SEC488: **Cloud Security Essentials**

GCLD
Cloud Security Essentials
giac.org/gcld

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

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

Business Takeaways

- Understand the current cloud deployment
- Protect cloud-hosted workloads, services, and virtual machines
- Cost-effectively select appropriate services and configure properly to adequately defend cloud resources
- Get in front of common security misconfigurations BEFORE they are implemented in the cloud
- Ensure business is aligning to industry regulations and laws when operating in the cloud
- Decrease adversary dwell time in compromised cloud deployments

License to Learn Cloud Security

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

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

Hands-On Training

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

GCLD
Cloud Security Essentials
giac.org/gcld

GIAC Cloud Security Essentials

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

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

Section Descriptions

SECTION 1: Identity and Access Management

The first course section will set the stage for the course and then dive straight into all things Identity and Access Management (IAM). Students will learn very quickly that IAM arguably plays the most important role (no pun intended) in protecting the organization's cloud account. In this book, students will be able to:

- Identify security holes in their cloud account's IAM service
- Understand what it takes to implement cloud accounts which follow the concept of least privilege access
- Discover and protect various secrets related to cloud service authentication
- Use cloud vendor-provided IAM analysis tools to automate the discovery of any security shortcomings

TOPICS: Course Overview; Cloud Accounts; Policies and Permissions; Groups and Roles; Temporary Credentials; Secrets Management; Customer Account Management and External Access; More IAM Best Practices

SECTION 2: Compute and Configuration Management

Section 2 will cover ways to protect the compute elements in cloud providers' Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings. Students will determine early on that there is much more complexity when launching instances or virtual machines in the cloud as opposed to on-premise. As the book progresses, students will learn to:

- Securely deploy a compute instance/virtual machine in CSP environments
- Maintain the running instance throughout its lifecycle
- Create hardened images for re-use in the organization
- Understand the various threats that could affect cloud-based applications
- Lock down cloud storage to prevent spillage of sensitive information

TOPICS: Secure Instance/Virtual Machine Deployment: Host Configuration Management: Image Management: Application Security: Threat Modeling: Platform as a Service (PaaS) and Software as a Service (SaaS) Challenges: Container Services: Cloud Storage

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

SECTION 3: Data Protection and Automation

Section 3 will first focus on the protection of data in cloud environments. All too often, we are reading news articles about breaches that, very frequently, come down to a misconfiguration of a cloud service. Students will learn just what to look out for regarding these misconfiguration as well as:

- How to properly identify and classify their organization's data in various cloud services
- Encrypt data where it resides and as it traverses networks
- Ensure the data is available when it is required
- Leverage Infrastructure as Code (IaC) not only to automate operations, but also automate security configurations
- Identify gaps in cloud-based productivity services
- Learn how CASBs operate and what benefit they may add to the organization

TOPICS: Data Classification; Data at Rest Encryption; Availability; Data in Transit Encryption; Lifecycle Management; Infrastructure as Code; Productivity Services; Cloud Access Security Brokers (CASB)

SECTION 4: Networking and Logging

Section 4 is where many network security analysts, engineers, and architects will begin salivating as they will do a deep dive into the ins and outs of cloud networking and log generation, collection, and analysis to set themselves up for success to defend their IaaS workloads. Students will learn to:

- Control cloud data flows via network controls
- Add segmentation between computer resources of varying sensitivity levels
- Generate the proper logs, collect those logs, and process them as a security analyst
- Increase the effectiveness of their security solutions by gaining more network visibility
- Detect treats in real time as they occur in the cloud

TOPICS: Public Cloud Networking; Remote Management of IaaS Systems: Segmentation: Network Protection Services: Cloud Logging Services: Log Collection and Analysis: Network Visibility: Cloud Detection Services

SECTION 5: Compliance, Incident Response, and Penetration Testing

In Section 5, we'll dive headfirst into compliance frameworks, audit reports, privacy, and eDiscovery to equip you with the information and references to ensure that the right questions are being asked during CSP risk assessments. After covering special-use cases for more restricted requirements that may necessitate the AWS GovCloud or Azure's Trusted Computing, we'll delve into penetration testing in the cloud and finish the day with incident response and forensics. Student will learn to:

- Leverage the Cloud Security Alliance Cloud Controls Matrix to select the appropriate security controls for a given cloud network security architecture and assess a CSP's implementation of those controls using audit reports and the CSP's shared responsibility model
- Use logs from cloud services and virtual machines hosted in the cloud to detect a security incident and take appropriate steps as a first responder according to a recommended incident response methodology
- Perform a preliminary forensic file system analysis of a compromised virtual machine to identify indicators of compromise and create a file system timeline

TOPICS: Security Assurance; Cloud Auditing; Privacy; Government Clouds; Risk Management; Penetration Testing; Legal and Contractual Requirements; Incident Response and Forensics

SECTION 6: CloudWars

This final section consists of an all-day, CloudWars competition to reinforce the topics covered in Sections 1–5. Through this friendly competition, students will answer several challenges made up of multiple choice, fill-in-the-blank, as well as hands-on and validated exercises performed in two CSP environments. They will be given a brand-new environment to deploy in two different cloud vendors and will be tasked to take this very broken environment and make the appropriate changes to increase its overall security posture.

"Great way to bring participants up to speed in the cloud security principles. I am a novice to the area and the course was at the right level for me to come up to speed. Thank you for this course, it answers many questions I had about the cloud. Nice to walk through this course prior to leaping into cloud adoption at our organization."

—Natalija Saviceva, **FI**