Supply Chain Security & Kubernetes

How to use Tekton to secure your Supply Chain

Carmelo Sarta
Technical Account Manager

Valerio Muredda
Technical Graduate

Red Hat

What we'll discuss today

- What's a Supply Chain
- How does Tekton help us
- Tekton Chains Demo
- Conclusions
- ~~Don't~~ Do it at home!

What's a Supply Chain

And why do we need to secure it

The Supply Chain of a software is about everything (and everyone) that touches your code during the software development lifecycle (SDLC). It includes information about the application, like:

- The infrastructure used for its deployment
- Its dependencies
- Its **vulnerabilities**

Source:
https://foojay.io/today/evolving-landscape-software-supply-chains-java-developers/

Our dependencies are often vulnerable

A case for Log4J

"The Log4J download numbers show that even after almost two years since the first occurrence of Log4Shell and with a massive 250 Million downloads - about ⅓ of them are for Log4J versions that contain the vulnerability."

Source:
https://www.sonatype.com/state-of-the-software-supply-chain/introduction

How does Tekton help us

Optional subheading

Tekton is an open-source framework for creating CI/CD systems. A few years ago Tekton introduced Chains, a component that monitors all task run executions in a Kubernetes cluster.

Tekton Chains

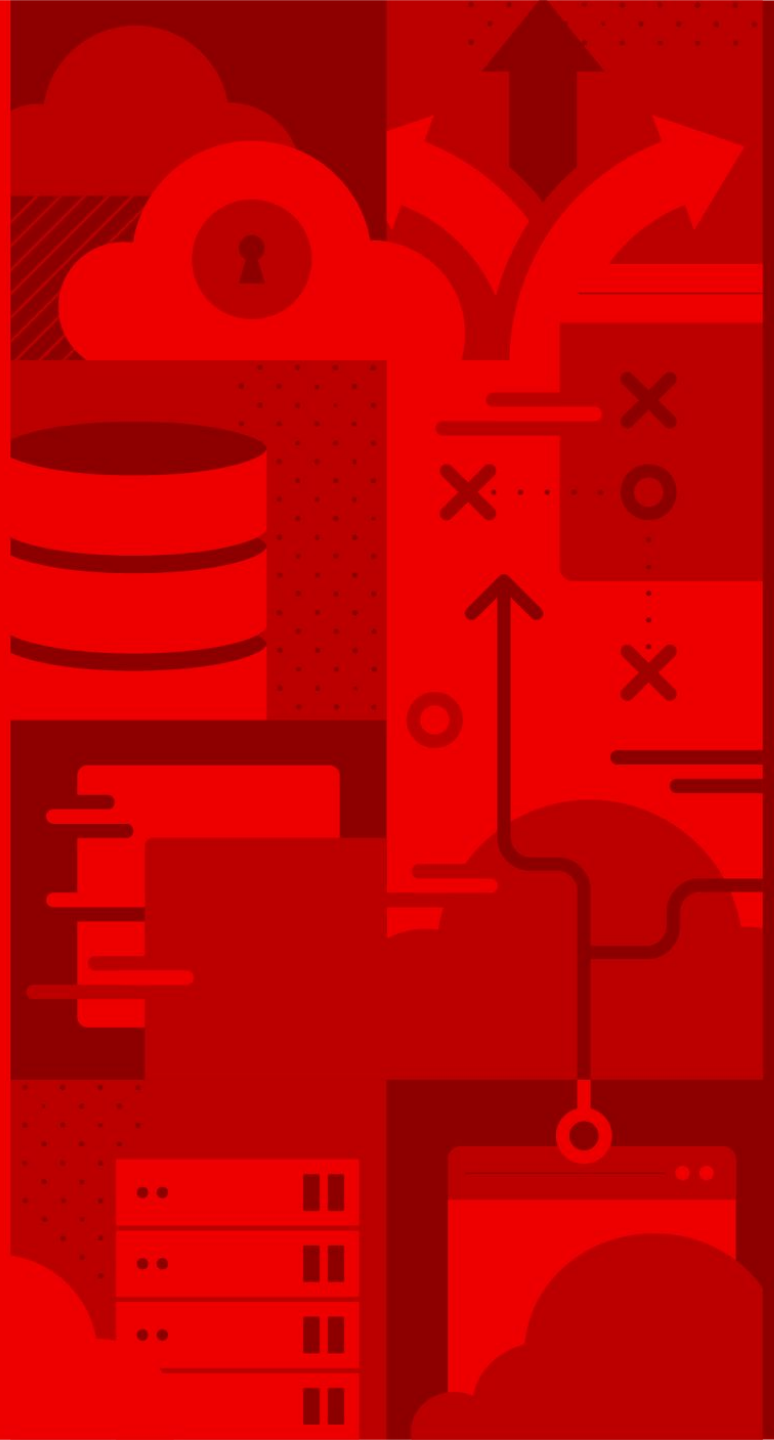
Main features:

- Signing task runs, task run results, and OCI registry images with cryptographic keys.
- Using attestation formats.
- Securely storing signatures and signed artifacts using OCI repository as a storage backend.

SLSA

Level	Description	Example
1	Documentation of the build process	Unsigned provenance
2	Tamper resistance of the build service	Hosted source/build, signed provenance
3	Extra resistance to specific threats	Security controls on host, non-falsifiable provenance
4	Highest levels of confidence and trust	Two-party review + hermetic builds

Source:
https://slsa.dev/spec/v0.1/levels



DEMO

Using Tekton Chains to sign and verify image and provenance

Red Hat

Conclusions

Red Hat

~~Don't~~ Do it at home!

Components used:

- RH Openshift v4.13.12
- RH pipeline operator v1.12.1 (Tekton)
- Cosign v2.1.1
- Rekor-cli v1.2.2

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat