OSINT, investigation en source ouverte

Cours Pratique de 3 jours - 21h
Réf : OST - Prix 2024 : 2 390CHF 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 :

Mener une investigation en source ouverte de manière autonome

Collecter, trier et analyser des données en source ouverte

Utiliser des outils d'investigations OSINT

LE PROGRAMME

dernière mise à jour : 01/2024

1) Concepts de base

- Principe de l'investigation et de la source ouverte.
- Types de sources : médias, réseaux sociaux, bases de données en ligne, etc.
- Éthique de l'investigation : respect de la vie privée, des droits de l'homme, de la légalité.
- Nomenclature.
- Sourcing.
- Organisation : MindMap, Notion, start.me, flux RSS.
- Moteurs de recherche avancés.

2) Préparation des données

- Collecte et préparation des données en source ouverte.
- Recherche sur une personne, un visage, un nom ou un fait.
- Réseaux sociaux.
- Bases de données en ligne.
- Techniques d'investigation : image, vidéo, caméra, cryptomonnaies, NFT, sociétés, documents et OCR.
- OpSec.
- Investigation sur Telegram.

Travaux pratiques : Collecte de données en source ouverte.

3) Les outils d'investigations

- Framework OSINT et threat hunting.
- Outils utilisables.

Travaux pratiques : Configuration et collecte des données en source ouverte avec Maltego et Lampyre.

4) Rédaction du rapport

- Bonnes pratiques de la rédaction de rapports et de la présentation de résultats.
- Collecter les informations.
- Structurer un rapport d'investigation en source ouverte.
- Rédiger un rapport clair et concis.

PARTICIPANTS

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

PRÉREQUIS

Maîtrise des outils informatiques de base : bureautique, Internet.

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.

- Présenter ses résultats.
- Threat hunting.

Travaux pratiques : Réalisation d'un rapport.

LES DATES

CLASSE À DISTANCE
2024 : 17 juin, 09 sept., 09 déc.