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

- Apply forensic tools and techniques to investigate intrusions across enterprise systems
- Perform root cause analysis using host, log, and memory artifacts
- Analyze attacker activity, including persistence, lateral movement, and C2 techniques
- Build and analyze timelines to reconstruct attack sequences
- Use memory and host-based analysis to identify malicious activity
- Counter anti-forensics techniques and recover deleted or hidden data
- Use AI-assisted analysis to support data review while maintaining forensically sound practices

"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**

"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**

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 training course provides analysts with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within Microsoft Windows-based enterprise networks, including APT state-sponsored adversaries, organized crime syndicates, ransomware operators, and hacktivists. The course focuses on training human analysts to find and interpret the artifacts that are left behind in modern Windows-based network intrusions, while also incorporating cutting-edge AI-assisted tools and techniques to allow individual analysts, or teams of analysts, to significantly scale their response efforts. Harnessing the power of artificial intelligence for incident response is quickly becoming a critical skill, as defenders must keep pace with the adversaries who also wield the technology.

As such, this course empowers analysts with the knowledge and tools necessary to combat today's most sophisticated threats. It also serves as a primary preparation path for the GCFA certification (GIAC Certified Forensic Analyst), which validates real-world skills in detecting and responding to advanced intrusions.

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

- Determine how and when a breach occurred and identify affected systems
- Assess scope and impact, including data accessed, stolen, or changed
- Contain and remediate incidents across enterprise environments
- Track attacker activity and develop threat intelligence for investigations
- Identify additional compromised systems using adversary techniques
- Improve incident response effectiveness and investigation efficiency
- Prepare for the GCFA certification, validating incident response and forensics skills

Business Takeaways

- Learn from curriculum that keeps pace with modern attacker tradecraft
- Build skills that map directly to day-to-day analyst work
- Understand attacker TTPs to perform proactive threat hunting and compromise assessments
- Leverage threat intelligence to track targeted adversaries in active investigations and prepare for future intrusion events
- Implement tools and strategies to harness AI for scalable respsonse
- Leads to the GCFA GIAC certification that validates analyst skills

Section Descriptions

SECTION 1: Advanced Incident Response and Threat Hunting

We start by examining the six-step incident response methodology as it applies to incident response for advanced threat groups. We discuss the importance of developing cyber threat intelligence to impact the adversaries' objectives and demonstrate forensic live response techniques that can be applied both to single systems and across the entire enterprise.

TOPICS: Real Incident Response Tactics; Incident Response and Hunting Across the Enterprise; Artificial Intelligence for Incident Response; Malware and Persistence Identification; Prevention 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!

TOPICS: Advanced Evidence of Execution Detection; Lateral Movement Adversary Tactics and Techniques; 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.

TOPICS: Endpoint Detection and Response; Memory Acquisition; Memory Acquisition and Forensic Analysis; Memory Forensics Examinations; Memory Analysis Toolsç

SECTION 4: Timeline Analysis

This section will step students through two primary methods of building and analyzing timelines used for DFIR analysis. We demonstrate how to create the timelines and how to use them effectively to find answers quickly. The section concludes with a discussion on agentic AI for further enhancing and accelerating DFIR investigations.

TOPICS: Timeline Analysis Overview; Filesystem Timeline Creation and Analysis; Super Timeline Creation and Analysis; Agentic AI for DFIR Investigations

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

In Section 5, we focus on recovering files, file fragments, and file metadata for the investigation. These trace artifacts can help the analyst uncover deleted logs, attacker tools, malware configuration information, exfiltrated data, and more. 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 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 initially, find other compromised systems via adversary lateral movement, and identify intellectual property stolen via data exfiltration.

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

GCFA

Forensic Analyst
giac.org/gcfa

GIAC Certified Forensic Analyst

The GCFA certification focuses on core skills required to collect and analyze data computer systems. 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.

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

Who Should Attend

- Incident response team members
- Threat hunters
- Security Operations Center analysts
- Experienced digital forensic analysts
- Detection engineers
- InfoSec professionals
- Federal agents and law enforcement professionals
- 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)

"It's hard to really say something that will properly convey the amount of mental growth I have experienced in this training."

—Travis Farral, **XTO Energy**