OSINT (investigation en source ouverte), niveau 2
investigation en source ouverte et cyber threat intelligence

Cours Pratique de 3 jours - 21h
Réf : OTI - Prix 2025 : 2 790 HT

La collecte d'information est aujourd'hui un savoir-faire indispensable pour préparer un test d'intrusion, comprendre un environnement ou un marché, pour mieux percevoir un acteur économique ou même le profil d'un individu. Ce cours montrera les différentes techniques d'investigation pour collecter des informations.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Développer des compétences en OSINT de manière approfondie en explorant des techniques avancées

Découvrir des outils puissants pour l'analyse et la collecte de données

Mener des investigations approfondies en ligne

LE PROGRAMME

dernière mise à jour : 11/2024

1) Techniques de collecte de données avancées

- Ethique et légalité dans l'OSINT avancée.
- Analyse de sites Web : techniques d'exploration approfondie des sites.
- Collecte d'informations à partir de forums et de blogs.
- Exploration des sources cachées : Dark Web, forums restreints, etc.
- Techniques d'extraction de données : scraping Web avancé.
- Collecte d'informations à partir de bases de données restreintes.

Travaux pratiques : Utilisation d'outils avancés de collecte de données.

2) Analyse de données avancée

- Analyse avancée des médias sociaux : analyse de sentiment, relations, comportements.
- Exploration d'outils de visualisation de données pour l'OSINT.
- Analyse de réseaux : cartographie des relations entre les entités.
- Exploration d'outils de cartographie et d'analyse de réseau.

Travaux pratiques : Analyse approfondie de données OSINT.

3) OSINT opérationnelle

- Introduction à l'OSINT opérationnelle : collecte en temps réel, surveillance.
- Planification et exécution d'une investigation OSINT avancée.
- Utilisation d'outils automatisés pour la surveillance continue.
- Les applications pratiques.

Travaux pratiques : Analyse complète d'une situation réelle.

4) OSINT et CTI

- Introduction aux bases de la CTI (Cyber Threat Intelligence).
- Nomenclature utilisée dans le domaine de la CTI.
- Techniques, tactiques, procédures et infrastructures courantes (TTP, ATP, IOC...).
- APT (menace persistante avancée) vs OPSEC (La sécurité opérationnelle).

PARTICIPANTS

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux, auditeurs et pentesters.

PRÉREQUIS

Connaissances équivalentes à celles apportées par le stage "OSINT, investigation en source ouverte" (réf. OST).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Utilisation d'outils tels qu'OTX AlienVault, Kaspersky Threat Data Feeds, Shodan, etc.
Travaux pratiques : Enquête et recherche d'indicateurs de compromission (IOC) liés à un malware.

LES DATES

CLASSE À DISTANCE
2025 : 26 mai, 23 juil., 20 oct.

PARIS
2025 : 19 mai, 16 juil., 13 oct.