SEC501

Applied Cyber Defense

Major Update: Investigation-Driven Applied Cyber Defense

SEC501 prepares experienced technologists to investigate modern enterprise attacks that span systems, teams, cloud services, and providers. Through 26 hands-on labs, students build the technical judgment to correlate evidence, establish incident scope, validate detections, and make confident response decisions across today's hybrid environments.

"In **75% of incidents**, critical evidence of the initial intrusion was present in the logs. Yet, due to complex, disjointed systems, that information wasn't readily accessible or effectively operationalized." (Source: Palo Alto Networks Unit 42 Global Incident Response Report 2025)

2026 Major Update: SEC501 has been reimagined around a continuous enterprise investigation that teaches students how to follow suspicious activity across networks, endpoints, cloud services, SaaS platforms, and third-party providers. The update introduces an integrated investigative storyline, expanded coverage of AI-assisted operations and provider-held records, refreshed hands-on labs, and new decision-focused exercises that reflect how modern incident response teams investigate today's attacks.

6 Days | 38 CPEs | In-Person, Virtual, or Self-Paced

New Content

- Correlating records across cloud, SaaS, MSSP, and enterprise systems
- Investigating AI agent activity and unapproved system changes
- Verifying AI-assisted analysis and handoffs against primary evidence
- Expanded software supply chain and provider-managed service investigations
- Ransomware investigation, including timeline reconstruction and encryption analysis
- Evidence validation and incident scoping under uncertainty

Updated Features

- Course redesigned around a single end-to-end investigation instead of isolated technical domains
- 26 integrated labs reinforce how visibility, detection, hardening, incident response, and malware analysis work together
- Modern enterprise scenarios reflect today's hybrid infrastructure and distributed security operations
- Stronger emphasis on validating evidence before escalation, containment, and recovery decisions
- Updated capstone reinforces real-world investigative workflows across multiple security disciplines

Lab Refresh

- Network architecture labs now establish investigative baselines and validate audit evidence
- Detection labs connect packet analysis, SIEM correlation, Zeek, and Suricata to real incident investigations
- Hardening labs validate exposure, configuration drift, identity risk, and controlled remediation
- DFIR labs expand incident scoping, ransomware analysis, evidence recovery, and response decision-making
- Malware analysis now directly informs enterprise detection, containment, and recovery activities
- Capstone challenges require students to correlate evidence across multiple systems to determine scope and prioritize response

For more information: sans.org/SEC501

SANS | GIAC CERTIFICATIONS