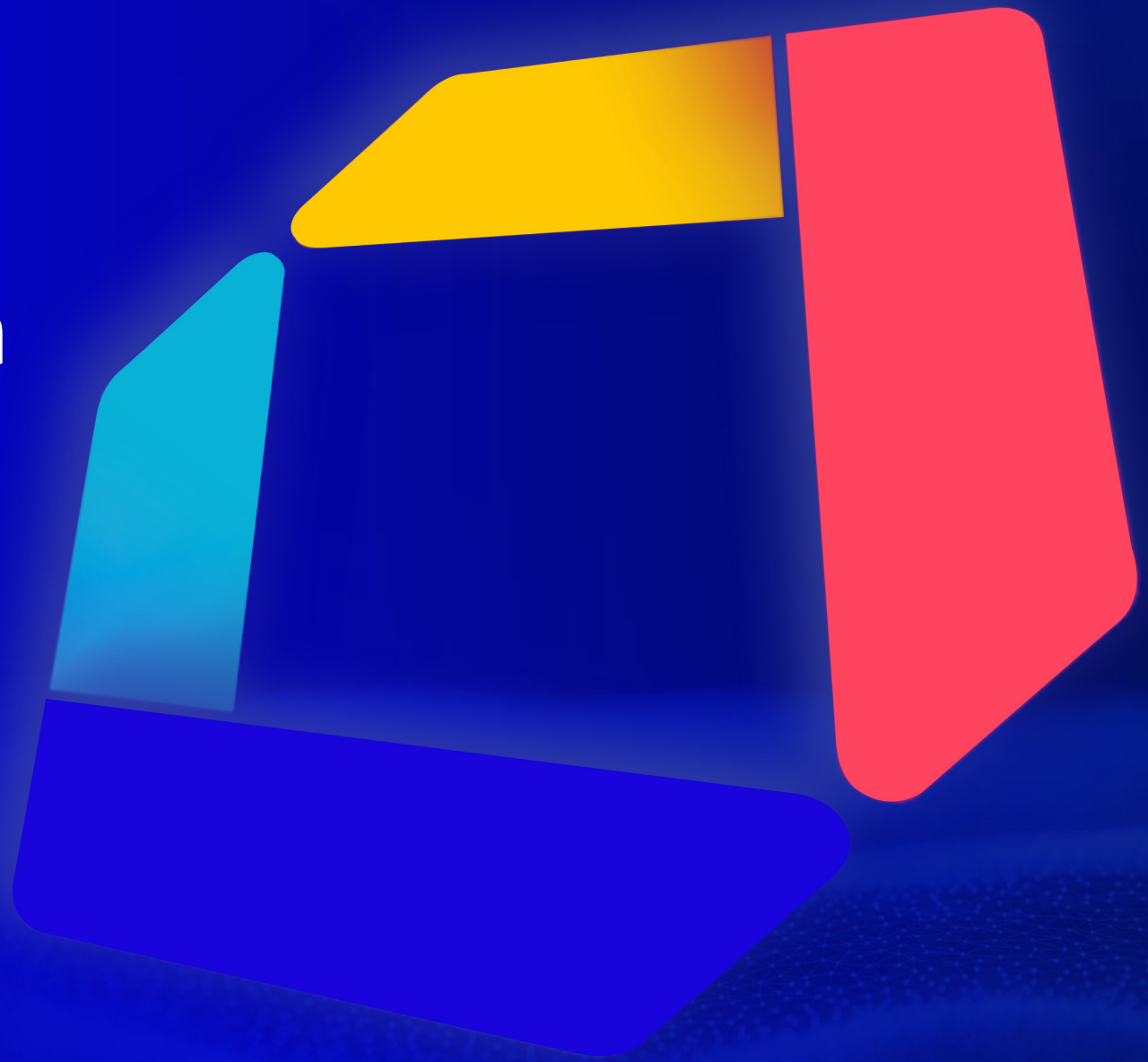
aqua

Desmistificando as Vulnerabilidades em Golang

GOPHERCON
BRASIL 2022
5 ANOS



in/carolgv

krol3

@krol_valencia

Agenda

- Intro
- Vulnerabilities
- Secure Golang in the SDLC

Security is Hard

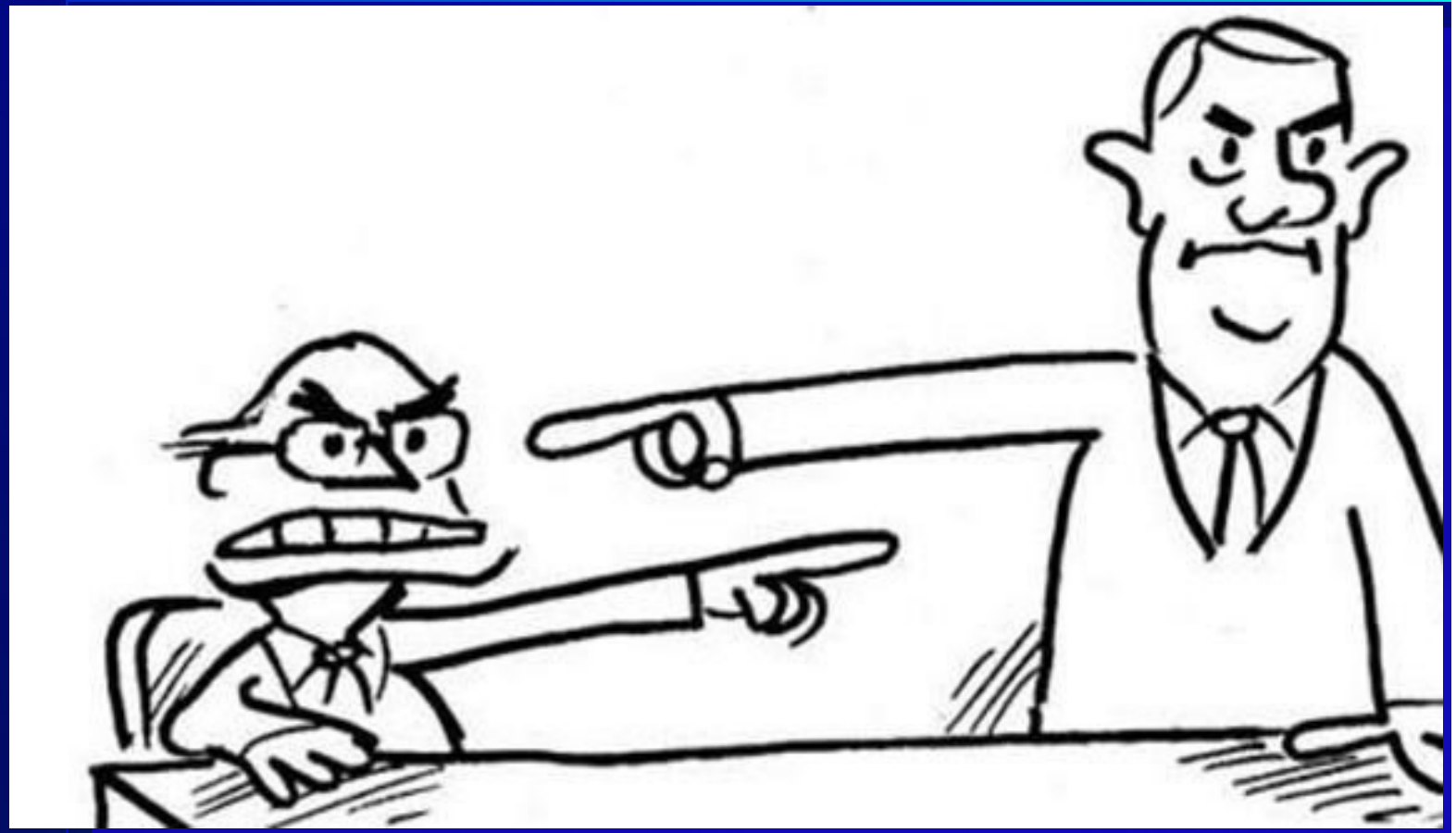
Process, People and Technology

Cybersecurity?

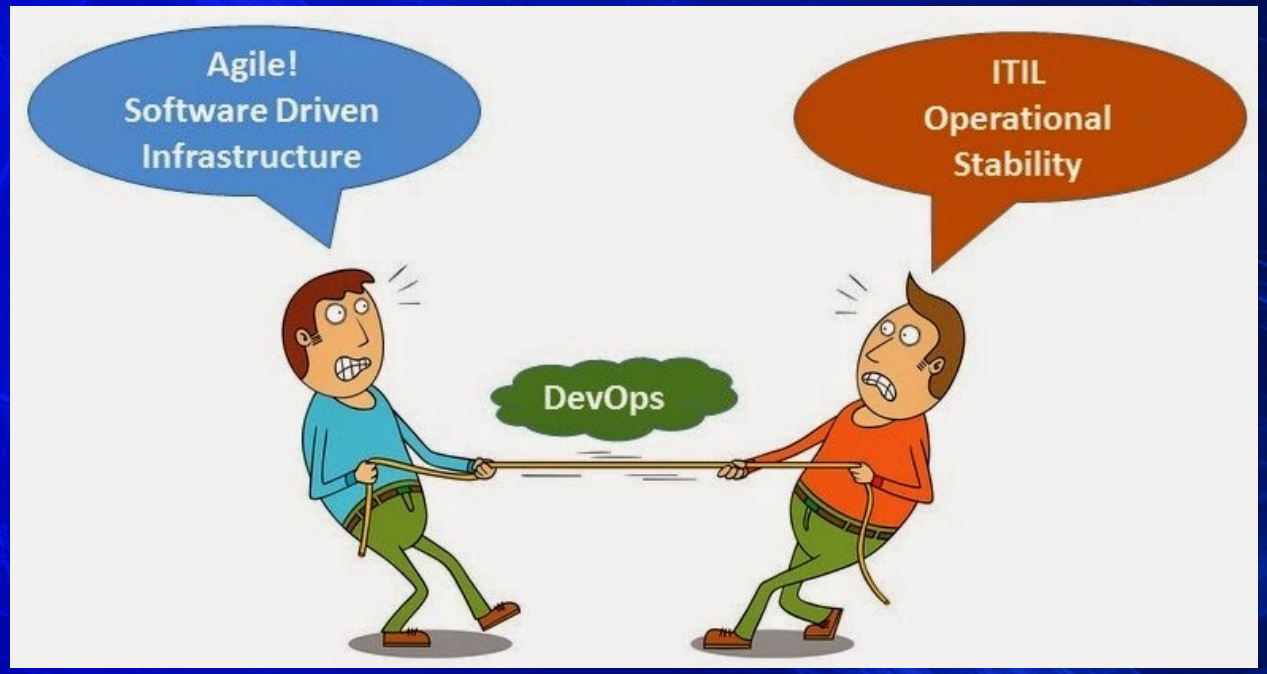
Container security?
k8s security?


Today
Slackbot 2:59 PM
@dchristopher changed posting permissions using the channel management tool.
Pinned by Joe Nash
Nwave 3:00 PM
Hi @here
I announce i am a
Slack has been st
have also been st
#uberunderpaisd
repos from phabricator
YOU HAVE BEEN
dreamstime
HACKED !
Lucas Ruiz 3:05 PM

Who blame for the security breach ?



Maturity Model in my company – Agile process



Maturity Model in my company – Agile process

aqua

Applying Devops ….

Bitbucket Source Code Management

CI

CD

Code

Build

Deploy

Run

DOCKERFILE

Terraform

AWS CloudFormation

WEBASSEMBLY

kubernetes

Where is the vulnerabilities in my SDLC? ….

OCI Registry

Container Lifecycle - SDLC

Vulnerabilities

A flaw or weakness that may allow harm to occur to an IT system or activity.

Common Vulnerabilities and Exposures

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

Is it Exploitable vulnerability?

CVE-2022-23772 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Rat.SetString in math/big in Go before 1.16.14 and 1.17.x before 1.17.7 has an overflow that can lead to Uncontrolled Memory Consumption.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2022-23772
NVD Published Date:
02/10/2022
NVD Last Modified:
08/04/2022
Source:
MITRE

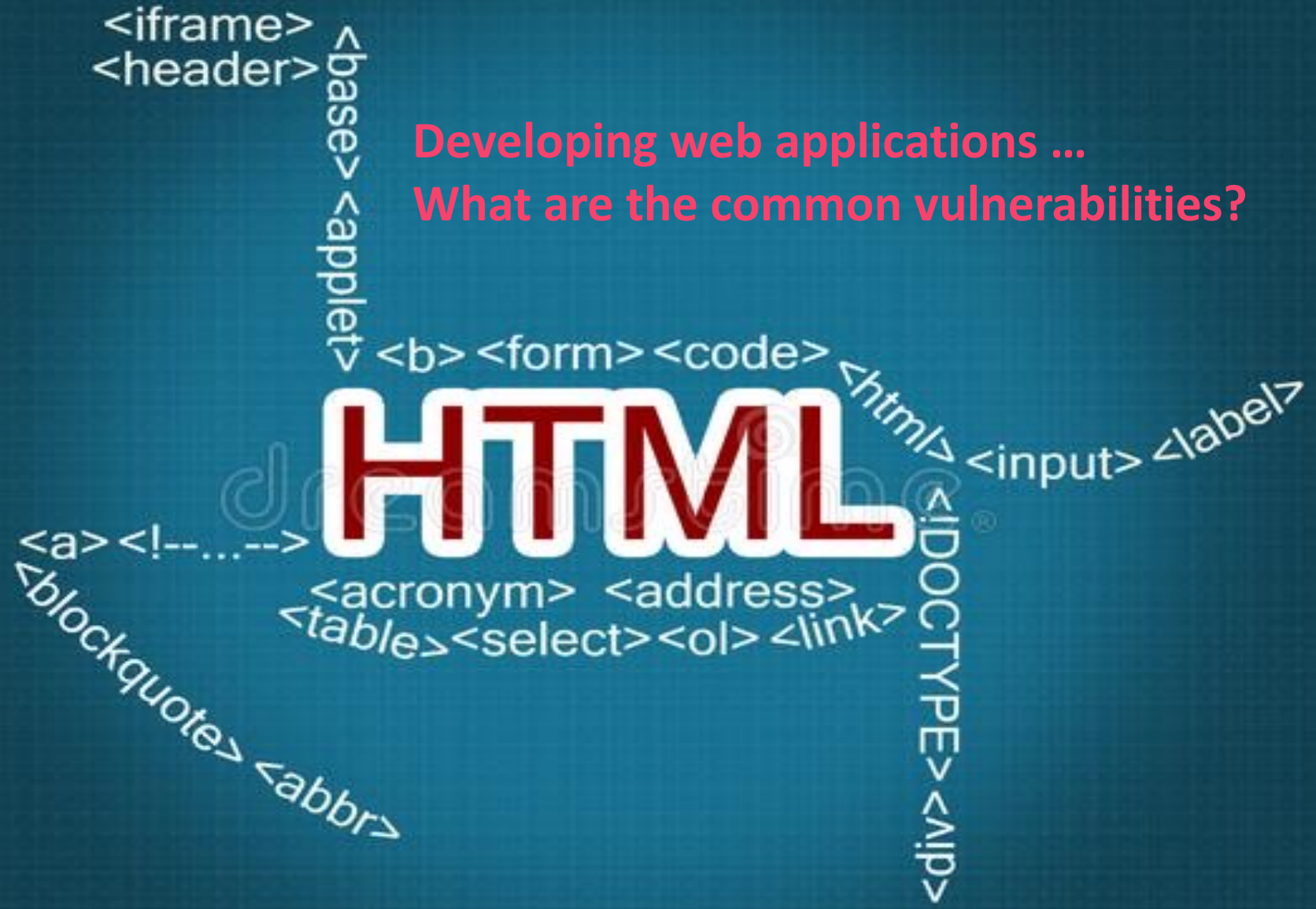
aqua

CISO

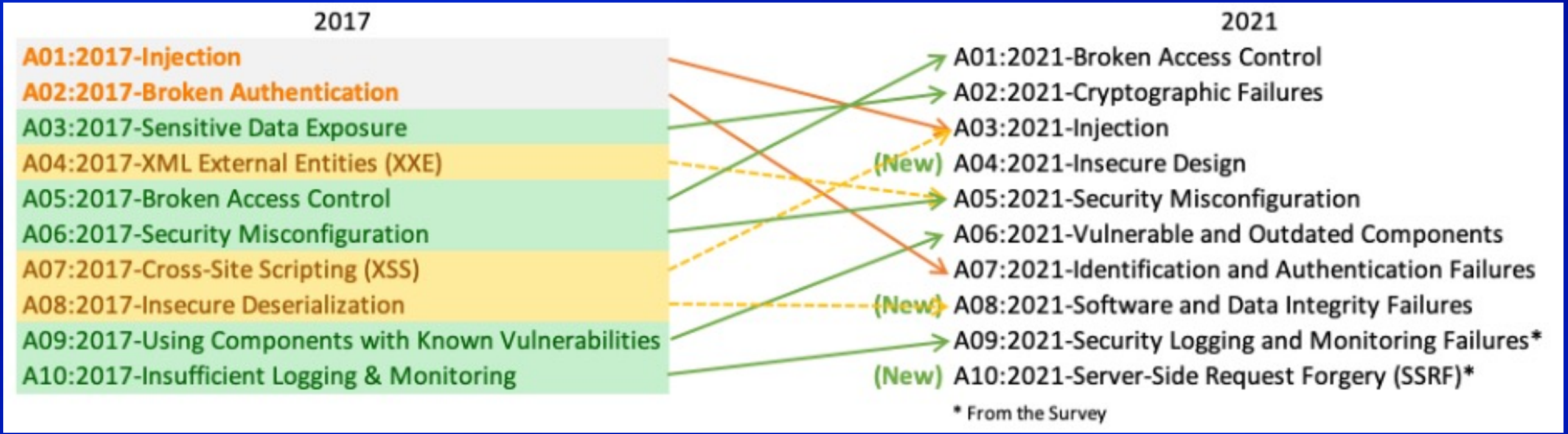
Chief Information Security Officer

Log4Shell™

Zero day

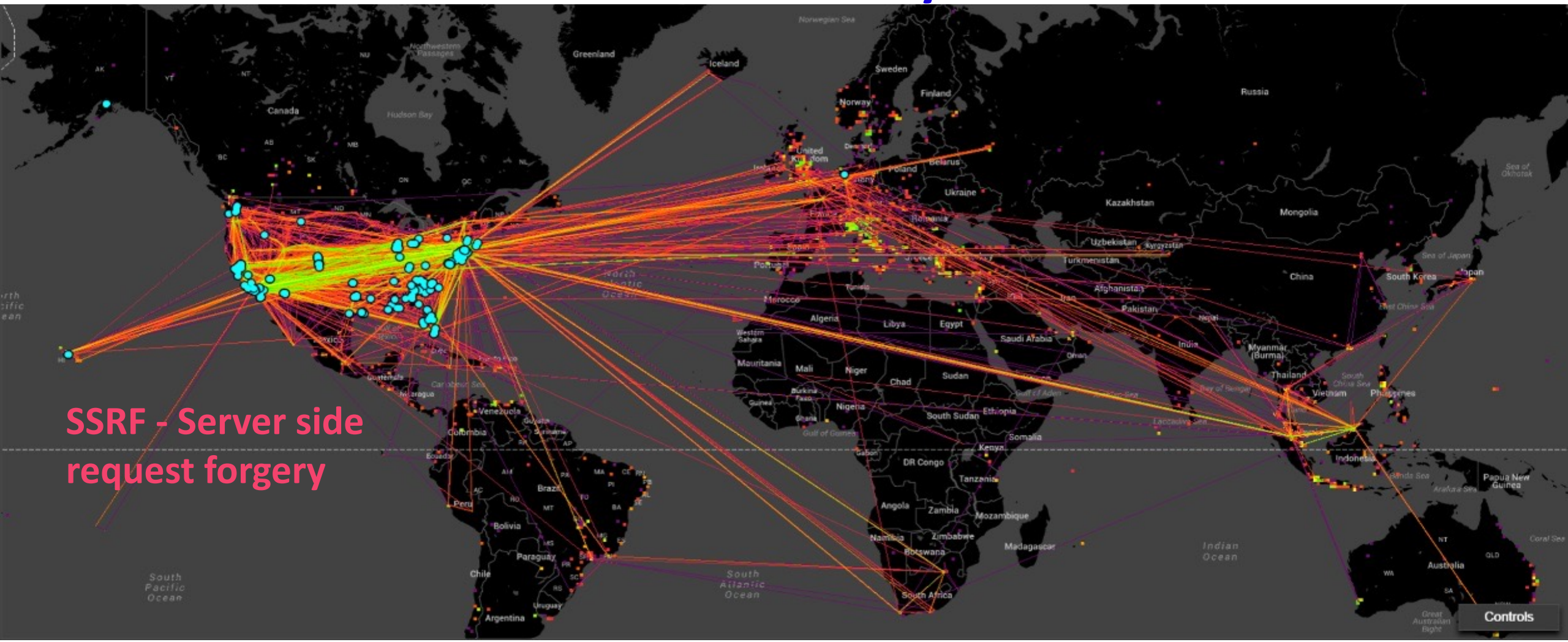

Developing web applications …
What are the common vulnerabilities?
<iframe>
<header>
<base> <applet>
<b> <form> <code>
HTML
<html> <input> <label>
<!DOCTYPE> <ip>
<a> <!--...-->
<acronym> <address>
<table> <select> <link>
<blockquote> <abbr>

OWASP Top 10



Open Web Application Security Project – Top 10

Go net library affected by critical ip address validation vulnerability



https://www.bleepingcomputer.com/news/security/go-rust-net-library-affected-by-critical-ip-address-validation-vulnerability/

aqua

Secure Golang

in the Software Development Lifecycle (SDLC)

aqua

Go vulnerability check

vuln.go.dev

Go Vulnerability Database

This is the Go vulnerability database. It is meant to be accessed by programs that want to find vulnerabilities associated with Go modules.

For details, see go.dev/security/vuln.

See vuln.go.dev/privacy for privacy information about this service.

See vuln.go.dev/copyright for copyright and licensing information about the reports in this database.

Julie Qiu, for the Go security team
6 September 2022

aqua

Go vulnerability check

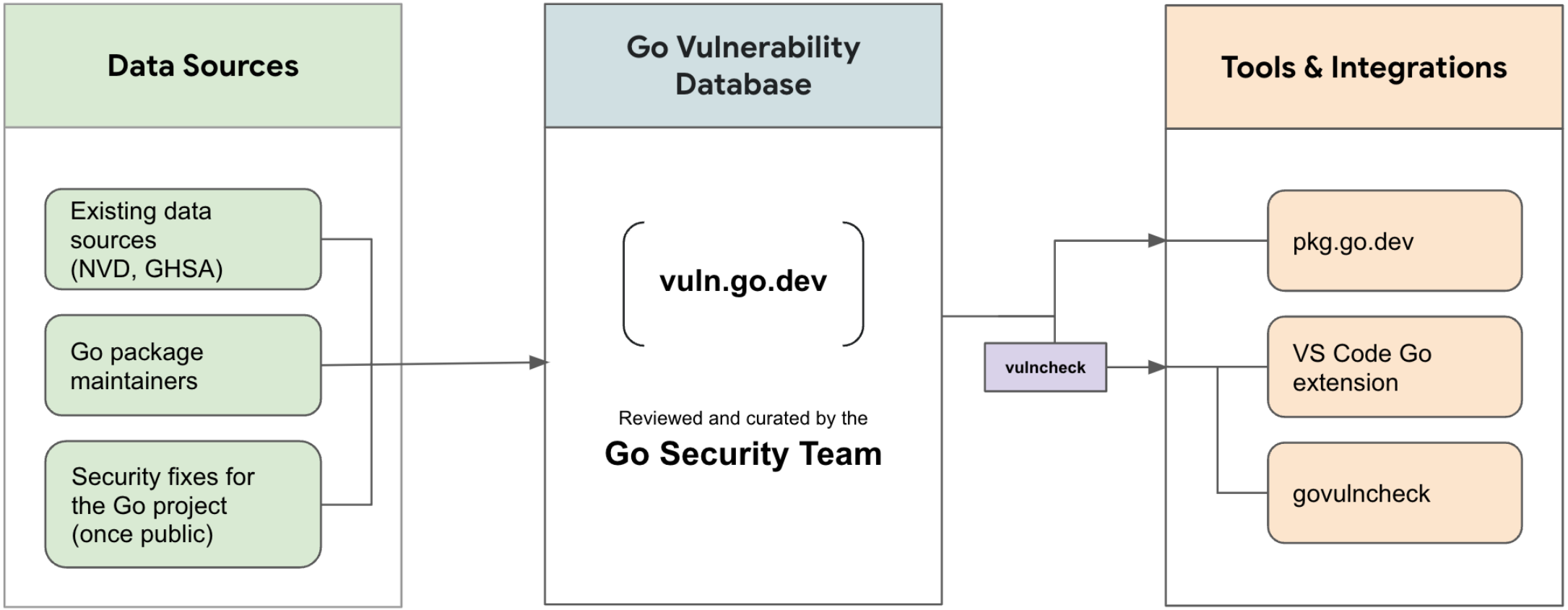
```
demo-go-xss → go install golang.org/x/vuln/cmd/govulncheck@latest
go: downloading golang.org/x/vuln v0.0.0-20220929184650-cabc70cc795b
go: downloading golang.org/x/tools v0.1.13-0.20220928184430-f80e98464e27

demo-go-xss → govulncheck ./...
govulncheck is an experimental tool. Share feedback at https://go.dev/s/govulncheck-feedback.

Scanning for dependencies with known vulnerabilities...
No vulnerabilities found.
```

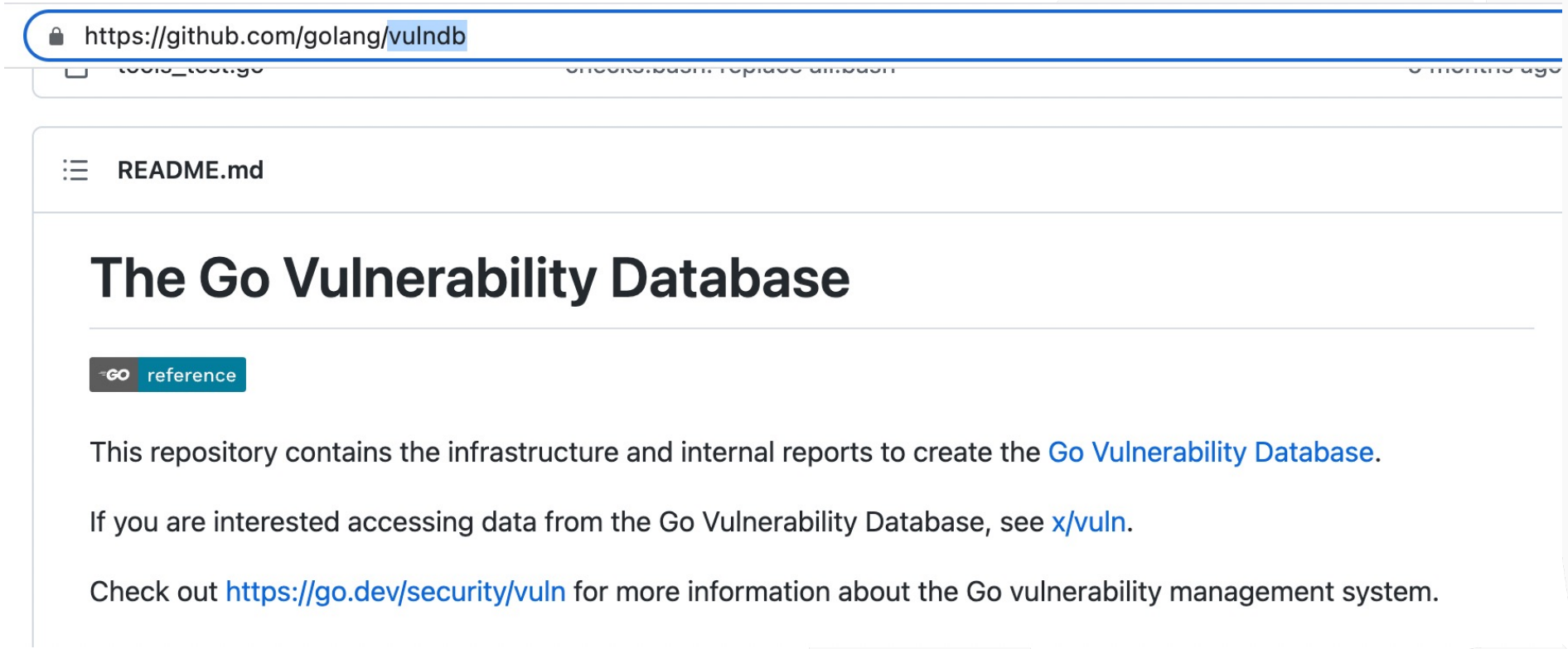

aqua

Go vulnerability check



https://go.dev/security/vuln/

Before vulncheck



Scanners automatically detects the following files in the container and scans vulnerabilities in the application dependencies.

Language	File	Image	Rootfs	Filesystem	Repository	Dev dependencies
Ruby	Gemfile.lock	-	-	✅	✅	included
	gemspec	✅	✅	-	-	included
Python	Pipfile.lock	-	-	✅	✅	excluded
	poetry.lock	-	-	✅	✅	included
	requirements.txt	-	-	✅	✅	included
	egg package[^1]	✅	✅	-	-	excluded
	wheel package[^2]	✅	✅	-	-	excluded
PHP	composer.lock	✅	✅	✅	✅	excluded
Node.js	package-lock.json	-	-	✅	✅	excluded
	yarn.lock	-	-	✅	✅	included
	pnpm-lock.yaml	-	-	✅	✅	excluded
	package.json	✅	✅	-	-	excluded
Go	Binaries built by Go[^6]	✅	✅	-	-	excluded
	go.mod[^7]	-	-	✅	✅	included

How scanners work?

How to find CVEs?

aqua

Golang Dependency Management

aqua

```
module github.com/krol3/go-docker

go 1.19

require (
        github.com/Microsoft/go-winio v0.5.2 // indirect
        github.com/docker/distribution v2.8.1+incompatible // indirect
```

```
github.com/Microsoft/go-winio v0.5.2 h1:a9IhgEQBCUEk6QCdml9CiJGhAws+YwffDHEMp1VMrpA=
github.com/Microsoft/go-winio v0.5.2/go.mod h1:WpS1mjBmmwHBEWmogvA2mj8546UReBk4v8QkMxJ6pZY=
github.com/davecgh/go-spew v1.1.0/go.mod h1:J7Y8YcW2NihsgmVo/mv3lAwl/skON4iLHjSsI+c5H38=
github.com/davecgh/go-spew v1.1.1/go.mod h1:J7Y8YcW2NihsgmVo/mv3lAwl/skON4iLHjSsI+c5H38=
github.com/docker/distribution v2.8.1+incompatible h1:Q50tZOPR6T/hjNsyc9g8/syEs6bk8XXApsHjKukMl68=
github.com/docker/distribution v2.8.1+incompatible/go.mod h1:J2gT2udsDAN96Uj4KfcMRqY0/ypR+oyYUYmja8H+y+w=
github.com/docker/docker v20.10.17+incompatible h1:JYCuMrWaVNophQTOrMMoSwudOVEfcegoZZrleKc1xwE=
github.com/docker/docker v20.10.17+incompatible/go.mod h1:eEKB0N0r5NX/I1kEveEz05bcu8tLC/8azJZsviup8Sk=
github.com/docker/go-connections v0.4.0 h1:El9xVISelRB7BuFusrZozjnkIM5YnzCViNKohAFqRJQ=
github.com/docker/go-connections v0.4.0/go.mod h1:Gbd7IOopHjR8Iph03tsViu4nIes5XhDvyHbTtUxmeec=
github.com/docker/go-units v0.5.0 h1:69rxXcBk27SvSaaxTtLh/8llcHD8vYHT7WSdRZ/jvr4=
github.com/docker/go-units v0.5.0/go.mod h1:fgPhTUdO+D/Jk86RDLlptpiXQzgHJF7gydDDbaIK4Dk=
github.com/gogo/protobuf v1.3.2 h1:Ov1cvc58UF3b5XjBnZv7+opcTcQFZebYjWzi34vdm4Q=
github.com/gogo/protobuf v1.3.2/go.mod h1:P1XiOD3dCwIKUDQYPy72D8LYyHL2YPYrpS2s69NZV8Q=
```

go.mod **go.sum**

aqua

Lock file ? - Dependency Confusion

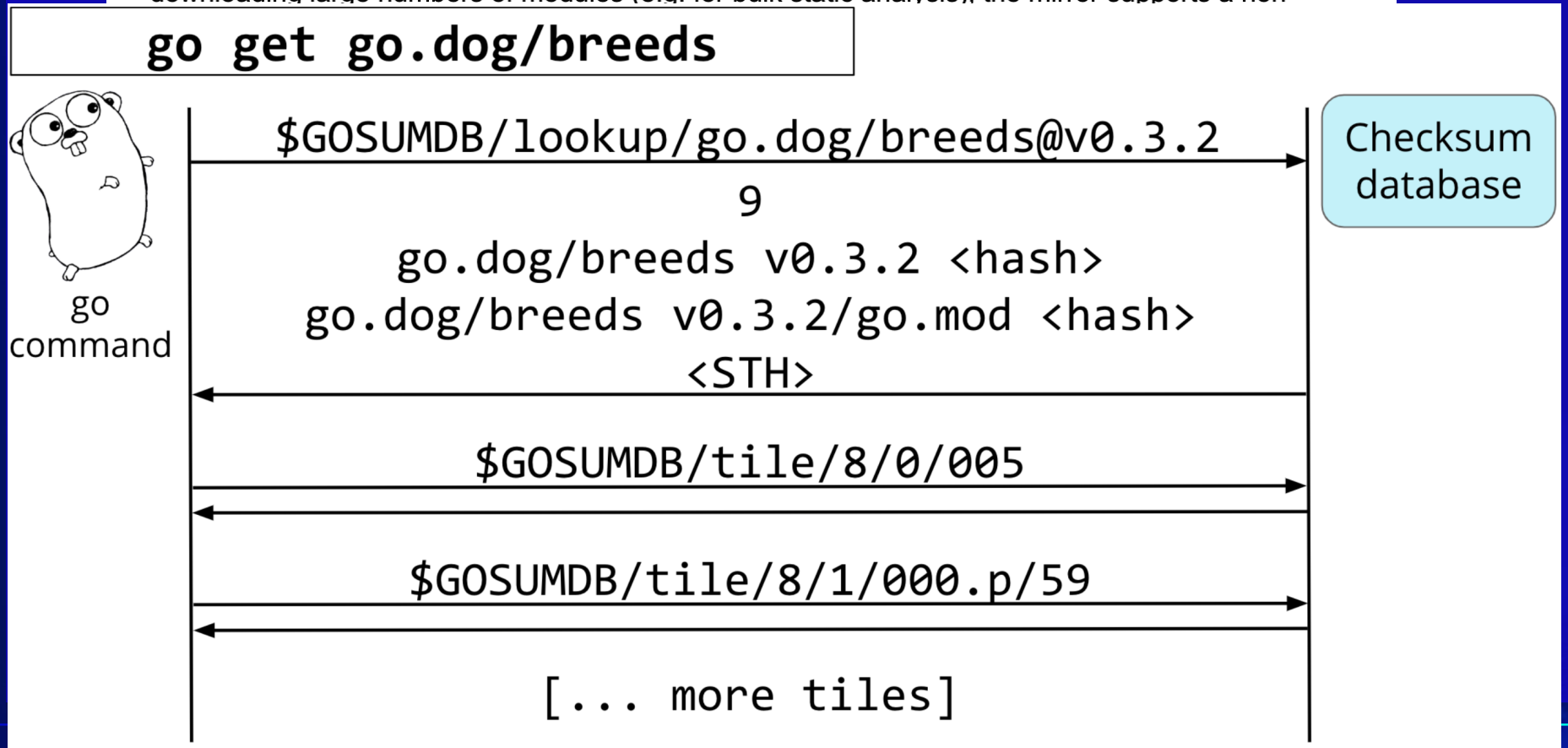
```
"dependencies": {
  "express": "^4.3.0",
  "dustjs-helpers": "~1.6.3",
  "continuation-local-storage": "^3.1.0",
  "pplogger": "^0.2",
  "auth-paypal": "^2.0.0",
  "wurfl-paypal": "^1.0.0",
  "analytics-paypal": "~1.0.0"
}
```


aqua

Auditable Checksum database

Services

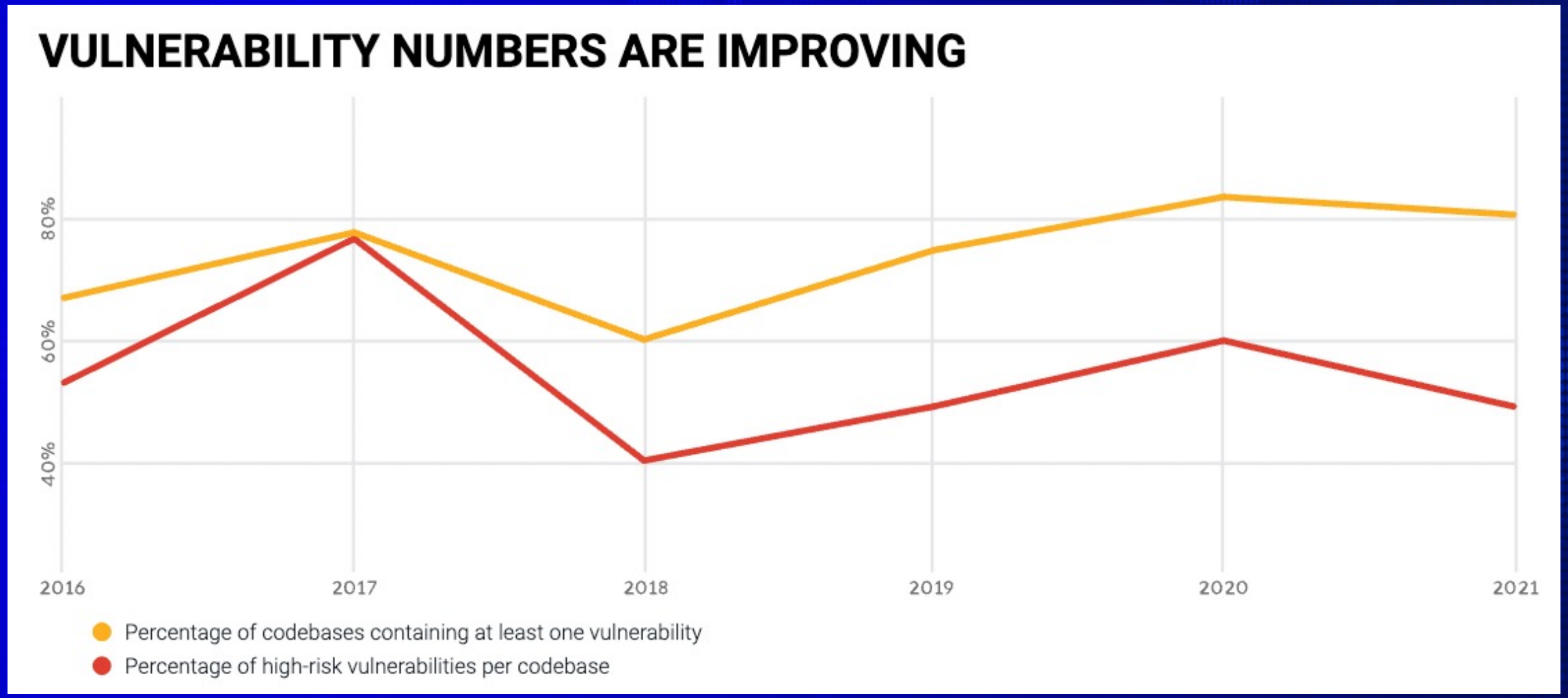
proxy.golang.org - a module mirror which implements the module proxy protocol. For users downloading large numbers of modules (e.g. for bulk static analysis), the mirror supports a non-



https://go.dev/blog/module-mirror-launch

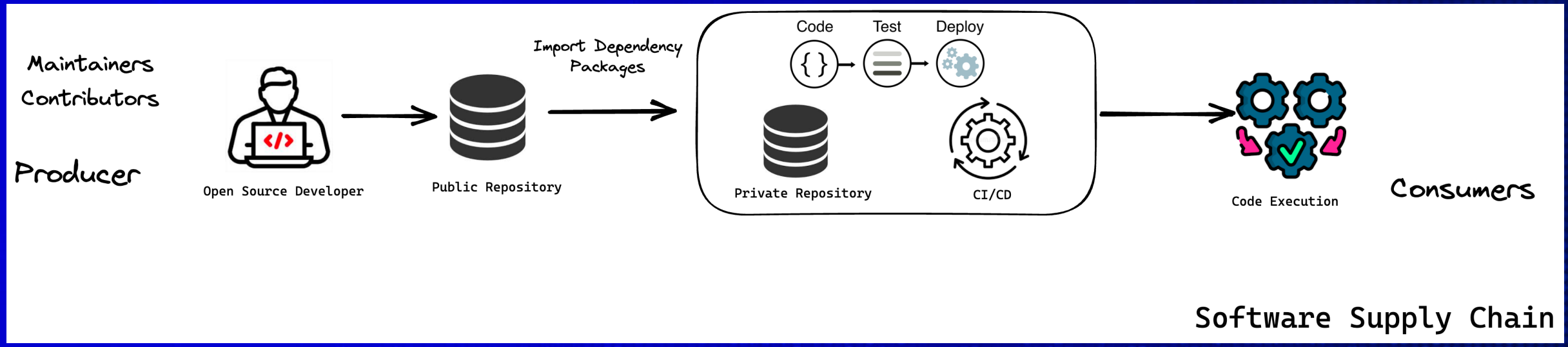
aqua

Open Source Vulnerabilities

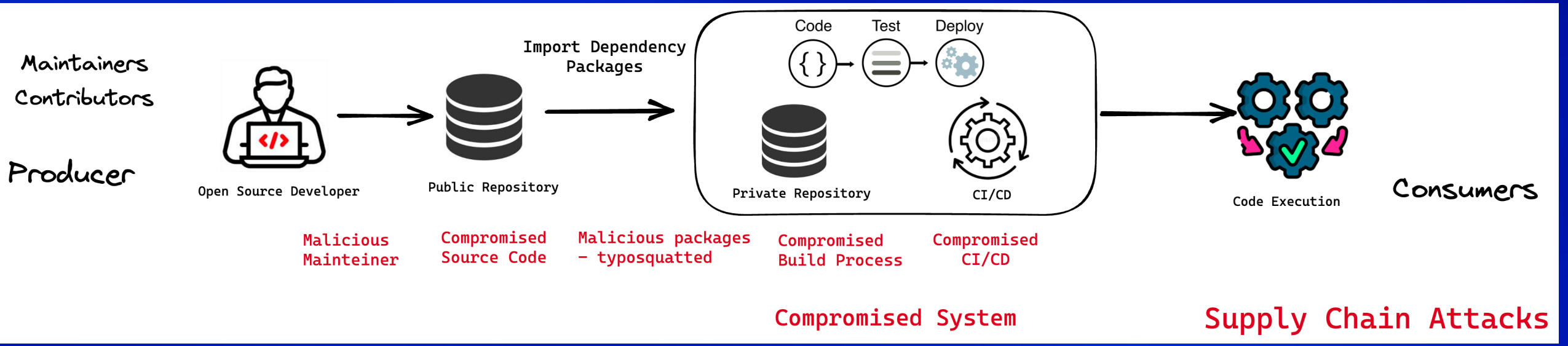


https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

Consumer / Producer Code – Supply chain



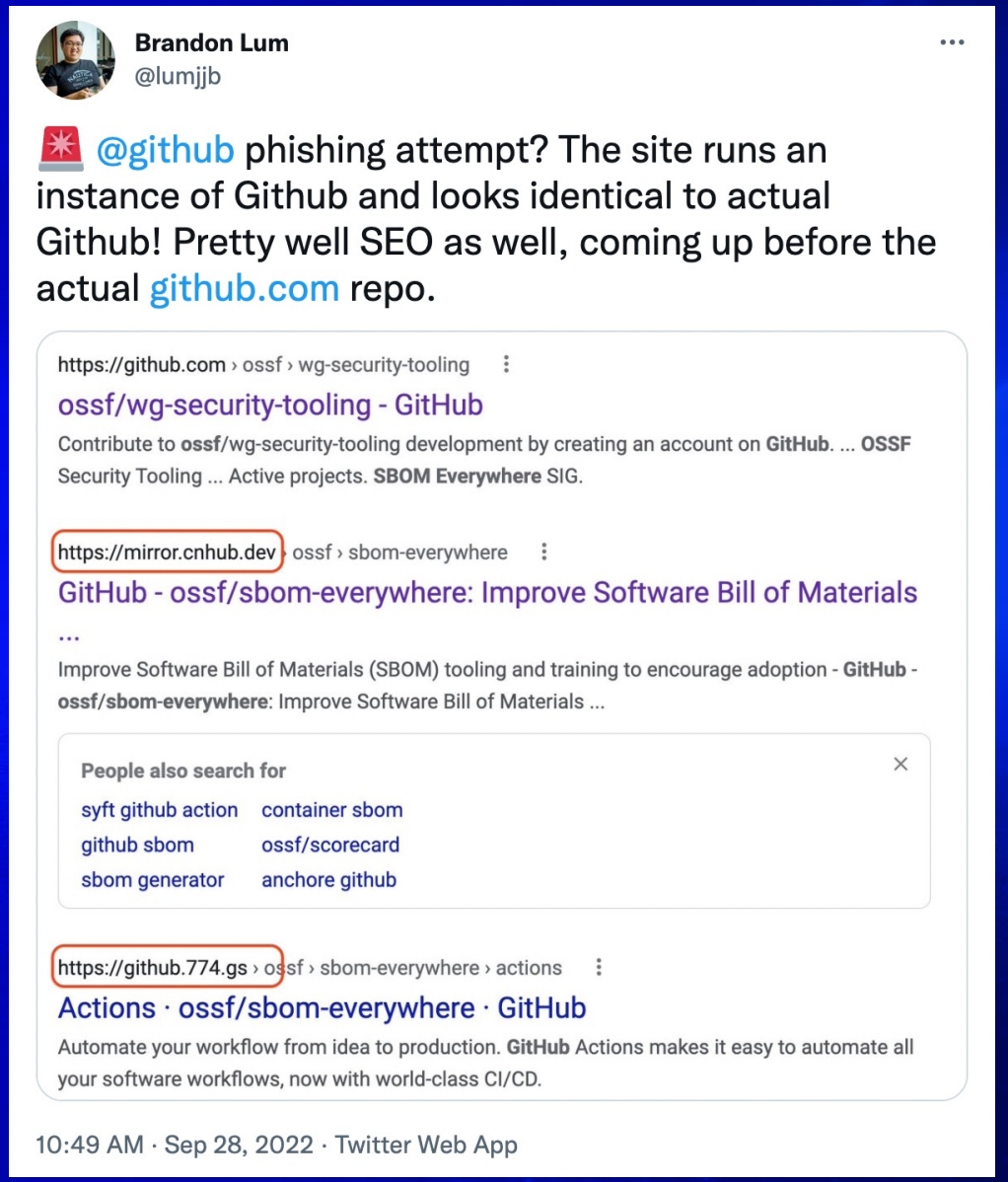
Supply Chain Attacks



scala-network/GUI-miner

dstellitecoin/gui-miner

Supply Chain Attacks



Supply Chain Attacks

Dr Owain Kenway
@owainkenway

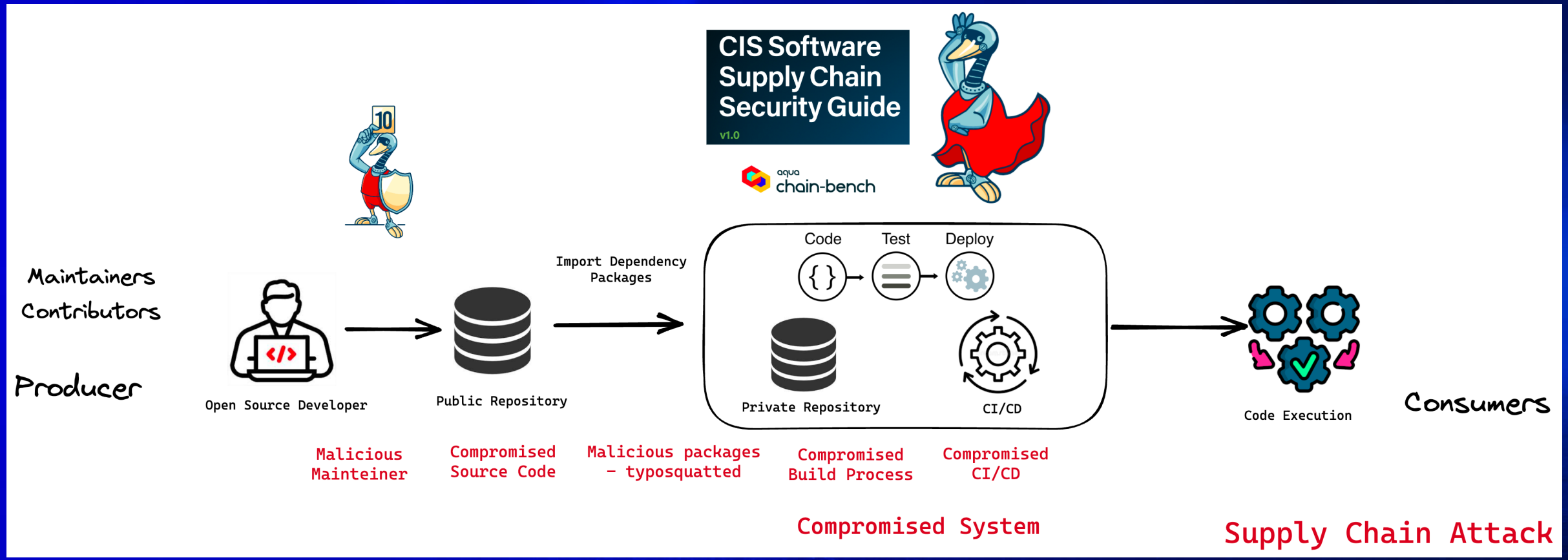
Tl;dr of the attack:

🟢 don't use people's random forks of the repo you want
🟢 git's attribution is trivially spoofed so you can't look at a commit that isn't gpg signed and say that person did it.
🟢 don't use any packages that pull in random forks as part of their build

5:19 AM · Aug 3, 2022 · Twitter for iPad

aqua

Supply Chain Attacks



Supply Chain Security Tool

aqua chain-bench

```
kubernetes-security-checklist → chain-bench scan -v --repository-url https://github.com/krol3/helloworld --access-token [redacted]
2022-08-21 16:49:14 INF       Fetch Starting
2022-08-21 16:49:16 INF       Fetching Repository Settings Finished
2022-08-21 16:49:16 INF       Fetching Branch Protection Settings Finished
2022-08-21 16:49:18 INF       Fetching Pipelines Finished
2022-08-21 16:49:18 INF       Fetch succeeded
```

ID	Name	Result	Reason
1.1.3	Ensure any change to code receives approval of two strongly authenticated users	Failed	
1.1.4	Ensure previous approvals are dismissed when updates are introduced to a code change proposal	Failed	
1.1.5	Ensure that there are restrictions on who can dismiss code change reviews	Failed	
1.1.6	Ensure code owners are set for extra sensitive code or configuration	Failed	
1.1.8	Ensure inactive branches are reviewed and removed periodically	Passed	
1.1.9	Ensure all checks have passed before the merge of new code	Failed	
1.1.10	Ensure open git branches are up to date before they can be merged into codebase	Failed	
1.1.11	Ensure all open comments are resolved before allowing to merge code changes	Failed	
1.1.12	Ensure verifying signed commits of new changes before merging	Passed	
1.1.13	Ensure linear history is required	Failed	MergeCommit is enabled for repository
1.1.14	Ensure branch protection rules are enforced on administrators	Failed	
1.1.15	Ensure pushing of new code is restricted to specific individuals or teams	Failed	
1.1.16	Ensure force pushes code to branches is denied	Passed	
1.1.17	Ensure branch deletions are denied	Failed	
1.2.1	Ensure all public repositories contain a SECURITY.md file	Failed	
1.2.2	Ensure repository creation is limited to specific members	Unknown	Organization is not fetched
1.2.3	Ensure repository deletion is limited to specific members	Unknown	Organization is not fetched
1.2.4	Ensure issue deletion is limited to specific members	Unknown	Organization is not fetched
1.3.1	Ensure inactive users are reviewed and removed periodically	Passed	
1.3.3	Ensure minimum admins are set for the organization	Unknown	Organization is not fetched
1.3.5	Ensure the organization is requiring members to use MFA	Unknown	Organization is not fetched
1.3.7	Ensure 2 admins are set for each repository	Failed	
1.3.8	Ensure strict base permissions are set for repositories	Unknown	Organization is not fetched
1.3.9	Ensure an organization's identity is confirmed with a Verified badge	Unknown	Organization is not fetched
2.3.1	Ensure all build steps are defined as code	Passed	
2.3.5	Ensure access to the build process's triggering is minimized	Unknown	Organization is not fetched
2.3.7	Ensure pipelines are automatically scanned for vulnerabilities	Passed	
2.3.8	Ensure scanners are in place to identify and prevent sensitive data in pipeline files	Failed	Repository is not scanned for secrets
2.4.2	Ensure all external dependencies used in the build process are locked	Failed	6 task(s) are not pinned
2.4.6	Ensure pipeline steps produce an SBOM	Failed	2 pipeline(s) contain a build job without SBOM generation
3.1.7	Ensure dependencies are pinned to a specific, verified version	Failed	6 dependencies are not pinned
3.2.2	Ensure packages are automatically scanned for known vulnerabilities	Passed	
3.2.3	Ensure packages are automatically scanned for license implications	Passed	
4.2.3	Ensure user's access to the package registry utilizes MFA	Unknown	Registry is not fetched
4.2.5	Ensure anonymous access to artifacts is revoked	Unknown	Registry is not fetched
4.3.4	Ensure webhooks of the package registry are secured	Passed	

```
Total Passed Rules: 9 out of 26
2022-08-21 16:49:18 INF Scan completed: 4s
```

CIS Software Supply Chain Security Guide

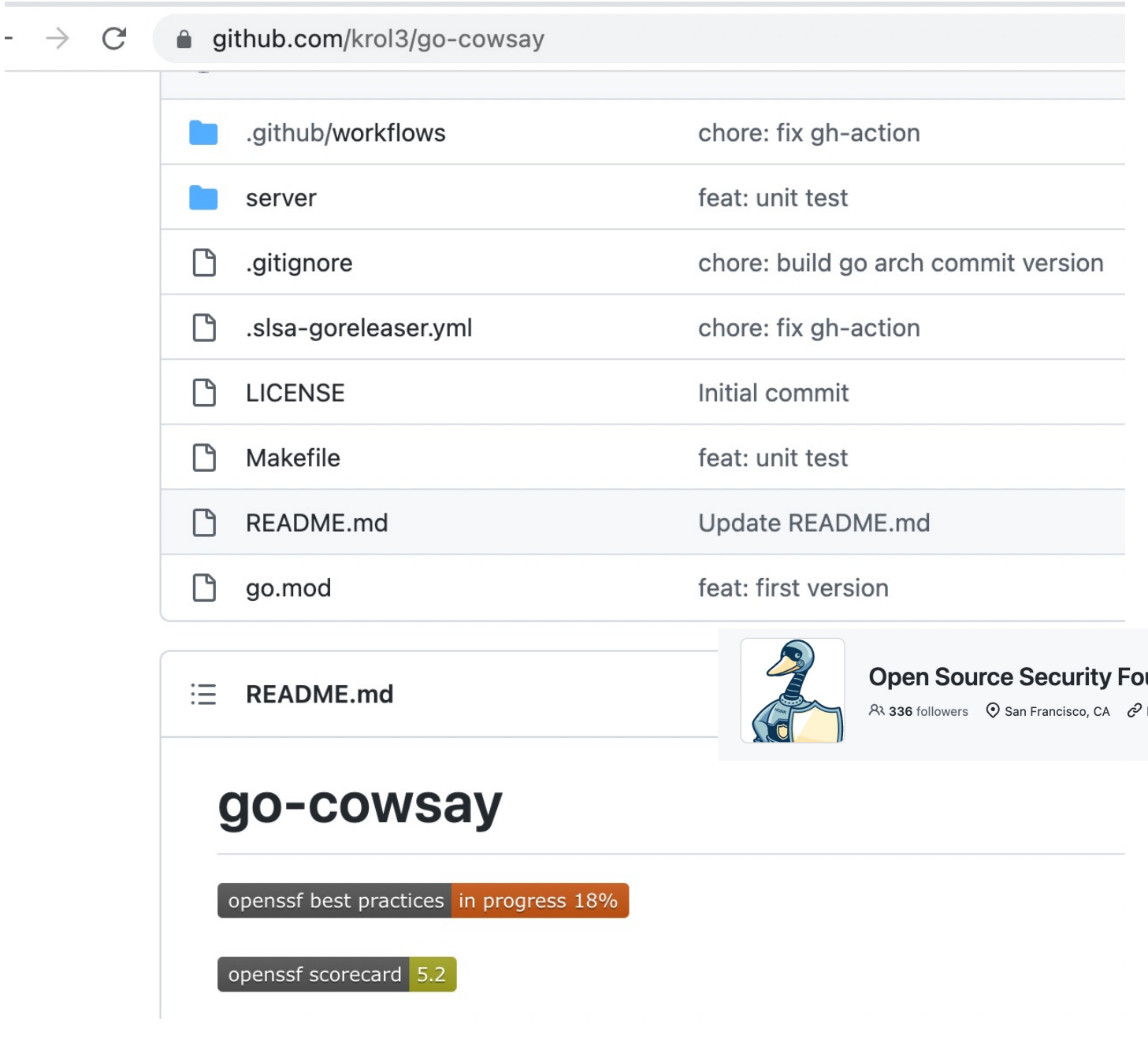
v1.0

aqua

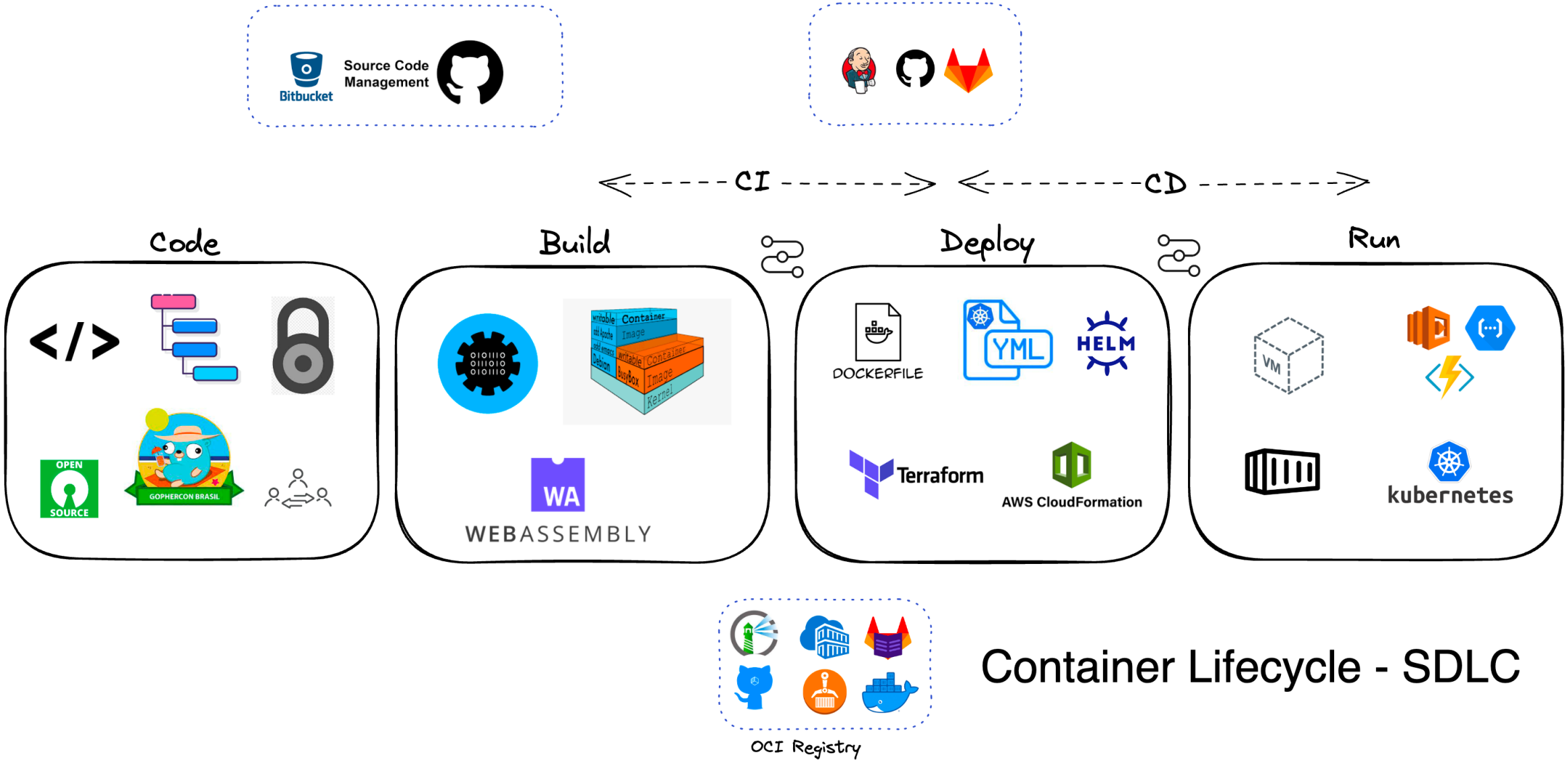
Scorecard Results

Project	Score	Date	Commit
github.com/nektos/act	6.2	2022-09-13	3a0fe6967fd8ecd3cb86550d0225d55a0bb37ac9
github.com/beego/beego	6.4	2022-09-13	e84b93919f7b41a7518329c6d5f084f89a15bdfe
github.com/caddyserver/caddy	6.6	2022-09-13	754fe4f7b4dddbfc7a8ee7fee405cee057da858e
github.com/aquasecurity/chain-bench	6.3	2022-09-13	b998b0fd23bb7d6273d3e8f373458cb4d82ff51d
github.com/Dreamacro/clash	4.9	2022-09-13	425b6e0dc098535874a29ccc45a5c5ebece324ce
github.com/cli/cli	7.8	2022-09-13	e16bf033edbe507219e033aa16c630a8833349b7
github.com/spf13/cobra	6.4	2022-09-13	7e289f46f1d1b2567b123cc26db0e7cd76644c32
github.com/cockroachdb/cockroach	6.8	2022-09-13	0dd5e5954738502fc922b2a29e8ff845d05afd4c
github.com/docker/compose	6.3	2022-09-13	1ed37ef7bdc52f21585ac74e9a89e5d5d3b9adfe
github.com/hashicorp/consul	6.3	2022-09-13	0150e88200aae78ae163a05bea947aeefaa39012
github.com/schollz/croc	4.6	2022-09-13	1517767129b7f32e6e1c8d1caceace4fb8fda0be
github.com/wagoodman/dive	4.8	2022-09-13	c7d121b3d72aeaded26d5731819afaf49b686df6
github.com/harness/drone	6.4	2022-09-13	d3dad5796875b75f5cfe2d7f53cb0ccf0b7ef1ce
github.com/labstack/echo	5.2	2022-09-13	50e7e569f0660b2b02ef457687b451072c106c40
github.com/etcd-io/etcd	6.8	2022-09-13	bbcbcd9db43f43ab901855f9f20151c057f160dd
github.com/openfaas/faas	5	2022-09-13	9da2ec244f9648156d5d90559453fa12d3d25663
github.com/gofiber/fiber	7.4	2022-09-13	8ec62a64cc8367372cd9eb1fc48eba380ee01bdf
github.com/fatedier/frp	5.6	2022-09-13	6ecc97c8571df002dd7cf42522e3f2ce9de9a14d
github.com/junegunn/fzf	6.6	2022-09-13	b5efc68737e8231001d2a18234c18aa3f658a973

aqua


github.com/krol3/go-cowsay
.github/workflows
chore: fix gh-action
server
feat: unit test
.gitignore
chore: build go arch commit version
.slsa-goreleaser.yml
chore: fix gh-action
LICENSE
Initial commit
Makefile
feat: unit test
README.md
Update README.md
go.mod
feat: first version
README.md
Open Source Security Foundation (OpenSSF)
336 followers
San Francisco, CA
https://openssf.org
go-cowsay
openssf best practices
in progress 18%
openssf scorecard
5.2

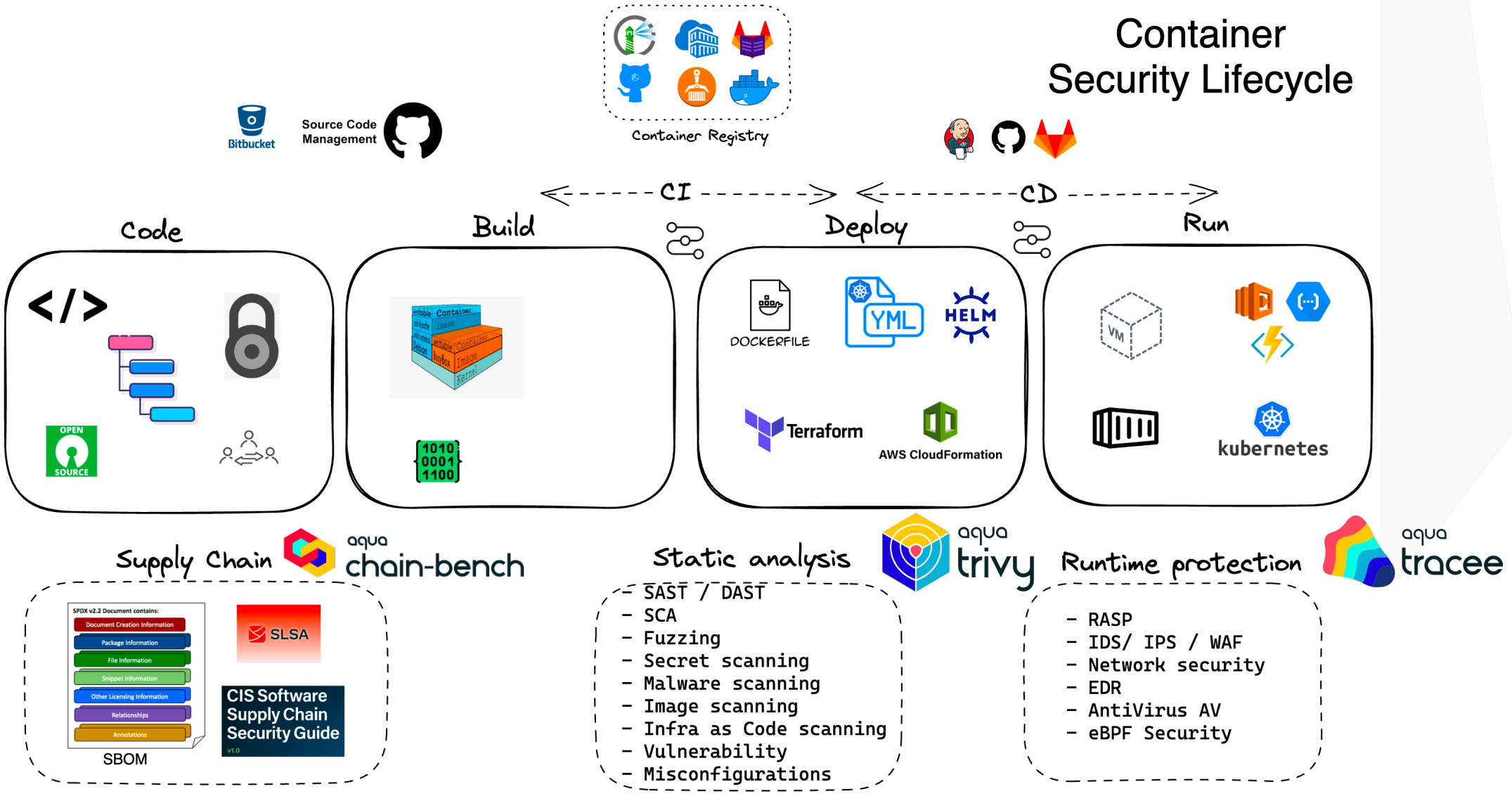
Applying Devops ….



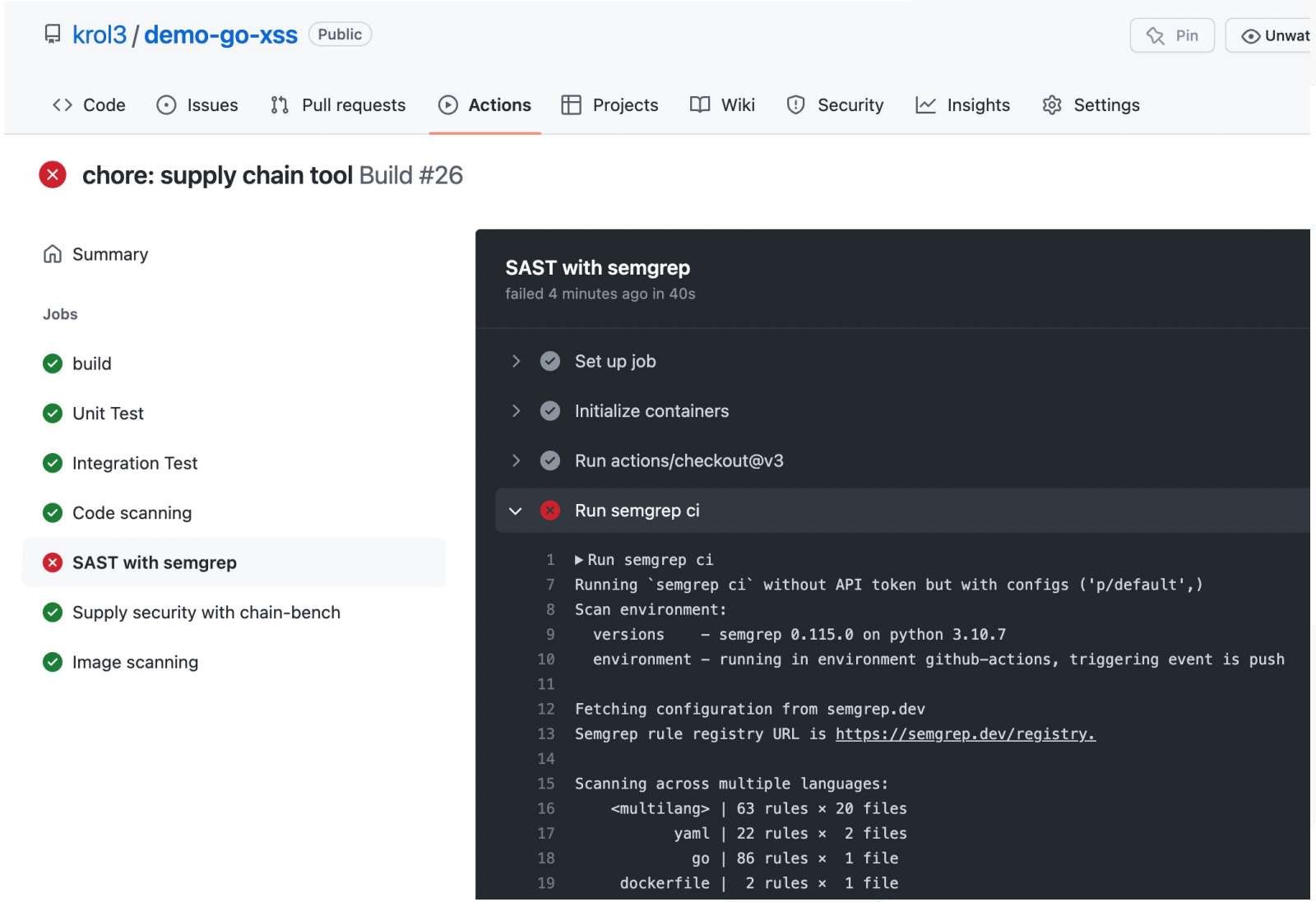
Container Lifecycle - SDLC


New technology ...
new security holes ...
new security best practices.
EVERGREEN

Applying DevSecOps ….



Pipeline sample



https://github.com/krol3/demo-go-xss/

Pipeline sample – Detecting xss

```
go.lang.security.audit.xss.no-fprintf-to-responsewriter.no-fprintf-to-responsewriter
   Detected 'Fprintf' or similar writing to 'http.ResponseWriter'. This bypasses HTML escaping
   that prevents cross-site scripting vulnerabilities. Instead, use the 'html/template' package
   to render data to users.
   Details: https://sg.run/7oqR

    41┆ fmt.Fprintf(w, "missing parameter ?%s=xxxxx", queryKey)
      ⋮┆----------------------------------------
go.lang.security.audit.xss.no-io-writestring-to-responsewriter.no-io-writestring-to-
responsewriter
   Detected 'io.WriteString()' writing directly to 'http.ResponseWriter'. This bypasses HTML
   escaping that prevents cross-site scripting vulnerabilities. Instead, use the
   'html/template' package to render data to users.
   Details: https://sg.run/gLwn
```

aqua

Thanks

in/carolgv

krol3

@krol_valencia