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 your journey to become a Cloud Security Ace.

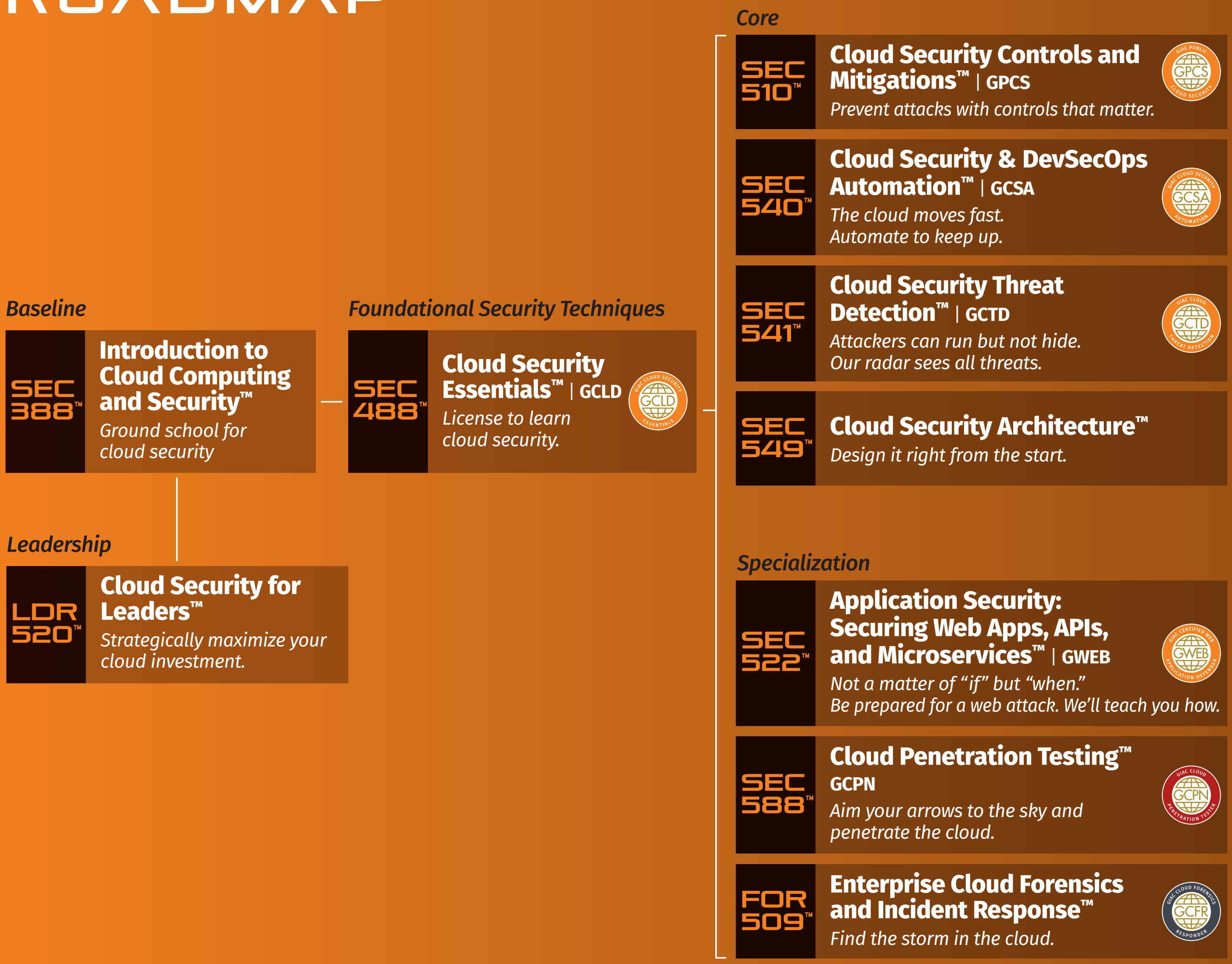
Our curriculum has been developed through an industry consensus process and is a holistic, hands-on approach to address public cloud security, which includes multicloud and hybrid-cloud scenarios for the enterprise and developing organizations alike. Learn how various CSPs interact and the nuances among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

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

Leadership

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

Foundational Security Techniques

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

Core

SEC510™ Cloud Security Controls and Mitigations™ | GPCS
Prevent attacks with controls that matter.

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

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

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

Specialization

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

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

FOR509™ Enterprise Cloud Forensics and Incident Response™
Find the storm in the cloud.

Flight Plan – Career Progression

CURRICULUM

BASELINE

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

FOUNDATIONAL

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

CORE

SEC510™ **Cloud Security Controls and Mitigations™**
Prevent attacks with controls that matter.
GPCS

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

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

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

SPECIALIZATION

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

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

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

LEADERSHIP

LDR520™ **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	18	Laptop
Day Course	CPEs	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 training 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 training 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 training'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

- Spot organizational deficiencies in cloud security
- Speak the language of cloud security confidently with both technical and leadership teams
- Navigate your organization through the current security challenges and opportunities presented by cloud services
- Identify risks associated with various services offered by cloud service providers (CSPs)
- Select appropriate security controls for different cloud network security architectures
- Evaluate CSPs based on their documentation, security controls, and audit reports
- Confidently use services from leading CSPs, including AWS, Azure, and GCP
- Protect secrets and sensitive information within cloud environments
- Leverage cloud logging capabilities to establish accountability for events in the cloud
- Determine risk control ownership based on deployment and service delivery models of CSP products
- Assess the trustworthiness of CSPs using their security documentation, service features, and third-party attestations
- Secure access to CSP management consoles and environments
- Implement native network security controls in AWS and Azure
- Conduct penetration testing following guidelines from AWS and Azure to test full-stack cloud applications

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

Essential Knowledge for a Secure Cloud Environment

Attackers are targeting everything that uses code to compute, making insecure cloud environments highly vulnerable to breaches. SEC488 is your solution for securely migrating to the cloud and continuously enhancing cloud security. This course offers comprehensive cloud security knowledge, delivering quick and powerful results in areas such as identity guardrails, cloud storage, virtual machines, automation, remote management, cloud logging, legal and contractual requirements, and more. Safeguarding critical issues like Identity and Access Management (IAM) and securing S3 Buckets are crucial for mitigating risks associated with lift-and-shift transitions.

Maximize your time and resources with this curated, hands-on course that goes beyond theory. Engage in fun, interactive, live-fire labs within actual cloud service provider (CSP) environments on both AWS and Azure. Learn to effectively limit and mitigate the impact of cloud security breaches, preventing issues like service shutdowns due to computational limits or excessive charges from unauthorized covert bitcoin mining operations. Enhance compliance, protect your organization's reputation and assets, and strengthen your security posture while boosting employee retention and team knowledge with SEC488.

Hands-On Training

SEC488: Cloud Security Essentials training 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:™ **Cloud Security Controls and Mitigations™**

GPCS
Public Cloud Security
giac.org/gpcs

5 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Make informed decisions in the Big 3 cloud service providers by understanding the inner workings of each of their Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings
- Implement secure Identity and Access Management (IAM) with multiple layers of defense-in-depth
- Build and secure multi cloud networks with segmentation and access control
- Encrypt data at rest and in-transit throughout each cloud
- Control the confidentiality, integrity, and availability of data in each cloud storage service
- Support non-traditional computing platforms like Application Services and serverless Functions as a Service (FaaS)
- Integrate each cloud provider with one another without the use of long-lived credentials
- Automate security and compliance checks using cloud-native platforms
- Quickly adopt third-party cloud vendors while minimizing the risk introduced by granting them access to cloud resources
- Guide engineering teams in enforcing security controls using Terraform and Infrastructure-as-Code (IaC)

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

Prevent real attacks with controls that matter.

Protecting multicloud environments is challenging; Default security controls often fall short, and controls that work in one of the Big Three CSPs may not work in the others. Rather than focusing solely on compliance, organizations should prioritize attack driven controls to safeguard their most critical Cloud assets.

Whether an application is developed in-house or by a third party, accepting the inevitability of application flaws is key for implementing successful cloud security controls. While few cybersecurity professionals can fix vulnerable code, it's often easier to apply secure cloud configurations to mitigate these risks. Relying solely on CSP defaults and documentation is insufficient. SEC510 training reveals numerous instances of incorrect, incomplete, or contradictory CSP controls. Additionally, if there is a zero-day vulnerability in a cloud service used by your organization, you must brace for that impact by controlling what you can.

While standards and frameworks, such as the MITRE ATT&CK Cloud Matrix, the Center for Internet Security (CIS) Cloud Provider Benchmarks, and the Cyber Defense Matrix, are helpful tools of the trade, they still have limits. That's why SEC510 training goes beyond them to teach the techniques necessary to protect what matters to your organization. Mitigate the risk of common cloud mistakes with cloud security controls that matter and reduce your attack surface by eliminating misconfigurations.

Hands-On Training

SEC510: Cloud Security Controls and Mitigations training reinforces all the concepts discussed in the lectures through hands-on labs in real cloud environments. Each lab includes a step-by-step guide as well as a "no hints" option for students who want to test their skills without 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 use the lab instructions, application code, and IaC after the course concludes. With this, they can repeat every lab exercise in their own cloud environments as many times as they like.

SEC510 training 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 CSPs 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 entreprise 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
- Implement infrastructure security and configuration management
- Securely integrate cloud components into a web application
- Learn about authentication and authorization mechanisms, including single sign-on patterns
- Understand cross-domain web request security
- Leverage protective HTTP headers
- Defend SOAP, REST, and GraphQL APIs
- Securely implement Microservice architecture
- Defend against input-related flaws such as SQL injection, XSS, and CSRF
- Secure the integration of AI components into modern applications

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**

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

Over the course of SEC522 training, we demonstrate the real-world risks associated with web applications, emphasizing the many ways that sensitive data can be exposed or compromised. From here, participants learn practical techniques to mitigate these risks, assess vulnerabilities, and effectively communicate residual risks.

Students will be able to apply the skills that they learned in SEC522 training the moment they return to work, incorporating security early in the development process ("shifting left"). Not only does this ensure more efficient testing and decision-making, it also saves time, money, and resources while improving overall application security within 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 VM lab environment offers a realistic application setting where students can explore attacks and see the impact of defensive mechanisms. Structured as a challenge with helpful hints, the hands-on labs provide practical experience that students can apply immediately when they return to work. The 20 labs across Sections 1–5 culminate in an exciting 3–4 hour competitive Defend-the-Flag Capstone. This final challenge allows participants to put their skills to the test in a dedicated, immersive exercise.

- **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 Day Program | 38 CPEs | Laptop 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
- Parse security scanning results and display the data on CI/CD dashboards
- Manage secrets for CI/CD servers and cloud native applications
- Automate configuration management using Infrastructure as Code (IaC)
- Build, harden, and publish golden virtual machine images using CI/CD workflows
- Operate and secure container technologies using Docker and Kubernetes
- Manage the software supply chain using software provenance, attestations, artifact signing, software bill of materials (SBOM), and SBOM vulnerability scanning.
- Harden Kubernetes clusters with workload identity and admission control
- Monitor Kubernetes audit logs using cloud logging and monitoring services
- Deploy patches using cloud and Kubernetes blue/green deployments
- Refactor systems to take advantage of microservice and serverless architectures
- Automate cloud compliance and security policy guardrails and auto-remediation playbook

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:

- Malicious code, credential theft, and compromised extensions from improperly protected continuous integration and delivery pipelines.
- Unenforced peer code reviews and security approvals that do not meet change approval and audit requirements
- False positives, noise, and build failures from incorrectly automated security scanners
- Configuration drift between environments, resource misconfigurations, and public data exposure from insufficiently managed cloud infrastructure
- Failure to standardize golden virtual machine and container base images across the organization
- Ignoring software supply chain vulnerabilities inherited from malicious libraries, third-party software, and compromised build artifacts
- Operating Kubernetes services without policies that prevent lateral movement between workloads, reduce pod permissions, and monitor cluster activity
- Failing to release patches and close vulnerability windows due to code freezes and failed deployments
- Lacking inventory and visibility between microservices and serverless systems

Security teams can help organizations prevent these issues by developing a DevOps mindset and learning to apply cloud native security controls. 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 native infrastructure and software. Students learn how to attack and then harden the entire DevOps workflow, from version control to continuous integration and running cloud native workloads. Each step of the way, students explore the security controls, configuration, and policies required to improve the reliability, integrity, and security of on-premises and cloud-hosted systems. Students learn how to implement more than 20 DevSecOps security controls to build, test, deploy, harden, and monitor cloud native infrastructure and services.

Hands-On Training

SEC540 trainng 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 training 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 training 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, two 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.

SEC541:™ **Cloud Security Threat Detection™**

GCTD
Cloud Threat Detection
giac.org/gctd

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Understand how identities can be abused in cloud environments
- Monitor threat actors using cloud-native logging tools
- Define and understand compute resources such as virtual machines (VMs) and containers
- Detect and address attacker pivots within your cloud infrastructure
- Implement effective detection strategies using cloud provider tools
- Investigate and analyze instances in your compute resources for suspicious activities
- Perform detailed analysis and detection of threats in Microsoft 365 and Azure environments
- Pivot between different log sources to uncover the full narrative of an attack
- Build automation workflows to reduce repetitive security tasks
- Centralize and normalize data from various sources to enhance analysis and threat detection

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.

It's undeniable that cloud environments offer unparalleled benefits, however, poorly trained personnel can expose your organization to an ever-expanding list of dynamic threats. SEC541: Cloud Security Threat Detection training is designed to address these challenges by equipping professionals with the skills to identify, detect, and respond to threats in cloud infrastructures. This comprehensive course delves into cloud-native logging, threat models, intrusion detection, and continuous monitoring, ensuring that your organization can maintain a robust security posture in AWS, Azure, and Microsoft 365 environments.

SEC541 training immerses students in real-world scenarios, teaching them to navigate cloud-specific logs, build effective threat detection systems, and understand the unique aspects of cloud architecture. By mastering these skills, your team can significantly reduce detection and response times, enhance visibility into the cloud threat landscape, and effectively defend against sophisticated attacks.

SEC541 training boosts the proficiency of cloud security analysts and empowers teams to operate more efficiently and effectively, maximizing your organization's security capabilities. Equip your workforce with the latest knowledge in cloud security threat detection and ensure your organization is prepared to tackle the complexities of modern cloud security challenges.

Business Takeaways

- **Reduce Detection and Response Time—**Quickly identify and respond to critical cloud threats.
- **Enhance Visibility—**Gain comprehensive insights into your cloud environment.
- **Improve Security Posture—**Implement effective cloud-specific threat detection strategies.
- **Proactive Threat Management—**Address threats early, aiding in swift incident resolution.
- **Efficiency and Automation—**Increase efficiency with automated detection and response workflows.
- **Cost Savings—**Avoid financial fallout by proactively securing your cloud environment.
- **Upskill Workforce—**Equip your team with the latest cloud security knowledge and techniques to defend against sophisticated cloud threats.

Hands-on Training

The hands-on portion of SEC541 training is designed to provide students with practical, real-world experience in cloud security threat detection. Each student receives access to their own AWS and Azure accounts, where they can explore and interact with live cloud environments. The labs cover a wide range of topics, from analyzing cloud-native logs to detecting and responding to threats in AWS, Azure, and Microsoft 365. Students will perform attacks against their own accounts, generating the data needed for thorough analysis and investigation.

A key component of SEC541 training is the 21 interactive labs, making up about 40% of the course time, split evenly between AWS and Azure environments. These labs are essential for applying the lecture's lessons by allowing students to practice and hone their skills in a controlled environment. By engaging in these hands-on activities, students gain a deeper understanding of cloud-specific threats and the tools and techniques needed to detect and respond to them effectively. This immersive approach ensures that participants leave the course with the confidence and capability to secure their own cloud environments.

SEC549:™ **Cloud Security Architecture™**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Enable business through secure enterprise cloud security architectural designs
- Connect the dots between cloud architecture designs and real-life solutions
- Build a secure, scalable identity foundation in the cloud
- Centralize your organization's workforce identity to prevent sprawl
- Build micro-segmented networks using hub and spoke patterns
- Configure centralized network firewalls for inspecting north-south and east-west traffic
- Learn how to incorporate both network-based and identity-based controls
- Create data perimeters for cloud-hosted data repositories
- Centralize and share Key Management Service (KMS) resources across an organization
- Enable security operations and incident response in the cloud
- Understand the telemetry and logging available across service models (IaaS, PaaS, and SaaS)
- Design push and pull logging architectures for centralized log aggregation
- Plan for cloud recovery processes using multiple tiers of break-glass accounts

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

Design it right from the start.

SEC549 training teaches students how to design enterprise-scale, cloud infrastructure solutions for their organization. By learning the cloud providers' well-architected frameworks, security architects can design centralized security controls for their cloud estate while maximizing the speed of cloud adoption for the organization. Students will learn how threat models change in the cloud with new, vastly distributed perimeters and unfamiliar trust boundaries. With those challenges in mind, our focus shifts to designing strategies for centralizing and reinforcing workforce identity, conditional access, policy guardrails, network security controls, data perimeters, and log streams.

SEC549 training takes students through the cloud migration journey of a fictional company and the challenges they encounter along the way. As aspiring cloud security architects, students are tasked with phasing in a centralized identity plan for workforce cloud management and cloud-hosted application access along with supporting workload identity design principles for granting access to other cloud services. In addition, policy guardrails are put in place to create boundaries which help the organization maintain both security and compliance while providing flexibility for engineering teams. With identity and access management (IAM) in place, we start evaluating the pros and cons of various network and data lake designs to build a data perimeter for the organization. The final mission is monitoring network and data access by centralizing log data across the organization to secure access to critical resources.

Business Takeaways

- Mitigate the risks introduced by cloud technologies and their rapid adoption
- Decrease the risk of cloud migrations by planning a phased approach
- Prevent identity sprawl and technical debt through centralization
- Enable business growth by creating high-level guardrails
- Prevent costly anti-patterns from sprawling throughout a cloud organization
- Apply learned access patterns to help move your organization towards zero-trust
- 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 training is unique and especially suited to students who want to architect for the cloud. Each lab is performed by observing and correcting an anti-pattern presented as an architectural diagram. The completed version of each diagram is implemented as live infrastructure in AWS, Azure, or Google (depending on the topic) and made available for students to explore. In this course, students have access to an enterprise-scale AWS, Azure, and Google Cloud organization and can observe all details discussed in the labs and throughout the course.

> **"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**

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 for vulnerabilities
- Understand cloud environment construction and evidence-gathering
- Evaluate security risks in AWS and Azure
- Apply course knowledge directly to your work
- Test cloud environments through real-world labs
- Differentiate cloud-native, multi-cloud, and hybrid infrastructures
- Conduct penetration tests on microservices
- Understand container and CI/CD pipeline vulnerabilities
- Attack Kubernetes, serverless functions, and Windows containers
- Analyze and attack cloud identity systems and report findings to your organization

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

Aim your arrows to the sky and penetrate the cloud.

With the rise in cloud adoption, continuous technological advancements, and an ever-evolving threat landscape, organizations need to keep up with the complex security challenges specific to cloud-based services and infrastructure. Security professionals must develop penetration testing skills in cloud technologies that enable them to assess risk to the organization and recommend effective mitigations that will protect their critical assets.

This one-of-a-kind SANS course equips you with the knowledge and hands-on skills required to perform comprehensive cloud-focused penetration tests and assessments. You will learn the underlying technology powering cloud infrastructure and the vulnerabilities that adversaries leverage in their attacks. Through 27 hands-on labs and practitioner-led instruction, you'll master real-world attack tools and techniques to effectively identify risk to the organization.

Author Statement

When I was first asked about putting together a cloud penetration testing class, there were many questions. Could there be room for a class as niche as this? We felt the need to have a class with all new material and topics we had not covered in our other penetration testing classes. I believe we have met that need with SEC588 training in ways most could not have imagined. This course breaks the rules and allows us to help you test, assess, and secure cloud environments.

—Moses Frost

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

"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 Day Program | 36 CPEs | Laptop 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 respond 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
- InfoSec 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 training 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 training, 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

ACE
CLOUD DETECTION & RESPONSE
SEC541 DETECT · SEC588 ATTACK · FOR509 DISCOVER

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 training 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 secure the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Hands-On Cloud Security Strategy Training

LDR520 training 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**

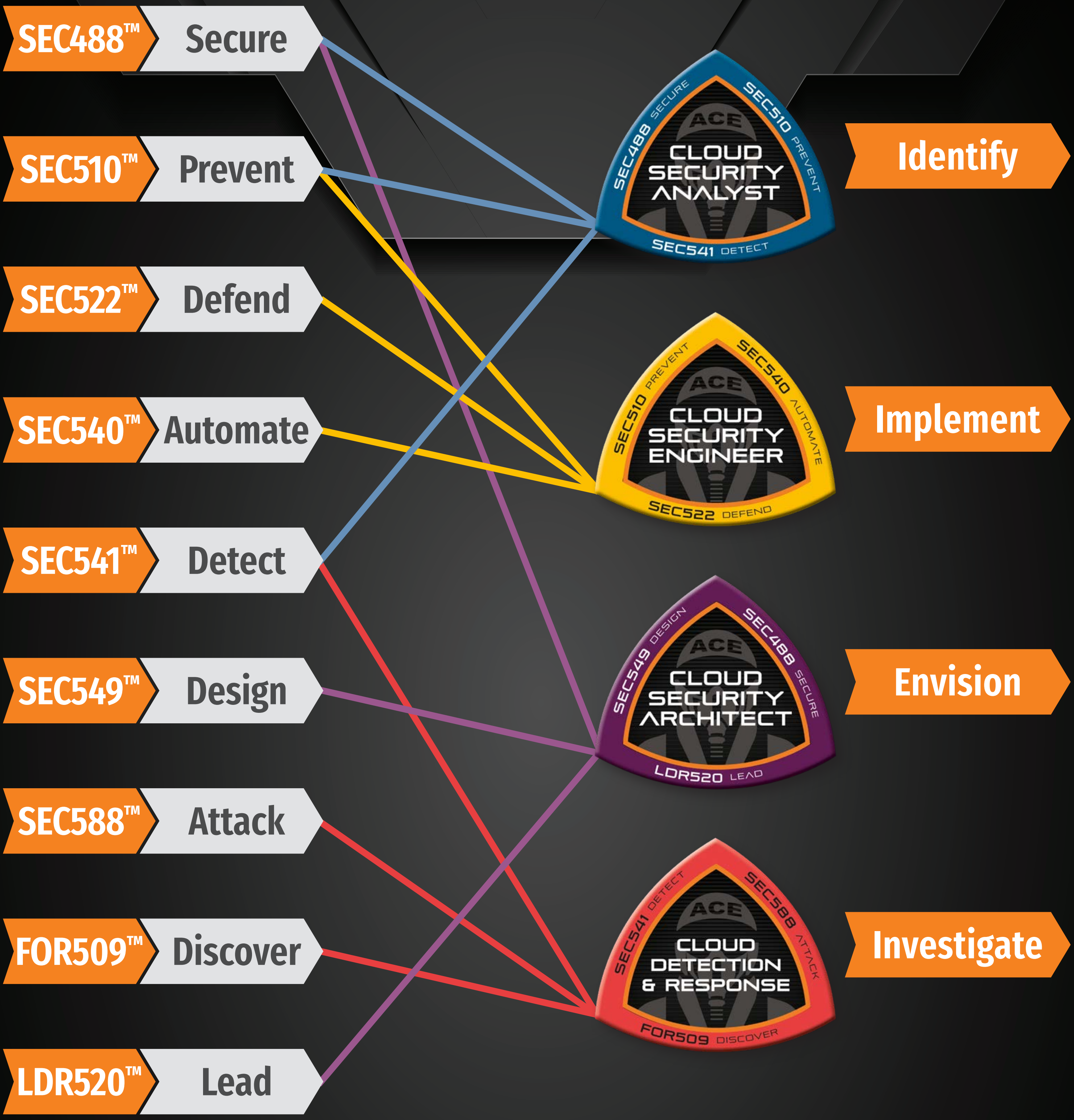
CLOUD SECURITY SERVICE MATRIX

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

CLOUD SECURITY WIREFRAME

sans.org/cloud-security/ace



SEC488™ Secure

SEC510™ Prevent

SEC522™ Defend

SEC540™ Automate

SEC541™ Detect

SEC549™ Design

SEC588™ Attack

FOR509™ Discover

LDR520™ Lead

SEC488 SECURE SEC510 PREVENT ACE CLOUD SECURITY ANALYST SEC541 DETECT

Identify

SEC510 PREVENT SEC540 AUTOMATE ACE CLOUD SECURITY ENGINEER SEC522 DEFEND

Implement

SEC549 DESIGN SEC488 SECURE ACE CLOUD SECURITY ARCHITECT LDR520 LEAD

Envision

SEC541 DETECT SEC588 ATTACK ACE CLOUD DETECTION & RESPONSE FOR509 DISCOVER

Investigate

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 LDR512,™ LDR514,™ 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™ and SEC549.™ 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.

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.™

WITH THESE EXPERTS

Ryan Nicholson SANS Senior 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.™

Shaun McCullough SANS Certified Instructor | @thecybergoof

Shaun spent 20+ years at the National Security Agency working in all aspects of cyber operations. A software engineer, manager, researcher, and operations lead, including as the technical director of the Blue, Red, and Hunt teams. Today, Shaun is a staff level Cloud Security Engineer at GitHub focusing on cloud infrastructure. Shaun is also the lead author of SEC541,™ which focuses on how attackers target cloud infrastructure and what security analysts, SOC operators, and detection engineers can do to protect their organizations.

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.™

Ahmed Abugharbia SANS Certified Instructor | @aagsec

Ahmed Abugharbia works for CDW's Managed Security Services. He manages a team of engineers that are responsible for building managed cloud security services. Ahmed is also a co-founder of Cystack consulting, which has been serving clients in the Middle East since 2010. Over the past 15 years, Ahmed has worked on a wide range of security projects and technologies, from securing networks and applications to penetration testing and incident handling. With introduction of cloud services, Ahmed has turned his interest into cloud security and DevSecOps. Ahmed is an instructor for SEC540.™

David Hazar SANS Certified Instructor | @HazarDSec

David is a security consultant based in Salt Lake City, Utah focused on vulnerability management, application security, cloud security, and DevOps. David has 20+ years of broad, deep technical experience gained from a wide variety of IT functions held throughout his career, including: developer, server admin, network admin, domain admin, telephony admin, database admin/developer, security engineer, risk manager, and AppSec engineer. David is a co-author and instructor for LDR516™ and SEC549,™ as well as an instructor for and contributor to SEC540,™ and has also developed and led technical security training initiatives at many of the companies for which he has worked.

SANS

CLOUD SECURITY

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

X – @SANSCloudSec

LinkedIn – www.linkedin.com/showcase/sanscloudsec

YouTube – www.youtube.com/SANSCloudSecurity

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

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