SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC502:™ Cloud Security Tactical Defense™

GCLD
Cloud Security Essentials
giac.org/gcld

5	36	Laptop
Day Program	CPEs	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: Cloud Security Tactical Defense™ prepares you to identify security weakness and protect data across cloud environments while address compliance challenges. Students gain experience through 40 immersive, live-fire labs and a remote capture-the-flag (CTF) challenge that reinforces real-world readiness. The course focuses on practical application, enabling you to secure identities, harden systems, detect threats, and lead response efforts with confidence.

Hands-On Labs

SEC502™ offers 15+ hours of hands-on labs in real AWS and Azure environments, allowing students to apply concepts through practical, scenario-based exercises. The labs follow a "choose your own adventure" format, giving students the option to work in their preferred cloud platform.

The Cloud Service Provider (CPS) environments virtual machines, storage, and security tools designed to mirror real-world conditions.

A gamified, self-paced CloudWars challenge reinforces skills by testing students across both cloud platforms. This immersive experience ensures learners are prepared to defend cloud environments 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

sans.org/sec502

- Watch a preview of this course
- Discover how to take this course: Online, In-Person

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: Segment Accounts; Least Privilege Policies; Zero Trust; Temporary Credentials and Manage Secrets; Strengthen Identity Controls

SECTION 2: Compute and Configuration Management

Deploy and harden virtual machines and containers. Leverage Infrastructure as Code (IaC) to automate security baselines and detect insecure configurations.

TOPICS: Secure VM Deployment; Host Configuration Management; Image Management, App Security; Threat Modeling; PaaS & SaaS Challenges; Container Services; IaC

SECTION 3: Data Protection

Classify, encrypt, and manage sensitive data in the cloud. Address legal, contractual, and lifecycle risks. Explore misconfiguration detection and resilience planning.

TOPICS: Cloud Storage; Data Hunting; Data in Transit; Data at Rest; Encryption; Availability; Lifecycle Management; Legal and Contract Concerns

SECTION 4: Networking and Detection

Secure and monitor cloud network traffic. Segment workloads, configure cloud-native detection, and build effective logging pipelines to support real-time visibility.

TOPICS: Public Cloud vs. On-Prem Networking; Remote Management of IaaS; Segmentation; Logging Services; Log Collection and Analysis; Network Visibility; Cloud Detection Services

SECTION 5: Compliance, Incident Response, and Penetration Testing

Explore compliance frameworks, audit reports, and privacy considerations for CSP risk assessments. Learn how to assess secure cloud architecture using the Cloud Controls Matrix, conduct cloud-based penetration testing, and respond to incidents using CSP logs and forensic techniques. Gain hands-on experience with CASB, CSPM, and CWPP tools to enhance cloud visibility and control.

TOPICS: Cloud Inventory; Privacy and Risk Management; Cloud-Based AI Security; CABs; CSPMs and CWPPs; 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.

Who Should Attend

- Cloud security engineers
- Cloud security analysts
- System administrators
- Risk managers
- Security managers
- Cloud security auditors
- Cloud security professionals
- Cloud architects
- IT professionals
- Developers working in cloud environments
- Compliance officers responsible for cloud security
- Network engineers transitioning to cloud security roles

NICE Framework Work Roles

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

> **"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**

sans.org/sec502

- Watch a preview of this course
- Discover how to take this course: Online, In-Person