



Security Automation with GitHub and AWS

Introduction to AWS Authority To Operate

Eric Baran - Segment Lead – DevOps – AWS

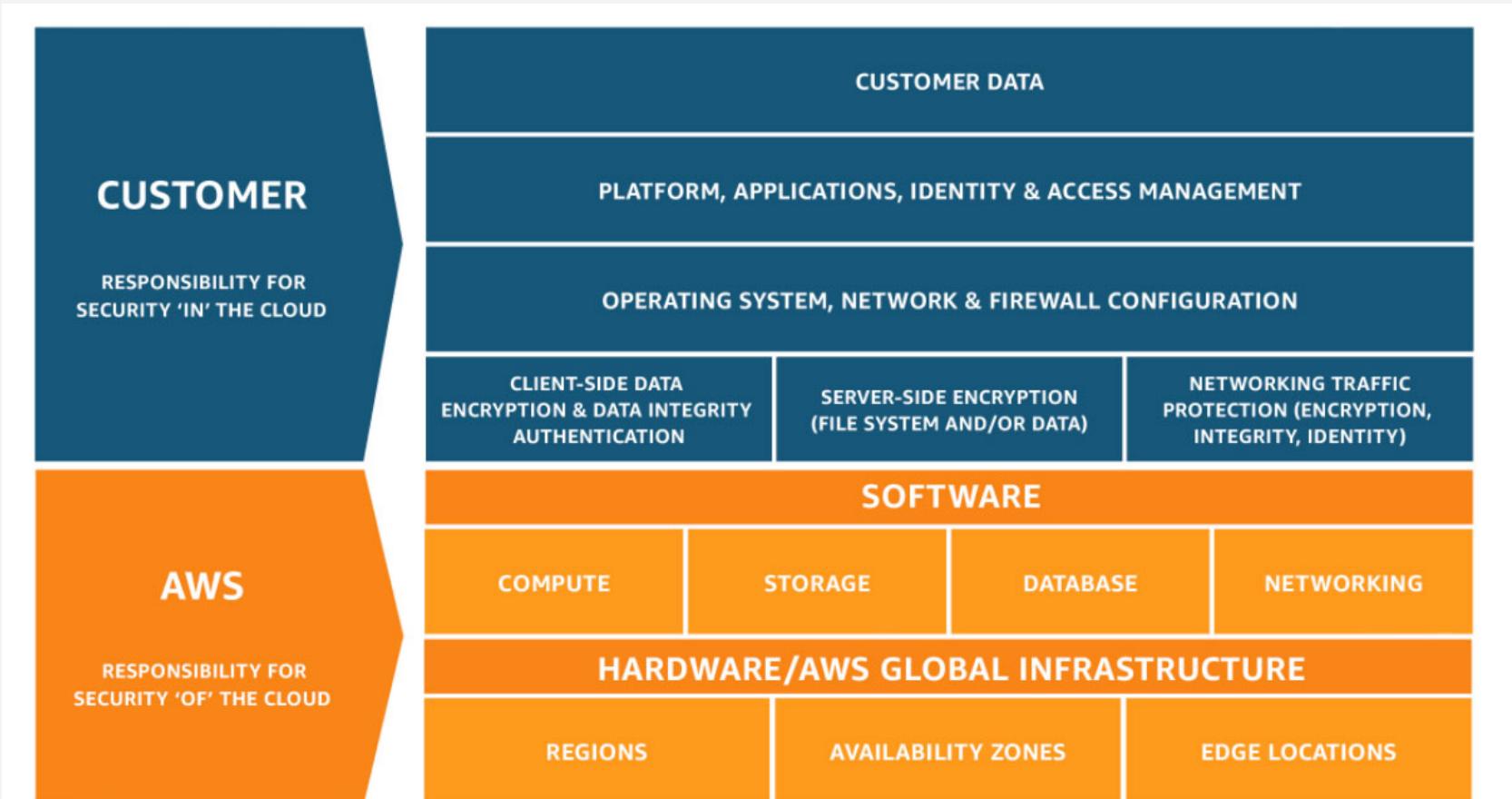
Natalie Bradley – Solutions Engineer - GitHub



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

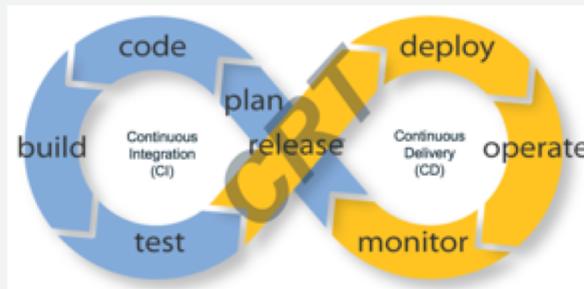
AWS Shared Responsibility Model



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)

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



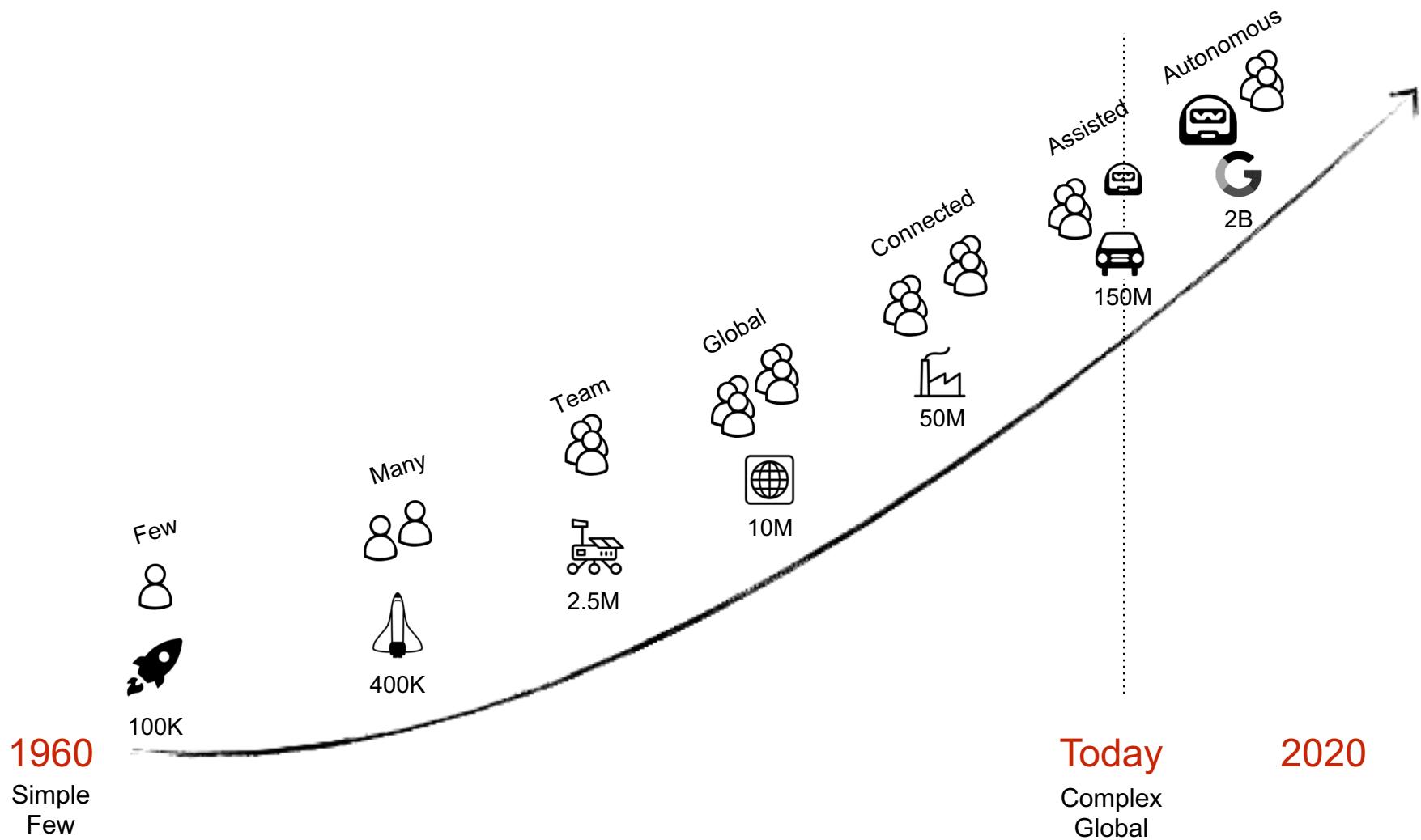
Booz | Allen | Hamilton

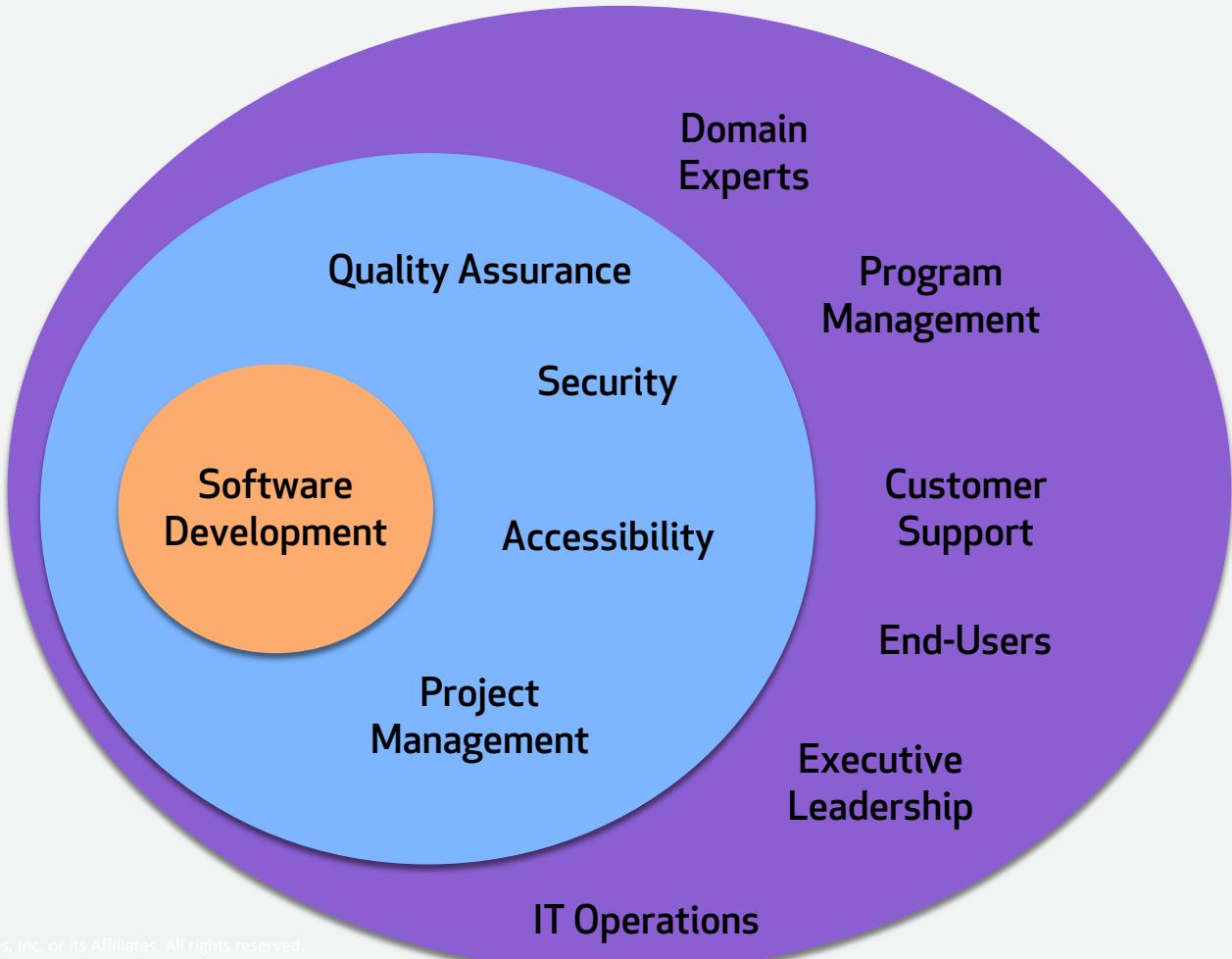


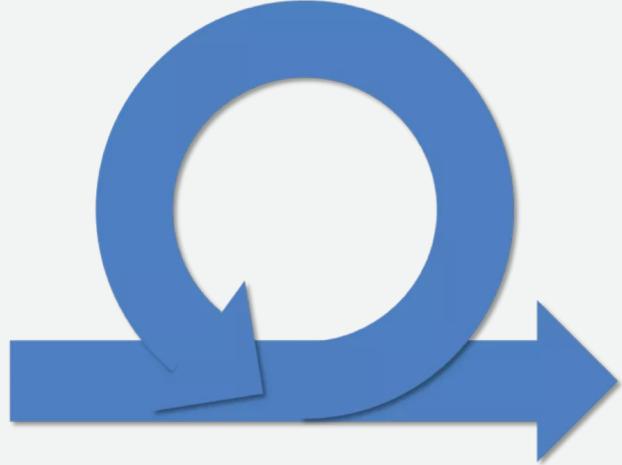
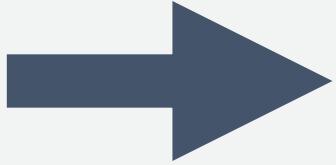
Software and DevSecOps overview

GitHub + AWS

“The Evolution of Software and Why We Evolved to DevSecOps”









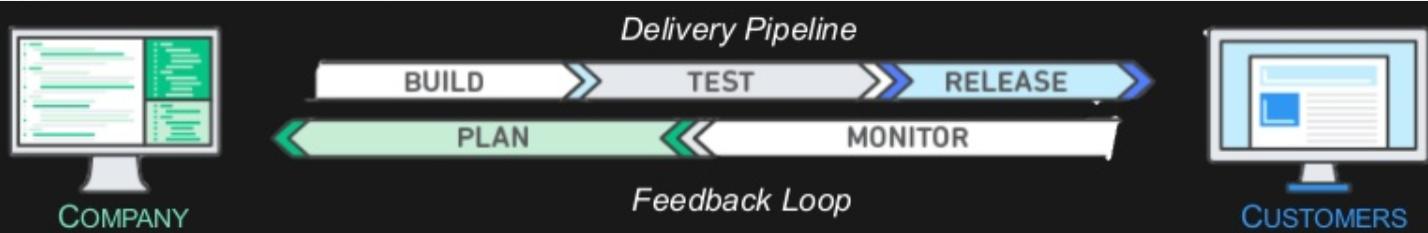
Problem Statement – Why can't we be Agile?

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.

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

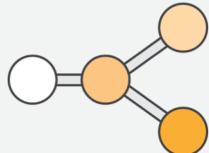
Source

Build

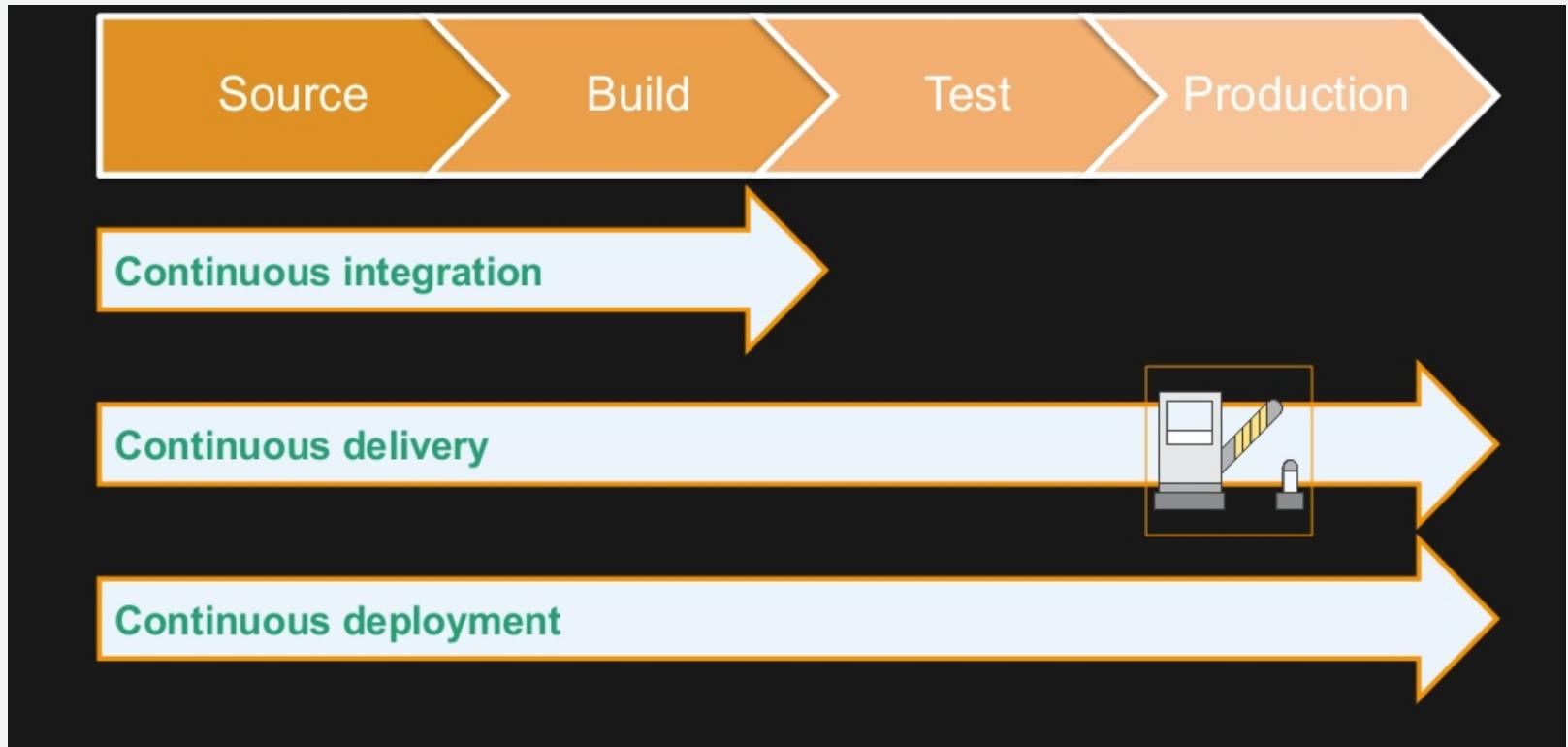
Test

Production

- 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



DEVSECOPS RELEASE PROCESSES: LEVELS



Developer Self-Service – In a Compliance Oriented World

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

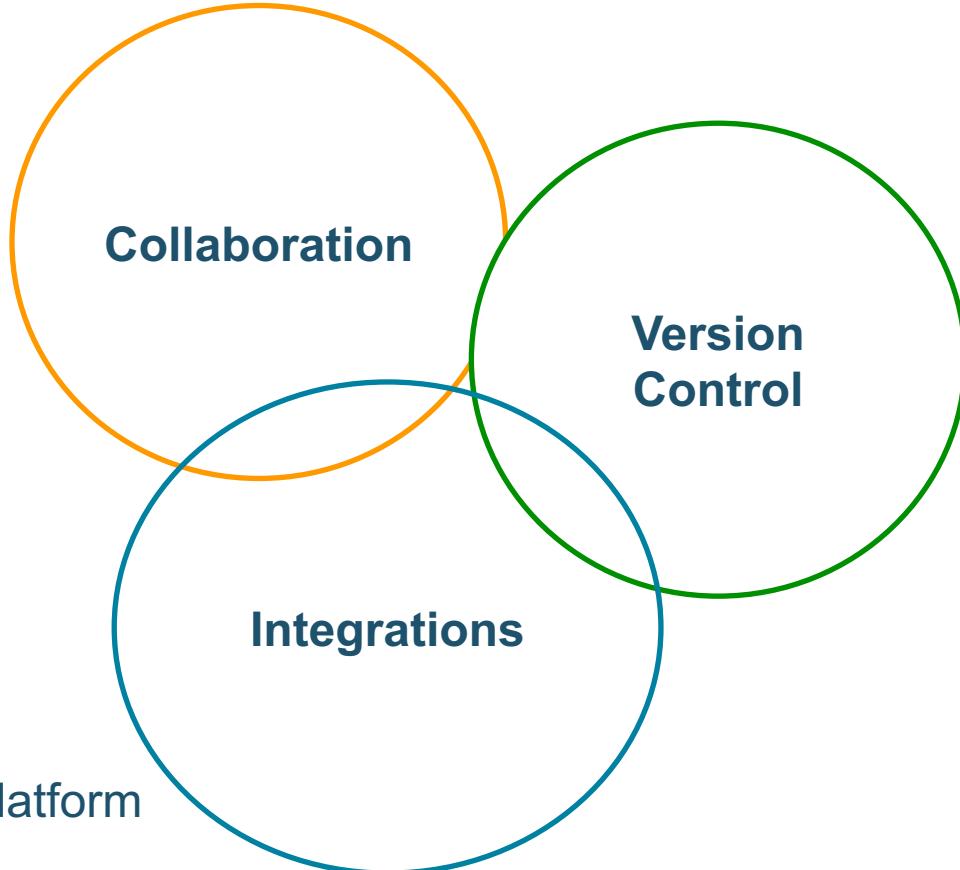
The biggest challenge is breaking out of the traditional security structures and eliminating the divide between developers, operations, and security.

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

AWSome! But what actually happens in Regulated environments today?



GitHub: The Software Development Platform



The Software Development Platform

Version Control

Code Issues 68 Pull requests 12 Projects 0 Wiki Insights ▾

History for [gh-ost / README.md](#)

- Commits on Jun 21, 2017
 -  Doc update for building from source
shlomi-noach committed 28 days ago [d153402](#) [🔗](#) [diff](#)
- Commits on May 4, 2017
 -  - Bad copy and paste. Coding gh-ost in README.md actually pointed to ...
jessbreckenridge committed on May 4 [b79185a](#) [🔗](#) [diff](#)
- Commits on May 3, 2017
 -  - Adding link to `coding-ghost.md` documentation.
jessbreckenridge committed on May 3 [13491a0](#) [🔗](#) [diff](#)
- Commits on Apr 9, 2017
 -  Add RDS link in README usage
jacobbednarz committed on Apr 9 [Verified](#) [8989944](#) [🔗](#) [diff](#)
- Commits on Apr 2, 2017
 -  Readme badges
jacobbednarz committed on Apr 2 [🔗](#) [diff](#)

Code Issues 68 Pull requests 7 Projects 3 Wiki Insights ▾

githubschool / [open-enrollment-classes-introduction-to-github](#) created by GitHub Classroom <https://services.github.com/on-demand...>

learning github github-enterprise

10,198 commits 56 branches 0 releases 2,964

Branch: master New pull request Create new file Upload files Find file

fleeper00 committed on GitHub Merge pull request #8714 from githubschool/fleeper00-edogawa ... Latest commit

 .github	Move pin to correct directory
 .layouts	capitalization issues for Lat and Lon
 .pins	Created "fleeper00-edogawa"
 images/cluster	Update map
 tests	Add mapsAPI.js
 .gitignore	I moved all the .json files into the pins folder
 .travis.yml	Bump Trvis CI Ruby version to 2.2
 .yamlint	add yamlint file
 Gemfile	change ruby to http instead of https
 Gemfile.lock	add site dir to gitignore
 README.md	Remove stray text from README
 _config.yml	exclude vendor in config
 createMap.topojson	add files from switch to jekyll
 index.html	update map
 mapsAPI.js	Revert "Fix images path"
 render.js	add files from switch to jekyll
 README.md	

Welcome

The map can be viewed [here](#).

COMMUNITY • DATA

DISASTER RECOVERY *
HIGH AVAILABILITY *
GEO-REPLICATION *
HOTPATCHING *



SEARCH



ORGANIZATIONS



TEAMS



GISTS



WIKIS



PAGES



PROJECTS



MILESTONES



SOCIAL CODING



INSIGHTS

CUSTOMER SUCCESS TEAM • SUPPORT TEAM



ISSUES



MENTIONS



REPOS



CODE REVIEW



PULL REQUESTS

DISCOVERY

ELASTICSEARCH

LDAP * SAML

MARKDOWN

DEPENDENCIES

GITHUB FLOW

COLLABORATION

DOCUMENTATION

PRODUCTIVITY

DISASTER RECOVERY *
HIGH AVAILABILITY *
GEO-REPLICATION *
HOTPATCHING *

REST API
GRAPHQL API
MONITORING
LOGGING

INTEGRATIONS • MARKETPLACE • PROFESSIONAL SERVICES



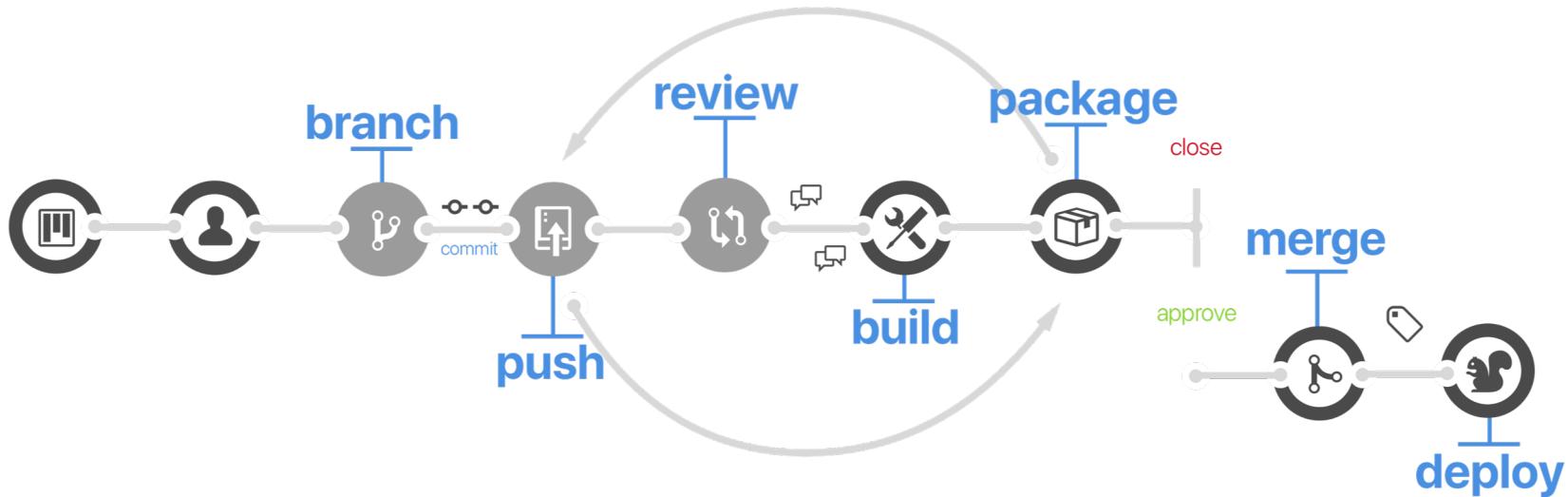
CONCEPT



CUSTOMER

* ENTERPRISE ONLY

Modern Developer Workflow



A screenshot of a GitHub pull request page for the RocketChat repository. The title is "[FIX] Support complete markdown specification #7454". The modal window is titled "Submit your review" and contains a "Review summary" section with a text input field labeled "Leave a comment". Below it are three radio button options: "Comment" (selected), "Approve", and "Request changes". A "Submit review" button is at the bottom right of the modal.

Changes from all commits ▾ Jump to... +700 -44

2 .meteor/versions

@@ -171,7 +171,7 @@ rocketchat:logger@0.0.1

171 rocketchat:login-token@1.0.0 171 rocketchat:
172 rocketchat:mailer@0.0.1 172 rocketchat:
173 rocketchat:mapview@0.0.1 173 rocketchat:
174 -rocketchat:markdown@0.0.2 174 +rocketchat:
175 rocketchat:mentions@0.0.1 175 rocketchat:
176 rocketchat:mentions-flextab@0.0.1 176 rocketchat:
177 rocketchat:message-attachments@0.0.1 177 rocketchat:

4 package.json

@@ -115,6 +115,10 @@

115 "jquery": "^3.2.1", 115
116 "mailparser-node4": "^2.0.2-2", 116
117 "mime-db": "^1.29.0", 117

118 "mime-type": "^3.0.5", 118 +
119 "moment": "^2.18.1", 119 +

"mime-db": "^1.29.0",
"markdown-it": "^8.3.1",
"markdown-it-sub": "^1.0.0",
"markdown-it-sup": "^1.0.0",
"markdown-it-checkbox": "^1.1.0",
"mime-type": "^3.0.5",
"moment": "^2.18.1",

... and security
checks

Code Review as documentation ...

I reviewed 8 days ago

[View changes](#)

models/repository/rpc_dependency.rb

```
... @@ -18,7 +18,7 @@ def rpc
18   18  #
19   19  # Returns a new instance of GitRPC::Client associated with this repository
20   20  def build_rpc
21 -  if name =~ /\\.wiki$/ && base_repo = Repository.nwo(name_with_owner.chomp(".wiki"))
21 +  if name =~ /\\.wiki$/ && base_repo = self.name_with_owner.chomp(".wiki")
```

sentinel 8 days ago

\$/ looks like a regular expression which uses anchors that match beginning/end of line. This could lead to the bypass of the intended input validation. If you intended to match the beginning/end of string please use \A/\z instead.

Reply...

Add more commits by pushing to the **Schroders-new-feature** branch on **Mediatric/reading-times**.



× Review required

At least one approved review is required by reviewers with write access. [Learn more.](#)

○ Some checks were not successful

1 failing and 6 successful checks

[Hide all checks](#)

× **continuous-integration/jenkins/linting** — Some code conventions are broken

[Details](#)

✓ **VersionEye** — All software dependencies are fine. You are awesome!

Required [Details](#)

✓ **continuous-integration/jenkins/branch** — This commit looks good

Required [Details](#)

✓ **continuous-integration/jenkins/branch/checkout** — Checking out complet...

Required [Details](#)

✓ **continuous-integration/jenkins/coverage** — Code coverage above 90%

× Merging is blocked

Merging can be performed automatically with one approved review.

Required Reviews restrict merges

Required Status prevent mistakes

Add more commits by pushing to the **governments-data-update** branch on **jcastle/government.github.com**.



✓ Changes approved

1 approved review [Learn more.](#)

[Show all reviewers](#)

× All checks have failed

1 failing check

[Hide all checks](#)

× **continuous-integration/travis-ci/pr** — The Travis CI build failed

Required [Details](#)

○ Required statuses must pass before merging

All required [status checks](#) on this pull request must run successfully to enable automatic merging.

[Update branch](#)

As an administrator, you may still merge this pull request.

[Merge pull request](#)

You can also [open this in GitHub Desktop](#) or view [command line instructions](#).

Secure Development

Changes from all commits ▾ Jump to... ▾ +70 -0

outline for RFI response

cesg_dod_cloud_rfi (#414)

jbjonesjr committed 2 days ago Verified

This commit was created on GitHub.com and signed with a verified signature using GitHub's key.

GPG key ID: 4AEE18F83AFDEB23

Learn about signing commits

70 response/

```
+## DOD_1
+ [RFI link](https://www.fbo.gov/index?s=opportunity&mode=form&id=6fa)
+ [CESG memo](https://assets.documentcloud.org/documents/4059163/DoD-)
+
```

Pull requests 0 Projects 0 Wiki Insights

Dependency graph

Dependencies Dependents

We found a potential security vulnerability in one of your dependencies. The `actionview` dependency defined in `Gemfile.lock` has a known moderate severity security vulnerability in version range `>=4.0.0, <=4.2.7` and should be updated. Only users who have been granted access to vulnerability alerts for this repository can see this message. Learn more about vulnerability alerts

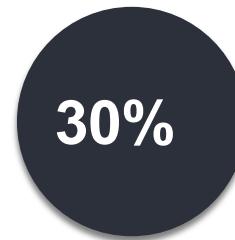
These dependencies have been defined in `VulnerabilityTestRepoRubyGems`'s manifest files, such as `Gemfile.lock` and `Gemfile`

Dependencies defined in `Gemfile.lock` 34

- > rails / rails actionmailer 4.2.7
- > rails / rails actionpack 4.2.7
- > rails / rails actionview Known security vulnerability in 4.2.7 Moderate severity vulnerability detected



OF PACKAGES HAVE A
SECURITY
VULNERABILITY



OF COMPANIES HAVE NO
PLAN FOR ADDRESSING
OPEN SOURCE DEPENDENCY
VULNERABILITY



OF PUBLIC GITHUB
REPOS DO NOT UPDATE
THEIR DEPENDENCIES,
EVER



Code Fixes

Suggested fix examples for CVE-2017-6317

The (1) jdom.rb and (2) rxml.rb components in Active Support in Ruby on Rails before 4.1.11 and 4.2.x before 4.2.2, when JDOM or REXML is enabled, allow remote attackers to cause a denial of service (SystemStackError) via a large XML document depth.

[More information about CVE-2017-12345](#)

4 suggested fix examples found across all public repositories on GitHub

Sort: Best match

Is this fix example helpful?

Like Yes 423 | Dislike No 12

user / repository

f9485c6 Jan 11, 2018 updating rails 4 gemfiles to fix security vulnerability

2 lines of code modified across 2 files:

2 ████ Gemfile

```
2 @@ -212,7 +212,7 @@ gem "secure_headers",      "5.0.1"
212 212   gem "serializable_attributes", :path => "vendor/internal-gems/serializable_attributes"
213 213   gem "simple_lockfile",      "~> 1.1.1"
214 214   gem "simple_uuid",         "~> 0.3.0"
215 215   -gem "sinatra",           "1.4.7.b2a590c"
215 215   +gem "sinatra",           "1.4.8"
216 216   gem "slop",               "~> 3.4"
217 217   gem "stackprof",          "0.2.10", :platforms => :mri # :mri_21
218 218   gem "statsd-ruby",        "0.3.0.github.3.38.gd478cc7"
```

View

2 ████ Gemfile

```
2 @@ -212,7 +212,7 @@ gem "secure_headers",      "5.0.1"
212 212   gem "serializable_attributes", :path => "vendor/internal-gems/serializable_attributes"
213 213   gem "simple_lockfile",      "~> 1.1.1"
214 214   gem "simple_uuid",         "~> 0.3.0"
215 215   -gem "sinatra",           "1.4.7.b2a590c"
215 215   +gem "sinatra",           "1.4.8"
216 216   gem "slop",               "~> 3.4"
217 217   gem "stackprof",          "0.2.10", :platforms => :mri # :mri_21
218 218   gem "statsd-ruby",        "0.3.0.github.3.38.gd478cc7"
```

View

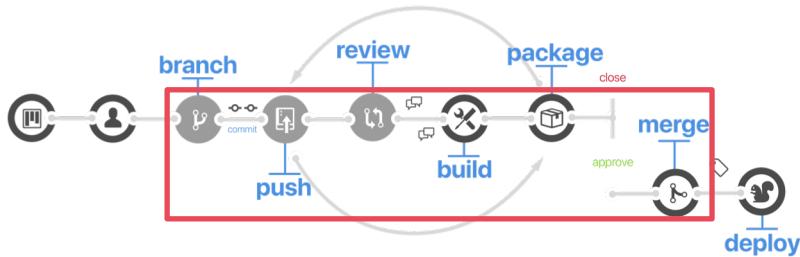
Is this fix example helpful?

Like Yes 4 | Dislike No 1.2k

user / repository

f9485c6 Jan 11, 2018 updating rails 4 gemfiles to fix security vulnerability

7 lines of code modified across 2 files:



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

@gromain @rodrigok is this still in the works ?

2

engel gabriel modified the milestones: 0.63.0, 0.65.0 26 days ago

Add more commits by pushing to the **develop-markdown** branch on **gromain/Rocket.Chat**.

Review required Show all reviewers
At least 1 approving review is required by reviewers with write access. [Learn more](#).

Some checks haven't completed yet Hide all checks
3 expected and 2 successful checks

- ci/circleci: build Expected — Waiting for status to be reported **Required**
- ci/circleci: test-with-oplog Expected — Waiting for status to be reported **Required**
- ci/circleci: test-without-oplog Expected — Waiting for status to be reported **Required**

continuous-integration/travis-ci/pr — The Travis CI build passed [Details](#)

license/cla — Contributor License Agreement is signed. **Required** [Details](#)

This branch has conflicts that must be resolved [Resolve conflicts](#)
Use the [web editor](#) or the [command line](#) to resolve conflicts.

Conflicting files

- package.json
- packages/rocketchat-markdown/markdown.js
- packages/rocketchat-ui-message/client/message.html
- packages/rocketchat-ui-message/client/renderMessageBody.js

Merge pull request You can also [open this in GitHub Desktop](#) or view [command line instructions](#).

Fix broken layout in profile view #1340

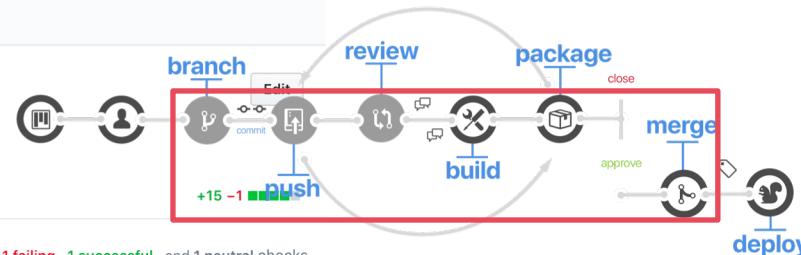
[Open](#) KellyKent wants to merge 19 commits into `master` from `kellykent/update-deps`

Conversation 8 · Commits 24

Checks 3

Files changed 7

6233092 — Wire up to work with debugger



Super-CI

Failed — 16 hours ago

[Re-run all](#)

core-app-tests

[syntax-linter](#)

syntax-linter

[Failed](#)

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

6233092 by @KellyKent

[kellykent/update-deps](#)

[Re-run](#)

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

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

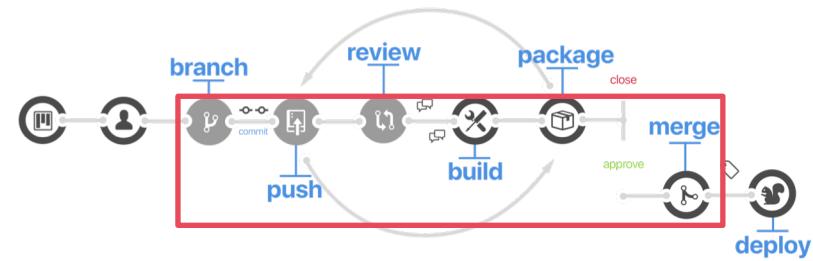
dgraham added some commits 4 days ago

- Convert project permissions to details-menu Verified b870406
- Remove unused form submit Verified ● 6fb42b7

dgraham reviewed 4 days ago

```
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   - })
```

dgraham 4 days ago

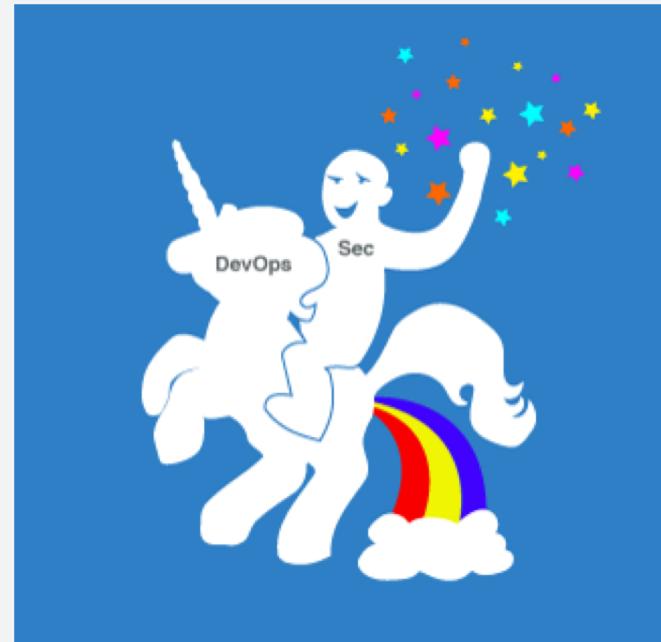


and track **those tools**
and **actions** over time



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)



**Thank You!
Questions?**

ATOonAWS@amazon.com

government@github.com