THE ESSENTIAL SECURITY GUIDES SERIES

JUST TELL ME WHAT I NEED TO KNOW...

DEVSECOPS

DEVELOP SECURELY. AUTOMATE INTELLIGENTLY. DELIVER CONFIDENTLY.

SHIFT LEFT
Integrate security early and continuously.

AUTOMATE
Build, test, and deploy with security built in.

COLLABORATE
Break down silos. Everyone owns security.

CONTINUUSLY MONITOR
Detect issues early and respond fast.

MEASURE & IMPROVE
Use metrics to drive security outcomes.

COMPLY EVERYWHERE
Meet regulatory and policy requirements.

DEVSECOPS PRINCIPLES

SECURITY BY DESIGN
Security is part of every step, not an afterthought.

AUTOMATION EVERYWHERE
Automate security controls and reduce human error.

INFRASTRUCTURE AS CODE
Manage and secure infrastructure through code and versioning.

INTEGRATE SECURITY TOOLS
Embed security scanning and testugh in the pipeline.

CONTINUOUS VISIBILITY
End-to-end visibility across applications, pipelines, and environments.

POLICY AS CODE
Enforce security policies consistently and at scale.

CULTURE OF OWNERSHIP
Empower teams to own and improve security together.

KEY DEVSECOPS PRACTICES

SECURE CODING	Follow secure coding standards and threat modeling.
SAST / DAST / SCA	Automated code, dependency, and application scanning.
SECRETS MANAGEMENT	Protect credentials and sensitive data in transit and at rest.
CONTAINER & K8s SECURITY	Scan images, enforce policies, and secure runtime.
COMPLIANCE AUTOMATION	Continuously check compliance and generate evidence.

DEVSECOPS DELIVERS

REDUCED RISK
Find and fix vulnerabilities early.

FASTER DELIVERY
Automate and streamline secure releases.

LOWER COST
Prevent issues instead of remediating later.

HIGHER QUALITY
Build reliable, secure, and trusted software.

STRONGER COMPLIANCE
Meet regulatory requirements with confidence.

CODE → BUILD → TEST → SCAN → DEPLOY → MONITOR → IMPROVE

Just Tell Me What I Need To Know

DevSecOps

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

Table of Contents

Introduction

Modern software is expected to be delivered faster than ever before, but it also has to be secure, reliable, resilient, and compliant.

Organizations can no longer afford development processes where security is added at the end of a project or where operations teams inherit software they had little involvement in building. Today's systems are developed, tested, deployed, monitored, and continuously improved using highly automated pipelines that integrate development, security, and operations into a single collaborative process.

This approach is known as DevSecOps.

The challenge is that DevSecOps is often misunderstood. Some people think it's simply DevOps with a few security tools added to the pipeline. Others assume it's only relevant to software developers or cloud engineers. In reality, DevSecOps represents a fundamental shift in how organizations design, build, secure, deploy, and operate modern applications and infrastructure.

That's where this book comes in.

The Just Tell Me What I Need to Know… series is designed to cut through the complexity and focus on the knowledge professionals actually need. Rather than overwhelming you with programming tutorials or vendor-specific implementations, each book delivers practical, real-world concepts in a clear, concise, and easy-to-understand format.

This book focuses on DevSecOps—the people, processes, technologies, and automation that enable organizations to deliver secure software quickly and consistently. You'll learn about secure software development, CI/CD pipelines, Infrastructure as Code, Policy as Code, software supply chain security, GitOps, cloud-native delivery, security automation, observability, platform engineering, and the metrics used to measure DevSecOps success.

Unlike books that focus on a single CI/CD platform or programming language, this book is vendor-neutral and technology-agnostic. The concepts apply whether your organization uses GitHub, GitLab, Jenkins, Azure DevOps, AWS, Kubernetes, or another platform. The emphasis is on understanding how secure software delivery works and how security becomes an integrated, automated part of the entire software lifecycle.

Whether you're an engineer, architect, cybersecurity professional, DevOps engineer, manager, project leader, student, or executive, understanding DevSecOps has become essential for building and operating secure, resilient, and scalable systems.

This book shows how to engineer, automate, and secure the software delivery lifecycle regardless of the tools being used.

This book should answer:

"How do I build, test, deploy, operate, and continuously secure modern software at enterprise scale?"

This is not a programming book. It's an engineering, architecture, security, and operations book. The purpose is to understand how to integrate security into modern software development, delivery, and operations through automation, continuous integration, continuous delivery, Infrastructure as Code, policy automation, and secure software supply chain management.

Our goal is simple:

Give you the knowledge you need, without making you read three books to get it.

So, let’s get started.

MODERN SOFTWARE MUST BE DELIVERED FAST—BUT IT ALSO HAS TO BE SECURE.

Today's organizations can't afford to bolt security onto applications at the end of development. Software is built, tested, deployed, and updated continuously, often dozens of times each day. Success depends on integrating development, security, and operations into a single, automated process that delivers secure, reliable software at enterprise scale.

The problem? Most DevSecOps books assume you're a software developer, dive deeply into programming, or focus on a specific tool, cloud platform, or CI/CD product. They rarely explain how all the pieces fit together from an engineering, architecture, and security perspective.

This book is different.

Just Tell Me What I Need To Know... DevSecOps provides a practical, business-focused guide to building secure software through automation, collaboration, and continuous improvement. You'll learn how modern DevSecOps integrates secure software development, CI/CD pipelines, Infrastructure as Code, Policy as Code, software supply chain security, GitOps, cloud-native architectures, container security, platform engineering, observability, and continuous compliance into a unified software delivery lifecycle. Rather than teaching a particular programming language or vendor platform, this book explains the principles and practices that apply across today's leading enterprise technologies.

DEVSECOPS: PEOPLE. PROCESS. TECHNOLOGY.

PEOPLE
Break down silos. Build trust. Deliver together.

PROCESS
Automate. Integrate. Improve continuously.

TECHNOLOGY
Secure by design. Deliver with confidence.

INSIDE YOU'LL LEARN HOW TO:

- Understand the complete DevSecOps lifecycle and culture
- Build secure CI/CD pipelines and automate security testing
- Integrate security throughout the Secure Software Development Lifecycle (Secure SDLC)
- Implement Infrastructure as Code, Policy as Code, and GitOps
- Secure containers, Kubernetes, cloud-native applications, and software supply chains
- Measure DevSecOps performance using meaningful engineering and security metrics
- Improve collaboration between development, security, and operations teams
- Build a mature, scalable DevSecOps program that delivers secure software at speed

THE DEVSECOPS LIFECYCLE

CORE DEVSECOPS PRINCIPLES

SECURITY BY DESIGN | AUTOMATE EVERYTHING | COLLABORATE CONTINUOUSLY | MEASURE WHAT MATTERS | IMPROVE RELENTLESSLY

KEY CAPABILITIES

SECURE SDLC | CI/CD PIPELINES | INFRASTRUCTURE AS CODE | POLICY AS CODE

SOFTWARE SUPPLY CHAIN | CONTAINER & K&S SECURITY | CLOUD-NATIVE SECURITY | OBSERVABILITY & MONITORING

DEVSECOPS DELIVERS

REDUCE RISK
Find and fix issues earlier in the lifecycle.

FASTER DELIVERY
Automate and streamline from code to production.

LOWER COST
Prevent defects, rework, and security incidents.

HIGHER QUALITY
Deliver secure, reliable software your customers trust.

STAY COMPLIANT
Continuous compliance built into every pipeline.

BUSINESS VALUE
Enable innovation, resilience, and competitive advantage.

Whether you're a security architect, software engineer, DevOps engineer, cloud engineer, CISO, project manager, consultant, or aspiring cybersecurity professional, this book provides the practical knowledge you need to **understand modern DevSecOps, reduce software risk, and build secure, resilient applications** in today's fast-moving technology landscape.

SECURE YOUR CODE. PROTECT YOUR CUSTOMERS. ACCEERATE YOUR BUSINESS.
BUILD SECURE SOFTWARE. DELIVER WITH CONFIDENCE.