New

OSINT

L'intelligence au service de la cybersécurité

Présentiel ou en classe à distance

3 jours (21 h)

Prix inter : 2.890,00 € HT
Forfait intra : 7.690,00 € HT

Réf.: MG231

La formation **OSINT** Open Source Intelligence permet d'acquérir une méthodologie rigoureuse pour **collecter, analyser et exploiter des informations issues de sources ouverte**s dans un cadre professionnel et légal. Elle couvre l'ensemble du cycle OSINT : définition des besoins, identification des sources (surface web, deep web, dark web, réseaux sociaux, APIs, métadonnées), collecte structurée, analyse critique et restitution du renseignement. Les participants apprennent à utiliser efficacement les principaux outils d'investigation tels que Shodan, Maltego, Recon-ng, Spiderfoot, Sherlock, FOCA, HaveIBeenPwned ou encore les techniques avancées de dorking, d'analyse de métadonnées et de recherche inversée d'images.
La formation met également l'accent sur l'**automatisation de l'OSINT** et l'apport de l'intelligence artificielle pour filtrer, corréler et synthétiser de grands volumes d'informations. Grâce à des ateliers pratiques, les apprenants conçoivent des pipelines de veille, exploitent des API, mettent en place des tableaux de bord de surveillance et produisent des **rapports OSINT** exploitables pour des contextes tels que l'investigation SOC, la veille cyber, la lutte contre la fraude ou la threat intelligence.

A qui s'adresse cette formation ?

Pour qui

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

Prérequis

- Connaissance de base en informatique, notions en analyse de données et de rédaction
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction à l'OSINT : Fondamentaux, enjeux et cadre légal

- Définition de l'OSINT : périmètre, utilité, différences avec le renseignement clos
- Enjeux cyber, renseignement d'entreprise, due diligence, cyberdéfense
- Légalité et éthique de l'OSINT : RGPD, CNIL, cadre juridique, autorisation VS interdiction Méthodologie de collecte OSINT : modèles (cycle de renseignement, modèle OSINT Framework)
- Typologie des sources : surface web, deep web, dark web, APIs, métadonnées Responsabilité sociétale et OSINT : limites éthiques, impact réputationnel et usage responsable de la donnée
  Atelier

  Cartographie d'un besoin de renseignement à partir d'un cas (ex : analyse pré-incident ou investigation SOC)

2 - Recherche d'informations sur des individus (people OSINT)

- Techniques de dorking Google, Yandex, Bing
- Extraction d'informations personnelles à partir des réseaux sociaux (LinkedIn, Facebook, Twitter/X, Instagram)
- Recherche inversée d'images, visages et avatars (Google Lens, Pimeyes, Yandex, Exif)

- Outils et plateformes : Sherlock, Maigret, WhatsMyName, GHunt, Recon-ng
- Analyse de métadonnées dans fichiers, images, PDF (ExifTool, FOCA, etc.)

Atelier

Profilage complet d'une personne cible fictive (avec identité, email, photo, alias) à partir de sources ouvertes

3 - Recherche d'informations sur des entreprises, infrastructures et noms de domaine

- Recherche WHOIS, DNS, sous-domaines (Subfinder, DNSDumpster, crt.sh)
- Identification de technologies utilisées (WhatWeb, Wappalyzer, BuiltWith)
- Analyse passive : Shodan, Censys, ZoomEye, LeakLooker, BinaryEdge
- Collecte de fuites de données (HaveIBeenPwned, Dehashed, BreachDirectory)
- Surveillance de domaines, mails, leaks (Holehe, IntelX, LeakCheck)

Atelier

Réalisation d'une investigation OSINT sur un domaine d'entreprise fictif, avec identification des informations publiques disponibles et détection de potentielles fuites de données associées

4 - Automatiser l'OSINT avec des outils open source et scripts

- Utilisation avancée de recon-ng : modules, chaînes d'exploitation, rapports
- Automatisation avec Spiderfoot, Maltego CE
- Scraping web et API : requests, BeautifulSoup, Selenium (introduction simple)
- Veille automatisée : RSS feeds, alertes Google, API AbuseIPDB, Twitter API
- Création de son propre dashboard de veille OSINT avec OpenCTI ou TheHive

Atelier

Conception d'un pipeline automatisé de collecte et de veille OSINT sur un acteur ciblé (personne ou organisation), à l'aide d'outils open source et de scripts personnalisés

5 - OSINT et Intelligence Artificielle : Enrichissement, tri et analyse

- IA pour le résumé et l'analyse de rapports : GPT / LLM
- Traduction automatique multilingue (DeepL, Google Translate, AI translate)
- OCR et reconnaissance d'images pour l'analyse de documents ou flyers
- Analyse de masse de résultats avec IA : résumé, extraction d'entités, classification
- Chatbots OSINT et assistants IA : requêtes à la volée sur de grandes bases publiques

Atelier

Analyse automatisée d'un corpus de documents et d'images à l'aide d'un modèle de langage (LLM ChatGPT, Claude, Mistral), avec extraction d'insights pertinents à partir des contenus traités

6 - Exploitation opérationnelle de l'OSINT : intégration dans les missions cybersécurité

- Cas d'usage réels : investigation SOC, threat hunting, veille cyber, fraude, recrutement
- Intégration dans un SOC ou une cellule CTI : playbooks, enrichissement d'alertes
- Production d'un rapport OSINT efficace (format, sources, fiabilité, traçabilité)
- Mise en place d'une chaîne OSINT interne : outils, rôles, pratiques recommandées
- Simulation Red Team/Blue Team : ce que voit un attaquant, ce que peut utiliser un analyste

Atelier

Rédaction d'un rapport de renseignement à partir d'un scénario simulé (menace sur une entreprise ciblée, collecte d'indicateurs, priorisation, synthèse)

Les objectifs de la formation

- 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

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- L'apprentissage par la pratique : les phases théoriques sont complétées d'ateliers favorisant un ancrage durable des acquis
- Les nombreux retours d'expérience et conseils des consultants spécialistes du sujet
- Utilisation d'environnements proches du contexte professionnel

Dates et villes 2026 - Référence MG231

Dernières places disponibles Session garantie

Sophia Antipolis

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

A distance

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.
du 1 juin au 3 juin	du 28 sept. au 30 sept.	

Paris

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.
du 1 juin au 3 juin	du 28 sept. au 30 sept.	

Rouen

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Lille

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Strasbourg

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Aix-en-Provence

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Toulouse

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Lyon

du 1 juin au 3 juin	du 28 sept. au 30 sept.

Nantes

du 1 juin au 3 juin	du 28 sept. au 30 sept.

Rennes

du 1 juin au 3 juin	du 28 sept. au 30 sept.