KubeCon CloudNativeCon North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022

From Security Testing to Deployments in a Single PR

Sarah Khalife
Solutions Engineering @ GitHub

Grant Griffiths
Software Engineering @ Portworx

GitHub

Sarah Khalife

@skhalife

@_skhalife

Principal Solutions Engineer

- 3 years @ GitHub
- Previously Cloud Apps & Platform Engineer
- Focused on automation, security, and developer tools
- For fun, I enjoy volleyball, travel, and the beach!

portworx

Grant Griffiths

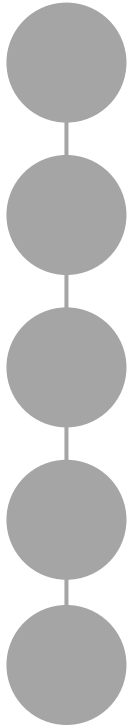
@ggriffiths

@griffithsgrant

Member of Technical Staff

- 4 years @ Portworx - CSI Driver, Open source
- Previously Data Services & Platform Engineer @ GE
- Contributor to SIG Storage and Kubernetes-CSI
- For fun, I like climbing, surfing, and trail running 🧗 🌊

Agenda



- Introduction + Overview
- Security Scanning
- Automation + CI
- Live Demo
- Takeaways + Benefits

Agenda

- **Introduction + Overview**
- Security Scanning
- Automation + CI
- Live Demo
- Takeaways + Benefits

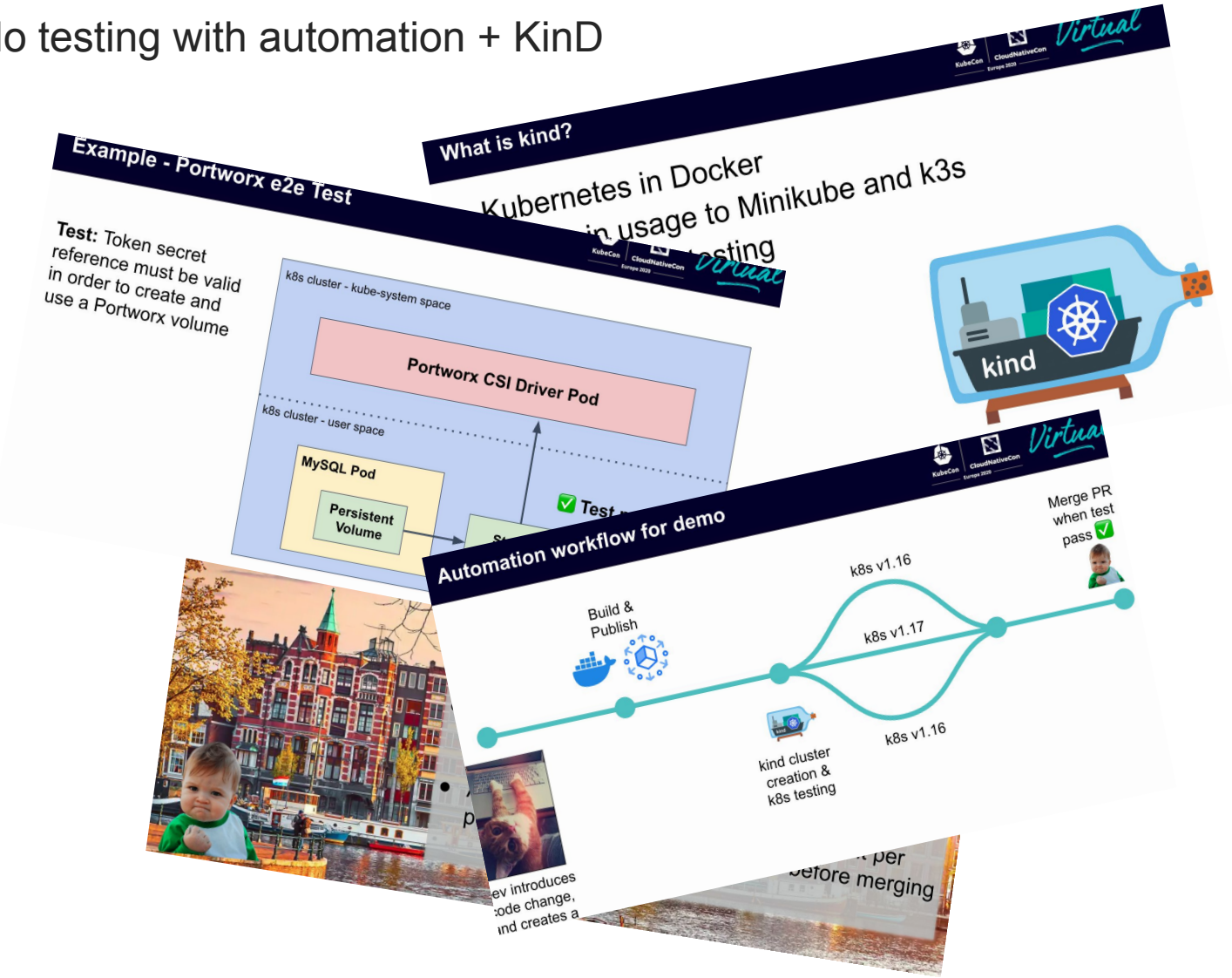
Previously…

We gave a talk at KubeCon EU 2020 on how to do testing with automation + KinD

KubeCon CloudNativeCon Europe 2020 Virtual

Kind-ly Validating your K8s Apps Automatically per PR

Sarah Khalife & Grant Griffiths



What we'll cover

1. Simple set of steps to automate build process, while incorporating security from the start
2. Leveraging open source and free tooling to run scans across code, dependencies, and cloud native components
3. Automate the containerization and triggering security scans per pull request, validating before merging new code

Goals

Run integration + security test on all new code changes

- Reduce amount of bugs
- Scan for vulnerabilities
- Build + validate at one time

Configure branch rules for relevant scans and testing

- Maintain consistency in results
- Set expectation for required tests

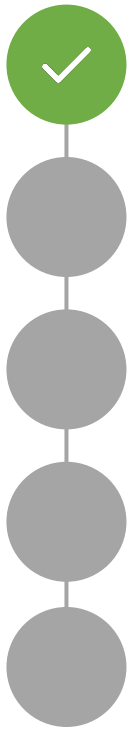
Detect earlier and block merge if tests have failed and alerts aren't fix

- Don't introduce vulnerable code into main branch
- Fix issue with the right context

Automate everything with event triggers

- Standardize on types of scans and tools
- Repeatable and easy to implement

Agenda



Introduction + Overview

Security Scanning

Automation + CI

Live Demo

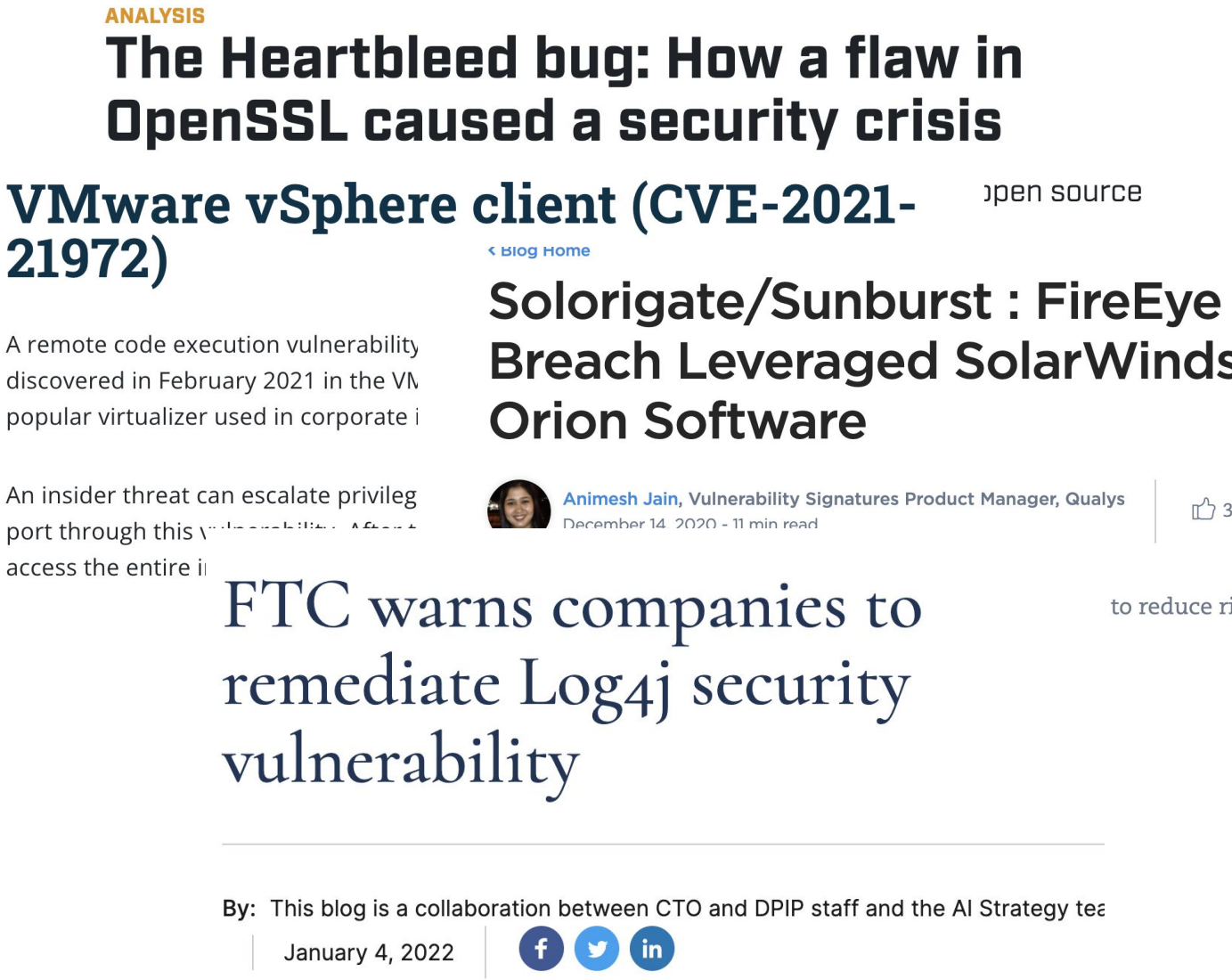
Takeaways + Benefits

Motivation

- Recent vulnerability exploits
- Going back and fixing issues is never a fun process
- Security scans can be frustrating or cause friction
- Splunk state of security:

65% of organizations worldwide report an increase in attempted cyberattacks.

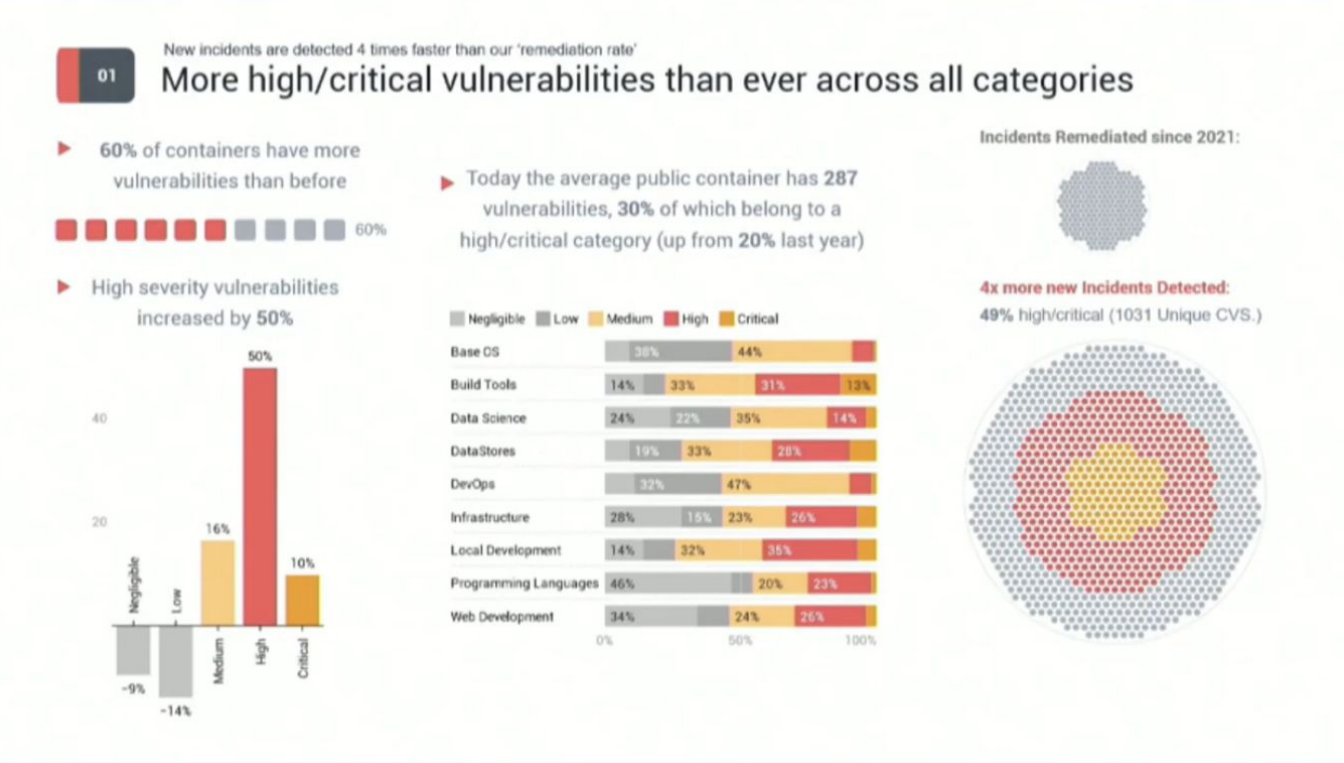
59% of security teams say they had to devote significant time and resources for remediation (up from 42% a year ago).



Motivation

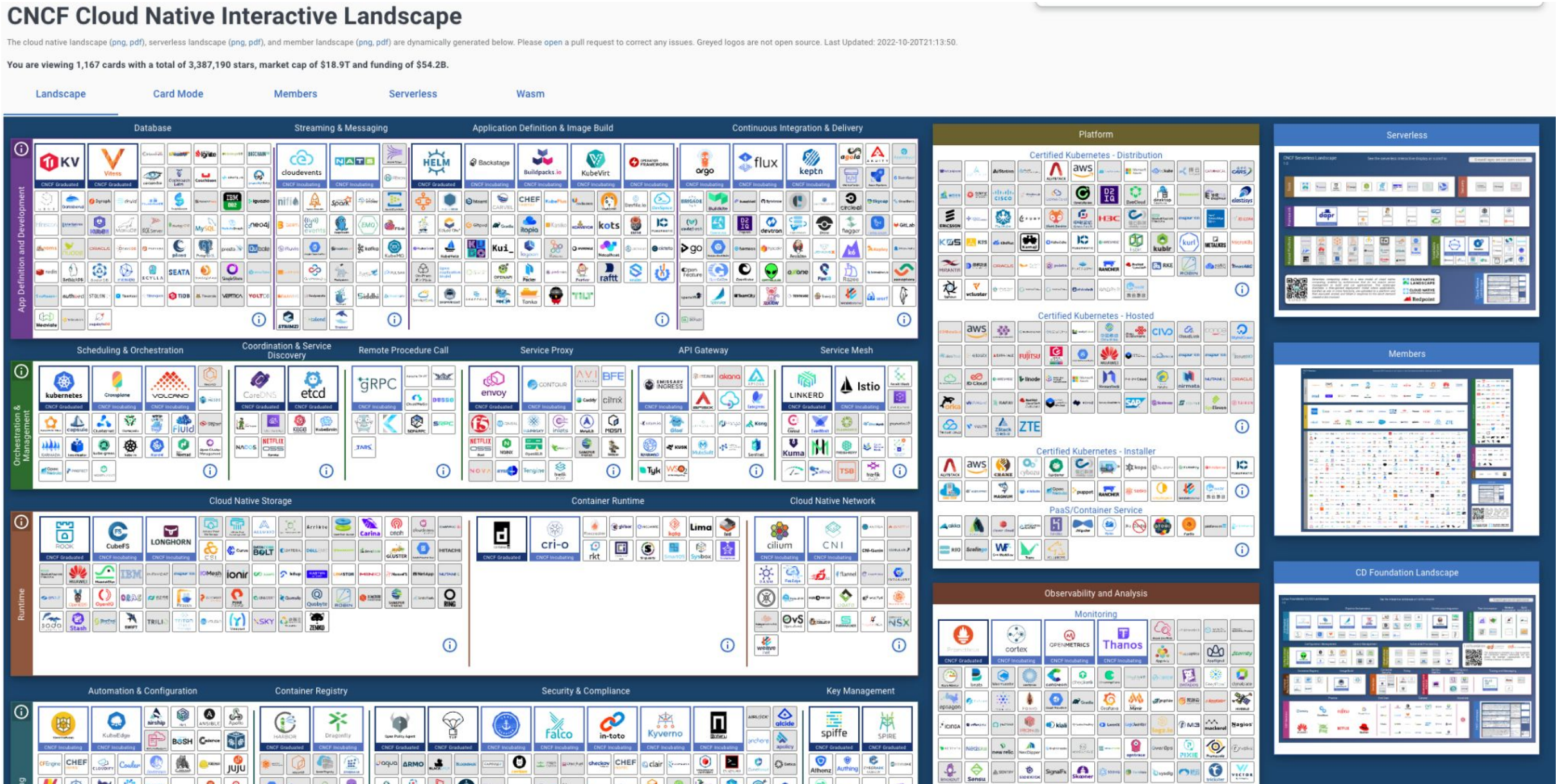
From the Keynote session on Wednesday, slim.ai's findings

- More **High/Critical** vulnerabilities than before!



CNCF Security Ecosystem

KubeCon CloudNativeCon North America 2022



Types of Security Scanning

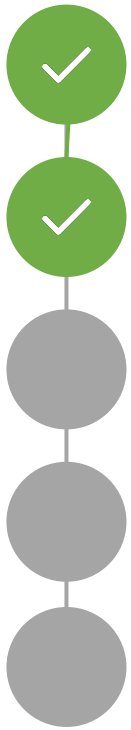
1. **Image scanning:** Build image, scan it

2. **Dependency checks:** Check for known vulnerabilities in your dependencies

3. **Static code analysis:** Analyze your code

4. **Configurations checks:** Check k8s YAMLs and other Infrastructure as code

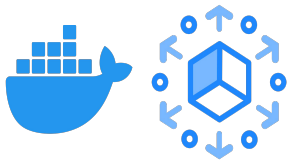
Agenda



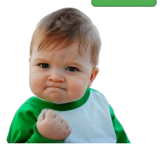
- Introduction + Overview
- Security Scanning
- **Automation + CI**
- Live Demo
- Takeaways + Benefits

Typical Workflow

Build job
Build image and test



Merge PR
When tests pass ✅



Dev complete
Let's release soon!

QA Team
Runs all security scans

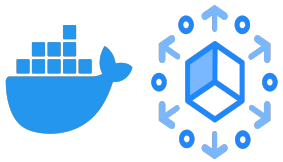
Missed Deadline

Dev introduces code change, and creates a PR

Scan Failed!
File issue and assign to dev

Improved Workflow

Build job
Build image and test



Dev introduces code change, and creates a PR

Parallel Vulnerability Scanning

Containers:
Trivy

Dependencies:
Dependabot

Static Analysis:
CodeQL

Infrastructure:
TFSec

Merge PR:
When tests pass

Deploy Image!

Agenda

- Introduction + Overview
- Security Scanning
- Automation + CI
- **Live Demo**
- Takeaways + Benefits

Demo Project: Stork

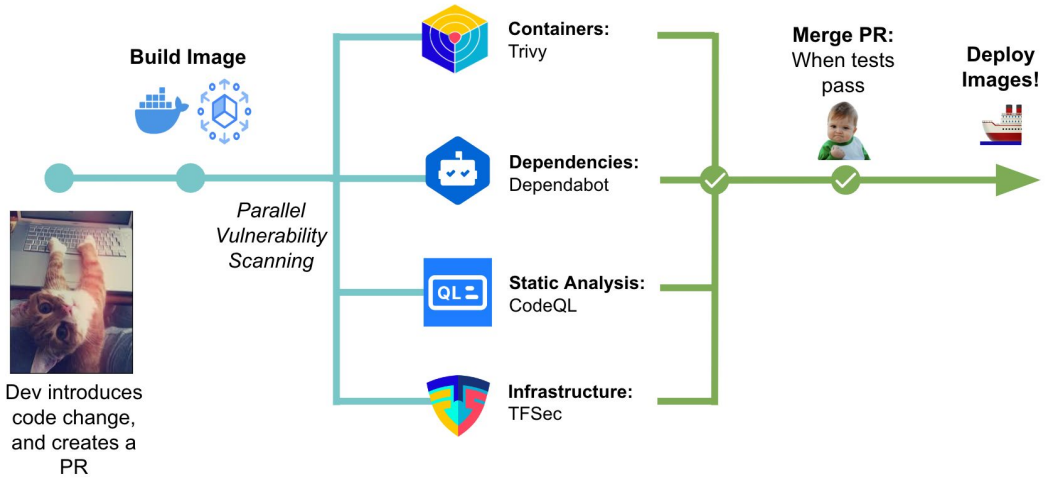
- Open source project by Portworx
  - K8s scheduler plugin
  - Volume Group Snapshots
  - Object Service controller

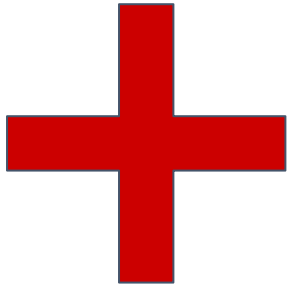
- github.com/libopenstorage/stork

portworx
by Pure Storage

What we'll demo

1. Show open pull requests
   - Failed builds - vulnerabilities
   - Branch protection rules
2. Merge successful PR
3. Image deployed to DockerHub





Sample PRs

1. **TFSec IaC Config file scan:** https://github.com/stork-kubecon22/stork/compare/master...add-db
2. **SQL Injection**: github.com/stork-kubecon22/stork/pull/7
3. **Dependency Review:** github.com/stork-kubecon22/stork/pull/9
4. **Trivy Image Scan:** github.com/stork-kubecon22/stork/pull/11

Demo Time!

Demonstrated Workflow

Dev introduces code change, and creates a PR

Build job
Build image and test

Parallel Vulnerability Scanning

Containers:
Trivy

Dependencies:
Dependabot

Static Analysis:
CodeQL

Infrastructure:
TFSec

Merge PR:
When tests pass

Deploy Image!

Agenda

- Introduction + Overview
- Security Scanning
- Automation + CI
- Live Demo
- **Takeaways + Benefits**

Takeaways

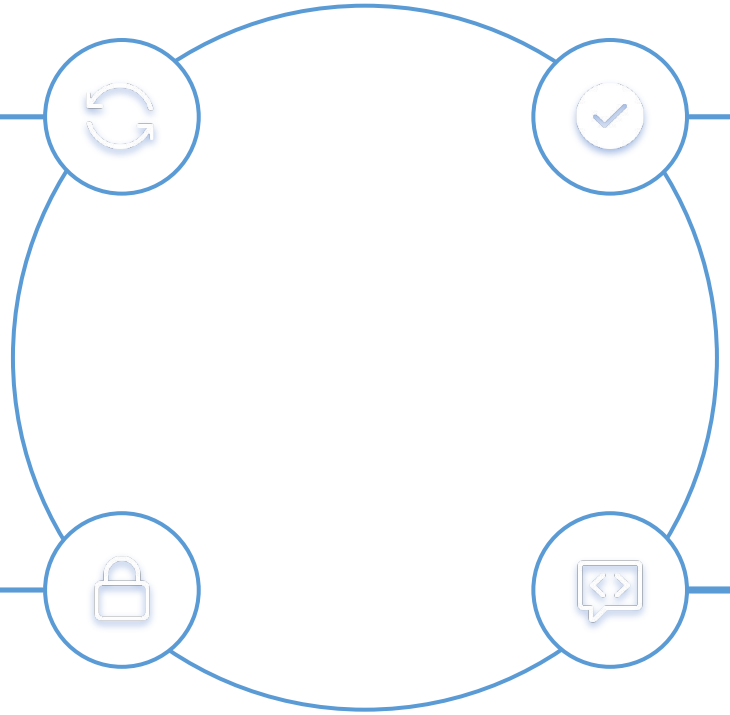
Providing transparency on requirements + fixing vulnerabilities within PR

Continuous Integration

Kick off builds automatically
Run integrations tests
Trigger security scans
Get results before merge

Provide Transparency

Set consistent expectations
Configure branch protection rules
Supply chain analysis
Code Scanning results



Fix in minutes

Build + Security alerts in PR
Automated triggers + fixes
Scoped to your build process
No context switching

Collaboration

Make it easy!
Open conversation
Vulnerability fixes w/ code review
Share knowledge with team

Q&A

- Introduction + Overview
- Security Scanning
- Automation + CI
- Live Demo
- Takeaways + Benefits

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Please scan the QR Code above to
leave feedback on this session

Thank you

Sarah Khalife

Solutions Engineering @ GitHub

Grant Griffiths

Software Engineering @ Portworx

Thank you

ABSTRACT

Automating cloud native app development and incorporating security through a transparent and consistent process is key in building any production level applications. On a daily basis, think about how often you build your application and scan for vulnerabilities in the code. This is mostly an afterthought and not always considered as the easy part of developing any applications. However, the recent vulnerability exploits reinforced the need for a secure development lifecycle. Simplifying and automating the process all in a single pull request makes it much easier for any cloud app developer to add security!

This talk will cover how to leverage available open source tooling to build and test a cloud native application, run security scans across it, and package it for shipping. For automation, we will have a step-by-step demonstration on how to set it up all within a PR to provide consistency and push the containerized application to a Kubernetes environment.

BENEFITS TO THE AUDIENCE

The cloud native ecosystem, as well as, the amount of kubernetes application developers are constantly growing. When talking about deploying k8s applications, a common focus is on efficiency or cost cutting, but not on security. Yet, security has also been a growing discussion over the last several years, and that has definitely been reinforced over the last few months.

The goal of this talk is to bring awareness for developers to incorporate code and container scanning early more often. This will make it much easier to fix any vulnerabilities when committing new code rather than waiting to run scans after the fact.

I believe the audience will be able to jump into this session and gain practical knowledge when working with security. In a live demo of an k8s app deployment, I will cover the benefits of

- containerizing your application,
- running security scans of code,
- and automating it all in the pull request (including concepts around CI/CD).

From Security Testing to Deployments in a Single PR

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2022

Sarah Khalife
Solutions Engineering
@ *GitHub*

Grant Griffiths
Software Engineer
@ *Portworx*

KubeCon | CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022