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

Updated on 09/17/2026

Sign Up

GIAC GSOA Certification Training

5 days (35 hours)

Overview

The GIAC GSOA Certification Training prepares you for the official GIAC Strategic OSINT Analyst certification and for conducting advanced, reliable, structured OSINT investigations tailored to cybersecurity challenges.

The GIAC Strategic OSINT Analyst certification validates your ability to collect, verify, correlate, and report information from open sources. It covers topics such as automation with Python, large-scale data analysis, disinformation, the Dark Web, cryptoassets, and multimedia investigations.

Our training course enables you to methodically prepare for the GIAC GSOA exam by covering the assessed skill areas. You will learn to build a robust investigative approach, apply structured analysis techniques, maintain your OPSEC, and produce actionable findings for decision-makers.

You will develop advanced methods for collecting, scraping, monitoring, and qualifying sources. Hands-on exercises will guide you in using Python, APIs, and techniques for verifying images, videos, and audio, as well as analyzing infrastructure, social media, and blockchain data.

Upon completion of the course, you will be able to prepare for the official exam under conditions similar to those of the certification, handle complex scenarios, and demonstrate operational skills in open-source intelligence.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Master the skill areas assessed by the GIAC Strategic OSINT Analyst certification
- Conduct advanced OSINT investigations using a rigorous and traceable methodology
- Automate data collection, enrichment, and monitoring using Python and APIs
- Assess the reliability of sources, detect disinformation, and minimize analytical biases
- Analyze multimedia content, infrastructure, Dark Web activities, and blockchain transactions
- Prepare for the hands-on format and scenarios of the GIAC GSOA exam

Target Audience

- OSINT Analyst
- CTI Analyst
- SOC Analyst
- DFIR Analyst
- Cybersecurity Investigator

Requirements

- Practical experience in OSINT collection and analysis
- Knowledge of intelligence analysis principles and source evaluation
- Proficiency in the fundamentals of networks, web services, and Linux environments
- Basic knowledge of Python programming and JSON data manipulation

Technical Prerequisites

- Linux lab environment equipped with Python and the libraries needed for data collection, parsing, and enrichment exercises
- API keys and demo accounts configured for the OSINT sources used during the investigations
- Isolated browsing environment for OPSEC, persona, and Dark Web research exercises
- Tools for verifying and analyzing images, videos, audio files, and metadata used during multimedia investigations
- Datasets and analysis tools required for infrastructure mapping and blockchain transaction exercises

GIAC GSOA® Training Program

[Day 1 - Morning]

Strategic Framework for OSINT and Intelligence Analysis

- Overview of the GIAC Strategic OSINT Analyst certification and mapping of assessed competencies

- The intelligence cycle, requirements formulation, assumptions, and collection criteria
- Assessing reliability using the Admiralty and CRAAP models
- Reducing cognitive biases through structured analysis techniques, including ACH and Key Assumptions Check
- Hands-on Workshop: Analyzing an information campaign, evaluating sources, and building a matrix of competing hypotheses

[Day 1 – Afternoon]

Disinformation and International Investigations

- Differences between misinformation, disinformation, and malinformation
- Indicators of coordinated inauthentic behavior, amplification, and narrative laundering
- Collection and contextualization of international, multilingual, and sector-specific sources
- Exam preparation: analytical reasoning, formulating confidence levels, and justifying conclusions
- Hands-on workshop: identifying an influence operation based on social, temporal, and technical signals

[Day 2 – Morning]

OSINT automation with Python

- Targeted Python refresher for investigations, data structures, files, and JSON processing
- Web queries, content parsing, indicator extraction, and error handling
- Using third-party APIs to enrich investigations and consolidate results
- Principles of attribution, rate limiting, and collection that respects operational constraints
- Hands-on Workshop: Developing a Python script to collect and enrich entities from open sources

[Day 2 - Afternoon]

Dashboards and continuous monitoring

- Designing a pipeline for data collection, normalization, deduplication, and timestamping
- Creating an automated intelligence dashboard with Python
- Persistent monitoring of platforms, channels, and sites using alerts and APIs
- Deploying automated tasks in the cloud and securely managing secrets
- Hands-on Workshop: Setting Up an Automatically Updated Dashboard and Generating a Monitoring Summary

[Day 3 - Morning]

Multimedia Forensics and AI Applied to OSINT

- Image verification, reverse image search, metadata, geolocation, and consistency analysis
- Video validation, visual clue extraction, and manipulation detection
- Audio analysis, transcription, translation, diarization, and speaker recognition
- Uses and Limitations of AI for the Analysis, Automation, and Detection of Synthetic Content
- Hands-on Workshop: Verifying Suspicious Multimedia Content and Writing a Sourced Analytical Conclusion

[Day 3 – Afternoon]

Advanced asset discovery and infrastructure mapping

- Searching for exposed assets, related domains, subdomains, and cloud resources
- Analyzing WHOIS, DNS, TLS certificate, and technical fingerprint data
- Passive enumeration, site attribution, and identification of relationships between infrastructures
- Analysis of exposure surfaces without intrusive interaction with targets
- Hands-on workshop: mapping the public infrastructure of a fictional organization and prioritizing investigation pivots

[Day 4 - Morning]

OPSEC, personas, and Dark Web investigations

- OPSEC management, identity separation, trace reduction, and compartmentalization
- Creating and maintaining fictitious personas within a legal and ethical framework
- Cybercriminal ecosystems, marketplaces, credential-stealing logs, and specialized forums
- Searching for Dark Web content and de-anonymization techniques based on

- Hands-on workshop: designing a Dark Web investigation plan that integrates operational security, data collection, and traceability

[Day 4 - Afternoon]

Blockchain and wireless intelligence

- Fundamentals of public blockchains, transactions, addresses, services, and pivot points
- Tracing cryptoasset flows and identifying risky or sanctioned interactions
- Exploiting open-source intelligence related to the radio spectrum, Wi-Fi, Bluetooth, and drones
- Exam preparation: solving practical scenarios, prioritizing evidence, and time management
- Hands-on Workshop: Tracking a Set of Blockchain Transactions and Correlating the Results with investigative leads

[Day 5 - Morning]

Surveillance, sector-specific data, and the search for secrets

- Web monitoring tools, self-hosted search engines, and workflow automation
- Data visualization and network analysis to reveal relationships between entities
- OSINT Applied to Transportation, Aviation, Maritime, and Location Data
- Identifying classified documents, exposed secrets, and compromised credentials in open sources
- Hands-on workshop: Building a threat monitoring workflow and qualifying discovered

[Day 5 - Afternoon]

Certification simulation and operational debriefing

- Comprehensive review of the GIAC Strategic OSINT Analyst certification objectives
- Preparation strategy: resource indexing, lead prioritization, and exam time management
- Solving practical challenges combining collection, automation, analysis, and validation
- Developing a decision-maker-oriented report, including confidence levels, limitations, and recommendations
- Hands-on workshop: conducting a timed case study and presenting the findings of the investigation

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Assessment at the Start of Training

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor, supported by examples and

reflection sessions and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.