Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)

ID CBRTHD **Prix** CHF 3 890,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

- Personnel du centre des opérations de sécurité
- Analystes de niveau 2 du centre des opérations de sécurité (SOC)
- Chasseurs de menaces
- Analystes des cybermenaces
- Gestionnaires de menaces
- Gestionnaires des risques

Cette formation prépare à la/aux certifications

Cisco Certified Cybersecurity Professional (CCNP CYBERSECURITY)

Pré-requis

Les connaissances et compétences que vous êtes censé avoir avant de suivre cette formation sont les suivantes :

- Connaissances générales des réseaux
- Certification Cisco CCNP Security

Ces compétences peuvent être acquises dans les formations Cisco suivantes :

- Implementing and Administering Cisco Solutions (CCNA)
- !Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Performing CyberOps Using Cisco Security Technologies (CBRCOR)
- Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Objectifs

- Définir la chasse aux menaces et identifier les concepts clés utilisés pour mener des investigations de chasse aux menaces
- Examiner les concepts d'investigation de chasse aux menaces, les cadres de travail et les modèles de menaces
- Définir les fondamentaux du processus de chasse aux cybermenaces
- Définir les méthodologies et procédures de chasse aux menaces
- Décrire la chasse aux menaces basée sur le réseau
- Identifier et examiner la chasse aux menaces basée sur les points de terminaison
- Identifier et examiner les menaces basées sur la mémoire des points de terminaison et développer la détection de menaces basée sur les points de terminaison
- Définir les méthodes, processus et outils Cisco qui peuvent être utilisés pour la chasse aux menaces
- Décrire le processus de chasse aux menaces d'un point de vue pratique
- Décrire le processus de rapport de chasse aux menaces

Contenu

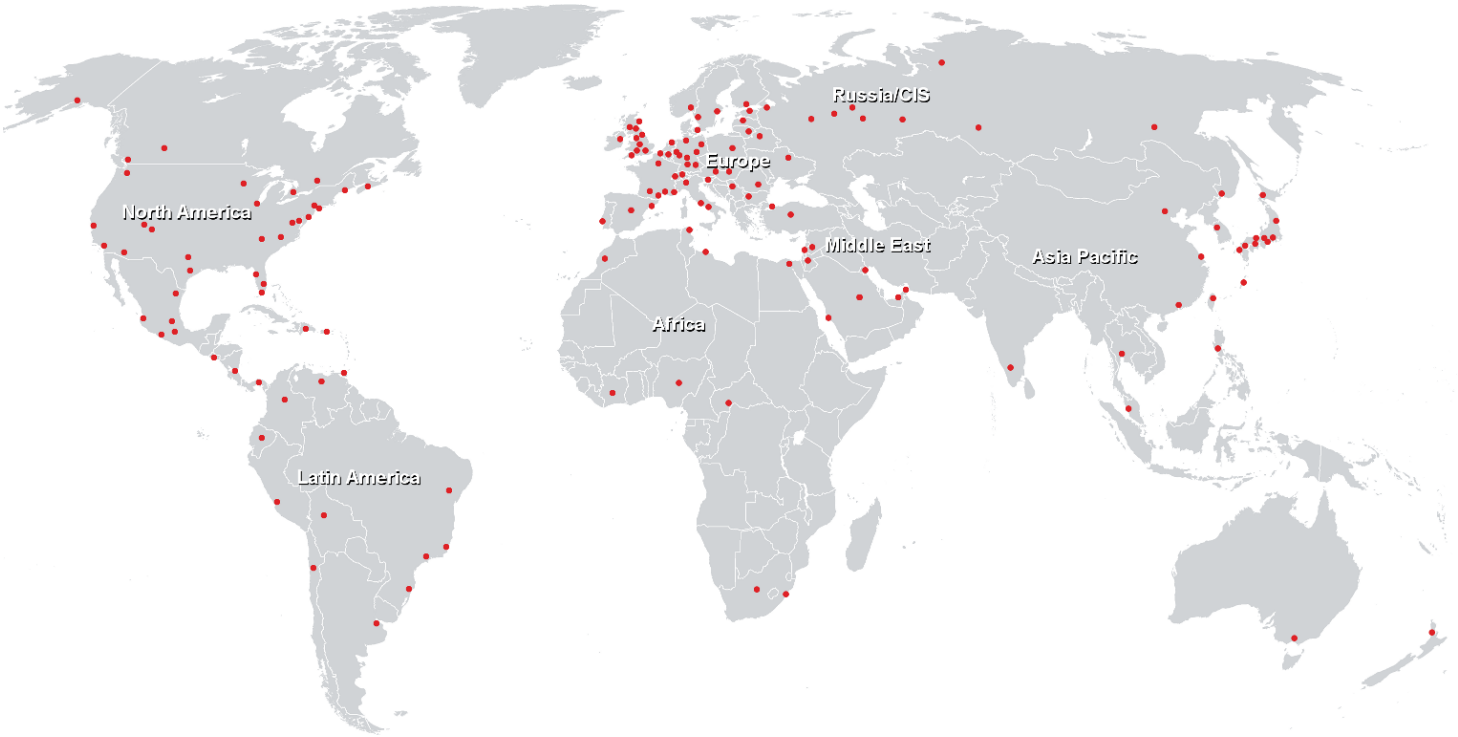
- Théorie de la chasse aux menaces
- Concepts, cadres et modèles de menaces pour la chasse aux menaces
- Fondamentaux du processus de chasse aux menaces
- Méthodologies et procédures de chasse aux menaces
- Chasse aux menaces basée sur le réseau
- Chasse aux menaces basée sur les points de terminaison
- Développement de la détection des menaces basée sur les points de terminaison
- Chasse aux menaces avec les outils Cisco
- Résumé de l'enquête de chasse aux menaces : une approche pratique
- Rapport sur les résultats d'une enquête de chasse aux menaces

Labs

- Catégoriser les menaces avec les tactiques et techniques de MITRE ATTACK
- Comparer les techniques utilisées par différents APTs avec MITRE ATTACK Navigator
- Modéliser les menaces en utilisant MITRE ATTACK et D3FEND
- Prioriser la chasse aux menaces en utilisant le cadre MITRE ATTACK et la Cyber Kill Chain
- Déterminer le niveau de priorité des attaques avec MITRE

CAPEC
- Explorer la méthodologie TaHiTI
- Effectuer des recherches d'analyse de menaces en utilisant l'OSINT
- Attribuer les menaces à des groupes d'adversaires et des logiciels avec MITRE ATTACK
- Émuler des adversaires avec MITRE Caldera
- Trouver des preuves de compromission en utilisant des outils natifs de Windows
- Rechercher des activités suspectes en utilisant des outils open source et SIEM
- Capture de trafic réseau
- Extraction d'IOC à partir de paquets réseau
- Utilisation de la pile ELK pour la chasse aux grandes quantités de données réseau
- Analyser les journaux d'événements Windows et les mapper avec la matrice MITRE
- Acquisition de données des points de terminaison
- Inspecter les points de terminaison avec PowerShell
- Effectuer de la forensic mémoire avec Velociraptor
- Détecter des processus malveillants sur les points de terminaison
- Identifier des fichiers suspects en utilisant l'analyse des menaces
- Mener la chasse aux menaces en utilisant Cisco Secure Firewall, Cisco Secure Network Analytics, et Splunk
- Mener une chasse aux menaces en utilisant le centre de contrôle Cisco XDR et Investigate
- Initier, mener et conclure une chasse aux menaces

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