CERTIFIED THREAT INTELLIGENCE ANALYST

Découvrez les menaces internes et externes en apprenant une méthodologie solide basée sur un JTA (Job Task Analysis)

Code : CTIA

NOUVEAUTÉ

Certified Threat Intelligence Analyst (C|TIA) est une formation certifiante conçue et développée en collaboration avec des experts en cybersécurité et en renseignements. Elle a pour objectif d'aider les organismes à identifier et réduire les risques au sein d'une entreprise en découvrant des menaces internes et externes jusqu'ici inconnues.
Cette formation de 3 jours, rigoureusement basée sur un Job Task Analysis (JTA), enseigne une méthodologie détaillée afin établir une threat intelligence efficace.
Dans un monde où les menaces se font de plus en plus précises, le C|TIA couvre des concepts allant de la planification du projet de threat intelligence jusqu'à l'élaboration d'un rapport et de sa diffusion.
Grâce aux laboratoires EC-Council, 40% de la formation est consacré à l'apprentissage de compétences pratiques pour permettre aux apprenants d'acquérir une expérience pratique des derniers outils, techniques, méthodologies, cadres, scripts, etc. de renseignement sur les menaces. Ces labs se compose des derniers systèmes d'exploitation, y compris Windows 10 et Kali Linux, pour la planification, la collecte, l'analyse, l'évaluation et la diffusion de renseignements sur les menaces.

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).
Modalités d'évaluation : En amont de la formation, une évaluation des compétences de l'apprenant est effectuée. Ensuite, les objecti fs sont régulièrement évalués tout au long de la formation (40% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur, puis par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Introduction to Threat Intelligence
- **Module 2 :** Cyber Threats and Attack Frameworks
- **Module 3 :** Requirements, Planning, Direction, and Review
- **Module 4 :** Data Collection and Processing
- **Module 5 :** Data Analysis
- **Module 6 :** Intelligence Reporting and Dissemination
- **Module 7 :** Threat Hunting and Detection
- **Module 8 :** Threat Intelligence in SOC Operations, Incident Response, and Risk Management

CERTIFICATION CSA
(incluse avec la formation)

Passage de l'examen : l'examen CTIA (312-38) aura lieu à distance, depuis le lieu de votre choix.

- **Titre de l'examen :** Certified Threat Intelligence Analyst
- **Nombre de questions :** 50
- **Durée :** 2 heures
- **Score requis :** 70%

RÉSULTAT

Directement disponible en fin d'examen.

PROCHAINES DATES 4 MARS - 11 MAI - 14 SEPT - 16 NOV

OBJECTIFS

- Connaître les principes fondamentaux du renseignement sur les menaces (y compris les types de renseignement sur les menaces, le cycle de vie, la stratégie, les capacités, le modèle de maturité, les cadres, etc.)
- Planifier les différentes étapes d'un programme de renseignement sur les menaces (exigences, planification, orientation et examen)
- Collecter et acquérir des données de renseignement sur les menaces par le biais du renseignement de source ouverte (OSINT), du renseignement humain (HUMINT), du cyber contre-espionnage (CCI), des indicateurs de compromission (IoC) et de l'analyse des logiciels malveillants
- Maîtriser le processus complet d'analyse des menaces comprenant la modélisation des menaces, la mise au point, l'évaluation, le runbook et la création d'une base de connaissances.
- Découvrir différents outils d'analyse des données, de modélisation des menaces et de renseignement sur les menaces

INFORMATIONS GÉNÉRALES

Code : CTIA

Durée : 3 jours

Prix : 2 590 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) - en présentiel uniquement

Examen : inclus. Valable 12 mois à date de réception. Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Hacker étique
- Professionnels de la sécurité, Ingénieurs, Analystes, Spécialistes, Architectes, Managers
- Analyste Threat Intelligence, Consultant, Chercheurs, Diplômés
- Professionnels SOC
- Analystes Malware et de forensique digital
- Membre d'une équipe d'intervention en cas d'incident
- Tout professionnel de la cybersécurité ayant une expérience minimum de 3-5 ans

PRÉ-REQUIS

Il n'y a pas de conditions préalables à la participation au cours, mais pour s'inscrire à l'examen, il faut pouvoir justifier d'une expérience professionnelle d'au moins trois ans dans le domaine de la sécurité de l'information ou de la conception de logiciels.

RESSOURCES

- Support de cours officiel
- 40% d'exercices pratiques
- 1 PC par personne