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

GIAC CERTIFICATIONS

SEC450: Blue Team Fundamentals: Security Operations and Analysis

6	36	Laptop
Day Program	CPEs	Required

Business Takeaways

This course will help your organization:

- Make the most of security telemetry including endpoint, network, and cloud-based sensors
- Reduce false positives to a minimum
- Quickly and accurately triage security incidents
- Improve the effectiveness, efficiency, and success of your SOC

Why Choose SANS SEC450 Over the Competition?

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

- Nearly 1000 pages of instructional content with extensive notes and documentation
- 15 hands-on exercises putting real SOC tools and situations in front of students to emphasize lessons and a 400+ page in-depth instructional exercise workbook to go with them
- Full lab walkthrough videos, recorded and explained step by step by the course author
- A custom course Linux virtual machine filled with SOC tools
- A full day capture-the-flag contest experience with 75 challenges where students will apply their learning and put their 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!

If you're looking for the gold standard in cyber security analyst training, you've found it! SANS SEC450 and the accompanying GIAC GSOC certification are the premier pair 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 and don't miss the free demo available by clicking the "Course Demo" button!

Designed for teams of all types, 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.

Designed By Security Analysts, For Security Analysts

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: Blue Team Tools and Operations

This section starts with an introduction to the blue team, the mission of a Security Operations Center (SOC), and how to understand an organization's threat model and risk appetite. It is focused on top-down learning to explain the mindset of an analyst, the workflow, and monitoring tools used in the battle against attackers. Throughout this course section, students will learn how SOC information management tools fit together, including incident management systems, threat intelligence platforms, SIEMs, and SOAR tools. We end the section describing the various groups of attackers, how their methods differ, and their motivations.

TOPICS: Introduction to the Blue Team Mission; SOC Overview; Defensible Network Concepts; Events, Alerts, Anomalies, and Incidents; Incident Management Systems; Threat Intelligence Platforms; SIEM; Automation and Orchestration; Who Are Your Enemies?

SECTION 2: Understanding Your Network

Section 2 begins the technical journey of understanding the environment. To defend a network, you must thoroughly understand its architecture and the impact that it will have on analysis. This day introduces the concepts of a modern organization's network traffic flow by dissecting a basic home Internet connection and describing the features necessary for segmentation and monitoring. These modules ensure that students have a firm grasp on how network design affects their "view of the world" as an analyst. We then go in-depth on common network services. Section 2 provides thorough working explanations of the current and upcoming features of DNS, HTTP(S), SMTP, and more, with a focus on the most important points for analysts to understand. These sections explain what normal data look like, as well as the common fields and areas that are used to spot anomalous behavior. The focus will be on quickly recognizing the common tricks used by attackers to turn these everyday services against us.

TOPICS: Corporate Network Architecture; Traffic Capture and Visibility; Understanding DNS; DNS Analysis and Attacks; Understanding HTTP and HTTPS; Analyzing HTTP for Suspicious Activity; How SMTP and Email Attacks Work; Additional Important Protocols

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: Understanding Endpoints, Logs, and Files

It is extremely difficult to succeed at cyber defense without knowing where and how your data is produced, so section 3 takes us down to the host, logging, and file level. Starting with a survey of common endpoint-based attack tactics, we orient students to the array of techniques that are used against their hosts. These first sections, followed by a section on defense in-depth, will give students an idea of how each step of the attack lifecycle aligns with its defensive tools, and what students can use to prevent and detect adversary attack advancement on their endpoints. The course section then turns to the parsing and enrichment of logs, as well as how the SIEM normalization and categorization processes work. These topics give a complete view of what happens from the moment a log is generated to when it shows up in our security tools. The final part of section 3 provides students with the concepts needed to reason through the answer, diving into files at the byte level. Students will finish this section understanding how different common file formats work, how they are typically weaponized, and how to quickly decide whether or not a given sample is likely to be malicious.

TOPICS: Endpoint Attack Tactics; Endpoint Defense In-Depth; How Windows Logging Works; How Linux Logging Works; Interpreting Important Events; Kerberos and Active Directory Events; Log Collection, Parsing, and Normalization; File Contents and Identification; Identifying and Handling Suspicious Files

SECTION 4: Triage and Analysis

Now that the course has covered the ground required to understand the tools and data most frequently encountered by analysts, it's time to focus on the process of analysis itself. This day will focus on how the analysis process works and explain how to avoid the common mistakes and biases new analysts can slip into. To accomplish this, this day examines how our memory perception affects analysis and how cognitive biases cause us to fail to see what is right in front of us. The goal is to teach students not only how to think clearly and methodically, but also how to explain how they reached their conclusions in a way that can support future analysis. In addition to analysis technique, this day 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 which must be attended to first. Afterward, safe analysis techniques and analysis operational security concerns are discussed to ensure that analysts do not tip their hand to attackers during the investigation process. The day finishes discussing both how to react to identified intrusions and considerations for doing so as well as how to ensure high-quality documentation for incidents is produced and maintained. The goal is for students to leave this day better prepared to understand their alert queues, perform error-free investigation, and be able to choose the best response for any given attack situation.

TOPICS: Alert Triage and Prioritization; Perception, Memory, and Investigation; Mental Models for Information Security; Structured Analysis Techniques; Analysis Questions and Tactics; Analysis OPSEC; Intrusion Discovery; Incident Closing and Quality Review

SECTION 5: Continuous Improvement, Analytics, and Automation

Repetitive tasks, lack of empowerment or challenges, poorly designed manual processes - analysts know these pains all too well. While these are just some of the common painful experiences in day-to-day SOC work, they are also major contributing factors to unhappiness and burnout that can cause turnover in a SOC. Do things have to be this way? Of course not! But it will take some understanding and work on your part to do things differently. This day focuses squarely on improving the 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 improving everyone's life in the process. This day 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: Improving Life in the SOC; Analytic Features and Enrichment; New Analytic Design, Testing, and Sharing; Tuning and False Positive Reduction; Automation and Orchestration; Improving Operational Efficiency and Workflow; Containing Identified Intrusions; Skill and Career Development

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, day six 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.