KubeCon | CloudNativeCon

Europe 2022

WELCOME TO VALENCIA

KubeCon | CloudNativeCon Europe 2022

# Introducing "Kirvis" OSS Security Chaos Engineering for Kubernetes

Aaron Rinehart, Verica.io
Matas Kulkovas, Cast AI


**Aaron Rinehart**

CTO & Co-Founder at Verica

Pioneer of Security Chaos Engineering

O'Reilly Author

@aaronrinehart

**Matas Kulkovas**

Engineer, CAST AI


O'REILLY
Compliments of
NETFLIX
Chaos Engineering
Building Confidence in Sy
through Experiments
O'REILLY
Chaos Engineering
System Resiliency in Practice
O'REILLY
Security Chaos Engineering
Gaining Confidence in Resilience
DEVOPS DAYS TAMPA BAY

# Why will you learn?

- Complexity in Modern Software
- Chaos Engineering
- Security Chaos Engineering (SCE)
- Use Cases
- New K8s Open Source Tool
- How to get started!

# In this Session we will cover

KubeCon | CloudNativeCon Europe 2022

# We're Not Getting Better

**Southwest Airlines says [illegible] system outage' affecte[illegible] nationwide, including i[illegible] Houston-area**

The airline says the outage is resolved, however, passengers could still face delays

Bloomberg

U.S. E

Technology | Politics | Wealth | Pursuits | Opinion | Businessweek | Equality | Green

Technology

**Apple Resolves Outage That Hobbled Apps and Internal Systems**

- Music, iCloud and maps didn't work for some users Monday
- Problems prevented corporate staff from working from home

**Google suffers another Outage as Google Cloud servers in the us-east1 region are cut off**

By Amrata Joshi - July 3, 2019 - 9:55 am 200 0

Healthcare IT News TOPI

Global Edition Electronic Health Records (EHR, EMR)

**EHR outage takes down federal Cerner systems**

Clinicians at dozens of Defense Department, Coast Guard and Veterans Affairs sites were unable to update medical records for hours this past Wednesday.

**Apple iCloud services recover from nationwide outage**

Service outages are increasingly becoming a headache for tech companies and consumers alike

By Humza Aamir on July 5, 2019, 8:18 AM

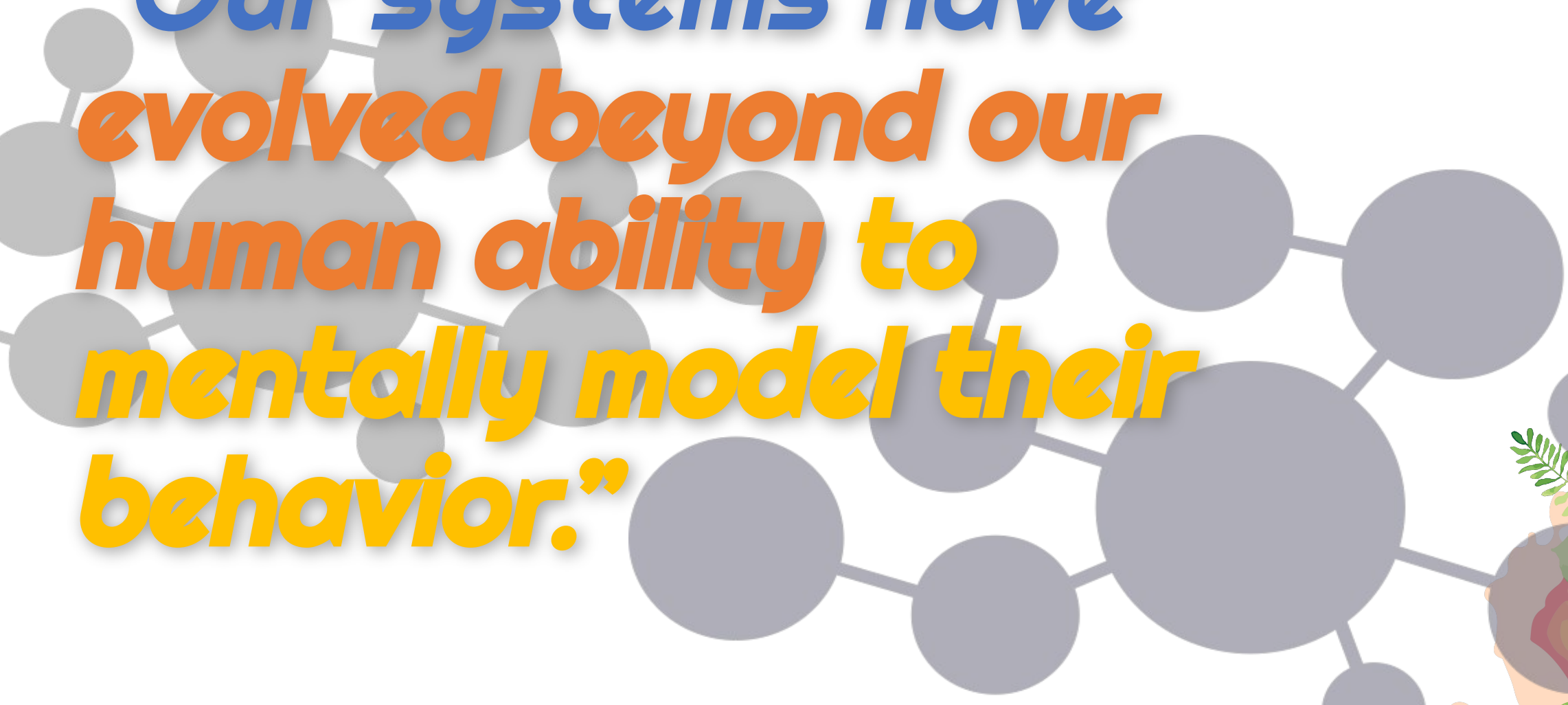
**The PlayStation Network recovers from an outage affecting players on PS5 and PS4**

*The outage began around 8:30AM ET*

By Emma Roth | Updated Mar 23, 2022, 12:44pm EDT

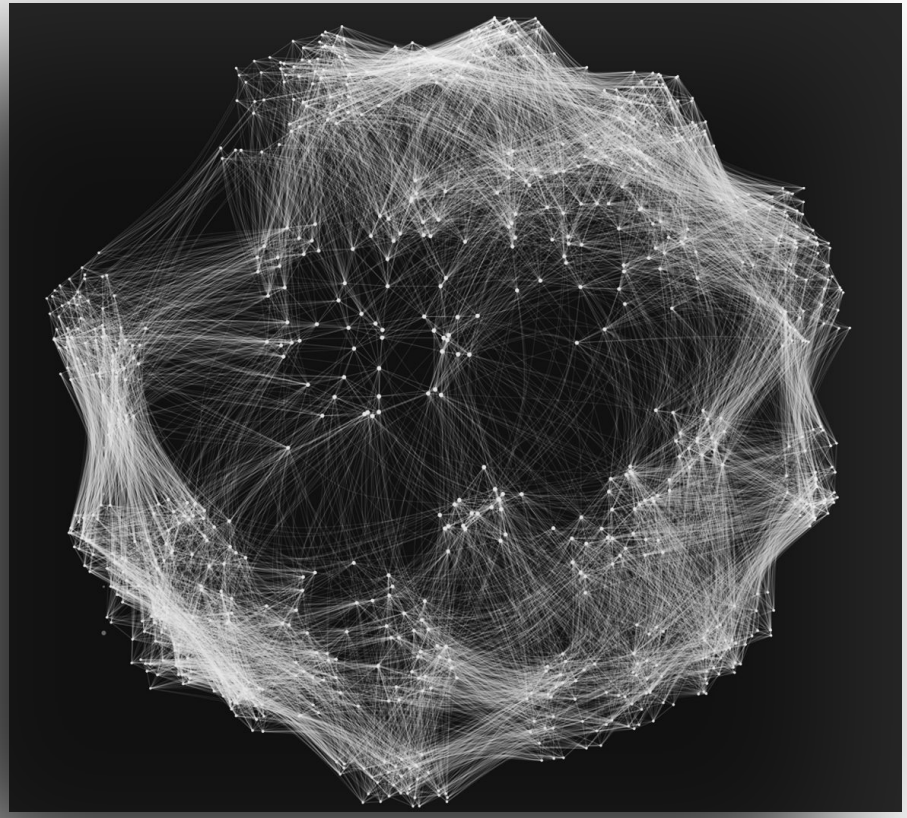
# Why is this?
# What are we doing wrong?

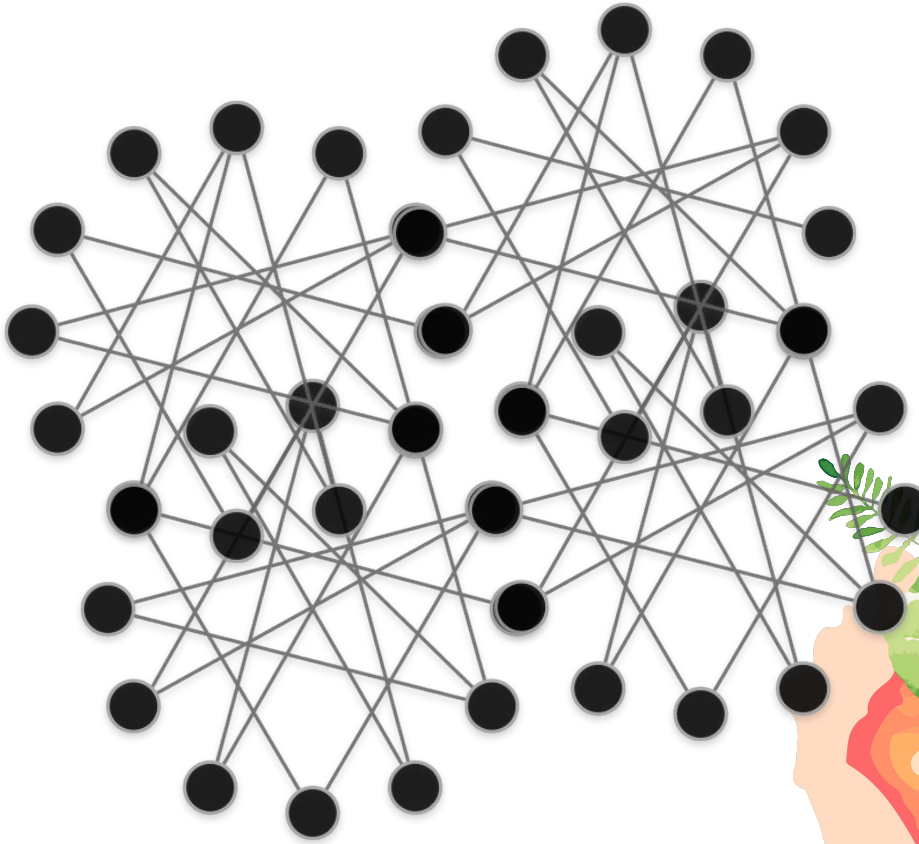
"Our systems have evolved beyond our human ability to mentally model their behavior."



# Speed, Scale, & Complexity of Modern Software is Challenging

KubeCon | CloudNativeCon Europe 2022





# Where does it come from?



Continuous Delivery

**Distributed Systems**

Microservice Architectures

**Blue/Green Deployments**

Containers

Automation Pipelines

**Auto Scaling**

**DevOps**

**Continuous Integration**

Infracode

*CI/CD*

**Immutable Infrastructure**

**Service Mesh**

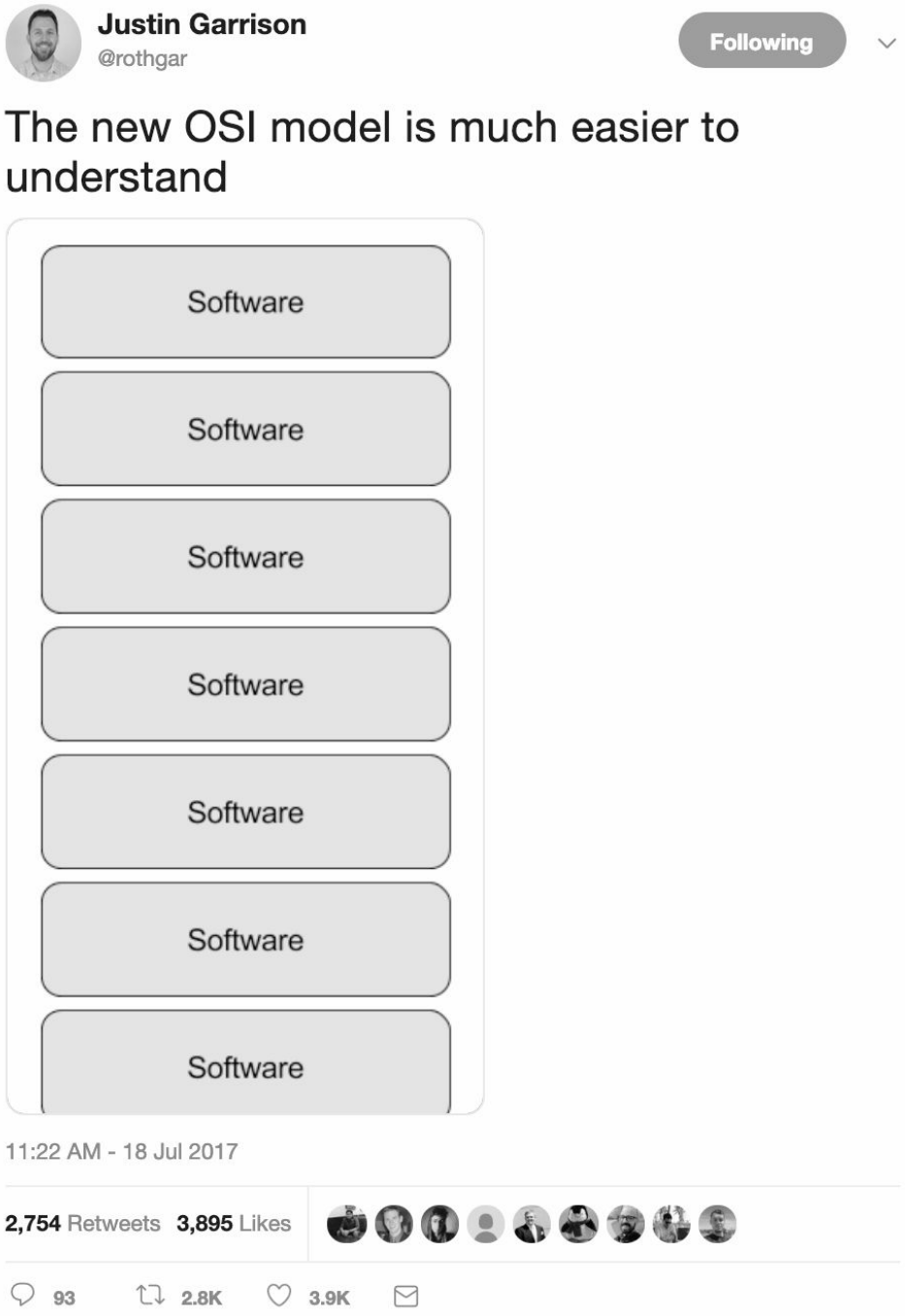
Auto Canaries

Cloud Computing

***Circuit Breaker Patterns***

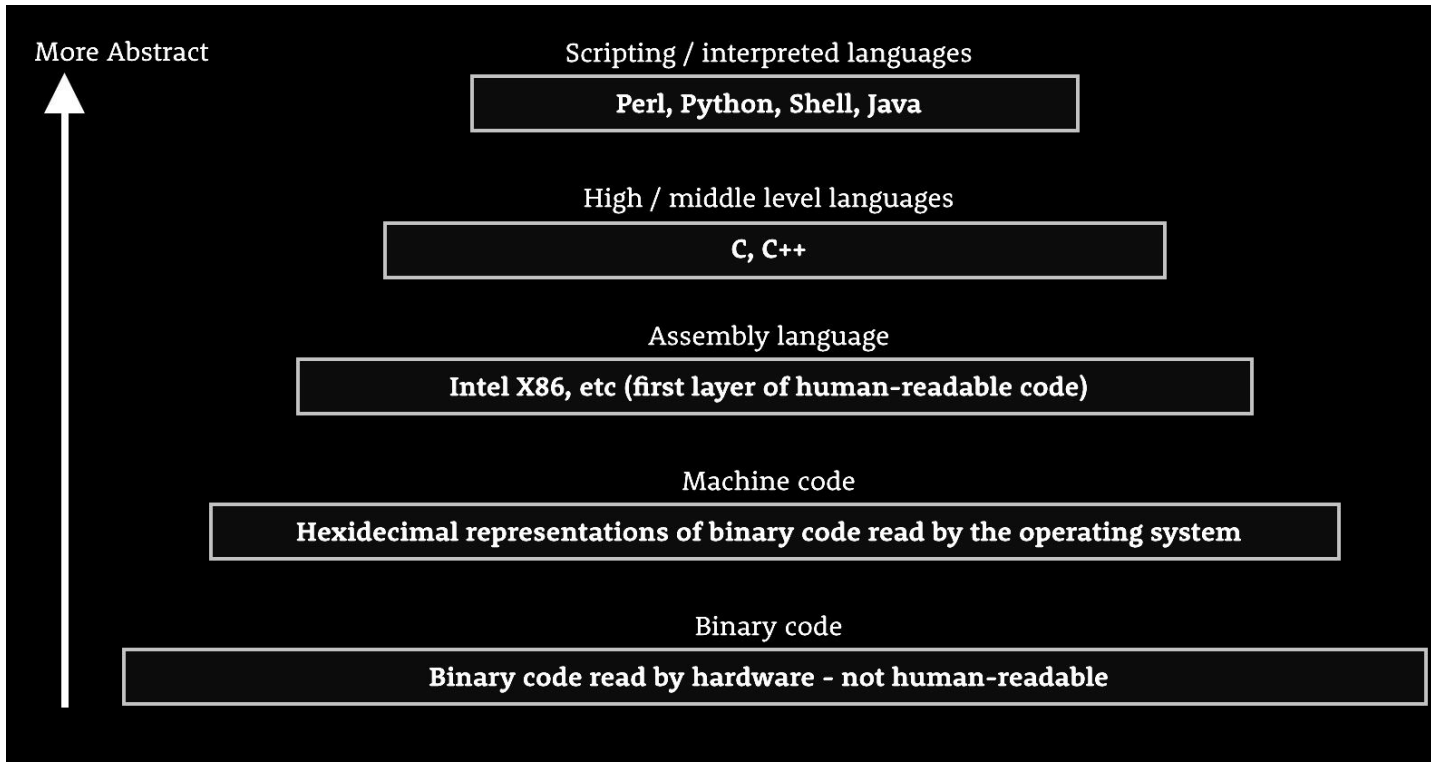
**API**

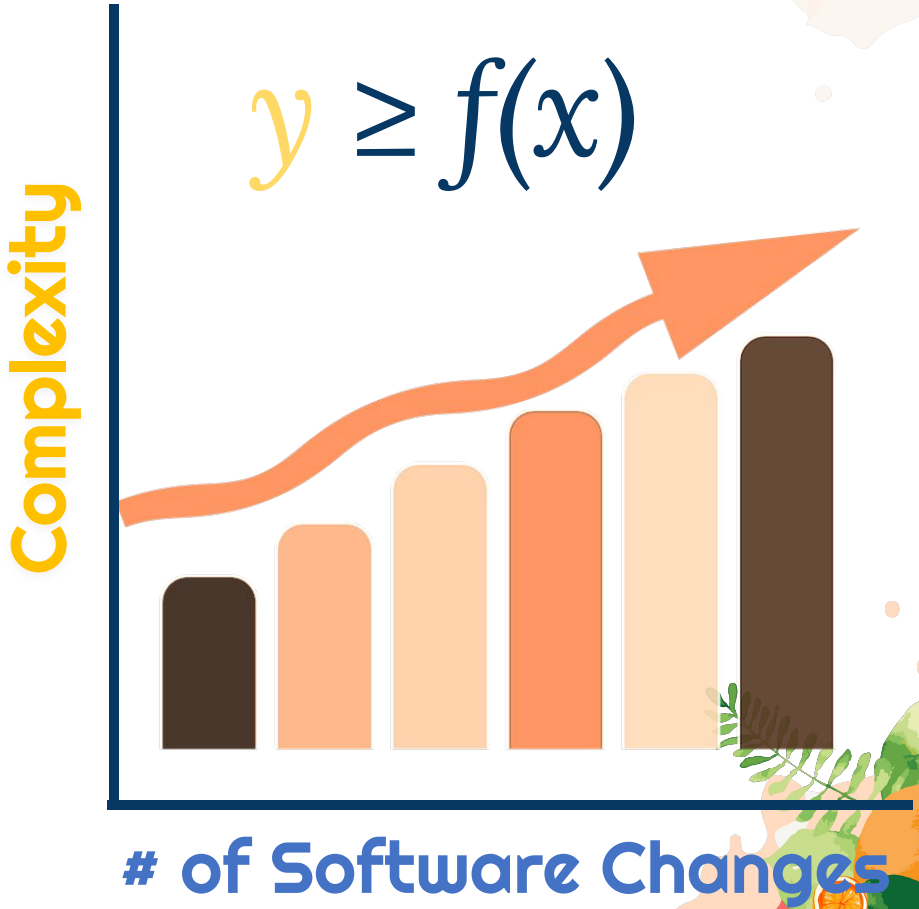
# Software has officially taken over



# Software ONLY Increases in Complexity





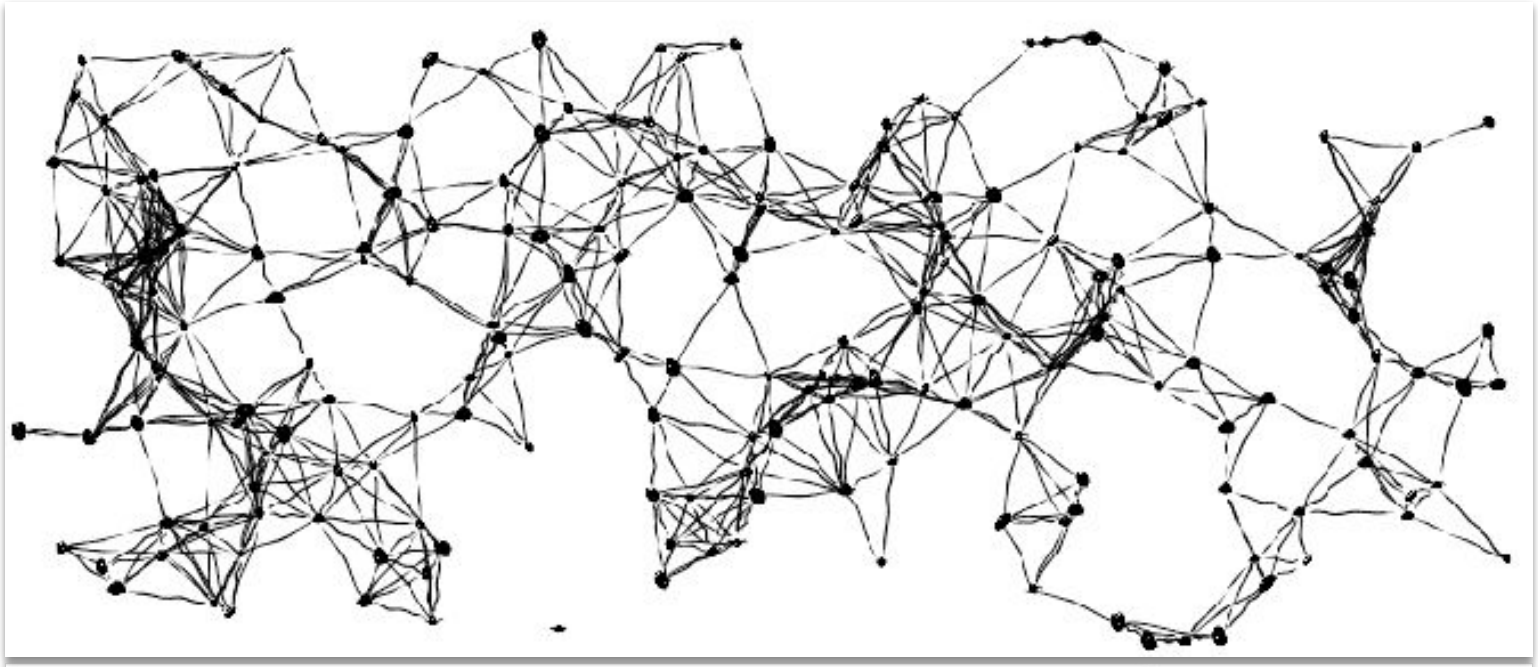

Change(x) ∞ Complexity(y)

# Software Complexity



## Accidental Complexity

## Essential Complexity

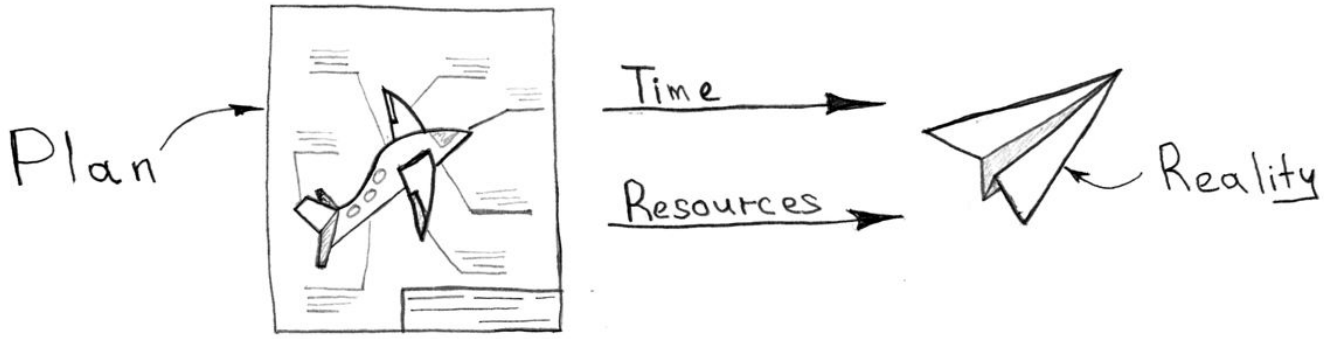


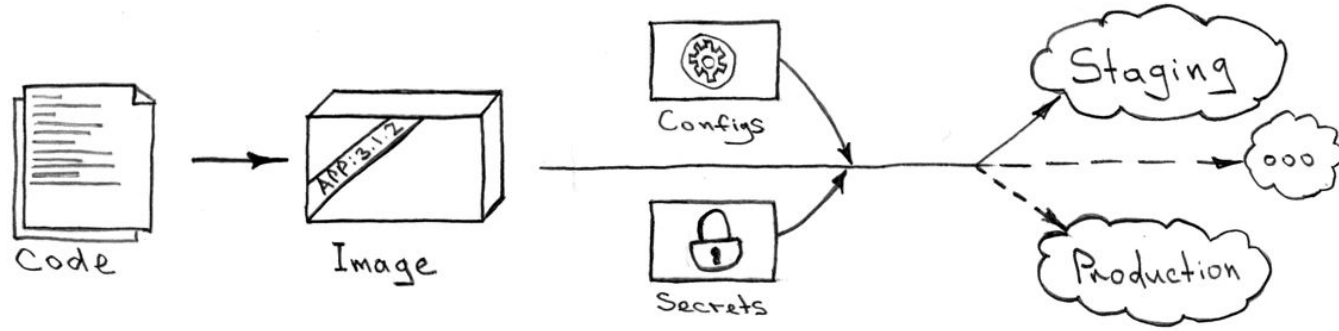
# Learn to Navigate Complexity with Chaos Engineering

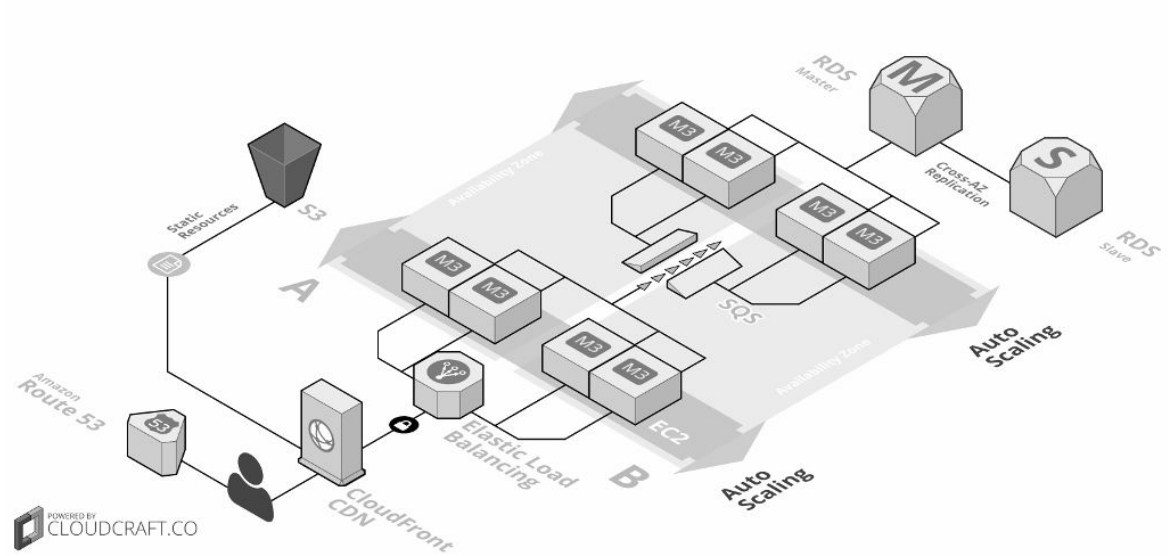
# We forget that.....

## Systems Engineering is Messy

# In the beginning...we think it looks like



# After a few months....

KubeCon CloudNativeCon Europe 2022

Hard Coded Passwords

Network is Unreliable

New Security Tool

Autoscaling Keeps Breaking

Identity Conflicts

Regulatory Audit

Refactor Pricing

Rolling Sev1 Outage on Portal

Lead Software Engineering finds a new job at Google

Cloud Provider API Outage

Code Freeze

DNS Resolution Errors

Expired Certificate

300 Microservices Δ-> 850 Microservices

Scalability Issues

WAF Outage -> Disabled

Delayed Features

Large Customer Outage

# Years?....

Orphaned Documentation

Hard Coded Passwords

Network is Unreliable

New Security Tool

Portal Retry Storm Outage

Regulatory Audit

Identity Conflicts

Refactor Pricing

Cloud Provider API Outage

Code Freeze

Budget Freeze

Expired Certificate

Database Outage

Hard Coded Passwords

DNS Resolution Errors

Network is Unreliable

Autoscaling Keeps Breaking

Scalability Issues

300 Microservices Δ-> 4000 Microservices

Corporate Reorg

Migration to New CSP

Refactor Pricing

Misconfigured FW Rule Outage

Firewall Outage -> Disabled

Large Customer Outage

Upgrade to Java SE 12

Cloud Provider API Outage

Exposed Secrets on Github Code Freeze

Expired Certificate

DNS Resolution Errors

300 Microservices Δ-> 850 Microservices

Regulatory Audit

Scalability Issues

WAF Outage -> Disabled

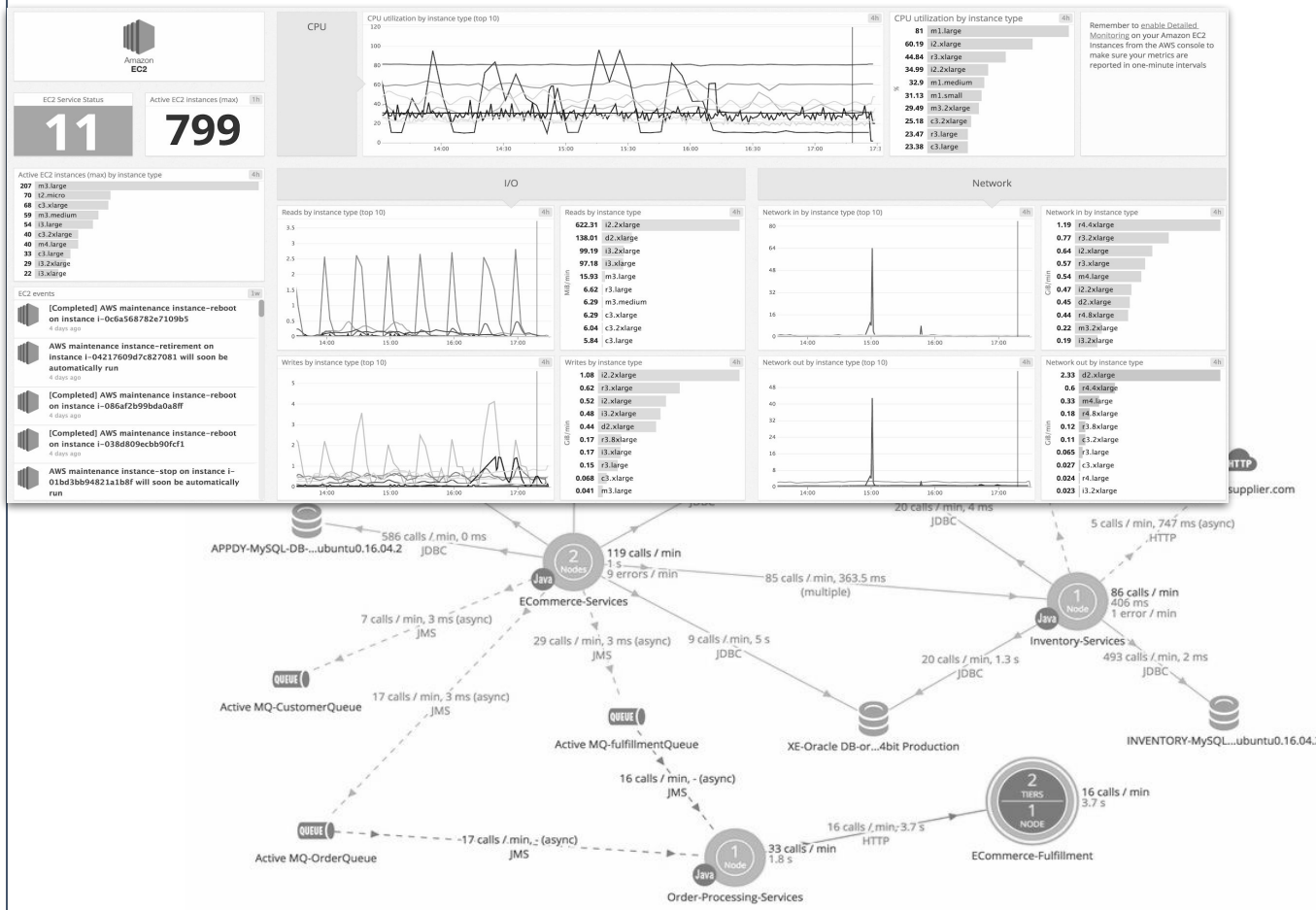
Delayed Features

Large Customer Outage

Rolling Sev1 Outage on Portal

KubeCon CloudNativeCon Europe 2022

# Our systems have become more complex and messy than we remember



# What does this $€%* have to do with Security?

KubeCon | CloudNativeCon Europe 2022

*Putting off critical tasks until everyone forgets about them*


*If there's time*

O RLY?

*@ThePracticalDev*

# Cyber Security is Context Dependent

Flexibility to Change System Rapidly

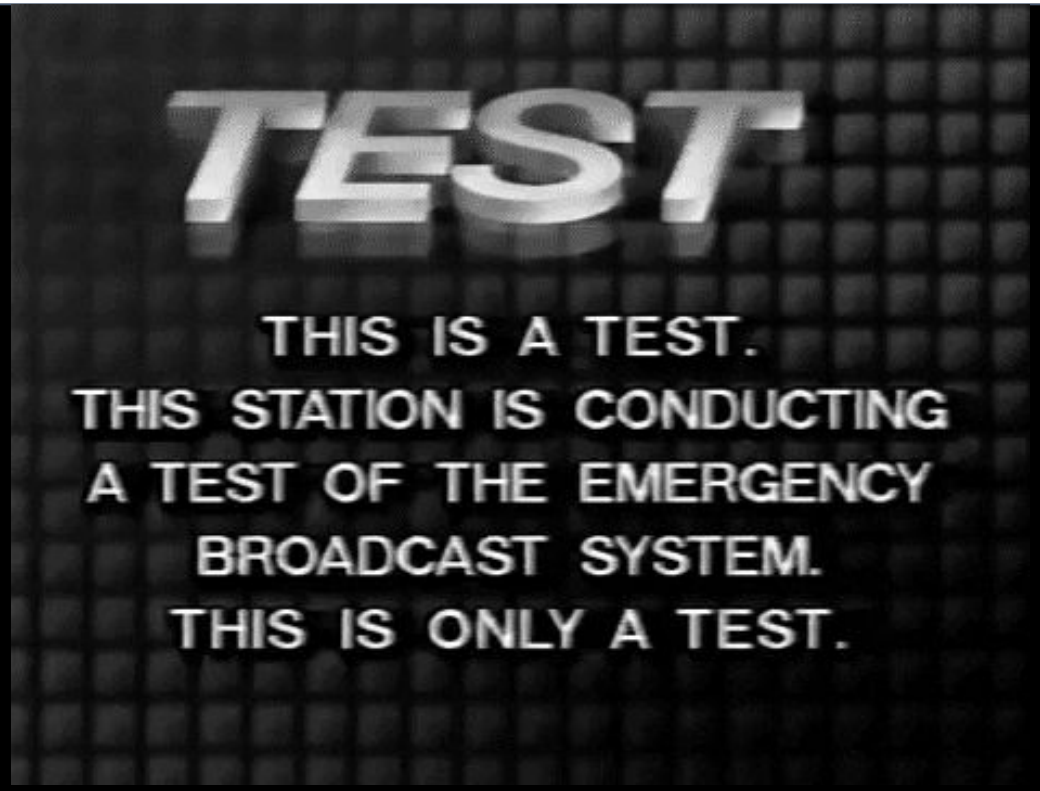
VS.

Ability to Apply Secure Context to System Changes

# Instrumenting Chaos

KubeCon CloudNativeCon Europe 2022

## Testing vs Experimentation




KubeCon | CloudNativeCon
Europe 2022

# Chaos Engineering

# Chaos Engineering



*"Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in the system's ability to withstand turbulent conditions"*

# Chaos Monkey Story

NETFLIX

- During Business Hours
- Born out of Netflix Cloud Transformation
- Put well defined problems in front of engineers.
- Terminate VMs on Random VPC Instances

The purpose of Chaos Engineering is **NOT** to "Break Things on Purpose".

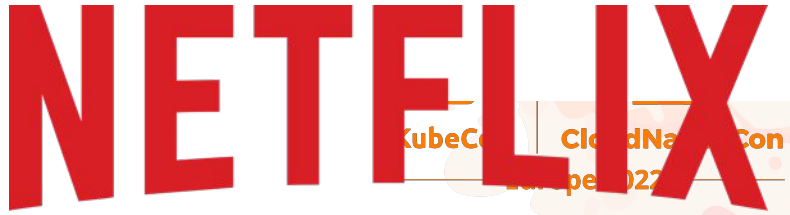
If anything we are trying to "Fix them on Purpose"!

CHAOS ENGINEERING IS ABOUT CONTINUOUS VERIFICATION + ORDER

"I'm pretty sure I won't have a very long if I break things on purpose all day."
-CASEY ROSENTHAL

*Reference: Nora Jones 8 Traps of Chaos Engineering*

# Who is doing Chaos?




KubeCon | CloudNativeCon Europe 2022

























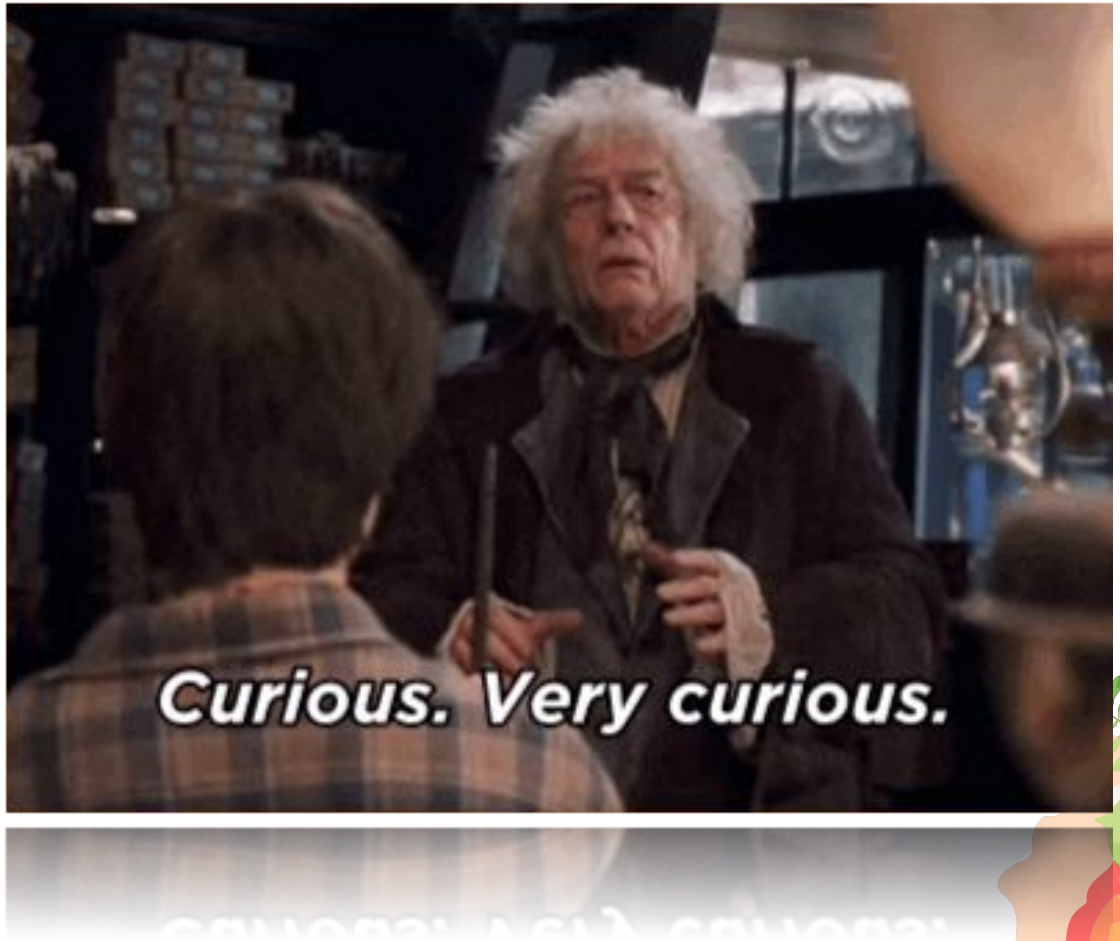







# SECURITY CHAOS ENGINEERING

# How do I know if my Security Really Works???



# Hope is Not

KubeCon CloudNativeCon Europe 2022

# an Effective Strategy

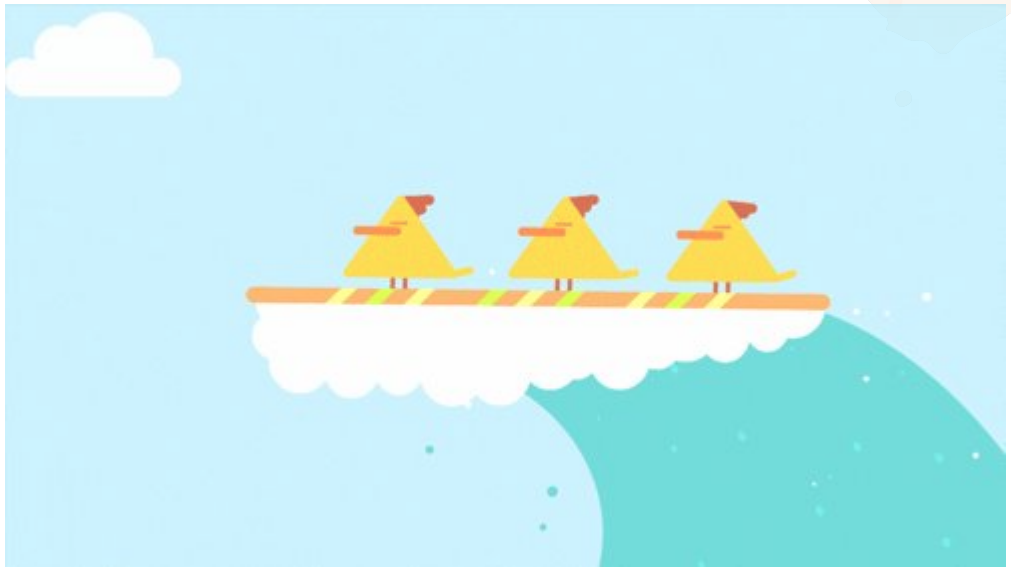

*"It worked in Star Wars but it won't work here"*

# “Understand your system and its security gaps before an adversary does”

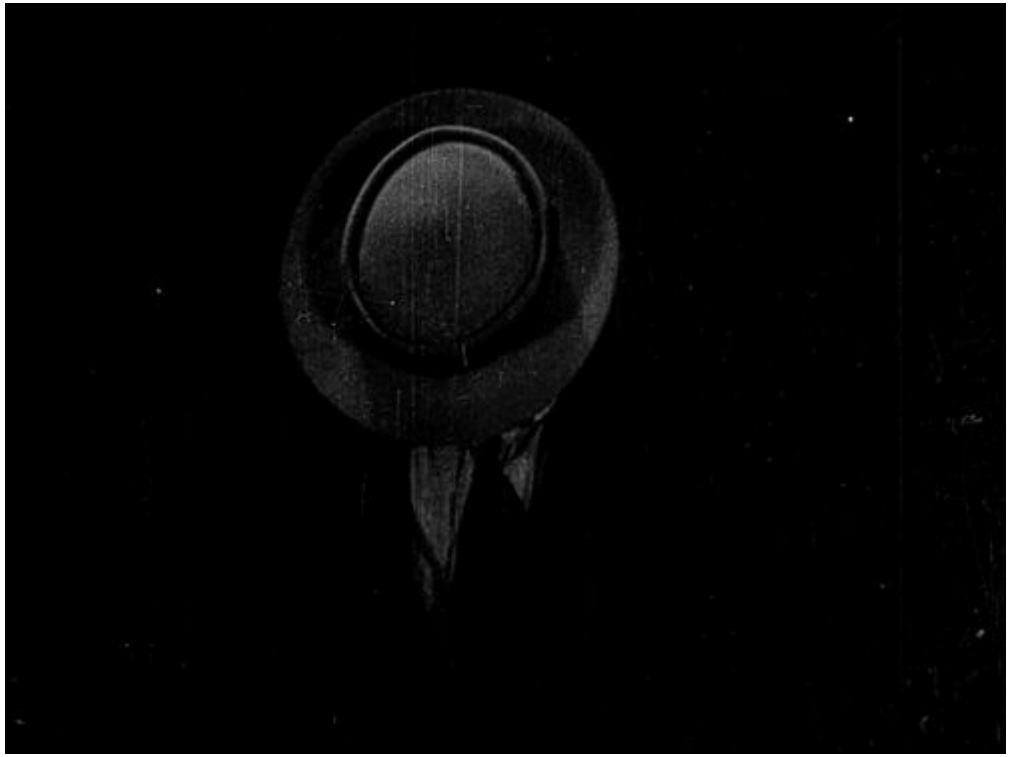
# Use Cases



- Incident Response
- Security Control Validation
- Security Observability
- Compliance Monitoring

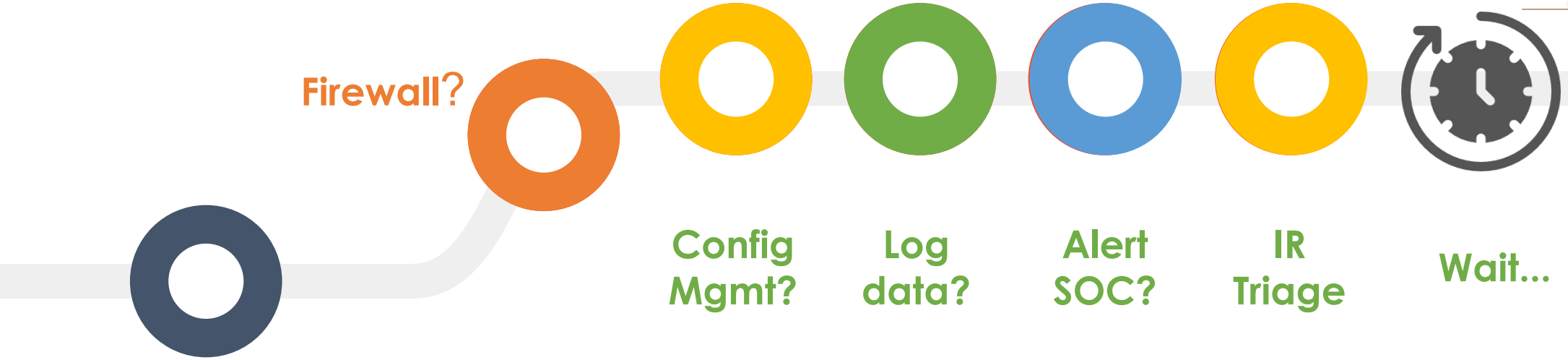


# So how does it work?



# ChaoSlingr

# An Open Source Tool




**Hypothesis:**

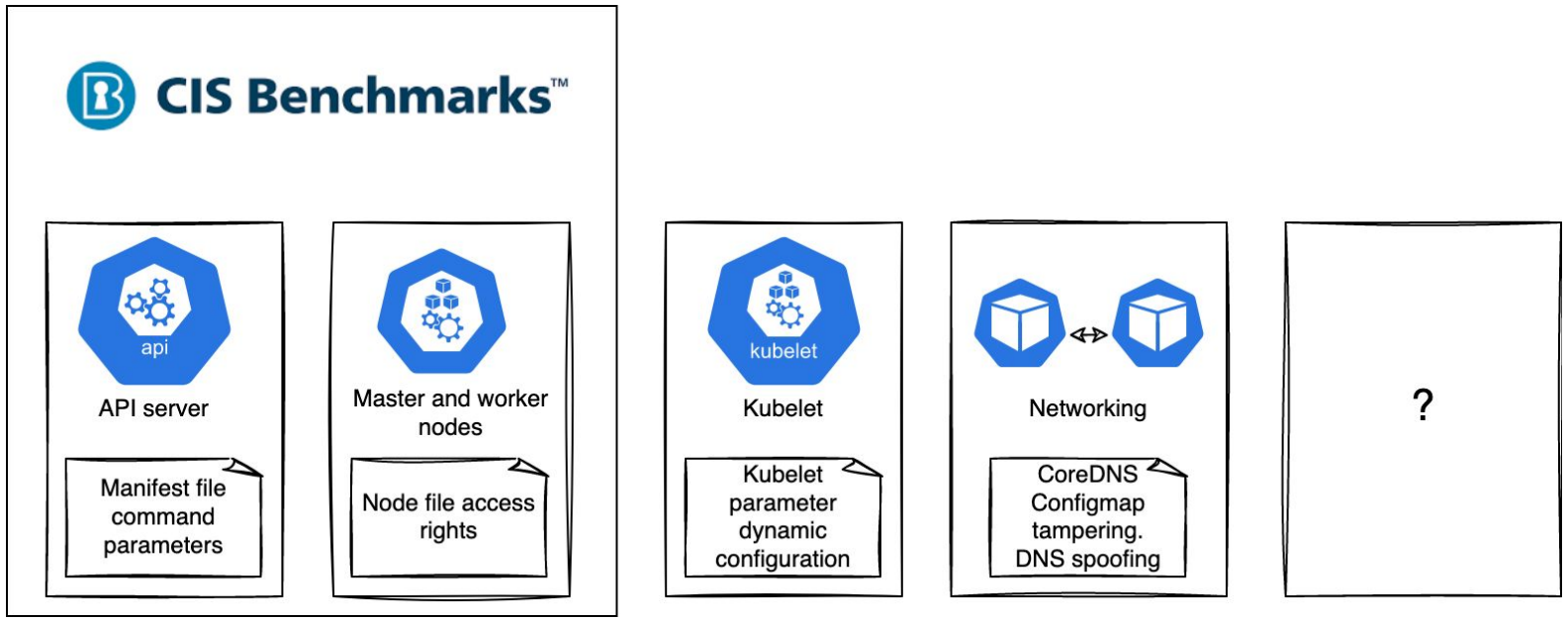
If someone accidentally or maliciously introduced a misconfigured port then we would immediately detect, block, and alert on the event.

# “Kirvis”

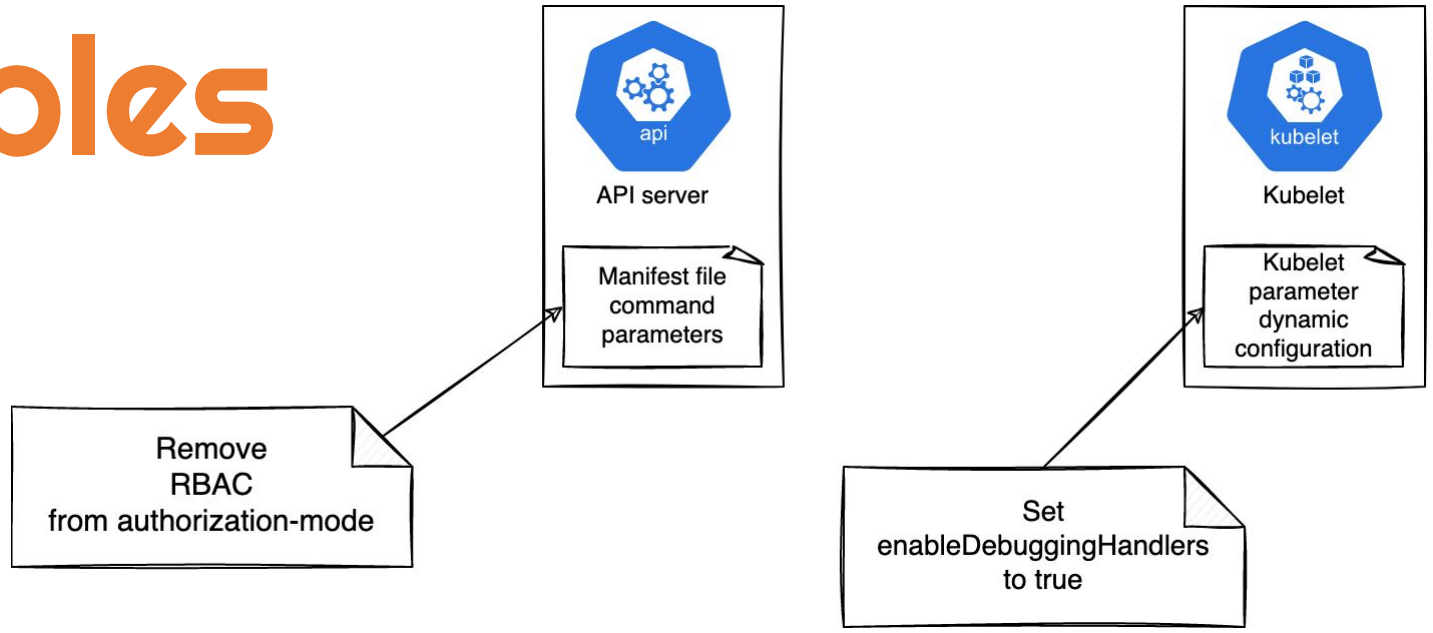
KubeCon CloudNativeCon Europe 2022

# An Open Source Tool

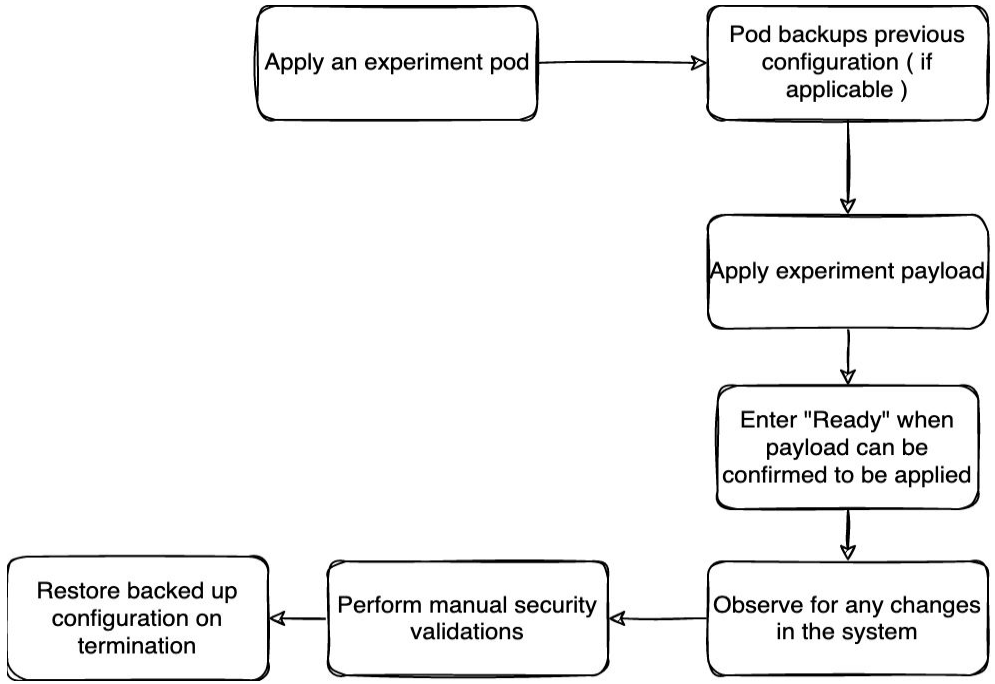
# Targets


CIS Benchmarks™
api
API server
Manifest file command parameters
Master and worker nodes
Node file access rights
kubelet
Kubelet
Kubelet parameter dynamic configuration
Networking
CoreDNS Configmap tampering. DNS spoofing
?

# Experiment examples



# Experiment usage



# Demo Overview

# Demo Video

# Summary

- Learn to navigate complexity with Chaos Engineering
- Use SCE to build confidence in your security
- Chaos Engineering & Security CE are about being proactive
- Email A.A.Ron for a FREE copy of the SCE Report

# Q&A



- How is it different than the other Security Crayons (Red/Blue/Purple/)?
- What's the best way to get started?
- Can you share an example of an SCE Experiment in Kubernetes?

# The End