SEC555: **Detection Engineering and SIEM Analytics™**

GCDA
Detection Analyst
giac.org/gcda

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Create a detection lab
- Create rules for adversary detection
- Optimize your SIEM architecture
- Use tools to perform adversary emulation, so you can review related activity logs
- Use log data to establish security control effectiveness
- Simplify the handling and filtering of the large amount of data generated by various devices
- Gain insight into both on-premises and cloud SIEM tools and log sources
- Obtain knowledge of MITRE ATT&CK and gain an ability to map detections to specific tactics and techniques
- Record and monitor detection capabilities across numerous data sources
- Know how SOAR optimization can significantly enhance detection engineering and reduce response time
- Establish baselines, identify trends, and discover outliers, pointing to adversary activity

Business Takeaways

- Reduce business risk by identifying and mitigating threats in near real-time
- Establish a process of proper vendor evaluation, to choose suitable security partners
- Prioritize threats based on potential business impact and asset criticality
- Compile an effective asset database to aid monitoring of critical assets
- Understand how detection engineering aligns with broader organizational objectives, such as regulatory compliance and operational efficacy
- Gain insight into the importance of detection precision, to avoid alert fatigue, and operational inefficiencies
- Explore how detection engineering supports cross-departmental collaboration, with teams like IT, security, and compliance
- Assess and manage risks effectively by leveraging detection data to inform business-critical decisions.
- Adopt a strategy promoting system scalability

Master the Art of Cyber Defense with Detection Engineering and SIEM Analytics

In a world where cyber threats grow more sophisticated by the day, organizations need skilled defenders who can stay one step ahead. This course is your gateway to mastering Detection Engineering—the craft of designing proactive defenses—and SIEM, the core of modern threat detection and response. Whether you're a Security Analyst looking to upskill or a new Detection Analyst, you'll gain the hands-on expertise to detect and investigate attacks. SEC555 is designed to provide students with training, methods, and processes for enhancing existing logging solutions and promote creation of healthy detection rules to enable proactive monitoring.

Uncover the Secrets Hidden in the Logs

This course dives deep into the "when, what, and why" behind logs, teaching you how to craft precise detection rules, fine-tune SIEM configurations, and analyze real-world scenarios to expose hidden threats, in both on-premises and cloud environments. You'll master the art of building automated alerts, leveraging data analytics, and understanding adversarial tactics to defend against sophisticated attacks. Security operations today face not a "Big Data" problem, but a "Data Analysis" challenge, and this course equips you to extract actionable insights from vast amounts of data.

Through hands-on learning, you'll demystify SIEM architecture and its integration into a fully operational Security Operations Center (SOC). You'll explore how to tailor and manage SIEM platforms effectively, enriching enterprise log data to uncover critical intelligence for crafting powerful detections.

What Is Detection Engineering?

Detection Engineering is the process of designing, implementing, and maintaining a proactive cybersecurity approach that focuses on identifying and responding to potential threats before they cause harm. It involves crafting precise detection rules, optimizing log collection and analysis, and building resilient systems to enhance threat visibility. Detection Engineering is essential for modern security operations, enabling teams to outpace adversaries and safeguard organizational assets effectively.

GCDA
Detection Analyst
giac.org/gcda

GIAC Certified Detection Analyst

The GIAC Certified Detection Analyst (GCDA) certification proves an individual knows how to collect, analyze, and tactically use modern network and endpoint data sources to detect malicious or unauthorized activity.

- SIEM Architecture and SOF-ELK
- Service Profiling, Advanced Endpoint Analytics, Baselining and User Behavior Monitoring
- Tactical SIEM Detection and Post-Mortem Analysis

"This course uses real-world events and hands-on training to allow me to immediately improve my organization's security stance. Day one back in the office I was implementing what I learned."

— Frank Giachino, **Bechtel**

Section Descriptions

SECTION 1: Detection Engineering and SIEM Architecture

Logging and analysis are the foundation of modern cyber defense, enabling both rapid response to threats and proactive identification of adversarial activities. When implemented effectively, they serve as the backbone of agile detection, providing deep visibility into the environment and empowering security teams to stay ahead of attackers. Over the years, logging tools and analysis techniques have evolved significantly, offering enhanced capabilities that are critical for modern detection strategies. This section dives into effective tools and cutting-edge techniques for making sense of logs and elevating traditional logging approaches to meet today's complex security challenges. Section 1 sets the stage by equipping all participants with a solid understanding of Detection Engineering and SIEM fundamentals. It establishes a strong baseline, ensuring students are prepared to engage with advanced concepts throughout the course. Additionally, this foundational day focuses on SIEM best practices, laying the groundwork for building efficient and effective detection systems that align with industry-leading methodologies.

TOPICS: SIEM Introduction; Detection Engineering Life Cycle & SIEM Planning; Creating a Detection Lab; Case Management; Log Collection and Enrichment; Log Aggregation, Parsing, and Analysis; Service Log Collection

SECTION 2: Network and Endpoint Analytics

The majority of network communication relies on a handful of key protocols, yet many organizations overlook the value of collecting and analyzing this data. We'll explore methods for gathering logs from services like DNS, SMTP and HTTP servers, as well as passive techniques for extracting the same data directly from the network. You'll also discover how to enrich and add valuable context to this data during the collection process, making it significantly more actionable. We will also explore endpoint logs, since they are a goldmine for detecting attacks, offering unparalleled visibility into post-compromise activities. When leveraged effectively, they can outshine other sources of detection. We will focus on the critical "why" and "how" of system log collection. You'll have an opportunity to explore various strategies and tools designed to simplify the collection, filtering, and handling of the vast amount of data generated by servers and workstations.

TOPICS: Network Analysis; Endpoint Analysis

Who Should Attend

- Detection engineer
- Detection analyst
- Security analyst
- Security engineer
- Threat hunter
- Incident handler/responder
- Security architect
- Security monitoring specialist
- Cyber threat investigator
- Penetration tester

NICE Framework Work Roles

- Data Analyst (OPM 422)
- Cybersecurity Defender (OPM 511)
- Incident Responder (OPM 531)
- Threat Analyst (OPM 141)

SECTION 3: Baselines and UEBA

"Know thyself" is a cornerstone of effective defense, yet one of the hardest strategies to achieve. Take, for example, something as seemingly simple as maintaining a complete inventory of all assets in your organization and identifying unauthorized devices on your network. While straightforward in theory, this task becomes daunting in today's dynamic and ever-evolving networks. This section tackles this challenge head-on, focusing on automated techniques to maintain an accurate list of assets and their configurations while distinguishing authorized from unauthorized devices. You'll learn how to identify key data sources that provide high-fidelity information and combine multiple streams of data to create a comprehensive and actionable master inventory. Beyond inventory, we'll expand into other aspects of "knowing thyself." You'll gain hands-on experience with network and system baselining, learning to monitor network flows and detect anomalies like command-and-control (C2) beaconing or unusual user activity.

TOPICS: Active Asset Discovery; Passive Asset Discovery; Identify Authorized vs. Unauthorized Software; Baseline Data; UEBA

SECTION 4: Cloud Logging and Monitoring

As organizations increasingly migrate to the cloud, achieving comprehensive visibility across platforms has never been more critical. This section emphasizes the importance of cross-vendor expertise in configuring robust cloud monitoring to protect your environment. You'll explore the various log types available, with a focus on those that can be leveraged to strengthen defenses and streamline incident response. Through hands-on guidance, you'll become familiar with the key logging tools in Microsoft Azure and AWS. You'll also analyze how attackers attempt to bypass cloud security measures, uncovering the traces they leave in logs. Finally, you'll learn how to optimize log configurations to ensure you capture critical events, leaving no gaps in your cloud monitoring strategy. This knowledge is essential to operationalize defenses and maintain a strong security posture in today's cloud-driven world.

TOPICS: Azure Cloud Logging; Defender Suite and Copilot for Security; Microsoft Sentinel and KQL; AWS Cloud Logging

SECTION 5: In-Depth Alerting, Post-Mortem Analysis, and Capstone Exercise

This section emphasizes the power of integrating security logs from multiple sources for centralized analysis. You'll learn methods to combine and correlate data streams, adding valuable context that enables analysts to prioritize effectively. By integrating asset data with security alerts, we'll demonstrate how to maximize analyst efficiency, reduce costs, and focus on addressing the most critical risks.

TOPICS: Alerts; Post-Mortem Analysis; Automated Detection Pipeline; Defend-the-Flag Challenge – Hands-on Experience