SEC450: Blue Team Fundamentals: Security Operations and Analysis

GSOC Security Operations Certified
giac.org/gsoc

6 Day Program | 36 CPEs | Laptop Required

Business Takeaways

This course will provide:

- A turn-key solution for SOC analyst training needs—giving analysts the skills they need to understand the tools, data, and defensive priorities required to defend your network from high-impact cyber attacks
- How to derive clear strategic priorities for your security operations team
- Show you how to make the most of security telemetry including endpoint, network, and cloud-based sensors
- A battle-tested method to reduce false positives to the lowest possible level
- The techniques for quick and accurate security incident triage
- The methods to improve the effectiveness, efficiency, and impact of your SOC

Why Choose SANS SEC450 Over the Competition?

Unmatched in the industry with its volume and depth, SEC450 includes:

- 1300 pages of instructional content and labs with extensive notes and documentation
- 20 hands-on exercises putting real SOC tools and situations in front of students to emphasize lessons with a virtual workbook containing extra challenges to test your understanding of the material
- A custom course Linux virtual machine filled with real SOC tools
- A capture-the-flag contest experience for students to apply their new knowledge and put their analysis skills to the test!
- Continuously updated material to cover the newest attackers and techniques

This depth of material makes SEC450 and the GSOC certification a cyber security analyst training class like no other, covering techniques, mindset, and tools at a level unmatched by other offerings. Whether you're taking SEC450 yourself or including it in your analyst training plan, we'd love to have you and your org join the growing list of alumni and GSOC certified security analysts helping to halt the flow of disruptive cyberattacks!

SEC450 is a course designed from the ground up to be the most comprehensive Security Operations Center (SOC) analyst training course available. If you are working in cyber defense operations, building a SOC, or want to improve the SOC you already have with better data, workflow, and analysis technique, SEC450 is the course for you! By providing a detailed explanation of the mission and mindset of a modern cyber defense operation, this course will jumpstart and empower those on their way to becoming the next generation of Blue Team members. With six days of training, six course books, 20 hands-on labs, and an all-day Defend-the-Flag Capstone competition, there is simply no other offering on the market as complete as SEC450 for SOC and security analyst training.

If you're looking for the gold standard in cybersecurity analyst training, you've found it! SANS SEC450 and the accompanying GIAC GSOC certification are the premier pairing for anyone looking for a comprehensive security operations training course and certification. Check out the extensive syllabus and description below for a detailed run-down of course content.

Designed for teams of all types, SEC450 will get you hands-on with the tools and techniques required to quickly detect and halt advanced cyberattacks! Whether you are part of a full SOC in a large enterprise, a small security ops group, or an MSSP protecting your customers, SEC450 will teach you and your team the critical skills for understanding how to defend a modern organization.

SEC450 is authored, designed, and advised by a group of veteran SOC analysts and managers to be a one-stop shop for all the essential techniques, tools, and data your team will need to be effective, including:

- **Security Data Collection –** How to make the most of security telemetry including endpoint, network, and cloud-based sensors
- **Automation –** How to identify the best opportunities for SOAR platform and other script-based automation
- **Efficient Security Process –** How to 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 data generation to detection, triage, analysis, and incident response
- **Quality Triage and Analysis –** How to quickly identify and 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
- **False Positive Reduction –** Detailed explanations, processes, and techniques to reduce false positives to a minimum
- **SOC Tools –** Includes hands-on exercises
- **Burnout and Turnover Reduction –** Informed with both scientific research and years of personal experience, this class teaches what causes cyber security analyst burnout and how you and your team can avoid it by understanding the causes and factors that lead to burnout. This class will help you build a long-term sustainable cyber defense career so you and your team can deliver the best every day!
- **Certification –** The ability to add on the GIAC GSOC certification that encourages students to retain the material over the long term, and helps you objectively demonstrate you and your team's level of skill

SEC450 takes the approach of not just teaching what to do, but also why these techniques work and encourages students to ask the critical question "How can we objectively measure that security is improving?" And 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 even beyond the class material to take their defensive skills and thinking to the next level. Don't just take our word for it, ask any of the course alumni! SEC450 instructors repeatedly see the long lists of improvement ideas students finish the class with, eager to bring them back to their organizations.

Section Descriptions

SECTION 1: Security Operations Teams, Tools, And Mission Overview

The course begins with laying the all-important foundations of a security team—understanding the mission of your SOC through the context of your organization and the external threat landscape. No matter where you are starting, SEC450 emphasizes the big-picture thinking on how to strategize and prioritize SOC processes and data to best detect and half high-impact cyberattacks. This section of the course teaches these concepts from the top down, ensuring students understand the mindset of an analyst, the required workflow, and the monitoring tools used in the battle against attackers. Throughout this section, students learn how monitoring data and security tools fit together (including incident management systems, threat intelligence platforms, SIEMs, and more) and see how to best integrate these tools into a seamless workflow that allows alert triage and response to flow smoothly.

TOPICS: Welcome to the Blue Team; SOC Foundations; SOC Organization and Functions; SOC Data Collection; An Introduction to SIEM; Building SIEM Queries; SIEM Visualizations and Dashboards; Knowing Your Enemy; Threat Intelligence Platforms; Alert Generation and Processing; Incident Management Systems and SOAR

SECTION 2: Network Traffic Analysis

Section 2 begins the journey of building a deep understanding of your network. To defend a network, you must thoroughly comprehend its architecture and the impact that it will have on analysis. After discussing network visibility points, zones, traffic capture types, and how your network setup will drive the speed at which your SOC will need to be able to respond, section 2 then goes in-depth on common network services. These sections provide a thorough explanation of the current and upcoming features of DNS, HTTP (versions 1.1, 2 and 3), TLS, and more, with a focus on the most important points security professionals need to understand. In each section there is a focus on what normal data looks like, as well as the common fields and areas that are used to spot anomalous behavior. This section's goal is to give analysts the ability to quickly recognize common tricks used by attackers to turn these everyday services against us.

TOPICS: Network Architecture; Traffic Capture and Analysis; Understanding DNS; DNS Analysis and Attacks; Understanding HTTP; HTTP(S) Analysis and Attacks; How HTTP/2 and HTTP/3 Work; Analyzing Encrypted Traffic for Suspicious Activity; Common Protocols for Post-Exploitation

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

SECTION 3: Endpoint Defense, Security Logging, and Malware Identification Overview

Section 3 opens with a discussion and demonstration of common endpoint attack techniques and the security controls and features organizations can use to disrupt and detect them. This includes an in-depth overview of how security logging is set up on Linux and Windows, and the decisions that will drive whether you are able to collect the logs needed to spot attacks. This section also covers practical concerns about the quality of your telemetry and how to ensure that your logs come with the context, categorization, and normalization required for analysts to make quick sense of them. Many new analysts struggle to understand how files are structured at a low level and therefore are hesitant when it comes to answering questions such as "could a file of type x be used for evil?" The second part of Section 3 provides students with the concepts needed to reason through the answer, diving into files at the byte level. Students finish this day understanding how different common file formats can be identified, how they are typically weaponized, and how to quickly decide whether a given sample is likely to be malicious.

TOPICS: Common Endpoint Attack Tactics; Endpoint Defense in Depth; How Windows Logging Works; How Linux Logging Works; Interpreting Security-Critical Log Events; Making Logs Usable – Log Collection, Parsing, and Normalization; Identifying Potentially Malicious Files; Dissecting Commonly Weaponized File Types; Fast Identification and Safe Handling of Malicious Files

SECTION 4: Efficient Alert Triage and Email Analysis

In this section of the course, we turn our focus to understanding and mastering the process of analysis with a focus on how to avoid common mistakes and biases. The section teaches a clear and methodical approach for alert triage and how to quickly sort opportunistic from potentially targeted attacks. In addition to analysis technique, this section covers both offensive and defensive mental models that are necessary to understand to perform high-quality analysis. Students will use these models to look at an alert queue and get a quick and intuitive understanding of which alerts may pose the biggest threat and need priority in investigation. It also covers cyber defense operational security (OPSEC) and safe investigation techniques to ensure that analysts do not tip their hand to attackers during the investigation process. In the final section of this day, phishing email investigation is covered in depth. With email being a primary entry vector for intrusions, it's incredibly important that analysts are confident in understanding multiple ways to detect the signs of a malicious email. Email header analysis is and verification protocols (SPF, DKIM, and DMARC) are explained in detail with the goal of teaching analysts how to quickly identify and dispose of clearly malicious and spoofed email. In addition, safe investigation of attached files, URLs, and email content is also covered so that analysts are ready for anything when it comes to the phishing triage inbox.

TOPICS: Alert Triage and Analysis; Structured Analytical Techniques for Alert Investigation; The Most Important Mentals Models for Security Analysts; Incident Documentation, Closing and Investigation Quality; Analysis Operational Security for Defenders – How to Not Tip Off Attackers of Defense Action; Detecting Malicious Emails through Email Header Analysis (SPF, DKIM, DMARC and more); Email Content, URL, and Attachment Analysis

SECTION 5: Continuous Improvement, Analytics, and Automation

Section 5 targets improving efficiency and team enthusiasm for SOC work by tackling the most common problems head-on. Through process optimization, careful analytic design and tuning, and workflow efficiency improvements, we can eliminate many of these common pain points. This frees us from the repetitive work we loathe and allows us to focus on what we do best—analysis! Having the time for challenging and novel work leads to a virtuous cycle of growth and engagement throughout the SOC—and improves everyone's life in the process. This section will focus on tuning your tools using clever analysis techniques and process automation to remove the monotonous and non-value-added activities from your day. It also covers containment activities including the containment techniques teams can use, and how to decide which option is best to halt a developing incident or infection. We'll wrap up the day with recommendations on skill growth, long-term career development, and how to get more involved in the cyber defense community.

TOPICS: Reducing Burnout and Retention Issues in the SOC; False Positive Reduction – Analytic Features and the Importance of Log Enrichment; New Analytic Design, Testing, and Sharing; Alert Tuning Methodology; SOC Automation and Orchestration (with and without SOAR); Improving Analyst Efficiency and Workflow; Methods for Quickly Containing Identified Intrusions; Skill and Career Development for SOC Staff

SECTION 6: Capstone: Defend the Flag

The course culminates in a day-long, team-based capture-the-flag competition. Using network data and logs from a simulated network under attack, Section 6 provides a full day of hands-on work applying the principles taught throughout the week. Your team will be challenged to detect and identify attacks to progress through multiple categories of questions designed to ensure mastery of the concepts and data covered during the course.

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).