SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC488: **Cloud Security Essentials**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- 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
- Create accounts and use the services of any one the leading CSPs and be comfortable with the self-service nature of the public cloud, including finding documentation, tutorials, pricing, and security features
- Articulate the business and security implications of a multicloud strategy
- Secure access to the consoles used to access the CSP environments
- Use command line interfaces to query assets and identities in the cloud environment
- Use hardening benchmarks, patching, and configuration management to achieve and maintain an engineered state of security for the cloud environment
- Evaluate the logging services of various CSPs and use those logs to provide the necessary accountability for events that occur in the cloud environment
- Configure the command line interface (CLI) and properly protect the access keys to minimize the risk of compromised credentials
- Use basic Bash and Python scripts to automate tasks in the cloud
- Implement network security controls that are native to both AWS and Azure
- Employ an architectural pattern to automatically create and provision patched and hardened virtual machine images to multiple AWS accounts
- Use Azure Security Center to audit the configuration in an Azure deployment and identify security issues
- Use Terraform to deploy a complete "infrastructure as code" environment to multiple cloud providers
- 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
- Follow the penetration testing guidelines put forth by AWS and Azure to invoke your "inner red teamer" to compromise a full stack cloud application
- 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

Learning the Language of Cloud Security

More businesses than ever are moving sensitive data and shifting mission-critical workloads to the cloud - and not just to one cloud service provider (CSP). Research shows that most enterprises have strategically decided to deploy a multicloud platform, including Amazon Web Services, Azure, Google Cloud, and others.

Organizations are responsible for securing their data and mission-critical applications in the cloud. The benefits in terms of cost and speed of leveraging a multicloud platform to develop and accelerate delivery of business applications and analyze customer data can quickly be reversed if security professionals are not properly trained to secure the organization's cloud environment and investigate and respond to the inevitable security breaches.

The SANS SEC488: Cloud Security Essentials course will prepare you to advise and speak about a wide range of topics and help your organization successfully navigate both the security challenges and opportunities presented by cloud services. Like foreign languages, cloud environments have similarities and differences, and SEC488 covers all of the major CSPs and thus all of the languages of cloud services.

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), and Software as a Service (SaaS).

New technologies introduce new risks. This course will equip you to implement appropriate security controls in the cloud, often using automation to "inspect what you expect." Mature CSPs have created a variety of security services that can help customers use their products in a more secure manner, but nothing is a magic bullet. This course covers real-world lessons using security services created by the CSPs as well as open-source tools. As mentioned, each course book 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.

You Will Be Able To

"More businesses than ever are shifting mission-critical workloads to the cloud. And not just one cloud – research shows that most enterprises are using up to five different cloud providers. Yet, cloud security breaches happen all the time and many security professionals feel ill-prepared to deal with this rampant change. SEC488 equips students to view the cloud through a lens informed by standards and best practices to rapidly identify security gaps. It provides class participants with hands-on tools, techniques, and patterns to shore up their organization's cloud security weaknesses."

sans.org/sec488

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

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:

TOPICS: 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

Who Should Attend

- 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:

- Lean how to control cloud data flows via network controls
- Add segmentation between compute 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: Private Cloud Networking; Public Cloud Networking; Network 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.