Affinis Campus

Département formation B2B

CATALOGUE COMPLET DES FORMATIONS

Formations en investigation numérique, OSINT et renseignement d'affaires. En présentiel, à distance ou sur mesure.

29 formations · 1 à 10 jours

2026–2027

DES MÉTHODES AUJOURD'HUI. DES IMPACTS DEMAIN.



Une offre modulaire, du ciblé à l'intensif

Des parcours adaptés aux objectifs, au niveau initial, au temps disponible et au contexte métier.

1 jour	2 jours	3 jours	4 jours	5 jours	10 jours
15 formations	4 formations	4 formations	2 formations	3 formations	1 formations

UNE BASE COMMUNE

Chaque fiche présente le positionnement, les objectifs, l'organisation, le programme détaillé, la pédagogie, les évaluations, l'accessibilité et le suivi.

UNE LOGIQUE DE PERSONNALISATION

Les modalités, exemples, exercices, horaires et formats peuvent être adaptés au contexte de l'entreprise, dans le respect des objectifs et des prérequis de la formation.

FORMATS

Présentiel · classe virtuelle synchrone · hybride · intra-entreprise selon la formation.

TARIFICATION

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

ACCÈS

Validation recommandée au moins 10 jours ouvrés avant le début, avec possibilité d'un délai plus court au cas par cas.

Comment lire ce catalogue

Chaque formation est présentée avec le même niveau de détail pour faciliter la comparaison et la contractualisation.

1 **POSITIONNEMENT**

Finalité professionnelle, public visé, prérequis et modalités de positionnement.

2 **OBJECTIFS**

Objectif général, objectifs opérationnels évaluables et compétences visées.

3 **ORGANISATION**

Durée, horaires, modalités, lieu, effectif, délai d'accès, tarif et contacts.

4 **PROGRAMME**

Séquences détaillées avec durée, objectif, contenus, méthodes / activités et évaluation / preuve.

5 **PÉDAGOGIE & ÉVALUATION**

Méthodes pédagogiques, ressources, profil du formateur, évaluations initiales, formatives et finales.

6 **ACCESSIBILITÉ & SUIVI**

Adaptations possibles, référent handicap, assiduité, satisfaction et indicateurs de résultats.

CHAMPS VOLONTAIREMENT NON PUBLIÉS

Le catalogue n'intègre pas le statut documentaire, la version du programme ni les modalités internes d'archivage des preuves.

Panorama — modules d'une journée

15 formations courtes pour cibler une compétence précise ou sensibiliser un collectif.

AC-OSINT-101
Fondamentaux opérationnels de l'OSINT

AC-OSINT-102
Recherche web avancée pour l'OSINT

AC-OSINT-103
Intelligence artificielle appliquée à l'OSINT

AC-SEC-101
OPSEC appliquée aux investigations en sources ouvertes

AC-SOC-101
Fondamentaux opérationnels du SOCMINT

AC-IMINT-101
Vérification d'images et de vidéos en sources ouvertes

AC-IE-101
Screening d'entreprise en sources ouvertes

AC-FIMI-101
Comprendre les manipulations de l'information et les ingérences numériques

SEC-ENT-01
SecOps en mobilité

SEC-ENT-02
SecOps spearphishing

SEC-ENT-03
Hygiène numérique personnelle

SEC-ENT-04
OSINT défensif — Maîtriser son empreinte numérique

SEC-ENT-05
Sécurité des échanges confidentiels

SEC-ENT-06
Sécurité des appareils mobiles

SEC-ENT-07
Intelligence économique — Comprendre l'adversaire

Panorama — parcours de 2 à 10 jours

Approfondir, pratiquer et conduire des investigations plus complexes, jusqu'au parcours intensif.

2 J · AC-OSINT-201	Fondamentaux opérationnels de l'OSINT
2 J · AC-SOC-201	Investigation avancée sur les réseaux sociaux
3 J · AC-OSINT-301	Investigation numérique professionnelle
3 J · AC-FIMI-301	Investiguer les manipulations de l'information
4 J · AC-OSINT-401	Analyste OSINT : conduire une investigation de bout en bout
5 J · AC-OSINT-501	Pratique professionnelle de l'OSINT
5 J · AC-FIMI-501	Investigation des ingérences et manipulations informationnelles
2 J · AC-DD-201	Due diligence en sources ouvertes
2 J · AC-FIMI-201	Détecter une opération informationnelle coordonnée
3 J · AC-DD-301	Due diligence approfondie et cartographie des risques
3 J · AC-CARTO-301	Cartographier une organisation et ses réseaux d'influence
4 J · AC-FIMI-401	Analyste des menaces informationnelles numériques
5 J · AC-DD-501	Due diligence et investigation économique avancées
10 J · AC-OSINT-1001	Parcours intensif d'investigation OSINT et d'analyse des menaces numériques

Une pédagogie conçue pour passer de l’information à la décision

Les programmes articulent cadrage, démonstration, pratique, traçabilité, évaluation et retour d’expérience.

01

CHERCHER

Cadrer le besoin, construire une stratégie, choisir les sources et les outils.

02

VÉRIFIER

Qualifier les sources, recouper, documenter les limites et le niveau de confiance.

03

ANALYSER

Relier les éléments, distinguer faits, hypothèses et opinions, construire une lecture exploitable.

04

DÉCIDER

Restituer de manière structurée, sourcée, traçable et adaptée au besoin métier.

DANS CHAQUE FICHE

Les contenus sont présentés sans simplification : programme détaillé, méthodes, moyens, modalités d’évaluation, accessibilité et suivi.

ADAPTATION

Le positionnement et le cadrage permettent d’ajuster les exemples, exercices, rythmes et modalités lorsque la fiche le prévoit.

Modalités pratiques

Des formats pensés pour l'entreprise, avec une organisation précisée dans chaque fiche.

PRÉSENTIEL

Affinis Campus, chez le client ou en salle louée selon la session.

DISTANCIEL

Classe virtuelle synchrone lorsque la formation le permet ; outil précisé sur la convocation.

HYBRIDE

Possible selon le programme, les objectifs, l'effectif et la logistique.

EFFECTIF

4 participants minimum / 10 maximum recommandé en présentiel ; au-delà, modalités à déterminer conjointement.

DÉLAI D'ACCÈS

Validation recommandée au moins 10 jours ouvrés avant le début ; un délai plus court peut être accepté au cas par cas.

TARIF

Sur devis. Le prix figure sur la proposition commerciale ou la convention de formation.

ASSIDUITÉ & TRAÇABILITÉ

Émargements par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

RÉSULTATS

Les indicateurs sont consolidés progressivement : satisfaction, assiduité, réussite et, lorsque pertinent, recommandation.

Inscription & accessibilité

Un point de contact identifié pour l'inscription et l'étude des besoins d'adaptation.

CONTACT INSCRIPTION

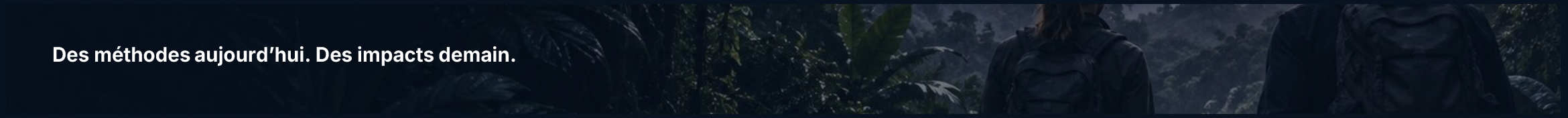
Clara Carriorbe — c.carriorbe@affinis-conseil.com
Philippe Chabrol — p.chabrol@affinis-conseil.com

RÉFÉRENTE HANDICAP

Clara Carriorbe — c.carriorbe@affinis-conseil.com

ACCESSIBILITÉ

Les besoins sont recueillis dès l'inscription et étudiés afin de mettre en place, lorsque cela est possible, des adaptations pédagogiques, organisationnelles ou techniques adaptées à la situation.



Affinis Campus

1 JOUR

15 formations

Cibler une compétence ou sensibiliser un collectif.



- AC-OSINT-101 — Fondamentaux opérationnels de l'OSINT
- AC-OSINT-102 — Recherche web avancée pour l'OSINT
- AC-OSINT-103 — Intelligence artificielle appliquée à l'OSINT
- AC-SEC-101 — OPSEC appliquée aux investigations en sources ouvertes
- AC-SOC-101 — Fondamentaux opérationnels du SOCMINT
- AC-IMINT-101 — Vérification d'images et de vidéos en sources ouvertes
- AC-IE-101 — Screening d'entreprise en sources ouvertes
- AC-FIMI-101 — Comprendre les manipulations de l'information et les ingérences numériques
- SEC-ENT-01 — SecOps en mobilité
- SEC-ENT-02 — SecOps spearphishing
- SEC-ENT-03 — Hygiène numérique personnelle
- SEC-ENT-04 — OSINT défensif — Maîtriser son empreinte numérique
- SEC-ENT-05 — Sécurité des échanges confidentiels
- SEC-ENT-06 — Sécurité des appareils mobiles
- SEC-ENT-07 — Intelligence économique — Comprendre l'adversaire

Fondamentaux opérationnels de l'OSINT

FINALITÉ PROFESSIONNELLE

Acquérir une méthode de recherche web structurée et produire des résultats fiables et traçables.

PUBLIC VISÉ

Professionnels de l'industrie, du conseil, des services, juristes, commerciaux, agents publics, fonctions support.

PRÉREQUIS

Aisance courante avec un navigateur web et un ordinateur.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le métier, les usages visés et l'aisance numérique ; test diagnostic court. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-101 · Fondamentaux opérationnels de l'OSINT

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Distinguer donnée, information, renseignement et preuve.
- Identifier les limites juridiques, éthiques et techniques d'une recherche.
- Appliquer des mesures élémentaires d'OPSEC.
- Transformer un besoin métier en questions de recherche.
- Construire un lexique, un plan de recherche et des requêtes avancées.
- Sélectionner des sources adaptées et en apprécier la fiabilité.
- Recouper les informations et distinguer faits, hypothèses et opinions.
- Produire une restitution courte, structurée et traçable.

COMPÉTENCES VISÉES

Construire un plan de recherche ; formuler des requêtes ; qualifier et recouper les sources ; documenter les résultats.

MÉTHODES PÉDAGOGIQUES

Apports courts, démonstrations, exercices individuels, étude de cas. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-OSINT-101 · Fondamentaux opérationnels de l'OSINT

OSINT / INVESTIGATION

0 · Accueil et positionnement - 0 h 30

OBJECTIF — Identifier les attentes et le niveau initial.
CONTENUS — Présentation, usages professionnels, questionnaire diagnostic.
MÉTHODES / ACTIVITÉS — Tour de table et questionnaire.
ÉVALUATION / PREUVE — Positionnement conservé.

1 · Comprendre l'OSINT - 0 h 45

OBJECTIF — Distinguer l'OSINT d'une simple recherche web.
CONTENUS — Donnée, information, renseignement, preuve ; usages ; WEBINT, SOCMINT, IMINT, GEOINT.
MÉTHODES / ACTIVITÉS — Apport illustré et classement de cas d'usage.
ÉVALUATION / PREUVE — Correction collective argumentée.

2 · Limites et difficultés - 0 h 45

OBJECTIF — Identifier les obstacles affectant une investigation.
CONTENUS — Surabondance, non-indexation, obsolescence, homonymie, contenus trompeurs, limites linguistiques et techniques.
MÉTHODES / ACTIVITÉS — Analyse d'un dossier comportant plusieurs obstacles.
ÉVALUATION / PREUVE — 3 limites et une adaptation pour chacune.

3 · Cadre juridique et éthique - 1 h 00

OBJECTIF — Repérer les pratiques licites, sensibles ou à proscrire.
CONTENUS — Données publiques, RGPD, finalité, minimisation, accès frauduleux, droit d'auteur, conservation et diffusion.
MÉTHODES / ACTIVITÉS — Étude de situations et grille de décision.
ÉVALUATION / PREUVE — Justification du classement.

OSINT / INVESTIGATION

4 · Méthodologie - Plan de recherche - Cadrer le besoin et élaborer la sémantique - 1 h 00

OBJECTIF — Transformer une demande vague en questions de recherche et en adapter le vocabulaire de recherche.
CONTENUS — Décision à éclairer, périmètre, temporalité, exclusions, livrable, critères d'arrêt.
MÉTHODES / ACTIVITÉS — Reformulation d'une demande fictive.
ÉVALUATION / PREUVE — Grille de cadrage complétée.

5 · Méthodologie - Plan de recherche - Identifier et qualifier les sources - 1 h 00

OBJECTIF — Sélectionner les familles de sources adaptées.
CONTENUS — Sources officielles, entreprises, presse, réseaux sociaux, archives, open data, documents techniques.
MÉTHODES / ACTIVITÉS — Association besoins / sources et analyse de fiabilité.
ÉVALUATION / PREUVE — Choix de sources complémentaires justifié.

6 · Méthodologie - Plan de recherche - Tracer et recouper les recherches - 0 h 45

OBJECTIF — Tenir un journal de recherche vérifiable.
CONTENUS — Requête, moteur, date, URL, extrait, fiabilité, statut, archivage et nommage.
MÉTHODES / ACTIVITÉS — Compléter un journal à partir d'une démonstration.
ÉVALUATION / PREUVE — Contrôle des champs indispensables.

7 · Cas pratique et bilan - 1 h 15

OBJECTIF — Conduire une recherche courte et restituer.
CONTENUS — Cadrage, requêtes, collecte, qualification, synthèse.
MÉTHODES / ACTIVITÉS — Mise en situation individuelle ou binôme.
ÉVALUATION / PREUVE — Cas pratique + quiz final.

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire préalable sur le métier, les usages visés et l'aisance numérique ; test diagnostic court. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Quiz final sur l'ensemble de la formation donnée.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Fiche méthode et grille de qualification des sources.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Recherche web avancée pour l'OSINT

FINALITÉ PROFESSIONNELLE

Optimiser la recherche d'informations difficiles à identifier sur le web ouvert.

PUBLIC VISÉ

Veilleurs, analystes, consultants, commerciaux, juristes, acheteurs, fonctions innovation.

PRÉREQUIS

Pratique de base de la recherche web.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable et test diagnostic portant sur les pratiques de recherche. Un échange avec le référent pédagogique est proposé en cas d'écart de niveau important.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-102 · Recherche web avancée pour l'OSINT

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Distinguer donnée, information, renseignement et preuve.
- Identifier les limites juridiques, éthiques et techniques d'une recherche.
- Appliquer des mesures élémentaires d'OPSEC.
- Transformer un besoin métier en questions de recherche.
- Construire un lexique, un plan de recherche et des requêtes avancées.
- Sélectionner des sources adaptées et en apprécier la fiabilité.
- Recouper les informations et distinguer faits, hypothèses et opinions.
- Produire une restitution courte, structurée et traçable.

COMPÉTENCES VISÉES

Construire des requêtes avancées ; sélectionner le moteur adapté ; exploiter les résultats et archives.

MÉTHODES PÉDAGOGIQUES

Démonstrations en direct, exercices progressifs, cas pratique. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-OSINT-102 · Recherche web avancée pour l'OSINT

OSINT / INVESTIGATION

0 · Accueil et diagnostic - 0 h 30

OBJECTIF — Évaluer les pratiques de recherche.
CONTENUS — Usages, moteurs maîtrisés, opérateurs connus.
MÉTHODES / ACTIVITÉS — Questionnaire et exercice flash.
ÉVALUATION / PREUVE — Diagnostic initial.

1 · Comprendre les moteurs et l'IA - 0 h 45

OBJECTIF — Expliquer exploration, indexation et classement.
CONTENUS — Crawlers, index, pertinence, personnalisation, limites des SERP.
MÉTHODES / ACTIVITÉS — Apport et comparaison de moteurs.
ÉVALUATION / PREUVE — Explication des écarts observés.

2 · Maîtriser la sémantique - 0 h 45

OBJECTIF — Construire un lexique précis et multilingue.
CONTENUS — Polysémie, synonymes, translittérations, acronymes, fautes, exclusions.
MÉTHODES / ACTIVITÉS — Atelier lexical.
ÉVALUATION / PREUVE — Lexique structuré.

3 · Opérateurs fondamentaux - 1 h 00

OBJECTIF — Combiner les opérateurs essentiels.
CONTENUS — Guillemets, OR, -, parenthèses, site:, filetype:.
MÉTHODES / ACTIVITÉS — Exercices guidés.
ÉVALUATION / PREUVE — Requêtes conformes.

OSINT / INVESTIGATION

4 · Opérateurs avancés et documents - 1 h 00

OBJECTIF — Cibler les zones et formats du web.
CONTENUS — intitle:, inurl:, allintitle:, allinurl:, recherches temporelles, documents oubliés.
MÉTHODES / ACTIVITÉS — Défis chronométrés.
ÉVALUATION / PREUVE — Résultats retrouvés et expliqués.

5 · Moteurs alternatifs et archives - 0 h 45

OBJECTIF — Choisir un moteur ou une archive selon le besoin.
CONTENUS — Bing, Brave, Yandex selon contexte, moteurs spécialisés, caches et archives web.
MÉTHODES / ACTIVITÉS — Comparaison sur cas identique.
ÉVALUATION / PREUVE — Choix du moteur justifié.

6 · Plan et journal de requêtes - 0 h 45

OBJECTIF — Organiser une stratégie itérative.
CONTENUS — Axes, requêtes testées, résultats, ajustements, critères d'arrêt.
MÉTHODES / ACTIVITÉS — Création d'un journal.
ÉVALUATION / PREUVE — Journal complet.

7 · Cas pratique final - 1 h 30

OBJECTIF — Résoudre une recherche complexe et reproductible.
CONTENUS — Recherche de documents, entités, dates et sources multiples.
MÉTHODES / ACTIVITÉS — Cas individuel ou binôme.
ÉVALUATION / PREUVE — Score sur pertinence, traçabilité et justification.

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire préalable et test diagnostic portant sur les pratiques de recherche. Un échange avec le référent pédagogique est proposé en cas d'écart de niveau important.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique final évalué sur la pertinence des recherches, la traçabilité et la justification des choix. Réussite : validation d'au moins 70 % des critères de la grille du cas pratique.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Mémento des opérateurs et trame de journal de recherche.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Intelligence artificielle appliquée à l'OSINT

FINALITÉ PROFESSIONNELLE

Utiliser l'IA comme assistant de recherche, d'extraction et d'analyse sans perdre la maîtrise des sources.

PUBLIC VISÉ

Analystes, consultants, juristes, chargés de veille, équipes commerciales et innovation.

PRÉREQUIS

Connaissances élémentaires en recherche web.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable et test diagnostic portant sur les pratiques de recherche. Un échange avec le référent pédagogique est proposé en cas d'écart de niveau important.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-103 · Intelligence artificielle appliquée à l'OSINT

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Distinguer donnée, information, renseignement et preuve.
- Identifier les limites juridiques, éthiques et techniques d'une recherche.
- Appliquer des mesures élémentaires d'OPSEC.
- Transformer un besoin métier en questions de recherche.
- Construire un lexique, un plan de recherche et des requêtes avancées.
- Sélectionner des sources adaptées et en apprécier la fiabilité.
- Recouper les informations et distinguer faits, hypothèses et opinions.
- Produire une restitution courte, structurée et traçable.

COMPÉTENCES VISÉES

Rédiger des prompts de recherche ; contrôler les résultats ; identifier biais et hallucinations ; protéger les données sensibles.

MÉTHODES PÉDAGOGIQUES

Ateliers guidés, comparaison de résultats, analyse critique. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-OSINT-103 · Intelligence artificielle appliquée à l'OSINT

OSINT / INVESTIGATION

0 · Accueil et positionnement - 0 h 15

OBJECTIF — Identifier usages et contraintes de l'IA.
CONTENUS — Outils utilisés, données manipulées, attentes.
MÉTHODES / ACTIVITÉS — Questionnaire et échanges.
ÉVALUATION / PREUVE — Diagnostic initial.

1 · Comprendre les IA génératives - 0 h 45

OBJECTIF — Identifier capacités, limites et risques.
CONTENUS — Fonctionnement général, hallucinations, biais, obsolescence, confidentialité.
MÉTHODES / ACTIVITÉS — Démonstrations comparées.
ÉVALUATION / PREUVE — Quiz de compréhension.

2 · Concevoir des prompts de recherche - 1 h 00

OBJECTIF — Rédiger des instructions structurées.
CONTENUS — Rôle, contexte, objectif, contraintes, format, critères de vérification.
MÉTHODES / ACTIVITÉS — Atelier de réécriture de prompts.
ÉVALUATION / PREUVE — Prompt évalué sur une grille.

3 · Enrichir un plan de recherche - 0 h 45

OBJECTIF — Utiliser l'IA pour explorer sans déléguer la décision.
CONTENUS — Lexique, hypothèses, traductions, axes, sources potentielles.
MÉTHODES / ACTIVITÉS — Comparaison manuel/IA.
ÉVALUATION / PREUVE — Apports et erreurs identifiés.

OSINT / INVESTIGATION

4 · Extraire, structurer et analyser des données - 1 h 15

OBJECTIF — Transformer des contenus fournis en données exploitables.
CONTENUS — Extraction d'entités, tableaux, chronologies, catégorisation.
MÉTHODES / ACTIVITÉS — Atelier sur corpus contrôlé.
ÉVALUATION / PREUVE — Exactitude et traçabilité vérifiées.

5 · Synthétiser avec prudence - 0 h 45

OBJECTIF — Produire une synthèse fidèle aux sources.
CONTENUS — Citations, incertitudes, contradictions, distinction faits/hypothèses.
MÉTHODES / ACTIVITÉS — Synthèse d'un dossier.
ÉVALUATION / PREUVE — Contrôle des affirmations.

6 · Sécurité et gouvernance - 0 h 45

OBJECTIF — Définir des règles d'usage professionnelles.
CONTENUS — Données sensibles, anonymisation, outils autorisés, conservation, validation humaine.
MÉTHODES / ACTIVITÉS — Atelier de protocole.
ÉVALUATION / PREUVE — Checklist de conformité.

7 · Cas pratique et protocole final - 1 h 30

OBJECTIF — Mobiliser l'IA dans une recherche vérifiée.
CONTENUS — Plan, prompts, extraction, contrôle, restitution.
MÉTHODES / ACTIVITÉS — Mise en situation.
ÉVALUATION / PREUVE — Cas pratique + protocole d'usage.

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire préalable et test diagnostic portant sur les pratiques de recherche. Un échange avec le référent pédagogique est proposé en cas d'écart de niveau important.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique et protocole d'usage évalués sur la qualité des prompts, le contrôle des résultats, la traçabilité, l'identification des biais et le respect des règles de sécurité. Réussite : validation d'au moins 70 % des critères de la grille du cas pratique.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Bibliothèque de prompts et checklist de vérification.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

OPSEC appliquée aux investigations en sources ouvertes

FINALITÉ PROFESSIONNELLE

Réduire les risques d'exposition du chercheur, de son organisation et de ses données.

PUBLIC VISÉ

Analystes, enquêteurs, veilleurs, consultants, agents publics, responsables sûreté.

PRÉREQUIS

Aucun prérequis technique avancé.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le métier, les usages visés et l'aisance numérique ; test diagnostic court. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-SEC-101 · OPSEC appliquée aux investigations en sources ouvertes

SECOPS / OPSEC

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable d'anticiper selon ses recherches, les règles élémentaires de sécurité opérationnelle à implémenter, et de trouver et mettre en oeuvre les outils et bonnes pratiques nécessaires.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Identifier les risques d'exposition associés à une recherche en sources ouvertes ;
- Evaluer le niveau de sensibilité d'une mission et déterminer les protections nécessaires ;
- Mettre en œuvre un cloisonnement adapté des environnements, comptes et identités de recherche ;
- Limiter les traces techniques et informationnelles susceptibles d'exposer le chercheur ou son organisation ;
- Elaborer et justifier un protocole OPSEC adapté à un cas d'usage professionnel.

COMPÉTENCES VISÉES

Identifier les risques ; cloisonner les environnements ; protéger identités, données et preuves ; définir une procédure OPSEC.

MÉTHODES PÉDAGOGIQUES

Démonstrations, autodiagnostic, atelier de conception de procédure. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-SEC-101 · OPSEC appliquée aux investigations en sources ouvertes

SECOPS / OPSEC

0 · Accueil et autodiagnostic - 0 h 15

OBJECTIF — Identifier les pratiques et risques actuels.
CONTENUS — Usages, équipements, comptes, données et contraintes.
MÉTHODES / ACTIVITÉS — Questionnaire OPSEC.
ÉVALUATION / PREUVE — Autodiagnostic conservé.

1 · Modéliser les risques - 0 h 45

OBJECTIF — Identifier actifs, menaces et impacts.
CONTENUS — Chercheur, organisation, client, cible, exposition technique et humaine.
MÉTHODES / ACTIVITÉS — Cartographie collective.
ÉVALUATION / PREUVE — Risques priorisés.

2 · Empreinte numérique - 1 h 00

OBJECTIF — Comprendre les traces laissées par une recherche.
CONTENUS — IP, navigateur, cookies, comptes, métadonnées, historique.
MÉTHODES / ACTIVITÉS — Démonstrations contrôlées.
ÉVALUATION / PREUVE — Traces identifiées.

3 · Cloisonner les environnements - 1 h 00

OBJECTIF — Séparer usages personnels et professionnels.
CONTENUS — Profils, navigateurs, machines virtuelles, comptes, stockage.
MÉTHODES / ACTIVITÉS — Atelier d'architecture.
ÉVALUATION / PREUVE — Schéma de cloisonnement.

SECOPS / OPSEC

4 · Protéger identités et accès - 0 h 45

OBJECTIF — Sécuriser les comptes de recherche.
CONTENUS — Mots de passe, MFA, récupération, pseudonymes, règles de création.
MÉTHODES / ACTIVITÉS — Checklist et cas.
ÉVALUATION / PREUVE — Mesures adaptées.

5 · Sécuriser collecte et fichiers - 0 h 45

OBJECTIF — Réduire les risques liés aux téléchargements.
CONTENUS — Fichiers, liens, macros, sandbox, métadonnées, antivirus, sauvegarde.
MÉTHODES / ACTIVITÉS — Étude d'incidents.
ÉVALUATION / PREUVE — Réponse correcte aux scénarios.

6 · Stocker et transmettre - 0 h 45

OBJECTIF — Protéger les preuves et livrables.
CONTENUS — Chiffrement, droits d'accès, partage, effacement, confidentialité.
MÉTHODES / ACTIVITÉS — Atelier procédure.
ÉVALUATION / PREUVE — Chaîne de traitement documentée.

7 · Plan OPSEC final - 1 h 45

OBJECTIF — Élaborer une procédure proportionnée.
CONTENUS — Matrice risques/mesures, rôles, validation, incidents, révision.
MÉTHODES / ACTIVITÉS — Travail individuel puis revue croisée.
ÉVALUATION / PREUVE — Plan OPSEC évalué.

AC-SEC-101 · OPSEC appliquée aux investigations en sources ouvertes

SECOPS / OPSEC

ÉVALUATION INITIALE

Questionnaire préalable sur le métier, les usages visés et l'aisance numérique ; test diagnostic court. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Evaluation sur l'élaboration par chacun d'un plan OPSEC par rapport à un contexte donné.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Checklist OPSEC et modèle de procédure interne.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Fondamentaux opérationnels du SOCMINT

FINALITÉ PROFESSIONNELLE

Collecter et analyser des informations publiques issues des réseaux sociaux dans un cadre licite.

PUBLIC VISÉ

Veilleurs, analystes, communication, conformité, sûreté, enquêteurs, consultants.

PRÉREQUIS

Maîtrise des fondamentaux de recherche web recommandée. Aisance sur ordinateur et navigateurs web.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-SOC-101 · Fondamentaux opérationnels du SOCMINT

SOCMINT

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Définir un périmètre de recherche SOCMINT compatible avec le besoin professionnel et le cadre autorisé.
- Retrouver des profils, comptes ou contenus publics à partir d'un nom, pseudonyme, identifiant ou autre indice disponible.
- Utiliser les moteurs de recherche et les fonctions natives des plateformes pour retrouver des contenus publics pertinents.
- Reconstituer une chronologie simple de publications ou d'activités à partir de sources ouvertes.
- Identifier des interactions, relations ou communautés visibles et en documenter les principaux liens.
- Recouper les éléments permettant de confirmer ou d'infirmer une hypothèse d'identité numérique.
- Conserver les éléments collectés de manière traçable et produire une synthèse SOCMINT argumentée.

COMPÉTENCES VISÉES

Rechercher profils et contenus ; effectuer des pivots ; établir une chronologie ; qualifier les relations et les limites.

MÉTHODES PÉDAGOGIQUES

Démonstrations, exercices par plateforme, étude de cas. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

SOCMINT

0 · Accueil et positionnement - 0 h 15

OBJECTIF — Identifier les plateformes et usages visés.
CONTENUS — Pratiques, contraintes, cadre des exercices.
MÉTHODES / ACTIVITÉS — Questionnaire.
ÉVALUATION / PREUVE — Diagnostic initial.

1 · Cadre et spécificités SOCMINT - 0 h 45

OBJECTIF — Distinguer collecte publique et interaction.
CONTENUS — Données publiques, éthique, RGPD, limites des plateformes.
MÉTHODES / ACTIVITÉS — Cas de conformité.
ÉVALUATION / PREUVE — Décisions justifiées.

2 · Identités et pseudonymes - 1 h 00

OBJECTIF — Rechercher et corréler des identités numériques.
CONTENUS — Pseudonymes, variantes, URLs, identifiants, avatars, biographies.
MÉTHODES / ACTIVITÉS — Exercices de pivots.
ÉVALUATION / PREUVE — Corrélations documentées.

3 · Recherche par plateforme - 1 h 15

OBJECTIF — Adapter la recherche aux principales plateformes.
CONTENUS — LinkedIn, X, Facebook, Instagram, Reddit, YouTube, Telegram.
MÉTHODES / ACTIVITÉS — Démonstrations et mini-défis.
ÉVALUATION / PREUVE — Résultats sourcés.

SOCMINT

4 · Chronologies et interactions - 1 h 00

OBJECTIF — Reconstituer une séquence d'activité.
CONTENUS — Dates, publications, réponses, partages, communautés.
MÉTHODES / ACTIVITÉS — Atelier chronologique.
ÉVALUATION / PREUVE — Chronologie cohérente.

5 · Qualifier les relations - 0 h 45

OBJECTIF — Distinguer lien observé et relation supposée.
CONTENUS — Interactions, récurrence, proximité, biais, niveau de confiance.
MÉTHODES / ACTIVITÉS — Analyse d'un réseau simple.
ÉVALUATION / PREUVE — Qualification prudente.

6 · Archivage et preuve - 0 h 30

OBJECTIF — Conserver les éléments de manière traçable.
CONTENUS — URLs, captures, horodatage, contexte, limites.
MÉTHODES / ACTIVITÉS — Journal de collecte.
ÉVALUATION / PREUVE — Champs obligatoires présents.

7 · Cas pratique multiréseaux - 1 h 30

OBJECTIF — Produire un dossier SOCMINT synthétique.
CONTENUS — Identité, contenus, chronologie, relations, limites.
MÉTHODES / ACTIVITÉS — Mise en situation.
ÉVALUATION / PREUVE — Dossier + restitution.

SOCMINT

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique multiréseaux évalué sur la qualité du dossier, la chronologie, la qualification prudente des relations et la traçabilité. Réussite : validation d'au moins 70 % des critères de la grille du cas pratique.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Grille SOCMINT et modèle de chronologie.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Vérification d’images et de vidéos en sources ouvertes

FINALITÉ PROFESSIONNELLE

Vérifier l’origine, la date, le lieu et le contexte d’un contenu visuel.

PUBLIC VISÉ

Journalistes, communicants, analystes, enquêteurs, juristes, équipes sûreté et veille.

PRÉREQUIS

Pratique courante du web.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable et test diagnostic portant sur les pratiques de recherche. Un échange avec le référent pédagogique est proposé en cas d’écart de niveau important.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D’ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-IMINT-101 · Vérification d’images et de vidéos en sources ouvertes

IMINT / GEOINT

OBJECTIF GÉNÉRAL

À l’issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Identifier les indices utiles à l’analyse d’une image ou d’une vidéo publiée en ligne.
- Effectuer une recherche inversée d’image à l’aide de plusieurs moteurs ou services adaptés.
- Exploiter les métadonnées disponibles lorsqu’elles sont présentes et en apprécier les limites.
- Détecter les principaux signes de réemploi, de recadrage, de montage ou de sortie de contexte d’un contenu visuel.
- Formuler et tester des hypothèses élémentaires de géolocalisation ou de chronolocalisation à partir d’indices visuels et de sources ouvertes.
- Recouper un contenu visuel avec des sources indépendantes afin d’en qualifier l’origine et le contexte.
- Rédiger une conclusion de vérification distinguant faits établis, indices, hypothèses et incertitudes.

COMPÉTENCES VISÉES

Effectuer une recherche inversée ; relever des indices visuels ; vérifier métadonnées, date et localisation ; formuler un niveau de confiance.

MÉTHODES PÉDAGOGIQUES

Démonstrations, ateliers visuels, mini-enquêtes. Alternance d’apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d’analyse ; cas pratiques ; visioconférence et partage d’écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d’une pratique opérationnelle de l’OSINT et de la formation d’adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d’OPSEC associés.

AC-IMINT-101 · Vérification d’images et de vidéos en sources ouvertes

IMINT / GEOINT

0 · Accueil et diagnostic - 0 h 15

OBJECTIF — Évaluer les pratiques de vérification visuelle.
CONTENUS — Usages, outils, typologies de contenus.
MÉTHODES / ACTIVITÉS — Questionnaire et image test.
ÉVALUATION / PREUVE — Diagnostic initial.

1 · Méthode de vérification - 0 h 45

OBJECTIF — Structurer une analyse visuelle.
CONTENUS — Source, contenu, contexte, date, lieu, auteur, diffusion.
MÉTHODES / ACTIVITÉS — Grille méthodologique.
ÉVALUATION / PREUVE — Grille appliquée.

2 · Recherche inversée - 1 h 00

OBJECTIF — Retrouver occurrences et versions antérieures.
CONTENUS — Moteurs d’images, recadrage, variantes, vignettes, limites.
MÉTHODES / ACTIVITÉS — Exercices guidés.
ÉVALUATION / PREUVE — Origine ou antériorité trouvée.

3 · Métadonnées et indices techniques - 0 h 45

OBJECTIF — Exploiter les métadonnées disponibles sans surinterpréter.
CONTENUS — EXIF, noms de fichiers, dimensions, compression, limites.
MÉTHODES / ACTIVITÉS — Analyse de fichiers.
ÉVALUATION / PREUVE — Indices qualifiés.

IMINT / GEOINT

4 · Géolocalisation élémentaire - 1 h 00

OBJECTIF — Identifier un lieu par indices convergents.
CONTENUS — Signalétique, architecture, relief, végétation, cartes, imagerie.
MÉTHODES / ACTIVITÉS — Mini-enquête.
ÉVALUATION / PREUVE — Lieu proposé avec niveau de confiance.

5 · Chronolocalisation - 1 h 00

OBJECTIF — Estimer une date ou période.
CONTENUS — Météo, ombres, événements, travaux, versions d’un lieu.
MÉTHODES / ACTIVITÉS — Atelier comparatif.
ÉVALUATION / PREUVE — Hypothèse datée et justifiée.

6 · Vidéos et contenus IA - 0 h 45

OBJECTIF — Vérifier une vidéo et repérer des anomalies.
CONTENUS — Images clés, audio, montages, deepfakes, provenance, prudence.
MÉTHODES / ACTIVITÉS — Analyse collective.
ÉVALUATION / PREUVE — Indices et limites listés.

7 · Cas pratique final - 1 h 30

OBJECTIF — Rédiger une note de vérification complète.
CONTENUS — Origine, lieu, date, contexte, confiance, limites.
MÉTHODES / ACTIVITÉS — Mise en situation.
ÉVALUATION / PREUVE — Note évaluée sur grille.

AC-IMINT-101 · Vérification d'images et de vidéos en sources ouvertes

IMINT / GEOINT

ÉVALUATION INITIALE

Questionnaire préalable et test diagnostic portant sur les pratiques de recherche. Un échange avec le référent pédagogique est proposé en cas d'écart de niveau important.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique final évalué sur une grille portant sur l'origine, la date, la localisation, le contexte, le niveau de confiance et les limites de la vérification. Réussite : validation d'au moins 70 % des critères de la grille.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Fiche de vérification IMINT.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Screening d’entreprise en sources ouvertes

FINALITÉ PROFESSIONNELLE

Réaliser un premier screening d’une entreprise, d’un fournisseur ou d’un partenaire.

PUBLIC VISÉ

Acheteurs, commerciaux, juristes, compliance, dirigeants de PME, consultants, investisseurs.

PRÉREQUIS

Aucun prérequis en analyse financière.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le métier, les usages visés et l’aisance numérique ; test diagnostic court. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D’ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-IE-101 · Screening d’entreprise en sources ouvertes

INTELLIGENCE ÉCONOMIQUE

OBJECTIF GÉNÉRAL

À l’issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Identifier juridiquement une entreprise ou un partenaire à partir de sources officielles et ouvertes.
- Reconstituer les principaux éléments de gouvernance : dirigeants, actionnariat, bénéficiaires, filiales ou établissements connus.
- Vérifier la cohérence entre l’activité déclarée, la présence numérique et les implantations observables de l’organisation.
- Rechercher des signaux de risque juridiques, réputationnels, réglementaires ou de conformité dans des sources ouvertes pertinentes.
- Identifier des incohérences ou signaux faibles nécessitant des vérifications complémentaires.
- Recouper les informations issues de plusieurs sources et qualifier leur niveau de fiabilité.
- Produire une synthèse de premier niveau mettant en évidence constats, points de vigilance et limites de la recherche.

COMPÉTENCES VISÉES

Identifier l’entité ; rechercher dirigeants et bénéficiaires ; repérer contentieux, sanctions, controverses et signaux financiers.

MÉTHODES PÉDAGOGIQUES

Apports, démonstrations sur registres, cas pratique. Alternance d’apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d’analyse ; cas pratiques ; visioconférence et partage d’écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d’une pratique opérationnelle de l’OSINT et de la formation d’adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d’OPSEC associés.

AC-IE-101 · Screening d’entreprise en sources ouvertes

INTELLIGENCE ÉCONOMIQUE

0 · Accueil et positionnement - 0 h 15

OBJECTIF — Identifier les besoins de screening.
CONTENUS — Usages achat, commercial, juridique, investissement.
MÉTHODES / ACTIVITÉS — Questionnaire.
ÉVALUATION / PREUVE — Diagnostic initial.

1 · Cadrer le screening - 0 h 45

OBJECTIF — Définir décision, risques et profondeur.
CONTENUS — Périmètre, entité, pays, période, critères d’arrêt.
MÉTHODES / ACTIVITÉS — Atelier de cadrage.
ÉVALUATION / PREUVE — Fiche validée.

2 · Identifier l’entité - 0 h 45

OBJECTIF — Vérifier l’existence et les données juridiques.
CONTENUS — Raison sociale, SIREN/équivalents, statuts, établissements, activité.
MÉTHODES / ACTIVITÉS — Démonstration registres.
ÉVALUATION / PREUVE — Identité corroborée.

3 · Dirigeants et actionnariat - 1 h 00

OBJECTIF — Reconstituer les principaux liens de contrôle.
CONTENUS — Dirigeants, bénéficiaires, filiales, participations, changements.
MÉTHODES / ACTIVITÉS — Cas pratique.
ÉVALUATION / PREUVE — Schéma simple et sources.

AC-IE-101 · Screening d’entreprise en sources ouvertes

INTELLIGENCE ÉCONOMIQUE

4 · Réputation et controverses - 0 h 45

OBJECTIF — Rechercher des signaux réputationnels.
CONTENUS — Presse, sanctions, contentieux, critiques, temporalité, contexte.
MÉTHODES / ACTIVITÉS — Recherche guidée.
ÉVALUATION / PREUVE — Signaux qualifiés.

5 · Signaux financiers élémentaires - 0 h 45

OBJECTIF — Repérer des incohérences ou fragilités simples.
CONTENUS — CA, résultat, capitaux propres, dettes, effectifs, cohérence activité.
MÉTHODES / ACTIVITÉS — Lecture de données.
ÉVALUATION / PREUVE — 3 constats prudents.

6 · Cotation et traçabilité - 1 h 00

OBJECTIF — Prioriser les risques et documenter.
CONTENUS — Fait, indice, hypothèse, probabilité, impact, sources.
MÉTHODES / ACTIVITÉS — Matrice de risques.
ÉVALUATION / PREUVE — Cotation justifiée.

7 · Cas pratique final - 1 h 45

OBJECTIF — Produire un screening exploitable.
CONTENUS — Identité, gouvernance, réputation, finance, synthèse.
MÉTHODES / ACTIVITÉS — Mise en situation.
ÉVALUATION / PREUVE — Fiche de risques et restitution.

AC-IE-101 · Screening d'entreprise en sources ouvertes

INTELLIGENCE ÉCONOMIQUE

ÉVALUATION INITIALE

Questionnaire préalable sur le métier, les usages visés et l'aisance numérique ; test diagnostic court. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique final évalué sur la qualité du screening, la qualification des risques, la traçabilité des sources et la restitution. Réussite : validation d'au moins 70 % des critères de la grille du cas pratique.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Grille de screening entreprise.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Comprendre les manipulations de l'information et les ingérences numériques

FINALITÉ PROFESSIONNELLE

Reconnaître les principaux mécanismes d'une opération informationnelle numérique.

PUBLIC VISÉ

Cadres, communicants, juristes, sûreté, institutions publiques, équipes de veille.

PRÉREQUIS

Aucun prérequis.

MODALITÉS DE POSITIONNEMENT

Questionnaire bref sur les fonctions exercées, l'exposition au sujet et les attentes. Aucun prérequis technique ni sélection.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-FIMI-101 · Comprendre les manipulations de l'information et les ingérences numériques

MENACES INFORMATIONNELLES

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Distinguer désinformation, propagande, influence, manipulation de l'information et ingérence numérique étrangère.
- Identifier les principales composantes d'une opération informationnelle : cible, narratif, contenu, canal, relais et temporalité.
- Repérer des marqueurs simples d'inauthenticité, de coordination ou d'amplification artificielle.
- Expliquer les mécanismes de primo-diffusion, blanchiment informationnel, amplification et reprises opportunistes.
- Identifier le rôle potentiel de faux comptes, bots, médias relais, sites ou contenus générés artificiellement dans une campagne.
- Analyser un cas documenté afin de distinguer éléments observables, hypothèses et attribution.
- Formuler une première appréciation structurée d'un phénomène informationnel sans surinterpréter les indices disponibles.

COMPÉTENCES VISÉES

Distinguer désinformation, influence et ingérence ; reconnaître narratifs, inauthenticité, amplification et blanchiment informationnel.

MÉTHODES PÉDAGOGIQUES

Apports illustrés, analyse collective de cas, quiz. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-FIMI-101 · Comprendre les manipulations de l'information et les ingérences numériques

MENACES INFORMATIONNELLES

0 · Accueil et diagnostic - 0 h 15

OBJECTIF — Identifier le niveau de sensibilisation.
CONTENUS — Usages, exposition, responsabilités.
MÉTHODES / ACTIVITÉS — Quiz initial.
ÉVALUATION / PREUVE — Résultats conservés.

1 · Définitions et cadre - 0 h 45

OBJECTIF — Distinguer désinformation, influence, propagande et ingérence.
CONTENUS — Concepts, acteurs, objectifs, critères de caractérisation.
MÉTHODES / ACTIVITÉS — Apport illustré.
ÉVALUATION / PREUVE — Quiz de distinction.

2 · Narratifs et contenus - 0 h 45

OBJECTIF — Analyser un récit trompeur sans juger une opinion.
CONTENUS — Narratif, cible, victimologie, émotion, faux contexte, deepfake.
MÉTHODES / ACTIVITÉS — Étude de contenus.
ÉVALUATION / PREUVE — Grille narrative.

3 · Diffusion et blanchiment - 1 h 00

OBJECTIF — Comprendre la chaîne de diffusion.
CONTENUS — Primo-diffusion, comptes jetables, médias tiers, blanchiment, reprises.
MÉTHODES / ACTIVITÉS — Reconstitution d'une chaîne.
ÉVALUATION / PREUVE — Schéma cohérent.

MENACES INFORMATIONNELLES

4 · Amplification et inauthenticité - 1 h 00

OBJECTIF — Repérer des marqueurs de coordination.
CONTENUS — Bots, faux comptes, horaires, répétition, comportements, multi-plateformes.
MÉTHODES / ACTIVITÉS — Analyse d’exemples.
ÉVALUATION / PREUVE — Marqueurs qualifiés.

5 · Infrastructures et TTP - 1 h 00

OBJECTIF — Identifier les actifs et techniques associés.
CONTENUS — Domaines, sites, comptes, métadonnées, TTP, limites d’attribution.
MÉTHODES / ACTIVITÉS — Démonstration.
ÉVALUATION / PREUVE — Actifs reliés avec prudence.

6 · Réaction et vigilance - 0 h 45

OBJECTIF — Définir des mesures adaptées.
CONTENUS — Vérification, remontée, communication, conservation, coordination.
MÉTHODES / ACTIVITÉS — Atelier réflexe.
ÉVALUATION / PREUVE — Plan de réaction.

7 · Étude de cas finale - 1 h 15

OBJECTIF — Identifier les mécanismes d’une opération.
CONTENUS — Narratif, diffusion, amplification, acteurs, incertitudes.
MÉTHODES / ACTIVITÉS — Cas collectif.
ÉVALUATION / PREUVE — Grille + quiz final.

MENACES INFORMATIONNELLES

ÉVALUATION INITIALE

Questionnaire bref sur les fonctions exercées, l'exposition au sujet et les attentes. Aucun prérequis technique ni sélection.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Étude de cas finale et quiz final portant sur l'identification des narratifs, marqueurs d'inauthenticité, mécanismes d'amplification, infrastructures et TTP. Réussite : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Lexique et grille de lecture d'une campagne informationnelle.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

SecOps en mobilité

FINALITÉ PROFESSIONNELLE

Adopter des réflexes de sécurité opérationnelle lors des déplacements professionnels afin de réduire les risques liés aux réseaux publics, aux supports piégés et à l'exposition physique des informations.

PUBLIC VISÉ

Commerciaux, dirigeants et plus largement professionnels amenés à se déplacer avec des équipements ou des informations professionnelles.

PRÉREQUIS

Aucun prérequis technique avancé. Utilisation courante d'un ordinateur et/ou d'un smartphone recommandée.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le contexte professionnel, les usages numériques concernés, le niveau d'aisance et les besoins d'adaptation. Échange de cadrage avec le commanditaire en intra. Les résultats servent à adapter les exemples, démonstrations et exercices ; ils ne constituent pas une sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra-entreprise. Classe virtuelle possible pour les parties compatibles avec les démonstrations et exercices, à confirmer selon la session.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel éventuel : outil précisé sur la convocation ; connexion stable et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 15/09/2026 · Responsable de validation : Clara Carriorbe

SÉCURITÉ NUMÉRIQUE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable d'identifier les principaux risques numériques et physiques rencontrés en mobilité et d'appliquer des mesures de protection adaptées avant, pendant et après un déplacement professionnel.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Identifier les risques associés aux Wi-Fi publics et comprendre le principe d'une interception de type MITM.
- Reconnaître les risques liés aux supports, câbles ou prises USB non maîtrisés.
- Repérer les situations d'exposition physique telles que le shoulder surfing.
- Mettre en œuvre des mesures simples : VPN, écran de confidentialité, verrouillage automatique et bonnes pratiques de connexion.
- Appliquer une checklist de préparation et de sécurité en déplacement.

COMPÉTENCES VISÉES

Évaluer une situation de mobilité ; identifier les risques numériques et physiques ; choisir des mesures de protection proportionnées ; appliquer une routine de sécurité avant et pendant les déplacements.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations, exercices progressifs, études de cas et mises en situation. Les activités sont adaptées au niveau, aux usages professionnels et aux contraintes de la session. Les démonstrations techniques sont réalisées exclusivement dans un environnement pédagogique contrôlé.

MOYENS ET RESSOURCES

Support de formation ; ordinateur et/ou smartphone selon le module ; connexion Internet ; navigateur récent ; environnement de démonstration contrôlé ; fiches pratiques et checklists correspondant au module ; vidéoprojecteur/écran en présentiel.

PROFIL DU FORMATEUR

Professionnel expérimenté en sécurité numérique, OSINT ou intelligence économique selon le module, disposant d'une pratique opérationnelle et d'une expérience de la formation d'adultes. Les démonstrations techniques sont réalisées dans un environnement pédagogique contrôlé.

SEC-ENT-01 · SecOps en mobilité

SÉCURITÉ NUMÉRIQUE

0 · Accueil et risques en mobilité - 30 min

OBJECTIF — Identifier les risques propres aux déplacements professionnels.
CONTENUS — Contexte de menace en mobilité ; situations à risque dans les transports, hôtels, espaces de coworking et lieux publics.
MÉTHODES / ACTIVITÉS — Apport illustré + échange à partir des pratiques des participants.
ÉVALUATION / PREUVE — Questions diagnostiques et identification de situations à risque.

1 · Wi-Fi publics et faux points d'accès - 45 min

OBJECTIF — Comprendre les risques associés aux Wi-Fi publics.
CONTENUS — Fonctionnement d'un réseau Wi-Fi public ; faux points d'accès ; risques de connexion dans un train, un hôtel ou un aéroport.
MÉTHODES / ACTIVITÉS — Apport court + étude de cas.
ÉVALUATION / PREUVE — Repérage des signaux d'alerte sur des scénarios proposés.

2 · Comprendre le MITM - 45 min

OBJECTIF — Comprendre le principe d'une interception de type MITM.
CONTENUS — Principe du Man-in-the-Middle ; données potentiellement observables ; différence entre trafic protégé et non protégé.
MÉTHODES / ACTIVITÉS — Schéma explicatif + démonstration pédagogique contrôlée.
ÉVALUATION / PREUVE — Reformulation du mécanisme et identification des mesures de protection.

3 · Démonstration d'interception contrôlée - 45 min

OBJECTIF — Observer une interception réseau en environnement contrôlé.
CONTENUS — Démonstration encadrée d'un scénario d'interception ; lecture des effets visibles pour l'utilisateur.
MÉTHODES / ACTIVITÉS — Démonstration commentée en environnement pédagogique sécurisé.
ÉVALUATION / PREUVE — Questions de compréhension et débriefing collectif.

SÉCURITÉ NUMÉRIQUE

4 · Réflexes de connexion en mobilité - 45 min

OBJECTIF — Choisir les bons réflexes de connexion en mobilité.
CONTENUS — Hotspot personnel ; VPN ; HTTPS ; désactivation des connexions automatiques ; vérification du réseau utilisé.
MÉTHODES / ACTIVITÉS — Atelier guidé + comparaison de pratiques.
ÉVALUATION / PREUVE — Mini-cas : choisir la mesure adaptée à chaque situation.

5 · Supports physiques non maîtrisés - 30 min

OBJECTIF — Reconnaître les risques liés aux supports physiques non maîtrisés.
CONTENUS — Clés USB, chargeurs, câbles et prises inconnus ; mécanismes de confiance et risques associés.
MÉTHODES / ACTIVITÉS — Apport illustré + exemples matériels.
ÉVALUATION / PREUVE — Classement de situations sûres / à éviter.

6 · Supports piégés : démonstration contrôlée - 45 min

OBJECTIF — Comprendre le fonctionnement de supports piégés.
CONTENUS — Démonstration pédagogique de supports USB ou accessoires compromis, sans mise en œuvre offensive hors environnement contrôlé.
MÉTHODES / ACTIVITÉS — Démonstration encadrée + analyse des signes d'alerte.
ÉVALUATION / PREUVE — Débriefing : mesures préventives à retenir.

7 · Exposition physique et shoulder surfing - 45 min

OBJECTIF — Réduire l'exposition physique des informations.
CONTENUS — Shoulder surfing ; écran visible ; perte ou vol opportuniste ; verrouillage automatique ; écran de confidentialité.
MÉTHODES / ACTIVITÉS — Mises en situation + observation croisée.
ÉVALUATION / PREUVE — Grille d'observation des bonnes pratiques.

SÉCURITÉ NUMÉRIQUE

8 · Atelier fil rouge : mobilité sécurisée - 60 min

OBJECTIF — Mettre en pratique une routine complète de mobilité sécurisée.
CONTENUS — Préparer le poste et le téléphone ; se connecter ; travailler dans un lieu public ; quitter le lieu ; réagir à un incident.
MÉTHODES / ACTIVITÉS — Atelier fil rouge en petits groupes sur scénario de déplacement.
ÉVALUATION / PREUVE — Validation d'une checklist de bonnes pratiques sur le scénario.

9 · Checklist déplacement et bilan - 30 min

OBJECTIF — Formaliser les réflexes à conserver après la formation.
CONTENUS — Checklist déplacement : réflexes avant départ, pendant le déplacement et au retour ; synthèse des points clés.
MÉTHODES / ACTIVITÉS — Synthèse participative + quiz final.
ÉVALUATION / PREUVE — Quiz final et engagement sur 3 actions à appliquer.

SÉCURITÉ NUMÉRIQUE

ÉVALUATION INITIALE

Questionnaire préalable et recueil des usages/attentes ; questions diagnostiques en début de session. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, exercices guidés, observation des pratiques, débriefings et corrections collectives tout au long de la journée. Les difficultés constatées peuvent conduire à adapter le rythme ou les démonstrations.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Évaluation finale par quiz et/ou mise en situation portant sur les réflexes et pratiques travaillés. Critère indicatif : au moins 70 % de réponses attendues ou validation de la grille de mise en situation. Seuil à confirmer lors de la validation finale du programme.

DOCUMENT REMIS AU PARTICIPANT

Checklist « sécurité déplacement » ; synthèse des réflexes de mobilité ; attestation de suivi et de fin de formation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

SecOps spearphishing

FINALITÉ PROFESSIONNELLE

Comprendre la construction d'une attaque de spearphishing afin de mieux détecter les signaux d'alerte et renforcer les procédures de vérification au sein de l'organisation.

PUBLIC VISÉ

Managers, équipes RH, directions et professionnels exposés à des sollicitations ciblées ou manipulant des informations sensibles.

PRÉREQUIS

Aucun prérequis technique avancé. Utilisation courante de la messagerie professionnelle et du web.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le contexte professionnel, les usages numériques concernés, le niveau d'aisance et les besoins d'adaptation. Échange de cadrage avec le commanditaire en intra. Les résultats servent à adapter les exemples, démonstrations et exercices ; ils ne constituent pas une sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra-entreprise. Classe virtuelle possible pour les parties compatibles avec les démonstrations et exercices, à confirmer selon la session.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel éventuel : outil précisé sur la convocation ; connexion stable et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 15/09/2026 · Responsable de validation : Clara Carriorbe

SEC-ENT-02 · SecOps spearphishing

SÉCURITÉ NUMÉRIQUE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable d'analyser un message ciblé, d'identifier les ressorts d'un spearphishing et d'appliquer une procédure de vérification avant toute action sensible.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Distinguer spearphishing et phishing générique.
- Identifier les éléments de crédibilité utilisés dans un message ciblé : prétexte, urgence, contexte et usurpation.
- Comprendre comment des informations publiques ou issues de fuites peuvent être utilisées pour personnaliser une attaque.
- Construire, dans un cadre pédagogique contrôlé, un scénario fictif afin d'identifier les points de vigilance côté défense.
- Appliquer une grille d'analyse et une procédure de vérification adaptées à l'organisation.

COMPÉTENCES VISÉES

Analyser un message suspect ; identifier les techniques d'ingénierie sociale et d'usurpation ; vérifier une sollicitation sensible ; contribuer à la prévention du spearphishing.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations, exercices progressifs, études de cas et mises en situation. Les activités sont adaptées au niveau, aux usages professionnels et aux contraintes de la session. Les démonstrations techniques sont réalisées exclusivement dans un environnement pédagogique contrôlé.

MOYENS ET RESSOURCES

Support de formation ; ordinateur et/ou smartphone selon le module ; connexion Internet ; navigateur récent ; environnement de démonstration contrôlé ; fiches pratiques et checklists correspondant au module ; vidéoprojecteur/écran en présentiel.

PROFIL DU FORMATEUR

Professionnel expérimenté en sécurité numérique, OSINT ou intelligence économique selon le module, disposant d'une pratique opérationnelle et d'une expérience de la formation d'adultes. Les démonstrations techniques sont réalisées dans un environnement pédagogique contrôlé.

SEC-ENT-02 · SecOps spearphishing

SÉCURITÉ NUMÉRIQUE

0 · Phishing et spearphishing - 30 min

OBJECTIF — Différencier phishing et spearphishing.
CONTENUS — Définitions ; objectifs ; profils ciblés ; enjeux pour managers, RH et directions.
MÉTHODES / ACTIVITÉS — Apport illustré + échanges sur les situations rencontrées.
ÉVALUATION / PREUVE — Questions diagnostiques.

1 · Anatomie d'un message ciblé - 45 min

OBJECTIF — Analyser l'anatomie d'un message ciblé.
CONTENUS — Prétexte, urgence, autorité, confiance, personnalisation, appel à l'action.
MÉTHODES / ACTIVITÉS — Analyse collective de messages fictifs.
ÉVALUATION / PREUVE — Repérage des ressorts de persuasion.

2 · Usurpation et spoofing - 45 min

OBJECTIF — Comprendre les mécanismes d'usurpation.
CONTENUS — Spoofing d'adresse, de domaine, d'identité affichée et de numéro ; indices vérifiables par l'utilisateur.
MÉTHODES / ACTIVITÉS — Apport + démonstration pédagogique défensive.
ÉVALUATION / PREUVE — Identification des indices d'usurpation sur exemples.

3 · Reconnaissance préalable - 45 min

OBJECTIF — Comprendre la phase de reconnaissance préalable.
CONTENUS — Informations publiques, réseaux sociaux, organigrammes, fuites de données et éléments contextuels utilisés pour personnaliser une attaque.
MÉTHODES / ACTIVITÉS — Étude de cas OSINT sur cible fictive.
ÉVALUATION / PREUVE — Liste des informations exploitables et mesures de réduction d'exposition.

SÉCURITÉ NUMÉRIQUE

4 · IA générative et personnalisation - 45 min

OBJECTIF — Mesurer l'apport et les limites de l'IA générative.
CONTENUS — Personnalisation de messages, variations linguistiques, automatisation ; signaux qui restent vérifiables.
MÉTHODES / ACTIVITÉS — Démonstration comparative + esprit critique.
ÉVALUATION / PREUVE — Analyse de messages générés et repérage d'anomalies.

5 · TP : collecte OSINT sur cible fictive - 45 min

OBJECTIF — Collecter les éléments nécessaires à un scénario fictif.
CONTENUS — Recherche contrôlée sur une cible fictive ; sélection d'informations utiles au scénario.
MÉTHODES / ACTIVITÉS — TP encadré en binômes.
ÉVALUATION / PREUVE — Fiche de collecte structurée.

6 · TP : construction du prétexte - 45 min

OBJECTIF — Construire un prétexte crédible sans passer à l'acte.
CONTENUS — Choix du contexte, de l'émetteur supposé, du motif et du canal ; cohérence du scénario.
MÉTHODES / ACTIVITÉS — Atelier de conception défensive.
ÉVALUATION / PREUVE — Présentation du scénario et critique croisée.

7 · TP : rédaction et analyse du message - 45 min

OBJECTIF — Rédiger puis déconstruire un message de spearphishing fictif.
CONTENUS — Objet, corps du message, demande formulée, éléments de confiance et signaux d'alerte.
MÉTHODES / ACTIVITÉS — Atelier rédaction + analyse défensive.
ÉVALUATION / PREUVE — Grille de détection remplie par un autre groupe.

SÉCURITÉ NUMÉRIQUE

8 · Mécanismes de piège en environnement sécurisé - 45 min

OBJECTIF — Comprendre les mécanismes de piège et de redirection.
CONTENUS — Liens, pièces jointes, formulaires et demandes d'action ; risques et contrôles à effectuer avant interaction.
MÉTHODES / ACTIVITÉS — Démonstration non opérationnelle en environnement isolé.
ÉVALUATION / PREUVE — Choix de la procédure de vérification adaptée.

9 · Routine de vérification et bilan - 30 min

OBJECTIF — Construire une routine de vérification anti-spearphishing.
CONTENUS — Vérification hors canal, signalement interne, conservation des éléments, réaction en cas de clic.
MÉTHODES / ACTIVITÉS — Synthèse + quiz final.
ÉVALUATION / PREUVE — Quiz final et checklist de vérification.

SEC-ENT-02 · SecOps spearphishing

SÉCURITÉ NUMÉRIQUE

ÉVALUATION INITIALE

Questionnaire préalable et recueil des usages/attentes ; questions diagnostiques en début de session. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, exercices guidés, observation des pratiques, débriefings et corrections collectives tout au long de la journée. Les difficultés constatées peuvent conduire à adapter le rythme ou les démonstrations.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Évaluation finale par quiz et/ou mise en situation portant sur les réflexes et pratiques travaillés. Critère indicatif : au moins 70 % de réponses attendues ou validation de la grille de mise en situation. Seuil à confirmer lors de la validation finale du programme.

DOCUMENT REMIS AU PARTICIPANT

Grille d'analyse rapide d'un mail suspect ; procédure de vérification ; attestation de suivi et de fin de formation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Hygiène numérique personnelle

FINALITÉ PROFESSIONNELLE

Renforcer les pratiques individuelles de sécurité numérique en réduisant les risques liés aux mots de passe, à l'authentification et aux usages d'outils non validés.

PUBLIC VISÉ

Tous collaborateurs.

PRÉREQUIS

Aucun prérequis technique. Venir avec son smartphone et, si possible, un ordinateur permettant les exercices de configuration.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le contexte professionnel, les usages numériques concernés, le niveau d'aisance et les besoins d'adaptation. Échange de cadrage avec le commanditaire en intra. Les résultats servent à adapter les exemples, démonstrations et exercices ; ils ne constituent pas une sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra-entreprise. Classe virtuelle possible pour les parties compatibles avec les démonstrations et exercices, à confirmer selon la session.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel éventuel : outil précisé sur la convocation ; connexion stable et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 15/09/2026 · Responsable de validation : Clara Carriorbe

SEC-ENT-03 · Hygiène numérique personnelle

SÉCURITÉ NUMÉRIQUE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de sécuriser ses principaux comptes, de mieux cloisonner ses usages professionnels et personnels et d'identifier les situations de Shadow IT présentant un risque pour l'organisation.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Comprendre les risques liés à la réutilisation des mots de passe et aux fuites d'identifiants.
- Mettre en place un gestionnaire de mots de passe et créer des pratiques robustes.
- Activer et utiliser une authentification à deux facteurs sur les comptes prioritaires.
- Identifier les principaux usages de Shadow IT et leurs impacts sur les données de l'entreprise.
- Appliquer des règles de cloisonnement entre usages professionnels et personnels.

COMPÉTENCES VISÉES

Sécuriser ses accès ; utiliser un gestionnaire de mots de passe ; activer le 2FA ; identifier les usages numériques non maîtrisés ; appliquer des règles de cloisonnement pro/perso.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations, exercices progressifs, études de cas et mises en situation. Les activités sont adaptées au niveau, aux usages professionnels et aux contraintes de la session. Les démonstrations techniques sont réalisées exclusivement dans un environnement pédagogique contrôlé.

MOYENS ET RESSOURCES

Support de formation ; ordinateur et/ou smartphone selon le module ; connexion Internet ; navigateur récent ; environnement de démonstration contrôlé ; fiches pratiques et checklists correspondant au module ; vidéoprojecteur/écran en présentiel.

PROFIL DU FORMATEUR

Professionnel expérimenté en sécurité numérique, OSINT ou intelligence économique selon le module, disposant d'une pratique opérationnelle et d'une expérience de la formation d'adultes. Les démonstrations techniques sont réalisées dans un environnement pédagogique contrôlé.

SEC-ENT-03 · Hygiène numérique personnelle

SÉCURITÉ NUMÉRIQUE

0 · Diagnostic des habitudes numériques - 30 min

OBJECTIF — Faire le diagnostic de ses habitudes numériques.
CONTENUS — Réutilisation, partage, stockage et mémorisation des mots de passe ; usages pro/perso.
MÉTHODES / ACTIVITÉS — Auto-diagnostic guidé.
ÉVALUATION / PREUVE — Identification de 3 pratiques à améliorer.

1 · Fuites de données et credential stuffing - 45 min

OBJECTIF — Comprendre les fuites de données et le credential stuffing.
CONTENUS — Origine des fuites ; réutilisation d'identifiants ; propagation d'une compromission entre services.
MÉTHODES / ACTIVITÉS — Apport illustré + cas pratique fictif.
ÉVALUATION / PREUVE — Reconstitution d'une chaîne de compromission.

2 · Limites des mots de passe faibles - 45 min

OBJECTIF — Comprendre les limites des mots de passe faibles.
CONTENUS — Longueur, unicité, prévisibilité ; principes des attaques par dictionnaire et réutilisation.
MÉTHODES / ACTIVITÉS — Démonstration pédagogique contrôlée.
ÉVALUATION / PREUVE — Comparaison de stratégies de mots de passe.

3 · Stratégie de mots de passe robuste - 45 min

OBJECTIF — Construire une stratégie de mots de passe robuste.
CONTENUS — Phrase de passe, unicité, comptes prioritaires, récupération et bonnes pratiques d'entreprise.
MÉTHODES / ACTIVITÉS — Atelier guidé.
ÉVALUATION / PREUVE — Élaboration d'une règle personnelle de gestion.

SÉCURITÉ NUMÉRIQUE

4 · Gestionnaire de mots de passe - 45 min

OBJECTIF — Prendre en main un gestionnaire de mots de passe.
CONTENUS — Fonctionnement, coffre, mot de passe maître, génération et remplissage automatique.
MÉTHODES / ACTIVITÉS — Démonstration + configuration sur environnement de test ou outil autorisé.
ÉVALUATION / PREUVE — Réalisation d'une configuration type.

5 · MFA / 2FA : principes et choix - 30 min

OBJECTIF — Comprendre le MFA / 2FA.
CONTENUS — SMS, application d'authentification, clé physique, passkeys ; avantages et limites.
MÉTHODES / ACTIVITÉS — Apport comparatif.
ÉVALUATION / PREUVE — Choix du facteur adapté à différents comptes.

6 · Configuration de l'authentification renforcée - 45 min

OBJECTIF — Configurer une authentification renforcée.
CONTENUS — Activation d'une application d'authentification ou démonstration sur compte de test ; codes de secours.
MÉTHODES / ACTIVITÉS — Atelier guidé.
ÉVALUATION / PREUVE — Validation de la procédure de configuration.

7 · Perte ou changement de téléphone - 30 min

OBJECTIF — Préparer la perte ou le changement de téléphone.
CONTENUS — Codes de récupération ; appareil secondaire ; récupération de compte ; sauvegarde sécurisée.
MÉTHODES / ACTIVITÉS — Étude de cas + checklist.
ÉVALUATION / PREUVE — Résolution d'un scénario de perte d'appareil.

SEC-ENT-03 · Hygiène numérique personnelle

SÉCURITÉ NUMÉRIQUE

8 · Shadow IT et séparation pro / perso - 60 min

OBJECTIF — Identifier et réduire le Shadow IT.
CONTENUS — Cloud personnels, messageries, outils collaboratifs, IA générative, transfert de fichiers et séparation pro/perso.
MÉTHODES / ACTIVITÉS — Cartographie d'usages + cas pratiques.
ÉVALUATION / PREUVE — Classement des usages selon le niveau de risque.

9 · Plan personnel d'hygiène numérique - 45 min

OBJECTIF — Construire son plan personnel d'hygiène numérique.
CONTENUS — Priorisation des comptes, actions immédiates, habitudes à maintenir et ressources internes.
MÉTHODES / ACTIVITÉS — Atelier individuel + quiz final.
ÉVALUATION / PREUVE — Plan d'action personnel + quiz de validation.

SEC-ENT-03 · Hygiène numérique personnelle

SÉCURITÉ NUMÉRIQUE

ÉVALUATION INITIALE

Questionnaire préalable et recueil des usages/attentes ; questions diagnostiques en début de session. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, exercices guidés, observation des pratiques, débriefings et corrections collectives tout au long de la journée. Les difficultés constatées peuvent conduire à adapter le rythme ou les démonstrations.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Évaluation finale par quiz et/ou mise en situation portant sur les réflexes et pratiques travaillés. Critère indicatif : au moins 70 % de réponses attendues ou validation de la grille de mise en situation. Seuil à confirmer lors de la validation finale du programme.

DOCUMENT REMIS AU PARTICIPANT

Gestionnaire de mots de passe configuré ; 2FA activé sur les comptes critiques lorsque possible ; checklist Shadow IT ; attestation de suivi et de fin de formation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

OSINT défensif — Maîtriser son empreinte numérique

FINALITÉ PROFESSIONNELLE

Comprendre ce qu'une recherche en sources ouvertes peut révéler sur un collaborateur ou une organisation et réduire son exposition numérique de manière proportionnée.

PUBLIC VISÉ

Managers, dirigeants, équipes communication et professionnels exposés publiquement au nom de leur organisation.

PRÉREQUIS

Aucun prérequis OSINT. Aisance courante avec un navigateur web et les réseaux professionnels.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le contexte professionnel, les usages numériques concernés, le niveau d'aisance et les besoins d'adaptation. Échange de cadrage avec le commanditaire en intra. Les résultats servent à adapter les exemples, démonstrations et exercices ; ils ne constituent pas une sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra-entreprise. Classe virtuelle possible pour les parties compatibles avec les démonstrations et exercices, à confirmer selon la session.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel éventuel : outil précisé sur la convocation ; connexion stable et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 15/09/2026 · Responsable de validation : Clara Carriorbe

SEC-ENT-04 · OSINT défensif — Maîtriser son empreinte numérique

SÉCURITÉ NUMÉRIQUE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable d'identifier les principales composantes de son empreinte numérique, d'évaluer les informations accessibles publiquement et de mettre en œuvre des actions de réduction d'exposition.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Définir l'OSINT et comprendre ses usages légaux ainsi que son utilisation possible dans une phase de reconnaissance.
- Identifier les informations qu'un tiers peut collecter à partir de réseaux sociaux, offres d'emploi, documents publics, métadonnées et fuites connues.
- Réaliser un audit défensif de son exposition numérique dans un cadre contrôlé.
- Paramétrer ses profils professionnels de manière plus prudente.
- Construire un plan d'action individuel de réduction d'exposition.

COMPÉTENCES VISÉES

Analyser son empreinte numérique ; identifier les informations exposées ; évaluer les risques de corrélation ; paramétrer ses profils professionnels ; prioriser des actions de réduction d'exposition.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations, exercices progressifs, études de cas et mises en situation. Les activités sont adaptées au niveau, aux usages professionnels et aux contraintes de la session. Les démonstrations techniques sont réalisées exclusivement dans un environnement pédagogique contrôlé.

MOYENS ET RESSOURCES

Support de formation ; ordinateur et/ou smartphone selon le module ; connexion Internet ; navigateur récent ; environnement de démonstration contrôlé ; fiches pratiques et checklists correspondant au module ; vidéoprojecteur/écran en présentiel.

PROFIL DU FORMATEUR

Professionnel expérimenté en sécurité numérique, OSINT ou intelligence économique selon le module, disposant d'une pratique opérationnelle et d'une expérience de la formation d'adultes. Les démonstrations techniques sont réalisées dans un environnement pédagogique contrôlé.

SÉCURITÉ NUMÉRIQUE

0 · OSINT défensif : principes et usages - 30 min

OBJECTIF — Comprendre l'OSINT dans une logique défensive.
CONTENUS — Définition, sources ouvertes, cadre légal et usages de reconnaissance par un adversaire.
MÉTHODES / ACTIVITÉS — Apport introductif + exemples.
ÉVALUATION / PREUVE — Questions diagnostiques.

1 · Cycle de ciblage d'une personne ou organisation - 45 min

OBJECTIF — Comprendre le cycle de ciblage d'une personne ou d'une organisation.
CONTENUS — Définition de cible, collecte, recoupement, qualification et exploitation de l'information.
MÉTHODES / ACTIVITÉS — Schéma méthodologique + étude de cas.
ÉVALUATION / PREUVE — Remise en ordre des étapes du cycle.

2 · Démonstration : reconstitution d'un profil fictif - 45 min

OBJECTIF — Observer la reconstitution d'un profil fictif.
CONTENUS — Démonstration de recherche sur une identité fictive ; corrélation de traces publiques.
MÉTHODES / ACTIVITÉS — Démonstration commentée.
ÉVALUATION / PREUVE — Identification des sources utilisées.

3 · Réseaux professionnels et informations publiques - 45 min

OBJECTIF — Analyser les informations issues des réseaux professionnels.
CONTENUS — LinkedIn, biographies, organigrammes, fonctions, relations, habitudes de publication.
MÉTHODES / ACTIVITÉS — Analyse guidée de profils fictifs.
ÉVALUATION / PREUVE — Repérage des informations sensibles ou corrélables.

SÉCURITÉ NUMÉRIQUE

4 · Traces organisationnelles publiques - 45 min

OBJECTIF — Exploiter les traces organisationnelles publiques.
CONTENUS — Offres d'emploi, pages institutionnelles, communiqués, photos et documents publics.
MÉTHODES / ACTIVITÉS — Recherche guidée sur cas fictif.
ÉVALUATION / PREUVE — Liste structurée des informations exposées.

5 · Documents publics et métadonnées - 45 min

OBJECTIF — Identifier les risques liés aux documents et métadonnées.
CONTENUS — Métadonnées, noms de fichiers, auteurs, versions, propriétés et traces documentaires.
MÉTHODES / ACTIVITÉS — Démonstration + exercice sur documents pédagogiques.
ÉVALUATION / PREUVE — Fiche de vérification des métadonnées.

6 · Atelier : audit de son empreinte numérique - 45 min

OBJECTIF — Auditer son empreinte numérique.
CONTENUS — Recherche de ses propres traces ou d'un profil de test ; classement par sensibilité et exploitabilité.
MÉTHODES / ACTIVITÉS — Atelier individuel encadré.
ÉVALUATION / PREUVE — Inventaire des traces identifiées.

7 · Qualification de l'exposition réelle - 45 min

OBJECTIF — Qualifier ce qui est réellement exploitable.
CONTENUS — Vraisemblance, actualité, recoupement, risque de fausse attribution, impact potentiel.
MÉTHODES / ACTIVITÉS — Atelier de qualification des résultats.
ÉVALUATION / PREUVE — Grille fiabilité / exposition / impact.

SÉCURITÉ NUMÉRIQUE

8 · Réduction de l'exposition numérique - 45 min

OBJECTIF — Réduire son exposition sans nuire à sa visibilité professionnelle.
CONTENUS — Paramètres de confidentialité, contenu public, séparation des usages, suppression ou correction de traces lorsque possible.
MÉTHODES / ACTIVITÉS — Atelier de remédiation.
ÉVALUATION / PREUVE — Plan de réduction d'exposition.

9 · Plan d'action à 48 heures - 30 min

OBJECTIF — Formaliser un plan d'action à 48 heures.
CONTENUS — Priorités immédiates, actions à moyen terme, veille personnelle et points de contrôle réguliers.
MÉTHODES / ACTIVITÉS — Synthèse + quiz final.
ÉVALUATION / PREUVE — Plan d'action individuel + quiz.

SÉCURITÉ NUMÉRIQUE

ÉVALUATION INITIALE

Questionnaire préalable et recueil des usages/attentes ; questions diagnostiques en début de session. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, exercices guidés, observation des pratiques, débriefings et corrections collectives tout au long de la journée. Les difficultés constatées peuvent conduire à adapter le rythme ou les démonstrations.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Évaluation finale par quiz et/ou mise en situation portant sur les réflexes et pratiques travaillés. Critère indicatif : au moins 70 % de réponses attendues ou validation de la grille de mise en situation. Seuil à confirmer lors de la validation finale du programme.

DOCUMENT REMIS AU PARTICIPANT

Rapport personnel d'empreinte numérique ou grille d'audit selon les modalités de la session ; checklist de réduction d'exposition ; attestation de suivi et de fin de formation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Sécurité des échanges confidentiels

FINALITÉ PROFESSIONNELLE

Sécuriser les échanges et documents sensibles en choisissant des outils et pratiques adaptés au niveau de confidentialité requis.

PUBLIC VISÉ

Directions, fonctions juridiques, RH et professionnels manipulant des informations sensibles ou confidentielles.

PRÉREQUIS

Aucun prérequis technique avancé. Utilisation courante d'un smartphone et des outils de communication professionnelle.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le contexte professionnel, les usages numériques concernés, le niveau d'aisance et les besoins d'adaptation. Échange de cadrage avec le commanditaire en intra. Les résultats servent à adapter les exemples, démonstrations et exercices ; ils ne constituent pas une sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra-entreprise. Classe virtuelle possible pour les parties compatibles avec les démonstrations et exercices, à confirmer selon la session.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel éventuel : outil précisé sur la convocation ; connexion stable et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 15/09/2026 · Responsable de validation : Clara Carriorbe

SEC-ENT-05 · Sécurité des échanges confidentiels

SÉCURITÉ NUMÉRIQUE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable d'identifier les risques liés aux échanges non sécurisés, de choisir des moyens de communication adaptés et d'appliquer des mesures simples de protection des fichiers et métadonnées.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Comprendre le rôle du chiffrement et les limites d'une protection faible par mot de passe.
- Identifier les risques d'interception associés à un échange non chiffré.
- Comparer les usages de plusieurs outils de messagerie et choisir une solution adaptée au contexte.
- Transmettre un document sensible par un canal approprié.
- Identifier et supprimer, lorsque nécessaire, les métadonnées d'un fichier avant diffusion.

COMPÉTENCES VISÉES

Évaluer la sensibilité d'un échange ; choisir un canal de communication adapté ; sécuriser un fichier avant envoi ; appliquer des réflexes de confidentialité et de minimisation des données.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations, exercices progressifs, études de cas et mises en situation. Les activités sont adaptées au niveau, aux usages professionnels et aux contraintes de la session. Les démonstrations techniques sont réalisées exclusivement dans un environnement pédagogique contrôlé.

MOYENS ET RESSOURCES

Support de formation ; ordinateur et/ou smartphone selon le module ; connexion Internet ; navigateur récent ; environnement de démonstration contrôlé ; fiches pratiques et checklists correspondant au module ; vidéoprojecteur/écran en présentiel.

PROFIL DU FORMATEUR

Professionnel expérimenté en sécurité numérique, OSINT ou intelligence économique selon le module, disposant d'une pratique opérationnelle et d'une expérience de la formation d'adultes. Les démonstrations techniques sont réalisées dans un environnement pédagogique contrôlé.

SEC-ENT-05 · Sécurité des échanges confidentiels

SÉCURITÉ NUMÉRIQUE

0 · Identifier les échanges sensibles - 30 min

OBJECTIF — Identifier les échanges et informations sensibles.
CONTENUS — Typologie des informations confidentielles ; canaux utilisés ; erreurs courantes de diffusion.
MÉTHODES / ACTIVITÉS — Cartographie rapide des usages.
ÉVALUATION / PREUVE — Identification des situations à risque.

1 · Comprendre le chiffrement - 45 min

OBJECTIF — Comprendre les principes du chiffrement.
CONTENUS — Chiffrement en transit, au repos et de bout en bout ; clés et limites des protections.
MÉTHODES / ACTIVITÉS — Apport illustré.
ÉVALUATION / PREUVE — Questions de compréhension.

2 · Interception d'un échange non sécurisé - 45 min

OBJECTIF — Observer l'interception d'un échange non sécurisé.
CONTENUS — Démonstration pédagogique contrôlée d'un échange insuffisamment protégé.
MÉTHODES / ACTIVITÉS — Démonstration commentée en environnement isolé.
ÉVALUATION / PREUVE — Repérage des informations exposées.

3 · Échange protégé vs non protégé - 45 min

OBJECTIF — Comparer un échange protégé et non protégé.
CONTENUS — Effets du chiffrement ; métadonnées encore visibles ; bonnes pratiques de canal.
MÉTHODES / ACTIVITÉS — Comparaison guidée.
ÉVALUATION / PREUVE — Choix du canal adapté à plusieurs cas.

SÉCURITÉ NUMÉRIQUE

4 · Protection des fichiers et pièces jointes - 45 min

OBJECTIF — Protéger les fichiers et pièces jointes.
CONTENUS — Protection par mot de passe, chiffrement, partage de secret, limites des fichiers faiblement protégés.
MÉTHODES / ACTIVITÉS — Démonstration + exercice.
ÉVALUATION / PREUVE — Mise en œuvre d'une procédure de protection sur fichier test.

5 · Comparatif des outils de messagerie - 45 min

OBJECTIF — Comparer les principaux outils de messagerie.
CONTENUS — Signal, WhatsApp, Teams, Telegram : usages, chiffrement, gestion des groupes, sauvegardes et limites.
MÉTHODES / ACTIVITÉS — Matrice comparative participative.
ÉVALUATION / PREUVE — Choix argumenté d'un outil selon un scénario.

6 · Atelier : canal d'échange sensible - 45 min

OBJECTIF — Configurer un canal d'échange sensible.
CONTENUS — Paramètres essentiels, vérification des interlocuteurs, messages éphémères si pertinent, gestion des pièces jointes.
MÉTHODES / ACTIVITÉS — Atelier guidé sur environnement autorisé ou démonstration.
ÉVALUATION / PREUVE — Checklist de configuration.

7 · Transfert sécurisé de documents - 45 min

OBJECTIF — Transférer un document de manière maîtrisée.
CONTENUS — Lien public vs lien restreint, expiration, droits, mot de passe séparé, contrôle des destinataires.
MÉTHODES / ACTIVITÉS — Cas pratiques.
ÉVALUATION / PREUVE — Sélection de la méthode adaptée.

SÉCURITÉ NUMÉRIQUE

8 · Métadonnées : détection et nettoyage - 45 min

OBJECTIF — Comprendre et nettoyer les métadonnées.
CONTENUS — Métadonnées de documents, images et PDF ; informations révélées ; principes de nettoyage.
MÉTHODES / ACTIVITÉS — Démonstration + atelier sur fichiers pédagogiques.
ÉVALUATION / PREUVE — Contrôle avant/après nettoyage.

9 · Mini-protocole d'échange confidentiel - 30 min

OBJECTIF — Formaliser un mini-protocole d'échange confidentiel.
CONTENUS — Règles de canal, de fichier, d'authentification, de validation et de conservation.
MÉTHODES / ACTIVITÉS — Synthèse en groupe + quiz final.
ÉVALUATION / PREUVE — Mini-protocole + quiz de validation.

SEC-ENT-05 · Sécurité des échanges confidentiels

SÉCURITÉ NUMÉRIQUE

ÉVALUATION INITIALE

Questionnaire préalable et recueil des usages/attentes ; questions diagnostiques en début de session. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, exercices guidés, observation des pratiques, débriefings et corrections collectives tout au long de la journée. Les difficultés constatées peuvent conduire à adapter le rythme ou les démonstrations.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Évaluation finale par quiz et/ou mise en situation portant sur les réflexes et pratiques travaillés. Critère indicatif : au moins 70 % de réponses attendues ou validation de la grille de mise en situation. Seuil à confirmer lors de la validation finale du programme.

DOCUMENT REMIS AU PARTICIPANT

Outil de messagerie sécurisé configuré lorsque la politique interne le permet ; réflexe métadonnées ; protocole d'échanges confidentiels adapté à l'équipe ; attestation de suivi et de fin de formation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Sécurité des appareils mobiles

FINALITÉ PROFESSIONNELLE

Comprendre les principales surfaces d'exposition d'un smartphone et savoir le paramétrer pour réduire les risques dans les usages quotidiens et en déplacement.

PUBLIC VISÉ

Tous collaborateurs utilisant un smartphone dans un contexte personnel et/ou professionnel.

PRÉREQUIS

Aucun prérequis technique. Venir avec son smartphone pour les exercices de paramétrage, sous réserve de la politique de l'organisation.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le contexte professionnel, les usages numériques concernés, le niveau d'aisance et les besoins d'adaptation. Échange de cadrage avec le commanditaire en intra. Les résultats servent à adapter les exemples, démonstrations et exercices ; ils ne constituent pas une sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra-entreprise. Classe virtuelle possible pour les parties compatibles avec les démonstrations et exercices, à confirmer selon la session.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel éventuel : outil précisé sur la convocation ; connexion stable et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 15/09/2026 · Responsable de validation : Clara Carriorbe

SEC-ENT-06 · Sécurité des appareils mobiles

SÉCURITÉ NUMÉRIQUE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable d'auditer les principaux paramètres de sécurité et de confidentialité de son smartphone et d'appliquer des mesures adaptées aux situations de déplacement.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Identifier les données, permissions et capteurs susceptibles d'exposer l'utilisateur.
- Auditer et ajuster les permissions des applications.
- Comprendre les risques associés aux réseaux, bornes de charge et périphériques USB non maîtrisés.
- Activer les protections essentielles : verrouillage, chiffrement, sauvegarde et mises à jour.
- Préparer son téléphone avant un déplacement, notamment à l'étranger.

COMPÉTENCES VISÉES

Auditer les permissions d'un smartphone ; ajuster les paramètres de sécurité ; identifier les risques liés aux connexions et périphériques ; préparer un appareil mobile pour un déplacement.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations, exercices progressifs, études de cas et mises en situation. Les activités sont adaptées au niveau, aux usages professionnels et aux contraintes de la session. Les démonstrations techniques sont réalisées exclusivement dans un environnement pédagogique contrôlé.

MOYENS ET RESSOURCES

Support de formation ; ordinateur et/ou smartphone selon le module ; connexion Internet ; navigateur récent ; environnement de démonstration contrôlé ; fiches pratiques et checklists correspondant au module ; vidéoprojecteur/écran en présentiel.

PROFIL DU FORMATEUR

Professionnel expérimenté en sécurité numérique, OSINT ou intelligence économique selon le module, disposant d'une pratique opérationnelle et d'une expérience de la formation d'adultes. Les démonstrations techniques sont réalisées dans un environnement pédagogique contrôlé.

SEC-ENT-06 · Sécurité des appareils mobiles

SÉCURITÉ NUMÉRIQUE

0 · Surface d'exposition d'un smartphone - 30 min

OBJECTIF — Comprendre la surface d'exposition d'un smartphone.
CONTENUS — Rôle du téléphone dans l'écosystème professionnel ; données, comptes, capteurs et connexions.
MÉTHODES / ACTIVITÉS — Apport introductif + auto-diagnostic.
ÉVALUATION / PREUVE — Identification des principales surfaces d'exposition.

1 · Données collectées et transmises - 45 min

OBJECTIF — Identifier les données collectées et transmises.
CONTENUS — Localisation, identifiants, télémétrie, données d'usage et synchronisations.
MÉTHODES / ACTIVITÉS — Apport illustré + lecture de paramètres.
ÉVALUATION / PREUVE — Questions de compréhension.

2 · Permissions applicatives - 45 min

OBJECTIF — Comprendre les permissions applicatives.
CONTENUS — Micro, caméra, contacts, photos, Bluetooth, localisation ; permissions permanentes ou ponctuelles.
MÉTHODES / ACTIVITÉS — Démonstration sur iOS/Android.
ÉVALUATION / PREUVE — Repérage des permissions excessives.

3 · Interception mobile : principes - 45 min

OBJECTIF — Comprendre le principe d'une interception mobile.
CONTENUS — Présentation pédagogique du rôle du réseau mobile et du principe d'un IMSI catcher, sans mise en œuvre offensive.
MÉTHODES / ACTIVITÉS — Démonstration conceptuelle / environnement contrôlé.
ÉVALUATION / PREUVE — Reformulation des risques et limites.

SÉCURITÉ NUMÉRIQUE

4 · Atelier : audit des permissions - 45 min

OBJECTIF — Auditer les permissions de son appareil.
CONTENUS — Revue guidée des applications et permissions ; suppression ou restriction des accès inutiles.
MÉTHODES / ACTIVITÉS — Atelier individuel, sous réserve de la politique de l'organisation.
ÉVALUATION / PREUVE — Grille d'audit complétée.

5 · Paramétrage de sécurité iOS / Android - 45 min

OBJECTIF — Renforcer les paramètres de sécurité iOS / Android.
CONTENUS — Verrouillage, biométrie, mises à jour, localisation de l'appareil, sauvegardes, confidentialité et comptes.
MÉTHODES / ACTIVITÉS — Atelier guidé.
ÉVALUATION / PREUVE — Validation d'une checklist de paramétrage.

6 · NFC, Bluetooth et connexions de proximité - 30 min

OBJECTIF — Comprendre les risques liés aux connexions de proximité.
CONTENUS — NFC, Bluetooth, Wi-Fi, bornes de charge et réseaux publics.
MÉTHODES / ACTIVITÉS — Apport + étude de cas.
ÉVALUATION / PREUVE — Choix du bon réflexe selon la situation.

7 · Périphériques USB non maîtrisés - 45 min

OBJECTIF — Comprendre le risque des périphériques USB non maîtrisés.
CONTENUS — Principe d'un Bad USB / Rubber Ducky présenté à des fins défensives ; mesures de prévention.
MÉTHODES / ACTIVITÉS — Démonstration pédagogique contrôlée.
ÉVALUATION / PREUVE — Identification des mesures de prévention.

SÉCURITÉ NUMÉRIQUE

8 · Chiffrement, sauvegarde et récupération - 45 min

OBJECTIF — Sécuriser stockage, sauvegarde et récupération.
CONTENUS — Chiffrement du stockage, sauvegarde, codes de récupération et procédures en cas de perte.
MÉTHODES / ACTIVITÉS — Atelier guidé + cas pratique.
ÉVALUATION / PREUVE — Vérification d'une stratégie de sauvegarde/récupération.

9 · Préparer son téléphone avant un déplacement - 45 min

OBJECTIF — Préparer son téléphone avant un déplacement.
CONTENUS — Voyage à l'étranger, applications nécessaires, données à emporter, comptes, connexions, conduite à tenir au retour.
MÉTHODES / ACTIVITÉS — Atelier checklist + quiz final.
ÉVALUATION / PREUVE — Checklist « téléphone sécurisé » + quiz.

SEC-ENT-06 · Sécurité des appareils mobiles

SÉCURITÉ NUMÉRIQUE

ÉVALUATION INITIALE

Questionnaire préalable et recueil des usages/attentes ; questions diagnostiques en début de session. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, exercices guidés, observation des pratiques, débriefings et corrections collectives tout au long de la journée. Les difficultés constatées peuvent conduire à adapter le rythme ou les démonstrations.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Évaluation finale par quiz et/ou mise en situation portant sur les réflexes et pratiques travaillés. Critère indicatif : au moins 70 % de réponses attendues ou validation de la grille de mise en situation. Seuil à confirmer lors de la validation finale du programme.

DOCUMENT REMIS AU PARTICIPANT

Checklist « téléphone sécurisé » ; paramètres essentiels revus pendant l'atelier lorsque possible ; attestation de suivi et de fin de formation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Intelligence économique — Comprendre l’adversaire

FINALITÉ PROFESSIONNELLE

Utiliser les sources ouvertes pour mieux connaître un individu, une entreprise ou un concurrent et produire une veille économique structurée au service de la décision.

PUBLIC VISÉ

Directions, business development, juristes et professionnels amenés à analyser des partenaires, concurrents ou acteurs d’un marché.

PRÉREQUIS

Aisance courante avec la recherche web. Aucun prérequis technique avancé en OSINT.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable sur le contexte professionnel, les usages numériques concernés, le niveau d’aisance et les besoins d’adaptation. Échange de cadrage avec le commanditaire en intra. Les résultats servent à adapter les exemples, démonstrations et exercices ; ils ne constituent pas une sélection, sauf inadéquation manifeste avec le public ou les prérequis.

DURÉE

1 jour - 7 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra-entreprise. Classe virtuelle possible pour les parties compatibles avec les démonstrations et exercices, à confirmer selon la session.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel éventuel : outil précisé sur la convocation ; connexion stable et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D’ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 15/09/2026 · Responsable de validation : Clara Carriorbe

SEC-ENT-07 · Intelligence économique — Comprendre l'adversaire

SÉCURITÉ NUMÉRIQUE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de conduire une recherche OSINT simple sur un individu ou une entreprise, de cartographier des éléments clés et de structurer une veille économique exploitable.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Comprendre les principes, sources et limites juridiques de l'OSINT appliqué à l'intelligence économique.
- Rechercher et structurer des informations publiques sur un individu fictif.
- Identifier les principales sources ouvertes utiles à l'analyse d'une entreprise.
- Reconstituer des éléments de structure : dirigeants, filiales, actionnaires et réseaux.
- Identifier des signaux faibles et définir une veille OSINT sur un secteur ou un concurrent.

COMPÉTENCES VISÉES

Cadrer une recherche d'intelligence économique ; collecter des informations en sources ouvertes ; cartographier un individu ou une organisation ; qualifier des signaux faibles ; structurer une veille.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations, exercices progressifs, études de cas et mises en situation. Les activités sont adaptées au niveau, aux usages professionnels et aux contraintes de la session. Les démonstrations techniques sont réalisées exclusivement dans un environnement pédagogique contrôlé.

MOYENS ET RESSOURCES

Support de formation ; ordinateur et/ou smartphone selon le module ; connexion Internet ; navigateur récent ; environnement de démonstration contrôlé ; fiches pratiques et checklists correspondant au module ; vidéoprojecteur/écran en présentiel.

PROFIL DU FORMATEUR

Professionnel expérimenté en sécurité numérique, OSINT ou intelligence économique selon le module, disposant d'une pratique opérationnelle et d'une expérience de la formation d'adultes. Les démonstrations techniques sont réalisées dans un environnement pédagogique contrôlé.

SEC-ENT-07 · Intelligence économique — Comprendre l'adversaire

SÉCURITÉ NUMÉRIQUE

0 · OSINT et intelligence économique - 30 min

OBJECTIF — Comprendre l'OSINT appliqué à l'intelligence économique.
CONTENUS — Définition, objectifs, sources ouvertes, cadre légal et éthique, limites de l'analyse.
MÉTHODES / ACTIVITÉS — Apport introductif + exemples métier.
ÉVALUATION / PREUVE — Questions diagnostiques.

1 · Méthode de recherche et qualification des sources - 45 min

OBJECTIF — Cadrer une recherche et qualifier ses sources.
CONTENUS — Question de recherche, mots-clés, sources primaires/secondaires, fiabilité, actualité et recoupement.
MÉTHODES / ACTIVITÉS — Méthode guidée + exercice court.
ÉVALUATION / PREUVE — Grille de qualification de sources.

2 · Recherche sur un individu - 45 min

OBJECTIF — Rechercher des informations publiques sur un individu.
CONTENUS — LinkedIn, réseaux sociaux, presse, registres et biographies publiques.
MÉTHODES / ACTIVITÉS — Démonstration + recherche sur profil fictif.
ÉVALUATION / PREUVE — Fiche de collecte structurée.

3 · Atelier : profil d'un individu fictif - 45 min

OBJECTIF — Reconstituer le profil d'un individu fictif.
CONTENUS — Fonctions, parcours, intérêts professionnels, relations et éléments de contexte.
MÉTHODES / ACTIVITÉS — Atelier en binômes.
ÉVALUATION / PREUVE — Restitution synthétique et justification des sources.

SÉCURITÉ NUMÉRIQUE

4 · Réseaux d’influence et relations professionnelles - 45 min

OBJECTIF — Identifier les réseaux d’influence et relations professionnelles.
CONTENUS — Relations directes/indirectes, affiliations, conseils d’administration, associations et événements.
MÉTHODES / ACTIVITÉS — Cartographie simple.
ÉVALUATION / PREUVE — Mini-carte de relations argumentée.

5 · Sources ouvertes sur les entreprises - 45 min

OBJECTIF — Identifier les sources ouvertes sur une entreprise.
CONTENUS — Registres, presse, sites institutionnels, offres d’emploi, brevets et bases spécialisées accessibles.
MÉTHODES / ACTIVITÉS — Démonstration + recherche guidée.
ÉVALUATION / PREUVE — Tableau des sources pertinentes par besoin.

6 · Dirigeants, filiales et actionnaires - 45 min

OBJECTIF — Cartographier dirigeants, filiales et actionnaires.
CONTENUS — Structure de groupe, liens capitalistiques, gouvernance et sociétés liées.
MÉTHODES / ACTIVITÉS — Atelier de cartographie sur entreprise fictive.
ÉVALUATION / PREUVE — Schéma organisationnel sourcé.

7 · Atelier : structure d’une entreprise fictive - 45 min

OBJECTIF — Reconstituer la structure d’une entreprise fictive.
CONTENUS — Consolidation des informations collectées ; chronologie et principaux acteurs.
MÉTHODES / ACTIVITÉS — Cas pratique en groupe.
ÉVALUATION / PREUVE — Restitution orale courte avec sources.

SÉCURITÉ NUMÉRIQUE

8 · Signaux faibles et mouvements stratégiques - 45 min

OBJECTIF — Détecter des signaux faibles et mouvements stratégiques.
CONTENUS — Recrutements, brevets, changements de dirigeants, nouveaux partenaires, implantation et communication.
MÉTHODES / ACTIVITÉS — Étude de cas + analyse collective.
ÉVALUATION / PREUVE — Qualification de signaux faibles et niveau de confiance.

9 · Mettre en place une veille OSINT simple - 30 min

OBJECTIF — Construire une veille OSINT simple et exploitable.
CONTENUS — Définition du périmètre, sources à suivre, fréquence, alertes, collecte et format de restitution.
MÉTHODES / ACTIVITÉS — Atelier de conception + quiz final.
ÉVALUATION / PREUVE — Mini-plan de veille + quiz de validation.

SÉCURITÉ NUMÉRIQUE

ÉVALUATION INITIALE

Questionnaire préalable et recueil des usages/attentes ; questions diagnostiques en début de session. Aucun critère de sélection, sauf inadéquation manifeste avec le public ou les prérequis.

ÉVALUATIONS FORMATIVES

Questions orales, exercices guidés, observation des pratiques, débriefings et corrections collectives tout au long de la journée. Les difficultés constatées peuvent conduire à adapter le rythme ou les démonstrations.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Évaluation finale par quiz et/ou mise en situation portant sur les réflexes et pratiques travaillés. Critère indicatif : au moins 70 % de réponses attendues ou validation de la grille de mise en situation. Seuil à confirmer lors de la validation finale du programme.

DOCUMENT REMIS AU PARTICIPANT

Méthodologie de veille OSINT économique ; cartographie réalisée en atelier ; attestation de suivi et de fin de formation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Affinis Campus

2 JOURS

4 formations

Approfondir une pratique et multiplier les mises en situation.



- AC-OSINT-201 — Fondamentaux opérationnels de l'OSINT
- AC-DD-201 — Due diligence en sources ouvertes
- AC-SOC-201 — Investigation avancée sur les réseaux sociaux
- AC-FIMI-201 — Détecter une opération informationnelle coordonnée

Fondamentaux opérationnels de l'OSINT

FINALITÉ PROFESSIONNELLE

Permettre à des professionnels de conduire une recherche simple en sources ouvertes, depuis la formulation du besoin jusqu'à une restitution courte, sourcée et exploitable pour la prise de décision.

PUBLIC VISÉ

Professionnels amenés à rechercher, vérifier ou analyser des informations externes : consultants, analystes, juristes, commerciaux, acheteurs, responsables sûreté ou conformité, agents publics et fonctions support.

PRÉREQUIS

Aisance courante avec un navigateur web et les outils bureautiques. Aucun prérequis technique avancé en OSINT. Disposer d'un ordinateur portable connecté à Internet pour les exercices.

MODALITÉS DE POSITIONNEMENT

Avant l'entrée en formation : questionnaire en ligne portant sur le métier, les usages visés, l'expérience en recherche web, la maîtrise des opérateurs et les besoins d'adaptation. Court test diagnostic de 10 questions. Les résultats servent à adapter les exemples et exercices ; ils ne constituent pas une sélection, sauf impossibilité manifeste de suivre la formation.

DURÉE

2 jours - 14 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel, classe virtuelle synchrone ou classe hybride ; formation inter ou intra-entreprise.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-201 · Fondamentaux opérationnels de l'OSINT

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Distinguer donnée, information, renseignement et preuve.
- Identifier les limites juridiques, éthiques et techniques d'une recherche, avec et sans IA.
- Appliquer des mesures élémentaires d'OPSEC.
- Transformer un besoin métier en questions de recherche.
- Construire un lexique, un plan de recherche et des requêtes avancées.
- Sélectionner des sources adaptées et en apprécier la fiabilité.
- Recouper les informations et distinguer faits, hypothèses et opinions.
- Produire une restitution courte, structurée et traçable.

COMPÉTENCES VISÉES

Cadrer une investigation simple ; planifier une collecte ; utiliser l'IA et les moteurs et opérateurs essentiels ; qualifier et recouper des sources ; tenir un journal de recherche ; formuler une conclusion prudente et exploitable ; respecter le cadre légal, la confidentialité et l'OPSEC.

MÉTHODES PÉDAGOGIQUES

Alternance d'apports courts, démonstrations en direct, exercices progressifs, études de situations, travail en binôme et cas fil rouge. Répartition indicative : 40 % d'apports méthodologiques et 60 % de pratique.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; moteurs et outils web accessibles ; trames de plan et journal de recherche ; fiches de qualification des sources ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté en OSINT, recherche web et investigations économiques ou numériques, disposant d'une pratique de la formation d'adultes et maîtrisant les enjeux juridiques, éthiques et d'OPSEC liés aux sources ouvertes.

AC-OSINT-201 · Fondamentaux opérationnels de l'OSINT

OSINT / INVESTIGATION

0 · Accueil et positionnement - 0 h 30

OBJECTIF — Identifier le niveau initial et les attentes.
CONTENUS — Présentation, tour de table, règles de travail, questionnaire diagnostic.
MÉTHODES / ACTIVITÉS — Échanges guidés et questionnaire individuel.
ÉVALUATION / PREUVE — Questionnaire initial conservé.

1 · Comprendre l'OSINT - 0 h 45

OBJECTIF — Distinguer l'OSINT d'une simple recherche web.
CONTENUS — Donnée, information, renseignement, preuve ; usages ; WEBINT, SOCMINT, IMINT, GEOINT.
MÉTHODES / ACTIVITÉS — Apport illustré et classement de cas d'usage.
ÉVALUATION / PREUVE — Correction collective argumentée.

2 · Limites et difficultés - 0 h 45

OBJECTIF — Identifier les obstacles affectant une investigation.
CONTENUS — Surabondance, non-indexation, obsolescence, homonymie, contenus trompeurs, limites linguistiques et techniques.
MÉTHODES / ACTIVITÉS — Analyse d'un dossier comportant plusieurs obstacles.
ÉVALUATION / PREUVE — 3 limites et une adaptation pour chacune.

3 · Cadre juridique et éthique - 1 h 00

OBJECTIF — Repérer les pratiques licites, sensibles ou à proscrire.
CONTENUS — Données publiques, RGPD, finalité, minimisation, accès frauduleux, droit d'auteur, conservation et diffusion.
MÉTHODES / ACTIVITÉS — Étude de situations et grille de décision.
ÉVALUATION / PREUVE — Justification du classement.

OSINT / INVESTIGATION

4 · OPSEC proportionnée - 1 h 00

OBJECTIF — Choisir des mesures de protection adaptées.
CONTENUS — Empreinte numérique, cloisonnement, comptes, VPN, téléchargements, métadonnées, stockage.
MÉTHODES / ACTIVITÉS — Mini-matrice risques / impacts / mesures.
ÉVALUATION / PREUVE — 3 mesures adaptées et justifiées.

5 · Méthodologie - Plan de recherche - Cadrer le besoin et élaborer la sémantique - 1 h 00

OBJECTIF — Transformer une demande vague en questions de recherche et en adapter le vocabulaire de recherche.
CONTENUS — Décision à éclairer, périmètre, temporalité, exclusions, livrable, critères d'arrêt.
MÉTHODES / ACTIVITÉS — Reformulation d'une demande fictive.
ÉVALUATION / PREUVE — Grille de cadrage complétée.

6 · Méthodologie - Plan de recherche - Identifier et qualifier les sources - 1 h 00

OBJECTIF — Sélectionner les familles de sources adaptées.
CONTENUS — Sources officielles, entreprises, presse, réseaux sociaux, archives, open data, documents techniques.
MÉTHODES / ACTIVITÉS — Association besoins / sources et analyse de fiabilité.
ÉVALUATION / PREUVE — Choix de sources complémentaires justifié.

7 · Méthodologie - Plan de recherche - Tracer et recouper les recherches - 0 h 45

OBJECTIF — Tenir un journal de recherche vérifiable.
CONTENUS — Requête, moteur, date, URL, extrait, fiabilité, statut, archivage et nommage.
MÉTHODES / ACTIVITÉS — Compléter un journal à partir d'une démonstration.
ÉVALUATION / PREUVE — Contrôle des champs indispensables.

OSINT / INVESTIGATION

8 · Évaluation intermédiaire - 0 h 15

OBJECTIF — Vérifier les acquis du jour 1.
CONTENUS — Quiz et reprise des difficultés.
MÉTHODES / ACTIVITÉS — Quiz individuel et correction commentée.
ÉVALUATION / PREUVE — Résultats et ajustement du jour 2.

9 · Comprendre les moteurs et l'IA - 1 h 15

OBJECTIF — Comprendre les limites de l'indexation.
CONTENUS — Exploration, indexation, classement, requête, affichage, personnalisation, moteurs alternatifs.
MÉTHODES / ACTIVITÉS — Comparaison d'une requête sur plusieurs moteurs.
ÉVALUATION / PREUVE — Explication de l'absence de résultat.

10 · Opérateurs essentiels - 0 h 45

OBJECTIF — Construire des requêtes avancées adaptées.
CONTENUS — Guillemets, OR, exclusion, parenthèses, site:, filetype:, intitle:, inurl:, recherche temporelle.
MÉTHODES / ACTIVITÉS — Exercices progressifs et démonstrations.
ÉVALUATION / PREUVE — 3 requêtes fonctionnelles et justifiées.

11 · Les prompts IA - 0 h 45

OBJECTIF — Développer les variantes utiles à une recherche.
CONTENUS — Synonymes, acronymes, noms antérieurs, translittérations, vocabulaire métier, exclusions, multilingue.
MÉTHODES / ACTIVITÉS — Atelier sur une entité fictive.
ÉVALUATION / PREUVE — Lexique couvrant 5 catégories.

OSINT / INVESTIGATION

12 · Poursuite du plan de recherche - 1 h 00

OBJECTIF — Organiser la collecte avant exécution.
CONTENUS — Axes, sous-questions, lexique, requêtes, sources, langues, formats, priorités, obstacles, critères d'arrêt.
MÉTHODES / ACTIVITÉS — Production en binôme sur le cas fil rouge.
ÉVALUATION / PREUVE — Grille de qualité du plan.

13 · IA comme assistant - 0 h 45

OBJECTIF — Utiliser l'IA sans lui déléguer la vérification.
CONTENUS — Lexique, traduction, structuration, extraction ; hallucinations, biais, confidentialité, contrôle humain.
MÉTHODES / ACTIVITÉS — Comparaison travail manuel / enrichi par IA.
ÉVALUATION / PREUVE — Apports et erreurs identifiés.

14 · Qualifier et recouper - 1 h 00

OBJECTIF — Évaluer une information avant restitution.
CONTENUS — Fait, affirmation, opinion, hypothèse, corroboration, date, indépendance, contradictions, niveau de confiance.
MÉTHODES / ACTIVITÉS — Analyse de contenus contradictoires.
ÉVALUATION / PREUVE — Fiche de qualification complétée.

15 · Cas pratique final - 1 h 30

OBJECTIF — Conduire une recherche simple de bout en bout.
CONTENUS — Cadrage, OPSEC, plan, requêtes, collecte, journalisation, qualification et synthèse.
MÉTHODES / ACTIVITÉS — Mise en situation en binôme ou petit groupe.
ÉVALUATION / PREUVE — Plan, journal et note courte évalués.

OSINT / INVESTIGATION

16 · Restitution et bilan - intégrée au cas final

OBJECTIF — Présenter les résultats et mesurer les acquis.
CONTENUS — Restitution orale, questions, quiz final, autoévaluation et satisfaction.
MÉTHODES / ACTIVITÉS — Présentation et retour méthodologique.
ÉVALUATION / PREUVE — Quiz final et grille du cas pratique.

AC-OSINT-201 · Fondamentaux opérationnels de l'OSINT

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire de positionnement et test diagnostic de 10 questions avant la formation ; recueil des attentes en début de session.

ÉVALUATIONS FORMATIVES

Exercices corrigés à chaque séquence, quiz intermédiaire, observation des productions, questions orales et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et exercices suivants.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique évalué sur 9 critères : cadrage, méthode, requêtes, diversité des sources, traçabilité, qualification, prudence analytique, restitution, légalité/OPSEC. Réussite considérée : au moins 70 % au quiz final et 6 critères sur 9 validés, dont obligatoirement cadrage, traçabilité, qualification des sources et respect du cadre juridique/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; trame de plan de recherche

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Due diligence en sources ouvertes

FINALITÉ PROFESSIONNELLE

Réaliser une due diligence structurée sur une personne morale et ses dirigeants.

PUBLIC VISÉ

Juristes, compliance, acheteurs, investisseurs, consultants, sûreté, directions commerciales.

PRÉREQUIS

Fondamentaux de recherche web; connaissance générale de l'entreprise.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

DURÉE

2 jours - 14 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / classe virtuelle / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-DD-201 · Due diligence en sources ouvertes

DUE DILIGENCE / IE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Cadrer une mission de due diligence en fonction de la décision à éclairer et des risques recherchés.
- Identifier précisément une personne morale, ses dirigeants, bénéficiaires, filiales et principales implantations.
- Rechercher les principaux signaux de risque juridiques, réputationnels, réglementaires, financiers et de conformité.
- Vérifier la cohérence entre déclarations publiques, activité économique, présence numérique et données officielles disponibles.
- Recouper les informations issues de plusieurs catégories de sources et distinguer faits, signaux faibles et hypothèses.
- Hiérarchiser les principaux risques selon leur importance et leur niveau de confiance.
- Produire une note de due diligence structurée comportant constats, sources, limites et recommandations de vérification.

COMPÉTENCES VISÉES

Cadrer la mission ; identifier les entités et dirigeants ; analyser réputation, conformité et risques ; produire une note.

MÉTHODES PÉDAGOGIQUES

Démonstrations, recherche guidée, cas pratique en groupe. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-DD-201 · Due diligence en sources ouvertes

DUE DILIGENCE / IE

0 · Accueil et positionnement - 0 h 30

OBJECTIF — Vérifier les acquis et attentes.
CONTENUS — Questionnaire, besoins métiers, cas d'usage.
MÉTHODES / ACTIVITÉS — Diagnostic.
ÉVALUATION / PREUVE — Positionnement conservé.

1 · Cadrer une due diligence - 1 h 00

OBJECTIF — Définir décision, périmètre et risques.
CONTENUS — OFR, profondeur, pays, période, sujets exclus, livrable.
MÉTHODES / ACTIVITÉS — Atelier de cadrage.
ÉVALUATION / PREUVE — Fiche validée.

2 · Identifier l'entité et ses actifs - 1 h 30

OBJECTIF — Vérifier identité, activité et implantations.
CONTENUS — Registres, statuts, établissements, sites, domaines, cohérence opérationnelle.
MÉTHODES / ACTIVITÉS — Démonstration et recherche.
ÉVALUATION / PREUVE — Tableau d'identité sourcé.

3 · Cartographier gouvernance et contrôle - 1 h 30

OBJECTIF — Identifier dirigeants, bénéficiaires et participations.
CONTENUS — Mandats, actionnariat, filiales, changements, liens capitalistiques.
MÉTHODES / ACTIVITÉS — Travail en binôme.
ÉVALUATION / PREUVE — Cartographie justifiée.

AC-DD-201 · Due diligence en sources ouvertes

DUE DILIGENCE / IE

4 · Sanctions, conformité et contentieux - 1 h 30

OBJECTIF — Rechercher les risques juridiques et réglementaires.
CONTENUS — Sanctions, PEP selon contexte, décisions, procédures, marchés publics.
MÉTHODES / ACTIVITÉS — Cas guidé.
ÉVALUATION / PREUVE — Signaux datés et qualifiés.

5 · Réputation et environnement relationnel - 1 h 30

OBJECTIF — Analyser controverses et réseaux.
CONTENUS — Presse, partenaires, dirigeants, associations, influence, biais.
MÉTHODES / ACTIVITÉS — Recherche multicanal.
ÉVALUATION / PREUVE — Chronologie et sources.

6 · Analyse financière orientée risque - 1 h 30

OBJECTIF — Repérer fragilités et incohérences.
CONTENUS — Bilan, résultat, ratios simples, tendances, cohérence activité/effectifs.
MÉTHODES / ACTIVITÉS — Lecture de comptes.
ÉVALUATION / PREUVE — Constats prudents.

7 · Cotation et niveau de confiance - 1 h 00

OBJECTIF — Hiérarchiser les risques.
CONTENUS — Probabilité, impact, matérialité, fiabilité, lacunes.
MÉTHODES / ACTIVITÉS — Matrice de cotation.
ÉVALUATION / PREUVE — Cotation argumentée.

DUE DILIGENCE / IE

8 · Cas pratique final et restitution - 3 h 00

OBJECTIF — Produire une note de due diligence.
CONTENUS — Plan de recherche, collecte, analyse, synthèse, recommandations, limites.
MÉTHODES / ACTIVITÉS — Mise en situation en groupe.
ÉVALUATION / PREUVE — Rapport court + oral + quiz.

AC-DD-201 · Due diligence en sources ouvertes

DUE DILIGENCE / IE

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Rapport court de due diligence avec cotation argumentée. Réussite proposée : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique, dont obligatoirement la traçabilité, la qualification des sources et le respect du cadre légal/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Investigation avancée sur les réseaux sociaux

FINALITÉ PROFESSIONNELLE

Conduire une investigation multiréseaux sur une identité, une organisation ou une campagne.

PUBLIC VISÉ

Analystes, enquêteurs, sûreté, communication, institutions publiques.

PRÉREQUIS

Maîtrise des fondamentaux OSINT ou expérience équivalente.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

DURÉE

2 jours - 14 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel recommandé.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-SOC-201 · Investigation avancée sur les réseaux sociaux

SOCMINT

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Élaborer une stratégie de recherche multiréseaux adaptée à une identité, une organisation ou un sujet donné.
- Corréler des pseudonymes, identifiants, contenus et traces publiques entre plusieurs plateformes.
- Reconstituer une chronologie d'activité et identifier les principaux changements de comportement ou événements associés.
- Cartographier des interactions, relais, communautés ou relations visibles entre comptes.
- Repérer des comportements atypiques, coordonnés ou potentiellement inauthentiques à partir d'indices observables.
- Vérifier les hypothèses d'identité ou d'appartenance par recoupement de sources indépendantes.
- Documenter l'investigation de façon traçable et produire un dossier SOCMINT argumenté.

COMPÉTENCES VISÉES

Corréler des identités ; cartographier des relations ; analyser comportements et chronologies ; documenter les résultats.

MÉTHODES PÉDAGOGIQUES

Ateliers pratiques, cas fil rouge, restitution collective. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

SOCMINT

0 · Accueil et diagnostic - 0 h 30

OBJECTIF — Évaluer la maîtrise SOCMINT.
CONTENUS — Plateformes, usages, contraintes.
MÉTHODES / ACTIVITÉS — Questionnaire.
ÉVALUATION / PREUVE — Diagnostic.

1 · Cadre, OPSEC et plan de collecte - 1 h 00

OBJECTIF — Préparer une investigation multiréseaux.
CONTENUS — Légalité, cloisonnement, objectifs, journal, critères d'arrêt.
MÉTHODES / ACTIVITÉS — Atelier plan.
ÉVALUATION / PREUVE — Plan validé.

2 · Corrélation d'identités - 1 h 30

OBJECTIF — Relier pseudonymes et comptes avec prudence.
CONTENUS — Identifiants, avatars, biographies, URLs, réutilisation, niveau de confiance.
MÉTHODES / ACTIVITÉS — Exercices de pivots.
ÉVALUATION / PREUVE — Corrélations documentées.

3 · Recherche approfondie par plateforme - 2 h 00

OBJECTIF — Exploiter les fonctions et recherches indirectes.
CONTENUS — X, LinkedIn, Meta, Reddit, YouTube, Telegram, moteurs externes.
MÉTHODES / ACTIVITÉS — Démonstrations et défis.
ÉVALUATION / PREUVE — Résultats sourcés.

SOCMINT

4 · Chronologie et comportement - 1 h 30

OBJECTIF — Analyser activité et évolutions.
CONTENUS — Création, rythme, horaires, suppressions, changements, interactions.
MÉTHODES / ACTIVITÉS — Atelier chronologique.
ÉVALUATION / PREUVE — Chronologie argumentée.

5 · Réseaux et communautés - 1 h 30

OBJECTIF — Cartographier des relations observables.
CONTENUS — Mentions, partages, communautés, centralités simples, limites.
MÉTHODES / ACTIVITÉS — Cartographie manuelle ou outil.
ÉVALUATION / PREUVE — Liens justifiés.

6 · Archivage et qualification - 1 h 00

OBJECTIF — Conserver et qualifier les preuves.
CONTENUS — Captures, URLs, contexte, horodatage, fiabilité, contradictions.
MÉTHODES / ACTIVITÉS — Journal et grille.
ÉVALUATION / PREUVE — Traçabilité complète.

7 · Cas pratique multiréseaux - 3 h 00

OBJECTIF — Conduire une investigation de bout en bout.
CONTENUS — Identité, contenus, réseau, chronologie, hypothèses, limites.
MÉTHODES / ACTIVITÉS — Travail en groupe.
ÉVALUATION / PREUVE — Dossier + présentation.

SOCMINT

8 · Évaluation finale et bilan - 2 h 00

OBJECTIF — Mesurer les acquis et consolider.
CONTENUS — Restitutions, questions, quiz, retour méthodologique.
MÉTHODES / ACTIVITÉS — Oral et quiz.
ÉVALUATION / PREUVE — Grille de compétences.

AC-SOC-201 · Investigation avancée sur les réseaux sociaux

SOCMINT

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Dossier multiréseaux et cartographie commentée. Réussite proposée : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique, dont obligatoirement la traçabilité, la qualification des sources et le respect du cadre légal/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Détecter une opération informationnelle coordonnée

FINALITÉ PROFESSIONNELLE

Distinguer une controverse organique d'une opération artificiellement structurée.

PUBLIC VISÉ

Cellules de veille, communication stratégique, analystes, institutions publiques, sûreté.

PRÉREQUIS

Fondamentaux OSINT recommandés.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

DURÉE

2 jours - 14 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel recommandé / classe virtuelle.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-FIMI-201 · Détecter une opération informationnelle coordonnée

MENACES INFORMATIONNELLES

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Définir le périmètre d'analyse d'une campagne informationnelle à partir d'un signal initial.
- Identifier et structurer les principaux narratifs, cibles, contenus et temporalités d'une campagne.
- Reconstituer une chaîne de diffusion depuis la primo-diffusion jusqu'aux phases d'amplification et de reprise.
- Repérer des marqueurs de coordination, d'inauthenticité ou d'automatisation parmi les comptes et relais observés.
- Identifier et relier les principaux actifs numériques ou infrastructures associés à la campagne.
- Décrire les tactiques, techniques et procédures observées en distinguant faits, indices et hypothèses.
- Produire une note de caractérisation argumentée assortie d'un niveau de confiance et de limites explicites.

COMPÉTENCES VISÉES

Analyser narratifs et cibles ; détecter coordination et inauthenticité ; relier comptes et infrastructures ; qualifier les hypothèses.

MÉTHODES PÉDAGOGIQUES

Études de cas inspirées de rapports publics, travaux en groupe. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

MENACES INFORMATIONNELLES

0 · Accueil et diagnostic - 0 h 30

OBJECTIF — Évaluer les acquis.
CONTENUS — Concepts, usages, attentes.
MÉTHODES / ACTIVITÉS — Quiz.
ÉVALUATION / PREUVE — Positionnement.

1 · Cadre d'analyse d'une opération - 1 h 00

OBJECTIF — Structurer l'analyse sans présumer l'attribution.
CONTENUS — Objectifs, cible, narratif, actifs, comportements, contexte, confiance.
MÉTHODES / ACTIVITÉS — Étude guidée.
ÉVALUATION / PREUVE — Grille complétée.

2 · Analyse narrative et victimologie - 1 h 30

OBJECTIF — Identifier récits, cibles et ressorts.
CONTENUS — Thèmes, émotions, opportunités, contenus fabriqués, adaptation locale.
MÉTHODES / ACTIVITÉS — Analyse de corpus.
ÉVALUATION / PREUVE — Cartographie narrative.

3 · Primo-diffusion et blanchiment - 1 h 30

OBJECTIF — Reconstituer la chaîne initiale.
CONTENUS — Comptes jetables, tiers rémunérés, médias, faux lanceurs d'alerte, CopyCop-like.
MÉTHODES / ACTIVITÉS — Chronologie de diffusion.
ÉVALUATION / PREUVE — Chaîne sourcée.

MENACES INFORMATIONNELLES

4 · Coordination et amplification - 1 h 30

OBJECTIF — Repérer des comportements inauthentiques.
CONTENUS — Répétition, temporalité, automatisation, comptes, hashtags, multi-plateformes.
MÉTHODES / ACTIVITÉS — Analyse comparative.
ÉVALUATION / PREUVE — Marqueurs qualifiés.

5 · Infrastructures numériques - 1 h 30

OBJECTIF — Relier domaines, sites et comptes.
CONTENUS — WHOIS, DNS, certificats, hébergement, métadonnées, CMS, erreurs opérateur.
MÉTHODES / ACTIVITÉS — Atelier technique non intrusif.
ÉVALUATION / PREUVE — Tableau d'actifs.

6 · TTP et caractérisation - 1 h 00

OBJECTIF — Décrire un mode opératoire.
CONTENUS — Tactiques, techniques, procédures, récurrences, IMS/MOI, niveau de confiance.
MÉTHODES / ACTIVITÉS — Matrice TTP.
ÉVALUATION / PREUVE — Caractérisation prudente.

7 · Mesures d'atténuation et alerte - 1 h 00

OBJECTIF — Proposer une réponse adaptée.
CONTENUS — Signalement, documentation, communication, plateformes, coordination.
MÉTHODES / ACTIVITÉS — Atelier plan d'action.
ÉVALUATION / PREUVE — Mesures priorisées.

MENACES INFORMATIONNELLES

8 · Cas pratique final - 3 h 00

OBJECTIF — Caractériser une opération simulée.
CONTENUS — Narratifs, diffusion, actifs, comportements, attribution limitée, impact.
MÉTHODES / ACTIVITÉS — Investigation en équipe.
ÉVALUATION / PREUVE — Note + briefing.

9 · Évaluation et bilan - 1 h 30

OBJECTIF — Vérifier les acquis.
CONTENUS — Quiz, soutenance, retour.
MÉTHODES / ACTIVITÉS — Évaluation individuelle et collective.
ÉVALUATION / PREUVE — Grille finale.

AC-FIMI-201 · Détecter une opération informationnelle coordonnée

MENACES INFORMATIONNELLES

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique final, note et briefing évalués sur la caractérisation des TTP, la prudence analytique, la qualité des mesures d'atténuation et la restitution. Réussite : validation d'au moins 70 % des critères de la grille finale.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Grille de caractérisation et chronologie-type.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

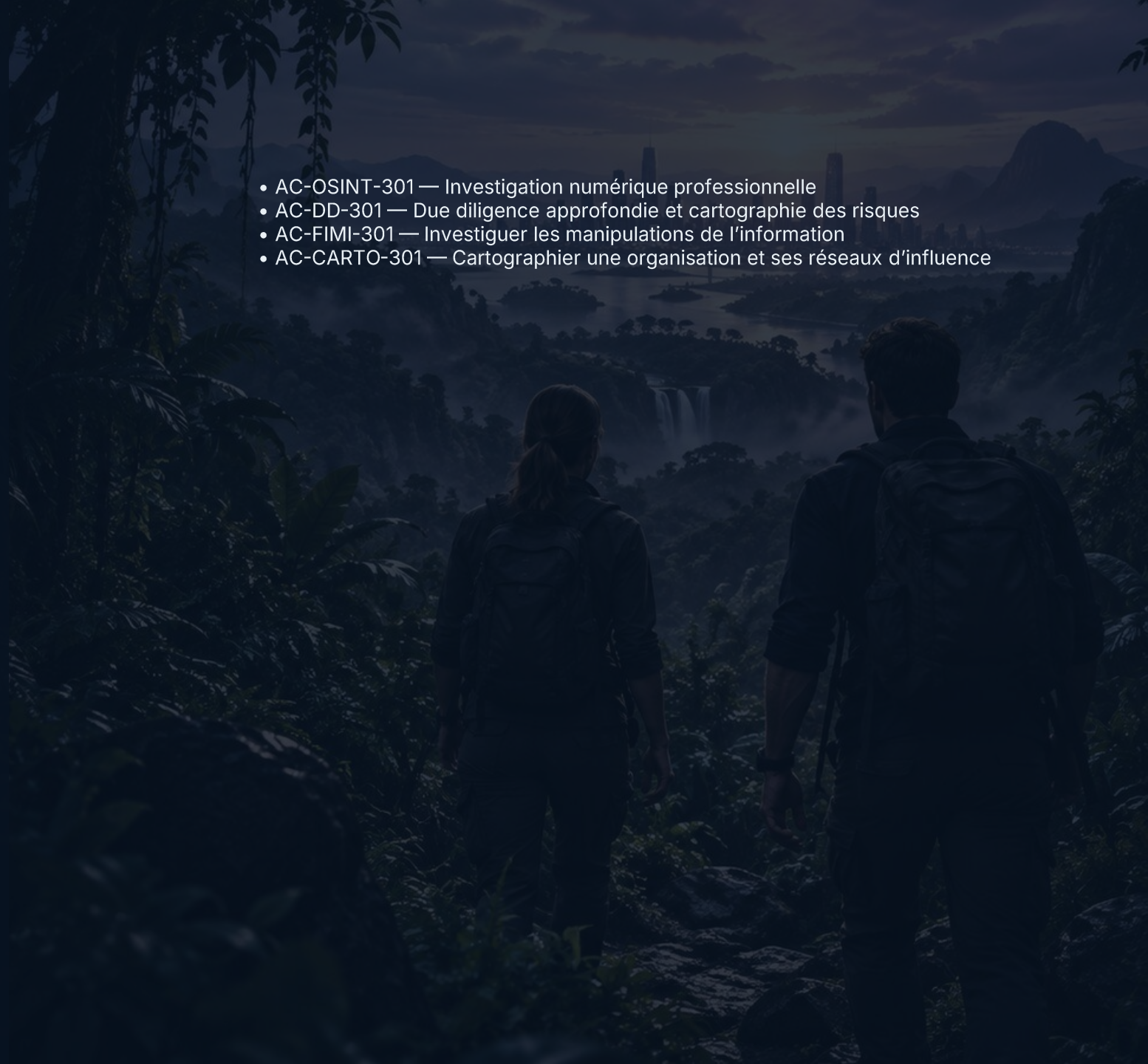
Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Affinis Campus

3 JOURS

4 formations

Approfondir une pratique et multiplier les mises en situation.



- AC-OSINT-301 — Investigation numérique professionnelle
- AC-DD-301 — Due diligence approfondie et cartographie des risques
- AC-FIMI-301 — Investiguer les manipulations de l'information
- AC-CARTO-301 — Cartographier une organisation et ses réseaux d'influence

Investigation numérique professionnelle

FINALITÉ PROFESSIONNELLE

Conduire une investigation numérique diversifiée et restituer un renseignement exploitable.

PUBLIC VISÉ

Analystes, consultants, enquêteurs, fonctions sûreté, intelligence économique et institutions.

PRÉREQUIS

Pratique régulière de la recherche web.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

DURÉE

3 jours - 21 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-301 · Investigation numérique professionnelle

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Cadrer une investigation numérique complexe à partir d'un besoin professionnel et d'hypothèses initiales.
- Construire un plan de collecte multi-sources intégrant recherche web, sources institutionnelles, SOCMINT, IMINT et infrastructures numériques.
- Mettre en œuvre des mesures juridiques, éthiques et d'OPSEC adaptées au niveau de sensibilité de la mission.
- Collecter, journaliser et qualifier des informations issues de plusieurs environnements numériques.
- Corréler des identités, organisations, contenus, domaines ou autres entités à partir d'indices convergents.
- Recouper les informations, gérer les contradictions et attribuer un niveau de confiance aux conclusions.
- Produire une restitution professionnelle comprenant synthèse, éléments probants, limites et axes de recherche complémentaires.

COMPÉTENCES VISÉES

Planifier la collecte ; exploiter sources web, sociales, visuelles et techniques ; analyser ; rédiger et présenter.

MÉTHODES PÉDAGOGIQUES

Cas fil rouge, ateliers, simulations de briefing. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

OSINT / INVESTIGATION

0 · Positionnement et cadre - 0 h 30

OBJECTIF — Adapter la formation aux profils.
CONTENUS — Diagnostic, attentes, règles.
MÉTHODES / ACTIVITÉS — Questionnaire.
ÉVALUATION / PREUVE — Positionnement.

1 · Méthode, droit et OPSEC - 2 h 00

OBJECTIF — Préparer une investigation professionnelle.
CONTENUS — Cycle, cadrage, légalité, éthique, risques, cloisonnement.
MÉTHODES / ACTIVITÉS — Cas et atelier.
ÉVALUATION / PREUVE — Plan initial.

2 · Moteurs, lexique et requêtes - 2 h 30

OBJECTIF — Construire une stratégie de recherche avancée.
CONTENUS — Sémantique, moteurs, opérateurs, archives, multilingue.
MÉTHODES / ACTIVITÉS — Exercices progressifs.
ÉVALUATION / PREUVE — Défis validés.

3 · Sources, traçabilité et qualification - 2 h 00

OBJECTIF — Collecter des données fiables et reproductibles.
CONTENUS — Typologie, journal, archivage, recoupement, confiance.
MÉTHODES / ACTIVITÉS — Atelier corpus.
ÉVALUATION / PREUVE — Journal contrôlé.

OSINT / INVESTIGATION

4 · Personnes et identités numériques - 2 h 00

OBJECTIF — Rechercher une personne dans un cadre proportionné.
CONTENUS — Homonymes, pseudonymes, parcours, présence publique, limites RGPD.
MÉTHODES / ACTIVITÉS — Cas fictif.
ÉVALUATION / PREUVE — Fiche identité prudente.

5 · Entreprises et écosystèmes - 2 h 30

OBJECTIF — Analyser une organisation et ses liens.
CONTENUS — Registres, dirigeants, filiales, domaines, partenaires, réputation.
MÉTHODES / ACTIVITÉS — Investigation guidée.
ÉVALUATION / PREUVE — Cartographie sourcée.

6 · SOCMINT - 2 h 00

OBJECTIF — Exploiter les réseaux sociaux publics.
CONTENUS — Pivots, contenus, chronologies, interactions, archivage.
MÉTHODES / ACTIVITÉS — Atelier multiréseaux.
ÉVALUATION / PREUVE — Dossier SOCMINT.

7 · IMINT et GEOINT - 2 h 00

OBJECTIF — Vérifier un contenu et un lieu.
CONTENUS — Recherche inversée, métadonnées, géolocalisation, chronolocalisation.
MÉTHODES / ACTIVITÉS — Mini-enquête.
ÉVALUATION / PREUVE — Note de vérification.

OSINT / INVESTIGATION

8 · Infrastructures web - 1 h 30

OBJECTIF — Identifier des actifs numériques associés.
CONTENUS — Domaines, DNS, certificats, archives, technologies, limites.
MÉTHODES / ACTIVITÉS — Atelier technique.
ÉVALUATION / PREUVE — Tableau d'actifs.

9 · Analyse et rédaction - 2 h 00

OBJECTIF — Transformer la collecte en renseignement.
CONTENUS — Faits, hypothèses, lacunes, niveaux de confiance, structure d'une note.
MÉTHODES / ACTIVITÉS — Atelier rédaction.
ÉVALUATION / PREUVE — Note intermédiaire.

10 · Cas final et soutenance - 2 h 00

OBJECTIF — Conduire une investigation complète.
CONTENUS — Cas fil rouge, livrables, oral.
MÉTHODES / ACTIVITÉS — Travail en groupe.
ÉVALUATION / PREUVE — Rapport + soutenance.

AC-OSINT-301 · Investigation numérique professionnelle

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Rapport d'investigation et soutenance individuelle ou en binôme. Réussite proposée : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique, dont obligatoirement la traçabilité, la qualification des sources et le respect du cadre légal/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Kit analyste OSINT.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Due diligence approfondie et cartographie des risques

FINALITÉ PROFESSIONNELLE

Évaluer de manière argumentée les risques liés à une entreprise, ses dirigeants et son environnement.

PUBLIC VISÉ

Consultants, juristes, compliance, investisseurs, directions achats, sûreté économique.

PRÉREQUIS

Fondamentaux OSINT; lecture générale des documents d'entreprise.

MODALITÉS DE POSITIONNEMENT

Questionnaire détaillé, test pratique et, lorsque nécessaire, entretien avec le référent pédagogique afin de vérifier la capacité à suivre les exercices avancés.

DURÉE

3 jours - 21 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-DD-301 · Due diligence approfondie et cartographie des risques

DUE DILIGENCE / IE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Définir un périmètre de due diligence approfondie en fonction des enjeux métier, géographiques et réglementaires.
- Reconstituer la structure juridique, capitalistique et opérationnelle d'une entreprise et de son environnement.
- Analyser les dirigeants, bénéficiaires, sociétés liées et réseaux professionnels afin d'identifier conflits, dépendances ou risques potentiels.
- Rechercher et qualifier les risques juridiques, réputationnels, réglementaires, éthiques et de conformité.
- Lire et interpréter les principaux états financiers et ratios utiles à l'identification de signaux faibles ou d'anomalies.
- Croiser les données financières avec les informations OSINT relatives aux activités, actifs, implantations et partenaires.
- Coter et hiérarchiser les risques selon leur gravité, leur vraisemblance et le niveau de confiance disponible.
- Produire un rapport de due diligence approfondie assorti de recommandations exploitables pour la décision.

COMPÉTENCES VISÉES

Analyser structure, gouvernance, réputation, conformité, finances et réseaux ; hiérarchiser les risques.

MÉTHODES PÉDAGOGIQUES

Ateliers, analyse documentaire, étude de cas réelle ou fictive. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-DD-301 · Due diligence approfondie et cartographie des risques

DUE DILIGENCE / IE

0 · Positionnement - 0 h 30

OBJECTIF — Identifier les acquis.
CONTENUS — Diagnostic métier et méthode.
MÉTHODES / ACTIVITÉS — Questionnaire.
ÉVALUATION / PREUVE — Positionnement.

1 · Cadrage et stratégie de collecte - 2 h 00

OBJECTIF — Définir le périmètre d'une due diligence approfondie.
CONTENUS — OFR, risques, pays, sources, limites, livrable.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Plan de recherche.

2 · Identité, gouvernance et actionnariat - 3 h 00

OBJECTIF — Reconstituer le contrôle et les changements.
CONTENUS — Registres, statuts, bénéficiaires, mandats, filiales, historiques.
MÉTHODES / ACTIVITÉS — Investigation guidée.
ÉVALUATION / PREUVE — Cartographie.

3 · Activités, actifs et implantations - 2 h 00

OBJECTIF — Vérifier la réalité opérationnelle.
CONTENUS — Établissements, production, sites, brevets, marchés, fournisseurs, GEOINT simple.
MÉTHODES / ACTIVITÉS — Cas pratique.
ÉVALUATION / PREUVE — Tableau de cohérence.

AC-DD-301 · Due diligence approfondie et cartographie des risques

DUE DILIGENCE / IE

4 · Dirigeants et réseaux - 2 h 00

OBJECTIF — Analyser parcours et relations pertinentes.
CONTENUS — Mandats, sociétés liées, réseaux professionnels, conflits potentiels.
MÉTHODES / ACTIVITÉS — Recherche multicanal.
ÉVALUATION / PREUVE — Fiches dirigeants.

5 · Conformité, sanctions et contentieux - 2 h 30

OBJECTIF — Identifier les risques juridiques et éthiques.
CONTENUS — Sanctions, PEP selon contexte, décisions, enquêtes, controverses.
MÉTHODES / ACTIVITÉS — Atelier sources.
ÉVALUATION / PREUVE — Chronologie sourcée.

6 · Réputation et parties prenantes - 2 h 00

OBJECTIF — Évaluer les signaux réputationnels.
CONTENUS — Presse, ONG, clients, salariés, concurrents, biais et campagnes.
MÉTHODES / ACTIVITÉS — Analyse de corpus.
ÉVALUATION / PREUVE — Qualification des signaux.

7 · Analyse financière - 3 h 00

OBJECTIF — Interpréter les états et ratios utiles.
CONTENUS — Bilan, résultat, cash, endettement, FR/BFR, tendances, anomalies.
MÉTHODES / ACTIVITÉS — Étude chiffrée.
ÉVALUATION / PREUVE — Diagnostic financier.

AC-DD-301 · Due diligence approfondie et cartographie des risques

DUE DILIGENCE / IE

8 · Cotation et recommandations - 1 h 30

OBJECTIF — Hiérarchiser les risques.
CONTENUS — Probabilité, impact, confiance, matérialité, mesures complémentaires.
MÉTHODES / ACTIVITÉS — Matrice.
ÉVALUATION / PREUVE — Cotation argumentée.

9 · Cas final et soutenance - 2 h 30

OBJECTIF — Produire un rapport complet.
CONTENUS — Synthèse exécutive, constats, risques, limites, recommandations.
MÉTHODES / ACTIVITÉS — Travail en équipe.
ÉVALUATION / PREUVE — Rapport + oral.

AC-DD-301 · Due diligence approfondie et cartographie des risques

DUE DILIGENCE / IE

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Rapport final et soutenance évalués sur la qualité de la collecte, la qualification des risques, l'analyse financière, la traçabilité des sources et les recommandations. Réussite : validation d'au moins 70 % des critères de la grille du cas pratique.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Matrice de due diligence approfondie.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Investiguer les manipulations de l’information

FINALITÉ PROFESSIONNELLE

Conduire une investigation structurée sur une campagne de manipulation de l’information.

PUBLIC VISÉ

Analystes, institutions publiques, communication stratégique, sûreté, cabinets spécialisés.

PRÉREQUIS

Fondamentaux OSINT et SOCMINT.

MODALITÉS DE POSITIONNEMENT

Questionnaire détaillé, test pratique et, lorsque nécessaire, entretien avec le référent pédagogique afin de vérifier la capacité à suivre les exercices avancés.

DURÉE

3 jours - 21 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel recommandé.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D’ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-FIMI-301 · Investiguer les manipulations de l'information

MENACES INFORMATIONNELLES

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Construire une démarche d'investigation adaptée à une suspicion de manipulation informationnelle.
- Identifier et analyser les narratifs, cibles, formats et temporalités d'une opération informationnelle.
- Reconstituer les phases de diffusion et documenter les mécanismes de primo-diffusion, blanchiment, amplification et reprise.
- Analyser des comportements de comptes afin de repérer coordination, automatisation ou inauthenticité.
- Cartographier les principaux actifs numériques, relais et infrastructures associés à l'opération.
- Comparer les tactiques, techniques et procédures observées avec celles de campagnes documentées.
- Formuler des hypothèses d'implication ou d'attribution avec un niveau de confiance proportionné aux éléments disponibles.
- Rédiger une note d'investigation distinguant clairement faits, indices, hypothèses, limites et besoins de collecte complémentaires.

COMPÉTENCES VISÉES

Reconstituer une chaîne de diffusion ; analyser contenus et comportements ; identifier les infrastructures ; produire une appréciation prudente.

MÉTHODES PÉDAGOGIQUES

Études de cas, travaux de groupe, exercices de cartographie. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-FIMI-301 · Investiguer les manipulations de l'information

MENACES INFORMATIONNELLES

0 · Positionnement - 0 h 30

OBJECTIF — Évaluer les acquis.
CONTENUS — Quiz et attentes.
MÉTHODES / ACTIVITÉS — Diagnostic.
ÉVALUATION / PREUVE — Positionnement.

1 · Cadres conceptuels FIMI - 2 h 00

OBJECTIF — Maîtriser les concepts et niveaux d'analyse.
CONTENUS — INE, MOI, IMS, TTP, acteurs, intention, impact, confiance.
MÉTHODES / ACTIVITÉS — Apport et cas.
ÉVALUATION / PREUVE — Quiz.

2 · Narratifs, contenus et victimologie - 2 h 30

OBJECTIF — Analyser le contenu d'une campagne.
CONTENUS — Cibles, récits, opportunités, deepfakes, montages, contenus IA.
MÉTHODES / ACTIVITÉS — Corpus.
ÉVALUATION / PREUVE — Matrice narrative.

3 · Chaînes de diffusion - 2 h 00

OBJECTIF — Reconstituer la circulation d'un contenu.
CONTENUS — Primo-diffusion, blanchiment, amplification, reprises.
MÉTHODES / ACTIVITÉS — Chronologie.
ÉVALUATION / PREUVE — Schéma sourcé.

MENACES INFORMATIONNELLES

4 · Comptes et comportements - 2 h 30

OBJECTIF — Détecter coordination et inauthenticité.
CONTENUS — Comptes jetables, bots, synchronisation, répétition, réseaux.
MÉTHODES / ACTIVITÉS — Analyse de données simples.
ÉVALUATION / PREUVE — Marqueurs justifiés.

5 · Infrastructures et actifs - 2 h 30

OBJECTIF — Cartographier l’écosystème numérique.
CONTENUS — Domaines, DNS, certificats, hébergement, métadonnées, sites, comptes.
MÉTHODES / ACTIVITÉS — Atelier technique.
ÉVALUATION / PREUVE — Cartographie.

6 · Attribution prudente - 1 h 30

OBJECTIF — Distinguer implication, proximité et attribution.
CONTENUS — Hypothèses concurrentes, indices, biais, niveaux de confiance.
MÉTHODES / ACTIVITÉS — Étude contradictoire.
ÉVALUATION / PREUVE — Conclusion calibrée.

7 · Évaluation de l’impact - 1 h 30

OBJECTIF — Apprécier visibilité et effets sans surinterpréter.
CONTENUS — Audience, engagement, reprises, temporalité, limites de mesure.
MÉTHODES / ACTIVITÉS — Atelier métriques.
ÉVALUATION / PREUVE — Appréciation prudente.

MENACES INFORMATIONNELLES

8 · Réponse et coordination - 1 h 30

OBJECTIF — Proposer des mesures d’atténuation.
CONTENUS — Alerte, plateformes, communication, acteurs victimes, documentation.
MÉTHODES / ACTIVITÉS — Plan d’action.
ÉVALUATION / PREUVE — Mesures priorisées.

9 · Cas final et briefing - 4 h 00

OBJECTIF — Conduire une caractérisation complète.
CONTENUS — Investigation, note, annexes, briefing décisionnel.
MÉTHODES / ACTIVITÉS — Équipe.
ÉVALUATION / PREUVE — Rapport + soutenance.

AC-FIMI-301 · Investiguer les manipulations de l'information

MENACES INFORMATIONNELLES

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Rapport final et briefing évalués sur la caractérisation de la campagne, l'attribution prudente, l'évaluation de l'impact, la traçabilité et les recommandations. Réussite : validation d'au moins 70 % des critères de la grille du cas pratique.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Trame de rapport FIMI et matrice TTP.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Cartographier une organisation et ses réseaux d’influence

FINALITÉ PROFESSIONNELLE

Identifier les acteurs, relations, relais et communautés d’un écosystème.

PUBLIC VISÉ

Analystes, consultants, affaires publiques, sûreté, intelligence économique, institutions.

PRÉREQUIS

Fondamentaux OSINT; aisance avec les tableurs.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable, test pratique court et recueil d’un cas d’usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

DURÉE

3 jours - 21 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel recommandé.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D’ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-CARTO-301 · Cartographier une organisation et ses réseaux d’influence

CARTOGRAPHIE / RÉSEAUX

OBJECTIF GÉNÉRAL

À l’issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Définir le périmètre, les entités et les types de relations pertinents pour une cartographie de réseau.
- Identifier des acteurs, organisations, relais et communautés à partir de sources ouvertes diversifiées.
- Documenter et qualifier les liens entre entités en distinguant relation avérée, proximité, hypothèse et absence de preuve.
- Structurer les données relationnelles dans un format exploitable pour la cartographie.
- Construire une représentation graphique lisible d’un réseau d’acteurs ou d’influence.
- Identifier les acteurs centraux, intermédiaires, communautés et points de connexion remarquables.
- Interpréter la cartographie sans confondre proximité structurelle et causalité.
- Produire une restitution combinant visualisation, sources, analyse et limites méthodologiques.

COMPÉTENCES VISÉES

Collecter les entités et liens ; qualifier les relations ; construire une cartographie ; interpréter centralités et communautés.

MÉTHODES PÉDAGOGIQUES

Ateliers de collecte et de cartographie, cas fil rouge. Alternance d’apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d’analyse ; cas pratiques ; visioconférence et partage d’écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d’une pratique opérationnelle de l’OSINT et de la formation d’adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d’OPSEC associés.

AC-CARTO-301 · Cartographier une organisation et ses réseaux d’influence

CARTOGRAPHIE / RÉSEAUX

0 · Positionnement - 0 h 30

OBJECTIF — Identifier les acquis en cartographie.
CONTENUS — Usages, outils, attentes.
MÉTHODES / ACTIVITÉS — Questionnaire.
ÉVALUATION / PREUVE — Diagnostic.

1 · Cadrer une cartographie - 1 h 30

OBJECTIF — Définir objet, niveau et limites.
CONTENUS — Question décisionnelle, nœuds, liens, période, sources, biais.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Cahier de cadrage.

2 · Identifier les acteurs - 2 h 30

OBJECTIF — Constituer une liste d’entités pertinente.
CONTENUS — Personnes, organisations, médias, institutions, comptes, doublons.
MÉTHODES / ACTIVITÉS — Recherche guidée.
ÉVALUATION / PREUVE — Référentiel d’acteurs.

3 · Qualifier les relations - 2 h 00

OBJECTIF — Définir des liens observables et datés.
CONTENUS — Capital, mandat, financement, partenariat, interaction, citation, proximité.
MÉTHODES / ACTIVITÉS — Atelier taxonomie.
ÉVALUATION / PREUVE — Dictionnaire de liens.

CARTOGRAPHIE / RÉSEAUX

4 · Collecter et normaliser - 2 h 00

OBJECTIF — Structurer les données pour la cartographie.
CONTENUS — Identifiants, sources, dates, poids, confiance, nettoyage.
MÉTHODES / ACTIVITÉS — Tableur.
ÉVALUATION / PREUVE — Jeu de données propre.

5 · Construire la carte - 2 h 30

OBJECTIF — Produire une représentation lisible.
CONTENUS — Outils, import, disposition, couleurs, filtres, légende.
MÉTHODES / ACTIVITÉS — Atelier logiciel.
ÉVALUATION / PREUVE — Carte fonctionnelle.

6 · Analyser communautés et centralités - 2 h 00

OBJECTIF — Interpréter sans confondre visibilité et influence.
CONTENUS — Degré, intermédiaires, clusters, isolats, limites.
MÉTHODES / ACTIVITÉS — Analyse guidée.
ÉVALUATION / PREUVE — Constats argumentés.

7 · Cartographier les réseaux numériques - 2 h 00

OBJECTIF — Intégrer comptes, sites et contenus.
CONTENUS — Mentions, partages, liens web, co-publications, temporalité.
MÉTHODES / ACTIVITÉS — Cas SOCMINT.
ÉVALUATION / PREUVE — Sous-carte numérique.

CARTOGRAPHIE / RÉSEAUX

8 · Restitution et narration visuelle - 1 h 30

OBJECTIF — Présenter une carte exploitable.
CONTENUS — Titre, légende, sources, limites, annexes, messages clés.
MÉTHODES / ACTIVITÉS — Revue croisée.
ÉVALUATION / PREUVE — Carte améliorée.

9 · Cas final - 4 h 30

OBJECTIF — Produire une cartographie d’influence complète.
CONTENUS — Collecte, base, carte, analyse, note.
MÉTHODES / ACTIVITÉS — Travail en équipe.
ÉVALUATION / PREUVE — Livrables + oral.

AC-CARTO-301 · Cartographier une organisation et ses réseaux d'influence

CARTOGRAPHIE / RÉSEAUX

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas final évalué sur les livrables cartographiques et la restitution orale : qualité des relations documentées, lisibilité, traçabilité, prudence analytique et narration visuelle. Réussite : validation d'au moins 70 % des critères de la grille.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Matrice entités-relations et modèle de légende.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Affinis Campus

4 JOURS

2 formations

Professionnaliser les pratiques et conduire des cas complets.



- AC-OSINT-401 — Analyste OSINT : conduire une investigation de bout en bout
- AC-FIMI-401 — Analyste des menaces informationnelles numériques

Analyste OSINT : conduire une investigation de bout en bout

FINALITÉ PROFESSIONNELLE

Maîtriser la conduite complète d'une investigation numérique professionnelle.

PUBLIC VISÉ

Analystes, enquêteurs, consultants, cellules de veille et sûreté.

PRÉREQUIS

Expérience de recherche professionnelle ou module de fondamentaux.

MODALITÉS DE POSITIONNEMENT

Questionnaire détaillé, test pratique et, lorsque nécessaire, entretien avec le référent pédagogique afin de vérifier la capacité à suivre les exercices avancés.

DURÉE

4 jours - 28 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-401 · Analyste OSINT : conduire une investigation de bout en bout

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Cadrer une investigation OSINT de bout en bout en définissant objectifs, périmètre, risques, hypothèses et livrables.
- Concevoir un plan de collecte multi-sources hiérarchisé et adapté aux contraintes de la mission.
- Appliquer un dispositif juridique, éthique et d'OPSEC proportionné à une investigation sensible.
- Mobiliser de manière complémentaire recherche web avancée, sources entreprises, SOCMINT, IMINT, GEOINT et investigation d'infrastructures.
- Corréler et qualifier des informations hétérogènes en documentant leur provenance et leur niveau de confiance.
- Identifier les lacunes, contradictions et biais susceptibles d'affecter l'analyse.
- Produire un rapport analytique structuré avec annexes de preuves et recommandations.
- Présenter et défendre oralement les conclusions d'une investigation devant un commanditaire ou un jury.

COMPÉTENCES VISÉES

Cadrer ; sécuriser ; collecter multi-sources ; corréler ; analyser ; documenter ; rédiger et soutenir les conclusions.

MÉTHODES PÉDAGOGIQUES

Pédagogie par projet, cas complexe, accompagnement individualisé. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-OSINT-401 · Analyste OSINT : conduire une investigation de bout en bout

OSINT / INVESTIGATION

0 · Positionnement et cadrage - 0 h 30

OBJECTIF — Adapter le parcours.
CONTENUS — Test et cas d'usage.
MÉTHODES / ACTIVITÉS — Diagnostic.
ÉVALUATION / PREUVE — Positionnement.

1 · Cycle d'investigation, droit et OPSEC - 3 h 00

OBJECTIF — Préparer une mission complète.
CONTENUS — OFR, plan, légalité, risques, cloisonnement, gouvernance.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Dossier de cadrage.

2 · Recherche web avancée - 3 h 30

OBJECTIF — Maîtriser moteurs, sémantique et archives.
CONTENUS — Opérateurs, moteurs, multilingue, documents, archives.
MÉTHODES / ACTIVITÉS — Défis.
ÉVALUATION / PREUVE — Requêtes évaluées.

3 · Personnes et identités - 3 h 00

OBJECTIF — Conduire une recherche proportionnée.
CONTENUS — Identités, pseudonymes, parcours, réseaux, limites.
MÉTHODES / ACTIVITÉS — Cas.
ÉVALUATION / PREUVE — Fiche sourcée.

OSINT / INVESTIGATION

4 · Entreprises et due diligence - 4 h 00

OBJECTIF — Analyser une organisation.
CONTENUS — Registres, gouvernance, actifs, réputation, conformité, finance.
MÉTHODES / ACTIVITÉS — Investigation.
ÉVALUATION / PREUVE — Matrice de risques.

5 · SOCMINT et cartographie - 3 h 30

OBJECTIF — Analyser réseaux et comportements.
CONTENUS — Pivots, chronologie, interactions, communautés, cartographie.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Carte + analyse.

6 · IMINT, GEOINT et infrastructures - 3 h 30

OBJECTIF — Vérifier contenus et actifs numériques.
CONTENUS — Images, vidéos, lieux, domaines, DNS, certificats, archives.
MÉTHODES / ACTIVITÉS — Mini-enquêtes.
ÉVALUATION / PREUVE — Notes de vérification.

7 · Analyse, rédaction et contrôle qualité - 2 h 30

OBJECTIF — Produire une note robuste.
CONTENUS — Faits/hypothèses, confiance, contradictions, relecture, confidentialité.
MÉTHODES / ACTIVITÉS — Atelier rédaction.
ÉVALUATION / PREUVE — Note intermédiaire.

OSINT / INVESTIGATION

8 · Cas final intégral - 4 h 00

OBJECTIF — Conduire l'investigation de bout en bout.
CONTENUS — Plan, collecte, analyse, rapport, annexes.
MÉTHODES / ACTIVITÉS — Équipe.
ÉVALUATION / PREUVE — Rapport évalué.

9 · Soutenance et bilan - 1 h 30

OBJECTIF — Défendre les conclusions.
CONTENUS — Briefing, questions, quiz, retour.
MÉTHODES / ACTIVITÉS — Oral.
ÉVALUATION / PREUVE — Grille finale.

AC-OSINT-401 · Analyste OSINT : conduire une investigation de bout en bout

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas final intégral, rapport et soutenance évalués sur la méthode, la qualité de la collecte, la traçabilité, la qualification des sources, l'analyse et la restitution. Réussite : validation d'au moins 70 % des critères de la grille finale.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Kit complet d'investigation.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Analyste des menaces informationnelles numériques

FINALITÉ PROFESSIONNELLE

Détecter, caractériser et restituer une menace informationnelle numérique complexe.

PUBLIC VISÉ

Institutions publiques, cellules de veille, communication stratégique, sûreté, cabinets spécialisés.

PRÉREQUIS

Fondamentaux OSINT/SOCMINT; capacités d'analyse.

MODALITÉS DE POSITIONNEMENT

Questionnaire détaillé, test pratique et, lorsque nécessaire, entretien avec le référent pédagogique afin de vérifier la capacité à suivre les exercices avancés.

DURÉE

4 jours - 28 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel recommandé.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-FIMI-401 · Analyste des menaces informationnelles numériques

MENACES INFORMATIONNELLES

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Planifier une investigation portant sur une menace informationnelle numérique à partir d'un signal initial.
- Analyser les narratifs, contenus, cibles, victimologie et opportunités exploitées par une campagne.
- Reconstituer la diffusion d'un contenu et identifier les mécanismes de coordination, amplification et inauthenticité.
- Cartographier les comptes, sites, domaines, infrastructures et autres actifs numériques liés à l'opération.
- Identifier et comparer les tactiques, techniques et procédures afin de caractériser un mode opératoire informationnel.
- Évaluer la solidité d'indices d'implication, d'extranéité ou d'attribution en formulant des hypothèses concurrentes.
- Apprécier la portée et les limites d'une campagne sans confondre visibilité observée et impact réel.
- Produire un rapport technique et un briefing synthétique distinguant faits, analyses, niveaux de confiance et limites.

COMPÉTENCES VISÉES

Analyser contexte, narratifs, comportements et infrastructures ; formuler des hypothèses ; évaluer impact et confiance.

MÉTHODES PÉDAGOGIQUES

Études de cas, exercices techniques, simulation de cellule d'analyse. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

MENACES INFORMATIONNELLES

0 · Positionnement - 0 h 30

OBJECTIF — Évaluer les acquis.
CONTENUS — Quiz et attentes.
MÉTHODES / ACTIVITÉS — Diagnostic.
ÉVALUATION / PREUVE — Positionnement.

1 · Doctrine, concepts et cadre analytique - 3 h 00

OBJECTIF — Structurer l'analyse d'une menace informationnelle.
CONTENUS — FIMI, INE, MOI, IMS, TTP, critères, droit et éthique.
MÉTHODES / ACTIVITÉS — Apport et cas.
ÉVALUATION / PREUVE — Quiz.

2 · Narratifs, contenus et cibles - 3 h 00

OBJECTIF — Analyser la dimension cognitive et contextuelle.
CONTENUS — Victimologie, récits, émotions, deepfakes, contenus IA.
MÉTHODES / ACTIVITÉS — Corpus.
ÉVALUATION / PREUVE — Matrice.

3 · Diffusion, blanchiment et amplification - 3 h 30

OBJECTIF — Reconstituer le schéma opérationnel.
CONTENUS — Primo-diffusion, médias tiers, réseaux, reprises, automatisation.
MÉTHODES / ACTIVITÉS — Chronologie.
ÉVALUATION / PREUVE — Chaîne sourcée.

MENACES INFORMATIONNELLES

4 · Comptes, comportements et réseaux - 3 h 30

OBJECTIF — Détecter coordination et inauthenticité.
CONTENUS — Marqueurs, temporalité, synchronisation, clusters, multi-plateformes.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Analyse comportementale.

5 · Infrastructures techniques - 3 h 30

OBJECTIF — Cartographier les actifs.
CONTENUS — Domaines, IP, DNS, SSL, métadonnées, CMS, erreurs, liens.
MÉTHODES / ACTIVITÉS — Atelier technique.
ÉVALUATION / PREUVE — Carte d'actifs.

6 · TTP, attribution et confiance - 3 h 00

OBJECTIF — Formuler des hypothèses prudentes.
CONTENUS — TTP, récurrences, hypothèses concurrentes, marqueurs d'extranéité.
MÉTHODES / ACTIVITÉS — Étude contradictoire.
ÉVALUATION / PREUVE — Niveau de confiance.

7 · Impact, alerte et atténuation - 2 h 30

OBJECTIF — Évaluer et proposer une réponse.
CONTENUS — Visibilité, effets, signalement, plateformes, communication, coordination.
MÉTHODES / ACTIVITÉS — Plan d'action.
ÉVALUATION / PREUVE — Mesures.

MENACES INFORMATIONNELLES

8 · Cas final complexe - 4 h 00

OBJECTIF — Caractériser une opération complète.
CONTENUS — Investigation, rapport technique, annexes.
MÉTHODES / ACTIVITÉS — Équipe.
ÉVALUATION / PREUVE — Rapport.

9 · Briefing décisionnel - 1 h 30

OBJECTIF — Présenter les résultats.
CONTENUS — Synthèse, incertitudes, recommandations, questions.
MÉTHODES / ACTIVITÉS — Soutenance.
ÉVALUATION / PREUVE — Oral + quiz.

AC-FIMI-401 · Analyste des menaces informationnelles numériques

MENACES INFORMATIONNELLES

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas final complexe, rapport et briefing décisionnel évalués sur la caractérisation des TTP, le niveau de confiance, l'évaluation de l'impact, les mesures d'atténuation et la restitution. Réussite : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille finale.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Référentiel de critères et modèles analytiques.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Affinis Campus

- AC-OSINT-501 — Pratique professionnelle de l’OSINT
- AC-DD-501 — Due diligence et investigation économique avancées
- AC-FIMI-501 — Investigation des ingérences et manipulations informationnelles

5 JOURS

3 formations

Professionnaliser les pratiques et conduire des cas complets.



Pratique professionnelle de l'OSINT

FINALITÉ PROFESSIONNELLE

Acquérir une autonomie opérationnelle sur les principales disciplines de l'OSINT.

PUBLIC VISÉ

Professionnels en reconversion ou montée en compétence, analystes, consultants, agents publics.

PRÉREQUIS

Aisance numérique; motivation pour les exercices pratiques.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable et test diagnostic portant sur les pratiques de recherche. Un échange avec le référent pédagogique est proposé en cas d'écart de niveau important.

DURÉE

5 jours - 35 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-501 · Pratique professionnelle de l'OSINT

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Cadrer et conduire une investigation OSINT professionnelle en respectant les contraintes juridiques, éthiques et d'OPSEC.
- Concevoir et exécuter une stratégie de recherche web avancée combinant lexique, opérateurs, moteurs, archives et recherche multilingue.
- Analyser une entreprise, ses dirigeants, ses implantations et son environnement à partir de sources ouvertes.
- Lire les principaux états financiers et mobiliser des ratios simples pour identifier des incohérences ou signaux faibles.
- Conduire des recherches SOCMINT et vérifier des contenus visuels ou géographiques à l'aide de techniques IMINT/GEOINT.
- Corréler des informations provenant de plusieurs catégories de sources et documenter le niveau de confiance associé.
- Structurer un journal de recherche et un dossier de preuves permettant la reproductibilité de l'investigation.
- Produire et présenter un rapport d'investigation complet à partir d'un cas fil rouge.

COMPÉTENCES VISÉES

Mettre en œuvre une investigation complète combinant web, entreprise, SOCMINT, IMINT et analyse.

MÉTHODES PÉDAGOGIQUES

Cas fil rouge, démonstrations, travaux individuels et en groupe. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

OSINT / INVESTIGATION

0 · Positionnement - 0 h 30

OBJECTIF — Adapter le parcours.
CONTENUS — Test, attentes, cas d'usage.
MÉTHODES / ACTIVITÉS — Diagnostic.
ÉVALUATION / PREUVE — Positionnement.

1 · Fondamentaux, droit et éthique - 3 h 00

OBJECTIF — Maîtriser le cadre professionnel.
CONTENUS — OSINT, cycle, limites, RGPD, accès, proportionnalité.
MÉTHODES / ACTIVITÉS — Apports et cas.
ÉVALUATION / PREUVE — Quiz.

2 · OPSEC et environnement de travail - 3 h 30

OBJECTIF — Sécuriser les recherches.
CONTENUS — Risques, cloisonnement, comptes, fichiers, stockage.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Plan OPSEC.

3 · Moteurs, sémantique et opérateurs - 4 h 00

OBJECTIF — Développer une recherche avancée.
CONTENUS — Fonctionnement, lexique, opérateurs, moteurs, archives.
MÉTHODES / ACTIVITÉS — Défis.
ÉVALUATION / PREUVE — Requêtes.

OSINT / INVESTIGATION

4 · Planification et traçabilité - 3 h 00

OBJECTIF — Organiser une collecte reproductible.
CONTENUS — OFR, plan, journal, archivage, qualification.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Plan et journal.

5 · Entreprises et due diligence - 4 h 00

OBJECTIF — Analyser une organisation.
CONTENUS — Registres, gouvernance, actifs, réputation, conformité.
MÉTHODES / ACTIVITÉS — Cas.
ÉVALUATION / PREUVE — Screening.

6 · Analyse financière - 3 h 00

OBJECTIF — Lire les principaux signaux.
CONTENUS — Bilan, résultat, ratios, tendances, incohérences.
MÉTHODES / ACTIVITÉS — Étude chiffrée.
ÉVALUATION / PREUVE — Diagnostic.

7 · SOCMINT - 3 h 00

OBJECTIF — Rechercher sur les réseaux sociaux.
CONTENUS — Pseudonymes, plateformes, chronologies, interactions.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Dossier.

OSINT / INVESTIGATION

8 · IMINT, GEOINT et infrastructures - 3 h 00

OBJECTIF — Vérifier contenus et actifs web.
CONTENUS — Images, vidéos, lieux, domaines, DNS, archives.
MÉTHODES / ACTIVITÉS — Mini-enquêtes.
ÉVALUATION / PREUVE — Notes.

9 · Analyse et rédaction - 2 h 00

OBJECTIF — Produire une restitution professionnelle.
CONTENUS — Faits, hypothèses, confiance, synthèse, annexes.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Note.

10 · Cas final fil rouge - 4 h 00

OBJECTIF — Mobiliser toutes les compétences.
CONTENUS — Investigation, rapport, briefing.
MÉTHODES / ACTIVITÉS — Équipe.
ÉVALUATION / PREUVE — Rapport + oral.

11 · Évaluation et bilan - 2 h 00

OBJECTIF — Valider les acquis.
CONTENUS — Quiz, soutenance, autoévaluation.
MÉTHODES / ACTIVITÉS — Évaluation.
ÉVALUATION / PREUVE — Grille finale.

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Cas pratique intégral, rapport et oral. Réussite proposée : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique, dont obligatoirement la traçabilité, la qualification des sources et le respect du cadre légal/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Support complet et boîte à outils.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Due diligence et investigation économique avancées

FINALITÉ PROFESSIONNELLE

Conduire une due diligence approfondie intégrant les dimensions juridiques, réputationnelles, financières et relationnelles.

PUBLIC VISÉ

Consultants, investisseurs, juristes, compliance, achats, intelligence économique.

PRÉREQUIS

Fondamentaux OSINT; connaissance de l'entreprise.

MODALITÉS DE POSITIONNEMENT

Questionnaire détaillé, test pratique et, lorsque nécessaire, entretien avec le référent pédagogique afin de vérifier la capacité à suivre les exercices avancés.

DURÉE

5 jours - 35 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-DD-501 · Due diligence et investigation économique avancées

DUE DILIGENCE / IE

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Cadrer une mission de due diligence complexe en fonction de la décision à éclairer, du secteur, du pays et des risques prioritaires.
- Reconstituer l'identité, la gouvernance, l'actionnariat, les bénéficiaires et l'historique d'une organisation.
- Vérifier la réalité opérationnelle d'une entreprise à travers ses activités, actifs, implantations, chaînes de valeur et partenaires.
- Analyser les dirigeants et réseaux associés afin d'identifier liens, conflits d'intérêts, dépendances ou risques cachés.
- Rechercher et qualifier sanctions, contentieux, controverses, risques réglementaires, réputationnels et éthiques.
- Analyser les états financiers et principaux ratios afin d'identifier tendances, fragilités et anomalies nécessitant approfondissement.
- Coter et hiérarchiser les risques en distinguant probabilité, impact et niveau de confiance.
- Formuler des recommandations de vérification ou de mitigation proportionnées aux constats.
- Produire et soutenir un rapport de due diligence complet, sourcé et décisionnel.

COMPÉTENCES VISÉES

Établir un périmètre ; collecter et analyser ; évaluer risques et dépendances ; rédiger une recommandation exploitable.

MÉTHODES PÉDAGOGIQUES

Pédagogie par cas, travaux de recherche, revue croisée. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

AC-DD-501 · Due diligence et investigation économique avancées

DUE DILIGENCE / IE

0 · Positionnement - 0 h 30

OBJECTIF — Évaluer les acquis.
CONTENUS — Diagnostic métier.
MÉTHODES / ACTIVITÉS — Questionnaire.
ÉVALUATION / PREUVE — Positionnement.

1 · Cadrage, droit et méthode - 3 h 00

OBJECTIF — Définir une mission robuste.
CONTENUS — Décision, risques, pays, RGPD, plan, sources.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Cahier de mission.

2 · Identité, gouvernance et actionnariat - 4 h 00

OBJECTIF — Reconstituer l'entité et le contrôle.
CONTENUS — Registres, statuts, bénéficiaires, filiales, mandats, historiques.
MÉTHODES / ACTIVITÉS — Investigation.
ÉVALUATION / PREUVE — Cartographie.

3 · Activités, actifs et chaîne de valeur - 3 h 30

OBJECTIF — Vérifier la réalité économique.
CONTENUS — Implantations, production, brevets, fournisseurs, clients, marchés.
MÉTHODES / ACTIVITÉS — Cas.
ÉVALUATION / PREUVE — Analyse de cohérence.

DUE DILIGENCE / IE

4 · Dirigeants et réseaux - 3 h 00

OBJECTIF — Analyser les personnes clés.
CONTENUS — Parcours, mandats, sociétés liées, conflits, réputation.
MÉTHODES / ACTIVITÉS — Recherche.
ÉVALUATION / PREUVE — Fiches dirigeants.

5 · Conformité et risques juridiques - 3 h 30

OBJECTIF — Identifier sanctions et contentieux.
CONTENUS — Sanctions, PEP, décisions, enquêtes, réglementation, éthique.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Chronologie.

6 · Réputation et environnement - 3 h 00

OBJECTIF — Qualifier les controverses.
CONTENUS — Presse, ONG, réseaux, campagnes, parties prenantes.
MÉTHODES / ACTIVITÉS — Corpus.
ÉVALUATION / PREUVE — Matrice.

7 · Analyse financière approfondie - 4 h 00

OBJECTIF — Évaluer solidité et anomalies.
CONTENUS — États, ratios, cash, dette, FR/BFR, tendances, consolidation.
MÉTHODES / ACTIVITÉS — Étude chiffrée.
ÉVALUATION / PREUVE — Diagnostic.

AC-DD-501 · Due diligence et investigation économique avancées

DUE DILIGENCE / IE

8 · Cotation, scénarios et recommandations - 2 h 30

OBJECTIF — Hiérarchiser les risques.
CONTENUS — Probabilité, impact, confiance, scénarios, mesures complémentaires.
MÉTHODES / ACTIVITÉS — Matrice.
ÉVALUATION / PREUVE — Cotation.

9 · Rédaction du rapport - 2 h 00

OBJECTIF — Structurer un livrable décisionnel.
CONTENUS — Executive summary, constats, preuves, limites, recommandations.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Brouillon évalué.

10 · Cas final et soutenance - 4 h 00

OBJECTIF — Produire une due diligence complète.
CONTENUS — Recherche, analyse, rapport, oral.
MÉTHODES / ACTIVITÉS — Équipe.
ÉVALUATION / PREUVE — Rapport + oral.

11 · Bilan - 2 h 00

OBJECTIF — Consolider les acquis.
CONTENUS — Quiz, retour, plan de progrès.
MÉTHODES / ACTIVITÉS — Évaluation.
ÉVALUATION / PREUVE — Grille finale.

AC-DD-501 · Due diligence et investigation économique avancées

DUE DILIGENCE / IE

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des fondamentaux.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Rapport complet et présentation en comité. Réussite proposée : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique, dont obligatoirement la traçabilité, la qualification des sources et le respect du cadre légal/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Modèle long form de due diligence.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Investigation des ingérences et manipulations informationnelles

FINALITÉ PROFESSIONNELLE

Mener une investigation complète sur un mode opératoire informationnel et en restituer les conclusions.

PUBLIC VISÉ

Analystes spécialisés, institutions publiques, cellules de veille, communication stratégique.

PRÉREQUIS

Pratique de l'OSINT et de la SOCMINT.

MODALITÉS DE POSITIONNEMENT

Dossier de positionnement, test pratique et entretien pédagogique. Les résultats permettent de confirmer l'adéquation du parcours et les adaptations nécessaires.

DURÉE

5 jours - 35 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel recommandé.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D'ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-FIMI-501 · Investigation des ingérences et manipulations informationnelles

MENACES INFORMATIONNELLES

OBJECTIF GÉNÉRAL

À l'issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Maîtriser les principaux cadres conceptuels utilisés pour décrire les manipulations informationnelles, les ingérences, les MOI, les IMS et les TTP.
- Construire et conduire une investigation complète sur une campagne informationnelle à partir de sources ouvertes.
- Analyser les narratifs, contenus, cibles, victimologie et temporalités afin de caractériser la composante informationnelle d'une opération.
- Reconstituer la chaîne de diffusion et identifier primo-diffusion, blanchiment, amplification, reprises et relais coordonnés.
- Analyser les comportements de comptes et réseaux afin de repérer automatisation, synchronisation, coordination ou inauthenticité.
- Cartographier les infrastructures techniques et actifs numériques associés : domaines, DNS, certificats, hébergement, métadonnées et archives.
- Comparer les tactiques, techniques et procédures afin d'identifier récurrences, évolutions et proximités entre campagnes.
- Formuler des hypothèses d'implication ou d'attribution selon un niveau de confiance explicite et des hypothèses alternatives.
- Évaluer la visibilité, les effets observables et les options d'atténuation sans surévaluer l'impact réel.
- Produire un rapport technique et défendre oralement les conclusions d'une investigation complexe.

COMPÉTENCES VISÉES

Détecter, documenter, caractériser et cartographier une campagne ; produire une appréciation stratégique.

MÉTHODES PÉDAGOGIQUES

Simulation d'investigation, cas fil rouge, travaux en cellule. Alternance d'apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d'analyse ; cas pratiques ; visioconférence et partage d'écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d'une pratique opérationnelle de l'OSINT et de la formation d'adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d'OPSEC associés.

MENACES INFORMATIONNELLES

0 · Positionnement - 0 h 30

OBJECTIF — Évaluer les acquis.
CONTENUS — Quiz et attentes.
MÉTHODES / ACTIVITÉS — Diagnostic.
ÉVALUATION / PREUVE — Positionnement.

1 · Cadres FIMI, INE, MOI et IMS - 3 h 00

OBJECTIF — Maîtriser les concepts.
CONTENUS — Définitions, critères, acteurs, TTP, droit, éthique.
MÉTHODES / ACTIVITÉS — Apport.
ÉVALUATION / PREUVE — Quiz.

2 · Narratifs, cibles et contenus - 3 h 30

OBJECTIF — Analyser la composante narrative.
CONTENUS — Victimologie, thèmes, émotions, contenus faux ou trompeurs, IA.
MÉTHODES / ACTIVITÉS — Corpus.
ÉVALUATION / PREUVE — Matrice.

3 · Chaîne de diffusion - 3 h 30

OBJECTIF — Reconstituer la propagation.
CONTENUS — Primo-diffusion, blanchiment, amplification, reprises opportunistes.
MÉTHODES / ACTIVITÉS — Chronologie.
ÉVALUATION / PREUVE — Schéma.

MENACES INFORMATIONNELLES

4 · SOCMINT comportementale - 3 h 30

OBJECTIF — Repérer coordination et inauthenticité.
CONTENUS — Comptes, automatisation, synchronisation, réseaux, plateformes.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Analyse.

5 · Infrastructures et investigation web - 4 h 00

OBJECTIF — Cartographier les actifs techniques.
CONTENUS — Domaines, DNS, SSL, IP, hébergement, métadonnées, archives.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Carte.

6 · TTP et comparaison de campagnes - 3 h 00

OBJECTIF — Identifier récurrences et évolutions.
CONTENUS — Taxonomie, signatures, adaptation, hypothèses.
MÉTHODES / ACTIVITÉS — Comparaison de cas.
ÉVALUATION / PREUVE — Matrice TTP.

7 · Attribution et niveau de confiance - 2 h 30

OBJECTIF — Formuler une appréciation prudente.
CONTENUS — Implication, proximité, extranéité, hypothèses concurrentes.
MÉTHODES / ACTIVITÉS — Exercice contradictoire.
ÉVALUATION / PREUVE — Conclusion calibrée.

MENACES INFORMATIONNELLES

8 · Impact et mesures d'atténuation - 2 h 30

OBJECTIF — Évaluer et répondre.
CONTENUS — Audience, effets, signalement, plateformes, communication, coordination.
MÉTHODES / ACTIVITÉS — Plan.
ÉVALUATION / PREUVE — Recommandations.

9 · Rédaction technique et briefing - 2 h 30

OBJECTIF — Produire des livrables adaptés.
CONTENUS — Rapport, annexes, synthèse, briefing, limites.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Note.

10 · Cas final complexe - 4 h 00

OBJECTIF — Conduire une investigation complète.
CONTENUS — Collecte, analyse, caractérisation, rapport.
MÉTHODES / ACTIVITÉS — Équipe.
ÉVALUATION / PREUVE — Rapport.

11 · Soutenance et bilan - 2 h 30

OBJECTIF — Défendre les conclusions.
CONTENUS — Oral, questions, quiz, retour.
MÉTHODES / ACTIVITÉS — Évaluation.
ÉVALUATION / PREUVE — Grille finale.

AC-FIMI-501 · Investigation des ingérences et manipulations informationnelles

MENACES INFORMATIONNELLES

ÉVALUATION INITIALE

Questionnaire préalable et test diagnostic.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Rapport analytique complet et briefing oral. Réussite proposée : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique, dont obligatoirement la traçabilité, la qualification des sources et le respect du cadre légal/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Kit d'investigation FIMI.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Affinis campus

10 JOURS

1 formation

Construire une maîtrise transversale et intensive.



- AC-OSINT-1001 — Parcours intensif d’investigation OSINT et d’analyse des menaces numériques

Parcours intensif d’investigation OSINT et d’analyse des menaces numériques

FINALITÉ PROFESSIONNELLE

Former des professionnels capables de conduire des investigations multi-sources et d’analyser des menaces numériques complexes.

PUBLIC VISÉ

Analystes, consultants, agents publics, cellules d’investigation, sûreté et intelligence économique.

PRÉREQUIS

Test de positionnement; aisance numérique; expérience professionnelle recommandée.

MODALITÉS DE POSITIONNEMENT

Questionnaire préalable, test diagnostic et échange pédagogique si nécessaire.

DURÉE

10 jours - 70 heures de formation

HORAIRES

Horaires indicatifs : 9 h 00-12 h 30 et 13 h 30-17 h 00. Horaires adaptables en intra-entreprise.

MODALITÉ

Présentiel / hybride / intra.

LIEU / OUTIL DISTANCIEL

Présentiel : Affinis Campus, chez le client ou salle louée. Distanciel : outil précisé sur la convocation ; connexion stable, webcam et accès web requis.

EFFECTIF MIN. / MAX.

4 participants minimum / 10 maximum recommandé en présentiel (modulable selon besoin et logistique) / Au-delà en distanciel ou hybride à déterminer conjointement

DÉLAI D’ACCÈS

Inscription ou validation de la session recommandée au moins 10 jours ouvrés avant le début, sous réserve de disponibilité et de réception des éléments administratifs. Un délai plus court peut être accepté au cas par cas.

TARIF / DEVIS

Sur devis. Le tarif figure sur la proposition commerciale ou la convention de formation.

CONTACT INSCRIPTION

Clara Carriorbe, c.carriorbe@affinis-conseil.com ; Philippe Chabrol, p.chabrol@affinis-conseil.com

Mise à jour : 29/07/2026 · Responsable de validation : Clara Carriorbe

AC-OSINT-1001 · Parcours intensif d’investigation OSINT et d’analyse des menaces numériques

OSINT / INVESTIGATION

OBJECTIF GÉNÉRAL

À l’issue de la formation, le participant sera capable de cadrer une demande de recherche, concevoir une stratégie de recherche en sources ouvertes, collecter et qualifier des informations accessibles publiquement, puis restituer des résultats sourcés dans le respect du cadre légal et des règles élémentaires de sécurité opérationnelle.

OBJECTIFS OPÉRATIONNELS ÉVALUABLES

- Planifier et conduire une investigation OSINT complexe en définissant objectifs, sources, méthodologies, risques et critères de clôture.
- Mettre en place un dispositif juridique, éthique et d’OPSEC adapté à une mission ou à une cellule d’investigation.
- Maîtriser les techniques de recherche web avancée, multilingue et archivistique, et en assurer la traçabilité.
- Utiliser l’IA et des formes d’automatisation raisonnée pour assister la collecte, l’extraction ou la structuration tout en maintenant un contrôle humain documenté.
- Analyser une entreprise, sa gouvernance, ses dirigeants, ses risques de conformité et ses principaux indicateurs financiers.
- Conduire des investigations SOCMINT, corréler des identités numériques et cartographier des interactions ou communautés.
- Vérifier des images, vidéos, localisations et infrastructures numériques au moyen de techniques IMINT, GEOINT et d’investigation web.
- Détecter et caractériser une opération de manipulation informationnelle en analysant narratifs, diffusion, inauthenticité, amplification et TTP.
- Corréler des données multi-sources, qualifier leur fiabilité et formuler des conclusions selon un niveau de confiance explicite.
- Produire un rapport d’investigation structuré, sourcé et reproductible, puis présenter et défendre les conclusions lors d’un briefing professionnel.

COMPÉTENCES VISÉES

Planifier et conduire une collecte ; exploiter web, entreprises, réseaux et images ; analyser les menaces informationnelles ; produire un renseignement stratégique.

MÉTHODES PÉDAGOGIQUES

Parcours par blocs, 60 % pratique, tutorat, travaux intersessions possibles. Alternance d’apports courts, démonstrations, exercices progressifs et mises en situation. Les activités sont adaptées au niveau et aux usages professionnels des participants.

MOYENS ET RESSOURCES

Support de formation ; ordinateur individuel connecté ; navigateur récent ; accès aux outils et sources mobilisés ; fiches méthodes ; trames de collecte et d’analyse ; cas pratiques ; visioconférence et partage d’écran en distanciel.

PROFIL DU FORMATEUR

Professionnel expérimenté dans le domaine enseigné, disposant d’une pratique opérationnelle de l’OSINT et de la formation d’adultes, maîtrisant les enjeux juridiques, éthiques, techniques et d’OPSEC associés.

AC-OSINT-1001 · Parcours intensif d'investigation OSINT et d'analyse des menaces numériques

OSINT / INVESTIGATION

0 · Positionnement et lancement - 1 h 00

OBJECTIF — Évaluer les acquis et cadrer le parcours.
CONTENUS — Test, entretien collectif, règles, cas fil rouge.
MÉTHODES / ACTIVITÉS — Diagnostic.
ÉVALUATION / PREUVE — Positionnement.

1 · Jour 1 - OSINT, cycle et cadre juridique - 6 h 00

OBJECTIF — Maîtriser les fondements professionnels.
CONTENUS — Définitions, cycle, finalité, RGPD, accès, éthique, preuve.
MÉTHODES / ACTIVITÉS — Apports, cas, exercices.
ÉVALUATION / PREUVE — Quiz et étude de situations.

2 · Jour 2 - OPSEC et gouvernance - 7 h 00

OBJECTIF — Sécuriser une cellule ou mission.
CONTENUS — Risques, cloisonnement, comptes, environnements, stockage, procédures.
MÉTHODES / ACTIVITÉS — Ateliers.
ÉVALUATION / PREUVE — Plan OPSEC.

3 · Jour 3 - Recherche web avancée - 7 h 00

OBJECTIF — Maîtriser moteurs, lexique et opérateurs.
CONTENUS — Indexation, sémantique, opérateurs, moteurs, archives, multilingue.
MÉTHODES / ACTIVITÉS — Défis.
ÉVALUATION / PREUVE — Requêtes et journal.

OSINT / INVESTIGATION

4 · Jour 4 - IA, extraction et automatisation raisonnée - 7 h 00

OBJECTIF — Utiliser l’IA et l’automatisation avec contrôle.
CONTENUS — Prompts, extraction, structuration, biais, confidentialité, scripts simples/no-code selon public.
MÉTHODES / ACTIVITÉS — Ateliers.
ÉVALUATION / PREUVE — Protocole et mini-livrable.

5 · Jour 5 - Entreprises et gouvernance - 7 h 00

OBJECTIF — Analyser une organisation.
CONTENUS — Registres, actionnariat, dirigeants, filiales, actifs, domaines.
MÉTHODES / ACTIVITÉS — Investigation.
ÉVALUATION / PREUVE — Cartographie.

6 · Jour 6 - Due diligence et finance - 7 h 00

OBJECTIF — Évaluer risques et solidité.
CONTENUS — Conformité, réputation, contentieux, états financiers, ratios, cotation.
MÉTHODES / ACTIVITÉS — Cas.
ÉVALUATION / PREUVE — Rapport intermédiaire.

7 · Jour 7 - SOCMINT et identités - 7 h 00

OBJECTIF — Conduire une investigation multiréseaux.
CONTENUS — Pseudonymes, plateformes, chronologie, comportements, cartographie.
MÉTHODES / ACTIVITÉS — Atelier.
ÉVALUATION / PREUVE — Dossier SOCMINT.

OSINT / INVESTIGATION

8 · Jour 8 - IMINT, GEOINT et infrastructures - 7 h 00

OBJECTIF — Vérifier contenus et actifs numériques.
CONTENUS — Images, vidéos, géolocalisation, domaines, DNS, certificats, archives.
MÉTHODES / ACTIVITÉS — Mini-enquêtes.
ÉVALUATION / PREUVE — Notes techniques.

9 · Jour 9 - Menaces informationnelles - 7 h 00

OBJECTIF — Détecter et caractériser une opération.
CONTENUS — Narratifs, diffusion, inauthenticité, amplification, TTP, attribution prudente.
MÉTHODES / ACTIVITÉS — Étude de campagne.
ÉVALUATION / PREUVE — Matrice de caractérisation.

10 · Jour 10 - Cas final et soutenance - 7 h 00

OBJECTIF — Mobiliser l’ensemble des compétences.
CONTENUS — Investigation en équipe, rapport, annexes, briefing, retour.
MÉTHODES / ACTIVITÉS — Cas fil rouge.
ÉVALUATION / PREUVE — Rapport + soutenance + quiz final.

AC-OSINT-1001 · Parcours intensif d'investigation OSINT et d'analyse des menaces numériques

OSINT / INVESTIGATION

ÉVALUATION INITIALE

Questionnaire préalable, test pratique court et recueil d'un cas d'usage. Entretien de positionnement en cas de doute sur la maîtrise des bases requises.

ÉVALUATIONS FORMATIVES

Exercices corrigés, observations des productions, questions orales, quiz intermédiaires et retours individualisés. Les difficultés constatées conduisent à ajuster les démonstrations et les activités suivantes.

ÉVALUATION FINALE ET CRITÈRES DE RÉUSSITE

Dossier final, rapport, soutenance et évaluation individuelle. Réussite proposée : au moins 70 % au quiz final et validation d'au moins 70 % des critères de la grille du cas pratique, dont obligatoirement la traçabilité, la qualification des sources et le respect du cadre légal/OPSEC.

DOCUMENT REMIS AU PARTICIPANT

Attestation de fin de formation mentionnant les objectifs travaillés et les résultats de l'évaluation ; support pédagogique ; Portfolio de livrables et kit complet.

ACCESSIBILITÉ ET ADAPTATIONS POSSIBLES

La formation peut faire l'objet d'adaptations pédagogiques, organisationnelles ou techniques selon les besoins identifiés : supports numériques accessibles, temps supplémentaire, rythme adapté, aide à la prise en main, aménagement du poste ou modalité distancielle. Les besoins sont recueillis dès l'inscription et étudiés avec le référent handicap.

RÉFÉRENT HANDICAP / CONTACT

Clara Carriorbe, c.carriorbe@affinis-conseil.com

ASSIDUITÉ

Feuilles d'émargement par demi-journée en présentiel ; relevés de connexion et émargement électronique en distanciel ; suivi des absences et retards.

SATISFACTION

Questionnaire de satisfaction à chaud en fin de formation et, lorsque pertinent, questionnaire à froid ou retour du commanditaire.

INDICATEURS DE RÉSULTATS

Après consolidation : taux de satisfaction, taux d'assiduité, taux de réussite et éventuellement taux de recommandation. Au lancement : « nouvelle formation - résultats en cours de consolidation ».

Affinis Campus

DES FORMATIONS POUR PASSER DE L'INFORMATION À LA DÉCISION

Présentiel · classe virtuelle · hybride · sur mesure

c.carriorbe@affinis-conseil.com · p.chabrol@affinis-conseil.com

AFFINIS CAMPUS · 2026–2027

