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

LONG COURSES

SEC488: Cloud Security Essentials
License to learn cloud securrity.

SEC510: Multicloud Security Assessment and Defense
Multiple clouds require multiple solutions.

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

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

SEC545: Cloud Security Architecture and Operations
In the cloud, no one can hear you scream. Architect it properly and you won't have to.

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.

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

SHORT COURSES

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

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

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

SEC488: Cloud Security Essentials

License to learn cloud security.

SEC488 is an introductory course that prepares students to advise and speak about a wide range of cloud services, and methods to secure them in multiple providers. Students will learn how to navigate both the security challenges, as well as the opportunities presented by various cloud service providers including Amazon Web Services, Azure, Google Cloud, and others.

Daily Topics:

1. Welcome to the Cloud
2. Securing Cloud Environment and Infrastructure Security
3. Application Security and Securing Services
4. Cloud Operations and Architecture
5. Legal/Compliance, Penetration Testing & Incident Response
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: Multicloud Security Assessment and Defense

Multiple clouds require multiple solutions.

SEC510 is an in-depth analysis of the security of the managed services for the big 3 cloud providers (AWS, Azure, and GCP). Students will leave the course confident that they know everything they need to consider when adopting 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 in the Clouds

"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 Essentials

GWEB
Web Application Defender
giac.org/gweb

6-Day Program	36 CPEs	Foundational

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

SEC522 is a security course that prepares the student to defend modern web applications across the entire lifecycle from planning, building to operations. Students will learn about how the common attacks work and, more importantly, how to scale up defenses against the common and recent attacks in an enterprise environment.

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

> "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 DevOps Automation

GCSA
Cloud Security Automation
giac.org/gcsa

5-Day Program	38 CPEs	Core

The cloud moves fast. Automate to keep up.

SEC540 provides development, operations, and security professionals with a methodology to build and deliver secure cloud infrastructure and software using the Secure DevOps toolchain.

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

> "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

SEC545: Cloud Security Architecture and Operations

**In the cloud, no one can hear you scream.
Architect it properly and you won't have to.**

SEC545 is an intermediate course that prepares students to design and implement a wide range of security architecture and operational controls. Students will learn how to architect a sound defensive control model within cloud service providers, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

Daily Topics:

1. Cloud Service Models and Controls
2. Cloud Security Architecture and Operations (Part 1)
3. Cloud Security Architecture and Operations (Part 2)
4. Cloud Security Offense and Defense Operations
5. Cloud Security Automation and Orchestration

> **"The course content really shows how cloud can become a security enabler within organizations! SEC545 is my Swiss knife for cloud security."**
> —Jeroen Vandeleur, NVISO

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

> **"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 towards the sky and penetrate the Cloud.

SEC588 is the course that unites the disciplines of network and web penetration testing with a look into how these skills will need to change to assess public cloud infrastructures and its associated services.

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

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

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

5-Day Program	30 CPEs	Core

Stop treating the symptoms. Cure the disease.

MGT516 provides a holistic view of vulnerability management and it equips students with the skills and techniques to effectively identify, analyze, and treat security vulnerabilities. As organizations move to the cloud, the differences and benefits that this brings to vulnerability management are detailed. The course highlights why many organizations are still struggling with vulnerability management today, and how to deal with these challenges.

Daily Topics:

1. Overview and Identify
2. Identify and Analyze
3. Communicate and Treat
4. Treatment, Buy-in, and Program
5. Managing Vulnerabilities: Capstone Lab Exercise

"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

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
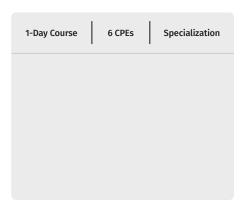2. Secure Infrastructure and Operations

> "Very informative and up-to-date with tools and processes used in today's development environments."
> —Thomas Dison, Patterson Dental

SEC541: Cloud Monitoring & Threat Hunting

1-Day Course	6 CPEs	Specialization

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

SEC541 is a deep-dive into the native services in AWS for gathering, analyzing, and detecting threats.We will cover common attack techniques against Cloud infrastructure, and then investigate how to detect those techniques in AWS. This class is all about gaining hands-on experience in detecting potential threats in your own environment. The class will also discuss architectural design patterns that can make detection easier, attacks harder, and automate where possible.

MGT520: Leading Cloud Security Design and Implementation

2-Day Course	12 CPEs	Core

Building and leading a cloud security program.

MGT520 focuses on what managers, directors, and security leaders need to know about developing their cloud security plan/roadmap and managing implementation of cloud security capabilities. It is applicable to all industries where the organizations are engaged in the journey to move computing workloads to the cloud, but of particular interest to larger organizations in industries with higher level of regulatory and compliance concerns.

Daily Topics:

1. Designing Your Cloud Security Program
2. Implementing Your Cloud Security Plan

		DevOps Professionals	Cloud Security Analyst	Cloud Security Engineer	Cloud Security Architect	Cloud Security Manager
BASELINE	COMING SOON	●	●			●
FOUNDATIONAL	SEC488: Cloud Security Essentials	●	●	●	●	●
	SEC522: Defending Web Applications Security Essentials — GIAC Certified Web Application Defender (GWEB)	●				
CORE	SEC510: Multicloud Security Assessment and Defense	●	●	●	●	
	SEC540: Cloud Security and DevOps Automation — GIAC Cloud Security Automation (GCSA)	●		●	●	
	SEC545: Cloud Security Architecture and Operations		●	●	●	
SPECIALIZATION	SEC541: Cloud Monitoring and Threat Hunting		●			
	SEC584: Cloud Native Security: Defending Containers and Kubernetes	●		●	●	
	SEC588: Cloud Penetration Testing — GIAC Cloud Penetration Tester (GCPN)		●			
MANAGEMENT	MGT516: Managing Security Vulnerabilities: Enterprise and Cloud					●
	MGT520: Leading Cloud Security Design and Implementation					●

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

- **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