FOR509: Enterprise Cloud Forensics and Incident Response™

GCFR
Cloud Forensics Responder
giac.org/gcfr

6 Day Program | 36 CPEs | Laptop Required

Course Topics

- Cloud Infrastructure and IR data sources
- Microsoft 365 and Graph API Investigations
- Azure Incident Response
- AWS Incident Response
- Google Workspace Investigations
- GCP Incident Response

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where it is located
- Identify and utilize new data only available from cloud environments
- Utilize cloud-native tools to capture and extract traditional host evidence
- Quickly parse and filter large data sets using scalable technologies such as the Elastic Stack
- Understand what data is available in various cloud environments

What You Will Receive

- SOF-ELK(R) Virtual Machine – a publicly SOF-ELK(R) Virtual Machine - a publicly available appliance running the Elastic Stack and the course author's custom set of configurations and lab data. The VM is preconfigured to ingest cloud logs from Microsoft 365, Azure, AWS, Google Workspace and GCP. It will be used during the class to help students wade through the large number of records they are likely to encounter during a typical investigation.
- Case data to examine during class.
- Electronic workbook with detailed step-by-step instructions and examples to help you master cloud forensics

"FOR509 was absolutely awesome! The depth of knowledge is unparalleled. I see this becoming a very popular class in the future."

—Terrie Myerchin, **AT&T**

Find the Storm in the Cloud

FOR509: Enterprise Cloud Forensics and Incident Response will help you:

- Understand forensic data only available in the cloud
- Implement best practices in cloud logging for DFIR
- Learn how to leverage Microsoft Azure, AWS and Google Cloud Platform resources to gather evidence
- Understand what logs Microsoft 365 and Google Workspace have available for analysts to review
- Learn how to move your forensic processes to the cloud for faster data processing

With FOR509: Enterprise Cloud Forensics and Incident Response, examiners will learn how each of the major cloud service providers (Microsoft Azure, Amazon AWS and Google Cloud Platform) are extending analysts capabilities with new evidence sources not available in traditional on-premise investigations. From cloud equivalents of network traffic monitoring to direct hypervisor interaction for evidence preservation, forensics is not dead. It is reborn with new technologies and capabilities.

Incident response and forensics are primarily about following breadcrumbs left behind by attackers. These breadcrumbs are primarily found in logs. Your knowledge of the investigation process is far more important than the mechanics of acquiring the logs.

This class is primarily a log analysis class to help examiners come up to speed quickly with cloud based investigation techniques. It's critical to know which logs are available in the cloud, whether they are turned on by default, and how to interpret the meaning of the events they contain.

Numerous hands-on labs throughout the course will allow examiners to access evidence generated based on the most common incidents and investigations. Examiners will learn where to pull data from and how to analyze it to find evil. The data will be available in your VM rather than accessed directly via the cloud to ensure a consistent lab experience.

Business Takeaways

- Understand digital forensics and incident response as it applies to the cloud
- Identify malicious activities within the cloud
- Cost-effectively use cloud-native tools and services for DFIR
- Ensure the business is adequately prepared to respond to cloud incidents
- Decrease adversary dwell time in compromised cloud deployments

"Thanks a lot for FOR509 course. I believe this course provides a great way to get a really compressed introduction into the different cloud service providers and what is forensically possible there."

—Marc Stroebel, **HvS-Consulting AG**

Section Descriptions

SECTION 1: Microsoft 365 and Graph API

There is a universe of data out there to be discovered.

Before you can begin exploring the universe of cloud data, you must learn where and how it exists. In this section, you will learn about the most popular cloud architectures (IaaS, PaaS, SaaS) and how each changes your investigative possibilities. You will understand what logging and data access is provided by each cloud architecture and how to extract and process this data.

We will introduce SOF-ELK, an open-source SIEM made for enterprise log analysis that easily extends into cloud forensics. We then go into Microsoft 365 which is a SaaS platform that provides the Microsoft Office suite of applications, including Excel and Word. In addition, Microsoft 365 implements several communications and collaboration tools such as Exchange, SharePoint, and Teams. We finish the day by exploring the Microsoft Graph API and reviewing the logs that it generates.

TOPICS: Introducing SOF-ELK; Key Elements of Cloud for DFIR; Microsoft 365 Unified Audit Log; Microsoft Graph API

SECTION 2: Microsoft Azure

One of the most popular cloud providers for large enterprises is the Microsoft Azure cloud. Azure offers an impressive array of services and with that comes numerous data sources for us to explore. In this section we will learn about Azure tenant, subscription, and diagnostics logs. Finally, we will find out how to deploy our own analysis tools in the cloud.

TOPICS: Understanding Azure; Networking, VMs, and Storage; Log sources for IR; Virtual Machine Logs; In-cloud IR

SECTION 3: Amazon Web Service (AWS)

Now that we understand what's possible in the Cloud and the new DFIR evidence sources that exist for us, it's time to turn to the market leader in Cloud services. In this section we will explore how AWS can be used for the responder, how to deploy your own analysis system into your region, the new and relevant log sources for your investigation and how to bring it all together in lab scenarios designed to help you quickly solve the most common AWS cases.

TOPICS: Understanding AWS; Networking, VMs, and Storage; Log sources for IR; Event Drive Response; In-cloud IR

SECTION 4: Google Workspace

This section will start with a high-level overview of Kubernetes and the logs available in each of the cloud providers. As one of the first SaaS solutions for organizations dating back to 2006, Google Workspace has a wide array of evidence artifacts for investigators to use when conducting incident response or internal investigations. Knowing the various locations to extract evidence, and how that evidence differs depending on where it's extracted, form one of the key concepts for Google Workspace investigations. Students will see four of the most common attacks in Google Workspace and how to investigate those attacks in depth.

As with all the cloud platforms, students will see the limitations of preserved evidence and how to extend the lifetime of evidence in Google Workspace. Students will get hands-on access to evidence and be taught skills for how to best analyze Google Workspace evidence.

TOPICS: Kubernetes Forensics and IR; Understanding Google Workspace; Google Workspace Evidence; ATT&CKing Workspace

SECTION 5: Google Cloud

Google Cloud Platform (GCP) offers many services and fundamentally changes how identity access management is treated compared to AWS and Azure, along with building in a lot of security and evidence items that are extremely useful to an incident response team. Using a combination of the GCP platform, its built-in auditing, agent-based logging, and external log analysis tools like ELK. This section will teach DFIR professionals with limited knowledge of GCP how to conduct investigations into common attacks on GCP.

TOPICS: Understanding GCP; Log Sources, Collection and Log Routing; VM and Storage Investigations; Google Cloud Network Forensics

SECTION 6: Multicloud Intrusion Challenge

In the final section, students will split into teams to solve an intrusion that spans all three major cloud providers. Students will need to refer to all their new knowledge for the week and divide and conquer the evidence to find out how the intrusion occurred. Multiple interconnected cloud systems will be examined as students work to determine what happened.

Students will then present their findings to the class to determine which team will be deemed FOR509 Lethal Forensicators!

"FOR509 is very much needed in the industry as there is very little training out there for Cloud DFIR. So the fact that this course exists and is huge."

—Chester Le Bron Jr, **Northwestern Mutual**

Who Should Attend

- **Incident Response Team Members** who may need to response to security incidents/intrusions impacting cloud hosted software, infrastructure or platforms and need to know how to detect, investigate, remediate, and recover from compromised systems across the enterprise cloud.
- **Threat Hunters** who are seeking to understand threats more fully and how to learn from them in order to more effectively hunt threats and counter their tradecraft.
- **SOC Analysts** looking to better understand alerts, build the skills necessary to triage events, and fully leverage cloud log sources.
- **Experienced Digital Forensic Analysts** who want to consolidate and enhance their understanding of cloud-based forensics.
- **Information Security Professionals** who directly support and aid in responding to data breach incidents and intrusions.
- **Federal Agents and Law Enforcement Professionals** who want to master advanced intrusion investigations and incident response, and expand their investigative skills beyond traditional host-based digital forensics.
- **SANS FOR500, FOR508, SEC541, and SEC504 Graduates** looking to add cloud-based forensics to their toolbox.

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)

GCFR
Cloud Forensics Responder
giac.org/gcfr

GIAC Cloud Forensics Responder

The GCFR certification validates a practitioner's ability to track and respond to incidents across the three major cloud providers. GCFR-certified professionals are well-versed in the log collection and interpretation skills needed to manage rapidly changing enterprise cloud environments.

- Log generation, collection, storage and retention in cloud environments
- Identification of malicious and anomalous activity that affect cloud resources
- Extraction of data from cloud environments for forensic investigations