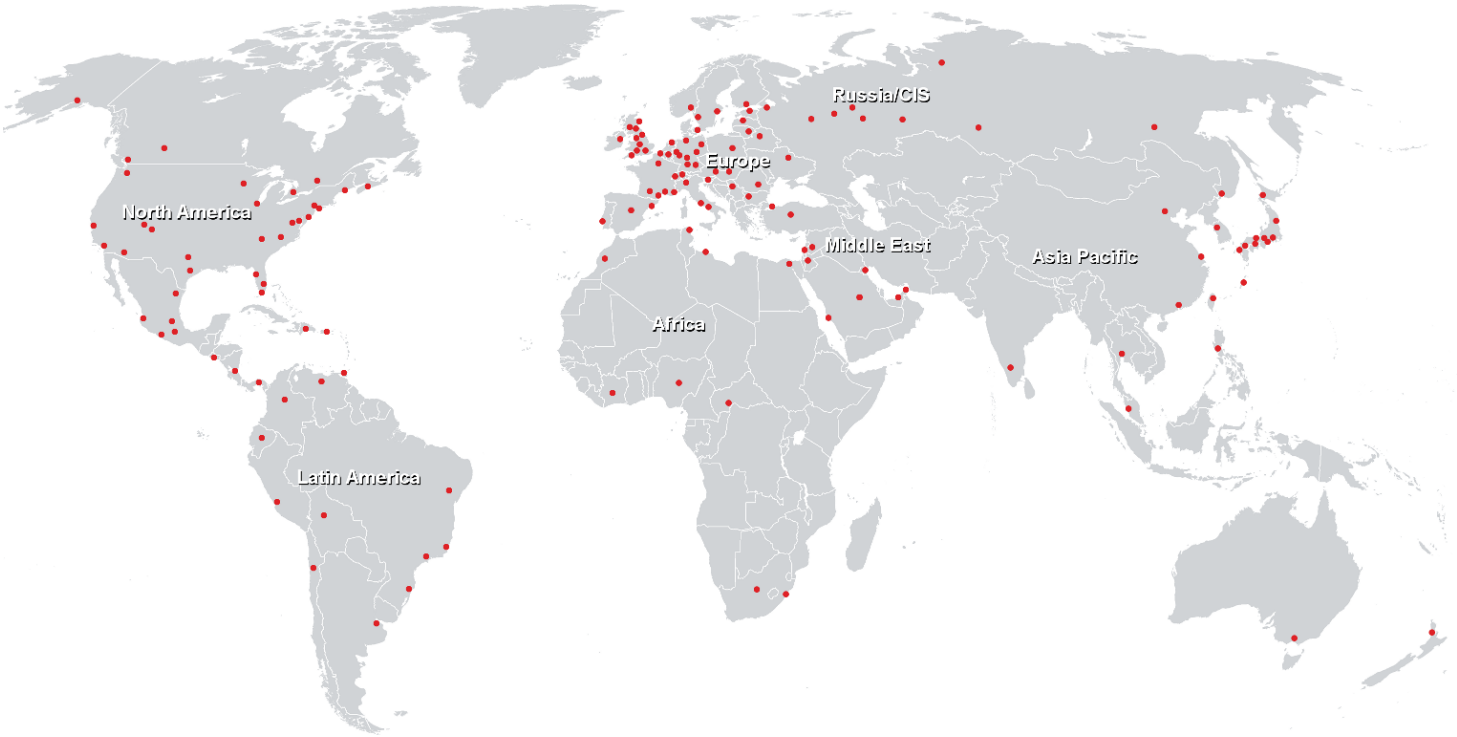
- Définir le centre des opérations de sécurité
- Comprendre l'infrastructure réseau et les outils de

surveillance de la sécurité réseau
- Explorer les catégories de types de données
- Comprendre les concepts de base de la cryptographie
- Comprendre les attaques TCP/IP courantes
- Comprendre les technologies de sécurité des points finaux
- Comprendre l'analyse des incidents dans un SOC centré sur les menaces.
- Identifier les ressources pour la chasse aux cybermenaces
- Comprendre la corrélation et la normalisation des événements
- Identification des vecteurs d'attaque courants
- Identifier les activités malveillantes
- Identifier les modèles de comportements suspects
- Mener des enquêtes sur les incidents de sécurité
- Utiliser un modèle de Playbook pour organiser la surveillance de la sécurité
- Comprendre les mesures du SOC
- Comprendre le flux de travail et l'automatisation du SOC
- Décrire la réponse aux incidents
- Comprendre l'utilisation de VERIS
- Comprendre les bases du système d'exploitation Windows
- Comprendre les bases du système d'exploitation Linux

Laboratoires

- Configuration de l'environnement initial du laboratoire de collaboration
- Utiliser les outils NSM pour analyser les catégories de données
- Explorer les technologies cryptographiques
- Explorer les attaques TCP/IP
- Explorer la sécurité des points de terminaison
- Étudier la méthodologie des pirates informatiques
- Traquer le trafic malveillant
- Corréler les journaux d'événements, les PCAP et les alertes d'une attaque.
- Enquêter sur les attaques par navigateur
- Analyser les activités DNS suspectes
- Explorer les données de sécurité pour analyse
- Enquêter sur les activités suspectes à l'aide de Security Onion
- Étudier les menaces persistantes avancées
- Explorer les Playbooks SOC
- Explorer le système d'exploitation Windows
- Explorer le système d'exploitation Linux

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer GmbH

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

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