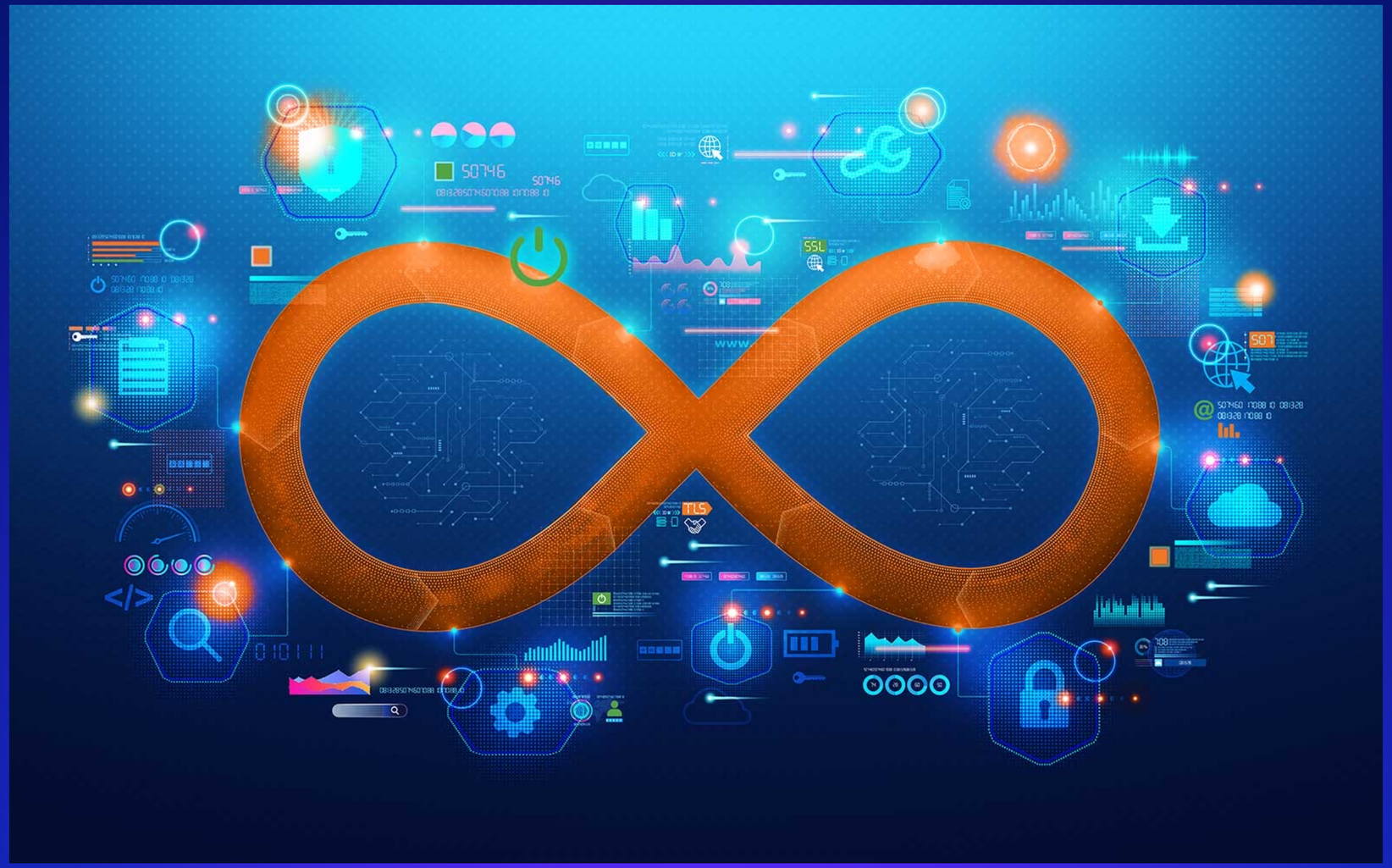
IS YOUR SOFTWARE SUPPLY CHAIN SECURE?

By Shiva Swaroop N K

LINKEDIN

GITHUB

What is a Software Supply Chain?

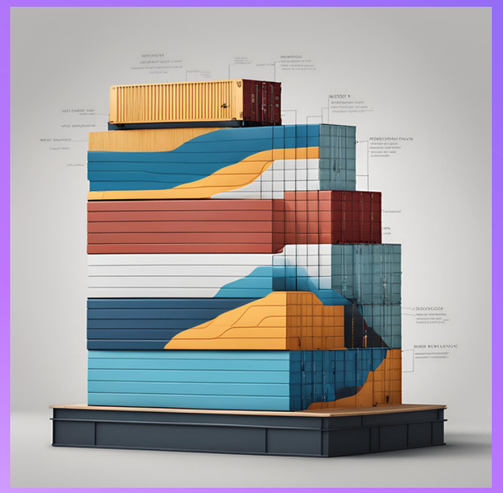


WHAT IF YOUR SOFTWARE SUPPLY CHAIN WAS COMPROMISED TOMORROW?

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

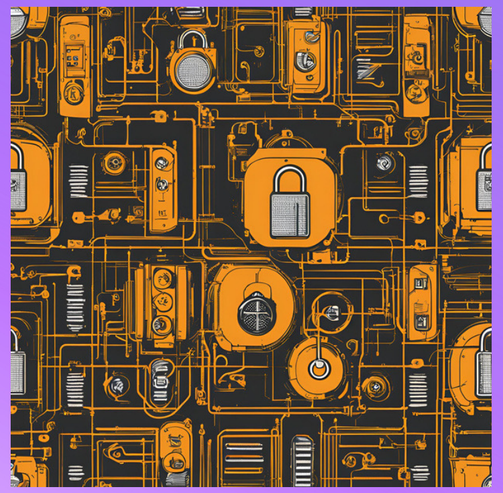
PRIMARY OBJECTIVES

0 CVE BASE IMAGE



ROBUST BUILD SYSTEMS

SIGNED AND VERIFIED ARTIFACTS



CAN WE ACHIEVE (almost)0 CVE?

- CHAINGUARD
- BUILDSAFE
- TRIVY/SNYK

ARE OUR SYSTEMS SECURE?

- NETWORK ISOLATION
- RBAC
- ACL

WHAT DOES SIGNING AN ARTEFACT ACHIEVE?

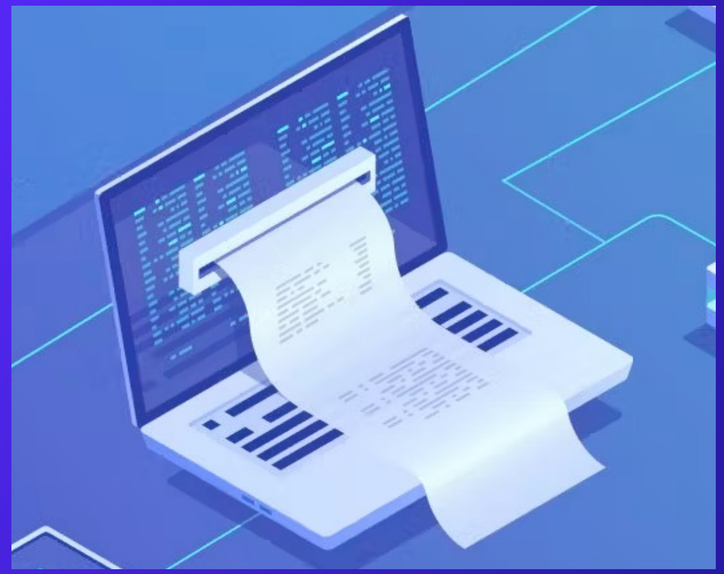
AUTHENTICITY

INTEGRITY

DEMO TIME

ADDITIONALLY..

- SBOM
- ATTESTATIONS
- LLMS
- Exposure Queries



THANK YOU!

LINKEDIN

GITHUB

REFERENCES

- LinkedIn: Saiyam Pathak Newsletter
- Sigstore with Kyverno
- Buildsafe

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