Cetified Threat Intelligence Analyst (CTIA)

Description

Devenez un expert en intelligence sur les menaces avec la certification CTIA

La certification Certified Threat Intelligence Analyst (CTIA) est conçue pour les professionnels de la cybersécurité qui souhaitent maîtriser les compétences critiques en matière de veille sur les menaces. Cette formation approfondie vous permettra de comprendre et d'analyser les menaces cybernétiques actuelles tout en développant des stratégies proactives pour protéger les infrastructures. Grâce à des modules spécialisés et une approche pratique, vous apprendrez à transformer les menaces inconnues en informations exploitables.

Avec le rôle croissant de la cybersécurité dans les entreprises, cette formation est indispensable pour tous ceux qui veulent sécuriser les systèmes contre les cyberattaques. En suivant cette formation, vous serez capable de prendre des décisions éclairées en matière de sécurité, de gérer les menaces émergentes et de collaborer efficacement au sein d'équipes SOC.

Niveau
Intermédiaire
Contenu du cours
Module 1 : Introduction à la veille sur les menaces

- Comprendre le renseignement
- Résumer le concept de renseignement sur les cybermenaces
- Expliquer le cycle de vie et les cadres de Threat Intelligence
- Comprendre les plateformes de renseignements sur les menaces (TIP)
- Comprendre les renseignements sur les menaces dans l'environnement cloud
- Comprendre les tendances futures et l'apprentissage continu

Module 2 : Cybermenaces et cadres d'attaque

- Comprendre les cybermenaces
- Expliquer les menaces persistantes avancées
- Expliquer la chaîne de cyber-kills
- Expliquer MITRE ATT&CK et le modèle Diamond
- Comprendre les indicateurs de compromis

Module 3 : Exigences, planification, orientation et examen

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

- Comprendre le paysage actuel des menaces de l'organisation
- Comprendre l'analyse des exigences
- Planifier un programme de renseignement sur les menaces
- Établir un soutien à la gestion
- Construire une équipe de renseignement sur les menaces
- Comprendre le partage de renseignements sur les menaces
- Examiner le programme de renseignement sur les menaces

Module 4 : Collecte et traitement des données

- Comprendre la collecte de données sur les menaces
- Résumer la gestion de la collecte de renseignements sur les menaces
- Expliquer les flux et les sources de renseignements sur les menaces
- Expliquer la collecte et l'acquisition de données sur les menaces
- Comprendre la collecte de données en masse
- Expliquer le traitement et l'exploitation des données
- Comprendre la collecte et l'enrichissement des données sur les menaces dans les environnements cloud

Module 5 : Analyse des données

- Résumer l'analyse des données
- Expliquer les techniques d'analyse des données
- Comprendre l'analyse des menaces
- Démontrer le processus d'analyse des menaces
- Expliquer l'analyse fine des menaces
- Comprendre l'évaluation des renseignements sur les menaces
- Créer des runbooks et une base de connaissances
- Utiliser les outils de renseignement sur les menaces

Module 6 : Rapports et diffusion du renseignement

- Comprendre les rapports de renseignements sur les menaces
- Comprendre la diffusion
- Participer au partage des relations
- Comprendre le partage de renseignements sur les menaces
- Expliquer les mécanismes de livraison
- Utiliser la plateforme de partage de renseignements sur les menaces
- Comprendre les lois et règlements sur le partage de renseignements
- Expliquer l'intégration des renseignements sur les menaces
- Comprendre le partage d'intelligence et la collaboration à l'aide des scripts Python

Module 7 : Chasse et détection des menaces

- Résumer les concepts de chasse aux menaces
- Comprendre l'automatisation de la chasse aux menaces

Module 8 : Intelligence sur les menaces dans les opérations SOC, la réponse aux incidents et la gestion des risques

- Comprendre les renseignements sur les menaces dans les opérations SOC
- Comprendre les renseignements sur les menaces dans la gestion des risques
- Comprendre les renseignements sur les menaces dans la réponse aux incidents

Documentation

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification Certified Threat Intelligence Analyst.
- Pour obtenir la certification Certified Threat Intelligence Analyst, les candidats doivent réussir l'examen : 312-85.
- Nombre de questions : 50
- Durée : 2 heures
- Si vous souhaitez passer cet examen, veuillez contacter notre secrétariat qui vous informera du coût des examens et prendra en charge toutes les démarches administratives nécessaires pour vous.

Profils des participants

- Ethical Hacker
- Professionnels de la sécurité
- Analystes en cybersécurité
- Consultants en sécurité informatique
- Ingénieurs SOC
- Architectes de sécurité

Connaissances Préalables

- Compréhension de base des concepts de cybersécurité
- Connaissance des principales menaces et attaques cybernétiques
- Expérience avec les outils de gestion de la sécurité
- Notions d'analyse des données en cybersécurité

Objectifs

- Comprendre le renseignement sur les cybermenaces
- Analyser les cadres et cycles de vie des menaces
- Maîtriser les plateformes de Threat Intelligence
- Collecter et traiter les données sur les menaces
- Analyser les menaces et leurs impacts
- Générer des rapports précis et exploitables
- Collaborer efficacement dans la chasse aux menaces

Description
Formation Cetified Threat Intelligence Analyst (CTIA)
Prix de l'inscription en Présentiel (CHF)
3950
Prix de l'inscription en Virtuel (CHF)
3800
Durée (Nombre de Jours)
3
Reference
CTIA

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.