EC-Council Certified Threat Intelligence Analyst + Voucher d'examen

Durée: 3 Jours **Réf de cours: CTIA**

Résumé:

Certified Threat Intelligence Analyst (C|TIA) est un programme de formation et d'accréditation conçu et développé en collaboration avec des experts en cybersécurité et en renseignement sur les menaces du monde entier afin d'aider les organisations à identifier et à atténuer les risques commerciaux en convertissant les menaces internes et externes inconnues en menaces connues. Il s'agit d'un programme complet de niveau spécialiste qui enseigne une approche structurée pour la mise en place d'une veille efficace sur les menaces.

Le programme s'appuie sur une analyse rigoureuse des tâches à accomplir dans le domaine du renseignement sur les menaces. Ce programme différencie les professionnels du renseignement sur les menaces des autres professionnels de la sécurité de l'information. Il s'agit d'un programme de formation intensif de trois jours, hautement interactif, complet, basé sur des normes, qui apprend aux professionnels de la sécurité de l'information à développer une veille professionnelle sur les menaces.

Plus de 40 % du temps de cours est consacré à l'apprentissage de compétences pratiques, et ce grâce aux laboratoires EC-Council. Le ratio théorie/pratique du programme C|TIA est de 60:40, ce qui permet aux étudiants d'acquérir une expérience pratique des derniers outils, techniques, méthodologies, cadres, scripts, etc. de renseignement sur les menaces. Le programme C|TIA est intégré à des laboratoires afin de mettre l'accent sur les objectifs d'apprentissage.
L'environnement de labs du C|TIA 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.
Mise à jour : 16.05.2024

Public visé:

Cette formation s'adresse à tout professionnel de la cybersécurité qui doit comprendre comment rassembler de grandes quantités d'informations pertinentes sur les menaces à partir d'une multitude de sources de renseignements, qui peuvent ensuite être analysées pour fournir des renseignements sur les menaces qui prédisent avec précision les menaces potentielles auxquelles une organisation peut être confrontée. Ces personnes peuvent remplir des rôles tels que : Hackers éthiques, analystes de renseignements sur les menaces, chasseurs de menaces, professionnels SOC, analystes en criminalistique numérique et en logiciels malveillants, réponse aux incidents,

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Types de cybermenaces, acteurs de la menace et leurs motivations, buts et objectifs des attaques de cybersécurité
- 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.)
- Méthodologie de la chaîne de la mort cybernétique, cycle de vie des menaces persistantes avancées (APT), tactiques, techniques et procédures (TTP), indicateurs de compromission (IoC) et pyramide de la douleur.
- Les différentes étapes de la planification d'un programme de renseignement sur les menaces (exigences, planification, orientation et examen)
- Différents types de flux de données, de sources et de méthodes de collecte de données
- Collecte et acquisition de données de renseignement sur les menaces par le biais du renseignement de source ouverte (OSINT), du renseignement humain (HUMINT), du cybercontre-espionnage (CCI), des indicateurs de compromission (IoC) et de l'analyse des logiciels malveillants.
- Collecte et la gestion de données en masse (traitement, structuration, normalisation, échantillonnage, stockage et visualisation des données)
- Différents types et techniques d'analyse des données, notamment l'analyse statistique des données, l'analyse des hypothèses concurrentes (ACH), l'analyse structurée des hypothèses concurrentes (SACH), etc.)
- 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.
- Différents outils d'analyse des données, de modélisation des menaces et de renseignement sur les menaces

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.

Test et certification

Recommandé comme préparation aux examens suivants :

312-85 - Analyste certifié en renseignement sur les menaces (Certified Threat Intelligence Analyst)

Pour obtenir cette certification, vous devrez prouver que vous avez suivi des cours auprès d'un partenaire accrédité par EC-Council et 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.

Contenu:

Introduction au renseignement sur les menaces

- Comprendre le renseignement
- Comprendre le renseignement sur les cybermenaces
- Vue d'ensemble du cycle de vie et des cadres du renseignement sur les menaces

Cybermenaces et méthodologie de la chaîne de la mort

- Comprendre les cybermenaces
- Comprendre les menaces persistantes avancées (APT)
- Comprendre la chaîne d'élimination des cybermenaces
- Comprendre les indicateurs de compromission (IoC)

Exigences, planification, orientation et examen

- Comprendre le paysage actuel des menaces de l'organisation
- Comprendre l'analyse des besoins
- Planification du programme de renseignement sur les menaces
- Mise en place du soutien de la direction
- Mise en place d'une équipe de renseignement sur la menace
- Vue d'ensemble de l'échange de renseignements sur les menaces
- Examen du programme de renseignement sur la menace

Collecte et traitement des données

- Vue d'ensemble de la collecte de données de renseignement sur les menaces
- Aperçu de la gestion de la collecte de renseignements sur la menace
- Présentation des sources et des flux de renseignements sur la menace
- Comprendre la collecte et l'acquisition de données de renseignement sur la menace
- Comprendre la collecte de données en masse
- Comprendre le traitement et l'exploitation des données

Analyse des données

- Aperçu de l'analyse des données
- Comprendre les techniques d'analyse des données
- Aperçu de l'analyse des menaces
- Comprendre le processus d'analyse des menaces
- Aperçu de l'affinage de l'analyse de la menace
- Comprendre l'évaluation du renseignement sur les menaces
- Création de Runbooks et d'une base de connaissances
- Présentation des outils de renseignement sur les menaces

Rapports et diffusion de renseignements

- Vue d'ensemble des rapports sur le renseignement sur les menaces
- Introduction à la diffusionParticiper aux relations de partageVue d'ensemble du partage de renseignements sur les menacesAperçu des mécanismes de diffusion
- Comprendre les plateformes de partage de renseignements sur les menacesAperçu des lois et règlements relatifs à l'échange de renseignements
- Vue d'ensemble de l'intégration du renseignement sur les menaces

Méthodes pédagogiques :

Support de cours officiel remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement