

Shift Left Security In a Containerized World

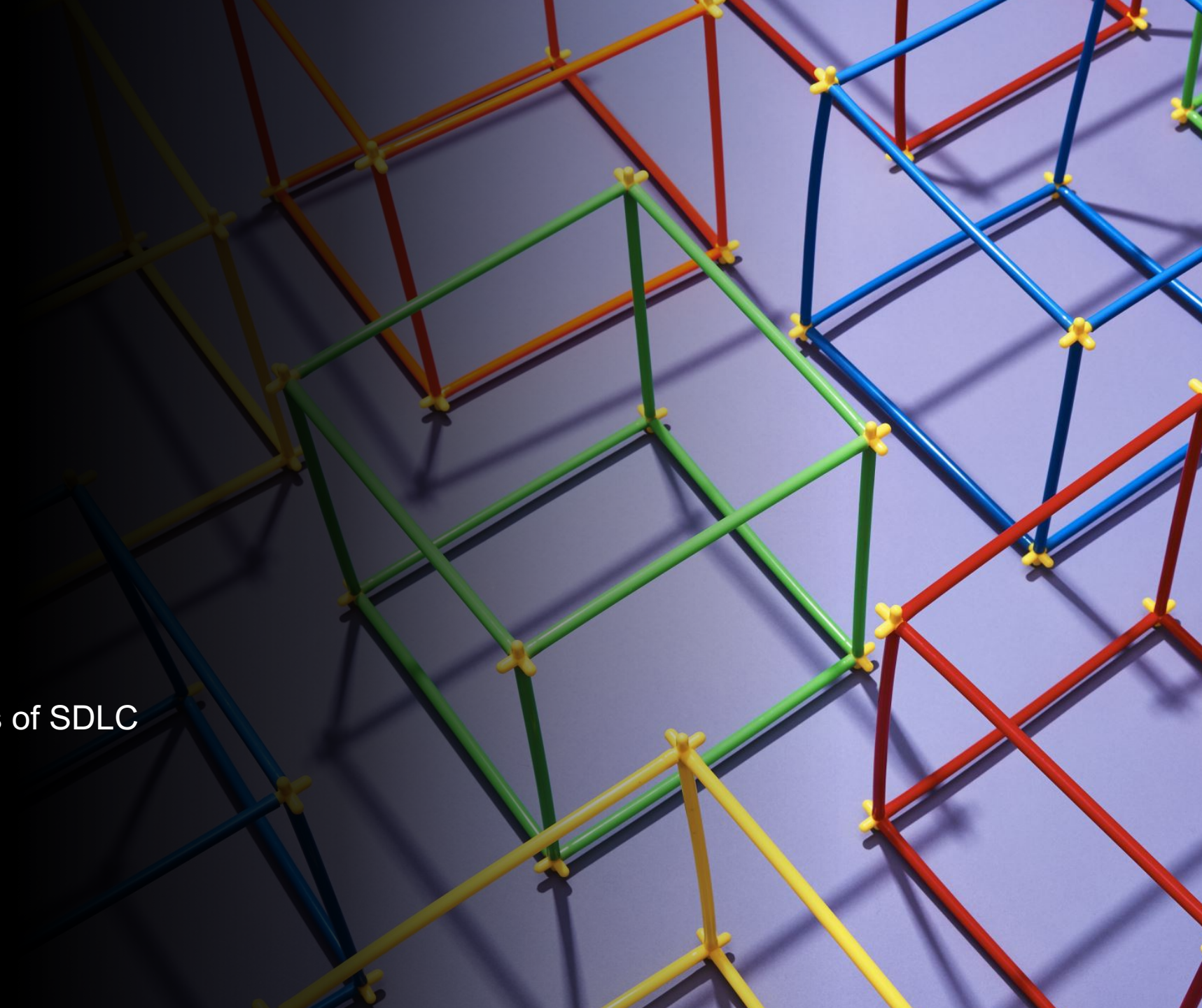
Gunjan Patel 
Sr. Cloud Architect,
Palo Alto Networks

**DEVOPS
WORLD**
by CloudBees



Outline

- Recent technology trends
- What goes into a container
- Code to prod flow
- Security team vs developers
- Security integration points
- Security tools for each stages of SDLC
- Reference Architecture



“An ounce of prevention is worth a pound of cure.”



Services

Monolith

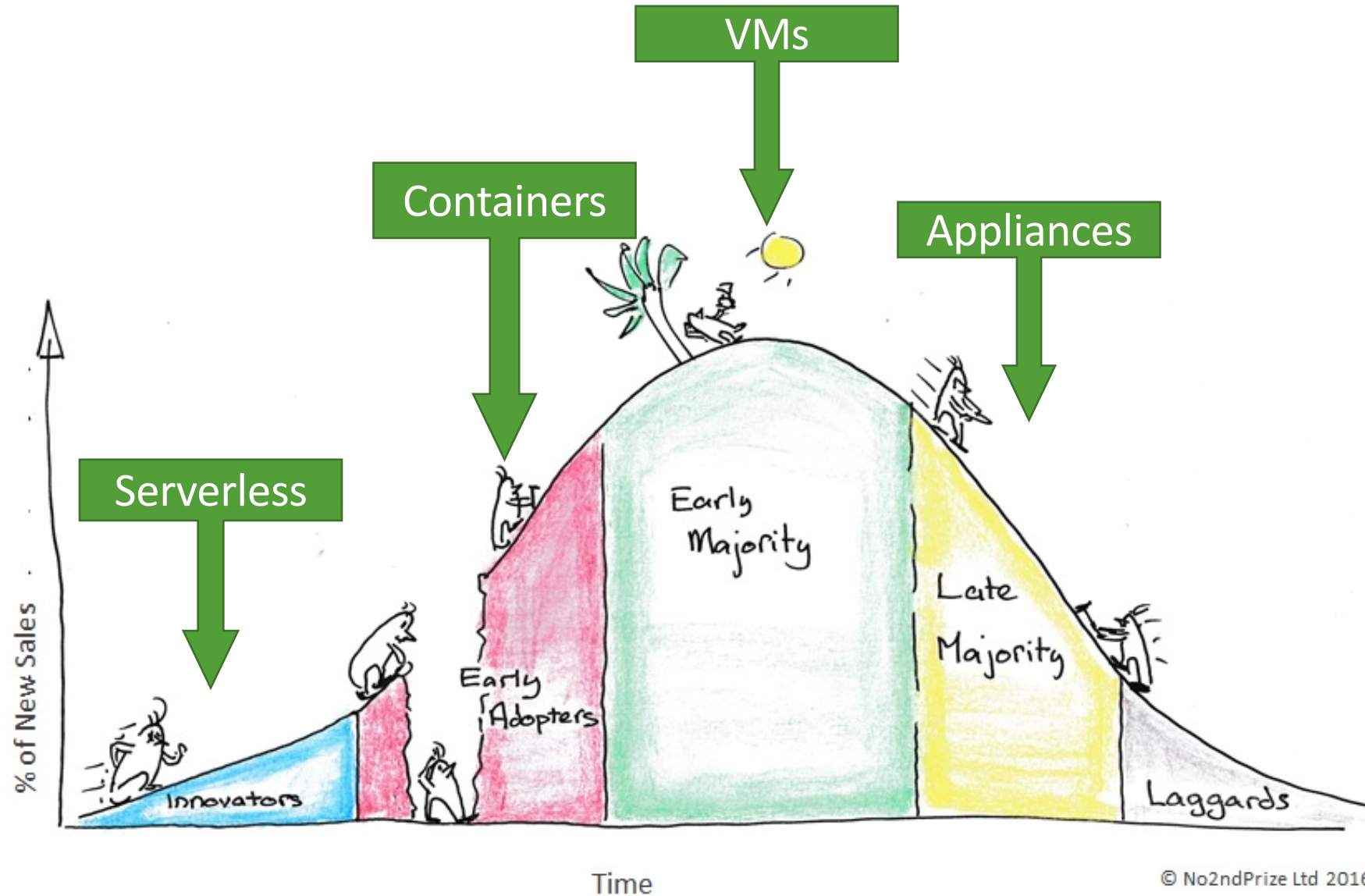
Serverless/FaaS

zzz/skull

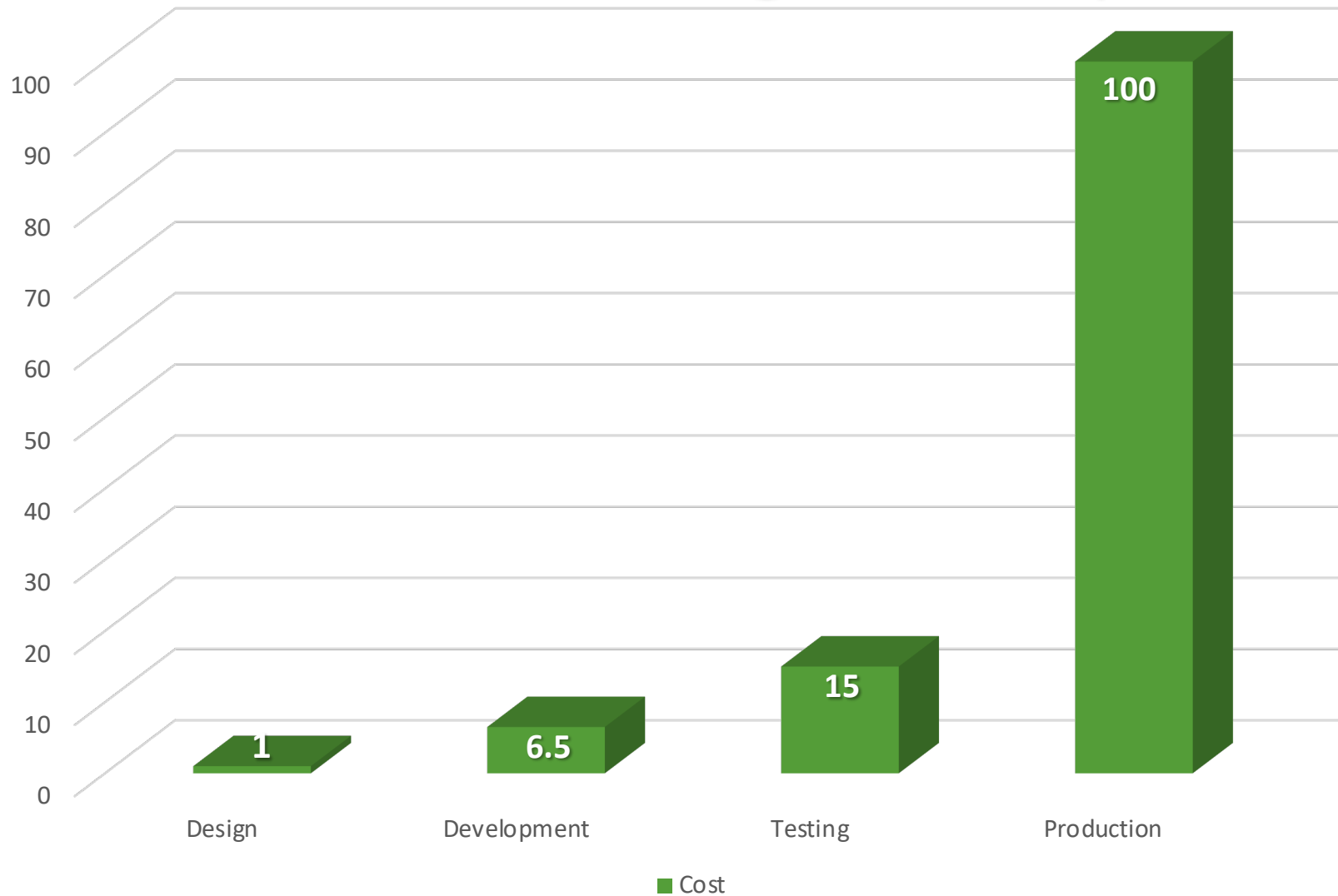
Hey I need you!

Java

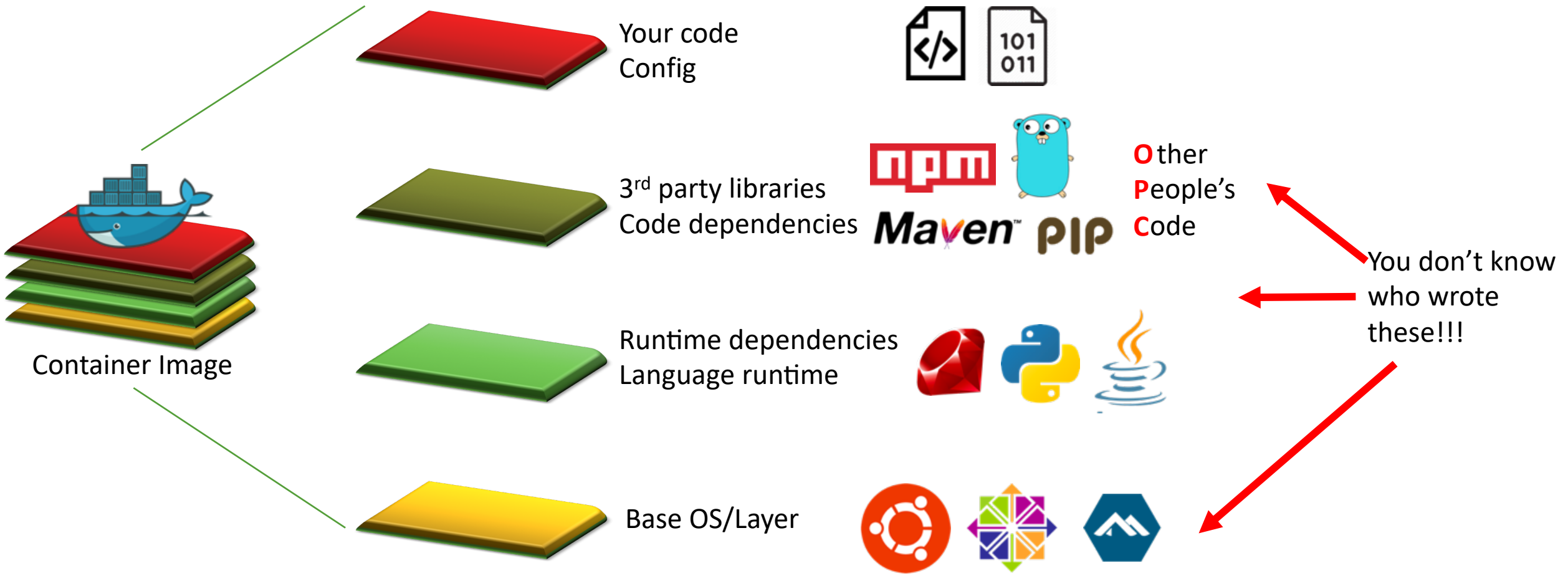
The Technology Adoption Curve



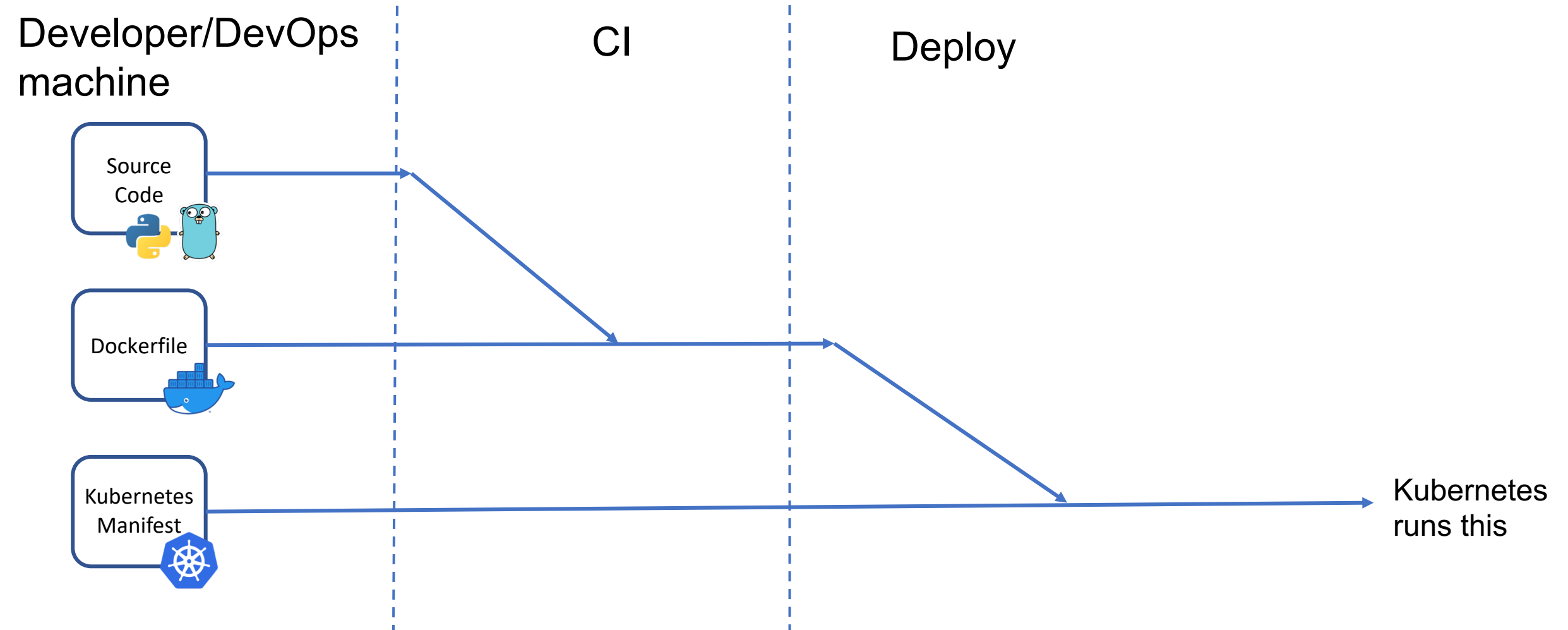
Relative Cost of Fixing Security Defects



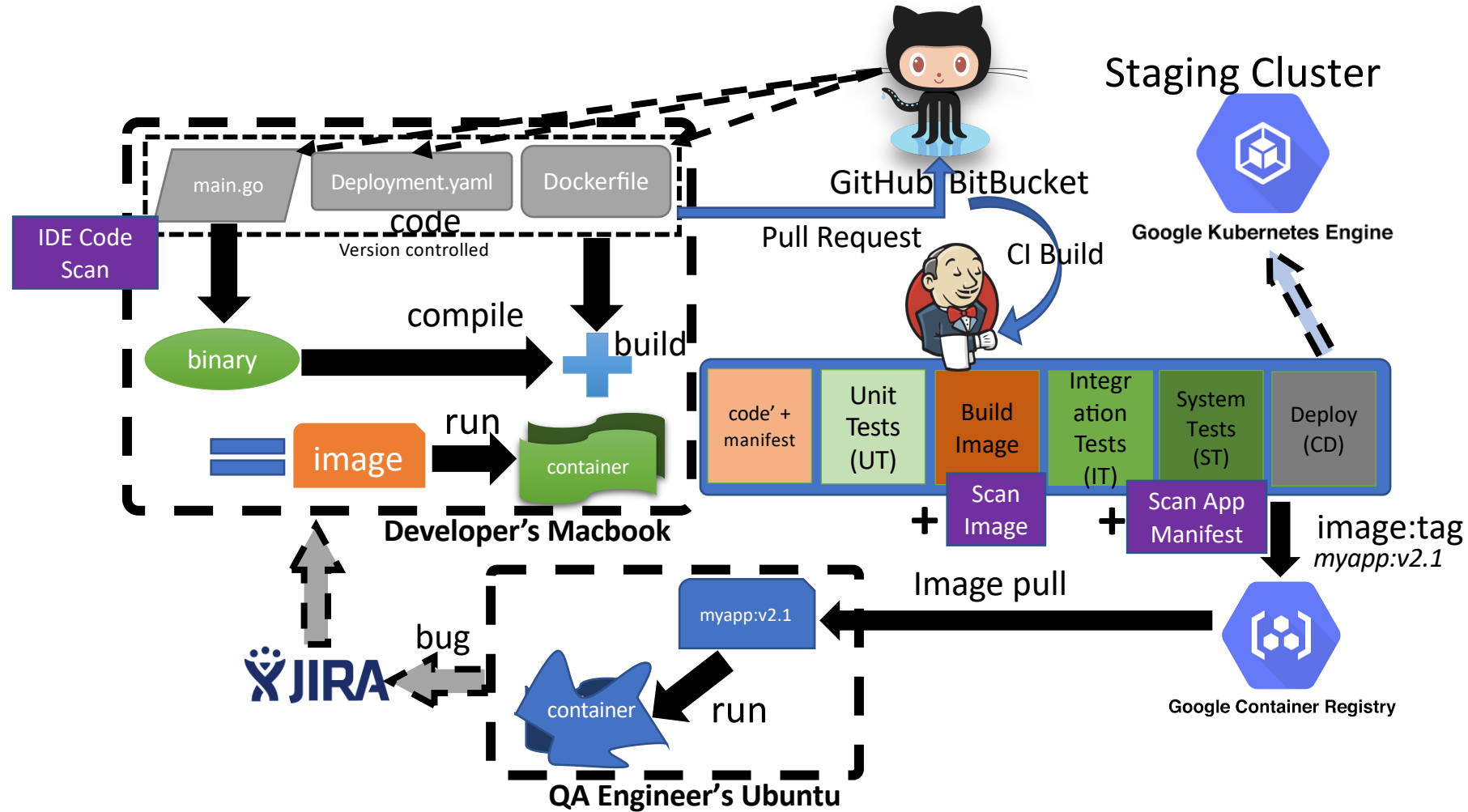
What Goes into a Container Image



Artifacts During Different Phases of SDLC



Code to Prod (SDLC)



Security Team VS Developers

- Low Risk
- Process
- Formal
- Slow and Thoughtful

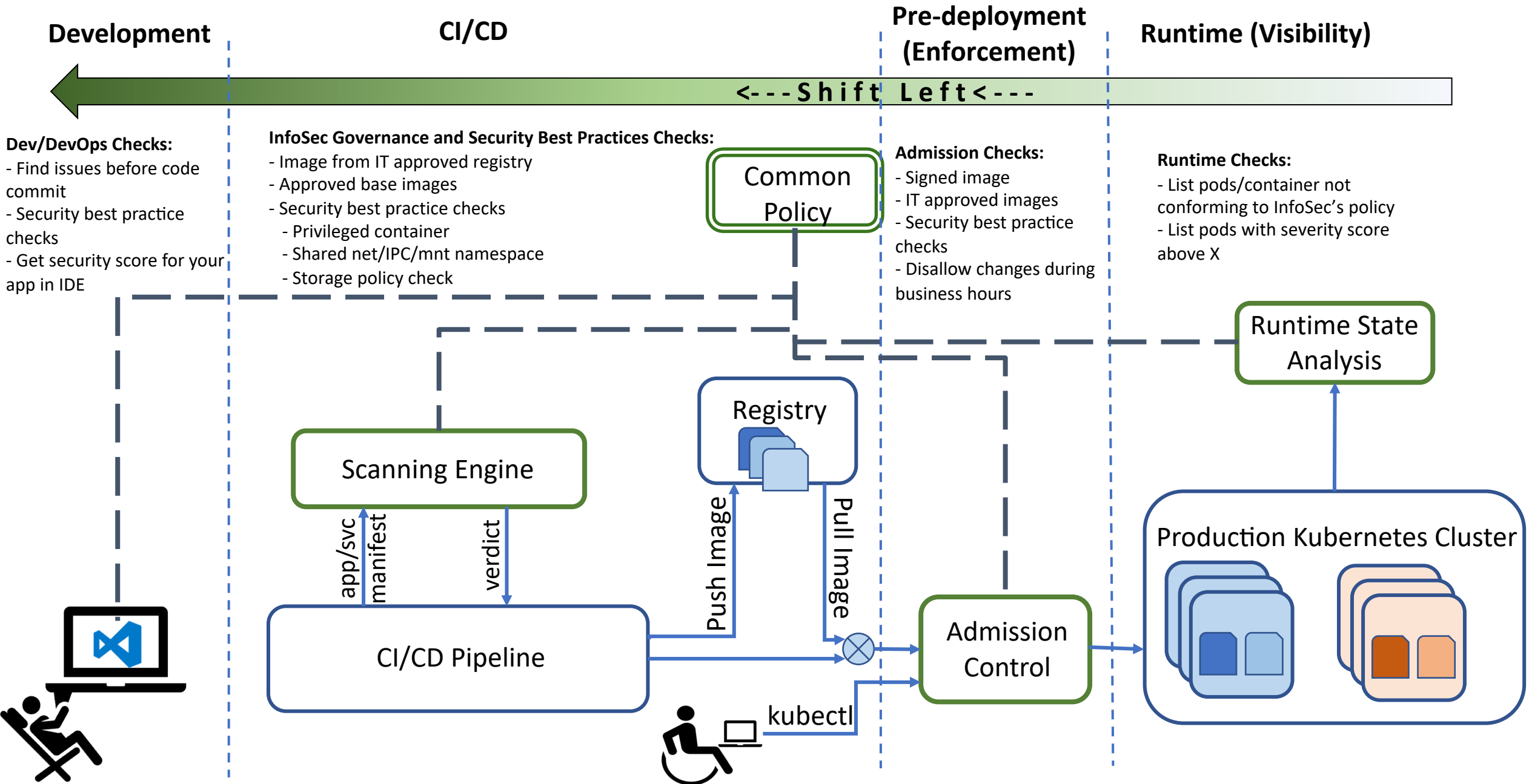


- Try new things
 - Automate
 - Informal
- Quick, fail fast

Left AND Right



Security Integration Points

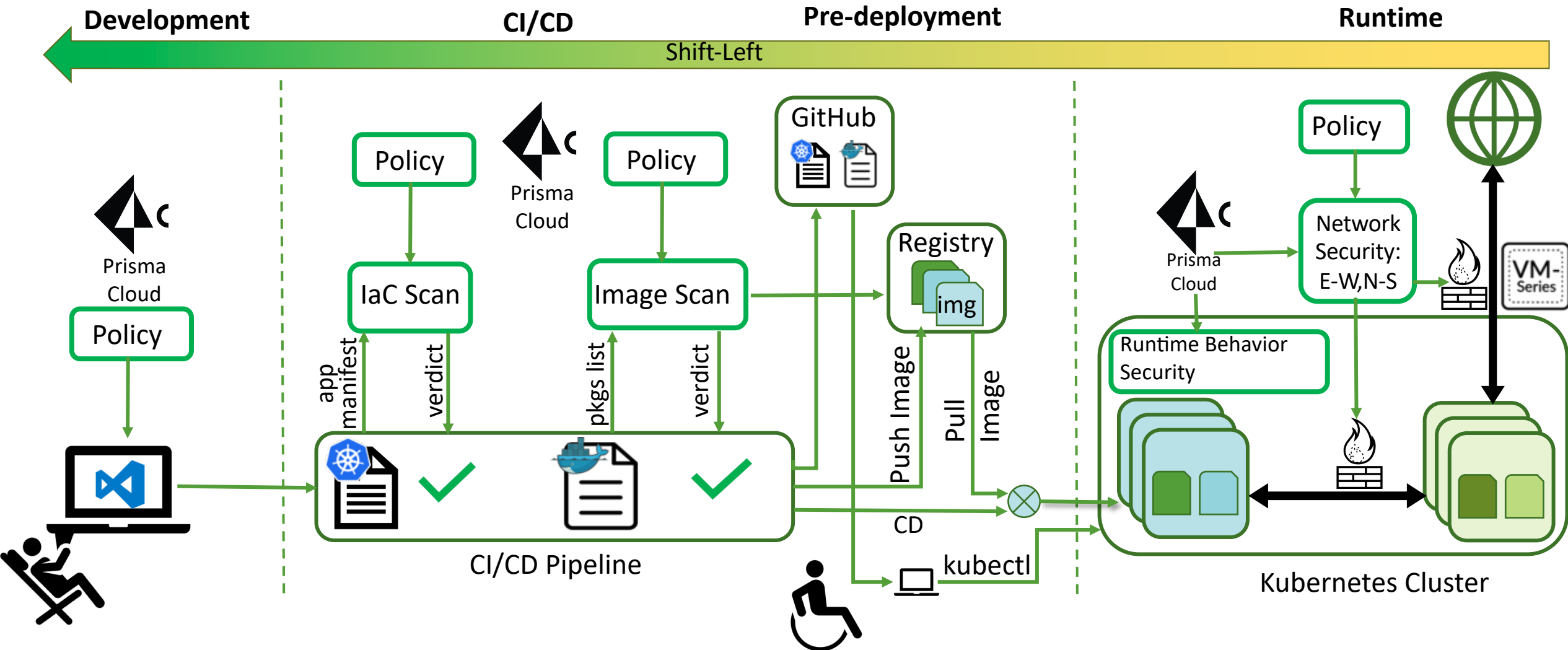


Tools for Each of the SDLC Security Stages

Development	CI/CD	Pre-deployment	Runtime
• Code Scanning • GoSec (Go) • Bandit (Python) • NodeJsScan (NodeJS) • SpotBugs (Java) • Kubernetes Manifest Scanning • KubeSec • Prisma Cloud IaC • Container Image Scanning • Prisma Cloud Compute • JFrog • Clair	• DAST • OWASP ZAP • Arachni • IAST • Contrast Community Edition (CE)	• Kubernetes Admission Controller • Prisma Cloud Compute • Open Policy Agent • Pod Security Policy	• Network • CN-series • Calico • Istio • Prisma Cloud Compute • Behavior • Prisma Cloud Compute • Falco • Access • IAM Analyzer • RBAC • Sandboxing • gVisor • Kata Containers • Nabla Containers

More: <https://github.com/gunjan5/shift-left-security>

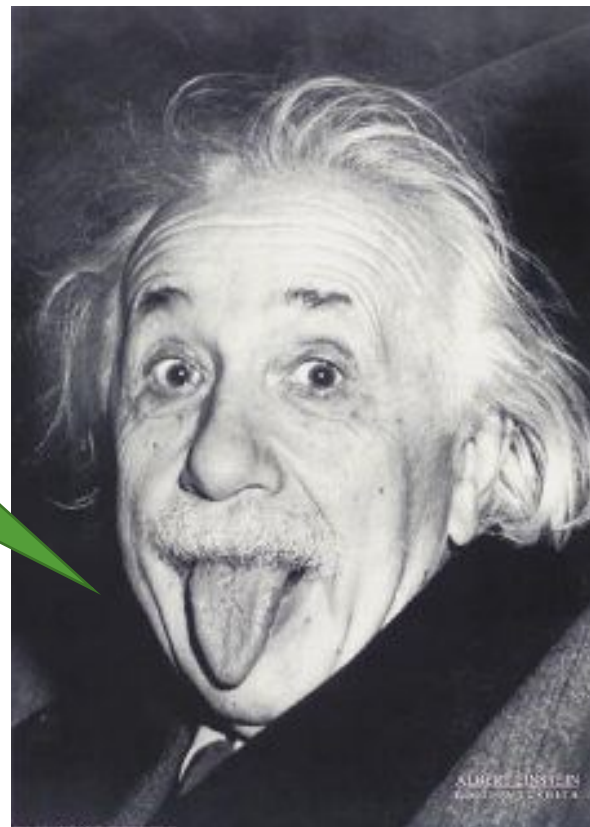
Container Security Reference Architecture





Security should not be an
afterthought

Intellectuals solve problems,
geniuses prevent them.



Resources

- <https://github.com/gunjan5/shift-left-security> (List of Tools for SDLC Security)
- <https://github.com/gunjan5/container-security> (Best Practices)
- <https://github.com/gunjan5/cloud-native-security> (Security Checklist)
- <https://youtu.be/q5gyrESlkFY> (Containers to Serverless Landscape)
- <https://youtu.be/yctITHCDtFU> (Container Security Best Practices)
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security.html>



twitter.com/Gunjan_Patel1



github.com/gunjan5



linkedin.com/in/gunjanpatel1

Thank you! 🍣