SEC540: **Cloud Security and DevSecOps Automation**

GCSA
Cloud Security Automation
giac.org/gcsa

5 Day Program	38 CPEs	Laptop Required

You Will Be Able To

- Understand how DevOps works and identify keys to success
- Wire security scanning into automated CI/CD pipelines and workflows
- Build continuous monitoring feedback loops from production to engineering
- Automate configuration management using Infrastructure as Code (IaC)
- Secure container technologies (such as Docker and Kubernetes)
- Use native cloud security services and third-party tools to secure systems and applications
- Securely manage secrets for Continuous Integration servers and applications
- Integrate cloud logging and metrics
- Perform continuous compliance and security policy scanning

Authors' Statement

"DevOps and the cloud are radically changing the way that organizations design, build, deploy, and operate online systems. Leaders like Amazon, Etsy, and Netflix are able to deploy hundreds or even thousands of changes every day, continuously learning, improving, and growing - and leaving - their competitors far behind. Now DevOps and the cloud are making their way from Internet 'Unicorns' and cloud providers into enterprises.

"Traditional approaches to security can't come close to keeping up with this rate of accelerated change. Engineering and operations teams that have broken down the "walls of confusion " in their organizations are increasingly leveraging new kinds of automation, including Infrastructure as Code, Continuous Delivery and Continuous Deployment, microservices, containers, and cloud service platforms. The question is: Can security take advantage of the tools and automation to better secure its systems?

"Security must be reinvented in a DevOps and cloud world."

— Ben Allen, Jim Bird, Eric Johnson,
and Frank Kim

The Cloud Moves Fast. Automate to Keep Up.

Common security challenges for organizations struggling with the DevOps culture include issues such as:

- Upfront peer code reviews and security approvals may not occur for change approval and audit requirements
- Missing infrastructure and application scanning can allow attackers to find an entry point and compromise the system
- Cloud security misconfigurations may publicly expose sensitive data or introduce new data exfiltration paths

Security teams can help organizations prevent these issues such as using DevOps tooling and cloud-first best practices. This course provides development, operations, and security professionals with a deep understanding of and hands-on experience with the DevOps methodology used to build and deliver cloud infrastructure and software. Students learn how to attack and then harden the entire DevOps workflow, from version control to continuous integration and running cloud workloads. Each step of the way, students explore the security controls, configuration, and tools required to improve the reliability, integrity, and security of on-premise and cloud-hosted systems. Students learn how to implement more than 20 DevSecOps security controls to build, test, deploy, and monitor cloud infrastructure and services.

Business Takeaways

- Build a security team that understands modern cloud security and DevSecOps practices
- Partner with DevOps and engineering teams to inject security into automated pipelines
- Leverage cloud services and automation to improve security capabilities
- Ensure your organization is ready for cloud migration and digital transformation initiatives

Hands-On Training

SEC540 goes well beyond traditional lectures and immerses students in hands-on application of techniques during each section of the course. Each lab includes a step-by-step guide to learning and applying hands-on techniques, as well as a "no hints" approach for students who want to stretch their skills and see how far they can get without following the guide. This allows students, regardless of background, to choose the level of difficulty they feel is best suited for them -always with a frustration-free fallback path. Immersive hand-on labs ensure that students not only understand theory, but how to configure and implement each security control.

The SEC540 lab environment simulates a real-world DevOps environment, with more than 10 automated pipelines responsible for building DevOps container images, cloud infrastructure, automating gold image creation, orchestrating containerized workloads, executing security scanning, and enforcing compliance standards. Students are challenged to sharpen their technical skills and automate more than 20 security-focused challenges using a variety of command line tools, programming languages, and markup templates.

The SEC540 course labs come in both AWS and Azure versions. Students will choose one cloud provider at the beginning of class to use for the duration of the course. Students are welcome to do labs for both cloud providers on their own time once they finish the first set of labs.

For advanced students, 2 hours of CloudWars Bonus Challenges are available during extended hours each day. These CloudWars challenges provide additional opportunities for hands-on experience with the cloud and DevOps toolchain.

Section Descriptions

SECTION 1: DevOps Security Automation

SEC540 starts by introducing DevOps practices, principles, and tools by attacking a vulnerable Version Control and Continuous Integration System configuration. Students gain an in-depth understanding of how the toolchain works, the risks these systems pose, and identify key weaknesses that could compromise the workflow. Next, we'll examine the security features available in various Continuous Integration (CI) and Continuous Delivery (CD) systems, such as Jenkins, GitHub, GitLab, Azure DevOps, and AWS CodePipeline, and then start hardening the environment. After automating various code analysis tools and discovering insecurely stored secrets, students will focus on storing sensitive data in secrets management solutions such as HashiCorp Vault, AWS Secrets Manager, and Azure Key Vault.

TOPICS: DevOps and Security Challenges; DevOps Toolchain; Securing DevOps Workflows; Pre-Commit Security Controls; Commit Security Controls; Secrets Management

SECTION 3: Cloud Security Operations

Section 3 prepares students to deploy and run containerized workloads in cloud-native orchestration services such as AWS Elastic Container Service (ECS) and Azure Kubernetes Service (AKS). Students analyze the cloud resources, identify common security misconfigurations, and leverage automation to quickly secure the workloads. The focus then shifts to monitoring workloads, analyzing log files, detecting an attack in real time, and sending alerts to the security team. Students finish the section by examining cloud-native data protection capabilities and encrypting sensitive data.

TOPICS: Cloud Deployment & Orchestration; Cloud Workload Security; Security in Cloud CI/CD; Continuous Security Monitoring; Data Protection Services

SECTION 5: Compliance as Code

Section 5 wraps up the journey with students learning to leverage cloud services to automate security compliance. Starting with Cloud Security Posture Management (CSPM) solutions students detect security issues in their cloud infrastructure. Next, using cloud-native Web Application Firewall (WAF) services, students enable monitoring, attack detection, and active defense capabilities to catch and block bad actors. The discussion then shifts to working in DevOps and how that affects policy and compliance. Students finish the course learning how to write policy as code for automated remediation using Cloud Custodian, and how to detect and correct cloud configuration drift.

TOPICS: Continuous Compliance; Runtime Security Protection; Automated Remediation

SECTION 2: Cloud Infrastructure Security

Section 2 challenges students to use their DevOps skills to deploy a code-driven cloud infrastructure with AWS CloudFormation and Terraform using more than 150 cloud resources. Students perform a cloud network assessment, identify insecure network configurations, and harden the network traffic flow rules. Moving to cloud virtual machines, students learn how to automate configuration management and build gold images using Ansible, Vagrant, and Packer. To finish the day, students focus on scanning and hardening container images before deploying workloads to the cloud.

TOPICS: Cloud Infrastructure as Code; Configuration Management as Code; Container Security; Acceptance Stage Security

SECTION 4: Cloud Security as a Service

Section 4 starts with students learning to leverage cloud-native services to patch containerized workloads and secure content delivery networks. From there, the discussion shifts to microservice architectures, best practices, and micro-segmentation with API Gateways. Finally, students learn how to build and deploy Functions as a Service (FaaS), such as Lambda and Azure Functions, along with resources to add guardrails to the microservice environment.

TOPICS: Blue/Green Deployment Options; Secure Content Delivery; Microservice Security; Serverless Security

> **"BEST class I have ever taken at SANS. This is one of those courses where I can log into work after class ends and immediately start applying into my daily tasks and responsibilities. I already went on my team's Slack channel and told them this needs to be the next class they take."**
>
> —Brian Esperanza, **Teradata**

Who Should Attend

- Anyone working in or transitioning to a public cloud environment
- Anyone working in or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to cloud and DevOps Continuous Delivery pipelines
- Anyone interested in learning how to migrate DevOps workloads to the cloud, specifically Amazon Web Services (AWS) and Microsoft Azure
- Anyone interested in leveraging cloud application security services provided by AWS or Azure
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

GCSA
Cloud Security Automation
giac.org/gcsa

GIAC Cloud Security Automation

"The GIAC Cloud Security Automation (GCSA) certification covers cloud services and modern DevSecOps practices that are used to build and deploy systems and applications more securely. The certification shows that you not only know how to speak the language of modern cloud and DevSecOps principles but can put them into practice in an automated and repeatable manner."
— Frank Kim, SEC540 Course Co-Author

- Using cloud services with DevSecOps principles, practices, and tools to build and deliver secure infrastructure and software
- Automating Configuration Management, Continuous Integration, Continuous Delivery, and Continuous Monitoring
- Use of open-source tools, the Amazon Web Services toolchain, and Azure services