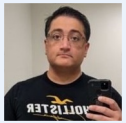
DASH HUDSON

DevSecOps Deciphered

AtlSecCon 2023



Sunny Jamwal
Director of CyberSecurity

DASH HUDSON

Outsmart Social

A social media management platform that delivers sophisticated insights and workflow tools, keeping you in the know and saving you time — so you and your team can get back to marketing.

TRUSTED BY BRANDS OF ALL SIZES

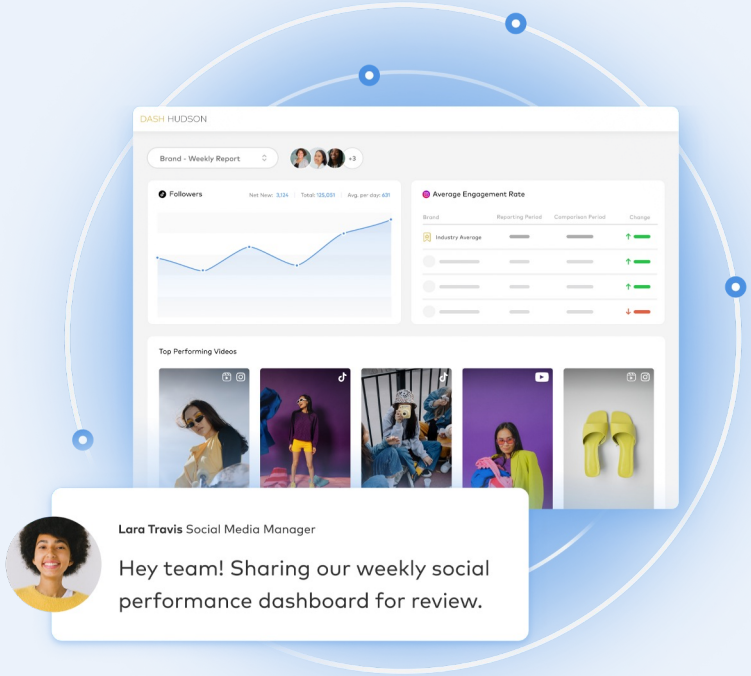
Rare Beauty

HARRY'S

Tripadvisor

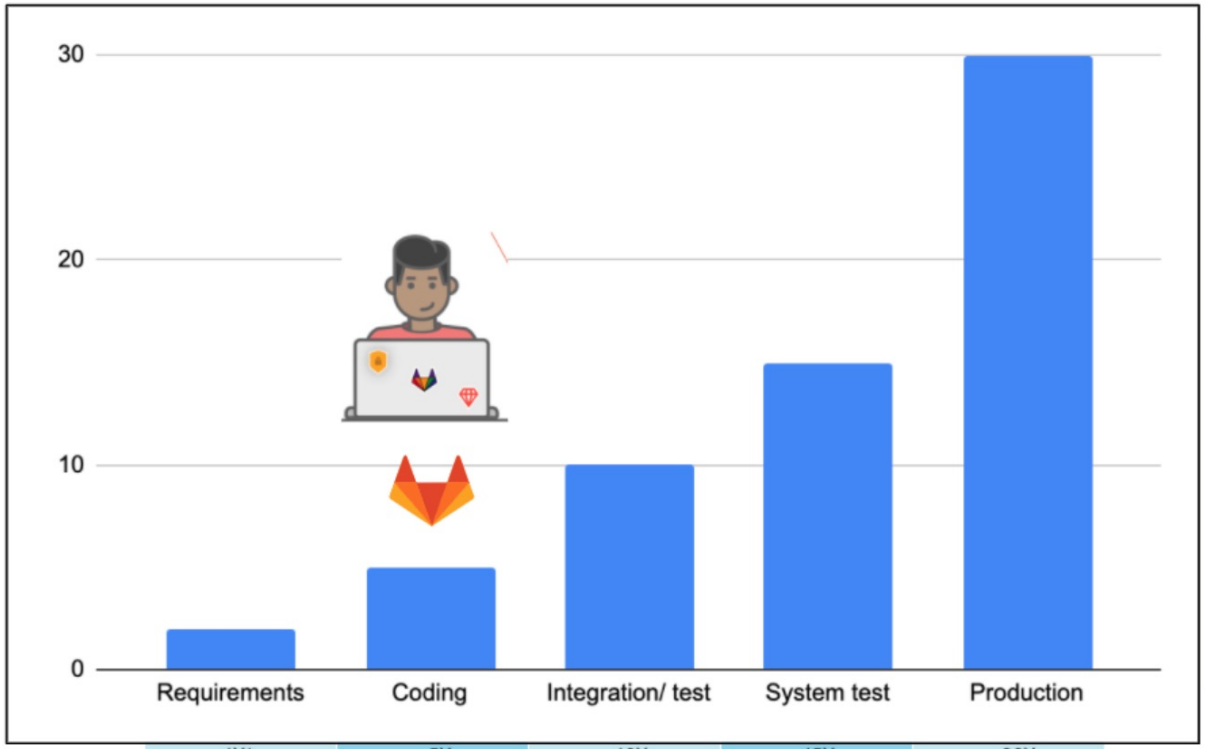
MEJURI

Crate&Barrel




why?
why?
why?
why?
why?

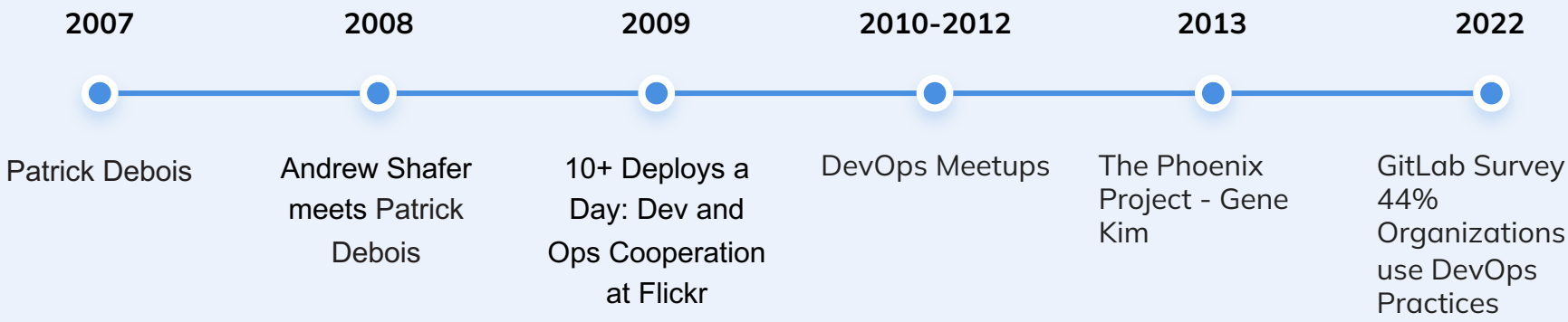
Stage of remediation

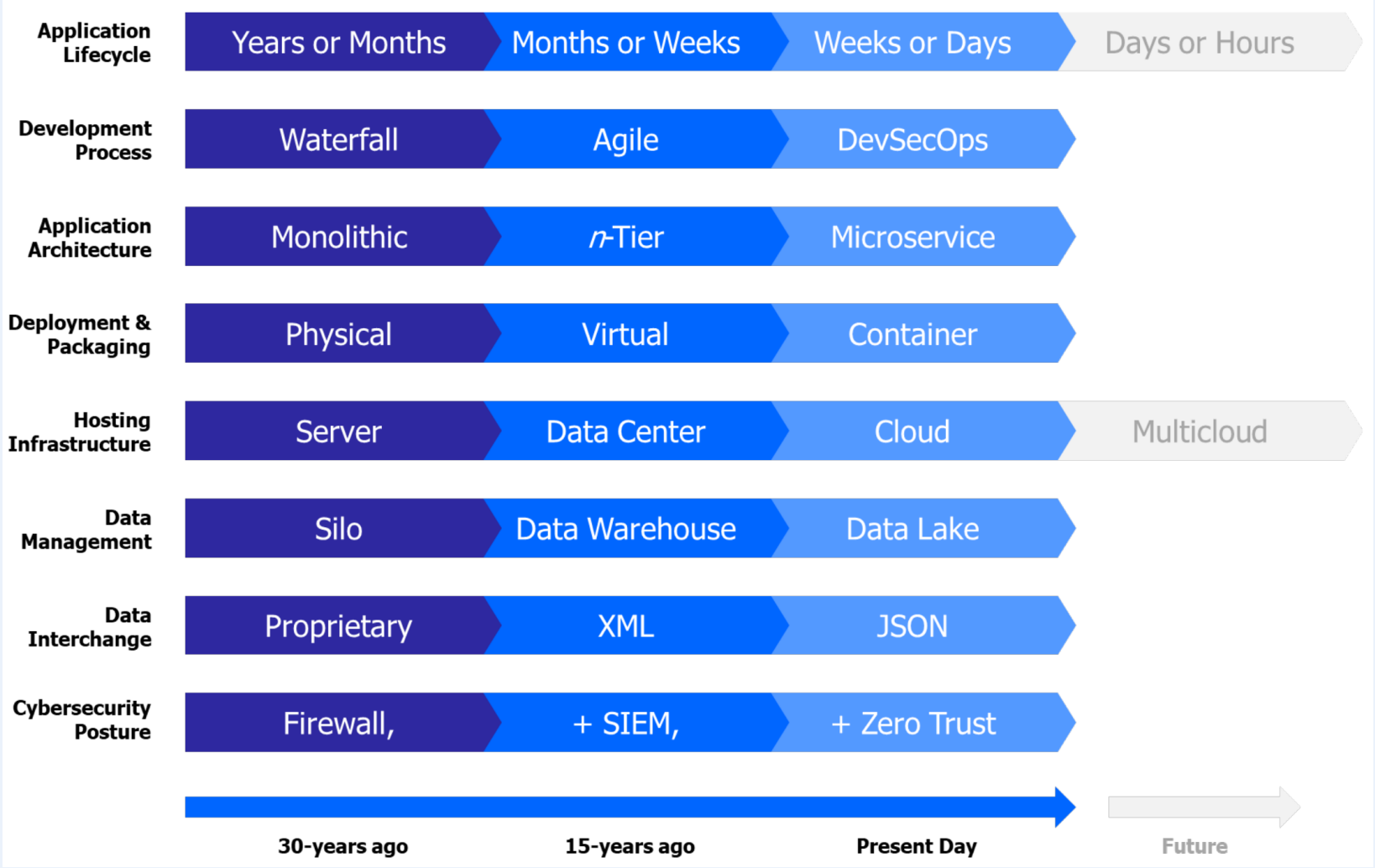


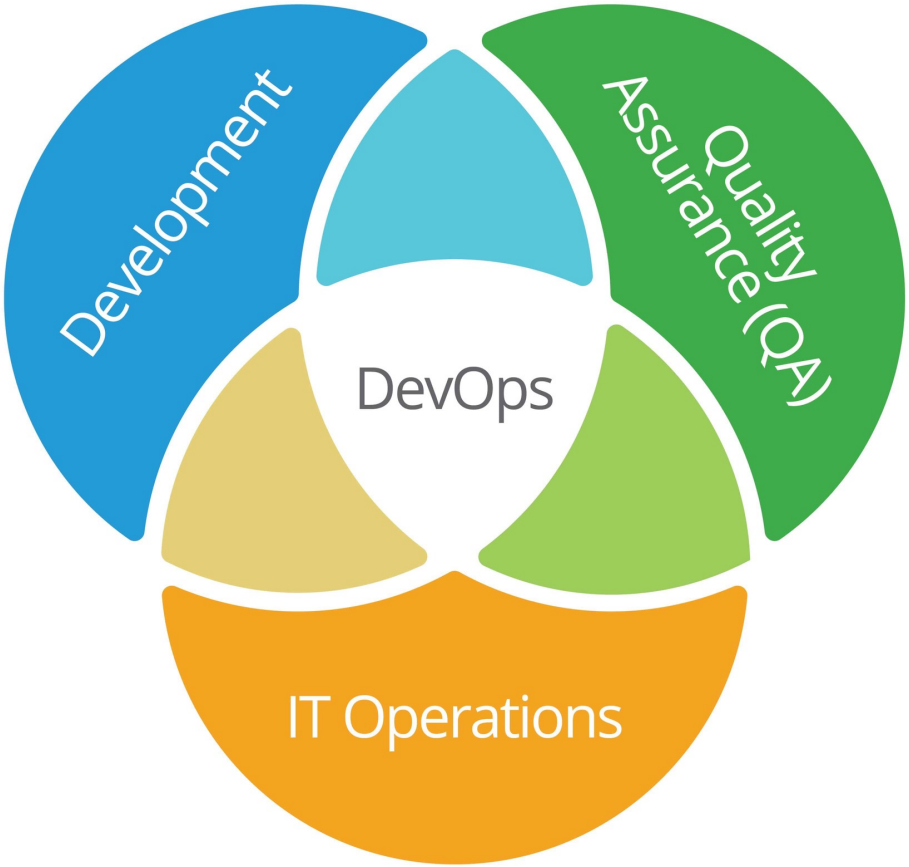
*X is a normalized unit of cost and can be expressed in terms of person-hours, dollars, etc.
Source: National Institute of Standards and Technology (NIST)†

DevOps

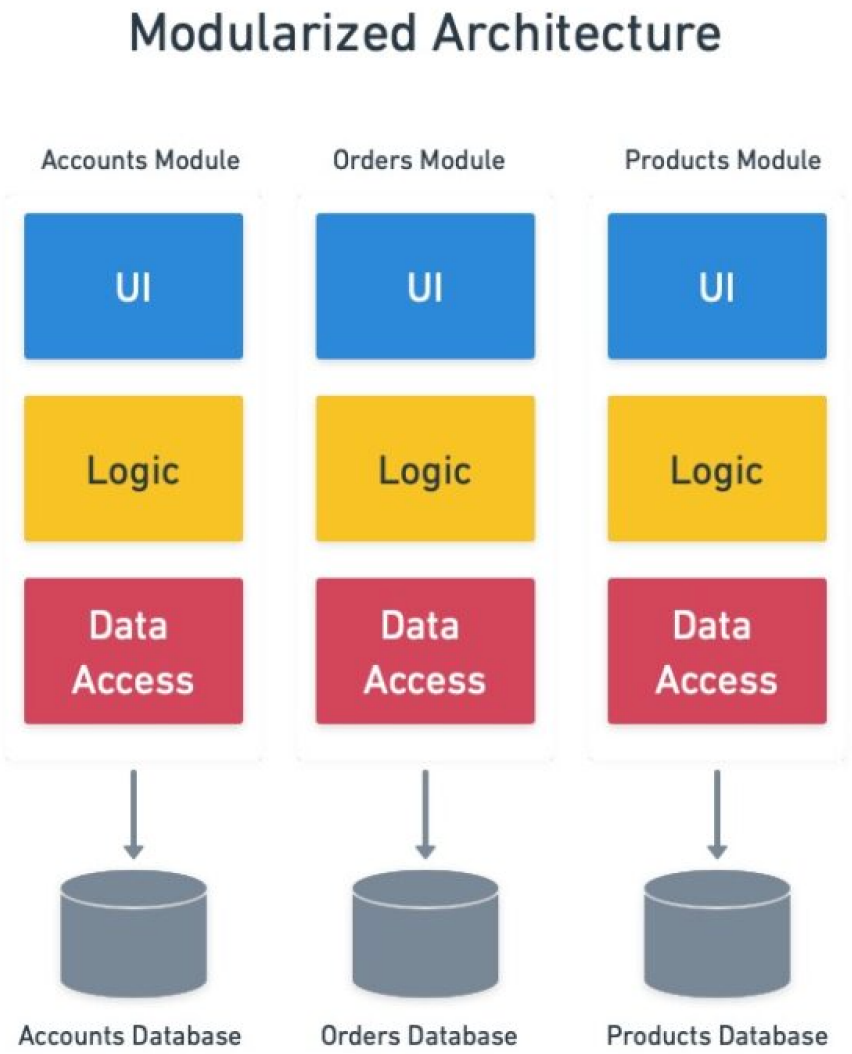
HISTORY




Application Lifecycle
Years or Months
Months or Weeks
Weeks or Days
Days or Hours
Development Process
Waterfall
Agile
DevSecOps
Application Architecture
Monolithic
n-Tier
Microservice
Deployment & Packaging
Physical
Virtual
Container
Hosting Infrastructure
Server
Data Center
Cloud
Multicloud
Data Management
Silo
Data Warehouse
Data Lake
Data Interchange
Proprietary
XML
JSON
Cybersecurity Posture
Firewall,
+ SIEM,
+ Zero Trust
30-years ago
15-years ago
Present Day
Future

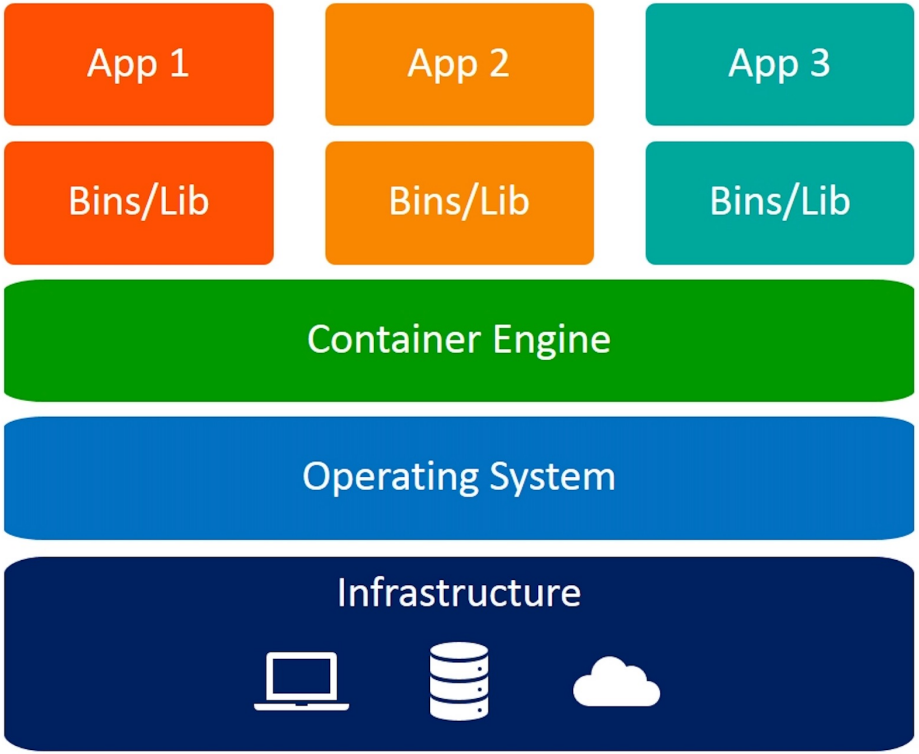


- Microservices
- Containers
- Kubernetes
- CI/CD
- Cloud



Microservices

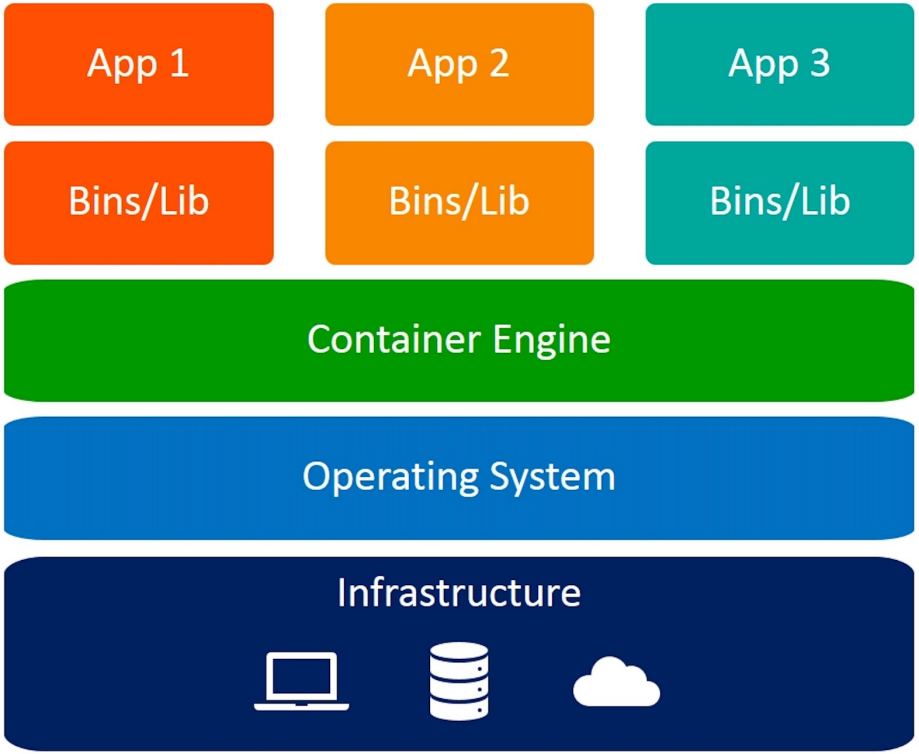
- ✓ Autonomous
- ✓ Agility
- ✓ Technological Freedom
- ✓ Resilience



Containers

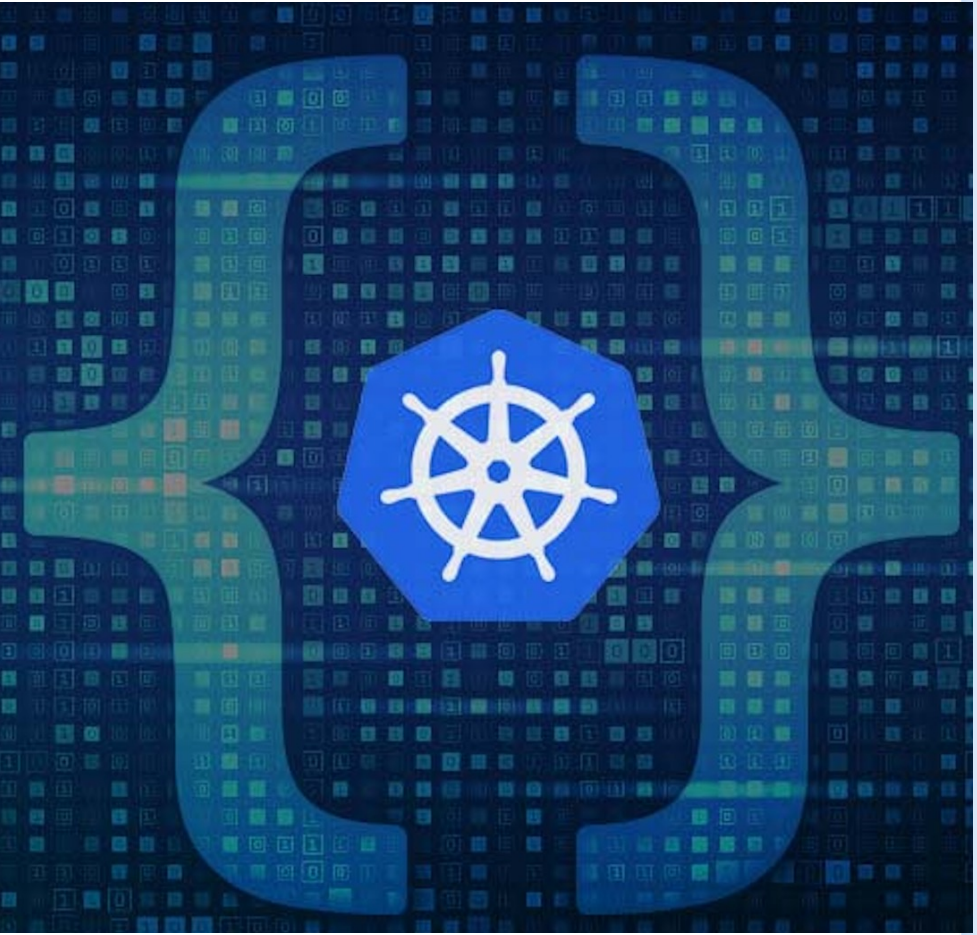
Containers

- ✓ *Containers virtualize an OS in order to run multiple applications in one OS.*
- ✓ *VMs virtualize hardware to run multiple OS.*



Containers

```
#Select Base Image
FROM nginx:1.23.4

#Change to working directory
WORKDIR /usr/share/nginx/html

#Copy the HTML File
COPY welcome.html ./

#Copy the image
COPY image.jpg ./

#Copy python file
COPY insecure.py ./

#Open port 80
EXPOSE 80
```



Kubernetes

- ✓ Kubernetes was developed by Google before being open-sourced in 2014.
- ✓ Kubernetes is a descendant of Borg, a container orchestration platform used internally at Google.
- ✓ Kubernetes is an orchestration platform for containers.
- ✓ Kubernetes handles the computing, networking, and storage on behalf of your workloads.

Monolithic Application

Recruitment Website

Job Applicants

Job Vacancies

Recruiters

Transition to Microservices

Recruitment Website

Recruiters

Job Applicants

Job Vacancies

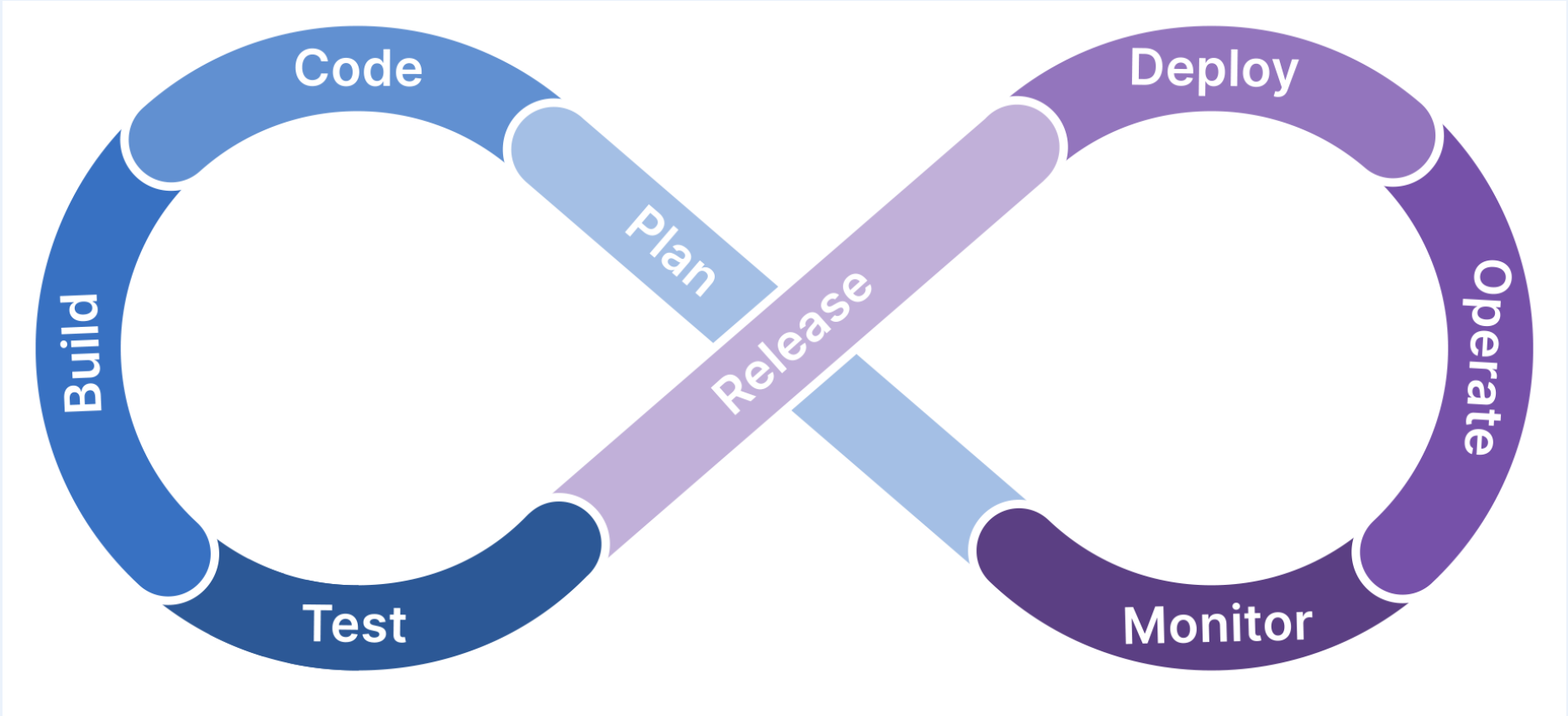
Docker

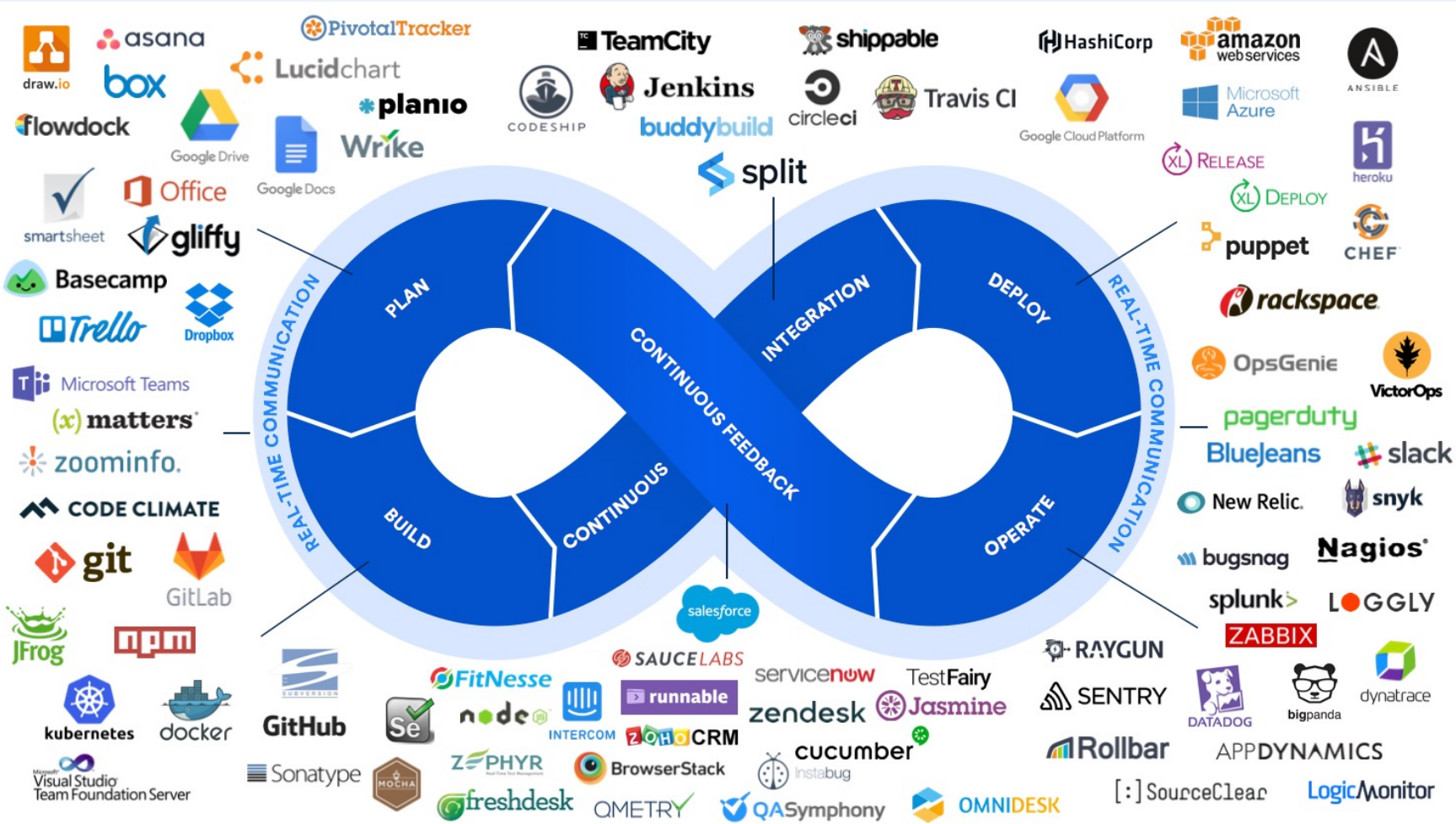
Create containers for your application

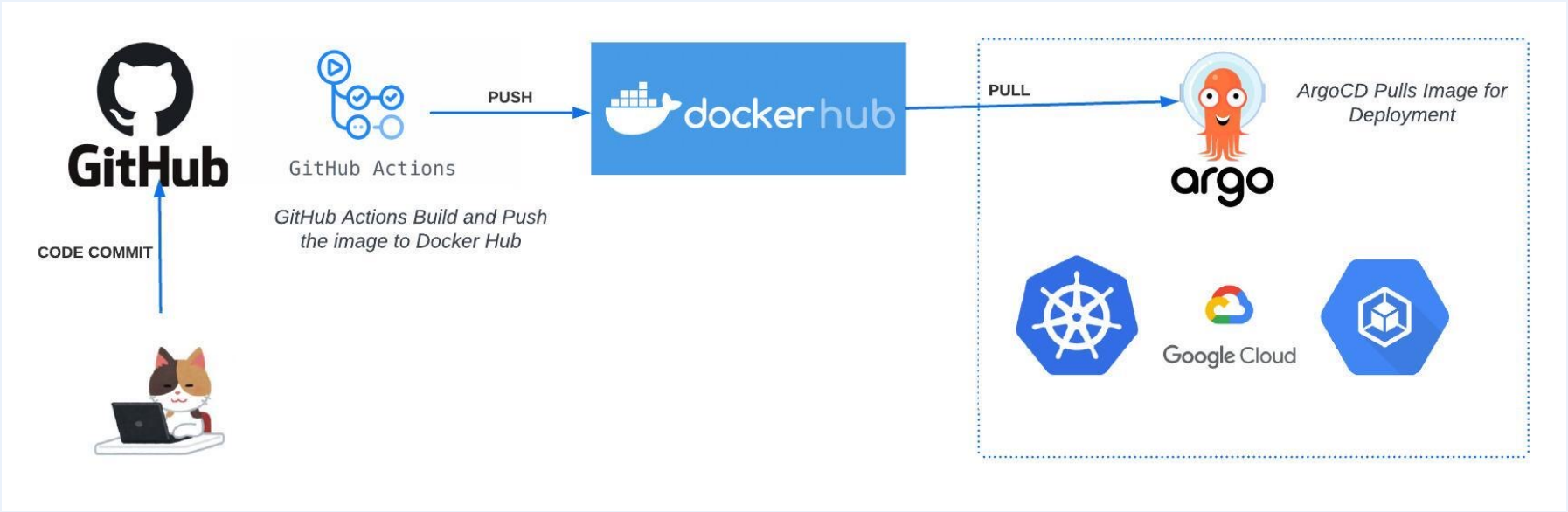
Kubernetes

Launch your containerised application in K8s

Continuous Integration / Continuous Development




draw.io
asana
box
flowdock
Google Drive
PivotalTracker
Lucidchart
planio
Google Docs
Wrike
CODESHIP
TeamCity
Jenkins
buddybuild
shippable
circleci
Travis CI
HashiCorp
Google Cloud Platform
amazon web services
Microsoft Azure
ANSIBLE
split
smartsheet
Office
gliffy
Basecamp
Trello
Dropbox
RELEASE
DEPLOY
heroku
puppet
CHEF
rackspace
PLAN
CONTINUOUS FEEDBACK
INTEGRATION
DEPLOY
REAL-TIME COMMUNICATION
REAL-TIME COMMUNICATION
BUILD
CONTINUOUS
OPERATE
Microsoft Teams
(x) matters
zoominfo.
CODE CLIMATE
git
GitLab
JFrog
npm
kubernetes
docker
GitHub
Visual Studio Team Foundation Server
Sonatype
OpsGenie
VictorOps
pagerduty
BlueJeans
slack
New Relic.
snyk
bugsnag
Nagios
splunk>
LOGGLY
ZABBIX
RAYGUN
SENTRY
DATADOG
bigpanda
dynatrace
Rollbar
APPDYNAMICS
[:] SourceClear
LogicMonitor
salesforce
SAUCELABS
FitNesse
servicenow
TestFairy
runnable
zendesk
Jasmine
INTERCOM
ZOHO CRM
cucumber
Instabug
ZEPHYR
BrowserStack
freshdesk
QMETRY
QASymphony
OMNIDESK


GitHub
CODE COMMIT
GitHub Actions
PUSH
docker hub
GitHub Actions Build and Push
the image to Docker Hub
PULL
argo
ArgoCD Pulls Image for
Deployment
Google Cloud

Welcome

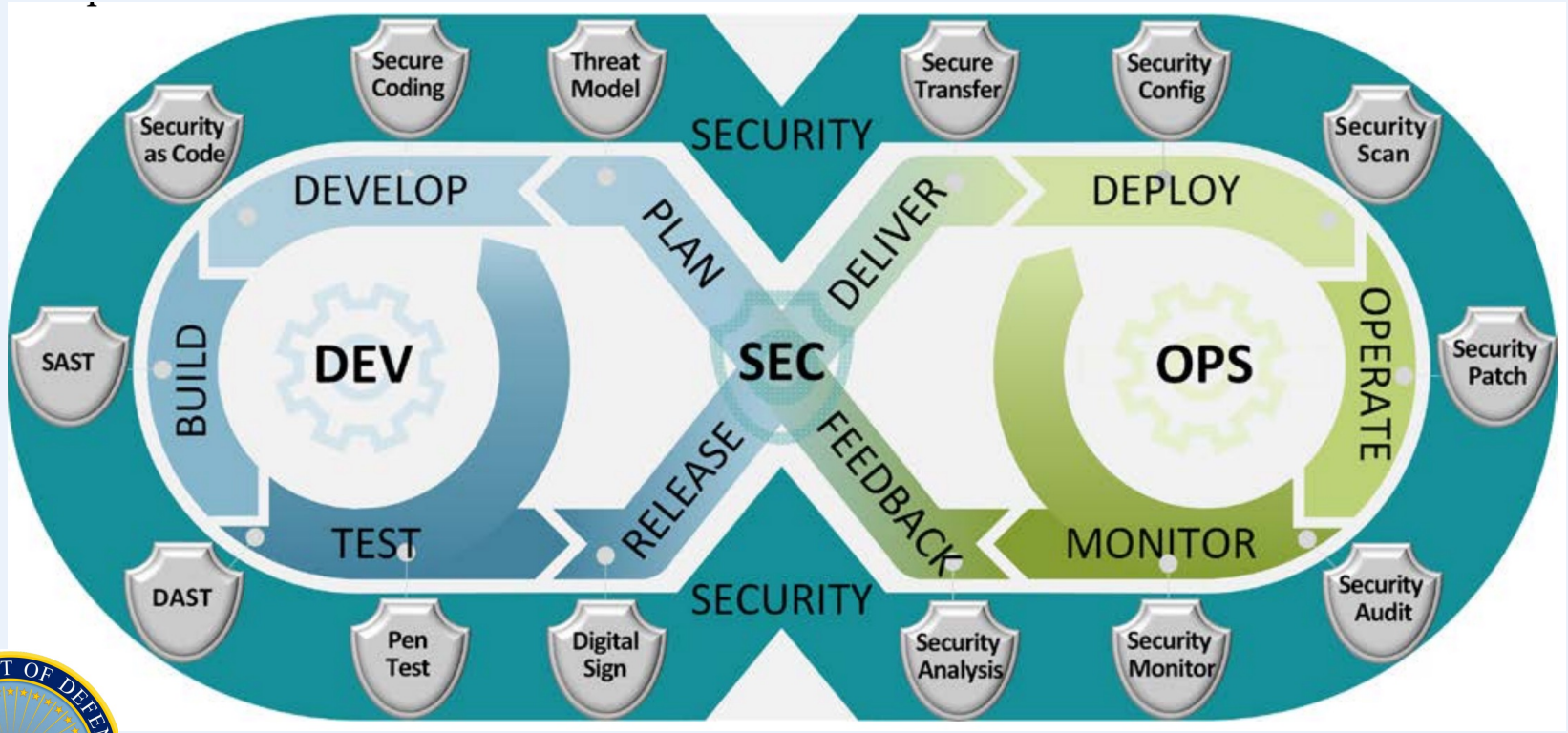
insecure

Welcome to AtlSecCon.

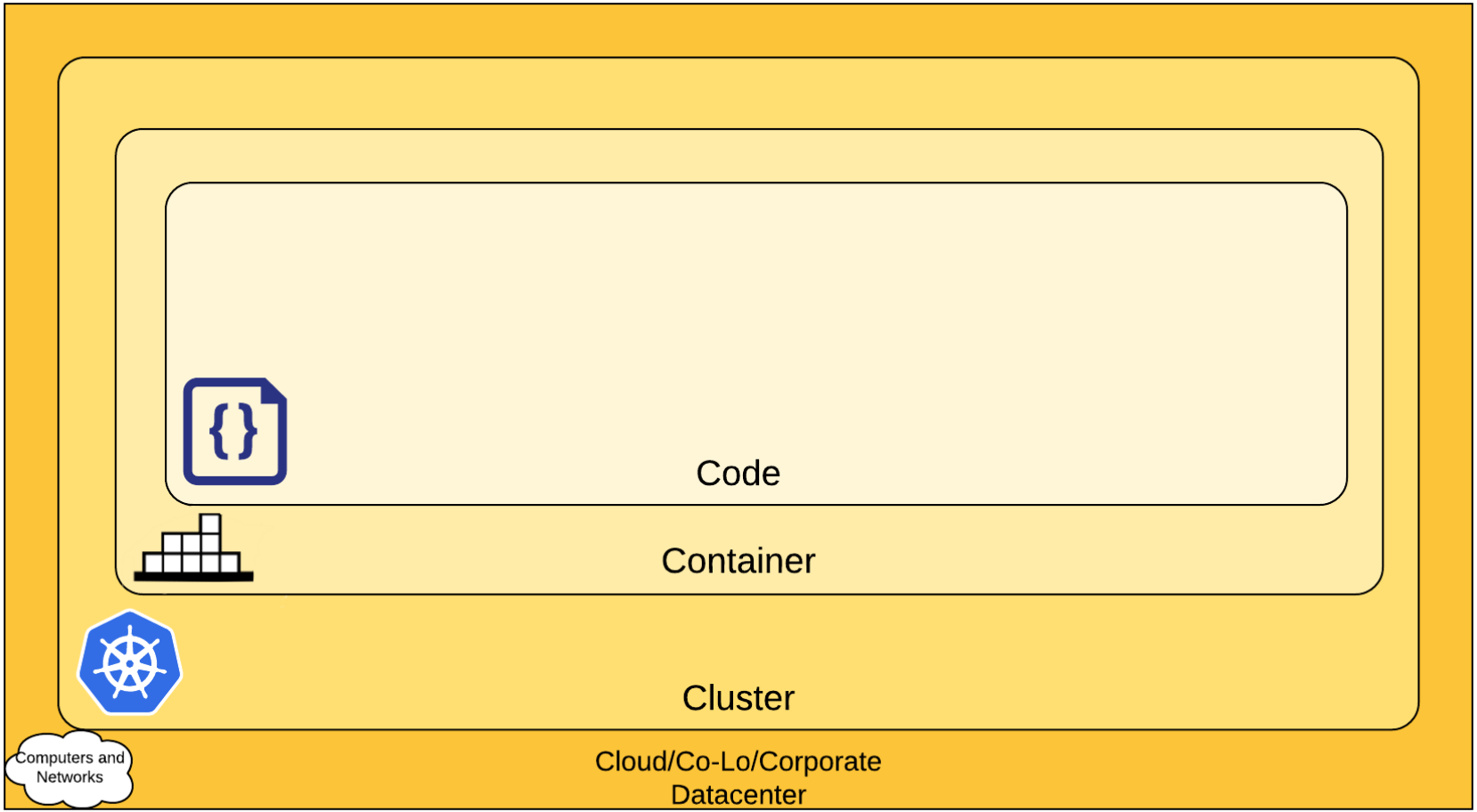
Welcome to AtlSecCon 2023! 👋

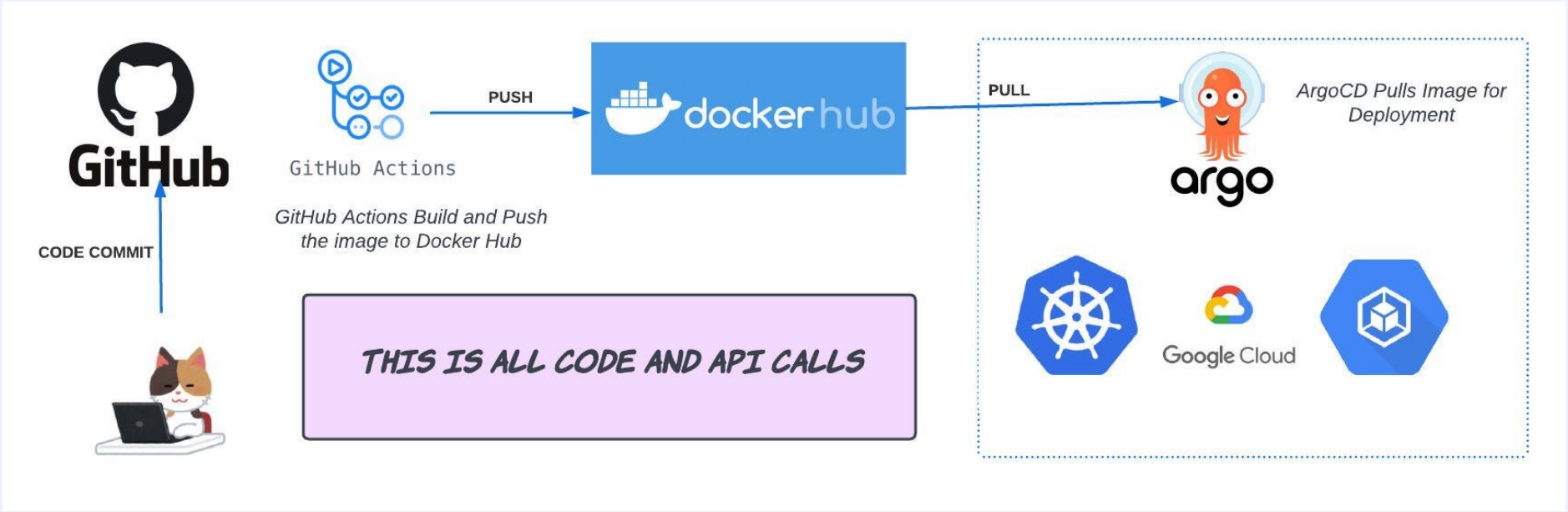
DASH HUDSON

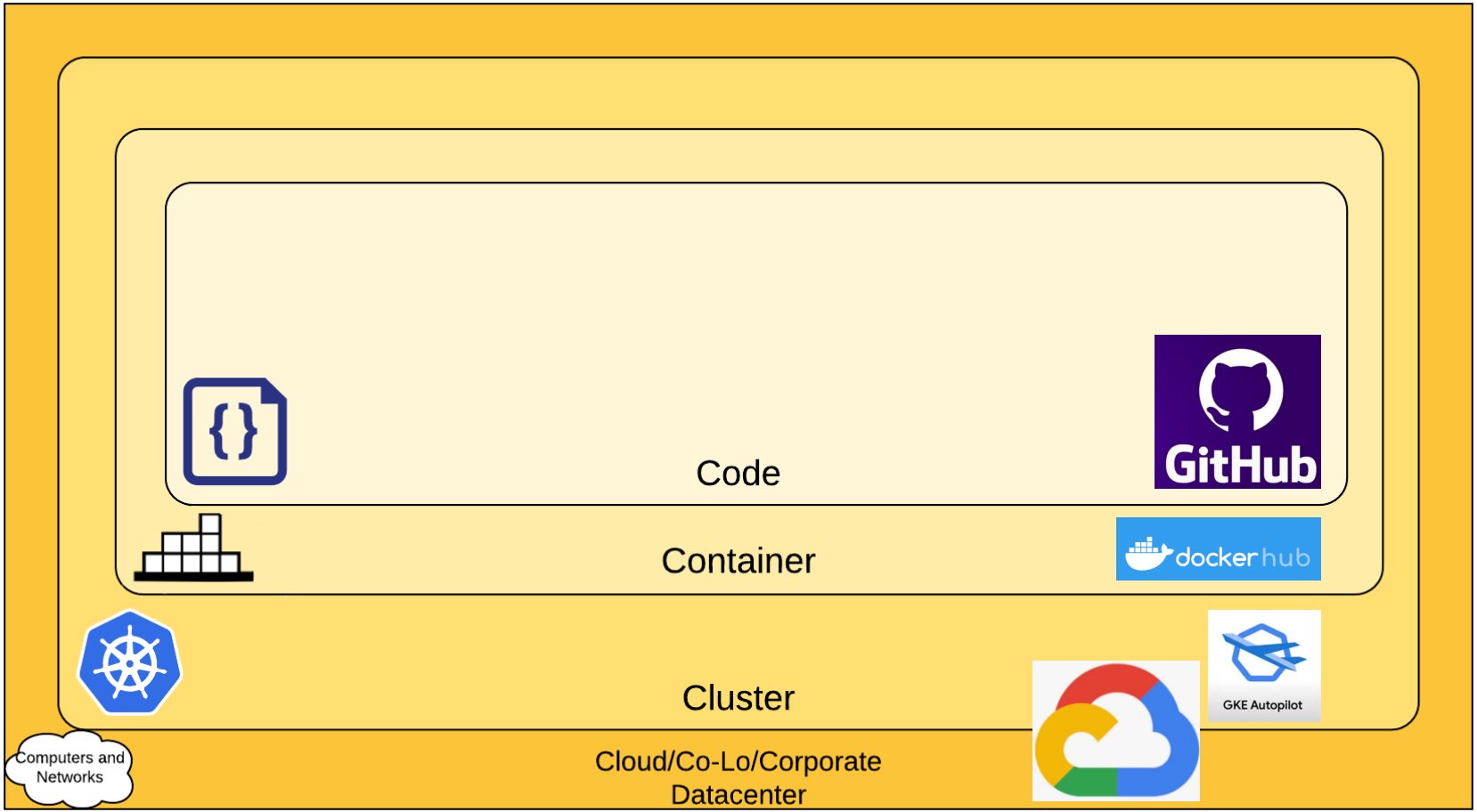

BRACE YOURSELF
LIVE DEMO IS COMING
makeameme.org



US Department of Defense


Code
Container
Cluster
Computers and Networks
Cloud/Co-Lo/Corporate Datacenter


GitHub
CODE COMMIT
GitHub Actions
PUSH
docker hub
GitHub Actions Build and Push
the image to Docker Hub
PULL
argo
ArgoCD Pulls Image for
Deployment
Google Cloud
THIS IS ALL CODE AND API CALLS


Code
GitHub
Container
docker hub
Cluster
GKE Autopilot
Computers and Networks
Cloud/Co-Lo/Corporate Datacenter

deployment.yaml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: k8demo
  labels:
    app: k8demo
spec:
  replicas: 2
  selector:
    matchLabels:
      app: k8demo
  template:
    metadata:
      labels:
        app: k8demo
    spec:
      containers:
        - name: k8demo
          image: sunnyjamwal/k8demo:main-48f379c7-1681159744
          ports:
            - containerPort: 8501
          env:
            - name: API_KEY
              value: c2333a7e3a607935c67c1e6f6810395decc9f66f59
```

Code

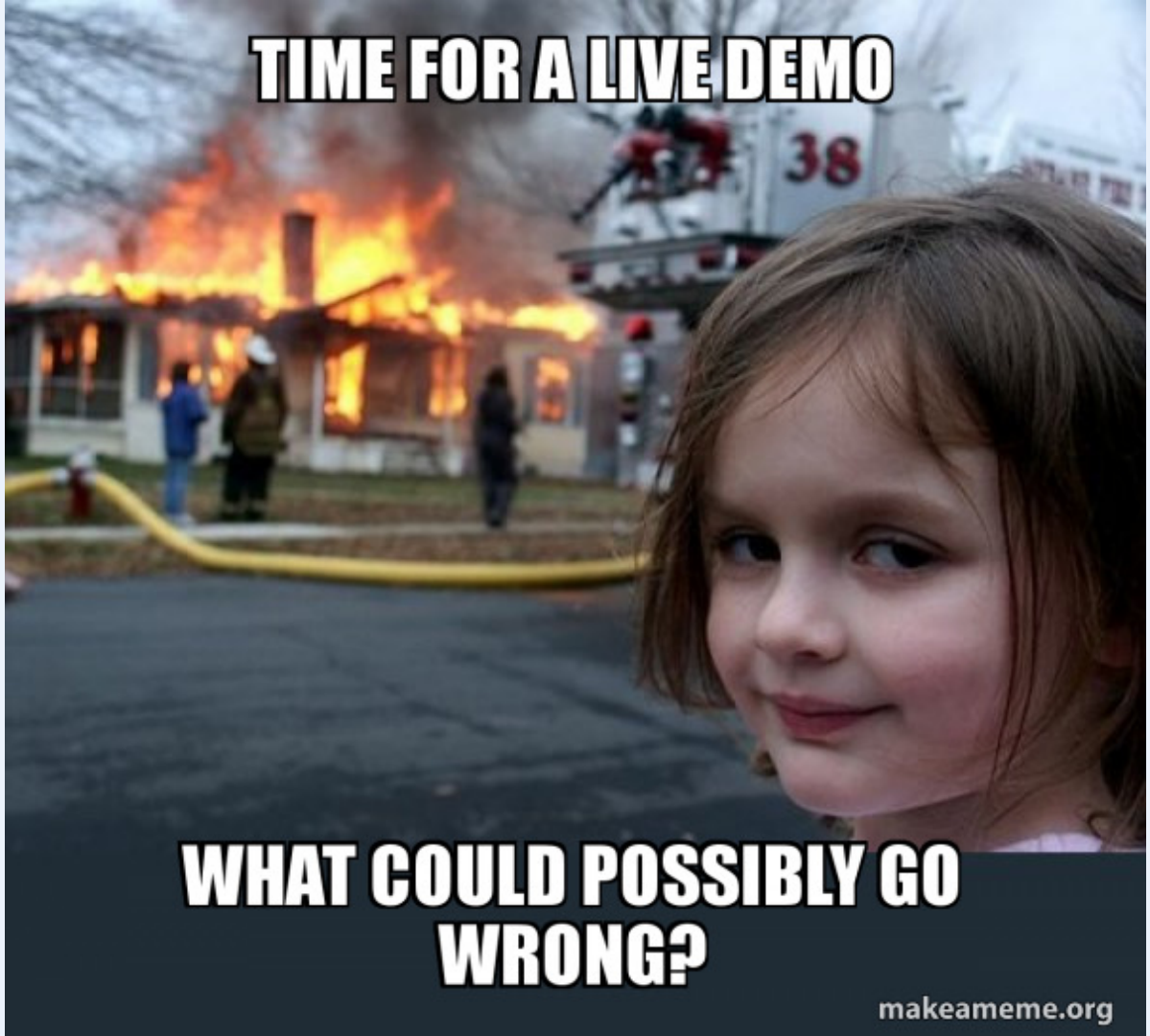
- ✓ Everything is Code
- ✓ Application Code, Infrastructure Code and Configuration Code
- ✓ Code Analysis

Dockerfile > ...

```
1   FROM python:3.9-slim
2
3   ENV MICRO_SERVICE=/home/app/webapp
4   # set work directory
5   RUN mkdir -p $MICRO_SERVICE
6   # where your code lives
7   WORKDIR $MICRO_SERVICE
8
9   # set environment variables
10  ENV PYTHONDONTWRITEBYTECODE 1
11  ENV PYTHONUNBUFFERED 1
12
13  # install dependencies
14  RUN pip install --upgrade pip
15  # copy project
16  COPY . $MICRO_SERVICE
17
18  RUN pip install -r requirements.txt
19  EXPOSE 8501
20  CMD streamlit run Welcome.py
```

Container

- ✓ Standardize container images
- ✓ Use official and current images.
- ✓ Regularly scan Images
- ✓ Don’t run as a root
- ✓ Read-only root filesystem


TIME FOR A LIVE DEMO
38
WHAT COULD POSSIBLY GO WRONG?
makeameme.org

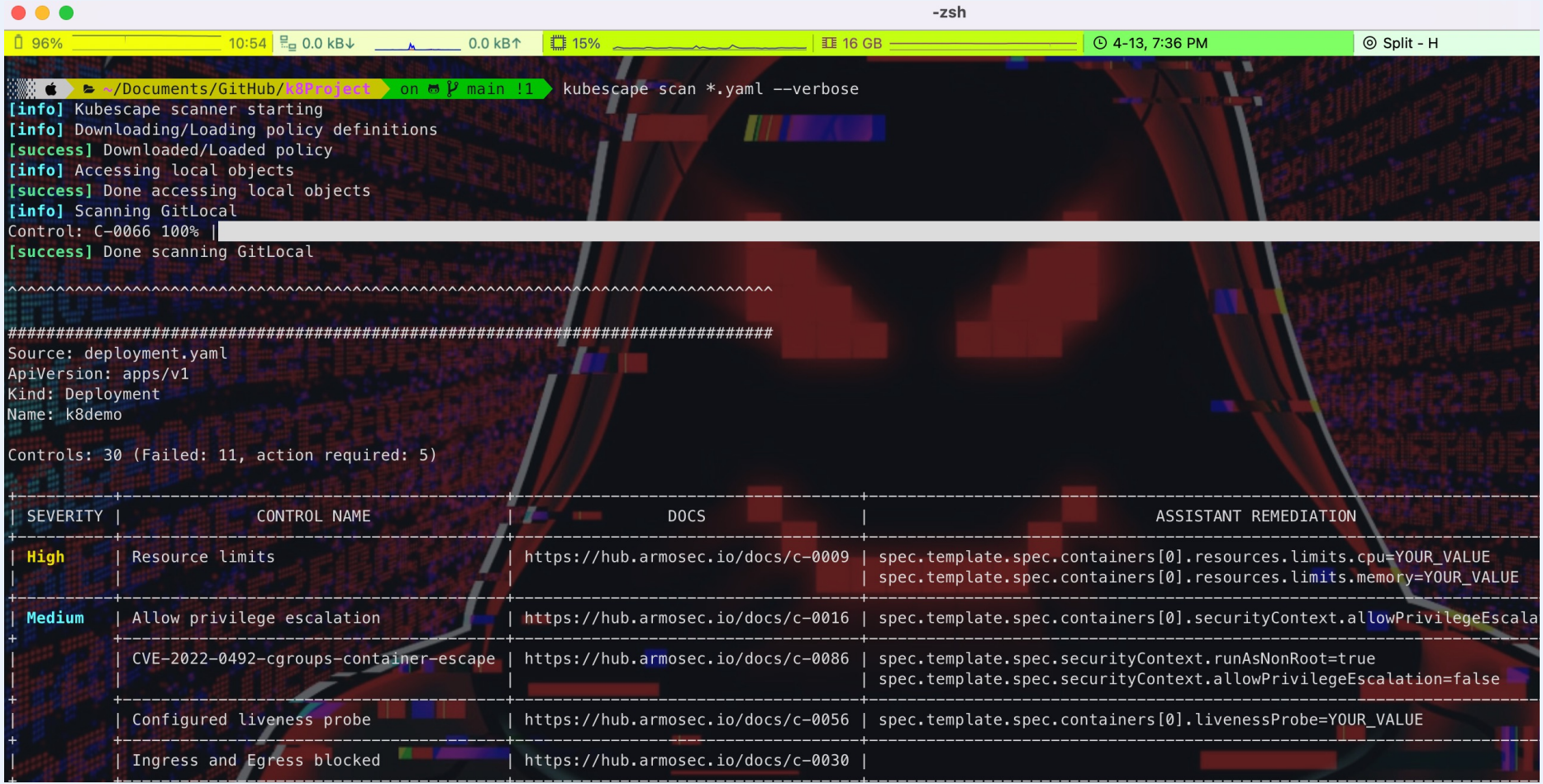
```
 ~/Documents/GitHub/k8Project on  main ↓1 !1 python3 -m flake8 --select=DUO .
./pages/insecure.py:16:10: DUO104 use of "eval" is insecure

 ~/Documents/GitHub/k8Project on  main ↓1 python3 -m flake8 --print-dlint-linters
DUO101 YieldReturnStatementLinter "inlineCallbacks" function cannot have non-empty "return" statement
DUO102 BadRandomGeneratorUseLinter insecure use of "random" module, prefer "random.SystemRandom"
DUO103 BadPickleUseLinter insecure use of "pickle" or "cPickle"
DUO104 BadEvalUseLinter use of "eval" is insecure
DUO105 BadExecUseLinter use of "exec" is insecure
DUO106 BadOSUseLinter insecure use of "os" module
DUO107 BadXMLUseLinter insecure use of XML modules, prefer "defusedxml"
DUO108 BadInputUseLinter use of "input" is insecure
DUO109 BadYAMLUseLinter insecure use of "yaml" parsing function, prefer "safe_*" equivalent
DUO110 BadCompileUseLinter use of "compile" is insecure
DUO111 BadSysUseLinter insecure use of "sys" module
DUO112 BadZipfileUseLinter use of "extract|extractall" is insecure
DUO113 InlineCallbacksYieldStatementLinter "inlineCallbacks" function missing "yield" statement
DUO114 ReturnValueInInlineCallbacksLinter "returnValue" in function missing "inlineCallbacks" decorator
DUO115 BadTarfileUseLinter use of "extract|extractall" is insecure
DUO116 BadSubprocessUseLinter use of "shell=True" is insecure in "subprocess" module
DUO117 BadDlUseLinter avoid "dl" module use
DUO118 BadGlUseLinter avoid "gl" module use
DUO119 BadShelveUseLinter avoid "shelve" module use
DUO120 BadMarshalUseLinter avoid "marshal" module use
DUO121 BadTempfileUseLinter use of "tempfile.mktemp" allows for race conditions
DUO122 BadSSLModuleAttributeUseLinter insecure "ssl" module attribute use
DUO123 BadRequestsUseLinter use of "verify=False" is insecure in "requests" module
DUO124 BadXmlrpcUseLinter instance with "allow_dotted_names" enabled is insecure
DUO125 BadCommandsUseLinter avoid "commands" module use
DUO126 BadPopen2UseLinter avoid "popen2" module use
DUO127 BadDuoClientUseLinter use of "ca_certs=HTTP|DISABLE" is insecure in "duo_client" module
DUO128 BadOneLoginKwargUseLinter insecure "OneLogin" SAML function call
DUO129 BadOneLoginModuleAttributeUseLinter insecure "OneLogin" SAML attribute use
DUO130 BadHashlibUseLinter insecure use of "hashlib" module
DUO131 BadUrllib3ModuleAttributeUseLinter "urllib3" warnings disabled, insecure connections possible
DUO132 BadUrllib3KwargUseLinter "urllib3" certificate verification disabled, insecure connections possible
DUO133 BadPycryptoUseLinter use of "Crypto" module is insecure
DUO134 BadCryptographyModuleAttributeUseLinter insecure "cryptography" attribute use
DUO135 BadDefusedxmlUseLinter enable all "forbid_*" defenses when using "defusedxml" parsing
DUO136 BadXmlsecModuleAttributeUseLinter insecure "xmlsec" attribute use
DUO137 BadItsDangerousKwargUseLinter insecure "itsdangerous" use allowing empty signing
DUO138 BadReCatastrophicUseLinter catastrophic "re" usage - denial-of-service possible

 ~/Documents/GitHub/k8Project on  main ↓1
```

```
 ~/Documents/GitHub/k8Project on  main trivy fs --scanners vuln,secret,config ./
2023-04-17T18:06:39.667-0300    INFO    Vulnerability scanning is enabled
2023-04-17T18:06:39.667-0300    INFO    Misconfiguration scanning is enabled
2023-04-17T18:06:39.667-0300    INFO    Secret scanning is enabled
2023-04-17T18:06:39.667-0300    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2023-04-17T18:06:39.667-0300    INFO    Please see also https://aquasecurity.github.io/trivy/v0.39/docs/secret/scanning/#recommendation for fast
2023-04-17T18:06:40.623-0300    INFO    Number of language-specific files: 1
2023-04-17T18:06:40.623-0300    INFO    Detecting pip vulnerabilities...
2023-04-17T18:06:40.624-0300    INFO    Detected config files: 4

requirements.txt (pip)

Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
gitpython	CVE-2022-24439	HIGH	3.0	3.1.30	GitPython: improper user input validation leads into a RCE https://avd.aquasec.com/nvd/cve-2022-24439

```
Dockerfile (dockerfile)

Tests: 25 (SUCCESSES: 23, FAILURES: 2, EXCEPTIONS: 0)
Failures: 2 (UNKNOWN: 0, LOW: 1, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

HIGH: Specify at least 1 USER command in Dockerfile with non-root user as argument
═══════════════════════════════════════════════════════════════════════════════
Running containers with 'root' user can lead to a container escape situation. It is a best practice to run containers as non-root users, which c
the Dockerfile.

See https://avd.aquasec.com/misconfig/ds002
───────────────────────────────────────────────────────────────────────────────


LOW: Add HEALTHCHECK instruction in your Dockerfile
═══════════════════════════════════════════════════════════════════════════════
You should add HEALTHCHECK instruction in your docker container images to perform the health check on running containers.

See https://avd.aquasec.com/misconfig/ds026
───────────────────────────────────────────────────────────────────────────────
```

DASH HUDSON


-zsh
96% 10:54 0.0 kB↓ 0.0 kB↑ 15% 16 GB 4-13, 7:36 PM Split - H
~/Documents/GitHub/k8Project on main !1 kubescape scan *.yaml --verbose
[info] Kubescape scanner starting
[info] Downloading/Loading policy definitions
[success] Downloaded/Loaded policy
[info] Accessing local objects
[success] Done accessing local objects
[info] Scanning GitLocal
Control: C-0066 100%
[success] Done scanning GitLocal
Source: deployment.yaml
ApiVersion: apps/v1
Kind: Deployment
Name: k8demo
Controls: 30 (Failed: 11, action required: 5)
SEVERITY | CONTROL NAME | DOCS | ASSISTANT REMEDIATION
High | Resource limits | https://hub.armosec.io/docs/c-0009 | spec.template.spec.containers[0].resources.limits.cpu=YOUR_VALUE
spec.template.spec.containers[0].resources.limits.memory=YOUR_VALUE
Medium | Allow privilege escalation | https://hub.armosec.io/docs/c-0016 | spec.template.spec.containers[0].securityContext.allowPrivilegeEscala
| CVE-2022-0492-cgroups-container-escape | https://hub.armosec.io/docs/c-0086 | spec.template.spec.securityContext.runAsNonRoot=true
spec.template.spec.securityContext.allowPrivilegeEscalation=false
| Configured liveness probe | https://hub.armosec.io/docs/c-0056 | spec.template.spec.containers[0].livenessProbe=YOUR_VALUE
| Ingress and Egress blocked | https://hub.armosec.io/docs/c-0030 |

DASH HUDSON

```
 ~/Documents/GitHub/k8Project on  main  trivy image myimage
2023-04-17T18:08:28.071-0300    INFO    Vulnerability scanning is enabled
2023-04-17T18:08:28.071-0300    INFO    Secret scanning is enabled
2023-04-17T18:08:28.071-0300    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2023-04-17T18:08:28.071-0300    INFO    Please see also https://aquasecurity.github.io/trivy/v0.39/docs/secret/scanning/#recommendation for faster secret detectio
2023-04-17T18:08:28.104-0300    INFO    Detected OS: debian
2023-04-17T18:08:28.104-0300    INFO    Detecting Debian vulnerabilities...
2023-04-17T18:08:28.114-0300    INFO    Number of language-specific files: 1
2023-04-17T18:08:28.114-0300    INFO    Detecting python-pkg vulnerabilities...

myimage (debian 11.6)

Total: 92 (UNKNOWN: 4, LOW: 62, MEDIUM: 10, HIGH: 15, CRITICAL: 1)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
apt	CVE-2011-3374	LOW	2.2.4		It was found that apt-key in apt, all versions, do not correctly... https://avd.aquasec.com/nvd/cve-2011-3374
bash	CVE-2022-3715	HIGH	5.1-2+deb11u1		bash: a heap-buffer-overflow in valid_parameter_transform https://avd.aquasec.com/nvd/cve-2022-3715
bsdutils	CVE-2022-0563	LOW	1:2.36.1-8+deb11u1		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
coreutils	CVE-2016-2781		8.32-4		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
	CVE-2017-18018				coreutils: race condition vulnerability in chown and chgrp https://avd.aquasec.com/nvd/cve-2017-18018
e2fsprogs	CVE-2022-1304	HIGH	1.46.2-2		e2fsprogs: out-of-bounds read/write via crafted filesystem https://avd.aquasec.com/nvd/cve-2022-1304
gpgv	CVE-2022-3219	LOW	2.2.27-2+deb11u2		gnupg: denial of service issue (resource consumption) using compressed packets https://avd.aquasec.com/nvd/cve-2022-3219
libapt-pkg6.0	CVE-2011-3374		2.2.4		It was found that apt-key in apt, all versions, do not correctly... https://avd.aquasec.com/nvd/cve-2011-3374
libblkid1	CVE-2022-0563		2.36.1-8+deb11u1		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563

PROBLEMS 15 OUTPUT DEBUG CONSOLE TERMINAL

```
 => => writing image sha256:3ac7fda38759edde5ec5aa02abbd99b572585c482523ce28add980eddb0ecb01
 => => naming to docker.io/library/myimage

 ~/Doc/GitHub/k8Project on  main ↓1 !2 docker scout cves myimage
Analyzing image myimage
    ✓ Image stored for indexing
    ✓ Indexed 203 packages
    ✗ Detected 18 vulnerable packages with a total of 27 vulnerabilities

  1C    0H    0M    0L  gitpython 3.0.0
pkg:pypi/gitpython@3.0.0

    ✗ CRITICAL CVE-2022-24439 [Improper Input Validation]
      https://dso.docker.com/cve/CVE-2022-24439
      Affected range : <=3.1.29
      Fixed version  : 3.1.30
      CVSS Score     : 9.8
      CVSS Vector    : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H


  0C    0H    1M    0L  setuptools 58.1.0
pkg:pypi/setuptools@58.1.0

    ✗ MEDIUM CVE-2022-40897
      https://dso.docker.com/cve/CVE-2022-40897
      Affected range : <65.5.1
      Fixed version  : 65.5.1
      CVSS Score     : 5.9
      CVSS Vector    : CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H


  0C    0H    0M    4L  pcre3 2:8.39-13
pkg:deb/debian/pcre3@2:8.39-13?os_distro=bullseye&os_name=debian&os_version=11
```

```
 ~/Doc/GitHub/k8Project on  main ↓1 docker sbom myimage 2> /dev/null
NAME                    VERSION                     TYPE
GitPython               3.0.0                       python
Jinja2                  3.1.2                       python
MarkupSafe              2.1.2                       python
Pillow                  9.5.0                       python
Pygments                2.15.0                      python
Pympler                 1.0.1                       python
adduser                 3.118                       deb
altair                  4.2.2                       python
apt                     2.2.4                       deb
attrs                   23.1.0                      python
base-files              11.1+deb11u6                deb
base-passwd             3.5.51                      deb
bash                    5.1-2+deb11u1               deb
blinker                 1.6.2                       python
bsdutils                1:2.36.1-8+deb11u1          deb
ca-certificates         20210119                    deb
cachetools              5.3.0                       python
certifi                 2022.12.7                   python
charset-normalizer      3.1.0                       python
click                   8.1.3                       python
coreutils               8.32-4                      deb
dash                    0.5.11+git20200708+dd9ef66-5 deb
ddt                     1.6.0                       python
debconf                 1.5.77                      deb
debian-archive-keyring  2021.1.1                    deb
debianutils             4.11.2                      deb
decorator               5.1.1                       python
diffutils               1:3.7-5                     deb
dpkg                    1.20.12                     deb
e2fsprogs               1.46.2-2                    deb
entrypoints             0.4                         python
findutils               4.8.0-1                     deb
gcc-10-base             10.2.1-6                    deb
gcc-9-base              9.3.0-22                    deb
gitdb                   4.0.10                      python
gitdb2                  4.0.2                       python
gpgv                    2.2.27-2+deb11u2            deb
grep                    3.6-1                       deb
gzip                    1.10-4+deb11u1              deb
hostname                3.23                        deb
idna                    3.4                         python
importlib-metadata      6.4.1                       python
init-system-helpers     1.60                        deb
jsonschema              4.17.3                      python
libacl1                 2.2.53-10                   deb
libapt-pkg6.0           2.2.4                       deb
```

DASH HUDSON

k8Project main

Code Analysis

Overview History Settings

Created Tue 13th Dec 2022 | Snapshot taken by snyk.io 2 hours ago | Retest now

IMPORTED BY
Sonny

PROJECT OWNER
Add a project owner

ANALYSIS SUMMARY
2 analyzed files (13%) Repo breakdown

Issues 1

Search...

SEVERITY
- High 1
- Medium 0
- Low 0

PRIORITY SCORE
Scored between 0 - 1000

STATUS
- Open 1
- Ignored 0

1 of 1 issues

Group by none Sort by highest severity

H Code Injection

SNYK CODE | CWE-94

SCORE
850

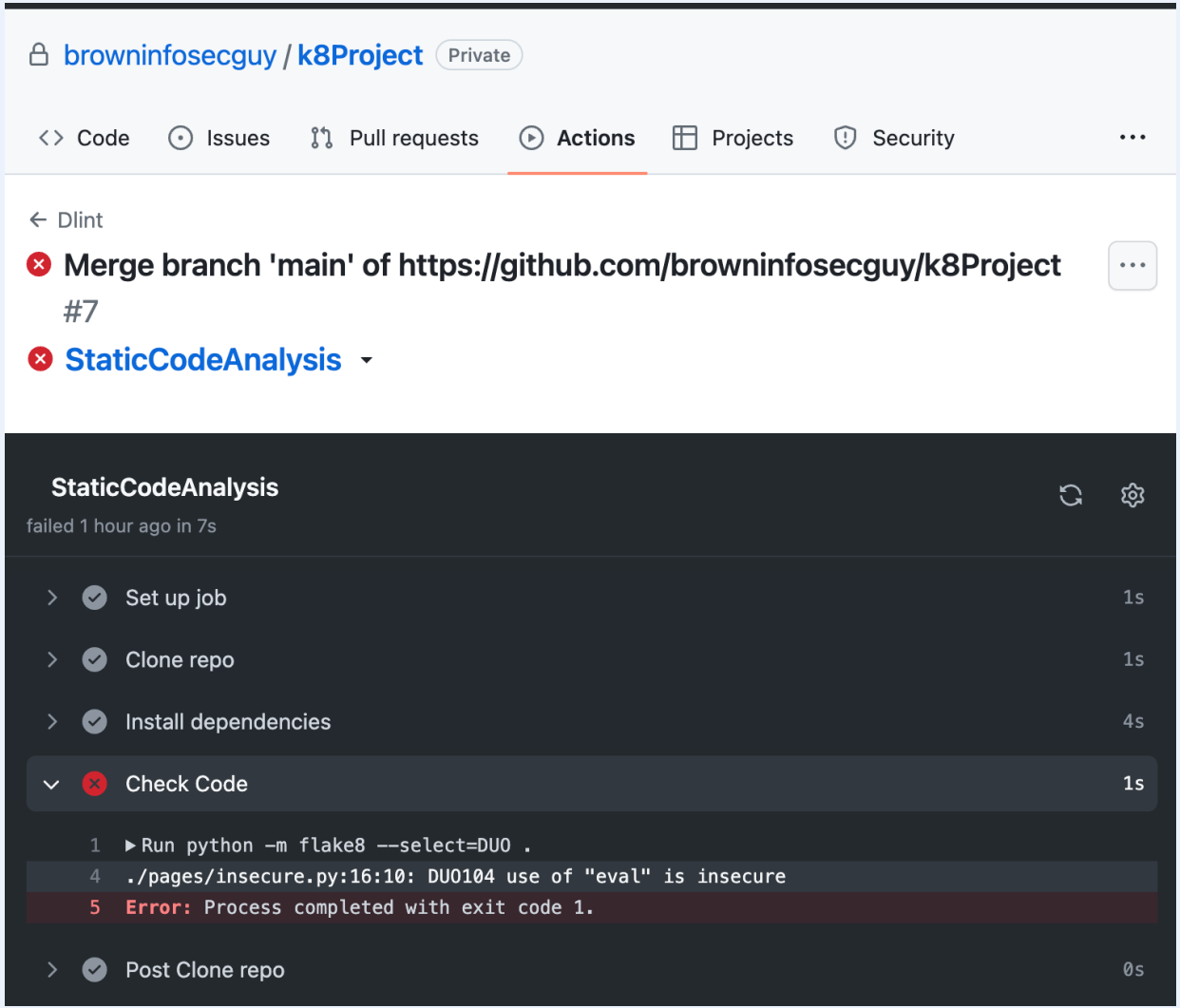
```
3 compute = input('\nYour expression? => ')
4 if not compute:
5  print ("No input")
6 else:
7  print ("Result =", eval(compute))
```

Unsanitized input from *a user input flows* into *eval*, where it is executed as Python code. This may result in a Code Injection vulnerability.

insecure.py

6 steps in 1 file

DASH HUDSON


browninfosecguy / k8Project
Private
Code
Issues
Pull requests
Actions
Projects
Security
Dlint
Merge branch 'main' of https://github.com/browninfosecguy/k8Project
#7
StaticCodeAnalysis
StaticCodeAnalysis
failed 1 hour ago in 7s
Set up job 1s
Clone repo 1s
Install dependencies 4s
Check Code 1s
1 ▶Run python -m flake8 --select=DUO .
4 ./pages/insecure.py:16:10: DUO104 use of "eval" is insecure
5 Error: Process completed with exit code 1.
Post Clone repo 0s

Remote Code Execution (RCE)

Affecting gitpython package, versions **[0,3.1.30)**

INTRODUCED: 13 NOV 2022 CVE-2022-24439 CWE-94 FIRST ADDED BY SNYK

Share

How to fix?

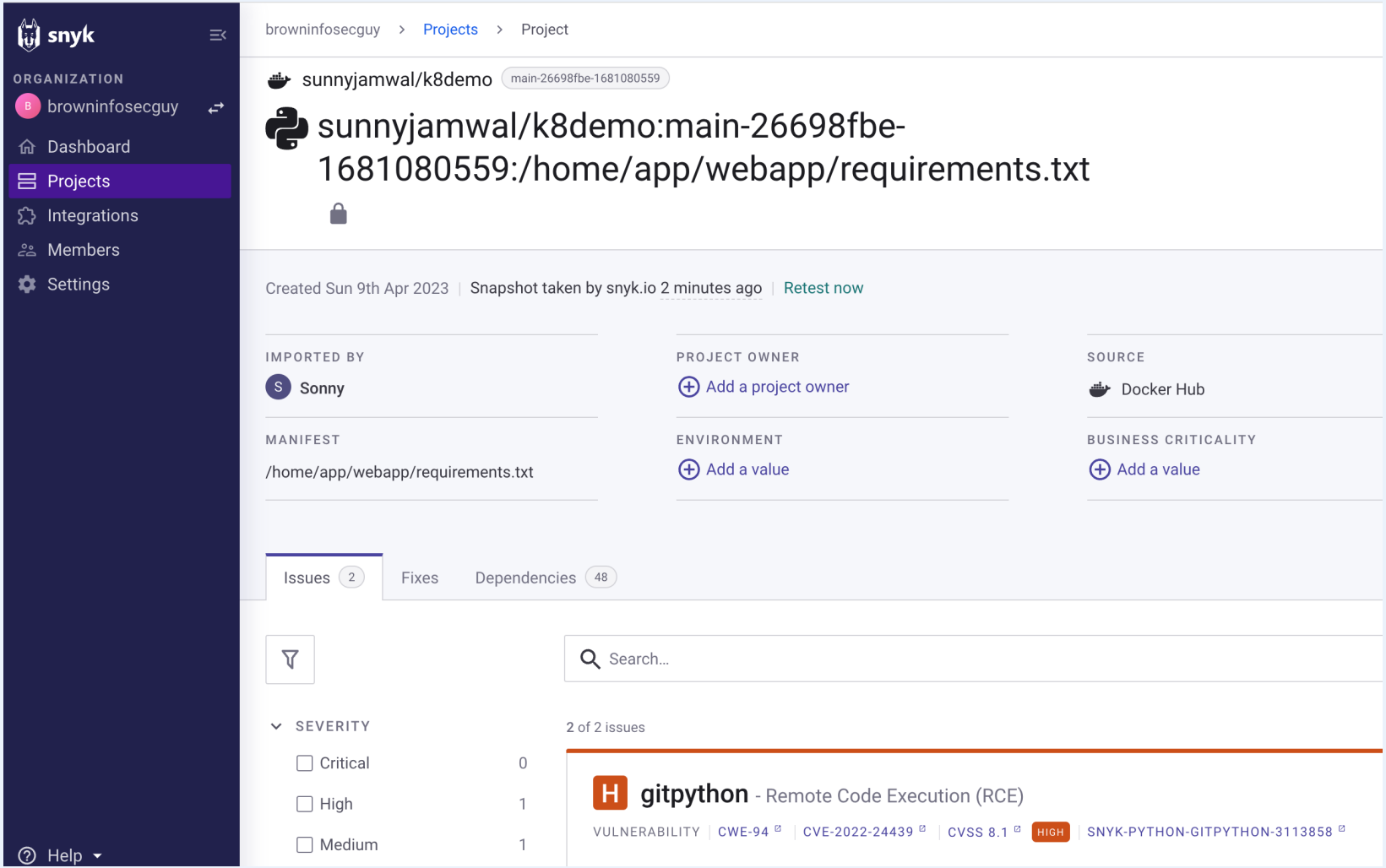
Upgrade `GitPython` to version 3.1.30 or higher.

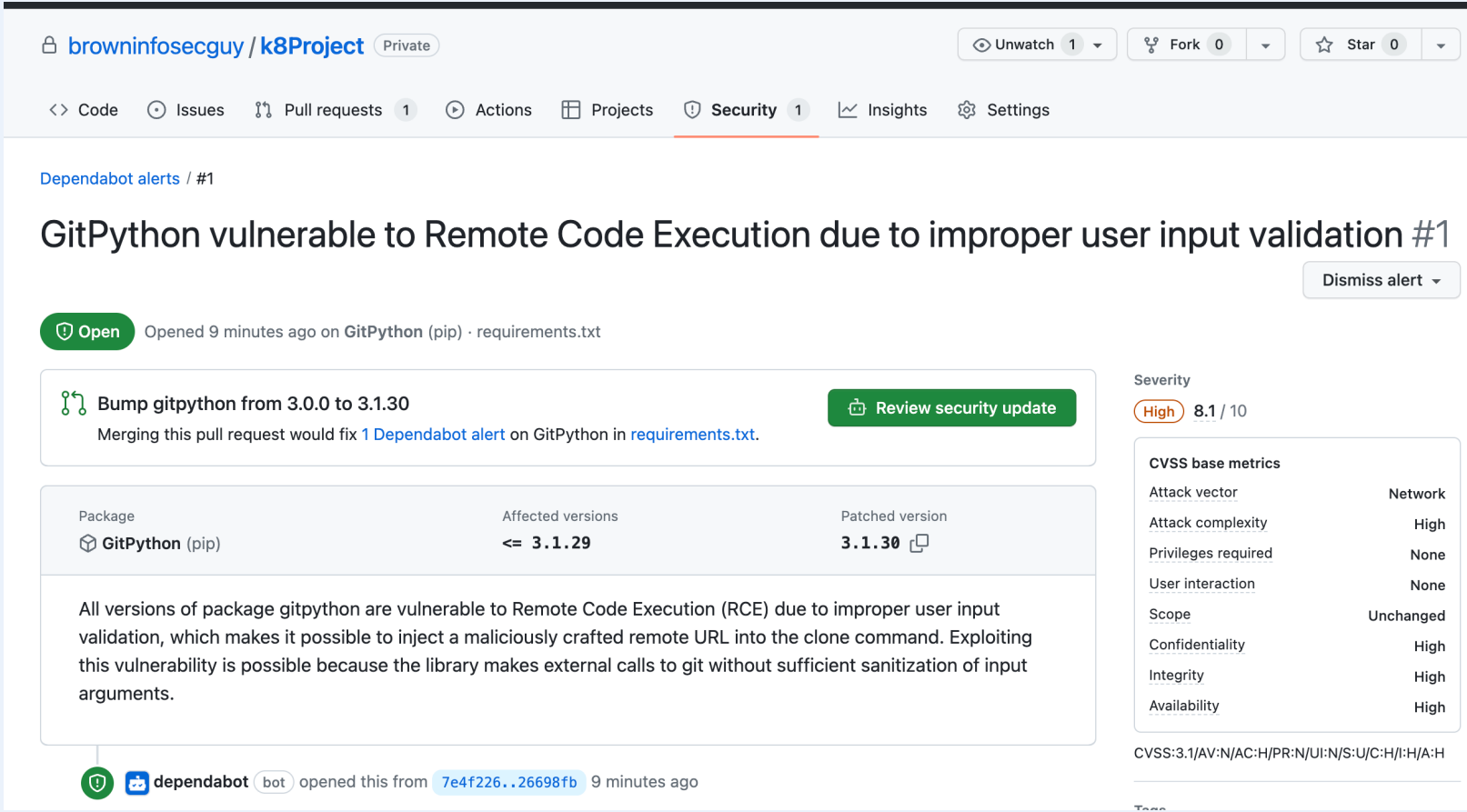
Overview

GitPython is a python library used to interact with Git repositories Affected versions of this package are vulnerable to Remote Code Execution (RCE) due to improper user input validation, which makes it possible to inject a maliciously crafted remote URL into the clone command. Exploiting this vulnerability is possible because the library makes external calls to `git` without sufficient sanitization of input arguments. This is only relevant when enabling the `ext` transport protocol.

PoC

```
from git import Repo r = Repo.init('', bare=True) r.clone_from('ext::sh -c touch%
/tmp/pwned', 'tmp', multi_options=["-c protocol.ext.allow=always"])
```


snyk
ORGANIZATION
browninfosecguy
Dashboard
Projects
Integrations
Members
Settings
Help
browninfosecguy > Projects > Project
sunnyjamwal/k8demo
main-26698fbe-1681080559
sunnyjamwal/k8demo:main-26698fbe-1681080559:/home/app/webapp/requirements.txt
Created Sun 9th Apr 2023 | Snapshot taken by snyk.io 2 minutes ago | Retest now
IMPORTED BY
Sonny
PROJECT OWNER
Add a project owner
SOURCE
Docker Hub
MANIFEST
/home/app/webapp/requirements.txt
ENVIRONMENT
Add a value
BUSINESS CRITICALITY
Add a value
Issues 2
Fixes
Dependencies 48
Search...
SEVERITY
Critical 0
High 1
Medium 1
2 of 2 issues
gitpython - Remote Code Execution (RCE)
VULNERABILITY | CWE-94 | CVE-2022-24439 | CVSS 8.1 | HIGH | SNYK-PYTHON-GITPYTHON-3113858


browninfosecguy / k8Project
Private
Unwatch 1
Fork 0
Star 0
Code
Issues
Pull requests 1
Actions
Projects
Security 1
Insights
Settings
Dependabot alerts / #1
GitPython vulnerable to Remote Code Execution due to improper user input validation #1
Dismiss alert
Open
Opened 9 minutes ago on GitPython (pip) · requirements.txt
Bump gitpython from 3.0.0 to 3.1.30
Merging this pull request would fix 1 Dependabot alert on GitPython in requirements.txt.
Review security update
Package
GitPython (pip)
Affected versions
<= 3.1.29
Patched version
3.1.30
All versions of package gitpython are vulnerable to Remote Code Execution (RCE) due to improper user input validation, which makes it possible to inject a maliciously crafted remote URL into the clone command. Exploiting this vulnerability is possible because the library makes external calls to git without sufficient sanitization of input arguments.
dependabot bot opened this from 7e4f226..26698fb 9 minutes ago
Severity
High 8.1 / 10
CVSS base metrics
Attack vector Network
Attack complexity High
Privileges required None
User interaction None
Scope Unchanged
Confidentiality High
Integrity High
Availability High
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

browninfosecguy / k8Project Private

Unwatch 1 | Fork 0 | Star 0

Code | Issues | Pull requests | Actions | Projects | Security | Insights | Settings

Dependabot alerts / #1

GitPython vulnerable to Remote Code Execution due to improper user input validation #1

Fixed Opened 1 hour ago on **GitPython** (pip) · requirements.txt · Fixed 2 minutes ago

Package	Affected versions	Patched version
GitPython (pip)	**<= 3.1.29**	**3.1.30**

All versions of package gitpython are vulnerable to Remote Code Execution (RCE) due to improper user input validation, which makes it possible to inject a maliciously crafted remote URL into the clone command. Exploiting this vulnerability is possible because the library makes external calls to git without sufficient sanitization of input arguments.

dependabot bot opened this from `7e4f226..26698fb` 1 hour ago

dependabot bot closed this as completed in `6888558..303bfd9` 2 minutes ago

Severity

High 8.1 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Tags

Direct dependency | Patch available

MyApp

Scan ID: d2d761dd-b601-47a8-866d-588730035d9c

Development | http://127.0.0.1:8501

Completed On	Duration	HawkScan Version
Apr 09, 2023 at 21:33 ADT	1 min 16 secs	3.0.0

0	15	23	0	0
High	Medium	Low	Assigned	Risk Ac

Plugin Summary | Findings (6) | Paths (42)

Finding	Criticality	New
Relative Path Confusion	MED	10
Application Error Disclosure	MED	1
Missing Anti-clickjacking Header	MED	1
Content Security Policy (CSP) Header Not Set	MED	3
X-Content-Type-Options Header Missing	LOW	11
Server Leaks Version Information via "Server" HTTP Response Header Field	LOW	12

DASH HUDSON

browninfosecguy/k8Project main

browninfosecguy/k8Project:Dockerfile

Overview | History | Settings

Created Tue 13th Dec 2022 | Snapshot taken by snyk.io 2 hours ago | Retest now

IMPORTED BY	PROJECT OWNER	SOURCE	TARGET OS
Sonny	Add a project owner	GitHub	debian:11
IMAGE TAG	**BASE IMAGE**	**REPOSITORY**	**MANIFEST**
3.8	python:3.8	k8Project	Dockerfile
ENVIRONMENT	**BUSINESS CRITICALITY**	**LIFECYCLE**	**LINKED IMAGES**
Add a value	Add a value	Add a value	Add a value

Recommendations for upgrading the base image

	BASE IMAGE	VULNERABILITIES	SEVERITY	
Current image	python:3.8	230	4 C 4 H 1 M 221 L	
Alternative upgrades	python:3.12.0a5-slim	50	0 C 0 H 0 M 50 L	Open a fix PR

Show more upgrade types

browninfosecguy/k8Project main

browninfosecguy/k8Project:Dockerfile

Overview History Settings

Created Tue 13th Dec 2022 | Snapshot taken by snyk.io 3 minutes ago | Retest now

IMPORTED BY	PROJECT OWNER	SOURCE	TARGET OS
Sonny	Add a project owner	GitHub	debian:11
IMAGE TAG	**BASE IMAGE**	**REPOSITORY**	**MANIFEST**
3.9-slim	python:3.9-slim	k8Project	Dockerfile
ENVIRONMENT	**BUSINESS CRITICALITY**	**LIFECYCLE**	**LINKED IMAGES**
Add a value	Add a value	Add a value	Add a value

The base image python:3.9-slim is up to date

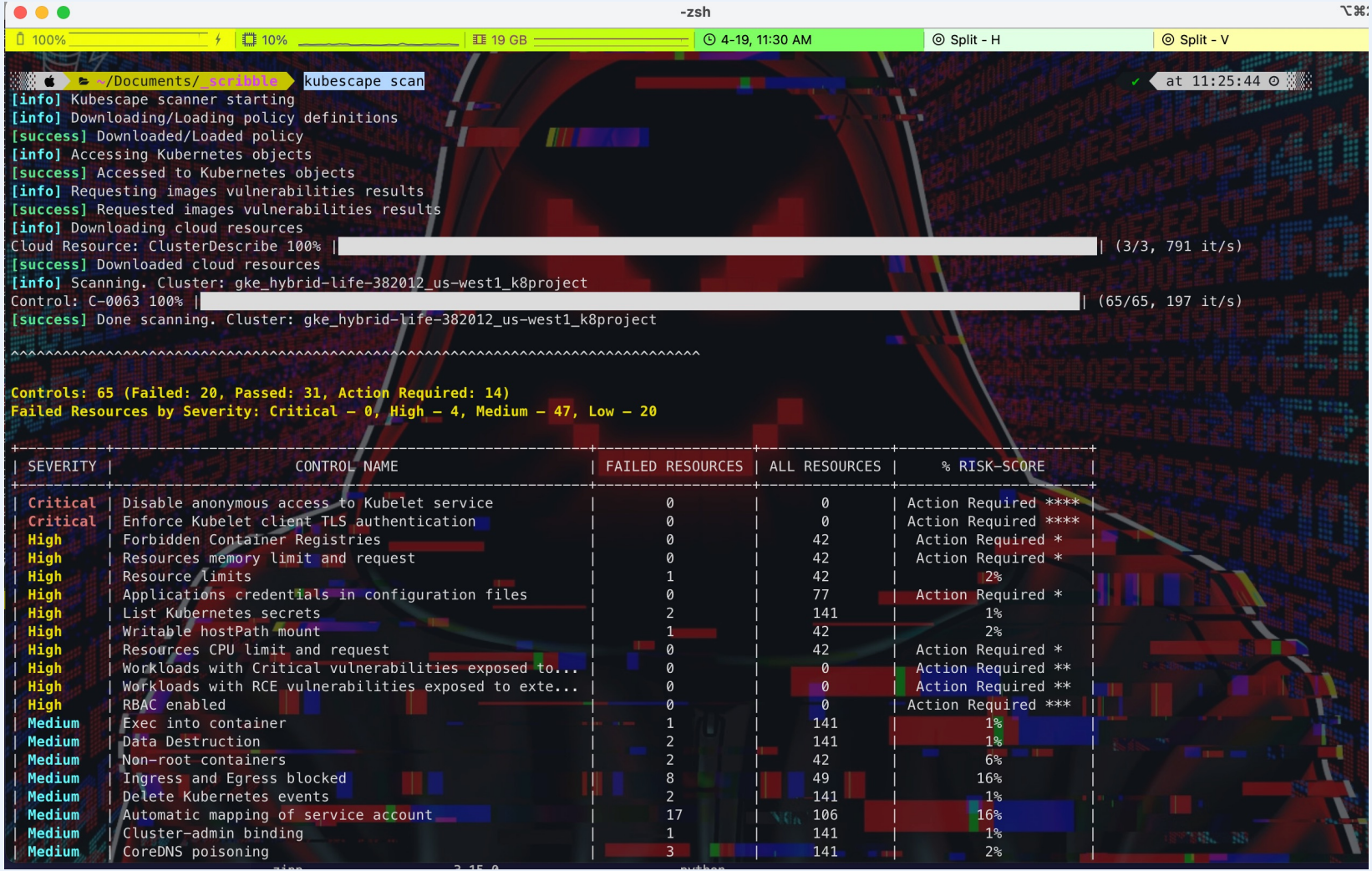
View docs

2 concerns

View by: (•) Concern ? ( ) Namespace ( ) Workload

Filter Enter property name or value ?

Severity ↑	Type	Concern	Workloads affected	Clusters affected
!!	Configuration	Pod container allows privilege escalation on exec	1	1
!!	Configuration	Pod container is allowed to run as root	1	1


-zsh
100%
10%
19 GB
4-19, 11:30 AM
Split - H
Split - V
~/Documents/_scribble
kubescape scan
at 11:25:44
[info] Kubescape scanner starting
[info] Downloading/Loading policy definitions
[success] Downloaded/Loaded policy
[info] Accessing Kubernetes objects
[success] Accessed to Kubernetes objects
[info] Requesting images vulnerabilities results
[success] Requested images vulnerabilities results
[info] Downloading cloud resources
Cloud Resource: ClusterDescribe 100% | (3/3, 791 it/s)
[success] Downloaded cloud resources
[info] Scanning. Cluster: gke_hybrid-life-382012_us-west1_k8project
Control: C-0063 100% | (65/65, 197 it/s)
[success] Done scanning. Cluster: gke_hybrid-life-382012_us-west1_k8project
Controls: 65 (Failed: 20, Passed: 31, Action Required: 14)
Failed Resources by Severity: Critical — 0, High — 4, Medium — 47, Low — 20
SEVERITY	CONTROL NAME	FAILED RESOURCES	ALL RESOURCES	% RISK-SCORE
Critical	Disable anonymous access to Kubelet service	0	0	Action Required ****
Critical	Enforce Kubelet client TLS authentication	0	0	Action Required ****
High	Forbidden Container Registries	0	42	Action Required *
High	Resources memory limit and request	0	42	Action Required *
High	Resource limits	1	42	2%
High	Applications credentials in configuration files	0	77	Action Required *
High	List Kubernetes secrets	2	141	1%
High	Writable hostPath mount	1	42	2%
High	Resources CPU limit and request	0	42	Action Required *
High	Workloads with Critical vulnerabilities exposed to...	0	0	Action Required **
High	Workloads with RCE vulnerabilities exposed to exte...	0	0	Action Required **
High	RBAC enabled	0	0	Action Required ***
Medium	Exec into container	1	141	1%
Medium	Data Destruction	2	141	1%
Medium	Non-root containers	2	42	6%
Medium	Ingress and Egress blocked	8	49	16%
Medium	Delete Kubernetes events	2	141	1%
Medium	Automatic mapping of service account	17	106	16%
Medium	Cluster-admin binding	1	141	1%
Medium	CoreDNS poisoning	3	141	2%

DASH HUDSON

GKE Security Posture PREVIEW REFRESH

DASHBOARD CONCERNS

Concerns

0 Critical
0 High
2 Medium
0 Low

See all concerns →

Types

2 Configuration
0 Vulnerability

Clusters

1 Affected
0 Unaffected

Workloads

1 Affected
7 Unaffected

Benefits of DevSecOps

Speed

Developers can remediate vulnerabilities while they're coding, which teaches secure code writing and reduces back and forth during security reviews.

Collaboration

Encouraging a security mindset across your app dev team aligns goals with security and encourages employees to work with others outside their functional silo.

Efficiency

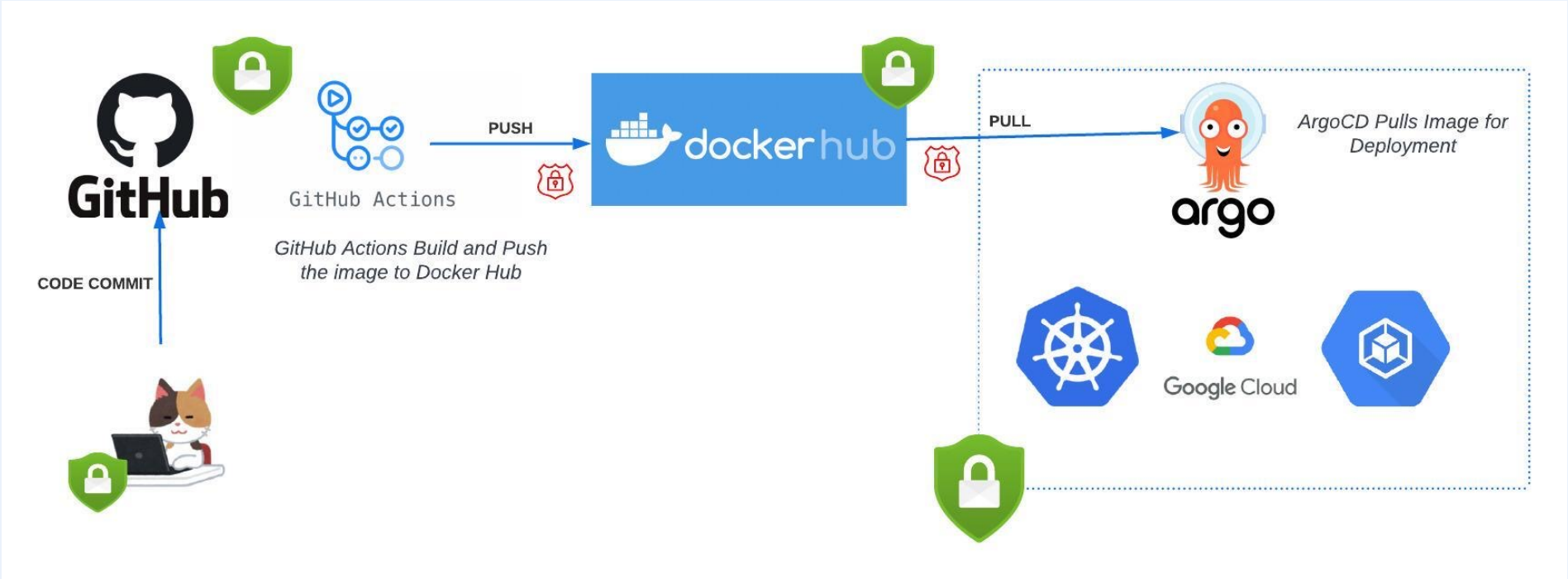
DevSecOps saves time, money, and employee resources over every launch and iteration - all valuable assets to IT and security teams suffering from skills and budget shortages.

Recommendations:

- Automate Security.
- Implement API Governance Program.
- Standardize Container Images.
- Implement secure code scan at PR (pull request) level.
- Software Bill of Material (SBOM).
- Peer Code review.
- Make CI/CD Pipeline less Complex.

Thanks!!!

Questions?


GitHub
CODE COMMIT
GitHub Actions
PUSH
docker hub
GitHub Actions Build and Push
the image to Docker Hub
PULL
argo
ArgoCD Pulls Image for
Deployment
Google Cloud

ORGANIZATION	PROCESS	TECHNOLOGY	GOVERNANCE
❖Culture shift & buy-in ❖Communication & collaboration ❖Security/QA throughout ❖Learn from success/ failure ❖Feedback and user-driven change	❖Collaborative design ❖Test-driven development ❖Common and automatable tasks ❖Continuous adaptation and improvement ❖Continuous ATO	❖Tool adoption ❖Automation and orchestration ❖Cloud and containerization ❖Infrastructure as Code ❖Security as Code	❖Built-in governance control ❖Uniform policy enforcement ❖Data-driven validation ❖Enhanced visibility ❖Inherited certifications and authorizations

DASH HUDSON

Initial access	Execution	Persistence	Privilege escalation	Credential access	Lateral movement	Defense evasion	Impact	Exfiltration
SCM authentication	Poisoned pipeline execution (3)	Change code/pipeline configuration in repository (3)	Secrets stored in private repositories	User credentials	Compromise build artifacts	Service logs manipulation	DDoS using pipeline compute resources	Clone for private repositories
CI/CD service authentication	Dependencies tampering (3)	Inject in artifacts	Commit from pipeline to protected branches	Service credentials	Registry injection	Compilation manipulation (2)	Crypto mining over pipeline compute resources	Access to pipelines logs
Configured webhooks	DevOps resources compromise	Modify images in registry	Certificates and identities from metadata services		Spread from pipeline into deployment resources	Reconfigure branch protections	Local DoS to CI/CD pipelines	Exfiltrate data from production resources
Organization's public repositories	Control of common registry	Create service credentials					Resource deletion	
Endpoint compromise								

Source: https://www.microsoft.com/en-us/security/blog/2023/04/06/devops-threat-matrix/