

Introduction to Supply Chain Security

Securing the Software Lifecycle with Attestation and the SLSA Framework

The growing risk in software supply chains

Modern software delivery introduces **complex risks across every stage of the software development lifecycle**. Threats target **source code creation** as well as storage, **third-party dependencies** integrated into applications, **CI/CD environments** during while building, and **active operational services** during usage. Securing the software supply chain **requires addressing all four vectors simultaneously** to maintain trust across the entire ecosystem.

- » **Source code integrity risks** stem from unauthorized contributions or unverified code storage facilities.
- » **Third-party dependencies** introduced into applications create unverified vectors of trust.
- » **Without hardened CI/CD pipelines** build environments can be compromised during compilation.
- » Operational services remain **vulnerable during active runtime execution**.
- » Traditional validation relies on **weak or ambiguous sources** of trust like checksums and PGP signatures.
- » Attestation standards like SLSA enable **end-to-end verification of sources, dependencies, and build provenance recursively**.

SLSA Framework & Attestation

SLSA Standard

An open standard backed by industry leaders to establish a standardized verification mechanism.

Provenance Tracking

Generates verifiable metadata to confirm exactly how, where, and by whom artifacts were built.

Source Safeguards

Enforce review processes for protected branches for your version control system.

Hardened Build Platform

Secure isolated CI/CD runners to prevent unauthorized tampering during build.

Registry Policy Gates

Blocks artifact downloads or uploads unless signed attestation proofs are present.

Recursive Verification

Validate the integrity of source code, dependencies, and build outputs across all stages.



How **Adfinis** Can Help



DevSecOps Assessment

We evaluate your development pipelines and security controls to identify vulnerability gaps and map a step-by-step path to compliance with frameworks.



Pipeline Hardening

We configure your CI/CD pipelines with automated artifact signing and provenance tools to support end-to-end cryptographic trust across every build.



Enablement & Managed Care

Our open-source experts upskill your team and deliver continuous 24/7 support to ensure operational resilience and compliance long-term.

Ready to **Secure Your Delivery Pipeline?**

Navigating supply chain security standards can be complex, but you don't have to do it alone. Whether you need an initial **DevSecOps assessment**, hands-on **CI/CD pipeline hardening**, or long-term **operational support**, Adfinis helps enterprise teams **bridge the gap between compliance requirements and real-world execution**. Explore how our open source security experts can help you build uncompromised trust across your **entire software lifecycle**.

Take the Next Step: **Join Our Live Deep-Dive Webinar**

While this guide covers the core principles of SLSA and attestation, putting supply chain security into practice comes with real-world complexities. Join Adfinis expert Lukas Grossar on November 12 for an interactive webinar that goes beyond the basics. We will walk through practical implementation strategies, demonstrate how to harden CI/CD runners against real-world attack vectors, and answer your specific pipeline security questions live.

November 12, 2026 - 11:00 – 12:00 CEST

SIGN UP NOW!

