Security Automation with GitHub and AWS

Introduction to AWS Authority To Operate

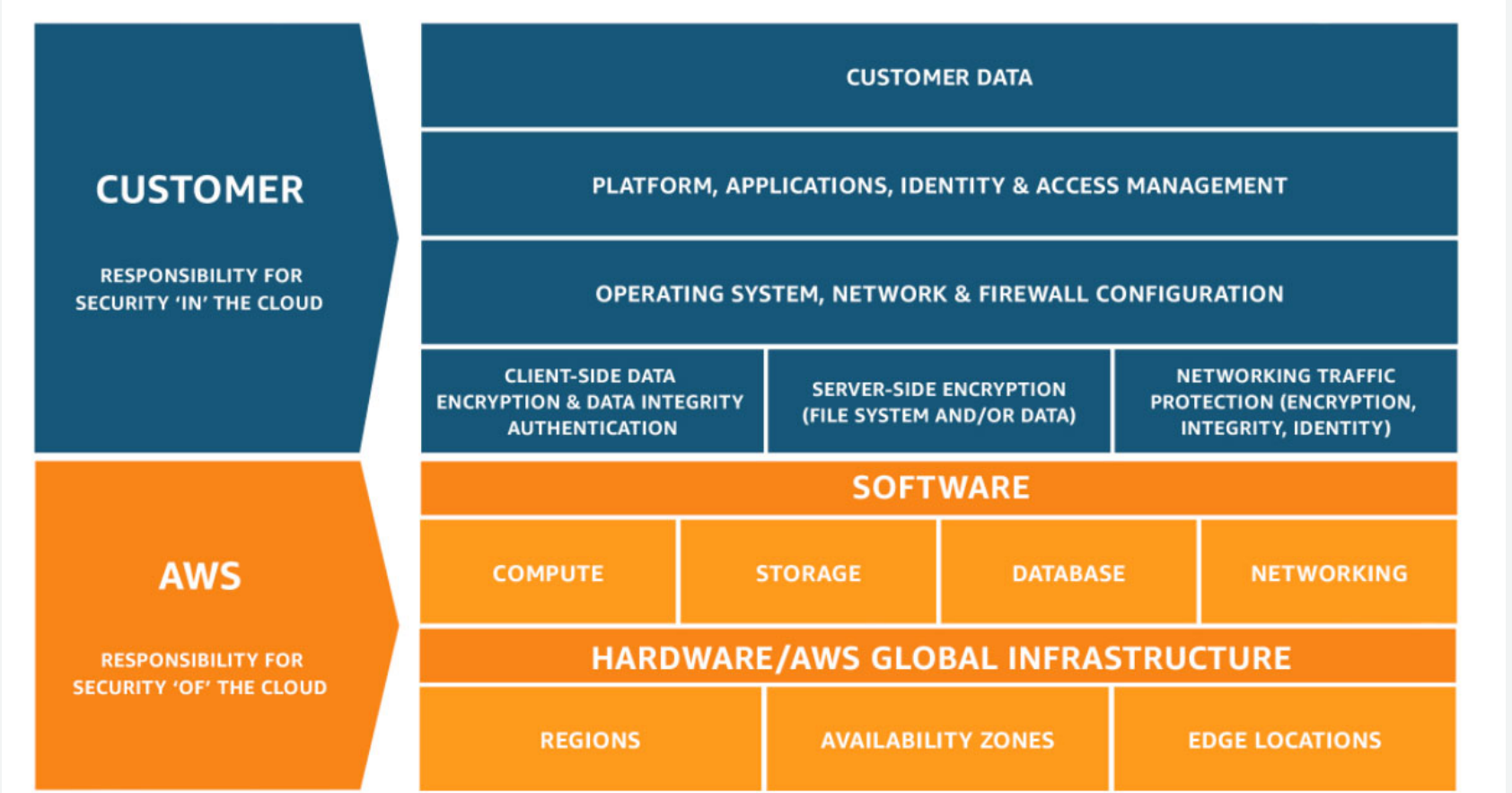
Eric Baran - Segment Lead – DevOps – AWS
Natalie Bradley – Solutions Engineer - GitHub

SESSION OVERVIEW

- DevSecOps – Authority to Operate on AWS
    - What is Secure DevOps?
    - What happens to our regulated customers today, in adopting DevSecOps models?
    - Introduction to Security Automation and Orchestration.
- Why GitHub
    - Developing Collaboratively and Securely
    - Shift to the Left mentality – Everything as Code

aws

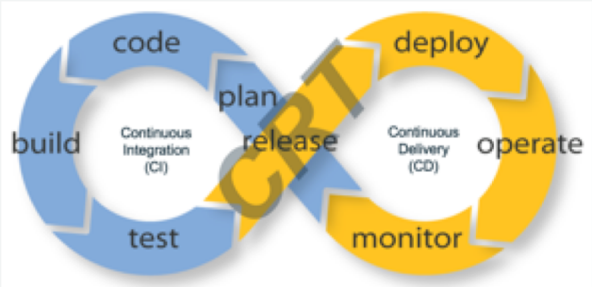
AWS Shared Responsibility Model



Solution Overview: SAO

Develop an **AWS Security Automation and Orchestration (SAO)** repository for constraining, tracking, publishing continuous security configurations, integration, deployments and treatments which are certified against common security frameworks (e.g. FedRAMP, DoD CC SRG, IRS 1075,CIS, PCI, etc.)

SAO will facilitate the orientation and association of **DevOps** and **Security** practices, changes and coordination of **Continuous Integration (CI)**, **Continuous Delivery (CD)** and **Continuous Risk Treatment (CRT)*** of an AWS customer account and/or multiple accounts.



* CRT is a process and technology approached which is designed to detect, maintain and in *MOST* case correct security, compliance and threats associated with an organization's solution and service deployment within their AWS account. CRT processes monitor security controls in real-time to ensure the risk and/or threat treatment (Control Intent) is working as designed or at least within an intended margin of acceptance base on guard rails, swim lanes and/or rules built into the control to allow for business operations.

Regulatory Standards – What will SAO Satisfy? – Phase One

1. The Payment Card Industry **Data Security** Standard (**PCI DSS**)
2. Defense Federal Acquisition Regulations Supplement (**DFARS**) NIST SP 800-171
3. Federal Risk and Authorization Management Program (**FedRAMP**) (**Moderate-Impact**)
4. Federal Risk and Authorization Management Program (**FedRAMP**) (**High-Impact**)
5. Department of Defense (*DoD*) Cloud Computing Security Requirements Guide (*SRG*) **Impact Level (*IL) 2***
6. Department of Defense (*DoD*) Cloud Computing Security Requirements Guide (*SRG*) **Impact Level (*IL) 4***
7. Internal Revenue Service (*IRS*) **Publication *1075* Tax Information Security Guidelines**
8. Minimum Acceptable Risk Standards for Exchanges (***MARS-E***) 2.0
9. The Criminal Justice Information Services Division (**CJIS**)
10. The Center for Internet *Security* (CIS)– Critical Security Controls
11. The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679)

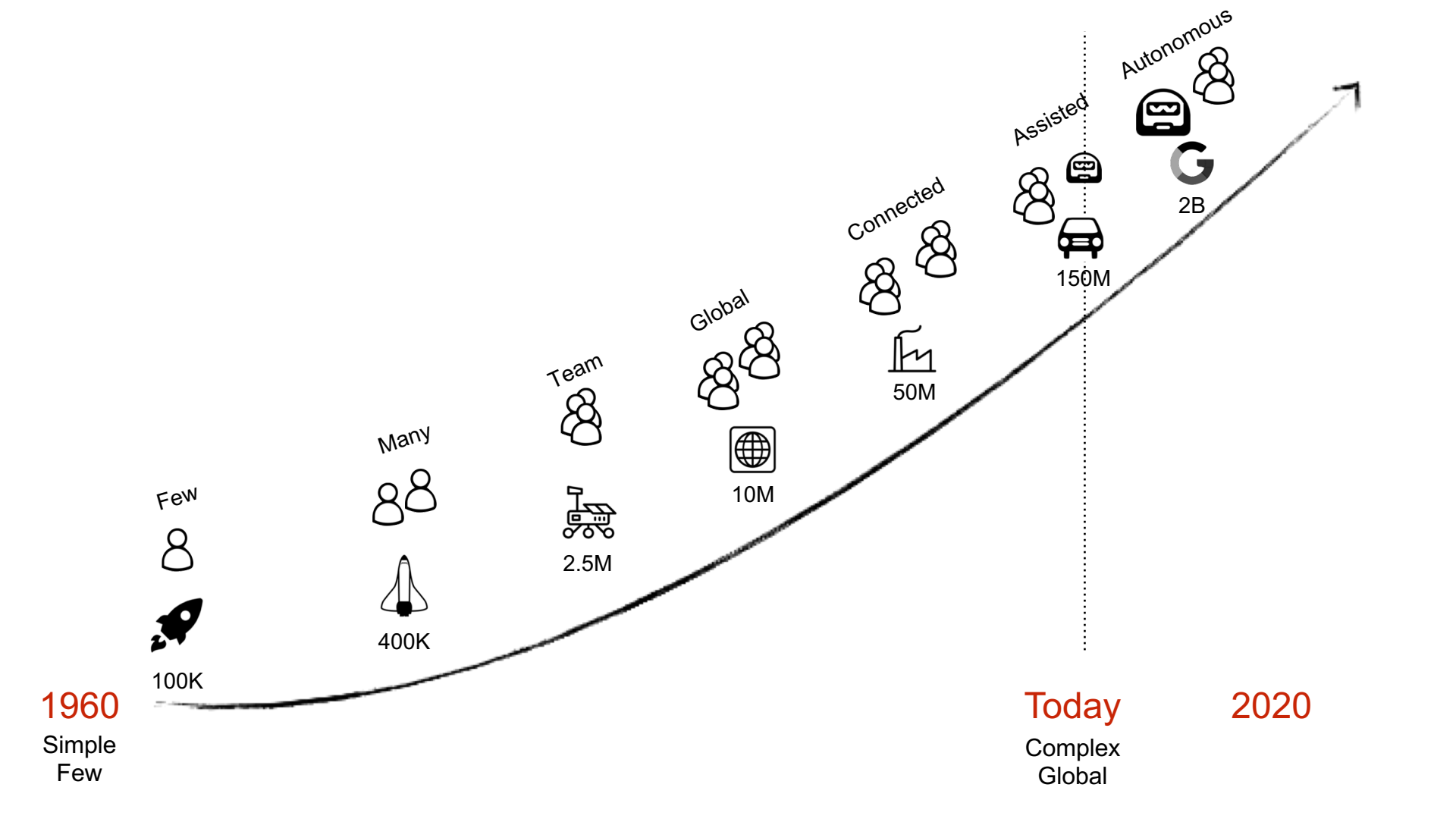
aws

SAO Community (to date) - Who's involved?

Software and DevSecOps overview GitHub + AWS

"The Evolution of Software and Why We Evolved to DevSecOps"

aws


Few
100K
Many
400K
Team
2.5M
Global
10M
Connected
50M
Assisted
150M
Autonomous
2B
1960
Simple
Few
Today
Complex
Global
2020

PERIODIC TABLE OF DEVOPS TOOLS (V2) (V1)

EMBED DOWNLOAD ADD

Os	Open Source
Fr	Free
Fm	Freemium
Pd	Paid
En	Enterprise

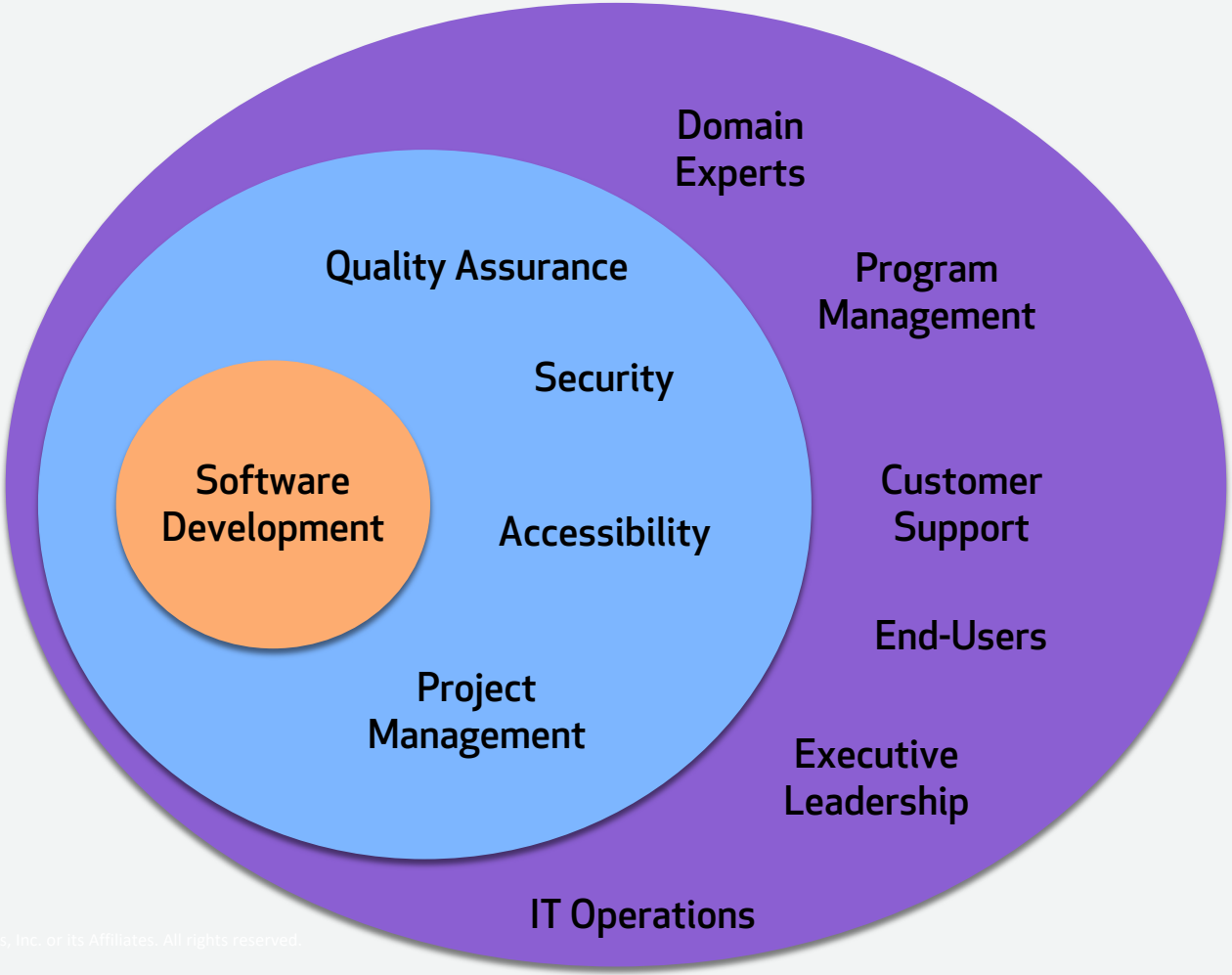
SCM	Database Mgmt	Build
CI	Repo Mgmt	Testing
Deployment	Config / Provisioning	Containerization
Cloud / Iaas / Paas	Release Mgmt	Collaboration
BI / Monitoring	Logging	Security

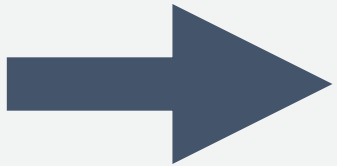
1 Fm Gh Github																		2 Fm Aws Amazon Web Services
3 Os Gt Git	4 Pd Dm DBmaestro												5 En Ch Chef	6 En Pu Puppet	7 Os An Ansible	8 En Sl Salt	9 Os Dk Docker	10 Pd Az Azure
11 Fm Bb Bitbucket	12 Os Lb Liquibase												13 Os Ot Otto	14 En Bl BladeLogic	15 Os Va Vagrant	16 Fr Tf Terraform	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

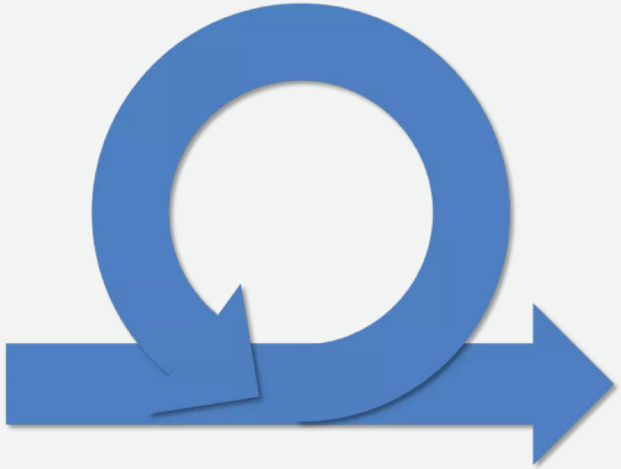
XebiaLabs
Deliver Faster

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







Problem Statement – Why can’t we be Agile?

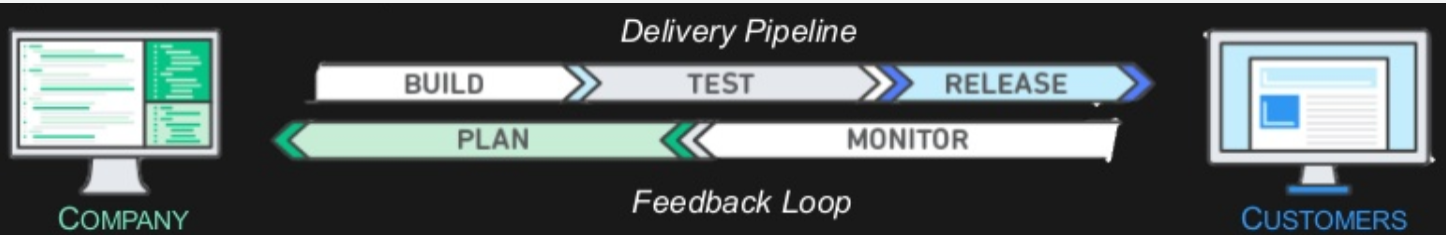
Security and risk management leaders continue to labor over **“How”** do they secure current, legacy and cloud resources consistently within their limited constraints.

While cloud services has provided streamlined ways to achieve innovation through the principles of DevSecOps and Developer Self-Service, regulated customers are still under mandate to follow strict security, governance, and accreditation standards, which are delivered during the production deployment phase.

aws

WHAT IS DEVSECOPS?

- Union of software development and operations
- Migration of Agile continuous development into continuous integration, continuous delivery, and continuous compliance.
- DevSecOps Model
  - No Silos – Puts emphasis on communication, collaboration and cohesion between disciplines
  - Best practices for change, configuration, and deployment automation
  - Deliver apps/services at a faster pace
  - High speed product updates
  - Everything is code



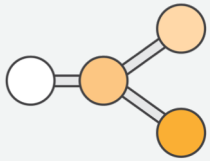
DEVSECOPS PROCESSES: 4 MAJOR PHASES

- Check-in source code
- Peer review new code

- Compile code
- Unit tests
- Style checkers
- Code metrics
- Create container images

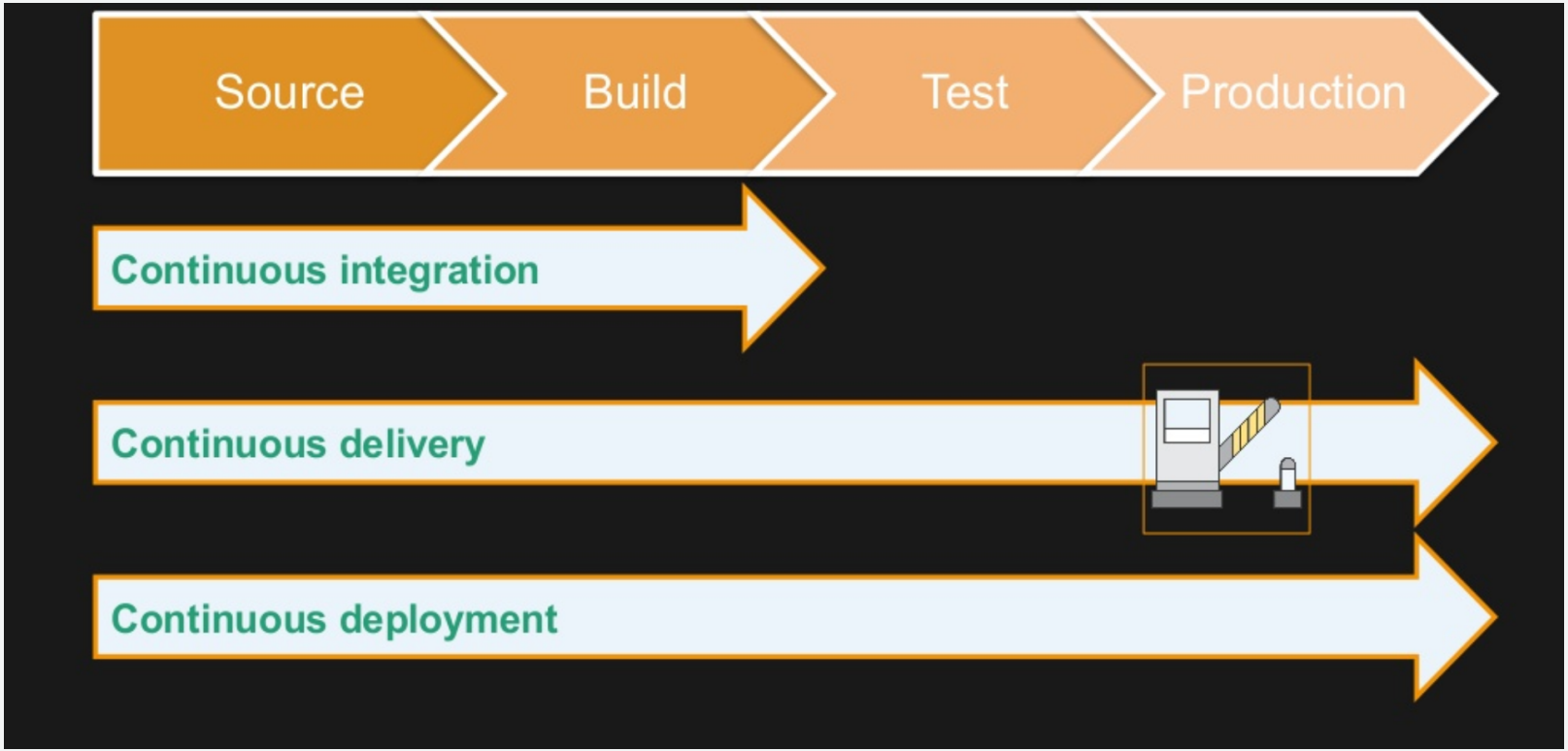
- Integration tests with other systems
- Load testing
- UI tests
- SecOps Scanning

- Deployment to production environments
- Continuous Monitoring



aws

DEVSECOPS RELEASE PROCESSES: LEVELS



aws

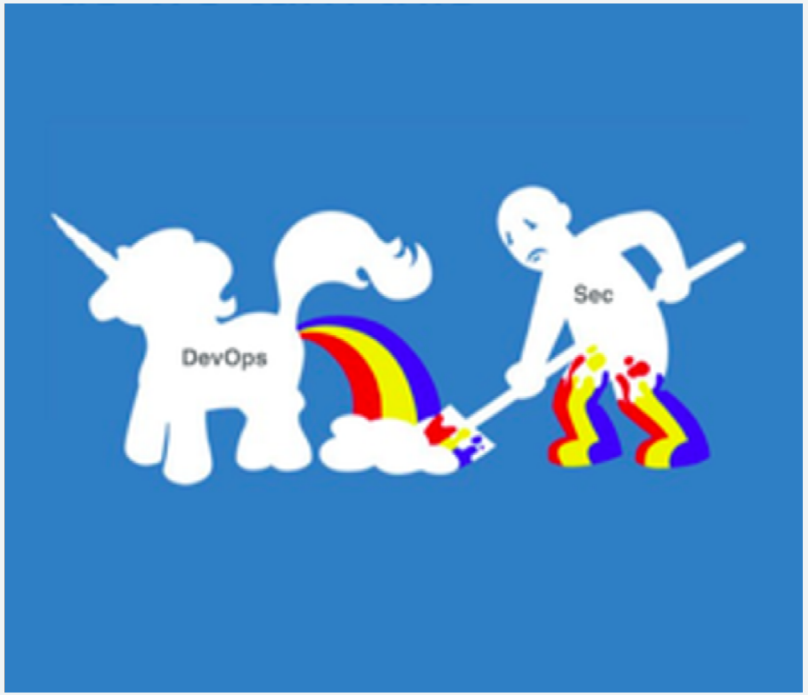
Developer Self-Service – In a Compliance Oriented World

DevOps enables the CI/CD pipeline which is the basis of automation within AWS.

The biggest challenge is breaking out of the traditional security structures and eliminating the divide between developers, operations, and security.

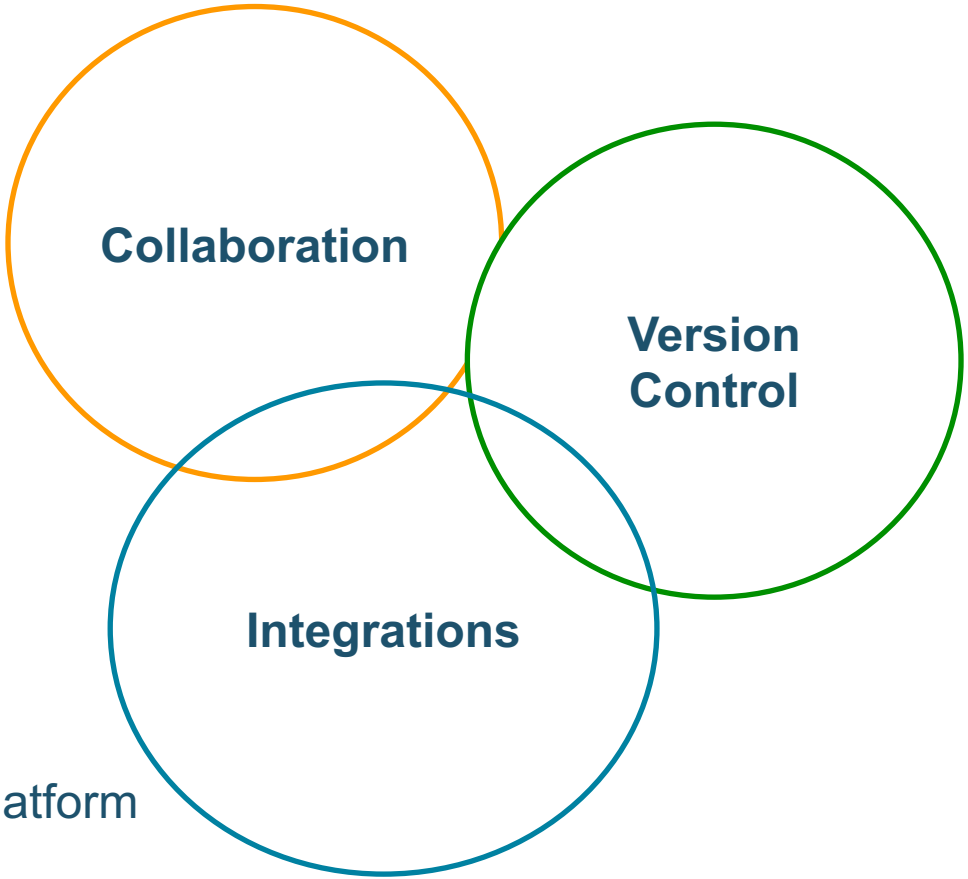
The CI/CD pipeline is the foundation for creating a repeatable, reliable and constantly improving process for taking software from concept to a secure, complaint production solution.

AWSome! But what actually happens in Regulated environments today?



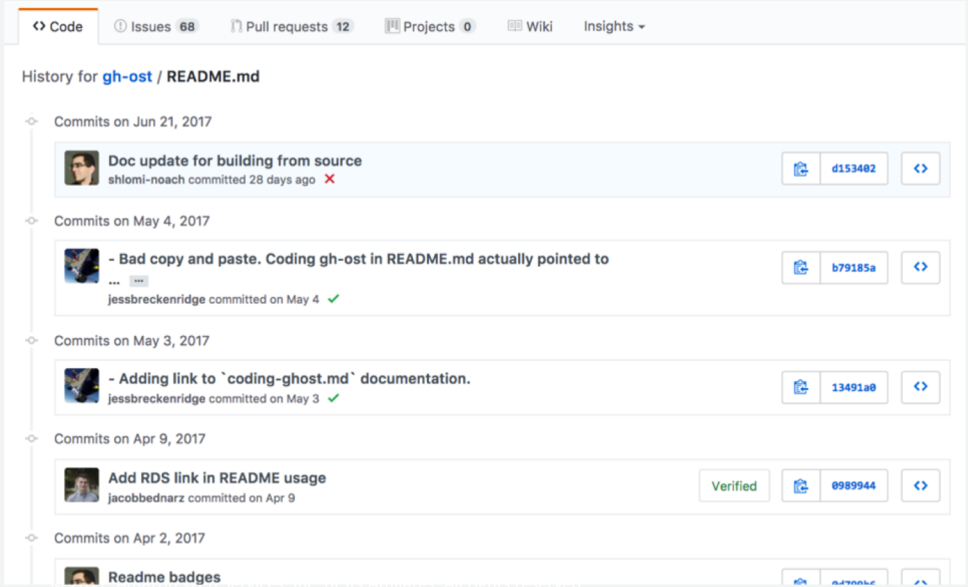
GitHub: The Software Development Platform

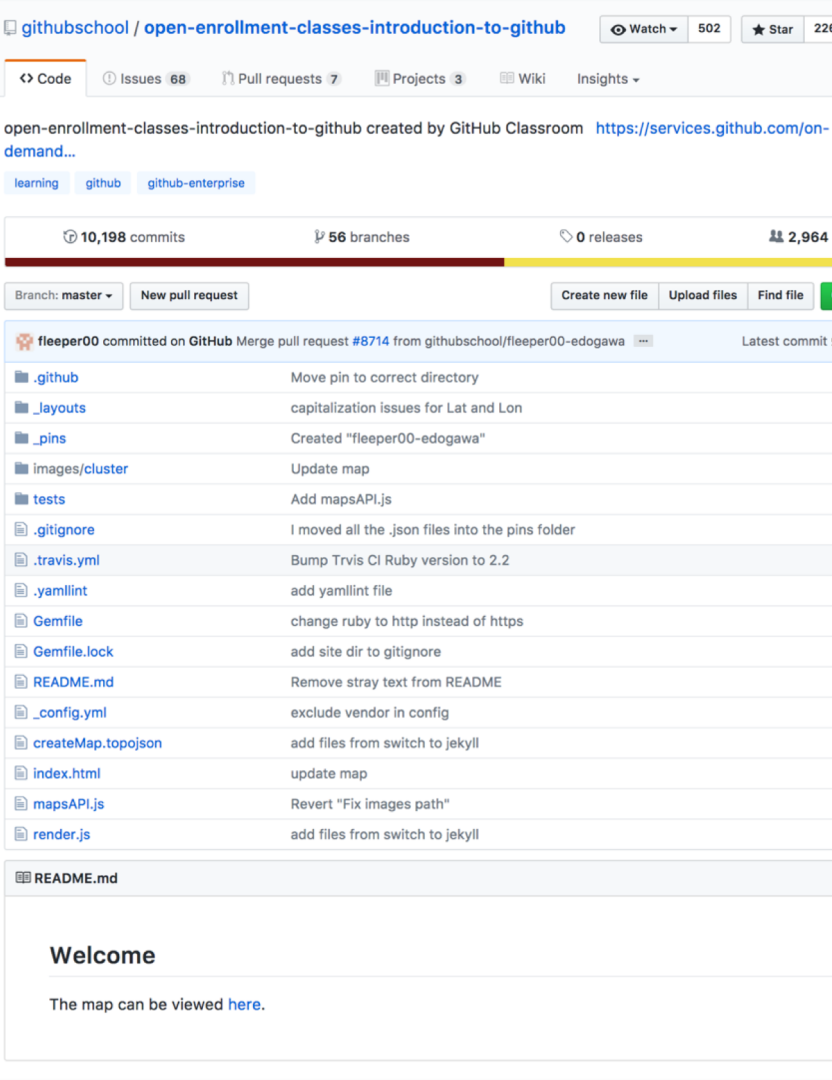
aws

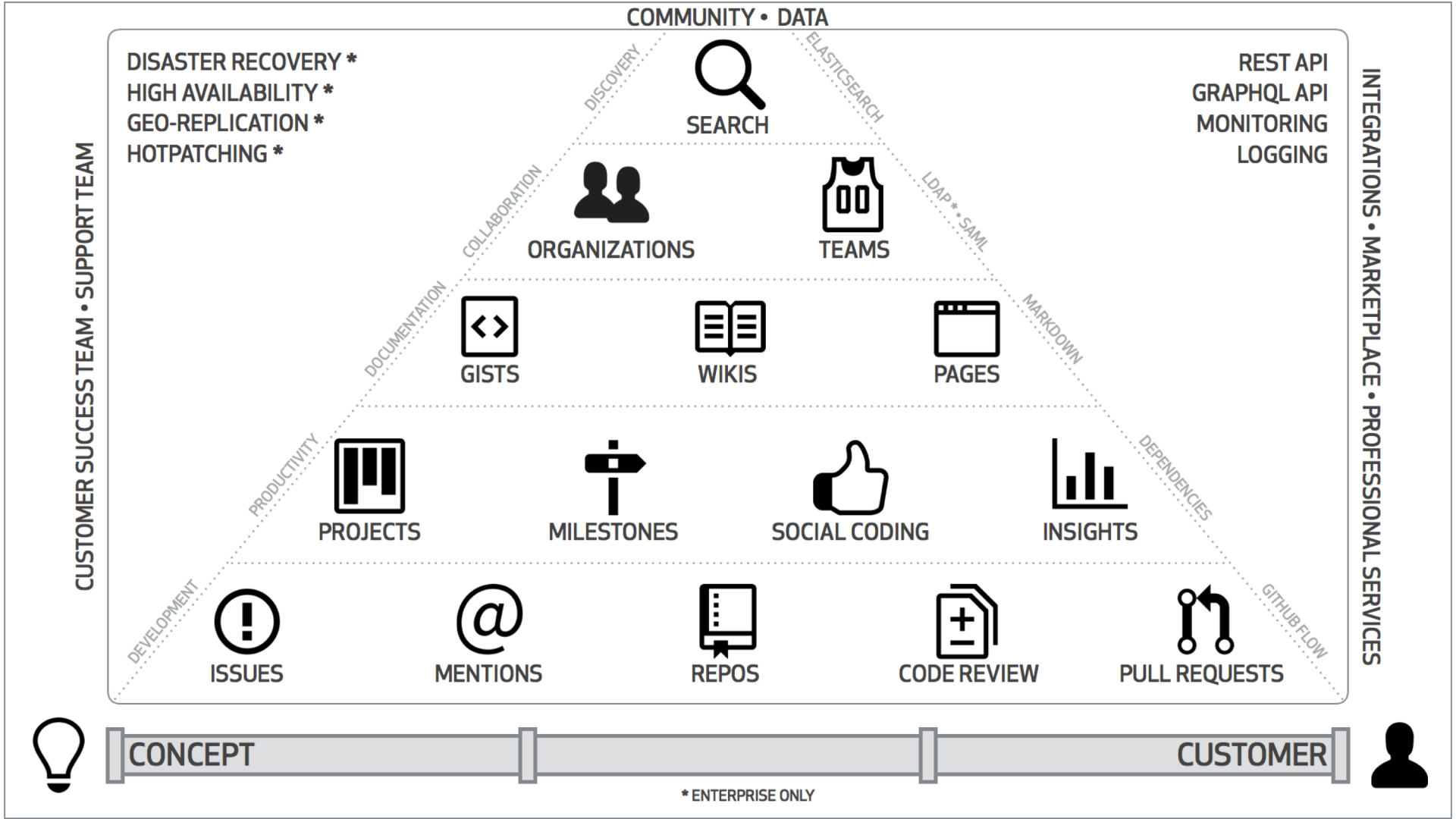


The Software Development Platform

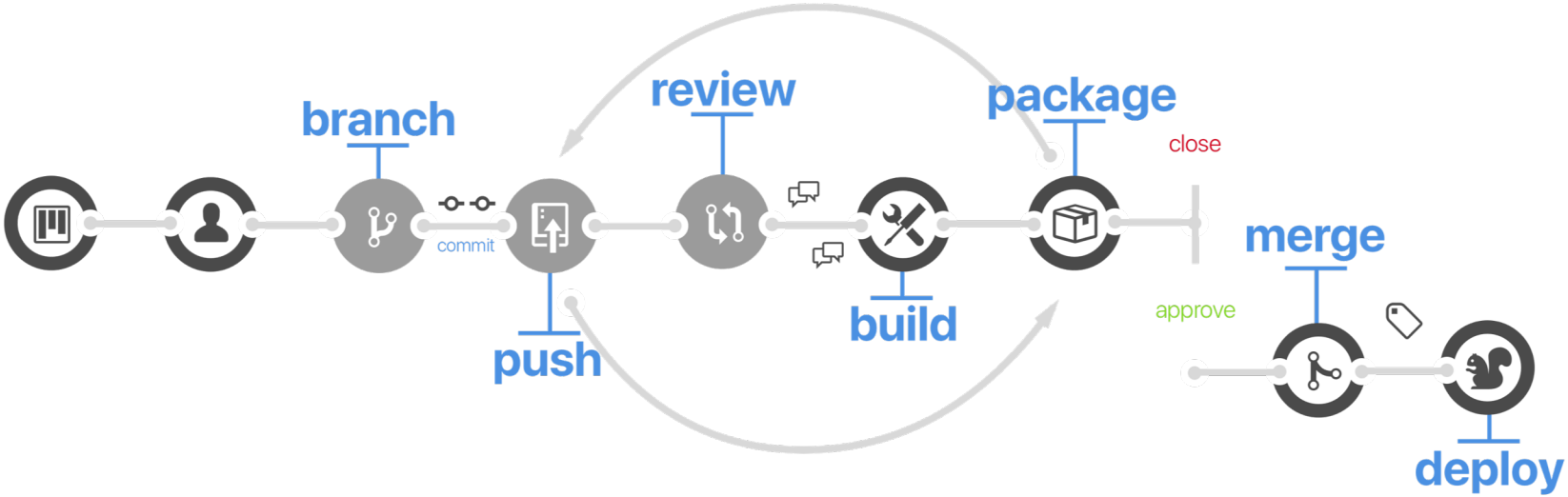
Version Control



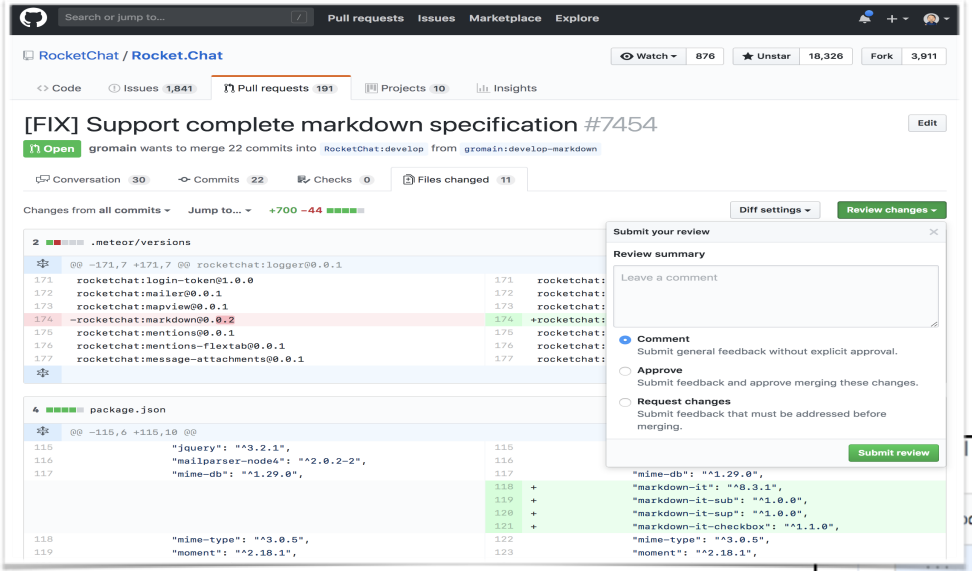



COMMUNITY • DATA
DISASTER RECOVERY *
HIGH AVAILABILITY *
GEO-REPLICATION *
HOTPATCHING *
REST API
GRAPHQL API
MONITORING
LOGGING
CUSTOMER SUCCESS TEAM • SUPPORT TEAM
INTEGRATIONS • MARKETPLACE • PROFESSIONAL SERVICES
DISCOVERY
ELASTICSEARCH
SEARCH
COLLABORATION
LDAP * • SAML
ORGANIZATIONS
TEAMS
DOCUMENTATION
MARKDOWN
GISTS
WIKIS
PAGES
PRODUCTIVITY
DEPENDENCIES
PROJECTS
MILESTONES
SOCIAL CODING
INSIGHTS
DEVELOPMENT
GITHUB FLOW
ISSUES
MENTIONS
REPOS
CODE REVIEW
PULL REQUESTS
CONCEPT
CUSTOMER
* ENTERPRISE ONLY

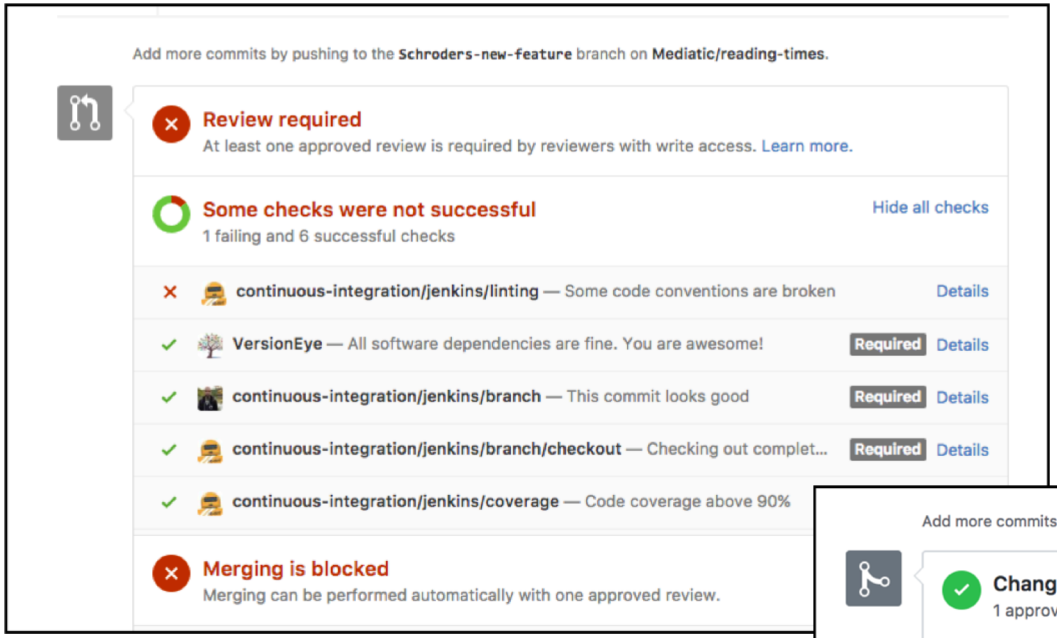
Modern Developer Workflow



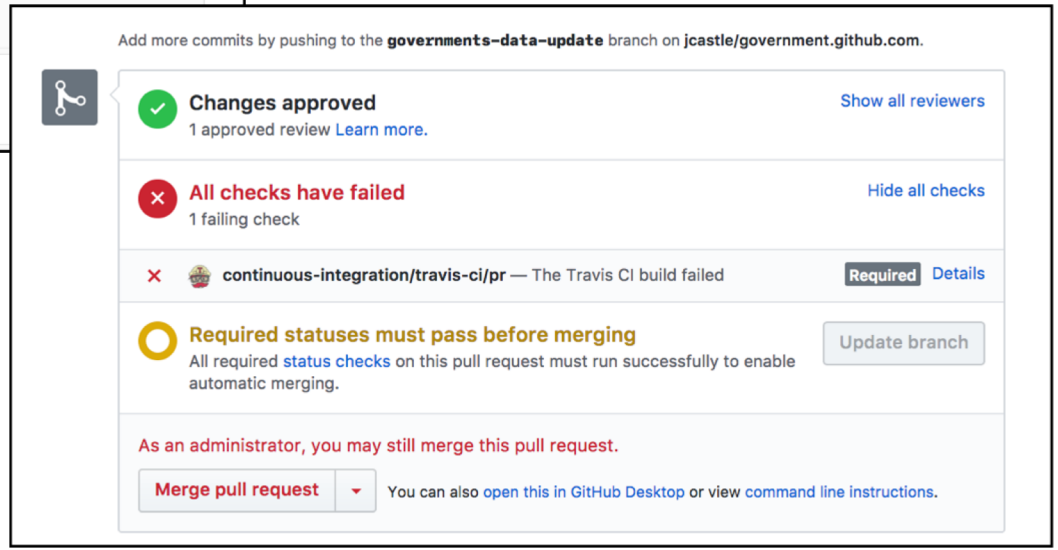
Code Review as documentation …



… and security checks

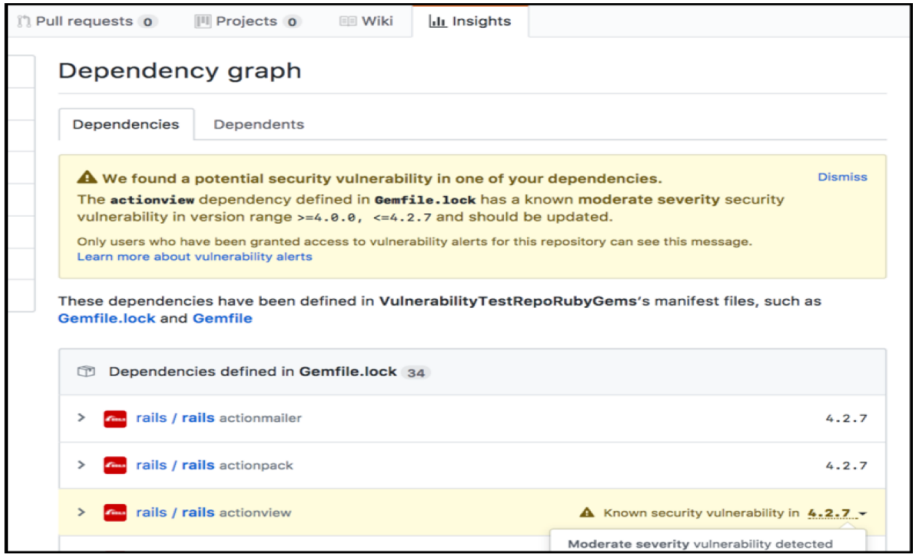


Required Reviews restrict merges



Required Status prevent mistakes

Secure Development



14%

OF PACKAGES HAVE **A SECURITY VULNERABILITY**

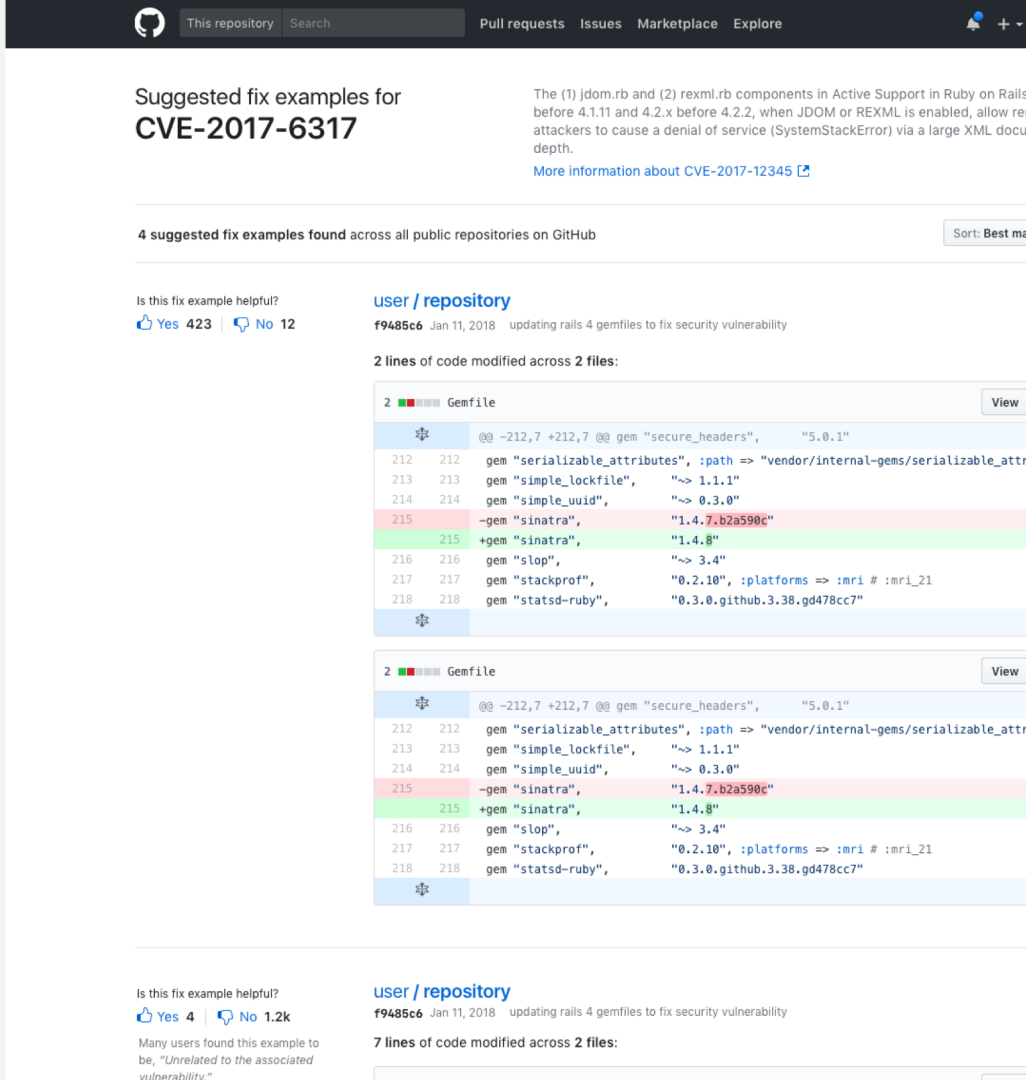
30%

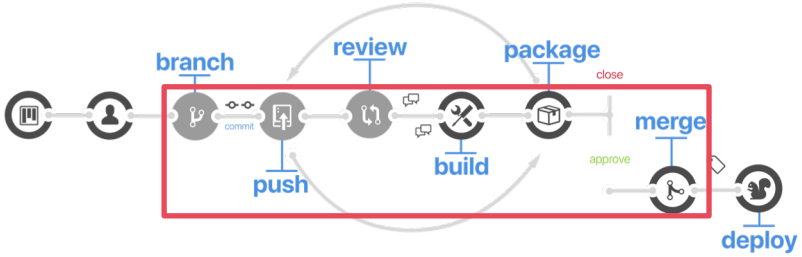
OF COMPANIES **HAVE NO PLAN** FOR ADDRESSING OPEN SOURCE DEPENDENCY VULNERABILITY

82%

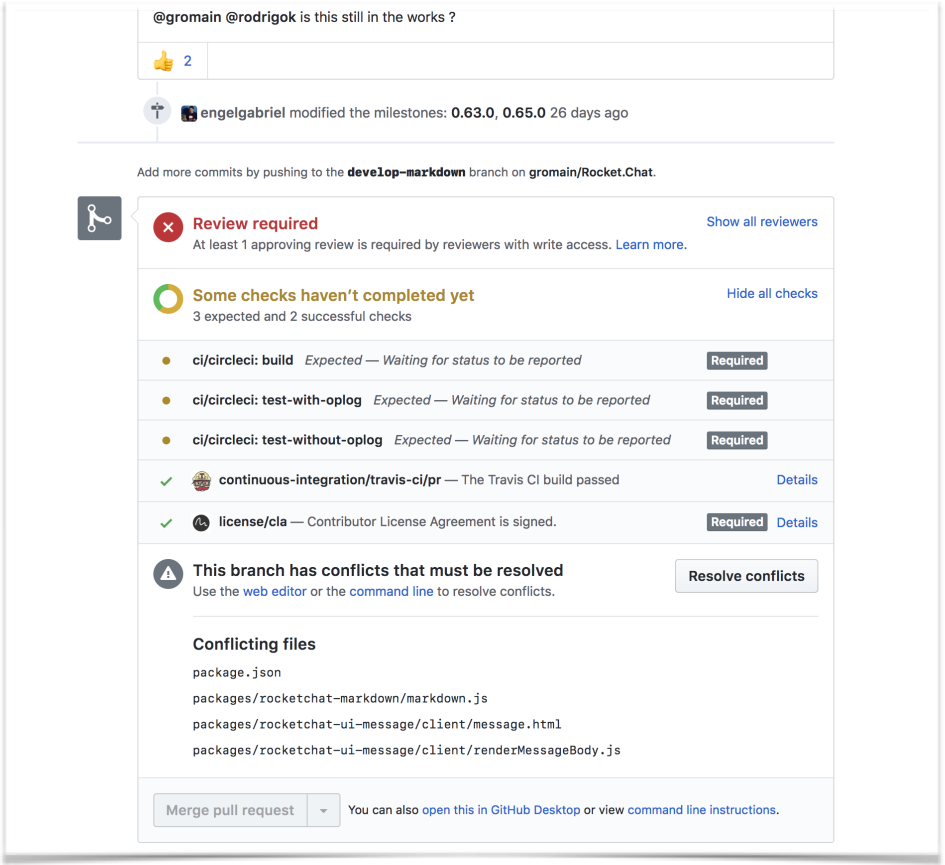
OF PUBLIC GITHUB REPOS DO NOT UPDATE THEIR DEPENDENCIES, **EVER**

Code Fixes





Enforce compliance policies with **branch statuses**, **branch protection**, **required reviews** and inline **conflict resolution**

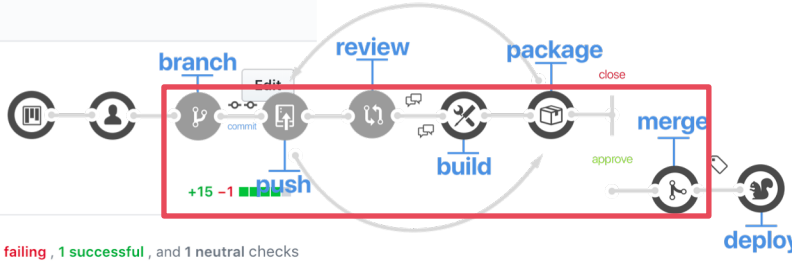


Code | Issues 32 | Pull requests 48 | Projects 4 | Wiki | Insights | Settings

Fix broken layout in profile view #1340

Open **KellyKent** wants to merge 19 commits into `master` from `kellykent/update-deps`

Conversation 8 | Commits 24 | Checks 3 | Files changed 7



`6233092` — Wire up to work with debugger

1 failing, 1 successful, and 1 neutral checks

Super-CI
Failed — 16 hours ago — Re-run all

- core-app-tests
- syntax-linter
- visual-diff

syntax-linter

Re-run

Failed

built **16 hours ago** in **less than 5 seconds** with **1 failure**

`6233092` by **@KellyKent**

kellykent/update-deps

Build report

Inspected 4,287 lines. 3 lines need your attention.

ANNOTATIONS

Check failure on line 9

Super-CI Syntax error: order/properties order

```
Error on LN9 of app/assets/stylesheets/profiles.scss
-----------------------------------------------
9:7    Expected "width" to come before "height"   order/properties-order
```

Show raw output

Check warning on line 84

Super-CI Warning: test all classes used in markup have associated styles

```
The following CSS classes were used in class attributes but have no style rules referencing them:

Class name                    Seen in
-------------------------------------
```

It's not just humans that need to collaborate, but **your tools as well**

Convert team repository permission to details-menu Verified a27c5e6

dgraham requested a review from **github/web-systems** 5 days ago

dgraham commented 5 days ago

I opened github/details-menu-element#11 to ignore clicks on the disabled buttons in this menu.

dgraham added some commits 4 days ago

`Update details-menu to 0.6.2` Verified 176a779

`Read test value from button menu item` Verified 88a4da4

dgraham requested review from **josh** and **keithamus** as code owners 4 days ago

`Convert team project permissions to details-menu` Verified 5fe64a6

dgraham requested a review from **github/github-projects** as a code owner 4 days ago

jakeboxer reviewed on behalf of **github/github-projects** 4 days ago View changes

Projects menu changes look good, 👍 from **@github/github-projects**

dgraham added some commits 4 days ago

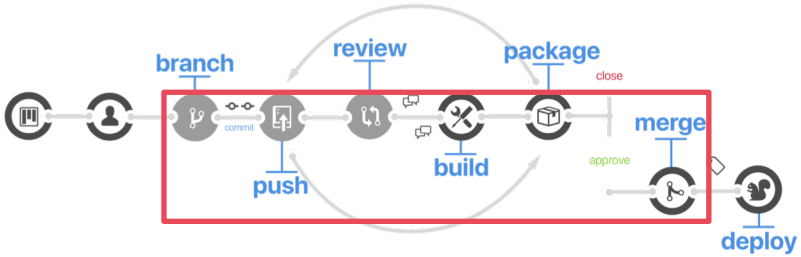
`Convert project permissions to details-menu` Verified b870406

`Remove unused form submit` Verified 6fb42b7

dgraham reviewed 4 days ago View changes

app/assets/modules/github/orgs/repo-permission-select.js

```
8  - // TODO Replace with details-menu and form submit buttons.
9  - on('selectmenu:selected', '.js-select-repo-permission', function(event)
10 -   submit(cast(event.currentTarget, HTMLFormElement))
11 - })
```



and track **those tools and actions** over time

The Result:
"AWS Trust Boundary In a Box"

1. Templates, Scripts, Functions and Recipes for securely deploying regulated workloads "Type Accreditation" (Pre-Audited), for all stages of Cloud Service adoption, (Migrator, Forward, Native)

2. Defined operational security and compliance tolerances scripts, functions and treatments (e.g. Guard Rails) for constrained secure operations across the DevOPS CI/CD and CRT through the use of **Governance as Code** (GoC) practices

3. Deployable Continuous Risk Treatments (CRT) resources (e.g. AWS & Partners solutions)

aws

Thank You!

Questions?

ATOonAWS@amazon.com

government@github.com