



SANS CLOUD SECURITY

SANS | GIAC
CERTIFICATIONS

Cloud Courses, Events and Free Resources

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



SEC488: Cloud Security Essentials
License to Learn Cloud Security



**SEC510: Public Cloud Security:
AWS, Azure, and GCP**
Multiple clouds require multiple solutions.



**SEC522: Defending Web Applications
Security Essentials**
It's not a matter of "if" but "when."
Be prepared for a web attack.
We'll teach you how.

**SEC534: Secure DevOps:
A Practical Introduction**
Principles! Practices! Tools! Oh my. Start your
journey on the DevSecOps road here.



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

**SEC541: Cloud Security Monitoring
and Threat Detection**
Attackers can run but not hide.
Our radar sees all threats.

**SEC557: Continuous Automation for
Enterprise and Cloud Compliance**

Using Cloud Security and DevOps Tools to
Measure Security and Compliance

**SEC584: Cloud Native Security:
Defending Containers & Kubernetes**
Deploy securely at the speed of cloud native.



SEC588: Cloud Penetration Testing
Aim your arrows to the sky and
penetrate the cloud.

**FOR509: Enterprise Cloud Forensics
and Incident Response**
Find the Storm in the Cloud

**MGT516: Managing Security
Vulnerabilities: Enterprise and Cloud**
Stop treating the symptoms.
Cure the disease.

**MGT520: Leading Cloud Security
Design and Implementation**
Building and leading a cloud
security program.



SEC488: Cloud Security Essentials



GCLD
Cloud Security
Essentials
giac.org/gclد

License to Learn Cloud Security

SEC488 covers Amazon Web Services, Azure, Google Cloud, and other cloud service providers (CSPs). Like foreign languages, cloud environments have similarities and differences, and this course will introduce you to the language of cloud security. Upon completion of this course, you will be able to advise and speak about a wide range of cybersecurity topics and help your organization successfully navigate the challenges and opportunities presented by cloud service providers.

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: Public Cloud Security: AWS, Azure, and GCP



GPCS
Public Cloud
Security
giac.org/gclد

Multiple clouds require multiple solutions.

SEC510 is an in-depth analysis of the security of managed services for the Big 3 cloud providers: Amazon Web Services, Azure, and Google Cloud Platform. Students will leave the course confident that they have the knowledge they need when adopting services and Platform as a Service (PaaS) offerings in each cloud. Students will launch unhardened services, analyze the security configuration, validate that they are insufficiently secure, deploy patches, and validate the remediation.

Daily Topics:

1. Cloud Credential Management
2. Cloud Virtual Networks
3. Encryption, Storage, and Logging
4. Serverless Platforms
5. Cross-Account and Cross-Cloud Assessment

5-Day Program | 38 CPEs | Core

“The course content was thorough, provided real-life applicable examples, and gave a better understanding of each provider, as well as ways they can be exploited with improper configurations. The labs were detailed and thought provoking – it gave great thought to existing implementation and real-world examples.”

—Collin Huber,
Allstate Insurance



SEC522: Defending Web Applications Security Essentials



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.

This is the course to take if you have to defend web applications! The quantity and importance of data entrusted to web applications is increasing, and defenders need to learn how to secure these critical data. Traditional network defenses such as firewalls fail to secure web applications. In covering the OWASP Top 10 Risks and beyond, SEC522 will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Daily Topics:

1. Web Fundamentals and Security Configurations
2. Defense Against Input-Related Threats
3. Web Application Authentication and Authorization
4. Web Services and Front-End Security
5. Cutting-Edge Web Security
6. Capture-and-Defend-The-Flag Exercise

6-Day Program

36 CPEs

Foundational

"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.

SEC534: Secure DevOps: A Practical Introduction

Principles! Practices! Tools! Oh my. Start your journey on the DevSecOps road here.

SEC534 explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. You will learn how DevOps principles, practices, and tools can be leveraged to improve the reliability, integrity, and security of systems.

Daily Topics:

1. Introduction to Secure DevOps
2. Secure Infrastructure and Operations

2-Day Course

12 CPEs

Foundational

"Very informative and up-to-date with tools and processes used in today's development environments."

—Thomas Dison,
Patterson Dental



SEC540: Cloud Security and DevSecOps Automation



GCSA
Cloud Security
Automation
giac.org/gcsa

The cloud moves fast. Automate to keep up.

SEC540 provides security professionals with a methodology for securing modern Cloud and DevOps environments. Students learn how to implement over 20 DevSecOps Security Controls for building, testing, deploying, and monitoring cloud infrastructure and services. Immersive hand-on labs ensure students not only understand theory, but how to configure and implement each security control. By embracing the DevOps culture, you will walk away battle tested and ready to build to your organization's Cloud & DevOps Security program.

Daily Topics:

1. Introduction to DevSecOps
2. Cloud Infrastructure and Orchestration
3. Cloud Security Operations
4. Cloud Security as a Service
5. Compliance as Code

5-Day Program

38 CPEs

Core

“SEC540 helped me understand the complex ecosystem of DevOps. I came away with a well-rounded understanding of how the different technologies work together and how security needs to be tied into the CI/CD aspect. More than that, I found a new enthusiasm to learn and explore DevOps.”

—Uday Pothakamury, Citi

SEC541: Cloud Security Monitoring and Threat Detection

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

SEC541 is a cloud security course that looks at how attackers are attacking the Amazon Web Services (AWS) and Microsoft Azure environments, what their characteristics are, and how to detect them and investigate suspicious activity in your cloud infrastructure. Every day, the class will analyze a real world set of attacks, break down how it happened, how they would detect it in their environment, and then dive into the AWS and Azure services analyzing logs, behaviors and building analytics that the students can bring back to their own cloud infrastructure.

Daily Topics:

1. Management Plane and Network Logging
2. Compute and Cloud Services Logging
3. Cloud Service and Data Discovery in AWS

3-Day Course

18 CPEs

Specialization

“This had the right mix of AWS infrastructure background and methods of using AWS log data for threat hunting.”

—Brad Schonhorst, Sony



SEC557: Continuous Automation for Enterprise and Cloud Compliance

Using Cloud Security and DevOps Tools to Measure Security and Compliance

SEC557 teaches professionals tasked with ensuring security and compliance how to stop being a roadblock and work at the speed of the modern enterprise. You'll learn how to measure and visualize security data using the same tools that developers and engineers are using, as well as how to extract, load, and visualize data from cloud services, on-premise systems, and security tools. The course includes PowerShell scripting, automation, time-series databases, dashboard software, and even spreadsheets to present management with the strategic information it needs and to facilitate the work of your operations staff with sound tactical data.

Daily Topics:

1. Scripting, Data Acquisition, and Visualization Tools
2. Acquiring and Visualizing Cloud Service Data
3. Acquiring and Visualizing Data from OSES, Virtualization, and Containers

3-Day Program

18 CPEs

Management

“SEC557 answers the question ‘How can the manager/auditor/security/compliance professional possibly keep up?’ It teaches you to leverage and integrate with the processes used by your developers and engineers so that you can enforce security and compliance requirements without becoming an obstacle.”

—Clay Risenhoover,
SEC557 Course Author

SEC584: Cloud Native Security: Defending Containers and Kubernetes

Deliver securely at the speed of cloud native.

SEC584 will perform a deep-dive into defending key infrastructure deployment components, focusing on containerization and orchestration exploits. Students will be thrust directly into detailed issues related to misconfiguration and known attack patterns and will learn how to properly harden and protect against these exploits.

Daily Topics:

1. Cloud Native Security
2. Container Security and Exploitation
3. Moving to Kubernetes

3-Day Program

18 CPEs

Specialization

“Great content. Loads of new things to learn. [Labs are] relevant to real-world tasks.”

—Nii Akai-Nettey, 6point6



SEC588: Cloud Penetration Testing



GCPN
Cloud Penetration
Tester
giac.org/gcpn

Aim your arrows towards 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 assess 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. Discovery, Recon, and Architecture at Scale
2. Mapping, Authentication, and Cloud Services
3. Azure and Windows Services in the Cloud
4. Vulnerabilities in Cloud Native Applications
5. Exploitation and Red Team in the Cloud
6. Capstone

6-Day Program

36 CPEs

Specialization

"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 and Incident Response

Find the Storm in the Cloud

The world is changing and so is the data we need to conduct our investigations. New 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.

Daily Topics:

1. Cloud Forensics Fundamentals and Microsoft 365
2. Amazon AWS
3. Microsoft Azure
4. Google Cloud (GCP)

4-Day Program

24 CPEs

Specialization

"FOR509 was written to give you a headstart in understanding, analyzing and solving cloud based investigations. Not only do we cover the most popular cloud solutions on the market we also help the student to understand now just how to interpret the data but how they can take their detection and response capabilities to the next level. "

—David Cowen



MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

Stop treating the symptoms. Cure the disease.

MGT516 helps you think strategically about vulnerability management in order to mature your organization's program, but it also provides tactical guidance to help you overcome common challenges. By understanding and discussing solutions to typical issues that many organizations face across both traditional and cloud operating environments, you will be better prepared to meet the challenges of today and tomorrow. The Cyber42 game that forms part of the course puts students in the driver's seat for the fictional Everything Corporation ("E-Corp") and allows them to select certain initiatives that will mature E-Corp's VM program. Students will also need to choose how to respond to 13 realistic events that are sure to have an impact on their program. Depending on how students respond, E-Corp's security culture and the maturity of the different components of its VM program will be impacted. These tabletop exercises will enable students to put the skills they are learning into practice when they return to work at their own organizations.

Daily Topics:

1. Overview: Cloud and Asset Management
2. Identify
3. Analyze and Communicate
4. Treat
5. Buy-in, Program, and Maturity

5-Day Program

30 CPEs

Core

"An understanding of vulnerability management and cloud security is becoming not only valuable, but a necessity to keep one's organization secure in this constantly changing and dynamic environment."

—Kae David, Ernst & Young

MGT520: Leading Cloud Security Design and Implementation

Building and Leading a Cloud Security Program

MGT520 teaches students how to build, lead, and implement a cloud security transition plan and roadmap, and then execute and manage ongoing operations. An organization's cloud transition requires numerous key decisions. This course provides the information security leaders need to drive a secure cloud model and leapfrog on security by leveraging the security capabilities in the cloud.

Daily Topics:

1. Security Program Design and Cloud Security Fundamentals
2. Cloud Security Features: Adoption and Maturing the Security Program
3. Cloud Security Features: Adoption and Maturing the Security Program

3-Day Course

18 CPEs

Core

"I like how the content builds and progresses. Jason clearly thought a lot about how to sequence the information to make it easy to digest."

—Jim Pruitt,
Revolutionary Security



		DevOps Professionals	Cloud Security Analyst	Cloud Security Engineer	Cloud Security Architect	Cloud Security Manager
BASELINE						
	COMING SOON					
FOUNDATIONAL						
	SEC488: Cloud Security Essentials GIAC Cloud Security Essentials (GCLD)					
	SEC534: Secure DevOps: A Practical Introduction					
CORE						
	SEC510: Public Cloud Security: AWS, Azure, and GCP GIAC Public Cloud Security (GPCS)					
	SEC522: Defending Web Applications Security Essentials GIAC Certified Web Application Defender (GWEB)					
	SEC540: Cloud Security and DevSecOps Automation GIAC Cloud Security Automation (GCSA)					
SPECIALIZATION						
	SEC541: Cloud Security Monitoring and Threat Detection					
	SEC584: Cloud Native Security: Defending Containers and Kubernetes					
	SEC588: Cloud Penetration Testing GIAC Cloud Penetration Tester (GCPN)					
	FOR509: Enterprise Cloud Forensics and Incident Response					
MANAGEMENT						
	MGT516: Managing Security Vulnerabilities: Enterprise and Cloud					
	MGT520: Leading Cloud Security Design and Implementation					
	SEC557: Continuous Automation for Enterprise and Cloud Compliance					

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
- **Management** – 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



- **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



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



Twitter – @SANSCloudSec



LinkedIn – www.linkedin.com/showcase/sanscloudsec



YouTube – www.youtube.com/c/SANSCloudSecurity