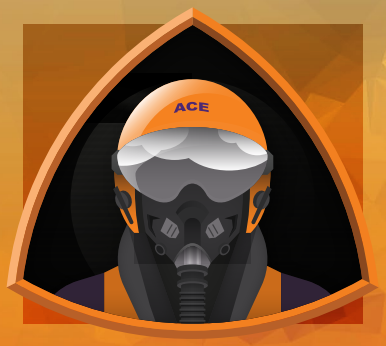

SANS GIAC CERTIFICATIONS

SANS CLOUD SECURITY

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

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

SEC 488 — **Cloud Security Essentials** | GCLD
License to learn cloud security.

SEC 510 — **Public Cloud Security: AWS, Azure & GCP** | GPCS
Multiple clouds require multiple solutions.

SEC 522 — **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.

SEC 534 — **Secure DevOps: A Practical Introduction**
Principles! Practices! Tools! Oh my. Start your journey on the DevSecOps road here.

SEC 540 — **Cloud Security & DevSecOps Automation** | GCSA
The cloud moves fast. Automate to keep up.

SEC 541 — **Cloud Security Monitoring & Threat Detection**
Attackers can run but not hide. Our radar sees all threats.

SEC 557 — **Continuous Automation for Enterprise and Cloud Compliance**
Measure what matters, not what's easy.

SEC 584 — **Cloud Native Security: Defending Containers and Kubernetes**
Deploy securely at the speed of cloud native.

SEC 588 — **Cloud Penetration Testing** | GCPN
Aim your arrows to the sky and penetrate the cloud.

FOR 509 — **Enterprise Cloud Forensics & Incident Response**
Find the storm in the cloud.

MGT 516 — **Managing Security Vulnerabilities: Enterprise and Cloud**
Stop treating the symptoms. Cure the disease.

MGT 520 — **Leading Cloud Security Design & Implementation**
Chart your course to cloud security.

SEC488: Cloud Security Essentials

GCLD
Cloud Security Essentials
giac.org/gcld

6-Day Program | 36 CPEs | Foundational

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

"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/gcld

5-Day Program | 38 CPEs | Core

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. Severless Platforms
5. Cross-Account and Cross-Cloud Assessment

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

GWEB
Web Application Defender
giac.org/gweb

6-Day Program | 36 CPEs | Foundational

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

"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

2-Day Course | 12 CPEs | Foundational

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

"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 and DevOps Security Program.

Daily Topics:

1. DevOps Security Automation
2. Cloud Infrastructure Security
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.

Cloud infrastructure provides organizations with new and exciting services to better meet the demands of their customers. However, these services bring with them new challenges, particularly for organizations struggling to make sense of the cloud native logs, keeping ahead of fast-moving development teams, and trying to learn how threats are adapting to cloud services. Securely operating cloud infrastructure requires new tools and approaches for better visibility into the cloud environment threat landscape, ability to capture appropriate data, and most importantly to be able to analyze and correlate the data effectively and accurately to understand if the specific threat is legitimate based on your organization's bigger picture.

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

5-Day Program | 30 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

5-Day Program | 30 CPEs | Management

Measure what matters, not what's easy.

Agile development, DevOps, cloud technologies, and virtualization have enabled organizations to build and deploy systems at a terrifyingly fast rate. The old and cumbersome manual ways to test security and compliance can't keep up. You need to understand and use the same tools and techniques that your developers and engineers are using, and you need to be able to generate results quickly and often - without slowing down your organization. SEC557 teaches professionals tasked with ensuring security and compliance how to stop being a roadblock and work at the speed of the modern enterprise.

Daily Topics:

1. PowerShell Fundamentals, Time-Series Databases & Visualization Tools
2. Advanced PowerShell Scripting and Automation, Gathering and Using Structured Data
3. System and Infrastructure Compliance Measurements
4. Cloud Compliance: AWS
5. Cloud Compliance: Azure/GCP, DevOps Compliance

"The content in this course is helping me understand the importance of scripting, data acquisition, and data automation. I think this course is a must for anyone looking to understand the importance of these topics."
—Robert Hymus, Here Corp

SEC584: Cloud Native Security: Defending Containers and Kubernetes

3-Day Course | 18 CPEs | Specialization

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 Infrastructure
2. Container Security and Exploitation
3. Moving to Kubernetes

"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

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 and Incident Response

4-Day Program | 24 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. Cloud Forensics Fundamentals and Microsoft 365
2. Amazon AWS
3. Microsoft Azure
4. Google Cloud (GCP)

"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

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

5-Day Program | 30 CPEs | Core

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

"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

3-Day Course | 18 CPEs | Core

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 and Capabilities
3. Securing Workloads, Operations, and Maturing the Program

"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

SANS CLOUD SECURITY

FLIGHT PLAN TO BECOMING A CLOUD ACE

		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: Application Security: Securing Web Apps, APIs & Microservices 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

SANS CLOUD SECURITY

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

SANS CLOUD SECURITY

RESOURCES

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

Twitter – @SANSCloudSec

LinkedIn – www.linkedin.com/showcase/sanscloudsec

YouTube – www.youtube.com/c/SANSCloudSecurity