Advanced DevSecOps on GitHub Actions Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid acceleration of digital transformation and the imperative of "Shift-Left Security" demand a radical integration of security into the CI/CD pipeline. Traditional security gating practices no longer suffice in a world dominated by microservices and cloud-native architecture. Advanced DevSecOps on GitHub Actions Training Course focuses on mastering Advanced DevSecOps on GitHub Actions, providing the deep technical skills needed to build a robust, scalable, and fully automated security posture. Participants will move beyond basic vulnerability scanning to implement sophisticated Policy-as-Code, Secrets Management, and Software Supply Chain Security, transforming security from a bottleneck into an accelerated enabler of high-velocity software delivery.

This hands-on training delves into GitHub Advanced Security features, emphasizing CodeQL customization, Container Security, and Infrastructure-as-Code Security automation. By adopting a developer-centric security approach, you will learn to leverage the power of GitHub Actions to enforce enterprise-wide security governance, achieve Continuous Compliance, and automate autonomous remediation workflows. The course is structured around real-world scenarios, preparing you to lead your organization's transition to a Zero Trust CI/CD ecosystem where security is intrinsically woven into every commit, branch, and deployment, ensuring Security Resilience and protecting the Open-Source Supply Chain.

Programme Curriculum

Advanced DevSecOps on GitHub Actions Training Course

Introduction

The rapid acceleration of digital transformation and the imperative of "Shift-Left Security" demand a radical integration of security into the CI/CD pipeline. Traditional security gating practices no longer suffice in a world

dominated by microservices and cloud-native architecture. Advanced DevSecOps on GitHub Actions Training Course focuses on mastering Advanced DevSecOps on GitHub Actions, providing the deep technical skills needed to build a robust, scalable, and fully automated security posture. Participants will move beyond basic vulnerability scanning to implement sophisticated Policy-as-Code, Secrets Management, and Software Supply Chain Security, transforming security from a bottleneck into an accelerated enabler of high-velocity software delivery.

This hands-on training delves into GitHub Advanced Security features, emphasizing CodeQL customization, Container Security, and Infrastructure-as-Code Security automation. By adopting a developer-centric security approach, you will learn to leverage the power of GitHub Actions to enforce enterprise-wide security governance, achieve Continuous Compliance, and automate autonomous remediation workflows. The course is structured around real-world scenarios, preparing you to lead your organization's transition to a Zero Trust CI/CD ecosystem where security is intrinsically woven into every commit, branch, and deployment, ensuring Security Resilience and protecting the Open-Source Supply Chain.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Automate Secure Supply Chain practices using advanced GitHub Actions.
2. Implement and customize GitHub Advanced Security for enterprise-wide coverage.
3. Master CodeQL for Custom Query development and advanced Static Application Security Testing.
4. Design and enforce Policy-as-Code using OPA Gatekeeper or similar tools within CI/CD.
5. Establish robust Secrets Management and scanning using specialized GitHub Actions.
6. Secure Infrastructure-as-Code (IaC) templates with automation.
7. Integrate and orchestrate Dynamic Application Security Testing and API Security scans.
8. Implement Container Image Security scanning in GitHub workflows.
9. Develop Continuous Compliance and audit reporting pipelines on GitHub Actions.
10. Apply Threat Modeling techniques to automate proactive security control deployment.
11. Build Autonomous Remediation workflows for common security findings.
12. Configure organization-level Security Governance and monitoring dashboards using GHAS.
13. Leverage GitHub Environments and Deployment Protection Rules for secure deployments.

Target Audience

1. DevSecOps Engineers
2. Senior DevOps/SREs
3. Security Architects
4. Application Security Specialists
5. Senior Software Engineers
6. Cloud Engineers/Architects
7. GitHub Administrators
8. Technical Leads/Engineering Managers

Course Modules

Module 1: Mastering GitHub Actions for Advanced DevSecOps

- Deep dive into GitHub Actions architecture and runner security.
- Securing self-hosted runners and runner groups.
- Advanced workflow composition.
- Implementing OpenID Connect for cloud provider authentication.
- Best practices for GH Actions hardening and integrity checks.
- Case Study: Designing a highly secure, immutable CI/CD pipeline leveraging OIDC and self-hosted runners for a multi-cloud deployment.

Module 2: GitHub Advanced Security (GHAS) Deep Dive

- Enabling and configuring GHAS features at the organization level.
- Advanced use of Code Scanning and customizing the CodeQL engine.
- Deep-dive into Secret Scanning and protecting against committed credentials.
- Managing and triaging security alerts at scale across multiple repositories.
- Integrating custom security rules via CodeQL query packs.
- Case Study: Customizing a CodeQL query to detect a novel internal security anti-pattern across 50+ microservices in a major financial institution.

Module 3: Static Analysis and Code Quality Automation

- Orchestrating SAST with CodeQL and third-party tools
- Implementing "Break the Build" strategies for high-severity vulnerabilities.
- Advanced Dependency Review and managing transitive dependencies.
- Automating Software Bill of Materials generation on every build.
- Leveraging custom security metadata and annotations in code.
- Case Study: Automating SBOM generation and using dependency-graph data to perform a post-incident impact analysis following a critical zero-day vulnerability

Module 4: Advanced Secrets and Credential Management

- Integrating Secrets Management tools with GitHub Actions.
- Implementing Gitleaks and other tools for pre-commit secret scanning.
- Best practices for GitHub Environment Secrets and rotation policies.
- Auditing and logging of secret access and usage within workflows.
- Transitioning from hardcoded secrets to OIDC and least-privilege principles.
- Case Study: Migrating a legacy CI/CD system from shared, long-lived access keys to a short-lived, environment-scoped OIDC-based credentialing system.

Module 5: Infrastructure-as-Code (IaC) Security

- Automating security scanning for Terraform and CloudFormation
- Integrating IaC security checks directly into Pull Request workflows.
- Enforcing Cloud Security Posture Management best practices via CI/CD.
- Writing and enforcing Policy-as-Code for IaC using Open Policy Agent.
- Implementing drift detection and remediation using GitHub Actions.
- Case Study: Developing an OPA policy to block any Terraform deployment that attempts to create an S3 bucket without mandatory server-side encryption enabled.

Module 6: Container and Kubernetes Security in CI/CD

- Automating Container Image Scanning post-build.

- Enforcing security policies on container base images and registries.
- Integrating Kubernetes Security checks into deployment workflows.
- Applying Immutable Infrastructure principles to container deployment.
- Using GitHub Actions for Kubernetes-native policy enforcement
- Case Study: Building a GitHub workflow to scan a Docker image, generate a vulnerability report, and block the deployment to a Kubernetes cluster if any critical vulnerability is found.

Module 7: Dynamic and Interactive Application Security Testing (DAST/IAST)

- Orchestrating DAST tools via GitHub Actions.
- Setting up temporary, secure test environments for DAST and IAST execution.
- Mapping DAST results back to the source code for developer-friendly feedback.
- Automating API Security testing against OpenAPI specifications.
- Integrating Security Observability/Runtime protection alerts back into the DevSecOps loop.
- Case Study: Implementing a multi-stage GitHub workflow that deploys a service to a temporary environment, runs an automated OWASP ZAP baseline scan, and automatically creates a GitHub Issue for any new high-risk finding.

Module 8: Continuous Compliance and Auditability

- Implementing Audit Trails and logging for all security-critical GitHub Actions events.
- Automating evidence collection for compliance frameworks
- Configuring Security Dashboards and metrics for executive reporting.
- Using GitHub Environments for change control and regulated deployments.
- Integrating compliance checks as code into pull requests and branch protection.
- Case Study: Configuring an automated compliance reporting workflow that aggregates SAST, IaC, and deployment logs to generate an evidence package for an annual security audit.

Module 9: Advanced Workflows for Security Governance

- Implementing Branch Protection Rules and Code Owners for critical security checks.
- Writing reusable Composite Actions for standardized security steps across teams.
- Automating Security Issue Triage and ticket creation
- Utilizing GitHub Dependabot for proactive dependency vulnerability management.
- Enforcing standardized security headers and configurations.
- Case Study: Designing an organization-wide policy using reusable actions to ensure every repository automatically runs secret scanning and dependency review on all pull requests.

Module 10: Security Chaos Engineering and Resilience

- Introducing principles of Security Chaos Engineering into the CI/CD cycle.
- Using GitHub Actions to simulate common security failures
- Automating Security Benchmarking and stress testing.
- Developing runbook automation for incident response via GitHub workflows.
- Measuring and reporting on DevSecOps security resilience metrics.
- Case Study: Building a "Chaos Action" that randomly injects a minor security misconfiguration into a deployment to test the effectiveness of runtime monitoring and alerting systems.

Module 11: Autonomous Remediation and Self-Healing Pipelines

- Developing GitHub Actions to automatically patch dependency vulnerabilities

- Automating Code Fixes for low-hanging SAST findings.
- Creating self-healing workflows that automatically rollback or restart failed secure deployments.
- Implementing automated PR creation for security updates and configuration changes.
- Using webhooks and external security events to trigger remediation workflows.
- Case Study: Configuring a workflow that, upon a non-critical SAST finding, automatically generates a new branch, applies a suggested code fix, and opens a pull request for review.

Module 12: Scaling DevSecOps Across the Enterprise

- Strategies for managing Security Templates and standardized workflows across hundreds of repositories.
- Implementing InnerSource practices for security tooling development.
- Cost optimization and performance tuning of security-heavy GitHub Actions.
- Onboarding and educating development teams on new security workflows.
- Centralizing security findings and reporting for C-level visibility.
- Case Study: Designing a phased rollout strategy for mandatory GHAS adoption across a 500+ developer organization, including automated migration of legacy CI/CD security checks.

Module 13: Future of DevSecOps: AI and Cloud-Native Security

- Exploring the use of AI/ML in DevSecOps workflows.
- Integrating Cloud-Native Application Protection Platforms with GitHub.
- Security considerations for Serverless and Edge deployments.
- Advanced runtime monitoring and integration with SIEM/SOAR tools.
- The impact of GitOps and Infrastructure-as-Code principles on DevSecOps architecture.
- Case Study: Building a proactive security workflow that integrates runtime vulnerability data from a CNAPP and automatically triggers a targeted code scan on GitHub for the affected repository.

Module 14: API Security and Gateway Enforcement

- Leveraging GitHub Actions to audit and secure API Gateways configurations.
- Automating security testing focused on the OWASP API Security Top 10.
- Integrating API security tools for schema validation and fuzz testing.
- Enforcing Authentication and Authorization policies using Policy-as-Code at the API level.
- Automating documentation generation and security review for new API endpoints.
- Case Study: Creating a GitHub workflow that runs an API fuzzing tool against a newly deployed service and uses the OpenAPI specification to ensure strict request/response validation.

Module 15: Incident Response and Forensic Readiness

- Using GitHub Actions to automate Log Collection and preservation post-incident.
- Implementing Ephemeral Environment destruction and forensic snapshots.
- Automating notification and communication workflows during a security breach.
- Preparing repositories and workflows for regulatory forensic requirements.
- Integrating with SOAR platforms for automated security playbooks.
- Case Study: Designing an Incident Response Action that, when triggered manually or via a critical alert, isolates the affected production environment, copies all relevant logs to a secure, immutable storage, and notifies the security team instantly.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com