

Formation OSINT – Investigation en source ouverte

Réf. SF34119

Apprenez à structurer une investigation OSINT grâce à notre formation de 2 jours !

2 j Durée	1 900 € HT Inter / participant	4 100 € HT Intra (≤12 pers.)	0 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

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 visé & prérequis

Public visé Administrateurs systèmes et réseaux, Architectes techniques, Tous

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

Programme détaillé

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.

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Nicolas L. — Formateur

Nicolas intervient notamment sur la gestion de projet et les certifications associées, ainsi que sur le pilotage de la DSI et la gouvernance. Son activité de formation a débuté en...

Ils nous font confiance

Cette année notre filière Cybersécurité et Protection des Données a accompagné plus de 69 entreprises dont :

AVEM MÉTROPOLE DE LYON ACTIMAGE CONSULTING SAS ADISTA ADVENTIEL AIGA ALCYOR ALDORIA ALSTOM ALTEN SA +59 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com