SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring

GMON Continuous Monitoring
giac.org/gmon

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Conduct comprehensive current state assessments to engineer and prioritize modern defenses.
- Apply threat-informed defense frameworks such as MITRE ATT&CK and Zero Trust.
- Perform threat hunting using advanced techniques and tools.
- Engineer visibility across modern, hybrid, decentralized infrastructure.
- Navigate modern domain name system (DNS) and transport layer security (TLS) encryption landscape to balance protection, detection, and privacy considerations.
- Understand the cloud security stack and tools like cloud-native application protection platform (CNAPP), cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), and cloud workload protection platform (CWPP) for robust cloud protection.
- Leverage NDR tools and techniques to enhance network visibility and detect threats.
- Conduct effective network threat hunting to identify post-exploitation communications, like command and control (C2) traffic.
- Analyze network data using tools like Suricata, Zeek, Tshark, and Wireshark for threat detection.
- Deploy and manage EDR solutions like Microsoft Defender.
- Implement application control and EPP for endpoint security.
- Monitor and defend identity and access through advanced authentication and user and entity behavior analytics (UEBA).
- Defend AI/LLM applications and secure the AI/software supply chain.
- Perform threat hunting and adversary emulation to assess and evolve detection capabilities.
- Automate security operations and enhance SOC capabilities with security orchestration, automation, and response (SOAR).

Shall We Play A Game?

NetWars gamification now permeates every single section of the course! Since the launch of SEC511, students have consistently found the NetWars-based Capstone to be great fun. Who would have guessed that a game would be fun, right? Students' praise extended beyond just "fun," they also found the game to be a tremendously effective way to further their learning. Inspired by this feedback, we have now incorporated a game-style environment into every section, not just Section 6.

Monitor, Detect, Protect: Master Advanced Threat Detection for Cloud, Network, and Endpoints

Cloud (AWS/Azure/Microsoft 365/Serverless), DevOps, Hybrid, Zero Trust, XDR, Blockchain, AI + ML... The pace of technological change continues to increase. Defending your organization as you did five years ago is a recipe for failure. However, chasing the latest trend or shiny new tool rarely leads to successful protection. Successfully defending a modern enterprise requires nimble pragmatism.

Defending an enterprise has never been easy. SANS SEC511 equips defenders with the necessary knowledge, skills, and abilities to protect and monitor a modern hybrid enterprise successfully. Leveraging the cybersecurity engineering and threat detection techniques taught in this course will best position your organization or Security Operations Center (SOC) to analyze, detect, and respond to modern threats across cloud, network, and endpoint environments. Threat-informed defense of a modern enterprise requires accounting for multiple public cloud providers, continued on-premises infrastructure, AI-empowered adversaries, and possibly a substantial number of remote workers who are not behind a traditional security perimeter.

SEC511 features 18+ hands-on labs, a final capstone challenge, and immersive gamified bootcamp challenges, providing defenders a comprehensive, real-world training experience. The course explores cybersecurity engineering topics and techniques such as cloud monitoring, network detection and response (NDR), endpoint detection and response (EDR), security information and event management (SIEM), endpoint protection platform (EPP), secure access service edge (SASE), Zero Trust, generative artificial intelligence (GenAI), and large language model (LLM) application defense, and more to evolve organizations' threat detection and hunting capabilities. Achieving the accompanying GIAC GMON certification demonstrates your understanding and application of these modern defensive techniques.

Adversaries constantly evolve techniques to ensure their continued success; we must vigilantly adapt our defenses to this changing threat landscape.

"SEC511's lab sessions provided critical practical experience that helped solidify the theoretical concepts."

—Olivia M., **BAH**

Cybersecurity engineering involves designing, implementing, and managing advanced defense mechanisms to protect modern enterprise environments, including cloud, network, and endpoint systems. It encompasses threat-informed defense frameworks, advanced threat detection techniques, and the application of tools such as NDR, EDR, and the MITRE ATT&CK framework to build a robust SOC. This discipline ensures comprehensive protection and monitoring against evolving cyber threats.

Business Takeaways

This course will help your organization:

- Enable effective cloud, network, and endpoint protection and detection strategies
- Engineer protection and threat detection capabilities
- Leverage threat informed defense practices to ensure properly refined security countermeasures
- Materially improve your organization's security operations capabilities
- Identify protection and detection gaps across hybrid infrastructure
- Defend GenAI and LLM applications to ensure trustworthy usage
- Maximize the capabilities of current infrastructure and assets
- Make sense of data to enable the detection of potential intrusions or unauthorized actions rapidly

Section Descriptions

SECTION 1: Threat-Informed Defense: Frameworks, Hunting, and Current State Assessment

In Section 1, students explore the foundational concepts and methodologies that shape modern cybersecurity strategies. Beginning with a current state assessment, they review traditional and modern attack techniques, understanding how these have evolved and the implications for modern post-exploitation scenarios. The section then delves into advanced cyber defense principles, emphasizing the shift from reactive to proactive measures in threat detection and response. Key techniques, models, and frameworks such as MITRE ATT&CK, CIS Controls, OWASP LLM Top 10, Zero Trust, and Long Tail Analysis are introduced, providing a conceptual toolkit to better understand and mitigate threats. Students learn how to utilize frameworks to better align their defenses with known adversary tactics and techniques.

TOPICS: Adversary Tactics and Cyber Defense Principles; Introducing Security Onion 2.X; Frameworks/Mental Models; Threat-Informed Defense and Hunting; GenAI/LLM Fundamentals

SECTION 2: Cloud, Edge, and Network: Visibility and Protection

This section covers the critical aspects of security visibility and protection across cloud, edge, and network environments. It begins with an exploration of network intrusion detection and prevention systems, including malware sandboxes and honeypots, highlighting their roles in identifying and mitigating threats. The impact and importance of encryption, particularly TLS inspection and DNS query encryption, is discussed in detail, providing students with insights into balancing protection of data in transit without compromising visibility. The module also introduces various cloud protection mechanisms, such as CSPM, CIEM, CWPP, and CNAPP, alongside the MITRE ATT&CK Cloud Security Mappings, focusing on securing cloud infrastructures and services like AWS. Edge security is another key focus, where students learn about services such as cloud access security broker, SASE, secure web gateway, and firewall-as-a-service. These are vital for protecting data and applications in a modern hybrid enterprise where data, applications, and users are no longer found exclusively on-premises. This section also covers boundary protection and detection strategies, including next-generation firewalls and web application firewalls, emphasizing their role in a layered security approach.

TOPICS: Security Visibility; Encryption; Cloud Protection and Detection; Edge Security

Who Should Attend

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

SECTION 3: Threat Hunting with Network Detection and Response (NDR)

In Section 3, students delve into the specialized field of NDR, exploring its role within the broader context of Network Security Monitoring (NSM) and SIEM. The content covers the essential components and tools of an NDR/NSM setup, emphasizing the importance and efficacy of various data sources, including cloud-specific considerations. These elements must be designed to provide comprehensive coverage and analytical capabilities, allowing security teams to detect and respond to threats swiftly. By leveraging advanced NDR tools and methodologies, students learn to identify and interpret suspicious activities, even within encrypted communications. Equipping students with the skills needed to identify anomalies and potential threats in network traffic requires exploration of various analytic approaches and techniques. The focus then shifts to the hands-on practice of network threat hunting, where students learn to track implants, detect C2 traffic, and analyze both decrypted and encrypted network traffic. Techniques for identifying malicious traffic via beacon discovery, entropy analysis, and behavior anomaly detection are covered in detail, with specific reference to modern adversary tactics and tooling. The practical labs in this section include pcap payload carving and analysis with Zeek, intrusion analysis with Security Onion, and TLS anomaly detection.

TOPICS: Network Detection Response (NDR); Network Threat Hunting

SECTION 4: Hybrid Enterprise Security: User and Endpoint Protection and Detection

This section focuses on the critical aspects of endpoint and user security within hybrid enterprise environments. Students begin with EDR technologies, exploring tools like Microsoft Defender for Cloud and Endpoint, and learn about the importance of comprehensive endpoint monitoring using solutions like Sysmon. The section also covers EPPs, with a particular emphasis on application control and Microsoft's Defender for Servers, highlighting the integration and management of security measures across various endpoints. User and identity monitoring is another vital component explored in this section. Students examine advanced techniques for defending identity and access, including privilege management, monitoring, and reduction. The content also addresses persistent challenges of legacy authentication and explores modern authentication methods including elements of multifactor authentication (MFA), passwordless, Windows Hello, and Azure AD/Entra ID. Coverage also includes protection and detection of evolving attacks against authentication systems. The concepts undergirding UEBA provide deeper insights into user activities and identification of potential security risks.

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

SECTION 5: GenAI Application Defense, Automation, Supply Chain Protection, and SOC

In the final content-driven section, students explore the emerging field of defending applications built on GenAI and LLMs. The courseware addresses the unique attack surfaces associated with AI technologies, focusing on the specific security challenges and defensive strategies for these applications. Topics such as AI and software supply chain security are covered, with a focus on asset and attack surface discovery, secure baseline configuration, and cloud-based configuration and change management. This section prepares students to tackle the complex issues surrounding the protection of traditional and AI-driven systems and associated data. The module also emphasizes the importance of automation and orchestration in modern SOCs. Students learn about the implementation of SOAR solutions to enhance SOC efficiency and effectiveness. Key topics include DNS threat hunting, adversary emulation, and the detection of lateral movement within networks.

TOPICS: Defending AI/LLM Applications; AI/Software Supply Chain; Service and Event Log Monitoring; Automation/SOAR/SOC

SECTION 6: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, section six provides a full day's worth of hands-on challenges 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 throughout the course.

TOPICS: Modern Cyber Defense: Protection, Detection, and Monitoring; Applied NDR, NSM, and EDR; Network, Endpoint, and Cloud-Oriented Threat Hunting; Analyzing Malicious Traffic with Security Onion, Wireshark, and CyberChef; Analyzing Malicious Windows Event Logs; Packet Analysis; Log Analysis; C2 Detection

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

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

—Robert Peden, **NextGear Capital**