SEC540: **Cloud Security and DevSecOps Automation**

GCSA
Cloud Security Automation
giac.org/gcsa

5	38	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Understand the Core Principles and Patterns behind DevOps
- Map and Implement a Continuous Delivery/Continuous Deployment Pipeline
- Understand the DevSecOps Methodology and Workflow
- Integrate Security into Production Operations
- Move Your DevOps Workloads to the Cloud
- Consume Cloud Services to Secure Cloud Applications

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.

Organizations are moving to the cloud to enable digital transformation and reap the benefits of cloud computing. However, security teams struggle to understand the DevOps toolchain and how to introduce security controls in their automated pipelines responsible for delivering changes to cloud-based systems. Without effective pipeline security controls, security teams lose visibility into the changes released into production environments. 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 using DevOps tooling and cloud-first best practices. SEC540 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.

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-aalways with a frustration-free fallback path.

SEC540 also offers students an opportunity to participate in CloudWars Bonus Challenges each day, providing more hands-on experience with the cloud and DevSecOps toolchain.

SEC540 will prepare you to:

- Understand the Core Principles and Patterns behind DevOps
- Understand the DevSecOps Methodology and Workflow
- Integrate Security into Production Operations
- Move Your DevOps Workloads to the Cloud
- Consume Cloud Services to Secure Cloud Applications

"Mind-blowing! If you are a traditional security architect, tip-toeing around DevOps, get into SEC540. It takes you into the depths of DevSecOps and sets you up for the future!"

— Jatin Sachdeva, **Cisco**

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 ToolchainSecurity in Acceptance; Securing DevOps Workflows; Pre-Commit Security Controls; Commit Security Controls; Secrets Management

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 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 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, along with resources to add guardrails to the microservice environment.

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

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-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 cloud compliance and monitoring scanners, such as CloudMapper and Cloud Custodian, and how to detect and correct cloud configuration drift.

TOPICS: Runtime Security Automation; Continuous Auditing; Cloud Security Monitoring

> **“SEC540 opened my eyes to a new way of thinking about operations and security unlike anything since SEC401: Security Essentials Bootcamp Style.”**
>
> — Todd Anderson, **OBE**

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 to migrate DevOps workloads to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in leveraging cloud application security services provided by AWS
- 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 Secure DevOps principles, practices, and tools to build & 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