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 how DevOps works and identify keys to success
- Wire security scanning into automated CI/CD pipelines and workflows
- Parse security scanning results and display the data on CI/CD dashboards
- Manage secrets for CI/CD servers and cloud native applications
- Automate configuration management using Infrastructure as Code (IaC)
- Build, harden, and publish golden virtual machine images using CI/CD workflows
- Operate and secure container technologies using Docker and Kubernetes
- Manage the software supply chain using software provenance, attestations, artifact signing, software bill of materials (SBOM), and SBOM vulnerability scanning.
- Harden Kubernetes clusters with workload identity and admission control
- Monitor Kubernetes audit logs using cloud logging and monitoring services
- Deploy patches using cloud and Kubernetes blue/green deployments
- Refactor systems to take advantage of microservice and serverless architectures
- Automate cloud compliance and security policy guardrails and auto-remediation playbook

Hands-On Training

SEC540 training 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—always with a frustration-free fallback path. Immersive hand-on labs ensure that students not only understand theory, but how to configure and implement each security control.

For students who want an extra challenge, two hours of CloudWars Bonus Challenges are available during extended hours each day. These CloudWars challenges provide additional opportunities for hands-on experience with the cloud and DevOps toolchain.

The Cloud Moves Fast. Automate to Keep Up.

Common security challenges for organizations struggling with the DevOps culture include issues such as:

- Malicious code, credential theft, and compromised extensions from improperly protected continuous integration and delivery pipelines.
- Unenforced peer code reviews and security approvals that do not meet change approval and audit requirements
- False positives, noise, and build failures from incorrectly automated security scanners
- Configuration drift between environments, resource misconfigurations, and public data exposure from insufficiently managed cloud infrastructure
- Failure to standardize golden virtual machine and container base images across the organization
- Ignoring software supply chain vulnerabilities inherited from malicious libraries, third-party software, and compromised build artifacts
- Operating Kubernetes services without policies that prevent lateral movement between workloads, reduce pod permissions, and monitor cluster activity
- Failing to release patches and close vulnerability windows due to code freezes and failed deployments
- Lacking inventory and visibility between microservices and serverless systems

Security teams can help organizations prevent these issues by developing a DevOps mindset and learning to apply cloud native security controls. This course 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 native infrastructure and software. Students learn how to attack and then harden the entire DevOps workflow, from version control to continuous integration and running cloud native workloads. Each step of the way, students explore the security controls, configuration, and policies required to improve the reliability, integrity, and security of on-premises and cloud-hosted systems. Students learn how to implement more than 20 DevSecOps security controls to build, test, deploy, harden, and monitor cloud native infrastructure and services.

Business Takeaways

- Build a modern security team that understands cloud native security and DevSecOps workflows
- Partner with DevOps and engineering teams to inject security into automated pipelines and earlier into the development process
- Leverage cloud native services to deploy, harden, and monitor software products
- Ensure your organization is ready to refactor, revise, and rebuild products during their cloud migration
- Use cloud monitoring and event triggered automation to improve security capabilities and respond to risk effectively

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 (CI) system. 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 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. After automating various code analysis tools, students learn how to parse various machine-readable data formats and display the results in CI dashboards. After discovering insecurely stored secrets, we shift focus to storing sensitive data in secrets management solutions, such as HashiCorp Vault, AWS Secrets Manager, and Azure Key Vault, that can be read at runtime by a CI workflow.

TOPICS: DevOps and Security Challenges; DevOps Toolchain; 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 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 Infrastructure as Code; Configuration Management as Code; Container Security Lifecycle; Software Supply Chain Security

SECTION 3: Cloud Native Security Operations

Section 3 prepares students to deploy and secure containerized workloads running in cloud-native Kubernetes services such as AWS Elastic Kubernetes Service (EKS) and Azure Kubernetes Service (AKS). After an introduction to Kubernetes architecture, students examine how ingress, service, and pod resources route traffic to a container and use GitLab CI to deploy a container image to the pod. With workloads running in Kubernetes, we shift focus to Kubernetes security controls such as authentication, role-based access control (RBAC), isolation, workload identity, and admission control. Students finish the section by enabling Kubernetes audit logs, monitoring workloads, analyzing log files, detecting an attack in real time, and sending alerts to the security team.

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

SECTION 4: Microservice and Serverless Security

Section 4 starts with students learning to leverage cloud-native Kubernetes ingress load balancers to patch containerized workloads using blue/green deployment patterns. From there, focus shifts to securing serverless systems using content delivery networks (CDN), API gateways, and functions as a service (FaaS). Students examine CDN services, system authentication to the backend origin, and signing requests for protected content. Then, we explore microservice architectures, edge authentication, and internal and micro-segmentation with API Gateways, Kubernetes network policy, and service mesh platforms. Students learn how serverless architectures enable DevOps teams to build dynamic systems using event triggers and Functions as a Service (FaaS). Finally, we wrap up the section analyzing a serverless deployment pipeline for Azure Functions and AWS Lambda.

TOPICS: Deployment Orchestration using Cloud Native Services; Secure Content Delivery; Microservice Security; Serverless Security

SECTION 5: Continuous Compliance and Protection

Section 5 wraps up the journey with students learning to leverage cloud services to automate security compliance. Starting with Cloud Security Posture Management (CSPM) solutions students detect security issues in their cloud infrastructure. Next, using 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 remediation using Cloud Custodian, and how to detect and correct cloud configuration drift.

TOPICS: Continuous Compliance; Runtime Security Protection; Automated Remediation

"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**

Who Should Attend

- Anyone working in or transitioning to a public cloud environment
- 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 Amazon Web Services (AWS) and Microsoft Azure
- Anyone interested in leveraging cloud application security services provided by AWS or 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