SANS | GIAC CERTIFICATIONS

CLOUD SECURITY

Courses and Free Resources

sans.org/cloud-security

SANS CURRICULUM FOCUS AREA

CLOUD SECURITY

Cloud computing represents the most transformational technology of our era and cloud security will play a pivotal role in its adoption. Cloud security must be focused on where the cloud is going, not where it is today. The future demands in-depth technical cloud capabilities coupled with knowledge of the security and service features for each of the major cloud service providers (CSPs). Begin you journey to become a Cloud Security Ace.

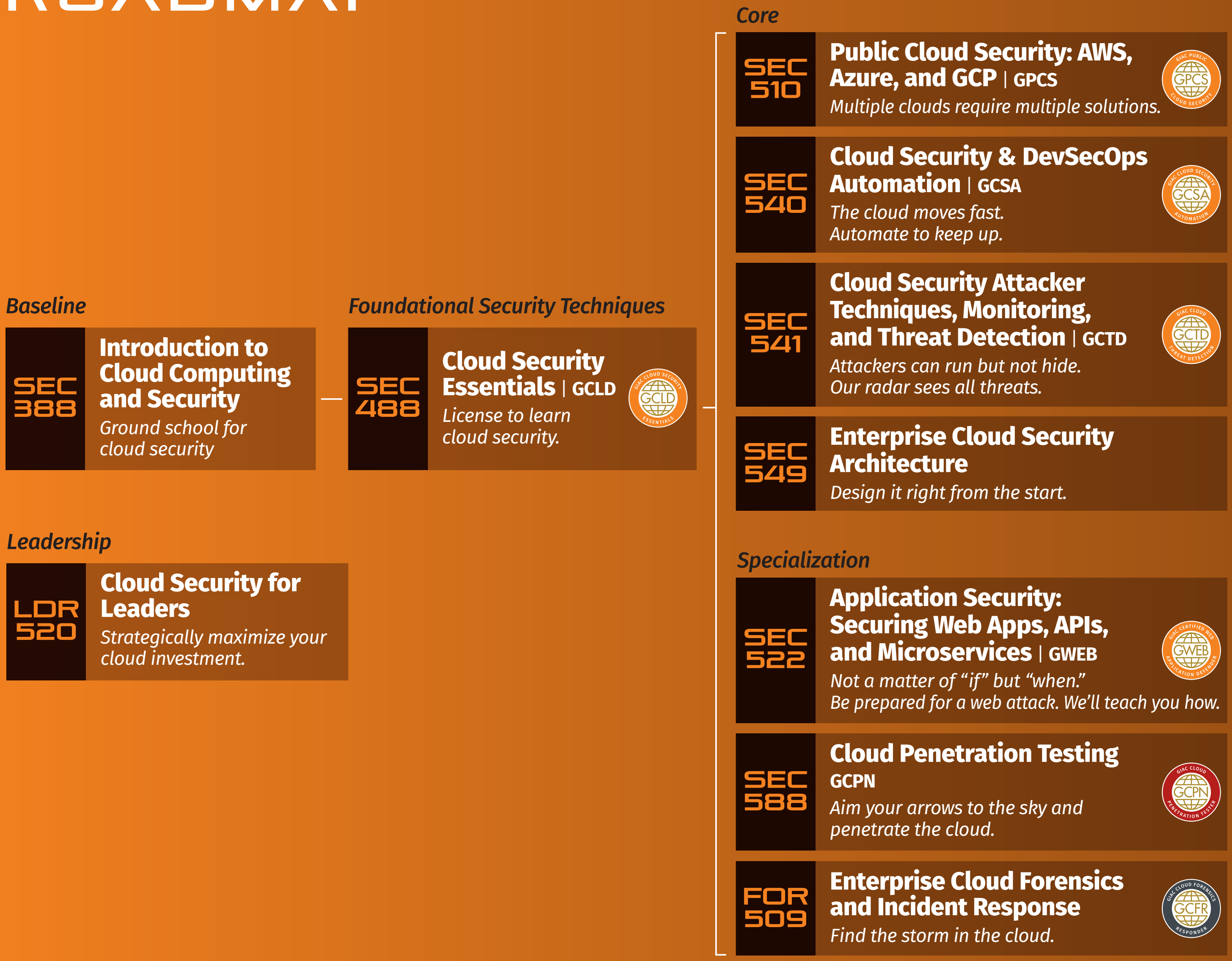
Our curriculum has been developed through an industry consensus process and is a holistic, hands-on approach to address public cloud security, which includes multicloud and hybrid-cloud scenarios for the enterprise and developing organizations alike. Learn how various CSPs interact and the nuances among them rather than merely learning the ins-and-outs of one platform.

Get you hands dirty in cloud security training by learning how to:

- Harden and configure public cloud services from AWS, Azure, and Google Cloud Platform (GCP)
- Automate security and compliance best practices
- Use cloud services to securely build and deploy systems and applications
- Inject security seamlessly into your DevOps toolchain
- Securely build, deploy, and manage containers and Kubernetes
- Discover vulnerabilities and weaknesses in your cloud environments
- Find attacker activity in your cloud logs

> **"The world has shifted to the cloud and we, as security professionals, have to make the same shift."**
>
> —Daniel Harrison,
> **Capital One**

CURRICULUM ROADMAP



Baseline

SEC 388 **Introduction to Cloud Computing and Security**
Ground school for cloud security

Leadership

LDR 520 **Cloud Security for Leaders**
Strategically maximize your cloud investment.

Foundational Security Techniques

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

Core

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

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

SEC 541 **Cloud Security Attacker Techniques, Monitoring, and Threat Detection** | GCTD
Attackers can run but not hide. Our radar sees all threats.

SEC 549 **Enterprise Cloud Security Architecture**
Design it right from the start.

Specialization

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

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

Flight Plan – Career Progression

BASELINE

SEC 388 — **Introduction to Cloud Computing and Security**
Ground school for cloud security

FOUNDATIONAL

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

CORE

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

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

SEC 541 — **Cloud Security Attacker Techniques, Monitoring, and Threat Detection**
Attackers can run but not hide. Our radar sees all threats.
GIAC Cloud Threat Detection GCTD

SEC 549 — **Enterprise Cloud Security Architecture**
Design it right from the start.

SPECIALIZATION

SEC 522 — **Application Security: Securing Web Apps, APIs, and Microservices**
Not a matter of "if" but "when."
Be prepared for a web attack. We'll teach you how.
GIAC Certified Web Application Defender GWEB

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

FOR 509 — **Enterprise Cloud Forensics and Incident Response**
Find the storm in the cloud.
GIAC Cloud Forensics Responder GCFR

LEADERSHIP

LDR 520 — **Cloud Security for Leaders**
Strategically maximize your cloud investment.

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

Cloud Security Analyst Use cloud security solutions to respond to incidents and enable defenses	**Cloud Security Engineer** Build security solutions for cloud workflows	**Cloud Security Architect** Design how security functions will adopt cloud services, define knowledge, tooling, and approach for cloud solutions	**Cloud Security Manager** Develop cloud security roadmap, plan, procurement models, ensure policy and procedure is defined to support cloud	**DevOps Professionals** Develop, deploy, and manage secure applications and systems
●			●	
●	●	●	●	
●	●	●		●
	●	●		●
●	●			
	●	●	●	
				●
●	●			
●				
		●	●	

SANS CLOUD SECURITY

SEC388: **Introduction to Cloud Computing and Security**

3 Day Course | 18 CPEs | Laptop Required

You Will Be Able To

- Make sense of different cloud-based services
- Understand and analyze risk in the cloud
- Interact with Azure and AWS environments using a browser and command line tools
- Change behavior and build a security-aware culture
- Deploy and integrate cloud services in AWS and Azure
- Get up to speed quickly on cloud security issues and terminology
- Detect and effectively respond to a simulated cloud breach
- Speak the same language as technical security professionals
- Learn how to automate common tasks using cloud shells
- Defend cloud services from attacks
- Track, audit and manage budgeting in your cloud environments

Who Should Attend

- People who are new to cloud security and in need of an introduction to the fundamentals of cloud security
- Those who feel bombarded with complex technical cloud security terms they don't understand but want to understand
- Professionals who need to be conversant in basic cloud security concepts, principles, and terms, but who don't need "deep in the weeds" detail
- Those who have decided to make a career change to take advantage of the job opportunities in cloud security and need formal training/certification
- Managers who worry their company may be the next cloud mega-breach headline story on the 6 o'clock news

Ground School for Cloud Security

The purpose of SEC388 is to learn the fundamentals of cloud computing and security. We do this by introducing, and eventually immersing, you in both AWS and Azure; by doing so, we are able to expose you to important concepts, services, and the intricacies of each vendor's platform. This course provides you with the knowledge you need to confidently speak to modern cybersecurity security issues brought on by the cloud, and become well versed with applicable terminology. You won't just learn about cloud security, you will learn the "how" and the "what" behind the critical cloud security topics impacting businesses today.

Business Takeaways

This course will help your organization:

- Develop professionals – technical or managerial – that know how to use AWS and Azure services
- Anticipate what cloud security threats are applicable to your business
- Learn how to mitigate threats
- Create a culture where security empowers the business to succeed

Hands-On Training

All labs in SEC388 are focused on Azure and AWS and involve directly interacting with each cloud service provider. Students will use a browser to access each cloud environment to gain familiarity with cloud computing concepts. During labs, students will implement cloud services, deploy a cloud-based website, and perform essential security tasks in order to become accustomed to cloud computing and cloud security. The total time committed to labs is about 37% of the course.

Author Statement

"Cloud computing is not new and the adoption of the cloud by organizations continues to grow at an astounding rate. Due to this, many people are finding themselves in the position where it clearly makes sense to learn more about cloud computing. Interestingly, this rise in cloud computing has brought forth a rise in cloud-related breaches – and it makes perfect sense why. As we see with any new frontier in computer science, what's old is new again, and many of the mistakes of the past, are being revived in today's modern world of cloud computing. It is critically important to develop the skills and knowledge needed to positively influence cloud security in every capacity we can influence. Regardless of your background, SEC388's entry-level approach and focus on cloud computing and security will help you prepare for a rewarding career, just as it will help level-up your skills as an accomplished professional, ultimately preparing you for success in a world of cloud computing."

—Serge Borso

> **"[SEC388] is useful for someone thinking about switching to security with an emphasis in the cloud. This course would give them an opportunity to see and briefly experience different aspects of security. It did have useful labs, for executives or professionals already in the field."**
>
> —Luz Bojorquez

SEC488: **Cloud Security Essentials**

GCLD
Cloud Security Essentials
giac.org/gcld

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Navigate your organization through the security challenges and opportunities presented by cloud services
- Identify the risks of the various services offered by cloud service providers (CSPs)
- Select the appropriate security controls for a given cloud network security architecture
- Evaluate CSPs based on their documentation, security controls, and audit reports
- Confidently use the services of any of the leading CSPs
- Protect secrets used in cloud environments
- Leverage cloud logging capabilities to establish accountability for events that occur in the cloud environment
- Identify the risks and risk control ownership based on the deployment models and service delivery models of the various products offered by cloud service providers (CSPs).
- Evaluate the trustworthiness of CSPs based on their security documentation, service features, third-party attestations, and position in the global cloud ecosystem.
- Secure access to the consoles used to access the CSP environments.
- Implement network security controls that are native to both AWS and Azure.
- Follow the penetration testing guidelines put forth by AWS and Azure to invoke your "inner red teamer"to compromise a full stack cloud application

Who Should Attend

Anyone who works in a cloud environment, is interested in cloud security, or needs to understand the risks using cloud service providers should take this course, including:

- Security engineers
- Security analysts
- System administrators
- Risk managers
- Security managers
- Security auditors
- Anyone new to the cloud

License to Learn Cloud Security

Research shows that most enterprises have strategically decided to deploy a multicloud platform, including Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), other cloud service providers. Mature CSPs have created a variety of security services that can help customers use their products in a more secure manner, but only if the customer knows about these services and how to use them properly. This course covers real-world lessons using security services created by the Big 3 CSPs, as well as open-source tools. Each section of the course features hands-on lab exercises to help students hammer home the lessons learned. We progressively layer multiple security controls in order to end the course with a functional security architecture implemented in the cloud.

This course will equip you to implement appropriate security controls in the cloud, often using automation to "inspect what you expect." We will begin by diving headfirst into one of the most crucial aspects of cloud - Identity and Access Management (IAM). From there, we'll move on to securing the cloud through discussion and practical, hands-on exercises related to several key topics to defend various cloud workloads operating in the different CSP models of: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Functions as a Service (FaaS).

Hands-On Training

SEC488: Cloud Security Essentials reinforces the training material via multiple hands-on labs in each section of the course. Labs are performed via a browser-based application rather than virtual machine. Each lab is designed to impart practical skills that students can bring back to their organizations and apply on the first day back in the office. The labs go beyond the step-by-step instructions by providing the context of why the skill is important and instilling insights as to why the technology works the way it does.

GCLD
Cloud Security Essentials
giac.org/gcld

GIAC Cloud Security Essentials

"The GIAC Cloud Security Essentials (GCLD) certification proves that the certificate holder understands many of the security challenges brought forth when migrating systems and applications to cloud service provider (CSP) environments. Understanding this new threat landscape is only half the battle. The GCLD certification goes one step further – proving that the defender can implement preventive, detective, and reactionary techniques to defend these valuable cloud-based workloads."
—Ryan Nicholson, SANS SEC488 Course Author

- Evaluation of cloud service provider similarities, differences, challenges, and opportunities
- Planning, deploying, hardening, and securing single and multi-cloud environments
- Basic cloud resource auditing, security assessment, and incident response

> **"Labs were solid and definitely brought home the objectives. I learned of many features we can implement to make our cloud environments more secure."**
>
> —Bob Hewitt, **Stellar Technology Solutions**

SEC510: **Public Cloud Security: AWS, Azure, and GCP**

GPCS
Public Cloud Security
giac.org/gpcs

5 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Understand the inner workings of cloud services and Platform as a Service (PaaS)/ Infrastructure as a Service (IaaS) offerings in order to make more informed decisions in the cloud
- Understand the design philosophies that undergird each provider and how these have influenced their services in order to properly prescribe security solutions for them
- Discover the unfortunate truth that many cloud services are adopted before their security controls are fully fleshed out
- Understand Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) in depth.
- Understand the intricacies of Identity and Access Management, one of the most fundamental concepts in the cloud and yet one of the last understood
- Understand cloud networking and how locking it down is a critical aspect of defense-in-depth in the cloud
- Analyze how each provider handles encryption at rest and in transit in order to prevent sensitive data loss
- Apply defense-in-depth techniques to protect data in cloud storage
- Compare and contrast the serverless platforms of each provider
- Utilize multicloud IAM and cloud Single Sign-On to provide secure access to resources across cloud accounts and providers

Who Should Attend

- Security analysts
- Security engineers
- Security researchers
- Cloud engineers
- DevOps engineers
- Security auditors
- System administrators
- Operations personnel
- Anyone who is responsible for:
  - Evaluating and adopting new cloud offerings
  - Researching new vulnerabilities and developments in cloud security
  - Identity and Access Management
  - Managing a cloud-based virtual network
  - Secure configuration management

Multiple clouds require multiple solutions.

SEC510 provides cloud security practitioners, analysts, and researchers with the nuances of multi-cloud security. Students will obtain an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud (often referred to as Google Cloud Platform, or GCP). SEC510 leverages industry-renowned standards and methodologies, such as the Center for Internet Security (CIS) Cloud Foundations Benchmarks, MITRE ATT&CK Cloud Matrix, and Cyber Defense Matrix alongside original research. Students will then apply that knowledge through hands-on exercises in real cloud environments for each provider, launching unhardened services, analyzing their security configurations, validating that they are insufficiently secure, deploying patches, and validating the remediation. This teaches students the philosophies that undergird each provider and how these have influenced their services. Students will leave the course confident that they have the knowledge they need to support their organization's adoption of Platform as a Service (PaaS)/ Infrastructure as a Service (IaaS) offerings in each cloud.

Hands-On Training

SEC510: Public Cloud Security: AWS, Azure, and GCP reinforces all of the concepts discussed in the lectures through hands-on labs in real cloud environments. Each lab includes step-by-step guide as well as a "no hints" option for students who want to test their skills without further assistance. This allows students to choose the level of difficulty that is best for them and fall back to the step-by-step guide as needed. Students can continue to access the lab instructions, application code, and infrastructure-as-code after the course concludes. With this, they can repeat every lab exercise in their own cloud environments as many times as they would like.

SEC510 also offers students an opportunity to participate in Bonus Challenges each day in a gamified environment, while also providing more hands-on experience with the Big 3 cloud sevice providers and relevant utilities. Can you win the SEC510 Challenge Coin?

Course Authors' Statement

"The use of multiple public cloud providers introduces new challenges and opportunities for security and compliance professionals. As the service offering landscape is constantly evolving, it is far too easy to prescribe security solutions that are not effective in all clouds. While it is tempting to dismiss the multicloud movement or block it at the enterprise level, this will only make the problem harder to control.

"Why do teams adopt multiple cloud providers in the first place? To make their jobs easier or more enjoyable. Developers are creating products that meet the organization's goals, not for the central security team. If a team discovers that a service offering can help get its product to market faster, it can and should use it. Security should embrace the inevitability of the multicloud movement and take on the hard work of implementing guardrails so the organization can move quickly and safely.

"The multicloud storm is coming, whether you like it or not."

—Brandon Evans and Eric Johnson

> **"Anyone working in a multicloud environment needs to understand the sometimes subtle differences among the different cloud services."**
>
> —Tom Wood, **Wood International, Inc.**

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

GWEB
Web Application Defender
giac.org/gweb

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Defend against the attacks specified in OWASP Top 10
- Infrastructure security and configuration management
- Securely integrating cloud components into a web application
- Authentication and authorization mechanisms, including single sign-on patterns
- Cross-domain web request security
- Protective HTTP headers
- Defending SOAP, REST and GraphQL APIs
- Securely implement Microservice architecture
- Defending against input related flaws such as SQL injection, XSS and CSRF

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with those requirements

> **"Lots of good hands-on exercises using real-world examples."**
>
> —Nicolas Kravec, **Morgan Stanley**

> **"The exercises are a good indicator of understanding the material. They worked flawlessly for me."**
>
> —Robert Fratila, **Microsoft**

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

During the course, we demonstrate the risks of web applications and the extent of sensitive data that can be exposed or compromised. From there, we offer real world solutions on how to mitigate these risks and effectively evaluate and communicate residual risks.

After attending the class, students will be able to apply what they learned quickly and bring back techniques to not only better secure their applications, but also do so efficiently by adding security early in the software development life cycle, shifting left security decisions and testing, thus saving time, money, and resources for the organization.

Business Takeaways

- Comply with PCI DSS 6.5 requirements
- Reduce the overall application security risks, protect company reputation
- Adopt the shifting-left mindset where security issues addressed early and quickly. This avoids the costly rework.
- Ability to adopt modern apps with API and microservices in a secure manner
- This course prepares students for the GWEB certification

Hands-on Training

The provided VM lab environment contains realistic application environment to explore the attacks and the effects of the defensive mechanisms. The exercise is structured in a challenge format with hints available along the way. The practical hands-on exercises help students gain experience to hit the ground running back at the office. There are 20 labs in section 1 to section 5 of the class and in the last section, there is a capstone exercise called Defending the Flag where there is 3–4 hours of dedicated competitive exercise time.

- **SECTION 1:** HTTP basics, HTTP/2 traffic inspection and spoofing, environment isolation, SSRF and credential-stealing
- **SECTION 2:** SQL Injection, Cross Site Request Forgery, Cross Site Scripting, Unicode and File Upload
- **SECTION 3:** Authentication vulnerabilities and defense, Multifactor authentication, Session vulnerabilities and testing, Authorization vulnerabilities and defense, SSL vulnerabilities and testing, Proper encryption use in web application
- **SECTION 4:** WSDL enumerations, cross domain AJAX, front-end features and CSP (Content Security Policy), Clickjacking
- **SECTION 5:** Deserialization and DNS rebinding, GraphQL, API gateways and JSON, SRI and Log review
- **SECTION 6:** Defending-the-flag capstone exercise

GIAC Certified Web Application Defender

GWEB
Web Application Defender
giac.org/gweb

The GIAC Web Application Defender certification allows candidates to demonstrate mastery of the security knowledge and skills needed to deal with common web application errors that lead to most security problems. The successful candidate will have hands-on experience using current tools to detect and prevent input validation flaws, cross-site scripting (XSS), and SQL injection as well as an in-depth understanding of authentication, access control, and session management, their weaknesses, and how they are best defended. GIAC Certified Web Application Defenders (GWEB) have the knowledge, skills, and abilities to secure web applications and recognize and mitigate security weaknesses in existing web applications.

- Access Control, AJAX Technologies and Security Strategies, Security Testing, and Authentication
- Cross Origin Policy Attacks and Mitigation, CSRF, and Encryption and Protecting Sensitive Data
- File Upload, Response Readiness, Proactive Defense, Input Related Flaws and Input Validation
- Modern Application Framework Issues and Serialization, Session Security & Business Logic, Web
- Application and HTTP Basics, Web Architecture, Configuration, and Security

SEC540: **Cloud Security and DevSecOps Automation**

GCSA
Cloud Security Automation
giac.org/gcsa

5	38	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Understand how DevOps works and identify keys to success
- Wire security scanning into automated CI/CD pipelines and workflows
- Build continuous monitoring feedback loops from production to engineering
- Automate configuration management using Infrastructure as Code (IaC)
- Secure container technologies (such as Docker and Kubernetes)
- Use native cloud security services and third-party tools to secure systems and applications
- Securely manage secrets for Continuous Integration servers and applications
- Integrate cloud logging and metrics
- Perform continuous compliance and security policy scanning

Who Should Attend

- Anyone working in or transitioning to a public cloud environment
- Anyone working in or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to cloud and DevOps Continuous Delivery pipelines
- Anyone interested in learning how to migrate DevOps workloads to the cloud, specifically Amazon Web Services (AWS) and Microsoft Azure
- Anyone interested in leveraging cloud application security services provided by AWS or Azure
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

The cloud moves fast. Automate to keep up.

Common security challenges for organizations struggling with the DevOps culture include issues such as:

- Upfront peer code reviews and security approvals may not occur for change approval and audit requirements
- Missing infrastructure and application scanning can allow attackers to find an entry point and compromise the system
- Cloud security misconfigurations may publicly expose sensitive data or introduce new data exfiltration paths

Security teams can help organizations prevent these issues such as using DevOps tooling and cloud-first best practices. This course provides development, operations, and security professionals with a deep understanding of and hands-on experience with the DevOps methodology used to build and deliver cloud infrastructure and software. Students learn how to attack and then harden the entire DevOps workflow, from version control to continuous integration and running cloud workloads. Each step of the way, students explore the security controls, configuration, and tools required to improve the reliability, integrity, and security of on-premise and cloud-hosted systems. Students learn how to implement more than 20 DevSecOps security controls to build, test, deploy, and monitor cloud infrastructure and services.

Hands-On Training

SEC540 goes well beyond traditional lectures and immerses students in hands-on application of techniques during each section of the course. Each lab includes a step-by-step guide to learning and applying hands-on techniques, as well as a "no hints" approach for students who want to stretch their skills and see how far they can get without following the guide. This allows students, regardless of background, to choose the level of difficulty they feel is best suited for them -always with a frustration-free fallback path. Immersive hand-on labs ensure that students not only understand theory, but how to configure and implement each security control.

The SEC540 lab environment simulates a real-world DevOps environment, with more than 10 automated pipelines responsible for building DevOps container images, cloud infrastructure, automating gold image creation, orchestrating containerized workloads, executing security scanning, and enforcing compliance standards. Students are challenged to sharpen their technical skills and automate more than 20 security-focused challenges using a variety of command line tools, programming languages, and markup templates.

The SEC540 course labs come in both AWS and Azure versions. Students will choose one cloud provider at the beginning of class to use for the duration of the course. Students are welcome to do labs for both cloud providers on their own time once they finish the first set of labs.

For advanced students, 2 hours of CloudWars Bonus Challenges are available during extended hours each day. These CloudWars challenges provide additional opportunities for hands-on experience with the cloud and DevOps toolchain.

> **"BEST class I have ever taken at SANS. This is one of those courses where I can log into work after class ends and immediately start applying into my daily tasks and responsibilities. I already went on my team's Slack channel and told them this needs to be the next class they take."**
>
> —Brian Esperanza, **Teradata**

SEC541: **Cloud Security Attacker Techniques, Monitoring, and Threat Detection**

GCTD
Cloud Threat Detection
giac.org/gctd

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Research attacks and threats to cloud infrastructure and how they could affect you
- Break down a threat into detectable components
- Effectively use AWS and Azure core logging services to detect suspicious behaviors
- Make use of cloud native API logging as the newest defense mechanism in cloud services
- Move beyond the cloud-provided Graphic User Interfaces to perform complex analysis
- Perform network analysis with cloud-provided network logging
- Understand how application logs can be collected and analyzed inside the cloud environment
- Effectively put into practice the AWS and Azure security specific services
- Integrate container, operating system, and deployed application logging into cloud logging services for more cohesive analysis
- Centralize log data from across your enterprise for better analysis
- Perform inventory of cloud resources and sensitive data using scripts and cloud native tooling
- Analysing Microsoft 365 activity to uncover threats
- Ability to leverage cloud native architecture to automate response actions to attacks

Who Should Attend

- Security analysts
- Security architects
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- System administrators
- Cloud administrators

> **"Labs gave great examples of real-world searches and pivots. The course was challenging and fun – tough combination to pull off."**
>
> —Jason Stoute, **Sanofi**

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

SEC541 is a cloud security course that investigates how attackers are operating against Amazon Web Services (AWS) and Microsoft Azure environments, the attacker's characteristics, and how to detect and investigate suspicious activity in your cloud infrastructure. You will learn how to spot the malice and investigate suspicious activity in your cloud infrastructure. In order to protect against cloud environment attacks, an organization must know which types of attacks are most likely to happen in your environment, be able to capture the correct data in a timely manner, and be able to analyze that data within the context of their cloud environment and overall business objectives.

SEC541 starts each day by walking through a real-world attack campaign against a cloud infrastructure. We will break down how it happened, what made it successful, and what could have been done to catch the attackers in the act. After dissecting the attacks, we learn how to leverage cloud native and cloud integrated capabilities to detect, threat hunt, or investigate similar attacks in a real environment, and building our arsenal of analytics, detections and best practices. The course dives into the AWS and Azure services, analysing logs and behaviors and building analytics that the students can bring back to their own cloud infrastructure.

Business Takeaways

- Decrease the average time an attacker is in your environment
- Demonstrate how to automate analytics, thus reducing time
- Help your organization properly set up logging and configuration
- Decreases risk of costly attacks by understanding and leveraging cloud specific security services
- Lessen the impact of breaches that do happen
- Learn how to "fly the plane", not just the ability to read the manual

Hands-on Training

The labs in this course are hands-on explorations into AWS and Azure logging and monitoring services. **About 75% of labs are AWS and 25% Azure.** Each lab will start by researching a particular threat and the data needed to detect it. In most labs, the students will conduct the attack against their accounts, generating the logs and data needed to perform analysis. Students will use native AWS and Azure services and open-source products to extract, transform, and analyze the threat. The course lecture coupled with the labs will give students a full picture of how those services within AWS and Azure work, the data they produce, common ways to analyze the data, and walk away with the ability to discern and analyze similar attacks in their own cloud environment.

- **SECTION 1:** SEC541 environment deployment, analysing cloud API logs with CloudTrail, parsing JSON-formatted logs with JQ, network analysis
- **SECTION 2:** Environment setup, application/OS log lab with OpenCanary, CloudWatch agent and customization, strange ECS behavior, finding data exfiltration
- **SECTION 3:** Metadata services and GuardDuty, cloud inventory, discovering sensitive data in unapproved location with Macie, vulnerability assessment with Inspector, data centralization with Graylog
- **SECTION 4:** Microsoft 365 Exchange investigation, introduction to Kusto Query Language, log analytics analysis using Azure CLI, Microsoft Defender for Cloud and Sentinel, Azure network traffic analysis
- **SECTION 5:** Setup the automate forensics workflow, analyze the results, participate in the CloudWars Challenge

SEC549: **Enterprise Cloud Security Architecture**

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Enable business through secure cloud architectural patterns
- Connect the dots between architectural patterns and real-life infrastructure
- Build a secure, scalable identity foundation in the cloud
- Centralize your organization's workforce identity to prevent sprawl
- Learn how to incorporate both network-based and identity-based controls
- Ability to create data perimeters for cloud-hosted data repositories
- Enable Security Operations to respond in the Cloud
- Understand the telemetry and logging available across service models (IaaS, PaaS and SaaS)
- Design recovery processes leveraging break-glass accounts
- Strategically approach a phased cloud migration

Who Should Attend

- Cloud security architects
- Security engineers
- Cloud engineers
- DevOps engineers
- Security auditors
- System administrators
- Operations
- Anyone who is responsible for:
  - Enabling business through secure cloud architecture
  - Evaluating and adopting new cloud offerings
  - Planning for cloud migrations
  - Identity and access management
  - Managing a cloud-based virtual network

> **"The problems we talk about are some that I face in my job every day or know I will face shortly. Getting definitive answers for many of these issues is very helpful for me. Getting years of experience from the instructors and what they have worked on is invaluable."**
>
> —Patrick Haughney, **Paylocity**

Design it right from the start

SEC549 takes an architectural lens to enterprise-scale, cloud infrastructure challenges. It addresses the security considerations architects need to tackle when tasked with business expansion into the cloud in order to both maximize the speed of cloud adoption and modernization of the organization. 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, students take away from this course a clear mental model of the cloud and the controls available to them. This allows students to shift their threat models to this new, vastly different world with distributed perimeters and unfamiliar trust boundaries.

It's inevitable that even the most mature organizations will have their security posture challenged, therefore in this course we dive deep into architectures which enable Security Operation Centers to monitor, detect, respond and recover from incidents in the cloud. In this enterprise cloud security architecture course, students learn how to effectively support business goals with robust logging of cloud telemetry and centralization of events and insights gathered at the edge. This course empowers the Architect to ensure adequate logging is configured in cloud environments and develop recovery strategies emphasizing the need to design for availability.

SEC549 is constructed around the cloud migration journey of a fictional company and the challenges they encounter along the way. Aspiring cloud security architect students are tasked with phasing in a centralized identity plan, and designing secure patterns for enabling cloud-hosted applications. Both network-layer and identity-layer controls are covered in-depth as complementary mechanisms for securing access to distributed resources.

Business Takeaways

- Mitigate the risk posed by nascent cloud technologies and their rapid adoption
- Decrease the risk of cloud migrations by planning for phased approach
- Help your organization prevent identity sprawl and tech debt through centralization
- Enable business growth by creating high-level guardrails
- Prevent costly anti-patterns from becoming entrenched
- Move your organization towards a Zero-Trust posture through the uplifting of existing access patterns
- Design effective Conditional Access Policies and learn how to place guardrails around business-driven policy exceptions

Hands-On Training:

The hands-on portion of SEC549 is unique and especially suited to the student who wants to architect for the cloud. Each lab is performed by observing and correcting an anti-pattern presented as an architectural diagram. The 'correct' version of each diagram is implemented as live infrastructure in AWS and made available to the student to explore the configurations. In this course, the students have access to an enterprise-scale AWS Organization and can observe all details discussed in the labs and throughout the course.

Each of the sections of the course discusses security design considerations for all three major clouds, however there is an emphasis on working with AWS and labs are structured around concepts in AWS.

SEC588: **Cloud Penetration Testing**

GCPN
Cloud Penetration Tester
giac.org/gcpn

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Conduct cloud based penetration tests
- Assess cloud environments and bring value back to the business by locating vulnerabilities
- Understand first-hand how cloud environments are constructed and how to scale factors into the gathering of evidence
- Assess security risks in Amazon and Microsoft Azure environments, the two largest cloud platforms in the market today

Who Should Attend

- Both attack and defense-focused security practitioners will benefit greatly from this course by gaining a deep understanding of vulnerabilities, insecure configurations, and associated business risk to their organizations
- Penetration testers
- Vulnerability analysts
- Risk assessment officers
- DevOps engineers
- Site reliability engineers

GCPN
Cloud Penetration Tester
giac.org/gcpn

GIAC Cloud Penetration Tester

"The GIAC Cloud Penetration Testing (GCPN) certification provides our industry with a first focused exam on both cloud technologies and penetration testing disciplines. This certification will require a mastery in assessing the security of systems, networks, web applications, web architecture, cloud technologies, and cloud design. Those that hold the GCPN have been able to cross these distinct discipline areas and simulate the ways that attackers are breaching modern enterprises."
— Moses Frost, Course Author SEC588: Cloud Penetration Testing

- Cloud Penetration Testing Fundamentals, Environment Mapping, and Service Discovery
- AWS and Azure Cloud Services and Attacks
- Cloud Native Applications with Containers and CI/CD Pipelines

Aim your arrows to the sky and penetrate the cloud

You have been asked to perform a Red Team penetration test assessment. The assets are located mainly in the cloud. What if you have to assess Azure Active Directory, Amazon Web Services (AWS) workloads, serverless functions, or Kubernetes? In this course, you will learn the latest penetration testing techniques focused on the cloud and how to assess cloud environments.

Computing workloads have been moving to the cloud for years. Analysts predict that most if not all companies will have workloads in public and other cloud environments very soon. While organizations that start in a cloud-first environment may eventually move to a hybrid cloud and local data center solution, cloud usage will not decrease significantly. So when assessing organizations' risks going forward, we need to be prepared to evaluate the security of cloud-delivered services.

The most commonly asked questions regarding cloud security are "Do I need training for cloud-specific penetration testing?" and "Can I accomplish my objectives with other pen test training and apply it to the cloud?" The answer to both questions is yes, but to understand why, we need to address the explicit importance of conducting cloud-focused penetration testing. In cloud-service-provider environments, penetration testers will not encounter a traditional data center design. Specifically, what we rely on to be true in a formal setting such as who owns the Operating System and the infrastructure, and how the applications are running will likely be very different. Applications, services, and data will be hosted on a shared hosting environment unique to each cloud provider.

SEC588: Cloud Penetration Testing draws from many skill sets that are required to properly assess a cloud environment. If you are a penetration tester, the course will provide a pathway to understanding how to take your skills into cloud environments. If you are a cloud-security-focused defender or architect, the course will show you how the attackers are abusing cloud infrastructure to gain a foothold in your environments.

The course dives into topics of classic cloud Virtual Machines, buckets, and other new issues that appear in cloud-like microservices, in-memory data stores, files in the cloud, serverless functions, Kubernetes meshes, and containers. The course also covers Azure and AWS penetration testing, which is particularly important given that AWS and Microsoft account for more than half of the market. The goal is not to demonstrate these technologies but rather to teach you how to assess and report on the actual risk that the organization could face if these services are left insecure.

> **"This emerging course perfectly complements the change in the direction of red team engagement scopes."**
>
> —Kyle Spaziani, **Sanofi**

> **"The SANS course 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**

GCFR Cloud Forensics Responder giac.org/gcfr

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where it is located
- Identify and utilize new data only available from cloud environments
- Utilize cloud-native tools to capture and extract traditional host evidence
- Quickly parse and filter large data sets using scalable technologies such as the Elastic Stack
- Understand what data is available in various cloud environments

Who Should Attend

- Incident Response Team Members who may need to response to security incidents/intrusions impacting cloud hosted software, infrastructure or platforms and need to know how to detect, investigate, remediate, and recover from compromised systems across the enterprise cloud.
- Threat Hunters who are seeking to understand threats more fully and how to learn from them in order to more effectively hunt threats and counter their tradecraft.
- SOC Analysts looking to better understand alerts, build the skills necessary to triage events, and fully leverage cloud log sources.
- Experienced Digital Forensic Analysts who want to consolidate and enhance their understanding of cloud-based forensics.
- Information Security Professionals who directly support and aid in responding to data breach incidents and intrusions.
- Federal Agents and Law Enforcement Professionals who want to master advanced intrusion investigations and incident response, and expand their investigative skills beyond traditional host-based digital forensics.
- SANS FOR500, FOR508, SEC541, and SEC504 Graduates looking to add cloud-based forensics to their toolbox.

Find the storm in the cloud.

FOR509: Enterprise Cloud Forensics and Incident Response will help you:

- Understand forensic data only available in the cloud
- Implement best practices in cloud logging for DFIR
- Learn how to leverage Microsoft Azure, AWS and Google Cloud Platform resources to gather evidence
- Understand what logs Microsoft 365 and Google Workspace have available for analysts to review
- Learn how to move your forensic processes to the cloud for faster data processing

With FOR509: Enterprise Cloud Forensics and Incident Response, examiners will learn how each of the major cloud service providers (Microsoft Azure, Amazon AWS and Google Cloud Platform) are extending analysts capabilities with new evidence sources not available in traditional on-premise investigations. From cloud equivalents of network traffic monitoring to direct hypervisor interaction for evidence preservation, forensics is not dead. It is reborn with new technologies and capabilities.

Incident response and forensics are primarily about following breadcrumbs left behind by attackers. These breadcrumbs are primarily found in logs. Your knowledge of the investigation process is far more important than the mechanics of acquiring the logs.

This class is primarily a log analysis class to help examiners come up to speed quickly with cloud based investigation techniques. It's critical to know which logs are available in the cloud, whether they are turned on by default, and how to interpret the meaning of the events they contain.

Numerous hands-on labs throughout the course will allow examiners to access evidence generated based on the most common incidents and investigations. Examiners will learn where to pull data from and how to analyze it to find evil. The data will be available in your VM rather than accessed directly via the cloud to ensure a consistent lab experience.

Course Topics

- Cloud Infrastructure and IR data sources
- Microsoft 365 and Graph API Investigations
- Azure Incident Response
- AWS Incident Response
- Google Workspace Investigations
- GCP Incident Response

> **"Thanks a lot for FOR509 course. I believe this course provides a great way to get a really compressed introduction into the different cloud service providers and what is forensically possible there."**
>
> —Marc Stroebel, **HvS-Consulting AG**

GCFR Cloud Forensics Responder giac.org/gcfr

GIAC Cloud Forensics Responder

The GCFR certification validates a practitioner's ability to track and respond to incidents across the three major cloud providers. GCFR-certified professionals are well-versed in the log collection and interpretation skills needed to manage rapidly changing enterprise cloud environments.

- Log generation, collection, storage and retention in cloud environments
- Identification of malicious and anomalous activity that affect cloud resources
- Extraction of data from cloud environments for forensic investigations

LDR520: **Cloud Security for Leaders**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Define a strategy for securing a workload in the cloud for medium and large enterprises that can support their business objectives
- Establish a security roadmap based on the security strategy that can support a fast-paced cloud adoption and migration path while maintaining a high degree of security assurance
- Understand the security fundamentals of the cloud environment across different types of service offerings, then explain and justify to other stakeholders the relevant strategic decisions
- Build an effective plan to mature a cloud security posture over time, leveraging security capabilities offered by cloud providers to leapfrog in security capabilities
- Explain the security vision of the organization in the Cloud domain to your Board Directors and executives, collaborate with your peers, and engage your workforce, driving the security culture change required for the cloud transformation

Who Should Attend

The primary target audience for this course is managers and directors who are in a position to lead or make key decisions on the IT transformation to cloud environments.

Prerequisites

Students should have three to five years of experience in IT and/or cybersecurity. This course covers the core areas of security leadership in migrating workloads to the cloud environment and assumes a basic understanding of technology, networks, and security.

Notice to Students

This course will have limited overlap with the SANS SEC488: Cloud Security Essentials course because it will provide foundational information on cloud services and cloud security to ensure that students are on the same page. This course 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.

Strategically maximize your cloud investment.

Cloud Security Strategy is a comprehensive plan to protect the organization's data, workload, and infrastructure residing in the cloud(s) environment.

Cloud adoption is popular across all types of industries, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Since cloud environments differ significantly from traditional on-premises IT environments, in terms of protection requirements and threat vectors, the traditional network perimeter is no longer the most effective defense in cloud solutions. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions without always understanding the numerous key decisions needed for an organization's successful cloud transition. This cloud security implementation course walks the audience through the journey to mature their cloud security in each of the relevant security domains of could security strategy from beginning to high maturity state.

LDR520 complements traditional IT management techniques that leaders are accustomed to and helps with making appropriately informed decisions around strategy, financial investment, and necessary team technical knowledge and skill. We cover the key objectives of security controls in the cloud environment, including planning, deploying, and running the environment from the starting point to a progressively more mature state. There will be a focus on locking down the environment, securing the data, maintaining compliance, enhancing security visibility to the operations, and managing the security response on a continuous basis. Students will learn the essentials to lead the security effort for the cloud transition journey.

Business Takeaways

- Establish cloud security program supporting the fast pace business transformation
- Understand current and future maturity level of the cloud security in contrast to the industry benchmarks
- Make informed decisions on cloud security program
- Anticipate the security capabilities and guardrails to build for the securing the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Hands-On Cloud Security Stategy Training

LDR520 uses case scenarios, group discussions, team-based security leadership simulations with embedded real life technical components to help students absorb both technical and management topics. About 60 minutes per day is dedicated to these learning experiences using the Cyber42 leadership simulation game. This web application-based game is a continuous exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

> **"Team is collaborative. We are all able to bounce ideas off of each other comfortably and using AWS to get hands-on makes it feel more real than if we were answering questions on a quiz."**
>
> —Richard Sanders, **Best Western International**

CLOUD SECURITY SERVICE MATRIX

SANS CLOUD SECURITY

	Used for...	Amazon Web Services (AWS)	Azure	Google Cloud Platform (GCP)
IDENTITY & ACCESS MANAGEMENT	Manage user access and encryption keys	AWS Identity & Access Management (IAM)	Azure Active Directory (Azure AD)	GCP Identity & Access Management (IAM)
	Cloud single-sign-on (SSO) service	AWS Single Sign-On	Azure Active Directory (Azure AD)	Cloud Identity
	Identity management for your apps	Amazon Cognito	Azure Active Directory (Azure AD)	Firebase Authentication
	Managed Microsoft Active Directory	AWS Directory Service	Azure Active Directory Domain Services	Managed Service for Microsoft Active Directory
	Secure service to share resources	AWS Resource Access Manager	Azure Resource Manager	Resource Manager
	Centrally governing and management across accounts	AWS Organizations	Azure Governance	
DETECTION	Security and compliance center	AWS Security Hub	Microsoft Defender for Cloud	Security Command Center
	Threat detection	Amazon GuardDuty	Microsoft Defender for Cloud	Security Command Center
	Analyzation of application security	Amazon Inspector	Azure Web Application Firewall	Google Cloud Armor
	View of the configurations of your resources	AWS Config	Azure Security Control	Cloud Asset Inventory
	Tracking user activity and API usage	AWS CloudTrail	Azure Audit Logs	Cloud Audit Logs
	Management of security for IoT devices	AWS IoT Device Defender	Azure IoT	Cloud IoT
INFRASTRUCTURE PROTECTION	Network security	AWS Network Firewall	Azure Firewall	Google Cloud Armor
	DDoS protection	AWS Shield	Azure DDoS Protection	Google Cloud Armor
	Filter malicious web traffic	AWS Web Application Firewall	Azure Web Application Firewall	Google Cloud Armor
	Central management of firewall rules	AWS Firewall Manager	Azure Firewall Manager	Google Cloud Armor
DATA PROTECTION	Discover and protect your sensitive data at scale	Amazon Macie	Azure Information Protection	Cloud Data Loss Prevention
	Key storage and management	AWS Key Management Service (KMS)	Azure Key Vault	Cloud Key Management Service
	Hardware based key storage for regulatory compliance	AWS CloudHSM	Azure Dedicated HSM	Cloud HSM
	Provision, manage, and deploy public and private SSL/ TLS certificates	AWS Certificate Manager	Azure Active Directory Certificate Authority	Certificate Authority Service
	Rotate, manage and retrieve secrets	AWS Secrets Manager	Azure Key Vault	Secret Manager
INCIDENCE RESPONSE	Investigate potential security issues	Amazon Detective	Azure Sentinel	Security Command Center
	Fast, automated, cost- effective disaster recovery	CloudEndure Disaster Recovery	Azure Site Recovery	Security Command Center
COMPLIANCE	No cost, self-service portal for on-demand access to compliance reports	AWS Artifact	Service Trust Portal	Compliance Reports Manager
	Continuously audit your usage to simplify how you assess risk and compliance	AWS Audit Manager	Service Trust Portal	Cloud Audit logs

SANS
CLOUD
SECURITY

CLOUD ACE JOURNEYS

Keep up with the speed of cloud. Upskill. Reskill. Continue the journey. Advance your career. Multiple collections of three courses by job role to become a well-rounded, future-thinking, cloud-security practitioner. Discover the benefits of completing a journey. **#SANSCloudAce**

ACE
CLOUD SECURITY ANALYST
SEC488 FOUNDATION
SEC510 MULTICLOUD
SEC541 DETECTION

I use cloud security solutions to enable defenses and detect attacks. I have:

- Established a security foundation -

- Enable comprehensive defenses -

- Learned to detect attacks -

ACE
CLOUD SECURITY ARCHITECT
SEC549 ARCHITECTURE
SEC510 MULTICLOUD
SEC540 AUTOMATION

I design cloud security solutions, architectures, and automation best practices. I have:

- Mastered architectural structure -

- Effectively design multicloud requirements -

- Utilized automation for speed and accuracy -

ACE
CLOUD SECURITY ENGINEER
SEC510 MULTICLOUD
SEC540 AUTOMATION
SEC549 ARCHITECTURE

I build security solutions for cloud workflows. I can:

- Build multicloud defenses -

- Maximize automation -

- Decipher architecture -

ACE
DEV SEC OPS
SEC540 AUTOMATION
SEC510 MULTICLOUD
SEC522 APPSEC

I develop, deploy, and manage secure applications and systems. I can:

- Maximize automation for speed and accuracy -

- Automate security across CSPs using IaC -

- Secure my applications -

ACE
CLOUD DETECTION & RESPONSE
SEC541 DETECTION
SEC588 PEN TESTING
FOR509 FORENSICS

I monitor and test cloud environments to detect and investigate threats. I can:

- Monitor and detect attacks -

- Pen test cloud environments -

- Investigate cloud threats -

SANS.ORG/CLOUD-SECURITY/ACE

BECOME A SANS CLOUD ACE

Frank Kim

SANS Faculty Fellow | @fykim

Frank Kim is the CISO-in-Residence at YL Ventures, supporting Israeli cybersecurity entrepreneurs with ideation and market research, conducting due diligence for potential investments, and engaging in go-to-market activities of the firm's portfolio companies. He leads the Cloud Security and Cybersecurity Leadership curricula to help shape and develop the next generation of security leaders. Frank is also the author and instructor of MGT512, MGT514, and co-author of SEC540.

Eric Johnson

SANS Senior Instructor | @emjohn20

Eric is a Co-founder and Principal Security Engineer at Puma Security and a Senior Instructor with the SANS Institute. His experience includes cloud security assessments, cloud infrastructure automation, static source code analysis, web and mobile application penetration testing, secure development lifecycle consulting, and secure code review assessments. Eric is the lead author and an instructor for SEC540 and a co-author and instructor for SEC510. Additionally, Eric is a SANS Security Awareness Developer Training Advisory Board Member and SANS Analyst for Application Security and DevSecOps Surveys.

Jason Lam

SANS Principal Instructor | @jasonlam_sec

Jason holds a leadership role at a large global financial company. In this role, he's accountable for global direction and management of cybersecurity defense and response. He has nearly two decades of experience in the information security industry, progressing from hands-on research work to securing large-scale enterprise environments. Over the years, Jason has performed and led intrusion detection, penetration testing, defense improvement programs and incident response in large enterprise environments. Jason is a co-author and instructor for SEC522 as well as sole author of LDR520.

Serge Borso

SANS Certified Instructor | @SergeBorso

When it comes to cybersecurity, Serge is among the best possible instructors to learn from due to his experience, accomplishments, and, quite frankly, his personality. Duplicate badges to walk right through security and access a "secure" facility – did that. Dumpster diving for sensitive information outside of a financial institution – to him, that was "lots of fun." Create an enterprise-wide, measurably successful security program for a billion-dollar company – one of his many accomplishments. All of them, in scope of the engagements. He's an instructor for SEC488 and author of SEC388, a published author, *President of the Denver Open Web Application Security Project (OWASP)* chapter, founder and CEO of the cybersecurity consulting firm, SpyderSec, he's discovered multiple 0-days, written OSINT tools for the community, and is a polished presenter who speaks regularly at national conferences. Truly, an expert in the field.

WITH THESE EXPERTS

Ryan Nicholson

SANS Certified Instructor | @ryananicholson

Ryan's passion for information technology started in 2001 when he found himself constantly trying to make his high school's computers and even calculators do things that they weren't exactly intended to do. They lacked games, so he learned how to create some. Yes, some may call this hacking. Ryan called it "fun," which led to attending college with intentions of becoming a software engineer. During school, Ryan obtained an internship with a very cybersecurity-minded organization—the Defense Information Systems Agency (DISA). Ever since then, he's been hooked on cybersecurity. Ryan is the author for SEC488, co-author of SEC541, and an instructor for SEC530.

Brandon Evans

SANS Certified Instructor | @brandonmaxevans

Brandon is the owner and an InfoSec Consultant at On-Brand Technologies LLC, a consultancy helping organizations secure their applications and other workloads in multi cloud environments, specializing in AWS, Azure, and Google Cloud. Prior to starting his consultancy, Brandon led the secure development training program at Zoom Video Communications. Brandon is lead author for SEC510 and a contributor and instructor for SEC540.

Shaun McCullough

SANS Certified Instructor Candidate | @thecybergoof

As a hands-on practitioner with a gift for architecture design, Shaun explores the good and bad of how the Cloud is changing the way the industry secures and runs infrastructure. During his 25+ years of experience, Shaun has spent equal parts in security engineer and operations as well as software development. With extensive experience within the Department of Defense, Shaun was the Technical Director of the Red and Blue operations teams, a researcher of advanced host analytics, and ran a threat intelligence focused open source platform based on MITRE ATT&CK. Previously, he was a consultant with H&A Security Solutions, focusing on analytic development, DevOps support, and security automation tooling. Shaun is co-author of SEC541.

Kat Traxler

Cloud Security Engineer | @NightmareJS

Kat Traxler is a Security Professional in the Twin Cities performing cloud research and security architecture in the areas of public cloud, container orchestration systems and IAM platforms. In her time in the security industry, she has had roles performing penetration testing targeting web applications, cryptographic infrastructure and fintech technologies. She has presented at various conferences including SANS Security Summit and fwd:CloudSec on topics such as privilege escalation and bughunting in the cloud. She is the author of SEC549.

SANS

CLOUD SECURITY

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

☎ 301-654-SANS (7267) ✉ support@sans.org