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 your 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.

- **SEC488** Cloud Security Essentials
  - License to learn cloud security.

Security Management

- **MGT520** Leading Cloud Security Design and Implementation
  - Chart your course to cloud security.

Foundational Security Techniques

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

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

  - **SEC541** Cloud Security Attacker Techniques, Monitoring, and Threat Detection
  - GCPN
  - Attackers can run but not hide. Our radar sees all threats.

  - **SEC549** Enterprise Cloud Security Architecture
  - GCFA
  - Design it right from the start.

Specialization

- 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.

- **SEC522** Cloud Penetration Testing
  - GCPN
  - Aim your arrows to the sky and penetrate the cloud.

- **SEC588** Enterprise Cloud Forensics and Incident Response
  - GCFR
  - Find the storm in the cloud.

COURSE | GIAC CERT
--- | ---
SEC388 | Introduction to Cloud Computing and Security | 6
SEC488 | Cloud Security Essentials | GCLD | 7
SEC510 | Public Cloud Security: AWS, Azure, and GCP | GPCS | 8
SEC522 | Application Security: Securing Web Apps, APIs, and Microservices | GWEB | 9
SEC540 | Cloud Security and DevSecOps Automation | GCSA | 10
SEC541 | Cloud Security Attacker Techniques, Monitoring, and Threat Detection | 11
SEC549 | Enterprise Cloud Security Architecture | 12
SEC588 | Cloud Penetration Testing | GCPN | 13
FOR509 | Enterprise Cloud Forensics and Incident Response | GCFR | 14
MGT520 | Leading Cloud Security Design and Implementation | 15
Flight Plan – Career Progression

**BASELINE**

**SEC 388**

**Introduction to Cloud Computing and Security**

Ground school for cloud security.

**SEC 488**

**Cloud Security Essentials**

License to learn cloud security.

**SEC 510**

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

Multiple clouds require multiple solutions.

**SEC 540**

**Cloud Security and DevSecOps Automation**

The cloud moves fast. Automate to keep up.

**SEC 541**

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

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

**SEC 549**

**Enterprise Cloud Security Architecture**

Design it right from the start.

**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.

**SEC 588**

**Cloud Penetration Testing**

Aim your arrows to the sky and penetrate the cloud.

**FOR 509**

**Enterprise Cloud Forensics and Incident Response**

Find the storm in the cloud.

**CORE**

**SEC 550**

**Leading Cloud Security Design and Implementation**

Chart your course to cloud security.

**Level Definitions**

**Baseline**

Courses that impart the baseline skills required of any information security professional involved in Cloud Security, whether active practitioner or manager.

**Foundational**

Courses that provide the basic knowledge to introduce students to a required skill set for the Cloud Security industry specifically.

**Core**

Courses that prepare professionals for more focused job functions in Cloud Security, including manager, architect, engineer, analyst, and developer.

**Specialization**

Courses for critical, advanced skills, or specialized roles in Cloud Security.

**Management**

Courses that prepare leaders to make sound strategic business decisions in regards to cloud security planning and implementation.
<table>
<thead>
<tr>
<th>Cloud Security Analyst</th>
<th>Cloud Security Engineer</th>
<th>Cloud Security Architect</th>
<th>Cloud Security Manager</th>
<th>DevOps Professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use cloud security solutions to respond to incidents and enable defenses</td>
<td>Build security solutions for cloud workflows</td>
<td>Design how security functions will adopt cloud services, define knowledge, tooling, and approach for cloud solutions</td>
<td>Develop cloud security roadmap, plan, procurement models, ensure policy and procedure is defined to support cloud</td>
<td>Develop, deploy, and manage secure applications and systems</td>
</tr>
</tbody>
</table>
**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
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.

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
Multiple clouds require multiple solutions.

SEC510 provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Students will launch unhardened services, analyze the security configuration, validate that they are insufficiently secure, deploy patches, and validate the remediation. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services and will leave the course confident that they have the knowledge they need when adopting services and Platform as a Service (PaaS) / Infrastructure as a Service (IaaS) offerings in each cloud.

The Big 3 cloud providers alone provide more services than any one company can consume. As security professionals, it can be tempting to limit what the developers use to the tried-and-true solutions of yesteryear. Unfortunately, this approach will inevitably fail as the product development organization sidelines a security entity that is unwilling to change. Functionality drives adoption, not security, and if a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. SEC510 gives you the ability to provide relevant and modern guidance and guardrails to these teams to enable them to move both quickly and safely.

Hands-On Training

SEC510: Public Cloud Security: AWS, Azure, and GCP consolidates all of the concepts discussed in the lectures through hands-on labs. In the labs, students will assess a modern web application written with Next.js, React, and Sequelize that leverages the cloud native offerings of each provider. 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.

SEC510 also offers students an opportunity to participate in CloudWars Bonus Challenges each day in a gamified environment, while also providing more hands-on experience with the cloud security and relevant tools.

Course Authors’ Statement

“The move to leveraging 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 accurate in all cases. 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 additional cloud solutions in the first place? To make their jobs easier or more enjoyable. Developers are creating products that make money for the business, not for the central security team. If a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. Security should embrace the inevitability of the multicloud movement and take on the hard work of implementing guardrails that enable the organization to move quickly and safely.

“The multicloud storm is coming, whether you like it or not.”
— Brandon Evans and Eric Johnson

“The course content has been very well put together, well researched, and is very applicable.”
—Dan Van Wingerden, Radiology Partners
SEC522: Application Security: Securing Web Apps, APIs, and Microservices

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

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

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.

“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

GIAC Certified Web Application Defender
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
- Application and HTTP Basics, Web Architecture, Configuration, and Security

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

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 |

sans.org/sec541
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
- Strategically approach a phased cloud migration

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts, engineers, and managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

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

Hands-On Training:

The hands-on portion of the 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 12correct 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.

- SECTION 1: Structuring Accounts to Create Effective Hierarchies, Transitioning Access from IAM Users to Roles, AWS SSO for Permission Management
- SECTION 2: Integrating Modern Authentication into Legacy Applications, Creating a Shared VPC Architecture, Access Control for Shared Data Sets

All three of today’s labs were helpful in cementing the concepts. The ‘See It In Action’ portions were particularly useful.”

—Oritse Uku

“The lab was straightforward and didn’t require much existing AWS cloud knowledge. The lab demonstrated the how and why policies need to be manageable.”

—Andrew Guggenberger

“The lab was straightforward and didn’t require much existing AWS cloud knowledge. The lab demonstrated the how and why policies need to be manageable.”

—Andrew Guggenberger

Design It Right From The Start

Without a mental model for threats in the cloud, architects attempt to strong-arm design patterns intended for the on-premise world onto cloud systems, hindering the speed of cloud adoption and modernization. Worse yet, failure to identify trust boundaries in the cloud results in missing security controls at the identity or network-planes and poor security outcomes. In the SEC549, students are introduced to security architecture as it applies to the cloud. Students take away from this course a clear mental model of the cloud and the controls available to them, allowing students to shift their threat models to this new, vastly different world with distributed perimeters and unfamiliar trust boundaries.

The course is constructed around the cloud migration journey of a fictional company and the challenges they encounter along the way. 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. The importance of centralising identity is a core take-away of this course as showcased through the discussion of fragmented identity and its perils, especially with the rise of the Cloud and the adoption of multiple cloud service providers. Students are taught the foundational concepts used when designing for phased identity consolidation so they can confidentially tackle similar challenges on the job.
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**

### 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.
- 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

---

**GIAC Cloud Forensics Responder**

The GCFR certification validates a practitioner’s ability to track and respond to incidents across the three major cloud providers. GIAC-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

---

**“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
Building and Leading a Cloud Security Program

Cloud adoption is popular across all types of industry, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions. However, an organization’s cloud transition requires numerous key decisions.

This course focuses on what managers, directors, and security leaders need to know to develop their cloud security roadmap, to manage the implementation of cloud security capabilities, as well as how to operate the cloud environment post-transition. Making the right security decisions when adopting the cloud requires understanding the technology, process, and people related to the cloud environment. This complements traditional IT management techniques that managers are accustomed to and helps with making the appropriate informed decisions. We will 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
- 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 Training

MG520 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.

“This type of training, i.e., cloud security from a management perspective, is rare and the quality of this one is definitely amazing.”

—Benoit Ramillon, UEFA

“I feel like there was a lot of valuable material and would be very relevant for people creating a cloud security program.”

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

Explore our new Cloud Security Journeys, easy-reference training and certification paths, curated by industry experts and based on common cloud security roles.

Still not sure of your next step?

Connect with our team to develop a training plan that meets your goals.

www.sans.org/job-roles-roadmap/cloud
Frank Kim
SANS Faculty Fellow | @fykim

Frank is the Founder of ThinkSec, a security consulting and CISO advisory firm, as well as a SANS Fellow and lead for both the SANS Cybersecurity Leadership and SANS Cloud Security curricula, overseeing two dozen SANS courses in the two fastest growing curricula. Previously, as CISO at the SANS Institute, Frank led the information risk function for the most trusted source of computer security training and certification in the world. 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 Certified 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 cyber security 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 MGT520.

Serge Borso
SANS Certified Instructor | @SergeBorso

When it comes to cyber security, 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 for the upcoming SEC388, a published author, President of the Denver Open Web Application Security Project (OWASP) chapter, founder and CEO of the cyber security 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.
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 works for Zoom Video Communications, in which he leads their internal Application Security training. As an application developer for most of his professional career, he moved into security full-time largely because of his many formal trainings through SANS. He’s a contributor to the OWASP Serverless Top 10 Project and a co-leader for the Nashville OWASP chapter. 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.