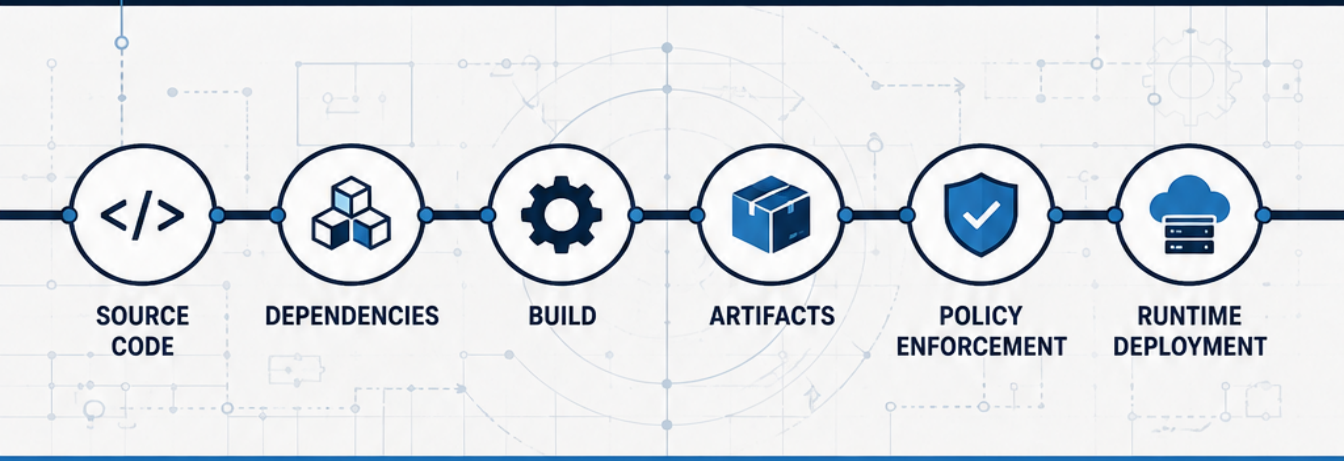
SECURE SOFTWARE SUPPLY CHAINS

END-TO-END SECURITY FOR MODERN SOFTWARE DELIVERY



- THREAT MODELS & REAL-WORLD INCIDENTS
- REPRODUCIBLE BUILDS WITH BAZEL & NIX
- SBOMS & PROVENANCE ATTESTATIONS
- SIGN ARTIFACTS WITH SIGSTORE
- ENFORCE POLICIES IN KUBERNETES CLUSTERS
- BUILD SECURE PIPELINES THAT SCALE

PRACTICAL TECHNIQUES. PROVEN TOOLS.
A COMPLETE APPROACH TO SUPPLY CHAIN SECURITY.

OLIVER REDFORD

Secure Software Supply Chains

End-to-End Security for Modern Software Delivery

Steve Publications

This book is available at https://leanpub.com/securesoftwaresupplychains

This version was published on 2026-08-01

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Contents

End-to-End Security for Modern Software Delivery

Every line of code you ship depends on hundreds of external components, automated build pipelines, and deployment systems that you do not fully control. The software supply chain is the longest attack surface in your infrastructure and the one most teams leave unprotected. This book shows you how to secure it from source code through dependencies, builds, artifacts, and runtime deployment using cryptographic verification, policy enforcement, and automation that works in production. You will learn the threat models behind real-world incidents like SolarWinds and Log4Shell, implement reproducible builds with Bazel and Nix, generate SBOMs and provenance attestations, sign artifacts with Sigstore, enforce policies in Kubernetes clusters, and wire everything together into a complete secure delivery pipeline that scales across teams. By the end you will understand not just which tools to use but why they work together, where they fail, and how to design a supply chain security program that survives audits, incidents, and organizational change.

Introduction: The Longest Attack Surface

In March 2024 a software engineer named Andres Freund noticed something strange in the build logs of his Linux system. The XZ Utils compression library, used by virtually every major Linux distribution, had grown significantly larger between versions without any obvious reason. After weeks of investigation he discovered a backdoor hidden inside liblzma that would have allowed an attacker to remotely execute code on any SSH server using the compromised library [1]. The attack had been in development for years. A threat actor under the name Jia Tan had gradually earned trust within the XZ project, contributed legitimate code, and then inserted malicious changes that evaded automated scanning tools and human review alike.

This incident was not an anomaly. It was a demonstration of what happens when software supply chains grow more complex than our security controls can track. Modern applications depend on thousands of third-party libraries, build through automated pipelines that execute code from dozens of sources, and deploy to environments where runtime behavior is often invisible until something goes wrong. The attack surface stretches from the moment a developer pulls a dependency to the moment a container starts in production, and every link in that chain is exploitable.

Why Traditional Security Fails

Perimeter security, endpoint protection, and network segmentation all assume that you can draw a boundary around what you are protecting and defend that boundary. Supply chain attacks defeat this assumption by entering through trusted channels. When SolarWinds was compromised in 2020, attackers injected malicious code into the Orion platform build process, and the resulting backdoor was distributed to customers through legitimate software updates signed with SolarWinds own cryptographic keys [2]. The update mechanism worked exactly as designed. That is the problem.

When Log4Shell was disclosed in December 2021, it affected an estimated 70 percent of public cloud workloads because Apache Log4j was embedded so deeply into Java applications that most organizations had no visibility into whether they used it [3]. The vulnerability existed since 2013. Teams could not patch quickly because they did not know what needed patching.

These incidents share a common pattern: the attack happens outside the perimeter, through channels that are supposed to be safe, using mechanisms that security tools cannot easily inspect. A compromised dependency looks like any other dependency. A tampered build artifact has the same structure as a legitimate one. A malicious CI/CD step runs with the same permissions as every other step in the pipeline.

What This Book Covers

This book takes a systematic approach to securing the software supply chain. We will not treat supply chain security as a single tool or control but as a layered system of verifiable trust that spans the entire lifecycle from development through deployment. Each chapter builds on previous material, so you can read sequentially to get the full picture or jump to specific topics based on your immediate needs.

The book is organized into three parts. The first part establishes foundations: threat models, attack vectors, and the principles that drive all supply chain security decisions. You will learn how attackers actually operate against supply chains, what they are trying to achieve, and how to model risk for your own organization. The second part covers the technical controls: dependency management, reproducible builds, artifact signing, provenance generation, SBOMs, secure CI/CD pipelines, container security, and Kubernetes enforcement. Each topic includes production-ready code examples and configuration files you can adapt directly. The third part brings everything together in a complete end-to-end implementation that demonstrates how all the pieces fit into a real-world pipeline, plus coverage of vulnerability management, compliance frameworks, and incident response.

Who Should Read This Book

This book is for engineers who design, build, or operate software delivery systems: DevOps engineers, platform engineers, security engineers, SREs, and

technical architects. You should be comfortable with Linux command-line tools, container technologies like Docker and Kubernetes, and at least one CI/CD platform. Prior security experience is helpful but not required; we explain the security concepts as we go.

If you are a security engineer new to software delivery, this book will give you the technical depth to work effectively with engineering teams on supply chain controls. If you are a DevOps or platform engineer adding security responsibilities, it will show you how to implement protections that do not slow down development. If you are a technical architect designing systems at scale, it will help you make informed decisions about tools, patterns, and tradeoffs.

How to Use the Code Examples

Every code example in this book is designed to work in a real environment. You can run them on Linux, macOS, or Windows with WSL. Where platform-specific behavior matters, we call it out explicitly. Most examples assume you have Docker, Git, and a basic Kubernetes cluster available (Kind, Minikube, or k3d work fine for local testing).

The code is organized to be practical rather than minimal. We include error handling, configuration management, and operational considerations that you would need in production. When there are multiple valid approaches, we show the one we recommend and explain why, then discuss alternatives and tradeoffs.

The Security Mindset

Before diving into tools and configurations, adopt a core principle that will guide every decision: trust must be earned, verified, and continuously re-verified. In a secure supply chain, nothing is trusted by default. Source code must be reviewed and signed. Dependencies must be locked and scanned. Builds must be reproducible and attested. Artifacts must be cryptographically signed and verified before deployment. Runtime behavior must be monitored against expected patterns.

This does not mean paranoia or slowing everything down to a crawl. It means designing systems where trust is explicit, automated, and machine-verifiable so that humans can focus on making decisions rather than checking

boxes. The tools and patterns in this book are designed to make that possible at scale.

Chapter 1: The Software Supply Chain Under Attack

The modern software supply chain is a complex system that spans source code repositories, package registries, build environments, artifact storage, CI/CD pipelines, container registries, orchestration platforms, and runtime infrastructure. Every stage introduces new dependencies, new tools, and new potential points of failure. Understanding this attack surface is the first step to defending it.

Anatomy of a Modern Build Pipeline

Consider a typical microservice built in 2026. A developer writes code in Go or Python, commits it to GitHub or GitLab, and triggers a CI/CD pipeline. The pipeline checks out the source, installs dependencies from npm, PyPI, Maven Central, or another registry, runs tests using containers pulled from Docker Hub, builds a container image with Docker or BuildKit, scans it for vulnerabilities, signs it with Cosign, pushes it to a private registry, and deploys it to Kubernetes via Argo CD or Flux.

This pipeline touches at least ten different external services before the application is running. Each one is a potential attack vector:

- The source repository can be compromised through account takeover or malicious pull requests
- Package registries can host malicious packages that look legitimate
- Base images on Docker Hub can be tampered with or contain vulnerabilities
- CI/CD runners can be exploited to steal secrets or inject code
- Container registries can serve modified images
- Kubernetes clusters can run unauthorized workloads

The pipeline itself depends on plugins, actions, and scripts from third parties. In GitHub Actions alone, the most popular third-party actions have billions

of runs. If an action maintainer is compromised or a malicious actor publishes a convincing fake action, every repository using it becomes vulnerable.

This is not theoretical. In 2024 researchers found that over 30 percent of public GitHub repositories used at least one potentially malicious or misconfigured third-party action [4]. The attack surface is real and growing.

High-Profile Breaches That Changed Everything

Several incidents in the past five years have fundamentally reshaped how the industry thinks about supply chain security. Each one exposed a different weakness and drove new defensive practices.

SolarWinds: Compromising Trust at Scale

The SolarWinds breach, disclosed in December 2020, remains the most consequential supply chain attack in history. A nation-state actor known as APT29 gained access to SolarWinds internal networks and injected a backdoor called SUNBURST into the Orion platform build process [5]. The malicious code was compiled into legitimate software updates and distributed to approximately 18,000 customers including nine US federal agencies and hundreds of private companies.

What made this attack devastating was its use of trusted channels. The infected updates were signed with SolarWinds own cryptographic certificate. Customers who installed the update received a backdoor that had passed all normal integrity checks. The attackers used the SUNSPOT tool to inject malicious code during the build, and the resulting implant communicated with command-and-control servers using domain generation algorithms to evade detection [6].

The incident revealed several critical lessons:

- Build environment compromise can defeat all downstream security controls
- Cryptographic signatures only prove who signed something, not that it is safe
- Software updates are a high-value target that requires specialized protections

- Detection of supply chain attacks often depends on behavioral analysis rather than signature matching

Log4Shell: The Dependency Problem

CVE-2021-44228, known as Log4Shell, was a remote code execution vulnerability in Apache Log4j discovered in November 2021 and publicly disclosed on December 9 [7]. The vulnerability allowed attackers to execute arbitrary code on any system that logged untrusted input using affected versions of Log4j. Within hours of disclosure, exploitation was observed worldwide.

The scale was staggering. Log4j is one of the most widely used Java libraries in existence. Major vendors including IBM, Microsoft, Oracle, Cisco, and VMware all had products affected. Minecraft servers were among the first targets because player chat messages are logged through Log4j [8].

Log4Shell exposed two fundamental problems with dependency management. First, most organizations had no visibility into their transitive dependencies. Teams knew they used Java but did not know whether their applications depended on Log4j directly or indirectly through another library. Second, patching was slow because the first fix (version 2.15.0) was incomplete, requiring additional upgrades to fully close the vulnerability [9].

The incident accelerated adoption of Software Bill of Materials (SBOM) requirements and drove regulatory action including US Executive Order 14028.

xz-utils: The Patient Attack

The xz-utils backdoor discovered in March 2024 demonstrated a new level of sophistication in supply chain attacks [10]. An attacker using the identity Jia Tan spent years building credibility within the open-source community before gradually gaining maintainer access to the XZ Utils project. Once in position, they introduced a series of changes that obfuscated malicious code inside the liblzma library.

The backdoor targeted SSH authentication. When an affected system used the compromised library for SSH connections, the attacker could intercept the authentication process and gain unauthorized access. The code was carefully designed to blend in with legitimate functionality and avoid detection by static

analysis tools. The changes included thousands of lines of additions that made the malicious code harder to distinguish from normal development.

What made this incident particularly alarming was that it would have been nearly impossible to detect through automated means alone. The attacker had legitimate commit access, contributed real features, and followed normal development workflows. Discovery required deep manual analysis by a security researcher who happened to notice unusual behavior in build logs.

The xz-utils incident highlighted risks in open-source governance:

- Maintainer accounts are high-value targets for long-term compromise
- Reputation-based trust models can be exploited through patient social engineering
- Build systems that use precompiled object files can hide tampering
- Randomized independent rebuilds are one of the few effective defenses against sophisticated backdoors

Codecov: CI/CD as an Attack Vector

In April 2021 Codecov disclosed that its Bash Uploader script had been compromised starting January 31, 2021 [11]. The malicious version exfiltrated environment variables from CI/CD pipelines of affected customers. The attack remained undetected for about 65 days and potentially impacted over 29,000 enterprise customers including Google, IBM, and HP.

The compromise began when an attacker extracted a credential from a Docker image that Codecov had inadvertently published with sensitive data. Using this credential they periodically modified the Bash Uploader script to include code that collected environment variables and sent them to an external server. Customers who ran the uploader in their CI/CD pipelines without verifying its integrity were exposed.

This incident revealed weaknesses specific to CI/CD tooling:

- Scripts downloaded and executed in build pipelines are a high-value target
- Environment variables in CI/CD often contain secrets that attackers can harvest
- Hash verification of external scripts is rarely implemented
- Build-time security is often weaker than runtime security

The Trust Model We Inherited

Modern software development rests on layers of implicit trust that were never designed to be secure. When you run `npm install` or `pip install`, you trust that the package registry has not been compromised and that the maintainer of each package is who they claim to be. When your CI/CD pipeline pulls a base image from Docker Hub, you trust that the image has not been tampered with. When Kubernetes deploys a workload, it trusts that the image digest matches what was approved.

This trust model works well for speed and convenience but poorly for security. It assumes that:

- Package maintainers are legitimate and not compromised
- Registry operators are honest and competent
- Build environments cannot be manipulated
- Cryptographic signatures provide complete assurance
- Downstream consumers will verify upstream integrity

None of these assumptions holds universally. Package maintainer accounts are regularly compromised through phishing. Registries have suffered outages and security incidents. Build environments run with elevated privileges and access to secrets. Signatures can be obtained from compromised systems. And most downstream consumers do not verify upstream provenance because the tooling is not available or too complex to use.

The industry response has been to layer cryptographic verification, transparency logs, and policy enforcement on top of this inherited trust model. The goal is not to eliminate trust entirely but to make it explicit, verifiable, and revocable.

Attack Surfaces Across the Lifecycle

To defend the supply chain effectively, we need a clear picture of where attacks can happen. The following sections map attack surfaces to stages in the software delivery lifecycle.

Source Code Stage

At the source code level, attackers can:

- Compromise developer accounts to push malicious commits
- Submit pull requests with backdoors that get merged through social engineering
- Inject secrets into repositories that are later harvested
- Modify build configuration files to change how artifacts are produced
- Tamper with version tags to redirect consumers to compromised releases

Defense requires branch protection rules, code review requirements, signed commits, and continuous secrets scanning.

Dependency Stage

At the dependency level, attackers can:

- Publish malicious packages that mimic legitimate ones (typosquatting)
- Compromise maintainer accounts and inject code into popular packages
- Exploit dependency confusion to substitute public packages for private internal ones
- Introduce vulnerabilities into widely used libraries that affect all consumers
- Use post-install scripts to execute code during package installation

Defense requires lock files, dependency pinning, automated scanning, and policy enforcement on what packages can be consumed.

Build Stage

At the build stage, attackers can:

- Compromise CI/CD runners to inject malicious code during compilation
- Modify build scripts or configuration to alter output artifacts
- Tamper with base images or build tools used in the pipeline
- Steal secrets from build environments to access downstream systems
- Introduce non-reproducible behavior that hides tampering

Defense requires isolated build environments, reproducible builds, artifact signing, and separation between build and release functions.

Distribution Stage

At the distribution stage, attackers can:

- Tamper with artifacts in transit or at rest in registries
- Compromise registry credentials to push malicious images
- Exploit mutable tags to serve different content over time
- Intercept update mechanisms to deliver compromised versions
- Poison caches that serve artifacts to multiple consumers

Defense requires cryptographic signatures, immutable tags, transparency logs, and verification before consumption.

Deployment and Runtime Stage

At the deployment level, attackers can:

- Deploy unauthorized or unsigned workloads to clusters
- Escalate privileges through misconfigured containers or service accounts
- Exfiltrate data from running applications
- Use compromised workloads as footholds for lateral movement
- Modify configuration at runtime to bypass security controls

Defense requires admission controllers, image verification policies, runtime monitoring, and least-privilege configurations.

Why Traditional Security Fails Supply Chains

Most organizations approach supply chain security by extending existing security practices into new domains. This creates gaps because traditional security controls are not designed for the realities of modern software delivery.

Network perimeter security assumes you can identify and block untrusted traffic. But supply chain attacks come through trusted channels: legitimate package registries, approved CI/CD systems, and signed software updates. Firewalls cannot distinguish between a good update and a malicious one if both come from authorized sources.

Endpoint protection relies on known malware signatures. Supply chain backdoors are custom-written for specific targets and do not match known patterns. The SolarWinds SUNBURST implant evaded detection by major security vendors for months because it was designed to look like normal application traffic [12].

Vulnerability scanning focuses on known CVEs in deployed systems. It does not detect malicious code that has no CVE because it is intentionally harmful rather than accidentally vulnerable. A backdoor in a dependency will not show up as a vulnerability until someone analyzes the code.

Identity and access management controls who can do what but does not control what they actually do. A legitimate developer with proper credentials can introduce a supply chain attack through a compromised laptop, a malicious pull request they did not notice, or a dependency they unknowingly included.

The solution is not to abandon these controls but to add supply chain-specific protections that address their limitations: cryptographic verification of artifacts, provenance attestation for builds, policy enforcement at admission time, and continuous monitoring of runtime behavior. These controls work with traditional security rather than replacing it.

What Comes Next

Understanding the threat landscape is essential but not sufficient. The next chapters will show you how to build defenses against each attack surface we have identified. We start with formal threat modeling to help you prioritize where to invest, then move into specific technical controls for dependencies, builds, artifacts, and deployment. Each chapter includes working code examples and configuration files that you can adapt for your own environment.

The goal is not theoretical perfection but practical improvement. You will not achieve complete supply chain security overnight, and no organization has. But by implementing the controls described in this book incrementally, you can significantly reduce your risk while maintaining development velocity. The tools and patterns are mature enough to work in production today.

Chapter 2: Threat Models and Adversary Playbooks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Threat Actor Profiles

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Nation-State Actors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Criminal Organizations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Insider Threats

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Opportunistic Attackers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

The Software Supply Chain Kill Chain

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Stage 1: Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Stage 2: Weaponization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Stage 3: Delivery

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Stage 4: Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Stage 5: Persistence and Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dependency Confusion and Typosquatting Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dependency Confusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Typosquatting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Build System Compromise Scenarios

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scenario 1: CI/CD Runner Compromise

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scenario 2: Build Script Tampering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scenario 3: Toolchain Compromise

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scenario 4: Supply Chain Pivot

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Modeling Your Own Risk

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Step 1: Identify Assets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Step 2: Identify Threats

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Step 3: Assess Likelihood and Impact

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Step 4: Map Controls to Threats

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Step 5: Validate and Iterate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 3: Securing Dependencies and Package Ecosystems

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Package Ecosystems Work

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

npm (Node.js)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

PyPI (Python)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Maven Central (Java)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Go Modules

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

NuGet (.NET)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Cargo (Rust)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

RubyGems (Ruby)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dependency Confusion Explained and Defended

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How It Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Real-World Example

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Defense Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Detecting Dependency Confusion Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Typosquatting and Malicious Packages

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Common Typosquatting Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Malicious Package Behaviors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Detection and Prevention

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Lock Files, Version Pinning, and Reproducible Resolutions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Lock Files Work

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Best Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Private Registries and Proxy Caching Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Architecture Options

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Implementation Examples

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Security Controls in Private Registries

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Software Composition Analysis (SCA) Tools in Practice

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How SCA Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Tool Comparison

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Implementing SCA in Your Pipeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 4: Secure Source Code and Repository Hygiene

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Branch Protection Rules That Actually Work

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Essential Rules

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Common Mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Code Review as a Security Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Security-Focused Review Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Automating Review Assistance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Review Culture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Secrets Detection in Source

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Tools for Secrets Detection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Implementing a Defense-in-Depth Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Responding to Leaked Secrets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Signed Commits and Tags with GPG/SSH Keys

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Why Sign Commits

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Setting Up GPG Signing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

SSH Key Signing (GitHub)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Enforcing Signed Commits

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Verification

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Repository Permissions and Least Privilege

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Permission Models

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Best Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Pre-Commit Hooks for Security Checks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Setting Up with pre-commit Framework

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Custom Security Hooks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Hook Adoption

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 5: Reproducible and Hermetic Builds

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Makes a Build Reproducible (and Why It Matters)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

The Definition

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Why It Matters for Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Challenges to Reproducibility

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Hermeticity: Eliminating Hidden Dependencies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Why Hermeticity Matters

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Hermetic Builds Work

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Bazel for Reproducible Builds

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Core Concepts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Implementing Reproducible Builds with Bazel

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Testing Bazel Build Reproducibility

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Nix as a Build System and Package Manager

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Core Concepts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Using Nix for Reproducible Builds

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Nix for Development Environments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

BuildKit and Docker Build Reproducibility

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Enabling BuildKit

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Reproducible Docker Builds

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Multi-Stage Builds for Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Testing Your Build Reproducibility

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Automated Reproducibility Tests

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Cross-Environment Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What to Do When Builds Are Not Reproducible

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Trade-offs and Practical Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 6: Artifact Signing and Cryptographic Identity

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

The Math Behind Artifact Signing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Signatures Work

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Signature Algorithms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Signatures Do and Do Not Guarantee

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Key Management Strategies for Organizations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Approach 1: Long-Lived Keys

Approach 2: Short-Lived Keys with Identity Binding

Approach 3: Hybrid

Cosign: Signing Containers and OCI Artifacts

Installation

Key-Based Signing

Keyless Signing

Signing in CI/CD

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Signing Attestations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Fulcio: Certificate Authority for Software Supply Chains

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Fulcio Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Trust Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Self-Hosting Fulcio

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Rekor: Transparency Log for Artifact Signatures

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Why Transparency Logs Matter

How Rekor Works

Using Rekor

Rekor in Verification

Policy Decisions: Long-Lived Keys vs Short-Lived Certificates

Recommended Default

What Comes Next

Chapter 7: Provenance, SLSA, and in-toto Attestations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Is Build Provenance and Why You Need It

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

The SLSA Framework Explained

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

SLSA Tracks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Build Levels

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Source Levels

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Mapping Your Current Pipeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

in-toto Attestation Format Deep Dive

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Envelope Structure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Statement Structure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Predicate Types

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Generating SLSA Provenance in CI/CD

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Using slsa-github-generator

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Using GitHub Artifact Attestations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Generating Provenance for Container Images

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Verifying Provenance Before Deployment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Verifying with slsa-verifier

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Verifying with Cosign

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Integrating Verification into Deployment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Mapping Your Current Pipeline to SLSA Levels

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 8: SBOM Generation, Consumption, and Policy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What an SBOM Is (and Is Not)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

SPDX vs CycloneDX Format Comparison

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

SPDX

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

CycloneDX

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Choosing a Format

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Generating SBOMs Across Ecosystems

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Syft (Anchore)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Grype (Anchore)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Trivy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Microsoft SBOM Tool

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

OWASP Dependency-Track

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Consuming SBOMs for Vulnerability Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Vulnerability Databases

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Integration Example

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

SBOM in Regulatory Context

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

US Executive Order 14028

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

EU Cyber Resilience Act

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Other Regulatory Contexts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Integrating SBOM Generation into CI/CD

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Build-Time SBOM Generation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

CI/CD Pipeline Integration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Publishing SBOMs

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 9: Secure CI/CD Pipeline Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Security Principles for CI/CD Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

GitHub Actions Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

OIDC-Based Authentication

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Workflow Permissions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Environment Protection Rules

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Hardening GitHub Actions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

GitLab CI Security Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Runner Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

CI/CD Variables Protection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dependency Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Jenkins Security Best Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Controller Hardening

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Pipeline Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Plugin Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Azure DevOps Pipeline Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Service Connections

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Variable Groups and Key Vault

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Environment Gates

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Tekton Pipelines for Kubernetes-Native CI/CD

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Architecture Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Tekton Chains for Supply Chain Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Common Mistakes Across Platforms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 10: Secrets Management in the Supply Chain

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Why Hardcoded Secrets Destroy Supply Chain Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

OIDC-Based Authentication for Cloud Providers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How OIDC Federation Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

AWS OIDC Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

GCP Workload Identity Federation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Azure Federation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Vault Integration in CI/CD Pipelines

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Vault Authentication Methods

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Kubernetes Auth for Tekton or In-Cluster Pipelines

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

AppRole for External CI/CD Systems

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dynamic Secrets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Kubernetes Secrets and External Secrets Operator

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Basic Kubernetes Secrets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

External Secrets Operator

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Short-Lived Credentials vs Long-Lived Keys

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Long-Lived Keys

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Short-Lived Credentials

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Migration Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Secrets Scanning and Rotation Automation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scanning in CI/CD

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Automated Rotation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 11: Container Image and OCI Artifact Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dockerfile Security Best Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Multi-Stage Builds

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Non-Root Users

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Minimal Base Images

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Pin Base Images by Digest

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Avoid Secrets in Dockerfiles

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Layer Optimization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Image Scanning in the Build Pipeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scanner Options

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scanning Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

False Positives and Context

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Registry Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Private Registries

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Image Signing in Registries

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

OCI Artifacts Beyond Containers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How OCI Artifacts Work

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Attaching SBOMs as OCI Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

GitHub Attestations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Cosign Policies for Image Verification

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Policy-Based Verification

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Integrating with Deployment Tools

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Immutable Tags and Content Addressing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 12: Kubernetes Supply Chain Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Admission Controllers as Gatekeepers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Admission Control Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

OPA Gatekeeper

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Kyverno

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Choosing Between Gatekeeper and Kyverno

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Image Verification with Cosign Admissions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Sigstore Policy Controller

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Using KMS Keys for Signing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Pod Security Standards and Policies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Pod Security Admission

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Using Kyverno for Enhanced Pod Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Network Policies for Supply Chain Isolation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Runtime Security Monitoring (Falco)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Falco Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Supply Chain-Relevant Falco Rules

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Integrating Falco Alerts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

GitOps Supply Chain Security (Argo CD, Flux)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Argo CD Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Flux Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 13: Infrastructure as Code Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Threat Model for IaC

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Terraform Security Best Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Remote State with Encryption

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Secrets Management in Terraform

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Least Privilege IAM

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Module Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Policy as Code with OPA/Conftest

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How Conftest Works with Terraform

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Example Policies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Integrating with CI/CD

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Cloud Configuration Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Checkov

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

tfsec

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Terrascan

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Choosing a Scanner

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

State File Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Encryption at Rest

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Access Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

State Locking

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Drift Detection and Compliance Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Detecting Drift with Terraform

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Continuous Compliance Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 14: Vulnerability Management and CVE Response

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

How the CVE Ecosystem Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

CVE Creation Process

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

CVSS Scoring

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Limitations of CVSS

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Scanning Strategies: SAST, DAST, SCA, Container Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Software Composition Analysis (SCA)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Static Application Security Testing (SAST)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dynamic Application Security Testing (DAST)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Container Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Prioritizing Vulnerabilities Beyond CVSS Scores

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Factors for Prioritization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

EPSS: Exploit Prediction Scoring System

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

VEX: Vulnerability Exploitability eXchange

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Automated Patching and Dependency Updates

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Dependabot

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Renovate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Choosing Between Dependabot and Renovate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Update Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Incident Response for Supply Chain Compromises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Detection Phase

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Assessment Phase

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Containment Phase

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Remediation Phase

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Post-Incident Phase

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Building a Vulnerability Management Program

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Key Components

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Metrics That Matter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What Comes Next

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Chapter 15: End-to-End Secure Pipeline Implementation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Architecture Overview and Design Decisions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Setting Up the Development Environment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Implementing the GitHub Actions Pipeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Signing and Attesting Artifacts with Sigstore

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Generating SBOMs and Verifying Provenance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Deploying to Kubernetes with Admission Control Enforcement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Monitoring, Auditing, and Alerting Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Troubleshooting Common Issues

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

What You Have Built

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/securesoftwaresupplychains.