FOR509

Enterprise Cloud Forensics and Incident Response

FOR509 is the most comprehensive multi-cloud forensics and incident response course available. It equips professionals with the advanced skills to investigate, analyze, and remediate security incidents across AWS, Azure, Google Cloud, Microsoft 365, Google Workspace, and Kubernetes. Students learn to uncover attacker activity, trace data exfiltration, and neutralize persistent threats in complex, cloud-native environments. With a strong emphasis on cross-platform evidence analysis and log correlation, the course ensures skills are transferable to any cloud provider and compatible with any investigative toolset to help respond quickly and effectively to modern cloud breaches.

"Over **92%** of large enterprises now operate in a multi-cloud environment, yet only **27%** have a unified incident response strategy." (Source: Flexera State of the Cloud Report 2025 & IDC Research)

Summer 2025 Update: FOR509 delivers now a significant expansion in multi-cloud DFIR coverage, adding deep dives into AWS, Azure, Google Cloud, Microsoft 365, Google Workspace, and Kubernetes. The update introduces new hands-on labs, a multi-cloud intrusion capstone, and enhanced tooling to address evolving attacker tradecraft, including advanced persistence methods, cloud-native service abuse, and cross-platform privilege escalation. These improvements equip students and teams with the skills to rapidly investigate, contain, and remediate breaches in today's complex, multi-cloud environments.

New Content

- •Expanded multi-cloud coverage across AWS, Azure, Google Cloud, Microsoft 365, Google Workspace, and Kubernetes to prepare students for any cloud breach.
- •New methods for detecting compromised accounts, tracking suspicious logins, and preventing data theft from cloud storage services.
- •Practical skills for investigating rogue virtual machines, abuse of OAuth in Google Workspace, and privilege escalation.
- •Enhanced Kubernetes forensics covering malicious containers, API server compromises, and crypto mining.
- •Step-by-step workflows for analyzing and tracking cross-cloud attacks from initial compromise to remediation.

Updated Features

- •25+ new and refreshed hands-on labs simulate real-world attacks, so students leave with directly applicable skills that organizations can rely on immediately during active investigations.
- •A multi-cloud intrusion capstone challenge takes teams through an investigation spanning AWS, Azure, and Google Cloud, strengthening collaboration skills and preparing organizations for coordinated, cross-platform responses.
- •The enhanced SOF-ELK® VM with updated log parsers for all supported environments minimizes setup time for students, allowing them to focus on analysis—translating to faster readiness and efficiency in real-world operations.
- •Integration of modern tools like AWS Athena/Detective, Microsoft KQL, and Google Policy Analyzer equips individuals with current industry techniques, enabling organizations to adopt the latest investigative methods without added ramp-up time.

Lab Refresh

- •Four new Microsoft 365 labs use Unified Audit Log, sign-in, and Graph API data to investigate suspicious emails, data theft, and unusual logins—improving detection skills and organizational response.
- •Azure labs teach detection of managed identity abuse, privileged role changes, and varied exfiltration methods, strengthening defenses against persistent threats.
- •Five AWS labs on CloudTrail logs cover account enumeration, illicit API keys, rogue VMs, and data exfiltration, sharpening forensic capabilities and accelerating incident response.
- •Google Workspace is fully re-written with three labs using Groups, Chat, and other sources to investigate SaaS-targeted attacks and leverage built-in response tools for faster containment.
- •GCP labs focus on compromised service accounts, exploitation of resources, and persistence, using Policy Analyzer and log queries to uncover and stop malicious activity.
- •The Capstone Challenge tests all skills in a simulated multi-cloud breach across AWS, Azure, and GCP, proving readiness for real-world incidents.

For more information: sans.org/FOR509

SANS | GIAC CERTIFICATIONS