SEC502: **Cloud Security Tactical Defense™**

GCLD
Cloud Security Essentials
giac.org/gcld

5 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Identify cloud security weaknesses and risks in CSP offerings
- Navigate challenges and choose effective cloud security controls
- Protect sensitive data and ensure accountability with cloud logging
- Assess CSP trustworthiness using documentation and audits
- Secure management access and deploy native network controls
- Perform penetration testing and leverage top CSP services
- Communicate cloud security concepts with teams and leadership

Business Takeaways

- **Reduce Risk:** Secure cloud environments and prevent vulnerabilities
- **Protect Resources:** Safeguard computing power and control costs
- **Meet Compliance:** Align with regulatory standards
- **Increase Efficiency:** Automate for streamlined operations
- **Support Your Team:** Improve security and staff retention
- **Preserve Reputation:** Defend your brand through strong cloud practices
- **Earn Trust:** Strengthen customer confidence with reliable protection

"Solid content, good pace, and great explanations, plus it's helpful to see how all of these cloud and security concepts can be integrated and applied in real life."

—Craig Harris, **SMBC**

License to Defend Cloud Infrastructure

Enterprises today face a rapidly evolving threat landscape in the cloud. From misconfigured services and excessive privileges to lateral movement and data exfiltration, cloud environments require more than basic knowledge—they demand tactical defense skills.

SEC502 builds on existing security and infrastructure experience, helping practitioners step confidently into cloud security roles. Through live AWS and Azure environments, participants translate their InfoSec knowledge into practical cloud defense capabilities by securing identities, protecting data, and controlling network access in modern cloud platforms.

The course develops tactical expertise across identity, data, and network layers while addressing real-world risks such as excessive privileges, credential abuse, and lateral movement. It prepares professionals to operate effectively in cloud environments and validate their expertise through the GIAC Cloud Security Essentials (GCLD) certification.

Hands-On Labs

SEC502 includes 40 scenario-driven labs in real AWS and Azure platforms, allowing you to apply security controls directly in live cloud environments. A self-paced CloudWars Capture-the-Flag challenge further reinforces decision-making and defensive skills across both platforms, helping practitioners operate confidently from day one.

"I learned a lot, went deeper technically than I expected to, and feel like this was absolutely a great use of my time. The instructors and TAs are top notch and made my experience taking this course a very positive one."

—Marni Reemer, **AWS**

GCLD
Cloud Security Essentials
giac.org/gcld

GIAC Cloud Security Essentials

The GIAC Cloud Security Essentials (GCLD) certification validates a practitioner's ability to implement preventive, detective, and reactionary techniques to defend valuable cloud-based workloads.

- Evaluation of cloud service provider similarities, differences, challenges, and opportunities
- Planning, deploying, hardening, and securing single and multicloud environments
- Basic cloud resource auditing, security assessment, and incident response

Section Descriptions

SECTION 1: Identity and Access Management (IAM)

Understand the role of Identity and Access Management (IAM) in cloud security. Secure identities and enforce least privilege using cloud vendor IAM tools.

TOPICS: Cloud Accounts and Groups; Policies and Permissions; Identity Guardrails; Temporary Credentials and Secrets Management; Cloud Application Account Architecture; Cloud Resource and External Identities; Zero Trust

SECTION 2: Compute and Configuration Management

Learn to secure cloud compute across IaaS, PaaS, and related service models while addressing the added complexity of operating virtual machines and workloads in cloud environments.

TOPICS: Secure VM Deployment; Host Configuration Management; Image Management, App Security; Threat Modeling; Beyond IaaS; Container Services; IaC

SECTION 3: Data Protection

Classify, encrypt, and manage sensitive data in the cloud. Address legal, contractual, and lifecycle risks. Learn how to prevent data exposure, enforce encryption in transit and at rest, and build resilience into cloud storage and productivity services.

TOPICS: Legal and Contractual Concerns; Cloud Storage; Availability; Data Hunting; Data-at-Rest Encryption; Data-in-Transit; Productivity Services; Lifecycle Management

SECTION 4: Networking and Detection

Dive into cloud networking with segmentation, secure remote management, and improved visibility. Learn to control data flows, apply cloud-native protections, and detect threats through effective logging and monitoring.

TOPICS: Cloud Network Architecture; Remote Management of IaaS; Cloud Routing, Traffic Management, and Connectivity; Threat-Aware Network Security; Cloud Account and Service Monitoring; Log Generation, Collection, and Analysis; Network Visibility; Cloud Detection Services

SECTION 5: Compliance, Incident Response, and Penetration Testing

Address compliance, risk management, penetration testing, and incident response within modern cloud environments. Extend asset inventory and governance into the cloud, leverage CASB, CSPM, and CWPP capabilities, and assess provider controls using audit reports and shared responsibility models. Conduct cloud-focused penetration testing, detect breaches early, and perform initial forensic analysis to contain threats effectively.

TOPICS: Cloud Asset Discovery and Inventory; Governance, Privacy, and Risk Management in Cloud; Cloud-Based AI Security; CNAPP; Penetration Tests; Incident Response and Forensics; Serverless for Defenders

SECTION 6: CloudWars

CloudWars* is a self-paced capture-the-flag (CTF) challenge that reinforces the tactical skills from the course. Students secure a vulnerable multicloud environment by identifying misconfigurations and defending against simulated threats.

*In-Person and Live Online students have two weeks of post-course access to the CTF. OnDemand students access CloudWars as part of their lab provisioning.

"Great way to bring participants up to speed in the cloud security principles. I am a novice to the area and the course was at the right level for me to come up to speed. Thank you for this course, it answers many questions I had about the cloud. Nice to walk through this course prior to leaping into cloud adoption at our organization."

—Natalija Saviceva, **FI**

Who Should Attend

SEC502 is designed for experienced practitioners transitioning into cloud security or reinforcing core cloud defense skills.

- Cloud security engineers
- Cloud security analysts
- System administrators moving into cloud roles
- Network engineers transitioning to cloud security
- IT infrastructure professionals
- Developers working in cloud environments who need security depth
- Risk and compliance professionals responsible for cloud security
- Cloud security auditors
- Security managers overseeing cloud environments
- Cloud architects seeking stronger operational security grounding

NICE Framework Work Roles

- Security Architect (OPM 652)
- Systems Security Analyst (OPM 461)
- Information Systems Security Manager (OPM 722)