# SEC450: AI-Enabled Security Operations: Hands-on Investigation, Detection, and Automation™

GSOC Security Operations Certified giac.org/gsoc

5 Day Program | 30 CPEs | Laptop Required

## You Will Be Able To

- Define SOC mission and scope so analysts focus on what matters most
- Use threat intel to prioritize threats and sharpen triage decisions
- Analyze network, endpoint, email, and file evidence across the SOC toolset
- Separate observed facts from assumptions and AI-generated inferences
- Apply structured methods like ACH to reduce bias in investigations
- Write, test, and document detections using Sigma and YARA concepts
- Evaluate agentic AI workflows for prompt-injection risk and approval gates

## Business Takeaways

- Sharper triage and evidence review mean analysts spend more time on real threats
- Get more value from SIEM, EDR/XDR, threat intel, and automation working together
- Speed up investigations with AI while preserving evidence and human decisions
- Turn investigation findings into tested, documented detections with Sigma/YARA
- Adopt AI with real controls: approval gates, audit trails, and least privilege
- Reduce analyst toil and burnout with better handoffs and documentation
- Build a team ready to oversee agentic AI and make defensible SOC decisions

GSOC Security Operations Certified giac.org/gsoc

## GIAC Security Operations Certified

The GIAC Security Operations Certified (GSOC) certification validates a practitioner's ability to defend an enterprise using essential blue team incident response tools and techniques. GSOC certification holders are prepared to run a security operations center (SOC) equipped with the practical technical knowledge and key advanced concepts essential for operating a modern, effective cyber defense team.

## A Practical SOC Analyst Course Built for the AI Era

Security Operations Centers are under pressure from growing telemetry volume, more complex attacks, constant alert noise, and increasing expectations for speed. At the same time, AI-assisted tools and agentic workflows are becoming part of the SOC toolset. Analysts need to understand what these systems can do, where they fit, where they fail, and how to keep human judgment at the right decision points.

This course teaches SOC analysis as an end-to-end operational discipline. Students start with the mission and scope of the SOC, then learn how to use security tools, threat intelligence, network evidence, endpoint logs, email artifacts, file and malware indicators, structured investigation methods, and detection engineering to reach defensible conclusions. Along the way, they learn how to use AI effectively for summarization, triage, enrichment, drafting, detection support, and automation without confusing generated output for evidence.

Students will work through realistic SOC workflows that connect alerts to action: collecting evidence, enriching context, building hypotheses, reducing false positives, writing and testing detections, documenting investigations, and deciding when to escalate. The course also covers agentic AI concepts, tool use, automation design, prompt-injection risk, approval gates, audit trails, and analyst sustainability.

By the end of the course, students will be better prepared to operate in modern SOCs where human analysts, security platforms, automation, and AI-enabled systems work together. The focus is practical: use the tools, validate the evidence, make better decisions, and help the organization reduce risk.

## What Is AI-Enabled Security Operations And Why Is It Important?

This is a practical SOC analyst course for the AI era. It does not treat AI as a replacement for analysts, and it does not teach AI as a standalone novelty. Instead, it teaches students how modern SOC work actually gets done: by combining mission clarity, evidence discipline, threat-informed prioritization, detection engineering, automation, AI-assisted workflows, and human judgment.

## How Will This Course Benefit My Career?

SEC450 is designed to build job-ready skills for those entering or advancing in defensive cybersecurity roles. Key career benefits are:

- **Hands-On SOC Skills:** Learn log analysis, SIEM operations, and incident triage, the core skills needed for Tier 1 and Tier 2 SOC analyst roles.
- **Career Acceleration:** Ideal for transitioning into cyber defense or strengthening early blue team experience.
- **GIAC Certification (GSOC):** Earn an industry-recognized credential that validates your ability to operate in real-world security environments.
- **Professional Network:** Connect with instructors and peers through SANS's global cybersecurity community.
- **Path to Advancement:** Builds a foundation for higher-level courses like SEC511 (Continuous Monitoring) and SEC555 (Detection Engineering).

**BOTTOM LINE:** SEC450 equips you with the practical knowledge, certification, and connections to launch or accelerate a career in blue team cybersecurity.

# Section Descriptions

### SECTION 1: Building the AI-Enabled SOC: Mission, Intelligence, Tools, and Workflow

Section 1 starts by defining the SOC's mission and toolset, then learn how CTI sharpens prioritization and how to build a threat-informed defense. You'll also get hands-on with AI fundamentals, from safe prompting to verifying AI-generated output before it becomes part of a case.

**TOPICS:**

- Course Framing, SOC Mission, and Scope
- SOC Tool Landscape
- CTI for Prioritization and Context
- Building a Threat-Informed Defense
- AI Basics, Usage, and the Analyst Workflow

### SECTION 2: Network Evidence and Agentic Enrichment: Protocols, OPSEC, and Tool Use

Section 2 builds the network evidence skills every SOC analyst needs: DNS, HTTP, and TLS traffic analysis, plus OPSEC considerations that keep your own investigation from creating risk. You'll also start applying agentic AI concepts, tool use, and iteration to enrich alerts faster.

**TOPICS:**

- Network Protocol Fundamentals: DNS, HTTPS, TLS, and more
- OPSEC
- Alert Enrichment and Evidence Quality
- Agentic AI Concepts: Planning, Tool Use, and Iteration
- Tools and Tool Use

### SECTION 3: From Telemetry to Investigation: Triage, Structured Analysis, and Agentic Automation

Section 3 moves from raw telemetry to real investigations. Collect and interpret host, endpoint, and cloud evidence, apply structured analytical techniques to reduce bias, and use automation and agent-based workflows to triage alerts and build phishing-triage pipelines.

**TOPICS:**

- Host, Endpoint, and Cloud Telemetry Collection and Formats
- Triage and Investigation Mindset, Process, and Techniques
- Structured Analytical Techniques
- Automation, Agent Configuration, Context, and Usage
- Alert Triage and Event Collection

### SECTION 4: From Phishing to Detection: Email, Malware Analysis, YARA-X, and Sigma

Section 4 goes deep on phishing and malware: analyze email headers, dissect weaponized file types, and learn malware analysis foundations. Then translate what you find into tested detection logic using YARA-X for files and Sigma for log-based detections.

**TOPICS:**

- Malicious Email Prevention and Spoofing
- File and Malware Analysis Foundations and Weaponized File Types
- Detection Engineering Concepts
- File and Malware Detection with YARA-X
- Log-Based Detection with Sigma

### SECTION 5: Operating the AI-Enabled SOC: Risk, Judgment, and Sustainable Performance

Section 5 finishes up by examining AI trust and risk, the analyst's evolving role in AI-enabled SOCs, and practices that reduce burnout and support career growth. The course ends with a capstone incident that pulls every skill from the course together.

**TOPICS:**

- AI Trust and Risk
- Analyst Role in AI-Enabled SOCs
- Burnout Reduction for Security Operations Teams
- Career Growth
- SEC450 Capstone Exercise

**"So far, SEC450 not only meets but goes beyond my expectations. One year ago I became a SOC team lead and this course adds to my knowledge and puts a more structured approach on what a SOC I am running should look like."**

—Radek Ochrymowicz, **Frontex**

## Who Should Attend

This course is designed for security professionals who work in or support security operations:

- SOC analysts and intrusion detection analysts
- Cyber defense analysts moving beyond basic alert handling
- Incident handlers building stronger triage, evidence, and documentation skills
- Detection engineers who want more operational context for rule development and tuning
- Security engineers supporting SIEM, EDR/XDR, SOAR, case management, and AI-enabled SOC tooling
- Threat intelligence analysts connecting CTI more directly to SOC prioritization
- SOC leads or managers who need to understand how AI, automation, and analyst process fit together

## NICE Framework Work Roles

- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

## What Are the Prerequisites for This Course?

SEC450 is part of the Cyber Defense curriculum.

Depending on your current or desired future role, one of these courses is a great next step in your cybersecurity journey:

**SOC Analyst**

- SEC503: Network Monitoring and Threat Detection In-Depth
- SEC504: Hacker Tools, Techniques, and Incident Handling

**Security Architect or Engineer**

- SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring
- SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

**SOC Lead or Manager**

- LDR551: Building and Leading Security Operations Centers
- LDR512: Security Leadership Essentials for Managers