RSAConference2020
Asia Pacific & Japan
A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: DPS-W06

Building Safety, Security and Resilience through Chaos

Jerome Walter
Director, Security Modernisation
VMWare
@jwalter_sec

Aaron Rinehart
CTO, Founder
Verica
@aaronrinehart

Jerome Walter,
Security Modernisation Director, VMware

- ***Digital Native***
- ***Engineering and Business studies***
- ***Former developer, SysEng, IT Manager***
- ***Former CSO @Natixis***
  Former Head of Security Arch. @Prudential
- ***Field CISO @Pivotal, now VMware***
  - Security Modernisation Advisor -
- ***On a personal journey to fix security***

VERIS vmware®

@jwalter_sec

/in/jwalter

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

Our organisations are under pressure

New technologies & patterns	Fixed Disaster Recovery Plans (DRP)
Fast iteration towards an unknown future	Risk assessment & standard-based blueprints
Lean planning	Protective security added around applications
Experiential culture	Policy violation & compliance culture

"The ability to resist, absorb, recover from or adapt to a change in conditions"
[DHS]

Robustness

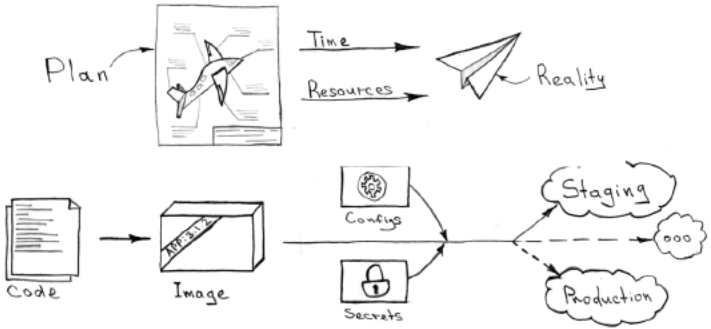
"[...] dependability when facing changes"
[Laprie]

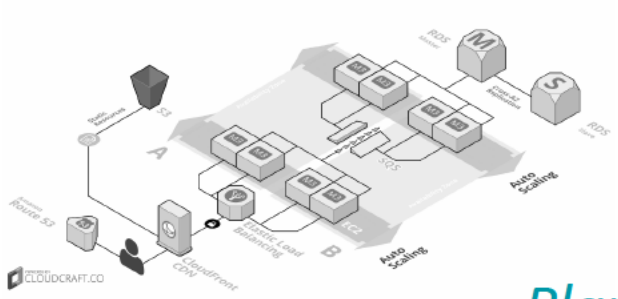
Resilience

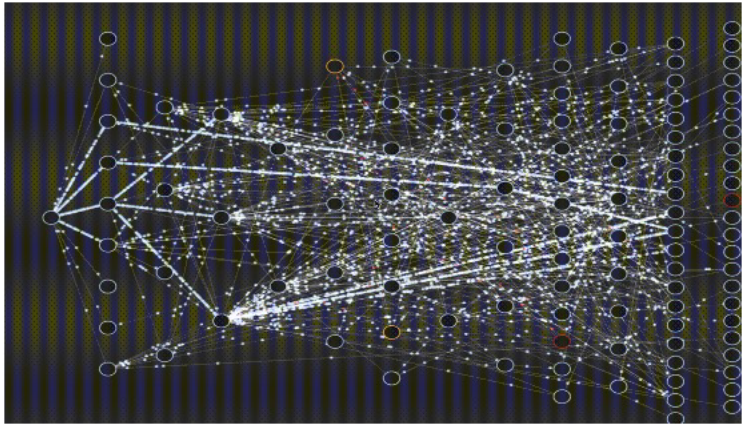
"flexibility of people and organisations, not just in reacting to individual incidents [...], but also in learning from them and thus developing an ability to react..."
[Strigini]

Recovery

We have developed flawed perceptions of our systems



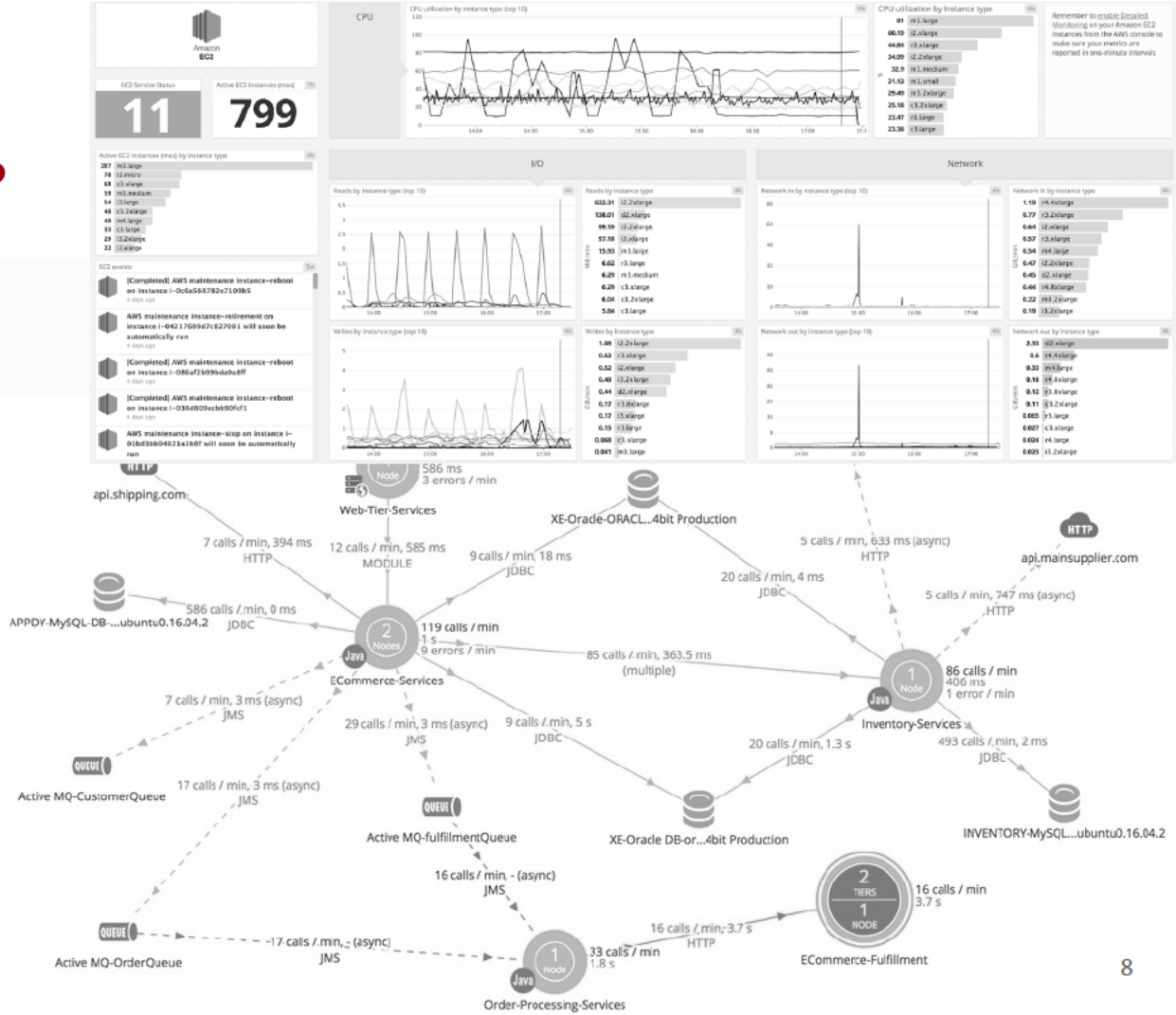




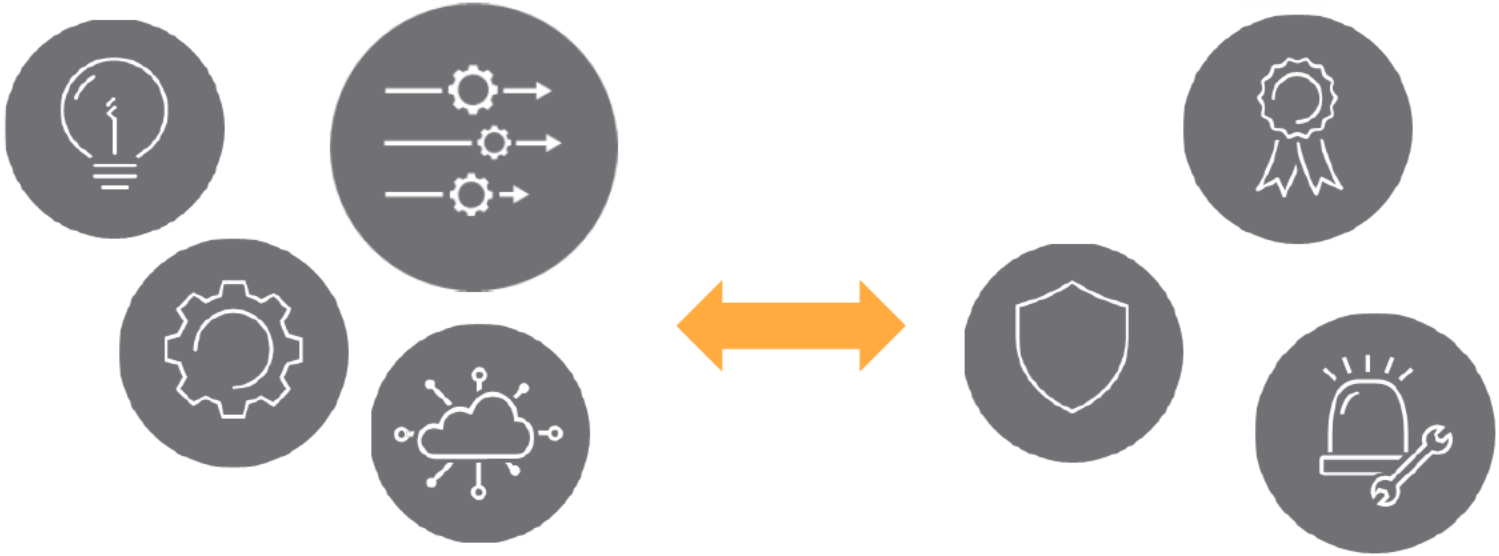
Plans vs Reality

These models do not do not resist the test of time

Our systems have become more complex and messy than we remember them



This division is also palpable in our organisations



Builders vs Defenders

RSAConference2020 APJ

A Virtual Learning Experience

The New Playbook:

Modern practices in building highly resilient and secure systems

DIE for Resilience

IDEAS for Security

5 cloud-native principles transform security and resilience

5 cloud-native attributes transform security and resilience

Immutable	Distributed	Ephemeral	Authenticated	Segmented
• Declarative programming • Increases consistency and predictability • Reduces insider threat & increases auditability • Facilitates state reconciliation	• Increases fault tolerance and resilience • Facilitates zero-downtime changes and patches • Facilitates state reconciliation	• Ensures code in prod is aligned with repository • Reduce window of opportunity for attack escalation • Reduce risk of credential misuse • Facilitates incident response	• Enforces Zero trust Model • Reduces exposure of all assets and risk of known vulnerabilities • Reduces risk of unauthorized workloads • Increases auditability	• Loosely coupled applications • Declarative network policies • Segmentation per domain / product • Reduces blast radius of errors and attacks

The new challenge:

Declarative programming & State Reconciliation

State Reconciliation

- Tools: Cloud Native
  - Kubernetes, PaaS, FaaS, Buildpacks.io
  - Chef, Puppet, Bosh, Ansible, Terraform…
  - Cloud-Native security, Compliance-as-Code
- Practices
  - Declarative programming & workload profiling
  - Repaving
  - Chaos Engineering

New cyber-security and resilience hygiene practices: 3Rs

Repair

Repair software as soon as vulnerabilities or flaws are discovered

Repave

Repave servers and applications from a known good state. Do this often

Rotate

Rotate user credentials frequently, so they are only useful for short periods of time

Reduce Your MTTR | Resist Advanced Persistent Threats | Reduce Leaked Credential threat

RSAConference2020 APJ

A Virtual Learning Experience

A Change in Mindset

@aaronrinehart @verica_io #chaosengineering

Hot Take:

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

VERICA vmware

RSAConference2020 APJ

A Virtual Learning Experience

Chaos Engineering

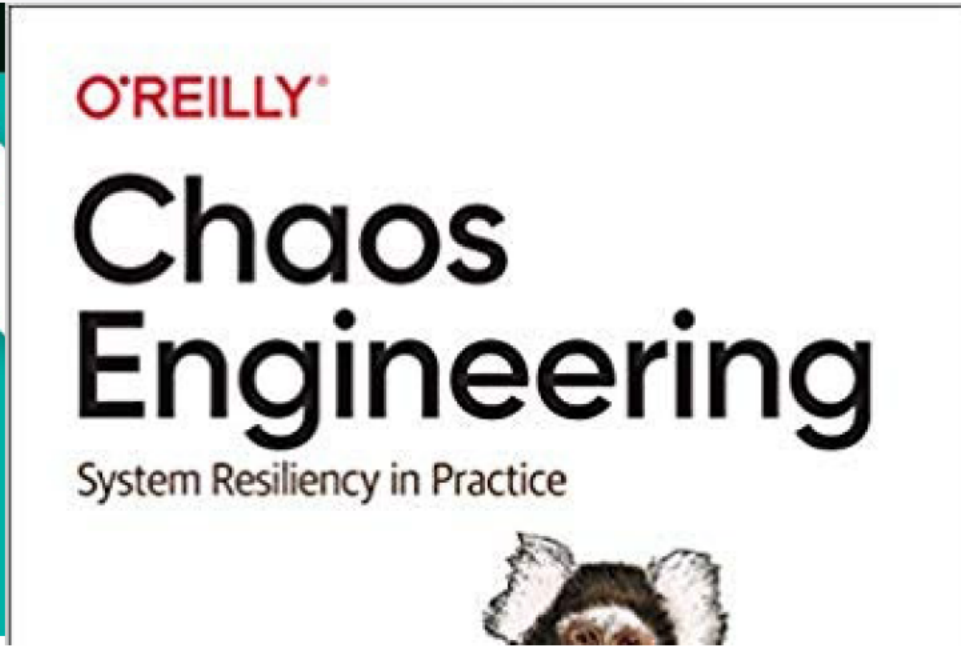
@aaronrinehart @verica_io #chaosengineering

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?


O'REILLY®
Compliments of
NETFLIX
Chaos
Engineering
Building Confidence in System Behavior
through Experiments


O'REILLY®
Chaos
Engineering
System Resiliency in Practice

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

RSAConference2020 APJ

A Virtual Learning Experience

Security Chaos Engineering

@aaronrinehart @verica_io #chaosengineering

Hope is Not

an Effective Strategy

"It worked in Star Wars but it won't work here"

Continuous Security Verification

Reduce Uncertainty by Building Confidence in how the system actually functions

Proactively Manage & Measure

Use Cases

Use Cases

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

Incident Response

"Response" is the problem with incident response.

Security Incidents are Subjective in Nature

No matter how much we prepare...

We really don't know very much

Where?

Why?

Who?

How?

What?

Lets Flip the Model

Post Mortem = Preparation


OMG!
What are your robot serial numbers?

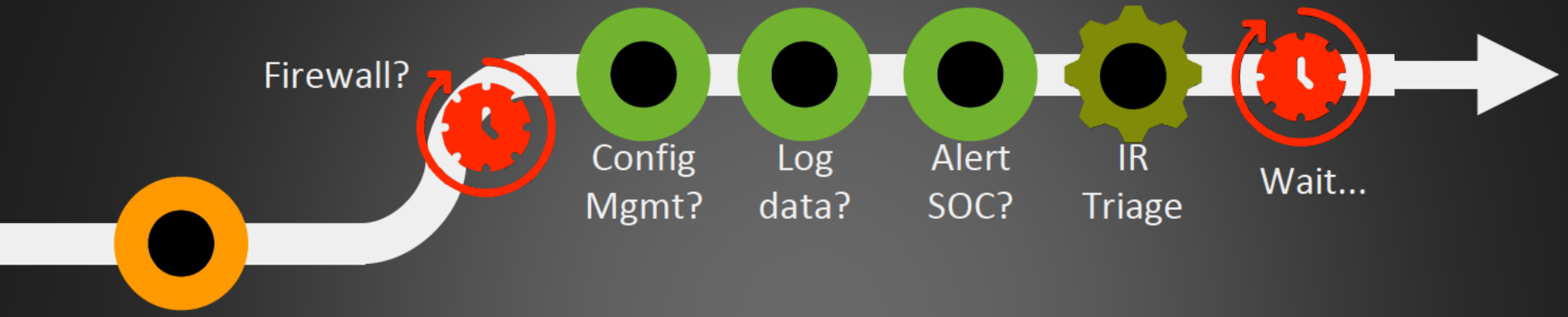
ChaoSlingr

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.

Takeaways

- Security by Design w/ IDEA & DIE
- Security Chaos Engineering provides proactive verification of how our security actually functions.
- Instrument your Security before someone else does
- Resilience is not what a system has, its something that a system has.

Apply it Forward

- **Next Week:**
  - Share this concept to your team
  - Find out if your organisation has Site Reliability Engineering, and discuss potential exercises for security
- **Next 3 Months:**
  - Get a copy of the official O'Reilly Book on Security Chaos Engineering
  - Review your user facing applications and assess your ability to repave without downtime and rotate secrets
  - Pick an application and a scenario and conduct your first GameDay exercise
- **Next 6 Months:**
  - Run your first automated Chaos Experiment for security

RSAConference2020 APJ

A Virtual Learning Experience

Questions & Answers

@aaronrinehart @verica_io #chaosengineering