

GOTO **CHICAGO 2023**

#GOTOchgo

Navigating Complexity and Reinforcing System Security



Aaron Rinehart

@aaronrinehart

Sr. Distinguished Engineer

Capital One

aaron.rinehart@capitalone.com



What will you learn?

- **Complexity in Modern Software**
- **Complex Adaptive Systems**
- **What is Resilience?**
- **Chaos Engineering**
- **Security Chaos Engineering (SCE)**
- **Example SCE Use Case & Experiment**

O'REILLY®

Security Chaos Engineering

Developing Resilience and Safety
at Speed and Scale



O'REILLY®

Chaos Engineering

System Resiliency in Practice

O'REILLY®

Security Chaos Engineering

Gaining Confidence in Resilience
and Safety at Speed and Scale

Aaron Rinehart & Kelly Shortridge

REPORT



About A.A.Ron

- Sr. Distinguished Engineer @CapitalOne
- Former CTO, Co-Founder @ Verica, Chief Security Architect @UnitedHealth, DoD, NASA Safety & Reliability Engineering
- Frequent speaker and author on Chaos Engineering, Resilience Engineering & Security
- O'Reilly Co-Author: Chaos Engineering, Security Chaos Engineering Books
- Pioneer behind Security Chaos Engineering
- Led ChaoSlingr team at UnitedHealth



goto;

What does it mean to be Resilient?

*“Resilience is the ability for a system to **adapt** its functioning in response to changing conditions so it can continue operating successfully. Instead of attempting to prevent failure, resilience encourages us to handle failure with grace.*

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

Facebook's image outage reveals how the company's AI tags your photos



Taylor Kerns

'Oh wow, the AI just tagged my office picture as basic'

By James Vincent |

GOOGLE

NEWS



Apple Cloud Service revealed from Twitter outage

Service is coming back online, but some users are still having trouble

By Humza Aamir on July 9, 2019, 8:18 AM

System Status

Apple ID	Available
Account	Available
Backup	Available
Bookmarks	Available
Calendar	Available
Cloud	Available
Contacts	Available
Files	Available
Health	Available
HomeKit	Available
iCloud	Available
iCloud Calendar	Issue
iCloud Photos	Available
iCloud Drive	Available
iCloud Mail	Available
iCloud Keychain	Available
iCloud Reminders	Available
iCloud Sync	Available
iCloud TV Shows	Available
iCloud Web Clips	Available
iCloud Web Pages	Available
iCloud Web Sites	Available
iCloud Web Videos	Available
iCloud Web Audio	Available
iCloud Web Images	Available
iCloud Web Documents	Available
iCloud Web Applications	Available
iCloud Web Games	Available
iCloud Web Music	Available
iCloud Web Movies	Available
iCloud Web TV Shows	Available
iCloud Web Podcasts	Available
iCloud Web News	Available
iCloud Web Sports	Available
iCloud Web Weather	Available
iCloud Web Finance	Available
iCloud Web Health	Available
iCloud Web Education	Available
iCloud Web Travel	Available
iCloud Web Shopping	Available
iCloud Web Food	Available
iCloud Web Entertainment	Available
iCloud Web Lifestyle	Available
iCloud Web Business	Available
iCloud Web Government	Available
iCloud Web Religion	Available
iCloud Web Science	Available
iCloud Web Technology	Available
iCloud Web Arts	Available
iCloud Web Sports	Available
iCloud Web Music	Available
iCloud Web Movies	Available
iCloud Web TV Shows	Available
iCloud Web Podcasts	Available
iCloud Web News	Available
iCloud Web Sports	Available
iCloud Web Health	Available
iCloud Web Education	Available
iCloud Web Travel	Available
iCloud Web Shopping	Available
iCloud Web Food	Available
iCloud Web Entertainment	Available
iCloud Web Lifestyle	Available
iCloud Web Business	Available
iCloud Web Government	Available
iCloud Web Religion	Available
iCloud Web Science	Available
iCloud Web Technology	Available
iCloud Web Arts	Available

3 min read

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.

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

Science & Technology

TweetDeck suffers outage, reason unknown

6 days ago



Popular

I could have done it
December 25th
Jersey

16 hours ago

Sept 21 morenz
injury wholesal

17 hours ago

We're Not Getting Better

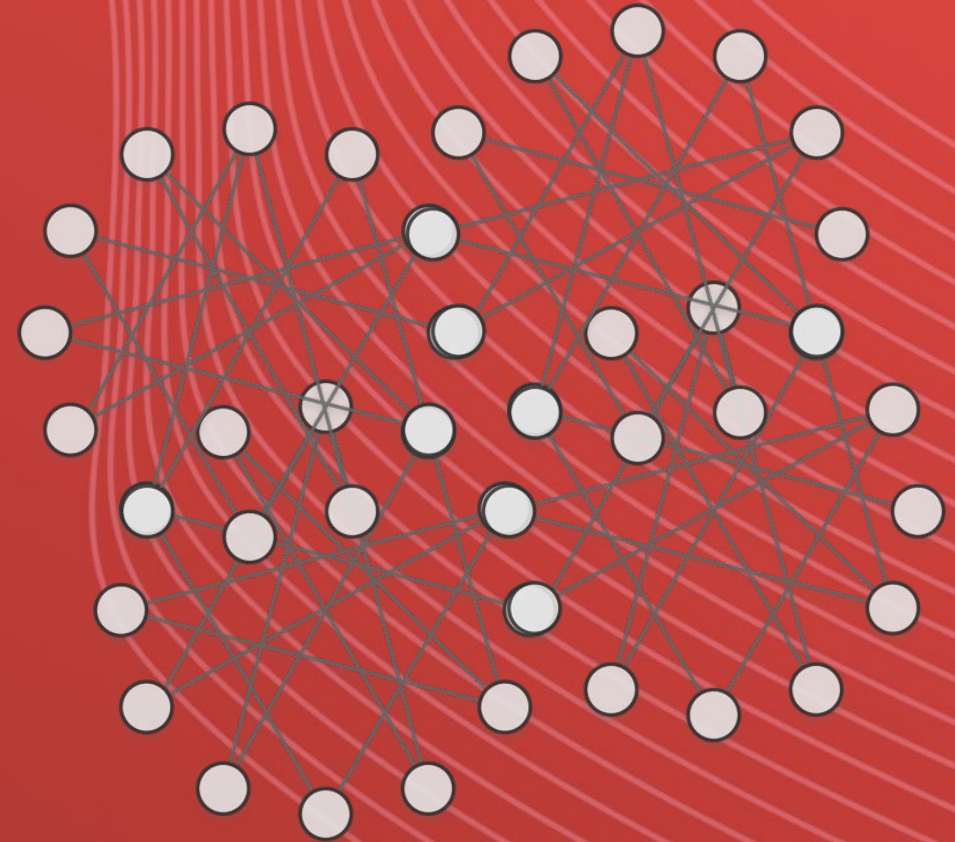
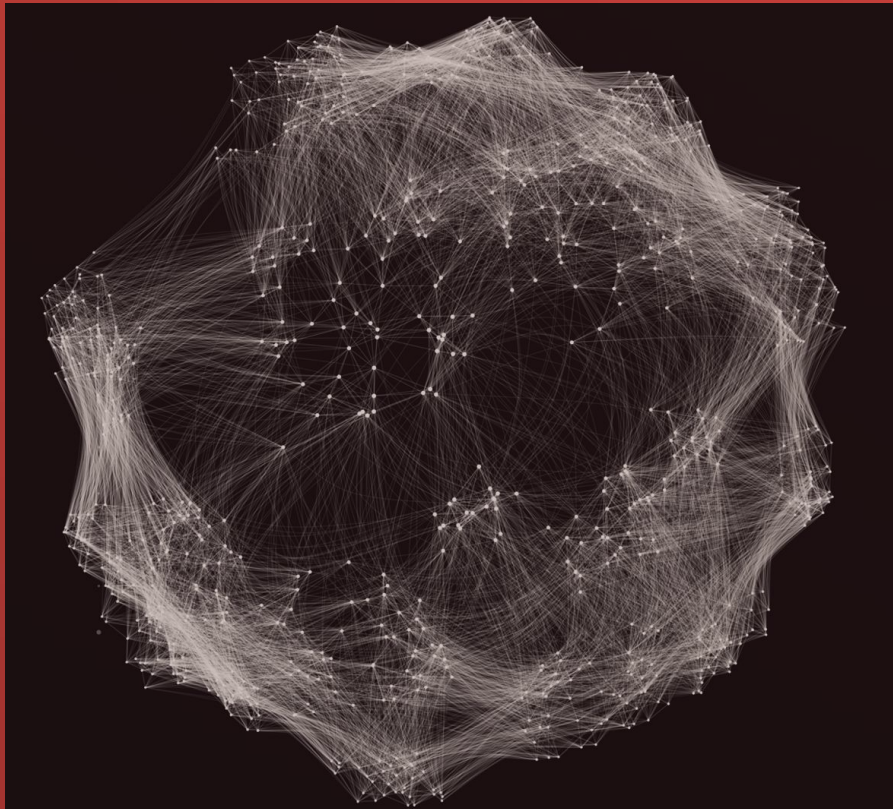
We are creating a snapshot of the industry, to keep developers and businesses at the forefront of an ever-changing tech market.

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

**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 `goto;` Modern Software is Challenging



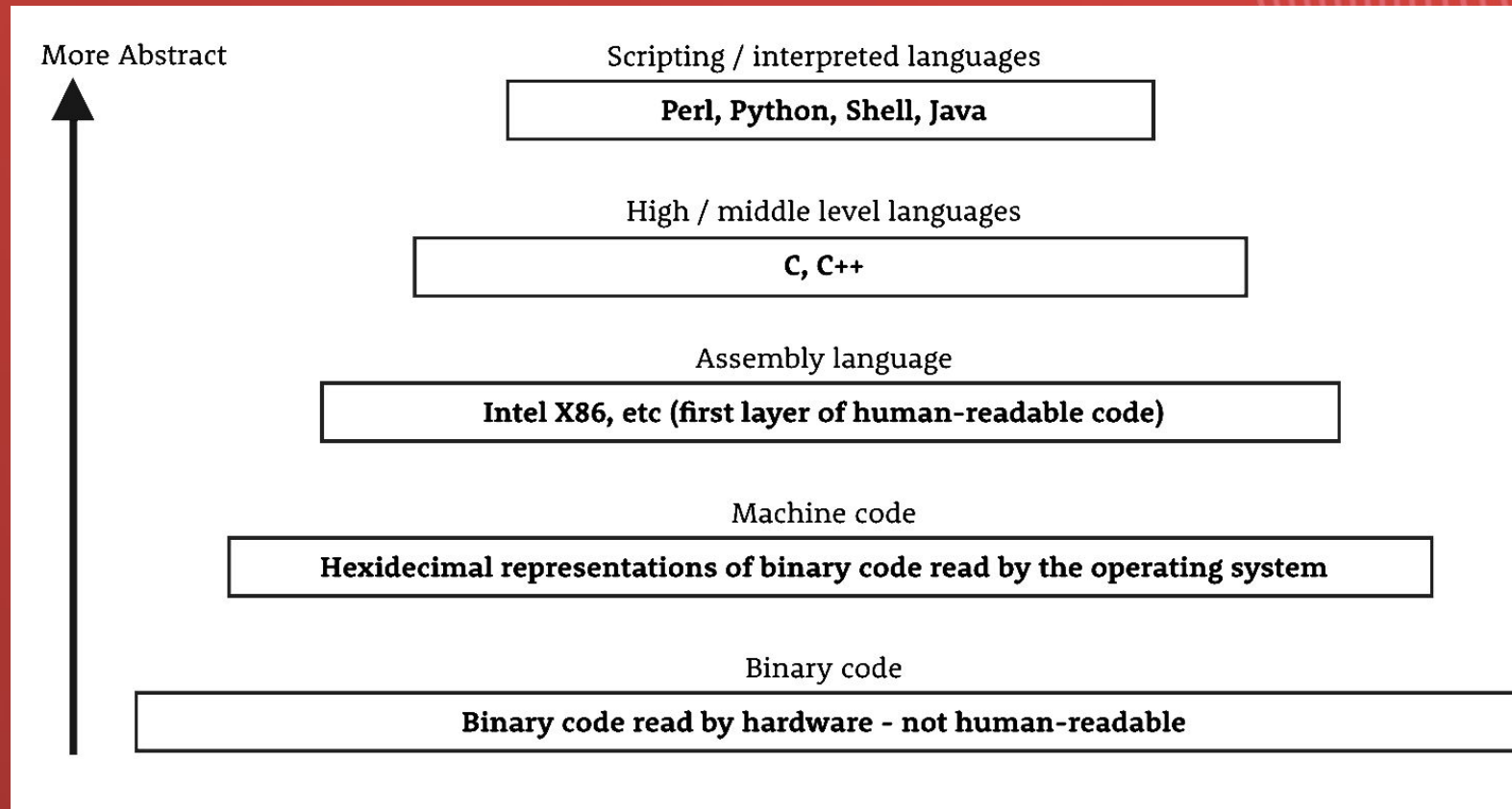
Software has officially taken over

The new OSI model is much easier to understand



Software Only Increases in Complexity

goto;



Let's talk about "Legacy" Systems

“Mature”

“Confident”

“Well
Understood”

“Dependable”

“Zero Downtime”

“*Business
Critical*”

“STABLE”

“*Mission Essential*”

“Flagship
Product”

“Good
Documentation”

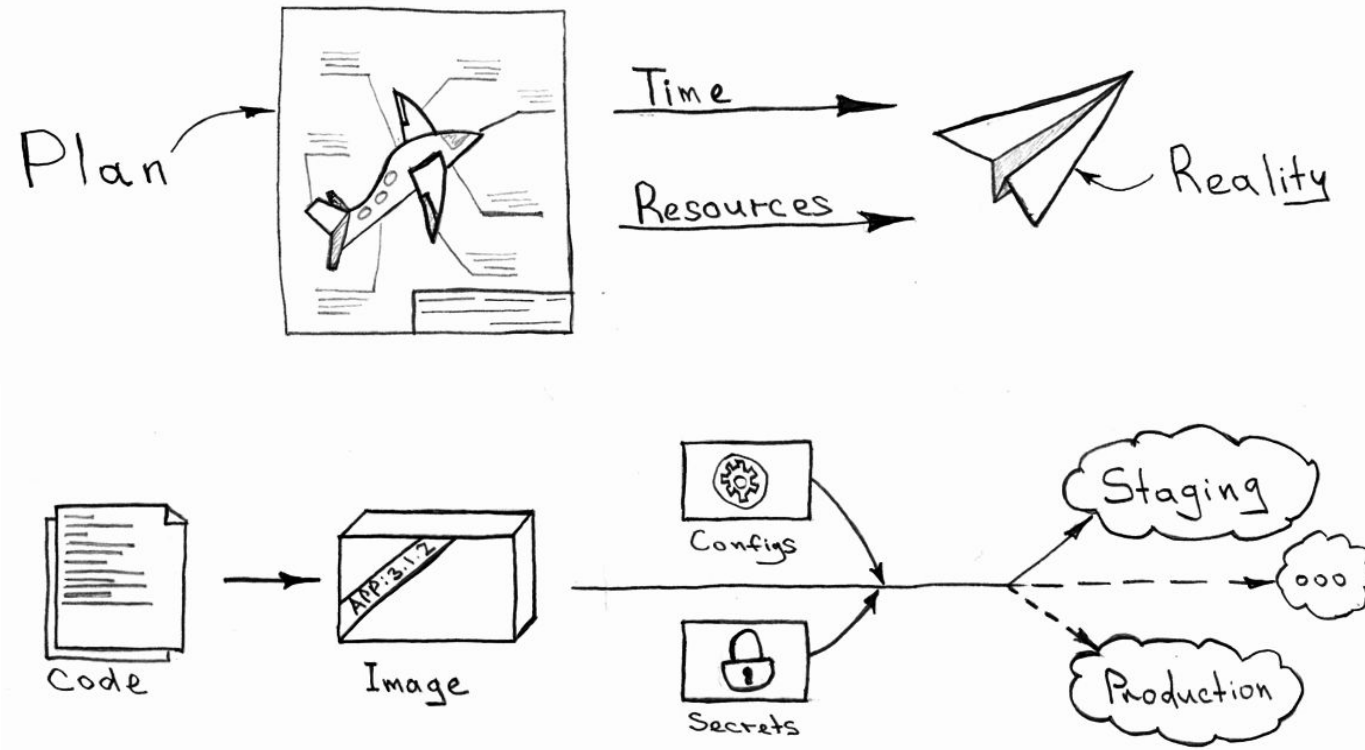
goto;

HOW? did
“LEGACY”
SYSTEMS become
“STABLE” ?

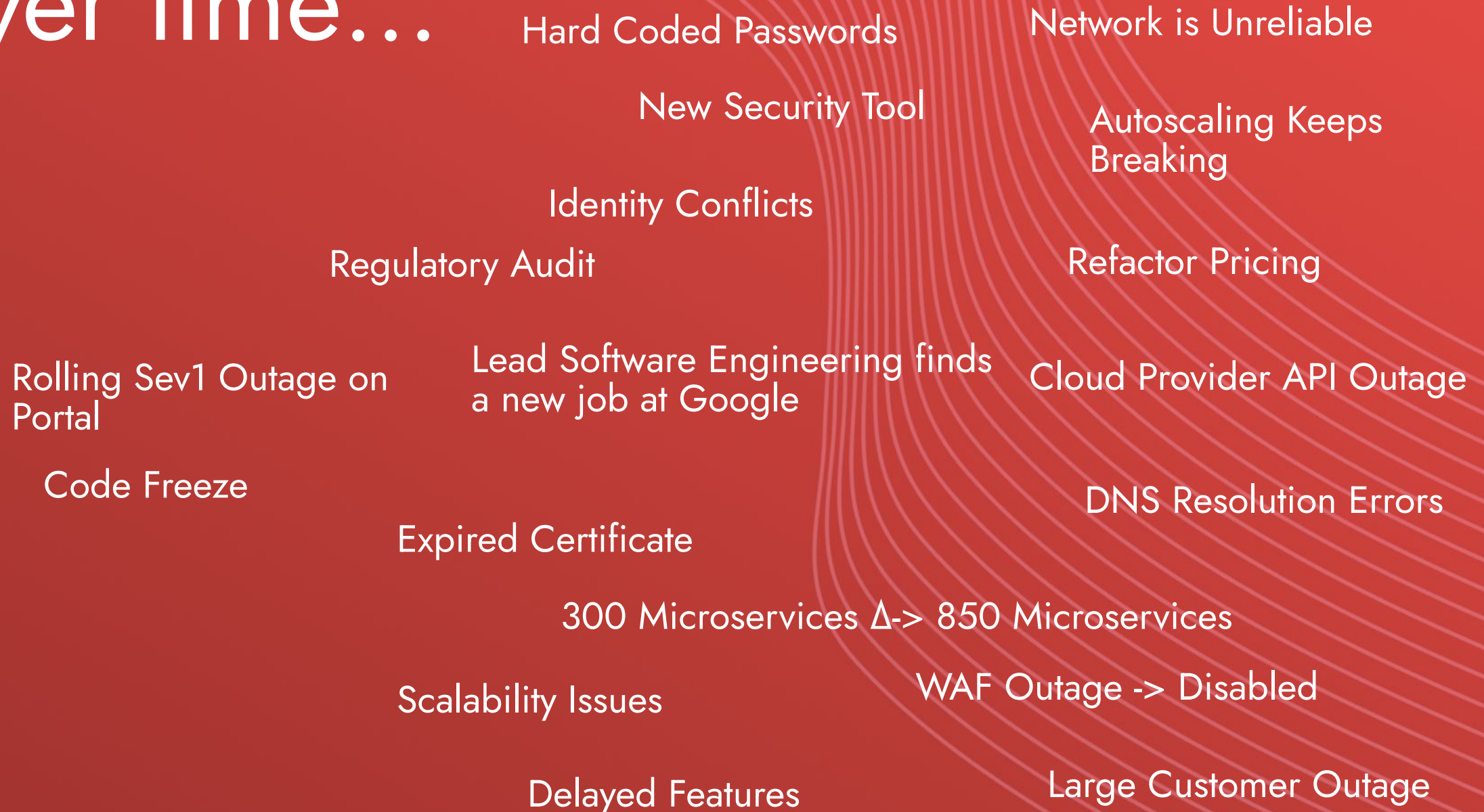
We forget
that.....

Systems
Engineering is
Messy

In the
beginning...
it seems so
simple



Over time...



Our systems
have become
more complex
and messy
than we
remember



**How does
this \$€%*
have to do
with
Security?**

Cyber Security is Context Dependent

**Flexibility to
Change System
Rapidly**

VS.

**Ability to Apply
Secure Context to
System Changes**

Instrumenting Chaos

Testing vs. Experimentation



How do we
typically
discover when
our security
measures fail?

Security Incidents

goto;

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

Learn to Navigate Complexity with Chaos Engineering

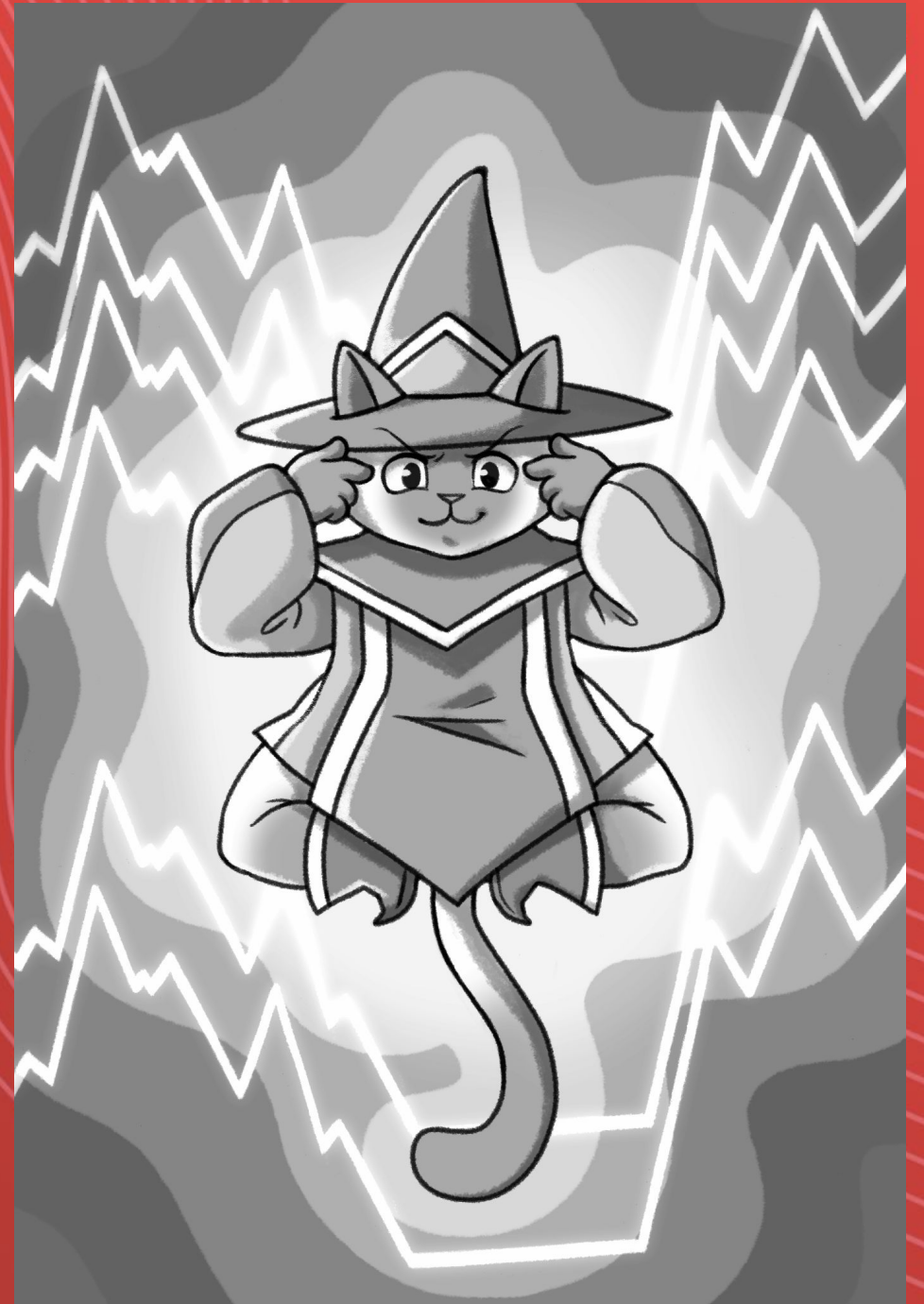


Chaos Engineering



“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”

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



O'REILLY®

Security Chaos Engineering

Developing Resilience and Safety
at Speed and Scale



Kelly Shortridge &
Aaron Rinehart

goto;

Security Theater

***Hope is Not an
Effective Strategy***

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

Achievement despite ignorance



Getting it to Work

And Having No Idea How

O RLY?

@ThePracticalDev

Getting Started

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

O'REILLY®

Security Chaos Engineering

Developing Resilience and Safety
at Speed and Scale



Kelly Shortridge &
Aaron Rinehart

Security is Subjective & Reactive goto;

No matter how much we prepare...
We really don't know very much

Where?

Why?

Who?

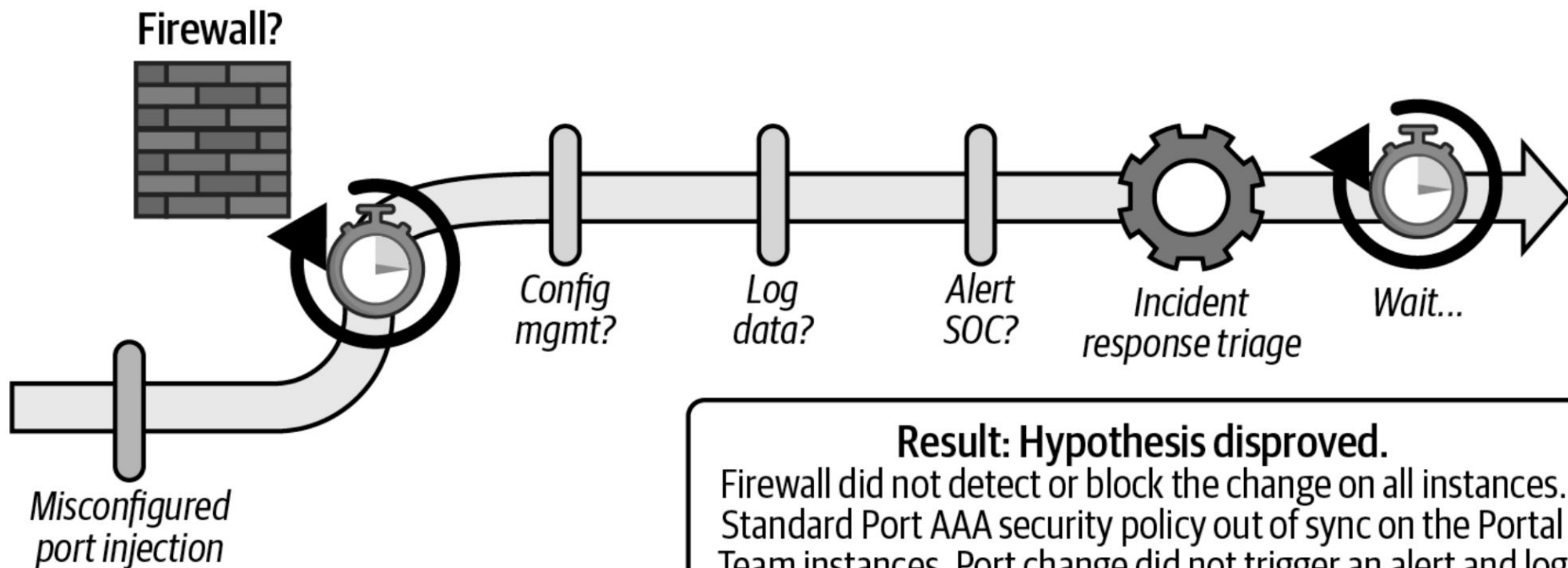
How?

What?

An Example SCE Experiment



oto;

**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 management tool caught the change and alerted the SOC.

Post-Mortem

- Learn to navigate complexity with SCE
- Use SCE to build confidence in your security
- Chaos Engineering & Security CE are about being proactive



Don't forget to
vote for this session
in the **GOTO Guide app**