KORUR

DEVSECOPS TRAINING · EXERCISE GUIDE

DevSecOps Exercise Guide

A practical companion to Korur's hands-on DevSecOps training — pipeline hardening, container scanning, and secure-by-default development.

AI coding assistants, supply chain attacks, and new regulation rewrote what secure development means. We train your developers on your stack, your tools, and your actual codebase.

Why DevSecOps Matters in 2026

AI coding assistants, supply chain attacks, and new regulation have rewritten what secure development means.

300%

Supply Chain Attacks Tripled

Software supply chain attacks increased 300% in 2024-2025. Developers are now the primary attack target, not the perimeter.

95%

Cloud Misconfigs Dominate Breaches

95% of cloud security failures trace back to misconfiguration or code errors, not sophisticated zero-days.

AI code

AI Code Introduces New Vulnerabilities

GitHub Copilot and Cursor generate insecure patterns at measurable rates. Developers who can't review AI output are a growing liability.

DORA

DORA Requires Shift-Left Security

The EU Digital Operational Resilience Act mandates security integration in the development lifecycle for financial services.

What Developers Walk Away With

Skills that ship with every developer who completes this training.

- Working knowledge of container and image scanning with tools like Trivy and Grype
- Hands-on CI/CD pipeline hardening: branch protection, SAST, dependency scanning
- Secrets management configuration for Vault, Azure Key Vault, and GitHub Actions
- OWASP Top 10 identification and remediation in their own codebase
- Supply chain security: SBOM generation, dependency pinning, artifact signing
- Secure code review technique for AI-generated code

Exercise Program

A dense, hands-on program. Attendees bring their own code and leave with it more secure.

1. **Environment Setup and Threat Modeling**

   We start by mapping the participant's actual pipeline, what tools they use, where secrets live, where the risky handoffs are.

2. **Container and Pipeline Security Labs**

   Hands-on exercises: scan a real image, find the CVEs, fix them. Configure a GitHub Actions workflow with SAST and secret scanning.

3 **OWASP Top 10 Code Review**

Participants review code samples, including AI-generated code, for injection, broken auth, insecure deserialization, and other common patterns.

4 **Supply Chain and Secrets Module**

Practical: generate an SBOM, set up dependency pinning, rotate a leaked secret, configure Vault or Azure Key Vault.

5 **Team Secure Development Policy**

We close with a collaborative session to draft or update the team's secure development checklist and code review criteria.

> This document is a companion to Korur's DevSecOps Exercise Guide. It summarizes the framework covered during the live training. The hands-on labs, role-specific breakouts, and Q&A take place during the session itself.

Ready to run this with your team?
Korur delivers this training on-site, tailored to your industry and stack. Book a session at **korur.nl/contact**.