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

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 the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premise and cloud-hosted applications.

Starting with on-premise deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management ("infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and 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, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software. SEC540 provides in-depth analysis of the Amazon Web Services (AWS) toolchain, while lightly covering comparable services in Microsoft Azure. Using the CI/CD toolchain, students build a cloud infrastructure that can host containerized applications and microservices. Hands-on exercises analyze and fix cloud infrastructure and application vulnerabilities using security services and tools such as API Gateway, Identity and Access Management (IAM), CloudFront Signing, Security Token Service (STS), Key Management Service (KMS), managed WAF services, serverless functions, CloudFormation, AWS Security Benchmark, and much more.

"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**

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Introduction to Secure DevOps

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 DevOps; Case Studies on DevOps Unicorns; Working in DevOps; Security Challenges in DevOps; Building a CD Pipeline; DevOps Deployment Data;Secure Continuous Delivery; Security in Pre-Commit; Security in Commit; Security in Acceptance

SECTION 2: Moving to Production

Building on the ideas and frameworks developed in section 1 of the course, and using modern automated configuration management tools like Puppet, Chef, and Ansible, you'll learn how secure Infrastructure as Code allows you to quickly and consistently deploy new infrastructure and manage configurations. Because the automated CD pipeline is so critically important to DevOps, you'll also learn to secure the pipeline using a variety of defensive approaches. As the infrastructure and application code moves to production, we'll spend the second half of the day exploring container security issues associated with tools such as Docker and Kubernetes, as well as how to protect secrets using Vault and how to build continuous security monitoring using Grafana, Graphite, and StatsD. Finally, we'll discuss how to build compliance into Continuous Delivery, using the security controls and guardrails that have been built in the DevOps toolchain.

TOPICS: Secure Configuration Management Using Infrastructure as Code; Securing Configuration Management and Continuous Integration/Continuous Delivery Pipelines; Container Security, Hardening, and Orchestration; Continuous Monitoring and Feedback Loops; Secure Secrets Management; Automating Compliance as Code

SECTION 3: Moving to the Cloud

Observing DevOps principles, you'll learn to deploy infrastructure, applications, and the CI/CD toolchain into the cloud. This section starts with an overview of Amazon Web Services (AWS) and introduces the foundational tools and practices you'll need to deploy an automated infrastructure pipeline to the AWS cloud. Students spend the second half of the section 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. Finally, students 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.

TOPICS: Introduction to the Cloud; Cloud Architecture Overview; Secure Cloud Deployment; Security Scanning in CI/CD

SECTION 4: Cloud Application Security

In this section, you'll learn to leverage cloud application security services to ensure that applications have appropriate encryption, authentication, authorization, and access control, while also maintaining functional and high-availability systems. Starting with cloud data protection, we will explore the various encryption services and how to implement secrets management in the cloud. Leveraging that knowledge, students will learn to protect static website content served by a Content Delivery Network (CDN) using private key signing. The second half of the section explores the world of microservices, protecting APIs with an API Gateway, and deploying serverless functions to manage authorization, data entitlements, and access control.

TOPICS: Data Protection; Secure Content Delivery; Microservice Security; Serverless Security

SECTION 5: Cloud Security Automation

Expanding on the foundation of the previous sections, DevSecOps practitioners shift their focus in this course section to leveraging cloud services to automate security tasks. Students start by deploying a security path to an application using blue/green environments to minimize downtime. Next, we review deploying and configuring a cloud web application firewall with monitoring, attack detection, and active defense capabilities to catch and block bad actors. Taking this concept to the next level, students finish off the course by building custom monitoring, detection, and enforcement of cloud compliance policies and hardening guidelines.

TOPICS: Blue/Green Deployment Options; Security Automation; Security Monitoring and Compliance

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

Course Preview
available at: **sans.org/demo**