Infrastructure as Code (IaC) Security Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid adoption of DevOps and Cloud-Native technologies has driven the critical shift to Infrastructure as Code, revolutionizing how cloud environments are provisioned. Tools like Terraform, AWS CloudFormation, and Kubernetes accelerate deployment velocity, but they also introduce new, significant Security Risks. Traditional perimeter security is insufficient, making a Shift Left approach paramount. Infrastructure as Code (IaC) Security Training Course addresses the urgent need for robust security by embedding Security Best Practices and Policy as Code directly into the DevSecOps pipeline, ensuring that security is proactive, automated, and scales with the speed of your infrastructure deployments.

Mastering IaC Security is non-negotiable for modern organizations seeking to achieve Continuous Compliance and prevent costly Cloud Misconfigurations. A single flaw in an IaC template, such as an overly permissive IAM Role or a hardcoded Secret, can instantly expose an entire production environment, leading to a catastrophic Data Breach. This training provides a deep dive into IaC Scanning tools, automated Vulnerability Management, and Drift Detection strategies. By the end, participants will possess the skills to build and maintain Immutable Infrastructure that is secure by design, transforming them into Cloud Security champions ready to implement a true Secure-by-Default methodology.

Programme Curriculum

Infrastructure as Code (IaC) Security Training Course

Introduction

The rapid adoption of DevOps and Cloud-Native technologies has driven the critical shift to Infrastructure as Code, revolutionizing how cloud environments are provisioned. Tools like Terraform, AWS CloudFormation, and Kubernetes accelerate deployment velocity, but they also introduce new, significant Security Risks. Traditional perimeter security is insufficient, making a Shift Left approach paramount. Infrastructure as Code (IaC) Security

Training Course addresses the urgent need for robust security by embedding Security Best Practices and Policy as Code directly into the DevSecOps pipeline, ensuring that security is proactive, automated, and scales with the speed of your infrastructure deployments.

Mastering IaC Security is non-negotiable for modern organizations seeking to achieve Continuous Compliance and prevent costly Cloud Misconfigurations. A single flaw in an IaC template, such as an overly permissive IAM Role or a hardcoded Secret, can instantly expose an entire production environment, leading to a catastrophic Data Breach. This training provides a deep dive into IaC Scanning tools, automated Vulnerability Management, and Drift Detection strategies. By the end, participants will possess the skills to build and maintain Immutable Infrastructure that is secure by design, transforming them into Cloud Security champions ready to implement a true Secure-by-Default methodology.

Course Duration

5 days

Course Objectives

1. Master the Shift Left Security paradigm in DevSecOps workflows.
2. Identify and mitigate top IaC Security Risks and common Cloud Misconfigurations.
3. Implement Policy as Code using tools like Open Policy Agent for automated governance.
4. Securely manage and protect Hardcoded Secrets and credentials within IaC templates.
5. Perform effective static analysis and automated IaC Scanning with popular tools
6. Secure IaC for major cloud platforms.
7. Apply Least Privilege Principle to IAM Roles and service accounts defined in code.
8. Enforce Supply Chain Security for IaC modules and dependencies.
9. Integrate security testing seamlessly into CI/CD Pipelines.
10. Implement strategies for Configuration Drift Detection and automated remediation.
11. Secure Kubernetes configurations using IaC security best practices.
12. Establish continuous monitoring for security and Compliance-as-Code
13. Practice incident response and secure rollback procedures for compromised IaC deployments.

Target Audience

1. DevOps Engineers and SREs
2. Cloud Engineers and Architects
3. Security Engineers and Analysts
4. Software Developers working with cloud infrastructure
5. Technical Leads and Engineering Managers
6. Compliance and Audit Professionals
7. Automation Specialists
8. Security Champions within development teams

Course Modules

Module 1: Foundations of IaC Security & Shift Left

- Understanding the IaC Threat Landscape and top attack vectors.
- The Shared Responsibility Model in a cloud and IaC context.
- Defining and implementing Shift Left Security in the SDLC.
- Introduction to IaC tools.

- Case Study: Analyzing a major cloud outage caused by a misconfigured Terraform block that exposed an unencrypted database.

Module 2: Automated Static Analysis and IaC Scanning

- Integrating Static Application Security Testing for IaC templates.
- Deep dive into popular scanning tools.
- Writing custom rules for organization-specific Security Policies.
- Differentiating between misconfiguration, vulnerability, and best-practice violation findings.
- Case Study: Implementing an automated Checkov scan in a pre-commit hook to block a hardcoded public IP address being pushed to a Git repository.

Module 3: Policy as Code (PaC) and Governance

- Principles and architecture of Policy as Code
- Using Open Policy Agent for cross-platform policy enforcement.
- Enforcing Compliance-as-Code for standards like CIS Benchmarks and SOC 2.
- Integrating PaC into the CI/CD Pipeline to gate deployments.
- Case Study: Developing and deploying an OPA policy to prevent the creation of IAM users without Multi-Factor Authentication enabled.

Module 4: Secure Secrets Management in IaC

- The dangers of Hardcoded Secrets in code.
- Best practices for external Secrets Management using HashiCorp Vault or cloud-native solutions
- Implementing variable injection and secret referencing securely.
- Securing Terraform State Files.
- Case Study: Refactoring a vulnerable CloudFormation template to replace embedded passwords with secure dynamic references from a centralized secret store.

Module 5: Identity and Access Management (IAM) Security

- Applying the Principle of Least Privilege to all IaC-defined roles and users.
- Auditing and minimizing Overly Permissive IAM Roles and wildcards.
- Securing service accounts and role assumption across cloud providers.
- Implementing boundary policies and fine-grained access control
- Case Study: Reviewing a vulnerable Kubernetes ServiceAccount definition and refactoring its associated IAM Policy to follow least privilege for external resource access.

Module 6: Securing Cloud and Containerized Infrastructure

- Best practices for securing network components.
- Enforcing encryption at rest and in transit for storage and databases.
- Securing Kubernetes manifests for pods, networks, and cluster roles.
- Automated checking for insecure defaults in cloud services.
- Case Study: Fixing a Dockerfile and a Kubernetes deployment manifest to run containers as a non-root user and ensure image pull policies are secure.

Module 7: CI/CD Integration and Supply Chain Security

- Integrating automated IaC security checks into GitHub Actions, GitLab CI, or Jenkins.
- Implementing Peer Review and Branch Protection for all infrastructure code changes.

- Securing the IaC Supply Chain by validating module sources and external dependencies.
- Automated testing.
- Case Study: Building a multi-stage CI/CD pipeline that runs static analysis, PaC checks, and unit tests before merging a pull request for a new infrastructure feature.

Module 8: Monitoring, Drift Detection, and Remediation

- Understanding and preventing Configuration Drift between code and runtime environment.
- Implementing continuous monitoring and alerting for security-relevant infrastructure changes.
- Using cloud-native tools for Drift Detection.
- Developing and testing automated remediation runbooks
- Case Study: Setting up real-time alerting to detect when a security group is manually modified in the AWS console, and triggering an automated Terraform refresh/plan to identify the drift.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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