SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC450:™ SOC Analyst Training – Applied Skills for Cyber Defense Operations™

GSOC
Security Operations Certified
giac.org/gsoc

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Make the most of security telemetry including endpoint, network, application, and cloud-based data
- Identify the best opportunities to make your team more efficient, utilizing scripts, SOAR, and AI agents
- Keep your security operations tempo on track with in-depth discussions on what a SOC or security operations team should be doing at every step from security monitoring to detection, triage, analysis, and beyond
- Quickly identify the separate typical commodity attack alerts from high-risk, high-impact advanced attacks, and how to do careful, thorough, and cognitive-bias free security incident analysis
- Give detailed explanations, processes, and techniques to reduce false positives to a minimum
- Demonstrate how to collect, organize, and use relevant threat data in a threat intelligence platform (TIP); principles of success for endpoint security data collection whether you use a SIEM, EDR, NDR, or XDR; how to quickly and accurately triage security incidents; crafting generative AI-powered automation workflows for common SOC activities; and how to best use case management systems to effectively analyze, document, track, and extract critical metrics from your security incidents

> **“SEC450 was an excellent insight into the tasks of a SOC. Not only did it have actionable lessons on the tools and techniques needed to run a SOC, but also gave insight on ways to improve the operations of the team.”**
>
> —Nathan H.

If you’re looking for the gold standard in SOC analyst training, you’ve found it. SANS SEC450™ transforms reactive analysts into expert threat hunters who catch sophisticated attacks others miss. Unlike other courses, SEC450™ has the depth to and hands-on content to teach you to think and investigate like an elite analyst using 22 hands-on labs using in a realistic SOC environment.

Designed for SOC analysts from organizations of all sizes, SEC450™ will get you hands-on with the tools and techniques required to stop advanced cyberattacks! Whether you are a part of a full SOC in a large organization, a small security ops group, or an MSSP responsible for protecting customers, SEC450™ will teach you and your team the critical skills for understanding how to defend a modern organization, including how to get the most out of the new capabilities provided by generative AI.

Transform overwhelmed analysts into confident threat hunters who identify compromise before it becomes a breach. Master advanced network traffic analysis, malware investigation, and the structured hunting techniques that separate elite defenders from those drowning in alerts. Learn detection engineering that actually works and investigation methods that catch sophisticated attacks automated tools miss.

SEC450™ covers the complete spectrum from strategic SOC operations and threat intelligence to hands-on packet analysis and malware dissection. You’ll work with fully integrated set of SOC tools configured exactly how they operate in production environments. Every technique directly translates to your workplace because it’s based on real SOC operations at enterprise scale. The course culminates in an intensive capture-the-flag competition where you’ll prove you can apply these advanced techniques under pressure—exactly what real SOC operations demand.

Hands-On SOC Analyst Training

This course delivers 22 hands-on labs that put you directly into realistic SOC scenarios to get interactively learning and using the real tools of the trade. Your virtual environment mirrors a real SOC with integrated SIEM, threat intelligence platforms, incident management systems, SOAR tools, full packet capture tools, and a toolkit of command-line tools that analysts use daily. Everything is pre-configured and ready to go so you can jump in to the workflow and gain skills that transfer immediately to your workplace.

You’ll tackle real-world challenges through practical exercises: analyzing HTTP, DNS, and email-based attacks, hunting for post-exploitation activity, and performing high-quality investigations under realistic constraints. The labs teach you to identify high-risk alerts quickly, understand how logs flow through detection pipelines, and get hands-on with tools to create detection rules for files and logs that actually work in production. By course end, you’ll have hands-on experience with the integrated tool workflows that separate effective SOCs from those drowning in alert fatigue—experience you can apply the moment you return to your own environment.

SEC450™ takes the approach of not just teaching what to do, but also why these techniques work. Unlike shorter security analyst training courses, SEC450™ has the time to cover the deeper reasoning and principles behind successful cyber defense strategies, ensuring students can apply the concepts beyond the class material and bring a successful defensive mindset back to their teams and organizations. Don’t just take our word for it, ask any of our thousands of course alumni and GIAC GSOC certified analysts!

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Blue Team Tools and Operations

Section 1 lays the groundwork for SOC analysts, covering threat models, analyst workflows, and key tools like SIEM and SOAR. It closes with how to apply generative AI in security operations, from improving documentation and analysis to understanding AI-driven threats and tools—preparing you for the future of AI in cyber defense.

TOPICS: Foundations of Security Operations; Cyber Threat Intelligence (CTI) and Building a Threat-Informed Defense; SOC Data and Tools; Generative AI for the SOC

SECTION 2: Understanding Your Network

Section 2 dives into network-based threat hunting. Learn to use routers, firewalls, flow logs, and full packet capture to track attacker activity. You'll analyze DNS, HTTP, and TLS traffic, spot encrypted threats without decryption, and explore post-exploitation protocols—building skills to detect threats others overlook.

TOPICS: Network Visibility & Traffic Analysis; DNS Monitoring & Threat Detection; HTTP Traffic Dissection; Encrypted Traffic Analysis; Post-Exploitation Protocols

SECTION 3: Understanding Endpoints, Logs, and Files

Section 3 builds your skills in log analysis and malware fundamentals. You'll learn to craft SIEM queries, visualize data, and spot attacker activity across Windows, Linux, and cloud logs. Then, dive into malware handling, static analysis, IOC extraction, and sandboxing to uncover threats hiding in weaponized files and complex data.

TOPICS: Deep Dive on SIEM for Threat Detection; How Windows and Linux Logging Works; Key Log Events for Threat Detection and How to Interpret Them; Cloud Logging; Malware Analysis Fundamentals

SECTION 4: Triage and Analysis

Section 4 builds expertise in phishing investigations and structured analysis. Learn to detect spoofed emails, block malicious links, and investigate BEC and MFA bypasses. Then sharpen your triage and decision-making with OPSEC best practices and structured techniques to reduce bias, prioritize alerts, and analyze threats with clarity under pressure.

TOPICS: Phishing Prevention; How to Investigate Common Phishing Techniques; Alert Triage and Prioritization; Structured Analysis Techniques; Operational Security (OPSEC) for SOC Analysts

SECTION 5: Continuous Improvement, Analytics, and Automation

Section 5 takes you from analyst to detection engineer. Learn to craft high-fidelity detections with tools like YARA-X and Sigma, reduce false positives, and tune alerts effectively. Explore where automation helps or hurts, assess investigation quality, and build sustainable skills to grow your cybersecurity career without burning out.

TOPICS: Detection Engineering; Alert Tuning and False Positive Reduction; Automation and Orchestration; Investigation Quality; How to Avoid Burnout for SOC Analysts

SECTION 6: Capstone: Defend the Flag

The course ends with a high-stakes, team-based capture the flag challenge. Using real network data in a simulated attack, you'll race to detect and analyze threats across multiple scenarios. It's a full day of hands-on problem solving that tests your ability to perform advanced threat hunting under real-world pressure.

Business Takeaways

- **Stop Missing Real Threats—**Your analysts will master advanced detection techniques that catch sophisticated attacks others miss, including network-based hunting, malware analysis, and structured investigation methods that quickly and accurately identify compromise.
- **Eliminate Alert Fatigue—**Learn proven detection engineering and tuning strategies that dramatically reduce false positives while maintaining security coverage, allowing your team to focus on actual threats.
- **Maximize Your Security Technology Investment—**Get full value from your SIEM, XDR, EDR, and threat intelligence platforms through proper integration, advanced query techniques, and workflow optimization that most organizations never achieve.
- **Accelerate Incident Response—**Implement structured triage processes, quality investigation frameworks, and AI-powered automation that cut response times and improve accuracy under pressure.
- **Build Sustainable Operations—**Develop your team's expertise in the advanced skills that prevent burnout, reduce turnover, and create the high-performing SOC analysts every organization struggles to find and retain.

Key Career Benefits

- **Hands-on SOC Skills—**Learn log analysis, SIEM operations, and incident triage—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)

Who Should Attend

- Security analysts
- Incident investigators
- Security engineers and architects
- Technical security managers
- SOC managers looking to gain additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC
- Anyone looking to start their career on the blue team

NICE Framework Work Roles

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

> **"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**

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-certified professionals are well-versed in the technical knowledge and key concepts needed to run a security operations center (SOC).