SEC540: **Cloud Security and DevOps Automation**

GCSA
Cloud Security Automation
giac.org/gcsa

5 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Build a Secure DevOps workflow in your organization
- Create automated security tasks in Continuous Integration/Continuous Delivery (CI/CD) systems
- Configure and run scanners from the Secure DevOps Toolchain
- Perform cloud infrastructure security audits for common misconfiguration vulnerabilities
- Perform secure secrets management using on-premise and cloud-hosted secrets management tools
- Audit microservice architectures for security vulnerabilities in containers, serverless, and API gateway appliances
- Leverage cloud automation to automate patching and software deployments without downtime
- Build serverless functions to monitor, detect and actively defend cloud services and configurations

"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**

The cloud moves fast. Automate to keep up.

SEC540 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how DevOps principles, practices, and tools can improve the reliability, integrity, and security of on-premise and cloud-hosted applications.

SEC540 examines the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular tools such as Jenkins, GitLab, Puppet, Vault, and Grafana to automate Configuration Management ("Infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), cloud infrastructure, containerization, micro-segmentation, Functions as a Service (FaaS), Compliance as Code, and Continuous Monitoring.

The lab environment starts with an on-premise CI/CD pipeline that automatically builds, tests, and deploys infrastructure and containerized applications. Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques. After laying the DevSecOps foundation, students put their DevSecOps skills to work by deploying and managing a real-world cloud infrastructure. Hands-on exercises deploy containerized workloads in the cloud, integrate on-premise configuration management with Puppet, and manage secrets with HashiCorp Vault and Cloud Key Management Service (KMS). Students analyze and fix cloud infrastructure vulnerabilities, perform cloud-hosted application vulnerability scanning, and defend microservices using tools such as API Gateway and FaaS. Cloud security compliance tools help monitor the infrastructure using code-driven Web Application Firewall (WAF) services, continuous auditing with CloudMapper, and continuous monitoring with Cloud Custodian.

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 a level of difficulty they feel is best suited for them - always with a frustration-free fallback path.

Course 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

Section Descriptions

SECTION 1: Introduction to DevSecOps

SEC540 starts by introducing DevOps practices, principles, and tools. We will examine how DevOps works, how work is done in DevOps, and the importance of culture, collaboration, and automation. Using case studies of DevOps "Unicorns" – the Internet tech leaders who have created the DevOps DNA – we'll consider how and why these leaders succeeded and examine the keys to their DevOps security programs. We'll then look at Continuous Delivery, which is the DevOps automation engine. We'll explore how to build up a Continuous Delivery or Continuous Deployment pipeline, including how to fold or wire the DevSecOps security controls into the Continuous Delivery pipeline, and how to automate security checks and tests in Continuous Delivery.

TOPICS: Introduction to the Cloud and DevOps; Case Studies on DevOps Unicorns; Security Challenges in DevOps; DevOps Deployment Kata; Secure Continuous Delivery; Security in Pre-Commit; Security in Commit; Security in Acceptance

SECTION 2: Cloud Infrastructure and Orchestration

Building on the ideas and frameworks developed in section 1, we'll examine how Cloud Infrastructure as Code can quickly and consistently deploy new infrastructure and services. Using modern automated configuration management tools like Puppet, Chef, and Ansible, we'll also cover how to enforce desired state configuration for cloud-hosted virtual machines. Since workloads are moving into container services, we'll explore the container security issues associated with tools such as Docker and Kubernetes.

TOPICS: Cloud Security Fundamentals; Secure Infrastructure as Code; Configuration Management as Code; Container Security Hardening

SECTION 3: Cloud Security Operations

Students start the day reviewing container orchestration options and scanning and testing their cloud infrastructure code for common cloud misconfiguration vulnerabilities. Correcting and committing infrastructure code changes will trigger an automated infrastructure pipeline to harden the cloud infrastructure code. Next, we will explore cloud continuous integration and delivery tools and leverage serverless computing to perform static analysis and software supply chain vulnerability scans before releasing containers into the orchestration services. We then shift focus to production and operations by building continuous security monitoring using Grafana, CloudWatch, and Slack. Section 3 wraps up with cloud data protection, exploring the various encryption services, how to implement secrets management in the cloud, and how to integrate on-premise secrets with cloud resources.

TOPICS: Securing Cloud Architecture; Security Scanning in CI/CD; Continuous Security Monitoring; Data Protection and Secrets Management

SECTION 4: Cloud Security as a Service

In this section we'll leverage cloud security services to lock down functional and high-availability systems. Students start by deploying a security patch to an application using blue/green environments to minimize downtime. Shifting focus, we move on to protecting static website content served by a Content Delivery Network (CDN) using private key signing. The second half of the day explores the world of microservices, protecting APIs with an API Gateway, and deploying serverless functions to manage authorization, data entitlements, and access control.

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

SECTION 5: Cloud Security Automation

Expanding on the foundation from previous sections, DevSecOps practitioners now shift to leveraging cloud services to automate security compliance. We start by deploying and configuring a cloud web application firewall with monitoring, attack detection, and active defense capabilities to catch and block bad actors. Next, we implement continuous compliance scanning for cloud misconfigurations. Finally, we work on enforcing policy as code 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