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

Mis à jour le 31/08/2026

S'inscrire

Formation Certification GIAC GOSI®

5 jours (35 heures)

Présentation

La formation Certification GIAC GOSI prépare à la certification officielle GIAC Open Source Intelligence et vous apporte les méthodes indispensables pour collecter, analyser et restituer du renseignement issu de sources ouvertes.

La certification GIAC Open Source Intelligence valide votre capacité à conduire des investigations OSINT structurées, à qualifier les informations recueillies et à produire une intelligence exploitable dans un contexte de cybersécurité, de réponse à incident ou de recherche de menace.

Notre formation vous permet de préparer l'examen en couvrant les domaines évalués : méthodologie d'investigation, recherche et collecte de données, analyse des personnes et des organisations, cartographie d'infrastructures, exploration du dark web et protection opérationnelle.

Vous apprendrez à formuler un besoin de renseignement, à sélectionner des sources pertinentes, à vérifier la fiabilité des informations et à documenter chaque étape de vos investigations. Les mises en situation vous entraînent à transformer des données publiques hétérogènes en éléments de décision traçables.

À l'issue de la formation, vous serez en mesure de préparer efficacement l'examen GIAC Open Source Intelligence, d'organiser vos supports de révision et d'appliquer les bonnes pratiques nécessaires à des investigations OSINT rigoureuses, éthiques et sécurisées.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Maîtriser les fondamentaux méthodologiques de l'OSINT et les objectifs de la certification GIAC Open Source Intelligence
- Collecter, qualifier et corréler des informations publiques sur des personnes, des organisations et des infrastructures
- Analyser les domaines, adresses IP, certificats et données exposées dans une démarche de renseignement
- Appliquer les principes d'OPSEC, de confidentialité et de traçabilité lors d'une investigation
- Construire un rapport de renseignement actionnable et se préparer au format de l'examen de certification

Public visé

- Analyste cybersécurité
- Analyste SOC
- Analyste DFIR
- Consultant cybersécurité
- Investigateur numérique

Pré-requis

- Connaissances fondamentales en cybersécurité et en investigation numérique
- Maîtrise courante de la navigation web et des moteurs de recherche
- Notions sur les réseaux TCP/IP, les noms de domaine et les adresses IP
- Capacité à lire une documentation technique en anglais

Pré-requis techniques

- Ordinateur récent équipé de Windows 10 ou 11, de macOS 12 ou version ultérieure, ou d'une distribution Linux récente
- Processeur double coeur,8 Go de RAM minimum et navigateur web récent tel que Google Chrome, Mozilla Firefox ou Microsoft Edge
- Connexion Internet stable, sans filtrage bloquant les services web et les environnements de recherche utilisés en formation
- Droits d'installation ou utilisation d'un environnement isolé, par exemple une machine virtuelle, pour les exercices de collecte et d'analyse

Programme de notre formation GIAC GOSI®

[Jour 1 - Matin]

Fondations de l'OSINT et cadre de certification

- Positionnement de la certification GIAC Open Source Intelligence et compétences validées

- Définition de l'OSINT, cycle du renseignement et transformation de la donnée en information actionnable
- Délimitation du périmètre, formulation des besoins et préparation d'un plan de collecte
- Cadres éthiques, réglementaires et principes de minimisation des données
- Présentation des objectifs de l'examen, de la méthode de révision et de l'organisation des références autorisées

[Jour 1 - Après-midi]

Recherche, sources et validation de l'information

- Typologie des sources ouvertes : web visible, archives, réseaux sociaux, registres et bases spécialisées
- Techniques de recherche avancée avec opérateurs, requêtes ciblées et pivots de recherche
- Évaluation de la fiabilité : source, date, contexte, corroboration et biais informationnels
- Collecte traçable des preuves, horodatage, conservation des éléments et prise de notes
- Atelier pratique : construire un plan de recherche et qualifier les sources sur un scénario d'investigation d'entreprise

[Jour 2 - Matin]

Investigation des personnes et présence numérique

- Recherche d'identités, pseudonymes et empreintes numériques dans le respect du cadre légal
- Analyse des profils publics, des relations, des publications et des signaux de contextualisation
- Corrélation des identifiants, adresses électroniques, images et métadonnées accessibles
- Prévention des erreurs d'attribution et validation d'une identité par recoupement
- Restitution factuelle des résultats et distinction entre observation, hypothèse et conclusion

[Jour 2 - Après-midi]

Investigation des organisations et risques exposés

- Collecte d'informations sur la structure, les activités, les partenaires et l'écosystème d'une organisation
- Identification des actifs publics, documents exposés, fuites de données et signaux de risque
- Analyse de l'empreinte numérique d'une entreprise à partir de sources publiques
- Qualification des impacts potentiels pour la sécurité, la fraude ou la réponse à incident
- Atelier pratique : réaliser un profil OSINT d'organisation et prioriser les constats selon leur niveau de risque

[Jour 3 - Matin]

Cartographie des infrastructures exposées

- Fondamentaux des DNS, domaines, sous-domaines, adresses IP et certificats numériques
- Découverte d'actifs publics et compréhension des liens entre services, hébergement et infrastructures
- Exploitation des données d'enregistrement, des journaux de certificats et des informations de routage
- Corrélation entre éléments techniques pour identifier une surface d'exposition
- Limites de l'attribution technique et précautions d'interprétation dans un rapport OSINT

[Jour 3 - Après-midi]

Collecte, traitement et automatisation légère

- Structuration des données recueillies : formats, normalisation, dédoublonnage et enrichissement
- Exploitation des métadonnées de documents, images et contenus publiquement accessibles
- Principes d'automatisation simple pour accélérer la collecte et le traitement des résultats
- Gestion des limites des outils, contrôle de la qualité et traçabilité des traitements
- Atelier pratique : analyser un jeu de données OSINT, extraire des indicateurs et produire une chronologie exploitable

[Jour 4 - Matin]

Deep web, dark web et renseignement de menace

- Distinction entre web visible, deep web et dark web
- Principes de recherche de données exposées, de fuites et de mentions d'organisations
- Évaluation de la crédibilité des informations issues d'espaces à accès restreint
- Identification des risques liés à l'exposition de données, aux campagnes malveillantes et à la fraude
- Intégration des résultats OSINT dans une démarche de threat intelligence

[Jour 4 - Après-midi]

Protection opérationnelle de l'investigateur

- Enjeux de confidentialité, d'anonymat et de sécurité lors des investigations en ligne
- Principes d'OPSEC : compartimentation, hygiène numérique, identité de recherche et réduction des traces
- Gestion des risques de contamination, de ciblage et d'exposition involontaire de données
- Choix d'un environnement de travail isolé et sécurisation des comptes utilisés pour la recherche
- Atelier pratique : concevoir un dispositif OPSEC adapté à une investigation sensible et identifier ses points de vigilance

[Jour 5 - Matin]

Analyse, synthèse et production de renseignement

- Transformation des données collectées en constats vérifiables et hiérarchisés
- Méthodes de corrélation, raisonnement analytique et gestion des incertitudes
- Construction d'un rapport : périmètre, méthodologie, éléments probants, analyse et recommandations
- Adaptation de la restitution aux analystes, équipes de sécurité, décideurs et parties prenantes
- Révision ciblée des domaines de compétences attendus pour l'examen GIAC Open Source Intelligence

[Jour 5 - Après-midi]

Préparation finale à l'examen de certification

- Rappel du format de l'examen, gestion du temps et lecture efficace des questions
- Organisation d'un index de révision et exploitation méthodique des supports autorisés
- Stratégies de réponse : élimination, priorisation, traitement des questions reportées et contrôle final
- Analyse des erreurs fréquentes sur la méthodologie OSINT, l'OPSEC et la qualification des résultats
- Atelier pratique : résoudre un cas de synthèse, justifier les réponses et établir un plan de révision personnel

Sociétés concernées

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

Positionnement à l'entrée en formation

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

Méthodes pédagogiques

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

Organisation

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

Validation

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

Sanction

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