FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics™

GCFA Forensic Analyst
giac.org/gcfa

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Identify living off the land techniques, including malicious use of PowerShell and WMI
- Target advanced adversary anti-forensics techniques like hidden and time-stamped malware, along with living off the land techniques used to move in the network and maintain an attacker's presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy/Restore Point analysis
- Identify lateral movement and pivots within your enterprise across your endpoints, showing how attackers transition from system to system without detection
- Understand how the attacker can acquire legitimate credentials—including domain administrator rights—even in a locked-down environment
- Track data movement as attackers collect critical data and shift it to exfiltration collection points
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis and artifact carving
- Use collected data to perform effective remediation across the entire enterprise

Threat hunting and incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident or contain propagating ransomware. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions. This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and ransomware operators.

FOR508: Advanced Incident Response and Threat Hunting Course will help you to:

- Understand attacker tradecraft to perform compromise assessments
- Detect how and when a breach occurred
- Quickly identify compromised and infected systems
- Perform damage assessments and determine what was read, stolen, or changed
- Contain and remediate incidents of all types
- Track adversaries and develop threat intelligence to scope a network
- Hunt down additional breaches using knowledge of adversary techniques
- Build advanced forensics skills to counter anti-forensics and data hiding from technical subjects

The course exercises and final challenges illustrate real attacker traces found via end point artifacts, event logs, system memory, and more:

- **Phase 1—**Patient zero compromise and malware C2 beacon installation
- **Phase 2—**Privilege escalation, lateral movement to other systems, malware utilities download, installation of additional beacons, and obtaining domain admin credentials
- **Phase 3—**Searching for intellectual property, network profiling, business email compromise, dumping enterprise hashes
- **Phase 4—**Find exfiltration point, collect and stage data for theft
- **Phase 5—**Exfiltrate files from staging server, perform cleanup and set long-term persistence mechanisms (alternatively this phase would be used to deploy ransomware)

Business Takeaways

- Understand attacker tradecraft to perform proactive compromise assessments
- Upgrade detection capabilities via better understanding of novel attack techniques, focus on critical attack paths, and knowledge of available forensic artifacts
- Develop threat intelligence to track targeted adversaries and prepare for future intrusion events
- Build advanced forensics skills to counter anti-forensics and data hiding from technical subjects for use in both internal and external investigations

"FOR508 exceeded my expectations in every way. It provided me the skills, knowledge, and tools to effectively respond to and handle APTs and other enterprise-wide threats."

—Josh M., **U.S. Federal Agency**

Section Descriptions

SECTION 1: Advanced Incident Response and Threat Hunting

This section was designed to help organizations increase their capability to detect and respond to intrusion events. This is an achievable goal and begins by teaching the tools and techniques necessary to find evil in your network. This course is designed to make you and your organization an integral part of the solution. To keep pace, incident responders and threat hunters must be armed with the latest tools, analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries with the ultimate goal of rapid remediation of incidents and damage mitigation. Further, incident response and threat hunting analysts must be able to scale their efforts across potentially thousands of systems in the enterprise. We start the day by examining the six-step incident response methodology as it applies to incident response for advanced threat groups. The importance of developing cyber threat intelligence to impact the adversaries' "kill chain" is discussed and forensic live response techniques and tactics are demonstrated that can be applied both to single systems and across the entire enterprise.

TOPICS: Real Incident Response Tactics; Threat Hunting; Threat Hunting in the Enterprise; Incident Response and Hunting Across the Enterprise; Malware Defense Evasion and Identification; Malware Persistence Identification; Prevention, Detection, and Mitigation of Credential Theft

SECTION 2: Intrusion Analysis

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker action leaves a corresponding artifact, and understanding what is left behind as footprints can be crucial to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. As an example, at some point an attacker will need to run code to accomplish their objectives. We can identify this activity via application execution artifacts. The attacker will also need one or more accounts to run code. Consequently, account auditing is a powerful means of identifying malicious. An attacker also needs a means to move throughout the network, so we look for artifacts left by the relatively small number of ways there are to accomplish internal lateral movement. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise. Get ready to hunt!

TOPICS: Advanced Evidence of Execution Detection; Lateral Movement Adversary Tactics, Techniques, and Procedures; Log Analysis for Incident Responders and Hunters; Investigating WMI and PowerShell-Based Attacks

SECTION 3: Memory Forensics in Incident Response and Threat Hunting

Memory forensics has come a long way in just a few years. It is now a critical component of many advanced tool suites (notably EDR) and the mainstay of successful incident response and threat hunting teams. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, PowerShell attacks, ransomware precursors, and advanced malware used by targeted attackers. In fact, some fileless attacks may be nearly impossible to unravel without memory analysis. Memory analysis was traditionally the domain of Windows internals experts and reverse engineers, but new tools, techniques, and detection heuristics have greatly leveled the playing field making it accessible today to all investigators, incident responders, and threat hunters. Further, understanding attack patterns in memory is a core analyst skill applicable across a wide range of endpoint detection and response (EDR) products, making those tools even more effective. This extremely popular section will cover many of the most powerful memory analysis capabilities available and give analysts a solid foundation of advanced memory forensic skills to super-charge investigations, regardless of the toolset employed.

TOPICS: Endpoint Detection and Response; Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

SECTION 4: Timeline Analysis

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. Temporal data is located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and browser history files all contain time data that can be correlated and analyzed to rapidly solve cases. Pioneered by Rob Lee as early as 2001, timeline analysis has grown to become a critical incident response, hunting, and forensics technique. New timeline analysis frameworks provide the means to conduct simultaneous examinations on a multitude of systems across a multitude of forensic artifacts. Analysis that once took days now takes minutes. This section will step you through two primary methods of building and analyzing timelines used during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create timelines and how to introduce the key analysis methods necessary to help you use those timelines effectively in your cases.

TOPICS: Malware Defense Evasion and Detection; Timeline Analysis Overview; Filesystem Timeline Creation and Analysis; Super Timeline Creation and Analysis

Who Should Attend

- Incident response team members
- Threat hunters
- Security Operations Center analysts
- Experienced digital forensic analysts
- Detection engineers
- Information security professionals
- Federal agents and law enforcement personnel
- Red team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates looking to take their skills to the next level

NICE Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

GCFA
Forensic Analyst
giac.org/gcfa

GIAC Certified Forensic Analyst

The GCFA certifies that candidates have the knowledge, skills, and ability to conduct formal incident investigations and handle advanced incident handling scenarios, including internal and external data breach intrusions, advanced persistent threats, anti-forensic techniques used by attackers, and complex digital forensic cases. The GCFA certification focuses on core skills required to collect and analyze data from Windows and Linux computer systems.

- Advanced Incident Response and Digital Forensics
- Memory Forensics, Timeline Analysis, and Anti-Forensics Detection
- Threat Hunting and APT Intrusion Incident Response

SECTION 5: Incident Response and Hunting Across the Enterprise | Advanced Adversary and Anti-Forensics Detection

Attackers commonly take steps to hide their presence on compromised systems. While some anti-forensics steps can be relatively easy to detect, others are much harder to deal with. As such, it's important that forensic professionals and incident responders are knowledgeable on various aspects of the operating system and file system which can reveal critical residual evidence. Criminal and ransomware syndicates have become particularly aggressive in their use of anti-forensic techniques. In this section, we focus on recovering files, file fragments, and file metadata of interest to the investigation. These trace artifacts can help the analyst uncover deleted logs, attacker tools, malware configuration information, exfiltrated data, and more. This often results in a deeper understanding of the attacker TTPs and provides more threat intelligence for rapid scoping of an intrusion and mitigating damage. In some cases, these deep-dive techniques could be the only means for proving that an attacker was active on a system of interest and ultimately determining root cause. While very germane to intrusion cases, these techniques are applicable in nearly every forensic investigation.

TOPICS: Volume Shadow Copy Analysis; Advanced NTFS Filesystem Tactics; Advanced Evidence Recovery

SECTION 6: The APT Threat Group Incident Response Challenge

This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the course and tests your newly acquired skills in an investigation into an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other compromised systems via adversary lateral movement, and identify intellectual property stolen via data exfiltration. Solving the final intrusion lab requires investigating artifacts on over thirty systems including Windows 10 and 11 workstations, DMZ servers, a domain controller, internal development servers, and hosted Exchange email. You will walk out of the course with hands-on experience investigating a real attack, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates to top-level ransomware groups.

TOPICS: Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery