+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 GSOA®

5 jours (35 heures)

Présentation

La Formation Certification GIAC GSOA vous prépare à la certification officielle GIAC Strategic OSINT Analyst et à la conduite d'investigations OSINT avancées, fiables, structurées et adaptées aux enjeux de la cybersécurité.

La certification GIAC Strategic OSINT Analyst valide votre capacité à collecter, vérifier, corréler et restituer des informations issues de sources ouvertes. Elle couvre notamment l'automatisation avec Python, l'analyse de données à grande échelle, la désinformation, le Dark Web, les cryptoactifs et les investigations multimédias.

Notre formation vous permet de préparer méthodiquement l'examen GIAC GSOA à travers les domaines de compétences évalués. Vous apprendrez à construire une démarche d'investigation robuste, à appliquer des techniques d'analyse structurée, à préserver votre OPSEC et à produire des conclusions exploitables par les décideurs.

Vous développerez des méthodes avancées de collecte, de scraping, de supervision et de qualification des sources. Les cas pratiques vous amèneront à utiliser Python, les API, les techniques de vérification d'images, de vidéos et d'audio, ainsi que l'analyse d'infrastructures, de réseaux sociaux et de données blockchain.

À l'issue de la formation, vous serez en mesure de préparer l'examen officiel dans des conditions proches de la certification, de traiter des scénarios complexes et de démontrer des compétences opérationnelles en renseignement d'origine open source.

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

Objectifs

- Maîtriser les domaines de compétences évalués par la certification GIAC Strategic OSINT Analyst
- Conduire des investigations OSINT avancées avec une méthodologie rigoureuse et traçable
- Automatiser la collecte, l'enrichissement et la surveillance de données avec Python et des API
- Évaluer la fiabilité des sources, détecter la désinformation et limiter les biais analytiques
- Analyser des contenus multimédias, des infrastructures, des activités Dark Web et des transactions blockchain
- Se préparer au format pratique et aux scénarios de l'examen GIAC GSOA

Public visé

- Analyste OSINT
- Analyste CTI
- Analyste SOC
- Analyste DFIR
- Investigateur cybersécurité

Pré-requis

- Expérience pratique de la collecte et de l'analyse OSINT
- Connaissances des principes d'analyse du renseignement et de qualification des sources
- Maîtrise des fondamentaux des réseaux, des services web et des environnements Linux
- Notions de programmation en Python et de manipulation de données JSON

Pré-requis techniques

- Un poste sous Windows 10 ou 11, macOS ou Linux avec droits d'installation
- Un processeur 64 bits avec virtualisation activée, au moins 16 Go de RAM et 80 Go d'espace disque disponible
- Un logiciel de virtualisation VMware Workstation, VMware Fusion ou VirtualBox
- Une connexion Internet stable, sans filtrage bloquant les services web, les API, les dépôts logiciels et les environnements de laboratoire
- Un navigateur récent Google Chrome ou Mozilla Firefox et un éditeur tel que Visual Studio Code

Programme de notre formation GIAC GSOA®

[Jour 1 - Matin]

Cadre stratégique de l'OSINT et analyse du renseignement

- Positionnement de la certification GIAC Strategic OSINT Analyst et cartographie des compétences évaluées
- Cycle du renseignement, formulation des besoins, hypothèses et critères de collecte
- Évaluation de la fiabilité avec les modèles Admiralty et CRAAP

- Réduction des biais cognitifs par les techniques d'analyse structurée, dont ACH et Key Assumptions Check
- Atelier pratique : analyser une campagne informationnelle, qualifier les sources et construire une matrice d'hypothèses concurrentes

[Jour 1 - Après-midi]

Désinformation et investigations internationales

- Différences entre misinformation , disinformation et malinformation
- Indicateurs de comportements inauthentiques coordonnés, amplification et blanchiment de narratifs
- Collecte et contextualisation de sources internationales, multilingues et sectorielles
- Préparation à l'examen : raisonnement analytique, formulation du niveau de confiance et justification des conclusions
- Atelier pratique : attribuer une opération d'influence à partir de signaux sociaux, temporels et techniques

[Jour 2 - Matin]

Automatisation OSINT avec Python

- Rappels ciblés de Python pour l'investigation, structures de données, fichiers et traitement JSON
- Requêtes web, parsing de contenus, extraction d'indicateurs et gestion des erreurs
- Utilisation d'API tierces pour enrichir les investigations et consolider les résultats
- Principes d'attribution, de limitation de débit et de collecte respectueuse des contraintes opérationnelles
- Atelier pratique : développer un script Python de collecte et d'enrichissement d'entités à partir de sources ouvertes

[Jour 2 - Après-midi]

Tableaux de bord et surveillance persistante

- Conception d'un pipeline de collecte, normalisation, déduplication et horodatage des données
- Création d'un tableau de bord de renseignement automatisé avec Python
- Surveillance persistante de plateformes, canaux et sites à l'aide d'alertes et d'API
- Déploiement de tâches automatisées dans le cloud et gestion sécurisée des secrets
- Atelier pratique : mettre en place un tableau de bord alimenté automatiquement et produire une synthèse de veille

[Jour 3 - Matin]

Forensique multimédia et IA appliquée à l'OSINT

- Vérification d'images, recherche inversée, métadonnées, géolocalisation et analyse de cohérence
- Validation de vidéos, extraction d'indices visuels et détection de manipulations
- Analyse audio, transcription, traduction, diarisation et reconnaissance de locuteurs
- Usages et limites de l'IA pour l'analyse, l'automatisation et la détection de contenus synthétiques
- Atelier pratique : vérifier un contenu multimédia suspect et rédiger une conclusion analytique sourcée

[Jour 3 - Après-midi]

Enumération avancée et cartographie d'infrastructure

- Recherche d'actifs exposés, domaines liés, sous-domaines et ressources cloud
- Exploitation des données WHOIS , DNS , certificats TLS et empreintes techniques
- Enumération passive, attribution de sites et identification de relations entre infrastructures
- Analyse des surfaces d'exposition sans interaction intrusive avec les cibles
- Atelier pratique : cartographier l'infrastructure publique d'une organisation fictive et prioriser les pivots d'investigation

[Jour 4 - Matin]

OPSEC, personas et investigations Dark Web

- Gestion de l'OPSEC , séparation des identités, réduction des traces et compartimentation
- Création et maintien de personas fictifs dans un cadre légal et éthique
- Écosystèmes cybercriminels, places de marché, journaux de voleurs d'identifiants et forums spécialisés
- Recherche de contenus Dark Web et techniques de désanonymisation fondées sur des sources ouvertes
- Atelier pratique : concevoir un plan d'investigation Dark Web intégrant sécurité opérationnelle, collecte et traçabilité

[Jour 4 - Après-midi]

Blockchain et renseignement sans fil

- Fondamentaux des blockchains publiques, transactions, adresses, services et points de pivot
- Traçage de flux de cryptoactifs et identification d'interactions à risque ou sous sanctions
- Exploitation des sources ouvertes liées au spectre radio, au Wi-Fi, au Bluetooth et aux drones
- Préparation à l'examen : résolution de scénarios pratiques, priorisation des preuves et gestion du temps
- Atelier pratique : suivre un ensemble de transactions blockchain et corréler les résultats à des éléments d'enquête

[Jour 5 - Matin]

Supervision, données sectorielles et recherche de secrets

- Outils de monitoring web, moteurs de recherche auto-hébergés et automatisation de workflows
- Visualisation de données et analyse de réseaux pour révéler des relations entre entités
- OSINT appliqué aux transports, à l'aviation, au maritime et aux données de localisation
- Identification de documents protégés, de secrets exposés et d'identifiants compromis dans des sources ouvertes
- Atelier pratique : construire un workflow de surveillance d'une menace et qualifier des informations sensibles découvertes

[Jour 5 - Après-midi]

Simulation de certification et restitution opérationnelle

- Révision transversale des objectifs de la certification GIAC Strategic OSINT Analyst
- Stratégie de préparation : indexation des ressources, arbitrage des pistes et gestion du temps d'examen
- Résolution de défis pratiques combinant collecte, automatisation, analyse et validation
- Construction d'une restitution orientée décideur, niveaux de confiance, limites et recommandations
- Atelier pratique : réaliser un cas fil rouge chronométré et présenter les conclusions de l'investigation

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.