RSAConference2022
San Francisco & Digital | February 7 – 10

TRANSFORM

SESSION ID: **DSO-W08**

Site Reliability Engineering and the Security Team They Love

Aaron Rinehart
CTO & Co-Founder
Verica.io
@aaronrinehart

James Wickett
Head of Research
Verica.io
@wickett

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Aaron Rinehart, CTO, Co-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

VERICA

@aaronrinehart

James Wickett (@wickett)

- Head of Research at Verica
- LinkedIn Learning Instructor
- Former Signal Sciences, Mentor Graphics, National Instruments, IBM
- Austin, TX
- Plans a lot of conferences…


O'REILLY
Compliments of
NETFLIX
Chaos Engineering
Building Confidence in Sy
through Experiments
O'REILLY
Chaos Engineering
System Resiliency in Practice
O'REILLY
Security Chaos Engineering
Gaining Confidence in Resilience

SRE & Security Hot Takes

These are NOT the Droids You Are Looking for

Observability != Monitoring

Root Cause Is A Fallacy

Chaos Engineering = Fixing NOT Breaking

Resilience != BCP/DR

Complexity CANNOT Be Simplified Away

DevOps IS NOT SRE

SRE IS NOT DevOps

The "S" in Security & SRE is Silent

Favor Context OVER Control

Complexity != Enemy of Security

Security Chaos Engineering != Penetration Testing

Humans ARE NOT the Problem

Guardrails = Incident Handcuffs

Understandability IS MORE IMPORTANT Simplicity

Humans ARE the Solution

VERICA

The Situation Isn't Improving

Southwest Airlines says 'planned system outage' affected flights nationwide, including in Houston-area

The airline says the outage is resolved, however, passengers could still face delays

Bloomberg

U.S. E

Live Now | Markets | Technology | Politics | Wealth | Pursuits | Opinion | Businessweek | Equality | Green

Technology

Apple Resolves Outage That Hobbled Apps and Internal Systems

- Music, iCloud and maps didn't work for some users Monday
- Problems prevented corporate staff from working from home

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

Healthcare IT News TOPI

Global Edition Electronic Health Records (EHR, EMR)

EHR outage takes down federal Cerner systems

Clinicians at dozens of Defense Department, Coast Guard and Veterans Affairs sites were unable to update medical records for hours this past Wednesday.

Apple iCloud services recover from nationwide outage

Service outages are increasingly becoming a headache for tech companies and consumers alike

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

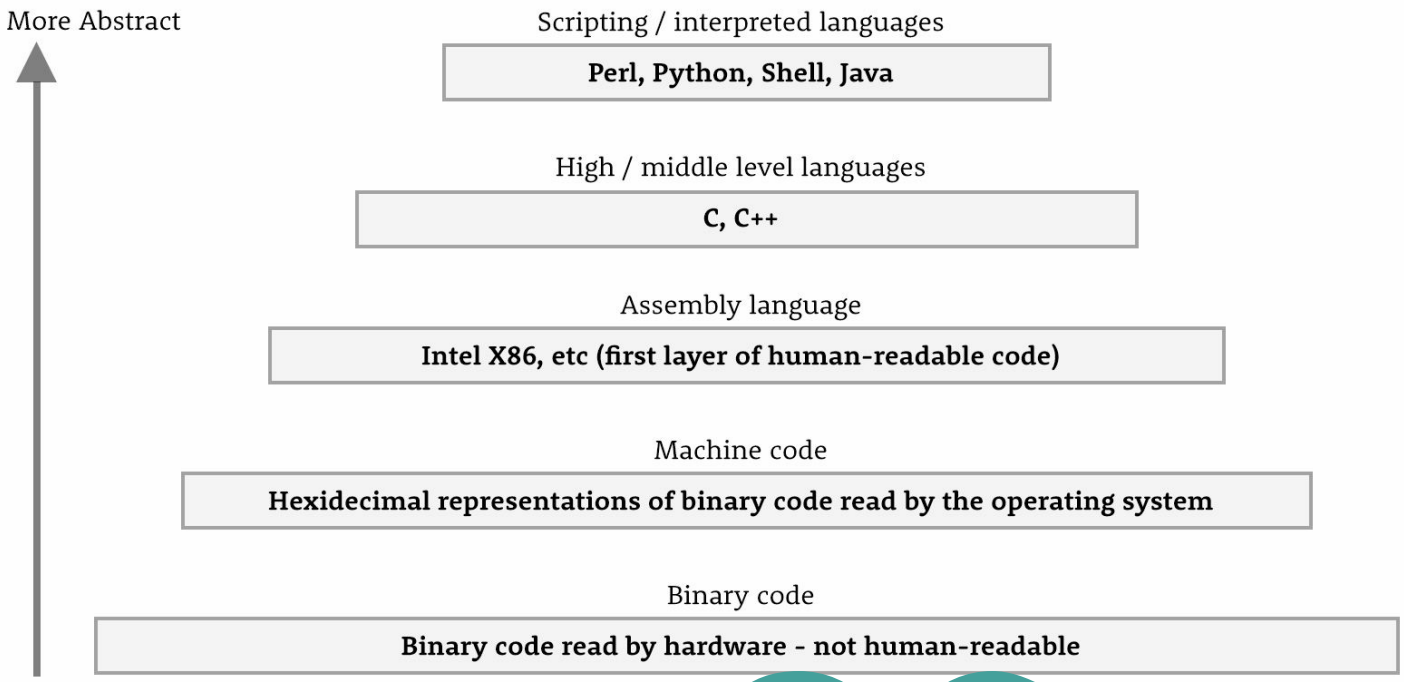
The PlayStation Network recovers from an outage affecting players on PS5 and PS4

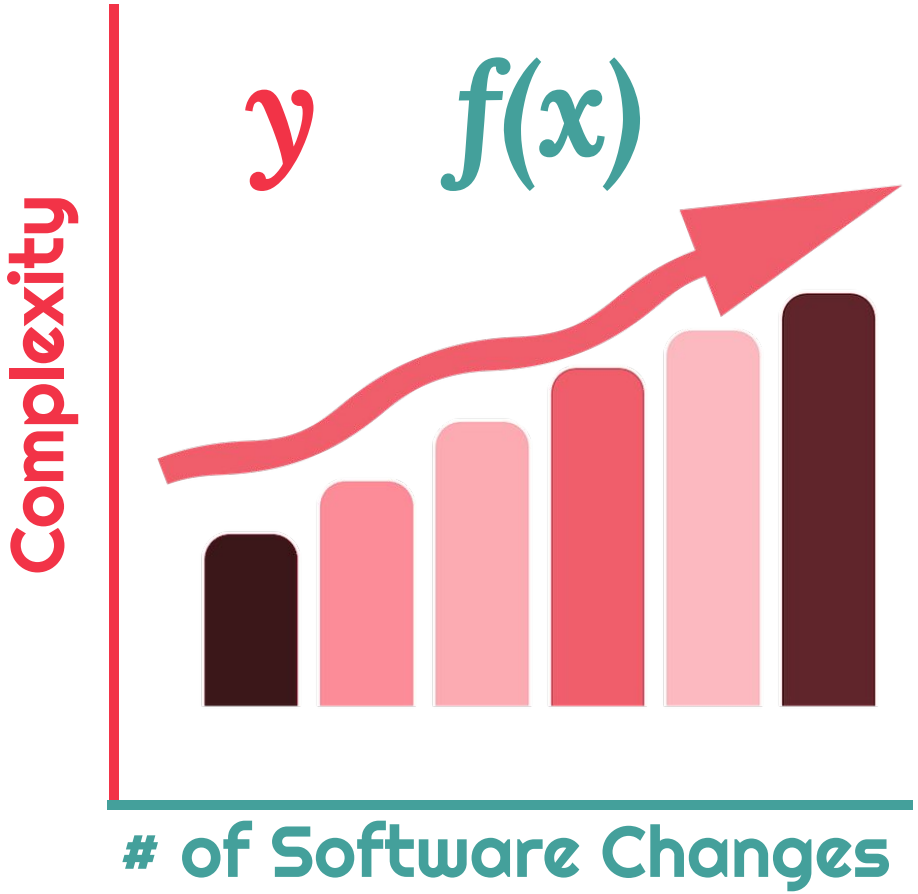
The outage began around 8:30AM ET

By Emma Roth | Updated Mar 23, 2022, 12:44pm EDT

Why is this? What are we doing wrong?

Software ONLY Increases in Complexity

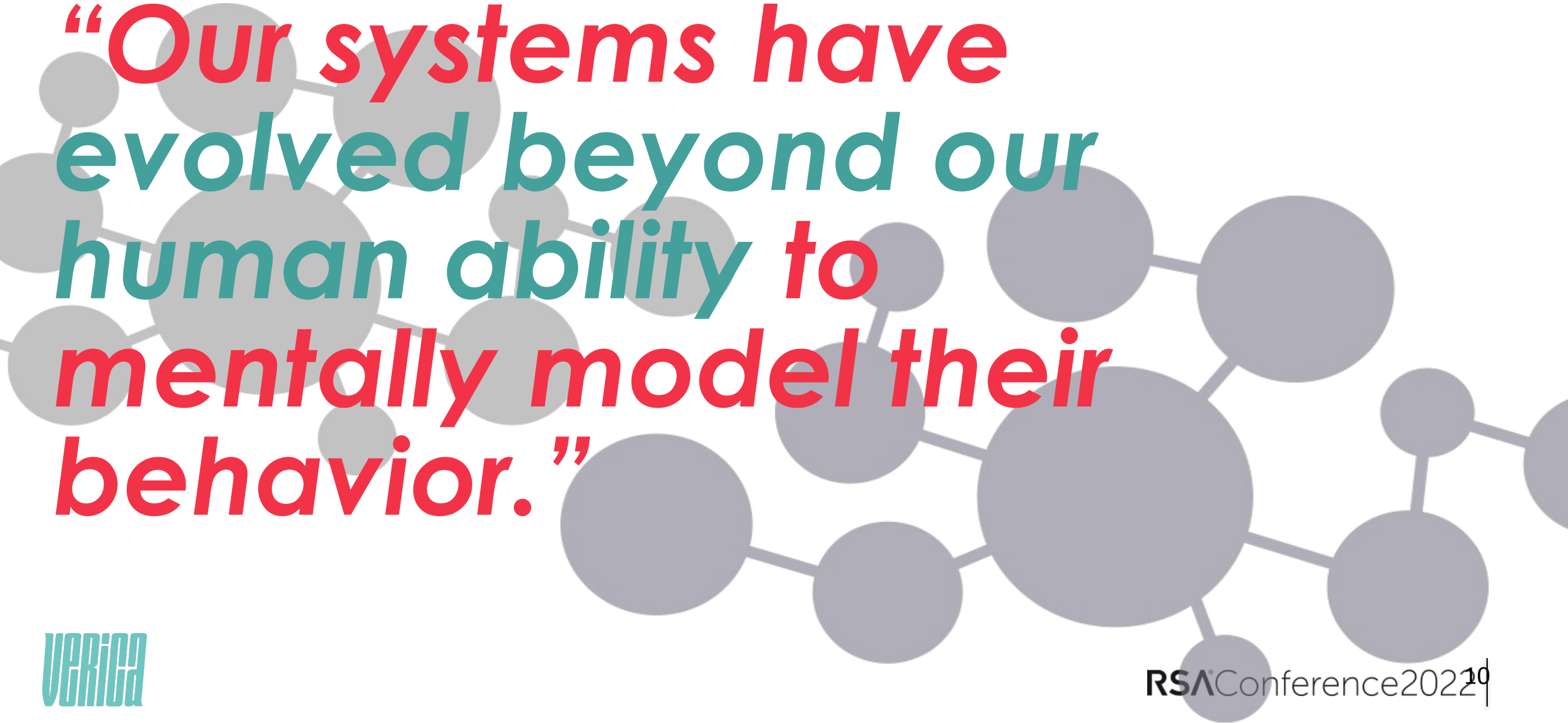




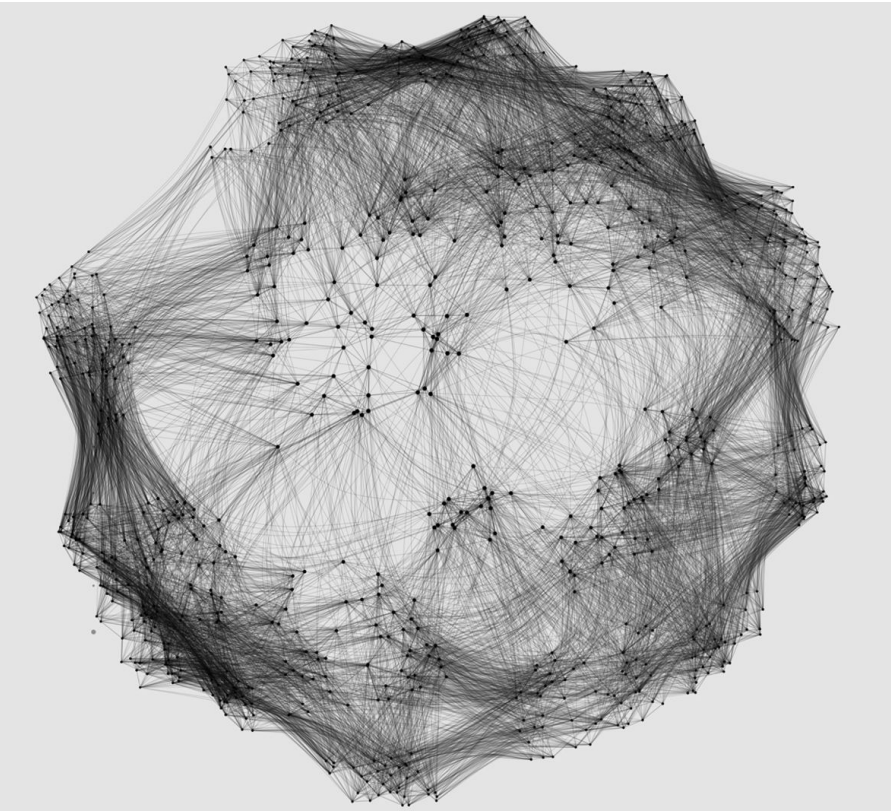
Change $\propto$ Complexity

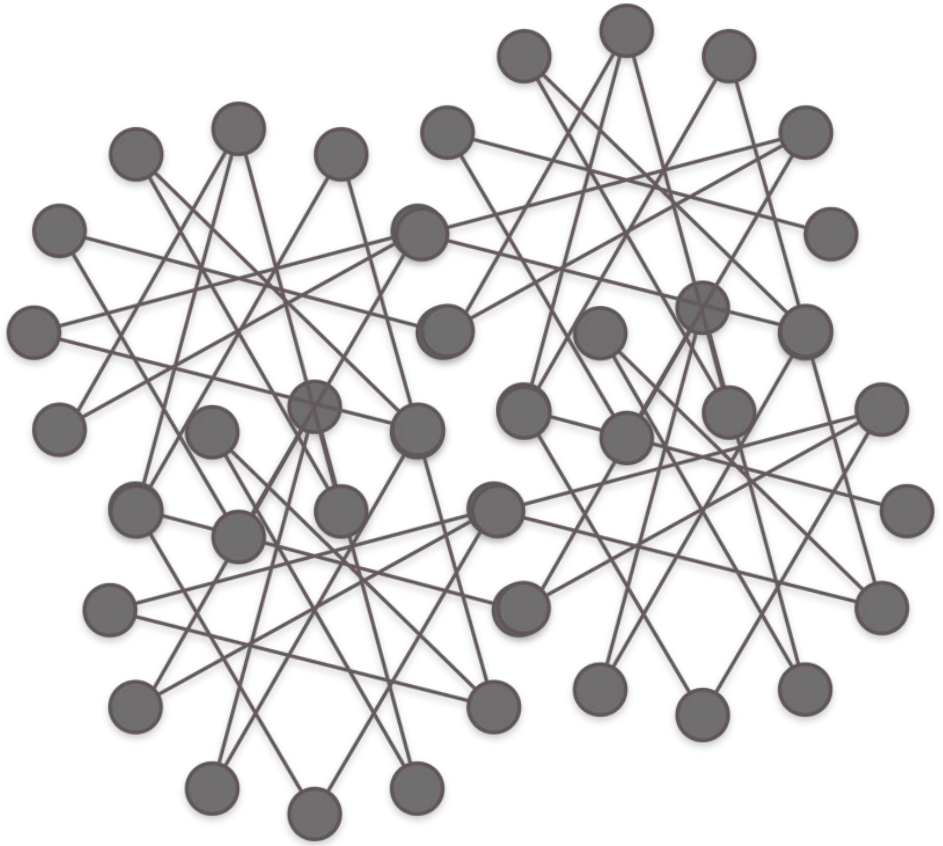
Complex Systems

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



Speed, Scale, & Complexity of Modern Software is Challenging





Where does it come from?

Continuous Delivery

Distributed Systems

Microservice Architectures

Blue/Green Deployments

Containers

Automation Pipelines

Auto Scaling

Infracode

Immutable Infrastructure

DevOps

Continuous Integration

CI/CD

Service Mesh

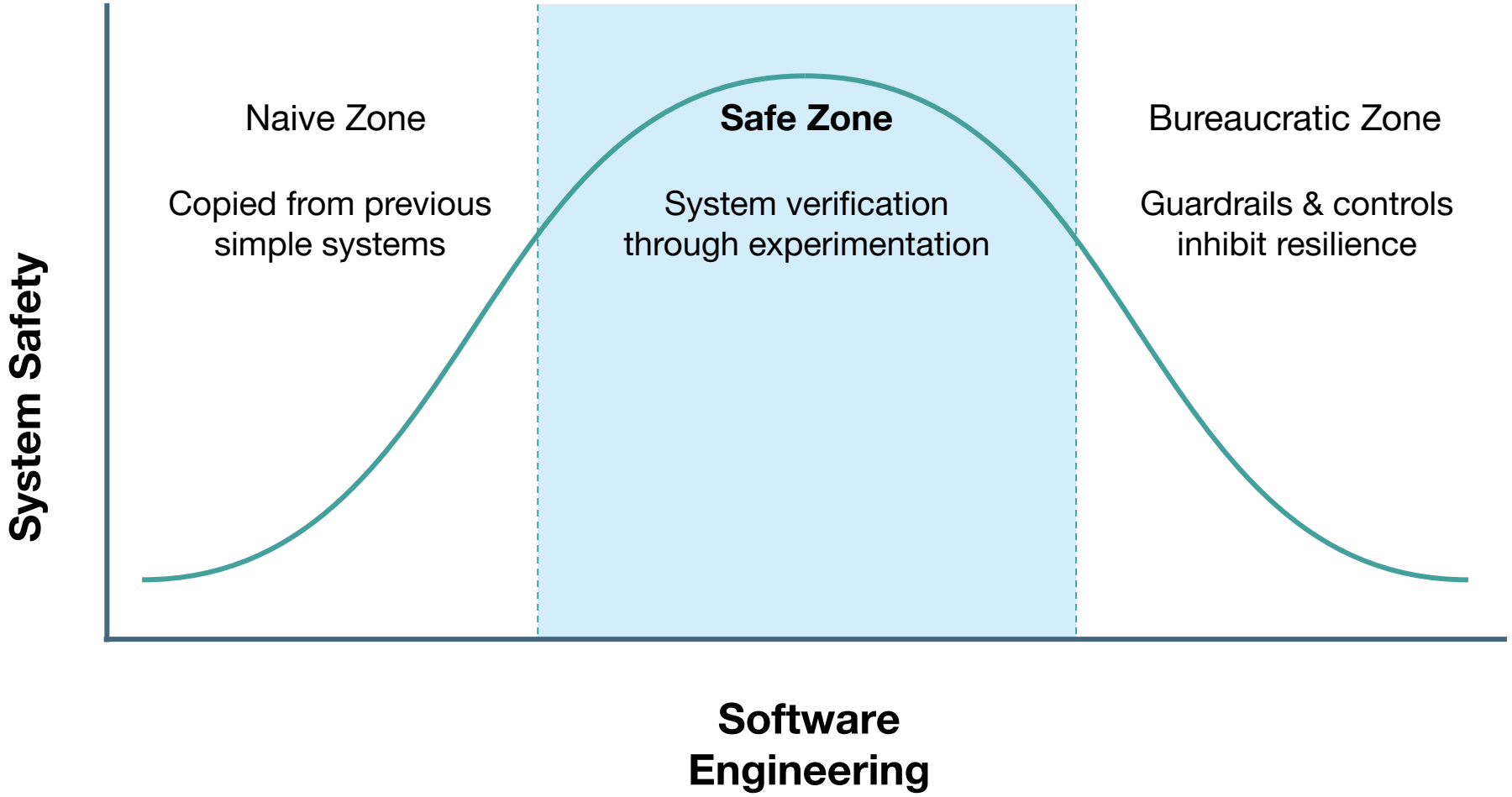
Auto Canaries

Cloud Computing

Circuit Breaker Patterns

API

Safety Margin in Complex Systems



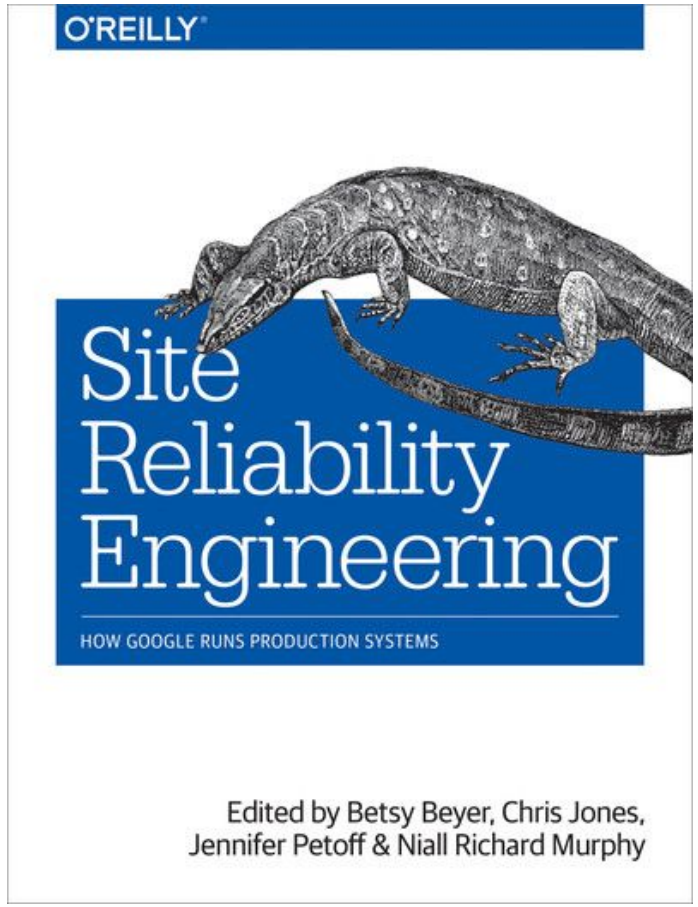
RSAConference2022

Site Reliability Engineering (SRE)

This IS SRE defined

SRE is an organizational model for running reliable online services by teams that are chartered to do reliability-focused engineering work.

As a discipline, SREs are devoted to helping an organization sustainably achieve the appropriate level of reliability for its services by implementing and continually improving data-informed production feedback loops to balance availability, performance, and agility.



VERICA

The Success in Security & SRE is Silent

Security & Reliability

Are NOT *Default Properties* of a System

They Are Human Constructed

No system is Perfectly Secure or Reliable


We need failure
to Learn & Grow

RSAConference2022

SRE and Security Share Common Struggles

Security & Reliability
Design Tension
Doing "It" Later

Doing it "Later"

The SRE & Security

"LATERGATOR"

The tendency for engineering teams to spend a lot of time deferring reliability and security design concerns to later points in the future. Usually justified for the sake of velocity and introducing potential delays into the release cycle.

There are many Tradeoffs Under Pressure


[adult swim]

James Wickett
@wickett

Totally unexplainable

10:46 AM · Jun 2, 2022 · Twitter for iPhone

Shallow Incident Data

If Grapes were described like computer outage post mortems.....

This bunch of grapes is 5.6 inches across at its widest point. The mean diameter of these grapes is 0.73 inches. The median color is 195/211/86 (RGB).

Reference: https://www.adaptivecapacitylabs.com/blog/2018/03/23/moving-past-shallow-incident-data/

Shallow incident data provides very little insight that can be used to understand critical elements of the story.....

How do they taste?

Reference: https://www.adaptivecapacitylabs.com/blog/2018/03/23/moving-past-shallow-incident-data/

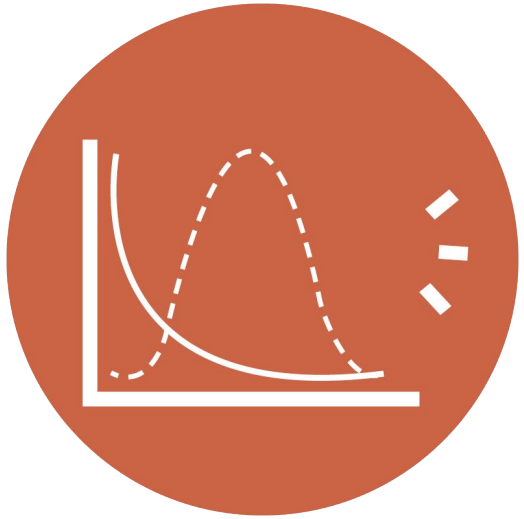
About the VOID

The Verica Open Incident Database (VOID) makes public software-related incident reports available to everyone, raising awareness and increasing understanding of software-based failures in order to make the internet a more resilient and safe place.

1,856 public incident reports from 610 organizations

WHY WE NEED THE VOID

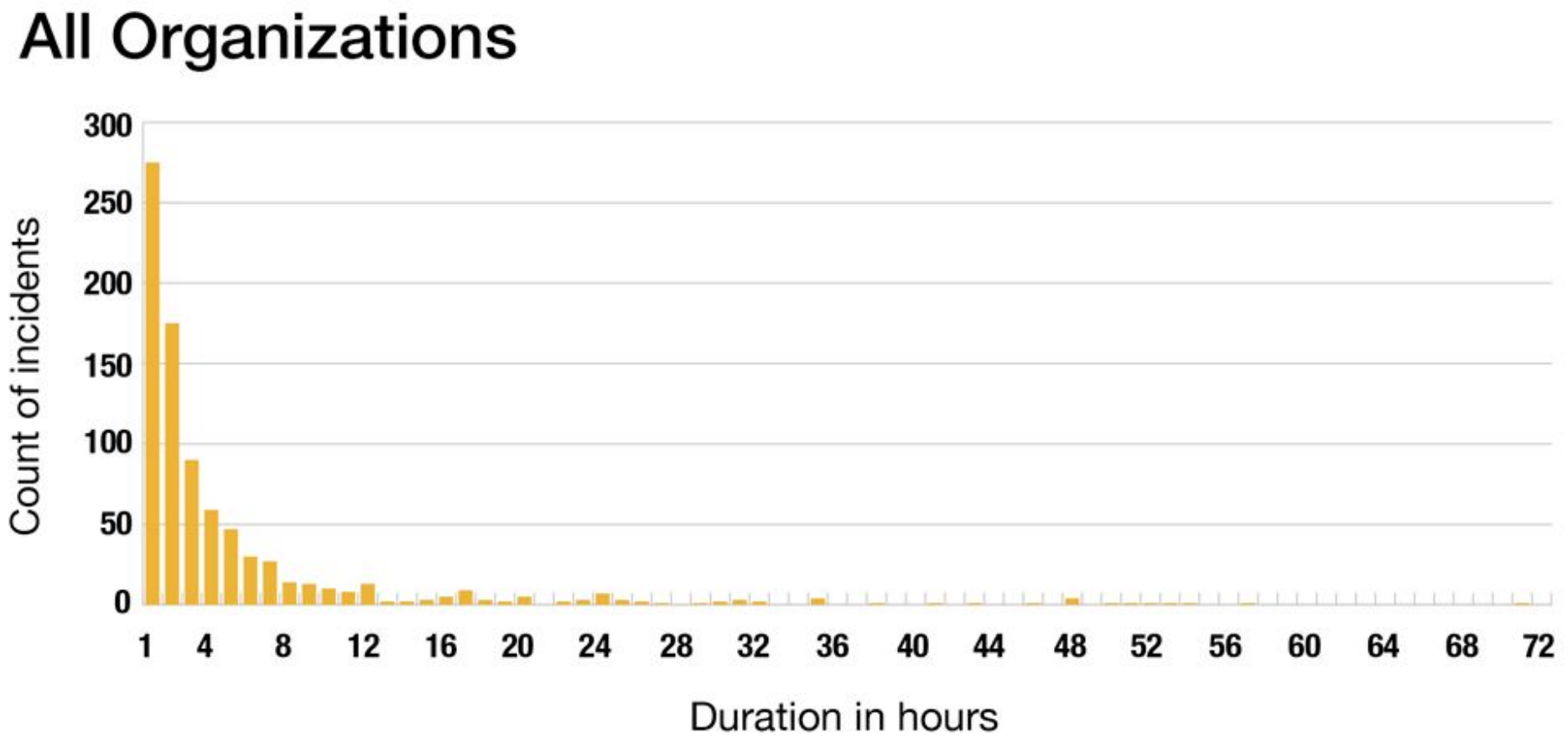
Accelerated Growth of Complex Systems



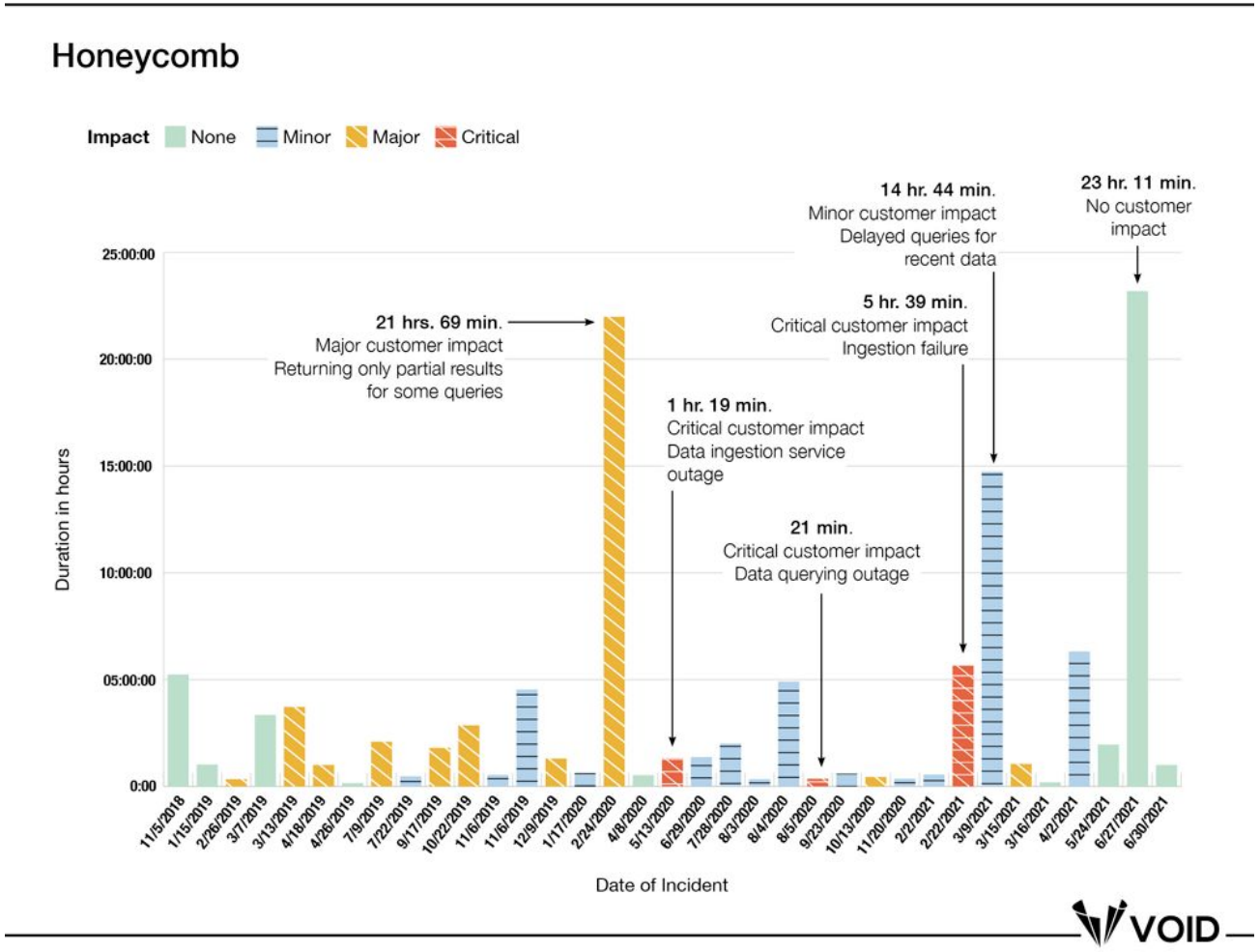
Incongruent Methods and “Best” Practices

People Seen As External Problems

Distribution of Duration Data in the VOID



But,Longer Incidents *Are* Worse, Right?



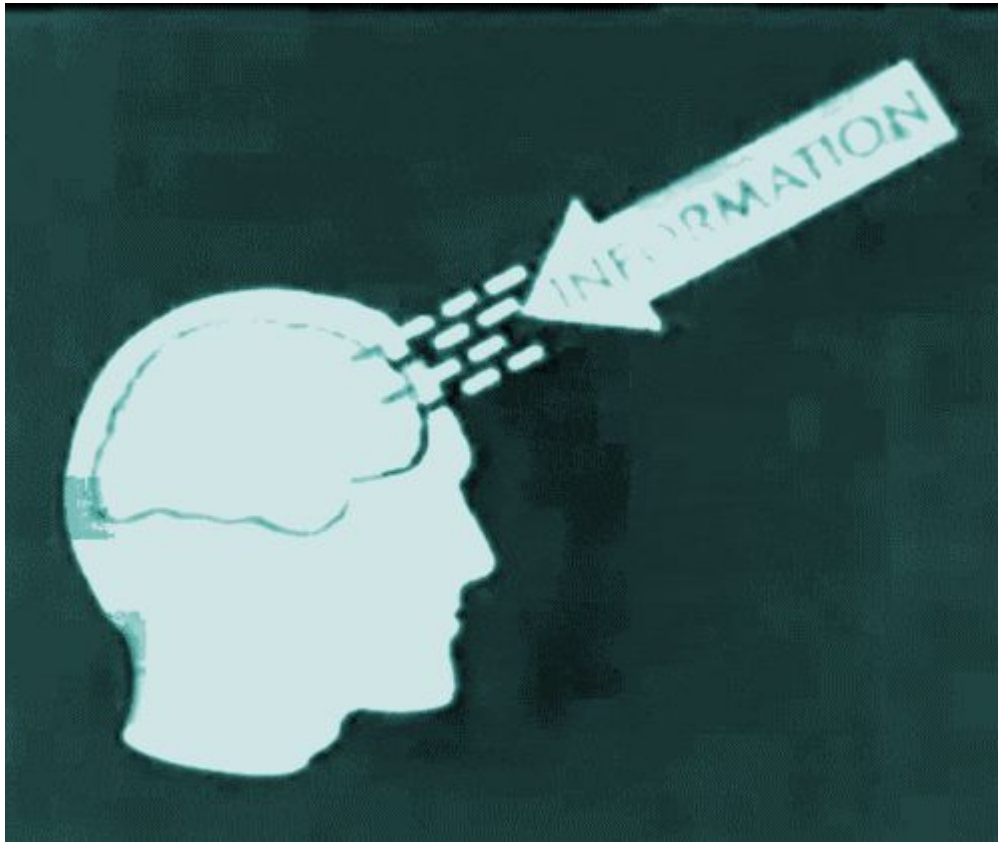
Security Observability

"After careful consideration of all 437 charts, graphs, and metrics,
I've decided to throw up my hands, hit the liquor store,
and get snockered. Who's with me?!"

RSAConference2022

Teamwork Patterns: The Do's

Context over Control

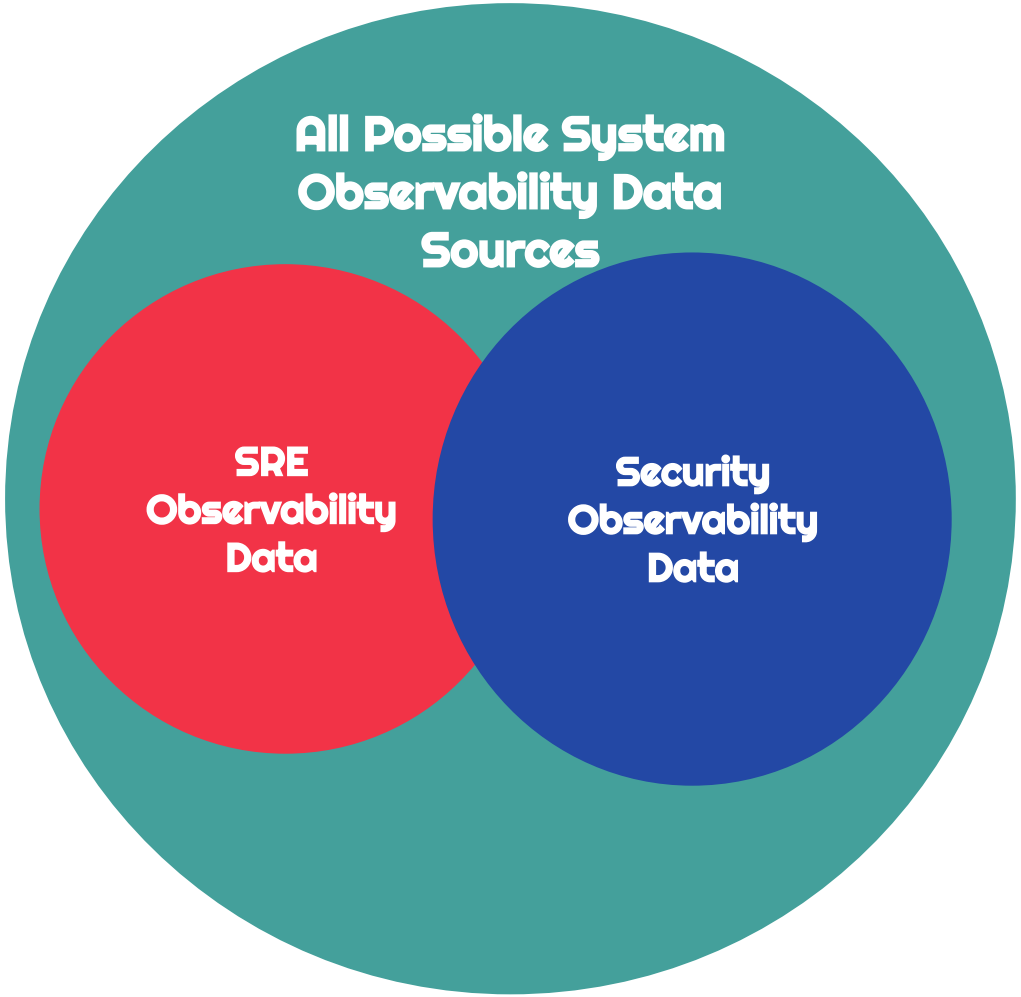


Learn to Communicate Effectively During Good Times if you Wish to Communicate Effectively During the Bad

Shared Observability

SRE

- Logs
- Metrics
- Tracing
- APM
- Testing



Security

- Logs
- Metrics
- Threat Intelligence
- Firewall Logs
- Security Scans

RSAConference2022

Teamwork Anti-Patterns: The Dont's

Everyday Life SRE & Security Anti-Patterns

- *Users shouldn't notice an outage before you do.*
- *Engineer solution to eliminate classes of errors rather than being satisfied with point fixes.*
- *Don't feed the machine with human toil.*
- *Failure is an opportunity to improve, not brandish pitchforks.*

Referenced from ADDO Session by Jennifer Petoff, Google Director of SRE Education on Everyday Life SRE Anti-Patterns

Root Cause is a Fallacy

Security Quick Fixes: A Double Edged Sword

The Blame, Name, & Shame Game

Poorly Documented Incidents

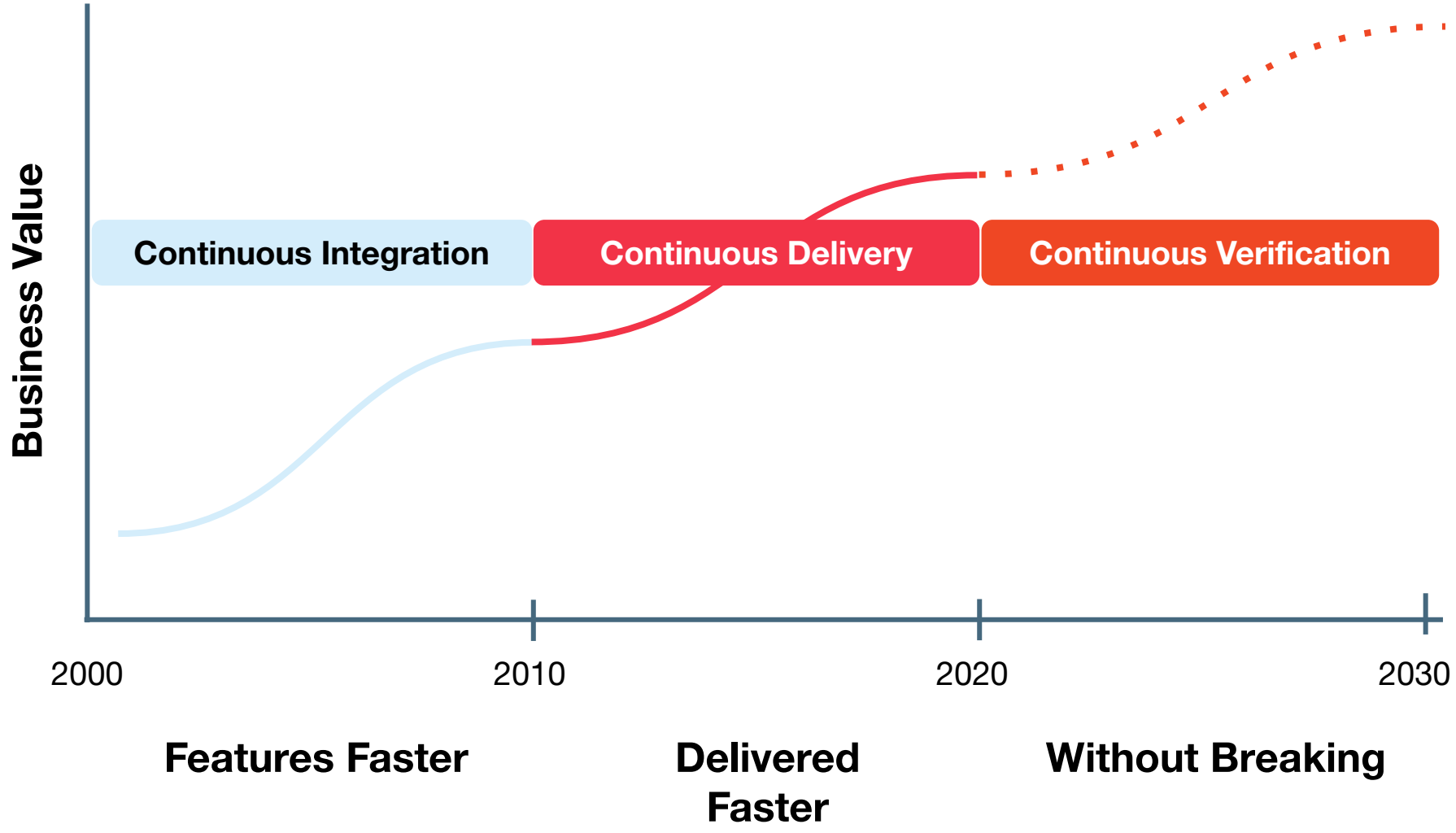
"The easiest way to remove motivation is to put paperwork in front of it."

- Casey Rosenthal

RSAConference2022

Tools & Techniques: What Works

Evolution to Continuous Verification



How to grow Continuous Verification

Equip leaders to make decisions about complex systems

Business Outcomes

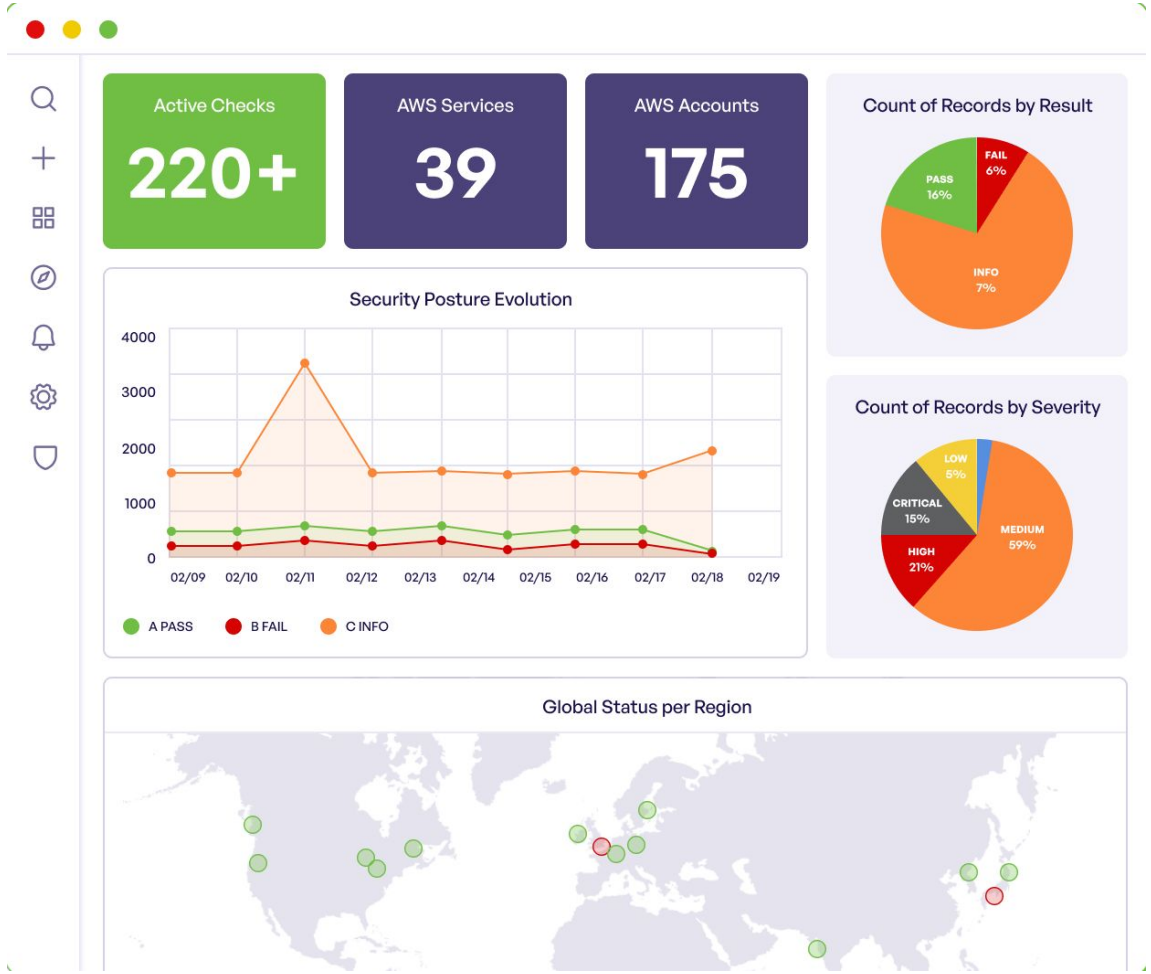
Verify infrequent code paths and properties of the system

Application

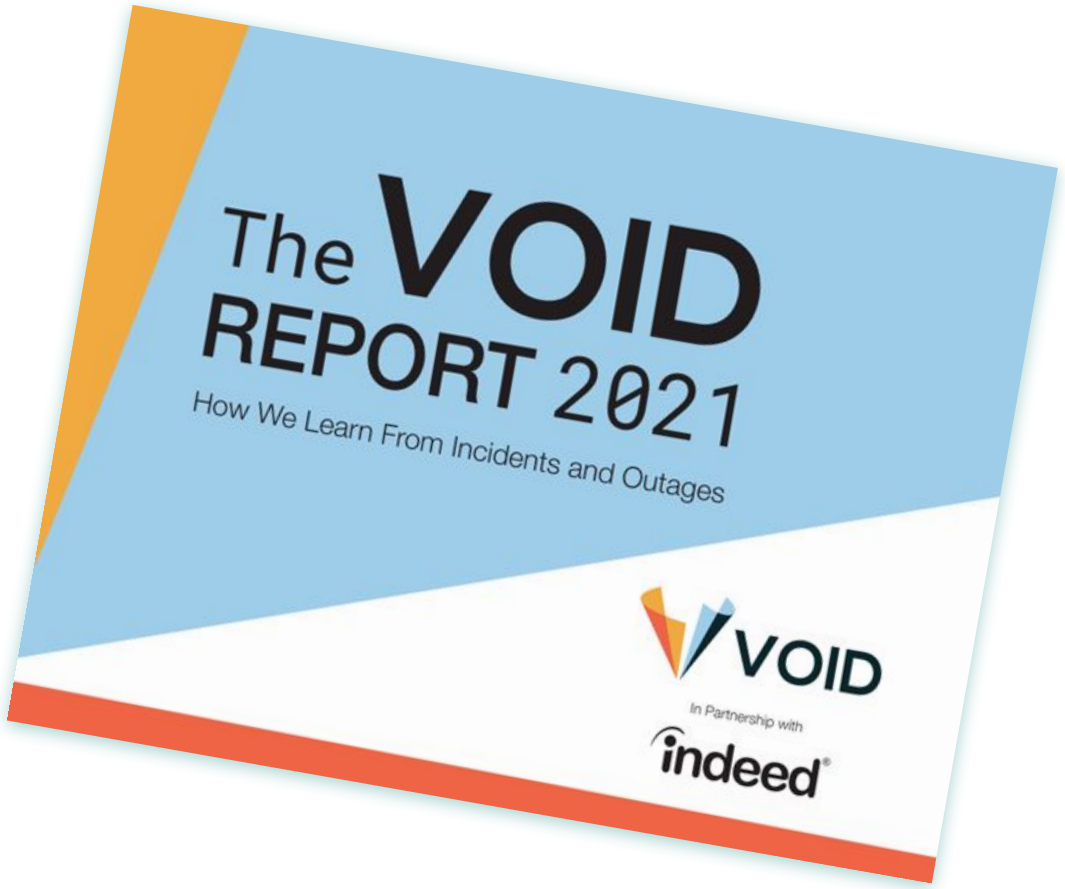
Learn how infrastructure impacts customer experience

Infrastructure

Paved Path for Devs with No Cloud Security “Surprises”



https://github.com/prowler-cloud/prowler



https://www.thevoid.community/report

A New Approach from the VOID

1. Treat Incidents as Opportunities to Learn
2. Favor In-depth Analysis Over Shallow Metrics
3. Treat Humans as Solutions, Not Problems
4. Study What Goes Right Along With What Goes Wrong

Measure Impact and Reaction instead of MTTR

Contributing Factor Investigation instead of Root Cause Analysis

Apply What You Have Learned Today

- Next week you should:
  - Find out if you have an Site Reliability Engineering function at your organization
- In the first three months following this presentation you should:
  - Understand the role of SRE in your organization
  - Seek to understand how Security can work to improve SRE and Vice Versa
- Within six months you should:
  - Begin implementing changes to improve common SRE & Security problem ares such as shallow incident data, poorly documented incidents, shared observability and improved incident management practices.
  - Begin exploring the adoption of some of the SRE & Security techniques in this presentation such as Blameless Postmortems, Chaos Engineering and Decision Trees
  -

SRE & Security Hot Takes

These are NOT the Droids You Are Looking for

Observability != Monitoring

Root Cause Is A Fallacy

Chaos Engineering = Fixing NOT Breaking

Resilience != BCP/DR

Complexity CANNOT Be Simplified Away

DevOps IS NOT SRE

SRE IS NOT DevOps

The "S" in Security & SRE is Silent

Favor Context OVER Control

Complexity != Enemy of Security

Security Chaos Engineering != Penetration Testing

Humans ARE NOT the Problem

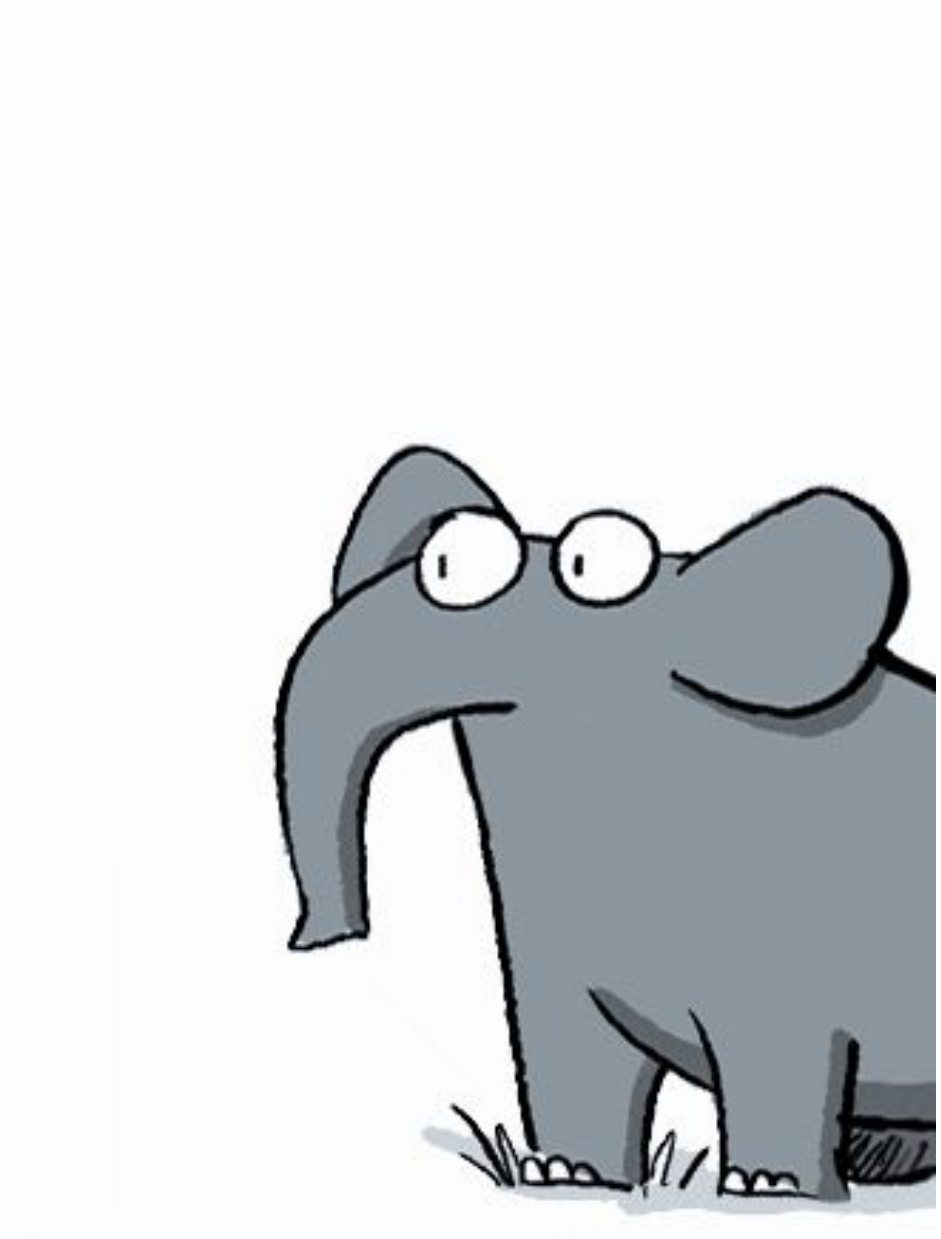
Guardrails = Incident Handcuffs

Understandability IS MORE IMPORTANT Simplicity

Humans ARE the Solution

VERICA

Q&A



Thank You!

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

– John Allspaw

SECURITY CHAOS ENGINEERING

ChaoSlingr

An Open Source Tool

Hypothesis:

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