SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC534: **Secure DevOps: A Practical Introduction**

2 Day Course	12 CPEs	Laptop Required

SEC534: Secure DevOps: A Practical Introduction explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. You will learn DevOps principles, practices, and tools and how they can be leveraged to improve the reliability, integrity, and security of systems.

Using lessons from successful DevOps security programs, this course will explain how Secure DevOps can be implemented. 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.

You Will Be Able To

- Understand the core principles and patterns behind DevOps, how work is done in DevOps, and what the keys to success in DevOps are
- Map out and implement a Continuous Delivery/Deployment pipeline
- Map out where security controls and checks can be added in Continuous Delivery and Continuous Deployment
- Integrate security into production operations
- Create a plan for introducing or improving security in a DevOps environment
- How to use DevOps to secure DevOps

Who Should Attend

- Developers, software architects, operations engineers, and system admins working in a DevOps environment, or transitioning to a DevOps environment, who want to understand how and where to add security checks, testing, and other controls.
- Security analysts, security engineers, auditors and risk managers, security consultants, and pen testers who want to understand how to adapt security practices to DevOps and Continuous Delivery.

> **"The material/contents of this class are excellent. They help me learn all the tools that are relevant to work."**
>
> — Hoan Le, **Ring Central**

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

Section Descriptions

SECTION 1: Introduction to Secure DevOps

SEC534 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've 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 Continuous Delivery pipeline is so critically important to DevOps, you'll also learn to secure the pipeline, including RASP and other run-time defense technologies. 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 will explain how to build compliance into Continuous Delivery, using the security controls and gates that we've already built in.

TOPICS: Secure Configuration Management Using Infrastructure as Code; Securing Configuration Management and the Continuous Integration/Continuous Delivery Pipelines; Container Security, Hardening, and Orchestration; Continuous Monitoring and Feedback Loops; Secure Secrets Management;; Automating Compliance as Code; Going Forward: Introducing Security into DevOps, and DevOps into Security; Quick Wins and Long-term Investments Needed to Succeed

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