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

- Master tools and techniques to detect, contain, and remediate adversaries
- Detect live, dormant, and custom malware across enterprise Windows systems
- Hunt threats and perform incident response at scale
- Identify malware beaconing, lateral movement, and C2 activity via memory analysis and Windows host forensics
- Analyze breaches to determine root cause, attack vectors, and persistence mechanisms
- Counter anti-forensics techniques, recover cleared data, and track attacker activity
- Use forensic tools to remediate threats and secure the enterprise

Should a Breach Occur, FOR508™ Graduates Will Have The Skills To:

- Detect how and when attack happened
- Quickly identify compromised and infected systems
- Perform damage assessments and determine what was read, stolen, or changed
- Contain and remediate incidents
- Hunt down additional breaches using knowledge of the adversary

"So much content! I am finally able to get into the weeds and learn about things that have been a mystery for so long! FOR508™ training really breaks down the complicated in a way that is easy to understand while still leaving so much more to be done. I love this class."

—Zachary T., **U.S. Federal Government**

Threat hunting and incident response tactics and procedures continue to evolve rapidly. 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 state-sponsored adversaries, organized crime syndicates, ransomware operators, and hacktivists.

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 accessed, stolen, or changed
- Contain and remediate incidents
- 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 techniques

The course exercises and final challenges illustrate real attacker activity 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 account credentials
- **Phase 4—**Find exfiltration point, collect and stage data for theft
- **Phase 5—**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
- Develop threat intelligence to track targeted adversaries and prepare for future intrusion events
- Build advanced forensics skills to counter anti-forensics

"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

Section 1 is designed to help organizations increase their capability to detect and respond to intrusion events. 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' objectives 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; Malware; Incident Response and Hunting Across the Enterprise; Malware Persistence Identification; Prevention, Detection, and Mitigation of Credential Theft

SECTION 2: Intrusion Analysis

In Section 2, 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! Even the most advanced adversaries leave footprints everywhere. Learn the secrets of the best hunters. 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 activity.

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

Section 3 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. 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.

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

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. Temporal data is located everywhere on a computer system. Filesystem modification/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.

TOPICS: Malware Defense; 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

Criminal and ransomware syndicates have become particularly aggressive in their use of anti-forensic techniques. In Section 5, 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. 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.

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.

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