Please

Ask questions through the app

Rate Session

Thank you!

@GOTOber

gotober.com

goto; berlin

Security & Chaos Engineering

@aaronrinehart @verica_io #chaosengineering

In this Session we will cover

Areas Covered

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

Verica

Aaron Rinehart, CTO, Founder

- Former Chief Security Architect @UnitedHealth responsible for security engineering strategy
- Led the 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

Incidents, Outages, & Breaches are Costly

[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:

Image may contain:

Image may contain: 1 person, outdoor

Image may contain: 1 person, sky, outdoor

Image may contain: 2 people, people

Apple iCloud services recover from nationwide outage

Service outages are incre

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

App Store

Apple Books

Apple Business Manager

Apple ID

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

3 min read

Ye rday, Google Clou servers in the us-east1

1.

Cloudflare suffers another major outage

By Mike Moore 7 days ago Internet

Third major outage in a matter of weeks

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

Science & Technology

TweetDeck suffers outage, reason unknown

6 days ago

TweetDeck suffers outage, reason unknown

San Francisco, July 2 (IANS) Adding to the chain of app outages happening frequently, Twitter's dashboard TweetDeck went down for sometime in Europe and America before it was restored later.

Popular

I could have do december 25th Jersey

16 hours ago

Sept 21 morenz, injury wholesal

17 hours ago

Co ete u rt ey you could w n te 0 A zo uchers.

The Obvious Problem

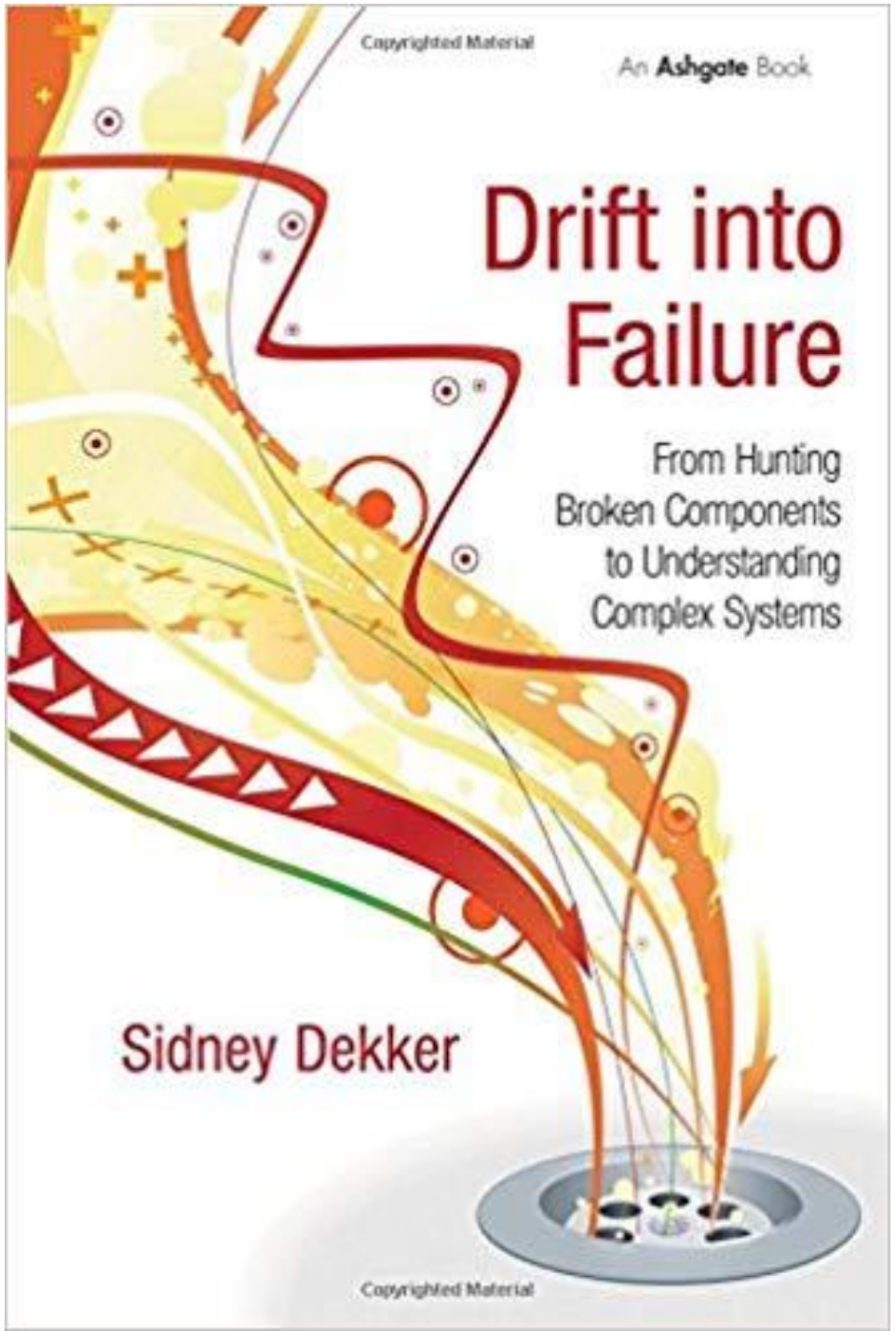
Why do they seem to be happening more often?

Combating Complexity in Software

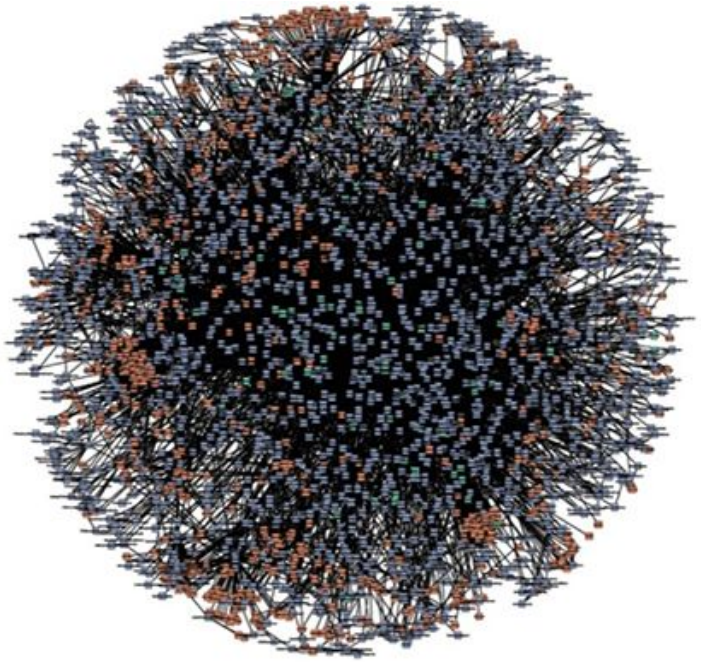
@aaronrinehart @verica_io #chaosengineering

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

-Sydney Dekker



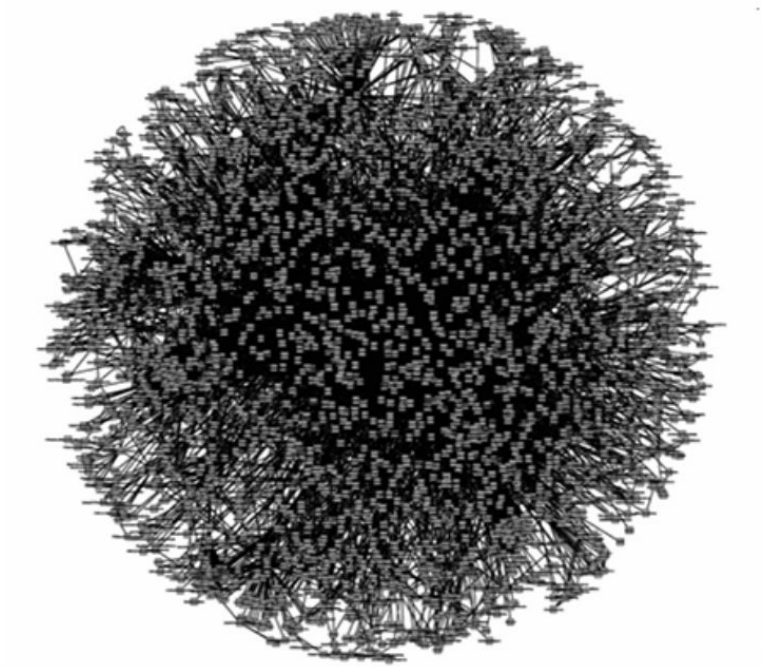
Our systems have evolved beyond human ability to mentally model their behavior.



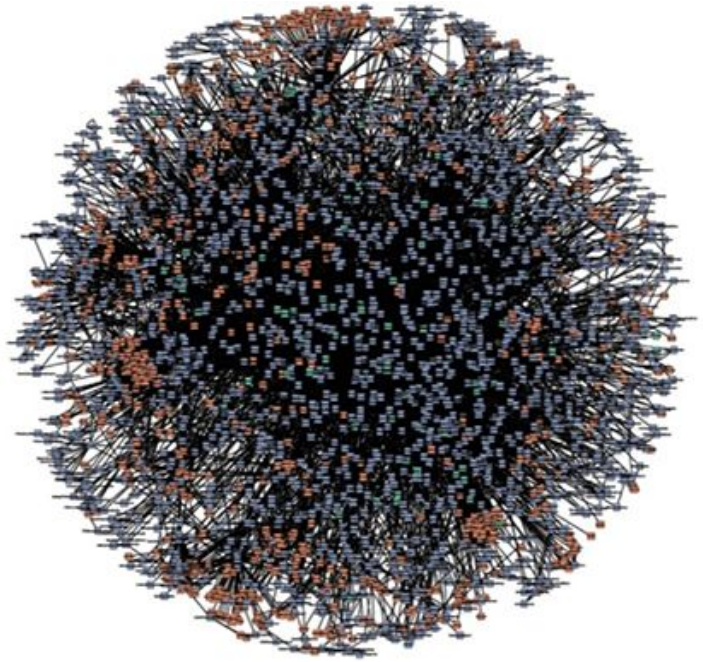
amazon.com

NETFLIX

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



everyone else



amazon.com

NETFLIX

Complex?

Microservice Architectures

Continuous Delivery

Distributed Systems

Automation Pipelines

Containers

Blue/Green Deployments

DevOps

Continuous Integration

Immutable Infrastructure

Infracode

Cloud Computing

CI/CD

Service Mesh

API

Auto Canaries

Circuit Breaker Patterns

Security?

Mostly Monolithic

Prevention focused

Defense in Depth

Expert Systems

Poorly Aligned

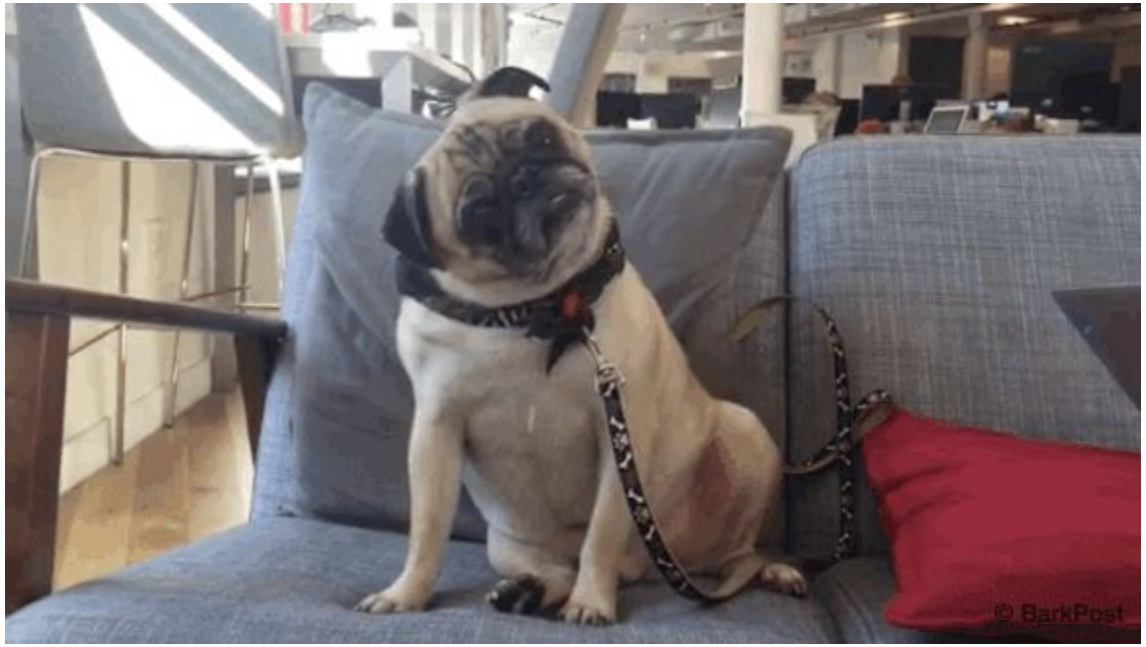
Requires Domain Knowledge

Stateful in nature

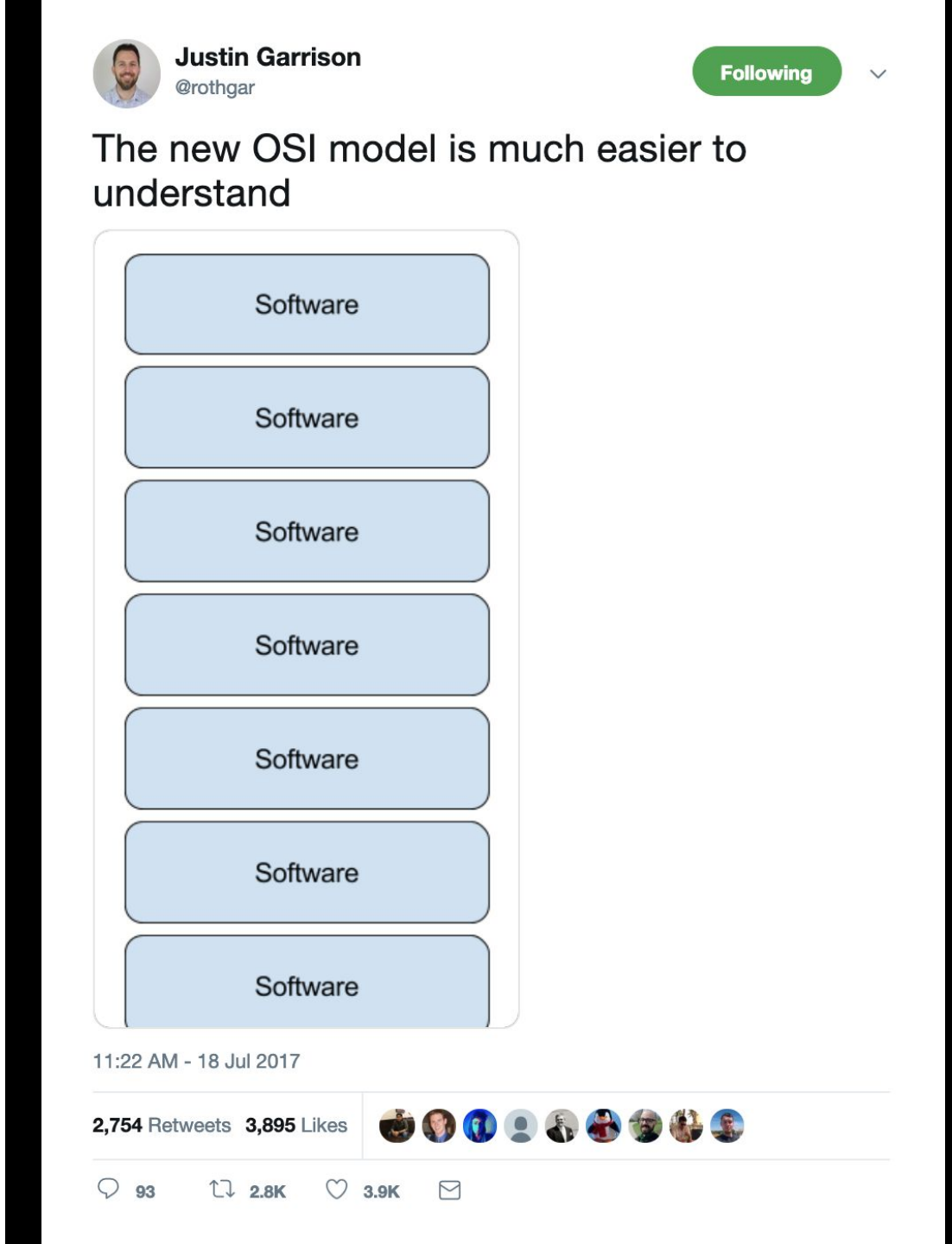
Adversary Focused

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

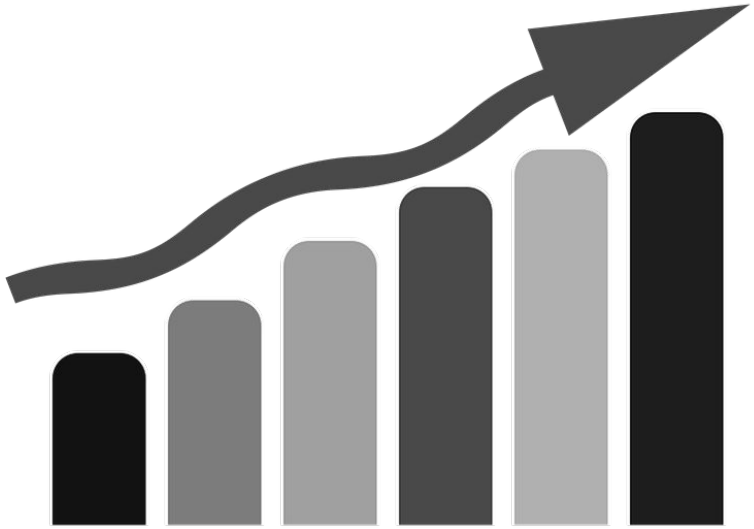
Intel X86, etc (first layer of human-readable code)

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"

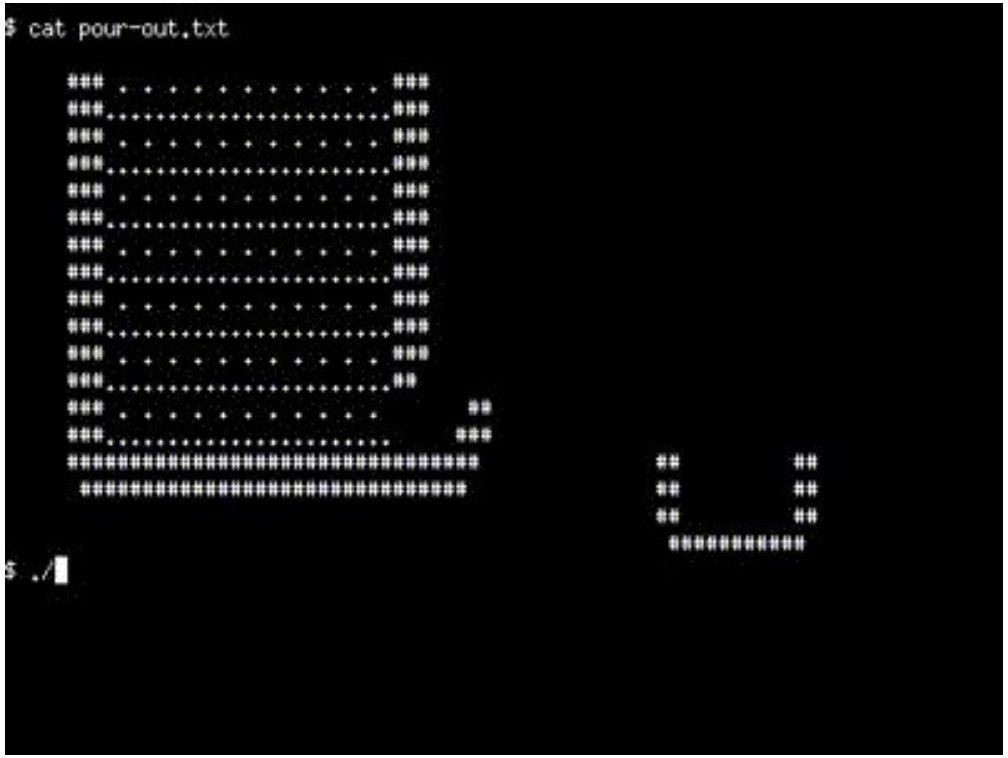
- Dr. David Woods

What about my systems?

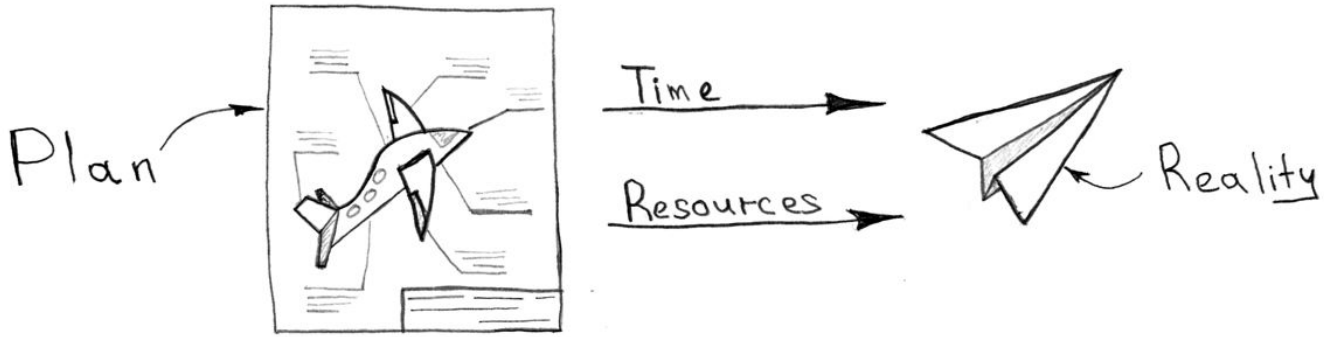
How well do you really understand how your system works?

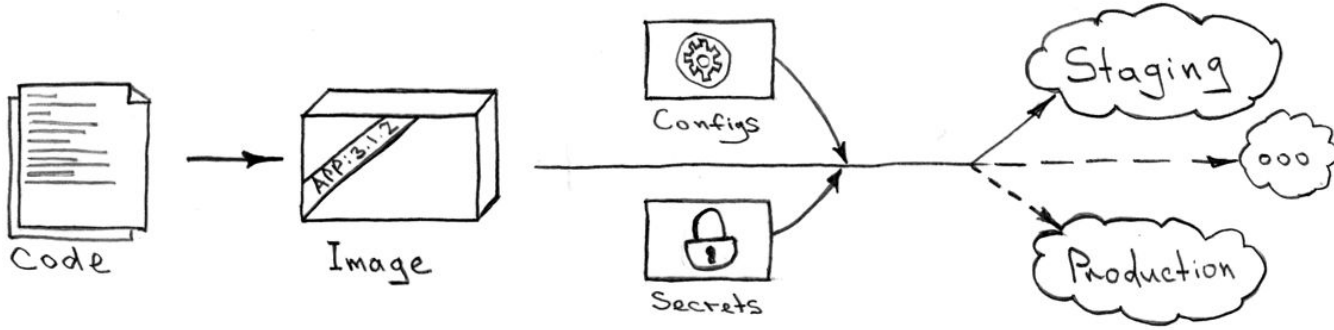
In Reality.....

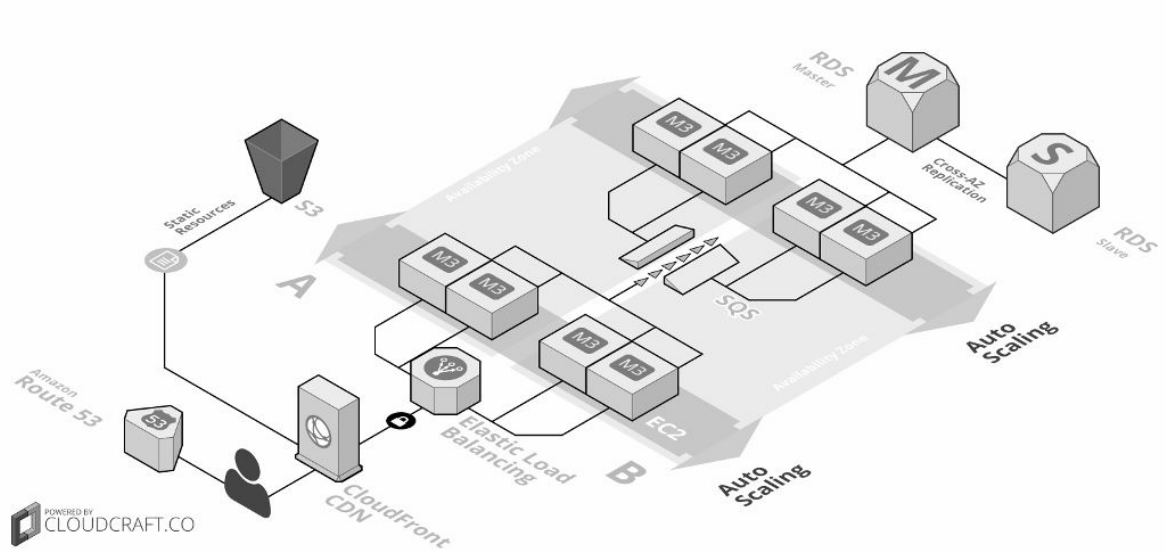
Systems Engineering is **Messy**



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 Outage

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 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

Delayed Features

Identity Conflicts

Migration to New CSP

Refactor Pricing

Misconfigured FW Rule Outage

Firewall Outage -> Disabled

Large Customer Outage

Lead Software Engineering finds a new job at Google

Cloud Provider API Outage

Exposed Secrets on Github

Upgrade to Java SE 12

Code Freeze

DNS Resolution Errors

Merger with competitor

Expired Certificate

300 Microservices Δ-> 850 Microservices

Regulatory Audit

Scalability Issues

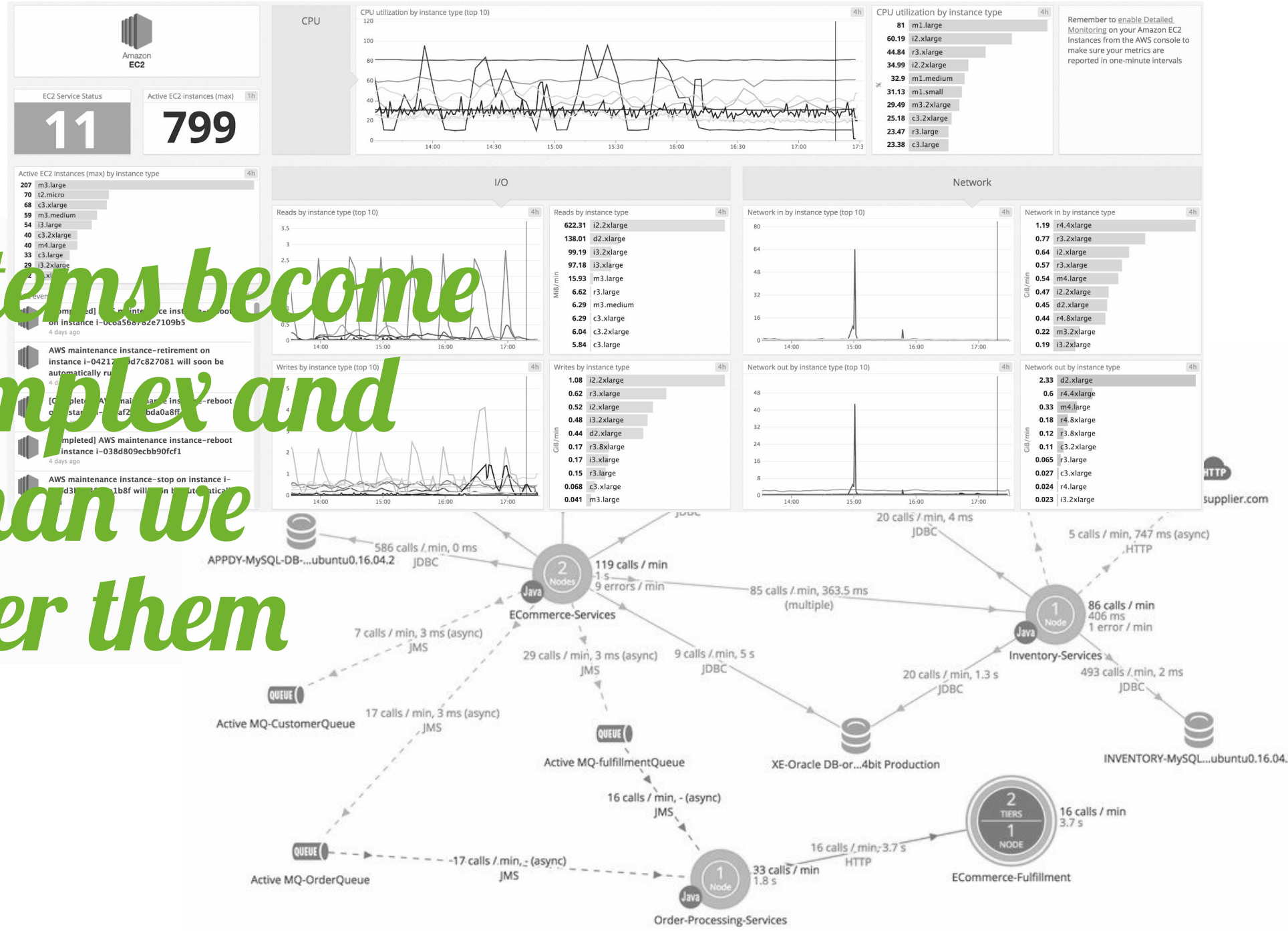
WAF Outage -> Disabled

Rolling Sevl Outage on Portal

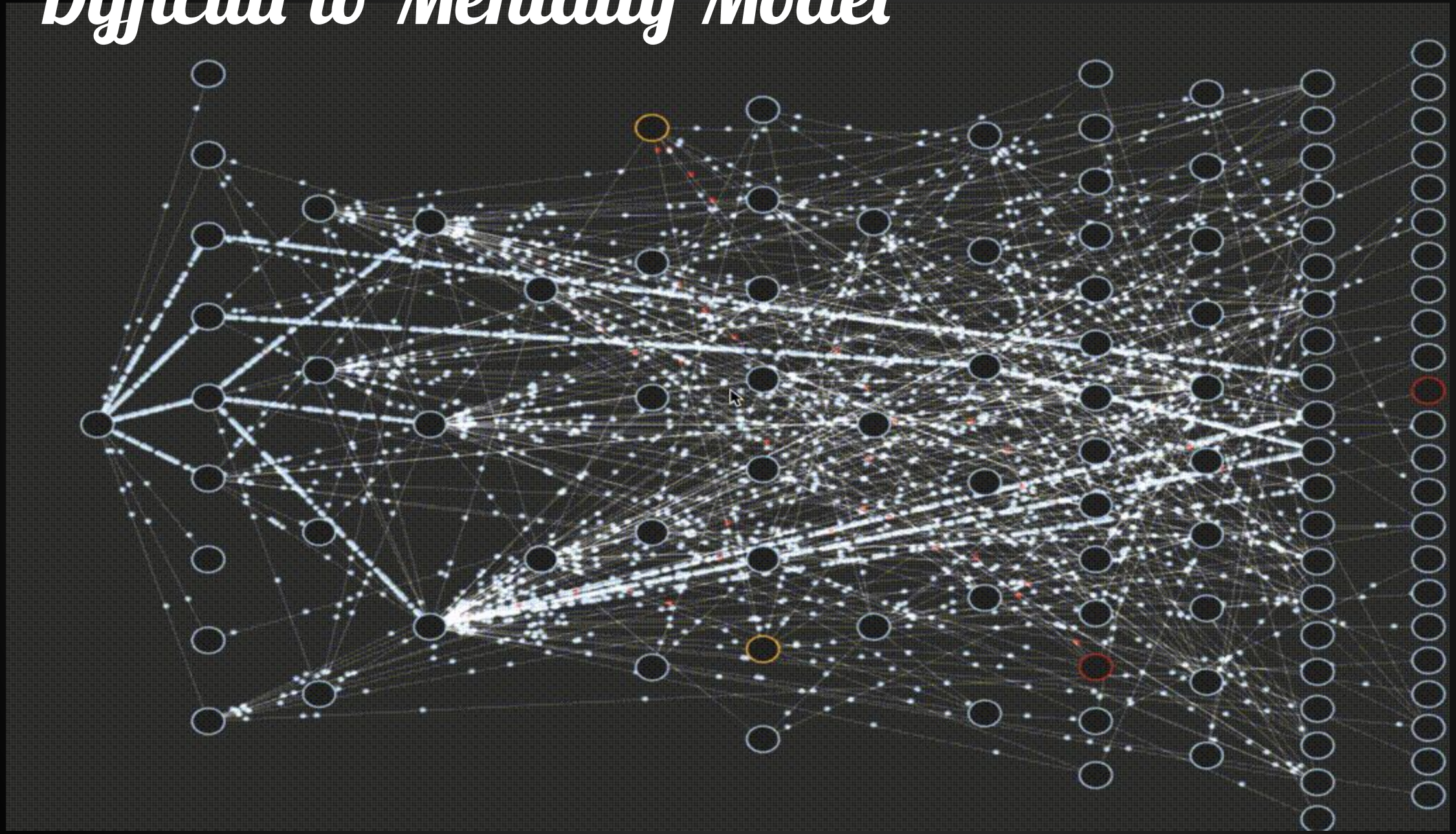
Delayed Features

Large Customer Outage

Our systems become more complex and messy than we remember them



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

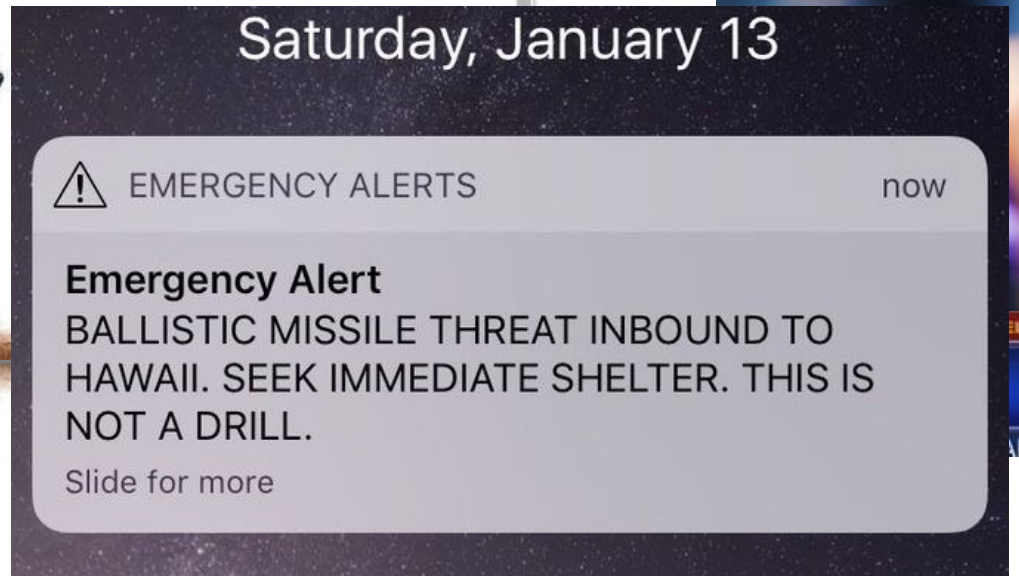
Getting Around to Security Next Month

If there's time

O RLY?

@ThePracticalDev

Failure Happens Alot



The Normal Condition is to

FAIL


We need failure
to Learn & Grow

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

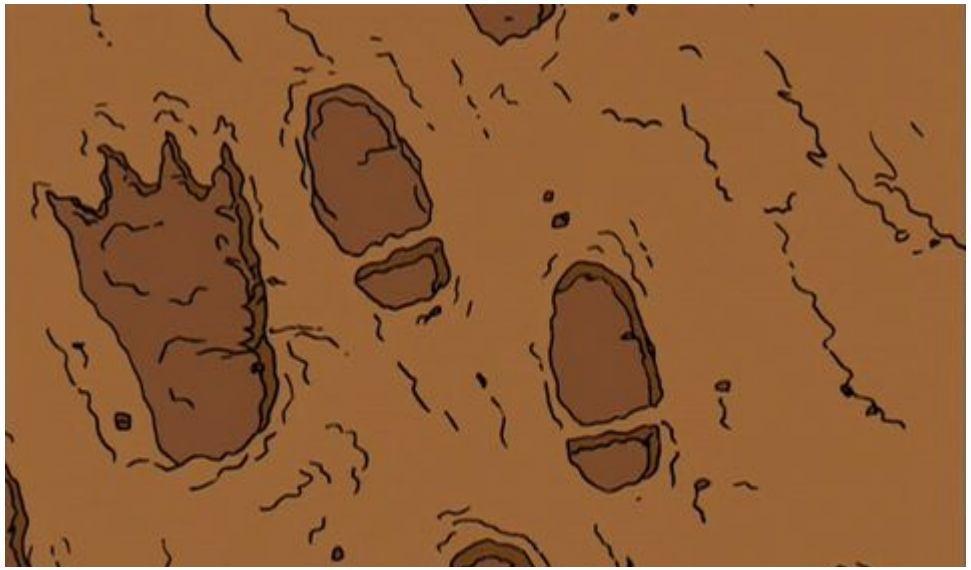
-Scott Sagan "The Limits of Safety"

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

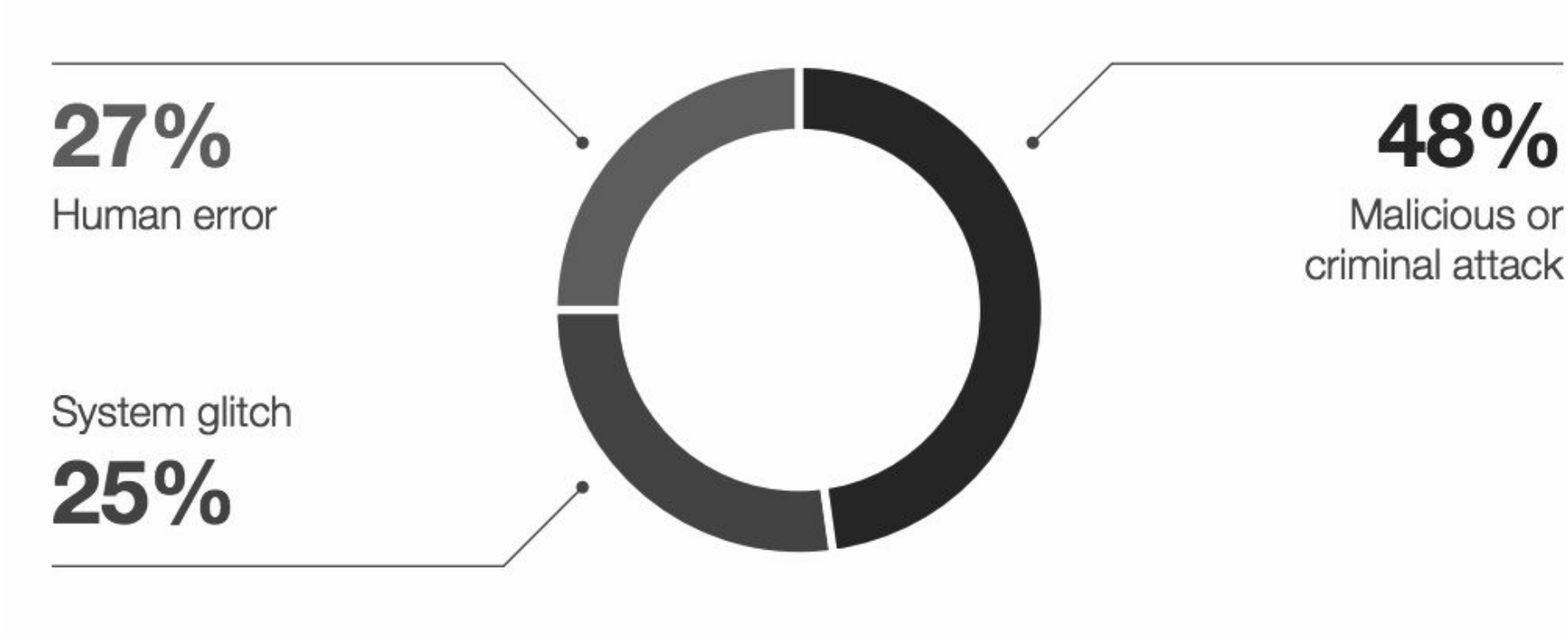
All we typically ever see is the Footsteps in the Sand
-Allspaw

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

What typically causes our security to fail?

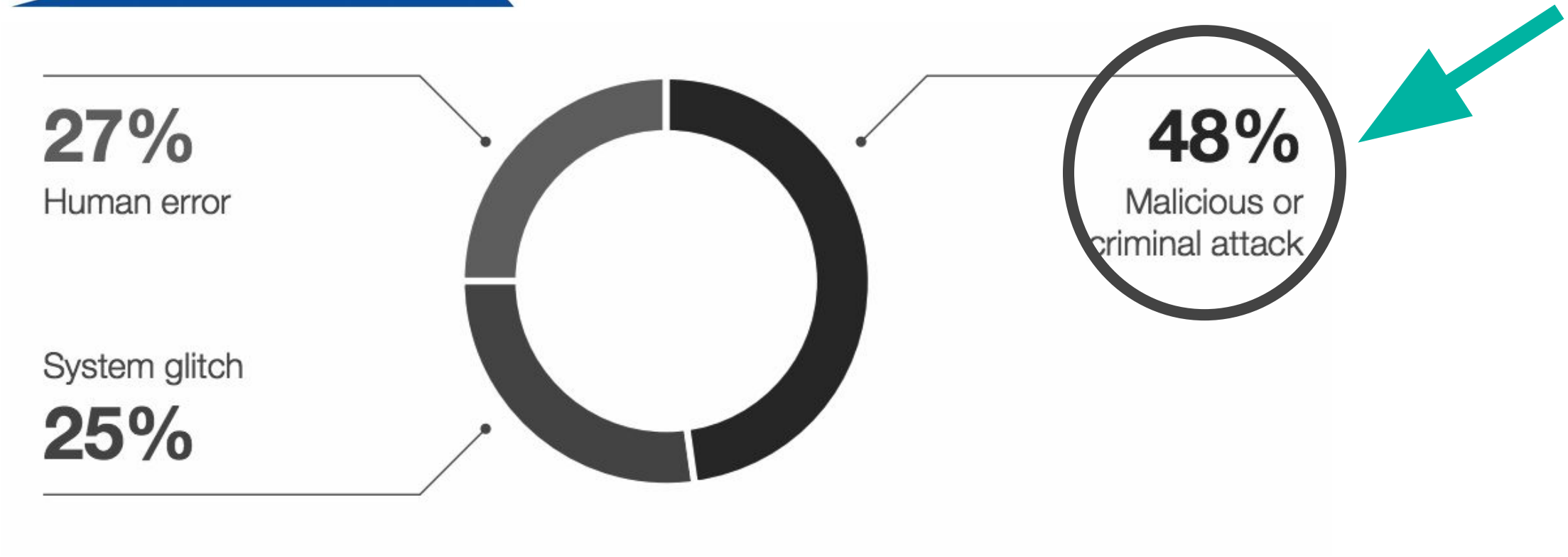
2018 Causes of Data Breaches

Ponemon INSTITUTE

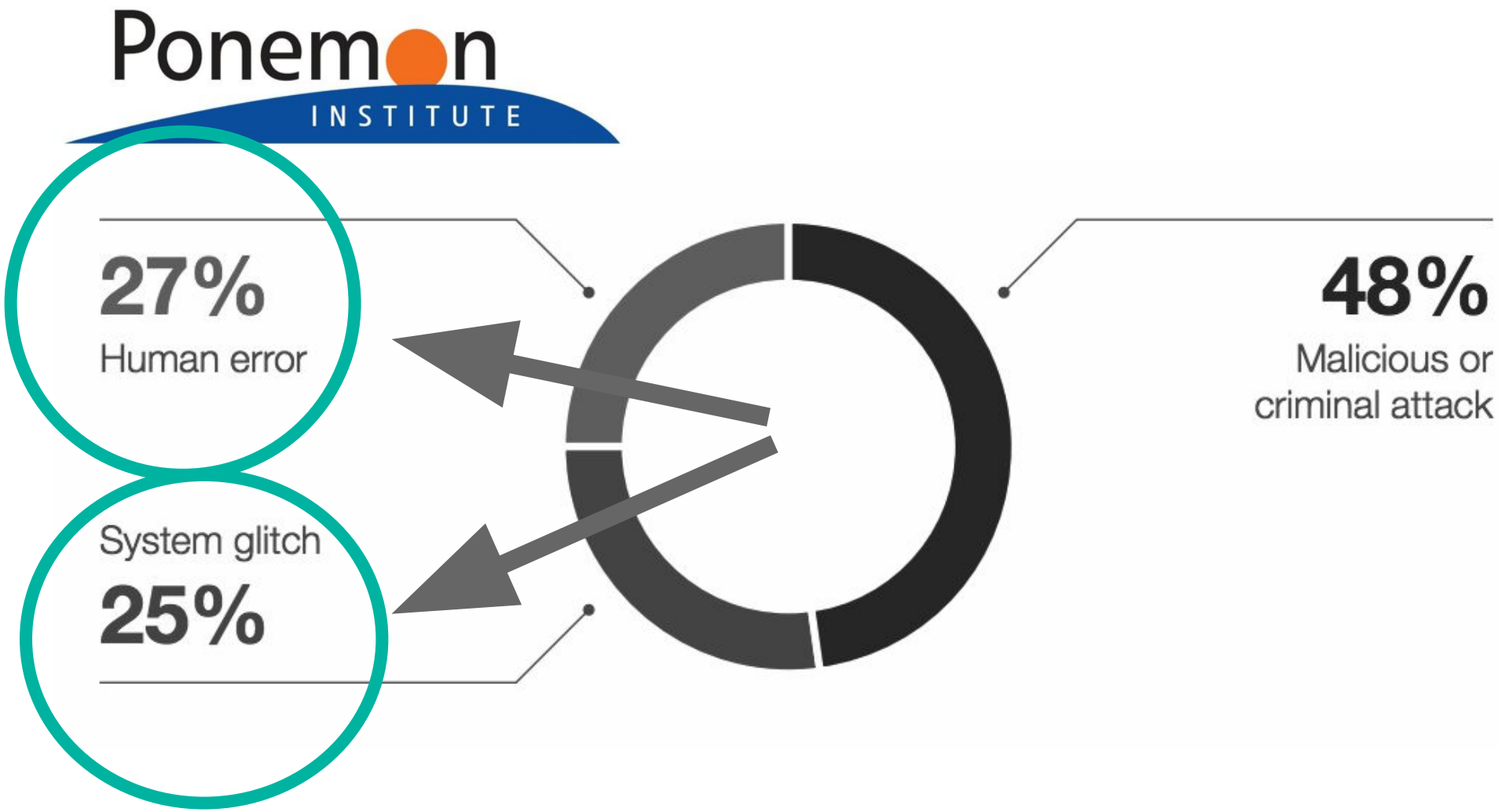


2018 Causes of Data Breaches

Ponemon INSTITUTE

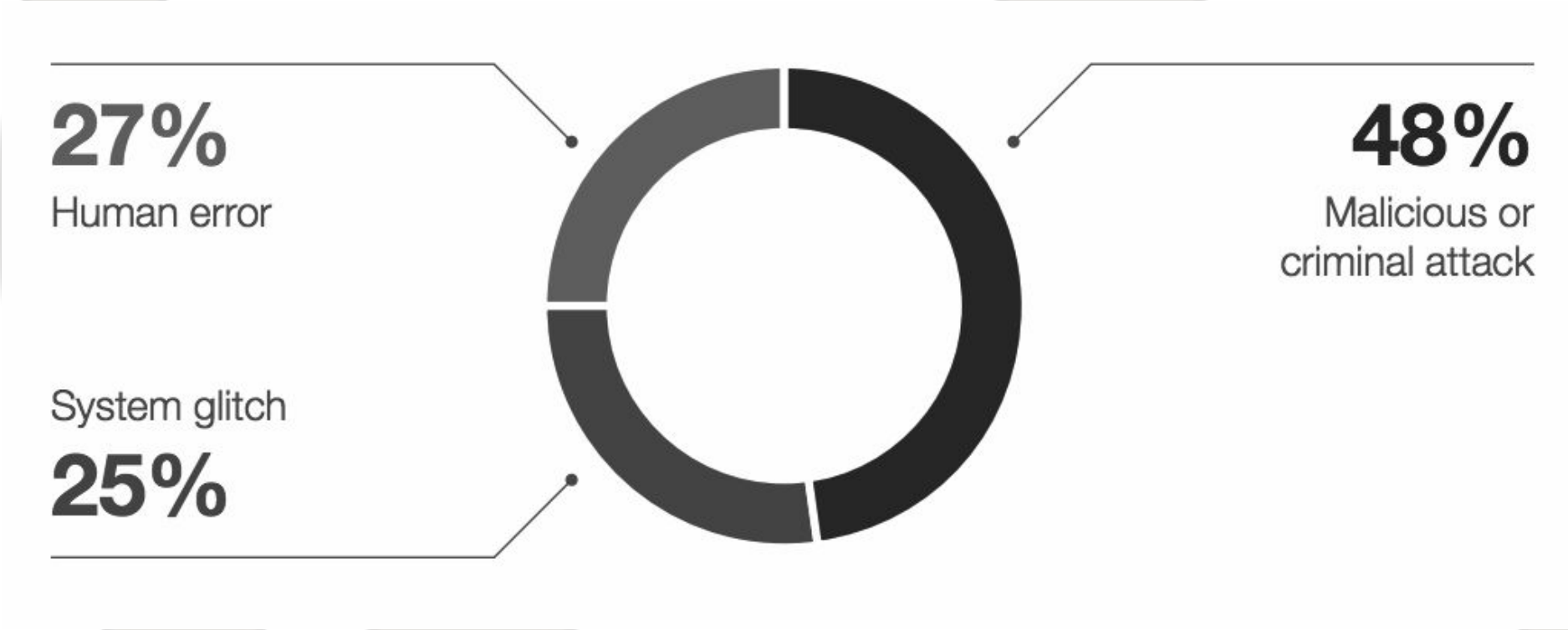


2018 Causes of Data Breaches



2018 Causes of Data Breaches

Ponemon INSTITUTE



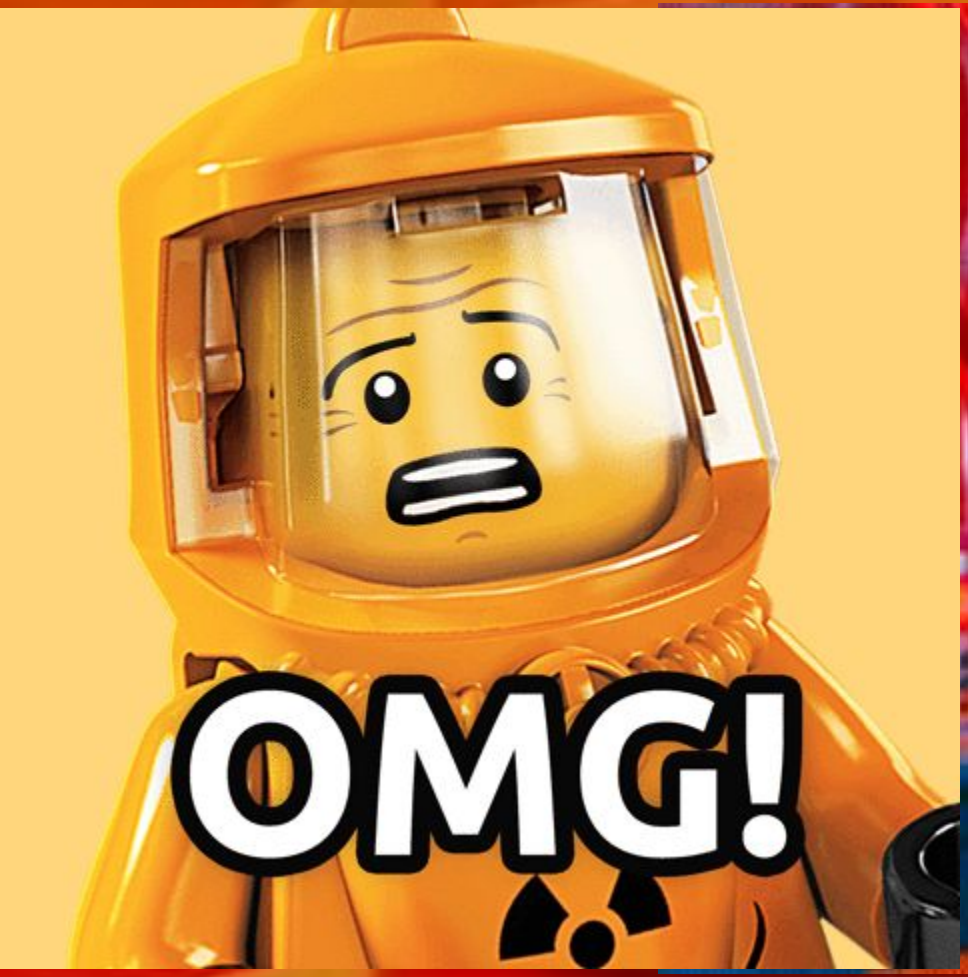
'Human-Error', Root Cause, & Blame Culture

[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.

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

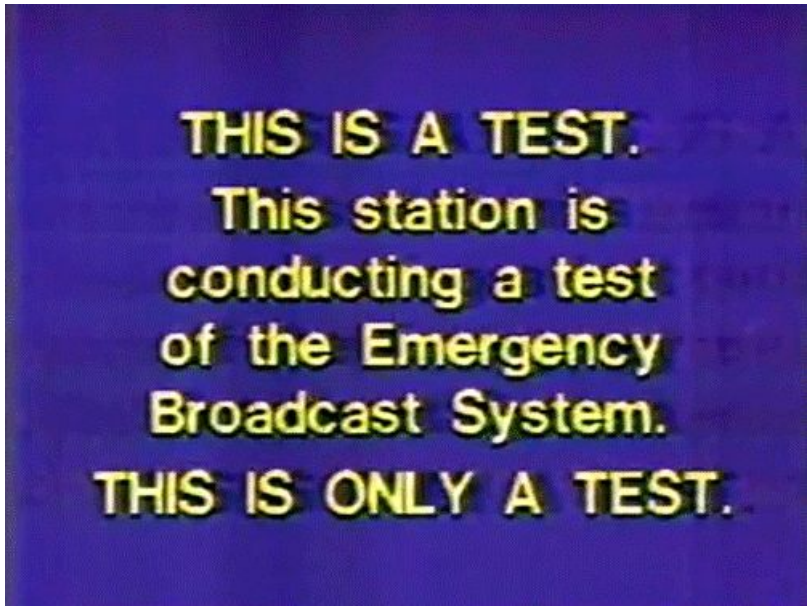
System Resiliency in Practice

"[Chaos Engineering is] empirical rather than formal. We don't use models to understand what the system should do. We run experiments to learn what it does."

- ***Michael T. Nygard***

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 Engineering Maturity

Despite what has been popularized on online tech blogs you do not start off performing Chaos Engineering on live production systems. There is a maturity ramp to getting there.

- **Validate Chaos Tools in Lower Environment**
- **Develop Competency & Confidence in Tooling**
- **Dry-run experiments**

Warning: Still be careful in Non-Prod environments as you will be surprised what hazards lie in Non-Prod. (Kafka Story)

Chaos Engineering Pro-Tips

- Don't perform an experiment when you expect it to fail
- Auto Remediation of Experiments will end in a fiery Hell!
- Transparency is a Must
- Webcast & Record GameDays
- The process of creating the experiment and sharing the learnings is the highest-value of Chaos Engineering
- Chaos Engineering Goal: Share Team Mental Models is of High Importance

Chaos Pitfalls: Auto-Remediation

Bring context or chase down vulnerabilities for the service owner instead of automating fixes as this leads to a Fiery Hell!

"...an operator will only be able to generate successful new strategies for unusual situations if he has an adequate knowledge of the process."
" Long term knowledge develops only through use and feedback about its effectiveness."

— Lisanne Bainbridge, The Ironies of Automation (1983)

Reference: Nora Jones 8 Traps of Chaos Engineering

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

Build Confidence in What Actually Works

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?

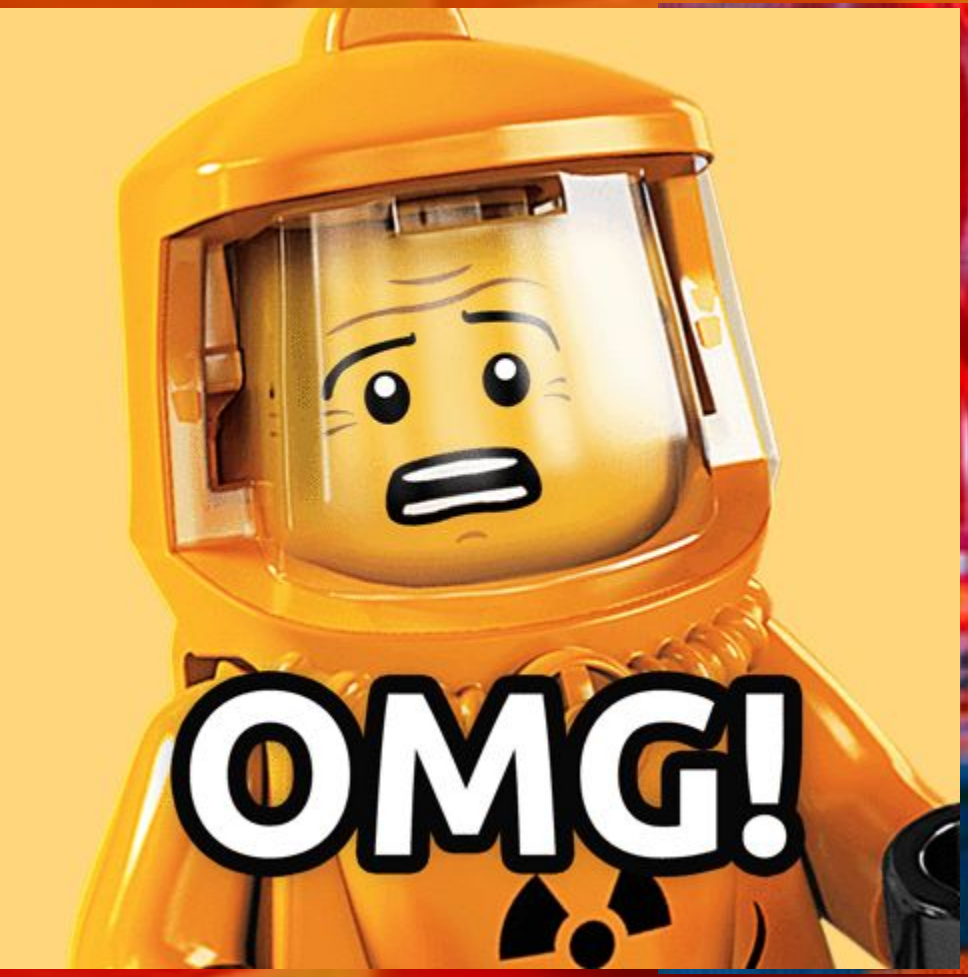
“*Response*” *is the problem with Incident Response*

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?

Solution Architecture

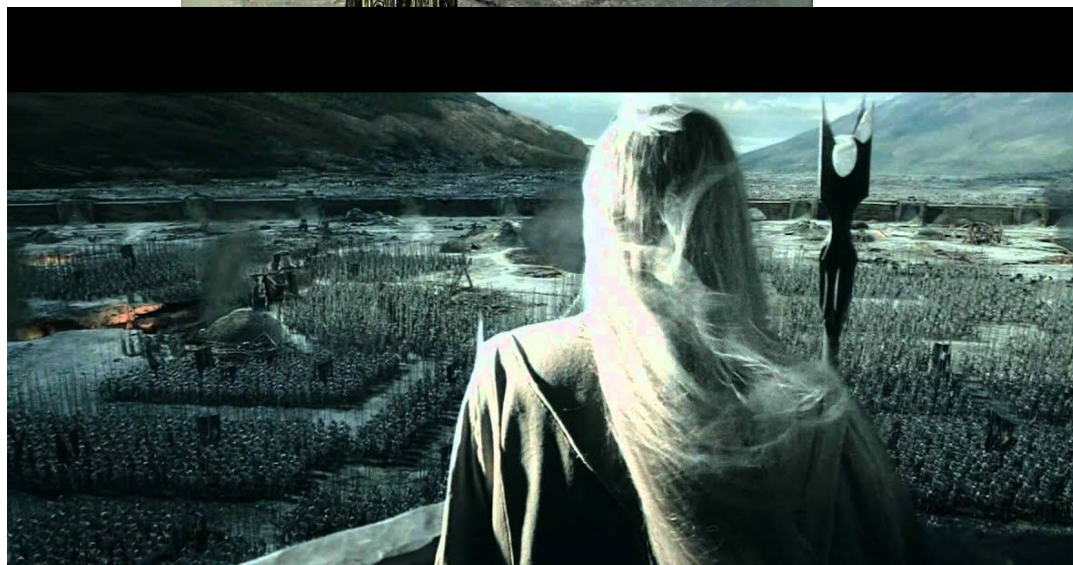
"More men (people) die from their remedies not their illnesses"

- Jean-Baptiste Poquelin

Ivory Tower Architecture

Solutions Architecture needs reinvention

Patterns never worked



Security Control Validation

Create Objective Feedback Loops about Security Effectiveness

ChaoSlingr

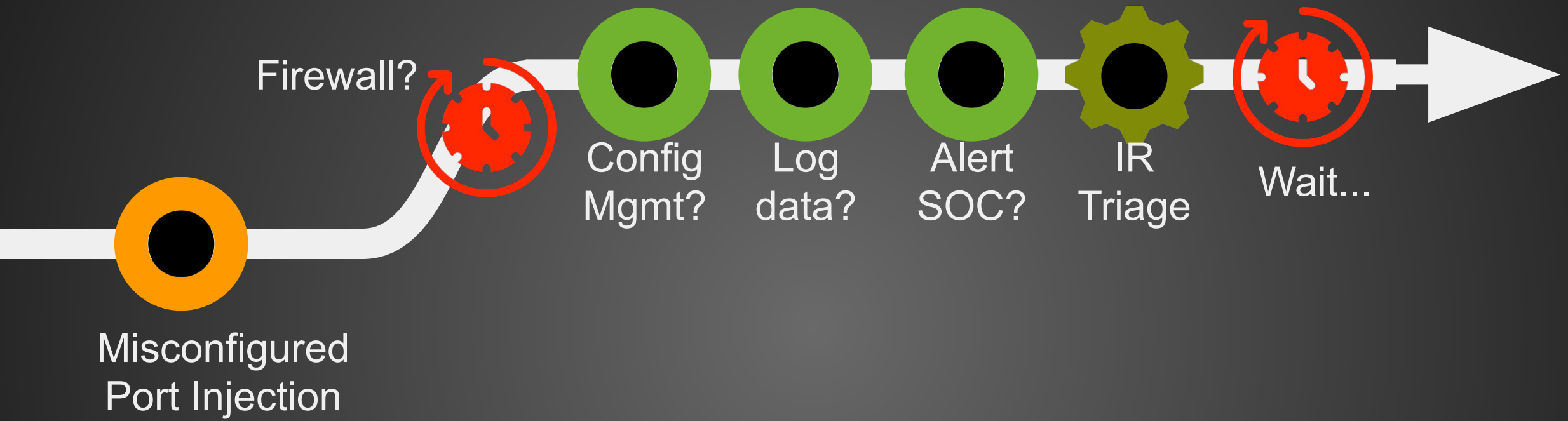
An Open Source Tool

ChaoSlingr Product Features

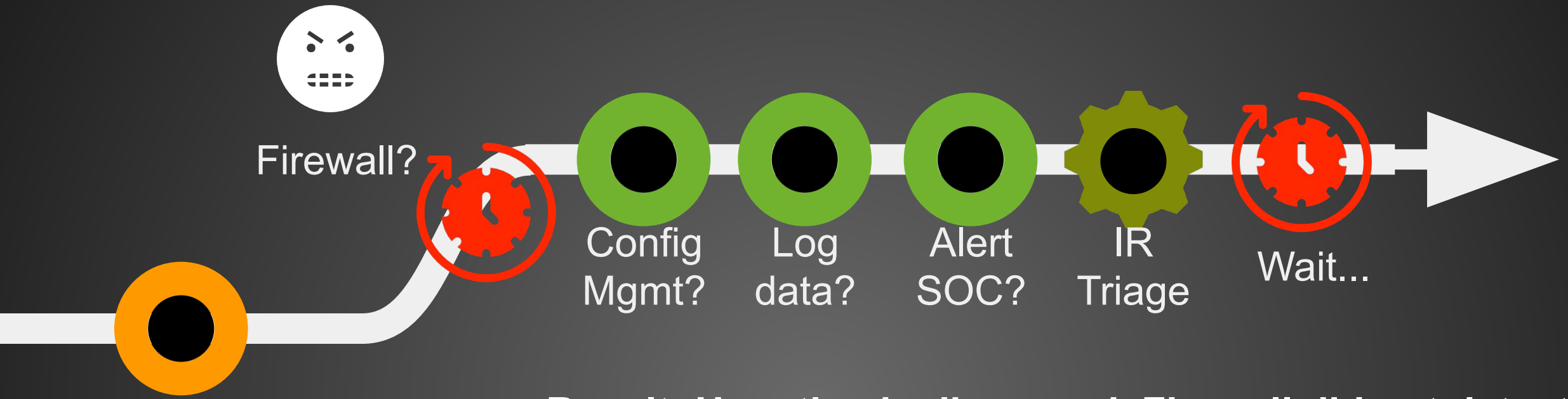
- ChatOps Integration
- Configuration-as-Code
- Example Code & Open Framework

- 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.

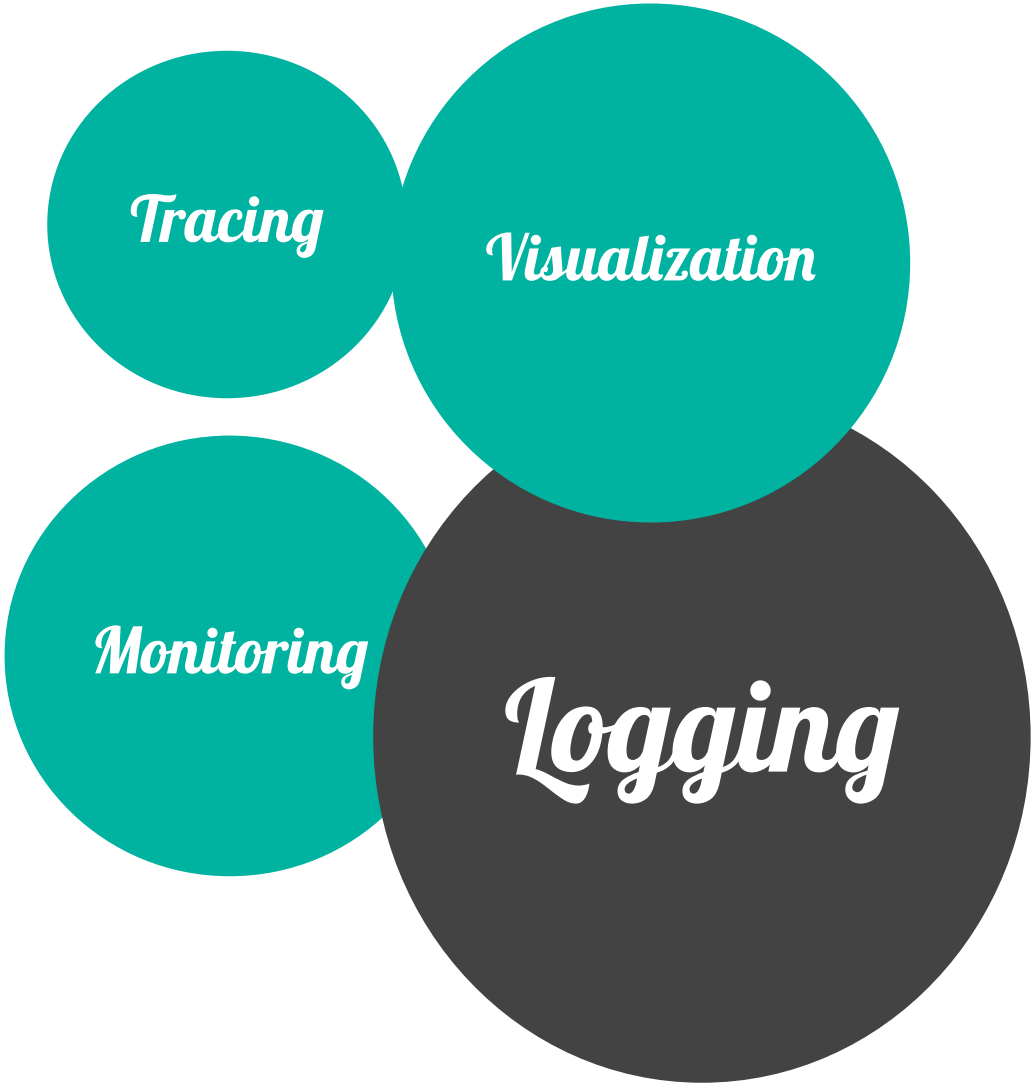


Result: Hypothesis disproved. Firewall did not detect or block the change on all instances. Standard Port AAA security policy out of sync on the Portal Team instances. Port change did not trigger an alert and log data indicated successful change audit. However we unexpectedly learned the configuration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

Stop looking for better answers and start asking better questions.

- John Allspaw

Security Log Pipelines



More Experiment Examples

- *Software Secret Clear Text Disclosure*
- *Permission collision in Shared IAM Role Policy*
- *Disabled Service Event Logging*
- *Introduce Latency on Security Controls*
- *API Gateway Shutdown*

- *Internet exposed Kubernetes API*
- *Unauthorized Bad Container Repo*
- *Unencrypted S3 Bucket*
- *Disable MFA*
- *Bad AWS Automated Block Rule*

Q&A

@aaronrinehart

aaron@verica.io