OSINT : Analyse et Investigation pour la Cybersécurité

Lien : https://innov-systems.com/formation/osint-analyse-et-investigation-pour-la-cybersecurite

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC299

CATÉGORIE
Cybersécurité technique

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Maîtriser la méthodologie d’enquête OSINT appliquée à la cybersécurité
- Identifier, collecter et corréler des informations issues de sources ouvertes pertinentes
- Exploiter des outils OSINT pour l’investigation et le profilage d’acteurs malveillants
- Automatiser la veille et la collecte de renseignements de menace
- Produire des rapports d’enquête exploitables pour le SOC, le CTI ou les équipes de réponse à incident

POUR QUI ?

- Analystes SOC
- Membres de CSIRT / CERT
- Analystes Cyber Threat Intelligence (CTI)
- Enquêteurs en cybersécurité
- Responsables de la veille et de la gestion des menaces

Programme détaillé

1 / INTRODUCTION À L'OSINT ET SON CADRE CYBERSÉCURITÉ

- Définitions, concepts et enjeux de l'OSINT
- Les différentes catégories de sources ouvertes
- Les limites éthiques, juridiques et opérationnelles de l'OSINT

2 / STRUCTURATION D'UNE ENQUÊTE OSINT

- Élaboration d'un plan de recherche et d'une problématique
- Gestion de la prise de note et construction d'une timeline d'enquête
- Méthodologie de corrélation entre sources multiples

3 / ENVIRONNEMENT ET OUTILS DE TRAVAIL

- Mise en place d'un environnement sécurisé d'investigation (VM, VPN, navigateur, hygiène OPSEC)
- Présentation des outils essentiels : navigateurs, extensions, moteurs spécialisés
- Gestion de l'identité numérique et anonymisation

4 / RECHERCHE ET CORRÉLATION DES INDICES DE COMPROMISSION (IOC)

- Identification et typologie des IoCs (hash, domaine, IP, e-mail, etc.)
- Techniques de pivot et recoupement d'indicateurs
- Exploitation d'outils OSINT (VirusTotal, ThreatMiner, Shodan, Censys)

5 / INVESTIGATION SUR LES INFRASTRUCTURES NUMÉRIQUES

- Cartographie et analyse des réseaux et protocoles
- Analyse WHOIS, DNS, ASN et historique d'infrastructures
- Détection d'activités suspectes et de patterns de compromission

Innov Systems

6 / EXPLOITATION DES MÉTADONNÉES ET TRACES NUMÉRIQUES

- Extraction et analyse de métadonnées de fichiers, images et documents
- Détection d’informations cachées ou résiduelles
- Corrélation d’empreintes numériques pour le profilage d’acteurs

7 / RECHERCHE AVANCÉE ET DORKING

- Syntaxe de recherche avancée (Google, Bing, Yandex)
- Dorking sur plateformes spécifiques (GitHub, Pastebin, LinkedIn)
- Identification d’informations sensibles exposées en ligne

8 / INVESTIGATION SUR LES RÉSEAUX SOCIAUX ET IDENTITÉS NUMÉRIQUES

- Techniques d’enquête sur comptes et interactions sociales
- Outils de recherche d’e-mails, alias et usernames
- Corrélation entre identités, organisations et comportements

9 / REVERSE IMAGE ET VEILLE MULTIMÉDIA

- Techniques de recherche inversée d’image (Google Lens, TinEye, Yandex)
- Détection de falsifications ou d’images réutilisées
- Analyse des images dans un contexte d’enquête cyber

10 / VEILLE ET AUTOMATISATION OSINT

- Stratégies de veille cyber : sources, périodicité, priorisation
- Automatisation via scripts et outils de scraping légaux
- Utilisation de frameworks d’automatisation (MISP, Maltego, Spiderfoot)

11 / CARTOGRAPHIE DE L’INFORMATION ET VISUALISATION

- Structurer les données OSINT pour la compréhension globale
- Visualisation de réseaux d’acteurs et d’IoCs

Inov Systems

- Présentation d’enquêtes sous forme de graphes (Gephi, Maltego, etc.)

12 / MISE EN PLACE D’UNE CELLULE OSINT INTERNE

- Organisation et rôles au sein d’une cellule OSINT
- Intégration avec un SOC, un CSIRT ou une équipe CTI
- Bonnes pratiques de documentation, versioning et partage de renseignement

13 / EXERCICE D’ENQUÊTE FIL ROUGE

- Investigation d’un scénario complet d’exposition de données
- Identification et corrélation d’indices techniques et humains
- Production d’un rapport opérationnel OSINT

14 / RESTITUTION ET ANALYSE COLLECTIVE

- Débriefing et validation des méthodes utilisées
- Discussion sur la reproductibilité et la fiabilité des sources
- Synthèse des apprentissages et axes d’amélioration

15 / CONCLUSION ET PERSPECTIVES

- Panorama des outils émergents en OSINT
- Intégration du renseignement OSINT dans la cybersécurité défensive
- Recommandations pour la montée en compétence continue

Inov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca
16 au 20 Août 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés