



KubeCon



CloudNativeCon

India 2026

5 Tactics to Forging a Hardened Software Chain

Pronomita Dey
Senior Software Engineer, Intuit



Five handoffs. Five hardening points.



KubeCon



CloudNativeCon

India 2026

01 Source

Insecure defaults
slip through

02 Build

Unknown vulnerabilities

03 Registry

Image tampered
in transit

04 Admission

Unsigned workloads
enter cluster

05 Runtime

Zero-day executes
inside pod

1. Standardise the Golden Path



KubeCon



CloudNativeCon

India 2026

RISK

Insecure defaults slip through

HOW

Make secure the default — platform injects it, developer just ships

2. Automate SBOMs at Every Build



KubeCon



CloudNativeCon

India 2026

RISK

Unknown dependency vulnerabilities

HOW

Know every ingredient — query your fleet
in 30 seconds when a CVE drops

3. Sign Everything



KubeCon



CloudNativeCon

India 2026

RISK

Image tampered in transit

HOW

Don't trust the tag. Trust the signature —
Cosign binds to the digest

4. Policy as Code Admission Gate



KubeCon



CloudNativeCon

India 2026

RISK

Unsigned workloads enter the cluster

HOW

If it's not signed, it doesn't run — policy lives in Git, not a wiki

5. eBPF Runtime Guardrails



KubeCon



CloudNativeCon

India 2026

RISK

Zero-day executes inside the pod

HOW

Kernel-level. Every syscall. Blocked the instant it happens



KubeCon



CloudNativeCon

India 2026

Stop securing a cluster. Start securing a lifecycle.

<https://medium.com/the-tech-matter/code-to-pod-security-the-cloud-native-way-f5654a158998>

