

SEC480: AWS Secure Builder

2 Day Program 12 CPEs Laptop Required

You Will Be Able To

- Implement industry-standard security best practices in AWS workloads
- Master AWS Identity and Access Management (IAM) including roles, policies, and permissions for secure access control
- Evaluate and assess AWS services based on security documentation, controls, and audit risks
- Monitor and respond to security incidents using AWS security tools for detection, response, and mitigation
- Automate security processes with AWS services like AWS Lambda and AWS GuardDuty
- Identify security deficiencies in Continuous Integration Continuous Delivery (CICD) pipelines and detect gaps in current cloud security practices
- Secure data in transit and at rest using encryption and other protective measures
- Conduct comprehensive security audits and assessments to ensure compliance and risk identification
- Ensure AWS deployments meet industry standards and regulatory requirements
- Develop and implement incident response plans tailored to AWS environments
- Continuously optimize your security posture with regular reviews and updates

Business Takeaways

- Facilitate scalable security solutions across your organization
- Increase customer trust and satisfaction
- Strengthen organizational security posture
- Boost employee confidence and skillset in secure AWS development
- Improve compliance with cloud security standards
- Enhance business agility through secure cloud practices
- Reduce the workload and stress on your security team

Why SEC480?

Data breaches of cloud infrastructure can often be traced back to inadvertent misconfigurations made by non-security personnel. Cloud developers, engineers, architects, and other security-adjacent roles require platform-specific training to effectively prioritize security and reduce the likelihood of harmful breaches. SEC480: AWS Secure Builder fulfills this requirement by equipping technical professionals with the skills needed to embed security fundamentals into Amazon Web Services (AWS) workloads from the start. This course features eight comprehensive modules, each accompanied by a hands-on lab, ensuring participants gain practical experience in building secure AWS environments.

Build In Security From The Start

SEC480: AWS Secure Builder addresses eight critical risk areas, providing students with the skills and knowledge to enable enterprises to securely move workloads to AWS. By completing this course, participants will be well-equipped to implement and enhance security controls, leading to immediate improvements in security and business enablement. With this training, organizations can be confident in their teams' ability to adopt, build, and deploy in the cloud without overburdening security teams.

This training is designed to scale across enterprise engineering and development teams, making a swift and significant impact on the security of AWS workloads.

Hands-On Training

The SEC480 lab environment immerses students in practical, real-world AWS scenarios, allowing them to apply the theory and skills learned throughout the course. Each student will receive a SANS-provisioned AWS account and a detailed lab workbook, ensuring consistent, repeatable, and relevant hands-on experience.

This dynamic lab environment includes essential cloud resources such as IAM privileges, virtual machines, security tools, and AWS services pre-installed and configured to simulate real-world scenarios. This setup allows students to focus on the most important parts of the lab, without worrying about setting up a complex environment. Each of the eight labs focuses on different aspects of AWS security, runs approximately 15 minutes each, and is designed to be clear, insightful, and easy to follow.

Author Statement

"I think everyone can agree on the importance of safeguarding assets in today's world of sustained threats and immeasurable technical complexity, especially in the realm of AWS. How we do that, and why specific actions are performed, however, is not common knowledge; which is why SEC480 exists - to fill that knowledge gap.

In this course, we'll delve into the intricacies of identity management, encryption, access controls, and secure coding. My goal is to teach you how to fortify applications, secure data, harden infrastructure, comply with GRC programs and work to ensure resilience against threats: All while accounting for the fact that we are not completely in control of our success. As we navigate the AWS ecosystem, we'll embrace the shared responsibility model, and lean into the fact that security is not an afterthought, but instead an integral part of every deployment.

With that said, let us explore the AWS cloud, understand cloud-native security solutions, and arm ourselves with the knowledge needed to implement best-in-class security controls."

—Serge Borso

Section Descriptions

SECTION 1: Secure Development and Deployment Practices in AWS

In Section 1 of Secure AWS Development, we'll concentrate on the shared responsibility model, hardening workloads, securing the CICD pipeline, and understanding the critical role of IAM in AWS.

Module 1: Responsibility To, For, and Of Security

Understand the shared responsibility model, the difference between cloud and on-premesis security, AWS security architecture, compliance requirements, and how to apply effective security controls.

TOPICS: Cloud Security and Shared Responsibility Model; Security and Compliance; AppSec in the Cloud

Module 2: Identification and Authorization

Implement best practices for IAM, explore workforce identity management, address common authentication failures, and apply secure access controls.

TOPICS: IAM in the Cloud; Workforce Identity; Identification and Authorization Failures

Module 3: Continuous Integration Continuous Delivery (CICD)

Master CICD pipelines, automate code deployment with AWS Code Pipeline, integrate security tools, and prevent misconfigurations through hands-on labs and real-world demos.

TOPICS: CICD Explained; Build Process; CICD Security

Module 4: Workload and Service Hardening

Harden AWS workloads and services like API Gateway, S3, EC2, and RDS, address misconfigurations, and ensure compliance through practical labs and real-world examples.

TOPICS: Common Services; AWS Workloads; Complexity Breeds Insecurity

SECTION 2: Securing AWS: Monitoring, Incident Response, and Trust

In Section 2 of Secure AWS Development, we turn our attention to understanding what happens when there are misconfigurations in our environment and how to deal with adversaries. In addition, we'll delve into what proper logging and monitoring entail, how to leverage an incident response plan, and strategies to minimize supply chain risks.

Module 5: Security Monitoring

Implement comprehensive security monitoring with logging at all levels, utilize monitoring tools, enhance alerting with artificial intelligence (AI), and set up early warning systems.

TOPICS: Logging; Monitoring; Alerting

Module 6: Exposure and Attack Vectors

Identify and mitigate exposure and attack vectors through open-source intelligence (OSINT), understand the anatomy of attacks, and minimize attack surfaces using threat modeling and compliance tools.

TOPICS: OSINT; Anatomy of an Attack; Minimizing Attack Surface

Module 7: Incident Response

Master the six-step incident response process, implement best practices with roles, playbooks, and technology, and prepare with tools and exercises.

TOPICS: Six-Step Incident Response Process; Incident Response Best Practices; Proper Preparation

Module 8: Trust, Control, and the Supply Chain

Evaluate vendor reliance and onboarding processes, implement Zero Trust principles, and defend against supply chain attacks to ensure secure vendor interactions and compliance.

TOPICS: Reliance on Vendors; Vendor Onboarding and Risk Evaluation; Zero Trust; Supply Chain Attacks

Who Should Attend

- · Cloud application developers
- · Cloud engineering leaders
- Cloud engineers
- · Cloud architects
- · Cloud administrators
- Anyone technical that will be building in, operating in, configuring and/or managing AWS Cloud environments

"Top notch! Serge makes his course work very interesting and engaging."

-Prasanth Chatti, KPMG

