SEC388: **Introduction to Cloud Computing and Security**

3 Day Program	18 CPEs	Laptop 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

"Serge is the best instructor I've ever had! He's so knowledgeable and has a great teaching style. Very relatable and helps when people have questions."

—Seth J., SEC542 student

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

Section Descriptions

SECTION 1: Account Set Up and Cloud Computing

The course starts with an introduction to both AWS and Azure by answering fundamental questions about the cloud: what it is, how it works, why its relevant, all while explaining pertinent vocabulary. The course continues by introducing common cloud services and highlighting how to interact with our cloud environments using both a web browser and the command line. With this foundation, the focus shifts to security concerns and detailing common mistakes which can lead to a breach. The section ends on the topic of budgeting and understanding how costs are calculated in a cloud computing environment.

TOPICS: Introduction to Cloud Computing; Cloud Service Providers; Cloud Interfaces; Cost Calculation

SECTION 3: Threats and Solutions

Section 3 focuses on identifying threats facing cloud environments, and understanding solutions to deal with those threats. After suffering a simulated breach of our cloud environment, we learn hands-on exactly how to respond to the situation and research the root cause. With first-hand experience dealing with cloud service deployment, and the inherent risks of exposing our infrastructure, we work to understand how to harden our environment against attacks. Finally, we look at automated, cloud-native security solutions, and discuss common attacks and defenses we can then speak to with a close look at best practices.

TOPICS: Incident Response; Hardening; Cloud Native Security Solutions; Cloud Attacks and Defenses

SECTION 2: Compute, Storage, and Networking

Section 2 delves into service integration and deployment. We start they day by understanding common cloud-based services and the role they play in supporting the business. We then begin deploying services to both AWS and Azure, as well as configuring security controls to allow and restrict access into our environment. The exposure to new services continues with the implementation of cloud storage, in conjunction with cloud computing. Within the context of enabling common business functions, we integrate a functional website in each cloud service provider's environment. Finally, within these newly deployed services, we work to understand the risk these actions inherently introduce, and work to limit that risk by implementing security monitoring and alerting controls.

TOPICS: Compute Services; Cloud Storage; Business Needs; Logging & Monitoring

Who Should Attend

- Professionals seeking a career change from a different industry into cloud
- People with no formal computer science background looking to start a career in the cloud
- Professionals looking to move laterally into cloud
- Students wanting to start a career in cloud
- Managers that oversee cloud services
- Analysts working in the cloud
- Engineers responsible for cloud services
- Executive leadership that need or want to understand technical components of the cloud

NICE Framework Work Roles

- Cyber Defense Analyst PR-CDA-001
- Cyber Operator CO-OPS-001
- Executive Cyber Leadership OV-EXL-001
- System Administrator OM-ADM-001
- Threat/Warning Analyst AN-TWA-001