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

GIAC CERTIFICATIONS

SEC503: Network Monitoring and Threat Detection - In-Depth

GCIA
Intrusion Analyst
giac.org/gcia

6 Day Program | 46 CPEs | Laptop Required

You Will Be Able To

- Configure and run Snort and Suricata
- Create and write effective and efficient Snort, Suricata and FirePOWER rules
- Configure and run open-source Zeek to provide a hybrid traffic analysis framework
- Create automated threat hunting correlation scripts in Zeek
- Understand TCP/IP component layers to identify normal and abnormal traffic for threat identification
- Use traffic analysis tools to identify signs of a compromise or active threat
- Perform network forensics to investigate traffic to identify TTPs and find active threats
- Carve out files and other types of content from network traffic to reconstruct events
- Create BPF filters to selectively examine a particular traffic trait at scale
- Craft packets with Scapy
- Use NetFlow/IPFIX tools to find network behavior anomalies and potential threats
- Use your knowledge of network architecture and hardware to customize placement of network monitoring sensors and sniff traffic off the wire

GCIA
Intrusion Analyst
giac.org/gcia

GIAC Certified Intrusion Analyst

The GIAC Intrusion Analyst certification validates a practitioner's knowledge of network and host monitoring, traffic analysis, and intrusion detection. GCIA certification holders have the skills needed to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files.

- Fundamentals of Traffic Analysis and Application Protocols
- Open-Source IDS: Snort and Bro
- Network Traffic Forensics and Monitoring

SEC503 is the most important course that you will take in your information security career – past students describe it as the most difficult but most rewarding course they've ever taken. If you want to be able to perform effective threat hunting to find zero-day activities on your network before public disclosure, this is definitely the course for you.SEC503 is not for people looking to understand alerts generated by an out-of-the-box network monitoring tool; rather, it is for those who want to deeply understand what is happening on their network today, and who suspect that there are very serious things happening right now that none of their tools are telling them about.

What sets SEC503 apart from any other course in this space is that we take a bottom-up approach to teaching network monitoring and network forensics, which leads naturally to effective threat hunting. Rather than starting with a tool and teaching you how to use it in different situations, this course teaches you how and why TCP/IP protocols work the way they do. The first two sections present what we call "Packets as a Second Language," then we move to presenting common application protocols and a general approach to researching and understanding new protocols. Throughout the discussion, direct application of this knowledge is made to identify both zero-day and known threats.

With this deep understanding of how network protocols work, we turn our attention to the most important and widely used automated threat detection and mitigation tools in the industry. You will you learn how to develop efficient detection capabilities with these tools, and you'll come to understand what existing rules are doing and identify whether they are useful. The result is that you will leave this course with a clear understanding of how to instrument your network and perform detailed threat hunting, incident analysis, network forensics, and reconstruction.

What makes SEC503 as important as we believe it is (and students tell us it is) is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today. Preserving the security of your network in today's threat environment is more challenging than ever, especially as you migrate more and more services into the cloud. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable.

Some of the specific technical knowledge and hands-on training in SEC503 covers the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, enabling you to intelligently examine network traffic for signs of compromise or zero-day threat. You will get plenty of practice learning to master a variety of tools, including tcpdump, Wireshark, Snort, Suricata, Zeek, tshark, SiLK, and NetFlow/IPFIX. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution, and evening Bootcamp sessions force you to apply the theory learned during the day to real-world problems immediately. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

SEC503 is most appropriate for students who monitor, defend, and conduct threat hunting on their network, including security analysts and those who work in Security Operations Centers, although red team members often tell us that the course also ups their game, especially when it comes to avoiding detection.

Section Descriptions

SECTION 1: Network Monitoring and Analysis: Part I

Section 1 begins our bottom-up coverage of the TCP/IP protocol stack, providing deep coverage of TCP/IP to prepare you to better monitor and find threats in your cloud or traditional infrastructure. This is the first step in what we think of as a "Packets as a Second Language" course. After the importance of collecting the packets used in zero-day and other attacks has been established, students are immediately immersed in low-level packet analysis to identify threats and identify TTPs. This section covers the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, and the meaning and expected behavior of every field in the IP header. Students are introduced to the use of open-source Wireshark and tcpdump tools for traffic analysis.

TOPICS: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

SECTION 2: Network Monitoring and Analysis: Part II

Section 2 completes the "Packets as a Second Language" portion of this course and lays the foundation for the much deeper discussions to come. Students will gain a deep understanding of the primary transport layer protocols used in the TCP/IP model, in addition to the modern trends that are changing how these protocols are used. We'll explore two essential tools, Wireshark and tcpdump, using advanced features to give you the skills to analyze your own traffic. The focus is on filtering large-scale data down to traffic of interest in order to identify threats in both traditional and cloud-based infrastructure using Wireshark display filters and tcpdump Berkeley Packet Filters. These are used in the context of our exploration of the TCP/IP transport layers covering TCP, UDP and ICMP. Once again, we discuss the meaning and expected function of every header field, covering a number of modern innovations that have very serious implications for modern network monitoring. We analyze traffic not just in theory and function but from the perspective of an attacker and defender, allowing us to expand our threat models of modern TTPs at the network level.

TOPICS: Wireshark Display Filters; Writing BPF Filters; TCP; UDP; ICMP; IP6; Real-World Analysis – Researching a network

SECTION 3: Signature-Based Threat Detection and Response

Section 3 builds on the foundation of the first two sections of the course, moving into the world of application layer protocols. Using this knowledge, we dive into the state-of-the-art detection mechanisms for threat detection used in cloud, endpoint, hybrid-network, and traditional infrastructure. Students are introduced to the versatile packet crafting tool Scapy, a very powerful Python-based tool that allows for the manipulation, creation, reading and writing of packets. Scapy can be used to craft packets to test the detection capability of any monitoring tool or next-generation firewall. This is especially important when a new user-created network monitoring rule is added, for instance for a recently announced vulnerability. Various practical scenarios and uses for Scapy are provided throughout the course.

TOPICS: Scapy; Advanced Wireshark; Introduction to Snort/Suricata; Effective Snort/Suricata; DNS; Microsoft Protocols; Modern HTTP; How to Research a Protocol; Real-world Application: Identifying Traffic of Interest

SECTION 4: Building Zero-Day Threat Detection Systems

The fundamental knowledge gained from the first three sections provides the foundation for deep discussions of modern and future network intrusion detection systems during Section 4. Everything that students have learned so far is now synthesized and applied to designing optimized threat detection capabilities that go well beyond what is possible with Snort/FirePower/Suricata and next-generation firewalls through the use of advanced behavioral detection using Zeek (or Corelight).

TOPICS: Network Architecture; Introduction to Network Monitoring at Scale; Zeek; IDS/IPS Evasion Theory

Who Should Attend

- Intrusion detection (all levels), system, and security analysts
  - Analysts will be introduced to or become more proficient in the use of traffic analysis tools for signs of intrusions.
- Network engineers/administrators
  - Network engineers/administrators will understand the importance of optimal placement of IDS sensors and how the use of network forensics such as log data and network flow data can enhance the capability to identify intrusions.
- Hands-on security managers
  - Hands-on security managers will understand the complexities of intrusion detection and assist analysts by providing them with the resources necessary for success.

> **"I got a deeper understanding of key topics from SEC503. This training will help me get more data out of my investigations."**
>
> — Alphonse Wichrowski, **Allegiant Air**

SECTION 5: Large-Scale Threat Detection, Forensics, and Analytics

This section continues the trend of less formal instruction and more practical application in hands-on exercises. The section covers three major areas, beginning with data-driven, large-scale analysis and collection using NetFlow and IPFIX. With the deep protocol background developed in the first sections of the course, NetFlow becomes an incredibly powerful tool for performing threat hunting in our cloud and traditional infrastructure. After covering the fundamentals, we'll walk students through more advanced analysis and threat detection using and building custom NetFlow queries. The second area continues the large-scale analysis theme with an introduction to traffic analytics. Various tools and techniques for zero-day threat hunting at the network level are introduced, after which students have the opportunity to put them into practice in hands-on exercises. We'll also discuss and demonstrate cutting-edge applications of artificial intelligence and machine learning techniques for anomaly detection. The final area involves digging into network forensics and incident reconstruction. Students work through three detailed hands-on incidents, utilizing all of the tools and techniques from the entire course.

TOPICS: Using Network Flow Records; Threat Hunting and Visualization; Introduction to Network Forensic Analysis;

SECTION 6: Advanced Network Monitoring and Threat Detection Capstone

The course culminates with a hands-on server-based Network Monitoring and Threat Detection capstone that is both fun and challenging. Students compete as solo players or on teams to answer many questions that require using tools and theory covered in the course. The challenge is based on six sections of live-fire real-world data in the context of a time-sensitive incident investigation. It is designed as a "ride-along" event, where students are answering questions based on the analysis that a team of professional analysts performed of these same data.

> **"SEC503 completely changed how I look at networking and how I approach problems, and it significantly increased my understanding of intrusion detection."**
>
> — Arnold Klein, **Topel Forman Information Services, LLC**