# SEC488: **Cloud Security Essentials**

5 Day Program | 30 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 on any one the leading CSPs and be comfortable with the self-service nature of the public cloud. This includes finding documentation, tutorials, pricing, and security features.
- Articulate the business and security implications of a multi-cloud 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.
- Implement, configure, and secure certificate-based SSH authentication to virtual machines launched in the cloud.
- Configure the 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.
- Configure cross-account role assumption, a best practice for AWS.
- 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.
- 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.

More businesses than ever are moving sensitive data and shifting mission-critical workloads to the cloud. And not just one cloud service provider (CSP) - research shows that most enterprises have strategically decided to deploy a multi-cloud 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 multi-cloud platform to develop and accelerate delivery of business applications and analyze customer data can quickly be reversed if security professionals aren't 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 as well as the opportunities presented by cloud services. Like foreign languages, cloud environments have similarities and differences, and SEC488 covers all of the major CSPs.

We will begin by showing how your day-to-day operations will change due to the evolution of Cloud. Expect changes from the different responsibility models to the different CSP models of Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service. From there we'll move on to securing the cloud, managing risk, and addressing the challenges you may experience as you look to achieve a specific level of security assurance.

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 and open-source tools. Each course day features hands-on lab exercises to help students hammer home the lessons learned. We progressively layer multiple security controls in order to end the week with a functional security architecture implemented in the cloud.

## Available Training Formats

### Live Training

**Live Events**
sans.org/information-security-training/by-location/all

**Summit Events**
sans.org/cyber-security-summit

# Section Descriptions

### SECTION 1: Welcome to the Cloud

The first course section will set the stage for how day-to-day operations could change as an enterprise looks at cloud technologies. Different service and delivery models will influence how a business changes based on the model that is being leveraged. In addition to learning about important cloud fundamentals, students will be able to:

- Identify the risks and risk control ownership based on the deployment and service delivery models of the various products offered by cloud service providers (CSPs).
- Evaluate the trustworthiness of cloud service providers 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 of the leading CSPs and be comfortable with the self-service nature of the public cloud. This includes finding documentation, tutorials, pricing, and security features.
- Articulate the business and security implications of a multi-cloud strategy.

**TOPICS:** What This Course Is Not; What Is the Cloud?; The Global Cloud Ecosystem; Pros and Cons of the Public Cloud

### SECTION 2: Securing the Cloud Environment and Infrastructure Security

Section 2 will cover ways you can access your cloud environments through new management interfaces, as well as programmatic access with APIs, access keys, and SDKs. We'll cover industry best practices for hardening the environments and securing workloads in different service providers and deployment models. We will finish the section by covering the different log sources you can pull from your environment to provide visibility, as well as the tools that can automatically review your accounts for compliance with best practices and industry benchmarks.

**TOPICS:** How Does Security Change in the cloud?; Interacting with CSPs; Infrastructure-as-a-Code; Serverless

### Who Should Attend

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

### SECTION 3: Application Security and Securing Services

This course section will build on our review of how developers can leverage the cloud's flexibility. After starting with a discussion of secrets management, we dive into Application Security, and apply cloud technologies, design patterns, and best practices to our cloud applications. Understanding and applying the basics of securing cloud applications will put you ahead of many residents of the cloud. Students will learn to:

- Implement, configure, and secure certificate-based SSH authentication to virtual machines launched in the cloud.
- Configure the 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.
- Learn to prevent secrets leakage in code deployed to the cloud.
- Use application security tools to threat model and assess the security of cloud-based web applications.

**TOPICS:** Application Security; Threat Modeling

### SECTION 4: Cloud OPs and Architecture

In section 4, we look at the components of cloud security architecture, including architecture frameworks and cloud network design principles and component technologies. We cover native cloud security services and their importance in a well-designed security architecture as well as important operational practices such as hardening and patching – using cloud automation, of course. Next, we leverage the flexibility of cloud services using capabilities that enable "infrastructure-as-code" for rapid deployments, including serverless technologies. After section 4, students will be able to:

- 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.

**TOPICS:** Architecture Considerations; Segmentation and Isolation

### SECTION 5: Legal/Compliance, Penetration Testing & Incident Response

In the fifth section, we dive headfirst into compliance frameworks, audit reports, privacy, and eDiscovery to equip you with the questions and references that ensure 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 delve into penetration testing in the cloud and finish the day with incident response and forensics. Section 5 will equip students 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; Privacy; Risk Management; Legal and Contractual Requirements