AMBIENT-IT

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

Updated on September 10, 2026

Sign Up

GIAC GOSI® Certification Training

5 days (35 hours)

Overview

The GIAC GOSI® Certification Training prepares you for the official GIAC Open Source Intelligence certification and provides you with the essential methods for collecting, analyzing, and reporting intelligence from open sources.

The GIAC Open Source Intelligence certification validates your ability to conduct structured OSINT investigations, assess the information gathered, and produce actionable intelligence in the context of cybersecurity, incident response, or threat hunting.

Our training course helps you prepare for the exam by covering the assessed areas: investigation methodology, data search and collection, analysis of individuals and organizations, infrastructure mapping, dark web exploration, and operational protection.

You will learn how to formulate an intelligence requirement, select relevant sources, verify the reliability of information, and document each step of your investigations. Practical exercises will train you to transform diverse public data into traceable decision-making elements.

Upon completion of the course, you will be able to effectively prepare for the GIAC Open Source Intelligence exam, organize your study materials, and apply the best practices necessary for rigorous, ethical, and secure OSINT investigations.

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 methodological fundamentals of OSINT and the objectives of the GIAC Open Source Intelligence certification
- Collect, qualify, and correlate publicly available information on individuals, organizations, and infrastructure
- Analyze domains, IP addresses, certificates, and exposed data as part of an intelligence-gathering process
- Apply the principles of OPSEC, confidentiality, and traceability during an investigation
- Compile an actionable intelligence report and prepare for the certification exam format

Target Audience

- Cybersecurity Analyst
- SOC Analyst
- DFIR analyst
- Cybersecurity consultant
- Digital Investigator

Prerequisites

- Basic knowledge of cybersecurity and digital forensics
- Proficiency in web browsing and search engines
- Basic understanding of TCP/IP networks, domain names, and IP addresses
- Ability to read technical documentation in English

Technical Prerequisites

- Isolated and compartmentalized research environment for OSINT exercises
- OSINT tools configured for searching for individuals, organizations, domains, IP addresses, certificates, and metadata
- Dedicated research accounts and identities for exercises involving social media and sources requiring authentication
- Secure environment dedicated to research exercises on the Deep Web and the Dark Web
- Datasets, documents, and investigative materials prepared for collection, correlation, and reporting exercises

GIAC GOSI® Training Program

[Day 1 - Morning]

OSINT Fundamentals and Certification Framework

- Positioning of the GIAC Open Source Intelligence certification and validated skills

- Definition of OSINT, the intelligence cycle, and transforming data into actionable intelligence
- Defining the scope, formulating requirements, and preparing a data collection plan
- Ethical and regulatory frameworks and data minimization principles
- Overview of exam objectives, study methods, and the organization of authorized reference materials

[Day 1 – Afternoon]

Research, sources, and validation of information

- Types of open-source data: the visible web, archives, social media, public records, and specialized databases
- Advanced search techniques using operators, targeted queries, and search filters
- Assessing reliability: source, date, context, corroboration, and informational biases
- Traceable evidence collection, timestamping, preservation of evidence, and note-taking
- Hands-on workshop: developing a research plan and evaluating sources based on a corporate investigation scenario

[Day 2 – Morning]

Investigating Individuals and Digital Presence

- Searching for identities, aliases, and digital footprints in compliance with the legal framework
- Analysis of public profiles, relationships, posts, and contextual cues
- Correlating accessible identifiers, email addresses, images, and metadata
- Preventing misattribution and validating an identity through cross-referencing
- Factual reporting of results and distinction between observation, hypothesis, and conclusion

[Day 2 - Afternoon]

Investigation of organizations and associated risks

- Gathering information on an organization’s structure, activities, partners, and ecosystem
- Identification of public assets, exposed documents, data leaks, and risk indicators
- Analysis of a company’s digital footprint using public sources
- Assessing potential impacts on security, fraud, or incident response
- Hands-on workshop: Creating an OSINT profile of an organization and prioritizing findings based on their risk level

[Day 3 - Morning]

Mapping exposed infrastructure

- Fundamentals of DNS, domains, subdomains, IP addresses, and digital certificates
- Identifying public assets and understanding the relationships between services, hosting, and infrastructure
- Analyzing registration data, certificate logs, and routing information
- Correlating technical elements to identify a surface of exposure
- Limitations of technical attribution and precautions for interpretation in an OSINT report

[Day 3 - Afternoon]

Collection, processing, and basic automation

- Structuring collected data: formats, standardization, deduplication, and enrichment
- Utilizing metadata from publicly accessible documents, images, and content
- Principles of simple automation to accelerate the collection and processing of results
- Managing tool limitations, quality control, and traceability of processing
- Hands-on workshop: analyzing an OSINT dataset, extracting indicators, and producing a usable timeline

[Day 4 – Morning]

The Deep Web, Dark Web, and Threat Intelligence

- Distinction between the visible web, the deep web, and the dark web
- Principles for searching for exposed data, leaks, and mentions of organizations
- Assessing the credibility of information from restricted-access sources
- Identifying risks related to data exposure, malicious campaigns, and fraud
- Integrating OSINT findings into a threat intelligence framework

[Day 4 - Afternoon]

Operational Protection for Investigators

- Confidentiality, anonymity, and security challenges during online investigations
- OPSEC principles: compartmentalization, digital hygiene, research identity, and minimizing digital traces
- Managing the risks of contamination, targeting, and unintentional data exposure
- Selecting an isolated work environment and securing accounts used for research
- Hands-on Workshop: Designing an OPSEC framework tailored to a sensitive investigation and identifying key areas of concern

[Day 5 - Morning]

Analysis, Synthesis, and Intelligence Production

- Transforming collected data into verifiable and prioritized findings
- Correlation methods, analytical reasoning, and managing uncertainties
- Report preparation: scope, methodology, supporting evidence, analysis, and recommendations
- Tailoring the report for analysts, security teams, decision-makers, and stakeholders
- Targeted review of the competency areas required for the GIAC Open Source Intelligence exam

[Day 5 - Afternoon]

Final preparation for the certification exam

- Review of the exam format, time management, and effective reading of questions
- Organizing a review index and methodically utilizing authorized materials
- Answering strategies: elimination, prioritization, handling deferred questions, and final review
- Analysis of common errors in OSINT methodology, OPSEC, and the evaluation of results
- Hands-on workshop: solving a case study, justifying answers, and creating a personal review plan Staff

Target Companies

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 professional knowledge or modern methods.

Pre-training Assessment

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 in 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 running 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.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg