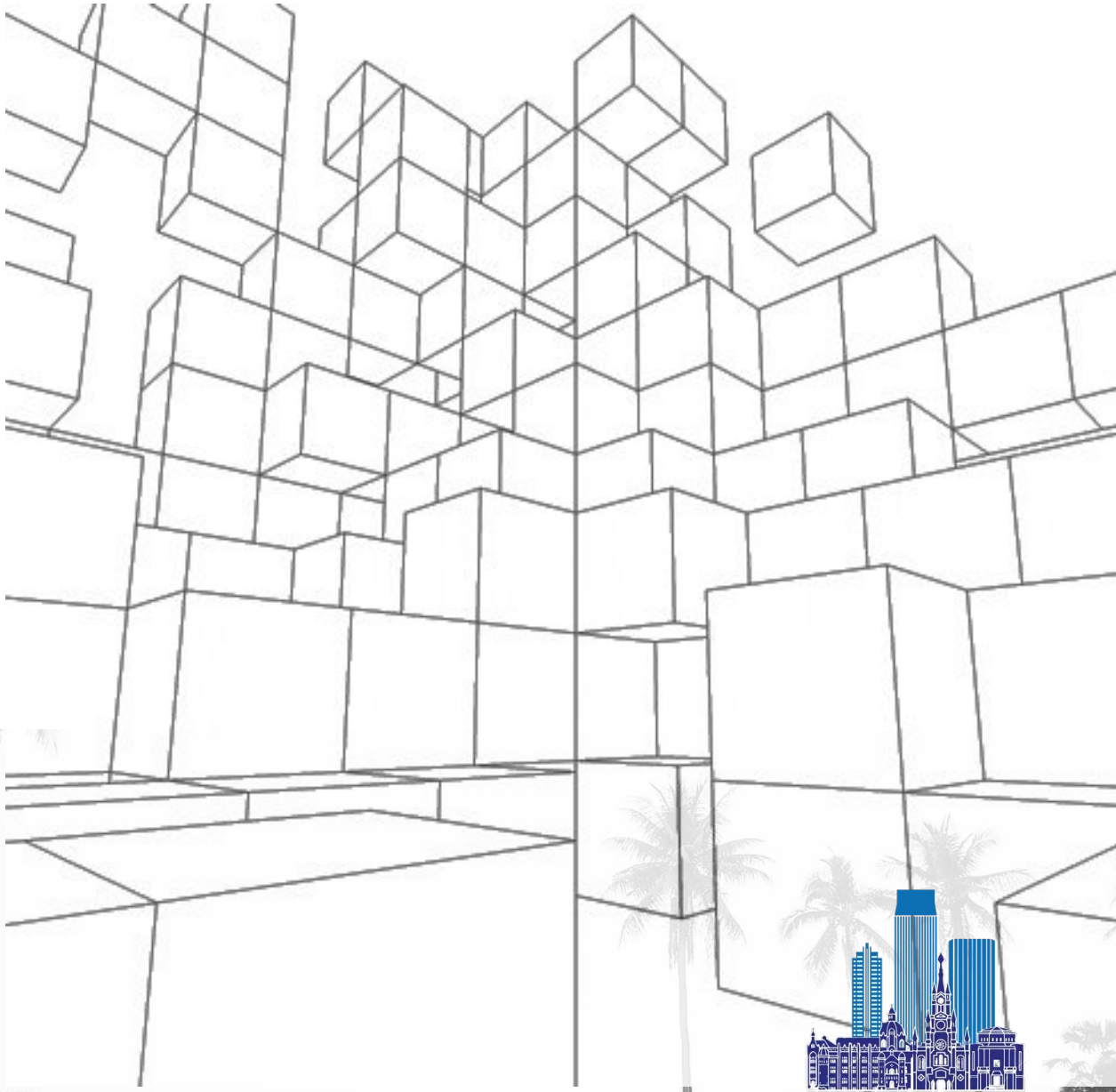
Security Chaos Engineering

@aaronrinehart @verica_io #chaosengineering

Areas Covered

- Combating Complexity in Software
- Chaos Engineering
- Resilience Engineering & Security
- Security Chaos Engineering



@aaronrinehart @verica_io #chaosengineering

DEVOPS DAYS MEDELLIN 2020

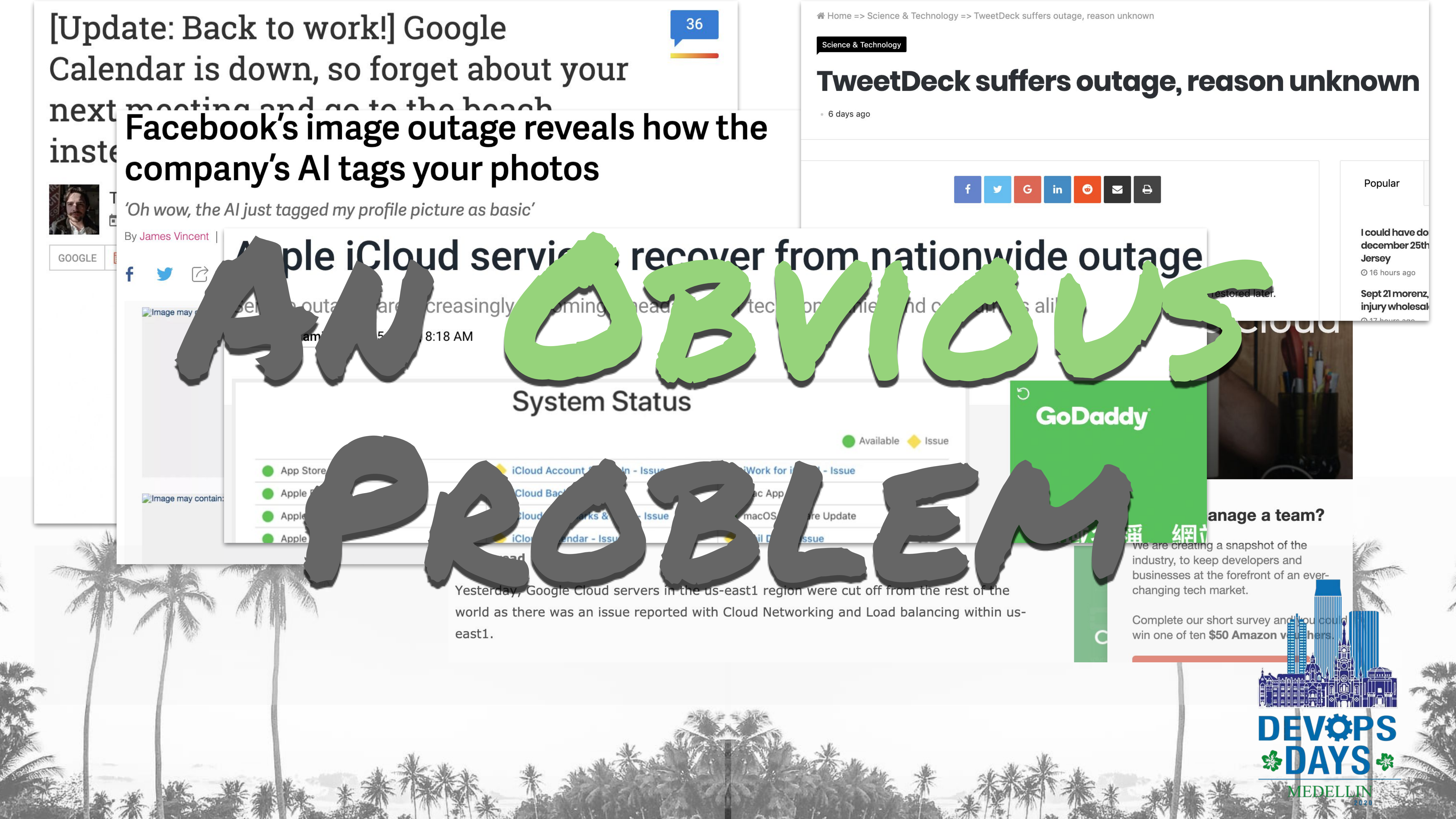
Aaron Rinehart, CTO, Founder

- Former Chief Security Architect @UnitedHealth
- Former DoD, NASA Safety & Reliability Engineering
- Frequent speaker and author on Chaos Engineering & Security
- O'Reilly Author: Chaos Engineering, Security Chaos Engineering Books
- Pioneer behind Security Chaos Engineering
- Led ChaoSlingr team at UnitedHealth

@aaronrinehart @verica_io #chaosengineering

verica

Incidents, Outages, + Breaches are Costly


AN OBVIOUS PROBLEM
[Update: Back to work!] Google Calendar is down, so forget about your next meeting and go to the beach
36
GOOGLE
Facebook's image outage reveals how the company's AI tags your photos
'Oh wow, the AI just tagged my profile picture as basic'
By James Vincent
Home => Science & Technology => TweetDeck suffers outage, reason unknown
Science & Technology
TweetDeck suffers outage, reason unknown
6 days ago
Popular
I could have do december 25th Jersey
16 hours ago
Sept 21 morenz, injury wholesal
restored later.
ple iCloud servi recover from nationwide outage
8:18 AM
System Status
Available
Issue
App Store
iCloud Account
iWork for
Issue
macOS
re Update
GoDaddy
anage a team?
We are creating a snapshot of the industry, to keep developers and businesses at the forefront of an ever-changing tech market.
Complete our short survey and you could win one of ten $50 Amazon vouchers.
Yesterday, Google Cloud servers in the us-east1 region were cut off from the rest of the world as there was an issue reported with Cloud Networking and Load balancing within us-east1.
DEVOPS DAYS
MEDELLIN
2020

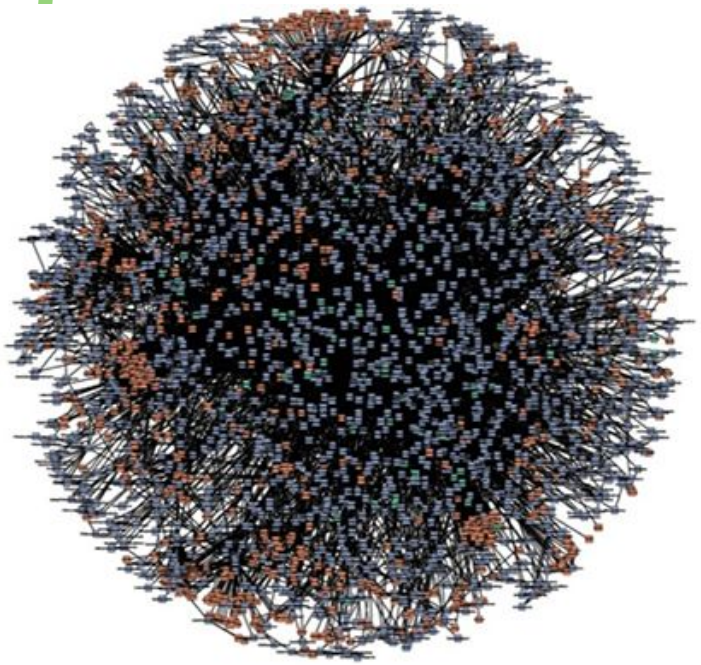
Why do they seem to be happening more often?

Combating Complexity in Software

@aaronrinehart @verica_io #chaosengineering

DEVOPS DAYS MEDELLIN 2020

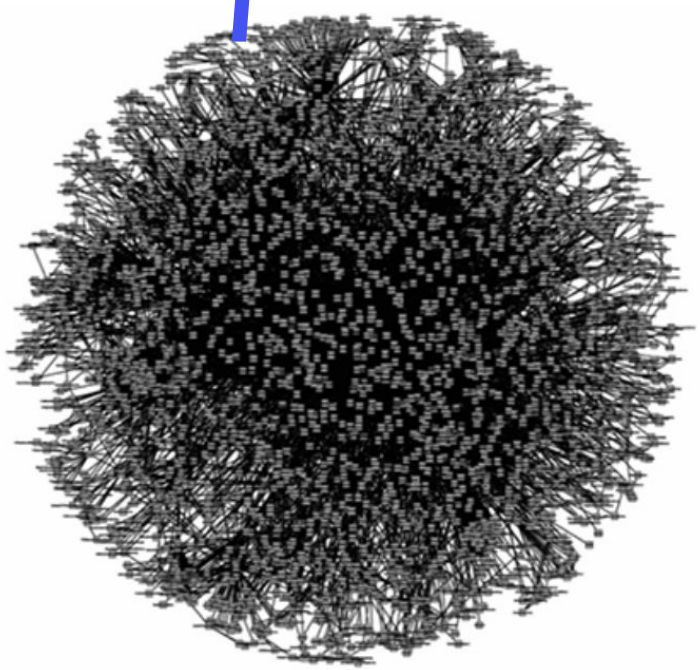
Our systems have evolved beyond human ability to mentally model their behavior.



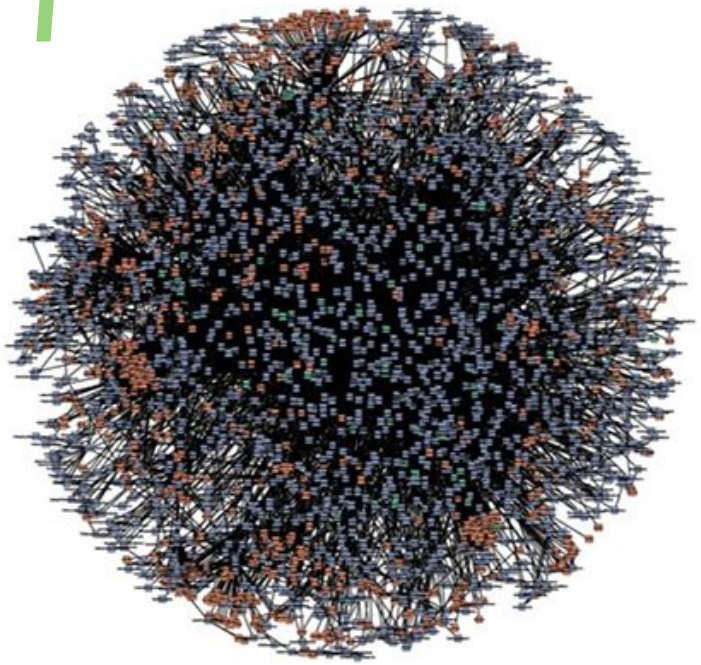
amazon.com

NETFLIX

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



everyone else

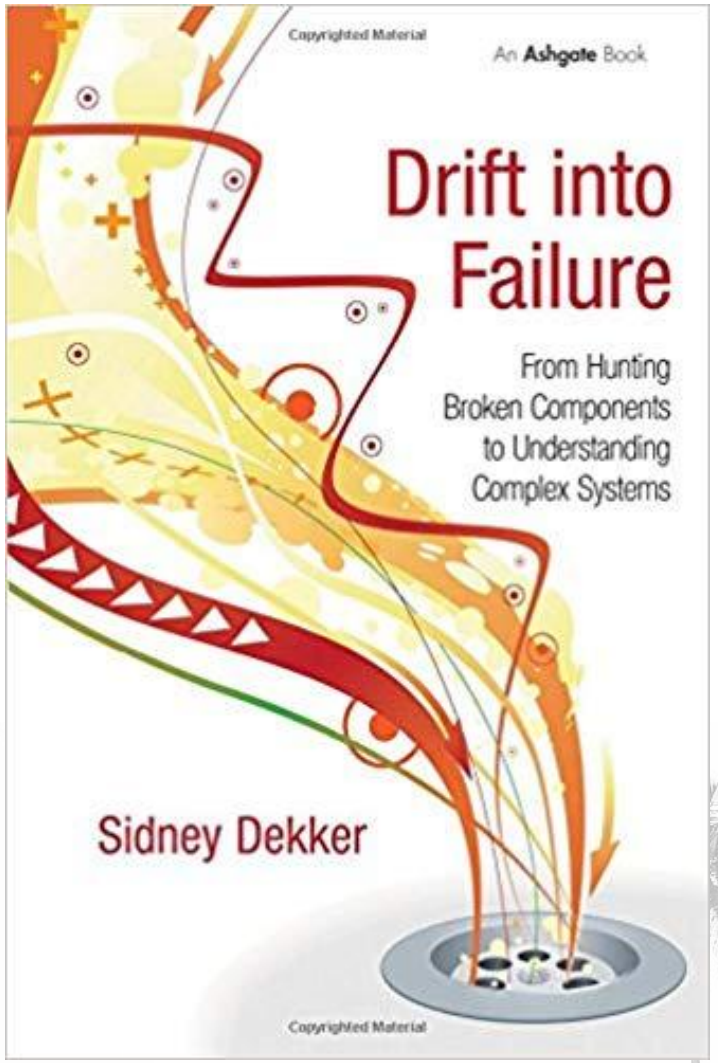


amazon.com

NETFLIX

"The growth of complexity in society has got ahead of our understanding of how complex systems work and fail"

-Sydney Dekker



What Do you Mean by Complex Systems?

@aaronrinehart @verica_io #chaosengineering

DEVOPS DAYS MEDELLIN 2020

Complex?

Continuous Delivery

Distributed Systems

Blue/Green Deployments

Containers

Automation Pipelines

Continuous Integration

DevOps

Infracode

Immutable Infrastructure

CI/CD

Cloud Computing

Service Mesh

Circuit Breaker Patterns

API

Auto Canaries

Microservice Architectures

Security?

Mostly Monolithic

Expert Systems

Stateful in nature

Prevention focused

Poorly Aligned

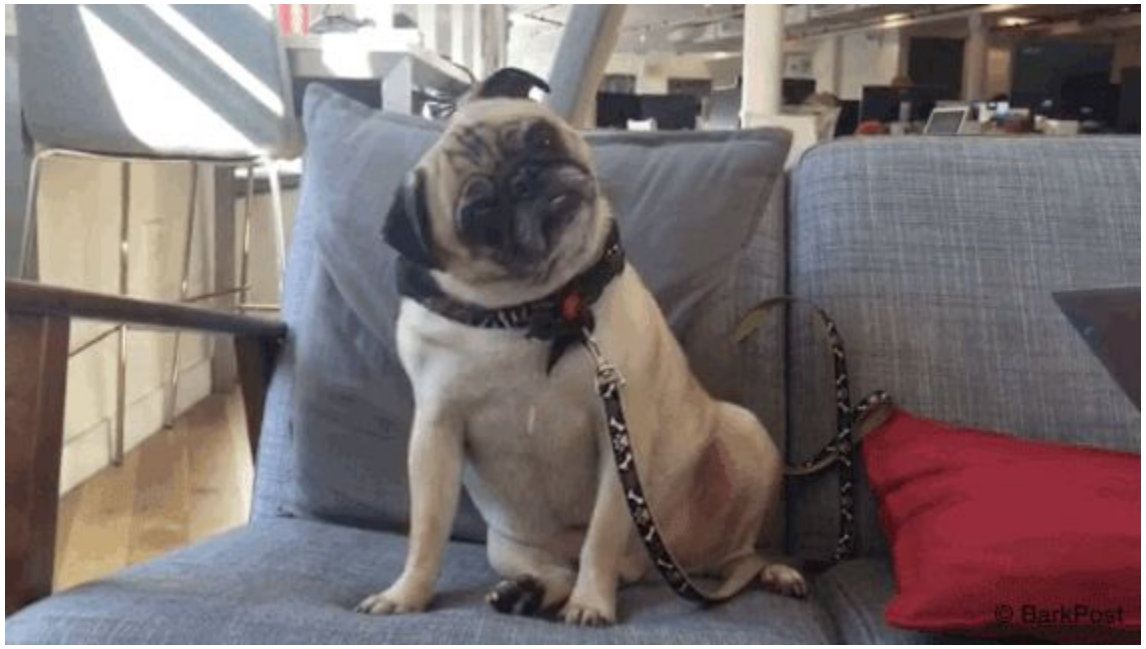
Adversary Focused

Defense in Depth

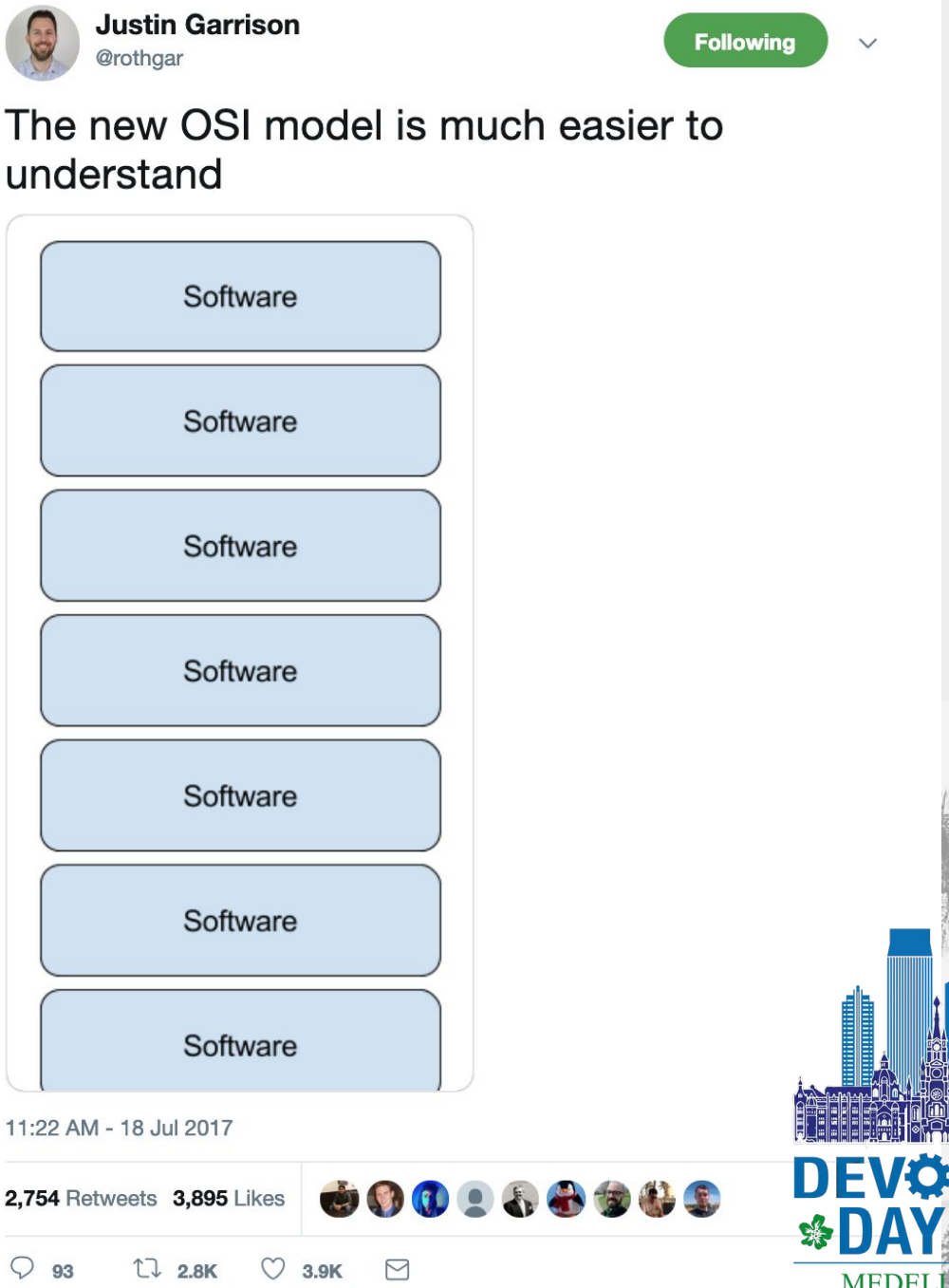
Requires Domain Knowledge

DevSecOps not widely adopted

SIMPLIFY?



Software has officially taken over



DEVOPS DAYS MEDELLIN 2020

Software Only Increases in Complexity

More Abstract

Scripting / interpreted languages

Perl, Python, Shell, Java

High / middle level languages

C, C++

Assembly language

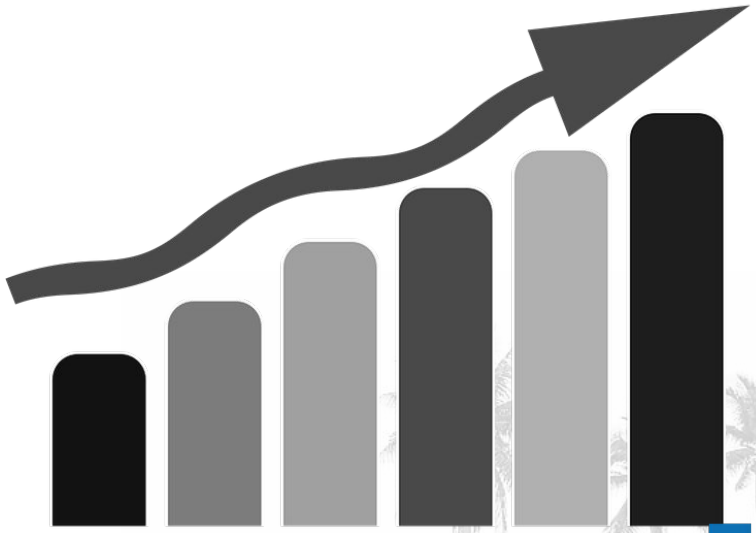
Intel X86, etc (first layer of human-readable code)

Machine code

Hexidecimal representations of binary code read by the operating system

Binary code

Binary code read by hardware - not human-readable



DEVOPS DAYS MEDELLIN 2020

Software Complexity

Accidental

Essential

DEVOPS DAYS MEDELLIN 2020

Woods Theorem:

"As the complexity of a system increases, the accuracy of any single agent's own model of that system decreases"

- Dr. David Woods

What does this have to do with MY SYSTEMS?

DEVOPS DAYS MEDELLIN 2020

Question

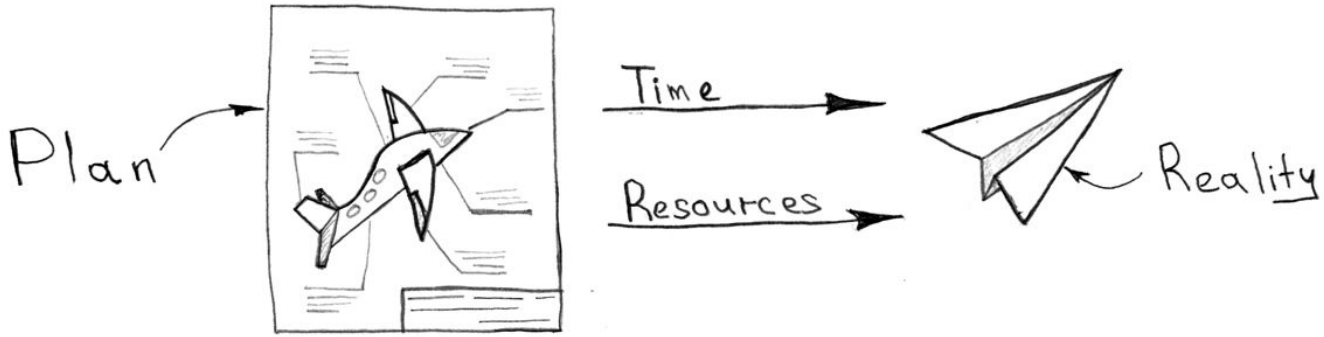
How well do you *really understand* your own systems?

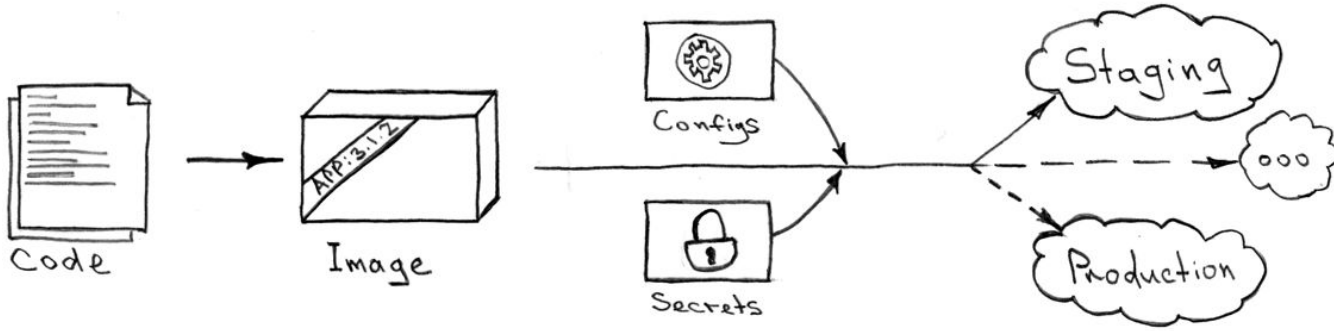
DEVOPS DAYS MEDELLIN 2020

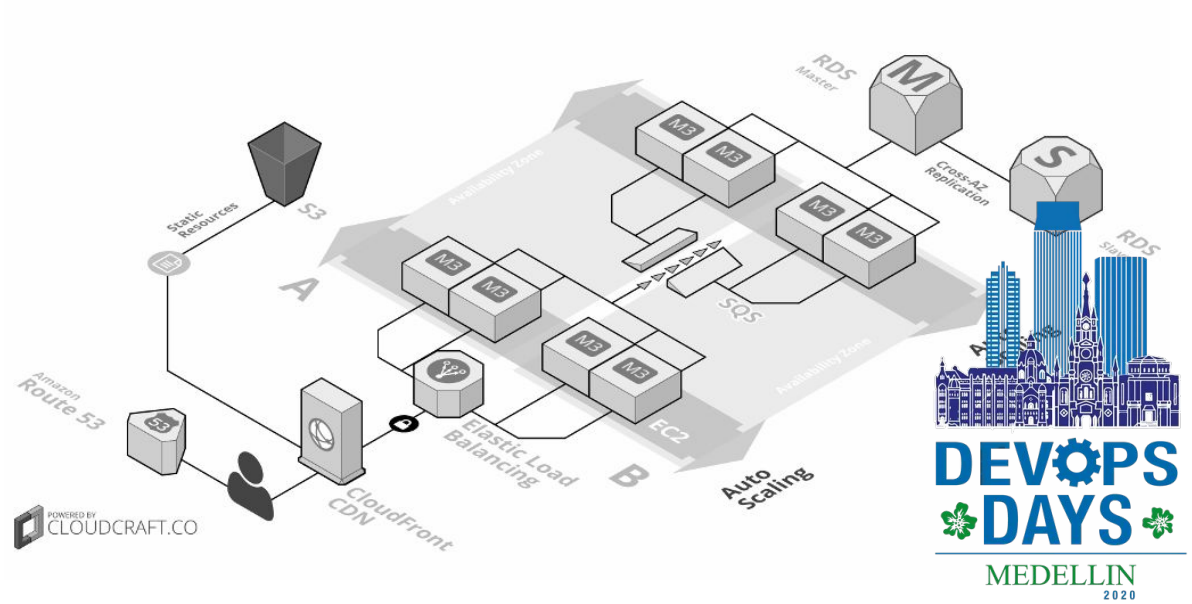
In Reality.....

Systems Engineering is Messy

In the beginning...we think it looks like







After a few months....

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

WAF Outage -> Disa

Scalability Issues

Delayed Features

Large Customer

Years?....

Orphaned Documentation

Hard Coded Passwords

Network is Unreliable

New Security Tool

Autoscaling Keeps Breaking

Portal Retry Storm Outage

Identity Conflicts

Regulatory Audit

Refactor Pricing

Rolling Sev1 Outages on Portal

Lead Software Engineering finds a new job at Google

Cloud Provider API Outage

Code Freeze

Expired Certificate

DNS Resolution Errors

Budget Freeze

Database Outage

Outsource overseas development

Hard Coded Passwords

Network is Unreliable

New Security Tool

Autoscaling Keeps Breaking

Scalability Issues

Corporate Reorg

300 Microservices Δ-> 4000 Microservices

Delayed Features

Identity Conflicts

Migration to New CSP

Firewall Outage -> Disabled

Refactor Pricing

Misconfigured FW Rule Outage

Large Customer Outage

Lead Software Engineering finds a new job at Google

Cloud Provider API Outage

Upgrade to Java SE 12

Exposed Secrets on GithuCode reeze

DNS Resolution Errors

Merger with competitor

Expired Certificate

300 Microservices Δ-> 850 Microservices

Regulatory Audit

WAF Outage -> Disabled

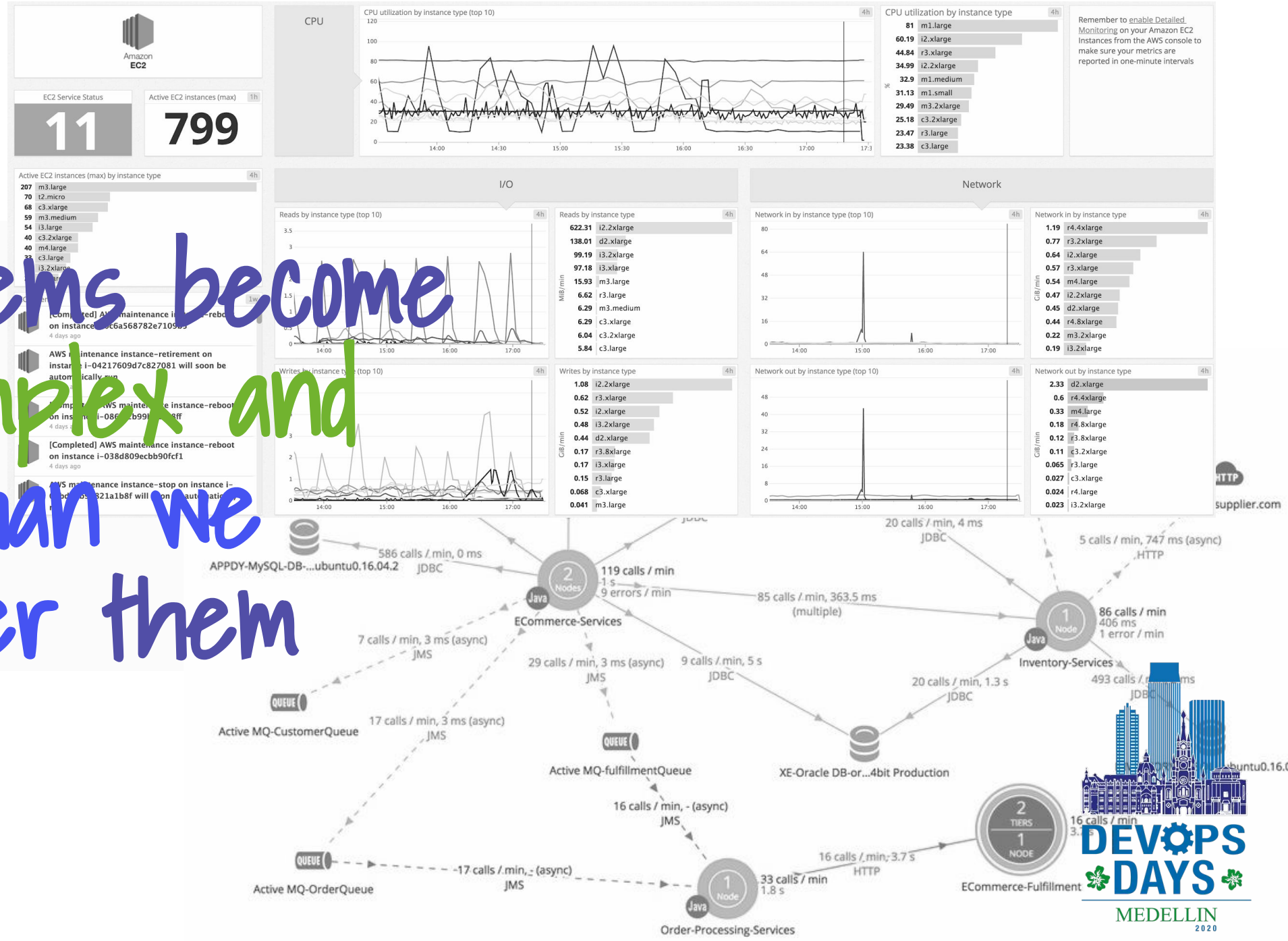
Scalability Issues

Rolling Sev1 Outages on Portal

Delayed Features

Large Customer Outage

Our systems become more complex and messy than we remember them



So what does all of this $&%* have to do with Security?

Putting off critical tasks until everyone forgets about them

Getting Around to Security Next Month

If there's time

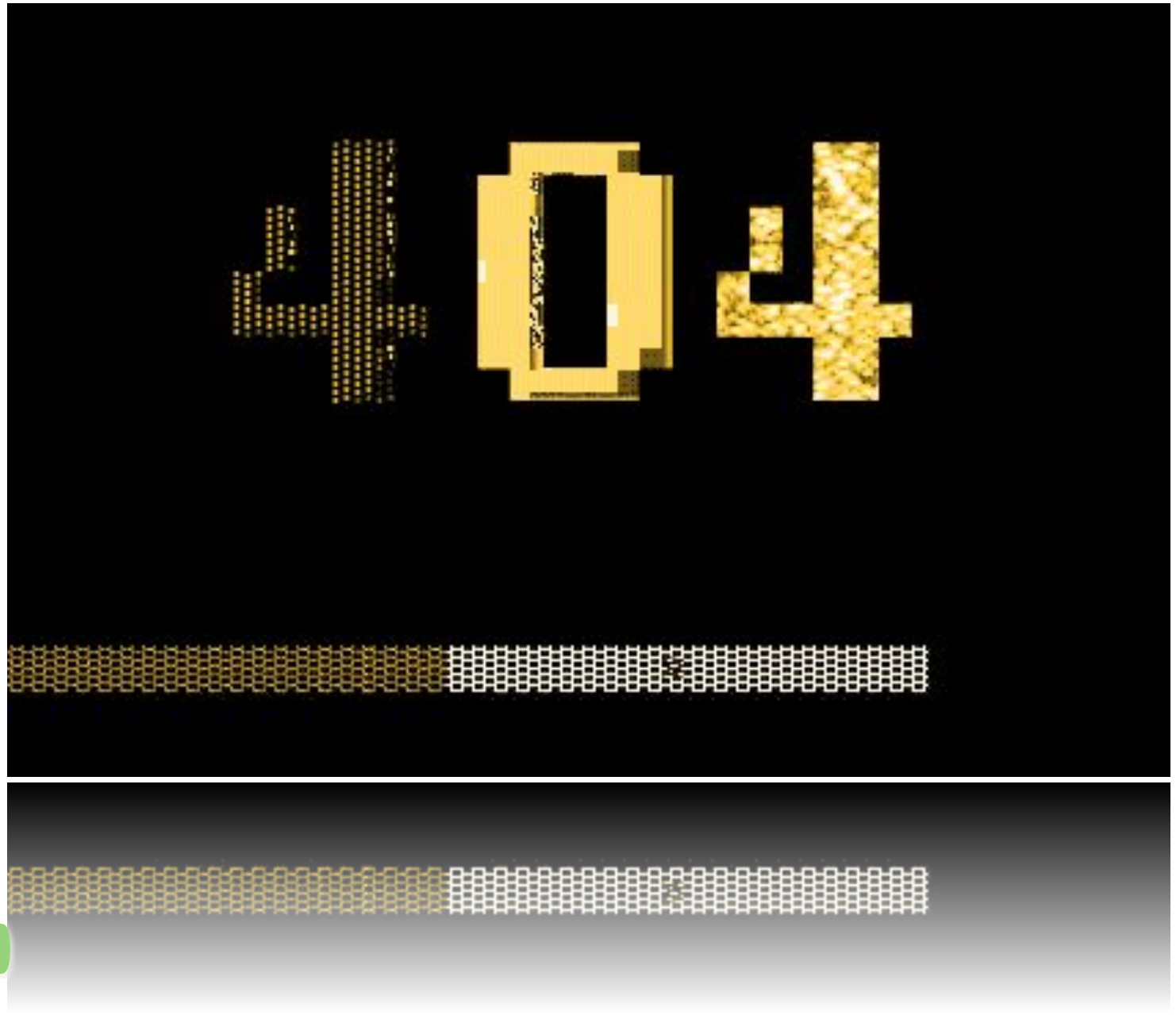
O RLY?

@ThePracticalDev

DEVOPS DAYS MEDELLIN 2020

The Normal Condition is to

FAIL




We need failure
to Learn & Grow

"things that have never happened before happen all the time"

-Scott Sagan "The Limits of Safety"

DEVOPS DAYS MEDELLIN 2020

How do we typically discover when our security measures FAIL?

DEVOPS DAYS MEDELLIN 2020

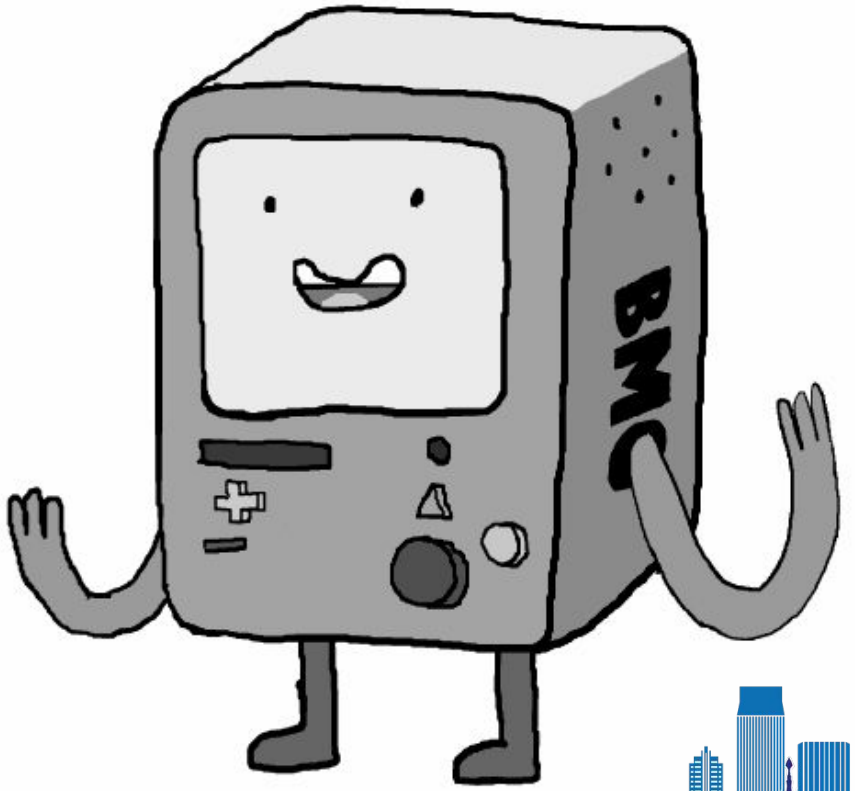
Security Incidents

Security incidents are not effective measures of detection because at that point it's already too late

No System is inherently Secure by Default, its Humans that make them that way.

DEVOPS DAYS MEDELLIN 2020

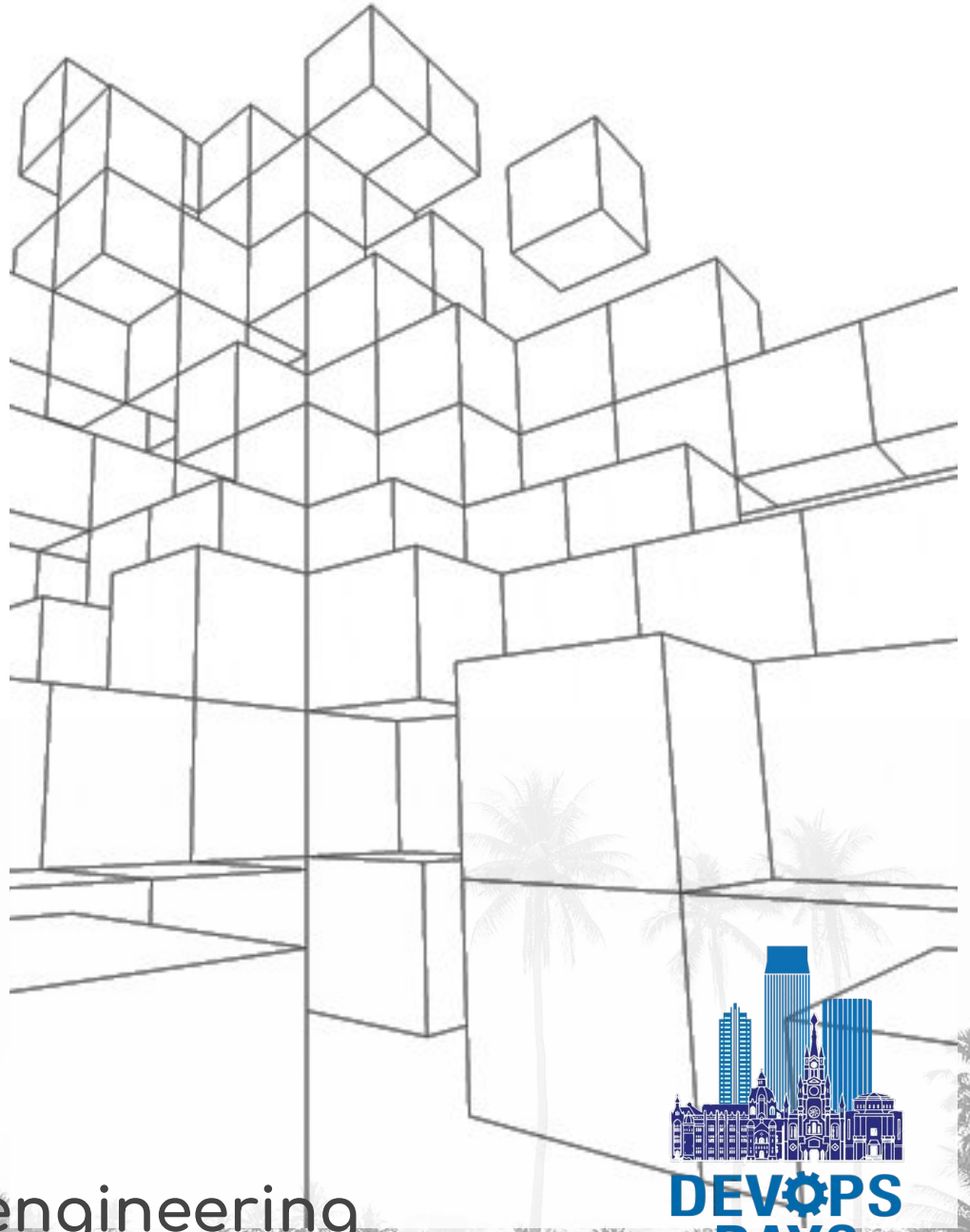
People Operate Differently when they expect things to fail



DEVOPS DAYS MEDELLIN 2020


Awesome!

Chaos Engineering



@aaronrinehart @verica_io #chaosengineering

DEVOPS DAYS MEDELLIN 2020

Chaos Engineering

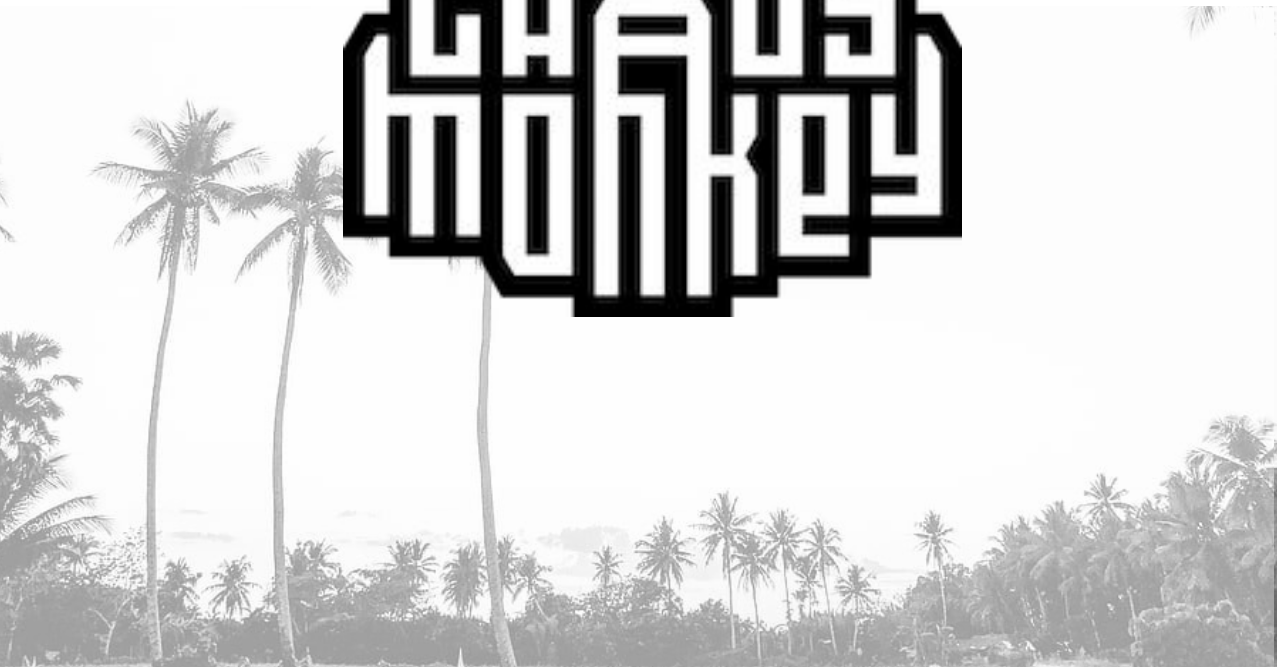
"Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in the system's ability to withstand turbulent conditions"

Chaos Engineerin

Is about establishing order from Chaos

DEVOPS DAYS MEDELLIN 2020

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

DEVOPS DAYS MEDELLIN 2020

Who is doing Chaos?

DEVOPS DAYS MEDELLIN 2020

O'REILLY

Compliments of NETFLIX

Chaos Engineering

Building Confidence through Experimen

O'REILLY

Chaos Engineering

System Resiliency in Practice

O'REILLY

Security Chaos Engineering

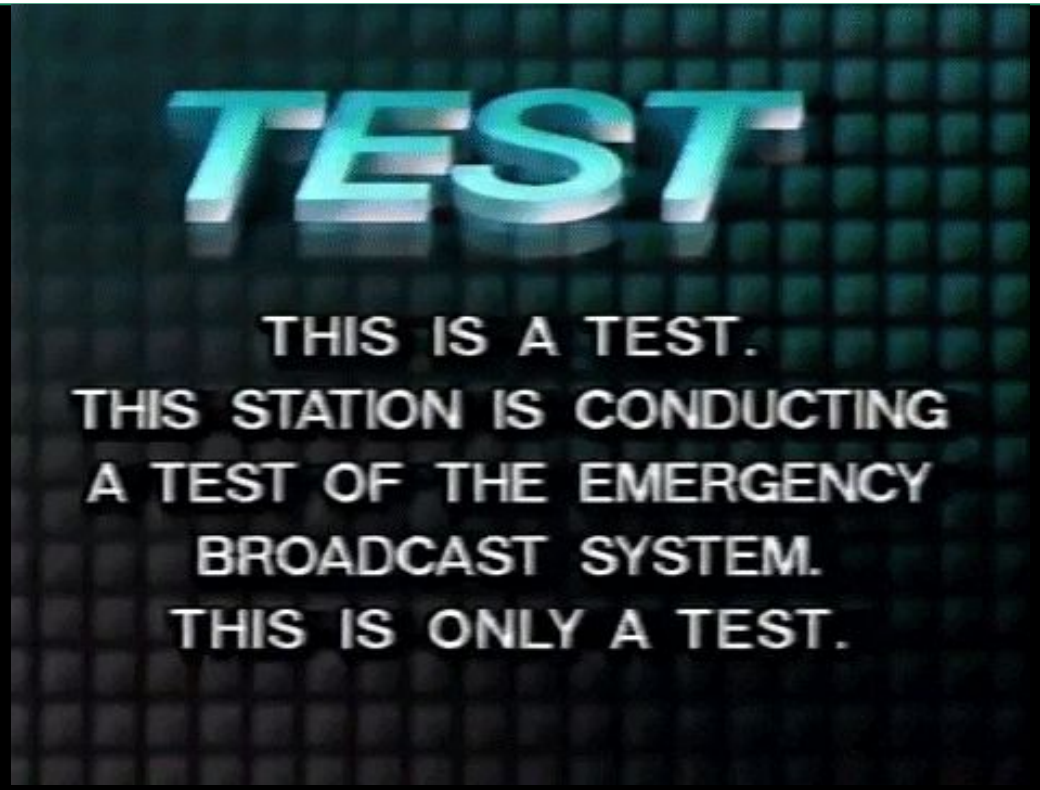
Continuous Security Verification in Practice

Release Fall 2020

DEVOPS DAYS MEDELLIN 2020

Instrumenting Chaos

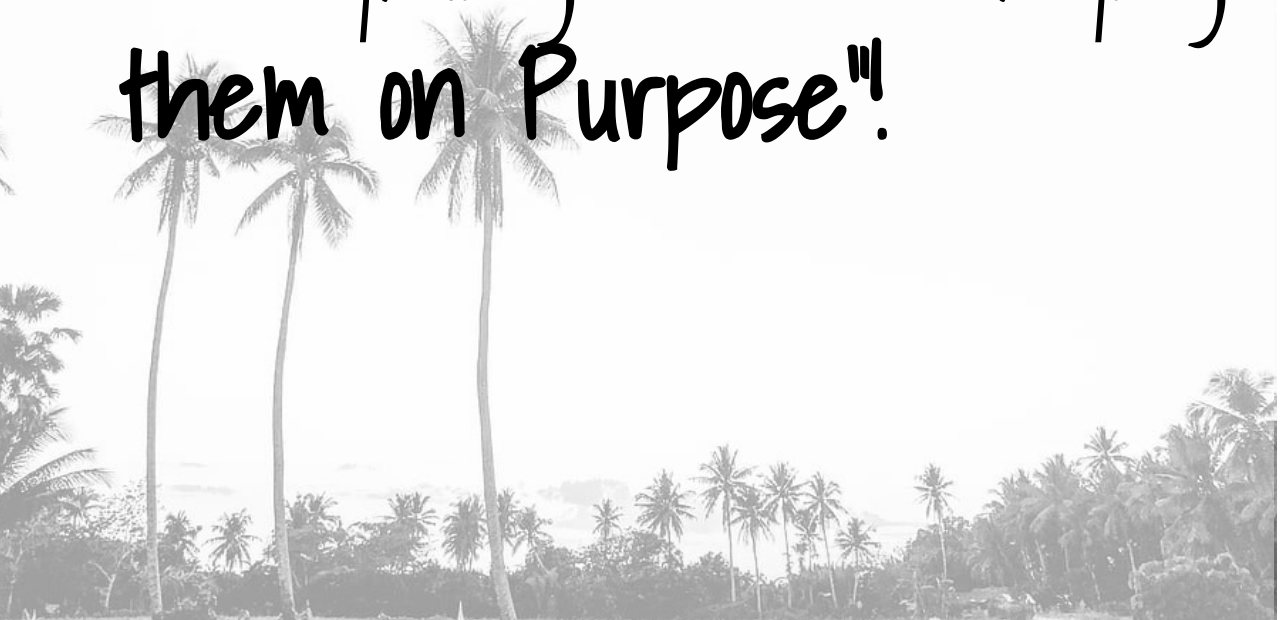
Testing vs. Experimentation



Chaos Pitfalls: Breaking things on Purpose

The purpose of Chaos Engineering is **NOT** to "Break Things on Purpose".
If anything we are trying to "Fix them on Purpose"!

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



Reference: Nora Jones 8 Traps of Chaos Engineering

DEVOPS DAYS MEDELLIN 2020

SECURITY

CHAOS ENGINEERING

DEVOPS DAYS MEDELLIN 2020

Hope is Not an Effective Strategy

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

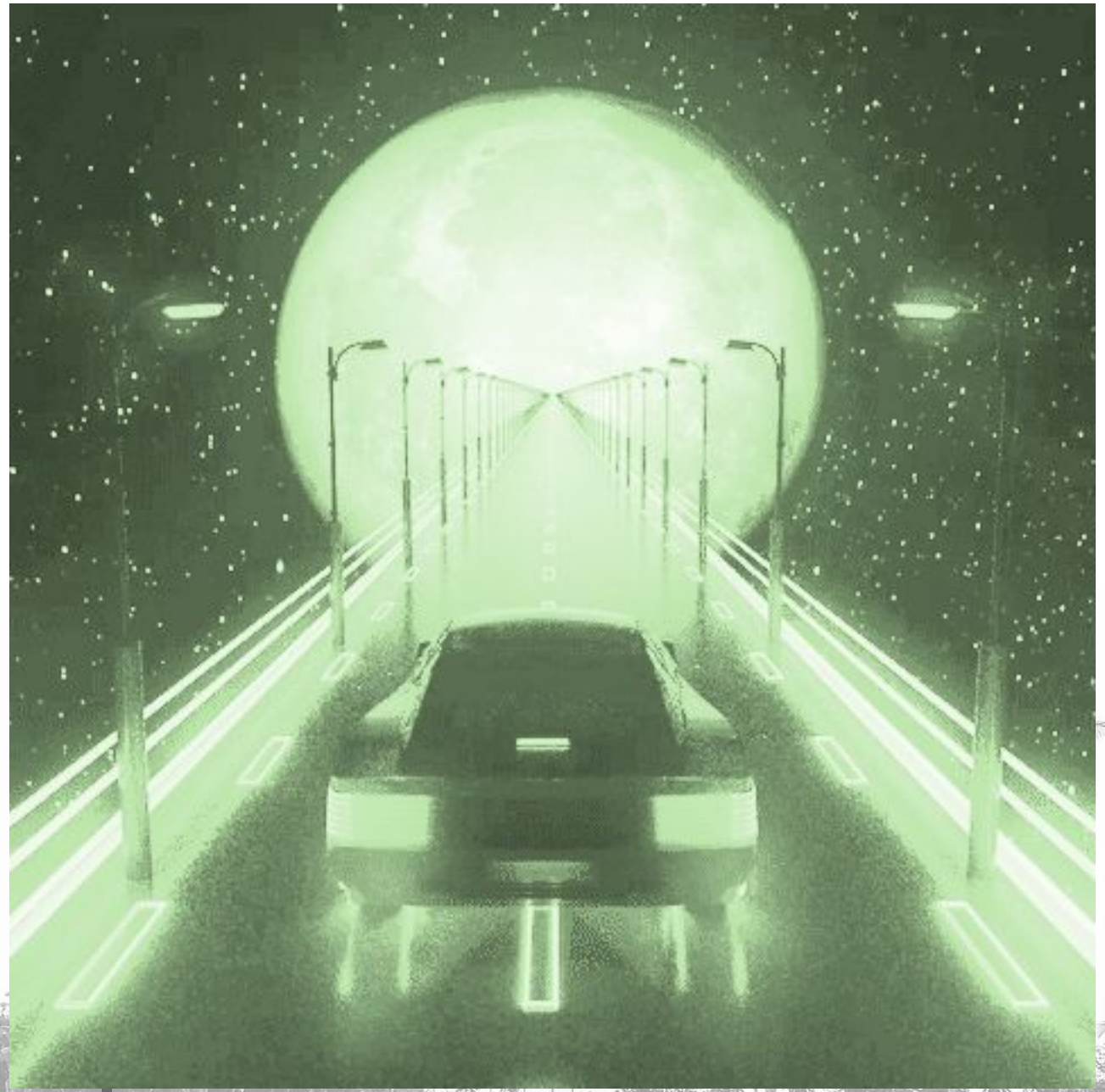
"Understand your system and where its security gaps are before an adversary does"

DEVOPS DAYS MEDELLIN 2020

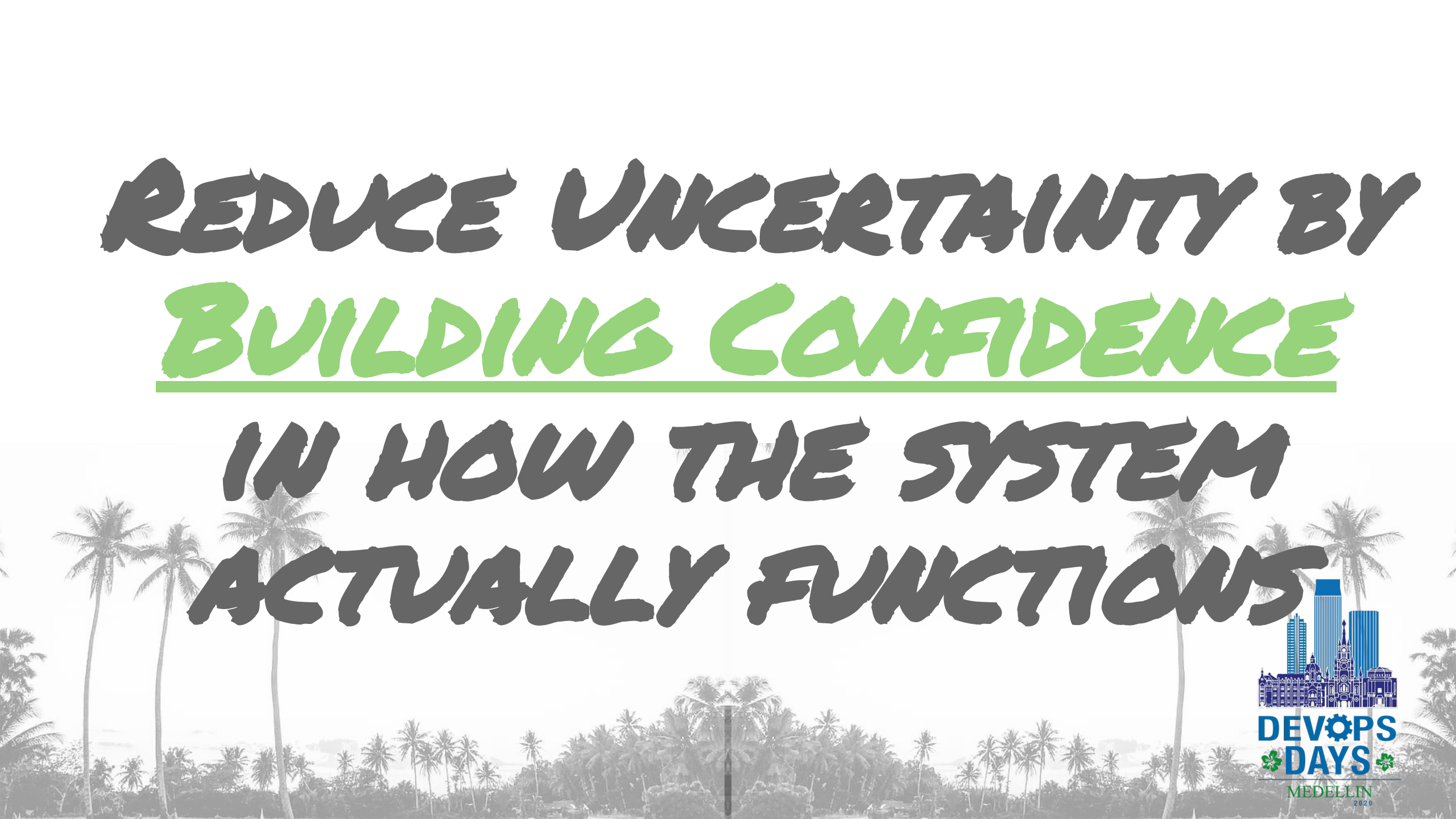
WE OFTEN MISREMEMBER WHAT OUR SYSTEMS REALLY ARE, AND AS A RESULT THE OPPORTUNITY FOR ACCIDENTS & MISTAKES INCREASES

DEVOPS DAYS MEDELLIN 2020

Continuous Security Verification



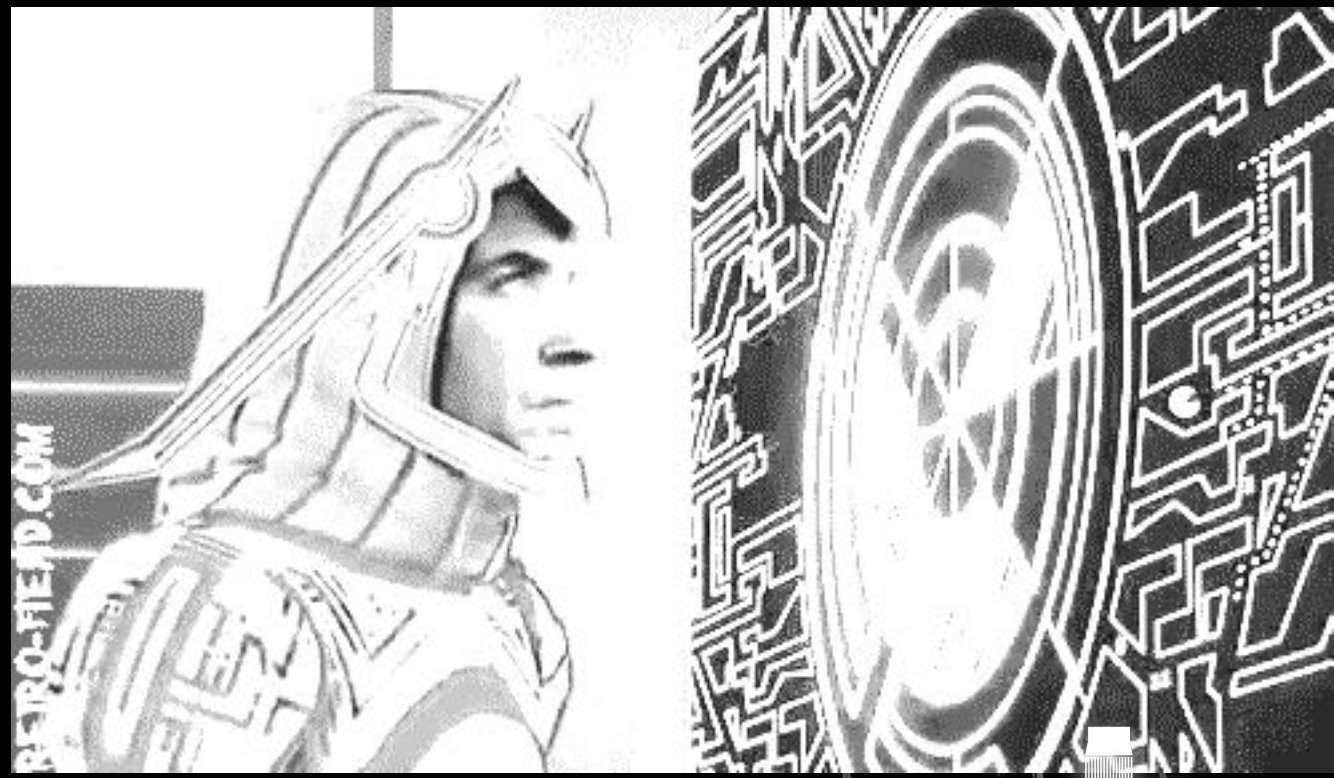
Reduce Uncertainty by Building Confidence in how the system actually functions



Use Cases

Use Cases

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



DEVOPS DAYS MEDELLIN 2020

Incident Response

"Response" is the problem with incident response.

Security Incidents are Subjective

No matter how much we prepare...

We really don't know very much

Where?

Why?

Who?

How?

What?

DEVOPS DAYS MEDELLIN 2020

Flip the Model

Post Mortem = Preparation

ChaoSlingr

An Open Source Tool

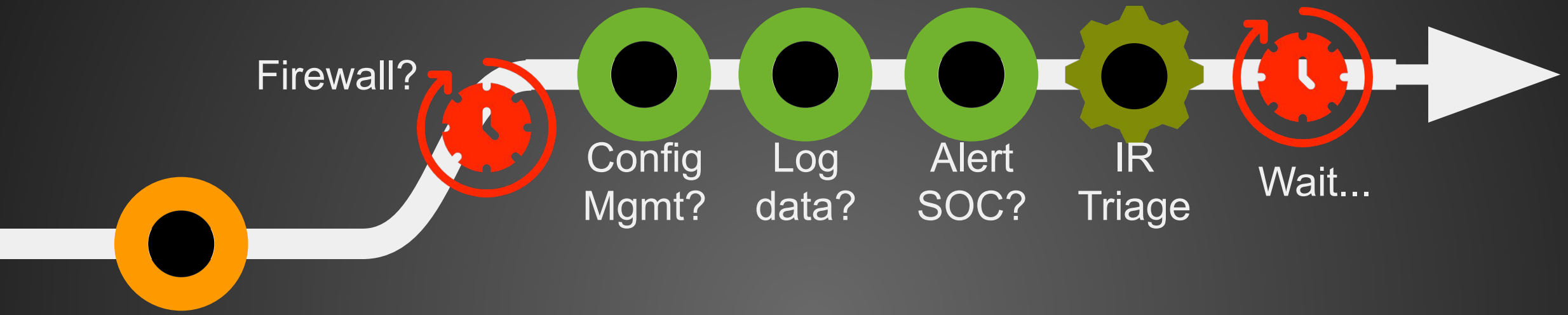
ChaoSlingr Product Features

- ChatOps Integration
- Configuration-as-Code
- Example Code & Open Framework
- Serverless App in AWS
- 100% Native AWS
- Configurable Operational Mode & Frequency
- Opt-In | Opt-Out Model

An Example: PortSlingr

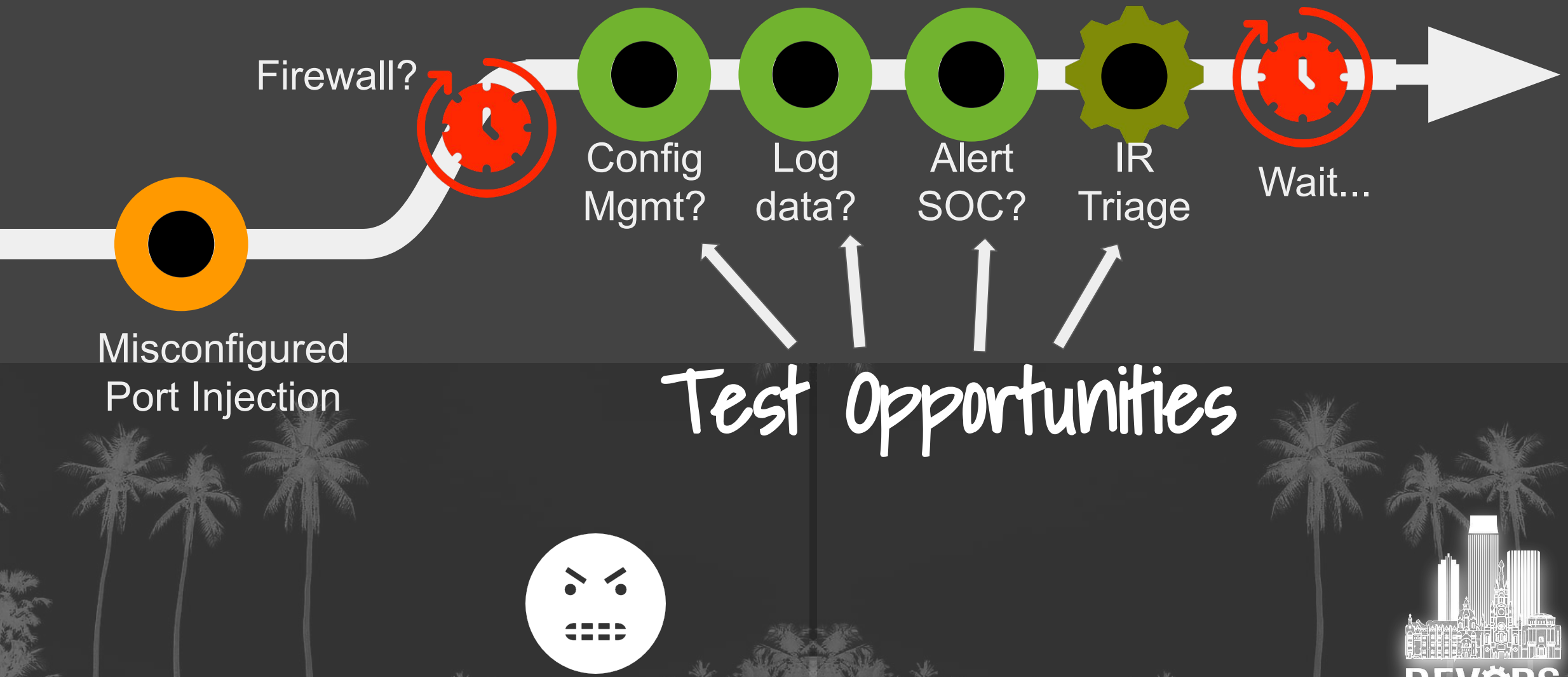
Experiment Hypothesis: A Misconfigured or Unauthorized Port Change in AWS

DEVOPS DAYS MEDELLIN 2020



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

DEVOPS DAYS MEDELLIN 2020



DEVOPS DAYS MEDELLIN 2020

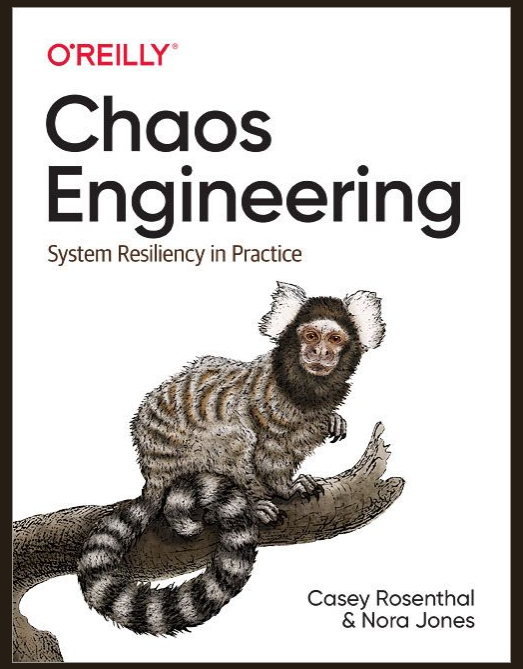
Stop looking for better answers and *start asking better questions.*

– John Allspaw

DEVOPS DAYS MEDELLIN 2020

Free copy mailed to you complements of Verica

VERICA



verica.io/book

DEVOPS DAYS MEDELLIN 2020