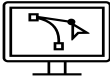# SEC502: Cloud Security Tactical Defense

SEC502: Cloud Security Tactical Defense is the next step in the evolution of **SEC488: Cloud Security Essentials**, aligned to meet today's expectations for comprehensive, applied cloud security training. While SEC488 was originally written as a 500-level course, it was listed as a 400-level. This transition ensures the course is accurately positioned as a tactical, 500-level offering—matching both industry expectations and the training investments made by organizations.

The 5-day format streamlines delivery without sacrificing depth, offering updated, hands-on labs in both AWS and Azure. Students will develop the skills to configure, monitor, and defend cloud environments, handle misconfigurations, and lead incident response efforts with confidence.

94% of enterprise organizations use cloud services, according to the 2025 Flexera State of the Cloud Report. This widespread adoption underscores the growing demand for skilled professionals who can secure and manage cloud environments.

Source: Flexera 2025 State of the Cloud Recap – SoftwareOne

NEW CONTENT

- **Expanded Focus on Least Privilege IAM Design, Including Auditing and Automation:** Helps prevent unauthorized access and lateral movement by teaching how to implement and audit precise, automated identity controls.

- **Aligns with Zero Trust Principles and Hybrid Cloud Security Best Practices:** Equips you to apply Zero Trust principles across AWS and Azure, creating consistent, breach-resistant defenses in hybrid environments.

- **Tackles Compliance Frameworks:** Prepares students to meet requirements like GDPR and HIPAA with practical controls and audit-aligned strategies they can apply immediately.

- **Cloud Resource Telemetry, Detection, and Response:** Enables proactive threat detection, investigation, and containment through integrated cloud telemetry and detection capabilities while augmenting existing logging tools to deliver faster, more effective incident response.

LAB REFRESH

- **41 Hands-On Labs**
  Train like you work—with hands-on labs in real-world cloud infrastructure that mirror the real challenges defenders face, not just theoretical exercises.

- **Realistic Attack Scenarios**
  Practice detecting and responding to misconfigurations, privilege escalation, and cloud-native threats—skills you'll use on day one back at work.

- **Immersive CloudWars CTF**
  Reinforce what you've learned by stepping into the attacker's world through a post-course Capture-the-Flag challenge designed to test your skills in realistic, high-pressure conditions.

UPDATED FEATURES

- **Streamlined from 6 Days to 5:** Makes high-impact cloud security training more accessible with less time away from work, without sacrificing substance.

- **CloudWars CTF Now Post-Course:** A flexible, self-paced Capture-the-Flag challenge gives students the opportunity to reinforce their skills on their own time—within 2 weeks of class.

- **GCLD certification** remains unchanged and respected across the industry.

- **Earn 36 CPEs,** with the credit amount unchanged and applicable toward certification renewal.

GIAC Cloud Security Essentials (GCLD)

For more information: sans.org/SEC502

SANS | GIAC CERTIFICATIONS