OSINT (Open Source Intelligence)

Durée: 3 Jours Réf de cours: GKOSINT Version: 1 Méthodes d'apprentissage: Classe à distance

Résumé:

Cette formation OSINT (Open Source Intelligence) vous fera découvrir le framework OSINT.
Vous apprendrez à collecter, analyser et interpréter des informations accessibles au public pour mener des enquêtes ou des analyses tout en utilisant les outils d'IA.

Mise à jour : 16.12.2025

Public visé:

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

Objectifs pédagogiques:

- A l'issue de la formation, les participants pourront :
- 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

Pré-requis:

- Connaissance de base en informatique, notions en analyse de données et de rédaction.

Contenu:

Jour 1 – Fondamentaux et méthodologie OSINT

Démarrage de la formation

- Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.

Module 1 : Introduction et terminologie :

- Historique et cadre de l'OSINT
- Typologie des sources (réseaux sociaux, blogs, forums, dark web…)
- Éthique, légalité, RGPD et limites
- Recherche avancée : Google Dorking, RegEx
- Organisation et structuration : cartes mentales

Introduction aux IoC (indicateurs de compromission)

- LAB 1 : QCM + exercices de recherche Google Dorks ; IOC

Jour 2 – Framework OSINT, extraction et IA

Module 2 : Framework OSINT :

- Présentation du framework OSINT
- Étapes clés : planification, collecte, exploitation, diffusion

Cycle de vie OSINT

- LAB 2 : QCM + mappage personnalisé du framework

Module 3 : Techniques avancées OSINT :

- Intelligence des réseaux sociaux (Facebook, X, LinkedIn)
- Surveillance du Dark Web (Tor, moteurs spécialisés)
- Extraction Web : scrapping, metadata, WHOIS

OSINT géospatiale : géolocalisation à partir de photos, vidéos

- LAB 3 : Tests d'outils open source : SpiderFoot, TheHarvester, etc.

Module 4 : IA et OSINT :

- IA au service de la veille : points forts / limites
- Extraction et tri automatique de données

Cas concrets : détection d'anomalies, entités nommées

- LAB 4 : QCM IA + démonstration sur extraction automatisée

Jour 3 – Analyse prédictive, intégration et mise en œuvre

Module 5 : IA avancée pour l'analyse OSINT :

Apprentissage supervisé / non supervisé

- Feature engineering et prétraitement

Détection d'activités suspectes via clustering

LAB 5 : Entraînement d'un modèle sur un jeu de données IOC

- LAB 6 : Classification de données textuelles via NLP (Python)

Module 6 : Intégrer l'OSINT dans son organisation :

- Définition des objectifs d'un service OSINT
- Identification des rôles et responsabilités
- Intégration dans le processus de cybersécurité : SOC, CERT
- Processus d'alerte, diffusion et archivage

Enjeux juridiques et suivi d'activité

- LAB 7 : QCM + atelier de conception d'un dispositif OSINT organisationnel

Clôture de la formation

Méthodes pédagogiques :

Démarche pédagogique Alternance entre exposés techniques, démonstrations d'outils, cas pratiques et mises en situation Études de cas concrets, collecte en temps réel, et analyse de scénarios d'incidents réels Labs guidés sur VM ou environnement cloud dédié Supports PDF interactifs, schémas, cartes mentales, QCM, documents d'analyse
Répartition théorie / pratique40 % Théorie (méthodes, cadre légal, IA, stratégie) 60 % Pratique (labs techniques, extraction, IA, framework OSINT)
Ressources & Outils fournisVM ou environnement préconfiguré avec :Maltego Community / SpiderFoot / TheHarvester / Recon-ng OSINT Framework, MindMap, Obsidian, NotionPython (scikit-learn, pandas, spaCy) pour IA Navigateur Tor, DarkSearch.io, Wireshark Jeux de données OSINT publics et IOC Templates de rapports OSINT Accès à une base documentaire & base d'indicateurs de compromission (IOC)
Méthodes pédagogiques
La formation repose sur une alternance entre apports théoriques (40%) et travaux pratiques (60 %)
L'animation participative via des outils collaboratifs, partages d'écran, analyses d'études de cas, exercices collaboratifs et activités de groupe simulant des contextes réels.
Accès à un espace de partage sécurisé contenant : Le support de cours officiel au format électronique Les QCM d'entraînement Les fichiers d'exercices et corrigés Les modèles de documents utilisés dans les travaux pratiques
Matériel fourni : Support de cours au format électronique Documentation synthétique utilisable en contexte professionnel après la formation
Suivi qualité et évaluation
Avant la formation : Questionnaire de positionnement / diagnostic envoyé aux participants afin de recueillir les attentes, le niveau initial et détecter d'éventuels besoins spécifiques (techniques, pédagogiques ou liés à l'accessibilité)
Pendant la formation :Évaluation à chaud en fin de première journée pour recueillir les ressentis immédiats et ajuster l'animation pédagogique si besoin Quiz, exercices, cas pratiques Mises en situation Échanges pédagogiques avec le formateur
À l'issue de la formation : Questionnaire de satisfaction à chaud (participant + formateur) Une attestation de suivi de fin de formation sera délivrée à chaque participant
Suivi d'exécution : Une feuille d'émargement est signée numériquement chaque demi-journée par les participants et le formateur En distanciel, la traçabilité de la présence est assurée via l'outil collaboratif (statistiques de connexions synchrones) et les échanges interactifs

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement