DevOps for Defense

December 2019

GitHub

Robert Freeman & Lucas Boyd

Special Guest

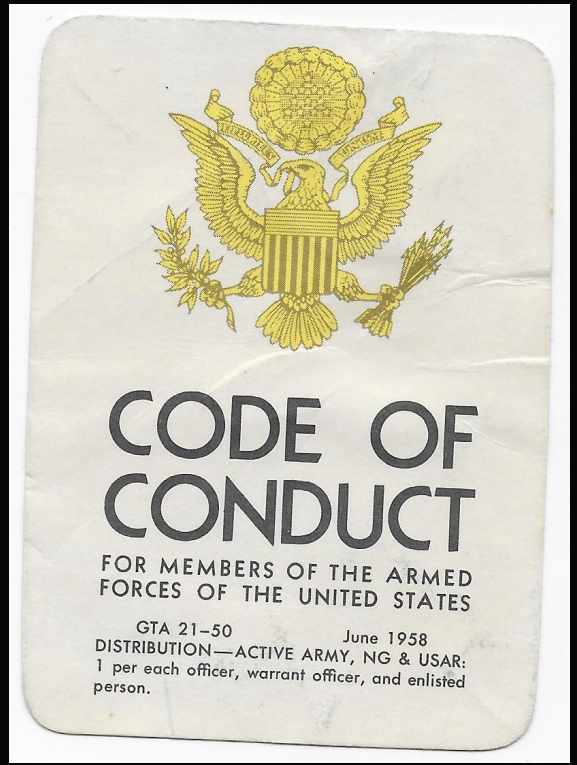
John Willis

https://devopsfordefense.org
https://www.meetup.com/DevOps-for-Defense/
https://github.com/jondavid-black/DevOpsForDefense
devopsfordefense@gmail.com
https://twitter.com/devops4defense

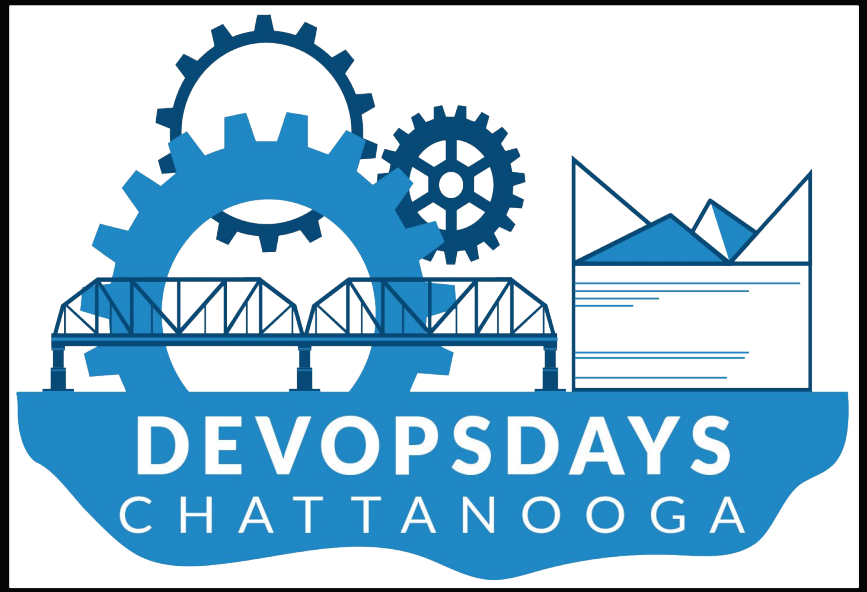
Sponsored by: TEKsystems Own change

DevOps for Defense Meetup: Code of Conduct

- UNCLASSIFIED ONLY!!!!
- Treat each other with respect and professionalism.
- Do not talk about private, sensitive, or proprietary work.
- Do talk about your experiences, needs, desires to improve work in our domain.
- Do share your thoughts.
- Do learn from others.
- Do respect & tip your bartenders!



DevOpsDays Chattanooga 2019



Lightning Talk - Community Driven DevOps Transformation

https://youtu.be/S6TQVkX6UaM

Thanks to everyone who took a personal day for professional development!

Now on

Subscribe to **DevOps for Defense** on **YouTube**

DevOps for Defense Community Challenge

Donate Time 1 Day a Month

https://girlswhocode.com/

Emeka Barclay Marshall
Language Arts | Liberty Middle Scho
Apple Teacher
Google Certified Educator
Microsoft Innovative Educator
Flipgrid Certified Educator

"Knowledge is power. Information is liberating. Education is the premise of progress, in every society, in every family." -Kofi Annan

Website: caffeinatedteacher.weebly.com
Twitter: @teacheremeka

Help Drive Positive Change

Support Girls Who Code through smiles.amazon.com


DevOps for Defense
2 Year
Anniversary

Dec 2017

Dec 2018

Sept 2019

Nov 2019

What a ride so far! Thank you all!!!

Images by JD Black (‘s phone...and taken by the great staff at Rocket Republic Brewing Co)

Celebrate & Show Your Support in Our Community!

GREEN PEA PRESS

Show your DevOps nerd cred!
Customize your own DevOps for Defense t-shirt!

$25 - 100% of proceeds support Girls Who Code!

Consider supporting us through GitHub Sponsors.
Multiple levels of support.

https://github.com/jondavid-black
No fees! - All donations directly support the future of DevOps for Defense meetup!

2020 - What's Next for DevOps for Defense?

January

Back to Basics

- DevOps 3 Ways
- The 4 Types of Work
- The 5 Ideals

February

Gradle

Hans Dockter
CEO Gradle Inc.
Powerful Automation & Insight

March

GitLab

Open source complete CI/CD toolchain out-of-the-box.

Beyond

(Still coordinating & planning, but here's what we're thinking.)

Nicolas M. Chaillan
USAF Chief Software Officer -
Bringing DevSecOps DoD-wide

Dr. Mik Kersten
CEO Tasktop -
Author of Project to Product

Hack-a-thon?
Opportunity to put our DevOps learning into practice.

Provide us feedback so we can tailor to your needs.

https://devopsfordefense.org

DevOps for Defense Meetup Presents

Featuring John Willis

2 Year Anniversary!

The world's largest source code repository with 40 million developers and 100 million repositories!.

GitHub

Lead Engineer for DoD and IC will provide an update on GitHub capability and security advancements.

Thursday, December 5th, 2019 at 6:00pm

Rocket Republic Brewing Co
289 Production Ave, Madison, AL

GitHub - Subsidiary of: Microsoft

Meetup Sponsored by: TEKsystems — Own change

GitHub 2019

Transforming how the mission builds software, securly

GitHub – Loved by developers, trusted by the Enterprise

GitHub DoD/IC Account Team

Lucas Boyd

Sales, DoD/IC

Robert Freeman

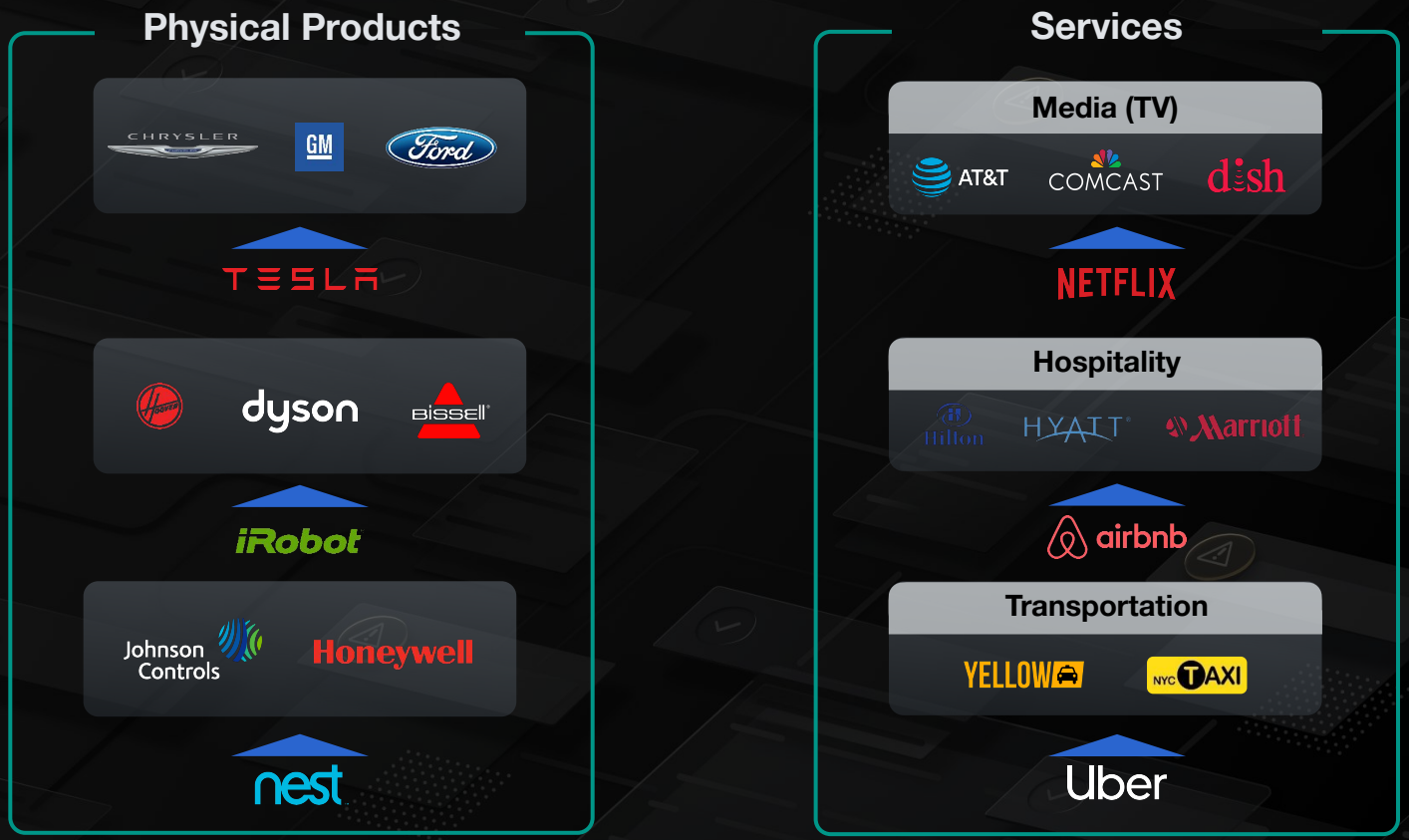
Technologist, DoD/IC

The Future is written in CODE

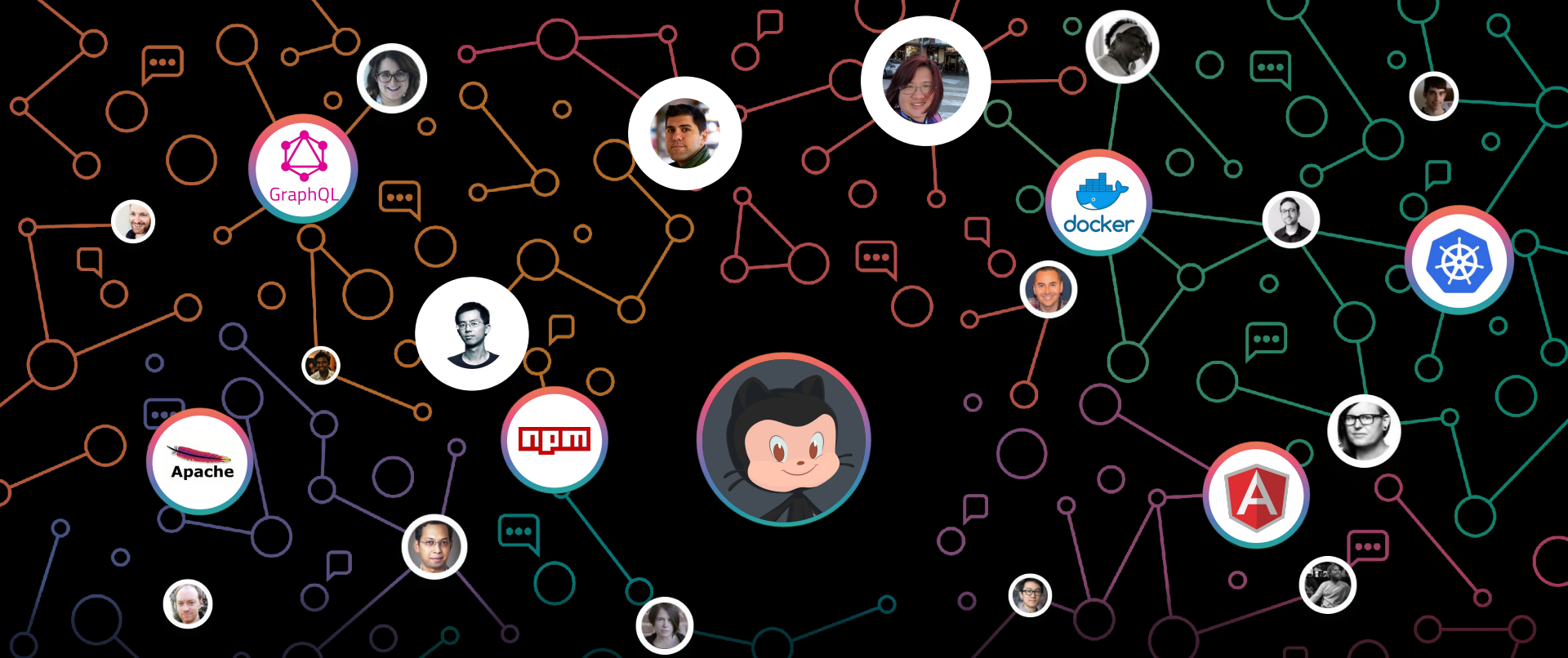
Nearly 50% of the S&P 500
will be replaced by 2026

To compete, every company
is becoming a software company

Disruption across every industry



Developers are at the heart of innovation



40,000,000 + Developers

GitHub is the home for the world's code.

GitHub is the largest developer community on Earth

40M+	120M+	1,000s	1B+	2M+	50%
Developers	Private and public repositories	Top open source communities	Contributions Per year	Organizations	Fortune 500 Companies

The most innovative companies

Most open source projects

Three powerful trends

Developers drive innovation

1M+ and growing developer shortage across industries

Open source is in your software supply chain

1,000's of developers have commit access to your production code

Cloud enables faster cycles

93% of DevOps implementations are not optimized

Sources: BLS, NSF, NCES, IDC, Gartner, LinkedIn, C+AI Corp Strat

Source: DORA State of Devops Report 2018

GitHub is a critical partner for your Digital Transformation

Collaboration

Retain your best talent with the platform developers know and love

Security

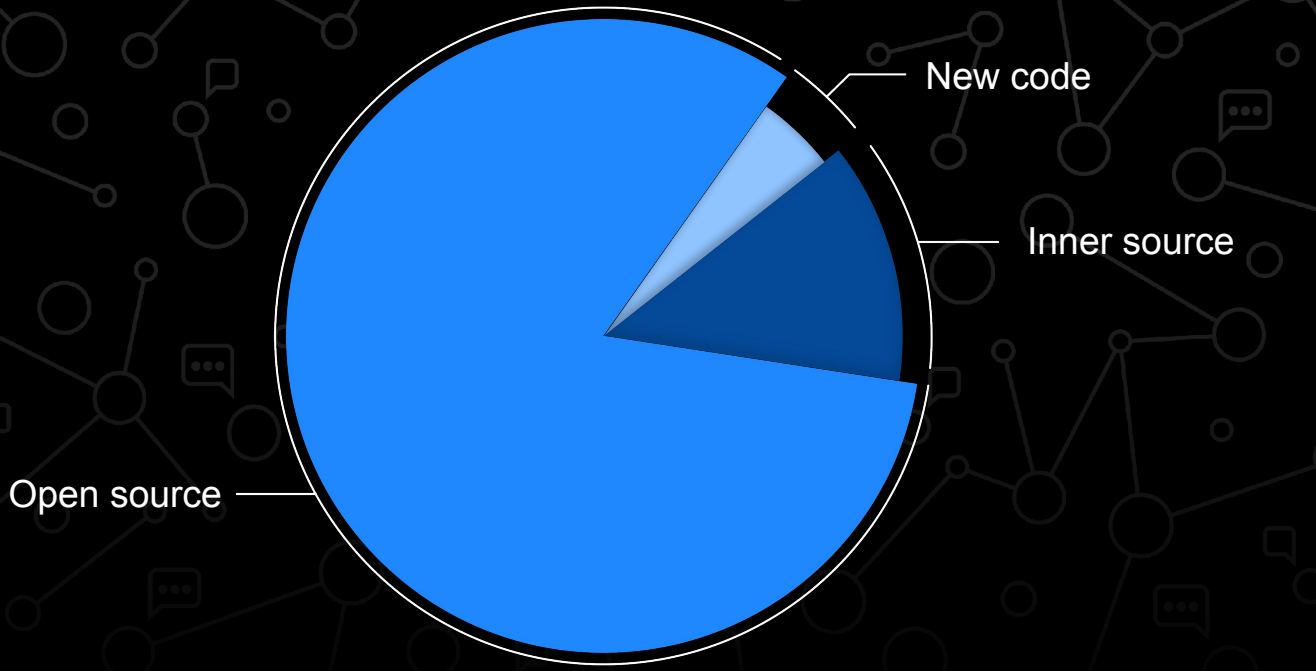
End-to-end security for your software supply chain

DevOps

Automate workflows from code to any cloud

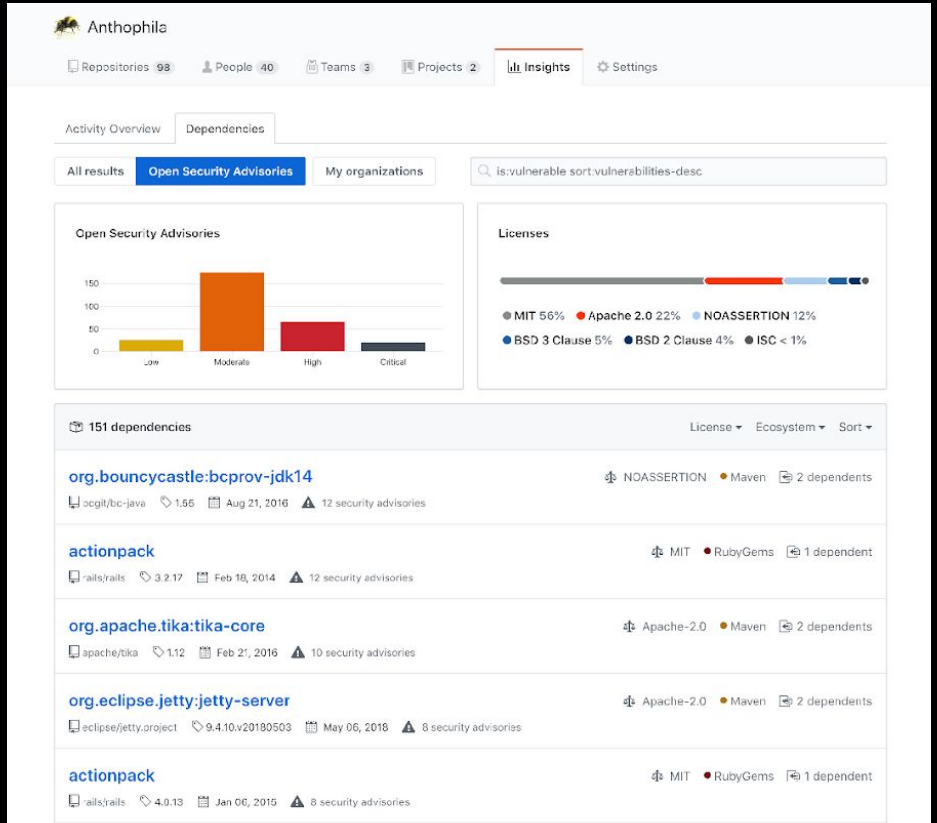
Collaboration

80-90% of the code in new applications comes from open source.



Dependency Insights

- Understand what your software stack actually looks like
- Track security advisories across your organization
- Continue to make good decisions about what open source software you use



What makes an open source community healthy?

	Active maintainer and contributors
	License
	Standard engineering practices
	Security best practices
	Healthy two-way communications

Inner Source in your company

Nationwide

90% reduction in merge times

Rewrote Nationwide Financial 6-months ahead of schedule and 40% below budget

Walmart

Faster, cheaper, & better

We want you to consume OS because it's better, but we want you to contribute to the community

NASA JPL
Jet Propulsion Laboratory
California Institute of Technology

Greater collaboration

Code reuse was greater than 90%. Collaboration increased 20-fold.

SCANIA

GitHub enabled transparency

PayPal

4x increase in performance

SONY

30% increase in productivity

IBM

Giving employees greater tools to affect positive culture change

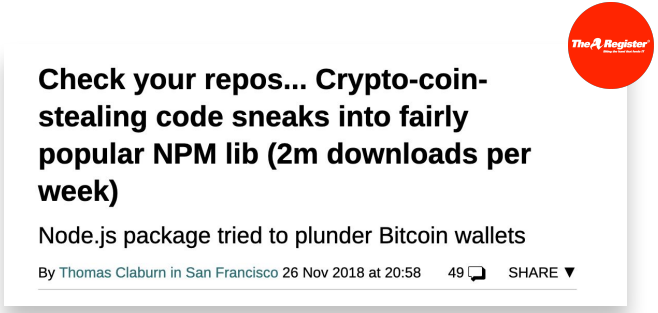
IBM teams using GitHub Enterprise to provide internal documentation - for engineering design, operations and support activities - have experienced 80% fewer escalation calls from first-line.

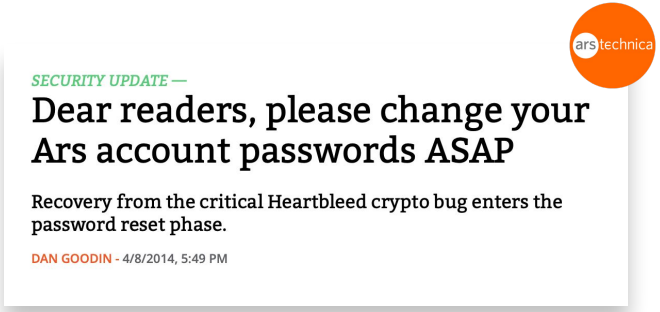
Security & Compliance

Security and compliance

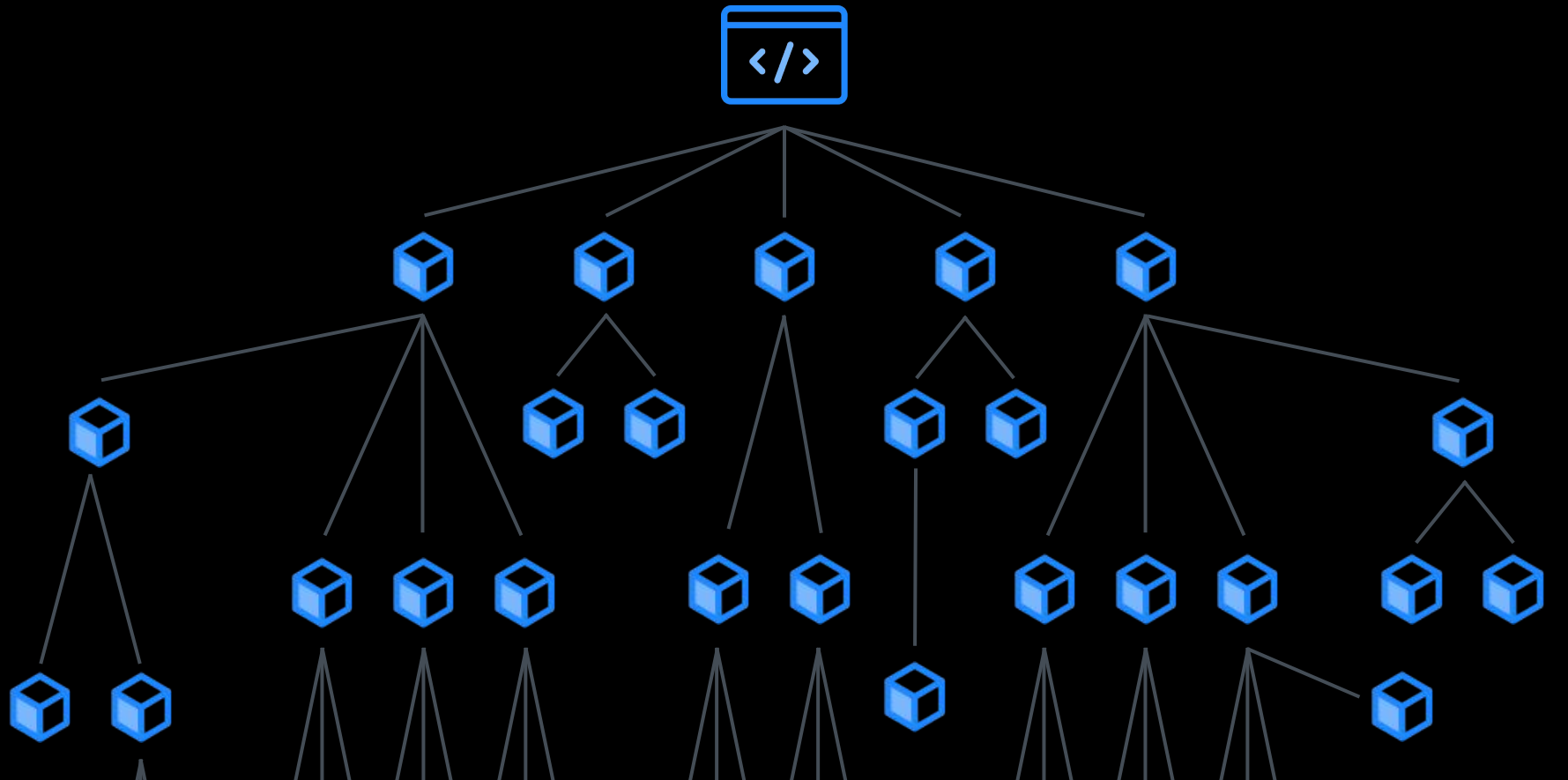
An existential challenge

Using open source introduces new challenges, including security and compliance risks.

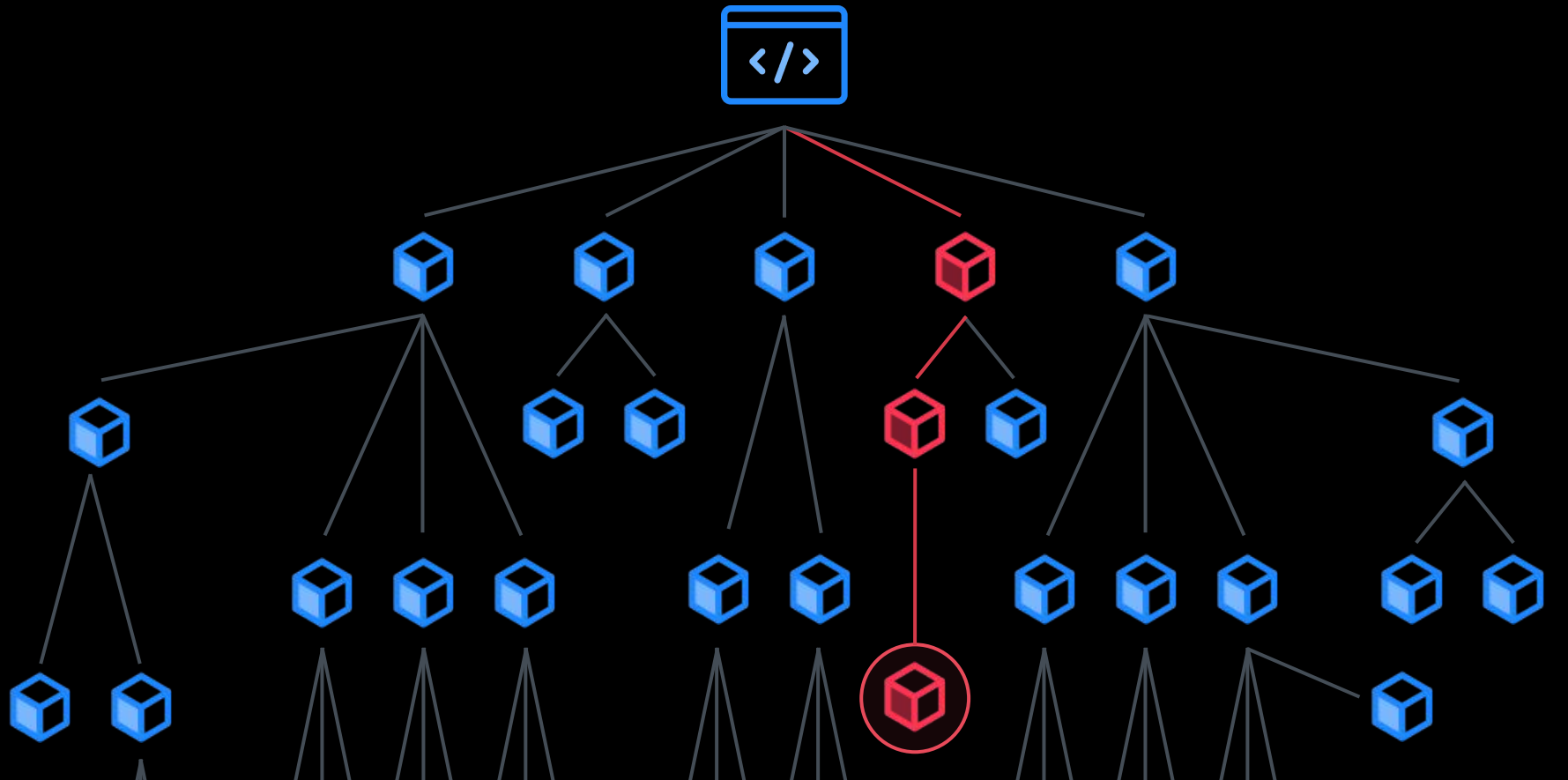




Software dependencies are pervasive

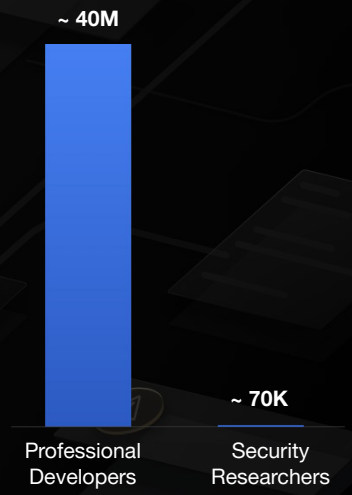


Securing code requires end-to-end approach

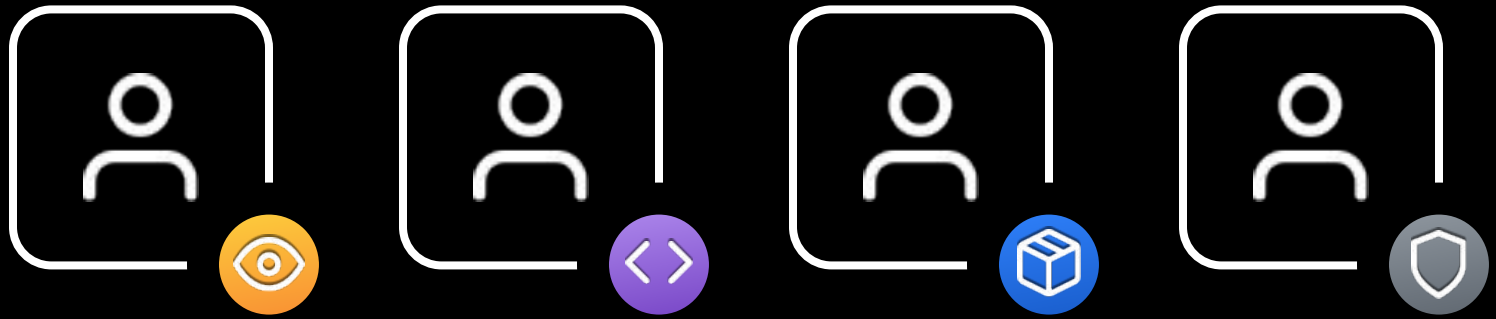


Secure development is shifting left

Vastly more cost effective to remediate during development



570x more developers than security researchers



Security Researchers

Maintainers

Developers

Security Teams

Only GitHub secures your end-to-end software supply chain

Securing all of open source

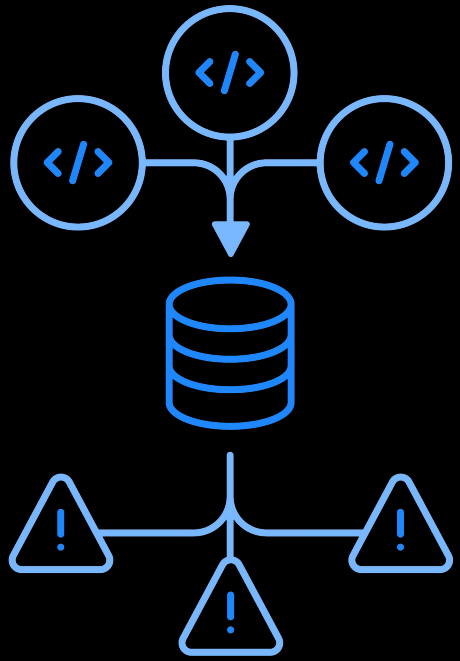
Proactive Code Scanning

Dependency Insights

Automated Security Fixes

Proactive Code Scanning: analyze your code as data

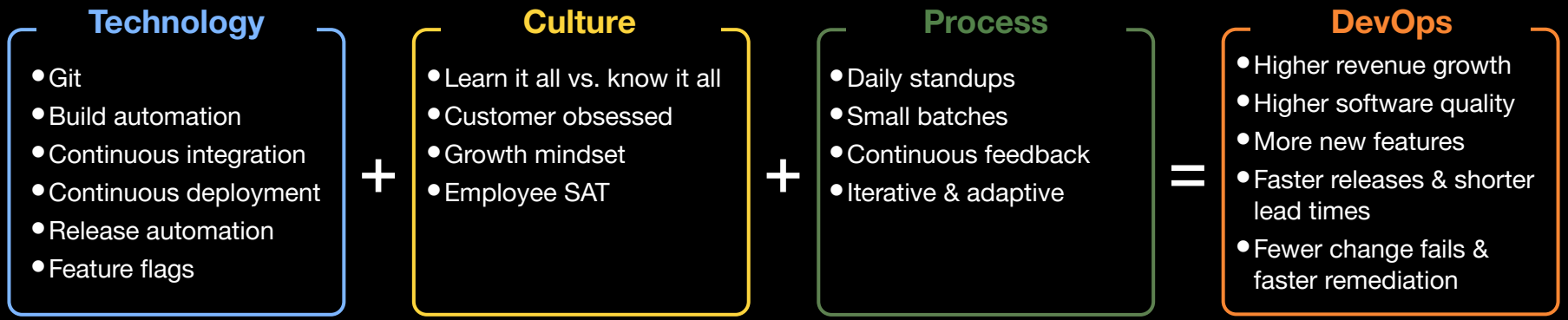
- World's most advanced semantic code analysis engine, combined with world's largest community
- Queries identify vulnerabilities and their variants
- Prevents known variants as part of your automated CI testing
- Community-led model continuously improves, 2000+ queries today



Google Uber Microsoft

DevOps

DevOps transforms technology and team culture



PERIODIC TABLE OF DEVOPS TOOLS (V2) (V1)

EMBED DOWNLOAD ADD

Os	Open Source
Fr	Free
Fm	Freemium
Pd	Paid
En	Enterprise

SCM	Database Mgmt
CI	Repo Mgmt
Deployment	Config / Provisioning
Cloud / Iaas / Paas	Release Mgmt
BI / Monitoring	Logging

Build	
Testing	
Containerization	
Collaboration	
Security	

1 Fm Gh Github																		2 Fm Aws Amazon Web Services
3 Os Gt Git	4 Pd Dm DBmaestro												5 En Ch Chef	6 En Pu Puppet	7 Os An Ansible	8 En Sl Salt	9 Os Dk Docker	10 Pd Az Azure
11 Fm Bb Bitbucket	12 Os Lb Liquibase												13 Os Ot Otto	14 En Bl BladeLogic	15 Os Va Vagrant	16 Fr Tf Terraform	17 Os Rk rkt	18 En Gc Google Cloud Platform
19 Os Gl GitLab	20 En Rg Redgate	21 Os Mv Maven	22 Os Gr Gradle	23 Os At ANT	24 Os Fn FitNesse	25 Fr Se Selenium	26 Os Ga Gatling	27 Fr Dh Docker Hub	28 Os Jn Jenkins	29 Pd Ba Bamboo	30 Os Tr Travis CI	31 Pd Gd Deployment Manager	32 Os Sf SmartFrog	33 Os Cn Consul	34 Os Bc Bcfg2	35 Os Lxc Linux Containers	36 En Rs Rackspace
37 Os Sv Subversion	38 En Dt Datical	39 Os Gt Grunt	40 Os Gp Gulp	41 Os Br Broccoli	42 Fr Cu Cucumber	43 Os Cj Cucumber.js	44 Fr Qu Qunit	45 Os Npm npm	46 Fm Cs Codeship	47 Pd Vs Visual Studio	48 Fm Cr CircleCI	49 Fr Cp Capistrano	50 Fr Ju JuJu	51 Os Rd Rundeck	52 Os Cf CFEngine	53 Fr Ds Swarm	54 Os Op OpenStack
55 En Hx Helix	56 En Dp Delphix	57 Fr Sb sbt	58 Os Mk Make	59 Os Ck CMake	60 Fr Jt JUnit	61 Fr Jm JMeter	62 Fr Tn TestNG	63 Os Ay Artifactory	64 Fm Tc TeamCity	65 Fm Sh Shippable	66 Os Cc CruiseControl	67 En Ry RapidDeploy	68 Fm Cy CodeDeploy	69 En Oc Octopus Deploy	70 En No CA Nolio	71 Os Kb Kubernetes	72 Fm Bx Bluemix
73 En Cw ISPW	74 En Id Idera	75 Os Msb MSBuild	76 Os Rk Rake	77 Fr Pk Packer	78 Os Mc Mocha	79 En Xltv XL TestView	80 Os Jm Jasmine	81 Os Nx Nexus	82 Os Co Continuum	83 Fm Ca Continua CI	84 Pd So Solano CI	85 En Xld XL Deploy	86 En EB ElasticBox	87 Fm Dp Deploybot	88 En Ud UrbanCode Deploy	89 Fr Fl Fleet	90 Os Os OpenShift

XebiaLabs
Deliver Faster

Follow @xebialabs

91 En Xlr XL Release	92 En Ur UrbanCode Release	93 En Bm BMC Release Process	94 En Hp HP Codar	95 En Au Automic	96 En Pl Plutora Release	97 En Sr Serena Release	98 Pd Tfs Team Foundation	99 Fm Tr Trello	100 Pd Jr Jira	101 Fm Rf HipChat	102 Fm Sl Slack	103 Fm Fd Flowdock	104 Pd Pv Pivotal Tracker	105 En Sn ServiceNow				
106 Os Ki Kibana	107 Fm Nr New Relic	108 Os Ni Nagios	109 Os Zb Zabbix	110 En Dd Datadog	111 Os El Elasticsearch	112 En Ss StackState	113 En Sp Splunk	114 Fm Le Logentries	115 Fm Sl Sumo Logic	116 Os Ls Logstash	117 Os Gr Graylog	118 Os Sn Snort	119 Os Tr Tripwire	120 En Ff Fortify				

Impact of DevOps

Teams innovate faster with DevOps

22%
Improved quality of deployed applications

Average ROI of Continuous Delivery Investments

21%
Increase in new software and services delivered

30-50x
Faster deployment cycles

High performing teams innovate faster

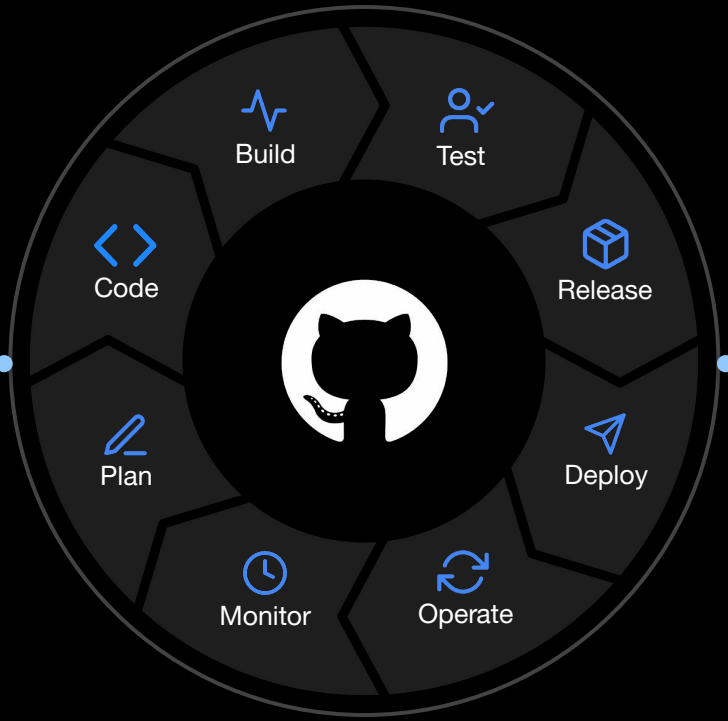
200-400x
Shorter time from code commit to deployment

Sources: DORA, Puppet Labs

Code-to-Cloud DevOps

Home for all developers
Home for the world's code

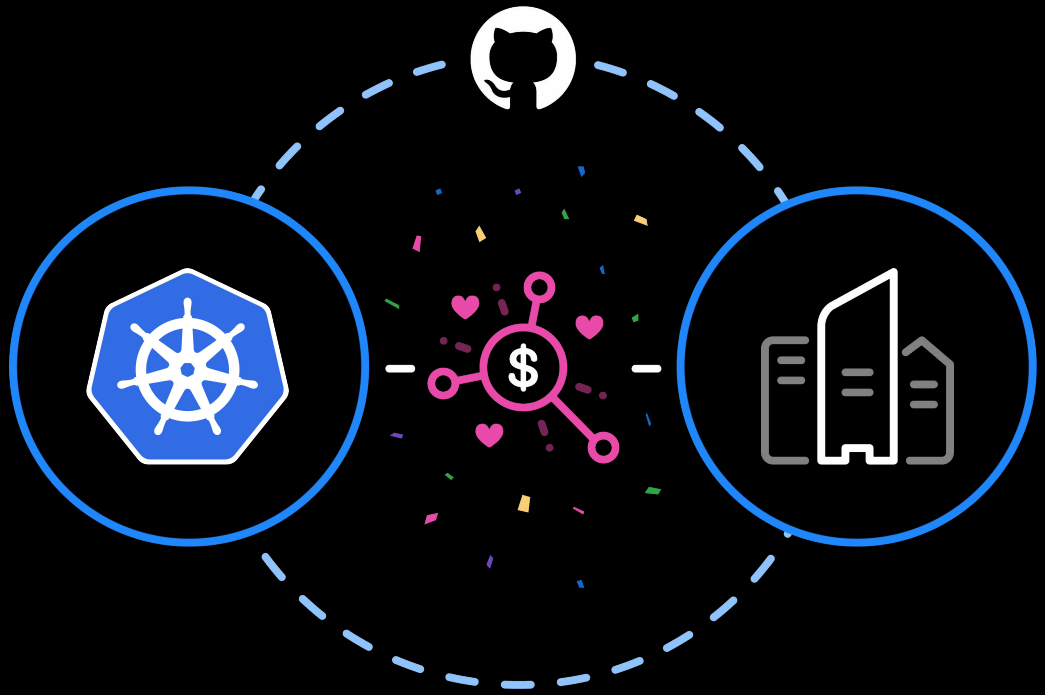
- Elastic, to any scale
- Fully managed
- Packages always the latest
- Supports all OS for CI/CD
- Largest ecosystem
- Community-led automation



Deploy anywhere, including your own data centers

Summary & Next Steps

GitHub Sponsors - ensure the success of projects in your supply chain



Learning Lab helps your teams continuously improve

GitHub Learning Lab

InnerSource Fundamentals

High level yet impactful InnerSource concepts to help transform your organization.

Start the course >

Picking InnerSource projects

Example projects that will help you determine candidates for trying InnerSource practices.

Go to resource >

Introduction to GitHub

An introduction to the simplest possible workflow: GitHub Flow.

Start the course >

Create a release based workflow

Learn and practice a workflow based around creating releases on GitHub.

Start the course >

How We Partner for Digital Transformation

GitHub One

GitHub
Transformation Services

DevOps

Security

Collaboration

John Willis
Benevolent
DevOps God

ubuntu

socketplane

DevOps Cafe
With
John Willis
Damon Edwards

DEV SEC OPS

DevOps Handbook
HOW TO CREATE WORLD-CLASS AGILITY, RELIABILITY, & SECURITY IN TECHNOLOGY ORGANIZATIONS

CHEF

docker

DEVOPSDAYS

DELL

Botchagalupe Technologies

DEVOPS ENTERPRISE SUMMIT
San Francisco
November 13-15, 2017

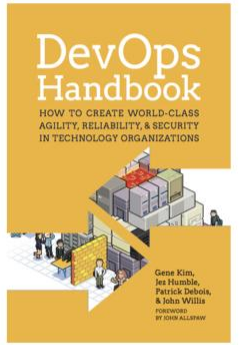
DIGITAL ANARCHIST

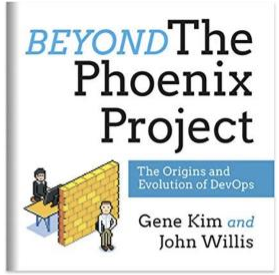
BEYOND The Phoenix Project
The Origins and Evolution of DevOps
Gene Kim and John Willis

https://github.com/botchagalupe/my-presentations

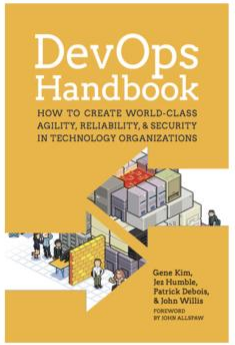
Security and Compliance Theater “The Seventh Deadly Disease”

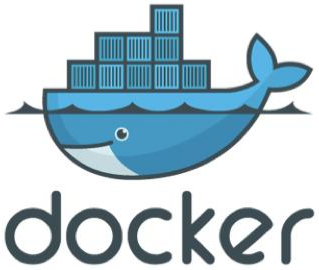
John Willis
@botchagalupe
jwillis@redhat.com

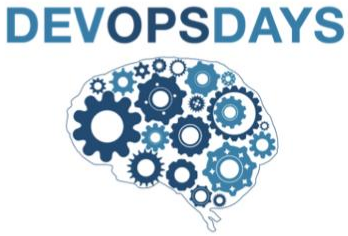


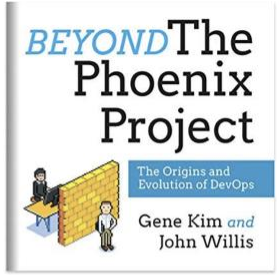


https://github.com/botchagalupe/my-presentations







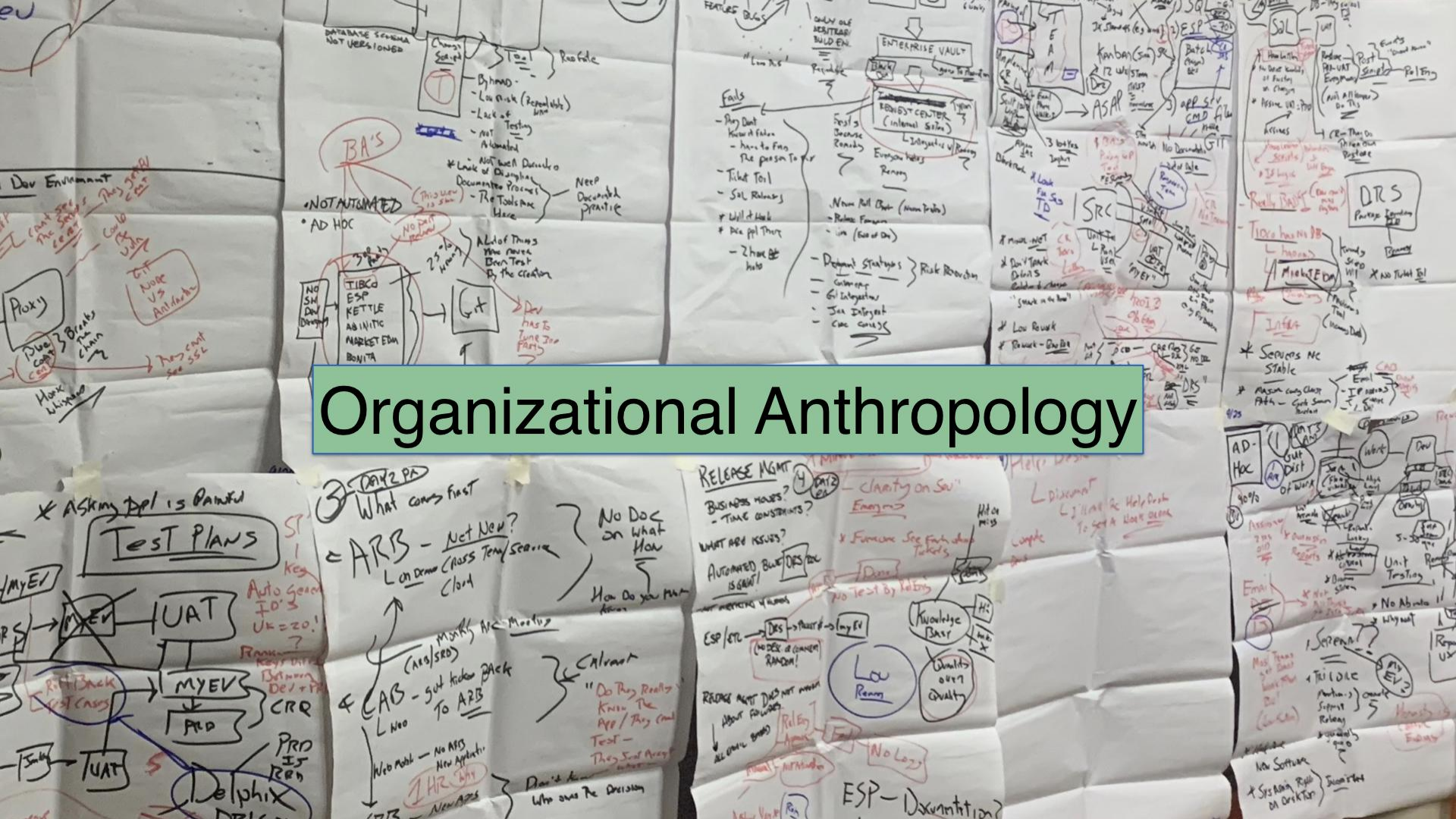


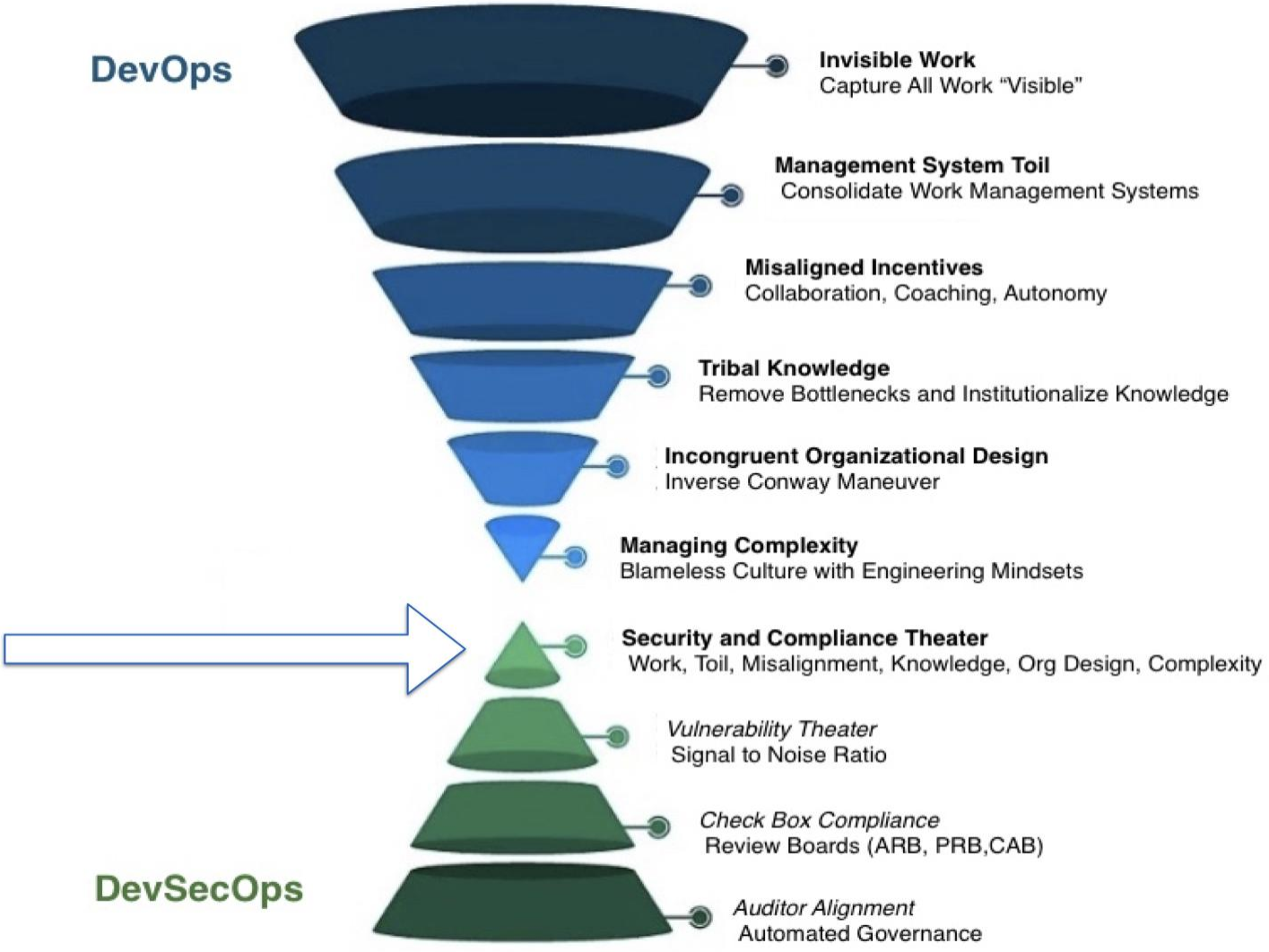
https://github.com/botchagalupe/my-presentations

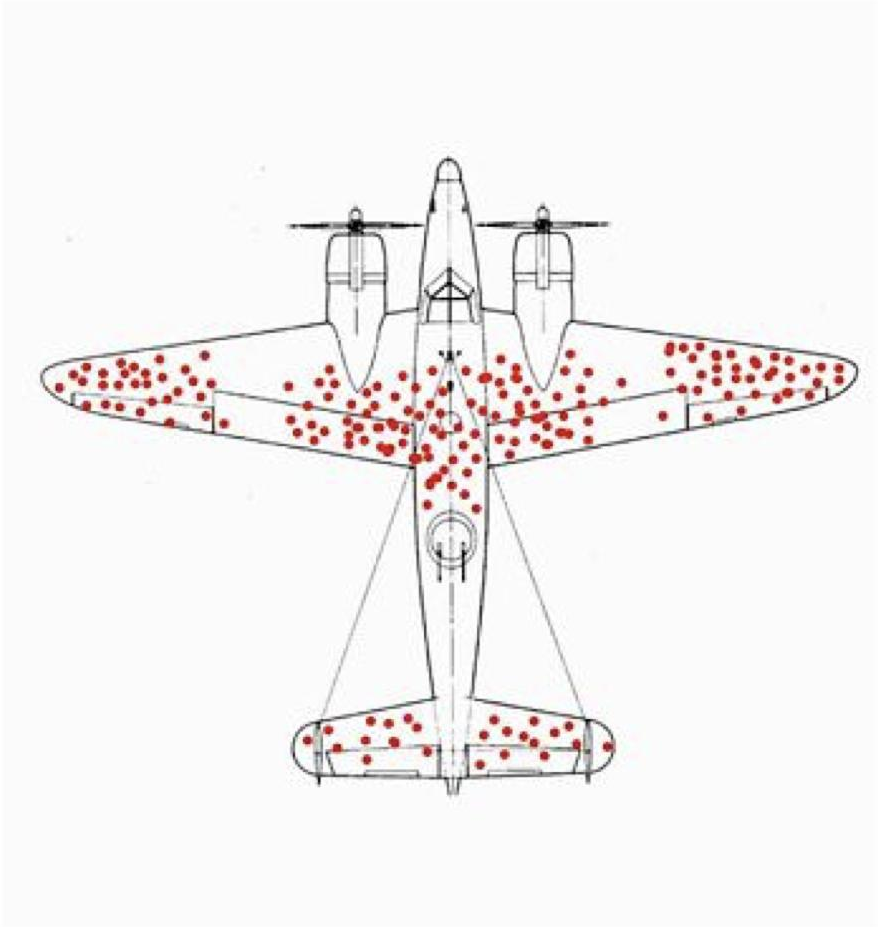
DEVOPS AUTOMATED GOVERNANCE REFERENCE ARCHITECTURE

Attestation of the Integrity of Assets in the Delivery Pipeline

You can't Lean, Agile, SAFE, Devops or even SRE your way around a bad organizational culture.


Organizational Anthropology

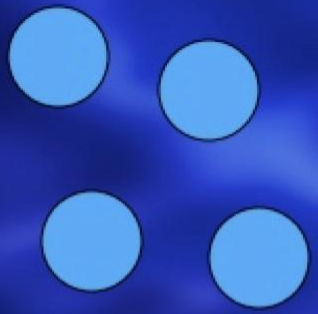

DevOps
Invisible Work
Capture All Work "Visible"
Management System Toil
Consolidate Work Management Systems
Misaligned Incentives
Collaboration, Coaching, Autonomy
Tribal Knowledge
Remove Bottlenecks and Institutionalize Knowledge
Incongruent Organizational Design
Inverse Conway Maneuver
Managing Complexity
Blameless Culture with Engineering Mindsets
Security and Compliance Theater
Work, Toil, Misalignment, Knowledge, Org Design, Complexity
Vulnerability Theater
Signal to Noise Ratio
Check Box Compliance
Review Boards (ARB, PRB,CAB)
DevSecOps
Auditor Alignment
Automated Governance



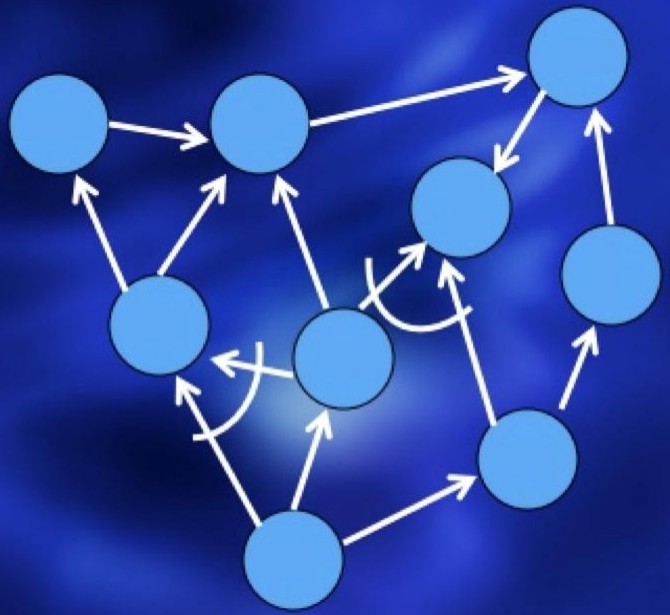
"What Abraham Wald found was a logical error known as Survival Bias"

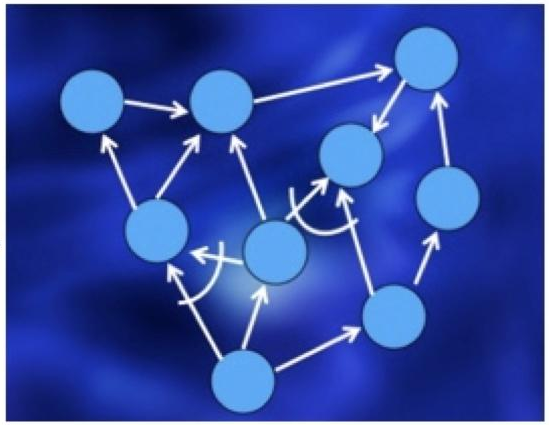
Complexity

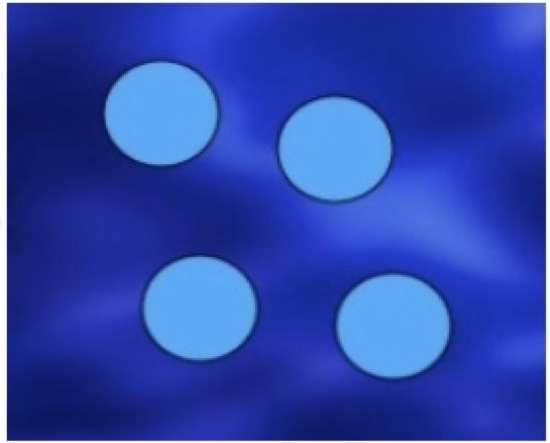
system A



system B







HTTP Request with curl containing Content-T

```
curl http://127.0.0.1:8900/struts2-showcase/
%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBEI
ntainer=#context['com.opensymphony.xwork2.Ac
nstance(@com.opensymphony.xwork2.ognl.OgnlUt
ar()).(#ognlUtil.getExcludedClasses().clear(
er.toString()) (#cmds=({'/bin/echo', #eps}))
java.lang.ProcessBuilder(#cmds)).(#p.redirec
rg.apache.struts2.ServletActionContext@getRe
o.IOUtils@copy(#process.getInputStream(),#rc

com.opensymphony.xwork2.inject.ContainerImpl
```

Former Equif ngle person who f

The company is still invest

By Russell Brandom | Oct 3, 2017, 1:03p

The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

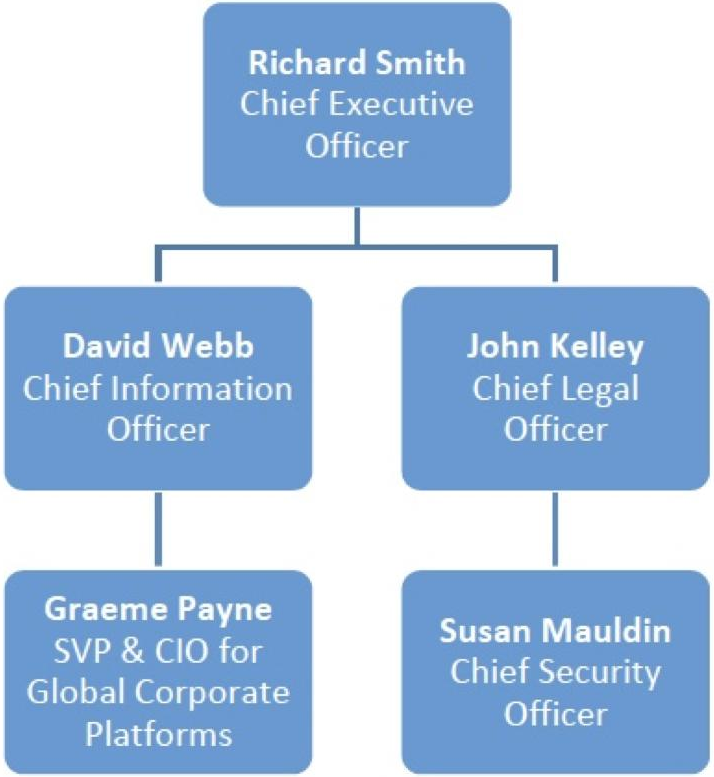
Conway's Law

An adage named after computer programmer Melvin Conway, who introduced the idea in 1967. It states that. "organizations which design systems ... are constrained to produce designs which are copies of the communication structures of these organizations."

The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018



The Equifax Data Breach

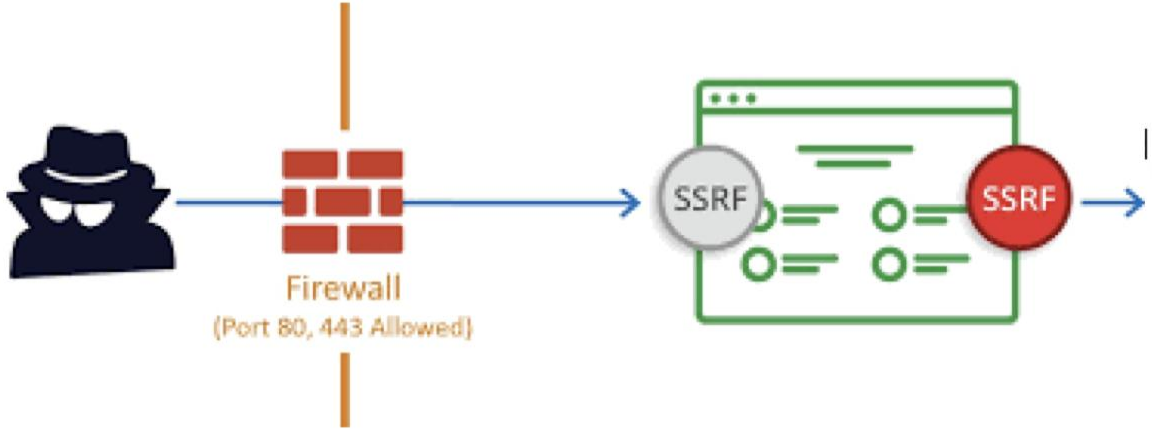
Majority Staff Report
115th Congress

December 2018

Based on information confirmed on July 31 by the lead forensic analyst, Mauldin stated "I felt like I knew at that point that PII had been involved in this incident."[247] She reported this to John Kelley on July 31, but did not inform David Webb.[248] Mauldin testified:

> Q. Is there any particular reason why you did not report to the CIO your belief that PII may have been exfiltrated in connection with the security incident we have been discussing?
>
> A. I don't remember a particular reason about that . . . . I just don't remember thinking about that.[249]

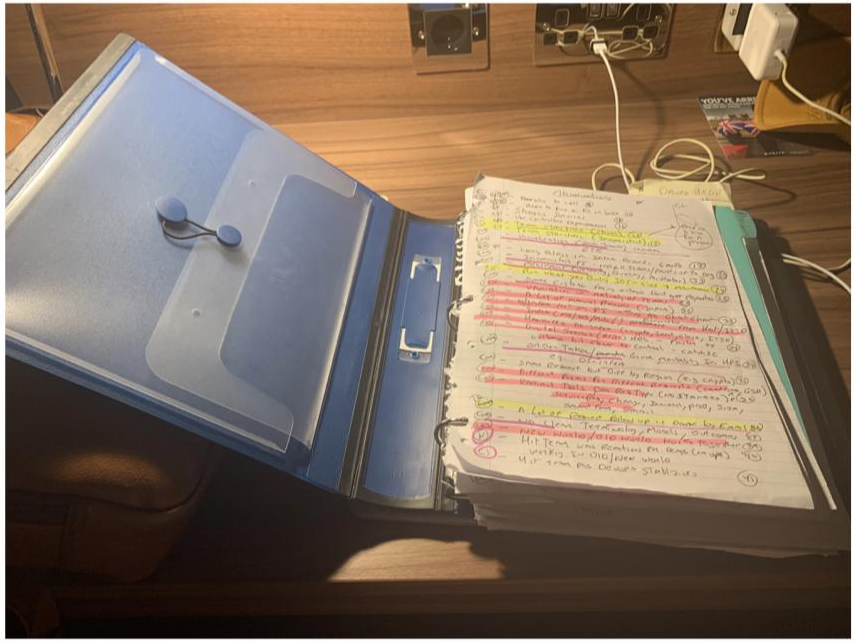
Capital One Data Breach Compromises Data of Over 100 Million



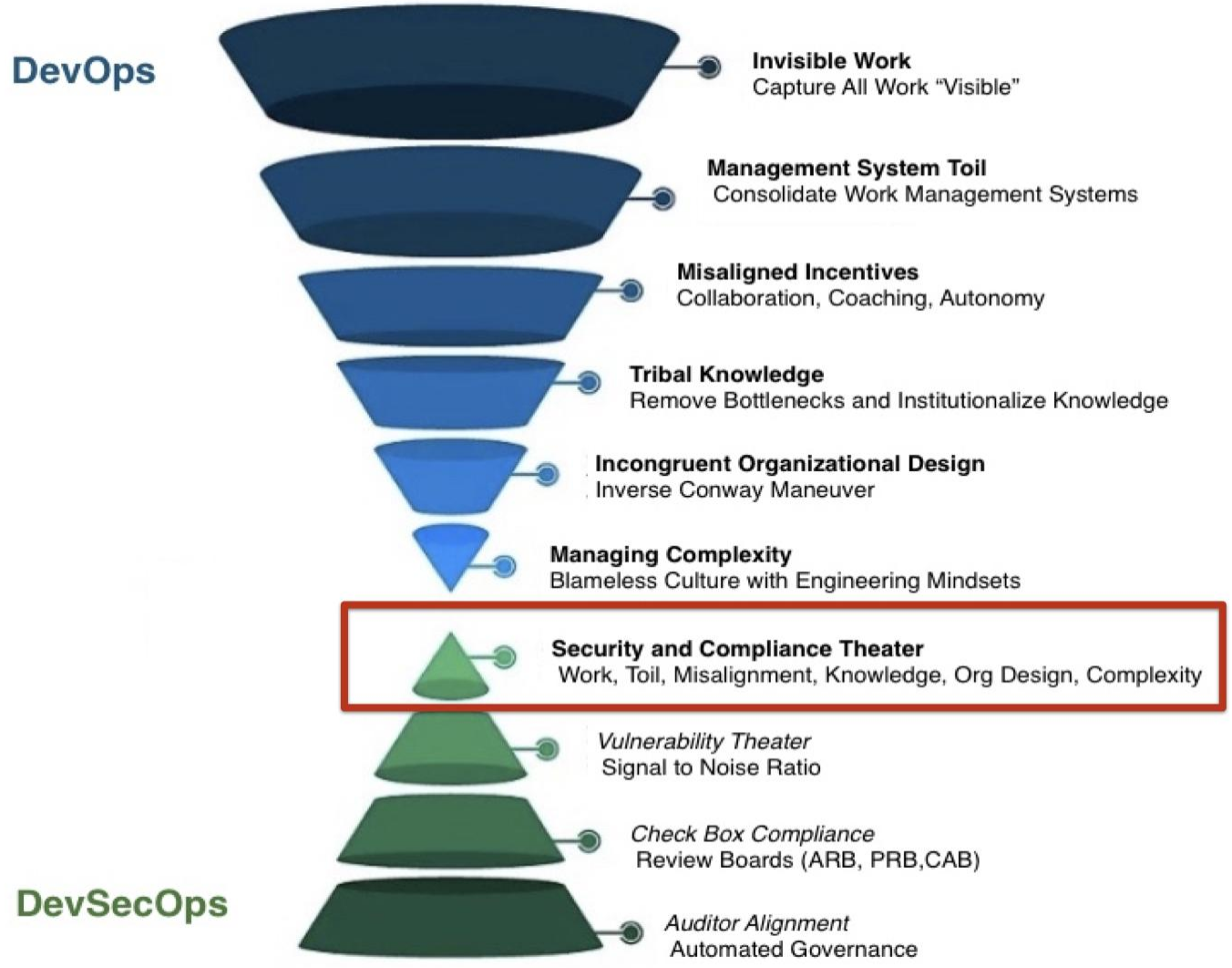

```
curl http://example.com/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/ISRM-WAF-Role
```

Organizational Anthropology

- 10 to 20 Pre-Assessment Calls
- 30 to 50 Assessment Meetings
- Interview 150-200 People
- Over 400 Pages of Notes
- 300 Summarized Observations



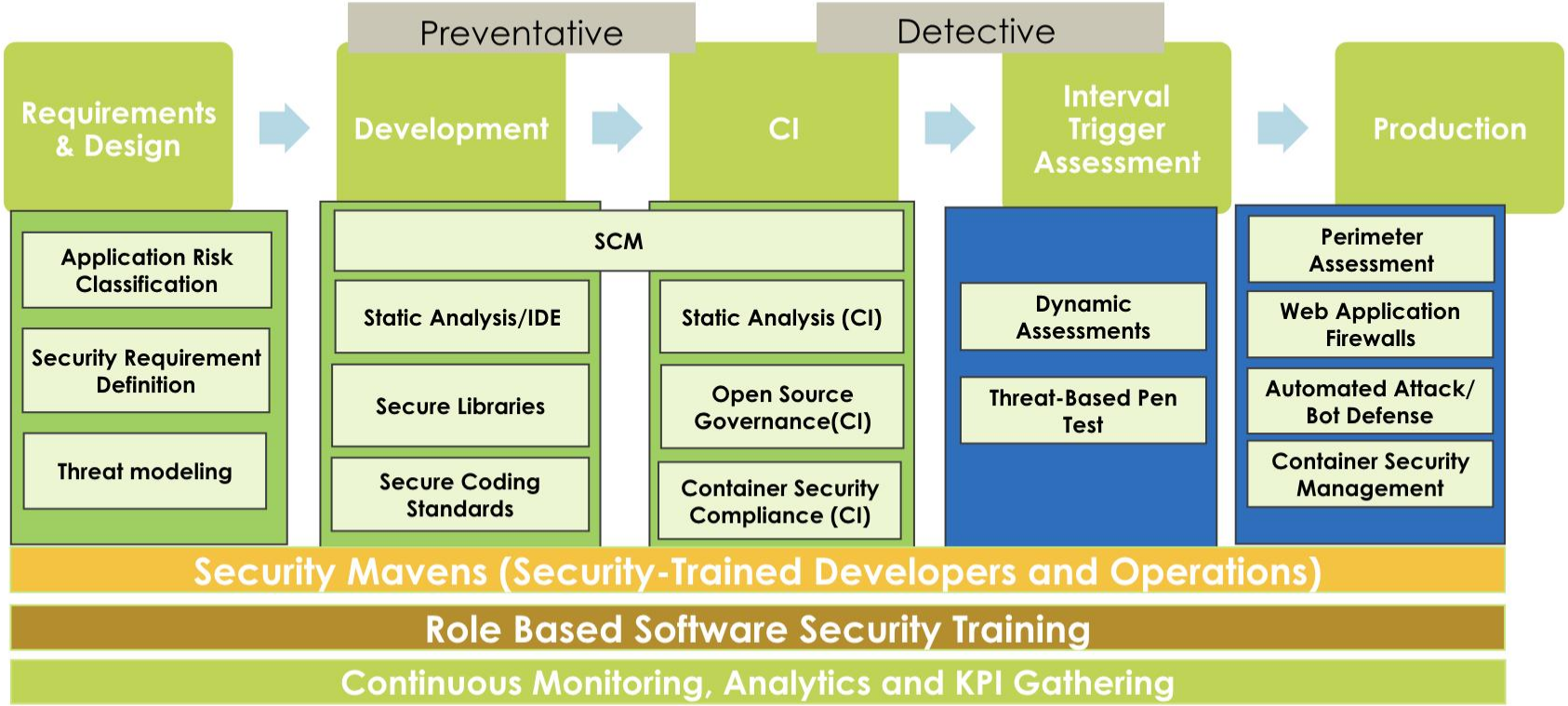
The Deadliest Disease!


DevOps
Invisible Work
Capture All Work "Visible"
Management System Toil
Consolidate Work Management Systems
Misaligned Incentives
Collaboration, Coaching, Autonomy
Tribal Knowledge
Remove Bottlenecks and Institutionalize Knowledge
Incongruent Organizational Design
Inverse Conway Maneuver
Managing Complexity
Blameless Culture with Engineering Mindsets
Security and Compliance Theater
Work, Toil, Misalignment, Knowledge, Org Design, Complexity
Vulnerability Theater
Signal to Noise Ratio
Check Box Compliance
Review Boards (ARB, PRB,CAB)
DevSecOps
Auditor Alignment
Automated Governance

Devops (Shift Left Auditors)

- Review Boards (ARB, PRB,CAB)
- Check Box Compliance
- Workarounds and Hidden Work
- Auditor Workarounds
- Vulnerability Theater
- Negative Risk RIO
- Policy Theater

DevSecOps


Preventative
Detective
Requirements & Design
Development
CI
Interval Trigger Assessment
Production
Application Risk Classification
Security Requirement Definition
Threat modeling
SCM
Static Analysis/IDE
Secure Libraries
Secure Coding Standards
Static Analysis (CI)
Open Source Governance(CI)
Container Security Compliance (CI)
Dynamic Assessments
Threat-Based Pen Test
Perimeter Assessment
Web Application Firewalls
Automated Attack/ Bot Defense
Container Security Management
Security Mavens (Security-Trained Developers and Operations)
Role Based Software Security Training
Continuous Monitoring, Analytics and KPI Gathering

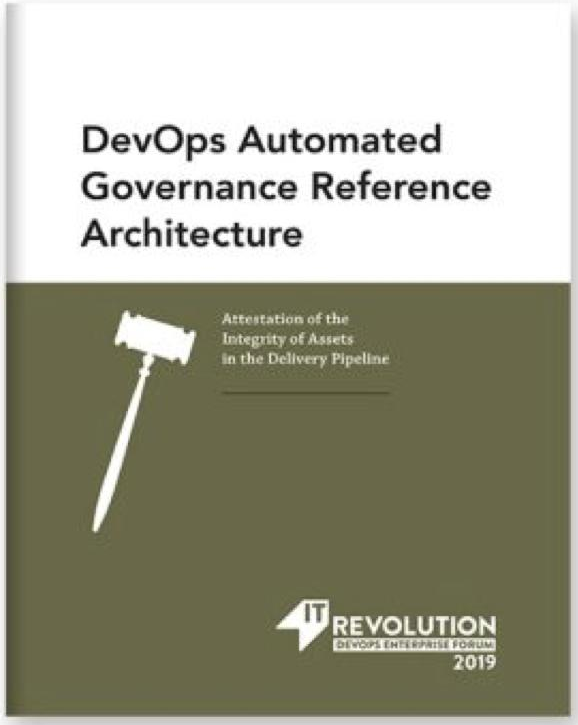
DevSecOps Operational Tips

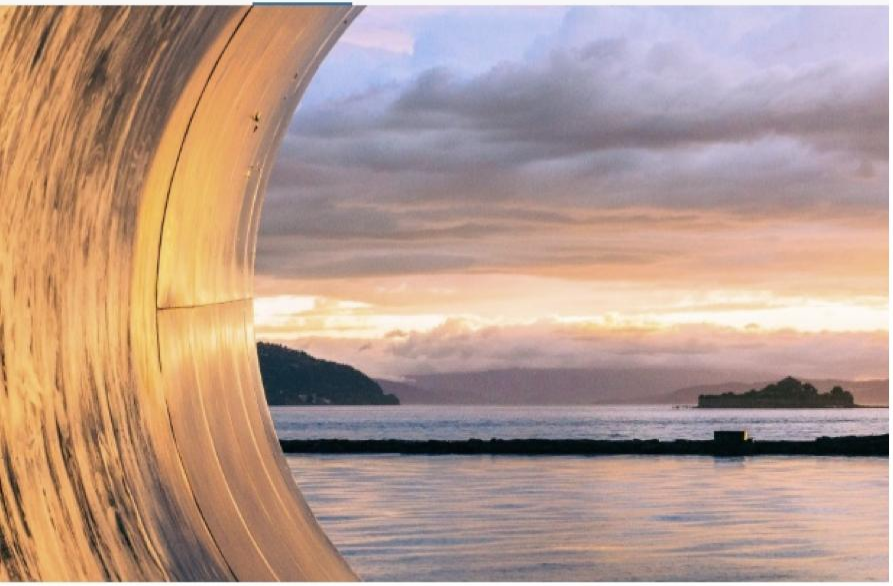
- Work with and educate your auditors
- Move Subjective Attestation to Objective Attestation
- Ruthlessly eliminate false positives to Developers
- Explain the vulnerabilities in business impact terms
- Devops the vulnerability (JIRA, backlog, Kanban)
- Open the code base to everyone in the organization
- Educate on how to fix

Changing subjective attestation into objective attestation

Devops Automated Governance

- **Attestation of the integrity of assets in the delivery pipeline**
  - **Automated Attestation in CI/ CD**
  - **Transform CAB (Change Advisory Board)**
  - **Reduce Effort w/ Compliance Activities - “Continuous Compliance”**





Focusing on the DevOps Pipeline

Creating Better Pipelines

So how do we design, measure, and improve our pipelines to avoid the above?

Pipeline Design

At Capital One, we design pipelines using the concept of the "16 Gates". These are our guiding design principles and they are:

- Source code version control
- Optimum branching strategy
- Static analysis
- >80% code coverage
- Vulnerability scan
- Open source scan
- Artifact version control
- Auto provisioning
- Immutable servers
- Integration testing
- Performance testing
- Build deploy testing automated for every commit
- Automated rollback
- Automated change order
- Zero downtime release
- Feature toggle

These gates are used to understand each and every product's progress through the DevOps process.

The Delivery Pipeline

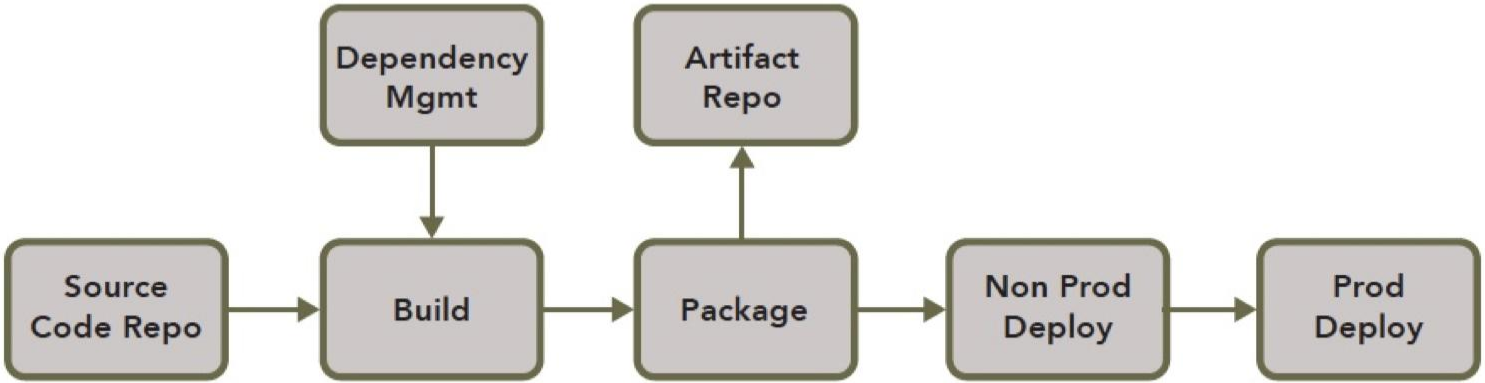
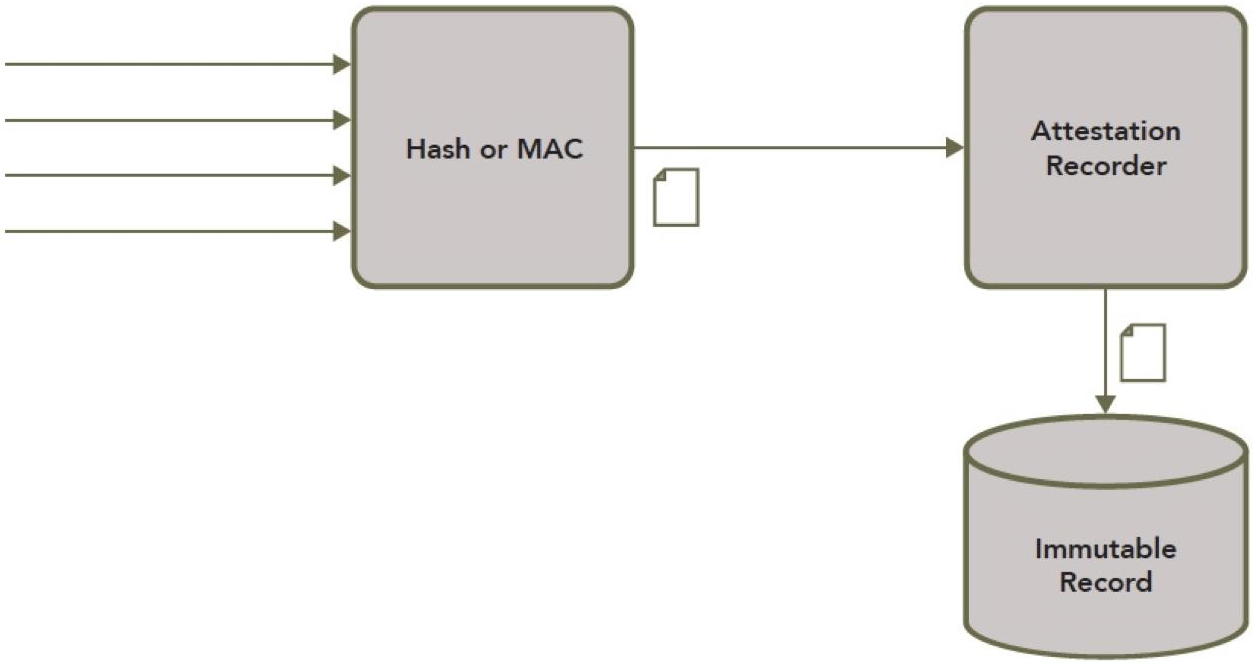
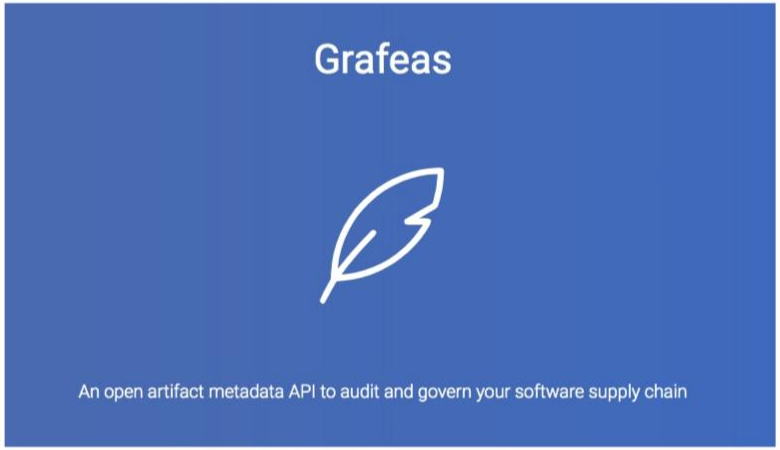


Figure 1: Delivery Pipeline

Constructing an Attestation



Attestation Database



Universal artifact metadata

Store, query, and retrieve critical metadata about all of your software artifacts, regardless of their type and where they are stored. Get 360-degree visibility across a variety of environments, including on-premises, private, and public cloud clusters.

Basic Governance Model

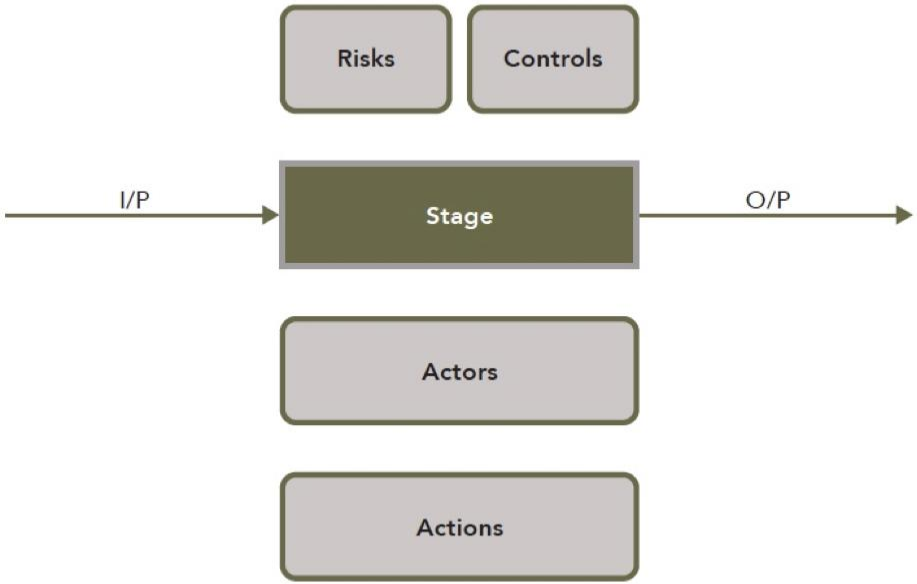
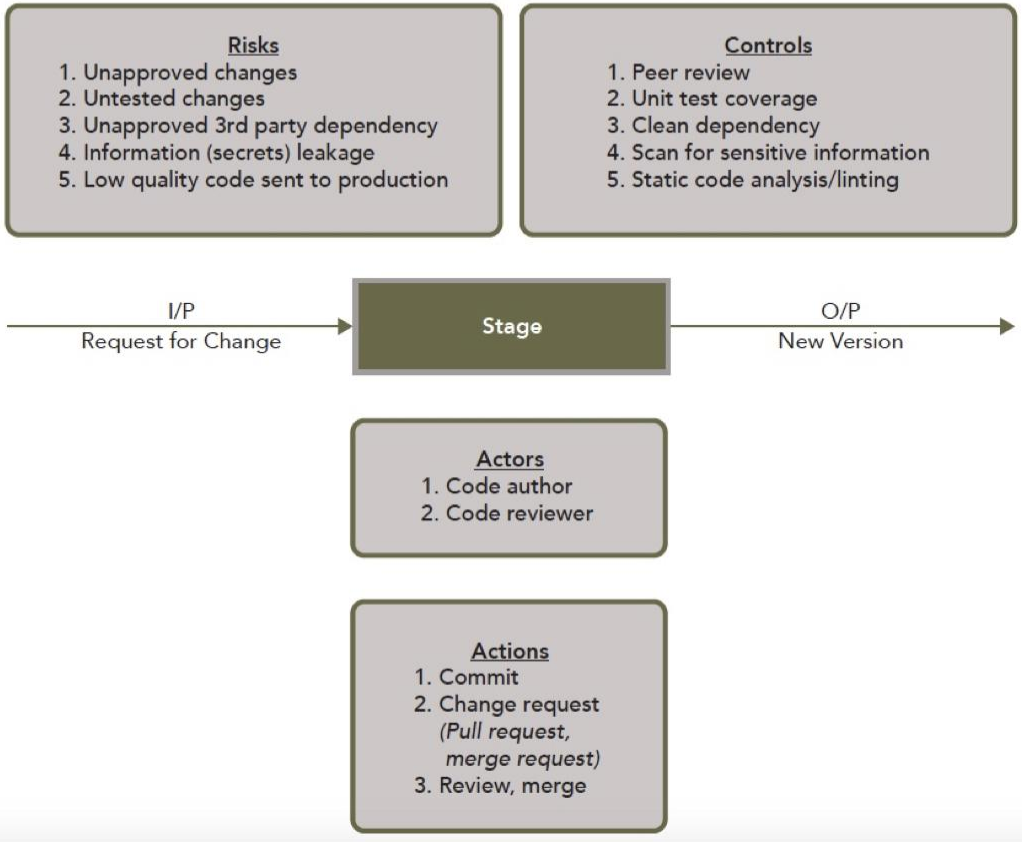
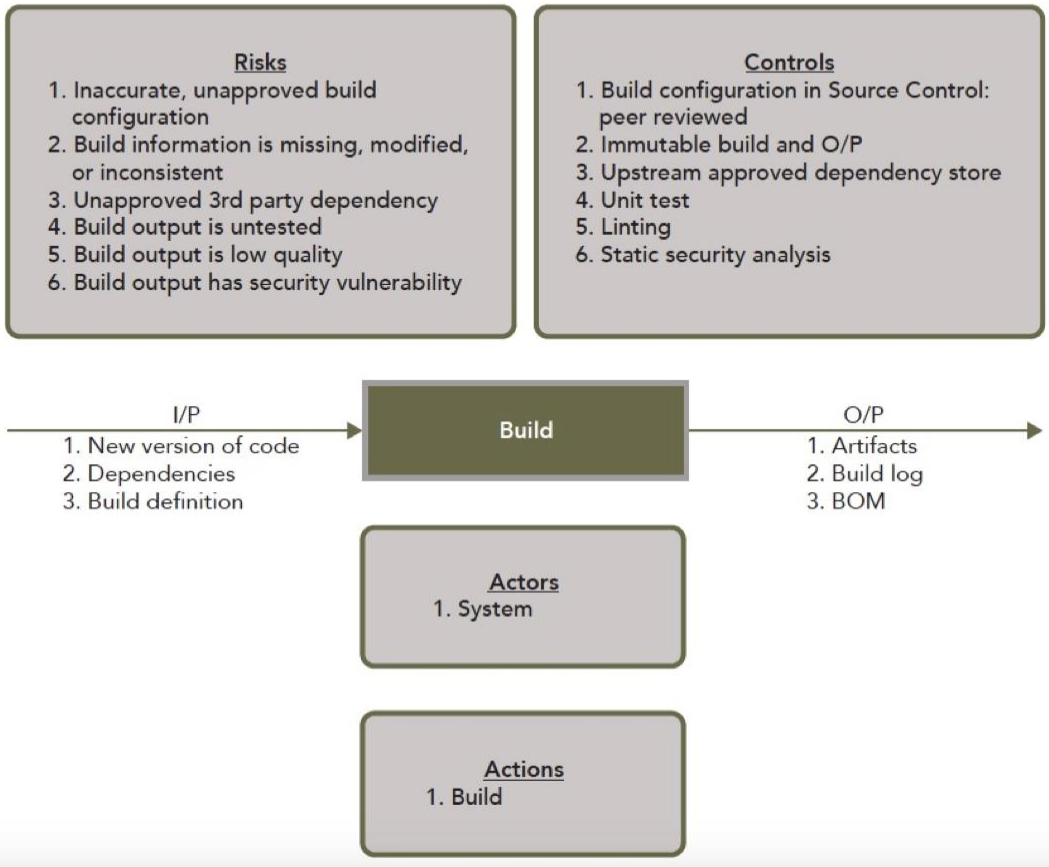


Figure 3: Basic Governance Model

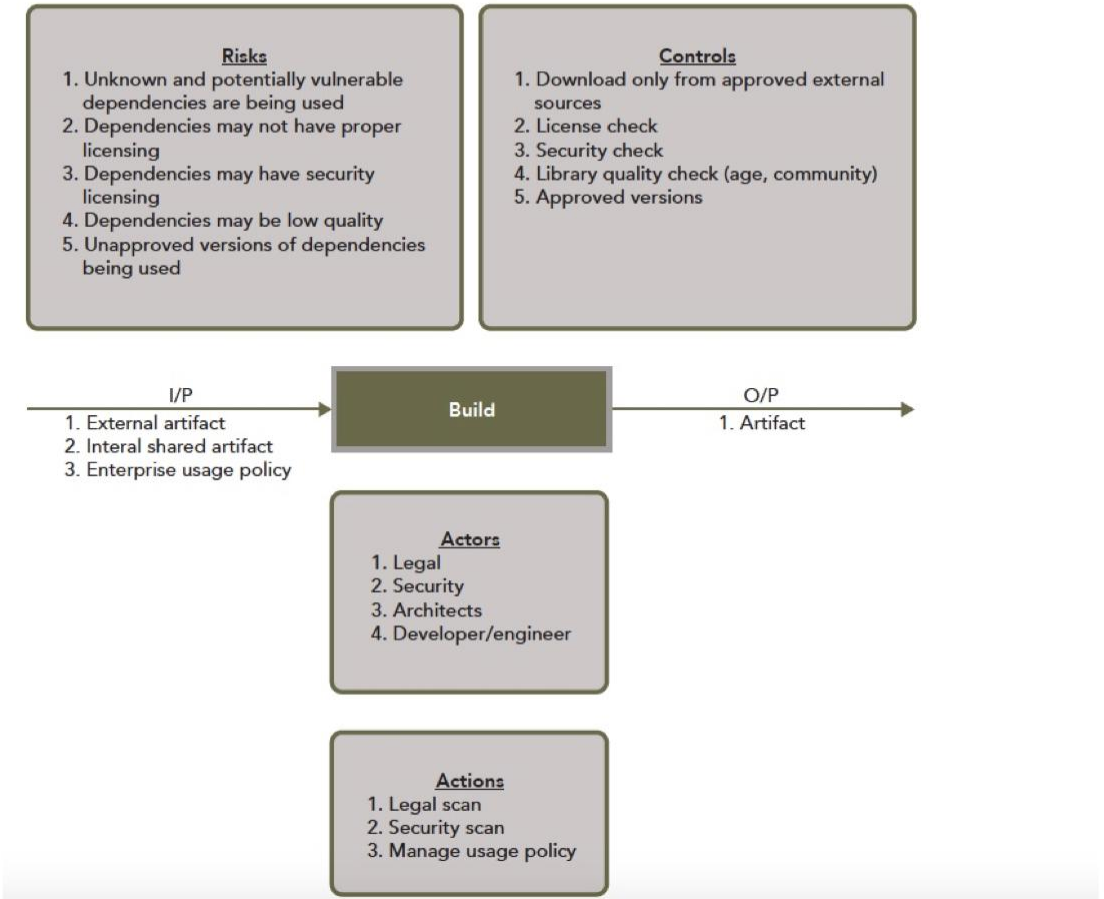
Source Code Repository Stage



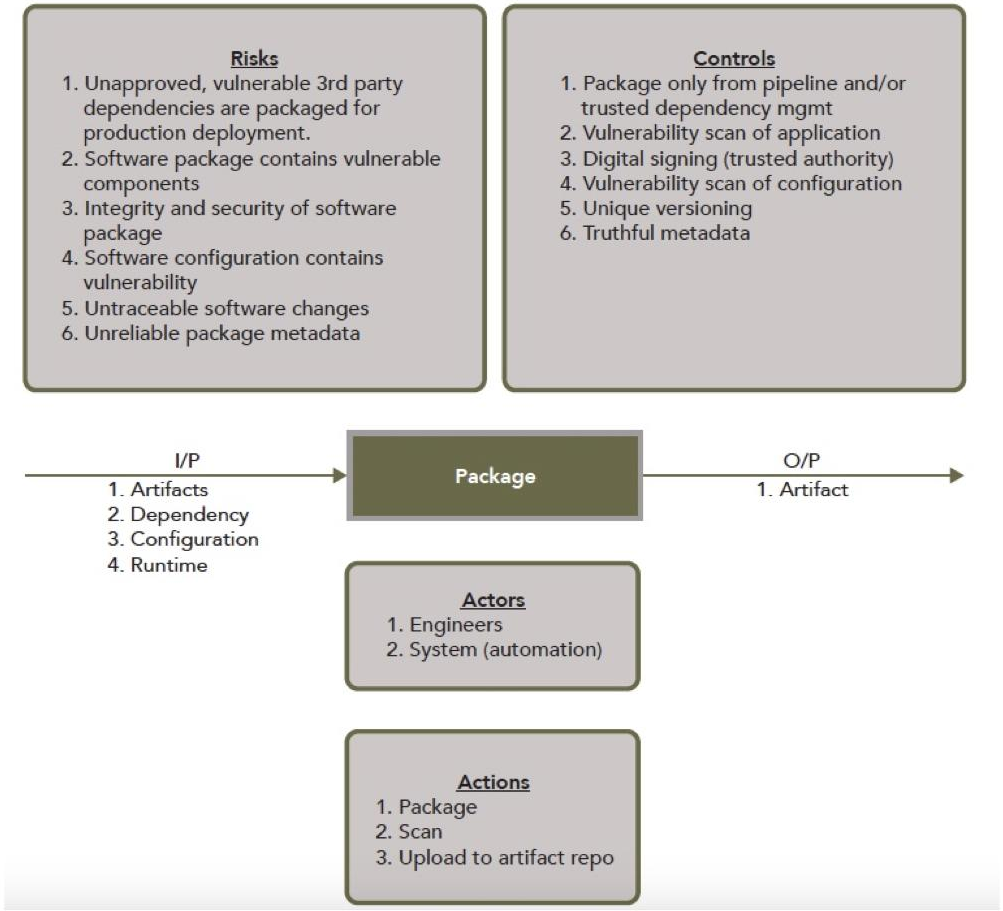
Build Stage


Risks
1. Inaccurate, unapproved build configuration
2. Build information is missing, modified, or inconsistent
3. Unapproved 3rd party dependency
4. Build output is untested
5. Build output is low quality
6. Build output has security vulnerability
Controls
1. Build configuration in Source Control: peer reviewed
2. Immutable build and O/P
3. Upstream approved dependency store
4. Unit test
5. Linting
6. Static security analysis
I/P
1. New version of code
2. Dependencies
3. Build definition
Build
O/P
1. Artifacts
2. Build log
3. BOM
Actors
1. System
Actions
1. Build

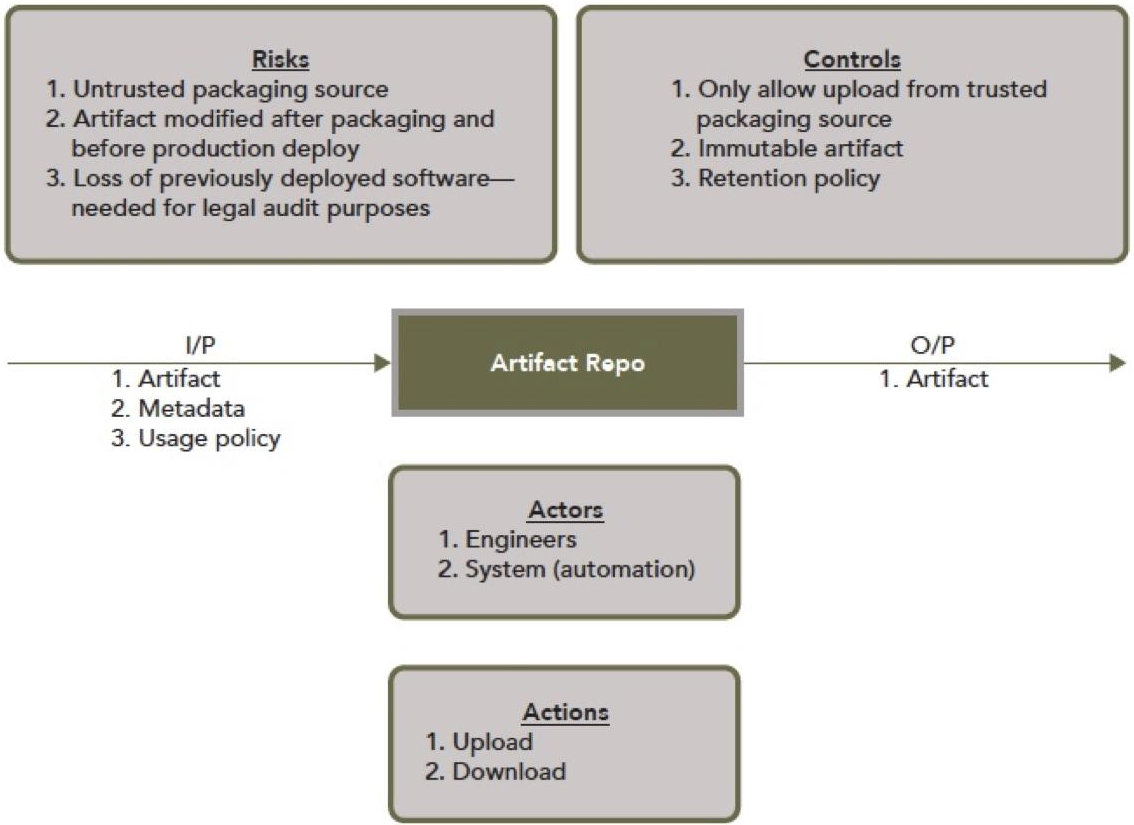
Dependency Management Stage



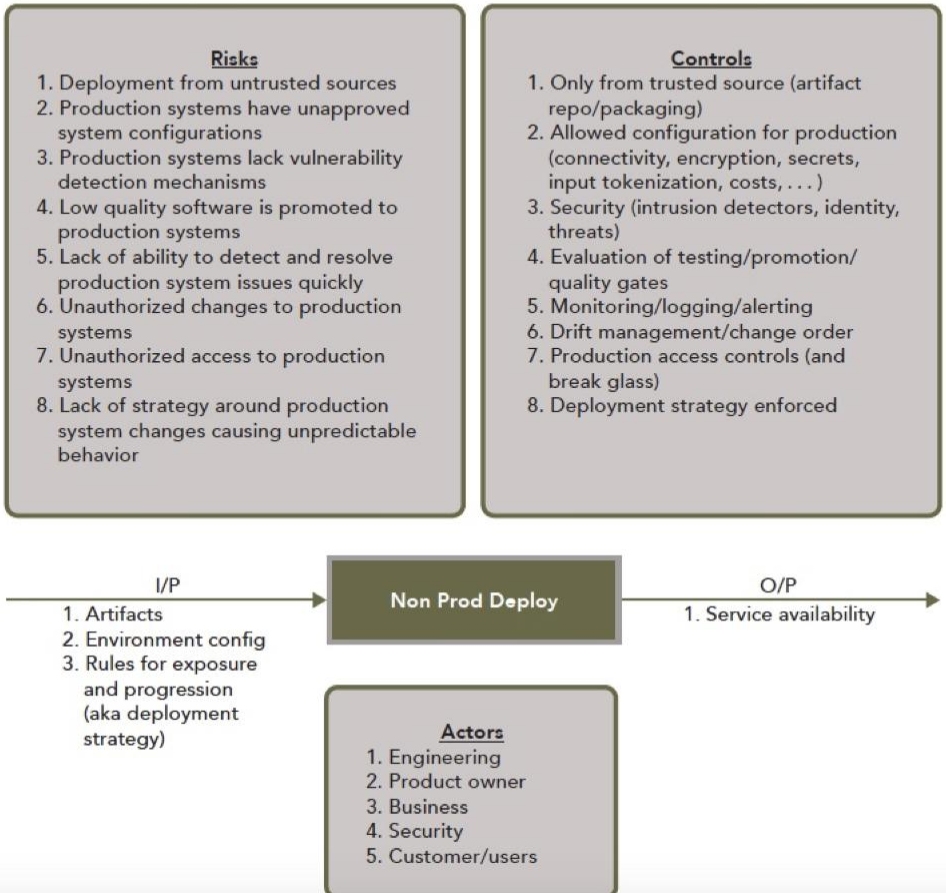
Package Stage



Artifact Stage



Prod Stage

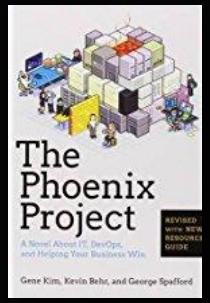

Risks
1. Deployment from untrusted sources
2. Production systems have unapproved system configurations
3. Production systems lack vulnerability detection mechanisms
4. Low quality software is promoted to production systems
5. Lack of ability to detect and resolve production system issues quickly
6. Unauthorized changes to production systems
7. Unauthorized access to production systems
8. Lack of strategy around production system changes causing unpredictable behavior
Controls
1. Only from trusted source (artifact repo/packaging)
2. Allowed configuration for production (connectivity, encryption, secrets, input tokenization, costs, . . .)
3. Security (intrusion detectors, identity, threats)
4. Evaluation of testing/promotion/ quality gates
5. Monitoring/logging/alerting
6. Drift management/change order
7. Production access controls (and break glass)
8. Deployment strategy enforced
I/P
1. Artifacts
2. Environment config
3. Rules for exposure and progression (aka deployment strategy)
Non Prod Deploy
O/P
1. Service availability
Actors
1. Engineering
2. Product owner
3. Business
4. Security
5. Customer/users

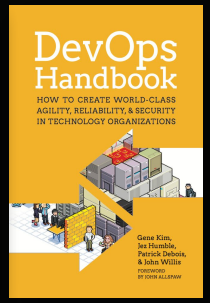
DevOps Resources

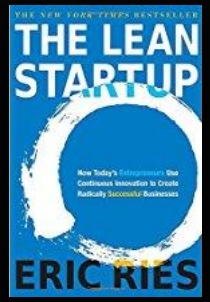
https://devopsfordefense.org/resources/

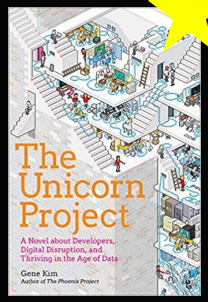
https://www.meetup.com/DevOps-for-Defense/
https://github.com/jondavid-black/DevOpsForDefense
devopsfordefense@gmail.com

Books / Publications:



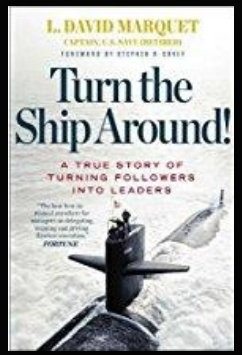


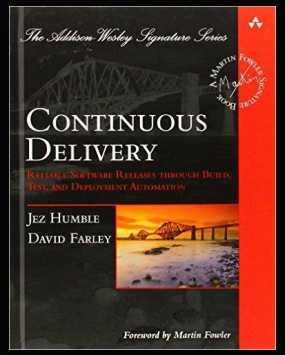


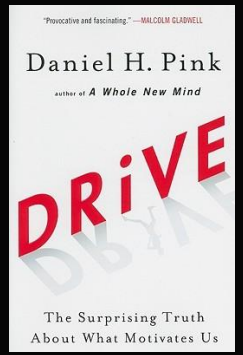


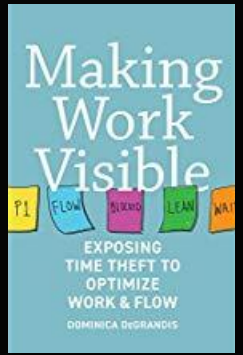
- DevOps Enterprise Summit (DOES)
- IT Revolution
- Velocity
- GoTo

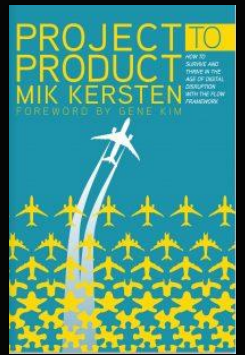
YouTube

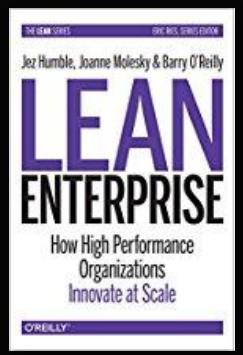


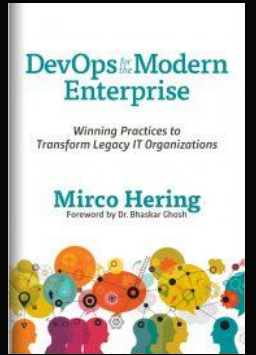






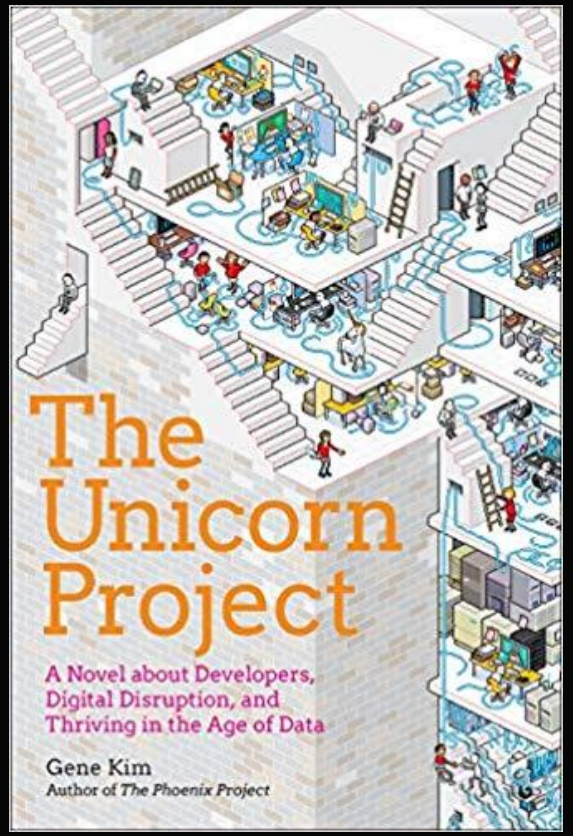






DevOps for Defense Book Club

Sponsored by: TEKsystems Own change



The Unicorn Project
By Gene Kim
Released Nov 26th, 2019

The 5 Ideals:

1. Locality & Simplicity
2. Focus, Flow, & Joy
3. Improvement of Daily Work
4. Psychological Safety
5. Customer Focus

Get your copy, put your name on the library card, read, and share!

Group Exercise: Lean Coffee

1. Each table has a facilitator.
2. The facilitator has a short introduction.
3. Everyone write down questions or topics for discussion on the subject. Place them in the middle of the table.
4. The group votes on each question or topic by placing a dot on the card. 3 votes per person.
5. Cards with most dots goes first. Set a timer for 5 minutes and discuss.
6. After 5 minutes, either vote (thumbs up/down) to keep going or move on to the next card.

Suggested Topics: “GitOps”, “Shift-Left”, “Git...All the Things!”