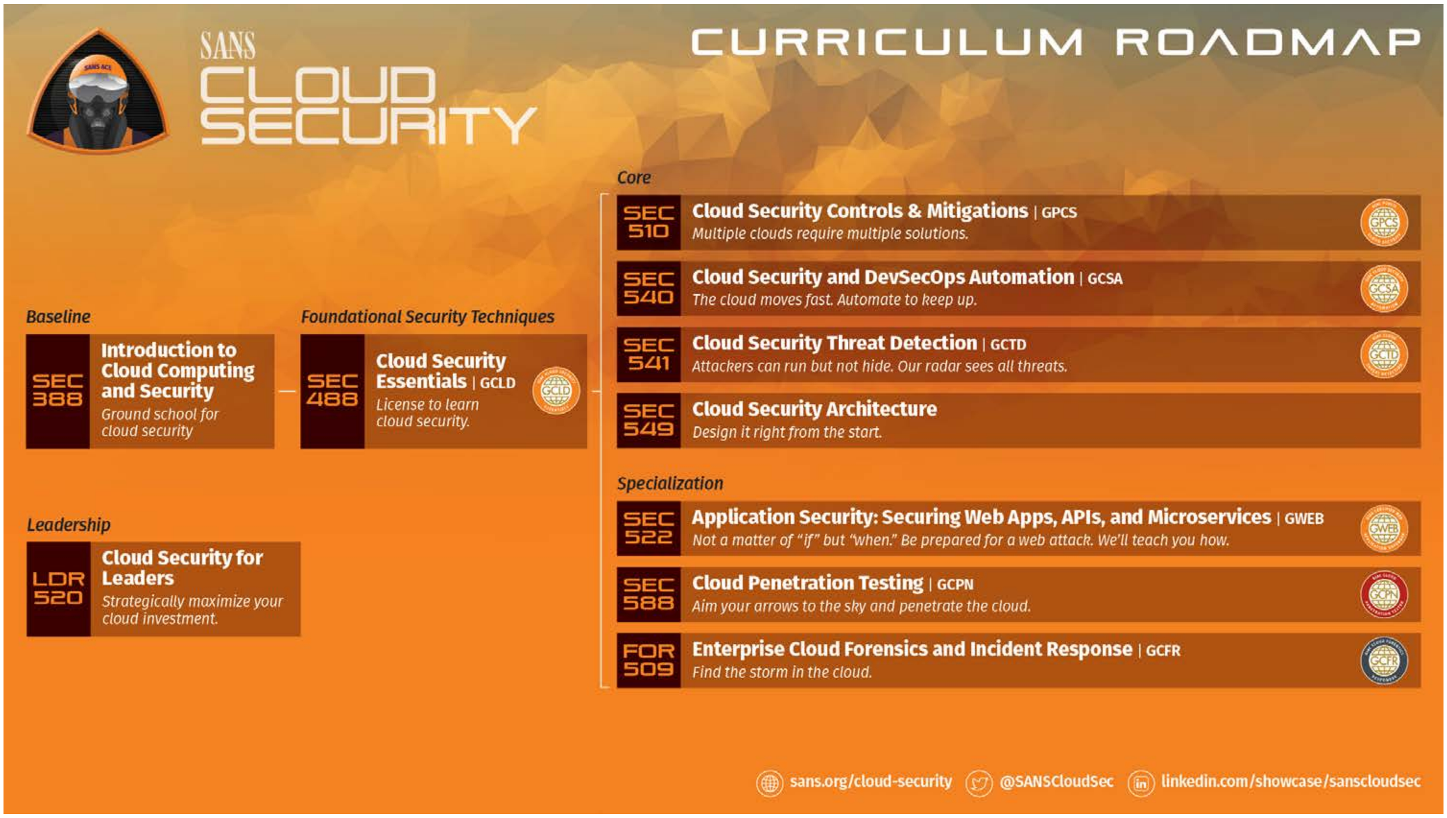
SANS | GIAC CERTIFICATIONS

SANS CLOUD SECURITY

Supporting Your Journey to Becoming a #SANSCloudAce

SANS Cloud Security focuses the deep resources of SANS on the growing threats to The Cloud by providing training, certification, research, and community initiatives to help security professionals build, deploy and manage secure cloud infrastructure, platforms, and applications.

SANS Cloud Security Curriculum provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and applications in the cloud against the most dangerous threats. The courses are full of important and immediately useful techniques that you can put to work as soon as you return to your office. The curriculum has been developed through a consensus process involving industry leading engineers, architects, administrators, developers, security managers, and information security professionals, and address public cloud, multicloud, and hybrid-cloud scenarios for the enterprise and developing organizations alike.



SANS CLOUD SECURITY

CURRICULUM ROADMAP

Baseline

SEC388 **Introduction to Cloud Computing and Security**
Ground school for cloud security

Foundational Security Techniques

SEC488 **Cloud Security Essentials** | GCLD
License to learn cloud security.

Leadership

LDR520 **Cloud Security for Leaders**
Strategically maximize your cloud investment.

Core

SEC510 **Cloud Security Controls & Mitigations** | GPCS
Multiple clouds require multiple solutions.

SEC540 **Cloud Security and DevSecOps Automation** | GCSA
The cloud moves fast. Automate to keep up.

SEC541 **Cloud Security Threat Detection** | GCTD
Attackers can run but not hide. Our radar sees all threats.

SEC549 **Cloud Security Architecture**
Design it right from the start.

Specialization

SEC522 **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB
Not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how.

SEC588 **Cloud Penetration Testing** | GCPN
Aim your arrows to the sky and penetrate the cloud.

FOR509 **Enterprise Cloud Forensics and Incident Response** | GCFR
Find the storm in the cloud.

sans.org/cloud-security @SANSCloudSec linkedin.com/showcase/sanscloudsec

SEC388: Introduction to Cloud Computing and Security

Ground School for Cloud Security

Today's world of cyber security moves quickly. Cloud security moves even faster, so getting started or moving into a career in this field can be intimidating if you do not have the foundation to be successful. SANS SEC388 solves this problem by helping you to learn the foundational elements of modern cloud computing and security. This course kicks off your journey to becoming a SANS Cloud Ace by taking an introductory yet critical look at cloud security. This course focuses on Azure and AWS, and shows you how to interact with each cloud provider by familiarizing you with common terminology, cloud services, security concerns, and solutions to cloud-based security shortcomings. Through hands-on labs, SEC388 puts you in real-world scenarios that challenge you to learn more about AWS, Azure, and relevant cloud computing and security concepts.

Daily Topics:

1. Account Set Up and Cloud Computing
2. Compute, Storage, and Networking
3. Threats and Solutions

3-Day Course	18 CPEs	Baseline

"This is a great course for system administrators and security practitioners who are transitioning, or thinking about transitioning, from a primarily on-premises workload to a public cloud workload."

—Flint Gatrell

SEC488: Cloud Security Essentials

GCLD
Cloud Security
Essentials
giac.org/gcld

License to Learn Cloud Security

More businesses than ever are moving sensitive data and shifting mission-critical workloads to the cloud, and not just to one cloud service provider (CSP). Organizations are responsible for securing their data and mission-critical applications in the cloud. The benefits in terms of cost and speed of leveraging a multicloud platform to develop and accelerate delivery of business applications and analyze customer data can quickly be reversed if security professionals are not properly trained to secure the organization's cloud environment and investigate and respond to the inevitable security breaches. New technologies introduce new risks. Help your organization successfully navigate both the security challenges and opportunities presented by cloud services.

Daily Topics:

1. Identity and Access Management
2. Compute and Configuration Management
3. Data Protection and Automation
4. Networking and Logging
5. Compliance, Incident Response, and Penetration Testing
6. CloudWars

6-Day Program	36 CPEs	Foundational

"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

SEC510: Cloud Security Controls & Mitigations

GPCS
Public Cloud Security
giac.org/gpcs

Multiple clouds require multiple solutions.

Today's organizations depend on complex, multicloud environments which must support hundreds of different services across multiple clouds. These services are often insecure by default. Similar services in different Cloud Service Providers (CSPs) need to be protected using very different methods. Security teams need a deep understanding of AWS, Azure, and Google Cloud services to lock them down properly. Checking off compliance requirements is not enough to protect the confidentiality, integrity, and availability of your organization's data, nor will it prevent attackers from taking your critical systems down. With the right controls, organizations can reduce their attack surface and prevent security incidents from becoming breaches. Mistakes happen. Limit the impact of the inevitable.

Daily Topics:

1. Cloud Identity and Access Management
2. Cloud Virtual Networks
3. Cloud Data Security
4. Cloud Application Services and User Security
5. Multicloud and Cloud Security Posture Management

5-Day Program | 38 CPEs | Core

> **"Overall, this was a great class for Security practitioners to understand and identify misconfigurations across the 'Big 3' (AWS, Azure, and GCP) cloud providers."**
>
> —Dustin Odya, The OCC

SEC522: Application Security: Securing Web Apps, APIs, and Microservices

GWEB
Web Application Defender
giac.org/gweb

It's not a matter of " if" but "when." Be prepared for a web attack. We'll teach you how.

Web Applications are increasingly distributed. What used to be a complex monolithic application hosted on premise has become a distributed set of services incorporating on-premise legacy applications along with interfaces to cloud-hosted and cloud-native components. Because of this coupled with a lack of security knowledge, web applications are exposing sensitive corporate data. Security professionals are asked to provide validated and scalable solutions to secure this content in line with best industry practices using modern web application frameworks. Attending this class will not only raise awareness about common security flaws in modern web applications, but it will also teach students how to recognize and mitigate these flaws early and efficiently.

Daily Topics:

1. Web Fundamentals and Secure Configurations
2. Input-Related Defenses
3. Authentication and Authorization
4. Web Services and Front-End Security
5. APIs and Microservices Security
6. DevSecOps & Defending the Flag

6-Day Program | 36 CPEs | Specialization

> **"This training is essential for anyone who needs to understand web protocol and application security and their limitations. This course provides a practical approach to many theoretical scenarios with relevant POCs within the course work."**
>
> —Joel Samaroo, Visa Inc.

SEC540: Cloud Security and DevSecOps Automation

GCSA
Cloud Security Automation
giac.org/gcsa

5-Day Program | 38 CPEs | Core

The cloud moves fast. Automate to keep up.

Organizations are moving to the cloud to enable digital transformation and reap the benefits of cloud computing. However, security teams struggle to understand the DevOps toolchain and how to introduce security controls in their automated pipelines responsible for delivering changes to cloud-based systems. Without effective pipeline security controls, security teams lose visibility into the changes released into production environments. SEC540 provides security professionals with a methodology to secure modern Cloud and DevOps environments. By embracing the DevOps culture, students will walk away from SEC540 battle-tested and ready to build to their organization's Cloud & DevSecOps Security Program.

Daily Topics:

1. DevOps Security Automation
2. Cloud Infrastructure Security
3. Cloud Native Security Operations
4. Microservice and Serverless Security
5. Continuous Compliance and Protection

> **"Every single person I've sent to class has loved it. It's been transformational for them because it goes beyond security concepts and teaches how modern operations and DevOps works. It's also impactful sending developers (who are not working in cloud yet) because they want to develop in cloud and get into concepts like Infrastructure as Code."**
> —Brett Cumming

SEC541: Cloud Security Threat Detection

GCTD
Cloud Threat Detection
giac.org/gctd

5-Day Program | 30 CPEs | Core

Attackers can run but not hide. Our radar sees all threats.

The rapid adoption of cloud services has created exciting new business capabilities and new cyber-attack opportunities. To detect these threats, companies require skilled security analysts who understand attack techniques, perform cloud security monitoring and investigations, and detection capabilities across the organization. The SEC541 course focuses on Cloud Threat Detection, covering various attack techniques used against cloud infrastructure and teaching the observation, detection, and analysis of cloud telemetry. With 20 hands-on labs and CTF, this course equips security analysts, detection engineers, and threat hunters with practical skills and knowledge to safeguard their organization's cloud infrastructure against potential threats. Upon completion, you can apply these newfound skills to help keep your organization's cloud infrastructure secure.

Daily Topics:

1. Management Plane and Networking Logging
2. Computer and Cloud Services Logging
3. Cloud Service and Data Discovery
4. Microsoft Ecosystem
5. Automate Response Actions and CloudWars

> **"This had the right mix of AWS infrastructure background and methods of using AWS log data for threat hunting."**
> —Brad Schonhorst, Sony

SEC549: Cloud Security Architecture

5-Day Program | 30 CPEs | Core

Design it right from the start.

The age of cloud computing has arrived as organizations have seen the advantages of migrating their applications from traditional on-premises networks. However, the rapid adoption of cloud has left architects scrambling to design on this new medium. A shift to the cloud requires cybersecurity professionals to reorient their security goals around a new threat model to enable business requirements while improving their organization's security posture. SEC549 is here to help enable this shift. The course takes an architectural lens to enterprise-scale, cloud infrastructure challenges. We address the security considerations architects need to address when tasked with business expansion into the cloud, from the centralization of workforce identity and network security controls, to the secure usage of shared cloud-hosted data, and the design of effective logging strategies.

Daily Topics:

1. Cloud Account Management and Identity Foundations
2. Implementing an Identity Perimeter in the Cloud
3. Network Access Perimeters for the Cloud
4. Data Access Perimeters in the Cloud
5. Enabling the Cloud-Focused SOC

> **"The labs were great! I enjoyed every second of this course and look forward to future SEC549 courses."**
> —Nevan Beal, Raymond James

SEC588: Cloud Penetration Testing

GCPN
Cloud Penetration Tester
giac.org/gcpn

6-Day Program | 36 CPEs | Specialization

Aim your arrows to the sky and penetrate the Cloud.

SEC588 will equip you with the latest in cloud focused penetration testing techniques and teach you how to assess cloud environments. In this course we dive into topics like cloud based microservices, in-memory data stores, serverless functions, Kubernetes meshes, and containers, as well as identifying and testing in cloud-first and cloud-native applications. You will also learn specific tactics for penetration testing in Azure and AWS, particularly important given that Amazon Web Services and Microsoft account for more than half of the market. It's one thing to asses and secure a datacenter, but it takes a specialized skill-set to truly assess and report on the risk that an organization faces if their cloud services are left insecure.

Daily Topics:

1. Architecture, Discovery, and Recon at Scale
2. Attacking Identity Systems
3. Attacking and Abusing Cloud Services
4. Vulnerabilities in Cloud-Native Applications
5. Infrastructure Attacks and Red Teaming
6. Capstone Event

> **"It's crucial information before you put your data in a cloud."**
> —Maria Lopez, NVCC

> **"SEC588 taught me more than I expected. With the rapid development of new technologies offered by cloud providers, SEC588 has given me an important framework for cloud pen testing."**
> —Jonus Gerrits, Phillips66

FOR509: Enterprise Cloud Forensics & Incident Response

GCFR
Cloud Forensics Responder
giac.org/gcfr

6-Day Program	36 CPEs	Specialization

Find the storm in the Cloud

The world is changing and so is the data we need to conduct our investigations. Cloud platforms change how data is stored and accessed. They remove the examiner's ability to put their hands directly on the data. Many examiners are trying to force old methods for on-premise examination onto cloud hosted platforms. Rather than resisting change, examiners must learn to embrace the new opportunities presented to them in the form of new evidence sources. FOR509 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.

Daily Topics:

1. Microsoft 365 and Graph API
2. Microsoft Azure
3. Amazon Web Service (AWS)
4. Google Workspace
5. Google Cloud
6. Multi-Cloud Intrusion Challenge

> **"FOR509 is very much needed in the industry as there is very little training out there for Cloud DFIR. So the fact that this course exists and is huge."**
> —Chester Le Bron Jr, Northwestern Mutual

LDR520: Cloud Security for Leaders

5-Day Program	30 CPEs	Leadership

Strategically Maximize Your Cloud Investment

Cybersecurity leadership is no longer just about technology. It is ultimately about organizational change - change not only in how people think about cybersecurity but in what they prioritize and how they act, from the Board of Directors to every corner of the organization. Students will learn how to build, manage, and measure a strong cybersecurity culture by leveraging the latest in organizational change models and real-world lessons learned. In addition, students will apply everything they learn through a series of 16 interactive labs and case studies.

Daily Topics:

1. Cloud Security Fundamentals and Identity Management
2. Cloud Security Environment Protection and Architecture
3. Data Protection, Security Detection, and Response
4. Securing Workload and Security Assurance
5. Multicloud and Capstone Exercise

> **"I loved the labs. They really help emphasize what we are learning."**
> —Jana Laney

SANS CLOUD SECURITY

FLIGHT PLAN TO BECOMING A CLOUD ACE

Level	Course	DevOps Professionals	Cloud Security Analyst	Cloud Security Engineer	Cloud Security Architect	Cloud Security Manager
BASELINE	**SEC388: Introduction to Cloud Computing and Security**		●			●
FOUNDATIONAL	**SEC488: Cloud Security Essentials** GIAC Cloud Security Essentials (GCLD)		●	●	●	●
CORE	**SEC510: Cloud Security Controls & Mitigations** GIAC Public Cloud Security (GPCS)	●	●	●	●	
	SEC540: Cloud Security and DevSecOps Automation GIAC Cloud Security Automation (GCSA)	●		●	●	
	SEC541: Cloud Security Threat Detection GIAC Cloud Threat Detection (GCTD)		●	●		
	SEC549: Cloud Security Architecture			●	●	●
SPECIALIZATION	**SEC522: Application Security: Securing Web Apps, APIs, and Microservices** GIAC Certified Web Application Defender (GWEB)	●				
	SEC588: Cloud Penetration Testing GIAC Cloud Penetration Tester (GCPN)		●			
	FOR509: Enterprise Cloud Forensics & Incident Response GIAC Cloud Forensics Responder (GCFR)		●	●		
LEADERSHIP	**LDR520: Cloud Security for Leaders**				●	●

Level Definitions

- **Baseline –** Courses that impart the baseline skills required of any information security professional involved in Cloud Security, whether active practitioner or manager
- **Foundational –** Courses that provide the basic knowledge to introduce students to a required skill set for the Cloud Security industry specifically
- **Core –** Courses that prepare professionals for more focused job functions in Cloud Security, including manager, architect, engineer, analyst, and developer
- **Specialization –** Courses for critical, advanced skills, or specialized roles in Cloud Security
- **Leadership –** Courses that prepare leaders to make sound strategic business decisions in regards to cloud security planning and implementation

Role Descriptions

- **DevOps Professional –** Responsible for code creation
- **Cloud Security Analyst –** Responsible for deciphering
- **Cloud Security Engineer –** Responsible for building
- **Cloud Security Architecture –** Responsible for designing
- **Cloud Security Manager –** Responsible for leading

HOW WE ARE DIFFERENT

- **Security Focused –** Providing technical training to properly secure services and workloads in the cloud
- **Multicloud Approach –** Providing training and comparisons on the Big Three public cloud providers
- **Hands-on Labs –** Extensively focuses on “the how” to properly deploy and secure a cloud environment using virtual machines, lab environments, and repeatable exercises
- **Instructors –** Versatile, real-world security practitioners
- **Courseware –** Providing access to slides, notes, and audio files for future reference

RESOURCES

Landing Page – www.sans.org/cloud-security

Twitter – @SANSCloudSec

LinkedIn – www.linkedin.com/showcase/sanscloudsec

YouTube – www.youtube.com/c/SANSCloudSecurity

Discord Channel – www.sansurl.com/cloud-discord