

GIAC Open Source Intelligence GOSI Exam Preparation Training Course

13 – 17 September 2027
Kuala Lumpur

AGILE LEADERS
Training Center

GIAC Open Source Intelligence GOSI Exam Preparation Training Course

Ref: 2223_262587 **Date:** 13 – 17 September 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

The GIAC Open Source Intelligence GOSI Exam Preparation Training Course is a one-week technical course designed for security analysts, threat researchers, and investigators seeking to build structured intelligence capabilities and prepare for the proctored exam. Practitioners often struggle to gather actionable external intelligence while maintaining rigorous operational security and adhering to data governance boundaries. The course addresses this through structured tradecraft spanning collection workflows, infrastructure analysis, and evidence management. The GIAC Open Source Intelligence GOSI Exam Preparation Training Course is delivered by Agile Leaders Training Center.

Who Should Attend

- Cyber threat intelligence analysts responsible for threat tracking, dark web collection, and incident indicators.
- Security operations and incident response specialists responsible for external asset exposure analysis and breach monitoring.
- Corporate investigators responsible for corporate entity analysis, fraud investigation, and background validation.
- Information security compliance officers responsible for aligning collection workflows with data privacy requirements.
- Law enforcement and forensic practitioners responsible for preserving evidentiary records from public electronic records.

The course assumes participants already conduct open-source investigations and basic network reconnaissance at work, leaving out foundational operating system administration and introductory networking concepts.

Departments and Industries

The course provides practical research workflows for specialists across diverse operating environments.

- Cyber Threat Intelligence and SOC Units in Banking and Financial Services
- Corporate Security and Fraud Prevention Units in Telecommunications
- Digital Forensics and Incident Response Teams in Energy and Critical Infrastructure
- Risk Management and Regulatory Compliance Departments in Aviation
- External Asset Defense Teams in Technology and Public Administration

Learning Objectives

By the end of this course, participants will be able to:

- Apply operational security controls, isolated environments, and sock puppets during online evidence collection.
- Analyze domain infrastructure, hosting metadata, and network assets using Censys, Shodan, and Amass.
- Evaluate person-of-interest indicators and breach datasets using structured collection tools and Hunchly verification.
- Diagnose corporate ownership structures, corporate affiliations, and third-party risk factors using open corporate registries.
- Prioritize threat intelligence indicators aligned with NCA ECC-2:2024 controls and SDAIA PDPL processing principles.
- Build an indexed reference binder and investigation procedure matching GOSI examination curriculum domains.

AGILE LEADERS
Training Center

Course Agenda

Day 1: OSINT Methodology and Operational Security

- Intelligence Cycle Fundamentals and Collection Planning Frameworks
- Virtual Machine Isolation and Hardware Fingerprint Obfuscation
- Investigative Account Persona Creation and Sock Puppet Maintenance
- SDAIA PDPL Compliance Assessment for Public Data Harvesting
- Anti-Cyber Crime Law Royal Decree M/17 Boundary Analysis

Day 2: Search Workflows, Data Extraction, and Evidence Preservation

- Advanced Web Search Operators and Cache Index Exploitation
- Automated Web Scraping Scripts using Python Extraction Routines
- Evidence Hashing, Chain of Custody, and Hunchly Case Capture
- Decentralized and Historical Archiving via WayBack Machine and Archive Today
- Obsidian Knowledge Graph Construction for Investigative Linking

Day 3: People Tracing, Social Networks, and Dark Web Collection

- Social Media Intelligence Extraction Across Multi-Platform Target Profiles
- Username, Handle, and Image Reverse-Lookup Verification Workflows
- Compromised Credential and Data Breach Repository Analysis
- Tor Onion Routing Network Navigation and Hidden Service Scraping
- Breach Intelligence Handling under NCA ECC Control 2-13-3-5

Day 4: Network Infrastructure and Corporate Entity Analysis

- Domain Name System Records and Reverse Whois Attribution Techniques
- Internet-Connected Device Asset Discovery via Censys and Shodan
- Attack Surface Mapping using OWASP Amass Frameworks
- Commercial Registry Enumeration and Cross-Border Beneficial Ownership
- Threat Sharing Notification Preparation under NCA ECC Control 2-13-3-4

Day 5: Examination Simulation and Investigation Capstone

- Exercise: Deploying Isolated Collection Workflows and Sock Puppets
- Exercise: Multi-Platform Entity Attribution and Evidence Preservation
- Exercise: Network Exposure Mapping and Third-Party Risk Profiling
- Exercise: Simulated 75-Question GOSI Objective Timed Practice Assessment
- Capstone Exercise: End-to-End Threat Attribution and Compliant Intelligence Dossier

Practical Exercises

The course includes structured practical activities designed to simulate realistic analytical workflows.

- **Persona and Environment Hardening:** Configure an isolated investigation browser environment and generate a managed sock puppet identity as a suggested activity.
- **Digital Asset Enumeration:** Execute domain mapping and service identification across simulated target infrastructure using Censys and Amass as a suggested activity.
- **Compliant Evidence Dossier:** Extract, verify, and preserve online target artifacts into Hunchly and Obsidian while validating compliance requirements as a suggested activity.

FAQs

Who suits the GIAC Open Source Intelligence GOSI Exam Preparation Training Course and what are the prerequisites?

The course suits cybersecurity professionals, threat analysts, and investigators tasked with external intelligence operations. Participants should have practical familiarity with basic internet protocols and foundational digital investigation concepts before enrolling.

How does this course differ from general intelligence analysis courses?

This course focuses on practical digital intelligence tradecraft, online persona protection, technical reconnaissance tools, and specific preparation for the 75-question proctored GOSI objective assessment, rather than high-level strategic intelligence theories.

What materials can be referenced during the GOSI examination attempt?

GIAC examinations allow physical printed materials, including printed notes and course indexes, but strictly prohibit electronic storage devices, digital index search tools, and live internet access during the testing session.

How does the course address local data privacy laws during open source collection?

The course incorporates legal collection principles aligned with the SDAIA Personal Data Protection Law and the Anti-Cyber Crime Law Royal Decree No. M/17 to ensure compliant intelligence processing.

What tools are practiced during the technical investigation modules?

Participants practice with operational security tools, Hunchly, Obsidian, Shodan, Censys, Amass, Python scraping scripts, Tor browser environments, and multi-source public repository platforms.

Conclusion

Participants complete the course with an indexed technical investigation binder and an evidence verification portfolio designed for operational intelligence units. This structured documentation provides standard operating procedures that improve investigation speed, chain of custody defensibility, and regulatory compliance across threat investigations. Organizations gain reliable external intelligence collection capabilities while mitigating organizational risk during intelligence-gathering tasks.