SEC555: **SIEM with Tactical Analytics**

GCDA Detection Analyst giac.org/gcda

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Deploy the SANS SOF-ELK VM in production environments
- Demonstrate ways most SIEMs commonly lag current open source solutions (e.g. SOF-ELK)
- Bring students up to speed on SIEM use, architecture, and best practices
- Know what type of data sources to collect logs from
- Deploy a scalable logs solution with multiple ways to retrieve logs
- Operationalize ordinary logs into tactical data
- Develop methods to handle billions of logs from many disparate data sources
- Understand best practice methods for collecting logs
- Dig into log manipulation techniques challenging many SIEM solutions
- Build out graphs and tables that can be used to detect adversary activities and abnormalities
- Combine data into active dashboards that make analyst review more tactical
- Utilize adversary techniques against them by using frequency analysis in large data sets
- Develop baselines of network activity based on users and devices
- Develop baselines of Windows systems with the ability to detect changes from the baseline
- Apply multiple forms of analysis such as long tail analysis to find abnormalities
- Correlate and combine multiple data sources to achieve more complete understanding
- Provide context to standard alerts to help understand and prioritize them
- Use log data to establish security control effectiveness
- Implement log alerts that create virtual tripwires for early breach detection
- Understand how to handle container monitoring and log collection
- Baseline and find unauthorized changes in cloud environments
- Integrate and write custom scripts against a SIEM

Business Takeaways

- Use log data to establish security control effectiveness
- Combine data into active dashboards that make analyst review more tactical
- Simplify the handling and filtering of the large amount of data generated by both servers and workstations
- Apply large data analysis techniques to sift through massive ammounts of endpoint data
- Quickly detect and respond to the adversary

Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of those sources for proper analysis. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. The class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a "Big Data" problem but rather a "Data Analysis" problem. Let's face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the "appropriate" use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, how to start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

GCDA Detection Analyst giac.org/gcda

GIAC Certified Detection Analyst

"The GIAC Certified Detection Analyst (GCDA) is an industry certification that proves an individual knows how to collect, analyze, and tactically use modern network and endpoint data sources to detect malicious or unauthorized activity. This certification shows individuals not only know how to wield tools such as Security Information and Event Management (SIEM) but that they know how to use tools to turn attacker strengths into attacker weaknesses."
— Justin Henderson, SEC555 Course Author

- 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: SIEM Architecture

Logging and analysis is a critical component in cyber network defense and allows for both reactive and proactive detection of adversarial activities. When properly utilized it becomes the backbone for agile detection and provides understanding to the overall environment. Logging and analysis products and techniques have been around for many years and are quickly gaining more and more functionality. This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to deal with the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Section 1 is designed to bring all students up to speed on SIEM concepts and bring them to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During this first course section, we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK (a VM co-maintained by Phil Hagen and Justin Henderson) and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.

TOPICS: State of the SOC/SIEM; Log Monitoring; Logging Architecture; SIEM Platforms; Planning a SIEM; SIEM Architecture; Ingestion Techniques and Nodes; Data Queuing and Resiliency; Storage and Speed; Analytical Reporting

SECTION 2: Service Profiling with SIEM

A vast majority of network communication occurs over key network protocols and yet it is uncommon for organizations to use or collect this data. The sheer volume can be overwhelming. However, these common data sources provide an opportunity in identifying modern day attacks. This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered as well as passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as it is collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.

TOPICS: Detection Methods and Relevance to Log Analysis; Analyzing Common Application Logs that Generate Tremendous Amounts of Data; Applying Threat Intelligence to Generic Network Logs; Active Dashboards and Visualizations

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

NICE Framework Work Roles

- Network Operations Specialist (OPM 441)

SECTION 3: Advanced Endpoint Analytics

The value in endpoint logs provides tremendous visibility in detecting attacks. Especially, with regard to finding post-compromise activity, endpoint logs can quickly become a vehicle that is second to none. However, logs even on a single desktop can range in the tens if not hundreds of thousand events per day. Multiply this by the number of systems in your environment and it is no surprise why organizations get overwhelmed. This section will cover the how and more importantly the why behind collecting system logs. Various collection strategies and tools will be used to gain hands-on experience and to provide simplification with handling and filtering the seemingly infinite amount of data generated by both servers and workstations. Workstations' log strategies will be covered in depth due to their value in today's modern attack vectors. After all, modern day attacks typically start and then spread from workstations.

TOPICS: Endpoint Logs

SECTION 4: Baselining and User Behavior Monitoring

Know thyself is often quoted to defenders as a key defense strategy. And yet this is one of the most difficult things to accomplish. Take something such as having a list of all assets in an organization and knowing if any non-company assets are on the network. The task sounds simple but ends up being incredibly difficult to maintain in today's ever-evolving networks. This section focuses on applying techniques to automatically maintain a list of assets and their configurations as well as methods to distinguish if they are authorized vs. unauthorized. Key locations to provide high-fidelity data will be covered and techniques to correlate and combine multiple sources of data together will be demonstrated to build a master inventory list. Other forms of knowing thyself will be introduced such as gaining hands-on experience in applying network and system baselining techniques. We will monitor network flows and identify abnormal activity such as C2 beaconing as well as look for unusual user activity. Finally, we will apply large data analysis techniques to sift through massive amounts of endpoint data. This will be used to find things such as unwanted persistence mechanisms, dual-homed devices, and more.

TOPICS: Identifying Authorized and Unauthorized Assets; Identifying Authorized and Unauthorized Software; Baseline Data

SECTION 5: Tactical SIEM Detection and Post-Mortem Analysis

Multiple security devices exist but often are designed to be independent. Analysts are commonly divided into specialty areas and focus on their respective area such as a network intrusion detection system. However, alerts from a single security device lack context and are akin to the common analogy of "looking up from the bottom of a well." This section focuses on combining multiple security logs for central analysis. More importantly we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts we will jump into new methods to utilize logging technology to implement virtual tripwires. While it would be ideal to prevent attackers from gaining access to your network, it is a given that at some point you will be compromised. However, compromise is just the beginning and not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires. Should a single one be "stepped on" we can quickly detect and respond to the adversary.

TOPICS: Centralizing NIDS and HIDS Alerts; Analyzing Endpoint Security Logs; Augmenting Intrusion Detection Alerts; Analyzing Vulnerability Information; Correlating Malware Sandbox Logs with Other Systems to Identify Victims Across the Enterprise; Monitoring Firewall Activity; SIEM Tripwires; Post-Mortem Analysis

SECTION 6: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, This final course section provides a full day of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted during the course. From building a logging architecture, augmenting logs, analyzing network logs, analyzing system logs, and developing dashboards to finding attacks, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

TOPICS: Defend-the-Flag Challenge – Hands-on Experience