SEC450

SOC ANALYST TRAINING – APPLIED SKILLS FOR CYBER DEFENSE OPERATIONS

In today's fast-moving threat environment, Security Operations Centers (SOCs) are on the front lines—tasked with identifying, analyzing, and responding to a constant stream of cyber threats. SEC450 equips analysts with the hands-on skills, modern tools, and practical knowledge needed to operate confidently in real-world SOCs, covering everything from threat detection and log analysis to AI integration and automation. With most SOC teams operating lean and overwhelmed by alert volume, this course also addresses the rising need for smarter workflows, adaptive automation, and sustainable analyst development to help reduce burnout and improve effectiveness across the board.

42% of SOCs are using AI/ML tools out of the box with no customization—and they remain among the lowest-rated technologies due to poor integration and unclear ownership. SEC450 addresses this gap head-on with practical instruction on how to thoughtfully incorporate AI, LLMs, and agents into everyday SOC workflows.

***Source: 2025 SANS SOC Survey**

Summer 2025 Update

This major update brings the largest refresh to SEC450 yet, with a sharp focus on modern SOC operations and the growing role of AI in cyber defense. New modules explore topics like AI-driven analysis, threat-informed defense, phishing detection, and cloud logging. The update also adds six new hands-on labs that cover detection engineering, malware analysis, and task automation, giving analysts practical skills to handle today's threats with modern tools and approaches.

NEW CONTENT

- Brand new modules covering:
  - AI, LLMs, and Agents in the SOC
  - Building a threat-informed defensive posture
  - YARA-X for file-based threat detection
  - Sigma for log-based threat detection
  - Logging in AWS, Azure, and Microsoft 365
  - Modern phishing prevention and detection techniques
  - The SOC mission and aligning security efforts with business goals

LAB REFRESH

- 6 new labs added, bringing the total to 22 hands-on labs
  - AI use in the SOC
  - YARA-X signature writing
  - Sigma-based detection
  - Static and sandbox malware analysis
  - Phishing document reverse engineering
  - automation with the n8n platform
- AI-enhanced tasks now integrated into relevant labs to highlight real-world LLM use cases

UPDATED FEATURES

- Existing content has been clarified and refined for clarity and relevance
- Virtual Machine upgrades include:
  - Ollama and multiple local LLMs
  - OpenWebUI for interacting with both local and external LLMs
  - Expanded malware analysis toolset

"AI can relieve pressure by turning repetitive triage into strategic, feedback-driven work—giving analysts room to grow instead of burn out." - SEC450 course author John Hubbard

For more information:
sans.org/SEC450

SANS | GIAC CERTIFICATIONS