EduGroupe
Accompagner pour réussir

Threat Intelligence

Référence : **SECTHREATI** Durée : **3 jours (21 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissances de base dans le fonctionnement des systèmes d'information et en cyber sécurité

Profil des stagiaires

- RSSI, SOC Manager, Analystes SOC, Consultant en cybersécurité ou toute personne en charge de la sécurité d'un système d'information d'entreprise

Objectifs

- Comprendre les fondamentaux de la CTI (Cyber Threat Intelligence)
- Savoir collecter et analyser les informations sur les menaces
- Utiliser l'intelligence artificielle (IA) pour automatiser la collecte, l'analyse et la corrélation d'informations liées aux menaces
- Transformer les données en données exploitables
- Intégrer les outils et méthodes de la CTI dans le processus de sécurité de son organisation

Certification préparée

- Aucune

Méthodes pédagogiques

- Groupes de 4 à 12 personnes
- Apports théoriques illustrés d'exemples concrets
- Exercices pratiques
- Étude de cas fil rouge
- Accès à une documentation pédagogique numérique
- Utilisation d'outils collaboratifs (Miro, Wooclap) pour la co-construction
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation

Formateur

- Consultant-formateur expert Threat Intelligence

Méthodes d'évaluation des acquis

- Participation et réalisation d'exercices tout au long de la formation
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestations des compétences acquises et de fin de stage adressée à chaque participant

EduGroupe
Accompagner pour réussir

Contenu du cours

1. JOUR 1 - Introduction à la CTI et collecte de l'information (7 heures)

2. Fondamentaux de la Cyber Threat Intelligence (3h30)

- Définitions, enjeux, typologies de menaces
- Cadres de référence : TTP, IOC, APT, OPSEC, ATT&CK, Diamond Model
- Éthique et cadre légal (RGPD, vie privée, surveillance, etc.)

3. OSINT et sources de renseignement (3h30)

- Typologie des sources (techniques, open source, deep/dark web, commerciales)
- Introduction aux outils : Shodan, Google dorking, Censys, Kaspersky Feeds
- 💡 *Cas pratique : Investiguer une cible avec des outils OSINT (niveau 1)*

4. JOUR 2 - Outils, corrélation et analyse CTI (7 heures)

5. Méthodologie d'analyse (3h30)

- Cycle de vie du renseignement (collecte, traitement, exploitation)
- Analyse de campagnes APT (MITRE ATT&CK en pratique)
- Élaboration de scénarios de menace (Threat Modelling)

6. MISP, OpenCTI et autres plateformes (3h30)

- Prise en main de MISP : import/export d'IOC, gestion de feeds
- OpenCTI : architecture, modélisation, taxonomies
- 💡 *Cas pratique : Corréler et enrichir des IOC via MISP et OpenCTI*

7. JOUR 3 - Intégration opérationnelle et restitution (7 heures)

8. Intégration de la CTI dans l'organisation (3h30)

- Positionnement de la CTI (SOC, CSIRT, Risk Management)
- Utilisation de STIX / TAXII et formats de partage
- Orchestration CTI : outils, automatisation, playbooks

9. Rédaction & partage d'un rapport CTI (3h30)

- Élaboration d'un livrable CTI (rapport stratégique ou technique)
- 💡 *Exercice fil rouge : réponse à une attaque fictive avec appui CTI*
- Débrief, retours d'expérience, pistes d'approfondissement

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.