DAWAN

Plan de la formation

www.dawan.fr

Formation OSINT (Open Source Intelligence)

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 475,00 € HT (standard) 1 980,00 € HT (remisé)
Public :	RSSI, SOC Manager, analystes SOC, consultants en cybersécurité, toute personne en charge de la sécurité d'un SI
Pré-requis :	Connaissances de base en informatique, notions en analyse de données et en rédaction
Objectifs :	Comprendre les principes, enjeux et limites de l'OSINT - Maîtriser les outils et techniques de collecte d'informations sur des sources ouvertes- Collecter, trier et analyser les données recueillies en respectant le cadre légal - Utiliser l'IA pour automatiser, filtrer et analyser des données OSINT - Intégrer l'OSINT dans un cadre opérationnel de cybersécurité
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102770-F
Note de satisfaction des participants:	Pas de données disponibles

Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre les fondamentaux, enjeux et cadre légal de l'OSINT

Définir l'OSINT et la distinguer des autres formes de renseignement
Identifier les bénéfices et les limites de l'OSINT pour la cybersécurité et la gestion des risques
Comprendre le cadre légal, éthique et réglementaire de la collecte d'informations ouvertes
Cartographier les principaux types de sources ouvertes : web, réseaux sociaux, registres, presse, documents publics
Atelier fil rouge : analyser un cas d'usage OSINT et en identifier les enjeux juridiques et éthiques

Collecter des informations sur les individus (people OSINT)

Utiliser les moteurs de recherche avancés et opérateurs pour affiner les recherches
Exploiter les réseaux sociaux et plateformes professionnelles pour profiler un individu
Recouper les informations pour vérifier l'identité et la cohérence des données
Identifier les risques de sécurité liés à l'exposition d'informations personnelles (ingénierie sociale, spear phishing)
Atelier fil rouge : réaliser une collecte d'informations OSINT contrôlée sur un profil fictif et produire une synthèse

Collecter des informations sur les entreprises, infrastructures et domaines

Rechercher des informations sur les organisations : registres publics, presse, bases de données spécialisées
Analyser les noms de domaine, certificats, services exposés et empreintes numériques (footprinting)
Identifier des fuites potentielles d'informations (dépôts publics, documents indexés, sous-domaines exposés)

Relier les informations collectées à des scénarios de risques pour l’organisation cible
Atelier fil rouge : construire une vue d’ensemble OSINT sur une organisation fictive et identifier les angles d’attaque possibles

Automatiser l’OSINT et utiliser l’IA pour filtrer et analyser

Découvrir des outils open source et scripts d’automatisation OSINT
Mettre en place des workflows d’agrégation, de filtrage et de corrélation des informations
Utiliser l’IA pour aider à la classification, au résumé et à l’analyse de grandes quantités de données OSINT
Conserver les traces, preuves et éléments d’analyse pour un usage ultérieur ou juridique
Atelier fil rouge : concevoir un mini-processus automatisé d’agrégation et de tri OSINT avec une brique IA

Exploiter l’OSINT dans les opérations de cybersécurité

Intégrer l’OSINT dans la détection des menaces, la CTI et la chasse aux menaces
Utiliser l’OSINT dans la préparation et la conduite d’audits de sécurité ou de tests d’intrusion
Exploiter l’OSINT pour la surveillance de la surface d’attaque et de l’e-réputation
Formaliser les livrables OSINT : rapports, fiches de renseignement, alertes
Atelier fil rouge final : produire un rapport OSINT opérationnel pour un cas de cybersécurité (entreprise ou individu fictif)