SKILUP SM DAYS

by: DevOps INSTITUTE

Security Precognition: Crafting Secure & Resilient Systems using Chaos Engineering

Name: Aaron Rinehart
Title: CTO, Founder
Organization: Verica
Twitter: aaronrinehart
Email: aaron@verica.io

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

In this Session we will cover

Incidents, Outages, & Breaches are Costly

Be right back.

We're making updates to the Apple Store. Check back soon.

An Obvious Problem

[Update: Back to work!] Google Calendar is down, so forget about your next meeting and go to the beach instead

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 |

Image may contain: 1 person, outdoor

Image may contain: 1 person, sky, outdoor

Image may contain: 2 people, people

Apple iCloud service recovers from nationwide outage

By Humza Aa... on July ...019 ...8 AM

System Status

App Store

Apple Books

Apple Business Manager

Apple ID

Cloud Account & Sign In - Issue

3 min re...

Yesterday, Google Cloud servers in the us-east1 world as there was an issue reported with Cloud east1.

Home => Science & Technology => TweetDeck suffers outage, reason unknown

Science & Technology

TweetDeck suffers outage, reason unknown

6 days ago

...ntly, Twitter's ...restored later.

Popular

I could have do... december 25th Jersey

16 hours ago

Sept 21 morenz, injury wholesal...

GoDaddy

...loudflare suffers another major outage

Mike ...7 ...

...hi... ...major ...ta... ...in ...matter of weeks

Complete our short survey and you could win one of ten **$50 Amazon vouchers**.

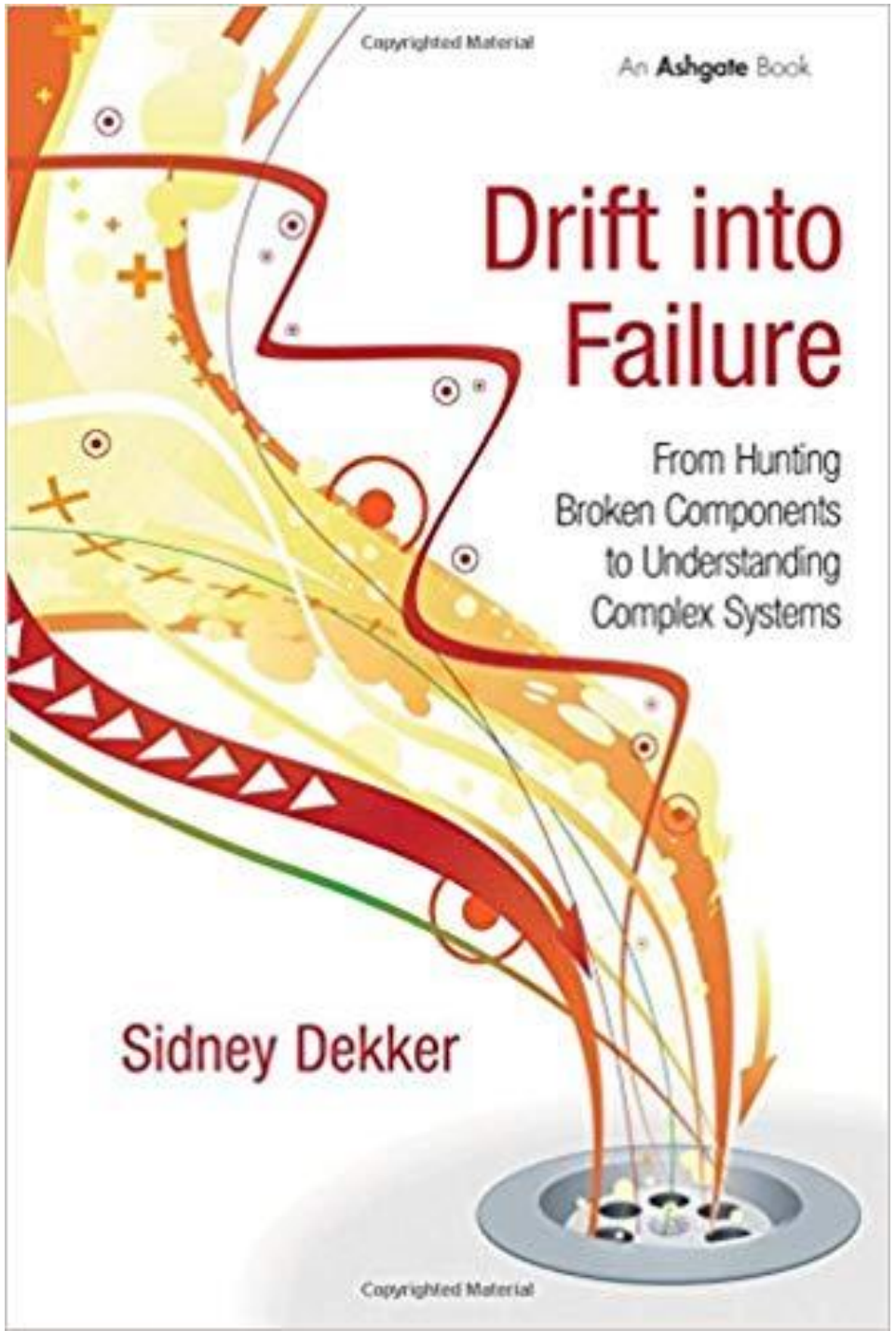
Why do they seem to be happening more often?

Combating Complexity in Software

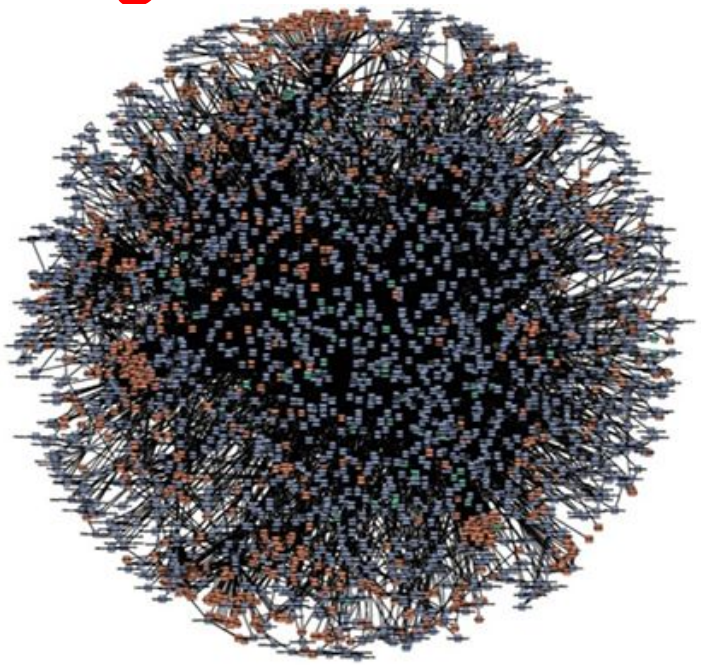
@aaronrinehart @verica_io #chaosengineering

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

-Sydney Dekker



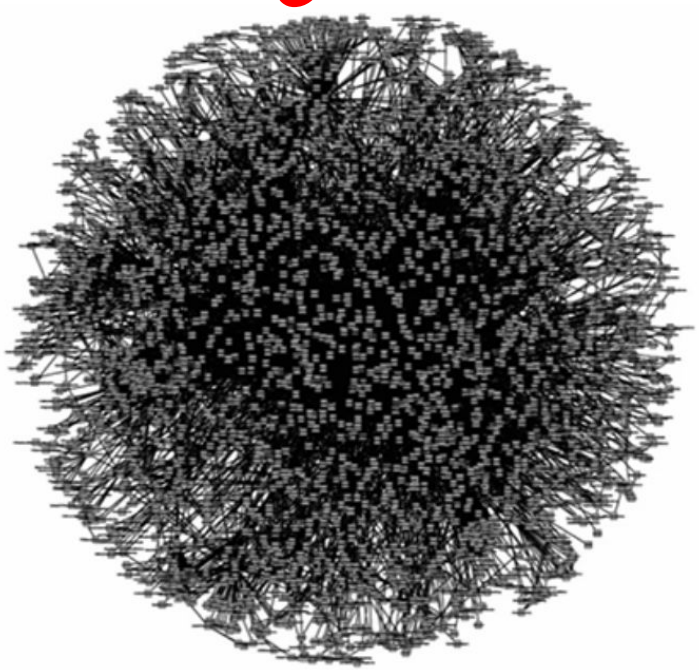
Our systems have evolved beyond human ability to mentally model their behavior.



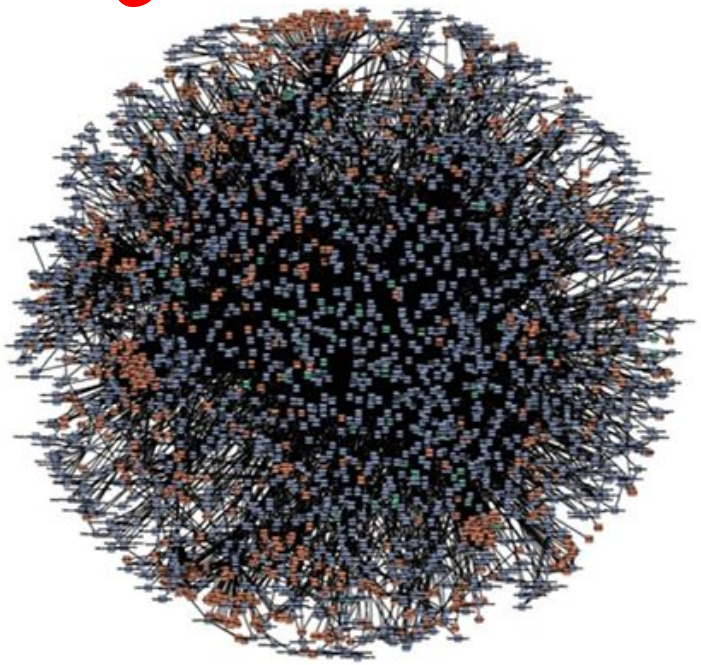
amazon.com

NETFLIX

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



everyone else



amazon.com

NETFLIX

Complex?

Continuous Delivery

Distributed Systems

Microservice Architectures

Blue/Green Deployments

Automation Pipelines

Containers

Continuous Integration

CI/CD

DevOps

Infracode

Immutable Infrastructure

Cloud Computing

Service Mesh

API

Auto Canaries

Circuit Breaker Patterns

Security?

Mostly Monolithic

Prevention focused

Defense in Depth

Expert Systems

Poorly Aligned

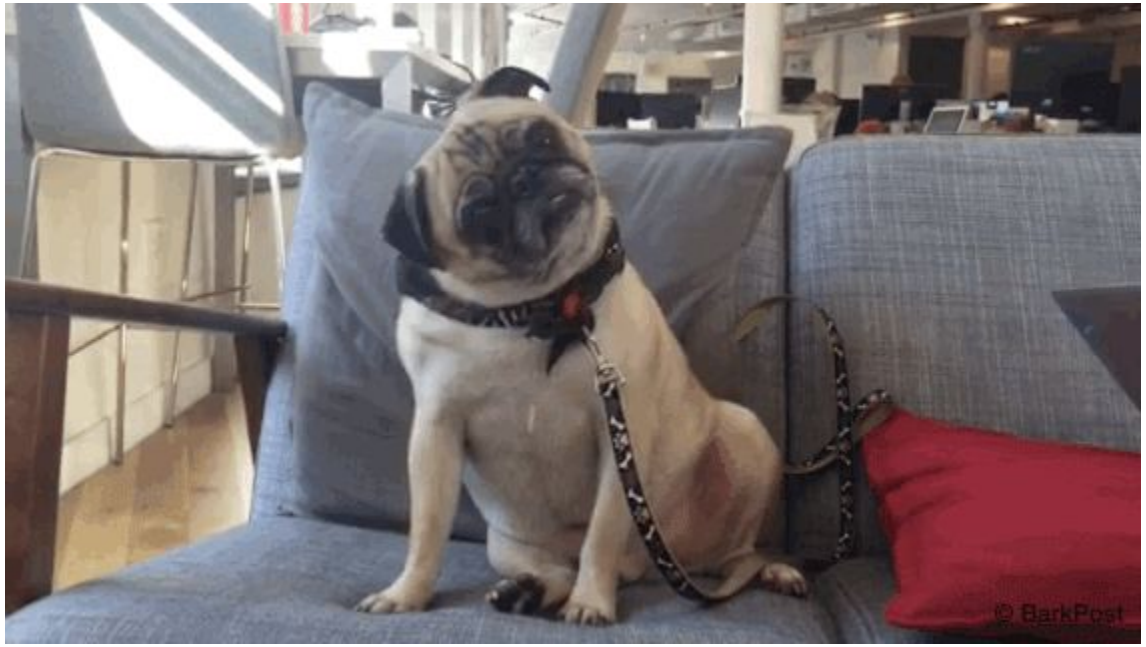
Requires Domain Knowledge

Stateful in nature

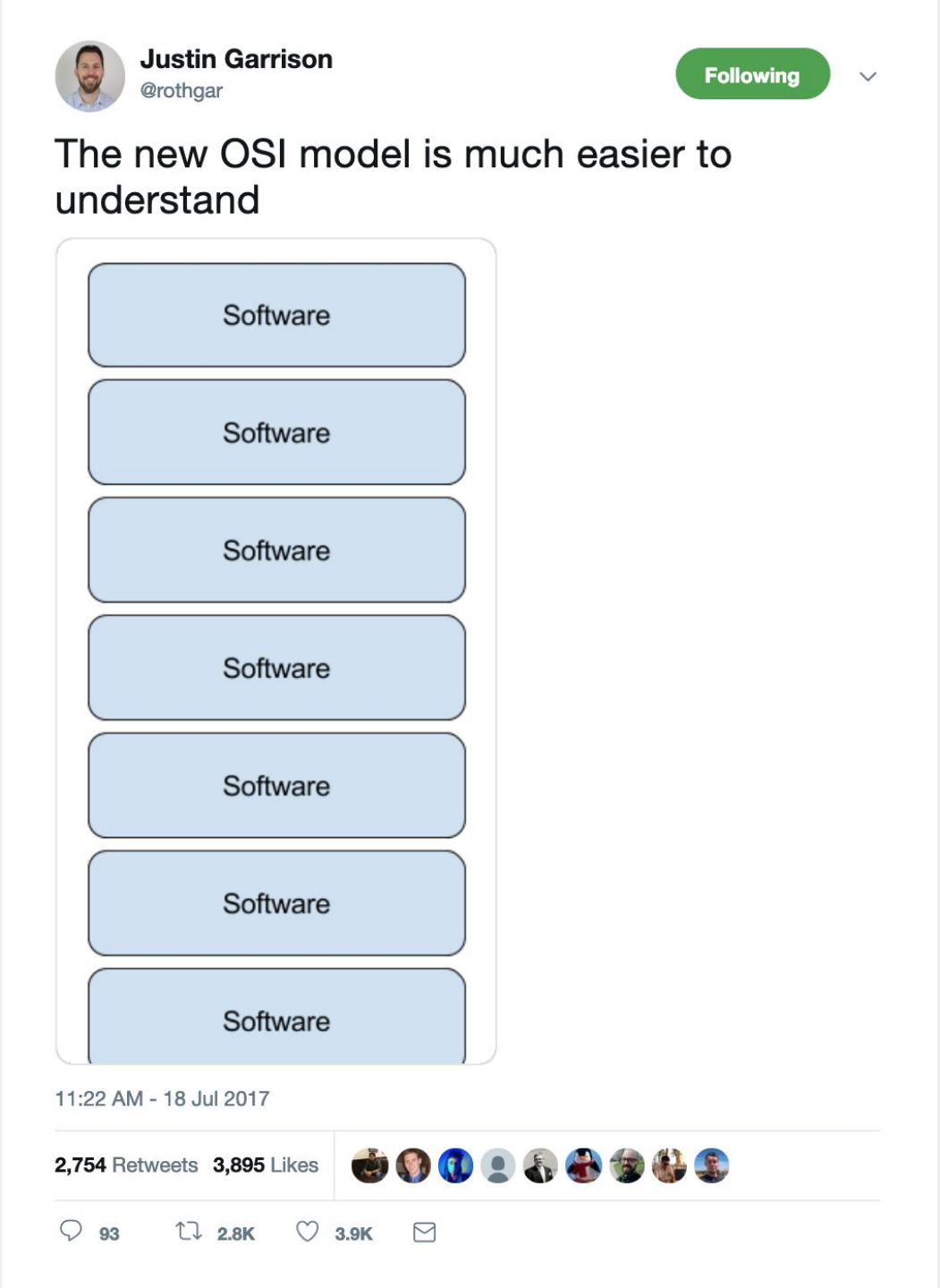
Adversary Focused

DevSecOps not widely adopted

Simplify?



Software has officially taken over



Software Only Increases in Complexity

More Abstract

Scripting / interpreted languages

Perl, Python, Shell, Java

High / middle level languages

C, C++

Assembly language

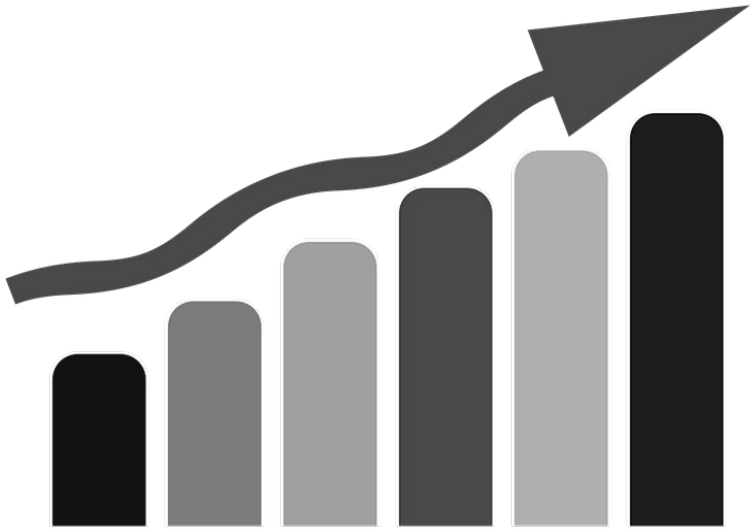
Intel X86, etc (first layer of human-readable code)

Machine code

Hexidecimal representations of binary code read by the operating system

Binary code

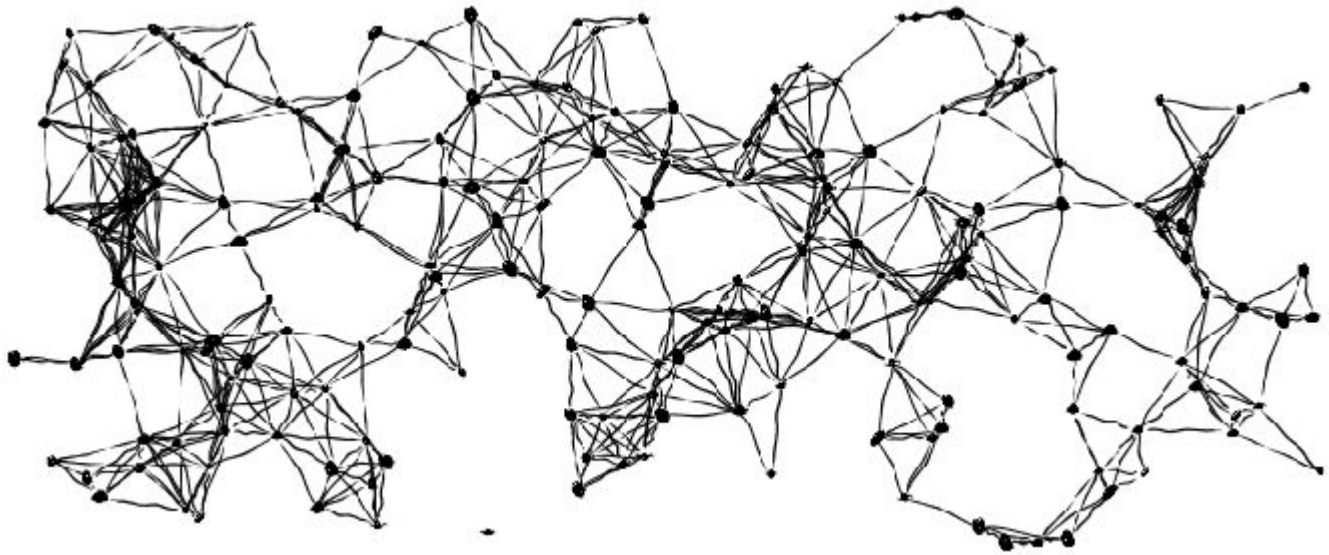
Binary code read by hardware - not human-readable



Software Complexity

Accidental

Essential



Woods Theorem:

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

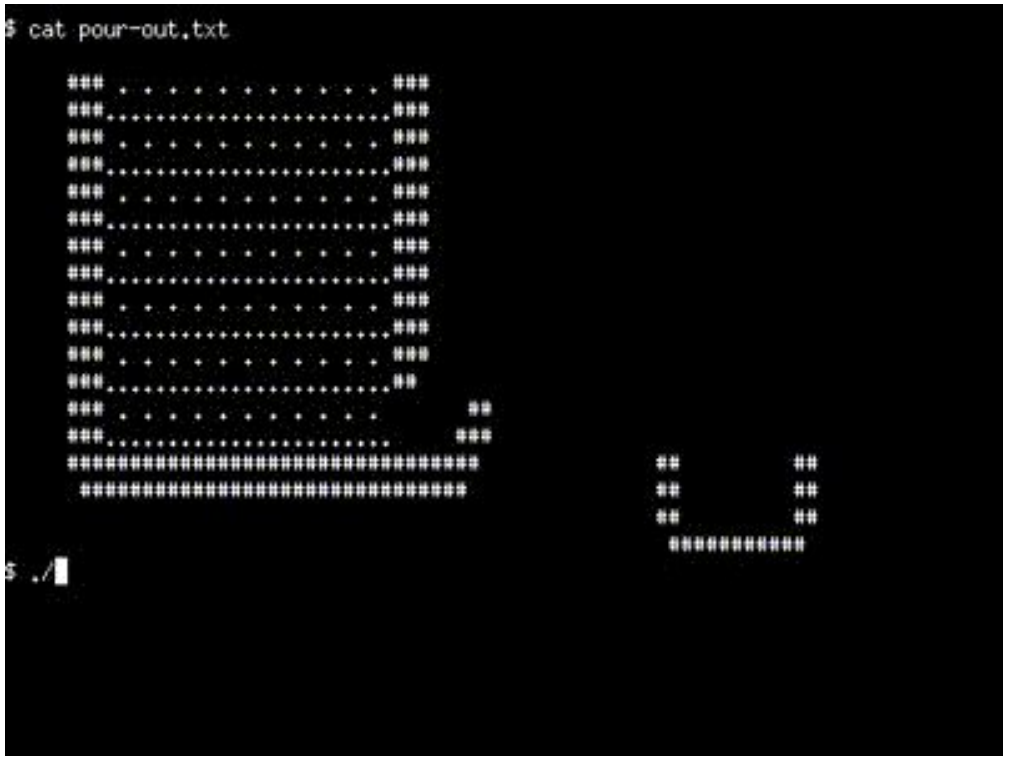
- Dr. David Woods

What does this have to do with my systems?

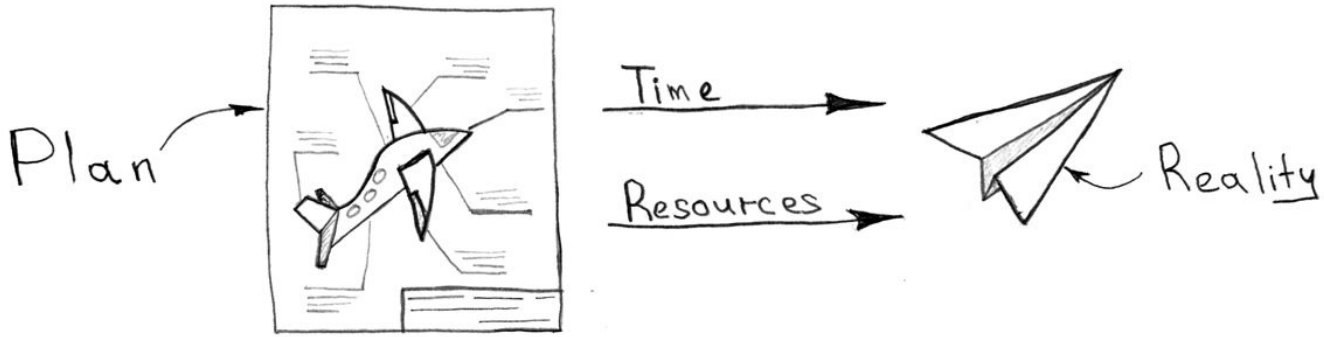
Question - How well do you really understand how **your system** works?

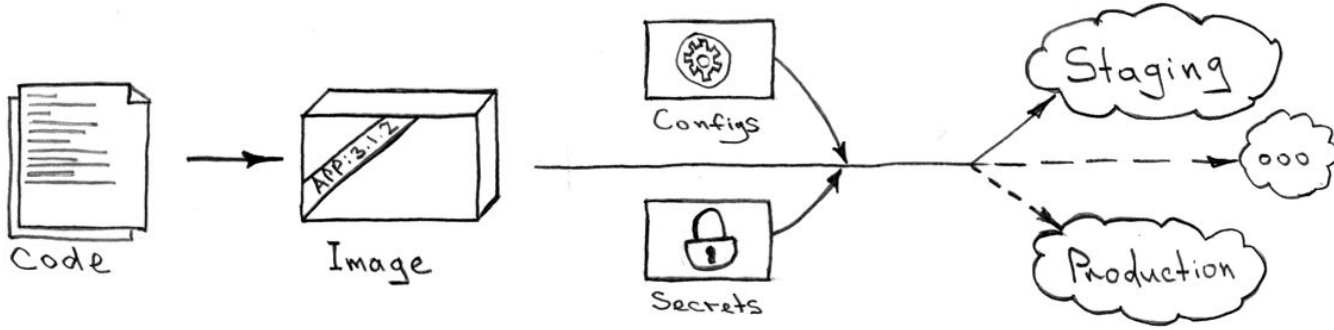
In Reality.....

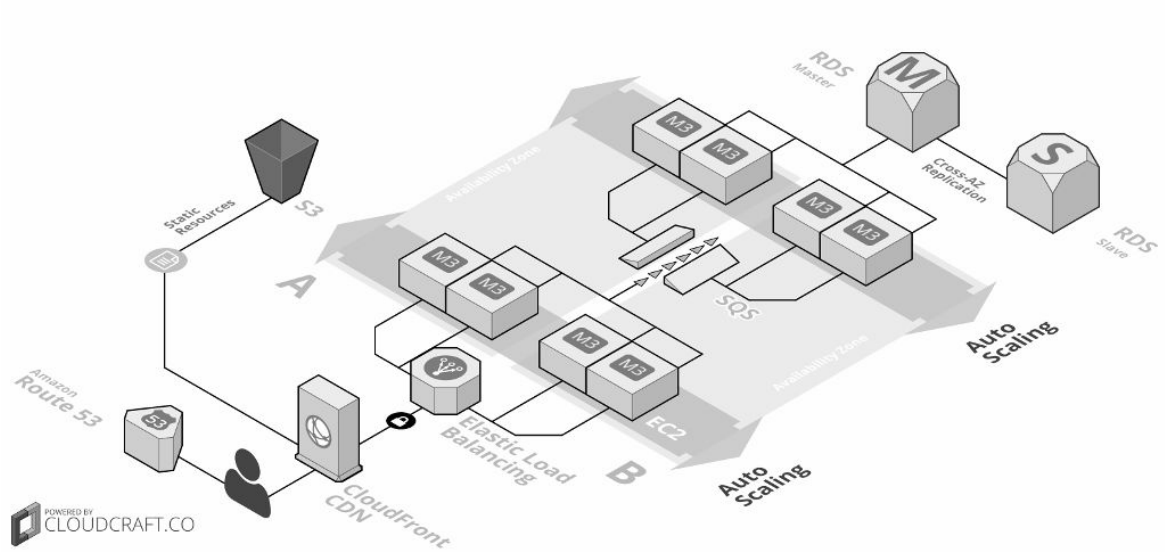
Systems Engineering is **Messy**



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 Sevl 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

Years?....

Orphaned Documentation

Portal Retry Storm Outage

Regulatory Audit

Rolling Sevl Outages on Portal

Code Freeze

Budget Freeze

Hard Coded Passwords

New Security Tool

Corporate Reorg

Identity Conflicts

Migration to New CSP

Refactor Pricing

Lead Software Engineering finds a new job at Google

Upgrade to Java SE 12

Expired Certificate

300 Microservices Δ-> 850 Microservices

Scalability Issues

Delayed Features

Hard Coded Passwords

New Security Tool

Identity Conflicts

Lead Software Engineering finds a new job at Google

Expired Certificate

Database Outage

Network is Unreliable

Scalability Issues

Delayed Features

Misconfigured FW Rule Outage

WAF Outage -> Disabled

Network is Unreliable

Autoscaling Keeps Breaking

Refactor Pricing

Cloud Provider API Outage

DNS Resolution Errors

Outsource overseas development

Autoscaling Keeps Breaking

300 Microservices Δ-> 4000 Microservices

Firewall Outage -> Disabled

Cloud Provider API Outage

Large Customer Outage

Exposed Secrets on GithuCode Freeze

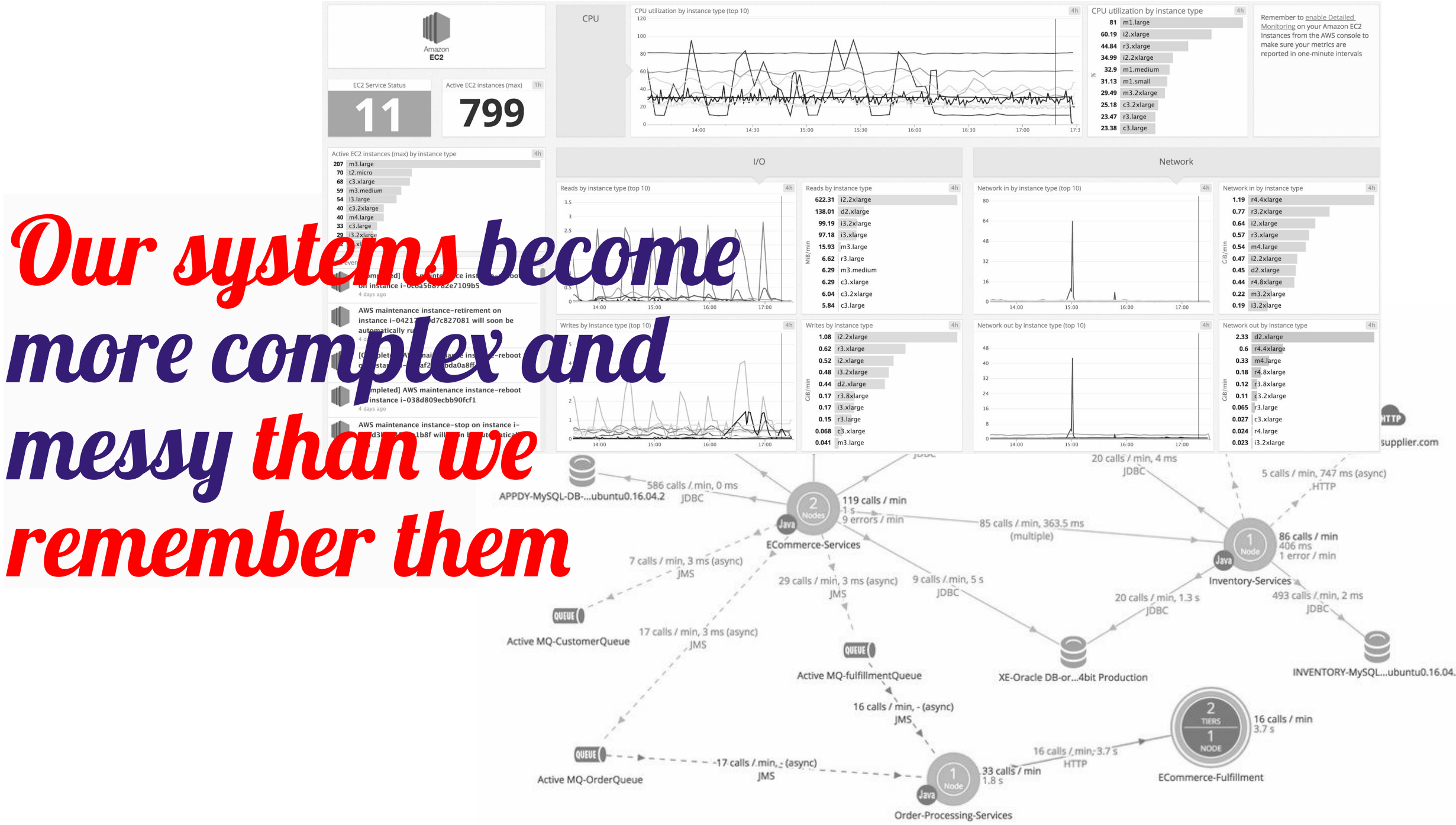
DNS Resolution Errors

Merger with competitor

Regulatory Audit

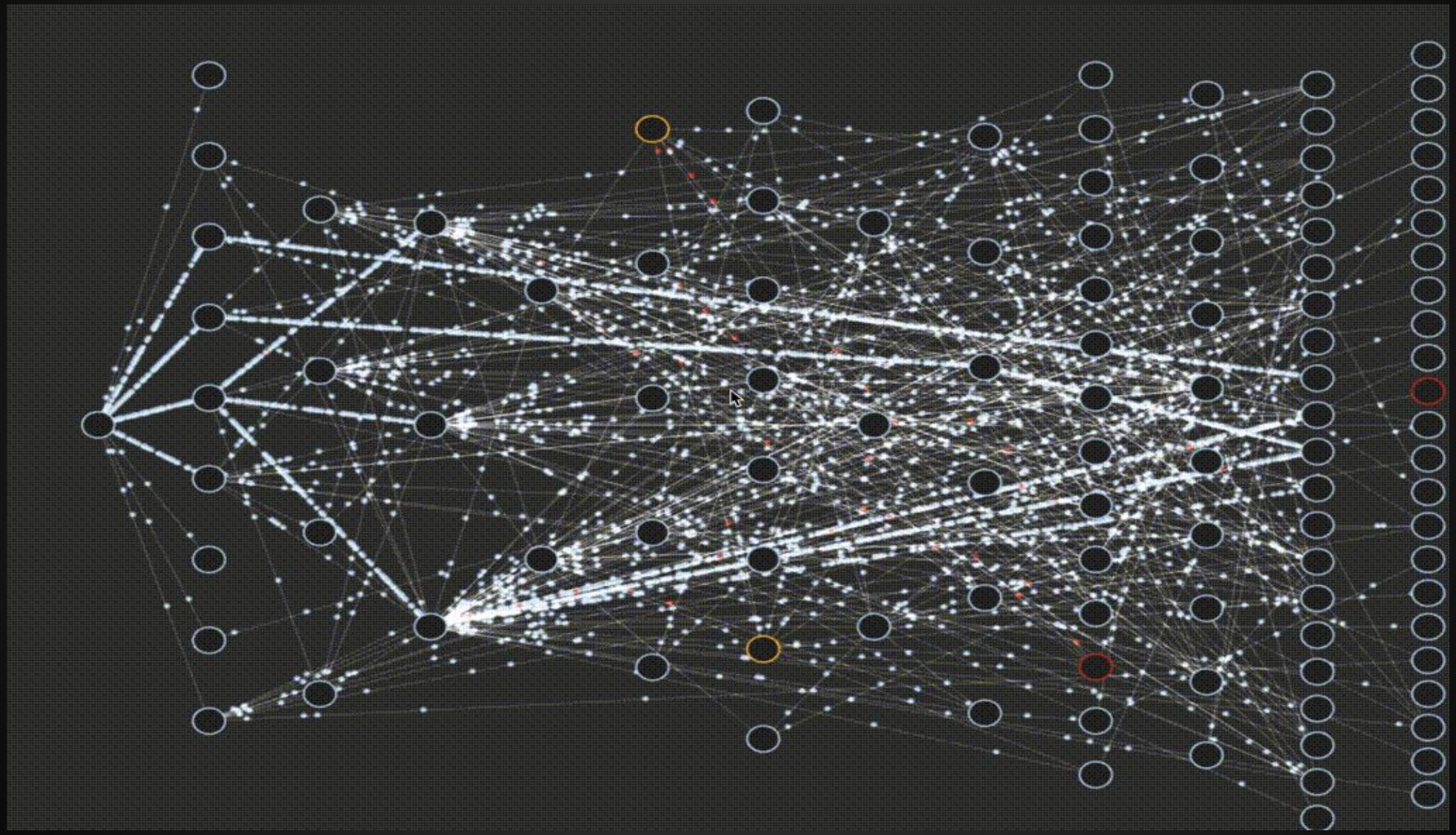
Rolling Sevl Outage on Portal

Large Customer



Our systems become more complex and messy than we remember them

Difficult to Mentally Model



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

Failure Happens Alot

The Normal Condition is to


We need failure
to Learn & Grow

“things that have never happened before happen all the time”

-Scott Sagan “The Limits of Safety”

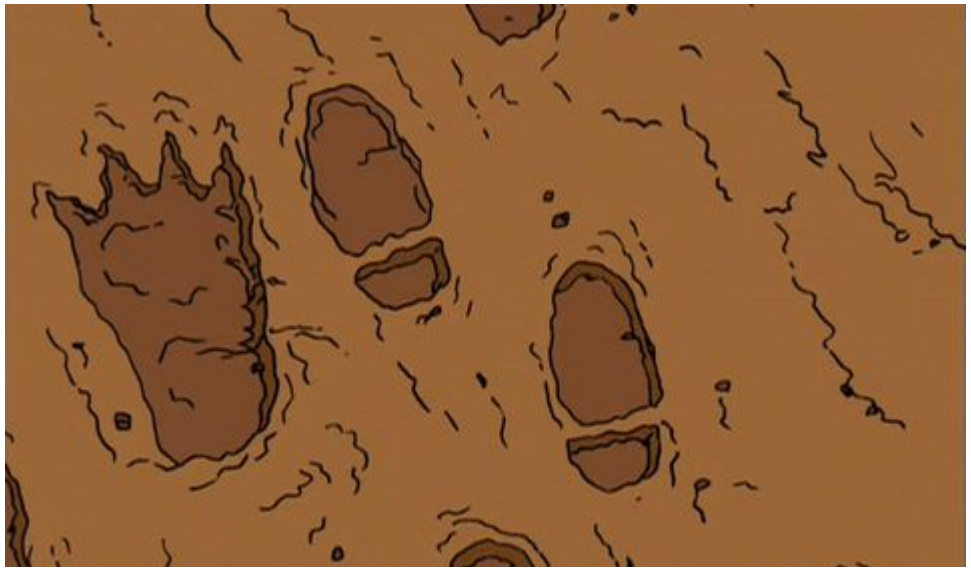
How do we typically discover when our security measures fail?

Security Incidents

Typically we dont find out our security is failing until there is an security incident.

Vanishing Traces

Logs, Stack Traces, Alerts



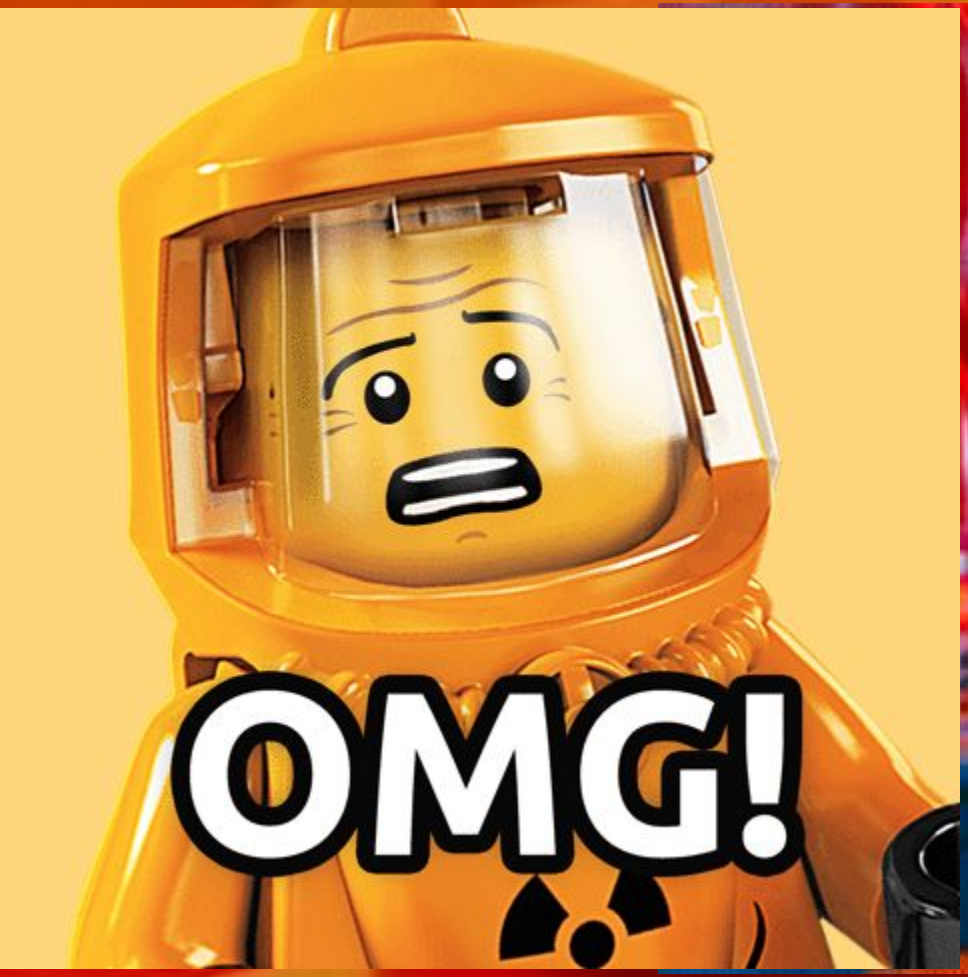
All we typically ever see is the Footsteps in the Sand
-Allspaw

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.

People **Operate Differently** when they **expect things to fail**


OMG!


What are your robot serial numbers?


Awesome!

Chaos Engineering

@aaronrinehart @verica_io #chaosengineering

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"

Who is doing Chaos?

Microsoft

Disney

mastercard

Google

salesforce

VISA

Capital One

in

hulu

amazon

vmware

indeed
one search. all jobs.

SIEMENS

twilio

BANK OF AMERICA

Dropbox

slack

Walmart

Pivotal

Fidelity
INVESTMENTS

UBER

GitHub

Bloomberg

audible
an amazon company

Kroger

SendGrid

ENDGAME.

cognitect

jet

Adobe

tinder

PRINCIPLES OF CHAOS ENGINEERING

Last Update: 2017 April

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

O'REILLY®

Compliments of NETFLIX

Chaos Engineering

Building Confidence in System Behavior through Experiments

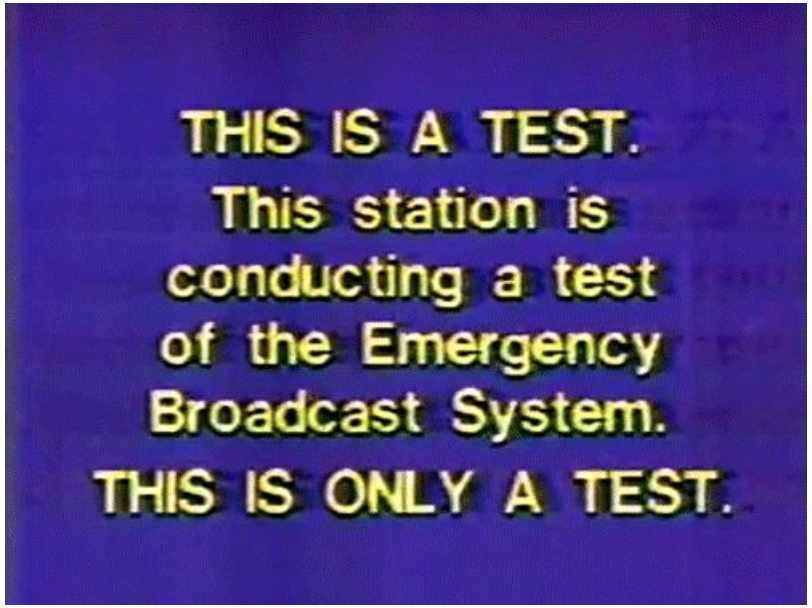
O'REILLY®

Chaos Engineering

System Resiliency in Practice

Use Chaos to Establish Order

Testing vs. Experimentation



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

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

Security Chaos Engineering

@aaronrinehart @verica_io #chaosengineering

Continuous Security Verification

Proactively
Manage & Measure

Reduce Uncertainty by Building Confidence in how the system actually functions

Security Chaos Engineering Use Cases

@aaronrinehart @verica_io #chaosengineering

Use Cases

- Incident Response
- Solutions Architecture
- Security Control Validation
- Security Observability
- Continuous Verification
- Compliance Monitoring

Incident Response

Security Incidents are Subjective in Nature

We really don't know very much

Where?

Why?

Who?

How?

What?

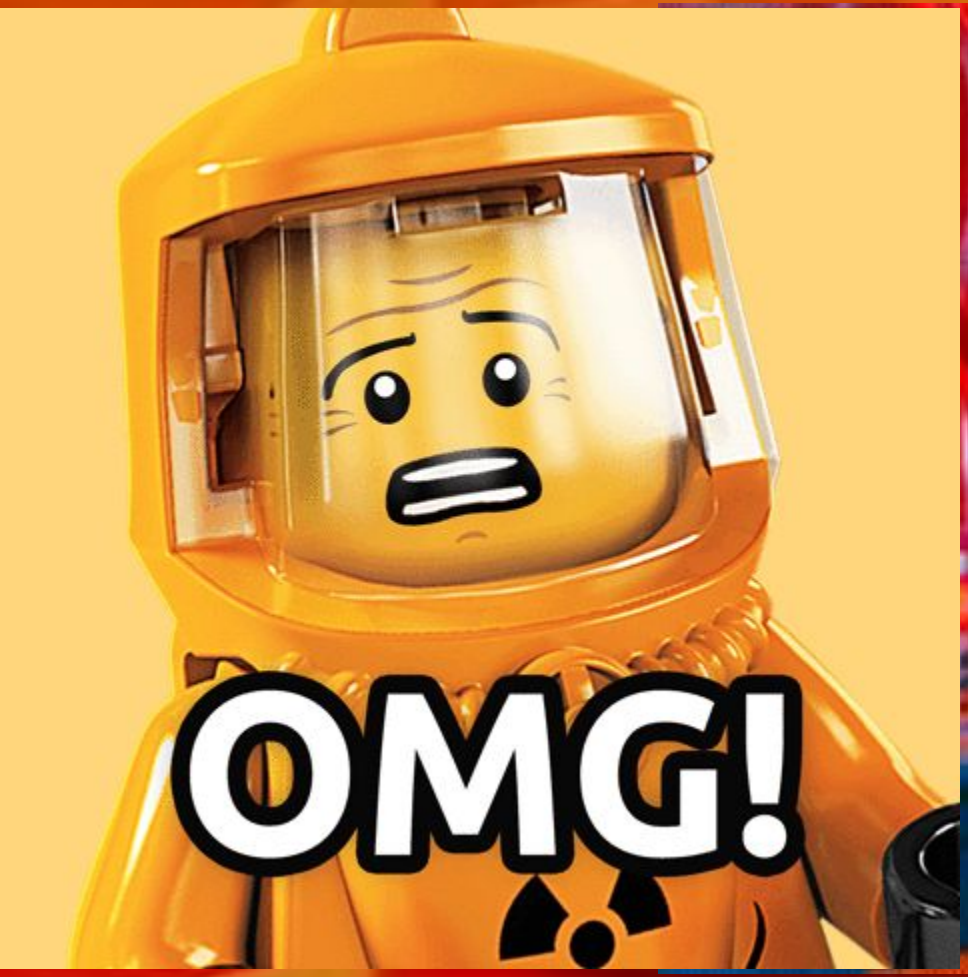
“Response” is the problem with Incident Response

Lets face it, when outages happen.....

Teams spend too much time reacting to outages instead of building more resilient systems.

Lets **Flip the Model**

Post Mortem = Preparation


OMG!


What are your robot serial numbers?

ChaoSlingr

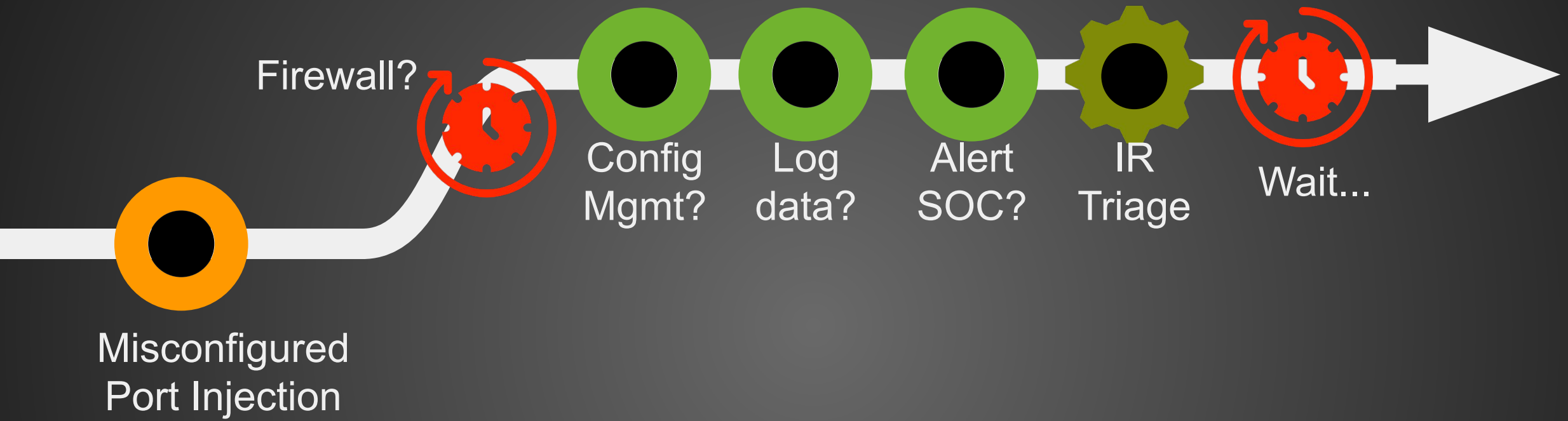
An Open Source Tool

ChaoSlingr Product Features

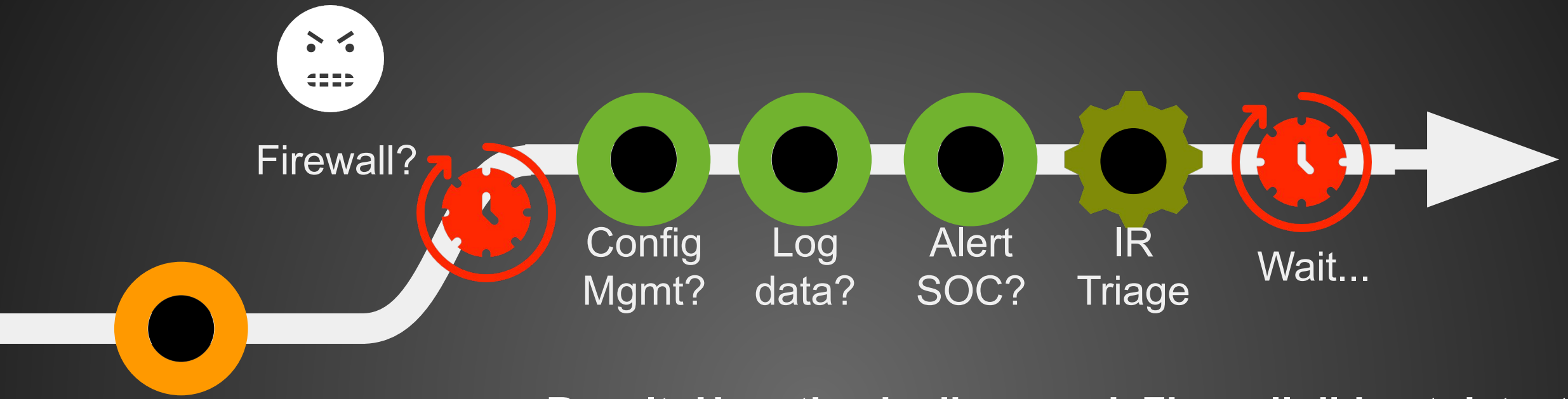
- ChatOps Integration
- Configuration-as-Code
- Example Code & Open Framework

- Serverless App in AWS
- 100% Native AWS
- Configurable Operational Mode & Frequency
- Opt-In | Opt-Out Model



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

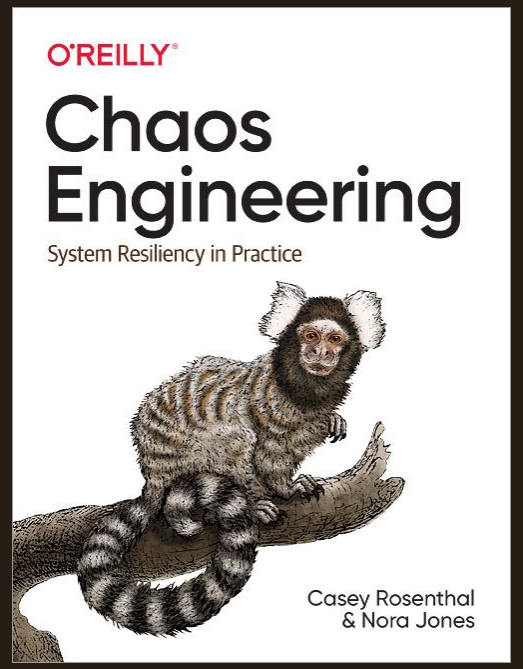


Result: Hypothesis disproved. Firewall did not detect or block the change on all instances. Standard Port AAA security policy out of sync on the Portal Team instances. Port change did not trigger an alert and log data indicated successful change audit. However we unexpectedly learned the configuration mgmt tool caught change and alerted the SoC.

Stop looking for better answers and start asking better questions.

- John Allspaw

Free copy mailed to you
complements of Verica



cutt.ly/verica-book

THANK YOU!

Meet me in the Network Chat Lounge for questions

SKILUP DAYS

Agenda

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

Headshot

Name

Title

Twitter Handle

Brief Bio