RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: DEV-R02

INTEGRATING SECURITY WITH DEVOPS TOOLCHAINS

Aaron Rinehart

Chief Enterprise Security Architect
UnitedHealth Group
@aaronrinehart

Dr. Chenxi Wang

Founder, General Partner
Rain Capital
@chenxiwang

Speakers Introduction

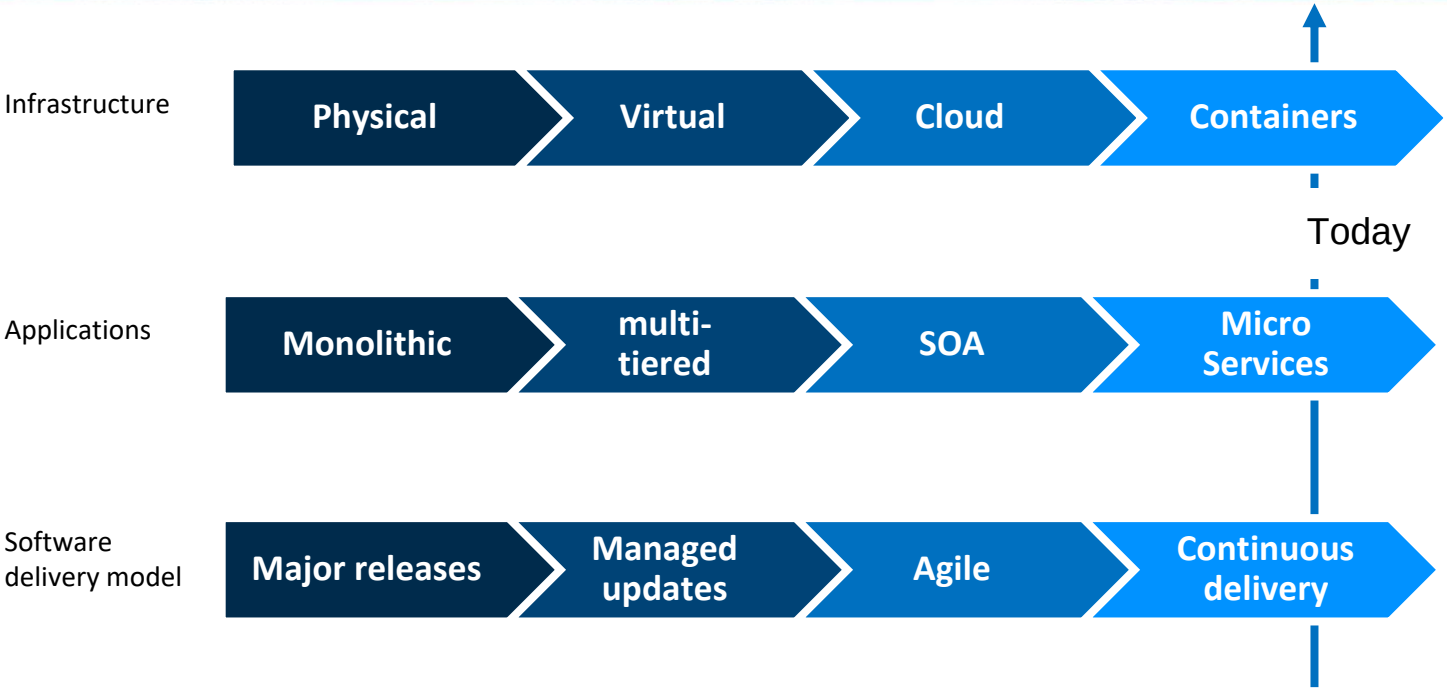
Aaron Rinehart
Chief Enterprise Security Architect
UnitedHealth Group
@aaronrinehart

Chenxi Wang, Ph.D.
General Partner, Rain Capital
OWASP, Board of Directors
@chenxiwang

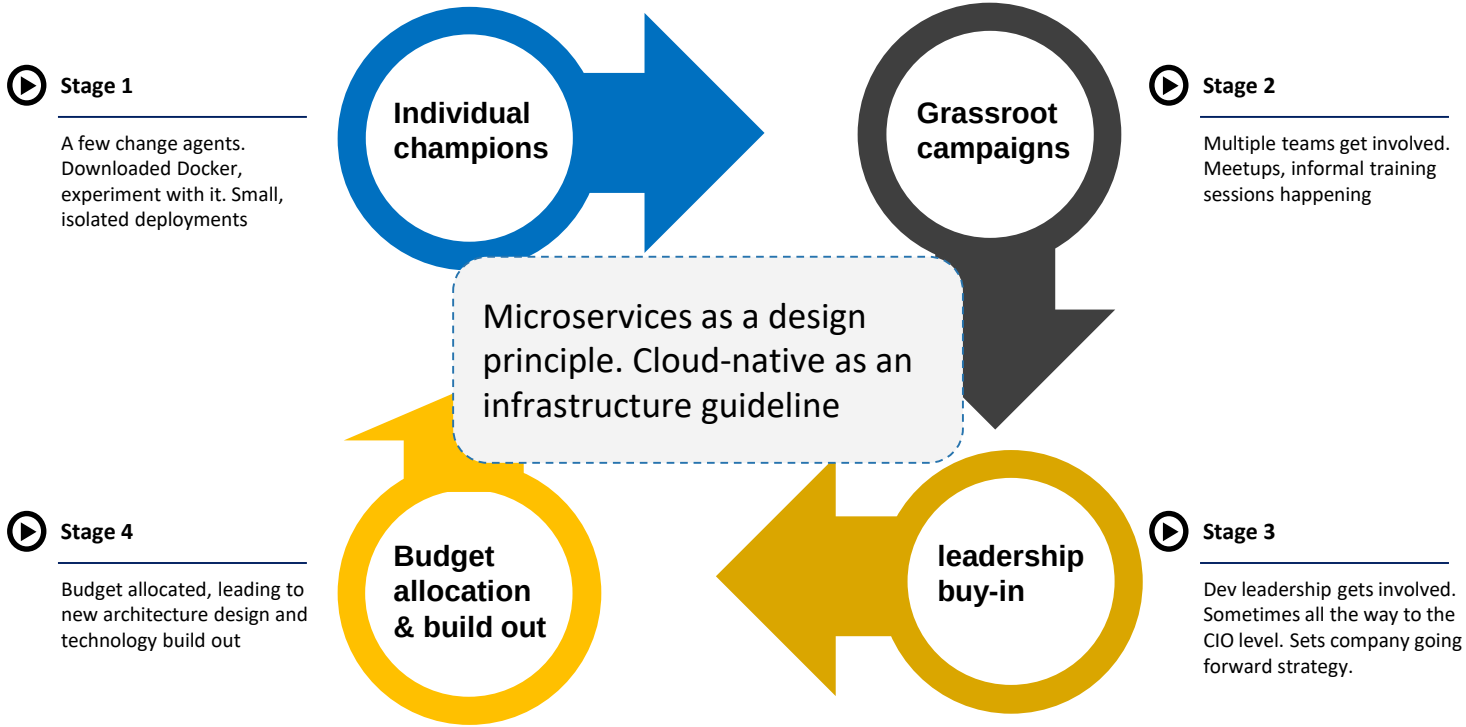
Session Outline: We Will Cover

- DevOps Movement & Security
- 3 Different Practitioner Transformation Stories: Good, Bad, and Ugly
- Recommendations
- New Techniques & Trends
- Shift back toward Product Delivery
- Applying what you learned

An Ongoing Journey In IT Transformation



How DevOps Takes Hold In A Company



Stage 1

A few change agents. Downloaded Docker, experiment with it. Small, isolated deployments

Stage 2

Multiple teams get involved. Meetups, informal training sessions happening

Stage 3

Dev leadership gets involved. Sometimes all the way to the CIO level. Sets company going forward strategy.

Stage 4

Budget allocated, leading to new architecture design and technology build out

Journeys of Three Different Companies

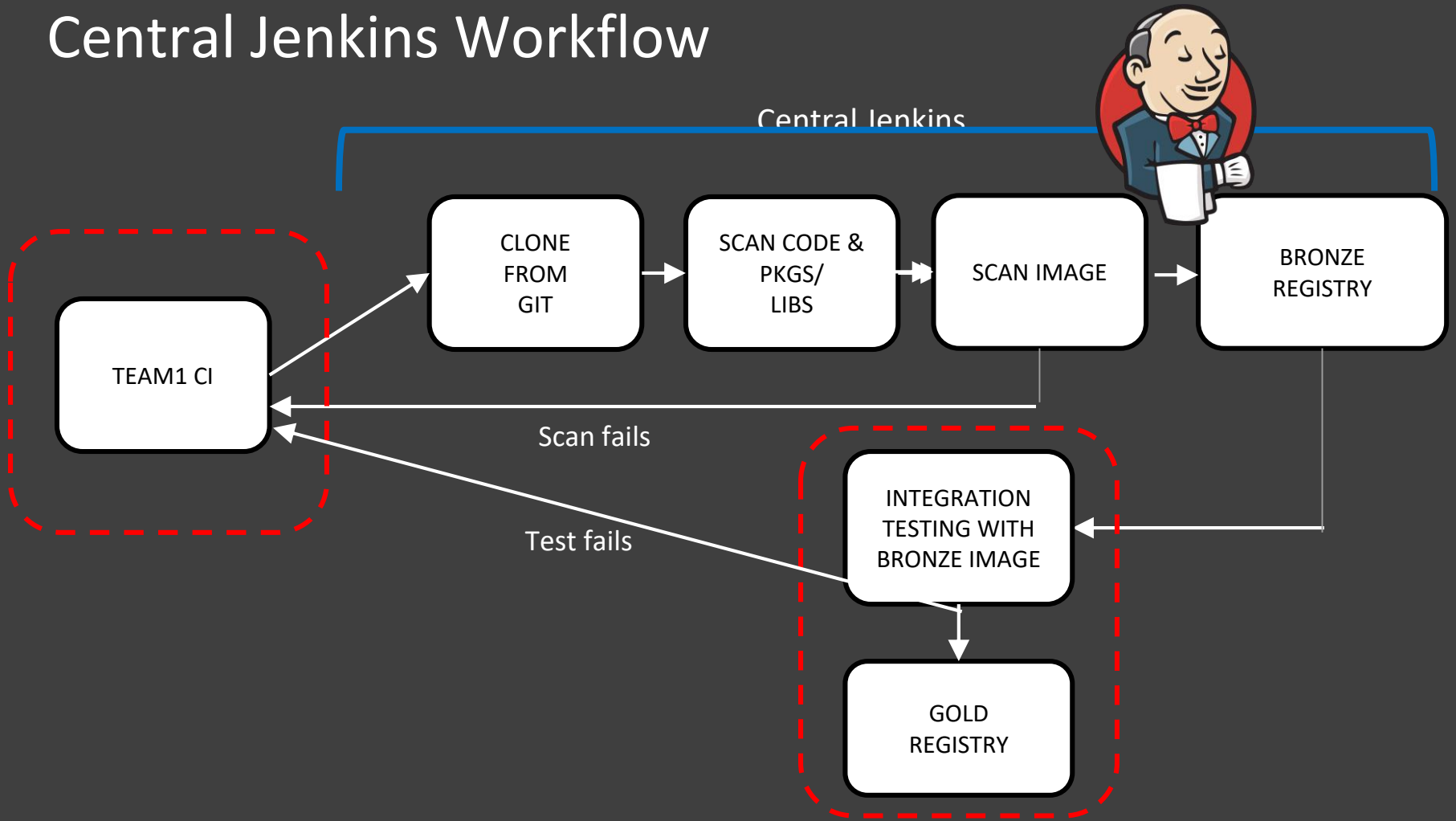
Different industries, different approaches

Cloud-based Financial Service Startup

- Environment
  - On AWS, with many APIs
  - Using micro-services and containers extensively
  - DevOps is king

- Requirements
  - Developer freedom and ease of use
  - Security vulnerability management
  - Clear traceability from container to code

Central Jenkins Workflow



Security Meets Business Demand

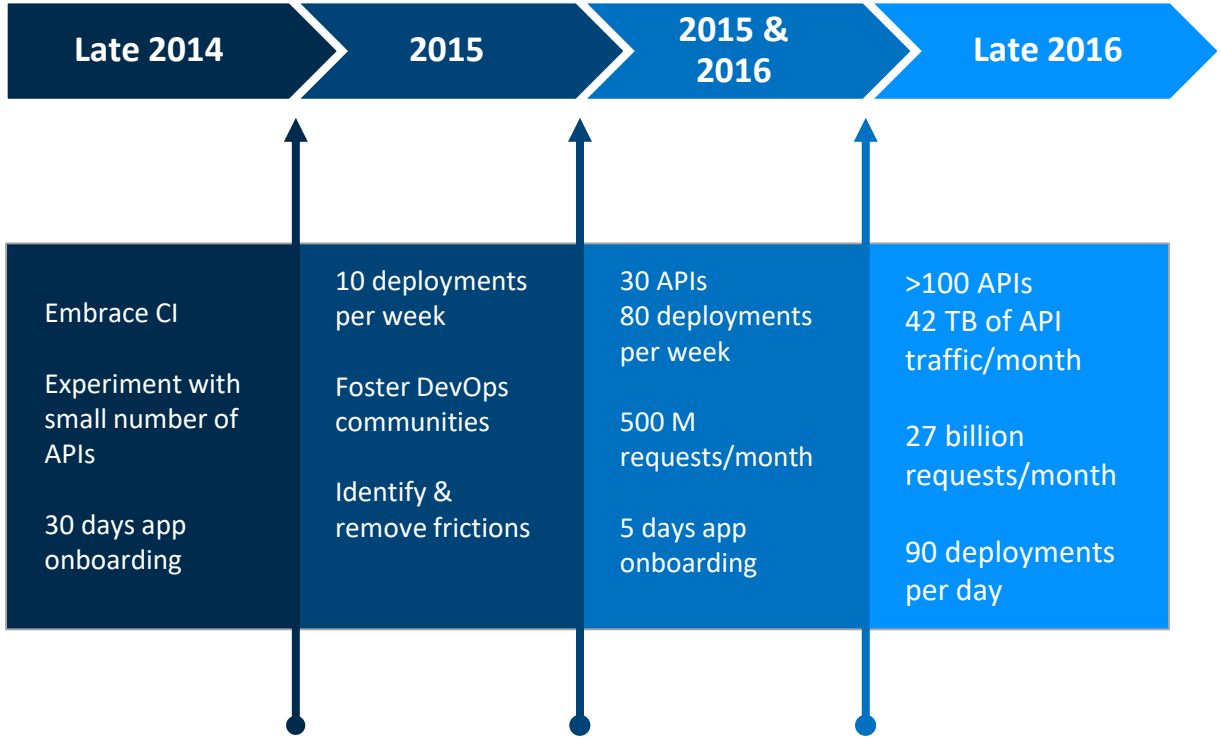
- Developer freedom and ease of use
  - Dev owns and manages their own CI
  - Central CI is automatically triggered
  - Supports multiple tech stacks
- Robust security vulnerability management
  - Central CI is on the critical path to deployment
  - Can fail build if scan fails
- Clear traceability from container to code
  - Central CI does consistent container tagging

Target - the Need to Move at Speed of Business

Target - The Need to Move At Speed of Business

- Holiday season at Target
  - 70,000 new workers
  - 170 million store transactions
- Prior to 2014
  - Nearly everything is monolithic
  - Many grass root micro-services/agile initiatives
  - Pull store location info into a new application takes 6 months
- 2014 - Target gets a new CIO
  - Corporate-wide mandate for microservices
  - Cloud first development

Target - DevOps Journey



Target - Security's Journey

Built a central security platform, focus on API-based development

- build security functions & security APIs centrally
- decentralized product APIs

A big focus on real-time security feedback loop

- Every day security operations metrics feedback to both security leads and engineering teams

Push secure-by-default: extend built-in security upstream as much as you can

Emphasized logging, telemetry, and near real-time visibility

- Process 6 TB of logs a day

UnitedHealth Group

UnitedHealth Group

"The Road from Rugged to Chaos"

- DevOps Transformation @UHG
- Building Security Tools into the Pipeline w/ Gauntlt
- Journey into Security + Chaos Engineering
- ChaoSlingr: Open Source Contribution

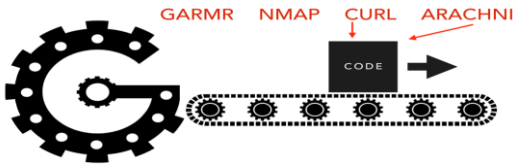
THE CHALLENGE: WE ARE LARGE & COMPLEX

- 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

“The Road from Rugged to Chaos”

Gauntlt: “Be Mean to Your Code”
Driving Security Testing into the Pipeline: Automated Vulnerability Scanning



https://github.com/gauntlt/

James Wickett

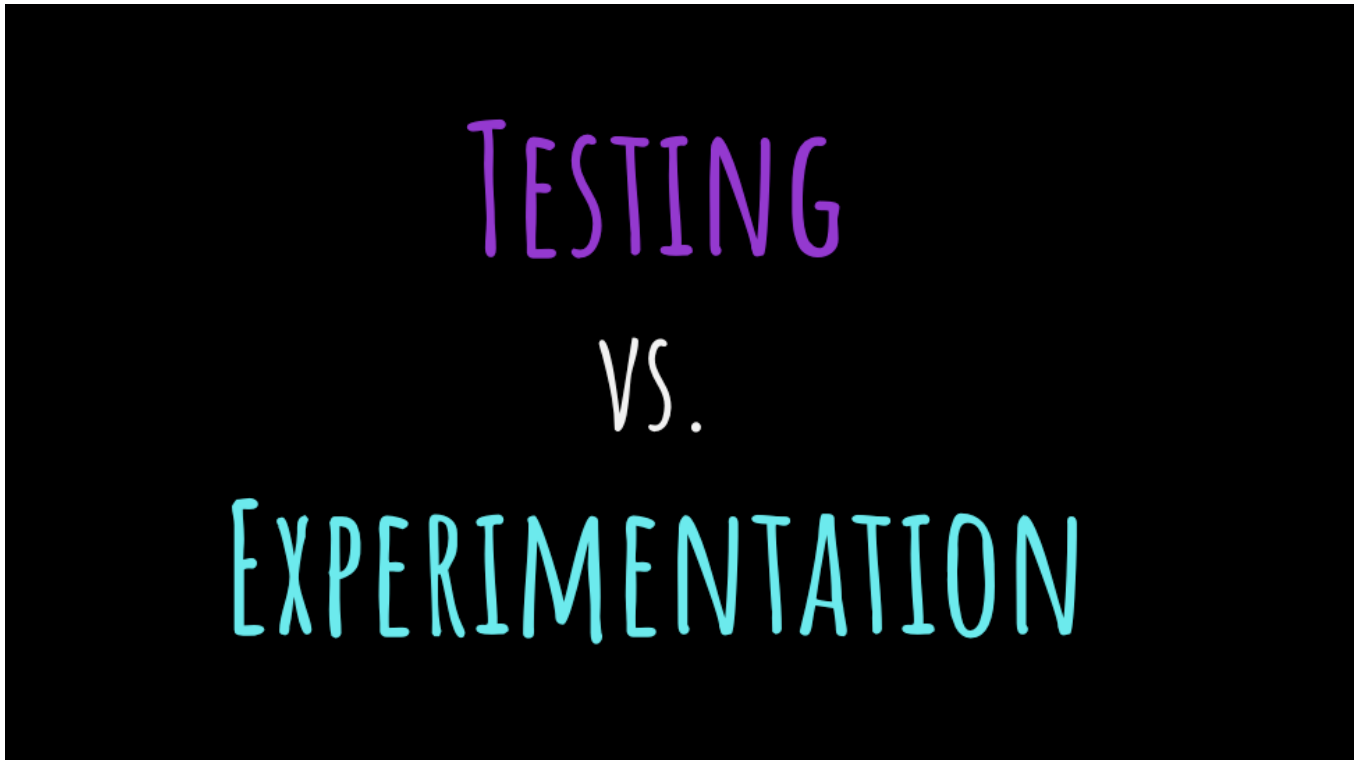
- An open source application vulnerability scanner engine that enables a self-service vulnerability resolution solution
- Automates use of multiple vulnerability security scanning tools
- Provides packages allowing developers to easily run self-service security checks against their applications
- Scans begin immediately and take only minutes to complete

“The Road from Rugged to Chaos”

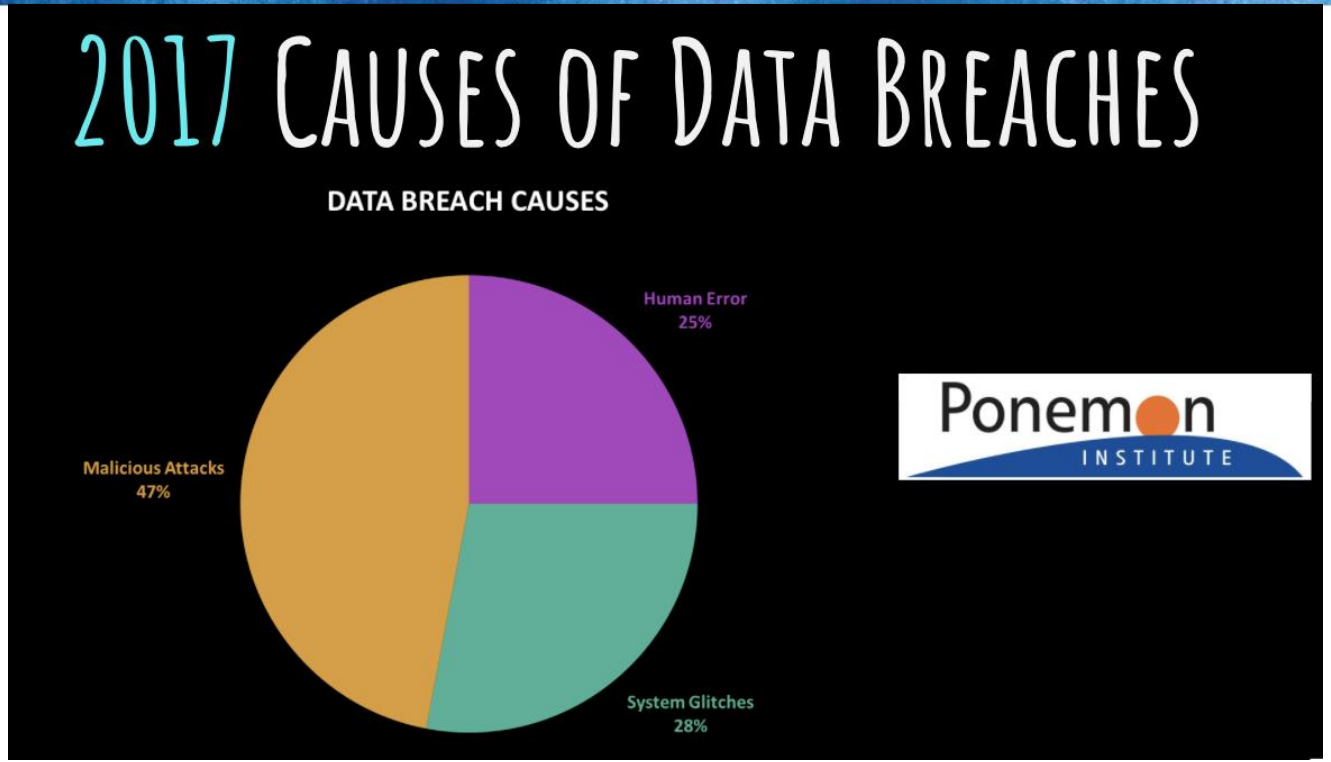
THE JANE BOND PROJECT UNITEDHEALTH GROUP®

Security + Chaos = Security Experimentation

“The Road from Rugged to Chaos”



"The Road from Rugged to Chaos"



“The Road from Rugged to Chaos”

"The Road from Rugged to Chaos"

"The Road from Rugged to Chaos"

ChaoSlingr: First UHG Open Source Tool

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



Summary

DevOps is Not A Destination

- All 3 companies still transforming
- DevSecOps is a journey
- Focus on
  - Continuous Improvement
  - Real-time feedback loop
  - Driving a metrics-driven culture

Some Useful Tips

- Start small
  - One change at a time
- Expect and embrace failure
  - Fail small, fail fast
- Remove friction
  - Drive out complexity
- Avoid Analysis Paralysis
  - DevOps is a living organism

Key Takeaways & Recommendations

- DevOps is not a fad, it is the future
  - It's a culture shift, not just about technology
- Security needs to focus on
  - **Automation**
    - Identify where human adds value & automate everything else
  - **Real-time feedback loop**
    - Build real-time visibility & close-loop control
  - **Build security for Ops, not for security teams**
    - Provide insight/hooks/control for actional operations
- #JFDI

Apply What You Have Learned Today

- Next week you should:
  - Understand DevOps projects & determine opportunity for security integration
- In the first three months following this presentation you should:
  - Choose one or two projects and design a security insertion point
  - Implement one pilot assess performance,
  - Build value proposition for larger initiatives
- Within six months you should:
  - Build a DevSecOps tribe

Questions

@aaronrinehart
@chenxiwang