EduGroupe
Accompagner pour réussir

OSINT

Référence : **SECOSINT** Durée : **3 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 principes et enjeux de l'OSINT
- Maîtriser les outils et techniques pour la collecte d'informations
- Collecter, trier et analyser les données recueillies
- Utiliser des outils d'intelligence artificielle (IA) pour automatiser, filtrer et analyser des données issues de sources ouvertes
- Intégrer l'OSINT dans un cadre opérationnel

Certification préparée

- Aucune

Méthodes pédagogiques

- Groupes de 4 à 12 personnes
- Formation immersive : alternance de cours magistraux, TP guidés, ateliers
- Études de cas fil rouge pour mettre en œuvre une investigation complète
- Accès à une documentation pédagogique numérique
- Utilisation d'outils collaboratifs (Miro, Wooclap) pour la co-construction
- Restitution orale et écrite en fin de parcours
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation

Formateur

- Consultant-formateur expert OSINT

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 - Fondamentaux, périmètre et outils de base (7 heures)

2. Comprendre l'OSINT : cadre, périmètre et sources ouvertes (3h30)

- Définition de l'OSINT : périmètre, cas d'usage, cadre légal et éthique
- Cycle de vie de l'investigation : planification, collecte, analyse, diffusion
- Cartographie des sources ouvertes : moteurs, bases de données, web visible/profond/sombre

3. Méthodologie et mise en place d'un environnement d'enquête (3h30)

- Méthodologie d'enquête (prise de notes, sourcing, timelines)
- Outils de base : dorking Google, advanced search, reconnaissance web
- 💡 *Pratique : création d'un environnement d'enquête (start.me, Notion, RSS, mindmap)*

4. JOUR 2 - Techniques de collecte avancée et exploitation (7 heures)

5. Recherches avancées sur individus et organisations (3h30)

- Recherches sur personnes physiques : noms, pseudos, visages, réseaux sociaux
- Recherches sur structures : noms de domaine, emails, sociétés, documents publics
- Métadonnées, reverse image, recherches inversées

6. OSINT technique et investigation d'infrastructures (3h30)

- Investigation en environnement technique : IP, ports, services, DNS, BGP
- Pratique d'outils : Sherlock, Recon-ng, Lampyre, Spiderfoot, etc.
- 💡 *Investigation semi-guidée à partir d'un profil ou d'un incident simulé*

7. JOUR 3 - Structuration des résultats et restitution (7 heures)

8. Analyse, corrélation et production de livrables OSINT (3h30)

- Techniques de croisement et de pivot : identifiants, emails, adresses, hash
- Organisation des données : fiches opérationnelles, fiches de veille, cartographies
- Modèles de livrables : IOC, TTP, profil d'acteur, dossier d'enquête

9. Atelier fil rouge : enquête complète et restitution (3h30)

- 💡 *Atelier fil rouge : cas d'enquête OSINT complet à traiter par groupe*
- 💡 *Restitution orale + rédaction d'un livrable synthétique*
- Bilan et corrections, remise des supports & attestations

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.