

Formation **OSINT** – Investigation en source ouverte

L'OSINT (Open Source Intelligence) est une méthode d'investigation basée sur la collecte, l'analyse et l'interprétation de données accessibles publiquement. Utilisée dans des contextes variés tels que la cybersécurité, les enquêtes privées, la veille stratégique ou la lutte contre les fraudes, l'OSINT permet d'extraire des informations clés à partir de sources ouvertes comme les réseaux sociaux, les forums, les bases de données publiques ou encore les moteurs de recherche spécialisés. Cette formation vous apprendra à structurer une investigation OSINT, à exploiter des outils avancés, et à transformer des données brutes en informations exploitables.

Durée

2 jours

Objectifs pédagogiques

- ❖ Comprendre les principes fondamentaux et les domaines d'application de l'OSINT.
- ❖ Identifier et exploiter des sources d'information ouvertes de manière structurée.
- ❖ Utiliser des outils et techniques avancés pour automatiser les recherches et analyser les données.
- ❖ Mener des investigations OSINT dans le respect des réglementations et de l'éthique.
- ❖ Rédiger un rapport clair et exploitable à partir des informations collectées.

Public

Tous

Prérequis

Connaissances de base en informatique et familiarité avec les médias sociaux.

Programme de formation

Phase d'inclusion

Accueil des participants, présentation des objectifs et contextes professionnels de chacun.

Introduction à l'OSINT

Définition et principes fondamentaux de l'OSINT.

Domaines d'application : cybersécurité, enquêtes, veille concurrentielle, etc.

Cadre légal et éthique : ce qu'il est permis et interdit de faire en OSINT.

Collecte d'informations en source ouverte

Identification des sources ouvertes : bases de données, réseaux sociaux, forums, moteurs de recherche.

Techniques avancées de recherche avec les moteurs traditionnels (Google dorking).

Utilisation de moteurs spécialisés : Shodan, Maltego, Censys, etc.

Analyse et traitement des données

Organisation et structuration des informations collectées.

Outils d'analyse et de visualisation : graphiques de relations, cartographies. Techniques pour valider la véracité et la pertinence des informations.

Outils et automatisation en OSINT

Présentation des outils courants : Maltego, Recon-ng, SpiderFoot, theHarvester. Automatisation des tâches de recherche avec des scripts et outils spécifiques (Python, OSINT Framework). Techniques de surveillance en temps réel (alertes, suivi des mots-clés).

Sécurité numérique et anonymat

Les risques liés aux investigations OSINT : traçabilité et contre-surveillance. Utilisation de VPN, Tor et autres outils pour protéger l'identité de l'enquêteur. Bonnes pratiques pour sécuriser les recherches et protéger les données collectées.

Atelier pratique et cas concrets

Étude de cas : mener une investigation OSINT complète sur un sujet défini (ex. fraude, analyse d'une entreprise, cybermenace). Élaboration d'un rapport structuré et exploitable. Feedback sur les stratégies et outils utilisés lors de l'exercice pratique.

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.
- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.
- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.