SEC450: **Blue Team Fundamentals: Security Operations and Analysis**

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Step into a Security Operations Center or cyber defense role with confidence
- Perform high-quality alert triage and investigation, free of bias and common mistakes
- Understand the most important protocols like DNS, HTTP(S), SMTP, ICMP, SMB, SSH, and more
- Use these protocols to identify malicious and anomalous traffic in your network, employing both heuristics and traffic content analysis
- Understand how logs are collected, parsed, enriched, and interpreted using a SIEM system
- Contain intrusions in both the short and long terms by picking the best tools for the job
- Use all the tools common to security operations – SIEMs, threat intelligence platforms, incident management systems, and automation
- Inspect and identify malicious files in a secure way
- Utilize network monitoring and tactical event logging to catch attacks before they become a problem
- Understand mental models for attack and defense to quickly evaluate any given situation
- Understand the technology, roles, and process required for efficient security operations
- Understand what it takes to defend a modern network

Course Preview
available at: **sans.org/demo**

Is your organization looking for a quick and effective way to onboard new security analysts, engineers, and architects? Do your Security Operations Center (SOC) managers need additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC?

SEC450 is an accelerated on-ramp for new cyber defense team members and SOC managers. This course introduces students to the tools common to a defender's work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know.

Students will learn the stages of security operations: how data is collected, where it is collected, and how threats are identified within that data. The class dives deep into tactics for triage and investigation of events that are identified as malicious, as well as how to avoid common mistakes and perform continual high-quality analysis. Students will learn the inner workings of the most popular protocols, and how to identify weaponized files as well as attacks within the hosts and data on their network.

The course employs practical, hands-on instruction using a simulated SOC environment with a real, fully-integrated toolset that includes:

- Security Information and Event Management (SIEM)
- An incident tracking and management system
- A threat intelligence platform
- Packet capture and analysis
- Automation tools

While cyber defense can be a challenging and engaging career, many SOCs are negatively affected by turnover. To preemptively tackle this problem, this course also presents research-backed information on preventing burnout and how to keep engagement high through continuous growth, automation, and false positive reduction. Students will finish the course with a full-scope view of how collection and detection work, how SOC tools are used and fit together, and how to keep their SOC up and running over the long term.

> **"Visualizing logs and understanding how they go to SIEM was super helpful, especially for someone about to become a SIEM admin. Malware Analysis portion was fantastic for analysts at every level."**
>
> — Troy Dinkel, **Aires**

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

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 analysis itself. This section will focus on how the analysis process works and explain how to avoid the common mistakes new analysts can slip into. We can combat the tendency to overlook the obvious by examining 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, but also how to explain and leave a trail of how they reached their conclusions that can support future analysis and act as an audit trail. In addition, we will cover many of the mental models and concepts used in information security from both the offensive and defensive perspectives. Students will then 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 thus must be attended to first. Safe analysis techniques and operational security concerns are covered to ensure that we do not give up our tactical advantage during the investigation process. We'll discuss specifics on alert triage methods and prioritization, as well as investigation techniques, so that students will leave this section better prepared to understand their alert queues and perform error-free investigation.

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

SECTION 5: Continuous Improvement, Analytics, and Automation

This section focuses squarely on improving the efficiency and enthusiasm of working in SOCs 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 – while improving 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. We also cover containment activities, including the tools you can use and how to decide how to halt a developing incident or infection from the host or network angle. We'll wrap up the section 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 team-based design, detect, and defend the flag competition. Powered by NetWars, section six provides a full day of hands-on work applying the principles taught throughout the week. Your team will be challenged to progress through multiple levels and missions designed to ensure mastery of the concepts and data covered during the course.