Build a Secure Software Supply Chain with VMware Tanzu Labs

Implement processes and tooling that enable your teams to ship software continuously with confidence.

Modern technologies and development methodologies enable your organization to ship new apps and features faster than ever before. Embracing cloud native and open source technologies often means accepting more dependencies in your code while also boosting developer velocity, resulting in pushing code to production faster and more frequently.

451 Research, part of S&P Global Market Intelligence, surveyed hundreds of enterprises and found that 63 percent of enterprises listed data protection and security as a top IT challenge and 42 percent listed governance and compliance.

Maintaining high developer productivity and leveraging cloud native open source technologies while delivering code securely, reliability and consistently requires a highly automated, closed loop delivery system. Security culture and practices must evolve to take advantage of automation and embrace a shared ownership of security across development, operations and security teams.

VMware Tanzu Labs consulting service helps you improve automated tooling and implement DevSecOps practices. Ship high quality code securely, reliably and consistently to production and fix security vulnerabilities faster.

A holistic approach to your software development supply chain

We’ll work with you to address the tooling, people and process considerations necessary to develop and deploy secure software continuously. We’ll help you optimize your existing tools or implement new tooling, and adopt modern governance and development practices that result in a more secure, consistent, closed-loop delivery system. We’ll implement a solution centered around these principles:

- **Code is simply and consistently delivered to production** as a frictionless and familiar extension of a developer’s workflow.
- **New software is easily and consistently onboarded** onto this delivery mechanism. All code flows through a standardized chain to production. There are no one-off delivery mechanisms.
- **Developers can easily interact with the supply chain** to investigate and fix delivery failures, as well as augment the system as needed.
- **The software delivery mechanism is secure** and adheres to the same security constraints as the software itself. An organization may restrict actions through role-based policy, certify software artifacts, audit production system modifications, and address runtime vulnerabilities.

> “We still often see security separated from the teams delivering software. To ensure we maintain robust security without compromising development velocity, we need new approaches, engineering practices, and tools. But most of all, we need to encourage better collaboration between security specialists and delivery teams.”

HANNAH FOXWELL
DIRECTOR, PLATFORM SERVICES
VMWARE TANZU LABS

BUILD A SECURE SOFTWARE SUPPLY CHAIN WITH TANZU LABS

- Automate and streamline your path to production for secure, reliable and consistent software delivery.
- Gain knowledge, skills and adopt practices necessary to successfully implement a DevSecOps model of continuous delivery.

Contact your VMware account team or reach us at *tanzu.vmware.com/labs*.

[1] 451 Research’s Voice of the Enterprise: Cloud, Hosting and Managed Services, Workloads & Key Projects, 451 Research, Part of S&P Global Market Intelligence, June 2021.

CREATE A CULTURE OF DEVSECOPS

Read about our approach to helping create a more collaborative culture between security specialists and delivery teams. *Read the blog* and find more on Tanzu's approach to DevSecOps and secure software supply chain *here*.

OWN YOUR APP MODERNIZATION JOURNEY

Learn how we help organizations around the world deliver business outcomes with modern apps and cloud native platforms at *tanzu.vmware.com/customers*.

Here's what we'll do together

We'll start with a detailed assessment of your current path to production to identify opportunities to improve security, speed and scalability. Then, we'll tailor your engagement to address your specific needs and goals across every stage of your software supply chain:

- **Secure app source code:** We'll enable developers to develop high quality code following security best practices covering topics such as code reviews, maintenance and access control of source code repo, regular scans and audit checks, and eliminating secrets from source code.
- **Dependency management:** Modern apps leverage hundreds (or more dependencies. These allow dev teams to build applications faster but also |introduces a lot of code that your teams didn't write. It's easy to become a victim of a vulnerability in third party code. We'll enable developers to fully understand their bill of materials, know how to acquire code libraries from trusted sources, and quickly patch their app dependencies when new vulnerabilities are discovered.
- **CI/CD Build Systems:** We'll help you implement practices to consistently test and scan code changes for vulnerabilities using automation before code is packaged. This includes implementing practices such as automated continuous integration, code linting, testing and scanning, Source Composition Analysis (SCA), Dynamic App Security Testing (DAST), and credential rotation. When a vulnerability is identified, you'll have the tooling needed to easily rebase on a newer version of a dependency.
- **Secure image build and registry:** Practices and processes will be implemented to guarantee the integrity of your application images, to store images in a secure registry and to scan images regularly for security vulnerabilities. Key steps are taken to create proper controls, harden and secure images for app developers.
- **Secure runtime environment:** Ensure that only what you've produced is running in production by securing your runtime infrastructure. We'll institute practices that promote workload isolation so that neighboring workloads cannot exploit other workloads and communications between services over your network are safe and reliable.

Let's go!

Together we'll assess your needs, develop a strategy tailored to meet your security, business and IT goals. Then, we'll get to work implementing tooling, practices and organizational changes to secure your software supply chain. Contact your VMware account team or reach us at *tanzu.vmware.com/labs*.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com