SEC511: Continuous Monitoring and Security Operations

GMON
Continuous Monitoring
giac.org/gmon

6 Day Program | 46 CPEs | Laptop Required

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Centers (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring
- Determine requisite monitoring capabilities for a SOC environment

While the above list briefly outlines the knowledge and skills you will learn, it barely scratches the surface of what this course has to offer. Hands-on labs throughout the course will reinforce key concepts and principles, as well as teach you how to use scripting to automate continuous monitoring. We look forward to seeing you soon!

GMON
Continuous Monitoring
giac.org/gmon

GIAC Continuous Monitoring Certification

Preventing all intrusions is impossible, but early detection is a must for the security of your enterprise. The proper use of Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring will support the hindrance of intrusions and allow for early detection of anomalous activity.

- Security Architecture and Security Operations Centers (SOCs)
- Network Security Architecture and Monitoring
- Endpoint Security Architecture, Automation and Continuous Monitoring

Analyze Threats. Detect Anomalies. Stop Intrusions.

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. SEC511 will teach you how to strengthen your skills to undertake that proactive approach.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and section five of this course will greatly increase your understanding and enhance your skills in implementing CM using the NIST framework.

SANS is uniquely qualified to offer this course. Course authors Eric Conrad (GSE #13) and Seth Misenar (GSE #28) hold the distinguished GIAC Security Expert Certification, and both are experienced, real-world, practitioners who apply the concepts and techniques they teach in this course on a daily basis. SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final section features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. The competition has been designed to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

With your training journey now complete and your skills enhanced and honed, it is time to go back to work and deliver on the SANS promise that you will be able to apply what you learn in this course the day you return to the office.

Section Descriptions

SECTION 1: Current State Assessment, Security Operations Centers, and Security Architecture

The prevention-dominant security model has failed. Given the frequency and extent of significant intrusions, this should not come as a surprise. In order to address the root of the problem, we must understand the current architecture and the design gaps that facilitate the adversary's dominance. What do we need to address to begin to make things better? Can we ever hope to win? What would winning look like? These are important questions that we must answer if we hope to substantially improve our security posture. We begin with the end in mind, and define the key techniques and principles that will allow us to achieve that state. An effective modern Security Operations Center or security architecture must enable an organization's ability to rapidly find intrusions to facilitate containment and response. Both significant knowledge and a commitment to continuous monitoring are required to achieve this goal.

TOPICS: Overview; Traditional Security Architecture; Introducing Security Onion 2.X; Modern Security Architecture Principles; Security Architecture – Key Techniques/Practices; Cloud Deployment Models; MITRE ATT&CK® & AWS Security Stack

SECTION 2: Network Security Architecture

Understanding the problems with the current environment and realizing where we need to get to is far from sufficient: we need a detailed roadmap to bridge the gap between the current and desired state. Section 2 introduces and details the components of our infrastructure that become part of a defensible network security architecture and SOC. We are long past the days when a perimeter firewall and ubiquitous antivirus were sufficient security. There are many pieces and moving parts that make up a modern defensible security architecture. In addition to discussing technologies like Next Generation Firewalls, UTM devices, Malware Detonation Devices, SIMs, DLP, and Honeypots that may not be found in all organizations, we will focus on repurposing traditional devices such as layer 3/4 firewalls, routers, switches, and NIDS. The goal of this course is not to give you a long list of items to add to the next year's budget, so we will focus on maximizing the capabilities of your current information security architecture, while pointing out new technologies that may offer a compelling return on investment.

TOPICS: SOCs/Security Architecture – Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts, engineers, and managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

SECTION 3: Network Security Monitoring

Designing a SOC or security architecture that enhances visibility and detective capabilities represents a paradigm shift for most organizations. However, the design is simply the beginning. The most important element of a modern security architecture is the emphasis on detection. The network security architecture presented in sections one and two emphasized baking visibility and detective capabilities into the design. Now we must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise. We must first understand the approach and goals of monitoring and define a methodology for analysis. Key terms such as Network Security Monitoring (NSM), Continuous Diagnostics and Mitigation (CDM), and Continuous Security Monitoring (CSM) can cause confusion, and we will make sure these terms are understood, enabling the security professional to guide an organization in using the best practices. Speaking of best practices, we will emphasize the continuous monitoring of the Critical Security Controls. Enabling continuous monitoring will be studied by developing a model for employing robust NSM. This will allow an organization to deal with and make sense of data to rapidly enable the detection of potential intrusions or unauthorized actions.

TOPICS: Evolution of NSM; The NSM Toolbox; NIDS Design; Analysis Methodology; Understanding Data Sources; Cloud NSM; Practical NSM Issues; Cornerstone NSM; Detecting Cobalt Strike

SECTION 4: Endpoint Security Architecture

One of the hallmarks of modern attacks is an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us. We must focus on mitigating the risk of compromise of clients. Section 4 details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities.

TOPICS: Endpoint Security Architecture; Endpoint Protection; Cloud Configuration Management; Endpoint Detection – Sysmon; Authentication Protection and Detection; Configuration Management/Monitoring

SECTION 5: Automation and Continuous Security Monitoring

Network Security Monitoring (NSM) is the beginning: we need to not only detect active intrusions and unauthorized actions, but also know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring proactively and repeatedly assesses and reassesses the current security posture for potential weaknesses that need be addressed. The volume of data that must be continuously sought and mined is vast: the goal of continuous monitoring would be out of reach without scripting and automation. Naturally, there are vendors and tools to scratch this itch, but they will be incomplete and require their own care, feeding, and monitoring. Day five describes how to perform continuous monitoring with simple tools and scripts. Knowing how to script and automate is pointless unless you know what data should be captured and analyzed on a continuous basis. Again, leaning on the Critical Security Controls, we will determine high-value targets for continuous monitoring in an enterprise.

TOPICS: Overview; Industry Best Practices; Winning CSM Techniques; Maintaining Situational Awareness; Host, Port and Service Discovery; Vulnerability Scanning; Monitoring Patching; Monitoring Applications; Monitoring Service Logs; Monitoring Change to Devices and Appliances; Leveraging Proxy and Firewall Data; Configuring Centralized Windows Event Log Collection; Monitoring Critical Windows Events; Scripting and Automation; Security Operations Center (SOC)

SECTION 6: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend-the-flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted all week long. From security architecture, network security monitoring, endpoint security, and continuous monitoring, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

TOPICS: Security Architecture; Continuous Security Monitoring; Applied NSM and CSM; Analyzing Malicious Traffic with Security Onion, Wireshark, and CyberChef; Analzying Malicious Windows Event Logs; Packet Analysis; Log Analysis; C2 Detection

"SEC511 is a VERY worthwhile addition to the Cyber Defense curriculum for Blue Teamers."

—Robert Peden, **NextGear Capital**