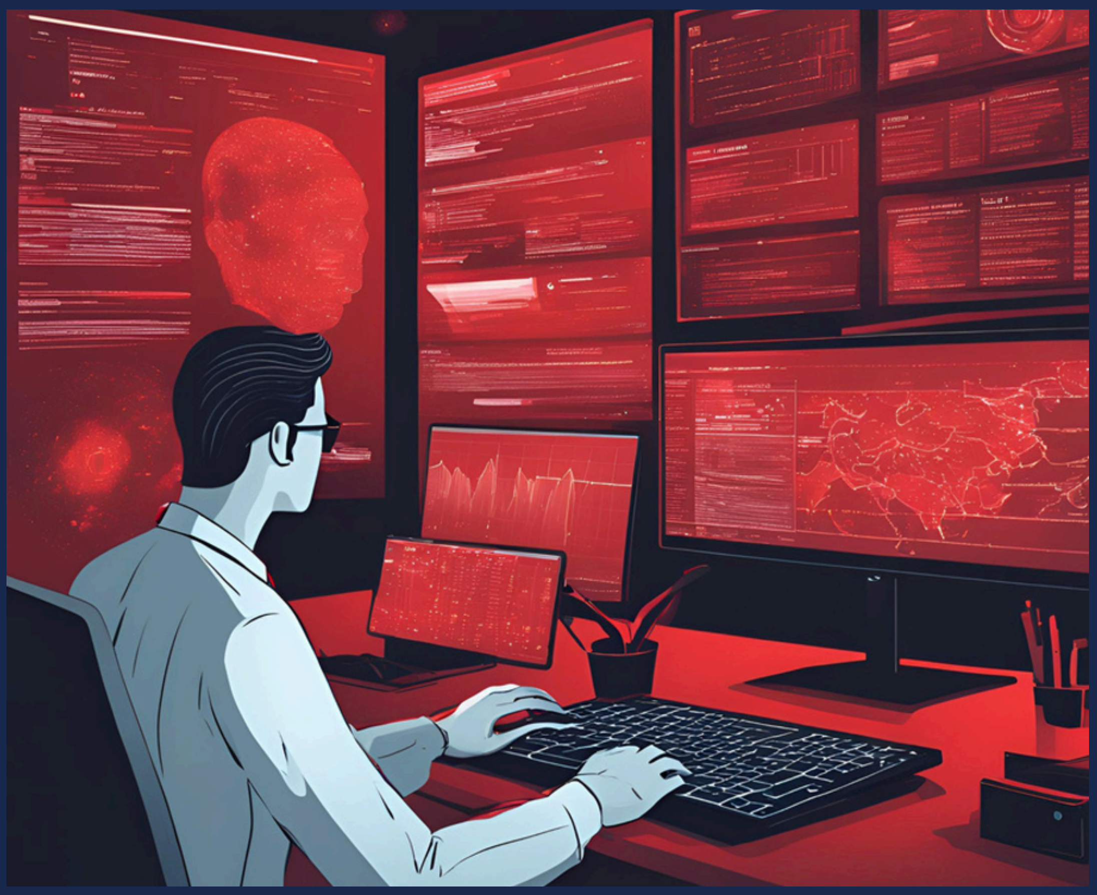
# IS YOUR SOFTWARE SUPPLY CHAIN SECURE?

SHIVASWAROOP N K
KTH

## WHAT IS IT?

The software supply chain is an End-to-End Workflow. It emphasizes Security and Integrity as well as Automation and Compliance



## WHY DO WE NEED IT?

The primary objectives of securing the software supply chain include aiming for an Almost Zero CVE Base Image, ensuring Signed and Verified Artifacts, and establishing Robust Systems

## WHAT HAPPENS IF NOT?

If we don't implement software supply chain security, we risk our supply chain being compromised, potentially leading to Vulnerability Main Damage Impact

GITHUB LINK

LINKEDIN

## HOW CAN WE SECURE IT?

- Aiming for an Almost Zero CVE Base Image using tools like Chainguard, Buildsafe, and Trivy/Snyk.
- Ensuring Signed and Verified Artifacts to guarantee Integrity, Authenticity, and Provenance, potentially using Sigstore with Kyverno
- Establishing Robust Systems through Network Isolation, Role Based Access Control (RBAC), and Access Control Lists (ACL).
- Adopting practices like Supply-Chain Levels for Software Artifacts (SLSA) with Software Bill of Materials (SBOM) and Attestations