# Performing CyberOps Using Cisco Security Technologies (CBRCOR)

**ID** CBRCOR **Prix** CHF 4 200,– (Hors Taxe) **Durée** 5 jours

## A qui s'adresse cette formation

Bien qu'il n'y ait pas de conditions préalables obligatoires, le cours est particulièrement adapté aux publics suivants :

- Ingénieur en cybersécurité
- Investigateur en cybersécurité
- Gestionnaire d'incidents
- Intervenant en cas d'incident
- Ingénieur réseau
- Analystes SOC occupant un poste de niveau débutant avec un minimum d'un an d'expérience.

## Cette formation prépare à la/aux certifications

Cisco Certified Cybersecurity Professional (CCCP)

## Pré-requis

Bien qu'il n'y ait pas de conditions préalables obligatoires, pour profiter pleinement de ce cours, vous devez avoir les connaissances suivantes :

- Familiarité avec les shells UNIX/Linux (bash, csh) et les commandes shell.
- Familiarité avec les fonctions de recherche et de navigation de Splunk.
- Compréhension de base de l'écriture de scripts à l'aide d'un ou plusieurs des langages suivants : Python, JavaScript, PHP ou similaire.

Offres recommandées de Cisco qui peuvent vous aider à vous préparer à ce cours :

- Implementing and Administering Cisco Solutions (CCNA)
- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

## Objectifs

Après avoir suivi ce cours, vous devriez être en mesure de :

- Décrire les types de services couverts par un SOC et les responsabilités opérationnelles associées à chacun.
- Comparer les considérations d'opérations de sécurité des plateformes cloud.
- Décrire les méthodologies générales de développement, de gestion et d'automatisation des plateformes SOC.
- Expliquer la segmentation des actifs, la ségrégation, la segmentation du réseau, la micro-segmentation, et les approches de chacun, dans le cadre des contrôles et protections des actifs.
- Décrire la confiance zéro et les approches associées, dans le cadre du contrôle et de la protection des actifs.
- Effectuer des enquêtes sur les incidents en utilisant la gestion des informations et des événements de sécurité (SIEM) et/ou l'orchestration et l'automatisation de la sécurité (SOAR) dans le SOC.
- Utiliser différents types de plateformes technologiques de sécurité de base pour la surveillance, l'investigation et la réponse en matière de sécurité.
- Décrire les processus DevOps et SecDevOps.
- Expliquer les formats de données courants, par exemple, JavaScript Object Notation (JSON), HTML, XML, Comma-Separated Values (CSV).
- Décrire les mécanismes d'authentification API.
- Analyser l'approche et les stratégies de détection des menaces, pendant la surveillance, l'enquête et la réponse.
- Déterminer les indicateurs de compromission (IOCs) et les indicateurs d'attaque (IOAs) connus.)
- Interpréter la séquence des événements lors d'une attaque basée sur l'analyse des modèles de trafic.
- Décrire les différents outils de sécurité et leurs limites pour l'analyse des réseaux (par exemple, les outils de capture de paquets, les outils d'analyse du trafic, les outils d'analyse des journaux réseau).
- Analyser les comportements anormaux des utilisateurs et des entités (UEBA).
- Effectuer une chasse proactive aux menaces en suivant les meilleures pratiques.

## Contenu

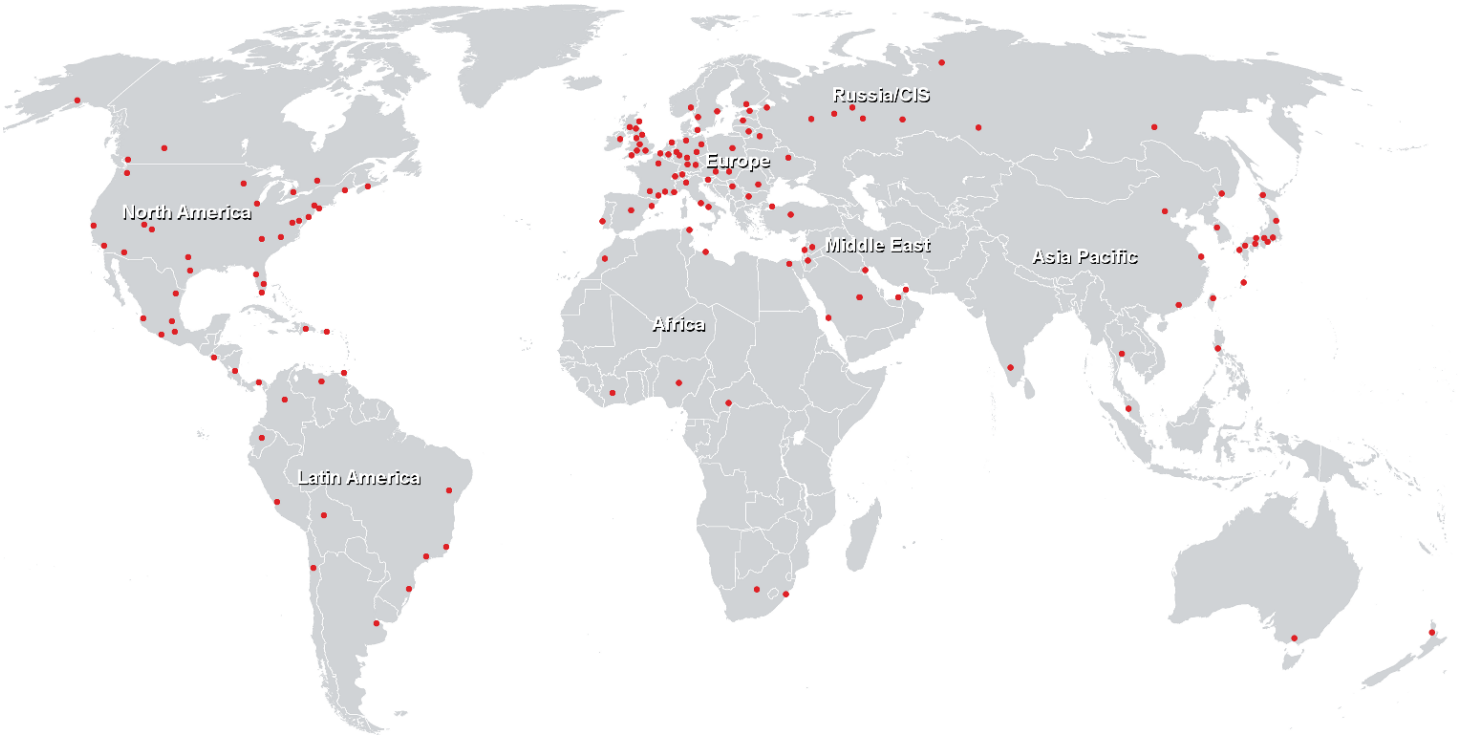
- Comprendre la gestion des risques et les opérations SOC
- Comprendre les processus analytiques et les playbooks
- Analyser les captures de paquets, les journaux et l'analyse

du trafic
- Analyser les logs des terminaux et des appliances
- Comprendre les responsabilités en matière de sécurité des modèles de services cloud.
- Comprendre les actifs de l'environnement de l'entreprise
- Mise en œuvre du Threat Tuning
- Pratiques de recherche et de renseignement sur les menaces
- Comprendre les API
- Comprendre les modèles de développement et de déploiement du SOC
- Analyser la sécurité et produire des rapports dans un SOC
- Notions de base sur les logiciels malveillants (Malware Forensics)
- Notions de base sur la chasse aux menaces
- Enquêter sur les incidents et y répondre

**Labs**

- Explorer l'orchestration Cisco SecureX
- Explorer les Playbooks Splunk Phantom
- Examiner les captures de paquets de Cisco Firepower et l'analyse PCAP
- Valider une attaque et déterminer la réponse à l'incident.
- Soumettre un fichier malveillant à Cisco Threat Grid pour analyse
- Scénario d'attaque basé sur les points d'accès en se référant à MITRE ATTACK
- Évaluer les actifs dans un environnement d'entreprise typique
- Explorer la politique de contrôle d'accès de Cisco Firepower NGFW et les règles Snort.
- Examiner les IOC du blog Cisco Talos à l'aide de Cisco SecureX
- Explorer la plateforme de renseignements sur les menaces ThreatConnect
- Suivre les TTP d'une attaque réussie en utilisant un TIP
- Interroger Cisco Umbrella à l'aide du client API Postman
- Corriger un script d'API Python
- Créer des scripts de base Bash
- Reverse Engineering d'un logiciel malveillant
- Effectuer une chasse aux menaces
- Réaliser une réponse à un incident

**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**