

Techniques de collecte de renseignements

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Sécurité offensive

Rubrique : Ethical Hacking - pentest

Code de formation : OSINT

€ Tarifs

Prix public : 3349 €

Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.

Le dispositif FNE-Formation.

L'OPCO (opérateurs de compétences) de votre entreprise.

France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

CPF -MonCompteFormation

Contactez nous pour plus d'information : contact@aston-institut.com

PRÉSENTATION

Objectifs & compétences

acquérir les compétences et la méthodologie pour une investigation via les techniques de collecte de renseignements.

Public visé

enquêteurs, détectives privés, analystes, veilleurs, avocats, cabinet de recouvrement, service de renseignement, Journalistes.

Pré-requis

connaissances générales en informatique et culturel, notions Word.

📍 Lieux & Horaires

Durée : 28 heures

Délai d'accès : Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

PROGRAMME

Jour 1 matin

Section 1 Présentation générale

OSINT – Les différentes branches de l'OSINT

OSINT – Open Source Intelligence

SOCMINT – Social Media Intelligence

IMINT/ROIM – Renseignement d'intérêt image

GEOINT – Renseignement Géospatial

Exercice 1 : Simple Recherche élémentaire – Test des compétences

Démonstration d'un attendu d'OSINT – Livrable

Explication du livrable

Éléments saillants

État d'esprit

Bonnes pratiques de sécurité

Rappel Juridique sur l'OSINT en France

Jour 1 après-midi

Section 2 Les Google dorks – Les Opérateurs Google

Voir l'invisible avec les opérateurs de recherches (Yandex, Google, Bing, Shodan)

Bloqué ? Supprimé ? Utiliser le cache et les archives

Création d'un avatar (Tips & Tricks)

Reverse Image – Retour d'expérience, tips & tricks sur cas concret

Enquête sur les cryptomonnaies

Recherche sur une société

LinkedIn Search API

Bases de données INPI

Sociétés chinoises

Agrégateur de données

Jour 2 matin

Section 3 SOCMINT

📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

Les outils et plugins à connaître
Recherche avancée sur Twitter
Analyse avancée de comptes
Analyse & croisement de données
Extraction de données avec des scripts python

Jour 2 après-midi

Recherche avancée sur Facebook
Tips & Tricks
Faire des recherches sur le nouveau Graph Search
Suivre la propagation d'URL
Recherche sur les différentes applications Google
Google Calendar / Documents / Contacts
Hangouts
Google Maps
GaiaID
Recherche avancée sur LinkedIn
Reverse Email

Jour 3 matin

Telegram
Présentation et utilisation de TDLib
Tips & Tricks
Réseaux sociaux mobiles (Whatsapp, Tiktok, Clubhouse, TamTam, Signal etc ..) via
Emulateur Android
Trouver qui se cache derrière un numéro de téléphone
Retrouver qui est cette personne
Jour 3 après-midi
Weibo & Wechat
Tips & Trics
Les différents bypass et retour d'expériences
Scraping Weibo via API
Geolocalisation sur Weibo
Recherche avancée sur Vkontakte
Extractions de données via script python
Utiliser la géolocalisation
Exercice SOCMINT combiné sur applications android & réseaux sociaux

Section 4 IMINT/GEOINT

Les outils
Utilisation de l'API Overpass
Cell Tower & Wifi Catching
Maritime & Aviation Intelligence
L'utilisation des fréquences radios dans l'OSINT
Cas Bombardiers russes – Conflit Ukraine
Etude de plusieurs cas concret de recherche d'un élément avec croisement

Jour 4 matin**Section 5 OSINT**

Les outils
Recherche sur une personne
Recherche par visage
Recherche par nom
Recherche par fait
Croisement
Analyse d'un site web
IP & DNS
Utilisation des pages d'erreurs
Structure du site
Cherchez selon la technologie
Créer son premier scraper de données avec mise en forme & visualisation simple
ADINT : Advertising Intelligence
Scraping sur des sites d'annuaires
Scraping sur des sites internet
Osint Actif : Social Engineering : Etat de l'art
Deep Web : Comment trouver ce que l'on cherche dans l'obscurité ?
Cas concret : Recherche d'une personne ayant fait de multiples fraudes et arnaques. Cette personne a disparu de la circulation.

Jour 1 après-midi

Section 6 Cas réel et analyse**MODALITÉS****Modalités**

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.

Pendant la formation : mises en situation, autodiagnostic, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.

Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.

Assiduité : certificat de réalisation.

Validations des acquis : grille d'évaluation des acquis établie par le formateur en fin de formation.