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

GIAC CERTIFICATIONS

SEC540: Cloud Native Security and DevSecOps Automation™

GCSA
Cloud Security Automation
giac.org/gcsa

5 Day Program	38 CPEs	Laptop Required

You Will Be Able To

- Understand DevOps principles for secure workflows
- Integrate AI security tools into developer environments and CI/CD pipelines
- Manage secrets and automate infrastructure with IaC
- Harden and monitor containers and Kubernetes workloads
- Secure software supply chain with SBOMs and artifact signing
- Defend microservices using cloud native identity provider and API Gateway services
- Automate compliance with policy guardrails and remediation

Business Takeaways

- Build a security team skilled in DevSecOps, AI, and cloud-native security
- Collaborate with DevOps to integrate security and AI guardrails early in development
- Utilize cloud-native services for deployment, hardening, and monitoring
- Prepare for container and Kubernetes migrations with adaptability
- Enhance security with API Gateway and cloud native observability services
- Implement centralized audit pipelines and policy-as-code

> **"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**

Secure Your Systems at Cloud Native Speed

SEC540 prepares security professionals to secure cloud-native and DevOps environments by embedding security controls directly into automated pipelines. Through hands-on labs, students address real-world risks including insecure CI/CD pipelines, container misconfigurations, software supply chain weaknesses, and Kubernetes vulnerabilities.

Common security challenges for organizations struggling with DevOps culture include:

- Compromised CI/CD pipelines, malicious code, and credential theft
- Misconfigured cloud infrastructure and configuration drift
- Software supply chain risks from third-party libraries and build artifacts
- Excessive Kubernetes permissions and weak workload isolation
- Ineffective security automation that creates noise instead of protection
- Lack of centralized identity, zero trust enforcement, and policy governance

SEC540 develops the DevSecOps mindset required to solve these problems. Students attack and harden the full delivery lifecycle, from source control and CI/CD to Kubernetes runtime. Along the way, they implement more than 20 practical security controls to build, test, deploy, and monitor cloud-native systems securely and at scale.

Hands-On Training

SEC540 is built around immersive, hands-on learning. Students configure and implement real security controls inside a fully simulated DevOps environment, choosing guided instructions or a "no hints" path for an added challenge.

The course includes:

- 19 DevSecOps and cloud native immersive hands-on labs:
  - 4 DevOps labs covering CI/CD, infrastructure as code, and configuration management
  - 3 AI-focused labs securing DevOps workflows using LLMs, MCP, and agents
  - 9 cloud-native labs focused on containers, supply chain security, and Kubernetes
  - 3 policy-as-code labs covering compliance, guardrails, and auto-remediation

Students can complete labs in either AWS or Microsoft Azure using the provider's managed Kubernetes service.

CloudWars Bonus Challenges provide additional advanced, hands-on exercises for those who want to push further.

sans.org/sec540

- Watch a preview of this course
- Discover how to take this course: Online, In-Person

Section Descriptions

SECTION 1: DevOps Security Automation

This section introduces DevOps practices, principles, and tools by attacking a vulnerable Version Control and Continuous Integration (CI) system. Students gain an in-depth understanding of how the toolchain works, the risks these systems pose, and key weaknesses that could compromise the workflow. Next, we examine the security features available in various Continuous Integration (CI) and Continuous Delivery (CD) systems, such as GitHub and GitLab, and then start hardening the workflow. Students then see how advanced code analysis capabilities can be included using Large Language Models (LLM), AI Agents, and Model Context Protocol (MCP) servers. Finally, students ensure secrets consumed by the workflows are stored securely in secrets management solutions, such as HashiCorp Vault, AWS Secrets Manager, and Azure Key Vault.

TOPICS: DevOps and Security Challenges; DevOps Toolchain; Pre-Commit Security Controls; Pre-Merge 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 Terraform using more than 100 cloud resources. Students scan the cloud infrastructure as code (IaC), identify insecure network configurations and harden the network traffic flow rules. With the cloud infrastructure in place, students learn how automate configuration management and publish golden images using Packer and Ansible. To finish the day, students begin preparing a container image to run on a Kubernetes cluster. Following the container security lifecycle, we review Dockerfiles and Kubernetes manifests for misconfigurations, scan the configuration file code analysis, rebuild the image using trusted suppliers, write container security policies as code, and scan images for vulnerabilities. Finally, students learn how to manage the container image's software supply chain using attestations, provenance, software bill of materials (SBOM), artifact signing, and SBOM vulnerability scanning.

TOPICS: Cloud IaC; Configuration Management as Code; Container Security Lifecycle; Software Supply Chain Security

SECTION 3: Cloud Native Security Operations

Section 3 introduces students to the Kubernetes control plane and core components used to group resources, store configuration data, and run containers. After an introduction to Kubernetes configuration and kubectl, students learn how to use an AI assistant to examine a cluster and its resources. Then, we shift focus to Kubernetes security controls such as authentication, role-based access control (RBAC), isolation, workload identity, and admission control.

TOPICS: Kubernetes Architecture, Resources, and Deployments; Kubernetes Risks and Security Controls; Kubernetes Workload Security; Kubernetes Runtime Security

SECTION 4: Microservice

Section 4 starts with students learning how security changes in the world of microservices. We explore microservice architectures using edge authentication and authorization with cloud native tooling, such as the Keycloak identity provider, Kong API Gateway, and Kubernetes cloud load balancer controllers. With the perimeter protected, students then learn how to establish intra-cluster microsegmentation using Kubernetes network policy and service mesh. Next, we learn how to leverage Kubernetes blue/green capabilities to transparently deploy a new version of an application. Finally, students learn how Open Telemetry and Grafana's LGTM stack provides microservice observability for the Kubernetes cluster's metrics, logs, and traces.

TOPICS: Microservice Fundamentals; Microservice UI and Identity Providers; Microservice API Gateways; Kubernetes Deployment Orchestration; Cloud Native Security Observability

SECTION 5: Continuous Compliance and Protection

Section 5 starts with a discussion on working in DevOps and how that affects policy and compliance. Students learn to leverage cloud native security tooling to automate cloud and Kubernetes compliance checks. Starting with Cloud Security Posture Management (CSPM), we start detecting security issues in the cloud and Kubernetes infrastructure. Next, students learn how to aggregate and correlate vulnerabilities from CI/CD pipelines into Application Security Posture Management (ASPM) tools. With vulnerability data in a centralized database, valid findings can establish a health score for each product. This allows governance teams to create policy as code that "pulls the andon cord" and marks a build as unhealthy or stops a pod from launching in a Kubernetes cluster. Students finish the course learning how to write policy as code for automated remediation to detect and correct cloud configuration drift.

TOPICS: Compliance as Code; Policy as Code; Automated Remediation

Who Should Attend

- Anyone working in or transitioning to a DevOps environment
- Anyone working in Kubernetes, containers, and microservices
- 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 and secure DevOps workloads in the cloud, specifically AWS) and Azure
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

NICE Framework Work Roles

- Software Developer (OPM 621)
- Secure Software Assessor (OPM 622)
- Enterprise Architect (OPM 651)
- Research & Development Specialist (OPM 661)
- Information Systems Security Developer (OPM 631)
- Systems Developer (OPM 632)

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