IS YOUR SOFTWARE SUPPLY CHAIN SECURE?

BY SHIVASWAROOP N K

WHO AM I?

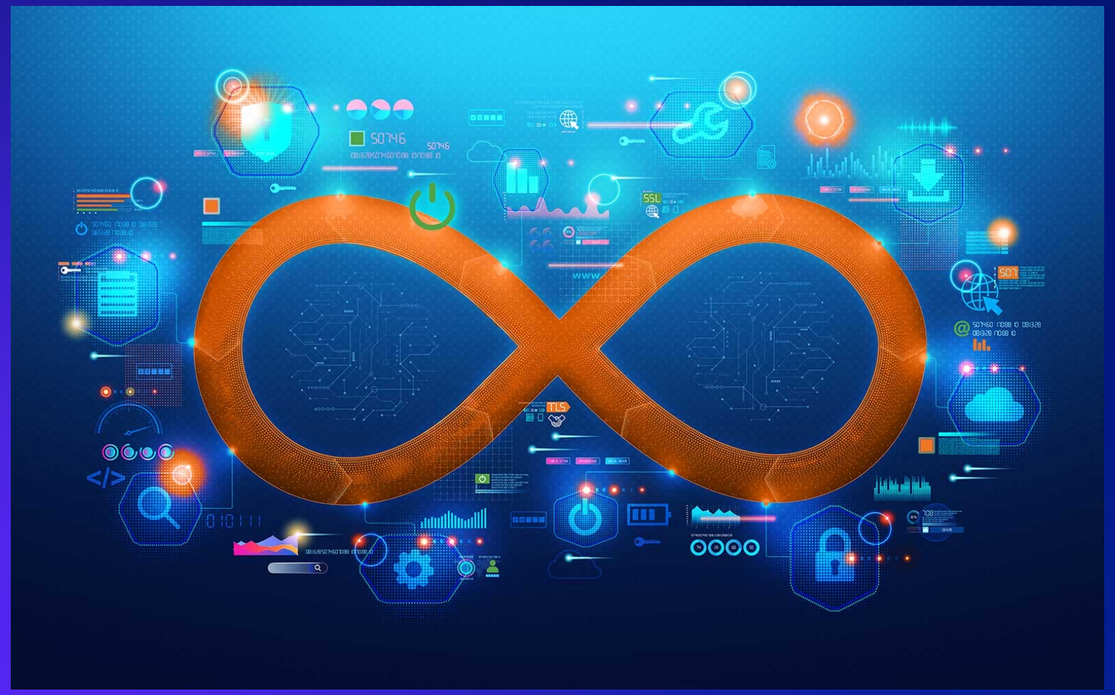
WHO IS THIS FOR?

WHAT IS A SOFTWARE SUPPLY CHAIN?

> End-to-End Workflow

> Security and Integrity

> Automation and Compliance



WHAT IF YOUR SOFTWARE SUPPLY CHAIN WAS COMPROMISED TOMORROW?

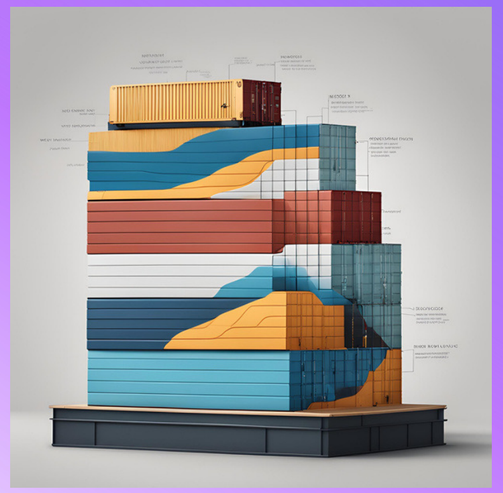
Vulnerability	Main Damage	Impact
Windows 10 (CrowdStrike)	System compromise, RCE, data theft	Enterprise systems vulnerable
XZ Utils	Code execution, DoS	Targeted Linux Systems
Log4j	RCE, botnets, cryptojacking, supply chain attacks	Global, Widespread impact
Heartbleed	Data leakage (keys, passwords)	Millions of Websites affected
Dirty Pipe	Privilege Escalation, Server Compromise	Critical Linux Environments

PRIMARY OBJECTIVES

Software Supply Chain

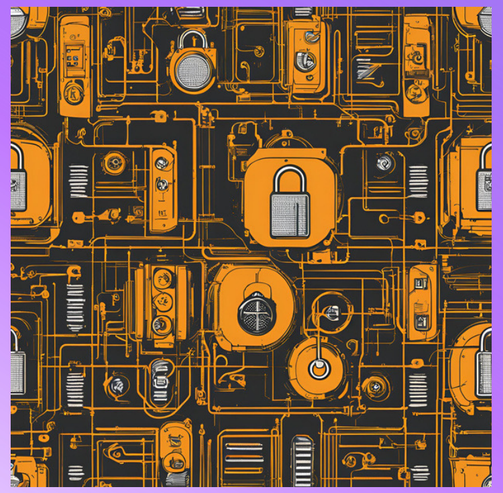
Zero CVE Base Image

(Almost)



Robust Systems

Signed and Verified Artifacts



CAN WE ACHIEVE ZERO CVEs?

> Chainguard

> Buildsafe

> Trivy/Snyk

ARE OUR SYSTEMS SECURE?

> Network Isolation

> Role Based Access Control (RBAC)

> Access Control Lists (ACL)

WHAT DOES SIGNING AN ARTIFACT ACHIEVE?

> Integrity

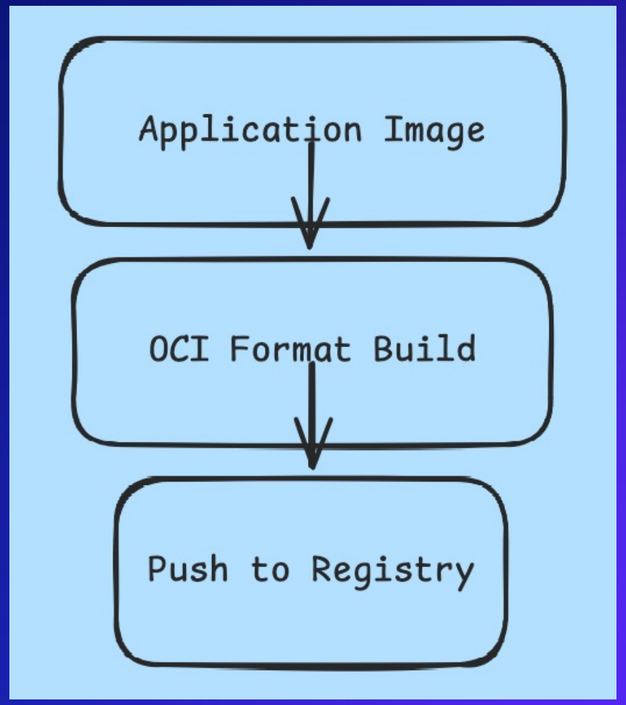
> Authenticity

> Provenance

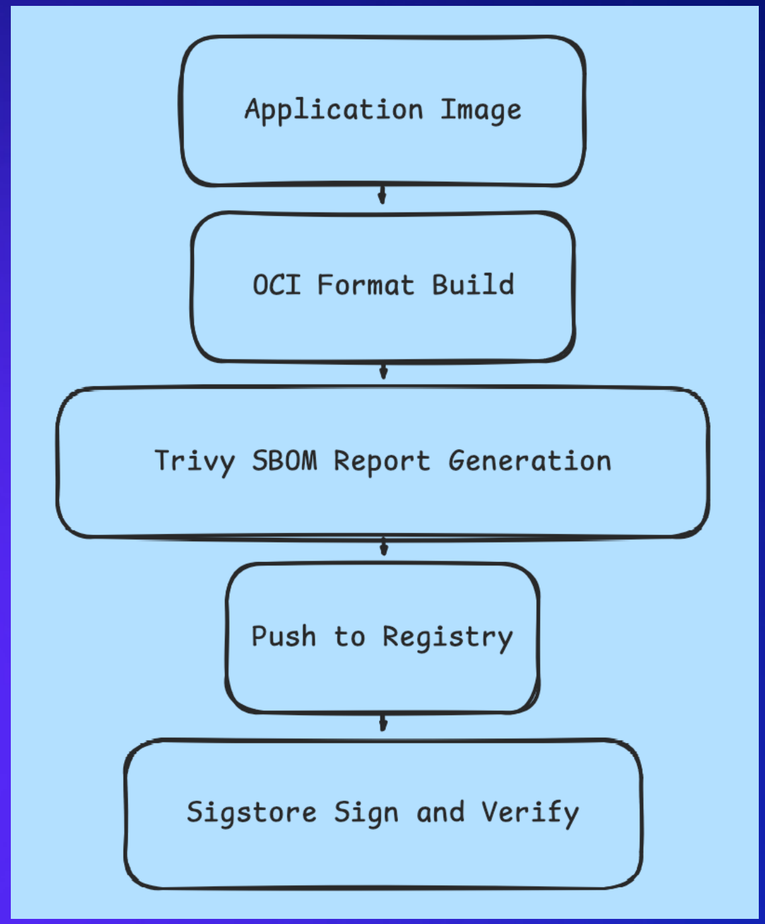
DEMO TIME

GITHUB ACTIONS FLOW

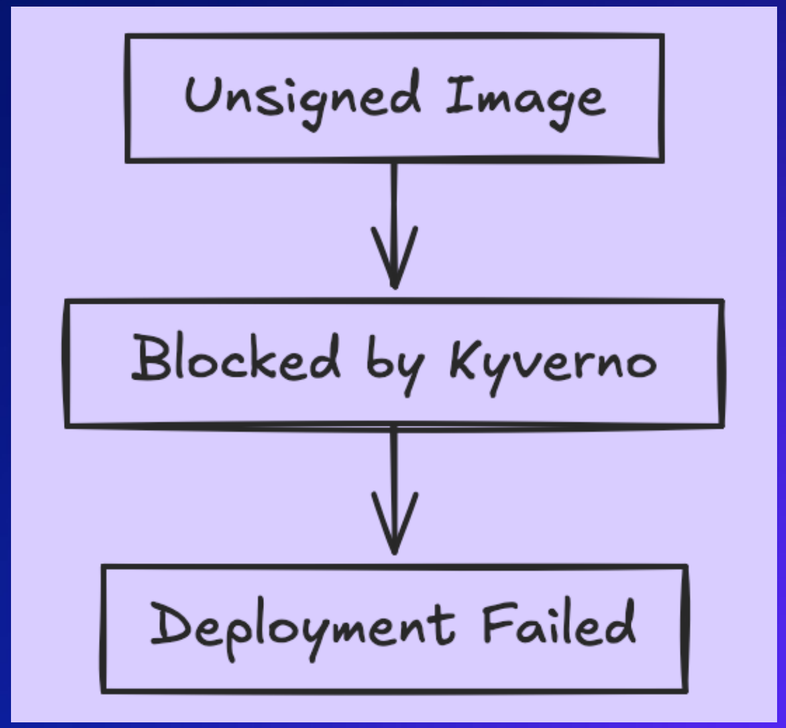
Unsigned Image

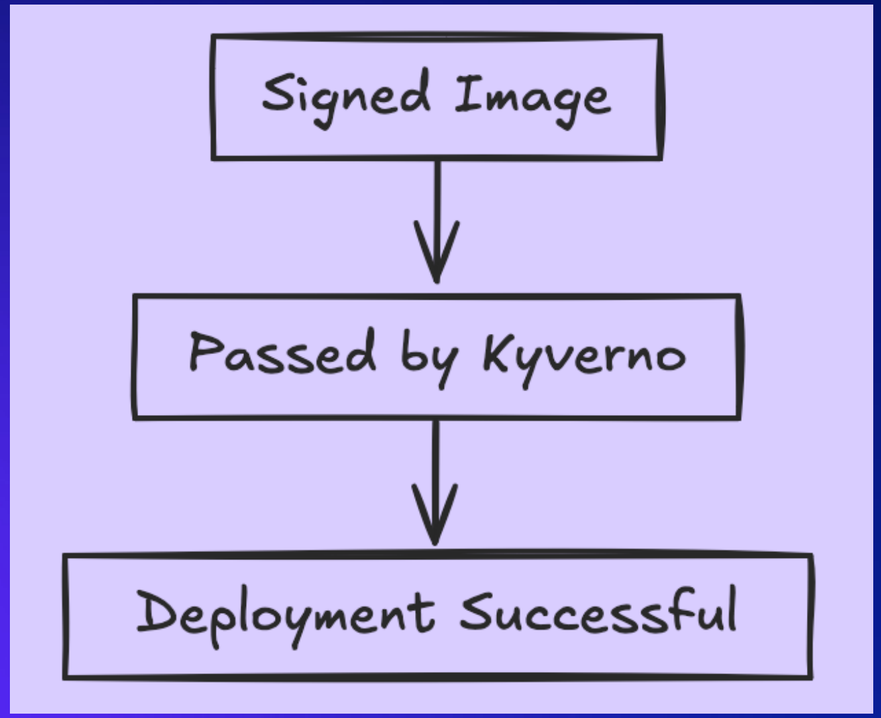


Signed Image



DEPLOYMENT FLOW





ADDITIONALLY..

> Scans using Private LLMs

> Supply-Chain levels for Software Artifacts (SLSA)

- Software Bill of Materials (SBOM)

- Attestations

REFERENCES

> LinkedIn: Saiyam Pathak Newsletter: https://www.linkedin.com/pulse/supply-chain-security-kubecon-india-saiyam-pathak-nxq6c

> Sigstore with Kyverno: kyverno.io/docs/writing-policies/verify-images/sigstore/

> Buildsafe: buildsafe.dev

> SLSA: slsa.dev

> Scaling up Supply Chain Security: https://openssf.org/blog/2024/02/16/scaling-up-supply-chain-security-implementing-sigstore-for-seamless-container-image-signing/

AI Amuse


SECURE SOFTWARE SUPPLY CHAIN
A SECURE SUPPLY CHAIN
A SECURE SUPPLY CHAIN
PLANNING
DEVELOPMENT
CODE
SECURITY
SECURITY LAYERS
BUILDING
TESTING
DEPLOYMENT
GIT
DEVELOPING
DEPLOYING
SECURITY LAYERS


A SECURE SOFTWARE SUPPLY CHAIN
PLANNING
DEVELOPMENT
SECURITY
SECURE SOFTWARE SUPPLY CHAIN
DEVELOPMENT SUPPLY CHAIN
TESTING
DEPLOYMENT
SECURE SOFTWARE SUPPLY CHAIN

THANK YOU!

FEEDBACK

LINKEDIN

GITHUB