

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center



#RSAC

SESSION ID: CSV-W04

ChaoSlingr: Introducing Security-Based Chaos Testing

Aaron Rinehart

Chief Enterprise Security Architect
UnitedHealth Group

Grayson Brewer

IT Security Consultant
UnitedHealth Group

Security + Chaos = Security Experimentation



About Aaron

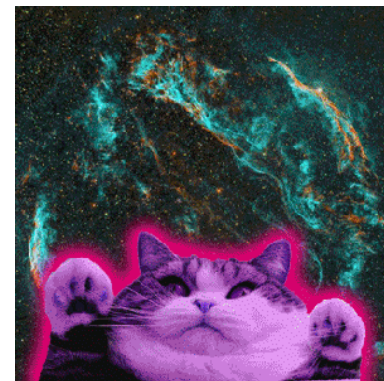


Aaron Rinehart
Chief Enterprise Security Architect
UnitedHealth Group

Contact Info
Rinehart.Aaron@gmail.com
@aaronrinehart



I'M FREAKING
MEOWGICAL



About Grayson



Grayson Brewer
Security Consultant
UnitedHealth Group

Contact Info
e.grayson.brewer@gmail.com
@BrewerSecurity



5



Overview UnitedHealth Group



UNITEDHEALTH GROUP®

THE CHALLENGE: WE ARE LARGE & COMPLEX

- Fortune 6 Company
- 360+ Companies & Growing
- 28,000+ Developers
- 8,000+ Applications
- HIPAA, HITRUST, FISMA, MARS-E, GDPR, ICFR(++++++)
- United Nations of Technology
- Largest HealthCare Company in World
- 1000+ Security Professionals
- Multinational Business
- Some DevOps
- Waterfall, Agile, & Others
- Security Testing: Mostly Human Driven
- Cloud Journey: Mixed



A Tool to Build or a Weapon to Destroy?



The Reality is.....



FAILURE HAPPENS.

Saturday, January 13



EMERGENCY ALERTS

now

Emergency Alert

BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

Slide for more

Failure is Necessary



HUMANS
NEED FAILURE
TO LEARN &
GROW



The background of the slide is a complex, abstract image. It features a dense arrangement of small, 3D rectangular blocks in shades of yellow, orange, and blue. These blocks are arranged in a way that creates a sense of depth and movement. In the center of the image, there is a dark, swirling vortex or spiral that draws the eye towards the middle. The overall effect is one of a dynamic, almost architectural landscape.

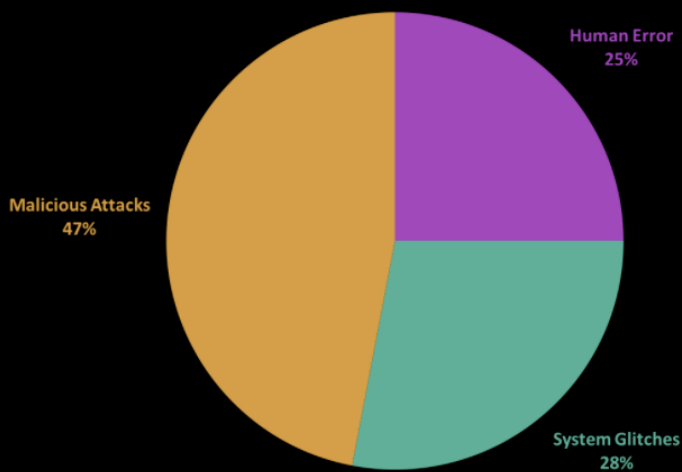
SO... WHAT DOES THIS HAVE TO DO
WITH SECURITY?

Revisiting the Problem



2017 CAUSES OF DATA BREACHES

DATA BREACH CAUSES



Where do Security Failures come from?



#RSAC



The Gap b/t Modern Software & Security



MODERN

SOFTWARE IS...

- HIGHLY DISTRIBUTED
- STATELESS
- ITERATIVE
- RAPID CHANGE EVOLUTION
- VERY COMPLEX

SECURITY IS...

- MOSTLY MONOLITHIC
- STATE DEPENDANT
- STATIC
- PREVENTATIVE DESIGN
- COMPLEX

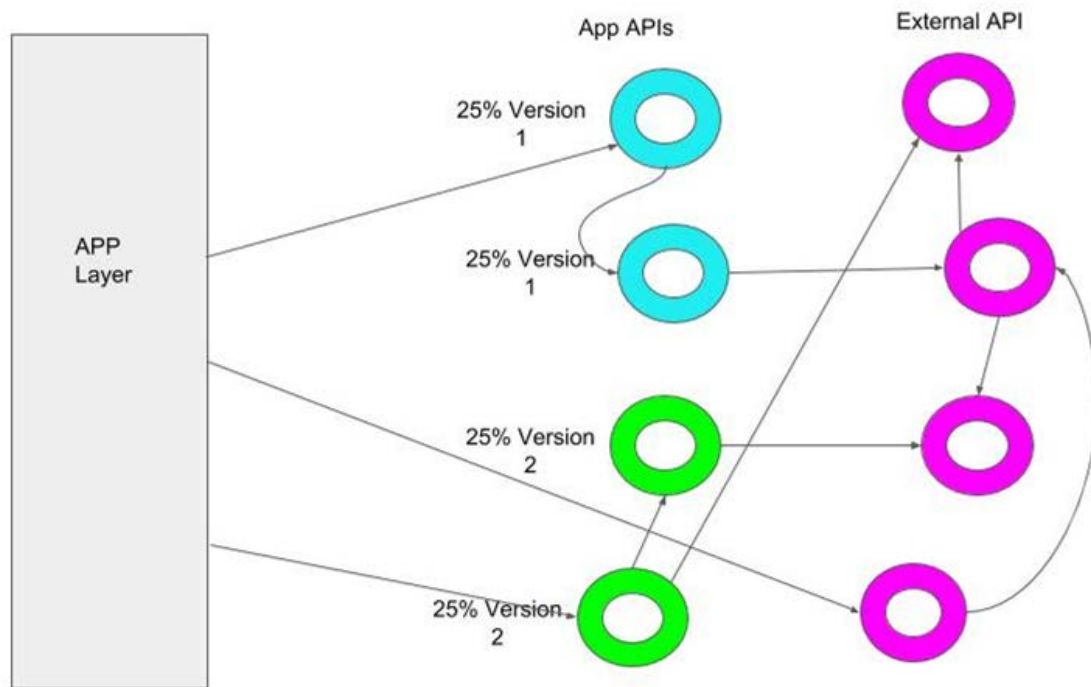
Distributed Systems Are Tricky



DISTRIBUTED SYSTEMS
CAN HAVE
UNPREDICTABLE
OUTCOMES



Distributed Systems Are Tricky



Don't Drift into the Unknown



HOW DO WE AVOID
DRIFTING INTO THE
UNKNOWN?

Ask Better Questions



DON'T LOOK FOR A BETTER ANSWER,
INSTEAD..

ASK BETTER QUESTIONS

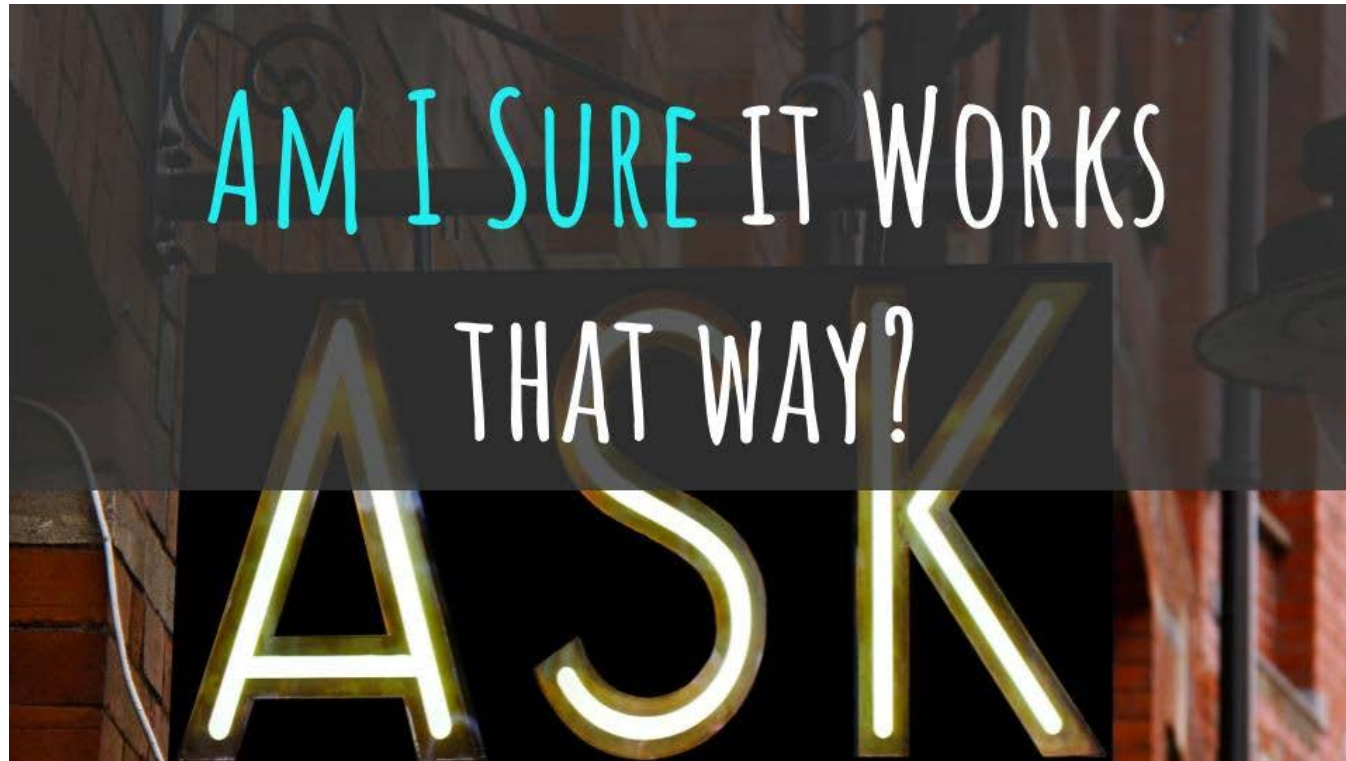
Ask yourself.....



HOW DOES MY SECURITY
REALLY WORK?

ASK

Ask yourself.....



Ask yourself.....



HOW WOULD I KNOW?

ASK

So in fact do we identify Security Failures?



LOGS???

SECURITY
SCANS??

PENETRATION
TESTS?
MONITORING
TOOLS???

SECURITY INCIDENTS!!!!

Its toooooo late.....



SECURITY INCIDENTS
ARE NOT
DETECTIVE MEASURES

It worked for Rebel Alliance but not here



Build Confidence through Instrumentation



BUILD CONFIDENCE
IN
WHAT ACTUALLY WORKS

What is 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"

A brief history of Chaos



#RSAC



NETFLIX



THE NEW PLAYBOOK

Security Experimentation



Do Less, Better



DON'T JUST TEST....EXPERIMENT



TESTING VS. EXPERIMENTATION

What's the Difference?



- **Testing** is assessment or validation of an **expected outcome**
- **Experimentation** seeks to derive new insights and information that were **previously unknown**

Security Experimentation: A Definition



"THE SECURITY DISCIPLINE OF EXPERIMENTATION IN
ORDER TO BUILD CONFIDENCE IN THE SYSTEM'S
ABILITY TO DEFEND AGAINST MALICIOUS
CONDITIONS."



Be Objective & Use Failure as a Tool



- **Drive** out failure.
- **Observe** failure.
- **Learn** from failure.
- **Build** resilient systems.

Build a Learning Culture



*"WOW, I WASN'T EXPECTING **THAT** TO
HAPPEN."* - YOU, LEARNING SOMETHING

Why do it?



- **Build Confidence** in Security Measures
- **Strengthen** Incident Management
- **Measure** Incident Response Readiness
- **Identify Security Failures** within the Security Control Plane
- **Proactively Detect** Security Failures
- **Measure Investments** in Security Technology

GameDays + Post Mortem



Value of Game Day Exercises



- Provides Objective Measurement for Security Incident Response
- Identify Control Coverage Gaps
- Keeping the Team Sharp and “Battle Ready”
- Learn how your Security Really Works vs. How you Assume it Works.

*“If you’re not cultivating **a Learning Culture**, you will probably end up losing to someone else who is.”*

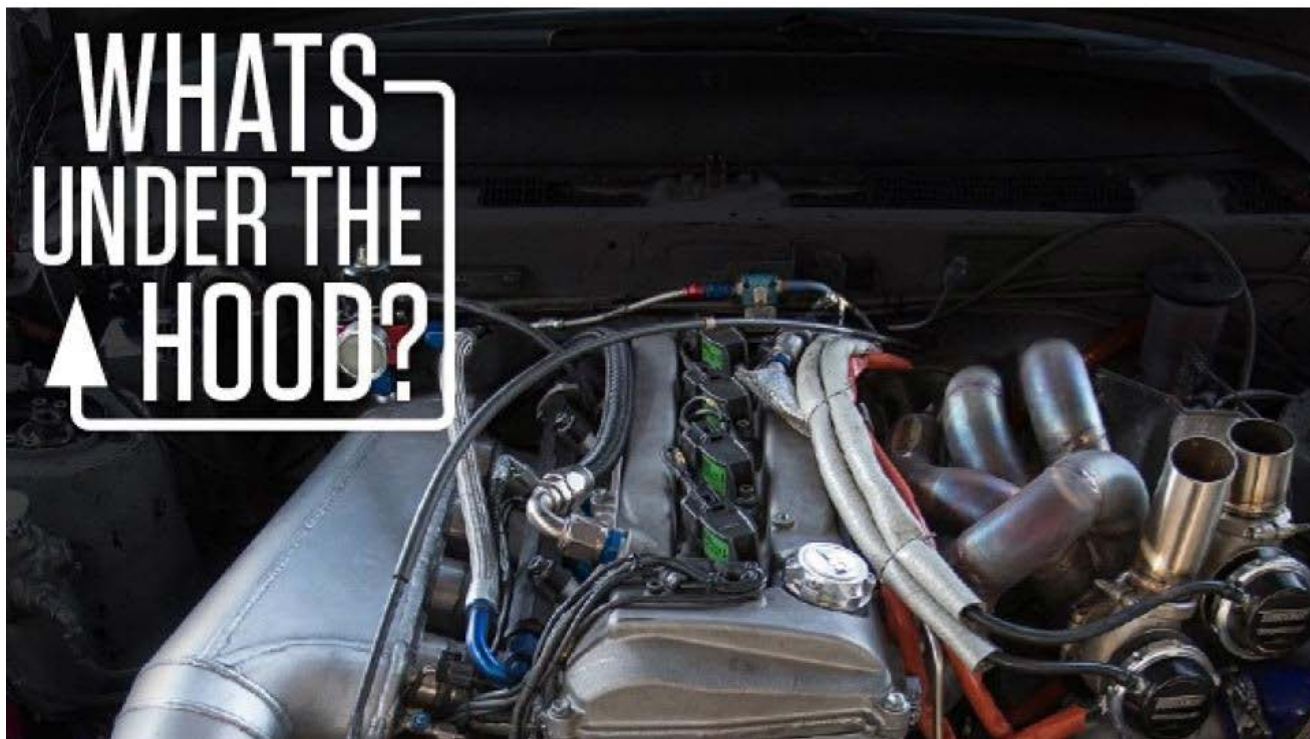


ChaoSlingr

AN OPEN SOURCE TOOL

40

So, eh, what is it exactly



FYI ChaoSlingr is on Github (FREE!)



- 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



HashiCorp
Terraform





PortSlingr

EXAMPLE CHAOSLINGR EXPERIMENT

UNAUTHORIZED
PORT CHANGE

An Example Security Experiment



EXAMPLE: UNAUTHORIZED PORT CHANGE

- 1 List Available EC2 VPC **Security Groups** within Account
- 2 **Select only** those Security Groups that are "Tagged" with the **Opt-In Tag** for Chaos Testing
- 3 Randomly Select a Security Group within the **Opt-In Model Pool**
- 4 Apply a Random **Open or Close Port Action** based on Existing Port Configuration

PortSlingr

How the experiment works



slingr



generatr



trackr



EXPERIMENT FRAMEWORK

Applies the configured **change**

Kicks off the experiment, Performs **Target Acquisition**, and **Stages Target** for changes

Tracks **changes made** by Generatr. Triggered by **monitoring** events that are monitoring for changes.

45

Summary: Takeaways



- Security Problems in Distributed Systems
- Chaos Engineering
- Security Experimentation
- ChaoSlingr: Open Source Tool
- Think Differently, Be Objective



Apply What You Have Learned Today



- Next week you should:
 - Start asking yourself the Right Questions
 - Go to Github and check out ChaoSlingr
 - Find out if your organization has an Site Reliability Engineer and tell them what you learned in this talk.
- In the first three months following this presentation you should:
 - Conduct your first GameDay Exercise and manual Security Chaos Experiment
 - Attend a Chaos Engineering Community Event near you
- Within six months you should:
 - Write your own experiments for ChaoSlingr or your own tool.
 - Run your first automated Security Chaos Experiment

The New Normal: Continuous Evolution



RSA[®]Conference2018

Hit us with some questions



Questions

@aaronrinehart
@BrewerSecurity

