The (Bad) Headlines

CSO

SolarWinds Shines Spotlight on Supply Chain Risks

HEIMDAL™ SECURITY

HashiCorp Affected by A Security Breach That Occurred Due to A Codecov Supply-Chain Attack

The Company Has Disclosed Exposure of GPG Signing Key Following the Codecov Attack.

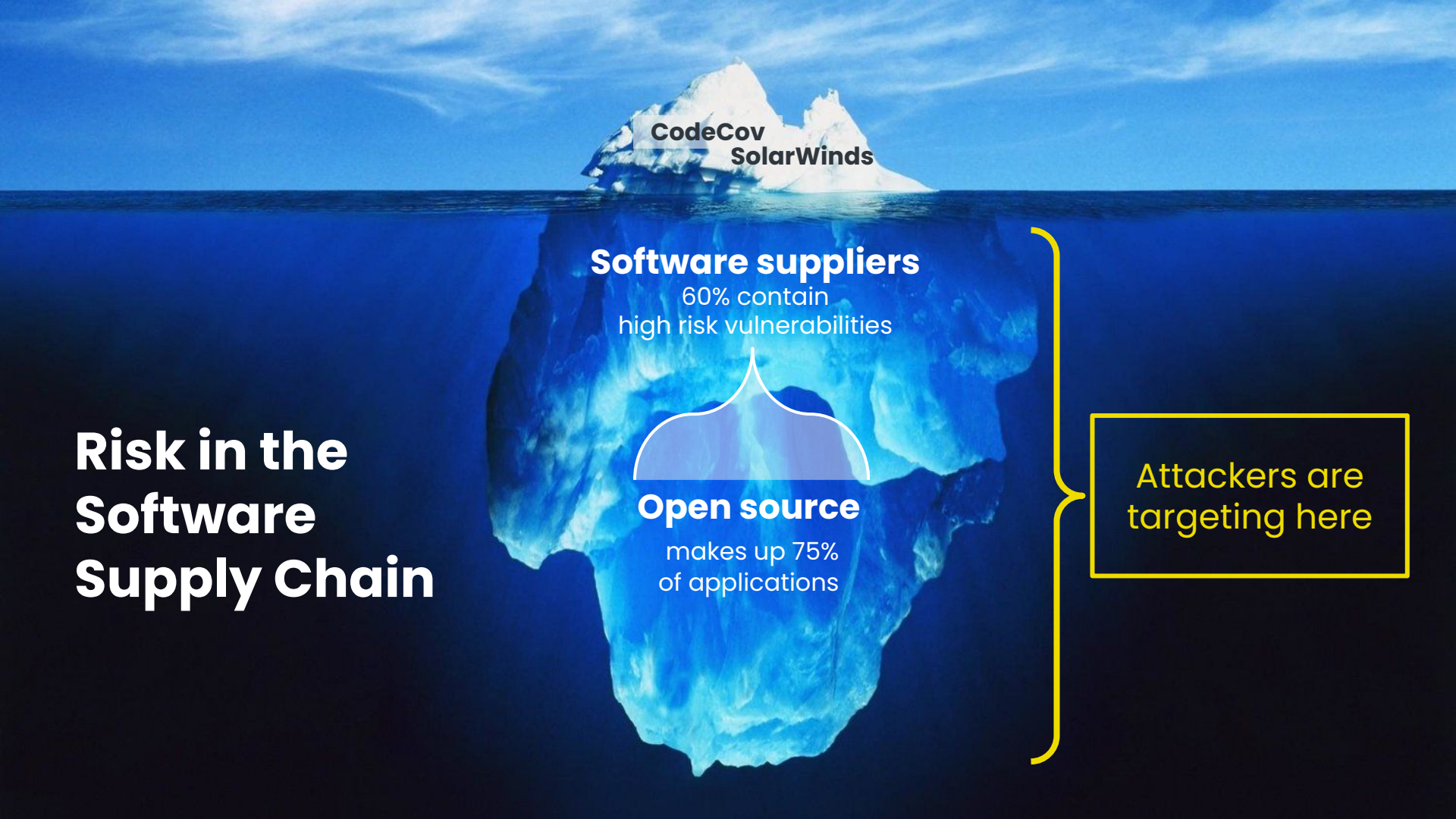
New type of supply-chain attack hit Apple, Microsoft and 33 other companies

ars technica

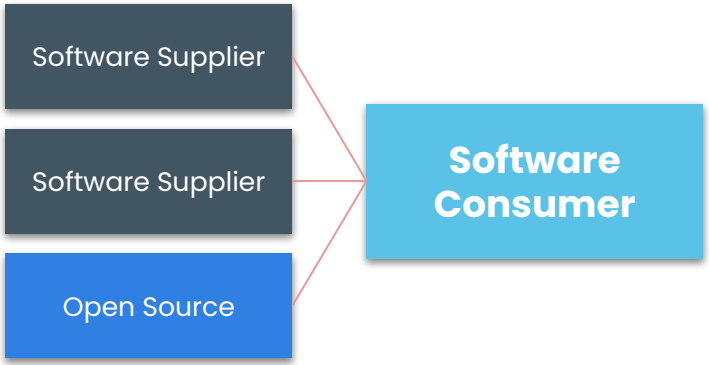
Supply chain attacks are on the rise: Check your software build pipeline security

ZDNet

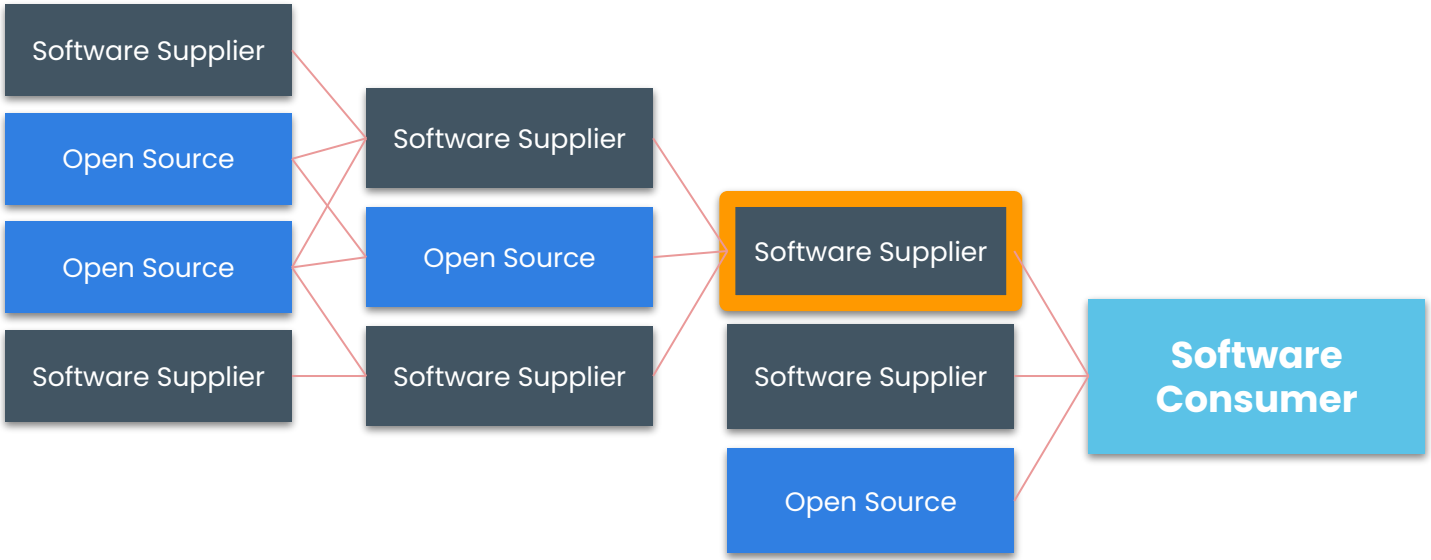
Risk in the Software Supply Chain



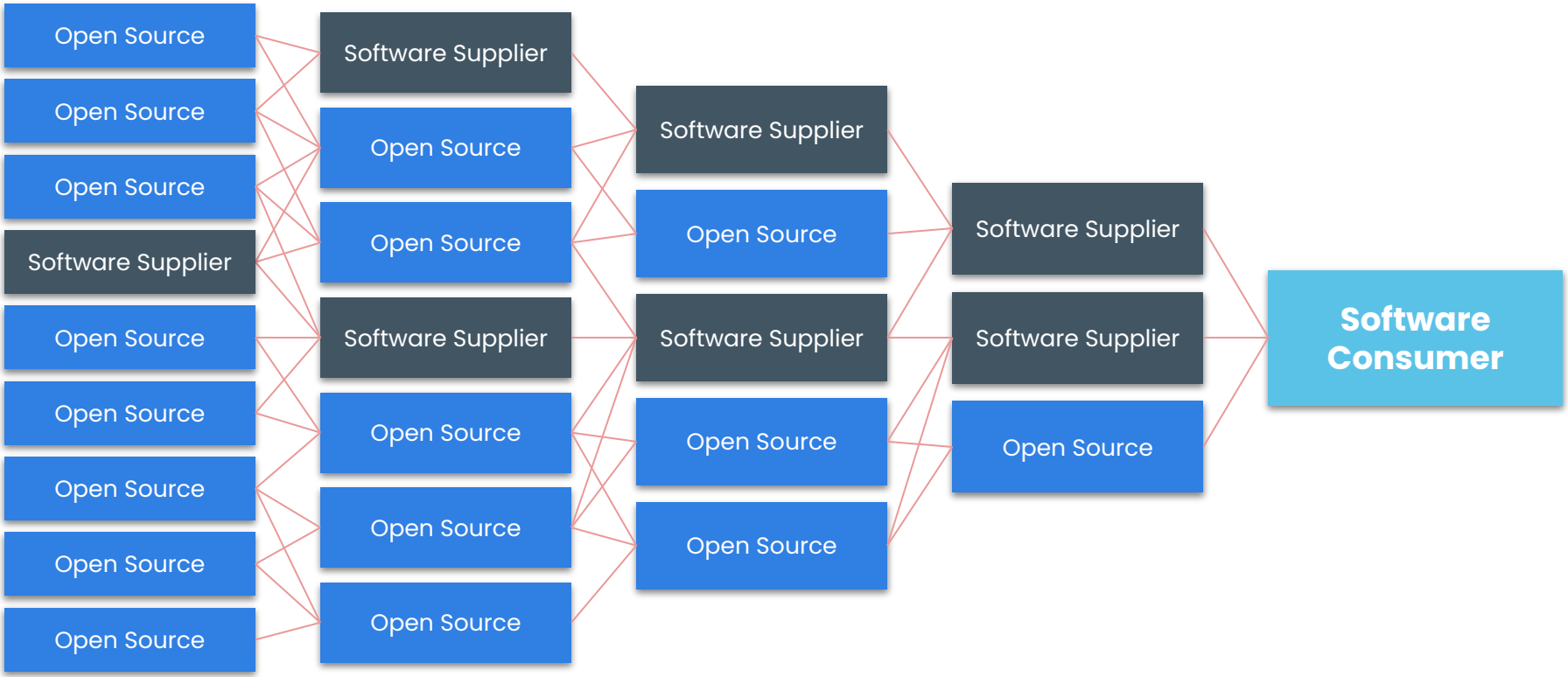
Software Supply Chain: Consumer View



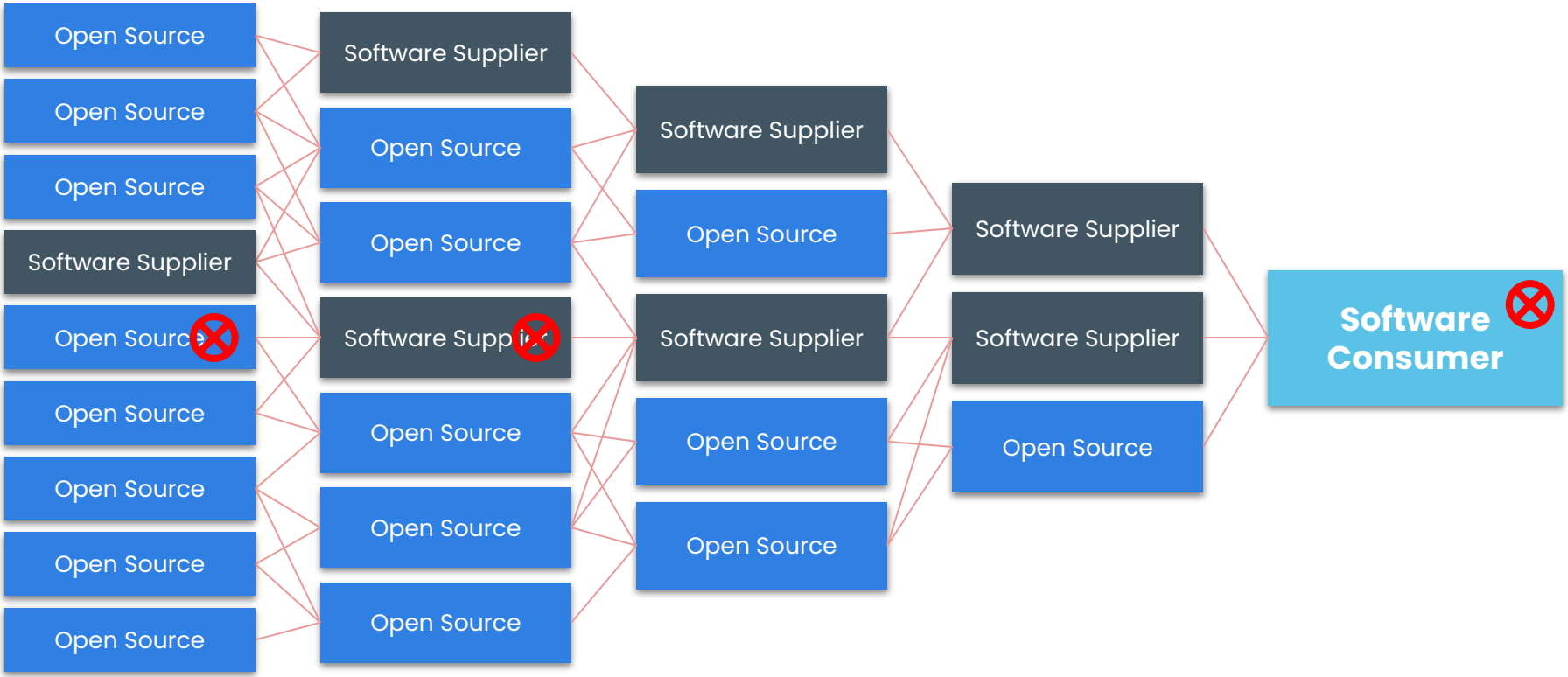
Software Supply Chain: Supplier View



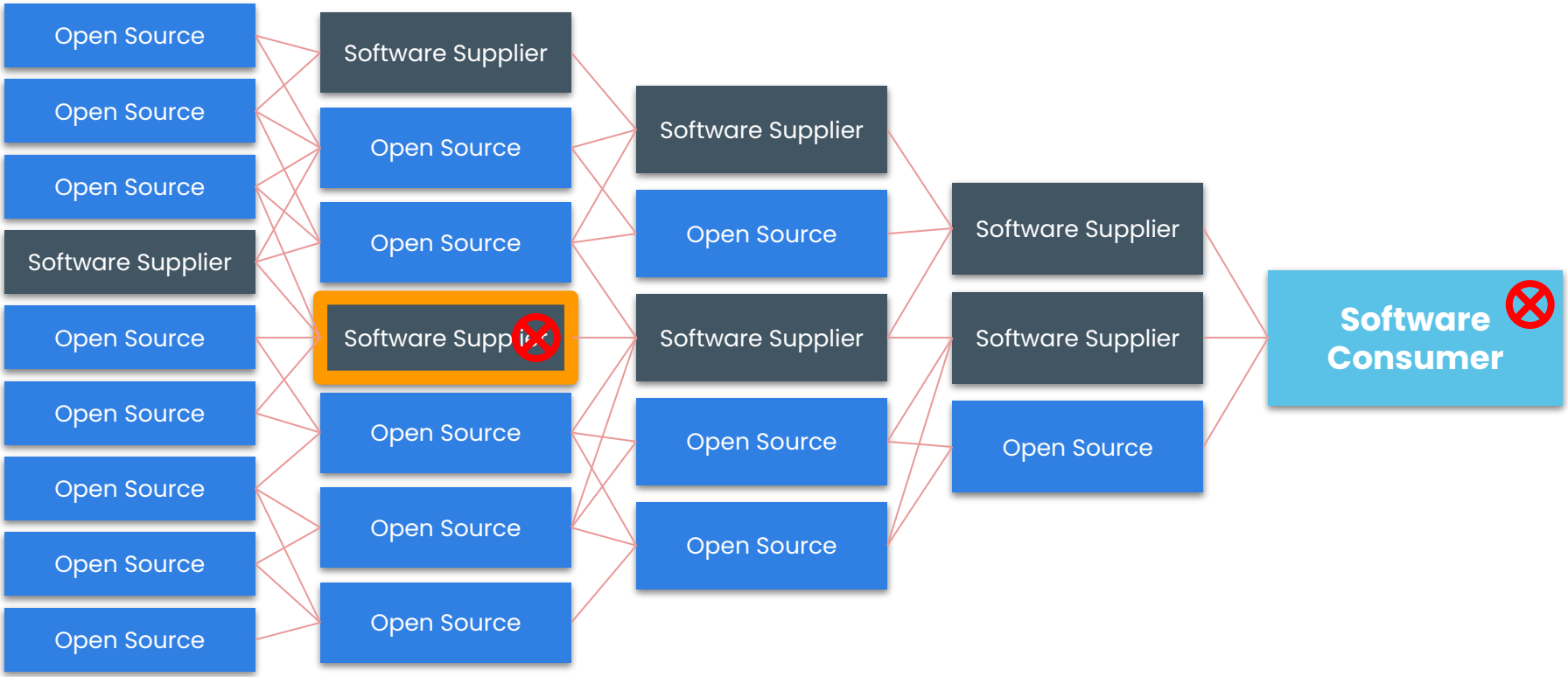
Software Supply Chain: Global View



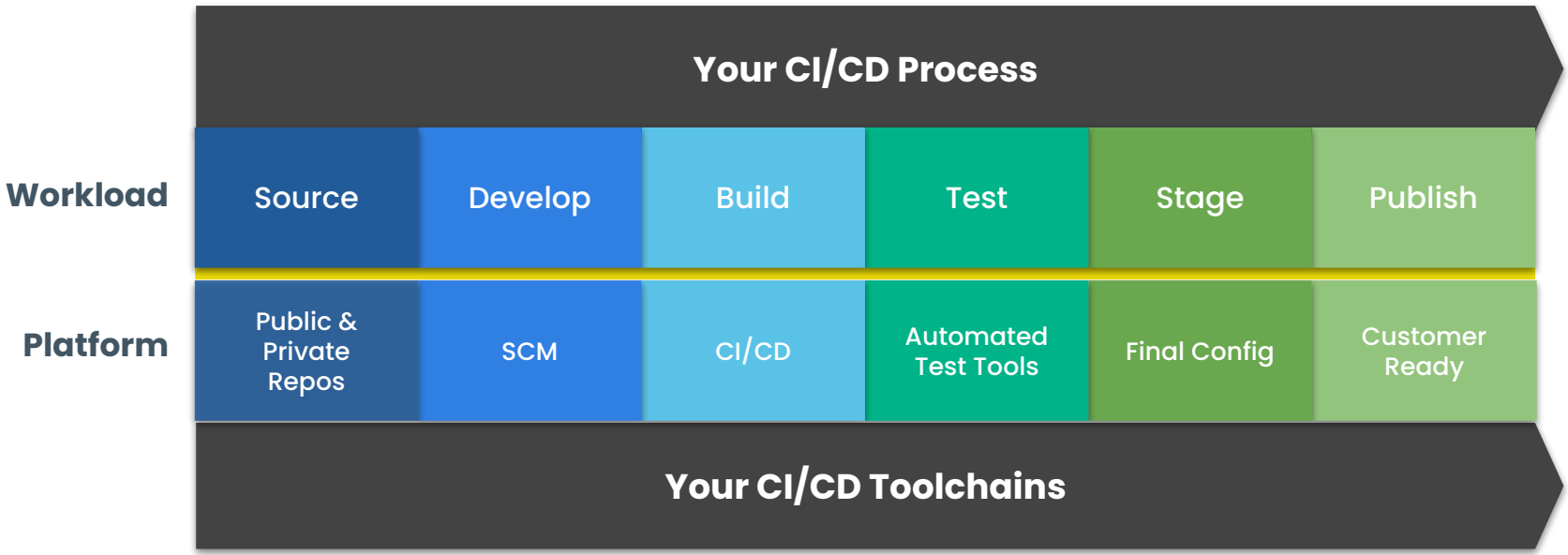
Software Supply Chain



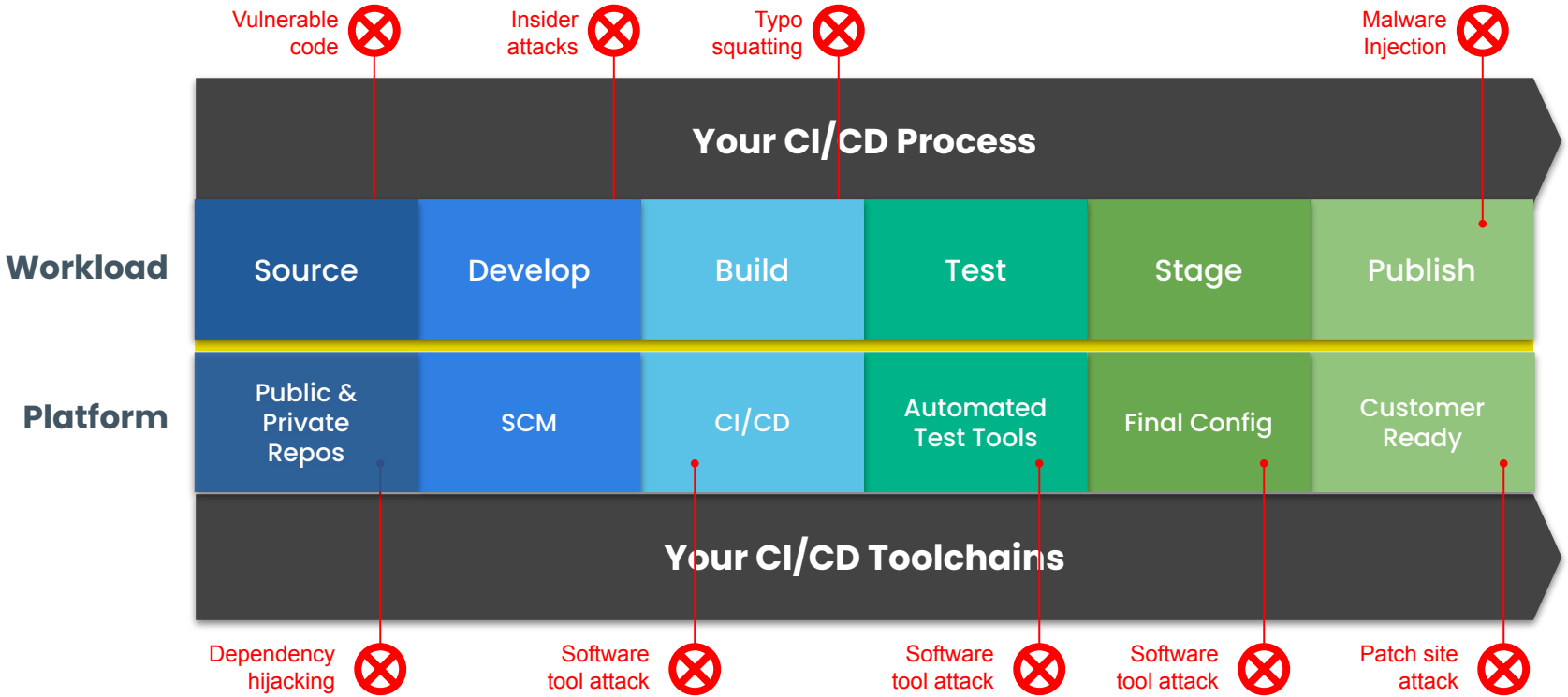
Software Supply Chain



Software Supplier DevOps Toolchain

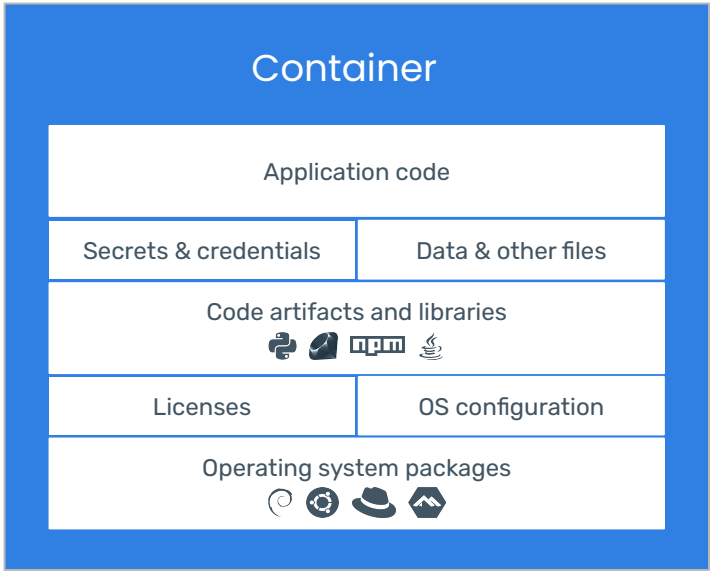


Security Risks Can Enter Anywhere



Containers Provide

...an easy way to package and deliver



...a potential source of security risks

...an opportunity to 'shift-left' security enforcement

Beyond the CVE: Container Exposures

01

Software Vulnerabilities

Known vulnerabilities affecting software components that container/applicatio n depends on - OS packages, directpplication dependencies.

02

Malware and Trojan Horses

Malicious code injected into regular application executables during build process.

03

Software Overrides

Attacks that result in unintentional versions of (typically) dependencies being installed. Name-squatting, max version attacks, typo-squatting.

04

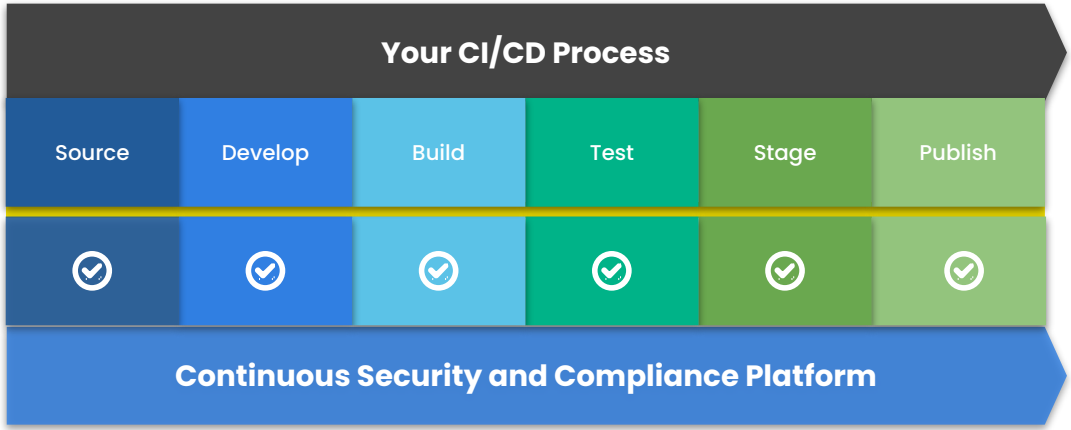
Credentials

Unintentional inclusion of dev or prod secrets, keys, or other credentials accidentally included in the container.

Software vulnerabilities (often reported as CVEs) are critical to detect and report, but many other build-time attack vectors must also be considered.

How to Secure your Software Supply Chain

Embed **continuous security and compliance** checks in every step of your software development process enabling quicker, easier, and lower cost remediation



Best practices for securing supply chain

01 Centralized, secure CI/CD process for all software

02 Build images from trusted sources

03 Automate security testing and policy enforcement

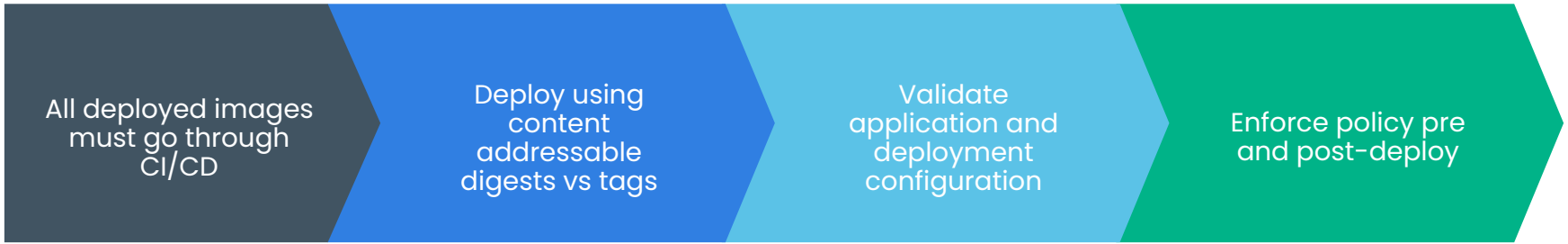
04 Deploy only trusted images into production

Secure CI/CD processes

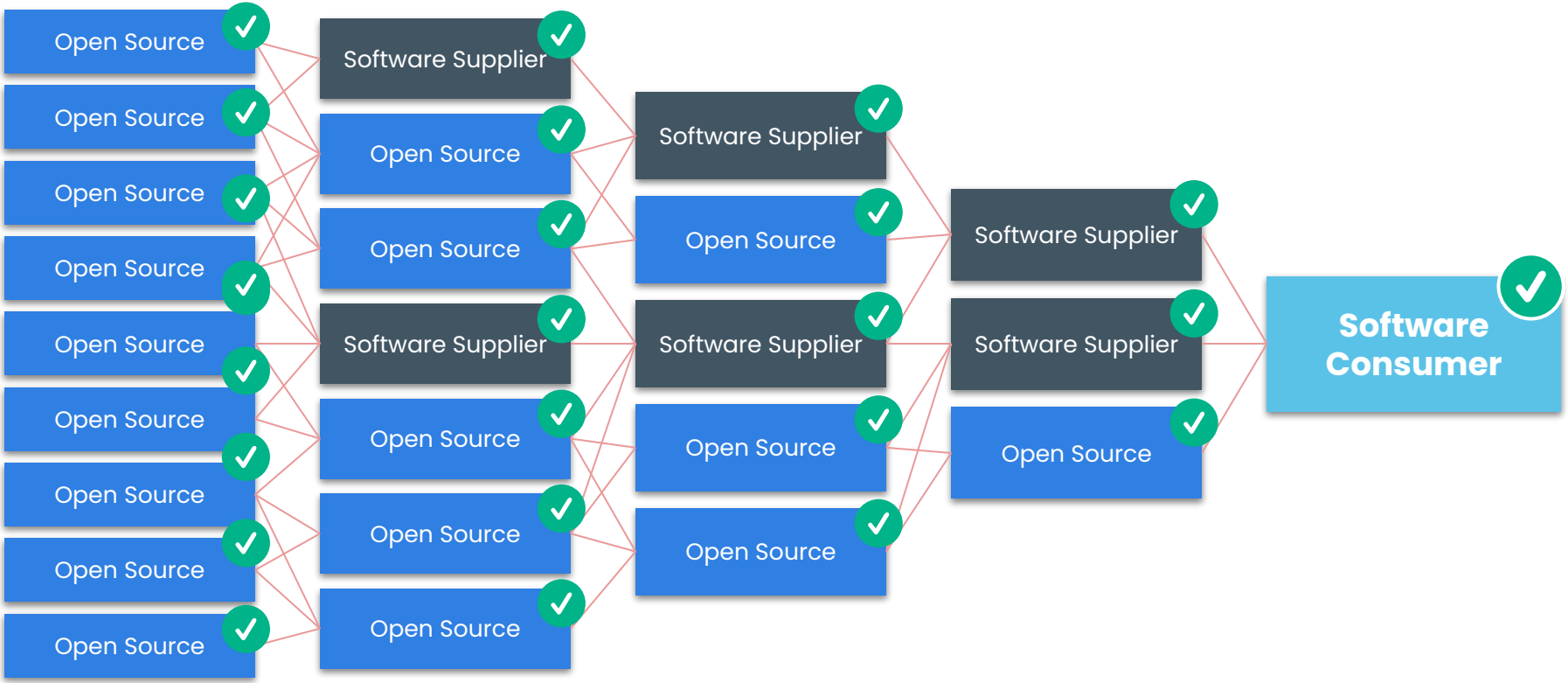
Build images from trusted sources

Automate testing and analysis

Deploy only trusted images



Let's Get to This!



Q&A

Ask questions at
#ask-the-speaker-track-4

Come chat or get a demo at
#xpo-anchore

Win a 49-inch Ultra-Wide Monitor

You will receive 5 entries for attending this session

Visit the Anchore booth to learn how to get additional entries

#xpo-anchore

anchore

Staying out of the (Bad) Headlines: Keeping Attackers out of Your DevOps Toolchain

Daniel Nurmi
CTO and Co-founder, Anchore

Paul Novarese
Senior Solutions Architect, Anchore

DEVOPS ENTERPRISE SUMMIT
AN IT REVOLUTION EVENT

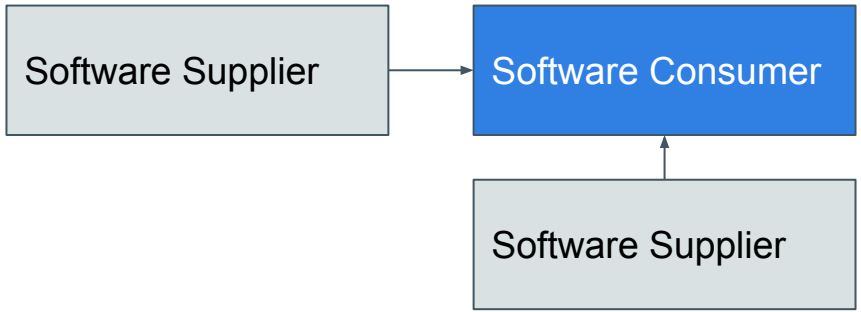
Abstract (reminder)

DevOps lets developers innovate faster. But some normal DevOps processes can create the opportunity for bad actors or dangerous code to enter your DevOps toolchains and your software applications. Where are the security risks and how can DevOps teams prevent attacks without slowing down delivery? We'll provide some easy tips and best practices to secure your toolchain while keeping your development moving.

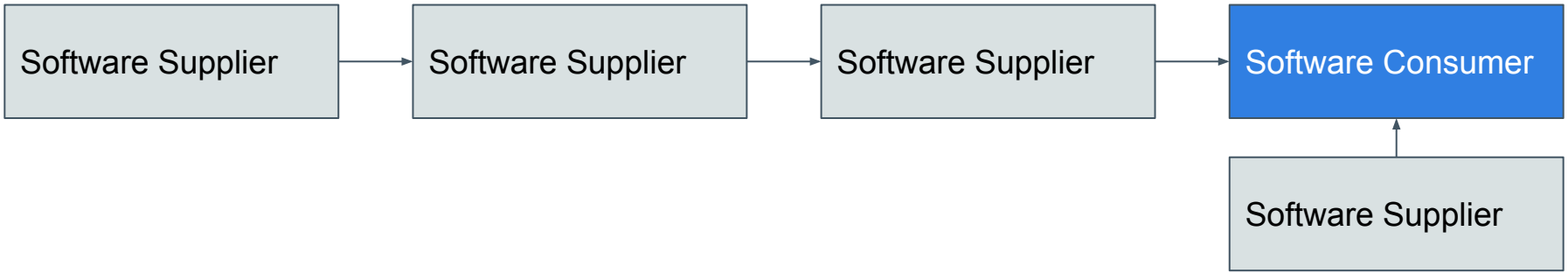
Notes: PVN has demos to show integration -- mostly with Jenkins
Our Jenkins plugin has policy checks
Would need a test image with different things to checkout - maybe use cryptominer
Spend more time on stuff besides vulnerabilities - secrets, curl, sudo, namesquatting - things a malicious actor would do
Can do evaluation earlier and analyze throughout
Early and often
Kubernetes admission controller

1. 10-15 mins preso Dan
    a. Touch on broader vuln capabilities and remediation
2. PVN slides to tee up demo
3. 15 mins demo Paul
    a. Show report
    b. Policies and capabilities
4. Wrapup Paul

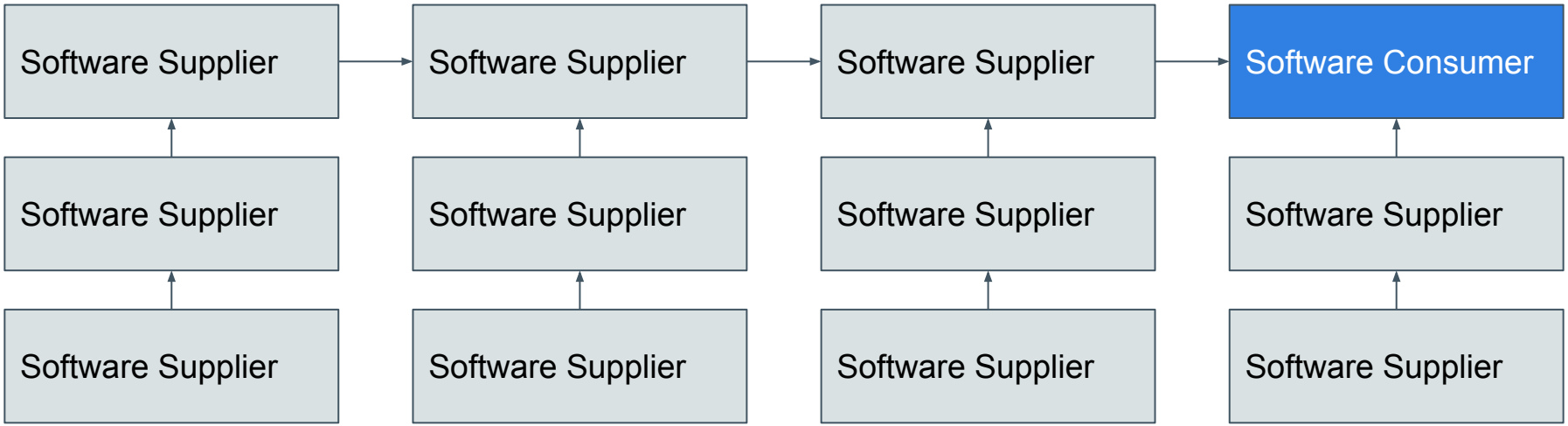
Supply Chain (consumer view)



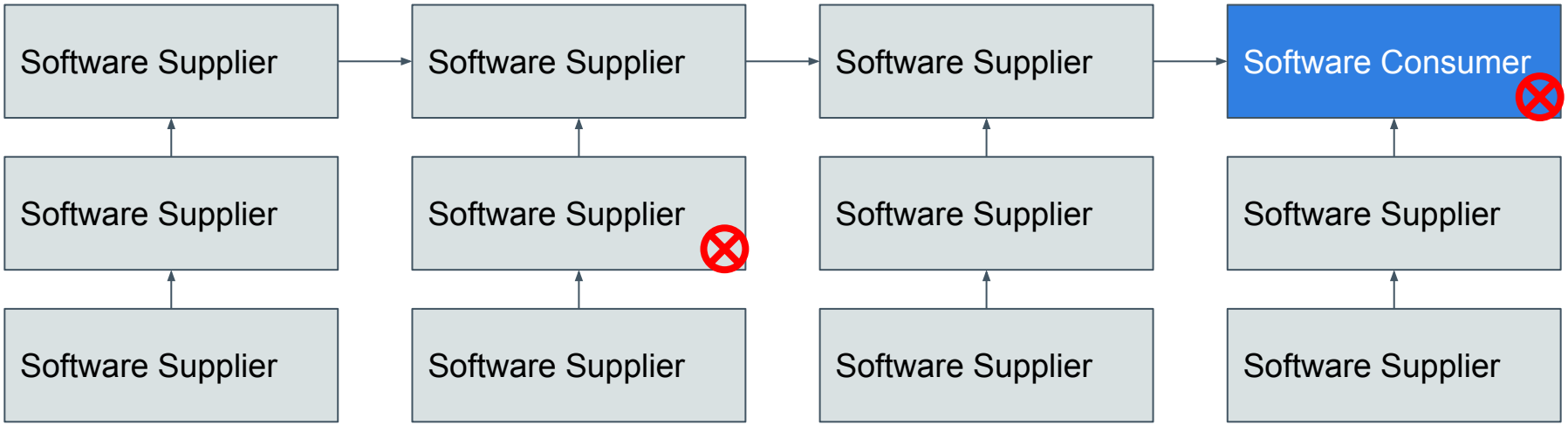
Supply Chain (supplier view)



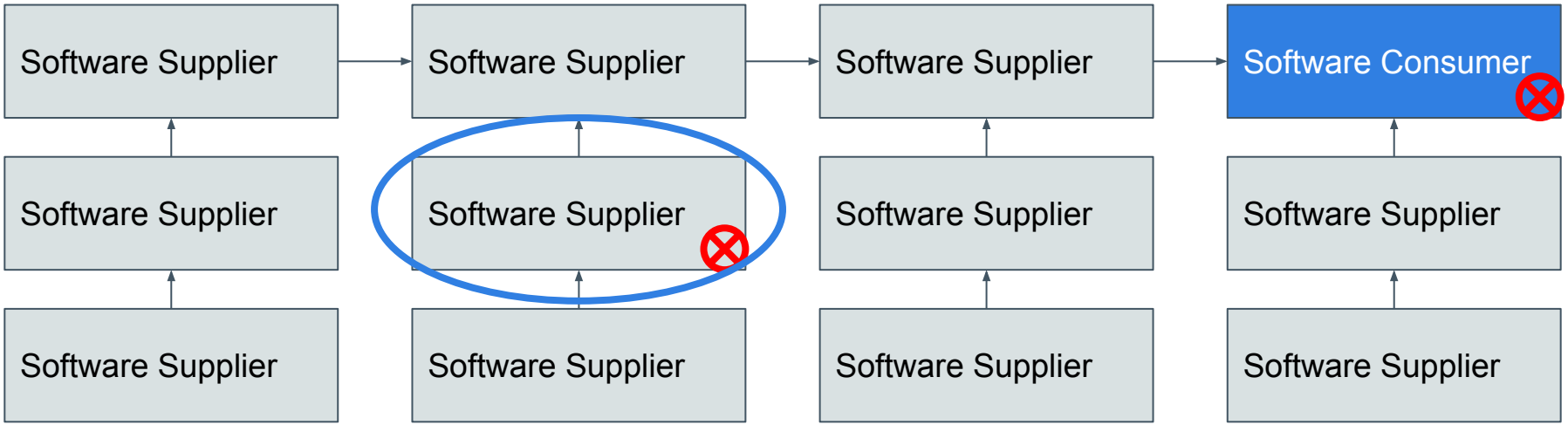
Supply Chain (global view)



Supply Chain



Supply Chain



Supply Chain: Lets get to this!