

# Code of Conduct



Be aware of others



Be welcoming and  
respectful



Be understanding of  
differences



Be friendly and  
patient



Be open to all  
questions and  
viewpoints



Be kind and  
considerate to others

# Thank you to our Sponsors!



{ } NDC Conferences

**Olmec**  
quality through innovation



Octopus Deploy



Sage



GitHub

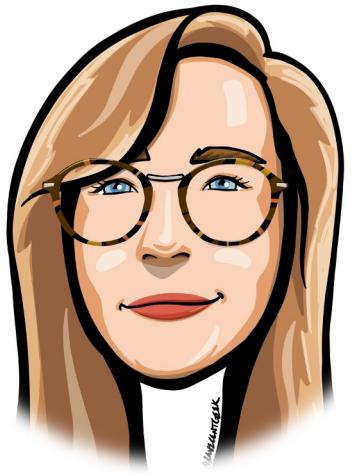


# **Securing Container Apps - Why and How!**

Annie Talvasto  
Karl Ots



@AnnieTalvasto @karlgots



**Annie Talvasto**

Sr PMM @ Camunda  
CNCF Ambassador, MVP



**Karl Ots**

Head of Cloud Sec @ EPAM  
CISSP, MVP, RD



@AnnieTalvasto

@karlgots

# Agenda

- Introduction
- Overview of Container & Cloud Native Security
- Container Security (in the Enterprise)
- Takeaways & Resources



# Changes with Cloud Native Security

## Ephemeral workloads

- Event-driven and agentless monitoring



@AnnieTalvasto

@karlgots

# Changes with Cloud Native Security

Ephemeral  
workloads

- Event-driven and agentless monitoring

Perimeter  
changes

- Identity-based perimeter
- Microsegmentation



@AnnieTalvasto

@karlgots

# Changes with Cloud Native Security

## Ephemeral workloads

- Event-driven and agentless monitoring

## Perimeter changes

- Identity-based perimeter
- Microsegmentation

## Growing share of OSS

- Supply chain lifecycle security



@AnnieTalvasto

@karlgots

# CNCF Microsurvey on Security

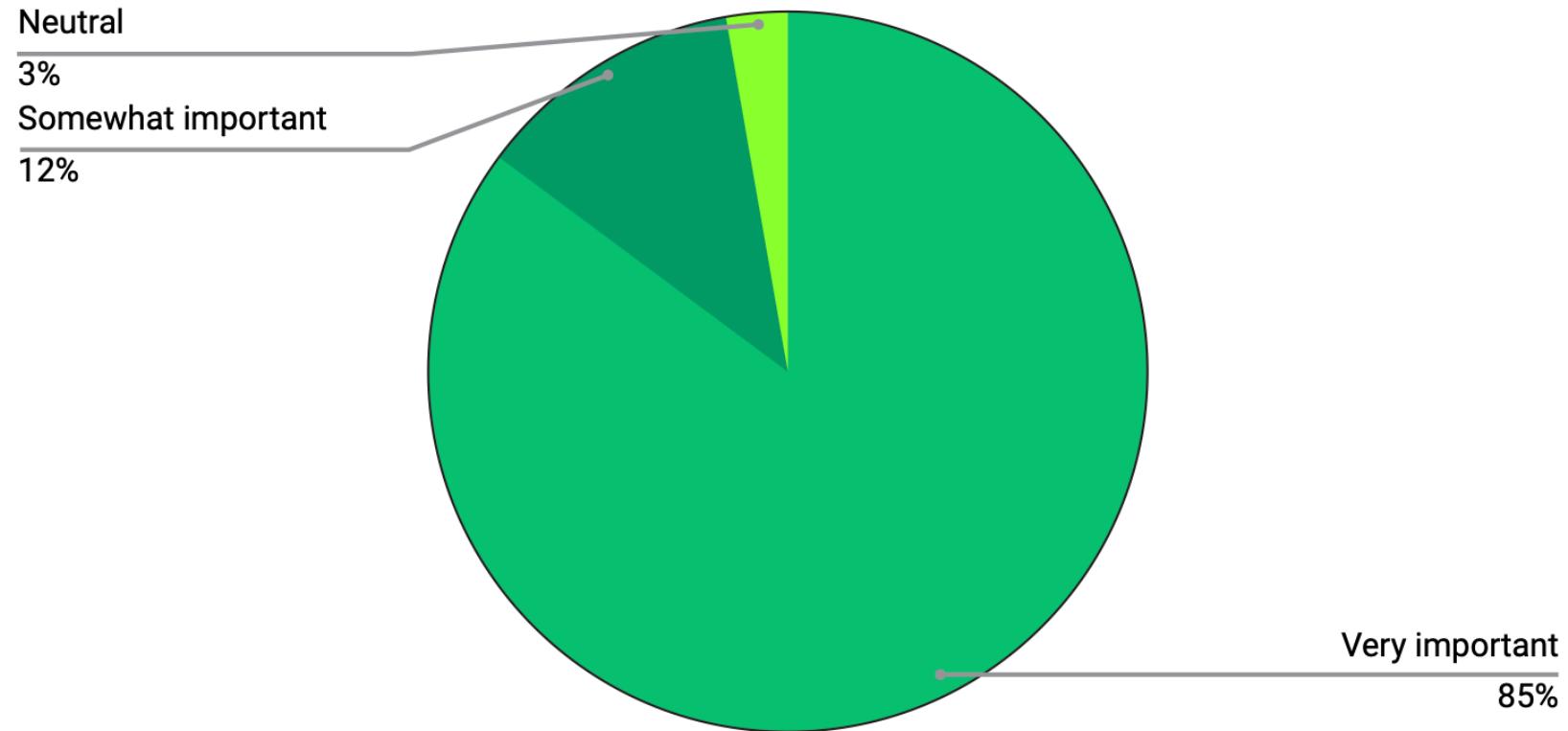
## Cloud Native Security Microsurvey:

More than 80% of organizations want to build modern security systems with open source software



# Importance of Cloud Native Security

How important is modernizing security to your cloud native environments?

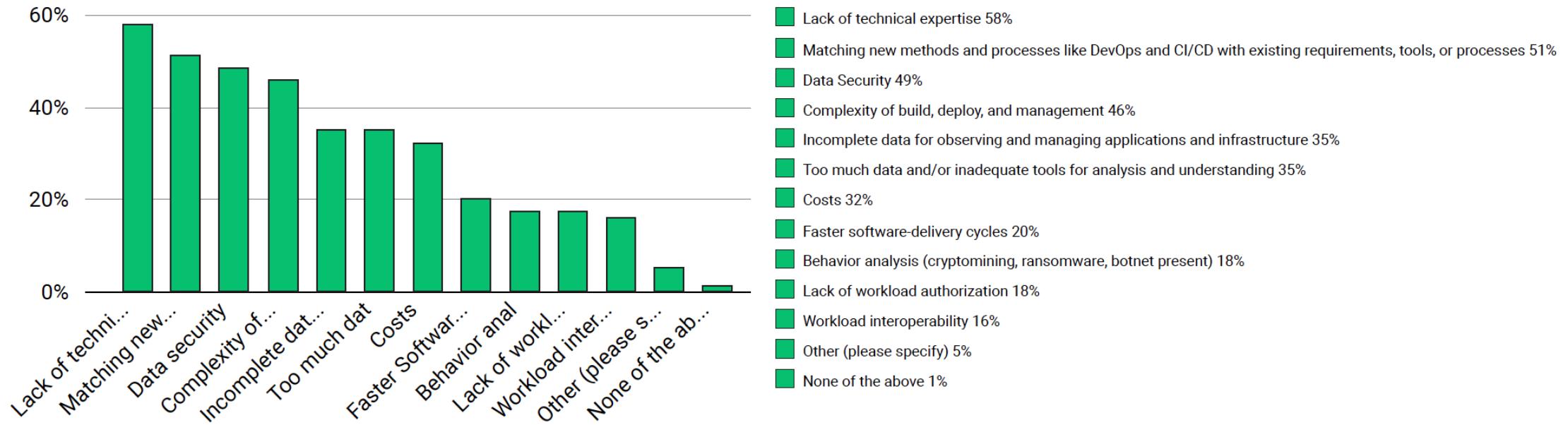


@AnnieTalvasto

@karlgots

# Challenges in Cloud Native Security

Which of the following challenges have you experienced in running cloud native environments? Please select all that apply.



@AnnieTalvasto

@karlgots

# Challenges in Cloud Native Security

1. A lack of technical expertise – 58%
2. Trouble matching new methods and processes like DevOps and CI/CD with existing requirements, tools, or processes – 51%
3. Data security – 49 %
4. The complexity of building, deploying, and management – 46%



@AnnieTalvasto

@karlgots

I FIND YOUR LACK OF CYBER SECURITY



DISTURBING

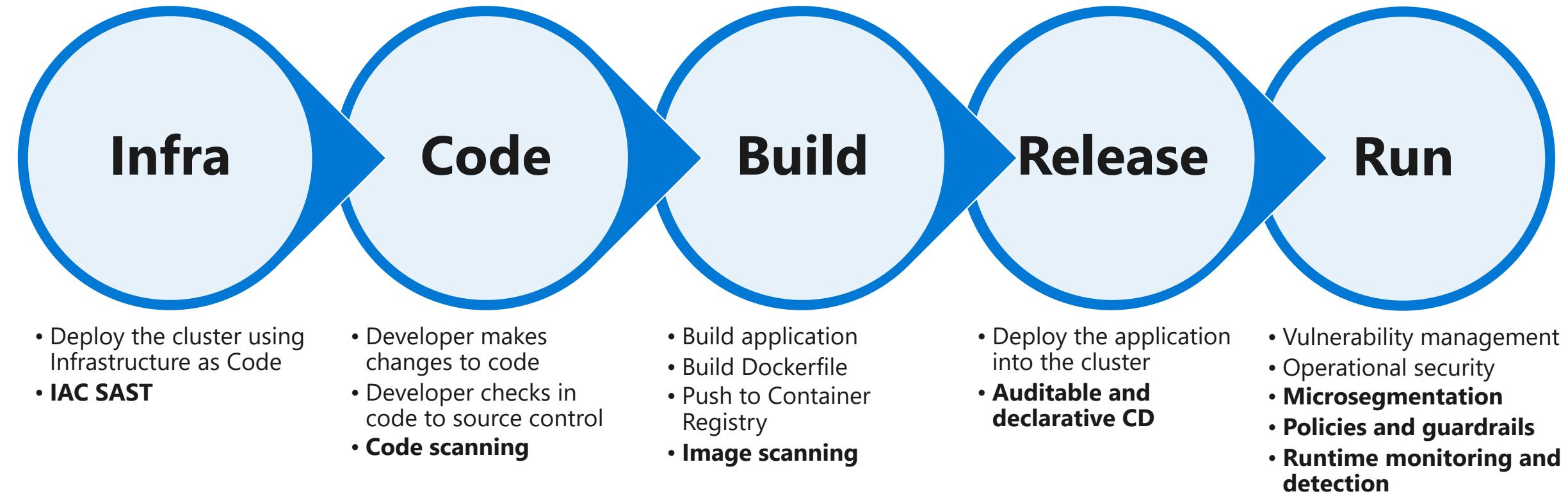
# Agenda

- Introduction
- Overview of Cloud Native security
- Cloud Native Security (in the Enterprise)
- Takeaways & Resources

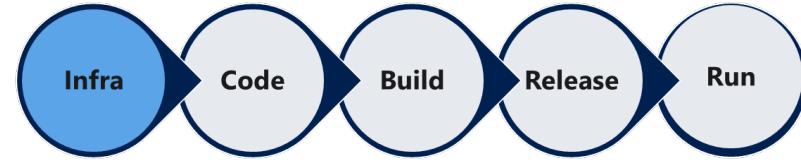


@AnnieTalvasto @karlgots

# Security Across the Cloud Native Lifecycle



# Security Testing IaC



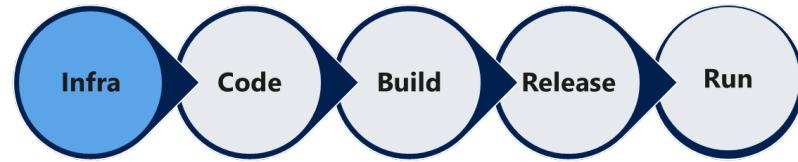
- Scan your IaC templates for vulnerabilities and security misconfigurations
- Run the scan continuously, as pre-deployment test or bring the rule set as recommendations in the IDE



@AnnieTalvasto

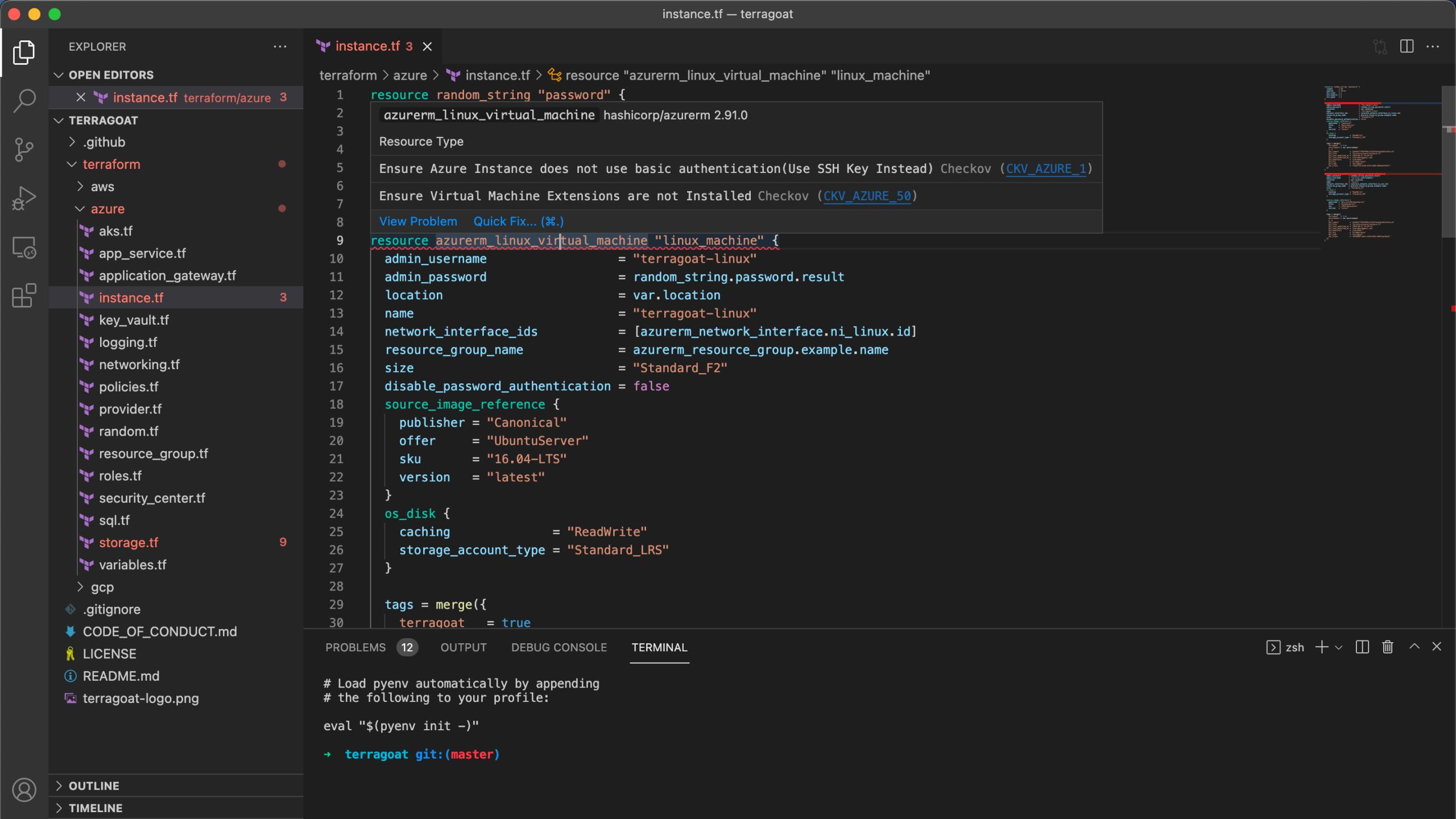
@karlgots

# Checkov



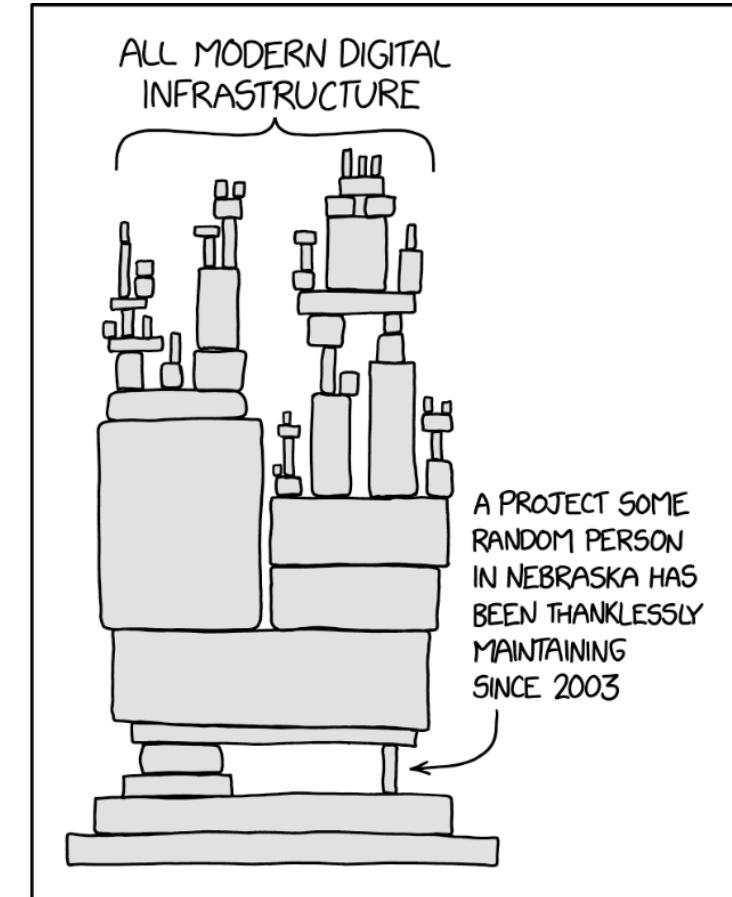
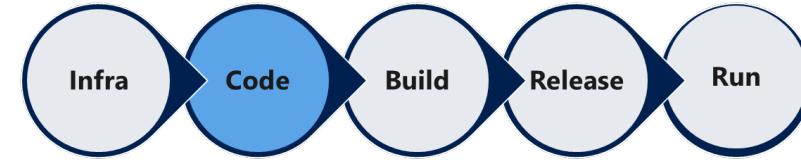
- Checkov scans cloud infrastructure configurations to find misconfigurations before they're deployed.
- Open source, commercial service available from BridgeCrew (part of Palo Alto)
- Provides common command line interface to manage IaC, and can scan across
  - Terraform
  - CloudFormation
  - Kubernetes
  - Helm
  - ARM templates
  - Serverless framework





# Code Scanning

- Complexity of polyglot applications requires going beyond static security testing, to also include composition analysis
- Scanners produce Software Bill of Materials, and map dependencies with OSS risk



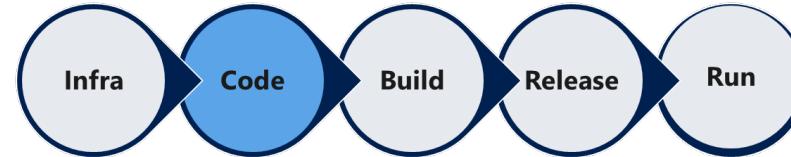
XKCD 2347



@AnnieTalvasto

@karlgots

# SonarQube



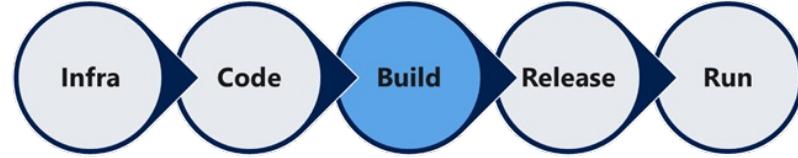
- Code scanning **enables vulnerabilities to be detected and remediated prior to release into production**, eliminating the cybersecurity risks that they pose.
- Enterprisey features include systematic tracking of Code Quality and Code Security



@AnnieTalvasto

@karlgots

# Container Image Scanning



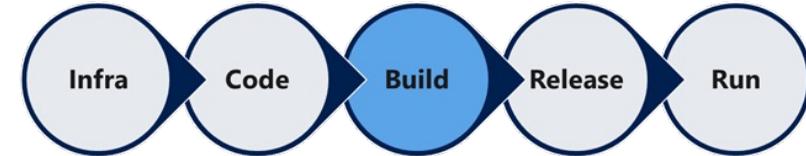
- Do you **really** know all the dependencies of all the base images of the containers that you are running?
- Untrusted container images violate the integrity of your Kubernetes cluster
- Scan the images against security vulnerabilities before pushing to registry



@AnnieTalvasto

@karlgots

# Docker Scan



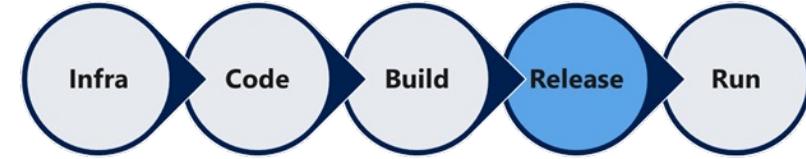
- Native vulnerability scanner for Docker images
- Based on Snyk engine
- Quickly detect and learn how to remediate CVEs in your images by running docker scan IMAGE\_NAME.
- Scan results:
  - Common Vulnerabilities and Exposures (CVEs)
  - Sources, such as OS packages and libraries
  - Versions in which they were introduced
  - Recommended fixed version



@AnnieTalvasto

@karlgots

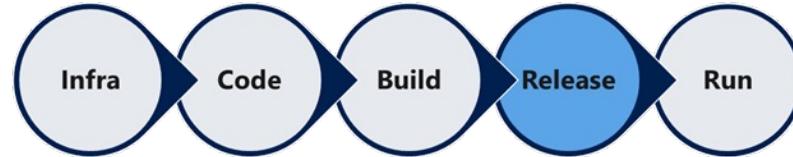
# Auditable and Declarative CD



- Sometimes referred to as GitOps
- Define your entire cloud native stack as code
  - Application
  - Configuration
  - Kubernetes environment
- Apply secure software development practices across the whole stack
  - Auditable
  - Repeatable



# ArgoCD



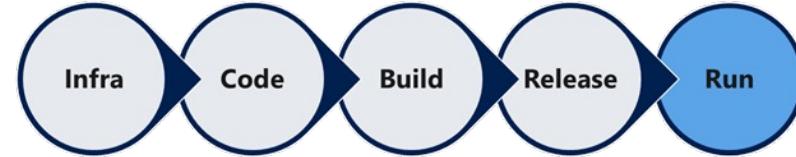
- Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes.
- Application definitions, configurations, and environments should be declarative and version controlled.
- Kubernetes manifests can be specified in several ways:
  - [kustomize](#) applications
  - [helm](#) charts
  - [jsonnet](#) files
  - Plain directory of YAML/json manifests



@AnnieTalvasto

@karlgots

# Runtime Security Monitoring



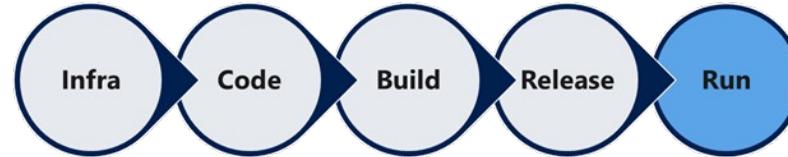
- Monitoring and detection of attacks in immutable and ephemeral environment is difficult
- You need to tap into new sources of logs and events
- You need real-time alerting



@AnnieTalvasto

@karlgots

# Falco



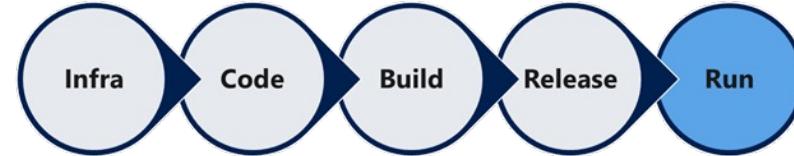
- Cloud-Native Runtime Security
- Falco, the cloud-native runtime security project, is the de facto Kubernetes threat detection engine.
- Detects threats at runtime by observing the behaviour of your applications and containers.
- Extends threat detection across cloud environments with Falco Plugins.



@AnnieTalvasto

@karlgots

# What does Falco check?



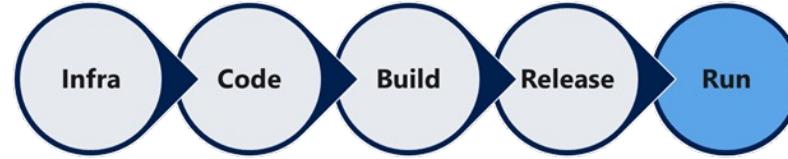
- Privilege escalation using privileged containers
- Namespace changes
- Read/Writes to well-known directories
- Executing shell binaries



@AnnieTalvasto

@karlgots

# Cluster Security



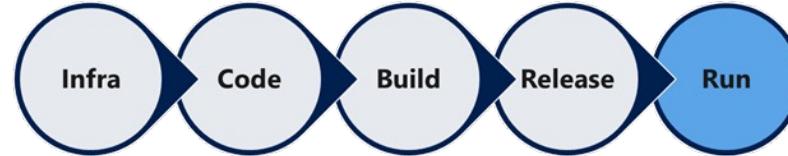
- Make sure container images deployed to Kubernetes are from a trustworthy source
- Do not use the default cluster namespace to deploy applications
- Do not run your container images as root
- Set cluster-wide guardrails using **policy as code**



@AnnieTalvasto

@karlgots

# Kyverno



- Kyverno is a policy engine designed for Kubernetes.
- With Kyverno, policies are managed as Kubernetes resources and no new language is required to write policies.
- This allows using familiar tools:
  - kubectl
  - Git
  - kustomize

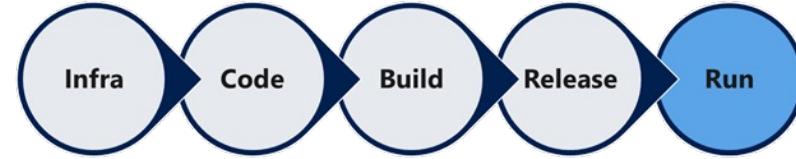


@AnnieTalvasto

@karlgots

# Microsegmentation

- Control the flow of traffic between pods in the cluster
- Network policies are translated into sets of allowed and disallowed IP pairs
- Kubernetes implements these pairs as IPTable rules



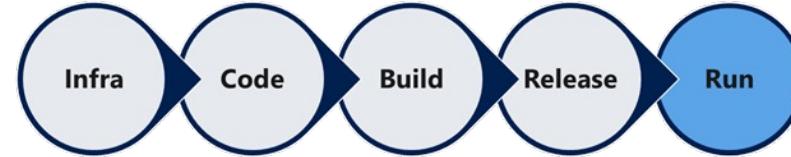
```
1 kind: NetworkPolicy
2 apiVersion: networking.k8s.io/v1
3 metadata:
4   name: backend-policy
5   namespace: development
6 spec:
7   podSelector:
8     matchLabels:
9       app: webapp
10      role: backend
11   ingress:
12     - from:
13       - namespaceSelector: {}
14         podSelector:
15           matchLabels:
16             app: webapp
17             role: frontend
```



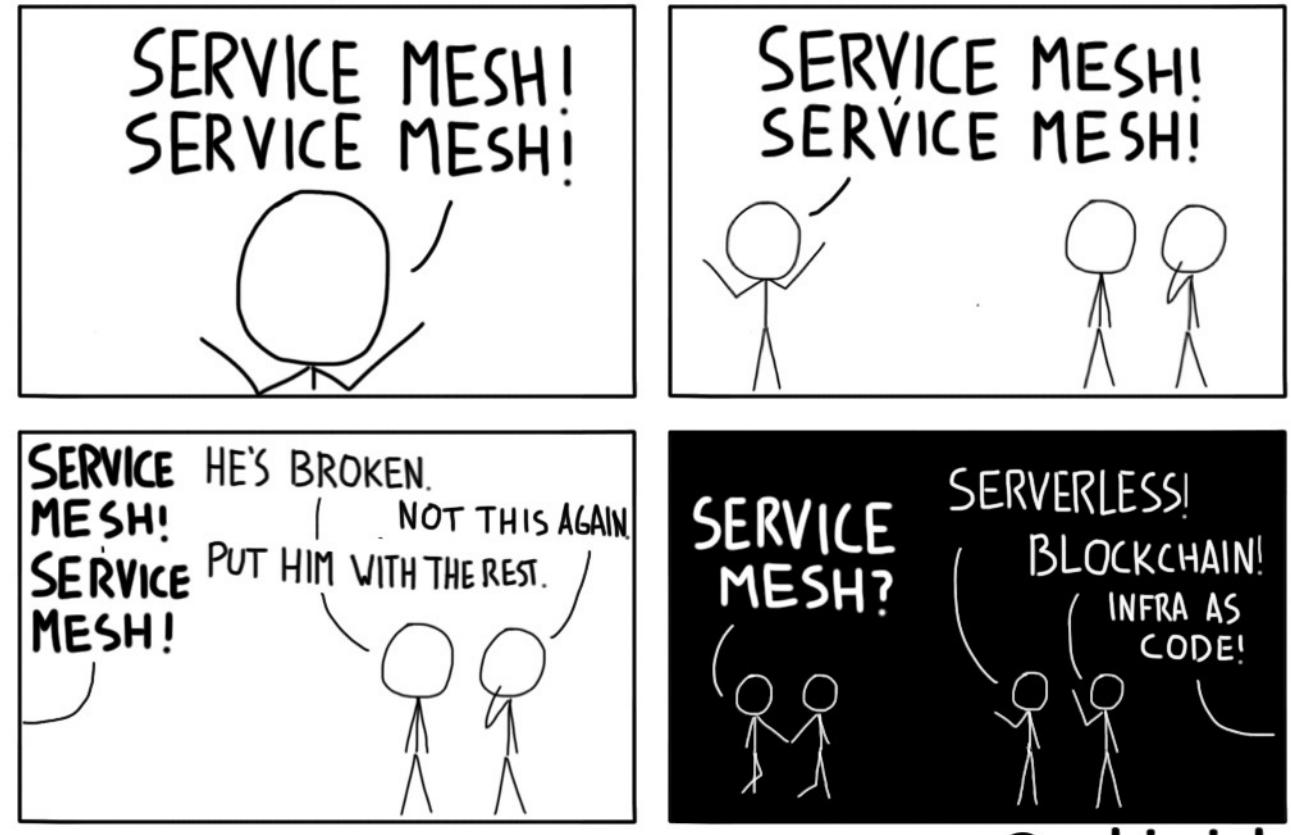
@AnnieTalvasto

@karlgots

# Microsegmentation: Service Meshes



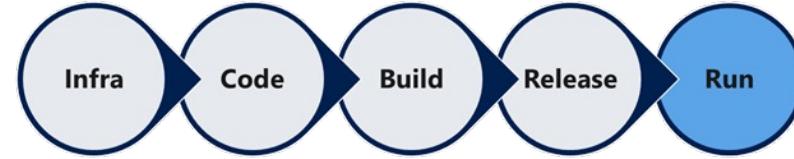
- Manage ingress and egress
- Control cross-pod, cross-namespace, cross-node and cross-cluster networking
- Sidecar or agentless
- Projects: Linkerd, Istio, Open Service Mesh



@AnnieTalvasto

@karlgots

# Linkerd



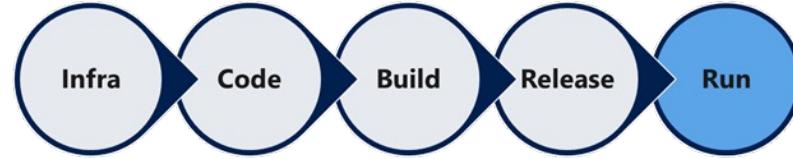
- Community, simple design
- Ultralight, ultrafast, security-first service mesh for Kubernetes.
- The overall goal is to reduce overhead of having a service mesh
- What does it do?
  - Observability
  - Reliability
  - Security



@AnnieTalvasto

@karlgots

# KubeAudit



- kubeaudit is a command line tool to audit Kubernetes clusters for various different security concerns, such as:
  - run as non-root
  - use a read-only root filesystem
  - drop scary capabilities, don't add new ones
  - don't run privileged
- tldr. kubeaudit makes sure you deploy secure containers



@AnnieTalvasto

@karlgots

- Kubeaudit  
nonroot

```
-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: microsoft-defender-pod-collector

-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: microsoft-defender-low-level-collector

-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: low-level-init

----- Results for -----
apiVersion: apps/v1
kind: DaemonSet
metadata:
  name: microsoft-defender-publisher-ds
  namespace: kube-system

-----
-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: microsoft-defender-publisher

-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: old-file-cleaner

----- Results for -----
apiVersion: batch/v1
kind: Job
metadata:
  name: batch-check-job
  namespace: default

-----
-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: batch-check

----- Results for -----
apiVersion: batch/v1
kind: Job
metadata:
  name: hidden-in-layers
  namespace: default

-----
-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: hidden-in-layers
```

```
name: microsoft-defender-publisher-ds
namespace: kube-system
```

---

```
-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: microsoft-defender-publisher

-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: old-file-cleaner
```

---

```
----- Results for -----
```

```
apiVersion: batch/v1
kind: Job
metadata:
  name: batch-check-job
  namespace: default
```

---

```
-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: batch-check
```

---

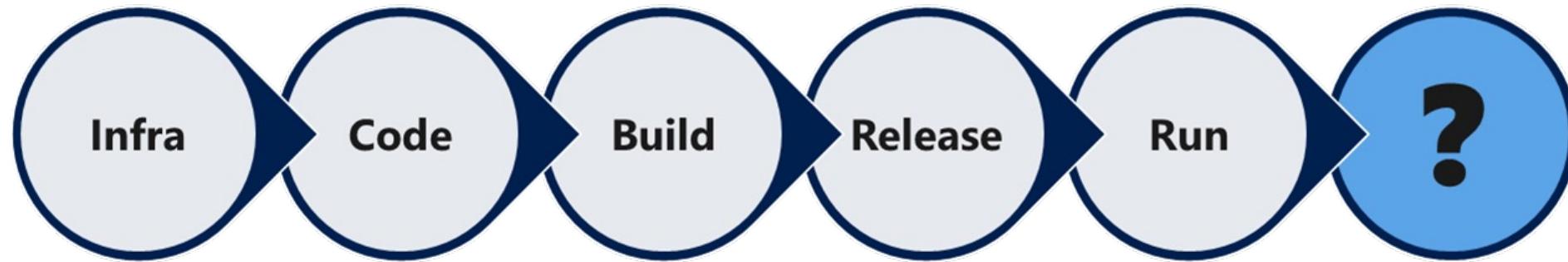
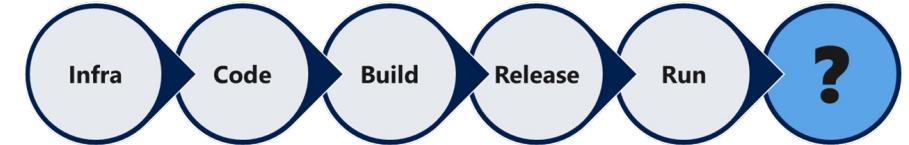
```
----- Results for -----
```

```
apiVersion: batch/v1
kind: Job
metadata:
  name: hidden-in-layers
  namespace: default
```

---

```
-- [error] RunAsNonRootPSCNilCSCNil
Message: runAsNonRoot should be set to true or runAsUser should be set to a value > 0 either in the container SecurityContext or PodSecurityContext.
Metadata:
  Container: hidden-in-layers
```

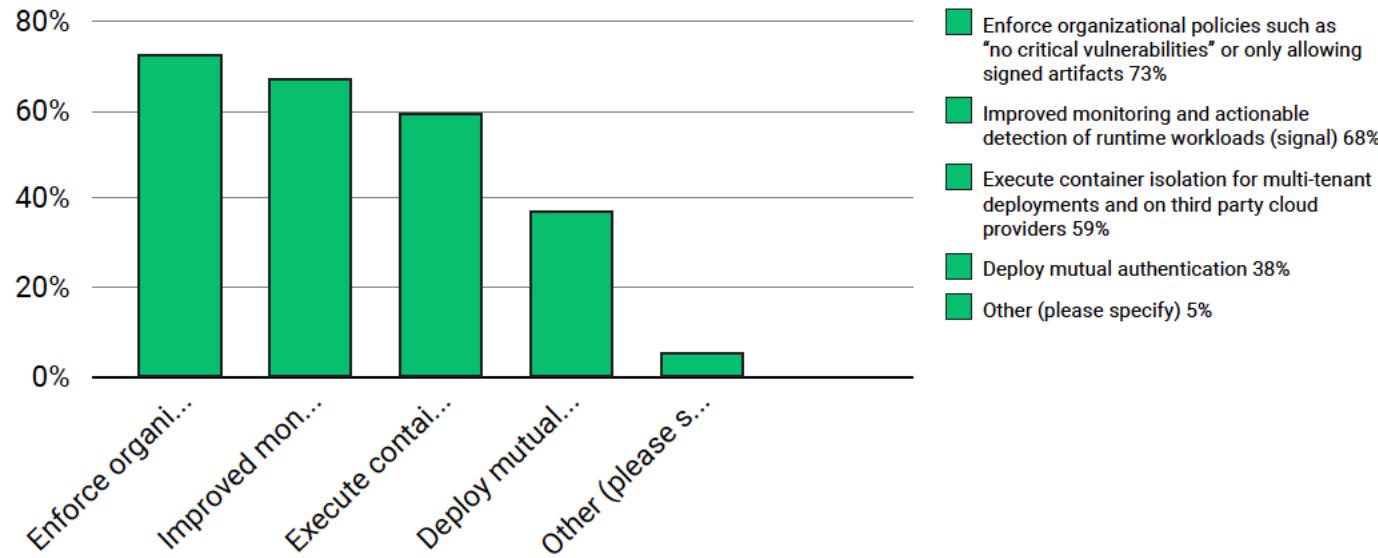
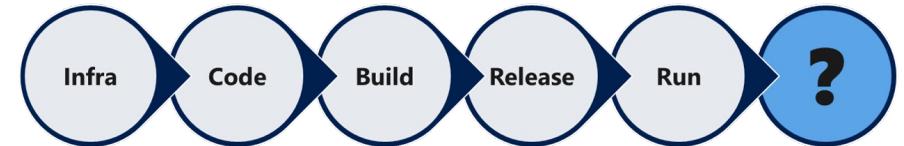
# Future & Predictions



@AnnieTalvasto

@karlgots

# Security Investments



Where do you intend to focus your efforts for greater security in cloud native over the next 2-5 years?



@AnnieTalvasto

@karlgots

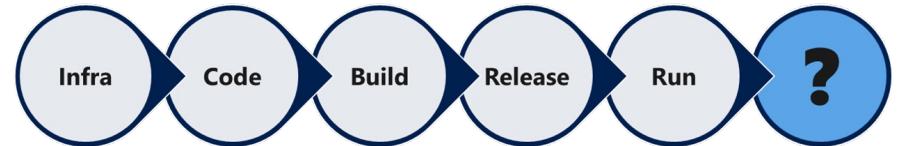
# Challenges in Cloud Native Security

1. A lack of technical expertise – 58%
2. Trouble matching new methods and processes like DevOps and CI/CD with existing requirements, tools, or processes – 51%
3. Data security – 49 %
4. The complexity of building, deploying, and management – 46%

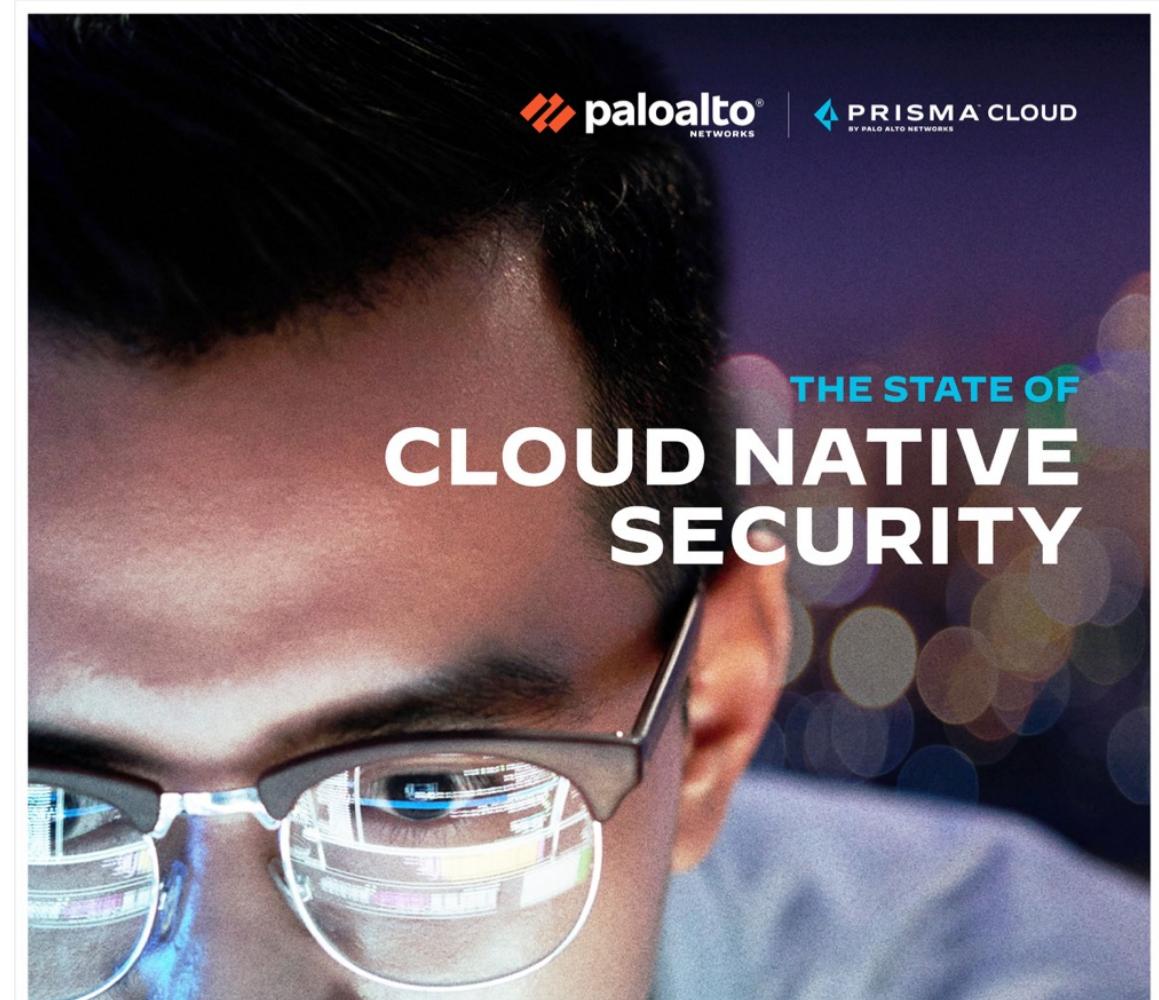


@AnnieTalvasto

@karlgots



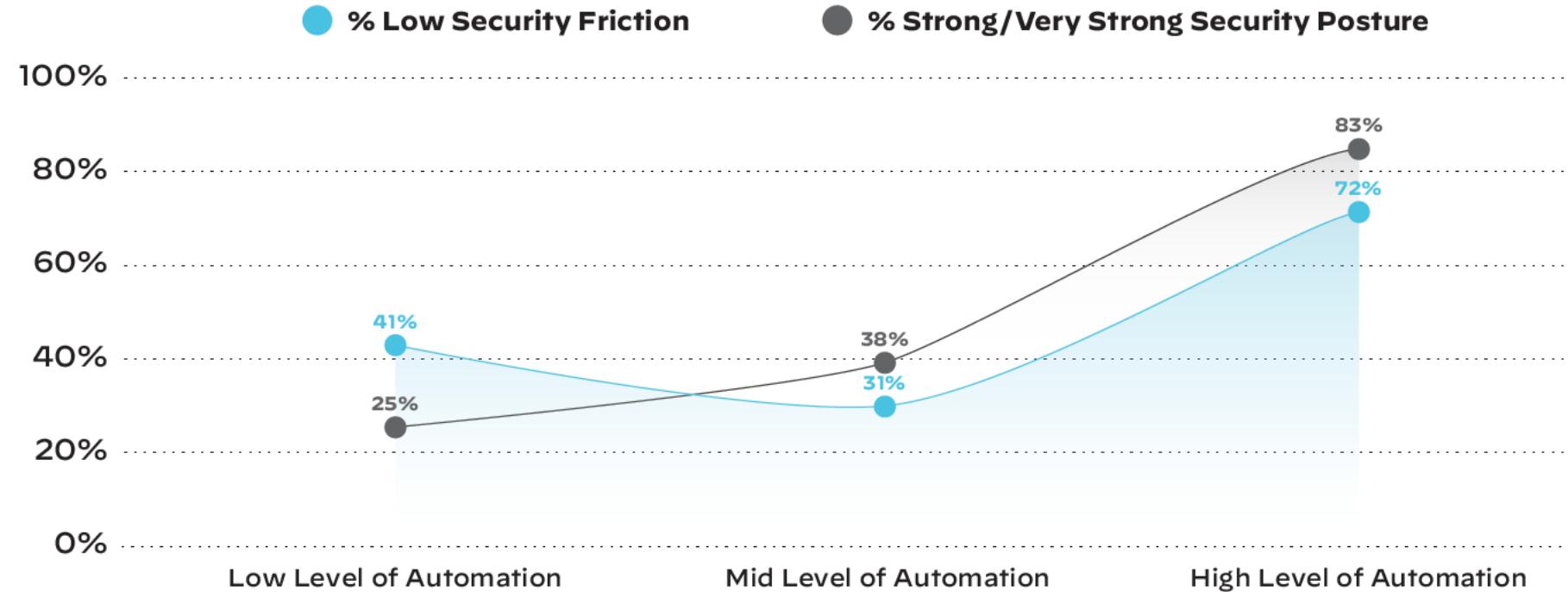
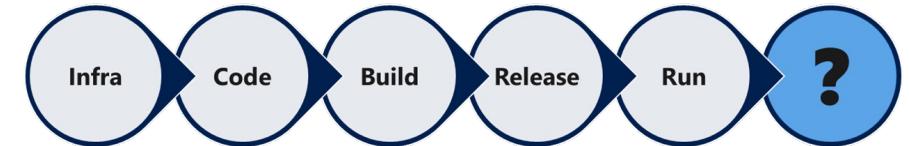
# State of Cloud Native Security Report



@AnnieTalvasto

@karlgots

# Cloud Native Security Report



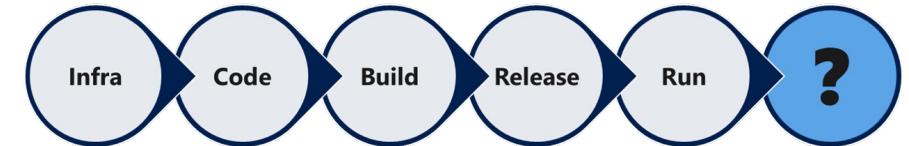
**Figure 16:** Automation as a driver of security outcomes



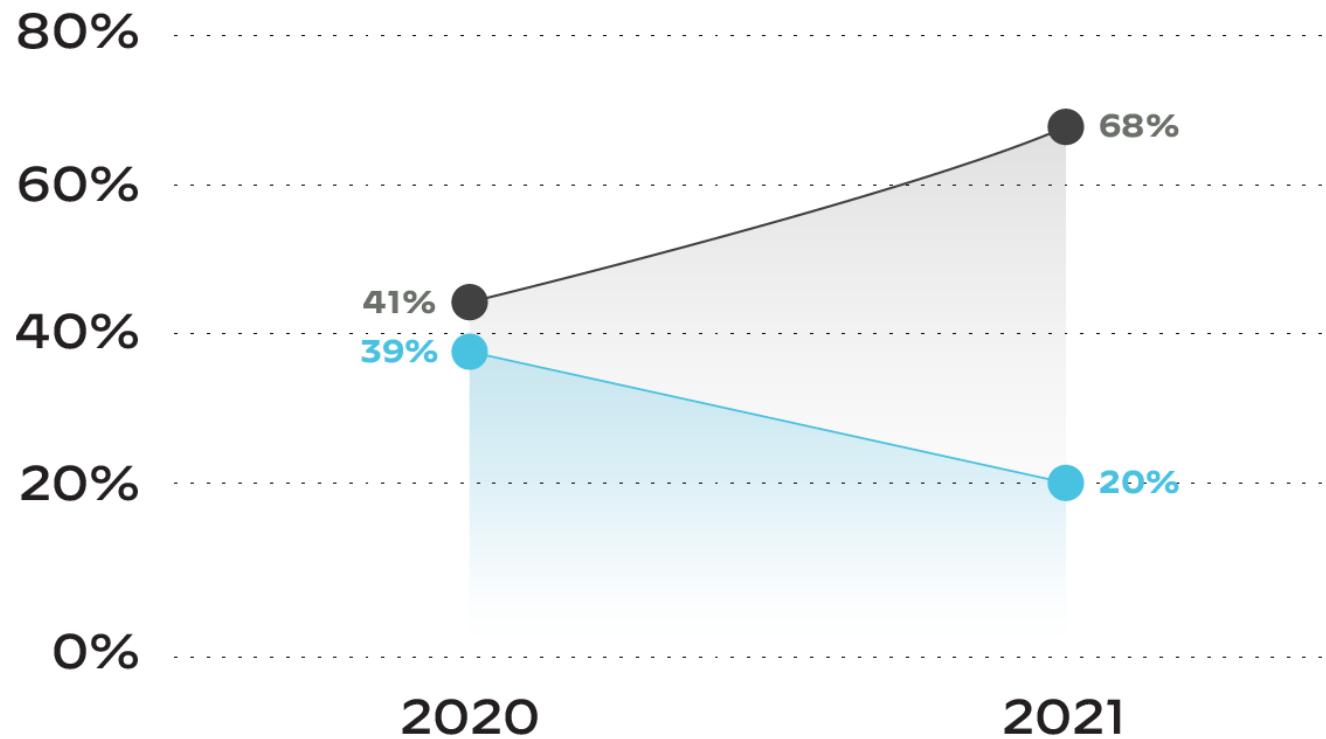
@AnnieTalvasto

@karlgots

# Cloud Native Security Report



● 1-5 Security Vendors   ● 6-10 Security Vendors



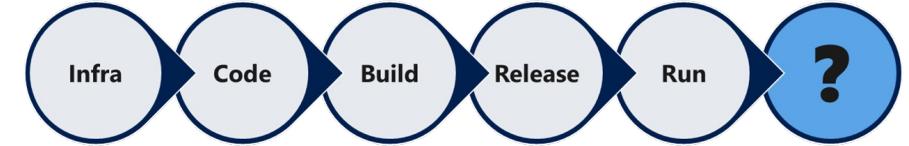
**Figure 8:** Changes to number of security vendors



@AnnieTalvasto

@karlgots

# Future & Predictions



- Containers will be more integrated with the cloud
- Kubernetes will get closer to PaaS because cloud providers have better security defaults



@AnnieTalvasto

@karlgots

# Agenda

- Introduction
- State of Cloud Native Security
- Cloud Native Security (in the Enterprise)
- Takeaways & Resources



@AnnieTalvasto @karlgots

# CNCF Landscape

## Security & Compliance



@AnnieTalvasto

@karlgots

# CNCF Resources

## Security TAG

- Advises other Kubernetes projects on security
- Coordinates the recurring pentest

## CNCF DevSecOps radar

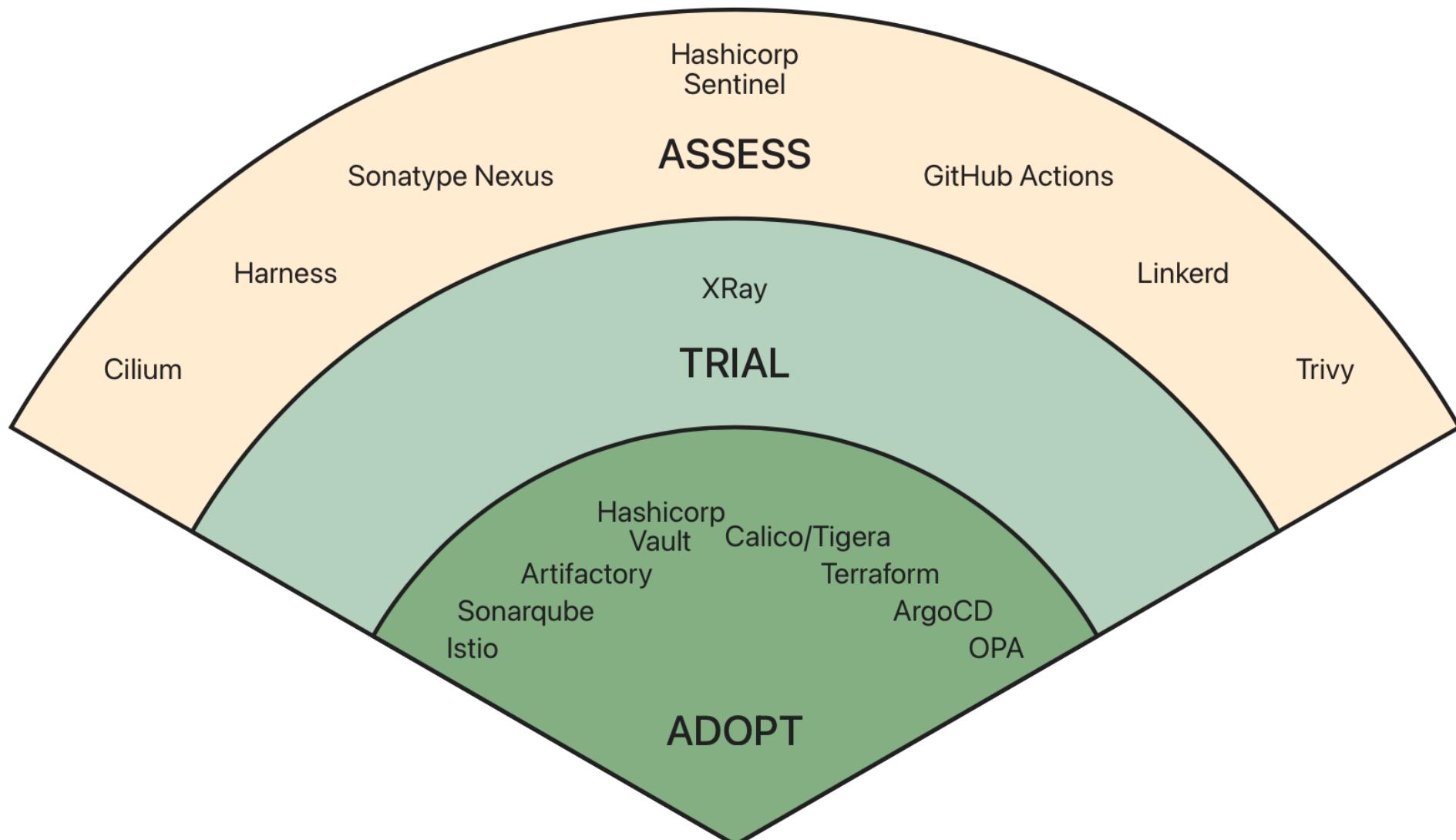
## CNCF Microsurvey on security



@AnnieTalvasto

@karlgots

# DevSecOps, September 2021



Download as [svg](#) or [png](#)

# CNCF Resources

## Security TAG

- Advises other Kubernetes projects on security
- Coordinates the recurring pentest

## CNCF DevSecOps radar

## CNCF Microsurvey on security



@AnnieTalvasto

@karlgots

# CNCF Microsurvey on Security

## Cloud Native Security Microsurvey:

More than 80% of organizations want to build modern security systems with open source software



# Tools

- IAC SAST
  - Checkov
  - Tenable
  - KICS
- Scanning tools
  - docker scan
  - Kubeaudit
- Runtime security
  - Kubescape
  - Falco
- Materials
  - CIS Security Benchmark for Kubernetes
  - NSA Kubernetes hardening guide
  - Threat matrix for Kubernetes
  - Kubernetes Goat
- Slides:
  - [github.com/AnnieTalvasto/presentations](https://github.com/AnnieTalvasto/presentations)



# Takeaways

- Compared to PaaS, Kubernetes allows for more security controls to be put in place
  - This comes with more responsibilities!
- Every application is different
  - You might not need all (or any) of the security controls listed in this session
- Cloud native security is continuously evolving
  - Check the backlog(s) and challenge your (perceived) security risks and controls

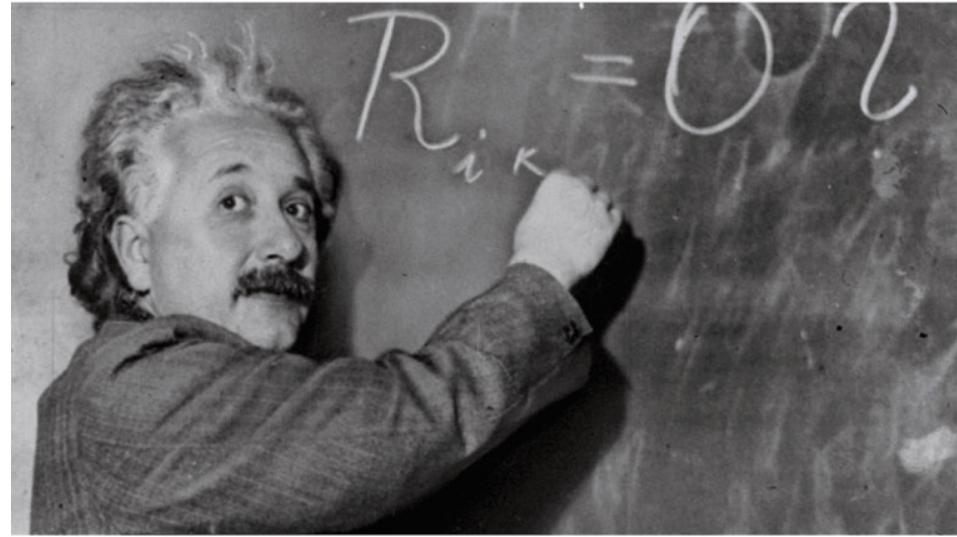


@AnnieTalvasto

@karlgots

# Thank you!

How I think I look explaining cyber risk to the board



How I actually look



# Thank you to our Sponsors!



{ } NDC Conferences

**Olmec**  
quality through innovation



Octopus Deploy



Sage



GitHub

