PROGRAMME DE LA FORMATION
OSINT – CONFIRMÉ (Mise à jour le 24 janvier 2026)

Aperçu

	Public cible - Analystes géopolitique, en renseignement d'affaire et/ou en sécurité et défense ; chargés de due diligence ; journaliste, professionnels de la lutte contre la désinformation agents de recherche privé, chercheurs dans le domaine de la géopolitique et domaines connexes ; criminologues, professionnels dans le secteur bancaire, de l'import/export, du conseil international, de la diplomatie, professionnels du domaine de la conformité, professionnels de certains services de l'armée, de la police nationale et du renseignement d'État, consultants et analystes en cybersécurité, enseignants, commerciaux, cadres et dirigeants d'entreprise, salariés du secteur des ONG, responsables des risques géopolitiques, analystes de risque pays, recruteurs …
	Nombre de participants – 10 personnes
	Modalités – Formation via Private Discuss
	Durée – 12h (6 séances de 2h)
	Niveau de la formation – Confirmé
	Pré-requis et recommandations – Disposer d'une bonne connexion internet. Avoir validé le niveau intermédiaire OU maîtriser des techniques approfondies de collecte et d'analyse d'informations pour des recherches OSINT complexes, et maîtriser l'évaluation et la validation des sources d'information. Avoir téléchargé une virtual box (ou équivalent) et la VM OSINT Lab.
	Langue : Français
	Accessibilité – Nous contacter

	Outils pédagogiques – Supports de formation
	Évaluation – QCM. Deux rapports de renseignement : renseignement d'affaire et cyber-menaces (projets personnels).
	Remise d'un certificat de réalisation et d'une attestation de réussite
	Accompagnement possible du formateur sur des travaux universitaires ou professionnels – Nous contacter

Objectifs pédagogiques

Intégrer l'OSINT dans la stratégie d'entreprise

Mettre en œuvre des stratégies de renseignement d'affaires, des techniques de renseignement concurrentiel et gérer efficacement des projets de renseignement en identifiant les besoins informationnels des décideurs, en transformant l'information en outil d'aide à la décision, et en concevant, pilotant et évaluant des projets de renseignement alignés avec les objectifs stratégiques, juridiques et opérationnels de l'organisation afin d'anticiper les risques et de soutenir la gouvernance.

Comprendre les enjeux de la cyber-sécurité et du cyber-renseignement

Cette séance vise à permettre aux apprenants d'identifier et d'analyser les menaces cybernétiques, informationnelles et réputationnelles pesant sur l'entreprise et son environnement, de comprendre et mettre en œuvre des mesures de protection des informations, des systèmes et des données sensibles dans une logique de prévention et de résilience, et d'articuler les approches d'OSINT, de cyber-renseignement et de cybersécurité afin de renforcer la maîtrise des risques informationnels et numériques.

Analyser les menaces cybernétiques et prendre des mesures de protection des informations.

Cette séance vise à permettre aux apprenants d'identifier, qualifier et hiérarchiser les principales menaces cybernétiques pesant sur les systèmes d'information et les actifs informationnels d'une organisation. Il s'agit également de comprendre et d'appliquer des mesures de protection techniques, organisationnelles et humaines afin de garantir la confidentialité, l'intégrité et la disponibilité des informations, dans une logique de prévention, de gestion des risques.

Programme détaillé

Séance 1 – 2h – Stratégies avancées de renseignement d’affaires

Cette séance s’attachera à se pencher sur les matrices à utiliser dans le cadre d’une stratégie de renseignement d’affaire à mettre en place. Ces matrices permettront de créer des grilles de lecture, utiles pour les stratégies de renseignement d’affaire.

Séance 2 – 2h - Cyber-renseignement et sécurité de l’information

À l’heure des cyber-attaques, ce module aura pour objet de se pencher sur les notions de sécurité, mais également pour l’introduction du cyber-renseignement de fournir les compétences nécessaires à l’anticipation des cyber-attaques, et aux mesures visant à protéger les données.

Séance 3– 2h - Sécurité opérationnelle

Ce cours vise à explorer les pratiques nécessaires à la sécurité opérationnelle, afin de pouvoir faire des investigations tout en se protégeant.

Séance 4 – 2h - Renseignement des menaces cyber et OSINT des cyber-attaques

Cette séance aura pour but d’initier au renseignement des cyber menaces et de découvrir comment faire de l'OSINT sur les cyber attaques.

Séance 5 et 6 – 4 h – Gestion de projets d’intelligence économique

Cette séance aura pour objet de travailler sur le sujet que les candidats choisiront, en utilisant toutes les techniques OSINT possibles, y compris la cartographie de réseaux, sans oublier les mesures de sécurité pour masquer leurs traces.

Évaluation

QCM sur la sécurisation et la sécurité opérationnelle – **QCM –** (1 QCM de 20 questions portant sur les connaissances acquises). **La réussite à ce QCM qui doit être rempli et renvoyé sous 48h conditionne la réalisation du projet personnel final qui évalue vos compétences professionnelles.**

Évaluation de deux rapports de renseignement sur des sujets proposés par le candidat et validés par le formateur. Le premier sujet porte sur le renseignement d'affaire et le second sujet porte sur le renseignement des cyber-menaces. Le même coefficient s'applique aux deux rapports.

Il s'agit de projets proposés par le candidat et validés par le formateur. **Ces projets doivent être finalisés dans un délai d'un mois après la dernière séance (cf.barème)**.

Important : Les thématiques des rapports de renseignement finaux devront être validés par le formateur à l'issue de la séance 1. C'est pourquoi elles vous sont déjà demandées par voie de questionnaire avant le début de la formation. Toute absence non justifiée à une séance de formation est sanctionnée d'un retrait de 2 points sur la note d'évaluation finale.

Modalités et contact

Contactez- nous à l'adresse suivante : **formations@eurasiapeace.org**

La sélection des candidats n'ayant pas préalablement validé la formation de niveau intermédiaire se fait par voie d'entretien avec le formateur.

Accessibilité

EurasiaPeace s'engage à favoriser l'accès à ses prestations aux personnes en situation de handicap. Pour tout besoin spécifique en terme d'accessibilité, veuillez adresser un mail à notre référent Handicap et Formation, Morgan Caillet, à l'adresse suivante : **formations@eurasiapeace.org**

Budget

Cette formation de 12h est à 600€ pour les particuliers et à 1200€ pour les entreprises.

Une réduction de 15% est appliquée aux particuliers abonnés à EurasiaPeace –Abonnez-vous pour 12€ par an !

Votre entreprise a une demande ou une attente particulière et souhaite un devis personnalisé, contactez-nous à l'adresse suivante : formations@eurasiapeace.org

Approfondissement

Nous vous proposons en complément de votre formation un accompagnement sur un projet professionnel. Contactez-nous !