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

- 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

Who Should Attend

This course 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

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, security teams will always find themselves playing catch-up, and the attacker will continue to achieve success.

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.

Business Takeaways

- Reduce financial and reputational impact of a breach by more efficiently and precisely managing the response
- Learn IR management techniques that optimize resource usage during an investigation
- Deploy collaboration and analysis platforms that allow teams to work across rooms, states, or countries simultaneously
- Understand and hunt for techniques attackers use to hide from EDR and application control tools on Windows systems
- Learn analysis techniques for responding to compromised Linux and macOS systems
- Be able to respond and analyze containerized microservices such as Docker containers
- Discuss best practices for responding to the most popular cloud environments—specifically Microsoft365/AzureAD, and AWS

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

Section Descriptions

SECTION 1: Proactive Detection & Response

Section 1 begins with discussions on current cyber defense concerns, and how incident responders and threat hunters can take a more active role in detection and response. Collaboration within the team and the community are a focus, as we look to incorporate shared knowledge from sources like the MITRE ATT&CK® framework. Furthermore, we discuss taking an active defense approach to slow attackers and facilitate detection.

When a compromise does occur, which is an unfortunate but inevitable truth, we continue the discussion with a focus on the processes and techniques that allow for efficient handling of intrusions. Concepts such as leading the response, managing team members, documenting findings, and communicating with stakeholders are covered in detail.

We continue the section with an examination of key threat intelligence concepts, including developing and implementing threat intelligence internally. External projects MITRE ATT&CK® matrix and Sigma are also leveraged. We discuss both MISP and OpenCTI as two comprehensive threat intel platforms for ingesting, tracking, and sharing threat intelligence.

We finish the section by using an alert triggered in our example company network as a pivot point into a potential attack.

TOPICS: Incident Response and Threat Hunting in the Enterprise; Managing Large-Scale Response; Intel-Driven Incident Response; Scalable & Collaborative Analysis with Timesketch

SECTION 2: Scaling Response and Analysis

Section 2 pivots directly from Section 1 as we continue to move into response mode. We will begin collecting evidence at scale to scope a potential intrusion against our example company, Stark Research Labs.

Moving beyond the analysis of commonly logged artifacts, we introduce the open-source Velociraptor tool as a powerful platform for incident response and threat hunting at scale. Velociraptor is adept at pulling forensic artifacts from across the enterprise, as well as providing analysts with a tool to deep dive individual hosts of interest.

One of many useful features of Velociraptor is its ability to push collected data into Elasticsearch. Elasticsearch is another powerful and flexible tool appropriate for any responder's toolkit. As such, we use Elasticsearch to ingest and process various data types, including data from Velociraptor, from the PowerShell IR framework, Kansa, and from the Log2timeline tool.

After having swept the network looking for indicators of compromise in EDR log data and with tools such as Velociraptor and Kansa, there will inevitably be a subset of hosts that warrant deeper dives. We present rapid response options for targeted data collections at scale, including multi-platform tools such as Velociraptor and CyLR.

TOPICS: EDR and EDR Bypass; Scaling Incident Response with Velociraptor; Scaling Analysis with ELK; Rapid Response Triage

SECTION 3: Modern Attacks Against Windows and Linux DFIR

Section 3 transitions to more traditional host-based forensic artifact analysis. The day starts with a look at some of the latest techniques for attacking Windows systems, including the now too-common ransomware attack. As part of looking for precursors to ransomware attacks, as well as other targeted attacks, we spend time focusing on attackers use of "living-off-the-land" techniques to avoid detection.

Following this initial discussion on Windows, the remaining part of the day focuses on Linux incident response and analysis.

FOR608 outlines common vulnerabilities in Linux systems and configurations, then covers common attacker exploits targeting these systems. Privilege escalation, persistence, and lateral movement are techniques we commonly associate with attacks against Windows environments, but they apply equally to Linux as well.

Providing students with the ability to investigate Linux intrusions is key goal of FOR608. Upon completion of the course, students will leave with important new skills and techniques for responding to large-scale intrusions across diverse enterprise networks.

TOPICS: Modern Attacks Against Windows; 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

In the next module, we move on to look at key aspects of the Apple macOS operating system. These hosts have become more prevalent in many enterprise networks. Therefore, it's important that incident responders have some understanding and training for responding to such systems. Before diving into the incident response techniques, we discuss the history and current ecosystem of macOS and Apple mobile devices.

After a discussion of the fundamentals, we turn our attention to the challenges and opportunities for responding to macOS incidents. Questions such as how best to acquire disk and triage data, how to review those acquisitions, and which logs and other artifacts are most useful in spotting suspicious activity, are all covered in detail.

After establishing a solid foundation for Linux and Mac forensic analysis, we then turn our attention to the concept of containerized microservices. Containers are a popular way to deploy applications and services in a reliable and repeatable way. The most common platform for containers is Docker, which is where we focus our attention in FOR608.

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

SECTION 5: Cloud Attacks and Response

This day is focused on responding to incidents in the major cloud platforms from Microsoft and Amazon. Although the analysis focuses on those platforms, we cover log analysis techniques, architecture designs, and automation initiatives that can be applied to just about any cloud provider. We also cover attacks instigated from cloud environments and the artifacts that may be left behind in such cases.

Cloud environments provide unique challenges for incident response, but some exciting opportunities too. A quick intro into these factors will start the day. Once again, we find that the MITRE ATT&CK® framework is useful for organizing our defenses and detections – specifically the Cloud Matrix.

Moving into Microsoft 365 (M365) and Azure, several popular SaaS offerings are discussed. These include M365 and Azure AD for hosted services like Exchange, SharePoint, and Active Directory authentication. Many organizations subscribe to these services, and predictably, attackers have become proficient at finding weaknesses in their implementations. We therefore look at many common attack scenarios against M365 and Azure.

The second part of the day delves into the Amazon Web Services (AWS) cloud platform. Its general architecture and components are covered to provide a solid foundation for those new to AWS.

The section concludes with discussions on architecting for response in the cloud for faster and more effective analysis. This involves setting up security accounts for a secure enclave within AWS. While the solutions presented in this section are AWS-centric, the concepts can (and should) be applied to almost any cloud platform with significant use by an organization.

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

SECTION 6: Capstone: Enterprise-Class IR Challenge

Section 6 will serve as a capstone for the class and a chance for students to put into practice the knowledge gained thus far. We will be providing an all-new Capture-the-Flag-style exercise that focuses on utilizing the tools and techniques discussed in the previous five sections. Students will be provided a data set from a compromised environment and will need to utilize the tools and techniques they've learned to uncover the steps of the breach, end-to-end.

As in most real-world incident response scenarios, students will work in teams to divide and conquer the analysis to solve this complex case most efficiently. As they work throughout the day, they will submit flags on a scoreboard and the winning team will be crowned at the end of the day based on the highest score.

TOPICS: Day 6 CTF Challenge

"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**