
ADDO
ALL DAY DEVOPS
AARON RINEHART
Hard Rock CAFE
AT&T

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs
Enterprise DevOps

cloudbees

Carnegie Mellon University
Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone
A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire

ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Security Pre-Cognition

DevSecOps & Chaos Engineering

ADDO
ALL DAY DEVOPS

Security Precognition

DevSecOps & Chaos Engineering

@aaronrinehart @verica_io #chaosengineering

ADDO
ALL DAY DEVOPS

In this Session we will cover

Areas Covered

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

ADDO
ALL DAY DEVOPS

Aaron Rinehart, CTO, Founder

- Former Chief Security Architect @UnitedHealth responsible for security engineering strategy
- DevOps and Open Source Transformation at UnitedHealth Group
- Former (DOD, NASA, DHS, CollegeBoard)
- Frequent speaker and author on Chaos Engineering & Security
- Pioneer behind Security Chaos Engineering
- Led ChaoSlingr team at UnitedHealth

@aaronrinehart @verica_io #chaosengineering

VERICA

ADDO
ALL DAY DEVOPS

Incidents, Outages, & Breaches are Costly

Be right back.

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

ADDO
ALL DAY DEVOPS

An Obvious Problem

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

36

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 |

GOOGLE

Apple iCloud services recover from nationwide outage

By Humza Aa on July 019 8 AM

System Status

App Store
Apple Books
Apple Business Manager
Apple ID

3 min re

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

Image may contain: 1 person, outdoor
Image may contain: 1 person, sky, outdoor
Image may contain: 2 people, people

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

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?

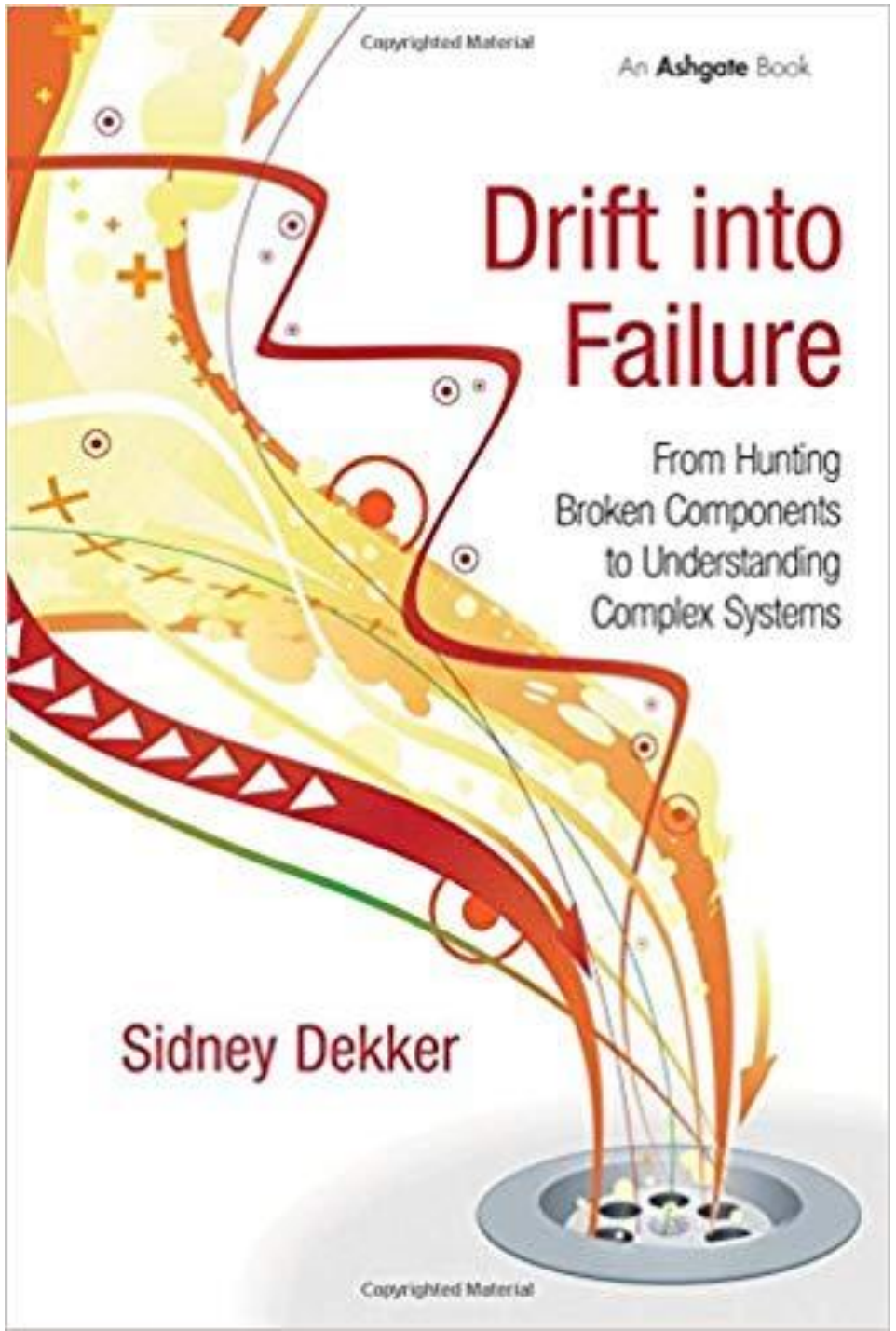
ADDO
ALL DAY DEVOPS

Combating Complexity in Software

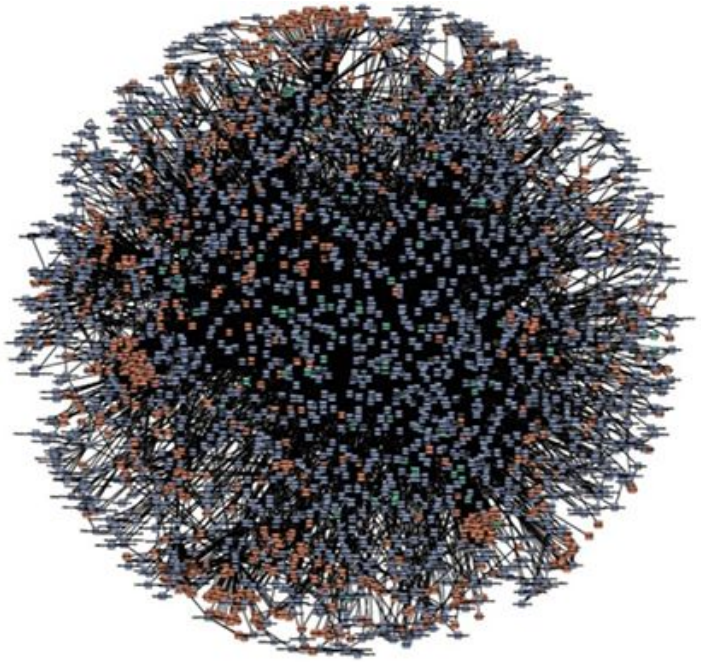
@aaronrinehart @verica_io #chaosengineering

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

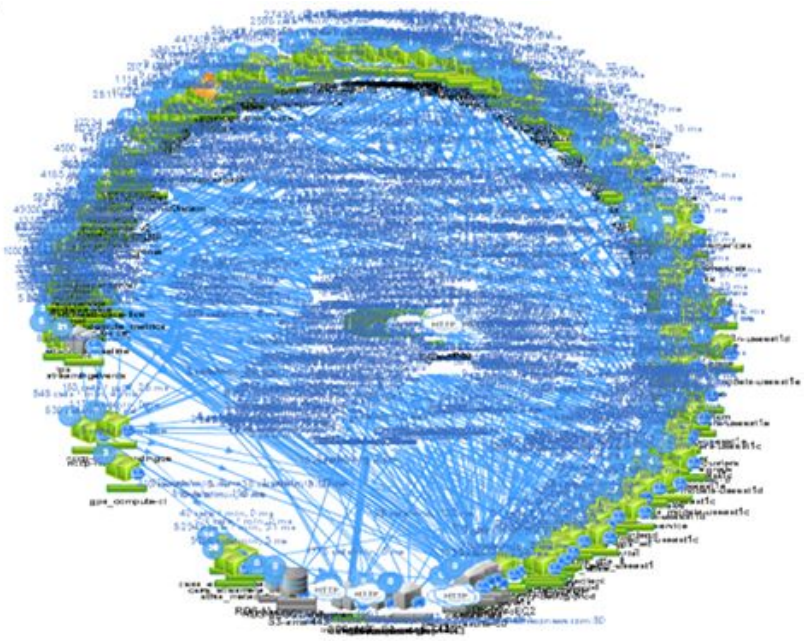
-Sydney Dekker



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

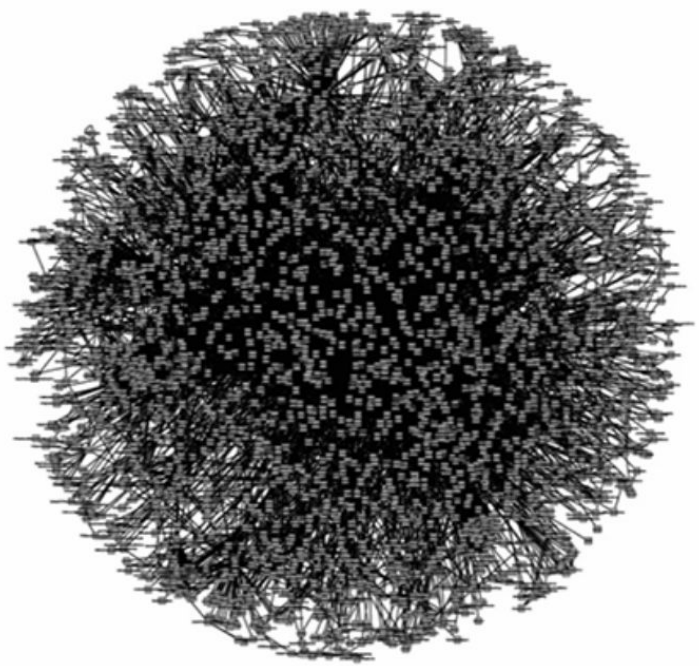


amazon.com

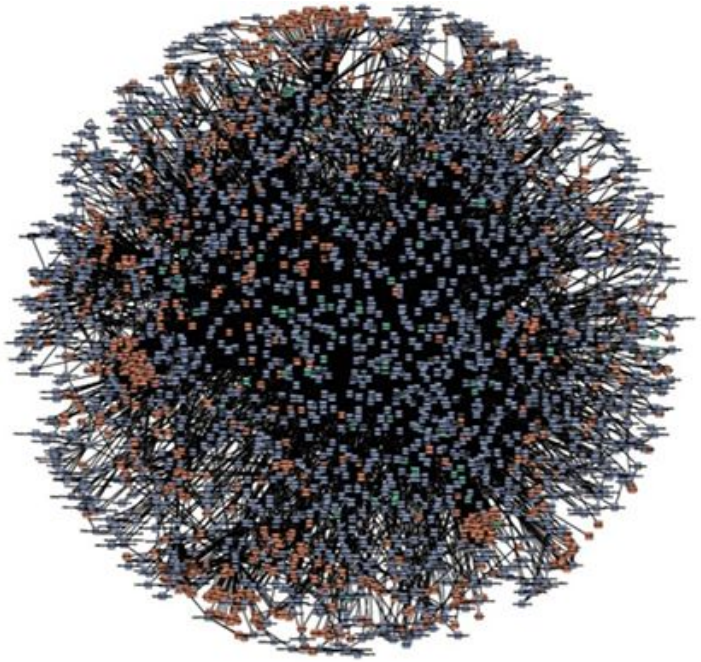


NETFLIX

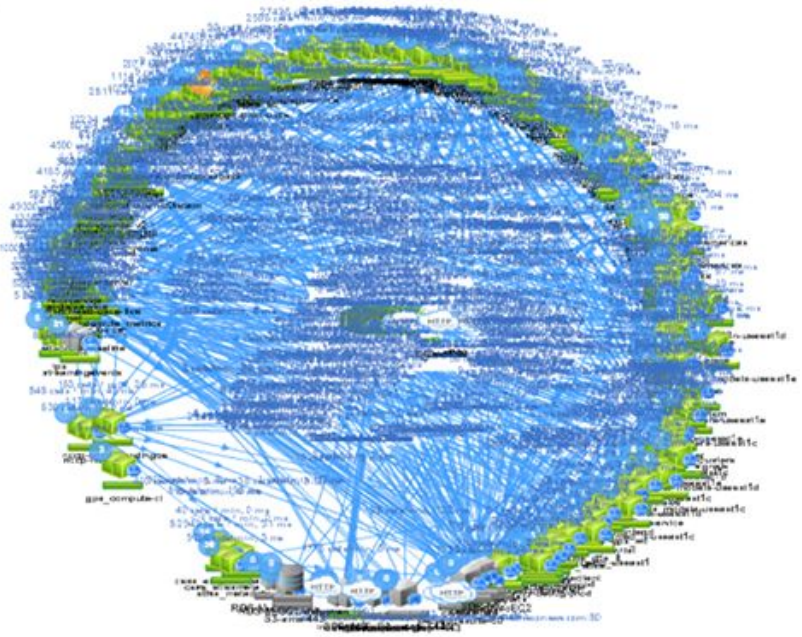
Our systems have evolved beyond human ability to mentally model their behavior.



everyone else



amazon.com



NETFLIX

Complex?

Continuous Delivery

Distributed Systems

Microservice Architectures

Blue/Green Deployments

Automation Pipelines

Containers

Continuous Integration

DevOps

CI/CD

Infracode

Immutable Infrastructure

Cloud Computing

Service Mesh

API

Auto Canaries

Circuit Breaker Patterns

Security?

Mostly Monolithic

Expert Systems

Stateful in nature

Prevention focused

Poorly Aligned

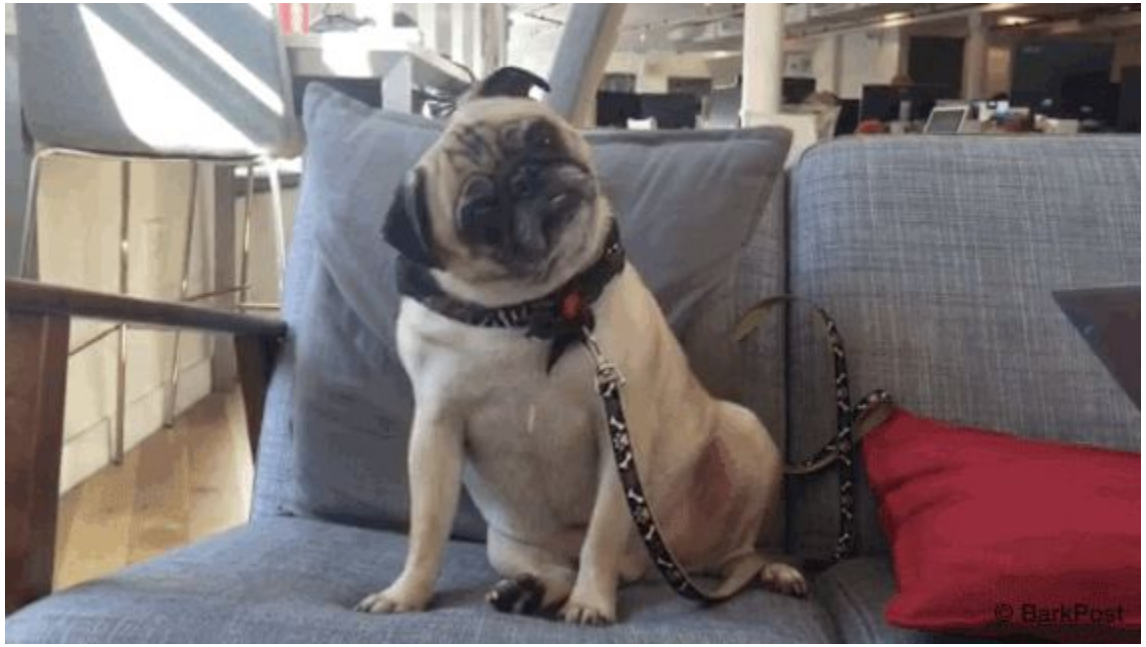
Adversary Focused

Defense in Depth

Requires Domain Knowledge

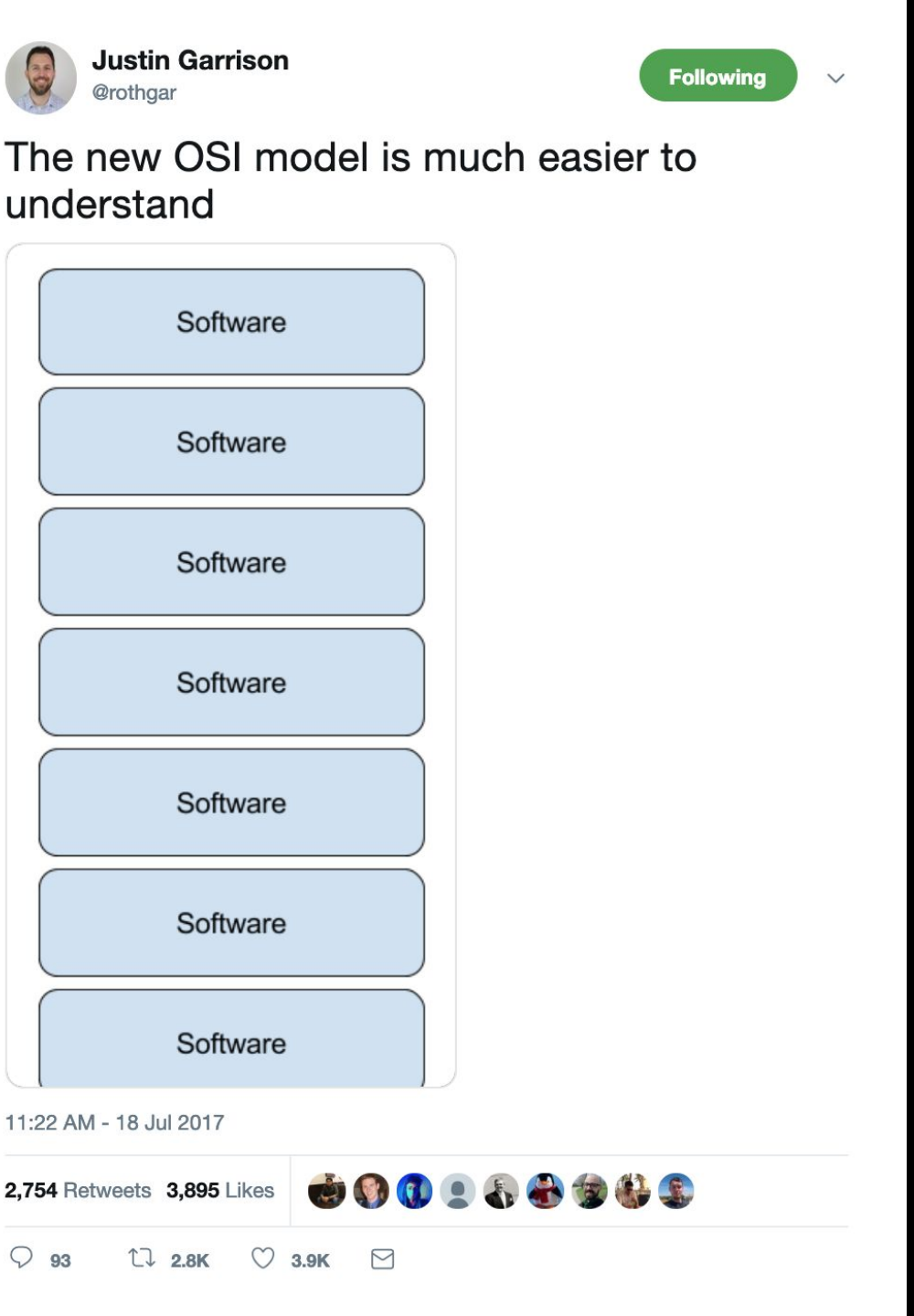
DevSecOps not widely adopted

Simplify?



ADDO
ALL DAY DEVOPS

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

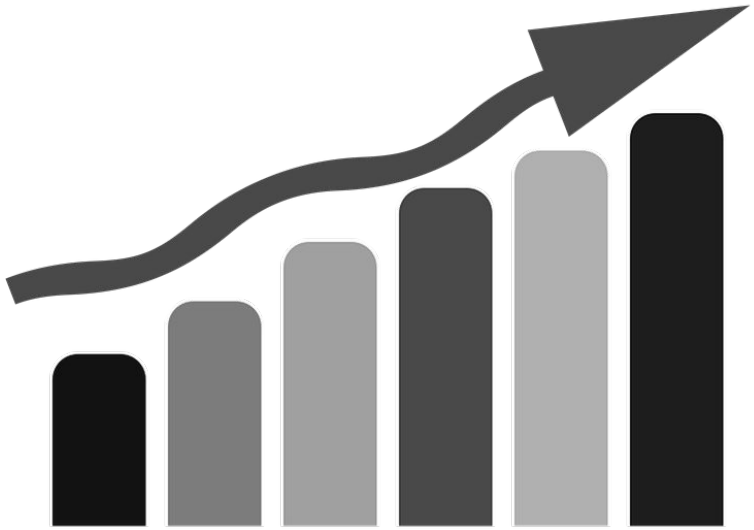
Intel X86, etc (first layer of human-readable code)

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"

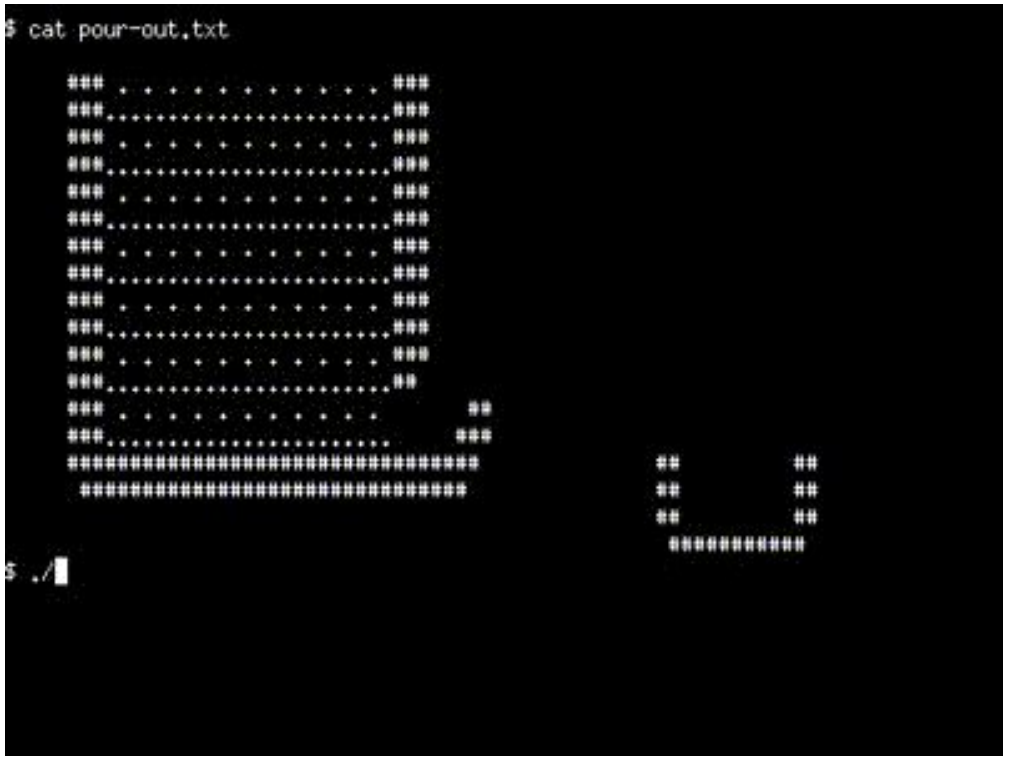
- Dr. David Woods

What does this have to do with my systems?

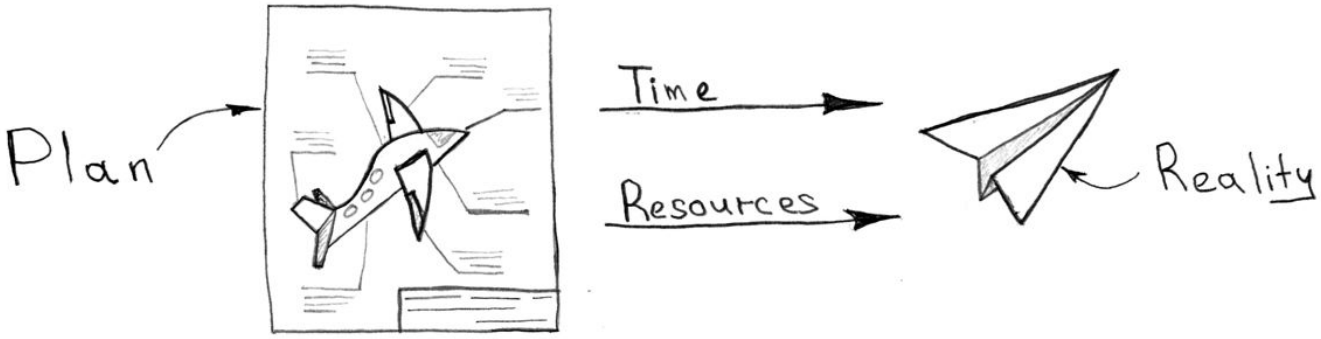
Question - How well do you really understand how your system works?

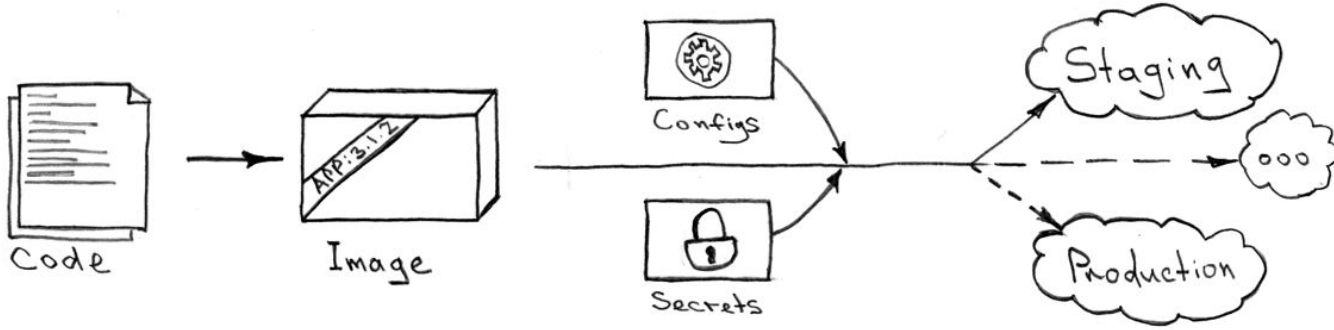
In Reality.....

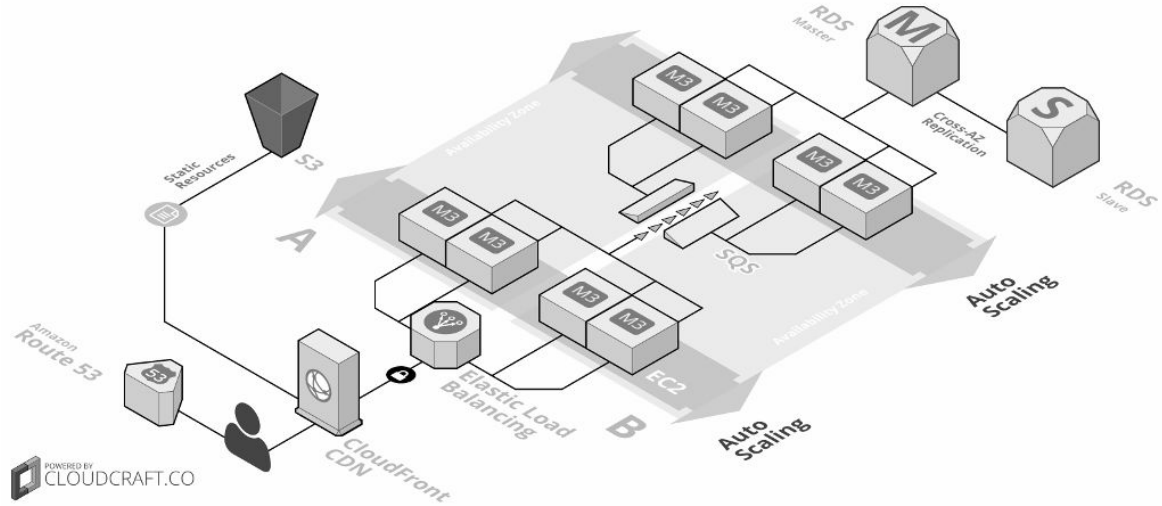
Systems Engineering is Messy



In the beginning...we think it looks like







ADDO
ALL DAY DEVOPS

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

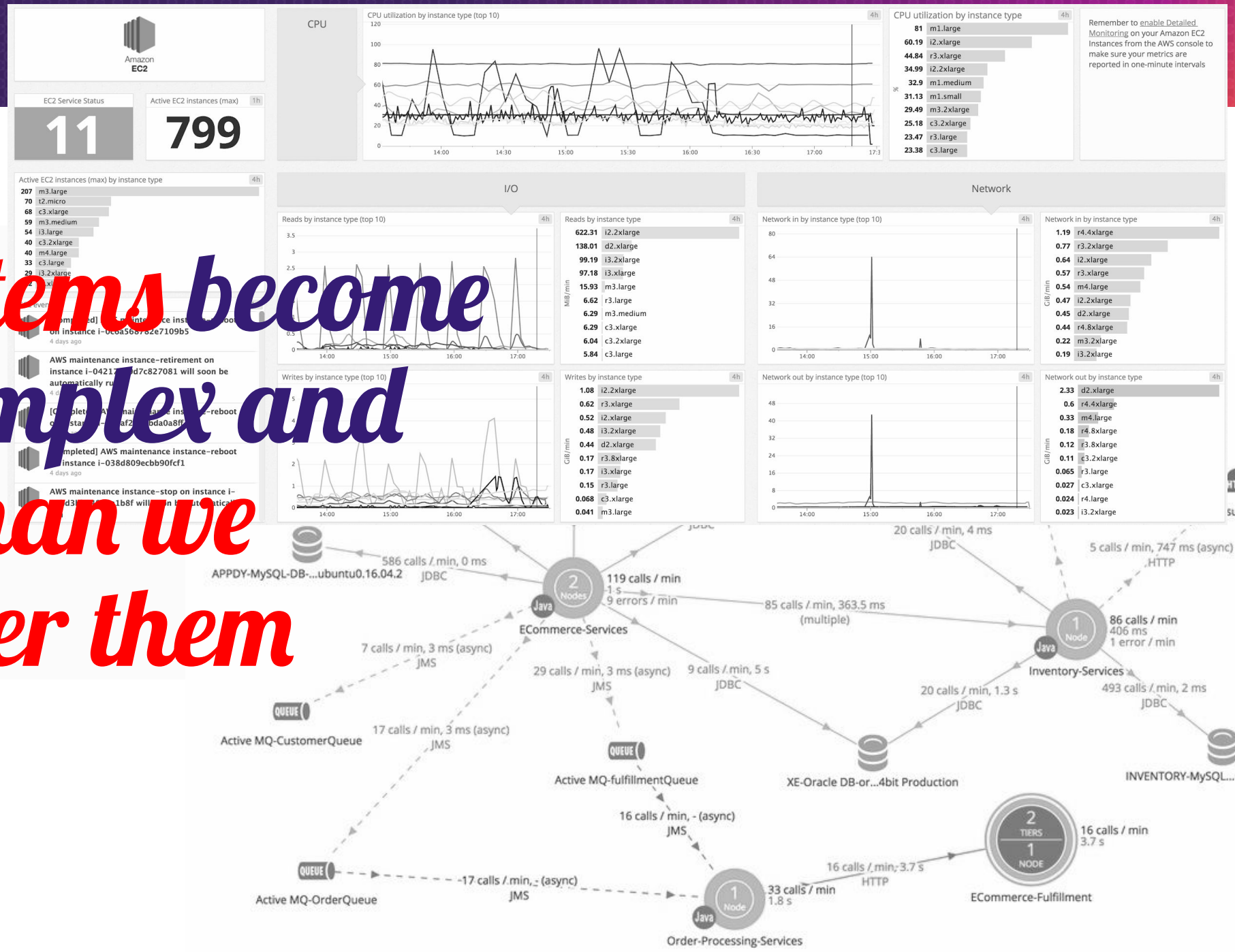
ADDO
ALL DAY DEVOPS

Years?....

Orphaned Documentation
Hard Coded Passwords
Network is Unreliable
New Security Tool
Autoscaling Keeps Breaking
Portal Retry Storm Outage
Identity Conflicts
Refactor Pricing
Regulatory Audit
Rolling Sevl 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
Identity Conflicts
Delayed Features
Migration to New CSP
Refactor Pricing
Misconfigured FW Rule Outage
Firewall Outage -> Disabled
Lead Software Engineering finds a new job at Google
Cloud Provider API Outage
Large Customer Outage
Upgrade to Java SE 12
Exposed Secrets on GithuCode Freeze
DNS Resolution Errors
Merger with competitor
Expired Certificate
300 Microservices Δ-> 850 Microservices
Regulatory Audit
Scalability Issues
WAF Outage -> Disabled
Rolling Sevl Outage on Portal
Delayed Features
Large Customer

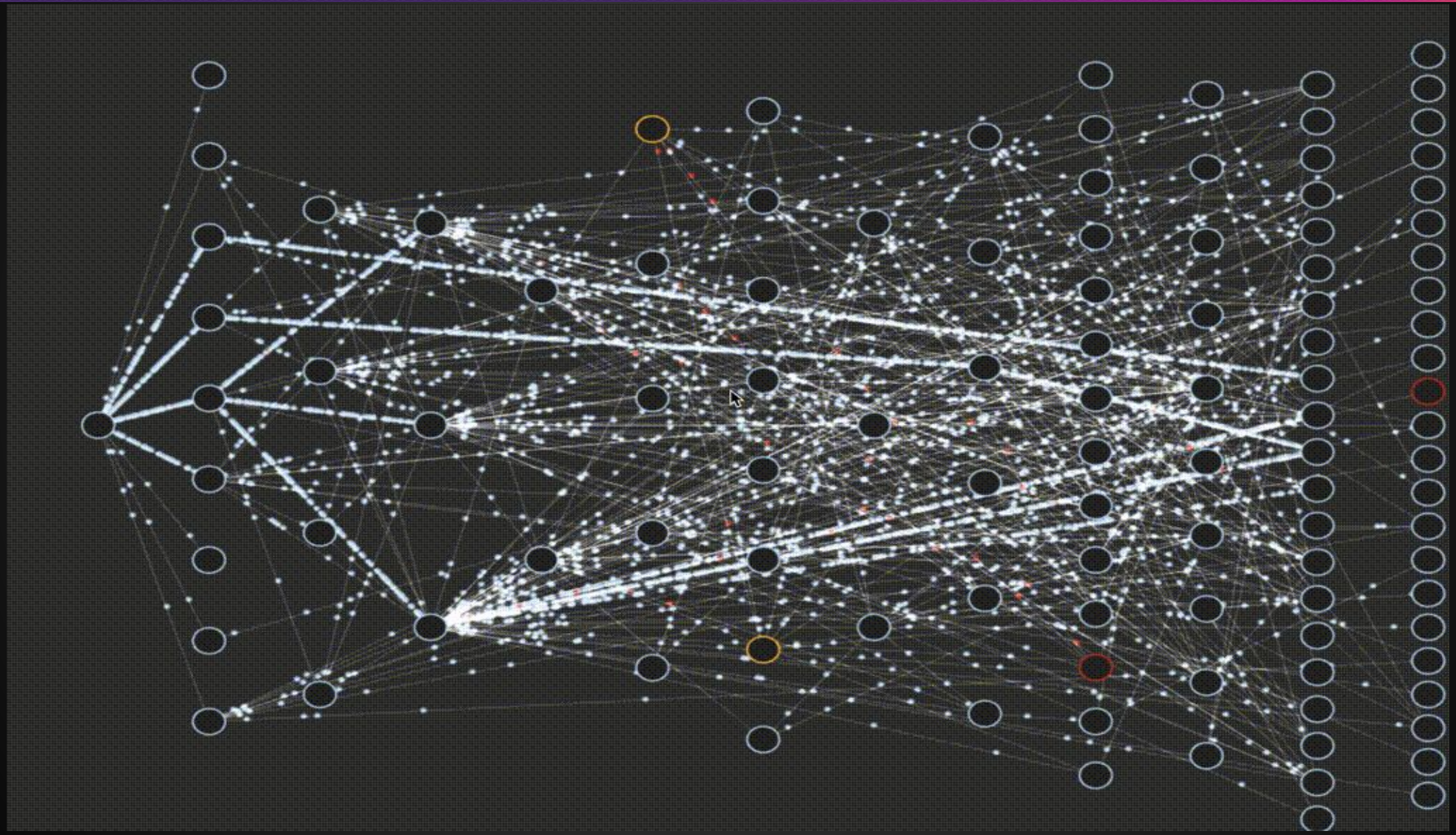
ADDO
ALL DAY DEVOPS

Our systems become more complex and messy than we remember them



ADDO
ALL DAY DEVOPS

Difficult to Mentally Model



Avoid Running in the Dark

@aaronrinehart @verica_io #chaosengineering

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

Putting off critical tasks until everyone forgets about them

If there's time

O RLY?

@ThePracticalDev

Failure Happens Alot

ADDO
ALL DAY DEVOPS

The Normal Condition is to

FAIL


We need failure
to Learn & Grow

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

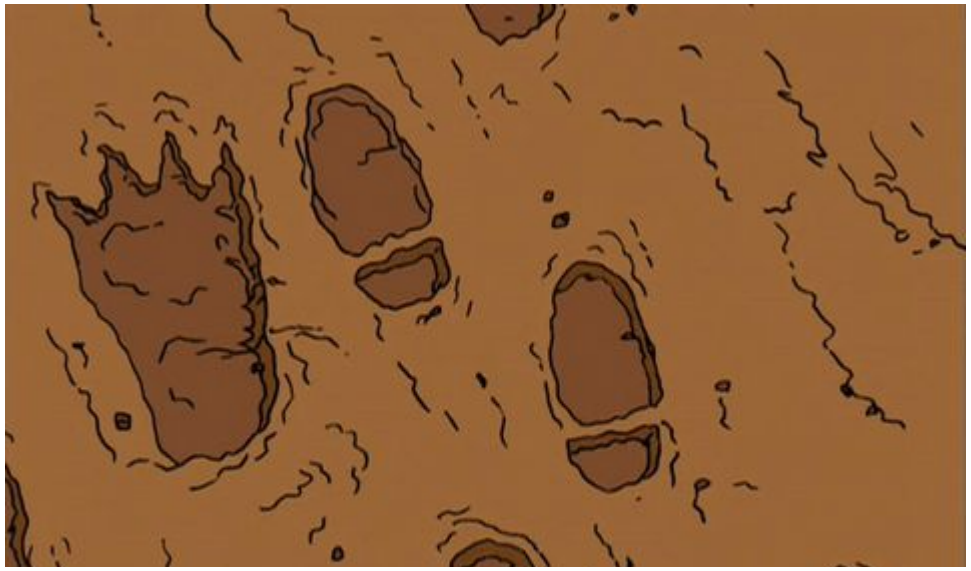
-Scott Sagan “The Limits of Safety”

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

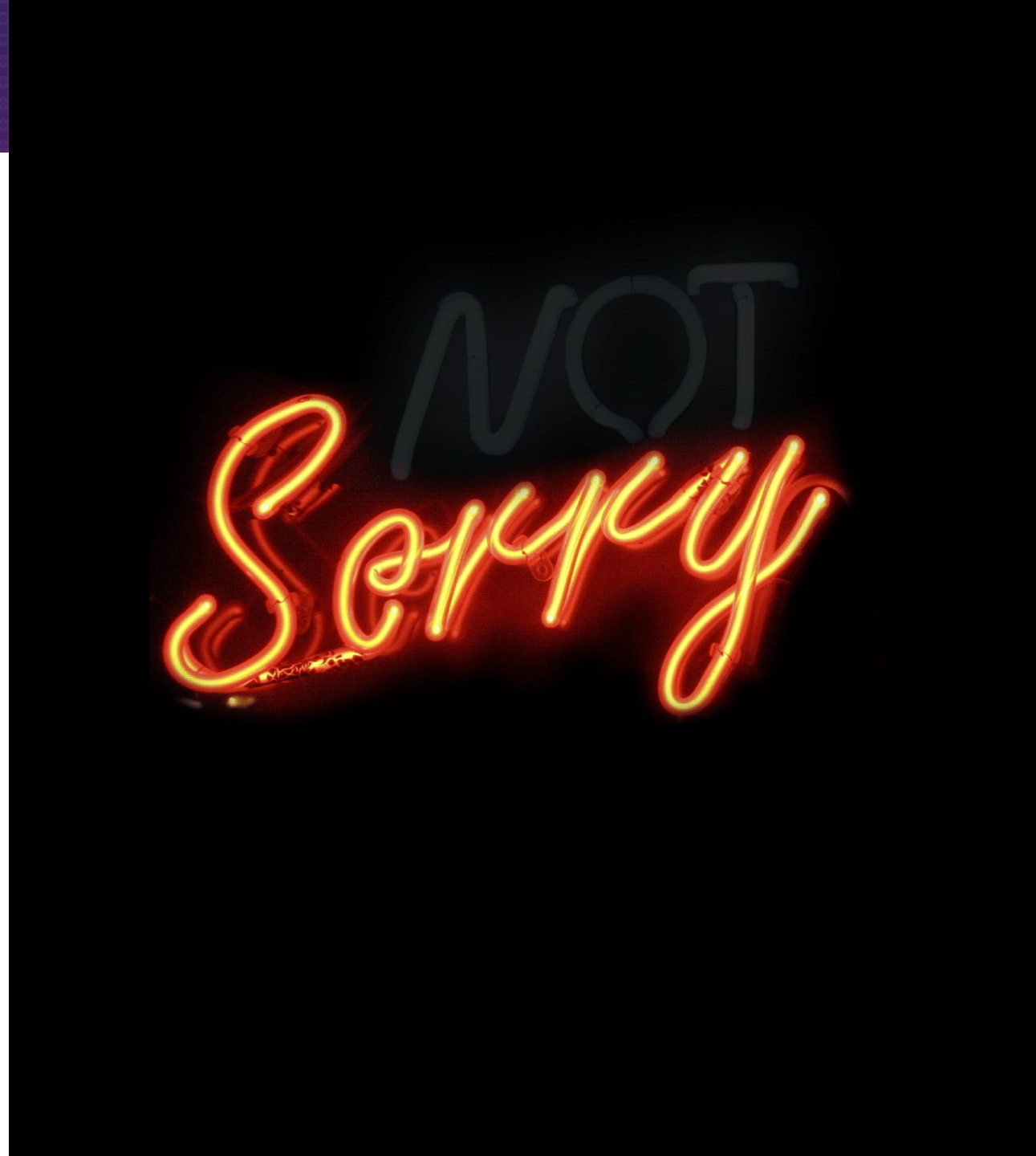


Logs, Stack Traces, Alerts

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

ADDO
ALL DAY DEVOPS

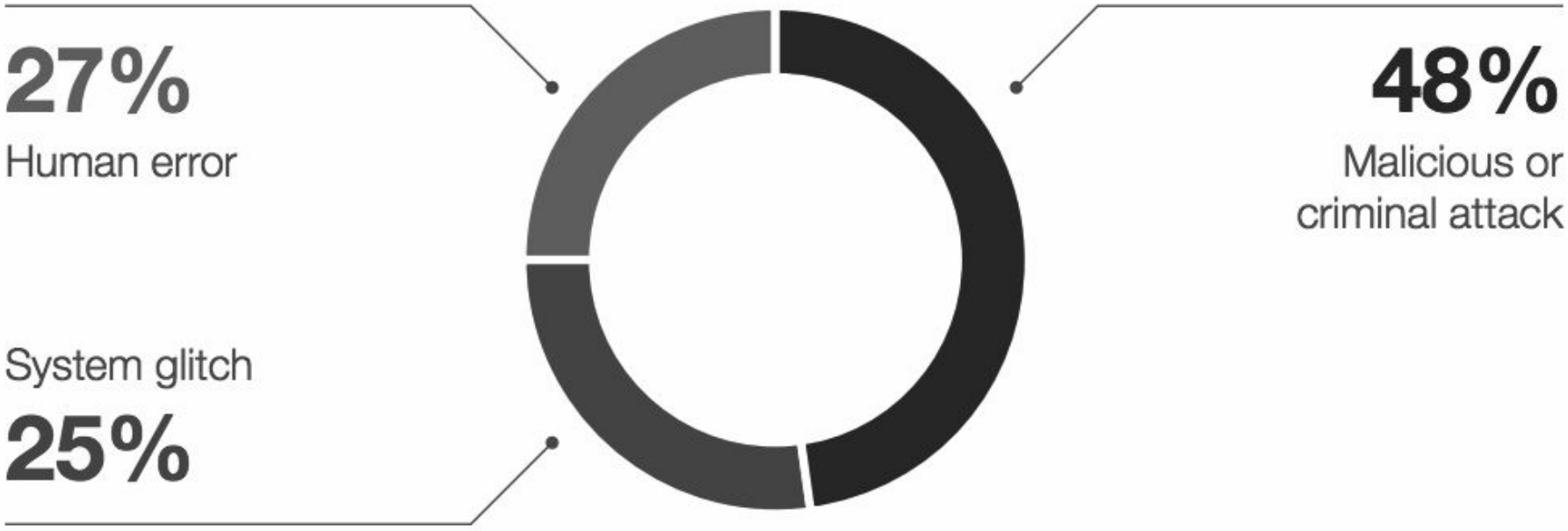
Security incidents are **not effective measures of detection** because at that point it's already too late



What typically causes our security to fail?

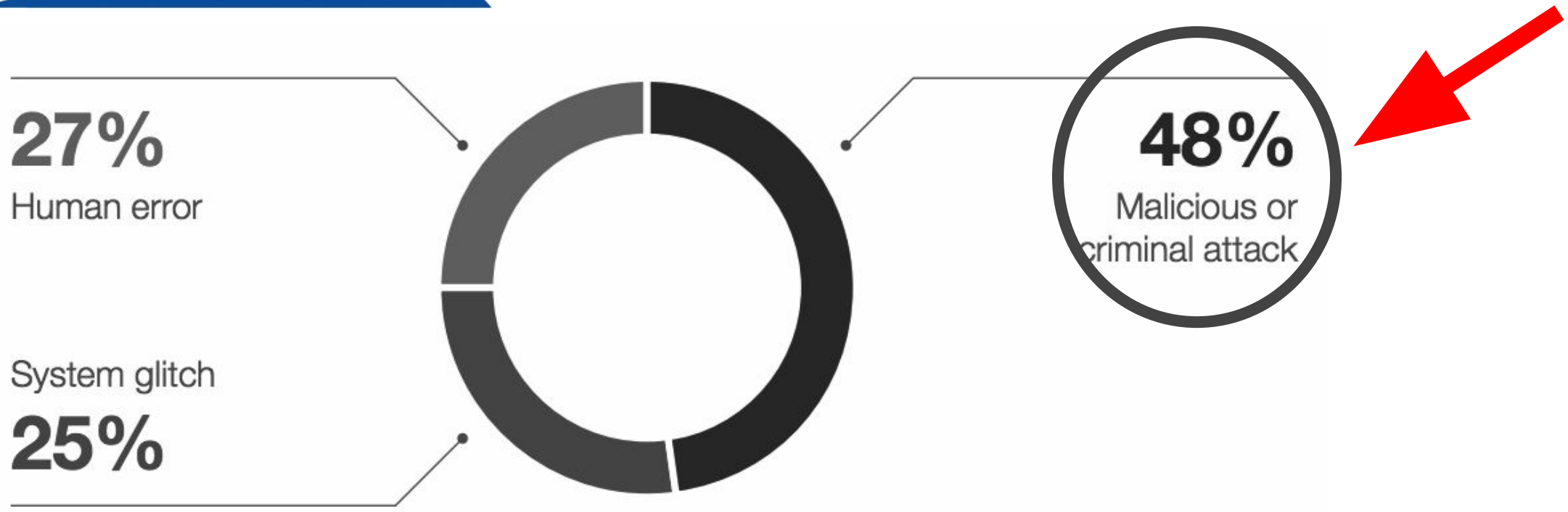
2018 Causes of Data Breaches

Ponemon INSTITUTE

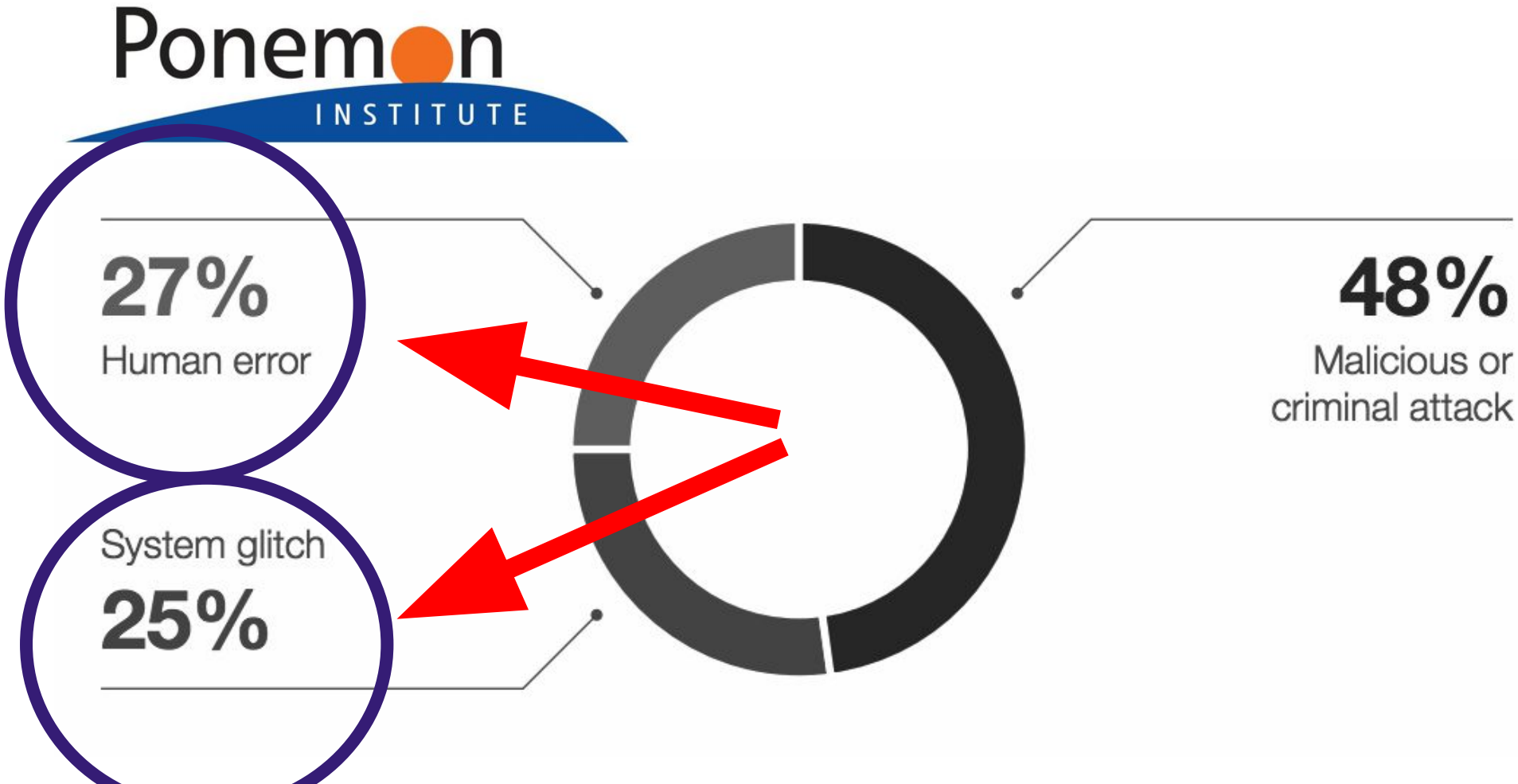


2018 Causes of Data Breaches

Ponemon INSTITUTE

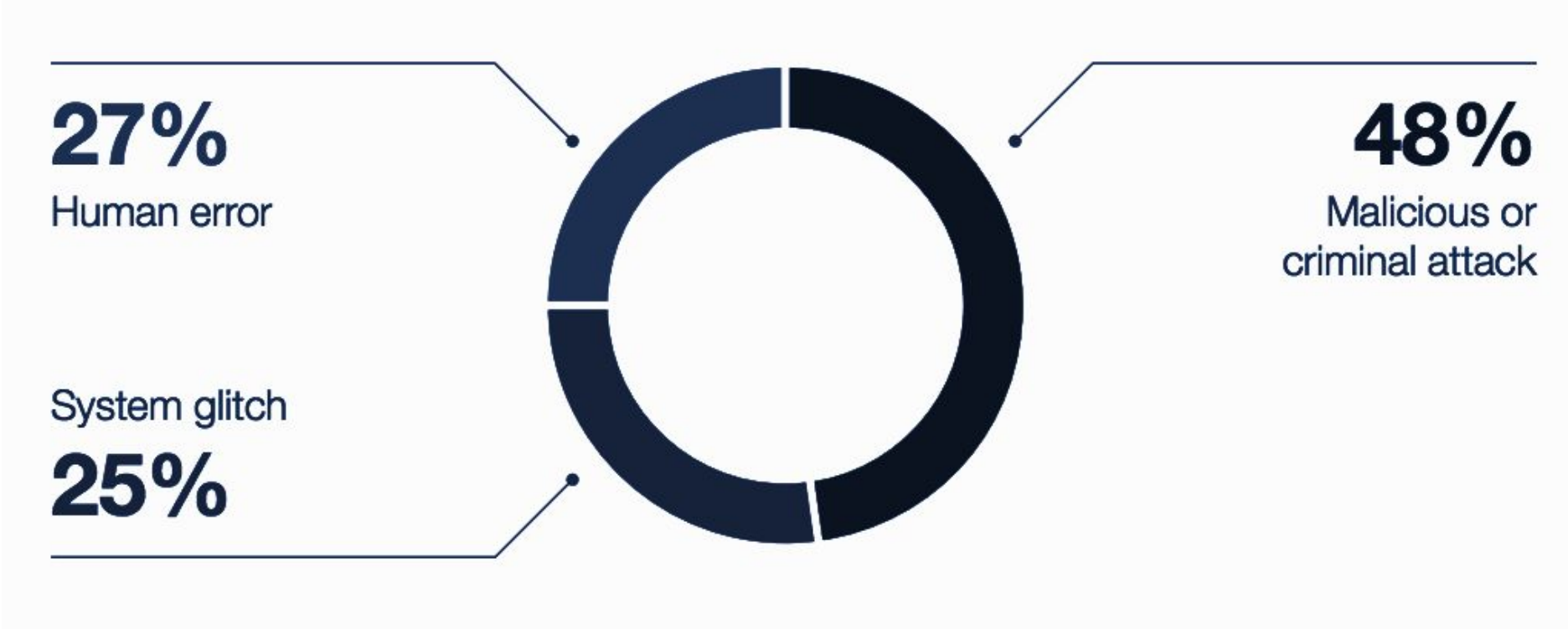


2018 Causes of Data Breaches



2018 Causes of Data Breaches

Ponemon INSTITUTE



'Human-Error', Root Cause, & Blame Culture

---

[10] Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation. Malicious attacks can be caused by hackers or criminal insiders (employees, contractors or other third parties).

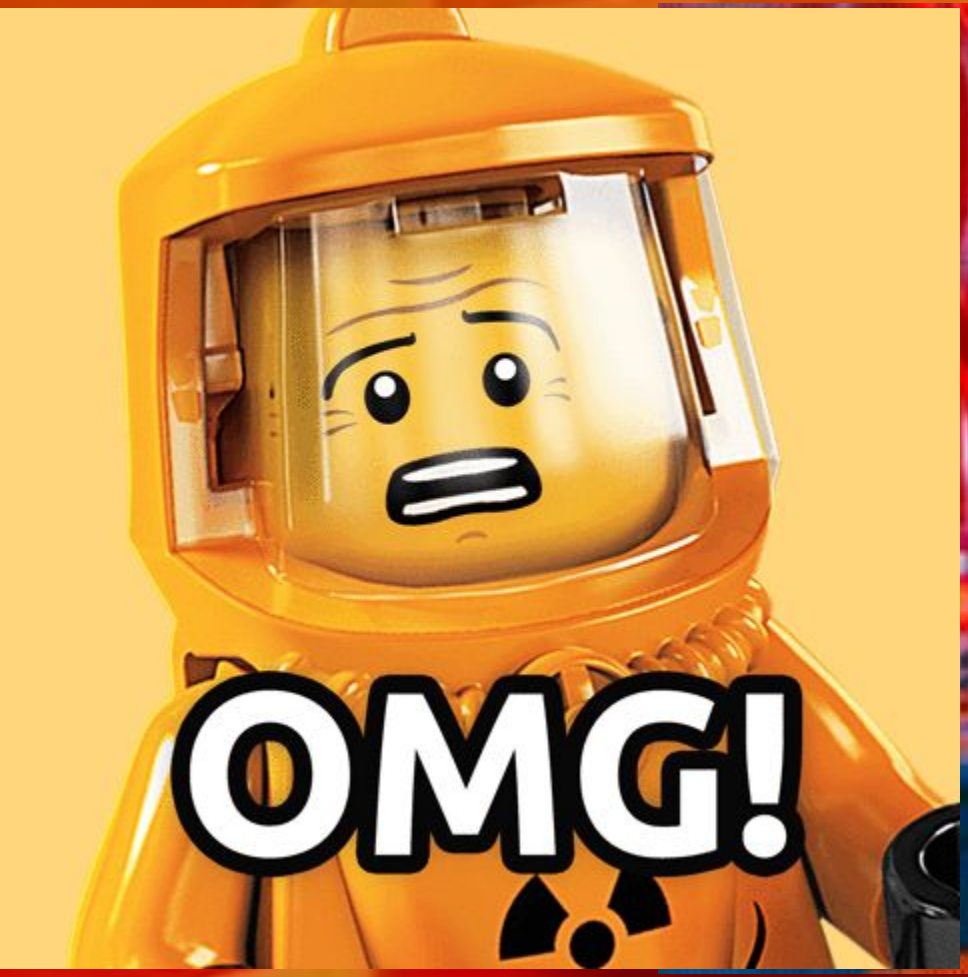
Ponemon INSTITUTE

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

Considerations in building a Learning Culture

Cognitive Load, Bias, and Blame

People Operate Differently when they expect things to fail


OMG!


What are your robot serial numbers?


Awesome!

ADDO
ALL DAY DEVOPS

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

Capital One

in

mastercard

Google

salesforce

VISA

hulu

amazon

vmware

indeed
one search. all jobs.

SIEMENS

twilio

BANK OF AMERICA

Dropbox

slack

Walmart

Pivotal

Bloomberg

Fidelity
INVESTMENTS

UBER

GitHub

audible
an amazon company

Kroger

SendGrid

ENDGAME.

cognitect

jet

Adobe

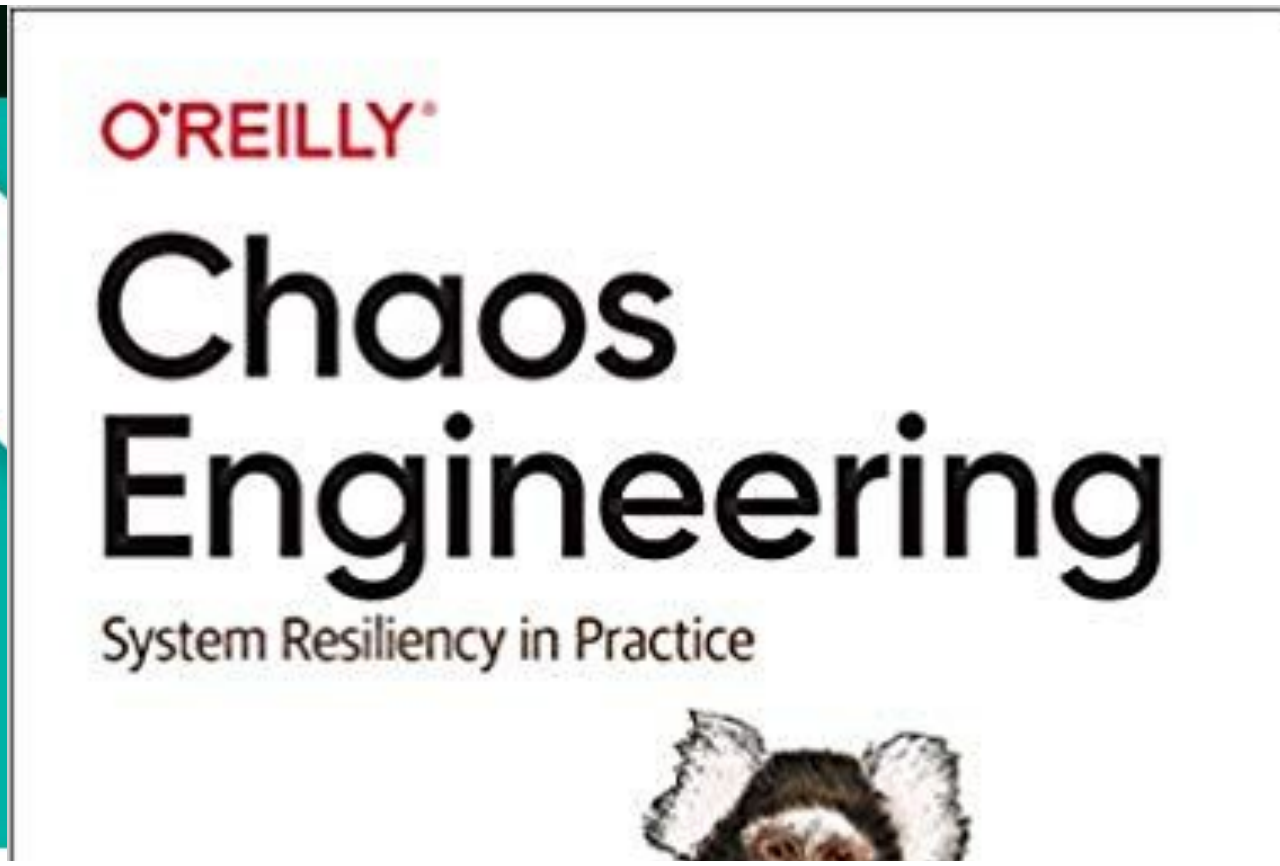
tinder

PRINCIPLES OF CHAOS ENGINEERING

Last Update: 2017 April

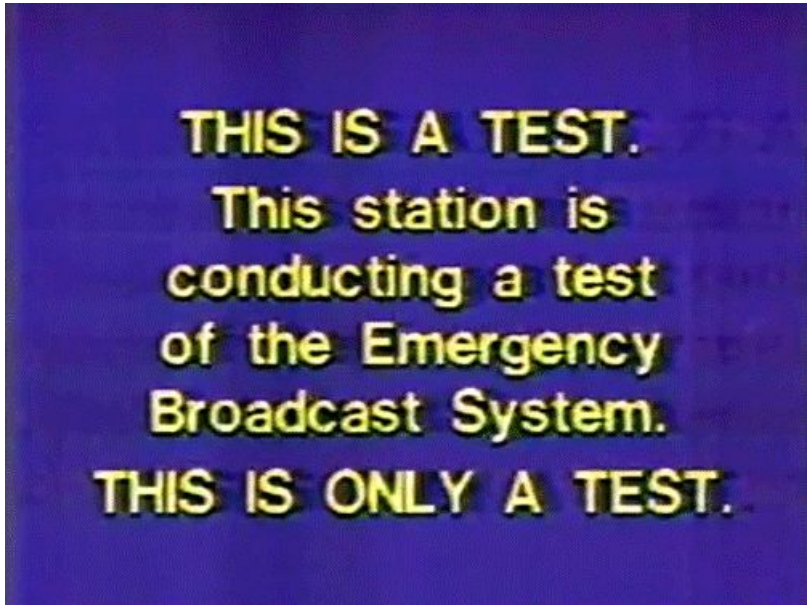
Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in the system's capability to withstand turbulent conditions in production.


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

ADDO
ALL DAY DEVOPS

Security Chaos Engineering

@aaronrinehart @verica_io #chaosengineering

Continuous Security Verification

Proactively Manage & Measure

Reduce Uncertainty by Building Confidence in how the system actually functions

ADDO
ALL DAY DEVOPS

Security Chaos Engineering Use Cases

@aaronrinehart @verica_io #chaosengineering

Use Cases

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

ADDO
ALL DAY DEVOPS

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

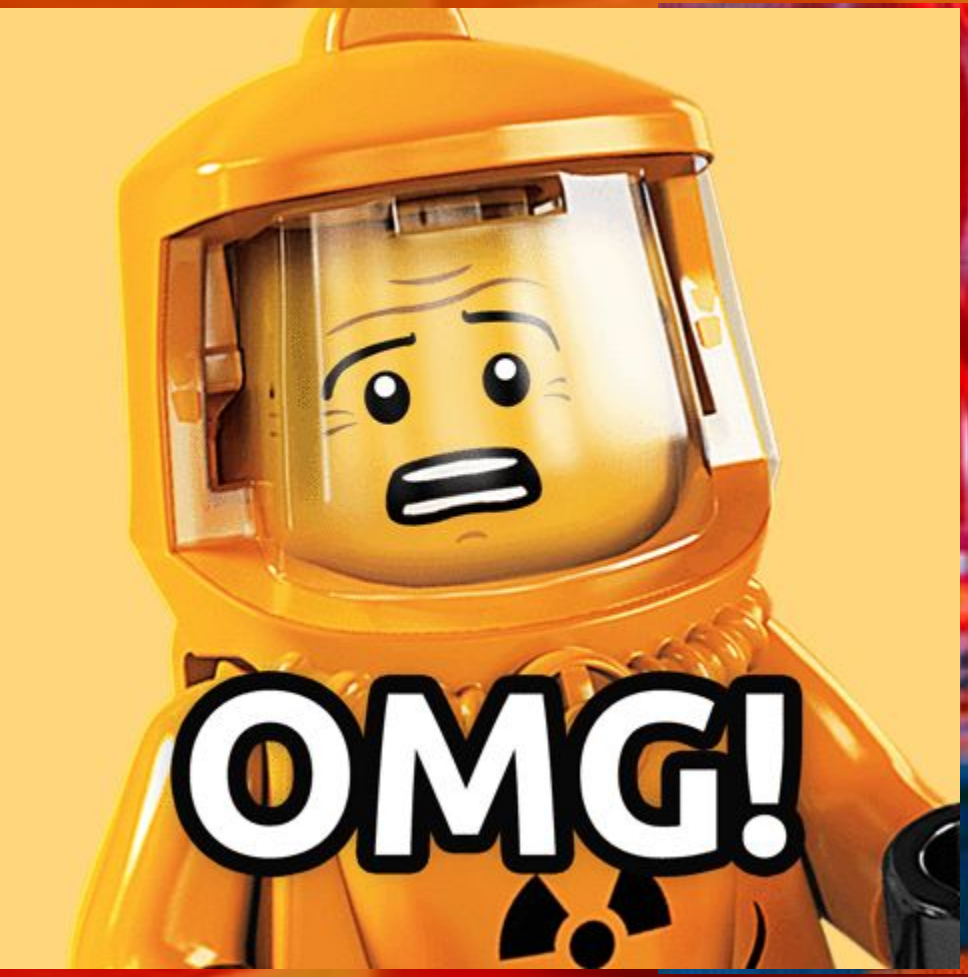
Lets face it, when outages happen.....

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

ADDO
ALL DAY DEVOPS

Lets **Flip the Model**

Post Mortem = Preparation


OMG!


What are your robot serial numbers?

ADDO
ALL DAY DEVOPS

Solution Architecture

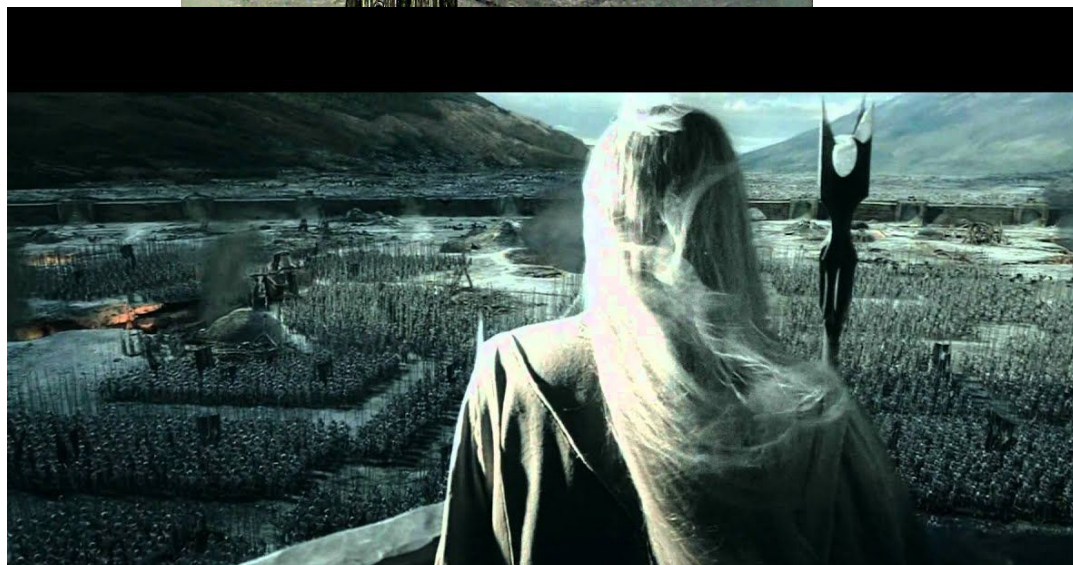
"More men (people) die from their remedies not their illnesses"

- Jean-Baptiste Poquelin

Ivory Tower Architecture

Solutions Architecture needs reinvention

Patterns never worked



ADDO
ALL DAY DEVOPS

Security Control Validation

Create Objective Feedback Loops about Security Effectiveness

ChaoSlingr

An Open Source Tool

ADDO
ALL DAY DEVOPS

ChaoSlingr Product Features

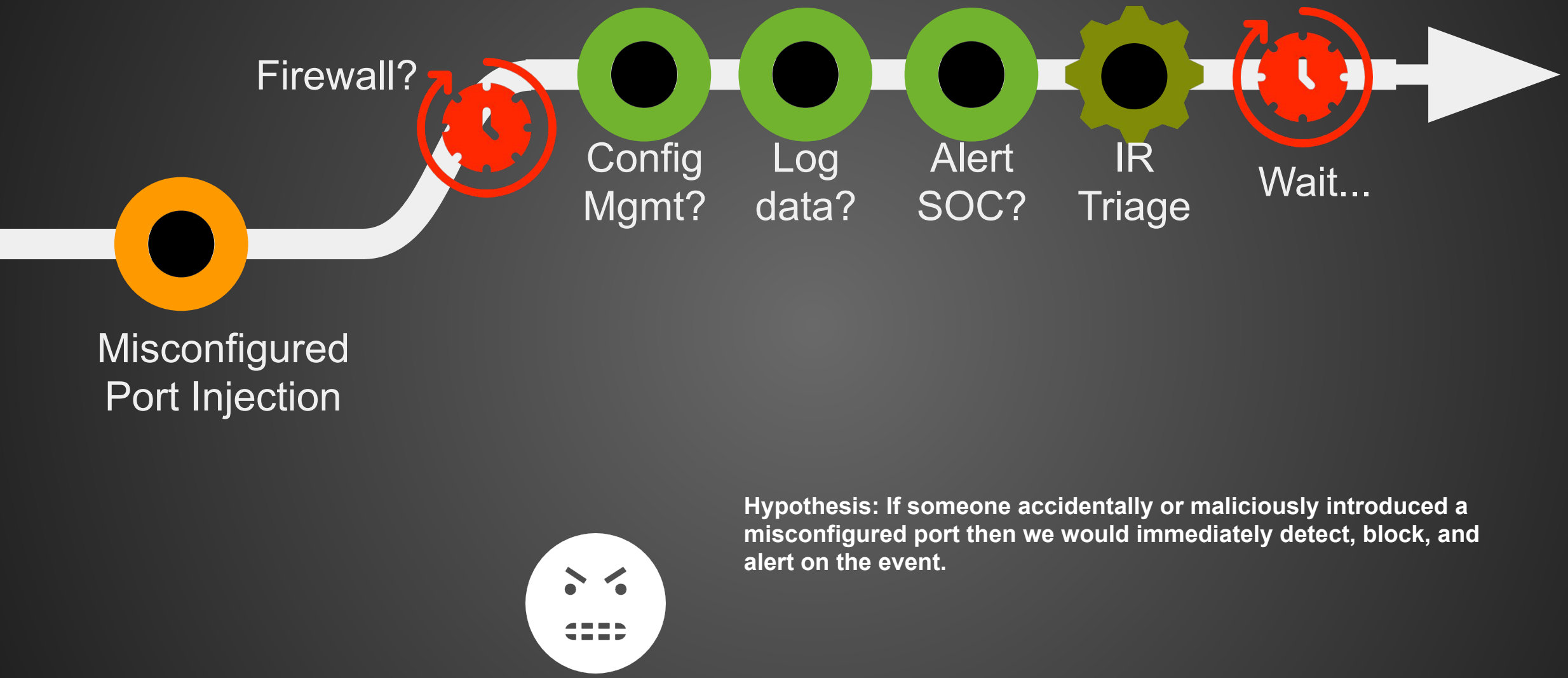
- ChatOps Integration
- Configuration-as-Code
- Example Code & Open Framework
- Serverless App in AWS
- 100% Native AWS
- Configurable Operational Mode & Frequency
- Opt-In | Opt-Out Model





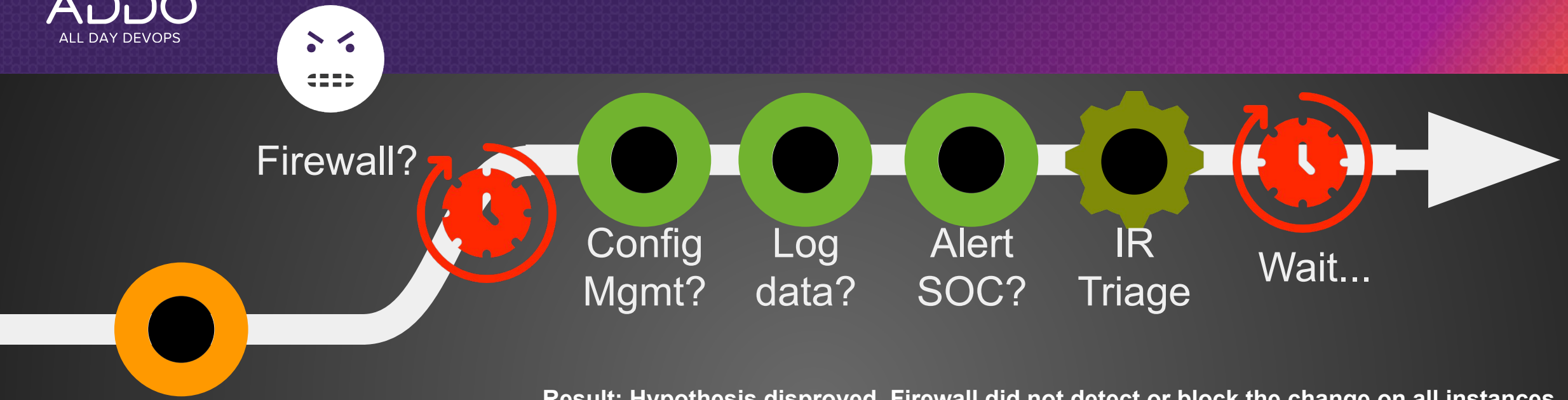


ADDO
ALL DAY DEVOPS



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

ADDO
ALL DAY DEVOPS



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

Q&A

@aaronrinehart

aaron@verica.io

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs
Enterprise DevOps

cloudbees

Carnegie Mellon University
Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone
A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire

ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Security Pre-Cognition

DevSecOps & Chaos Engineering