# FOR608: Enterprise-Class Incident Response and Threat Hunting™

**GEIR**
Enterprise Incident Responder
giac.org/geir

6 Day Program | 36 CPEs | Laptop Required

## You Will Be Able To

- Know when to perform deep host analysis vs. quick data collection at scale
- Use collaboration tools for seamless remote teamwork
- Gather forensic data from on-prem and cloud sources (M365, AWS)
- Analyze Linux, Mac, and containerized (e.g., Docker) environments
- Correlate data (network, endpoint, etc.) to uncover attacker actions
- Analyze structured and unstructured data to reveal attacker behavior
- Enrich data to identify IOCs, create detection signatures, and track incidents

## Business Takeaways

- Limit financial and reputational impact through precise incident response
- Maximize efficiency with effective IR resource management
- Collaborate seamlessly across teams using dedicated platforms
- Detect and counter EDR and app control evasion on Windows
- Analyze and respond to compromised Linux and macOS systems
- Handle incidents in Docker, M365, Entra ID, and AWS environments

**"The course content covers a lot of important topics focused on detection and response. I enjoyed the sections on Threat Driven Intelligence and TimeSketch for creating incident timelines."**

—Reggie M., **Amazon**

**"The elastic work was very impressive. I have been using it for a number of years, but it introduced me to new ways to ingest data that could have saved me a lot of work in the past."**

—Simon H.

## There Is No Teacher but the Enemy!

Enterprises today have thousands — maybe even hundreds of thousands — of systems ranging from desktops to servers, from on-site to the cloud. Although geographic location and network size have not deterred attackers in breaching their victims, these factors present unique challenges in how organizations can successfully detect and respond to security incidents. Our experience has shown that when sizeable organizations suffer a breach, the attackers seldom compromise one or two systems. Without the proper tools and methodologies, enterprise incident response security teams will always find themselves playing catch-up, and the attacker will continue to achieve success. This course also prepares students for the GEIR certification (GIAC Enterprise Incident Response), which validates advanced skills in large-scale, coordinated response operations.

FOR608 focuses on identifying and responding to incidents too large to focus on individual machines. The concepts are similar: gathering, analyzing, and making decisions based on information from hundreds of machines. This requires the ability to automate and the ability to quickly focus on the right information for analysis. By using example tools built to operate at enterprise-class scale, students will learn the techniques to collect focused data for incident response and threat hunting. Students will then dig into analysis methodologies, learning multiple approaches to understand attacker movement and activity across hosts of varying functions and operating systems by using timeline, graphing, structured, and unstructured analysis techniques.

FOR608: Enterprise-Class Incident Response & Threat Hunting will teach you how to:

- Understand when incident response requires in-depth host interrogation or light-weight mass collection
- Deploy collaboration and analysis platforms that allow teams to work across rooms, states, or countries simultaneously
- Collect host- and cloud-based forensic data from large environments
- Discuss best practices for responding to Azure, M365, and AWS cloud platforms
- Learn analysis techniques for responding to Linux and Mac operating systems
- Analyze containerized microservices such as Docker containers
- Correlate and analyze data across multiple data types and machines using a myriad of analysis techniques
- Conduct analysis of structured and unstructured data to identify attacker behavior
- Enrich collected data to identify additional indicators of compromise
- Develop IOC signatures and analytics to expand searching capabilities and enable rapid detection of similar incidents in the future
- Track incidents and indicators from beginning to end using built-for-purpose incident response engagement tooling

# Section Descriptions

### SECTION 1: Proactive Detection & Response

Section 1 focuses on proactive cyber defense through early detection, rapid response, and managing incident response teams effectively. It covers active defense tactics like honeypots and canaries, as well as efficient incident response with tools like Aurora, Velociraptor, and Timesketch.

**TOPICS:** Incident Response and Threat Hunting in the Enterprise; Managing Large-Scale Response; Rapid Response Triage; Scalable and Collaborative Analysis with Timesketch

### SECTION 2: Scaling Response and Analysis

Section 2 covers threat intelligence concepts, EDR technology and EDR bypass techniques, deploying Velociraptor for IR and threat hunting, and tactical use of Elasticsearch fast forensics in ad-hoc scenarios. The section concludes with a discussion on AI integration in DFIR, including MCP servers, agentic AI, and AI attack vectors.

**TOPICS:** Intel-Driven Incident Response; EDR and EDR Bypass; Scaling Incident Response with Velociraptor; Scaling Analysis with the Elastic Stack; Integrating AI into DFIR

### SECTION 3: Modern Attacks Against Windows and Linux DFIR

Section 3 focuses on host-based forensics, covering Windows modern attacks like "fileless" malware and "living of the land" techniques, with detection using Sigma rules, Elasticsearch, and Hayabusa. It then shifts to Linux DFIR, addressing exploits, file systems, logging, and hardening—building skills to investigate both Windows and Linux intrusions.

**TOPICS:** Modern Attacks Against Windows; Detect and Respond to Modern Attacks; Introduction to Linux; Modern Attacks Against Linux; Linux DFIR Fundamentals; Linux Log Analysis; Linux Triage Collection and Forensic Readiness

### SECTION 4: Analyzing macOS and Docker Containers

This section covers macOS incident response, including its ecosystem, data acquisition, log analysis, and key artifacts. It also introduces containerized environments, focusing on Docker and its role in modern enterprise investigations.

**TOPICS:** macOS Foundations; Apple Filesystems; Mac Incident Response; Containers in the Enterprise; DFIR for Containers

### SECTION 5: Cloud Attacks and Response

This section covers incident response in Microsoft Azure, M365, and AWS, highlighting unique cloud challenges and the MITRE ATT&CK® Cloud Matrix. It focuses on common attack scenarios, key logs, and tools like GuardDuty. It concludes with strategies for cloud response using security accounts, AMIs, and automation tools like Lambda and Step Functions.

**TOPICS:** DFIR in the Cloud; Incident Response in Azure and M365; Attackers in the Cloud; AWS Foundations; Incident Response in AWS; IR Automation in AWS

### SECTION 6: Capstone: Enterprise-Class IR Challenge

Section 6 is the capstone exercise, where students apply course concepts to analyze a multi-platform breach. Using real-world tools and techniques, they'll investigate an end-to-end incident across hosts and cloud systems, working in teams to simulate real-world response.

## Meet The Course Authors

**Mathias Fuchs**
*Senior Instructor*

"Renaissance man" may be the most fitting description of SANS instructor Mathias Fuchs, who is the Head of Investigation & Intelligence at the Swiss firm InfoGuard AG as well as a volunteer paramedic and a pilot.

**Mike Pilkington**
*Senior Instructor*

Current DFIR consultant, and former incident response lead at Shell and Halliburton, Mike's work has helped shape enterprise-scale incident response and directly advanced the global community's ability to combat cyber adversaries.

**Tarot (Taz) Wake**
*Certified Instructor*

With FOR577, Taz has authored the first course to systematize threat hunting on Linux systems. His operational leadership—from military intelligence to heading a FTSE100 CSIRT—has fortified global cyber defense capabilities across sectors.

**Marcus Guevara**
*Certified Instructor*

Marcus Guevara is a Texas native and the author of the philosophical book "Hacking Theology". He holds a bachelor's degree in Computer Science and a master's degree in Cybersecurity.

## Who Should Attend

FOR608 is aimed at digital forensics, incident response, intrusion detection, and threat hunting professionals in medium to large organizations, who constantly face battles with enterprise scale and complexity.

**Please note that FOR608 is an advanced course that skips over introductory material of Windows host- and network-based forensics and incident response. Although this class is not necessarily more technical than our 500-level classes, it does assume that prior knowledge so that topics and concepts are not repeated.**

## NICE Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

## Prerequisites

FOR608 is an advanced level course that skips over introductory material of Windows host- and network-based forensics and incident response. This class is not necessarily more technical than our 500-level classes, but it does assume that knowledge so that topics and concepts are not repeated.

Students must have multiple years of DFIR experience and/or have taken classes such as:

- FOR500: Windows Forensics Analysis, and/or
- FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting


**GEIR**
**Enterprise Incident Responder**
**giac.org/geir**

## GIAC Enterprise Incident Responder

The GIAC Enterprise Incident Response (GEIR) certification validates a practitioner's mastery of enterprise-class incident response and threat hunting tools and techniques. GEIR certification holders have demonstrated the ability to use analysis methodologies to understand attacker movement across varying functions and operating systems.

- Incident response team management and coordination
- Enterprise incident detection and threat hunting
- Large-scale-event correlation and timeline analysis
- Multi-platform artifact analysis
- Analysis of Windows Artifacts
- Analysis of Linux Artifacts
- Analysis of macOS Artifacts
- Analysis of Container Artifacts
- Analysis of Cloud Environment Artifacts