FOR509: Enterprise Cloud Forensics and Incident Response™

GCFR
Cloud Forensics Responder
giac.org/gcfr

6 Day Program	36 CPEs	Laptop Required

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 utilise new data only available from cloud environments
- Utilise 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

"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**

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

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 analyst's 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. This class focuses on log analysis 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, their retention, 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 analyse it to find evil.

What You'll Learn

- 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 resources to gather evidence
- Understand what logs Microsoft 365 and Google Workspace have available for analysts to review
- Gain a high-level understanding of Kubernetes and its log sources in each cloud
- Learn how to move your forensic processes to the cloud for faster data processing

Author Statement

"Many DFIR professionals have dismissed the cloud as 'someone else's computer' missing the wealth of new evidence sources and possibilities that now exist. From audit logs that attackers can't clear without full tenant compromise to the ability to turn on Netflow data with a single line of code/click and no additional hardware needed the cloud offers a world of new possibilities to those DFIR professionals who embrace what the cloud brings to them.

"FOR509 was written to give you a head start in understanding, analyzing, and solving cloud-based investigations. Not only do we cover the most popular cloud solutions on the market, but we also help the students to understand now just how to interpret the data but how they can take their detection and response capabilities to the next level. Cloud automation, flexible infrastructure on demand, and entire processing clusters on standby mean you can make your enterprise ready for an event at any scale. We've dealt with some of the biggest breaches in some of the biggest networks and we'll show students how they can be ready to do the same in the cloud."

—David Cowen

Section Descriptions

SECTION 1: Microsoft 365 and Graph API

Before exploring the universe of cloud data, you must understand where and how it exists. This section introduces foundational cloud concepts like snapshots and cloud flows. You will understand what kind of logging and data access is provided by each cloud architecture and the various log hierarchy to guide your investigations.

TOPICS: Course Introduction and SOF-ELK®; Key Elements of Cloud for DFIR; Microsoft 365 Unified Audit Log; Microsoft Graph API

SECTION 2: Microsoft Azure

In this section, you will learn to navigate Azure's various activity and diagnostics logs to track resources, investigate compromised virtual machines, and detect data exfiltration. We will also cover how to deploy your own analysis tools directly into the cloud for more efficient investigations.

TOPICS: Understanding Azure; Log Sources for IR; Virtual Machines; Storage and Networking; Resources

SECTION 3: Amazon Web Service (AWS)

This section explores how responders can leverage AWS for investigations, covering new and relevant log sources such as CloudTrail, VPC Flow logs, and S3 Access logs. In the labs, you will work through a realistic intrusion scenario that begins with the compromise of the AWS organization via a federated user account.

TOPICS: Understanding IR in AWS; Networking, VMs, and Storage; Virtual Networks; S3 Buckets; AWS Native Log Searching

SECTION 4: Kubernetes and Google Workspace

This section provides a foundational understanding of Kubernetes, the open-source container orchestration platform used by all major cloud providers. The course explains the evolution from traditional hardware to container deployments and breaks down the core architectural components.

TOPICS: Kubernetes Overview and Logs; Common Kubernetes Attacks; Understanding Google Workspace; Accessing Google Workspace Evidence; Investigating Google Workspace

SECTION 5: Google Cloud

This section equips DFIR professionals with the essential skills to investigate incidents within Google Cloud, starting with its unique approach to Identity and Access Management (IAM). You will learn to navigate Google Cloud's hierarchical structure of organizations, folders, and projects.

TOPICS: Google Cloud Overview and IAM; Logging; Virtual Machines; Cloud Storage and Networking

SECTION 6: Multicloud Intrusion Challenge

In this final capstone section, you will apply the knowledge gained throughout the week to a real-world challenge. Working in teams, you will investigate a complex intrusion that spans all three major cloud providers: AWS, Azure, and GCP. You must divide and conquer the evidence across multiple interconnected systems to determine the full scope of the incident. The challenge concludes with each team presenting its findings to the class to determine who will be named the 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.
- InfoSec 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)