RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CSV-W04

ChaoSlingr: Introducing Security-Based Chaos Testing

Aaron Rinehart
Chief Enterprise Security Architect
UnitedHealth Group

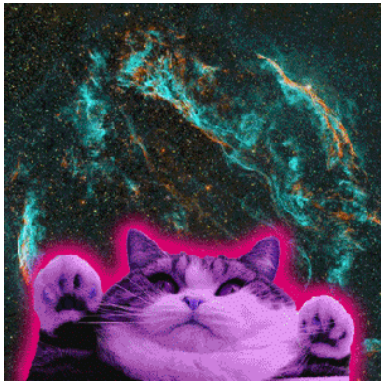
Grayson Brewer
IT Security Consultant
UnitedHealth Group

Security + Chaos = Security Experimentation

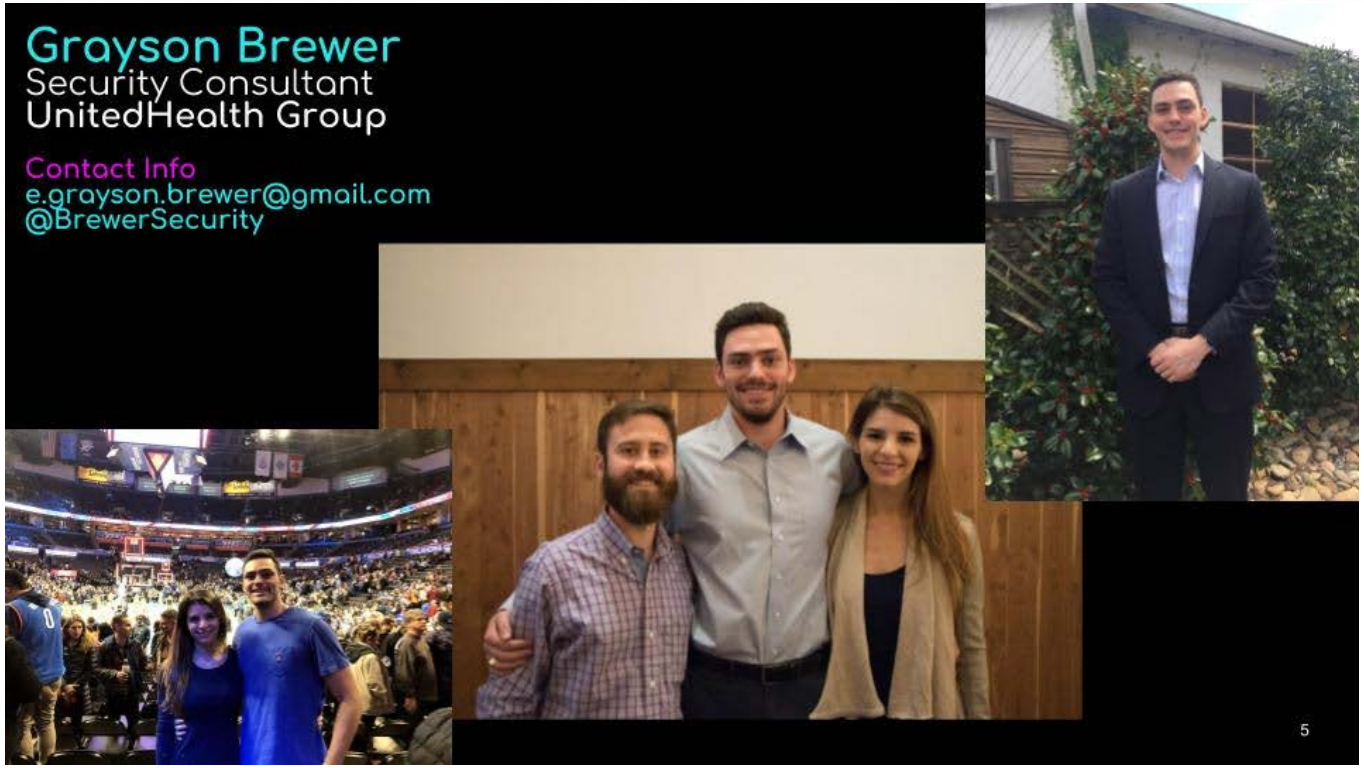
About Aaron

Aaron Rinehart
Chief Enterprise Security Architect
UnitedHealth Group

Contact Info
Rinehart.Aaron@gmail.com
@aaronrinehart



About Grayson



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

Outline


IN THIS SESSION WE WILL COVER
OBVERT
ACTIVITY
BAFFLING
MOVING
WISDOM
INSPIRE
GENESIS
PROTEAN
BECOMING
OBLIQUITY
EXPLORING
ASTONISHING
PHASE-SHIFT
ACTIVATING
OPPORTUNITY
DISORDER
VULNERABLE
EXPERIMENTING
HAPPENSTANCE
CREATIVE
CONSTRUCTIVIST
CURIOUS
GIVING
HACK
JUMP
NATURAL
PASSION
LIVING
CREATING
HUMOROUS
FORGIVING
JOCKEY
DREAMING
OFFSHOOTS
FLEXIBLE
IRREGULAR
LIFE
ENGAGEMENT
FLUCTUATING
GROWTH
DYNAMIC
AMAZING
ABANDON
GERMINATE
GENERATING
EXCITEMENT
PARTICIPATE
FRACTAL
BUILDING
FLUX
CHAOS
©JIMBRIGHT2012
CAN-DO
HUNCH
INTREPID
BOLD
CONFIDENCE
INVESTIGATE
DOING
BEING
JOLTING
FREELY
BRAVE
PLAYING
ENGAGING
EVERYDAY
AMBIGUITY
BREATHING
OPEN-MINDED
RE-THINK
OPPOSITIONAL
EXPERIMENTAL
JIG
ODDITIES
JAZZ
IMPROVISE
INVESTIGATE
LEFT-FIELD
CONNECTION
CHALLENGING

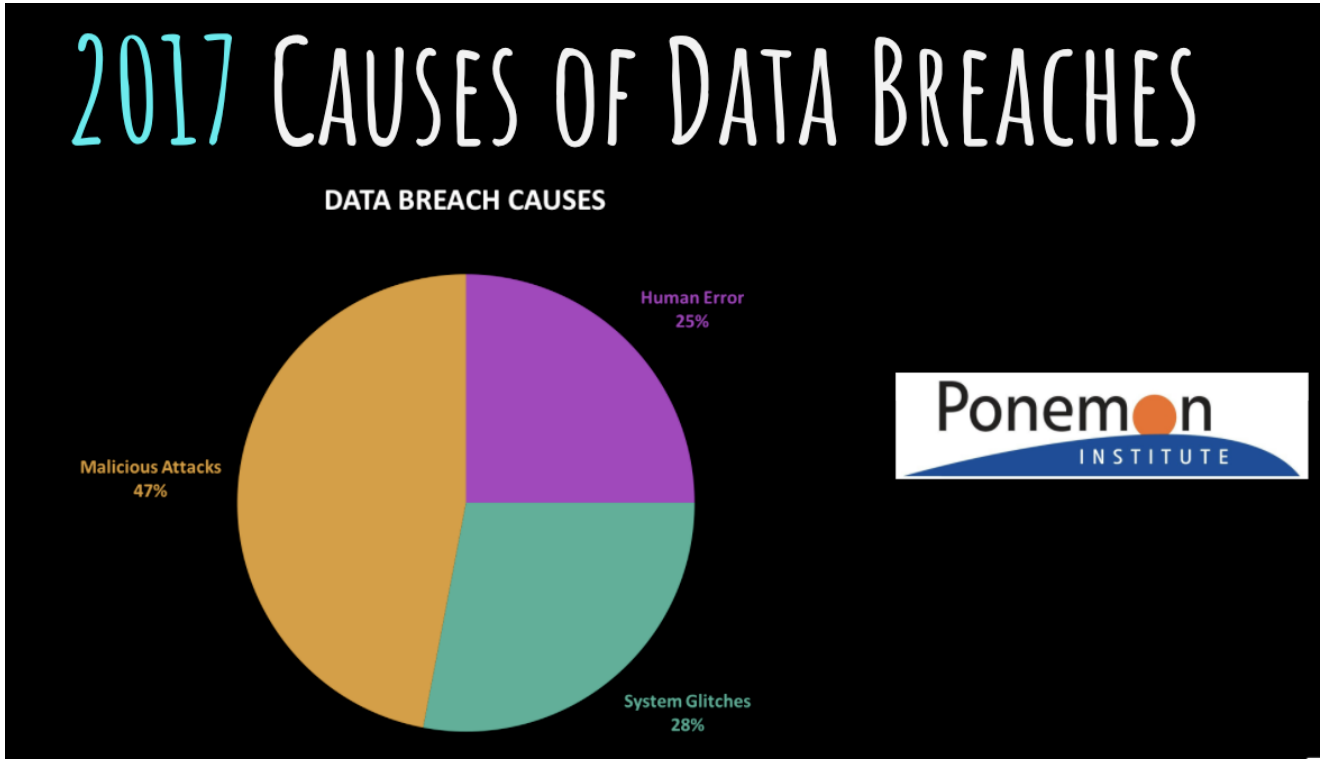
A Tool to Build or a Weapon to Destroy?

The Reality is……

Failure is Necessary

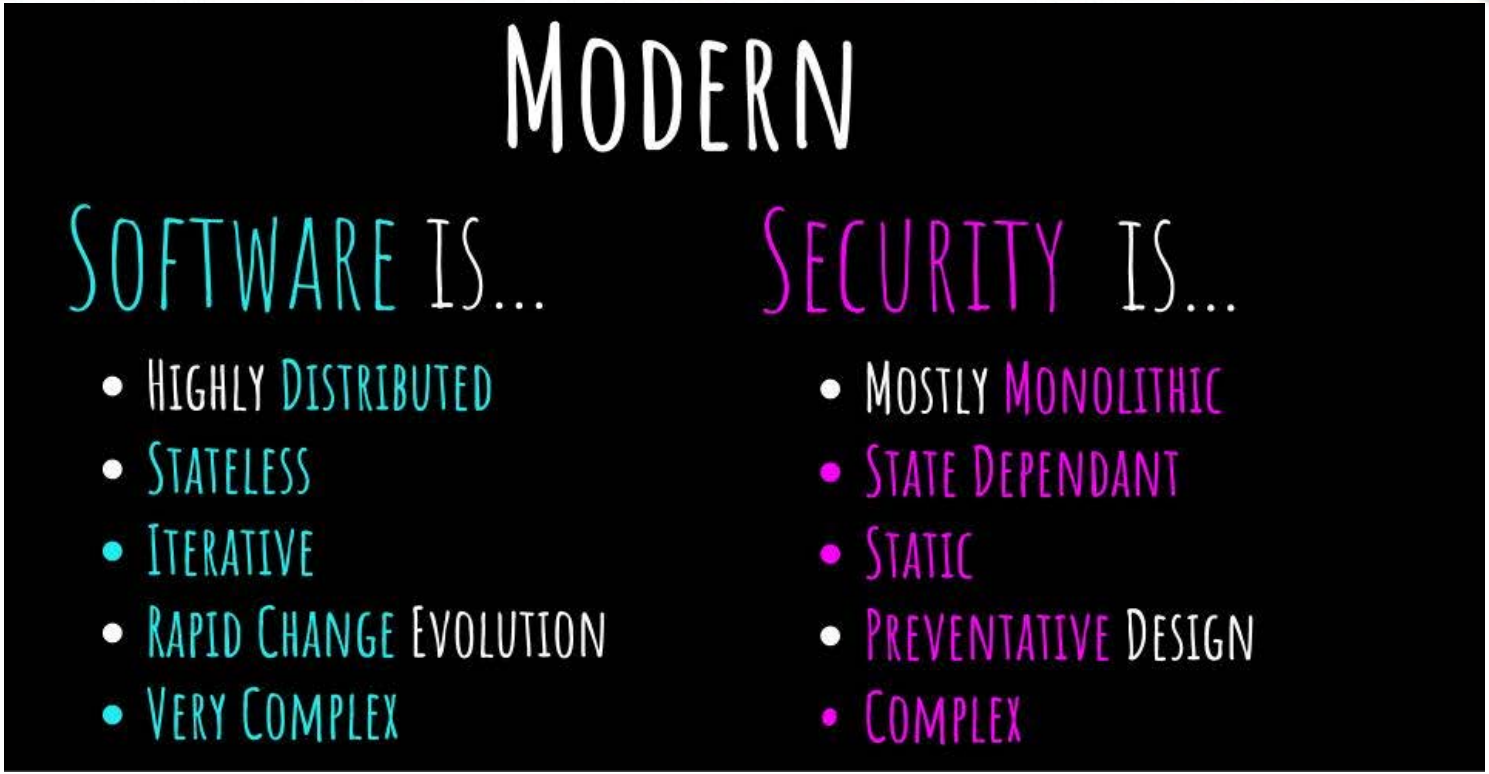

So...what does this have to do with Security?

Revisiting the Problem



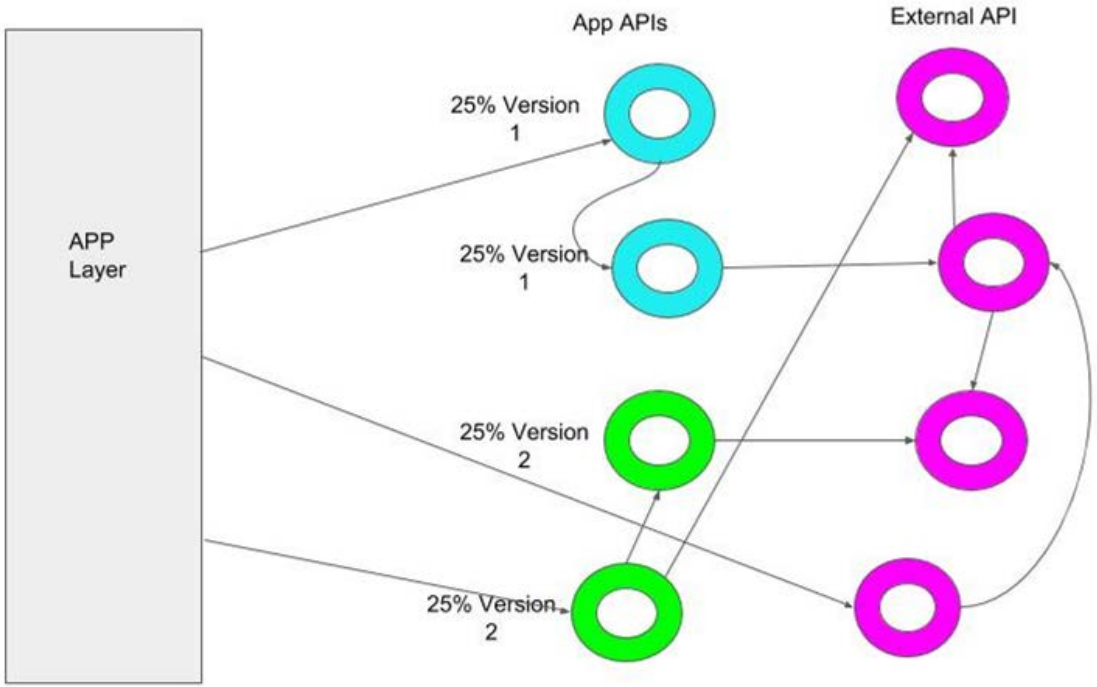
Where do Security Failures come from?

The Gap b/t Modern Software & Security



Distributed Systems Are Tricky

Distributed Systems Are Tricky

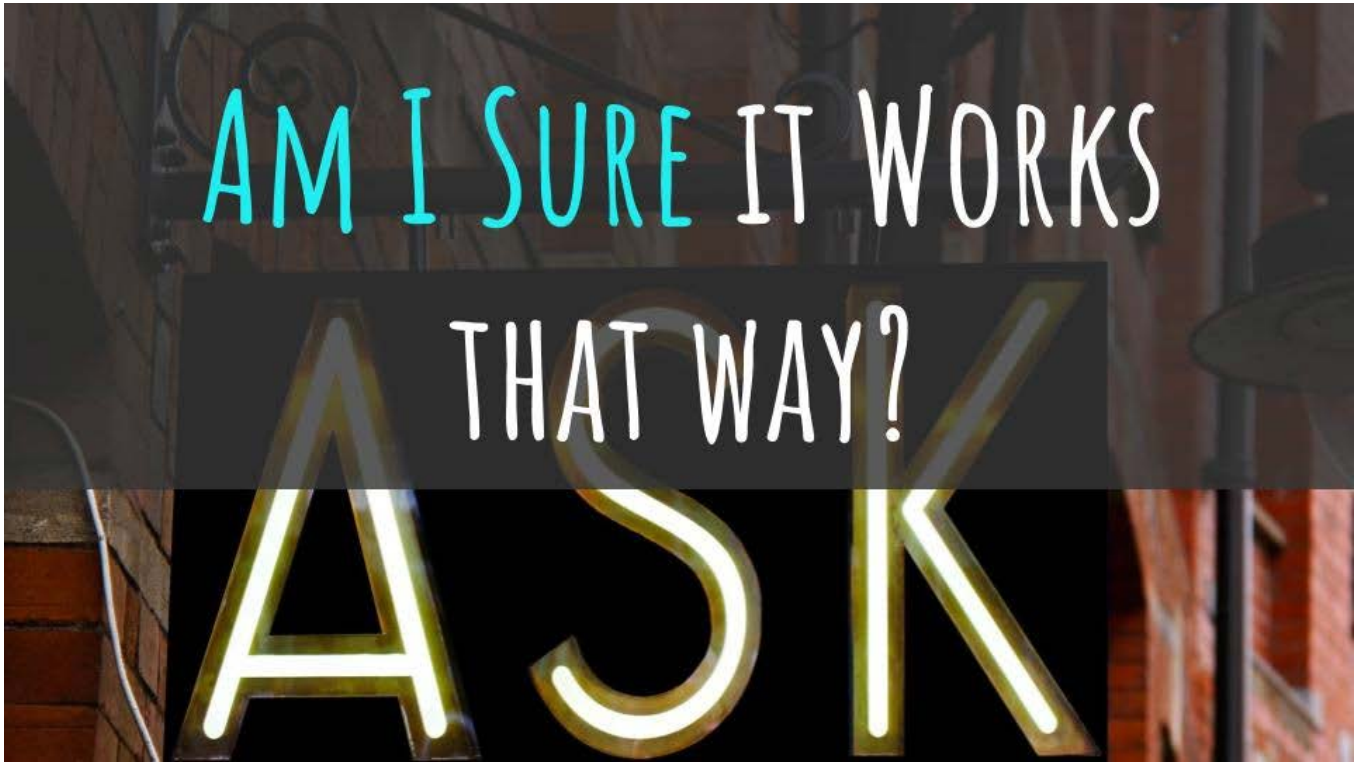


Don't Drift into the Unknown

Ask Better Questions

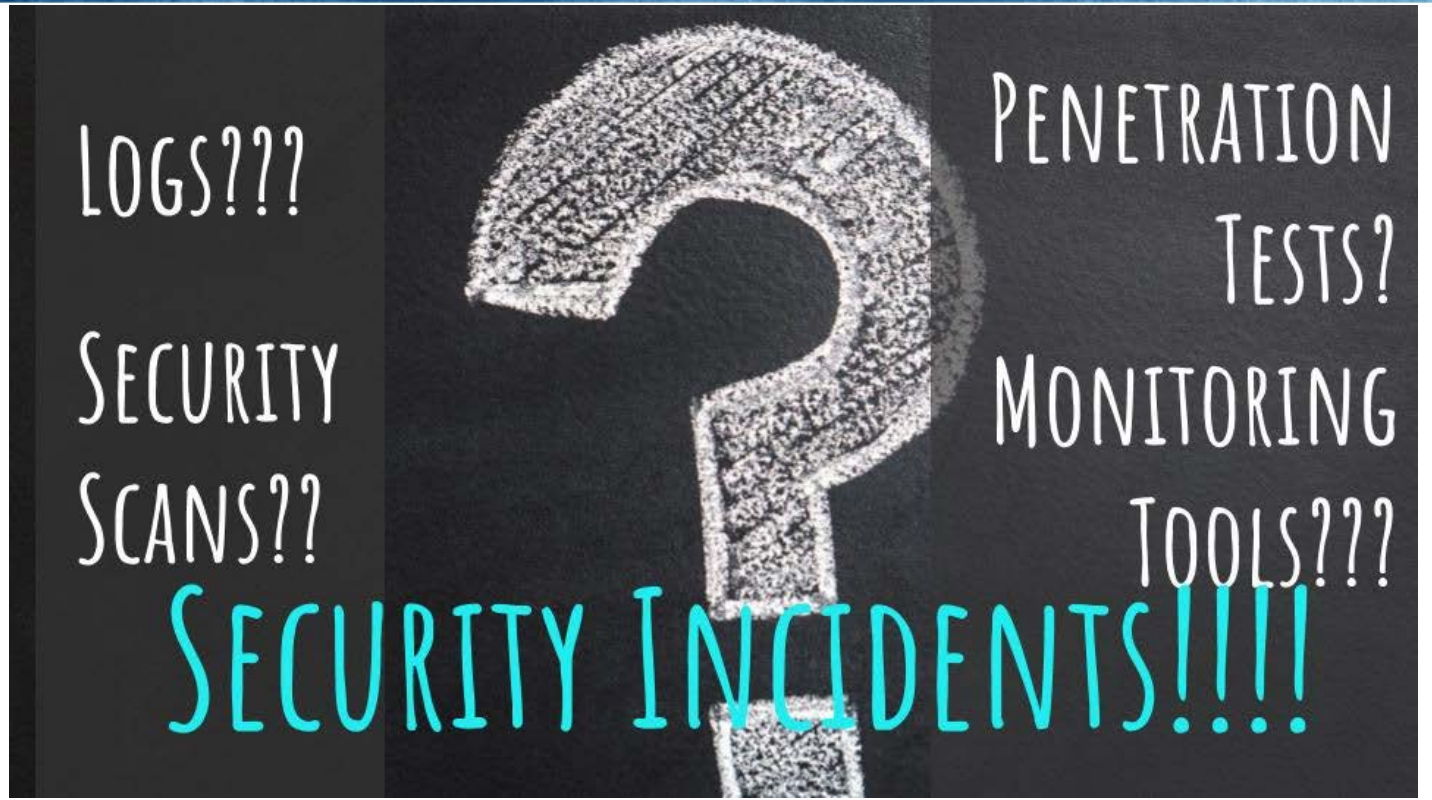
Ask yourself……

Ask yourself……



Ask yourself……

So in fact do we identify Security Failures?



Its toooooo late…..

It worked for Rebel Alliance but not here

Build Confidence through Instrumentation

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"

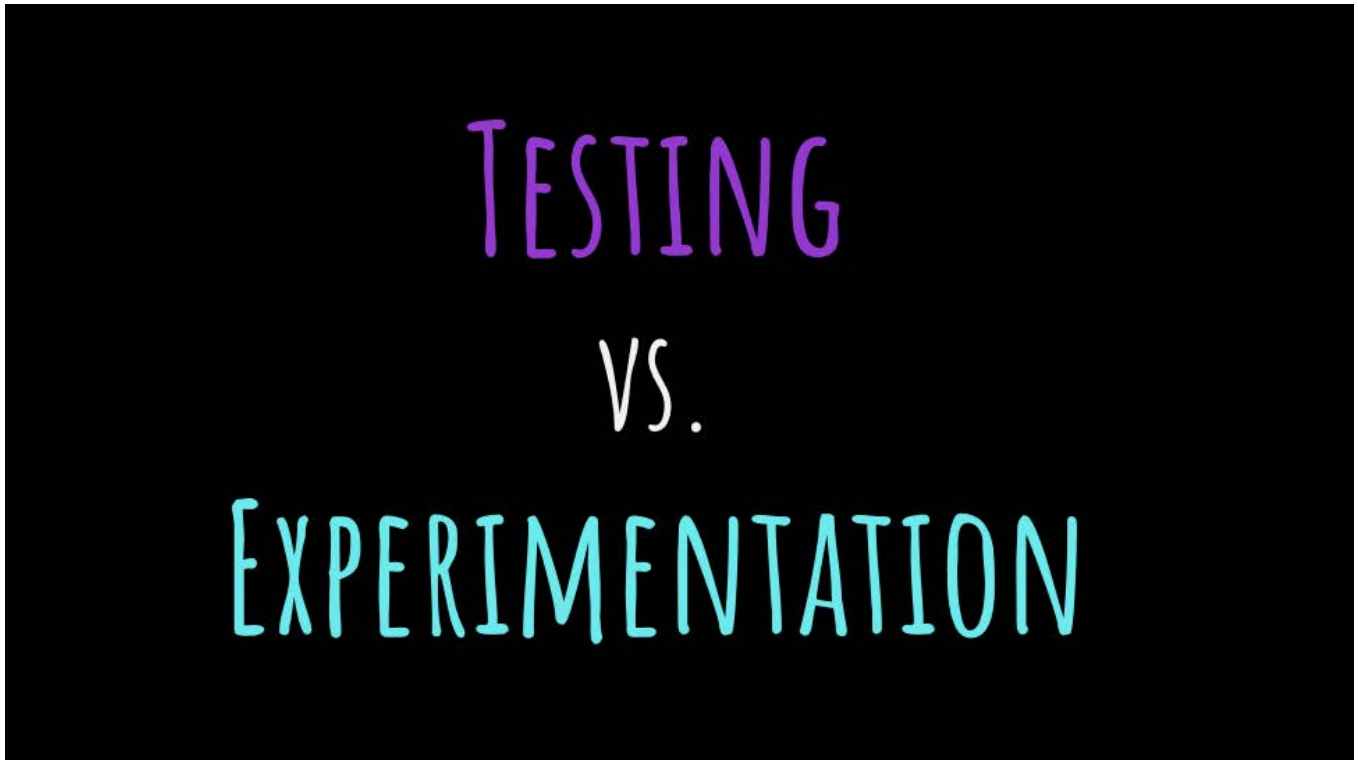
A brief history of Chaos

THE NEW PLAYBOOK

Security Experimentation

Do Less, Better

The New Playbook



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**

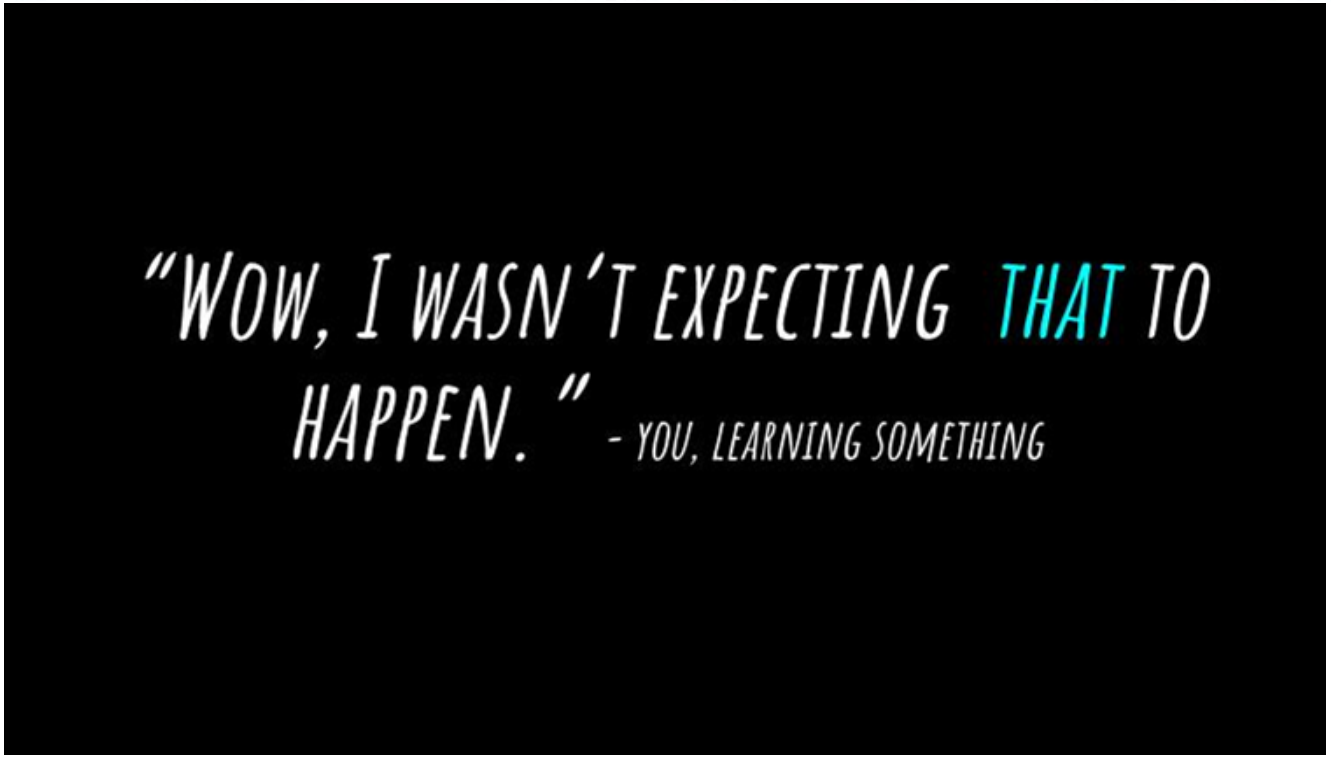
Security Experimentation: A Definition

"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



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

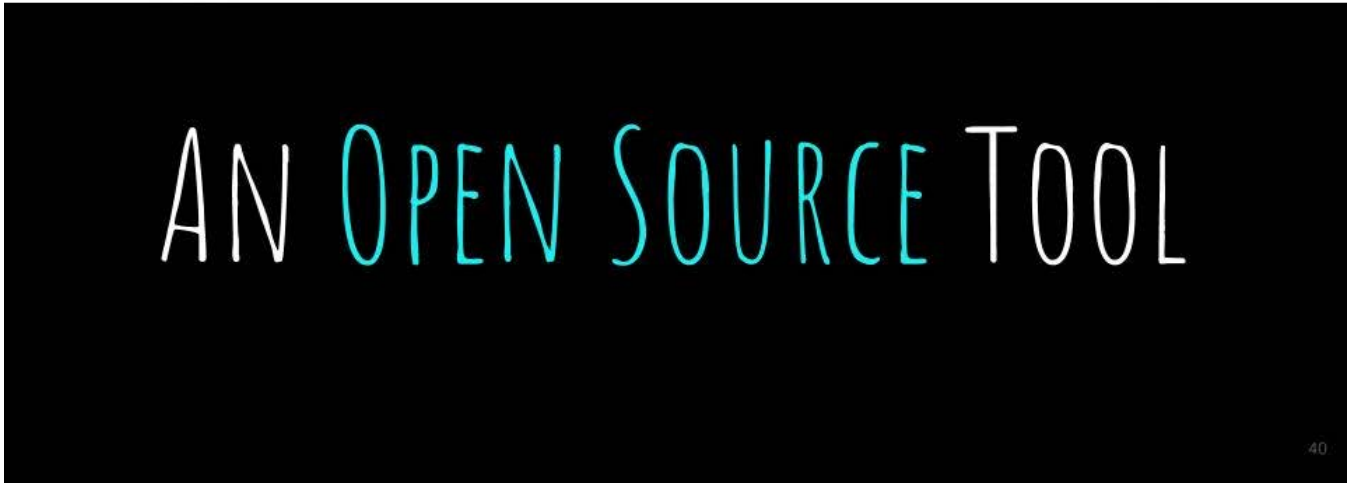
Value of Game Day Exercises

- 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.

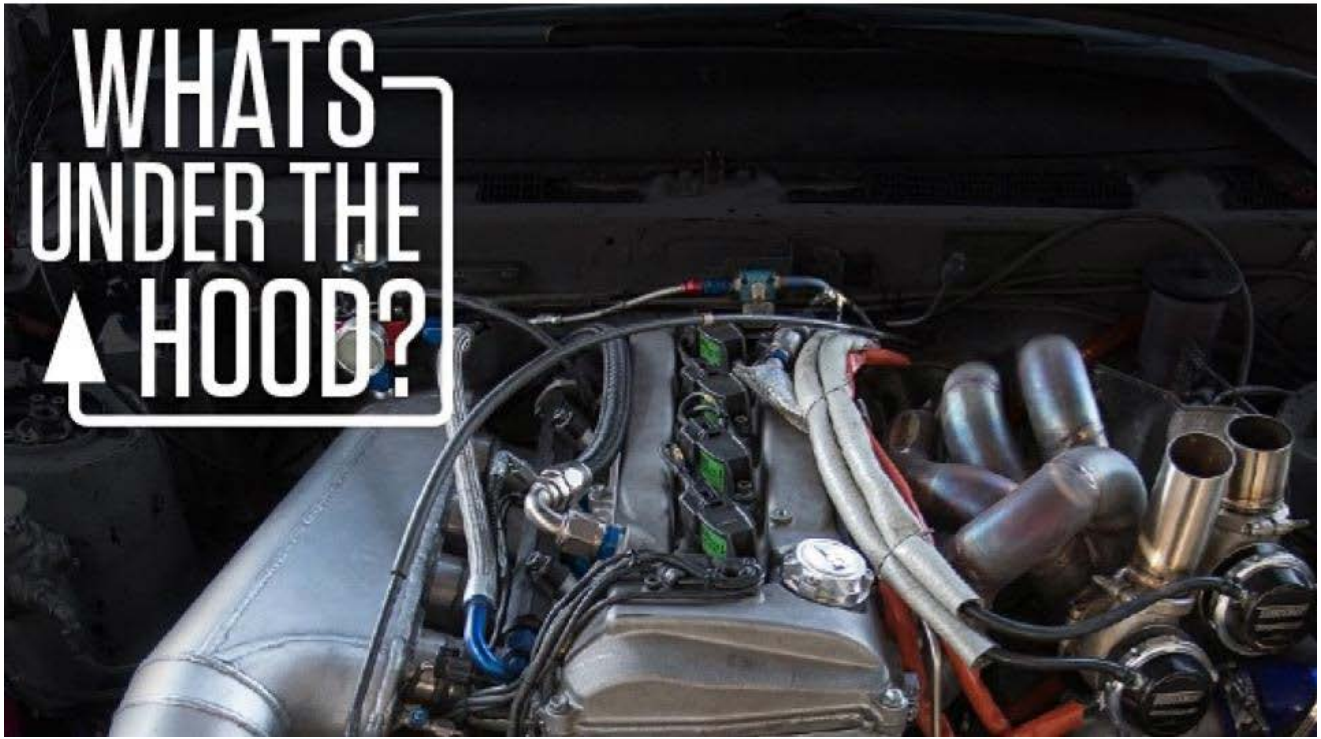
*“If you’re not cultivating **a Learning Culture**, you wlll probably end up losing to someone else who is.”*

Open Source Security Experimentation Tool

ChaoSlingr



So, eh, what is it exactly



FYI ChaoSlingr is on Github (FREE!)

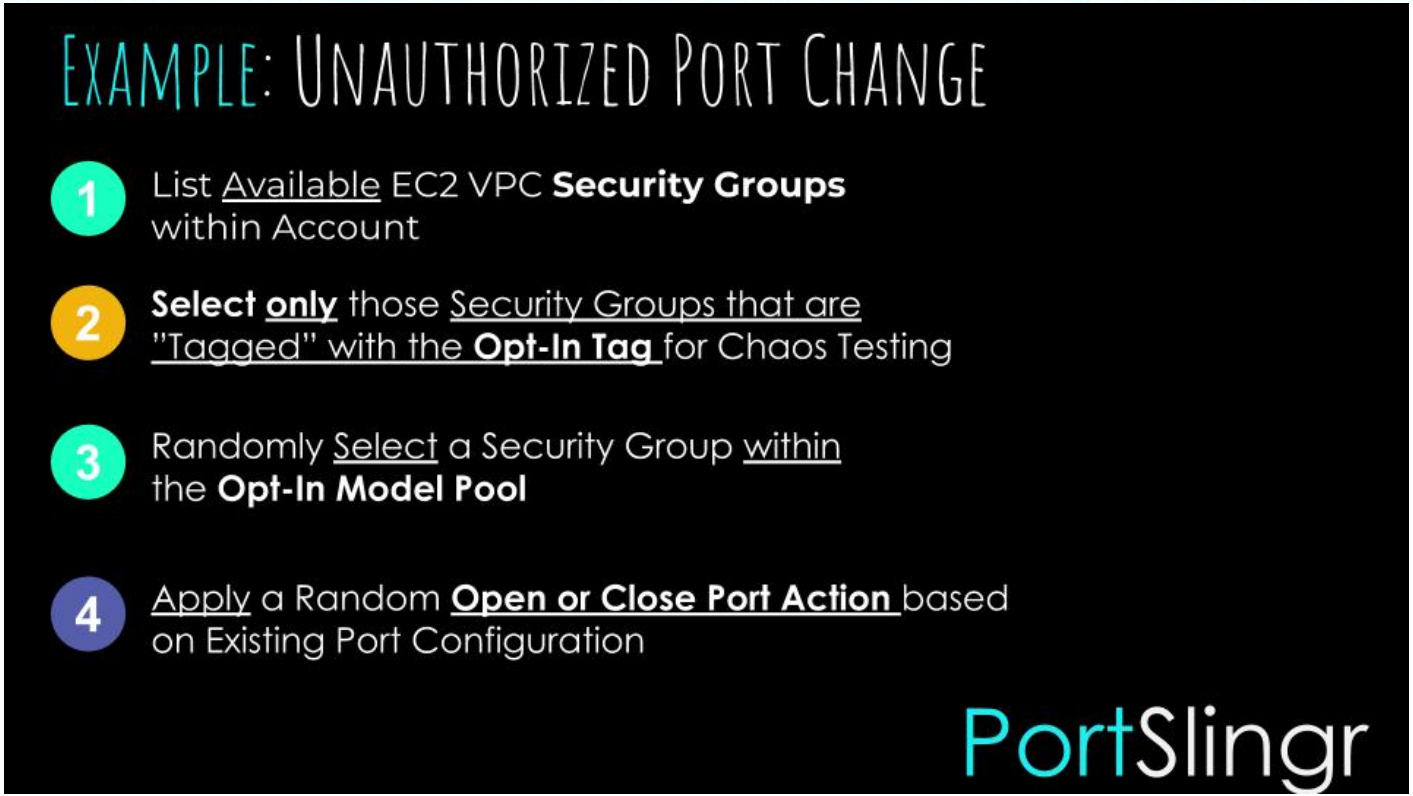
ChaoSlingr

- 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

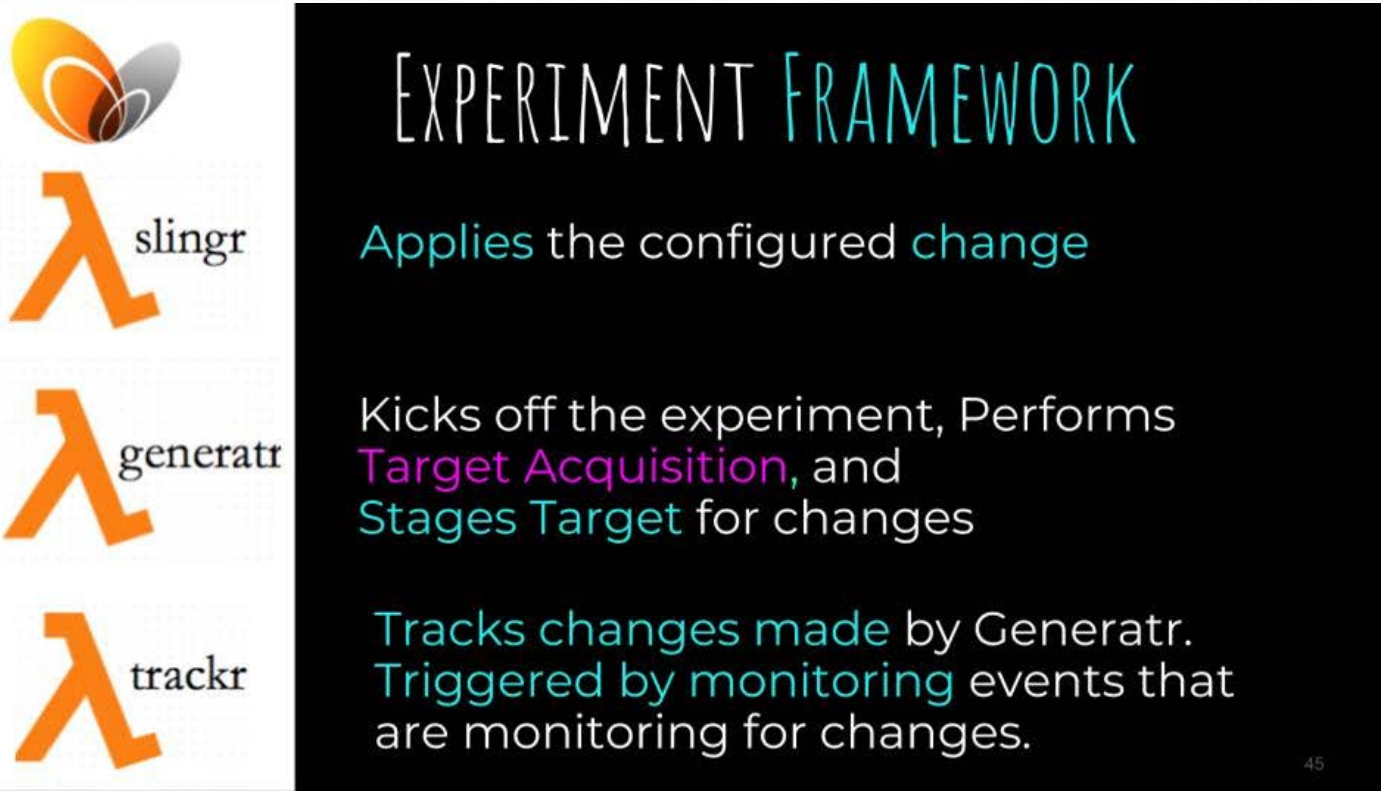


An Example Experiment Using ChaoSlingr

An Example Security Experiment



How the experiment works



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

Hit us with some questions

Questions

@aaronrinehart
@BrewerSecurity