Shift-Down Security!

How Platform Teams Can Help Break the Logjam



CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2024

JUNE 26-27 | SEATTLE, WA #CNSCon

About Us



Poonam Lamba

- Product Manager for GKE Policy & Compliance
- WG Policy Co-Chair



@JimBugwadia

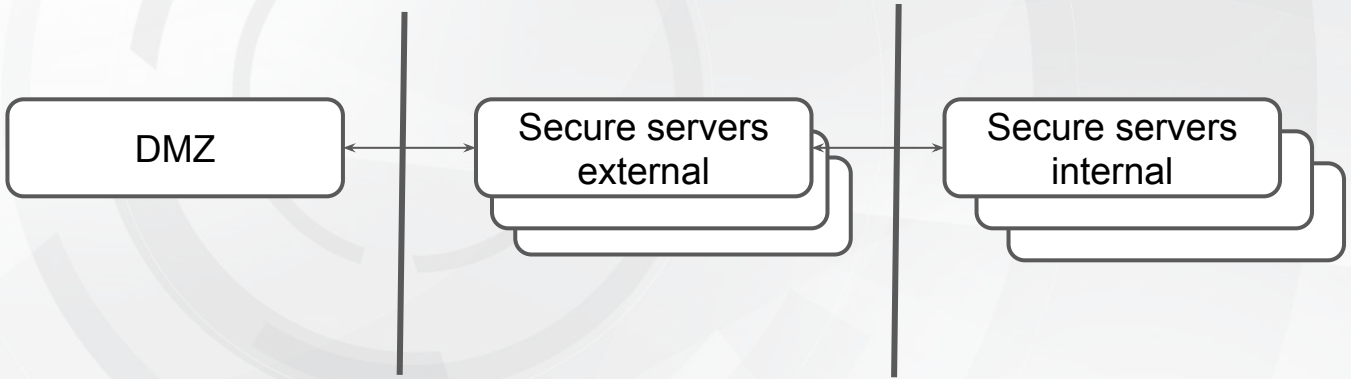
- Co-founder at Nirmata
- WG Policy Co-Chair
- Kyverno Maintainer

Agenda

- Cloud Native Security
- Shift-Left Security
- Shift-Down Security
- Next Steps

Cloud Native Security

A real world example of large scale financial system



The Journey to Cloud Native

Traditional

- Perimeter based
- Static environments
- Manual processes
- Monolithic apps

Cloud Native

- Zero Trust
- Dynamic Environments
- Continuous Delivery
- Loosely coupled services

Shift-Left Security

Shift-Left Security

1. Code scanning to show vulnerabilities and other issues
2. Security issues are directly in IDEs and other dev tools
3. Fix early in development cycle to save time and costs

Shift-left in action! 🤣





Chris Hughes

Shift-Left Challenges

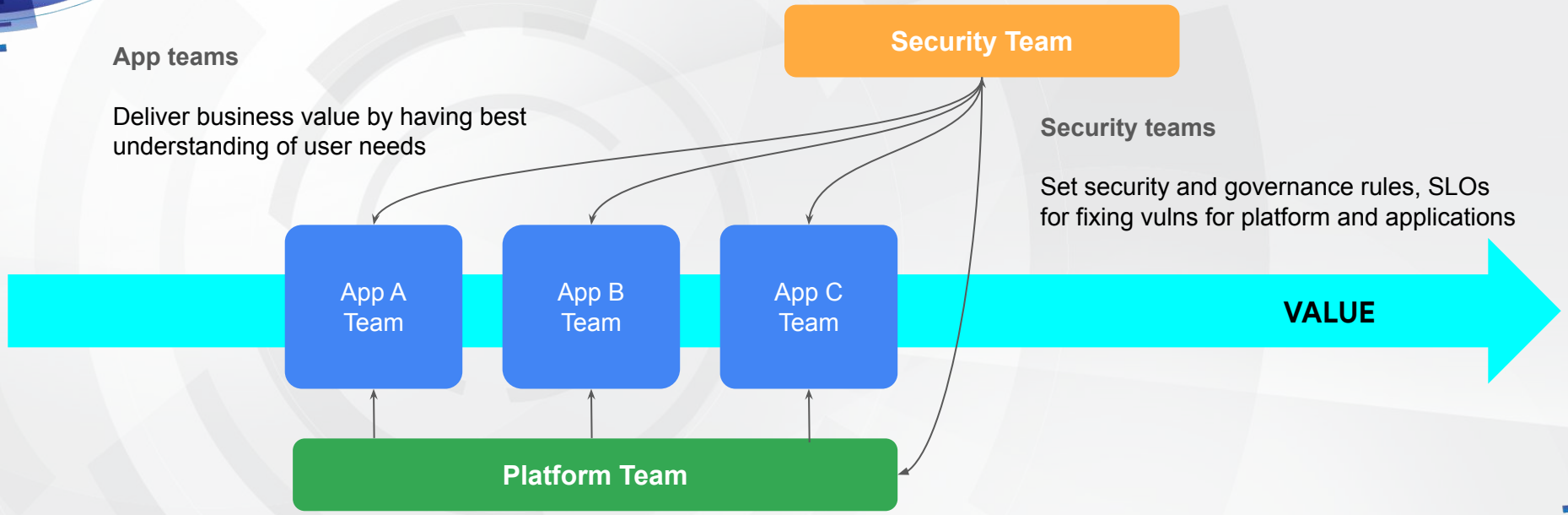
1. False positives, alert fatigue
2. Scaling shift-left in consistent way

Shift-Down Security

Roles and Responsibilities

App teams

Deliver business value by having best understanding of user needs



Security teams

Set security and governance rules, SLOs for fixing vulns for platform and applications

Platform teams

Unburdens app teams by bundling common needs into shared solutions

Why now?

1. Cloud native environments are different
2. Kubernetes provides a standardization layer
3. Platform engineering provides self-service automation

What Is Shift-Down Security?

1. Cross-cutting security concerns as part of the platform
2. Codified, Automated, and Collaborative
3. Complements shift-left and existing processes

How do we “shift-down” security?

Application team
- Develop features
- Fix defects

Security team
- Runtime Security
- Compliance
- Vulnerability Management
- Misconfigurations
- Software Supply Chain Security

Platform team
- Self-Service / Automation

How do we “shift-down” security?

Application team
- Develop features
- Fix defects

Security team
- Runtime Security
- Compliance

- Vulnerability Management
- Misconfiguration Management
- Supply Chain Security

Platform team
- **Self-Service Automation**
- **Vulnerabilities**: Manage base images
- **Misconfigurations**: Manage policies
- **Supply Chain**: Secure, sign, attest, verify

Shifting-Down For Vulnerability Management

Base Images

nginx:latest

├── 2 critical, 14 high, 32 medium, 4 low, 73 negligible

nginx:alpine

├── 0 critical, 2 high, 25 medium, 0 low, 0 negligible

xxxxx/nginx-distroless:latest

├── 0 critical, 0 high, 3 medium, 0 low, 7 negligible

cgr.dev/chainguard/nginx

├── 0 critical, 0 high, 0 medium, 0 low, 0 negligible

Best practices:

1. Reduce
2. Update
3. Patch



Vulnerability Exploitability eXchange (VEX)

- Allows developers / vendors to focus on what's important
- Provides information on non-exploitable vulnerabilities
- Assertions on the status of a vulnerability:
  - Not affected, Affected, Fixed, Under Investigation
- OpenVEX provides an OSS implementation

Shifting-Down
Preventing Misconfigurations with Policy as Code

CrowdStrike Discovers First-Ever Dero Cryptojacking Campaign Targeting Kubernetes

March 15, 2023 Benjamin Grap - Manoj Ahuje From The Front Lines



Aqua Blog

Kubernetes Exposed: One Yaml away from Disaster

Threat Alert



Snyk Blog

Leaky Vessels: Docker and runc container breakout vulnerabilities (January 2024)

Written by: JS Jamie Smith

January 31, 2024 8 mins read

Notes on Leaky Vessels

We will continue to update this blog with any key updates, including updates on the disclosure of any new related vulnerabilities. This blog includes links to detailed blogs on each of the disclosed vulnerabilities, as well as two open source tools to aid in exploit detection.

Aqua News

Aqua Nautilus Researchers Find Kubernetes Clusters Under Attack in Hundreds of Organizations

Malware and backdoors used in attacks affecting many Fortune 500 companies

https://www.cncf.io/blog/2023/12/05/the-new-standard-of-kubernetes-misconfiguration-remediation/

What are Policies?

Kubernetes docs:

> *[...] configurations that manage other configurations or runtime behaviors*

NIST 800-95:

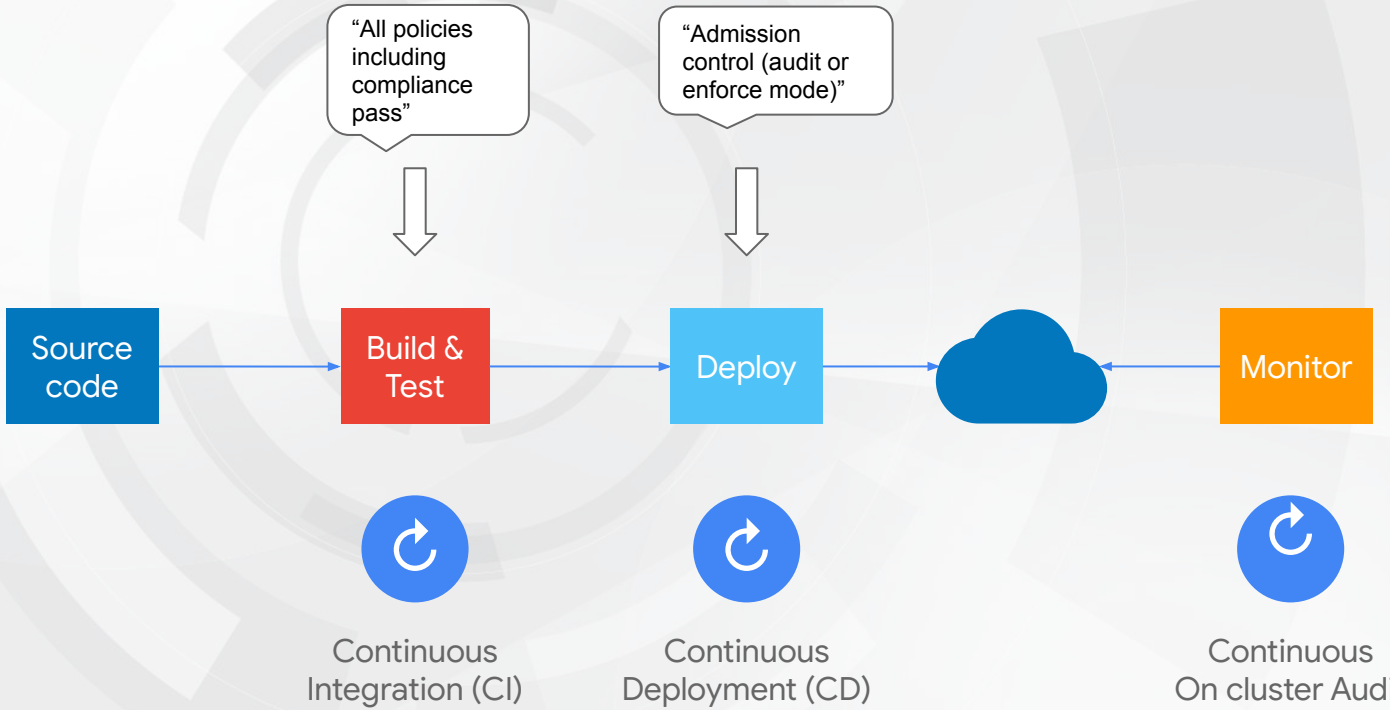
> *Statements, rules or assertions that specify the correct or expected behavior of an entity*

Policy Use Cases for Kubernetes

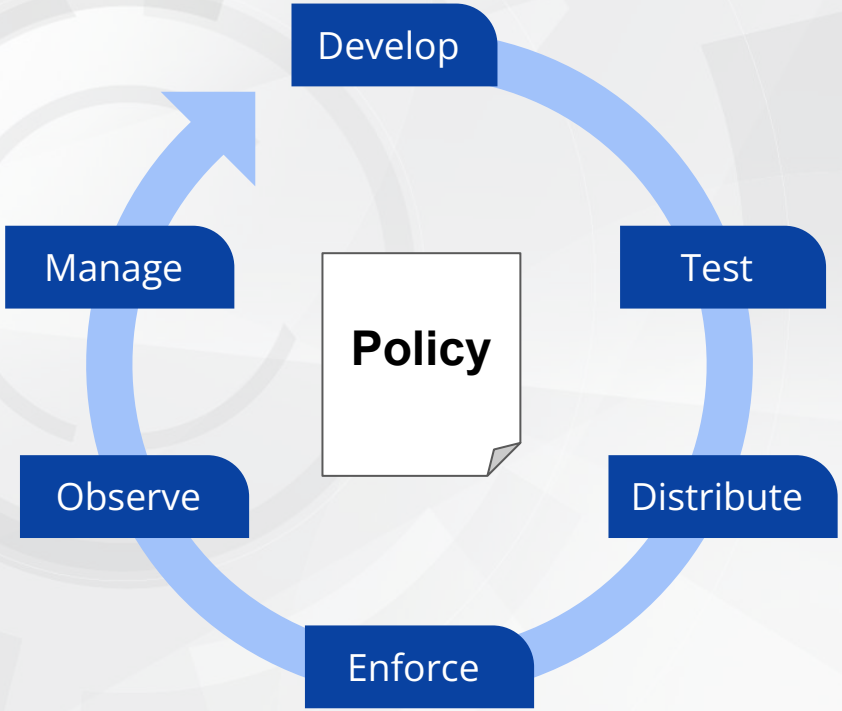
1. Pod Security
2. Workload Security
3. RBAC Configuration
4. Best Practices
5. Multi-tenancy
6. Micro-segmentation
7. Resource Optimization
8. Image Verification

Policies must also be applied to IaC pipelines and non-Kubernetes workloads, like cloud services!

Policy Enforcement



Policy as Code



Shifting-Down For
Secure Software Supply Chains

Software Supply Chain Security

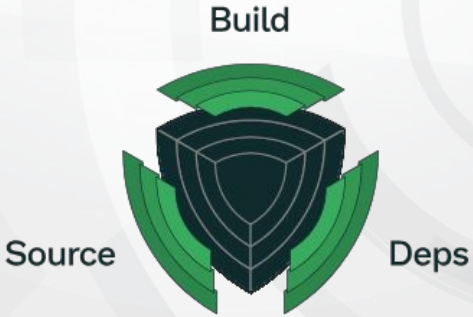
What can the platform team do?

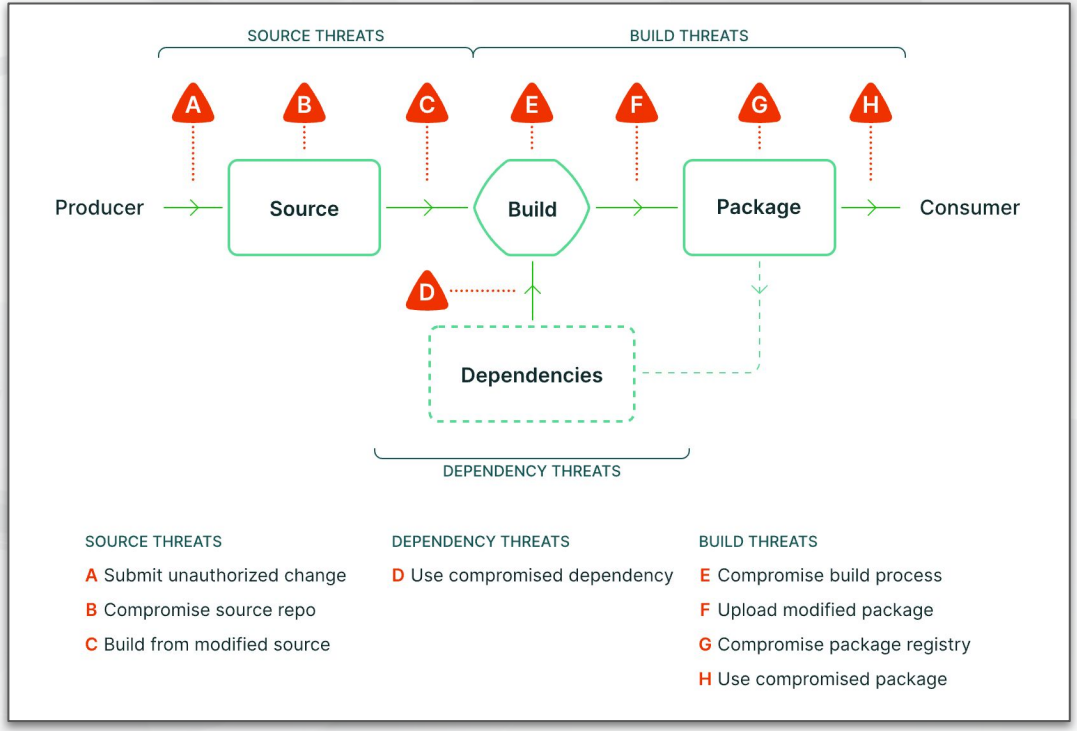
1. Ensure best practices across all repositories
2. Tools to create (signed) attestations during builds
3. Policies to verify signatures and attestations

SLSA (Supply-chain Levels for Software Artifacts)

https://slsa.dev/

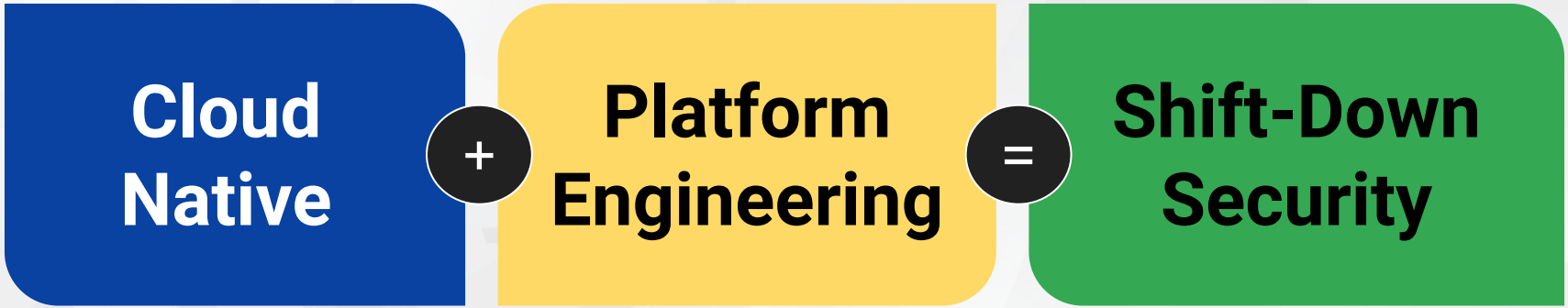
Threats & Mitigations





What’s next?

Security is at an inflection point!



Key Takeaways

- Security is a shared responsibility
- Platform teams must deliver agility ***and*** security
  - *off-load busy developers and security teams*
- Three ways platform teams can assist security:
  1. Eliminate vulnerabilities via base images and VEX
  2. Prevent misconfigurations with Policy as Code
  3. Secure software supply chains with SLSA v1

Additional Resources

CNCF Kubernetes Policy WG

- Bi-weekly community meetings on Wed 9:00 PT
- https://github.com/kubernetes/community/blob/master/wg-policy/README.md


Application Development

The Modernization Imperative: Shifting left is for suckers. Shift down instead

June 8, 2023 Richard Seroter, Google

https://cloud.google.com/blog/products/application-development/richard-seroter-on-shifting-down-vs-shifting-left

Thanks!