Security Chaos Engineering: When and How You Should Break Your System

Anais Urlichs

OWASP
LONDON

Disclaimer

This is me

aqua

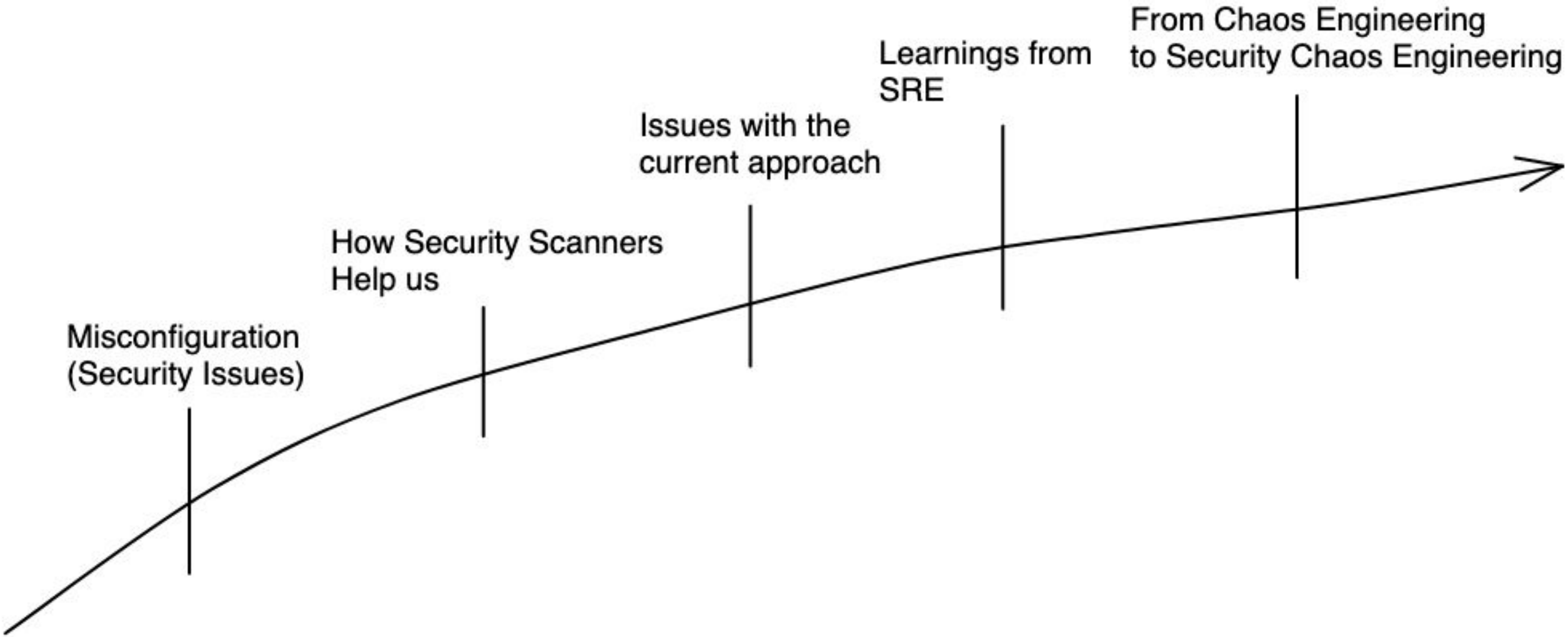
YouTube

anaisurl.com

CLOUD NATIVE COMPUTING FOUNDATION

Open:UK

What to expect from this presentation



Misconfiguration (Security Issues)

How Security Scanners Help us

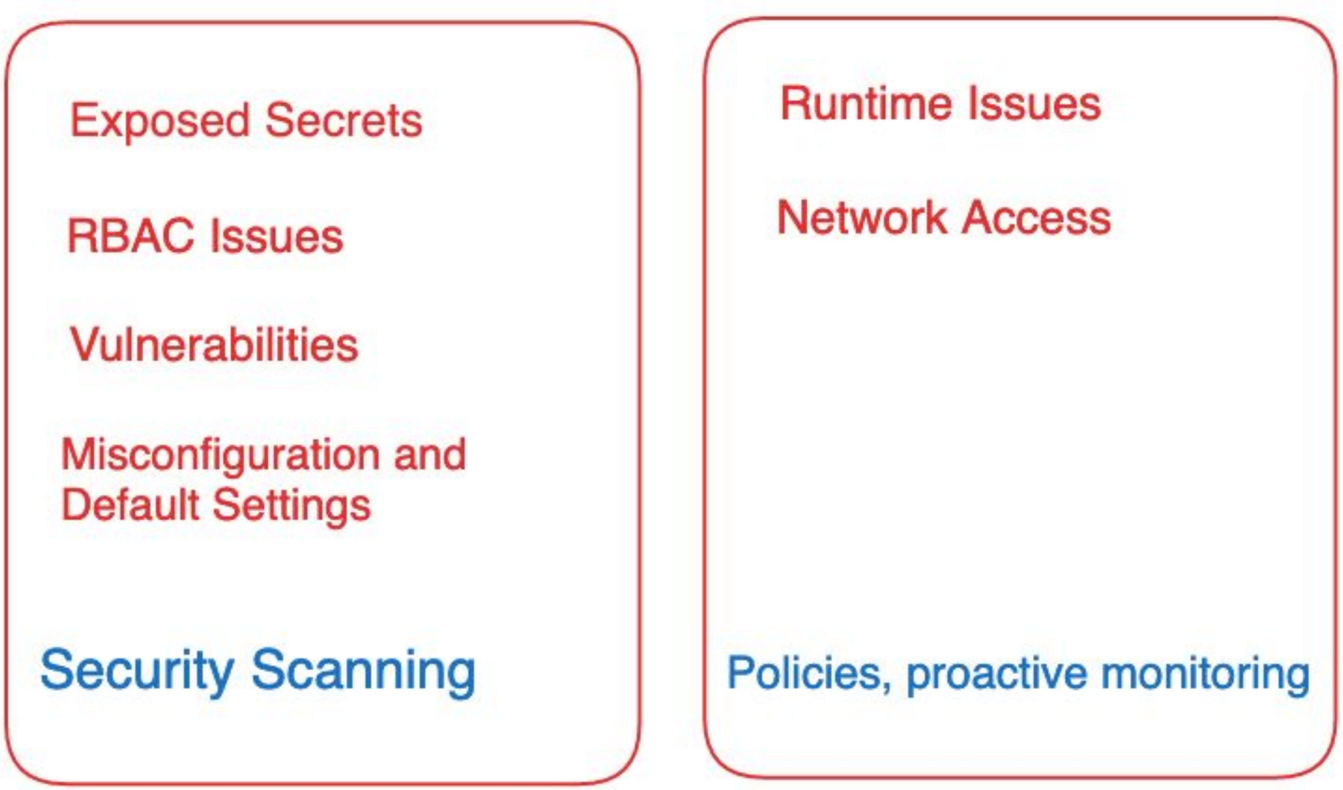
Issues with the current approach

Learnings from SRE

From Chaos Engineering to Security Chaos Engineering

Security Issues

In your Kubernetes cluster/cloud environment



Exposed Secrets

RBAC Issues

Vulnerabilities

Misconfiguration and Default Settings

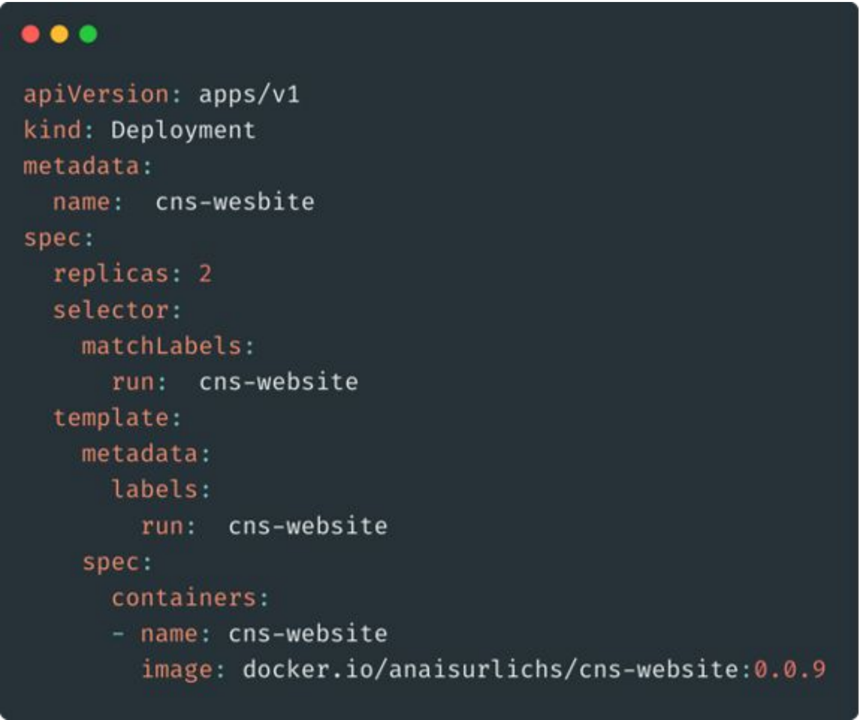
Security Scanning

Runtime Issues

Network Access

Policies, proactive monitoring

What are misconfiguration?

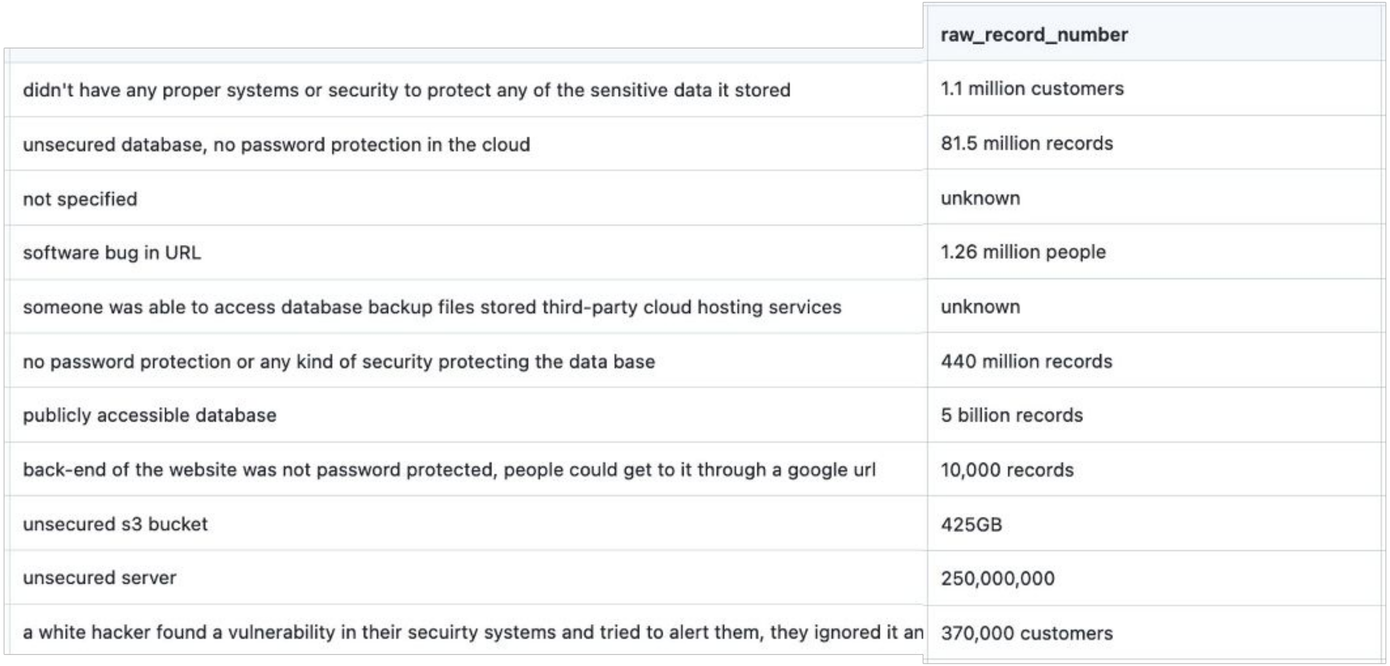


```
apiVersion: apps/v1
kind: Deployment
metadata:
  name:  cns-wesbite
spec:
  replicas: 2
  selector:
    matchLabels:
      run:  cns-website
  template:
    metadata:
      labels:
        run:  cns-website
    spec:
      containers:
      - name: cns-website
        image: docker.io/anaisurlichs/cns-website:0.0.9
```

Configuration Tools

Cloud Platforms/SaaS

Misconfigurations are everywhere

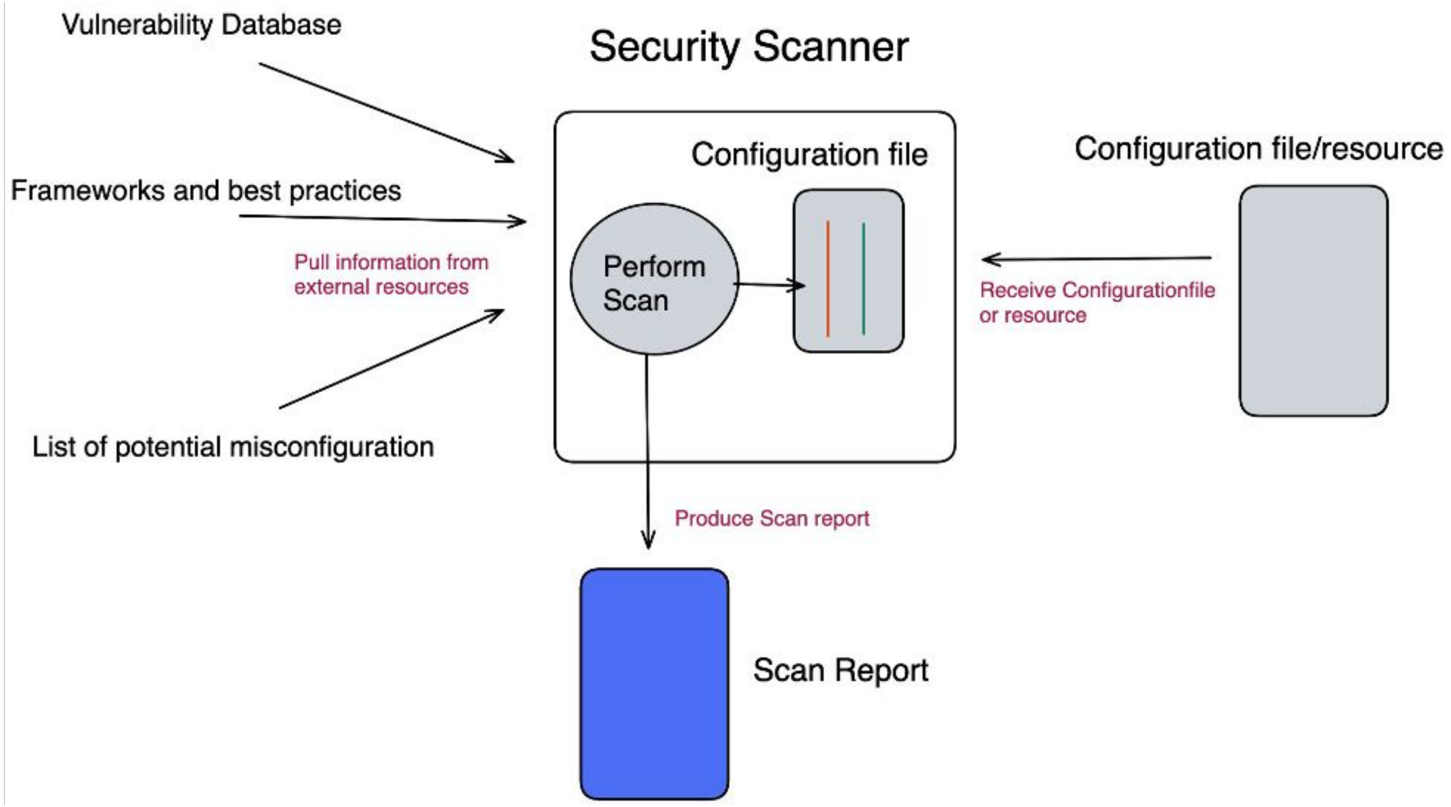


	raw_record_number
didn't have any proper systems or security to protect any of the sensitive data it stored	1.1 million customers
unsecured database, no password protection in the cloud	81.5 million records
not specified	unknown
software bug in URL	1.26 million people
someone was able to access database backup files stored third-party cloud hosting services	unknown
no password protection or any kind of security protecting the data base	440 million records
publicly accessible database	5 billion records
back-end of the website was not password protected, people could get to it through a google url	10,000 records
unsecured s3 bucket	425GB
unsecured server	250,000,000
a white hacker found a vulnerability in their secuirty systems and tried to alert them, they ignored it an	370,000 customers

Source: https://github.com/rapid7/data/blob/main/2021-cloud-misconfigurations/2021-cloud-misconfigurations.csv

How does Security Scanning Usually work?

How do security scanners work



Our main open source projects -- https://github.com/aquasecurity

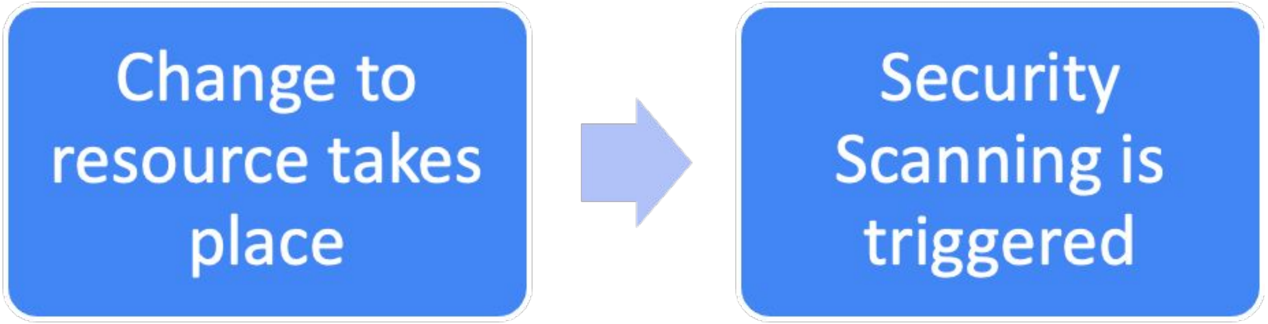
aqua trivy

Cloud native, open source security scanner

aqua tracee

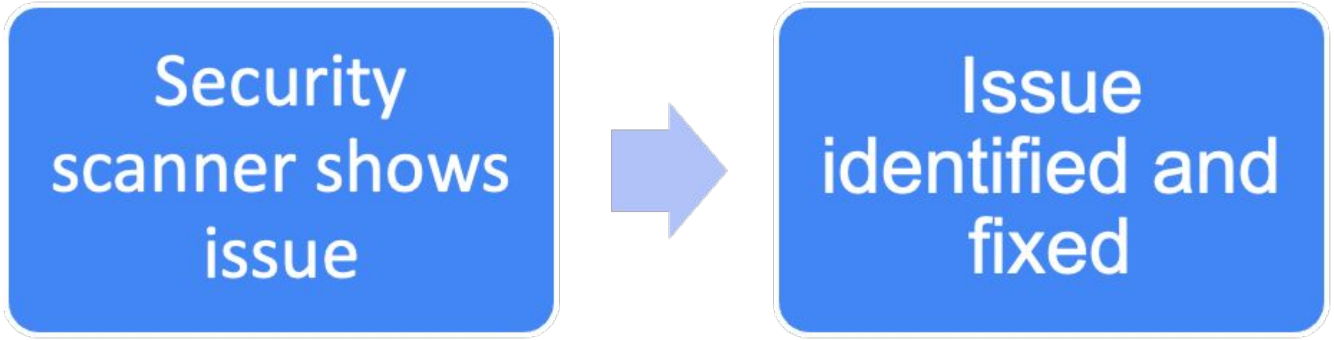
Runtime, security and forensic tool using ebpf

How does our workflow look like



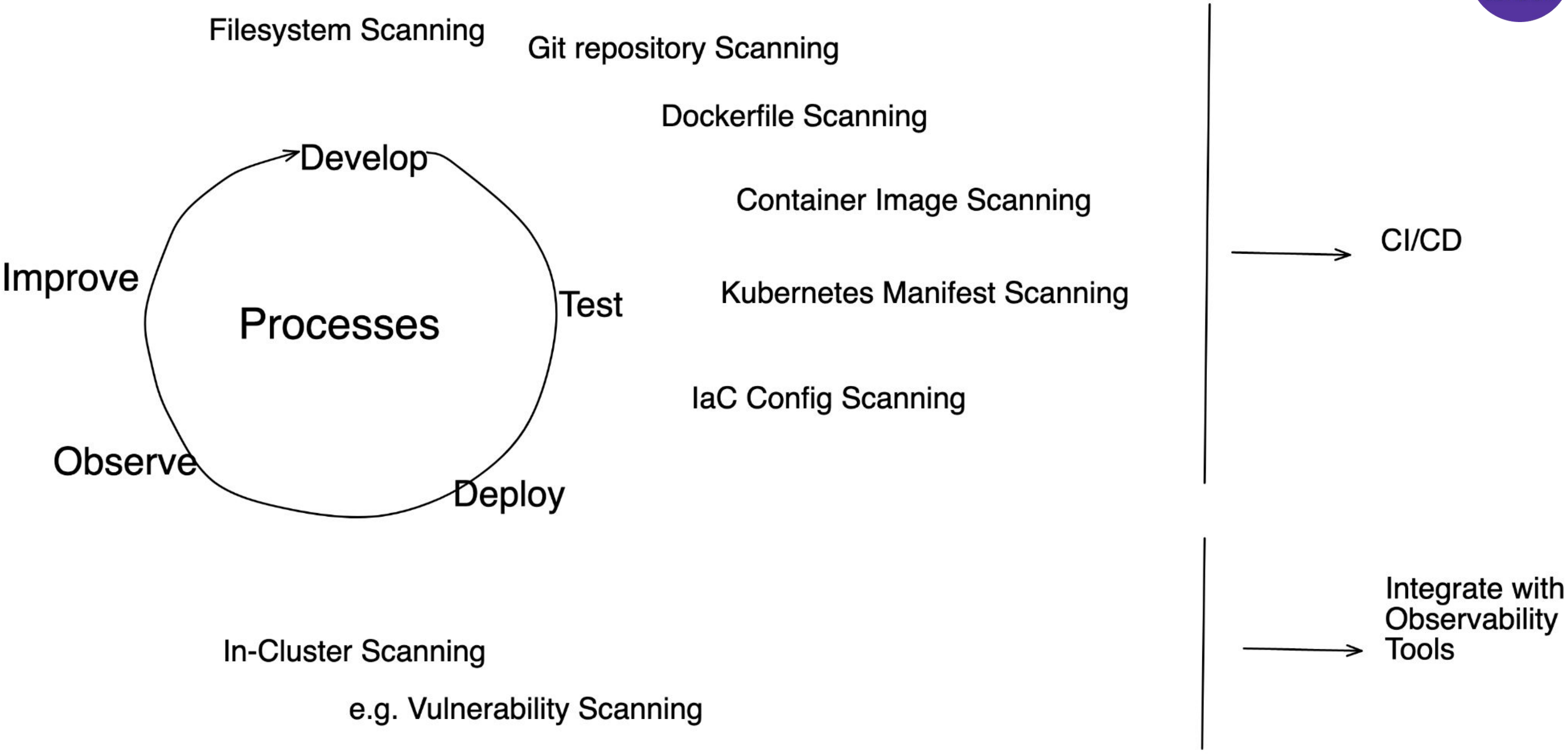
Change to resource takes place

Security Scanning is triggered



Security scanner shows issue

Issue identified and fixed



Processes

Develop

Test

Deploy

Observe

Improve

Filesystem Scanning

Git repository Scanning

Dockerfile Scanning

Container Image Scanning

Kubernetes Manifest Scanning

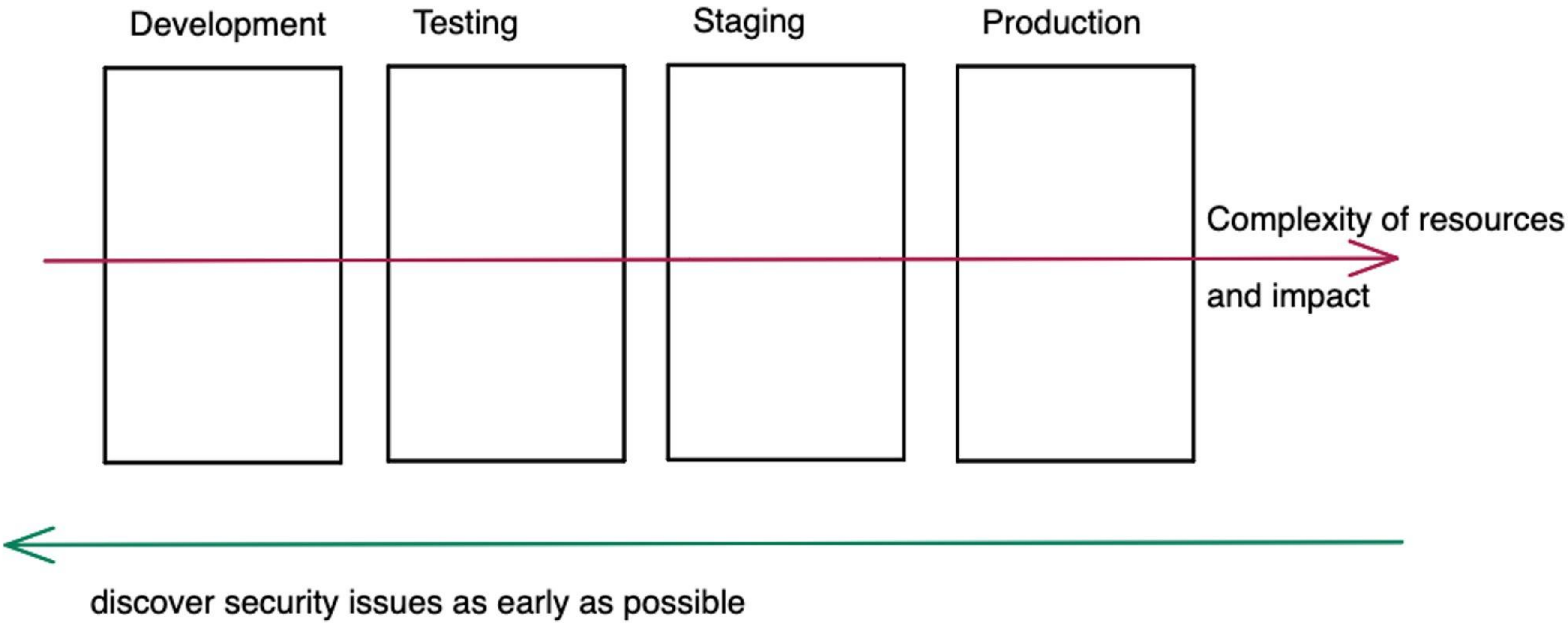
IaC Config Scanning

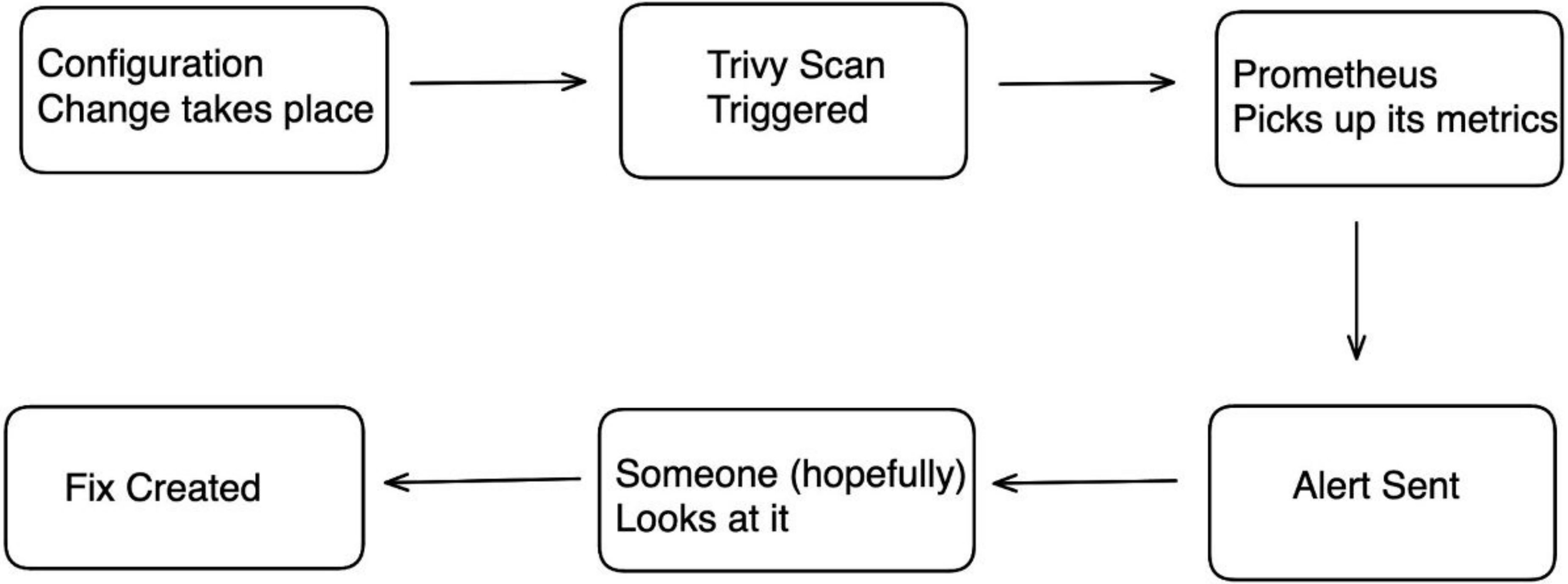
CI/CD

In-Cluster Scanning

e.g. Vulnerability Scanning

Integrate with Observability Tools


Development
Testing
Staging
Production
Complexity of resources
and impact
discover security issues as early as possible



Configuration Change takes place

Trivy Scan Triggered

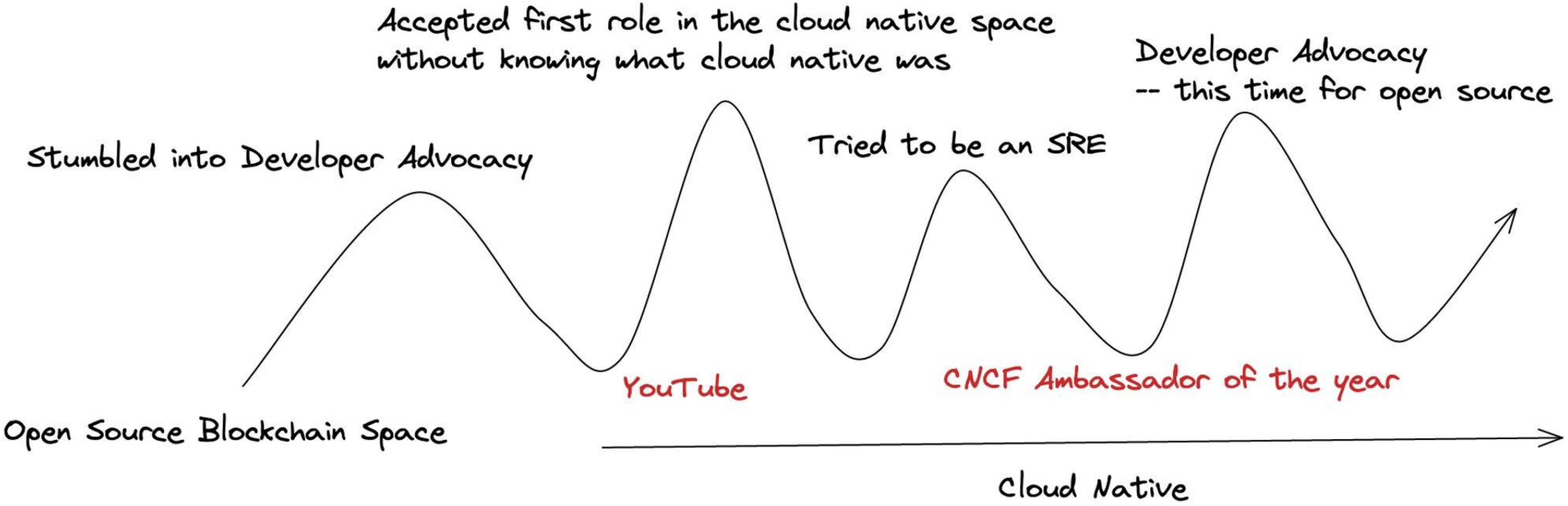
Prometheus Picks up its metrics

Alert Sent

Someone (hopefully) Looks at it

Fix Created

How can we ensure our processes are working as expected?



Accepted first role in the cloud native space without knowing what cloud native was

Developer Advocacy -- this time for open source

Stumbled into Developer Advocacy

Tried to be an SRE

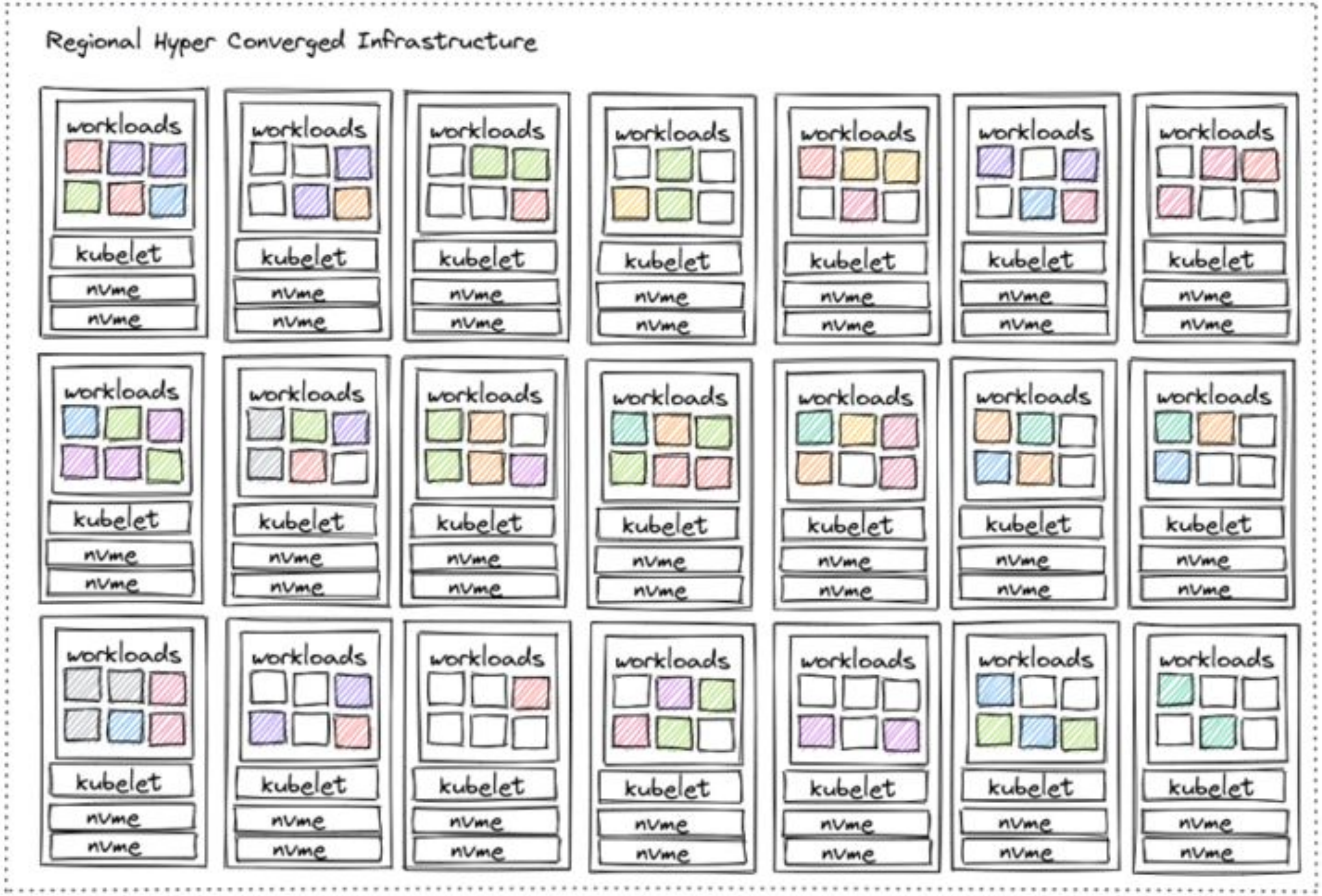
YouTube

CNCF Ambassador of the year

Open Source Blockchain Space

Cloud Native

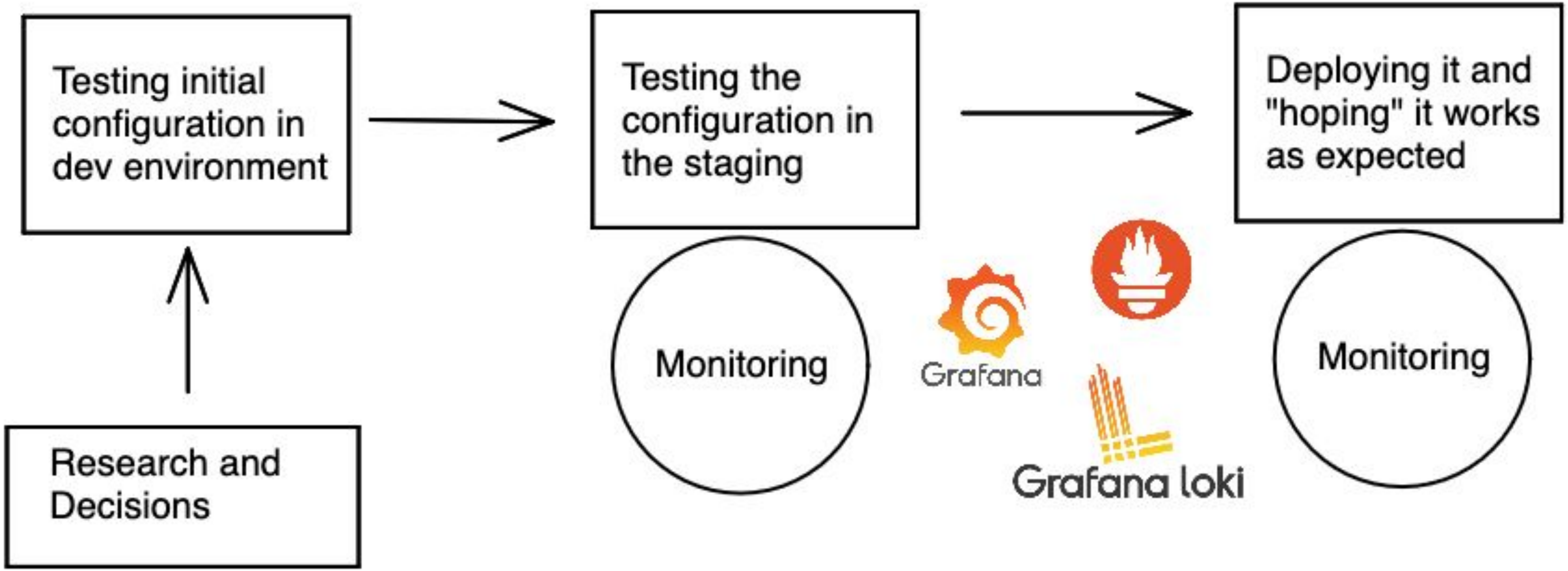
Supercluster design: compute



2xIntel Gold Xeon 20 core CPU
384GB 2666Mhz DRAM
100 Gb Networking

OPEN Compute Project®

Here are the processes we followed



Research and Decisions

Testing initial configuration in dev environment

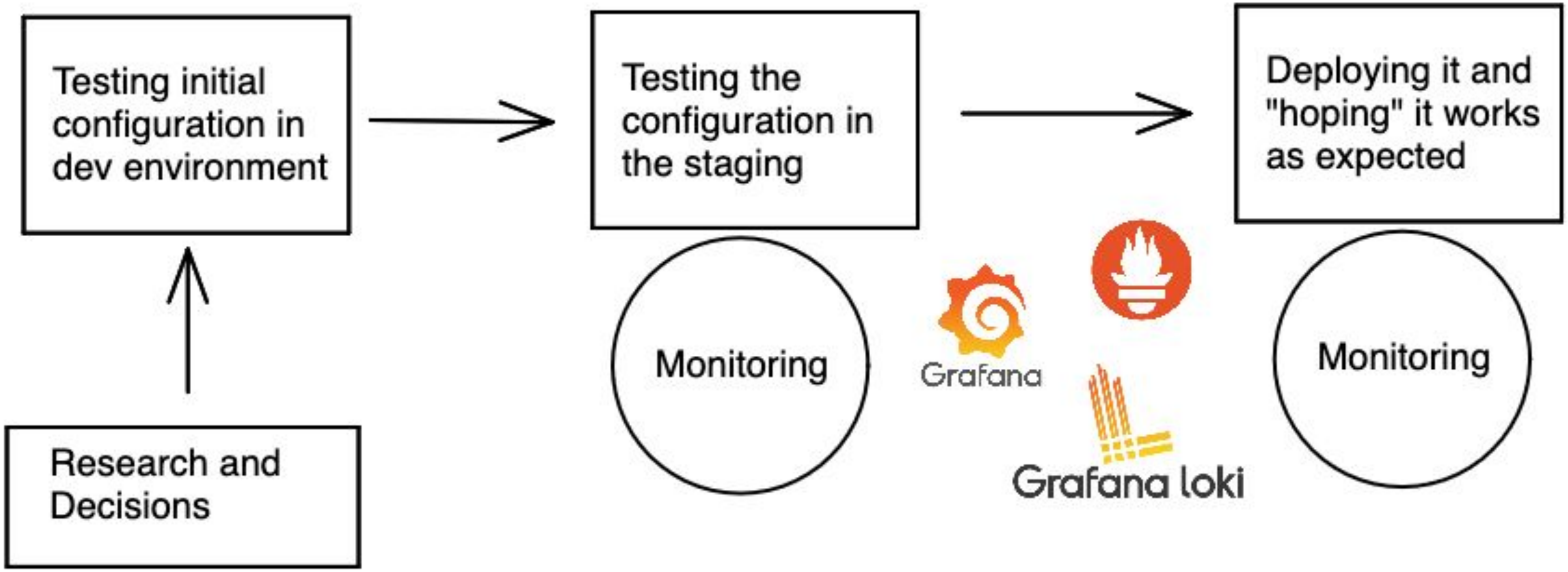
Testing the configuration in the staging

Monitoring

Deploying it and "hoping" it works as expected

Monitoring

Here are the processes we followed



Research and Decisions

Testing initial configuration in dev environment

Testing the configuration in the staging

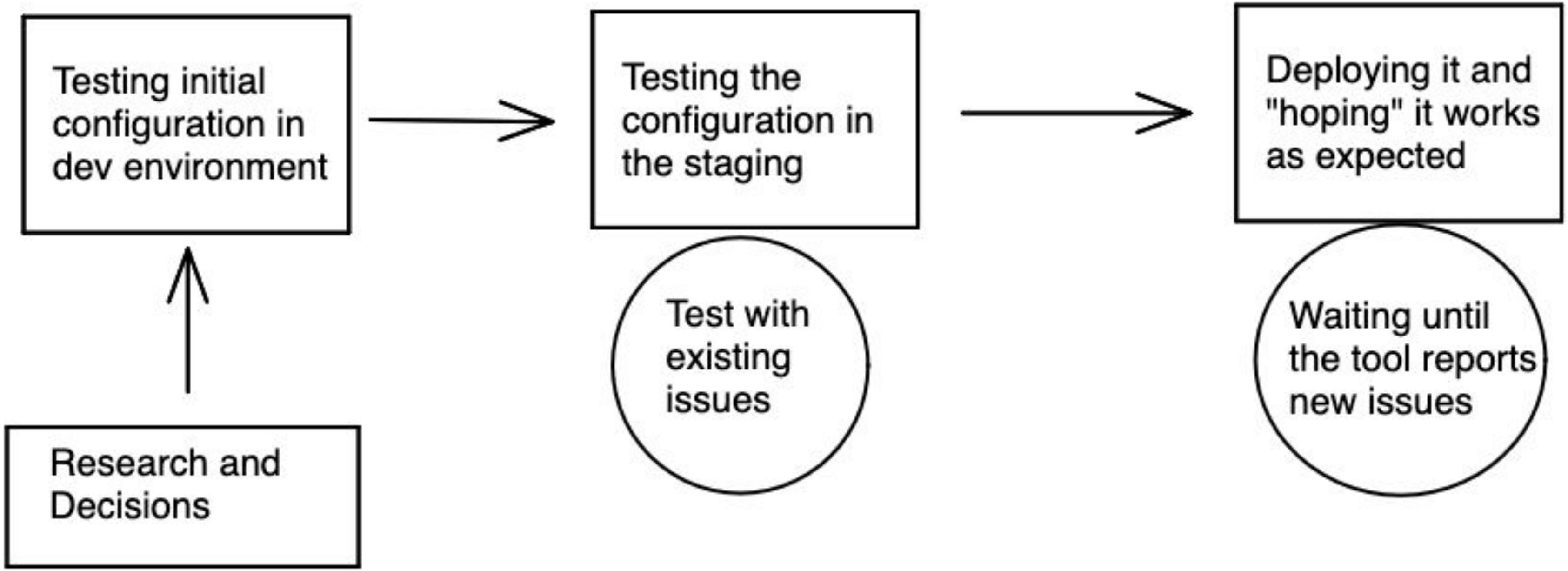
Deploying it and "hoping" it works as expected

Monitoring

Monitoring

“We did not expect things to “just” work”

In comparison: Security Setup



Research and Decisions

Testing initial configuration in dev environment

Testing the configuration in the staging

Test with existing issues

Deploying it and "hoping" it works as expected

Waiting until the tool reports new issues

SRE/Observability Space vs DevSecOps

SRE	DevSecOps
Failure Culture	Success Culture
Experimentation	Processes and Protocols
Systems are perceived as dynamic	Systems are perceived as static
Humans play a vital role	Reduce human-computer interaction

Chaos Engineering

Definition

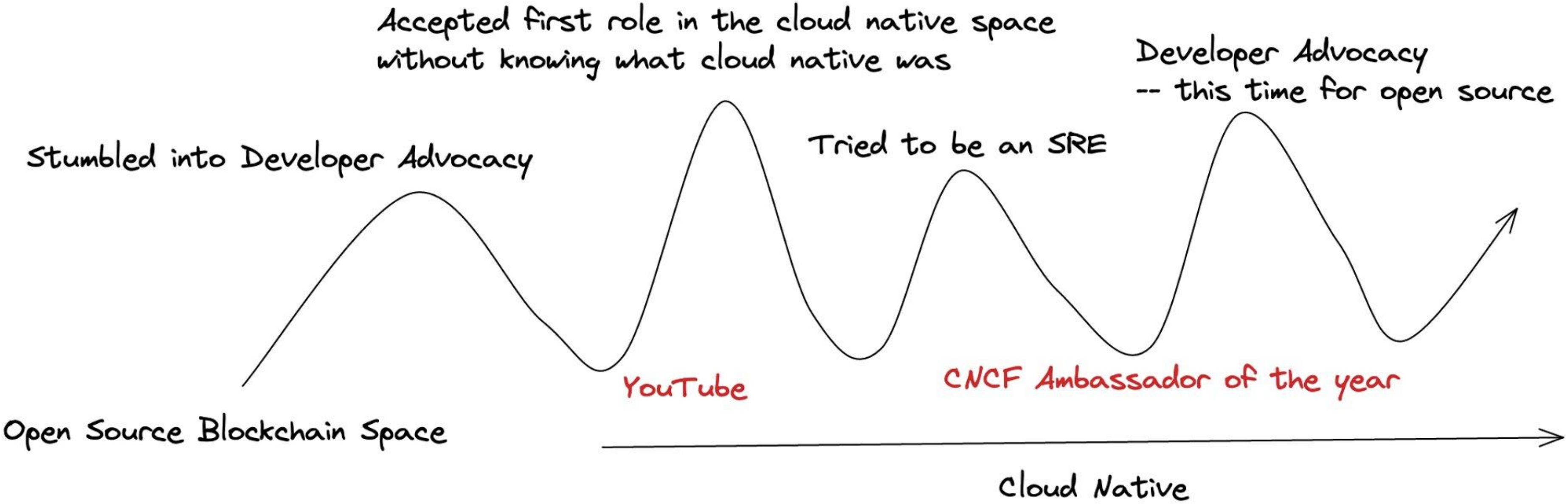
"Chaos Engineering is the discipline of experimenting on a system in order to build confidence in the system’s capability to withstand turbulent conditions in production."

- The Principles of Chaos Engineering

Litmus

Chaos Mesh

CHAOS MONKEY



Open Source Blockchain Space

Stumbled into Developer Advocacy

Accepted first role in the cloud native space without knowing what cloud native was

YouTube

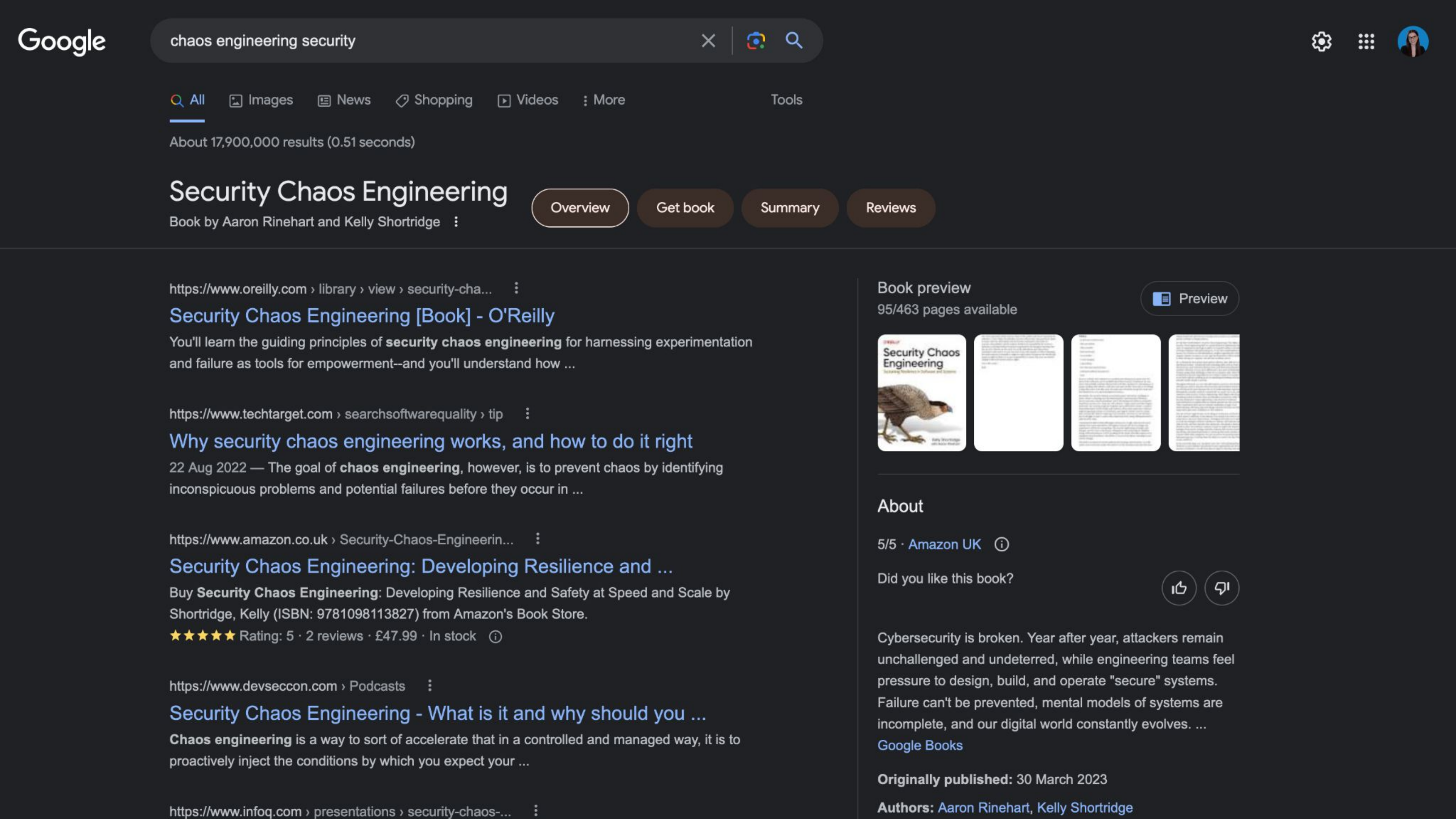
Tried to be an SRE

CNCF Ambassador of the year

Developer Advocacy -- this time for open source

Cloud Native

“What happens if you apply Chaos Engineering to Security”



About 17,900,000 results (0.51 seconds)

Security Chaos Engineering

Book by Aaron Rinehart and Kelly Shortridge

https://www.oreilly.com › library › view › security-cha...

Security Chaos Engineering [Book] - O'Reilly

You'll learn the guiding principles of **security chaos engineering** for harnessing experimentation and failure as tools for empowerment--and you'll understand how ...

https://www.techtarget.com › searchsoftwarequality › tip

Why security chaos engineering works, and how to do it right

22 Aug 2022 — The goal of **chaos engineering**, however, is to prevent chaos by identifying inconspicuous problems and potential failures before they occur in ...

https://www.amazon.co.uk › Security-Chaos-Engineerin...

Security Chaos Engineering: Developing Resilience and ...

Buy **Security Chaos Engineering**: Developing Resilience and Safety at Speed and Scale by Shortridge, Kelly (ISBN: 9781098113827) from Amazon's Book Store.

★★★★★ Rating: 5 · 2 reviews · £47.99 · In stock

https://www.devseccon.com › Podcasts

Security Chaos Engineering - What is it and why should you ...

Chaos engineering is a way to sort of accelerate that in a controlled and managed way, it is to proactively inject the conditions by which you expect your ...

https://www.infoq.com › presentations › security-chaos-...

Book preview

95/463 pages available

About

5/5 · Amazon UK

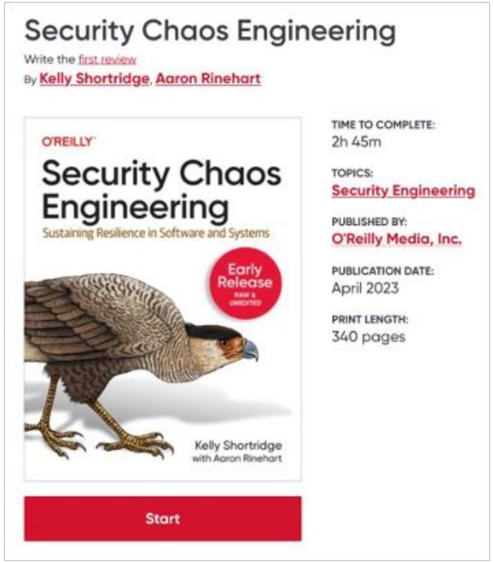
Did you like this book?

Cybersecurity is broken. Year after year, attackers remain unchallenged and undeterred, while engineering teams feel pressure to design, build, and operate "secure" systems. Failure can't be prevented, mental models of systems are incomplete, and our digital world constantly evolves. ...
Google Books

Originally published: 30 March 2023

Authors: Aaron Rinehart, Kelly Shortridge

Resources on Security Chaos Engineering



Security Chaos Engineering

Write the first review

By Kelly Shortridge, Aaron Rinehart

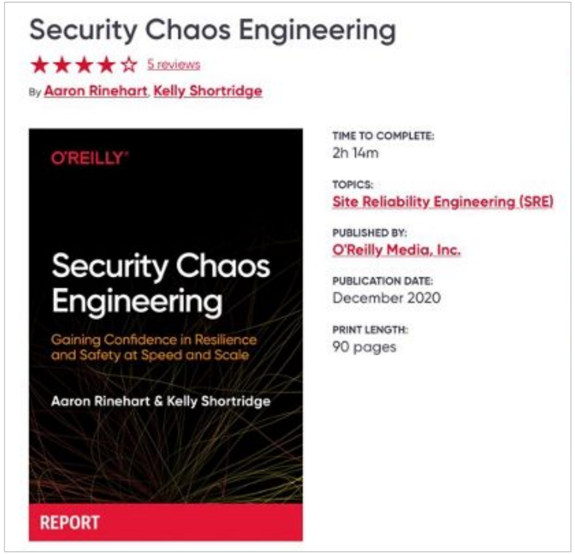
TIME TO COMPLETE:
2h 45m

TOPICS:
Security Engineering

PUBLISHED BY:
O'Reilly Media, Inc.

PUBLICATION DATE:
April 2023

PRINT LENGTH:
340 pages



Security Chaos Engineering

★★★★☆ 5 reviews

By Aaron Rinehart, Kelly Shortridge

TIME TO COMPLETE:
2h 14m

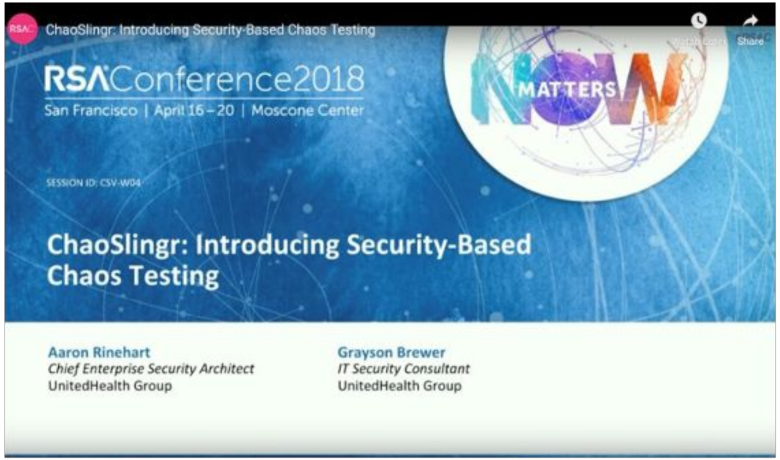
TOPICS:
Site Reliability Engineering (SRE)

PUBLISHED BY:
O'Reilly Media, Inc.

PUBLICATION DATE:
December 2020

PRINT LENGTH:
90 pages

O'REILLY
Security Chaos Engineering
Gaining Confidence in Resilience and Safety at Speed and Scale
Aaron Rinehart & Kelly Shortridge
REPORT



ChaoSlingr: Introducing Security-Based Chaos Testing

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CSV-W04

ChaoSlingr: Introducing Security-Based Chaos Testing

Aaron Rinehart
Chief Enterprise Security Architect
UnitedHealth Group

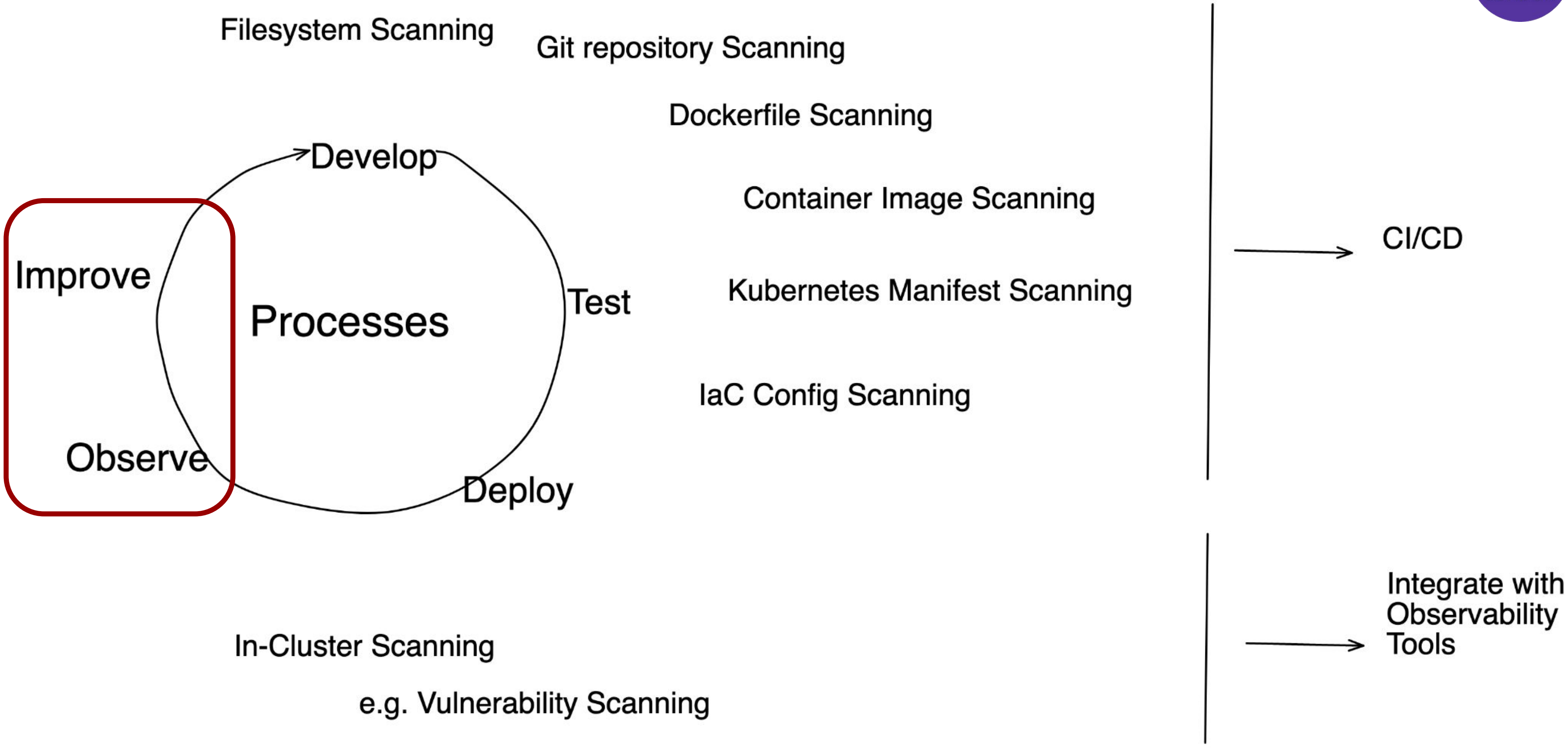
Grayson Brewer
IT Security Consultant
UnitedHealth Group

Definition

“The identification of security control failures through proactive experimentation to build confidence in the system’s ability to defend against malicious conditions in production.[1]”

- Security Chaos Engineering by Aaron Rinehart, Kelly Shortridge

ChaoSlingr



Filesystem Scanning

Git repository Scanning

Dockerfile Scanning

Container Image Scanning

Kubernetes Manifest Scanning

IaC Config Scanning

Develop

Test

Deploy

Observe

Improve

Processes

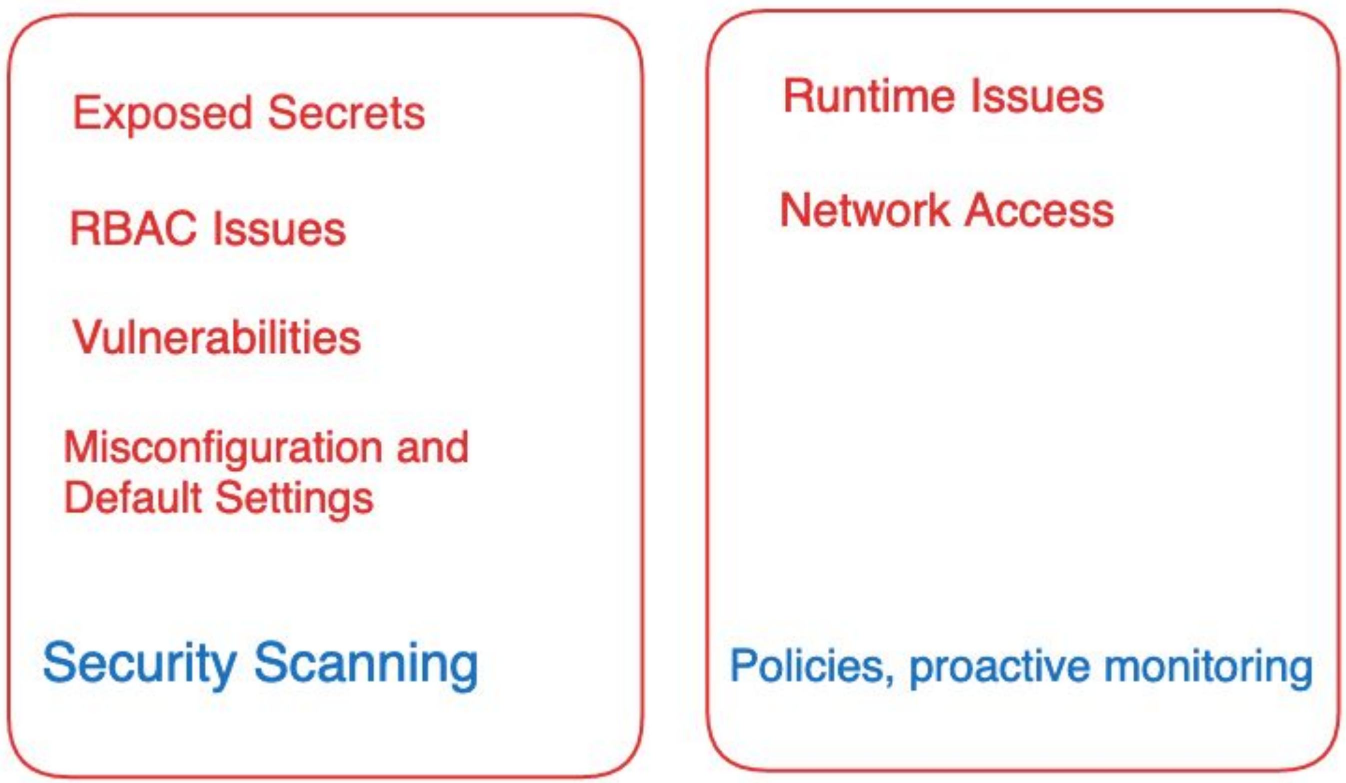
CI/CD

In-Cluster Scanning

e.g. Vulnerability Scanning

Integrate with Observability Tools

In your Kubernetes cluster/cloud environment



Exposed Secrets

RBAC Issues

Vulnerabilities

Misconfiguration and Default Settings

Security Scanning

Runtime Issues

Network Access

Policies, proactive monitoring

Key Principles of Security Chaos Engineering

- Seeks proactive, adaptive learning over reactive patching

- Building a learning culture around how organizations build, operate, instrument, and secure their systems

- Controlled test – you already know the issue & you are identifying the effect

Why should we “break” our systems

- A resilient system isn’t one that is robust but one that can withstand failure “Resilience should be thought of as a proactive and perpetual cycle of system-wide monitoring, anticipating disruptions, learning from success and failure, and adapting the system over time.”

- We build and run complex systems - complex systems are adaptive

- View our system like an attacker would

- Goal: Identify our system’s safety boundaries before they are exceeded

Implementing Security Chaos Engineering

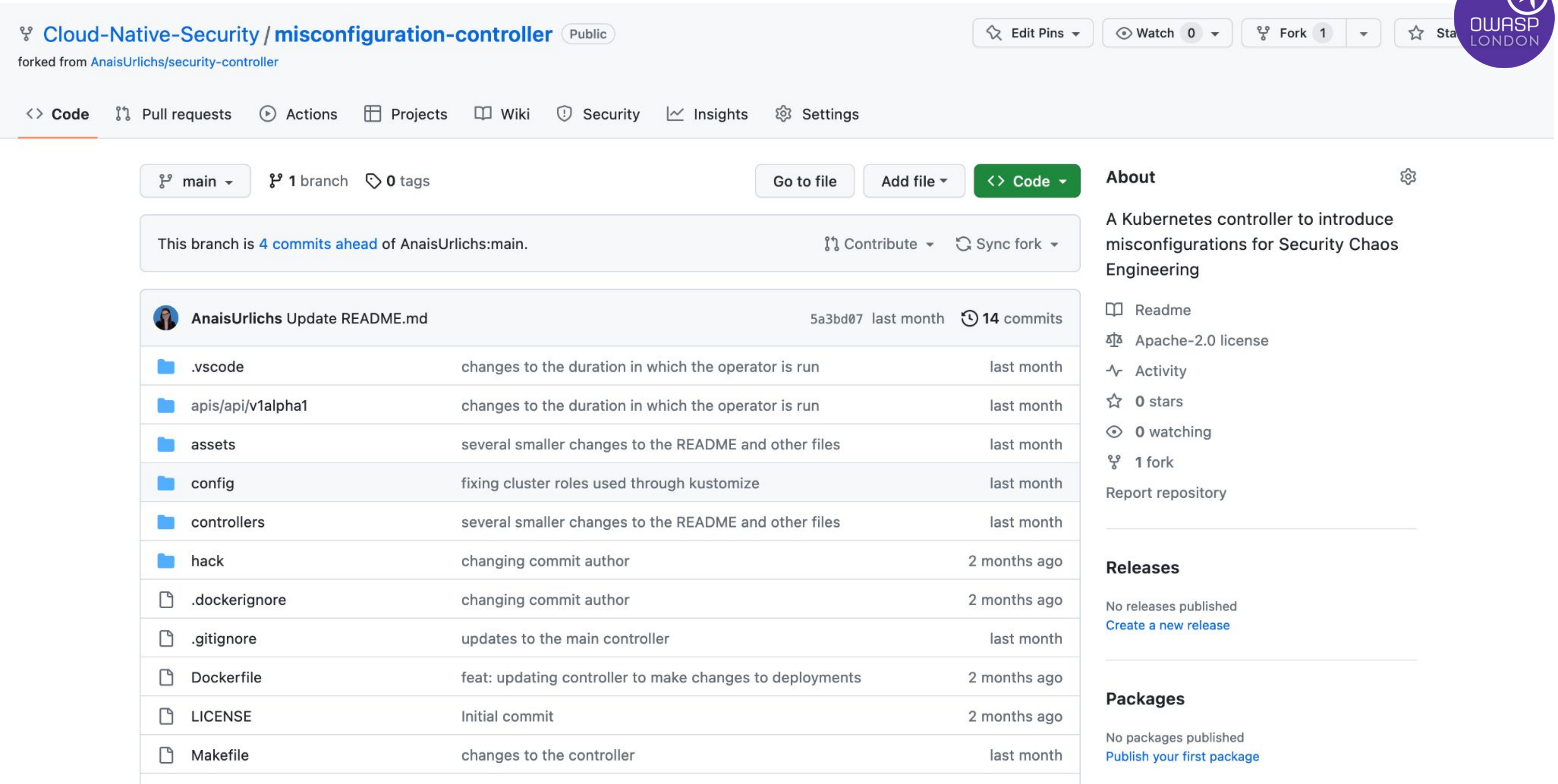
1. Perform manual changes

2. Adapting existing Chaos Engineering Tools

3. Building custom operators

Litmus

Chaos Mesh



forked from AnaisUrlichs/security-controller

This branch is 4 commits ahead of AnaisUrlichs:main.

AnaisUrlichs Update README.md 5a3bd07 last month 14 commits

.vscode	changes to the duration in which the operator is run	last month
apis/api/v1alpha1	changes to the duration in which the operator is run	last month
assets	several smaller changes to the README and other files	last month
config	fixing cluster roles used through kustomize	last month
controllers	several smaller changes to the README and other files	last month
hack	changing commit author	2 months ago
.dockerignore	changing commit author	2 months ago
.gitignore	updates to the main controller	last month
Dockerfile	feat: updating controller to make changes to deployments	2 months ago
LICENSE	Initial commit	2 months ago
Makefile	changes to the controller	last month

About

A Kubernetes controller to introduce misconfigurations for Security Chaos Engineering

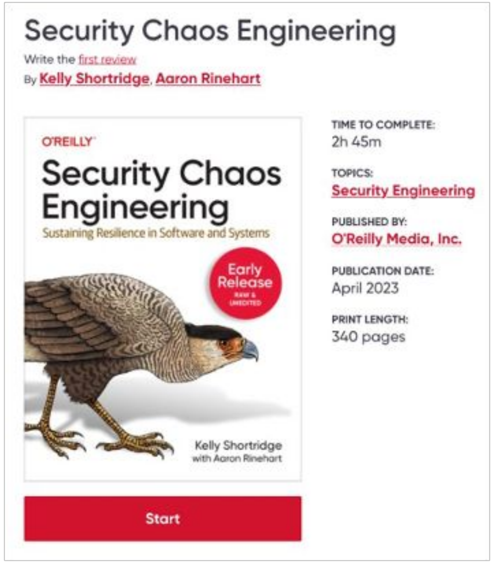
Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Resources on Security Chaos Engineering



Security Chaos Engineering

Write the first review

By Kelly Shortridge, Aaron Rinehart

O'REILLY

Security Chaos Engineering

Sustaining Resilience in Software and Systems

Early Release RAW & UNEDITED

Kelly Shortridge with Aaron Rinehart

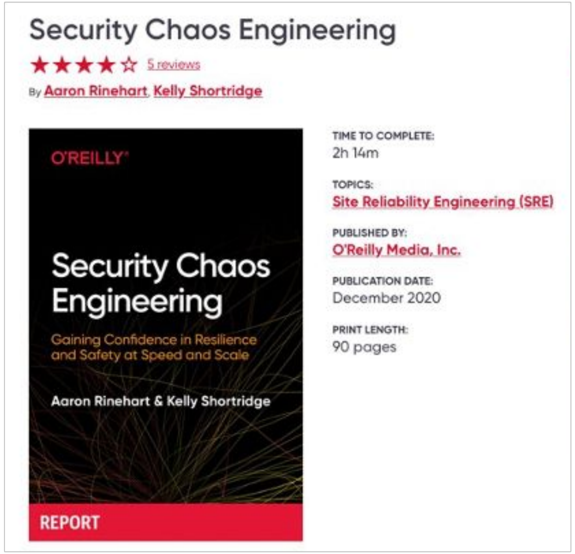
TIME TO COMPLETE: 2h 45m

TOPICS: Security Engineering

PUBLISHED BY: O'Reilly Media, Inc.

PUBLICATION DATE: April 2023

PRINT LENGTH: 340 pages



Security Chaos Engineering

★★★★☆ 5 reviews

By Aaron Rinehart, Kelly Shortridge

O'REILLY

Security Chaos Engineering

Gaining Confidence in Resilience and Safety at Speed and Scale

Aaron Rinehart & Kelly Shortridge

REPORT

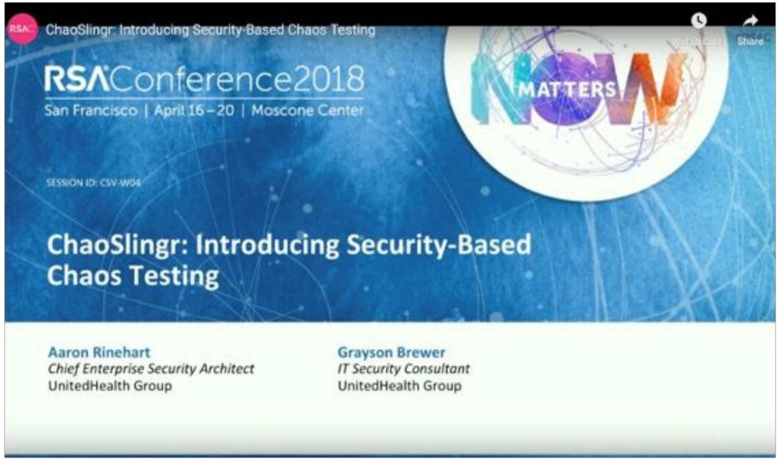
TIME TO COMPLETE: 2h 14m

TOPICS: Site Reliability Engineering (SRE)

PUBLISHED BY: O'Reilly Media, Inc.

PUBLICATION DATE: December 2020

PRINT LENGTH: 90 pages



RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CSV-W04

ChaoSlingr: Introducing Security-Based Chaos Testing

Aaron Rinehart
Chief Enterprise Security Architect
UnitedHealth Group

Grayson Brewer
IT Security Consultant
UnitedHealth Group

Thank you!

@urlichsanais

linkedin.com/in/urlichsanais/