PRODYNA

Secure Your Software Development Lifecycle

Motivation

Attacks on software supply chains have become one of the most critical threats facing modern enterprises. High-profile incidents such as SolarWinds, Log4Shell and XZ Utils have demonstrated that attackers no longer need to breach your security perimeter. Instead, they infiltrate your systems through the tools, libraries, and pipelines you trust. In response, regulators are introducing new, binding obligations on organizations to demonstrate control over their software supply chain through legislation such as the EU Cyber Resilience Act (CRA), US Executive Order 14028, NIS2, and the EU Digital Operational Resilience Act (DORA).

Achieving this level of trust is not just about the tools used. It requires a holistic approach that covers your source control practices, build pipelines, artifact management, open-source dependency governance and compliance reporting. PRODYNA can help you to navigate this complexity and establish a robust, auditable software supply chain grounded in industry standards such as SLSA and NIST SSDF. This supply chain will be aligned with the practices and tooling promoted by the OpenSSF community.

What We Bring

With over 20 years' experience in delivering enterprise software solutions and cloud-native platforms to some of the world's largest organizations, PRODYNA is well-placed to support your business. Our security engineers and DevSecOps specialists have in-depth, hands-on expertise across the entire security landscape.

- Framework expertise: They have practical experience of implementing SLSA (Supply Chain Levels for Software Artifacts), NIST SSDF (SP 800-218), OWASP SAMM and the OpenSSF Scorecard across a wide range of development organizations
- IaC-driven security: We codify security controls as infrastructure as code to ensure that every hardening measure is reproducible, version controlled, and auditable
- Toolchain integration: We integrate proven open-source and commercial tools into your existing CI/CD environment without disrupting developer workflows.
- Regulatory readiness: We translate compliance requirements (CRA, EO 14028, NIS2 and ISO 27001:2022) into specific technical controls and documentation ready for audits

What You Need

To enable a fast and efficient engagement, your organization should provide:

- Availability of key stakeholders
- Access to CI/CD pipelines and source repositories (e.g., GitHub, GitLab, Azure DevOps)
- Current toolchain inventory – a list of build tools, artifact registries, container base images, and third-party dependencies in use.
- Existing security policies or compliance obligations that should be reflected in the target architecture

Benefits

- **Regulatory readiness:** Implement documented controls that address the supply chain requirements of EU CRA, US EO 14028, NIS2 and ISO/IEC 27001:2022 directly
- **Provable build integrity:** Generate cryptographically verifiable SLSA provenance for your artifact to enable you to prove the integrity of every build
- **Reduced Attack Surface:** Eliminate dependency confusion risks, harden CI/CD pipelines and enforce signed artifact policies across your delivery chain
- **Accelerate your security maturity:** Use our tried-and-tested blueprints and toolchain integrations to achieve in days what would usually take months of iterative trial and error

Quick facts

- **Discovery Workshop:** One day review of pipelines, toolchain, and compliance obligations
- **Assessment & Strategy:** 1–2 weeks to establish SLSA baseline and define the hardening roadmap
- **Implementation (MVP):** 4–6 weeks of hands-on hardening, SBOM toolchain setup, and artifact signing
- **Adoption Phase:** 3–6 months scaling controls, embedding governance, and enabling internal ownership
- **Frameworks:** SLSA, NIST SSDF (SP800 218)

PRODYNA

What You Get

Our phased approach enables organizations to systematically strengthen their software supply chain, implement audit-ready compliance controls and foster internal ownership of security practices, balancing immediate gains with long-term sustainability.

PRODYNA will guide you and your staff through the process, which is divided into the following phases:

PHASE	ACTIONS
Discovery Workshop (1 day)	• Map current CI/CD pipeline architecture and identify critical paths • Review existing dependency management and artifact handling practices • Assess compliance obligations (CRA, EO 14028, NIS2, ISO 27001) • Identify quick wins and high risk areas for prioritization
Assessment & Strategy (generally 1-2 weeks)	• Establish SLSA maturity baseline across key pipelines • Evaluate current SBOM generation capabilities • Define target state and hardening roadmap • Align stakeholders on priorities and success criteria
Implementation of MVP (typically 4–6 weeks)	• Implement SBOM generation and artifact signing • Harden CI/CD pipelines according to SLSA requirements • Integrate vulnerability scanning and dependency governance • Establish provenance attestation workflows • Document controls for audit readiness
Adoption Phase (typically 3–6 months)	• Scale hardening patterns across additional pipelines • Embed governance processes and ownership • Train internal teams on tools and practices • Establish metrics and continuous improvement cycles • Enable internal leadership of supply chain security

Note: This is our standard methodology. We are happy to modify and adapt to the specific needs of your organization.

Get Started

To learn about pricing and how to get started, please contact info@prodyna.com.

About PRODYNA

PRODYNA is a technology consulting and software engineering company that helps organizations create business value through AI, cloud, data, and custom digital platforms, delivering solutions from strategy through implementation and operation.