+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 22/08/2025

S'inscrire

Formation OSINT

3 jours (21 heures)

Présentation

Notre formation « OSINT », orientée IA, vous permettra de maîtriser les méthodes et outils nécessaires pour exploiter efficacement les informations issues de sources ouvertes. L'OSINT (Open Source Intelligence) est devenu un atout stratégique pour les équipes de cybersécurité, et l'intégration de l'intelligence artificielle rend désormais possible l'automatisation, le tri et l'analyse rapide des données afin d'identifier les informations les plus pertinentes.

Notre formation OSINT orientée IA est conçue pour les professionnels de la cybersécurité (RSSI, SOC managers, analystes SOC, consultants en cybersécurité). Elle privilégie une approche pratique et opérationnelle, avec des ateliers concrets et une étude de cas fil rouge pour mettre en œuvre immédiatement les acquis.

Au cours de la formation, vous découvrirez les principes et enjeux de l'OSINT, vous apprendrez à collecter, trier et analyser des données issues de sources ouvertes, et vous mettrez en pratique l'utilisation d'outils d'IA (LLM, SpiderFoot HX, Maltego, 1 TRACE...) pour automatiser et enrichir vos investigations. Vous serez ainsi en mesure de conduire une investigation OSINT complète et de restituer une analyse directement exploitable pour renforcer la sécurité et la réactivité de votre organisation.

À l'issue, vous serez capable de conduire une investigation OSINT 360, de trier et analyser efficacement les données collectées, et d'intégrer l'OSINT dans un cadre opérationnel afin de renforcer la sécurité et la réactivité de votre organisation.

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

Public visé

- RSSI
- SOC Manager
- Analystes SOC
- Consultant en cybersécurité
- Toute personne en charge de la sécurité d’un système d’information d’entreprise

Pré-requis

- Connaissance de base en informatique
- Notions en analyse de données et de rédaction

PROGRAMME DE NOTRE FORMATION OSINT ORIENTÉE IA

[Jour 1 - Matin]

Introduction à l’OSINT et cadre légal

- Définition et enjeux de l’OSINT pour la cybersécurité
- Typologie des sources ouvertes (Surface Web, Deep Web, Dark Web)
- Limites, éthique et aspects légaux (RGPD, cadre juridique en France/UE)
- Cycle OSINT : Planification ? Collecte ? Analyse ? Diffusion
- Principes et enjeux de l’OSINT dans un contexte cybersécurité et organisationnel
- Atelier pratique : Cartographier les sources ouvertes pertinentes pour un cas SOC (sites, forums, réseaux sociaux, bases publiques).

[Jour 1 - Après-midi]

Méthodologie de collecte OSINT

- Élaboration d’un plan de recherche (hypothèses, mots-clés, scénarios)
- Techniques de recherche avancées (Google Dorks, moteurs alternatifs, metasearch)
- Archivage et préservation des preuves (hash, outils de capture)
- Maîtriser les outils et techniques pour la collecte d’informations
- Exercice pratique : Recherche d’informations sensibles sur une entreprise fictive.

Outils de base pour l’OSINT

- Navigateurs sécurisés et extensions utiles
- Collecte sur réseaux sociaux (Facebook, LinkedIn, Twitter/X, Instagram)
- Métadonnées (images, documents, fichiers PDF)
- Atelier pratique : Extraire et analyser des métadonnées d’un jeu de documents.

[Jour 2 - Matin]

OSINT sur les infrastructures techniques

- WHOIS, DNS, Shodan, Censys, Hunter.io, LeakLooker
- Exploration des réseaux et sous-domaines
- Cartographie des infrastructures exposées
- Atelier pratique : Identification des services exposés d'une cible fictive avec Shodan/Censys.

[Jour 2 - Après-midi]

OSINT et Threat Intelligence

- Corrélation des données collectées
- Recoupement avec des bases de leaks et paste sites (HaveIBeenPwned, BreachDirectory)
- Introduction à Maltego et aux graphes relationnels
- Savoir collecter, trier et analyser les données recueillies efficacement
- Atelier pratique : Créer un graphe relationnel d'une cible à partir de données collectées.

Automatisation de la collecte avec l'IA et scripts

- Présentation d'outils d'automatisation (TheHarvester, SpiderFoot HX, recon-ng, 1 TRACE, Maltego)
- Utilisation d'IA (LLMs, NLP) pour filtrer, catégoriser et prioriser des données
- Cas pratique avancé : filtrer un dump de données (CSV/JSON) avec un LLM et générer un tableau de priorisation
- Discussion : limites, biais et sécurité des données confiées à l'IA
- Utiliser des outils d'intelligence artificielle pour automatiser, filtrer et analyser des données issues de sources ouvertes
- Exercice pratique : Automatiser une recherche OSINT et générer un résumé avec l'IA.

[Jour 3 - Matin]

Intégration de l'OSINT dans un cadre opérationnel

- Rôle de l'OSINT dans un SOC et pour un RSSI
- Cas d'usage : investigations internes, Threat Hunting, veille concurrentielle, gestion de crise (cyberattaque, fuite de données)
- Formats de reporting OSINT et communication adaptée (RSSI, DG, équipes SOC)
- Intégrer l'OSINT dans un cadre opérationnel de sécurité
- Interopérabilité : intégration OSINT dans un SOC/SIEM/TIP
- Exercice pratique : Rédiger un mini-rapport OSINT à partir d'une collecte réelle.

[Jour 3 - Après-midi]

Étude de cas finale

- Mise en œuvre de la méthode OSINT du début à la fin :
- Définir la problématique
- Identifier et collecter les sources
- Trier et analyser les données
- Présenter un rapport opérationnel
- Étude de cas fil rouge : Investigation OSINT sur une cible fictive avec restitution finale devant le groupe.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.