FOR509: **Enterprise Cloud Forensics and Incident Response**

4 Day Program	24 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 utilize new data only available from Cloud environments
- Quickly parse and filter large data sets, using scalable technologies such as the Elastic Stack
- Learn how to profile attackers in different cloud environments
- Understand what data is available in different cloud environments

What You Will Receive

- SOF-ELK(R) Virtual Machine – a publicly available appliance running the Elastic Stack and the course author's custom set of configurations and dashboards. The VM is preconfigured to ingest cloud logs from AWS, Azure, and GCP, and will be used during the class to help students wade through the hundreds of millions of records they are likely to encounter during a typical investigation.
- Realistic case data to examine during class
- USB drive(s) loaded with case examples, tools, and documentation
- Exercise book with detailed step-by-step instructions and examples to help you master cloud forensics

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
- Properly handle rapid triage in cloud environments
- Learn how to leverage Microsoft Azure, AWS and Google Workspace resources to gather evidence
- Understand what Microsoft 365 has available for analysts to review
- Learn how to move your forensic process to the cloud for fast processing where the data lives

With Enterprise Cloud Forensics examiners will learn how each of the major cloud service providers (Microsoft Azure, Amazon AWS and Google Workspace) 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.

The new world does not end there. More organizations are moving critical resources into the cloud with Microsoft 365. Examiners no longer have direct access to the email servers and datastores for recovering actions; which means they need to learn the new methods available to them to recreate the same data. But why stop at recreation? These new platforms allow us to extend our reach to data we could not easily access before, which when properly configured, can allow for detection and remediation faster than ever before.

The assumption that a change in where or how data is stored always seems to lead to the false assumption that forensics is dead. With the cloud, forensics is given new capabilities and depth that do not exist in the on-premise world. Learn to preserve, configure and examine new sources of evidence that only exist in the Cloud. Learn how to bring your examination into the cloud and how to triage within the same environment. Constantly updated, the Enterprise Cloud Forensics course (FOR509) addresses today's need to bring examiners up to speed with the rapidly changing world of enterprise cloud environments, where their most valuable data is being uploaded to.

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.

Before, during, and after an investigation cloud resources are constantly changing, FOR509: Enterprise Cloud Forensics will train you and your team to turn on the logs you need for the future, work with the data you have today, and prepare to automate for tomorrow.

Section Descriptions

SECTION 1: Cloud Forensics Fundamentals and Microsoft 365

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. We will understand what kind of logging and data access is provided by each cloud architecture and how to extract and process the data.

We will introduce SOF-ELK an open source distribution made for enterprise and network forensics and analysis that easily extends into cloud forensics. We then go into Microsoft 365 which is a cloud-based service that provides the Microsoft Office desktop suite including applications such as Excel and Word. In addition, Microsoft 365 implements a number of communications and collaboration tools such are Exchange, SharePoint, Skype, and Teams.

TOPICS:
MODULE 1.1: What's the Cloud;
MODULE 1.2: Introducing SOF-ELK;
MODULE 1.3: Microsoft 365 Unified Audit Log (UAL)

SECTION 2: Amazon 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:
MODULE 2.1: Understanding AWS;
MODULE 2.2: Networking, VMs, and Storage;
MODULE 2.3: Log sources for IR;
MODULE 2.4: Event Drive Response;
MODULE 2.5: In-cloud IR

SECTION 3: 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 the various Azure activity and diagnostics logs. Finally, we will find out how to deploy our own analysis tools in the cloud.

TOPICS:
MODULE 3.1: Understanding Azure;
MODULE 3.2: Networking, VMs, and Storage;
MODULE 3.3: Log sources for IR;
MODULE 3.4: Virtual Machine Logs;
MODULE 3.5: In-cloud IR

SECTION 4: Google Cloud (GCP)

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:
MODULE 4.1: Understanding GCP;
MODULE 4.2: Log Sources, Collection & Log Routing;
MODULE 4.3: VM & Storage Investigations;
MODULE 4.4: GCP Network Forensics

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.