**2023 COURSE UPDATE**

FOR509

# Enterprise Cloud Forensics & Incident Response

FOR509: Enterprise Cloud Forensics addresses today's need to bring examiners up to speed with the rapidly changing world of enterprise cloud environments by uncovering the new evidence sources that only exist in the Cloud.

**Despite using multiple security tools to safeguard their cloud applications, 70% of organizations lack confidence in their ability to maintain consistent security measures across on-premise and multi-cloud environments.**

**Source: Radware Report**

Summer 2023 Update

Cloud environments delivers a challenge for Digital Forensic Investigators as they constantly get updated. The new update of FOR509 contains more than 50% new content with emphasis in new labs addressing the latest updates to Microsoft 365, Azure, AWS, Kubernetes, Google Workspace and Google Cloud Forensics.

## NEW CONTENT

- Expanded coverage of files being downloaded, deleted and otherwise breached in Microsoft 365.
- Coverage of the most popular forms of cloud based lateral movement using technologies such as Azure Run Commands and AWS SSM.
- Included coverage for AWS DNS logging via Route53 which allows the collection of accessed internet hosts.
- Use of SOFELK to find DNS C2 and other advanced attacker techniques.
- New Kubernetes coverage identifies the most common types of attacks and new full parser support allows cloud analysis to be done in one place.
- New open-source free tools to acquire and analyze Google Workspace logs.
- Included coverage of Google Policy Analyzer to answer questions about the current state the organization's Google Cloud.
- Easier ways to understand who and what has been accessed in Google Cloud IAM.

## UPDATED FEATURES

- Expanded support for Microsoft 365 with the ability to ingest more types of logs, better parsing of logs and expanded coverage of what's contained within for faster threat identification.
- Expanded open-source toolbox provides more options to extract Microsoft 365 logs (UAL) that can be used by organizations with either small or large user base.
- More coverage for finding malicious activity using Lightsail and other AWS services.
- Expanded coverage of AWS Systems Manager to include more threat hunting for lateral movement.
- Expanded escalation methods within cloud native environments, including novel techniques being exploited in the real world.
- Expanded Google Cloud VM coverage to find more data and real- world examples of what to hunt for within environments.

## NEW LABS

- Section 1 of the course added a new lab to cover real-world extortion scenario from a Microsoft 365 breach that tracks data been accessed, deleted and exfiltrated using examples within a network.
- Added more realistic data sets to cover the most common TTPs used by threat actors and applied them in a new scenario that extends over all five labs in Section 3 of the course.
- New Kubernetes lab  provides a hands-on experience in how to parse through Kubernetes logging to find malicious activity as well as the knowledge needed to understand what it all means.
- All new Google Cloud labs go from section to section to teach how to analyze new parts of Google Cloud while following the same incident to determine who, what, where and how the incident happened in the first place.

**80% of organizations encountered a significant security incident related to their cloud infrastructure within the past year.**

Source: Snyk's Report

"FOR509 is very much needed in the industry as there is very little training out there for Cloud DFIR. The fact that this course exists and is huge." - Chester L., Northwestern Mutual

GIAC CLOUD FORENSICS GCFR RESPONDER

**GIAC Cloud Forensic Responder (GCFR)**

For more information:
sans.org/FOR509

SANS | GIAC CERTIFICATIONS