+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 05/07/2024

S'inscrire

Formation OSINT et Contre OSINT

2 jours (14 heures)

Présentation

Notre formation OSINT (Open Source Intelligence) vous donnera la méthode et les outils pour réussir votre recherche d'informations publiques.

Avec l'émergence d'internet, le volume de données disponible a explosé. Pouvoir recueillir, traiter et analyser ces données est devenu une compétence rare. En effet, il est essentiel d'être à l'affut des dernières nouveautés ou signaux faibles pour gagner un avantage concurrentiel.

En suivant notre formation, vous apprendrez les rudiments de la recherche de données open-source, la législation sur la collecte de data, les impacts sociaux et éthiques ainsi que les différents outils de veille.

Vous saurez tout des tâches indispensables de l'Open Source Intelligence, à savoir les méthodes pour collecter des données open-source, notamment via des outils de veille, le respect des normes légales et éthiques ainsi que le processus garantissant une bonne analyse des données.

Nous vous enseignerons également le contre OSINT visant à se protéger des démarches OSINT. Cette partie vous enseignera les bonnes pratiques de sécurité et la protection de votre vie privée.

Objectifs

- Comprendre l'OSINT et son importance
- Comprendre les enjeux sociaux et éthiques de l'Open Source Intelligence
- Sécuriser ses données contre une démarche OSINT

Public visé

- Data scientists
- Data analysts
- Chefs de Projet
- Intelligence analysts
- Business analysts

Pré-requis

Aucun pré-requis.

Programme de la formation OSINT et Contre OSINT

JOUR 1 : Introduction à l’OSINT

- Qu’est-ce que le renseignement d'origine sources ouvertes / OSINT ?
- Objectifs de l’OSINT
- Les principaux utilisateurs de l’OSINT

Éthique de l’OSINT

- Impacts sociaux - Éviter la collecte illégale
- Principes éthiques - Respect de la vie privée

Études de cas

- Exemples d'utilisation de l’OSINT - Shodan - HaveIbeenpwnd
- Exemples d'utilisation de la protection OSINT - Identification de menaces

Collecte de données OSINT

- Suivi media (Interviews, News)
- Suivi d’articles (Recherche Académique, Journalisme)
- Suivi de rapports (ONG, gouvernements, Services de police et justice, agences internationales)
- Suivi internet (Sites, forums, réseaux sociaux)
- Suivi géospatial (GEOINT)
- Outils : Recon-ng, Maltego, Maps…

JOUR 2 : Analyse de données OSINT

- Techniques d'analyse - Cas pratique : Analyse de sentiments sur Twitter
- Visualisation de données

Protection contre l'OSINT

- Évaluation de la menace OSINT - Évaluation des risques
- Contremesures OSINT en amont et en aval (VPN, Wireshark…)

Sécurité de l’information

- Menaces à la sécurité - Ingénierie sociale et phishing
- Pratiques de sécurité - Authentification à deux facteurs

Protection de la vie privée

- Confidentialité en ligne
- Outils de protection de la vie privée - Cryptage de messagerie (Signal, ProtonMail et bonnes pratiques)

Module complémentaire (+1 jour) : Analyse concurrentielle et tableaux de bord

Stratégies OSINT

- Pourquoi établir une stratégie OSINT ?
- Processus de création d'une stratégie

L'analyse concurrentielle

- Pourquoi l'analyse concurrentielle est importante ?
- Comment effectuer une analyse concurrentielle OSINT ?
- Les meilleurs outils

Création de tableaux de bord OSINT

- Introduction
- Les différents éléments
- Les critères d'un bon dashboard pour l'OSINT
- Présentation des meilleurs outils

Protection avancée contre l'OSINT

- Techniques avancées pour protéger ses informations
- Étude de cas : Comment les organisations peuvent se protéger contre la collecte de données OSINT ?
- Scénarios de simulation pour appliquer les compétences acquises
- Analyse des résultats

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.