Security In An IaC Defined World

@mcdwayne
@mcdwayne

What Does Bad Security Look Like?


El sueño
de la razon
produce
monstruos


4 0339
WM


3:00 AM
WM

What Does Good Security Look Like?

Hi. I’m Dwayne.

Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of The Security Repo Podcast
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

@mcdwayne

About GitGuardian

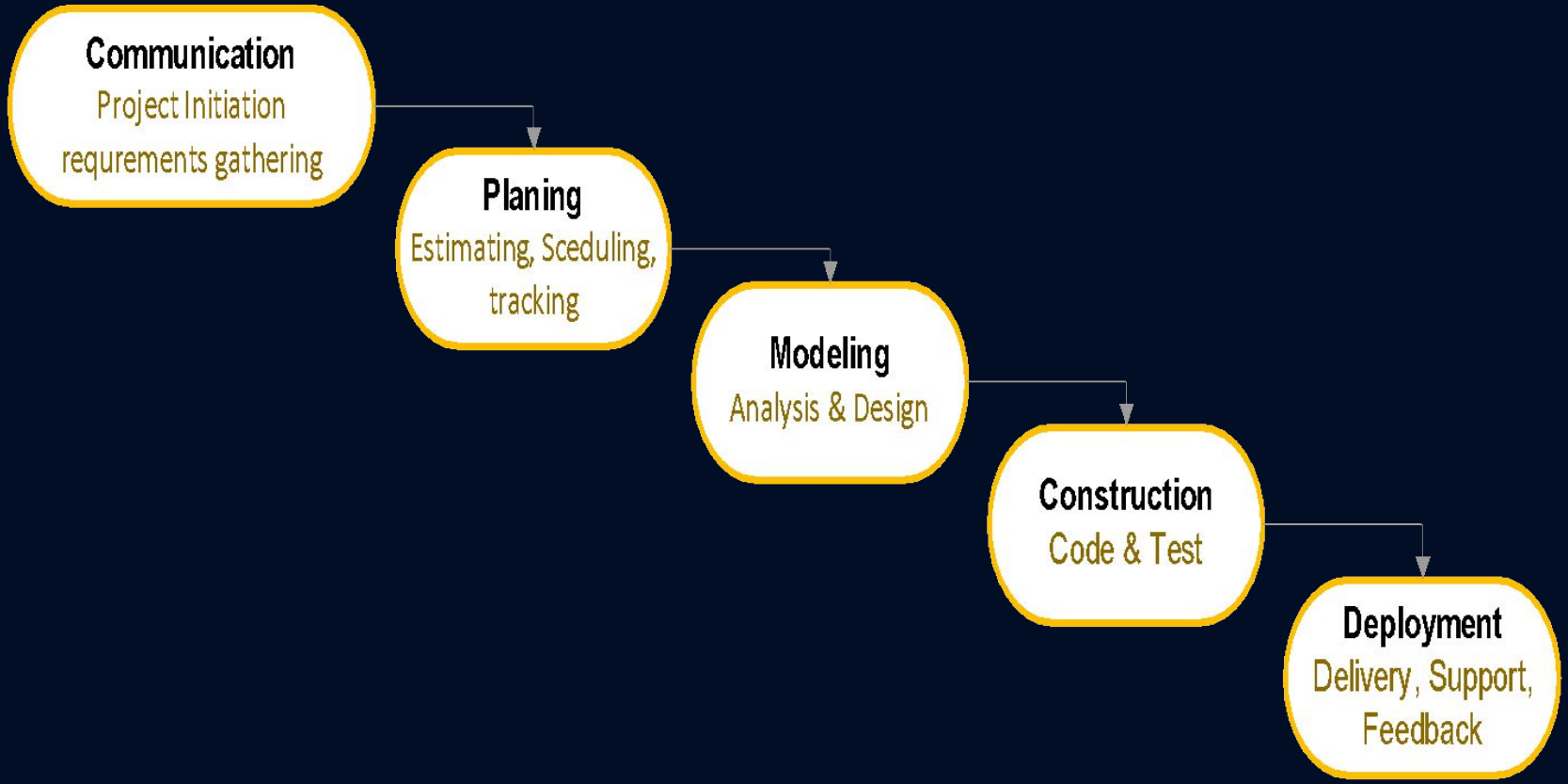
GitGuardian is the code security platform for the DevOps generation.

We help enterprises answer the issue of "Where are my hardcoded secrets and have they been leaked?"

@mcdwayne

A (too brief) history of DevOps and Infrastructure as Code (IaC)

@mcdwayne

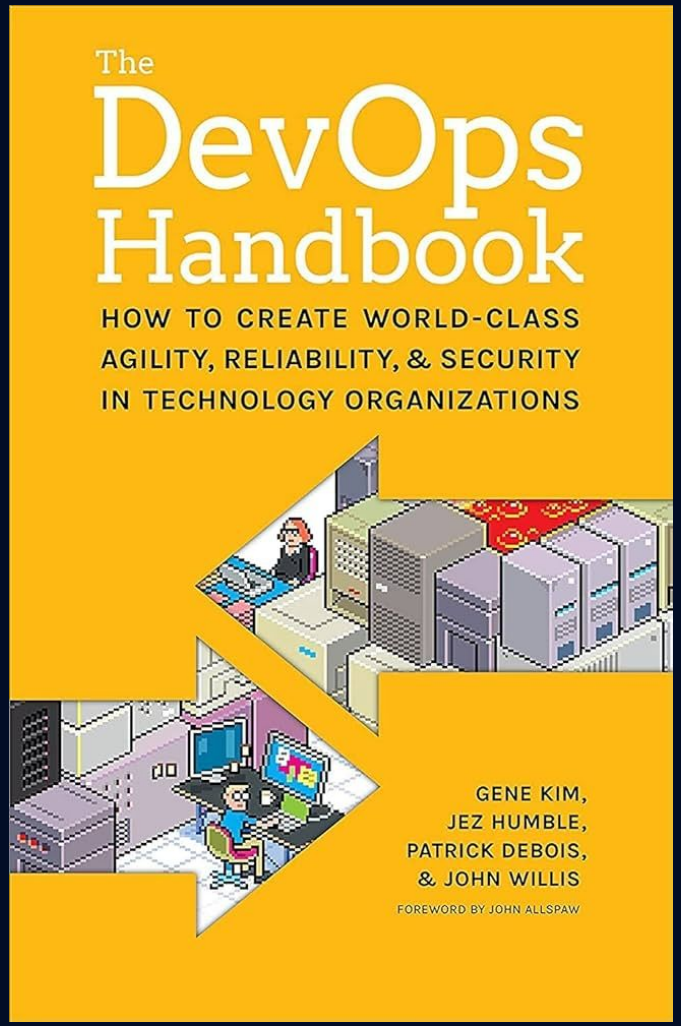


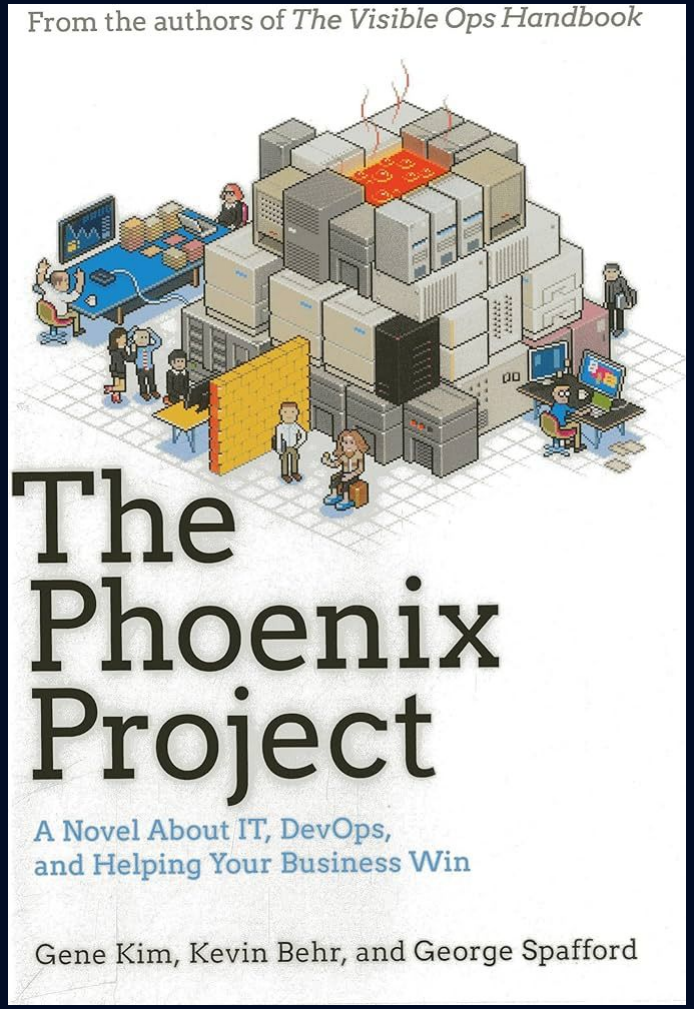
@mcdwayne

DEV

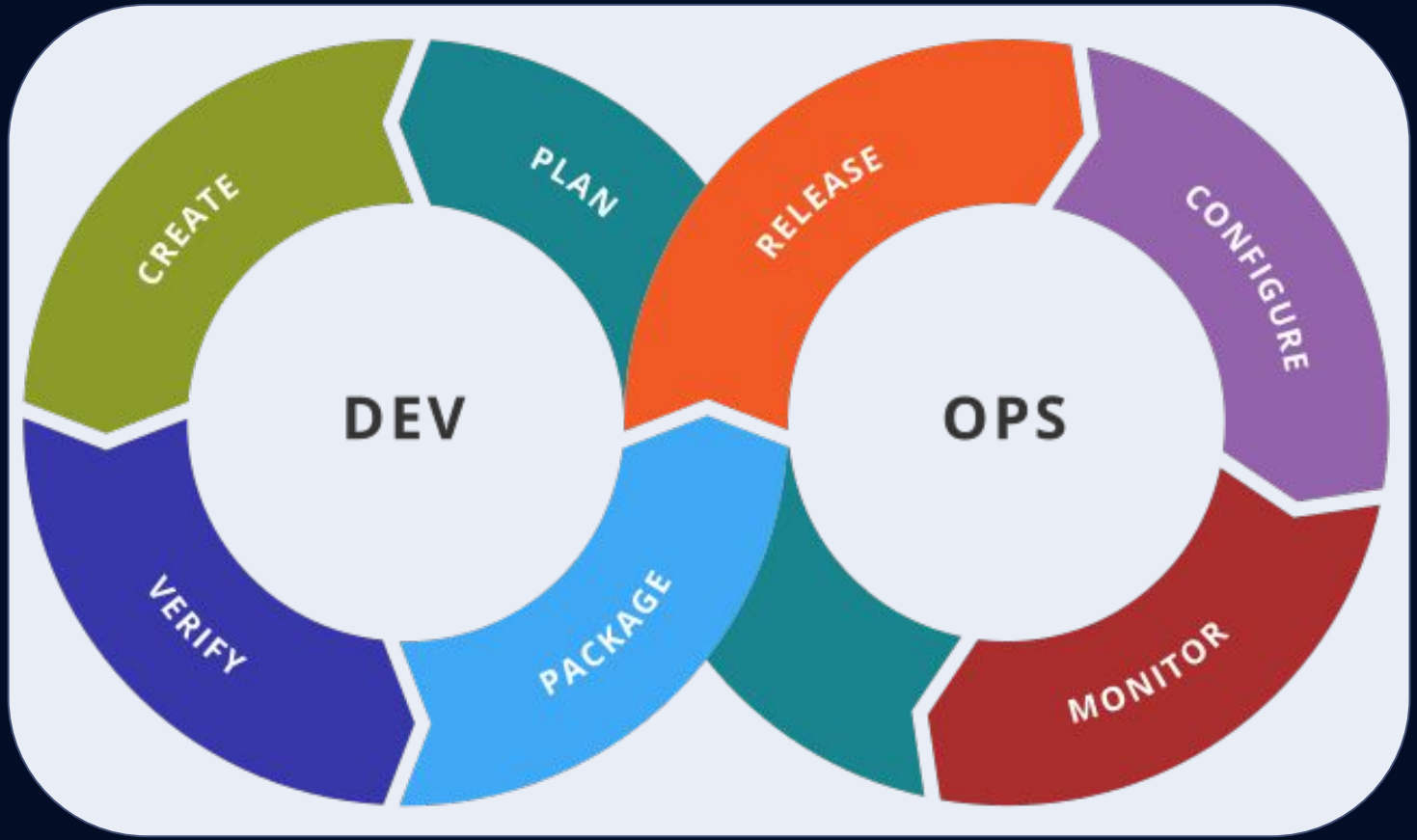
OPS

@mcdwayne

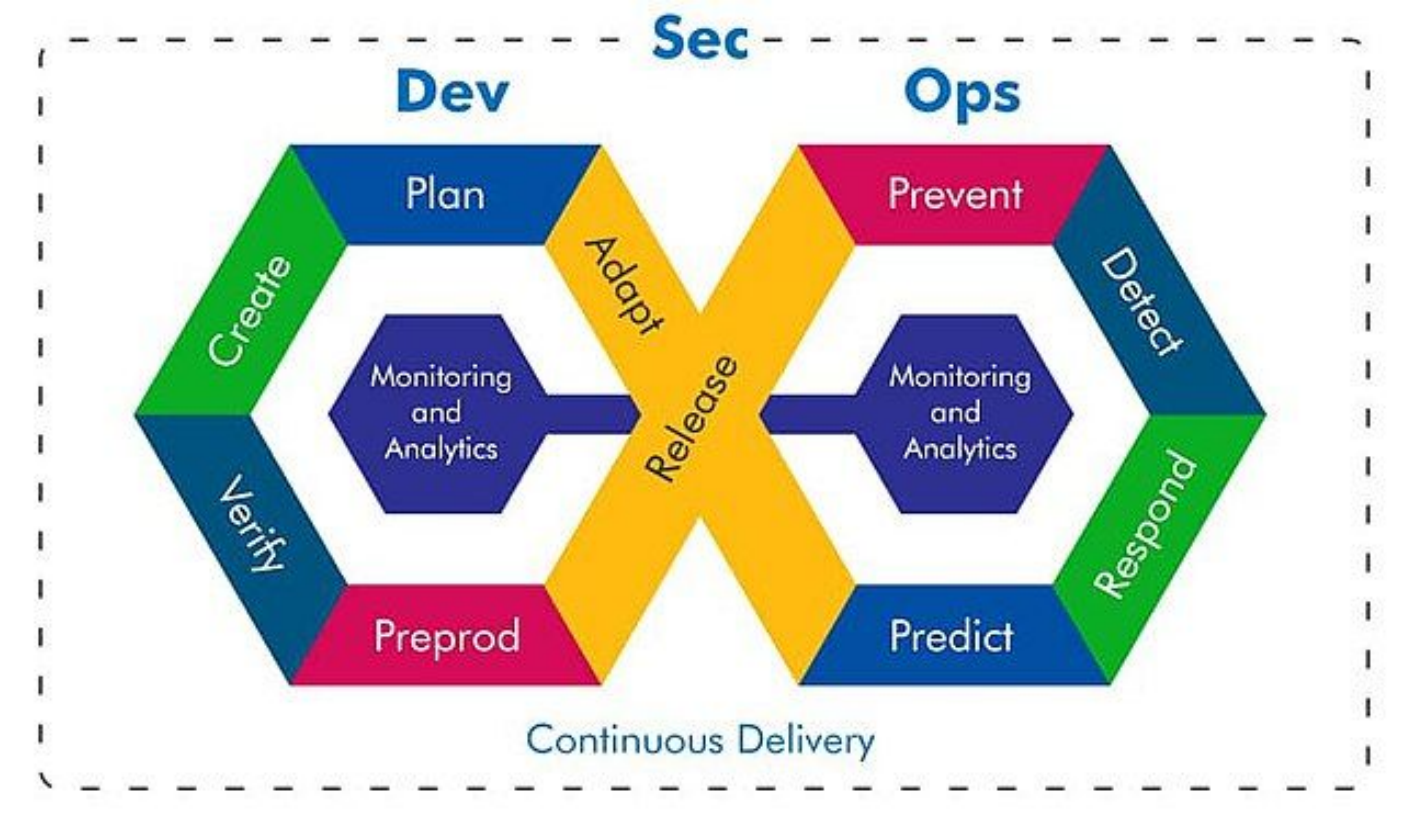




@mcdwayne


CREATE
PLAN
RELEASE
CONFIGURE
DEV
OPS
VERIFY
PACKAGE
MONITOR

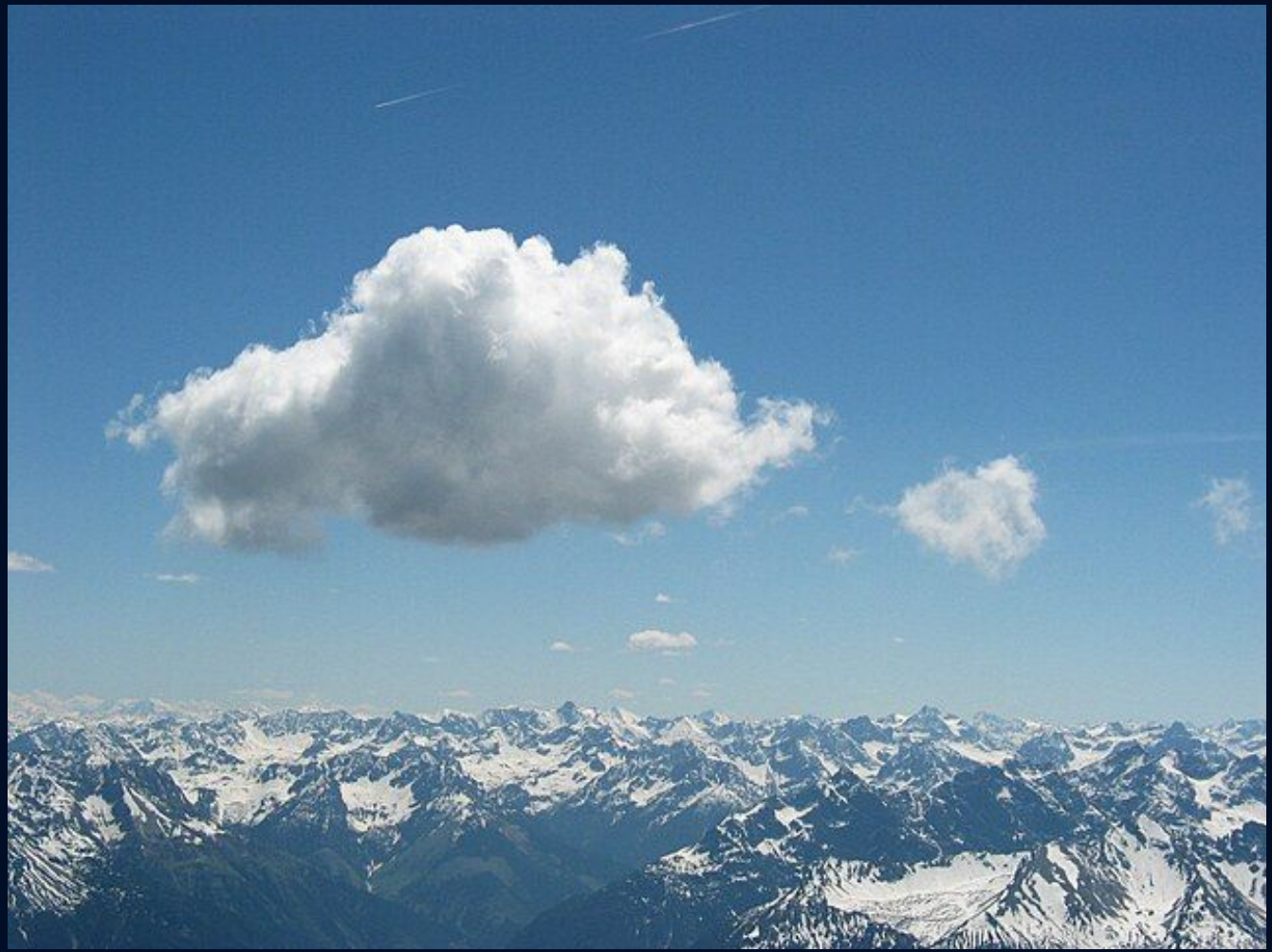
@mcdwayne


Sec
Dev
Ops
Plan
Create
Verify
Preprod
Monitoring and Analytics
Adapt
Release
Prevent
Detect
Respond
Predict
Monitoring and Analytics
Continuous Delivery

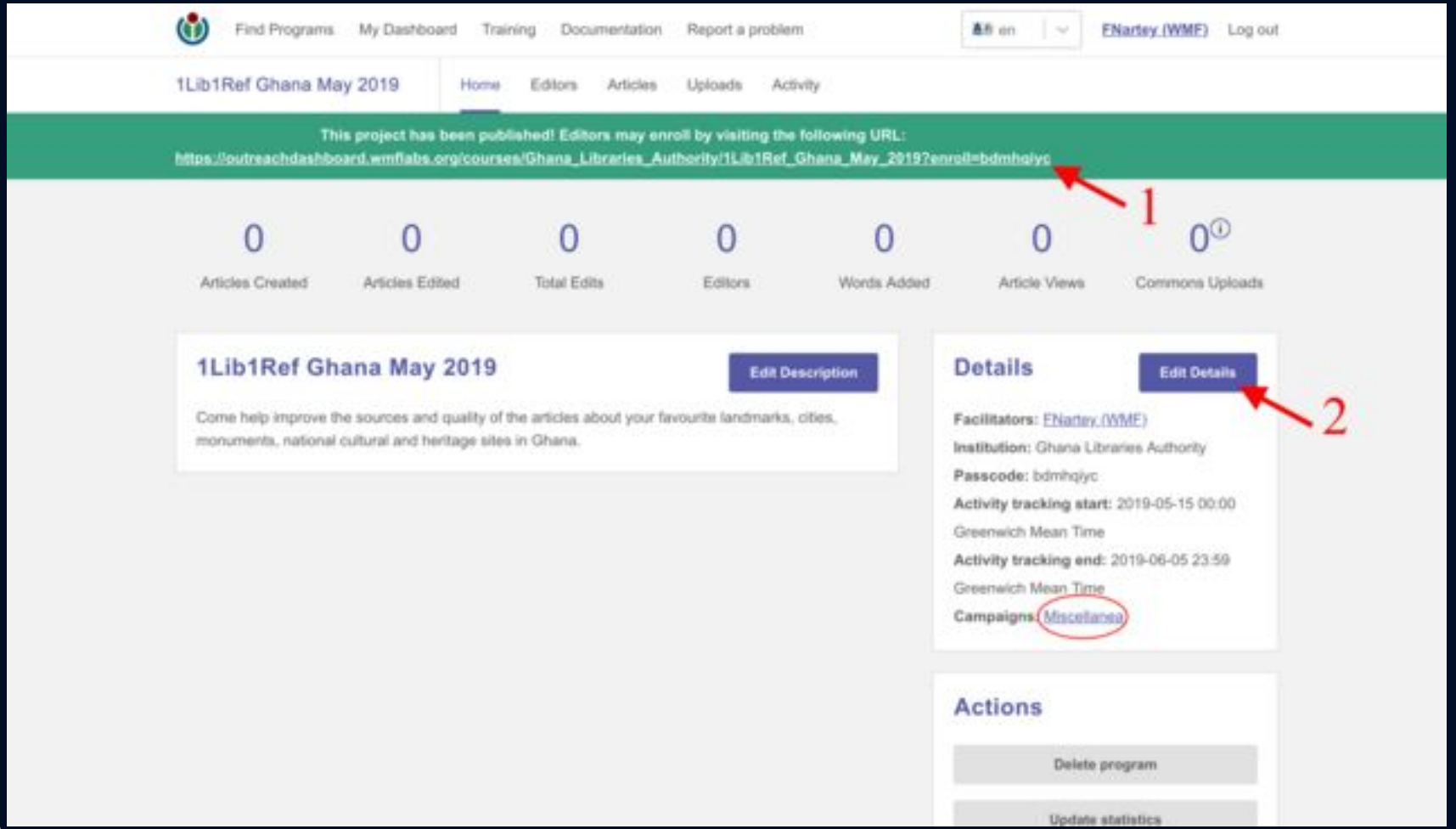
@mcdwayne


PROPRIETE CERN
PROPRIETE CERN
CERN
THIS machine IS A
DO NOT POWE
DOWN!!

@mcdwayne



@mcdwayne


Find Programs
My Dashboard
Training
Documentation
Report a problem
en
FNartey (WMF)
Log out
1Lib1Ref Ghana May 2019
Home
Editors
Articles
Uploads
Activity
This project has been published! Editors may enroll by visiting the following URL:
https://outreachdashboard.wmflabs.org/courses/Ghana_Libraries_Authority/1Lib1Ref_Ghana_May_2019?enroll=bdmhqiyc
1
0
Articles Created
0
Articles Edited
0
Total Edits
0
Editors
0
Words Added
0
Article Views
0
Commons Uploads
1Lib1Ref Ghana May 2019
Edit Description
Come help improve the sources and quality of the articles about your favourite landmarks, cities, monuments, national cultural and heritage sites in Ghana.
Details
Edit Details
2
Facilitators: FNartey (WMF)
Institution: Ghana Libraries Authority
Passcode: bdmhqiyc
Activity tracking start: 2019-05-15 00:00 Greenwich Mean Time
Activity tracking end: 2019-06-05 23:59 Greenwich Mean Time
Campaigns: Miscellaneo
Actions
Delete program
Update statistics

@mcdwayne

Cloud Provider Dashboards

Config files

menu.lst (/boot/grub) - gedit

File Edit View Search Tools Documents Help

menu.lst

```
## should update-grub create memtest86 boot option
## e.g. memtest86=true
##      memtest86=false
# memtest86=true

## should update-grub adjust the value of the default booted system
## can be true or false
# updatedefaultentry=false

title           Windows XP
root            (hd0,0)
savedefault
makeactive
chainloader     +1

title           Ubuntu Linux
root            (hd0,2)
kernel          /boot/vmlinuz-2.6.15-25-386 root=/dev/hda3 ro quiet splash
initrd          /boot/initrd.img-2.6.15-25-386
boot
```


@mcdwayne

~~Declared Infrastructure State Configurations Stored As Code~~

Infrastructure as Code

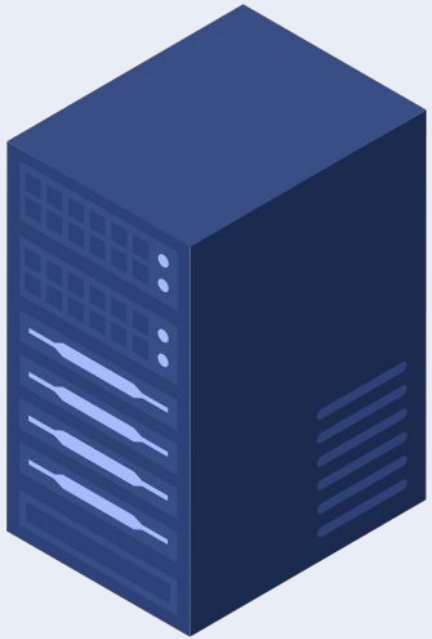
HashiCorp Terraform

Pulumi

AWS CloudFormation

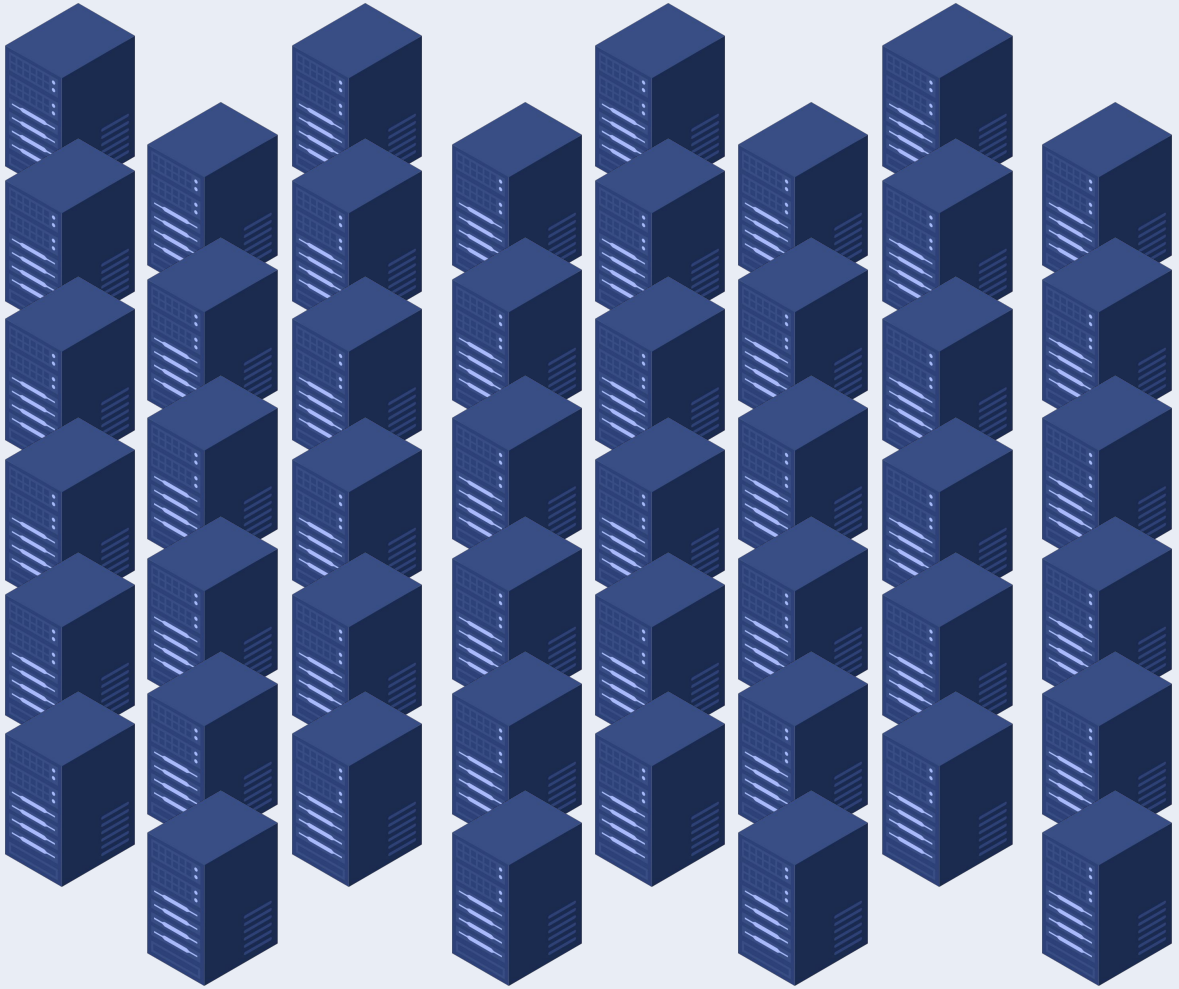
OpenTofu

Crossplane

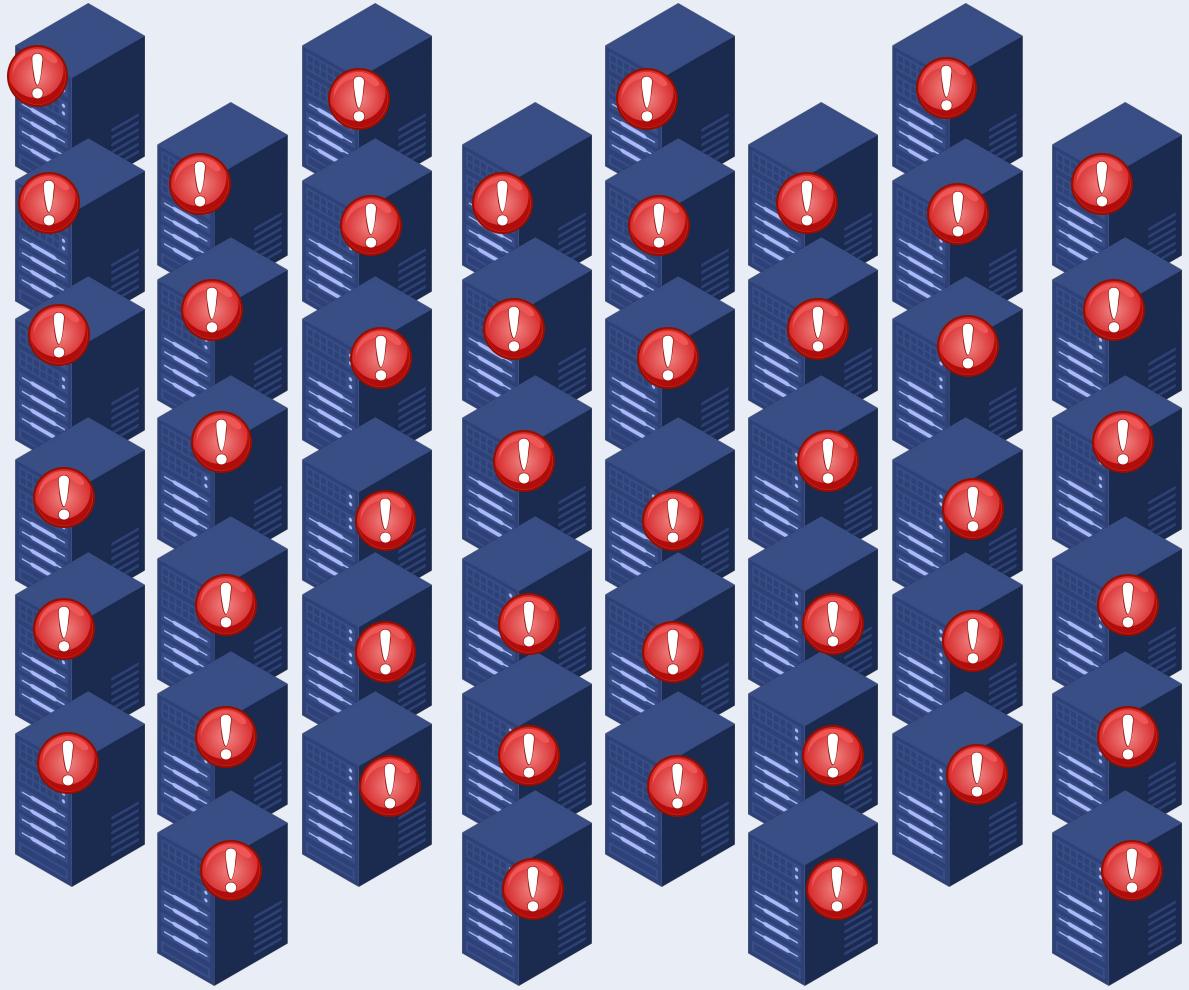


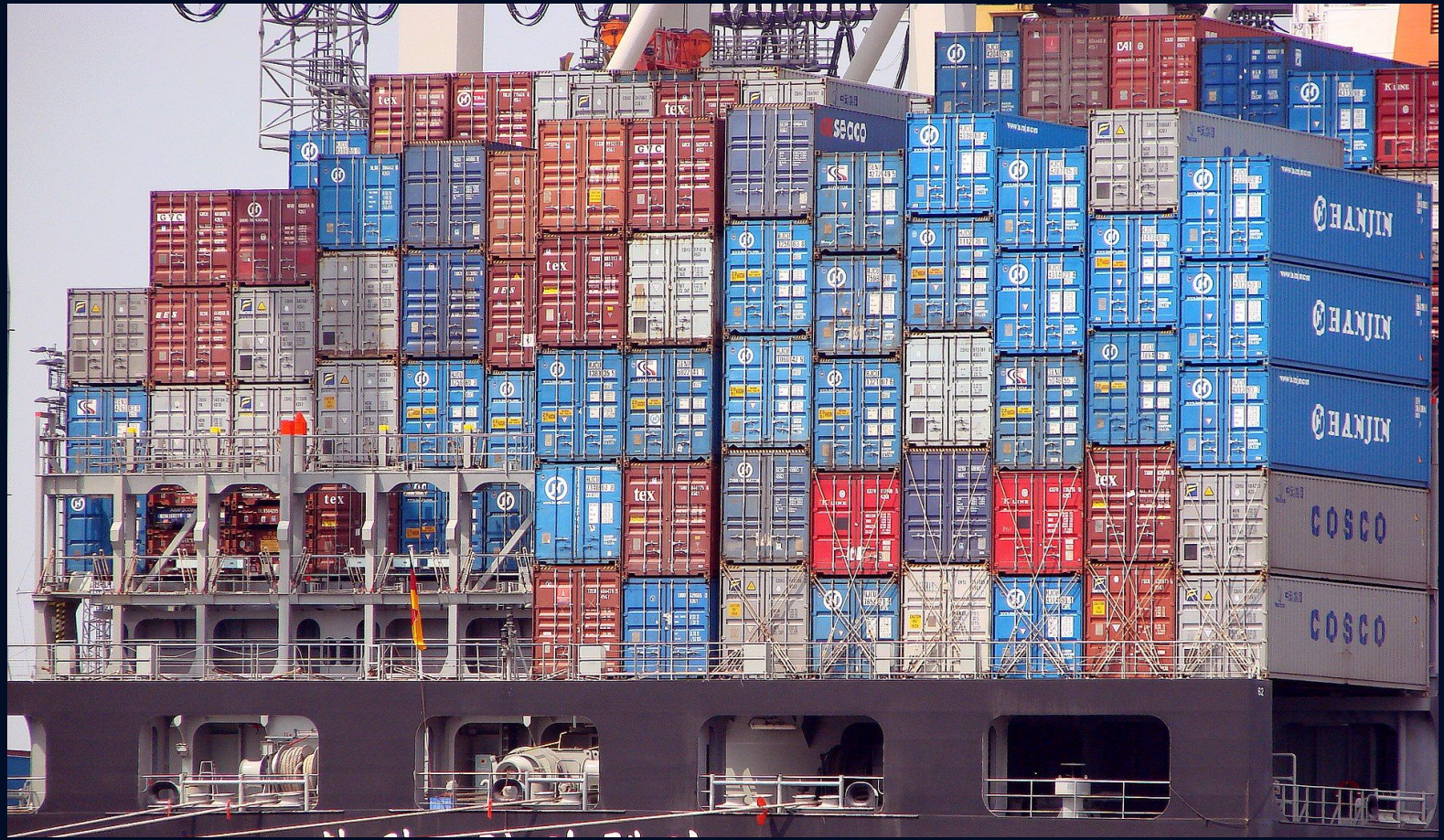
Number_of_Servers = 1

Number_of_Servers = 48



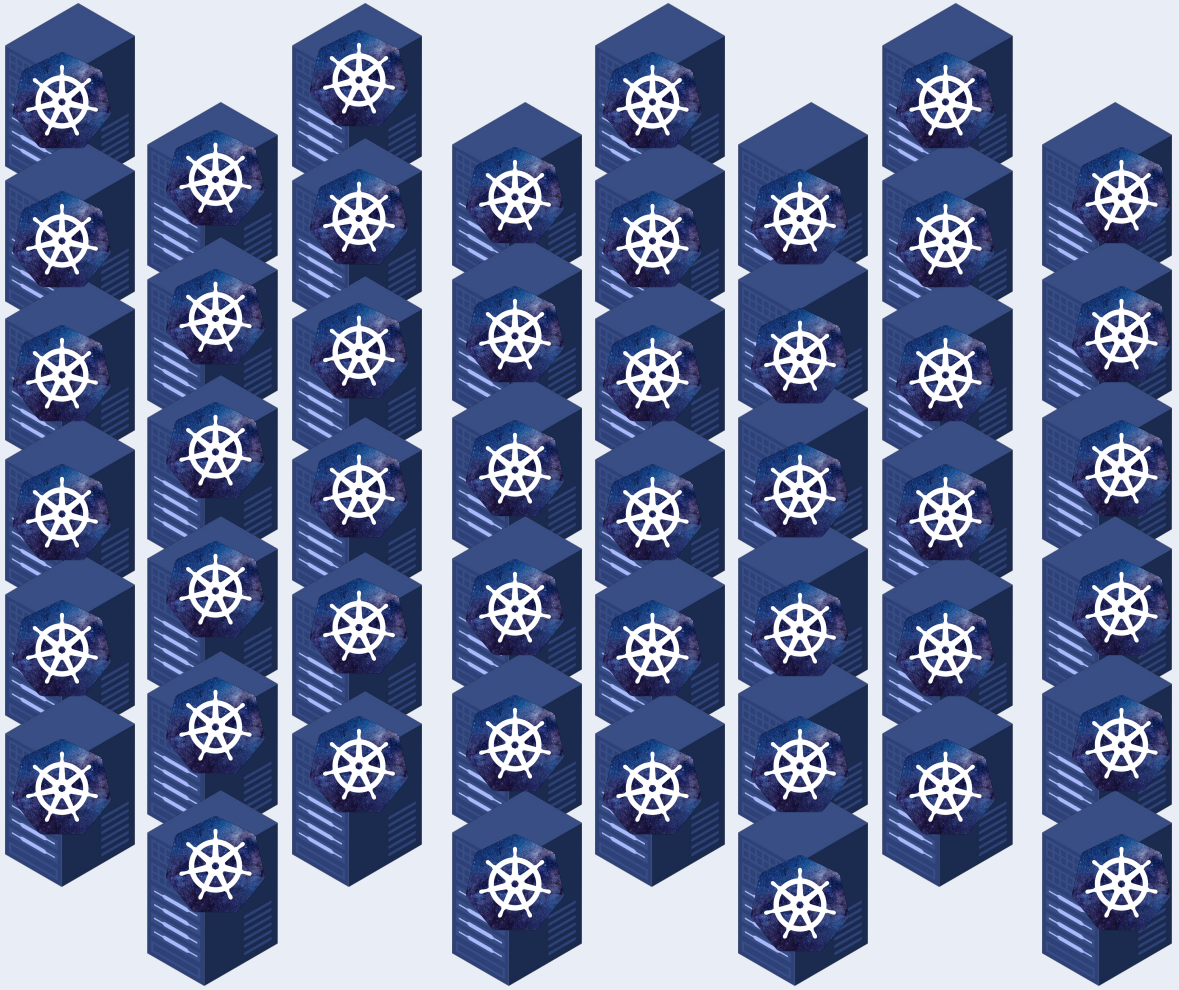
```
Number_of_Servers = 48
# DO NOT Allowed_IPs = /0.
Allowed_Inbound_IPs = /0.
```





@mcdwayne

```
securityContext:
  runAsNonRoot: false
```



Cloud misconfiguration causes massive data breach at Toyota Motor

News

Jun 06, 2023 • 4 mins

Cloud Security | Data Breach

Vehicle data and customer information were exposed for over eight years due to a cloud misconfiguration at Toyota Motor that impacted over 260,000 customers.

Related content

Misconfiguration biggest culprit in cloud security incidents

While vulnerabilities are a concern, misconfigurations are still the biggest player in cloud security incidents and, therefore, should be one of the greates causes for concern in organizations. By 2023, 75% of security failures will result from inadequate management of identities, access, and privileges, up from 50% in 2020, according to **Gartner**.

RiskOptics | FORMERLY RECIPROCITY Product Solutions Success

Unfortunately, Atlassian's error is all too common. Configuration errors were responsible for almost one-third of data breaches in 2021 and are expected t [99 percent of all firewall breaches](#) through 2023.

CROWDSTRIKE | BLOG Featured Recent Videos Cat

According to publicly available data, eight of the top 10 data breaches of 2023 were related to application attack surfaces.[1] These eight breaches alone exposed almost 1.7 billion records, illustrating the potential for tremendous data loss if applications are poorly configured and lack effective protection.

@mcdwayne

@mcdwayne

Areas Of IaC Security Concern

1. Misconfigurations
2. Access
3. Governance

Areas Of IaC Security Concern

1. Misconfigurations

OWASP Top 10

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

@mcdwayne

OWASP Top 10 Cloud Native

CNAS-1: Insecure cloud, container or orchestration configuration

CNAS-2: Injection flaws (app layer, cloud events, cloud services)

CNAS-3: Improper authentication & authorization

CNAS-4: CI/CD pipeline & software supply chain flaws

CNAS-5: Insecure secrets storage

- CNAS-6: Over-permissive or insecure network policies
- CNAS-7: Using components with known vulnerabilities
- CNAS-8: Improper assets management
- CNAS-9: Inadequate ‘compute’ resource quota limits
- CNAS-10: Ineffective logging & monitoring (e.g. runtime activity)

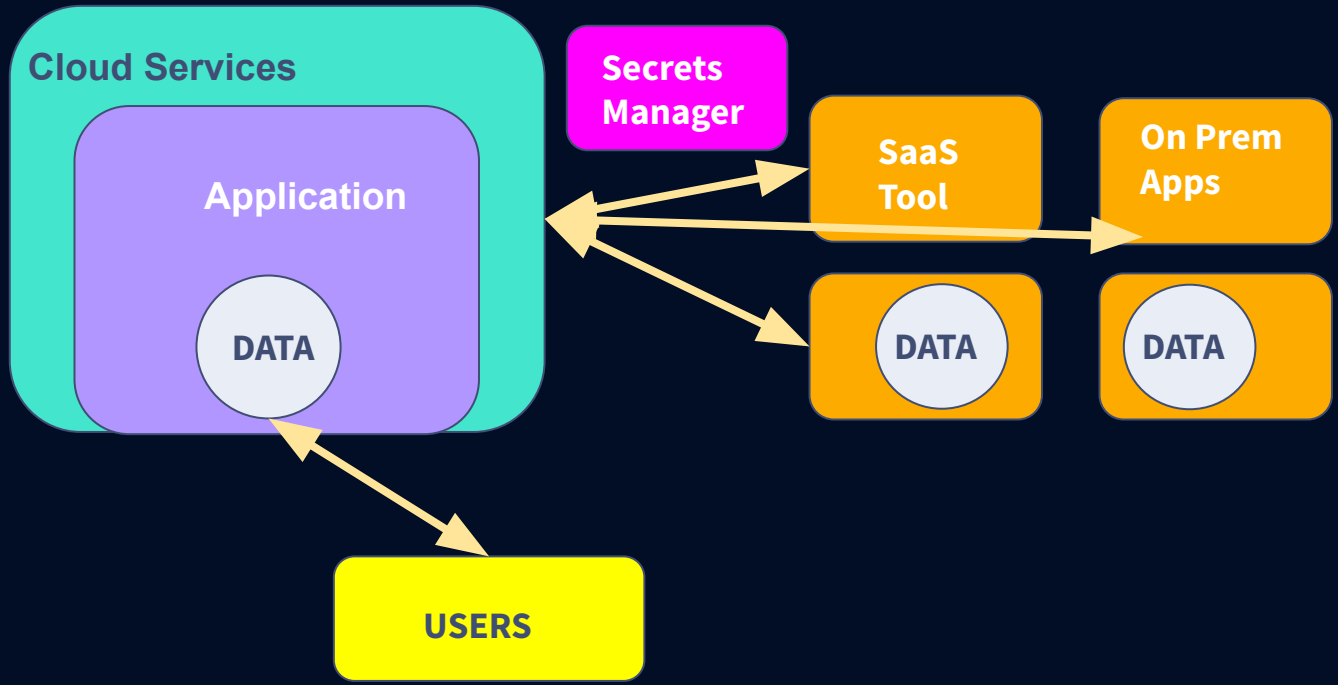
@mcdwayne

What Misconfigurations?

1. Network
2. Secrets
3. Permissions
4. Data
5. Other

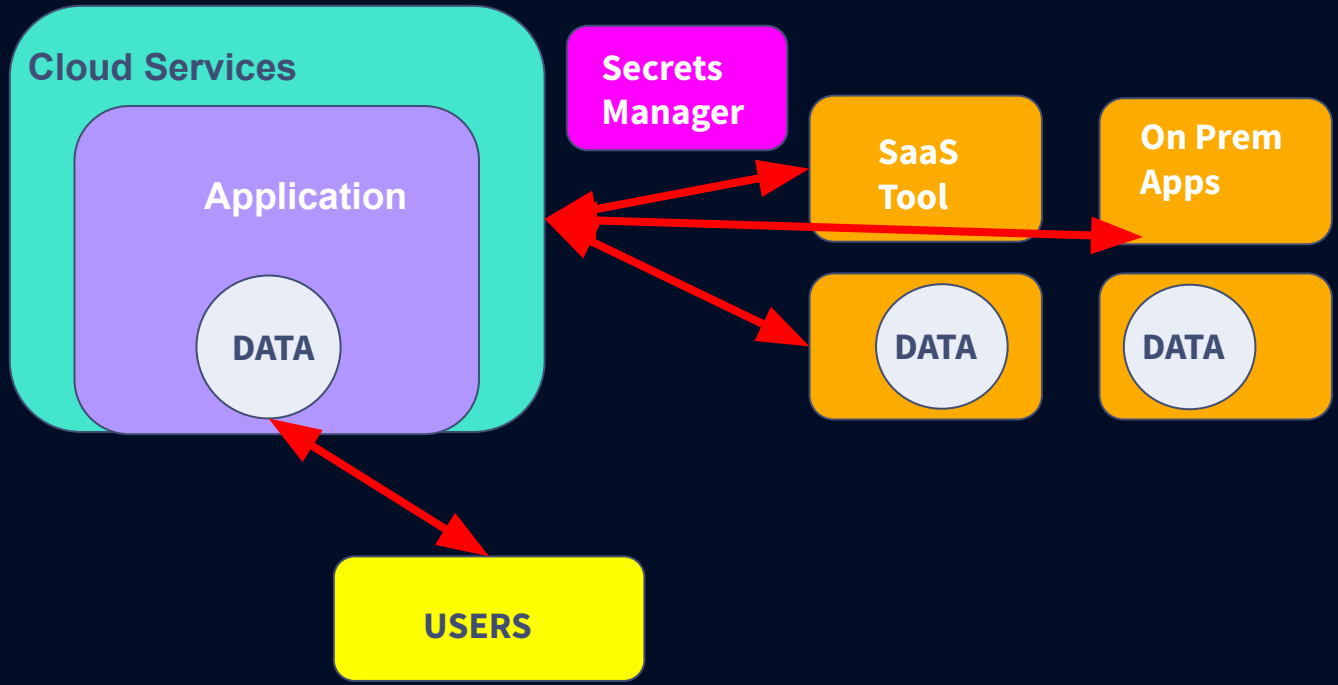
@mcdwayne

A fully realistic and complete scale model



@mcdwayne

Network Misconfigurations



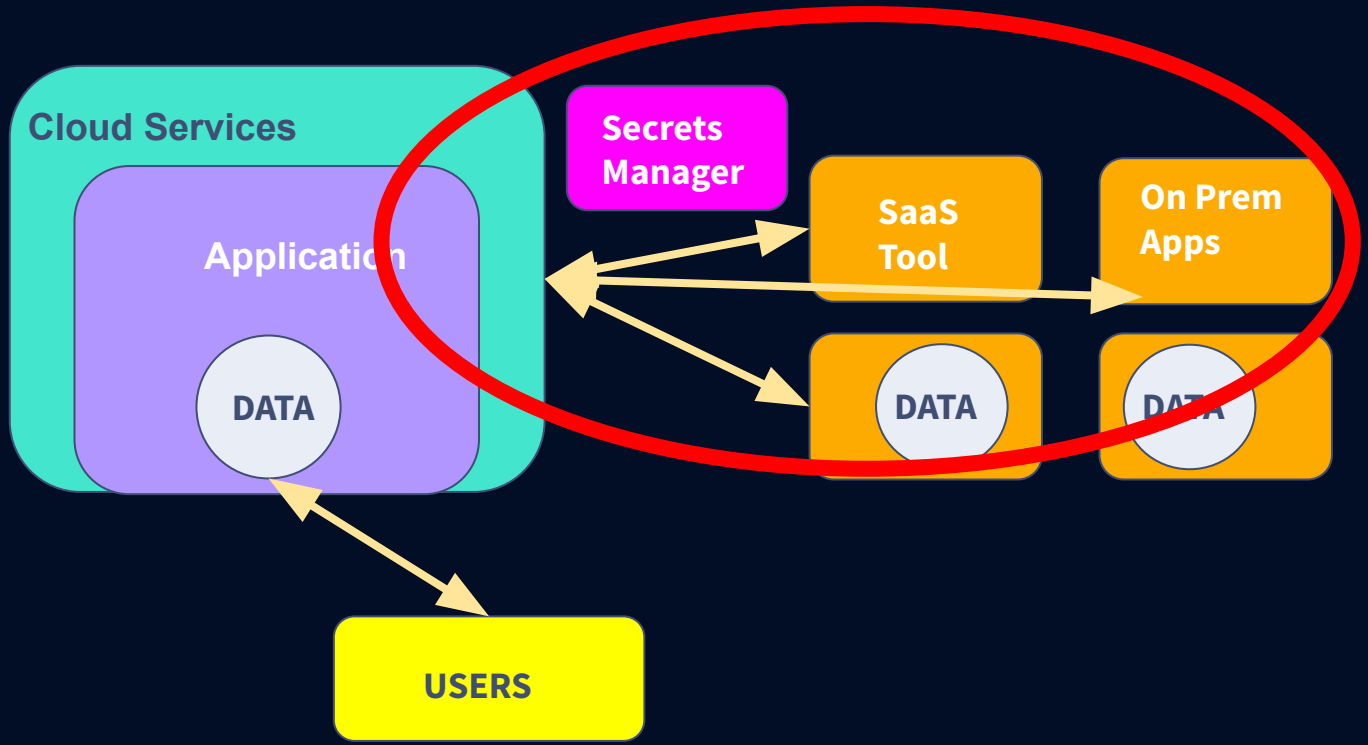
@mcdwayne

Common Network Misconfigurations

1. Leaving remote access accessible from the internet increases the attack surface
2. Key vault has no network Access Control List specified
3. Traffic to /0. allowed in firewall outbound rule
4. Traffic from /0. allowed in firewall inbound rule
5. Open access allowed in firewall inbound rule
6. Plain HTTP is used

@mcdwayne

Secrets Misconfigurations



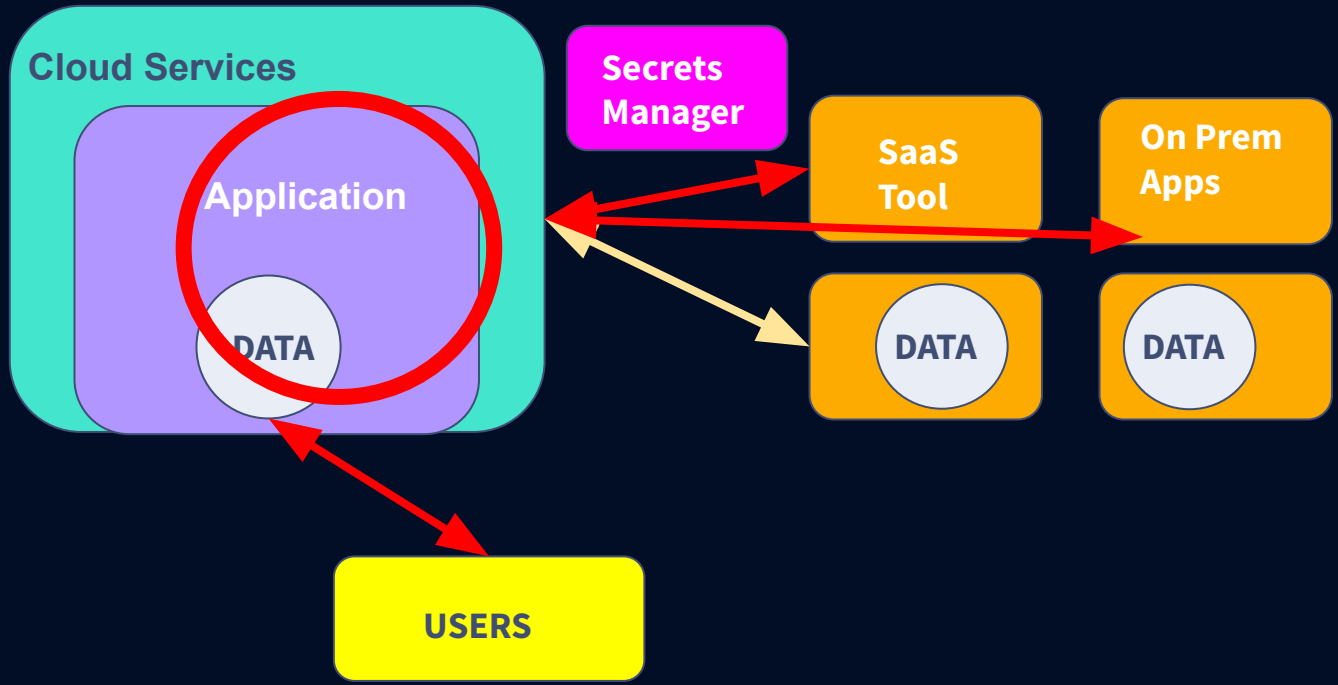
@mcdwayne

Common Secrets Misconfigurations

1. Exposing a sensitive environment variable in the configuration can lead to credentials leak
2. ECR image scanning should be enabled
3. Encrypting EKS secrets with AWS KMS adds another layer of security
4. HTTP data block can be used to leak secrets or variables outside of the organization
5. GKE metadata is not concealed
6. A GCP persistent disk is encrypted with a key specified in plain text

@mcdwayne

Permissions Misconfigurations



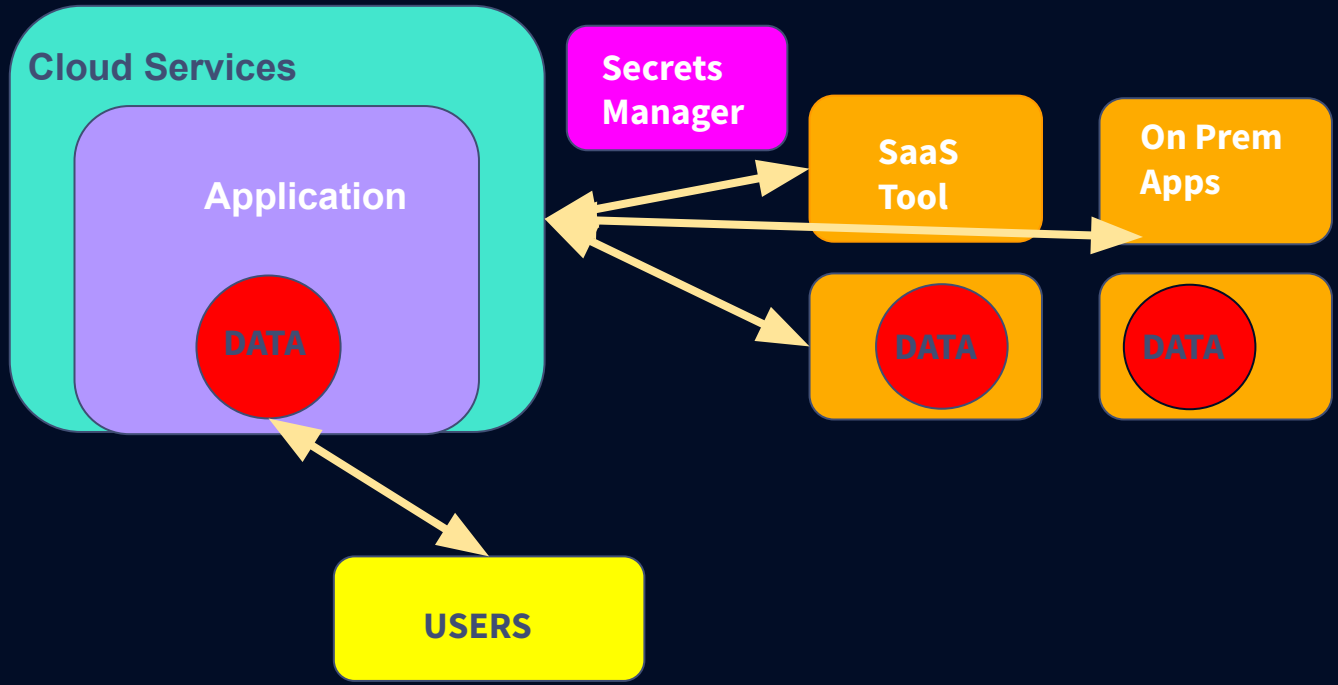
@mcdwayne

Common Permissions Misconfigurations

1. Giving sudo rights to a user allows privilege escalation attacks
2. Using the default service account on a compute instance allows an attacker to spread through the network
3. IAM policies should remove root access keys
4. Unencrypted S3 bucket can lead to data leak
5. Cloudtrail logs validation is not enabled
6. IAM policies should avoid using wildcards
7. Image should not have 'root' user

@mcdwayne

Data Misconfigurations



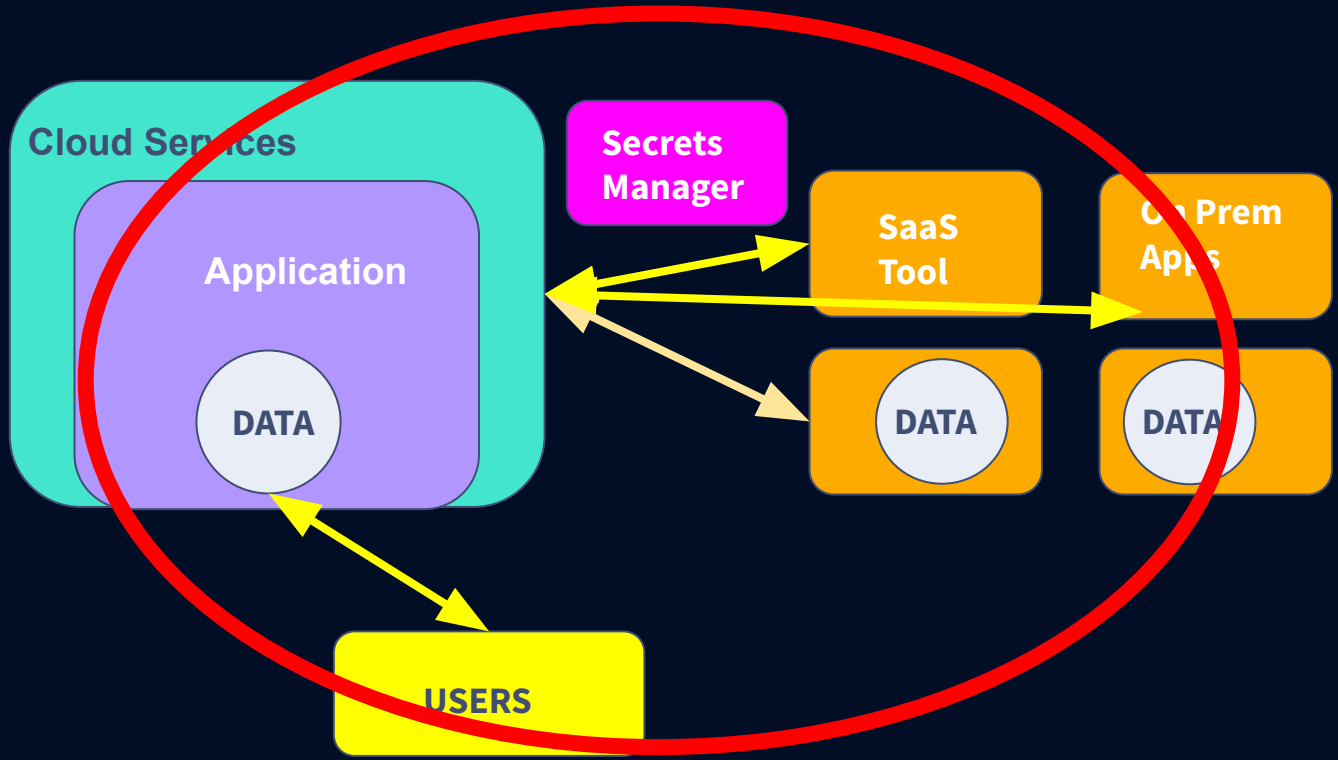
@mcdwayne

Common Data Misconfigurations

1. A CloudTrail bucket has public read Access Control List which can lead to private data exposure
2. Data Factory should not be publicly exposed
3. Not encrypting Athena query results can lead to data leak
4. Not enforcing Workgroup configuration in Athena can allow clients to disable encryption settings
5. EC2 instances use unencrypted block device
6. Not encrypting data at rest can lead to data leak

@mcdwayne

Other Misconfigurations



@mcdwayne

Other Common Misconfigurations

1. An AWS CloudFront distribution allows unencrypted communications over HTTP
2. No SSL connection on SQL database might lead to data exposure
3. ElasticSearch should use node-to-node encryption
4. ElastiCache should use in-transit encryption
5. Kinesis should use in-transit encryption
6. MSK clusters should use in-transit encryption

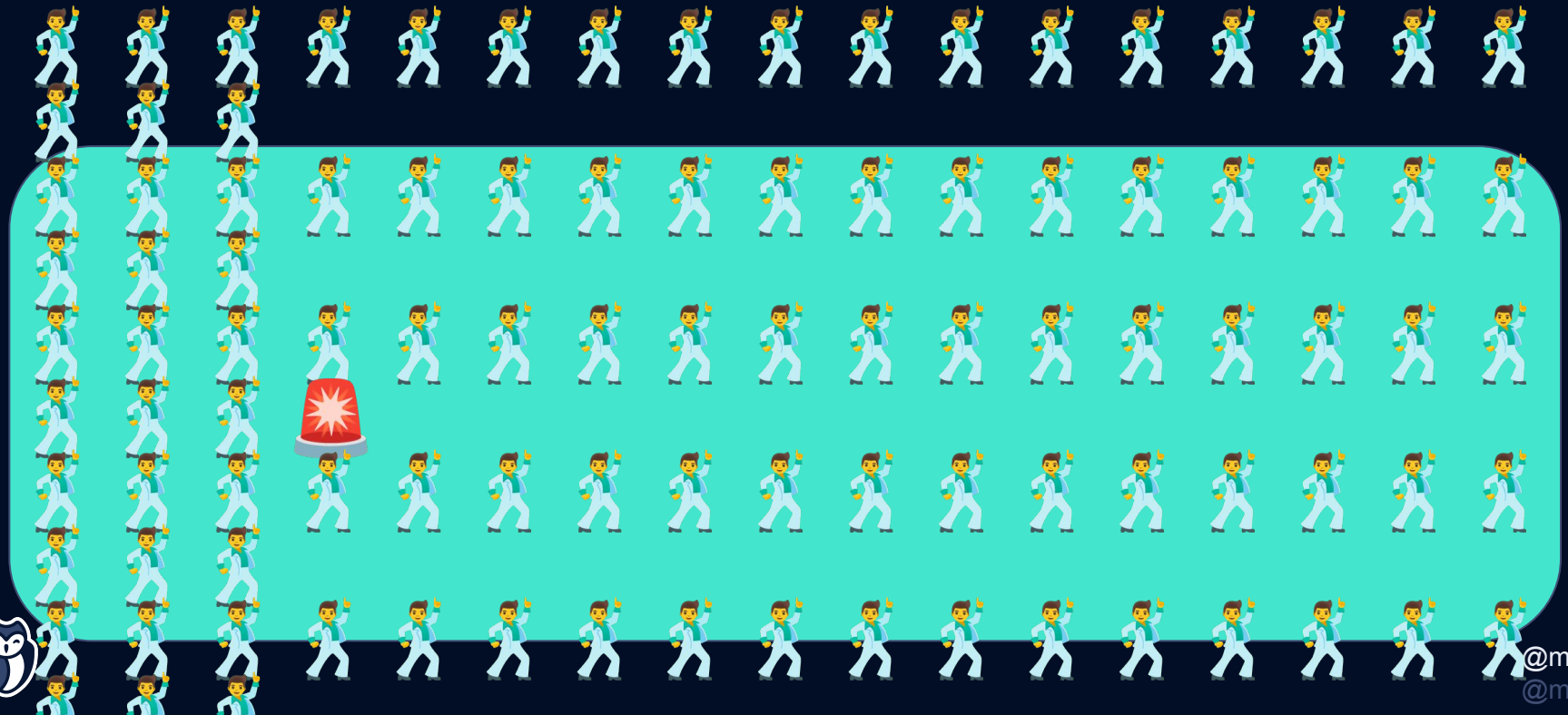
@mcdwayne


GUILTY
THRILLING
ALL
TALKING
DRAMA
A COLUMBIA
Production
Is it...
Devs?
Operations?
DevOps?
Security?

@mcdwayne

security team members 100:1

- Alex Rice, HackerOne



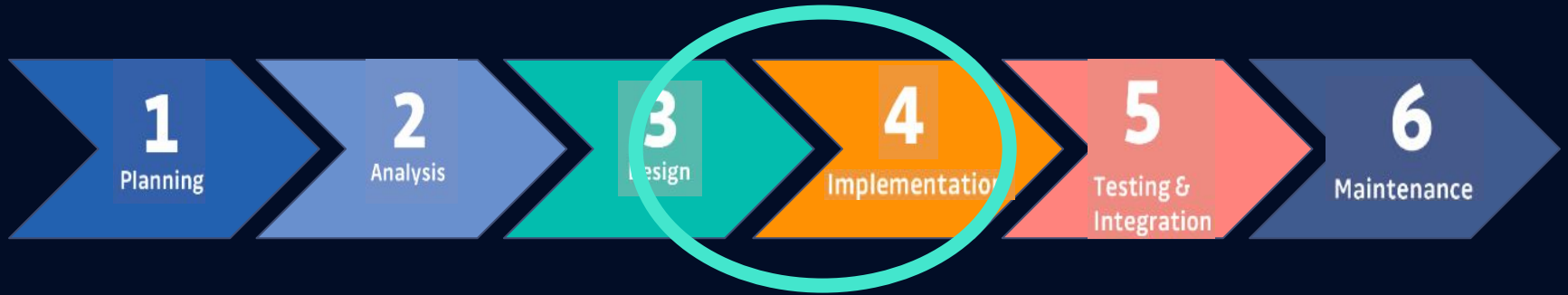
@mcdwayne

@mcdwayne

Shifting Left = Introducing Security Earlier In The Software Development Lifecycle

@mcdwayne

From the Developer's seat, "Shifting Left" gets interpreted as more local testing



@mcdwayne

Tools for scanning for IaC Misconfigurations Locally

1. KICS by Checkmarx - OSS
2. Checkov by Prisma Cloud - OSS
3. Terrascan by Tennable - OSS
4. Tfsec by Aquasecurity - OSS
5. GitGuardian IaC Security - Freemium
6. Snyk Infrastructure as Code - Freemium

@mcdwayne
@mcdwayne

@mcdwayne

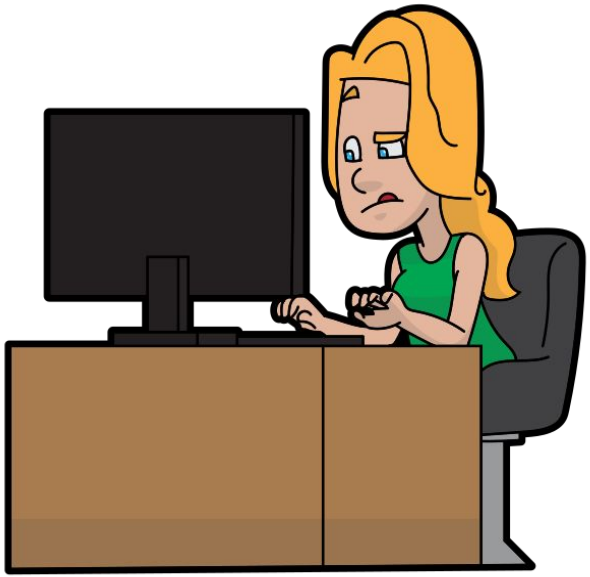
Areas Of IaC Security Concern

1. Misconfigurations
2. Access
3. Governance

Areas Of IaC Security Concern

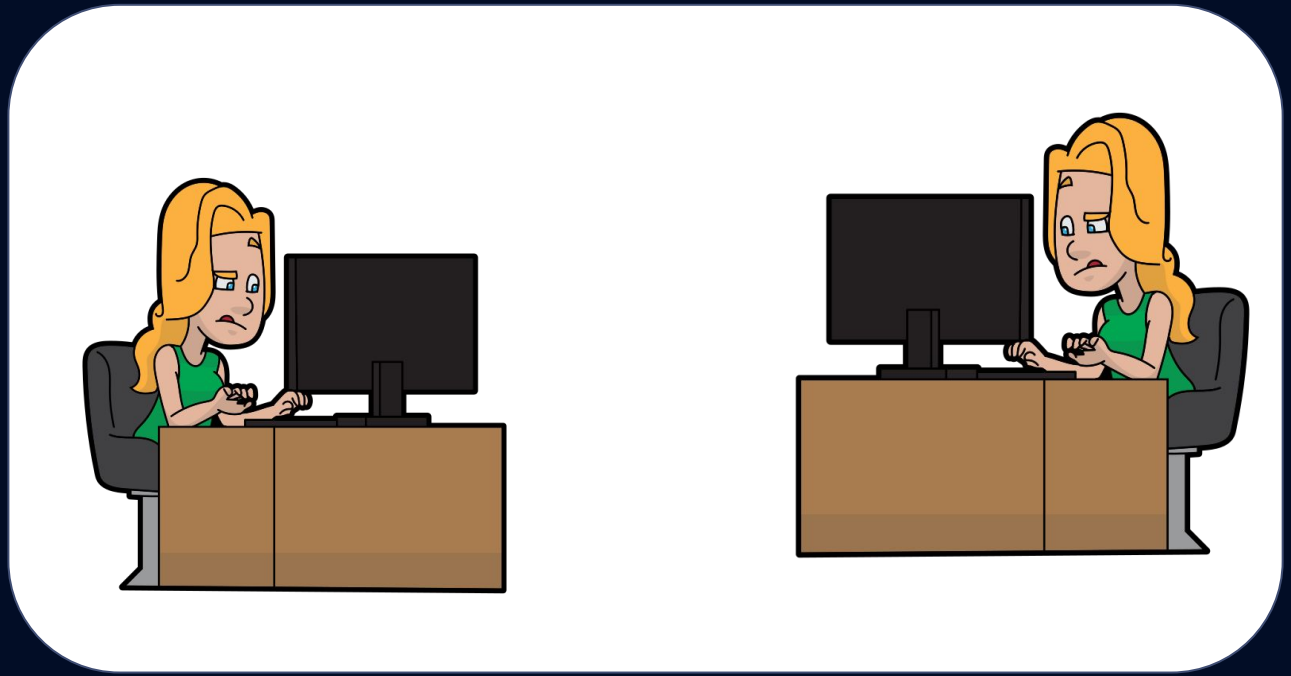
2. Access

Who can touch the code AND instances??



@mcdwayne

Can I access the same services from multiple accounts?



@mcdwayne

Cross team friction?

@mcdwayne
@mcdwayne

Cloud Provider Dashboards

VS

IaC

```
resource "google_compute_instance" "vm_instance" {
 name = "terraform-instance"
 machine_type = "f1-micro"
 initial_node_count = “3”
 boot_disk {
    initialize_params {
        image = "debian-cloud/debian-9"
        }
 }
 network_interface {
    network = google_compute_network.vpc_network.name
    access_config {
    }
 }
 }
```


@mcdwayne

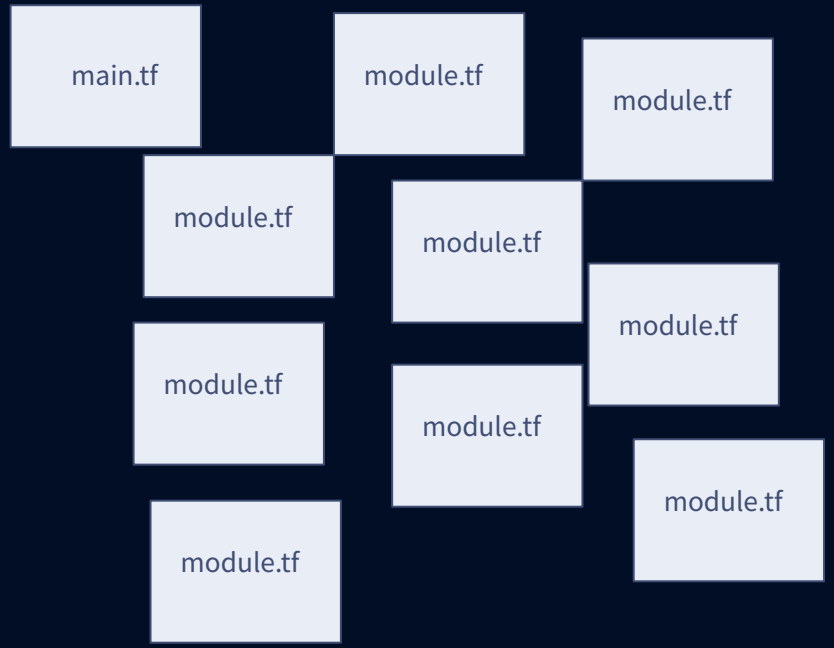
Where are you storing your IaC Code?

- In the same repo as your app code?
- Different repo than your apps?
- It depends on the project?
- What IaC code?

@mcdwayne

How modular is your IaC?

IaC Monolith



@mcdwayne

Are there valid, real secrets in your IaC Code that could give someone access?

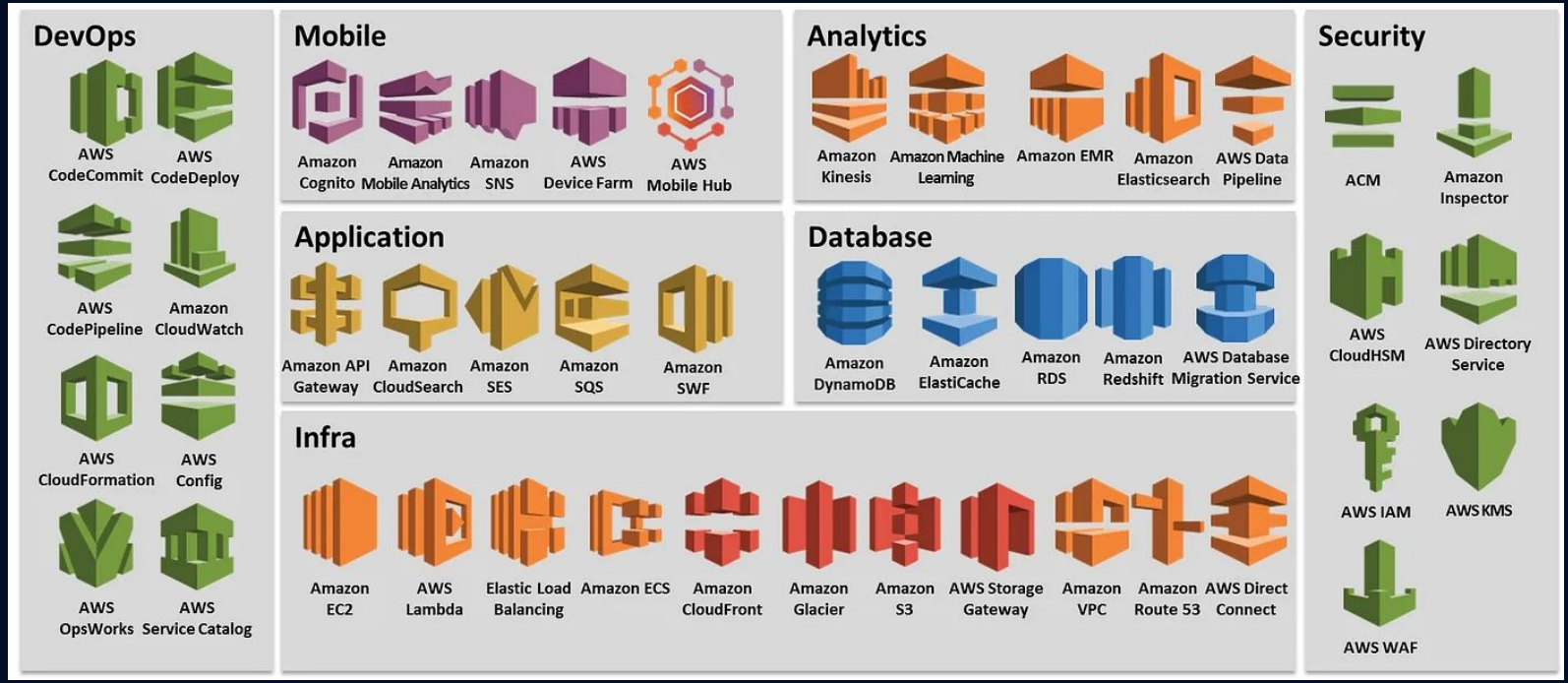
https://www.gitguardian.com/state-of-secrets-sprawl-report-2024

@mcdwayne

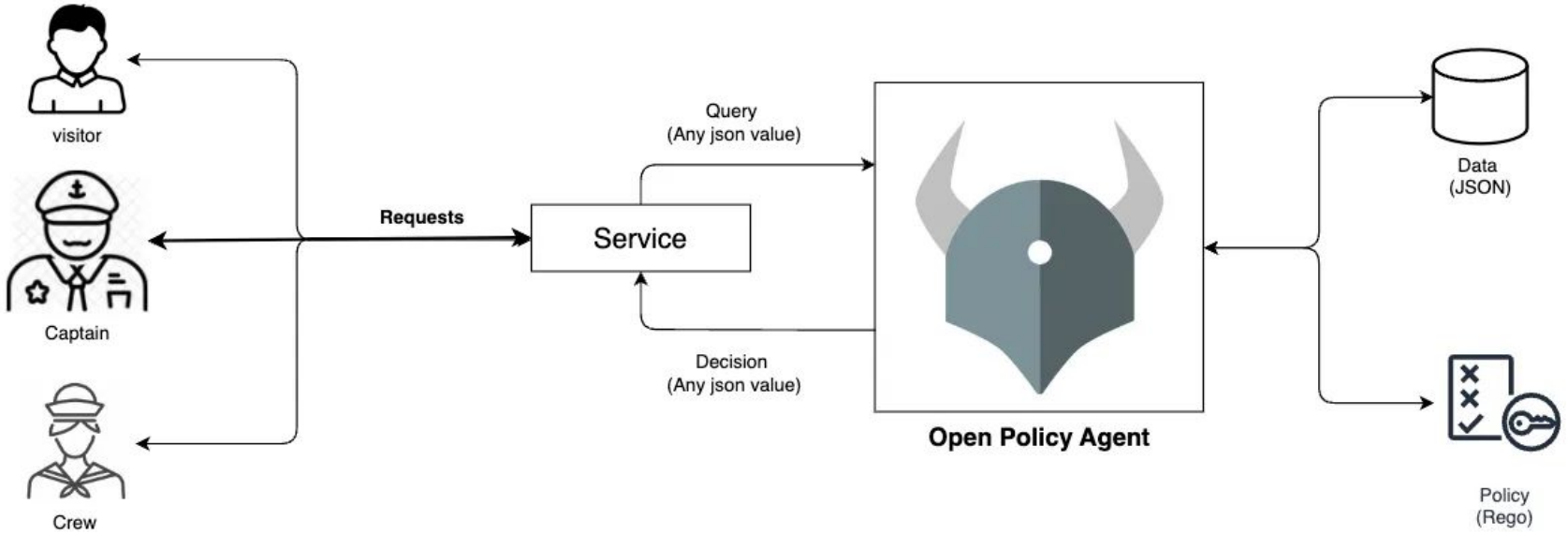
Areas Of IaC Security Concern

3. Governance

How do you manage what IaC invokes, and under which conditions?

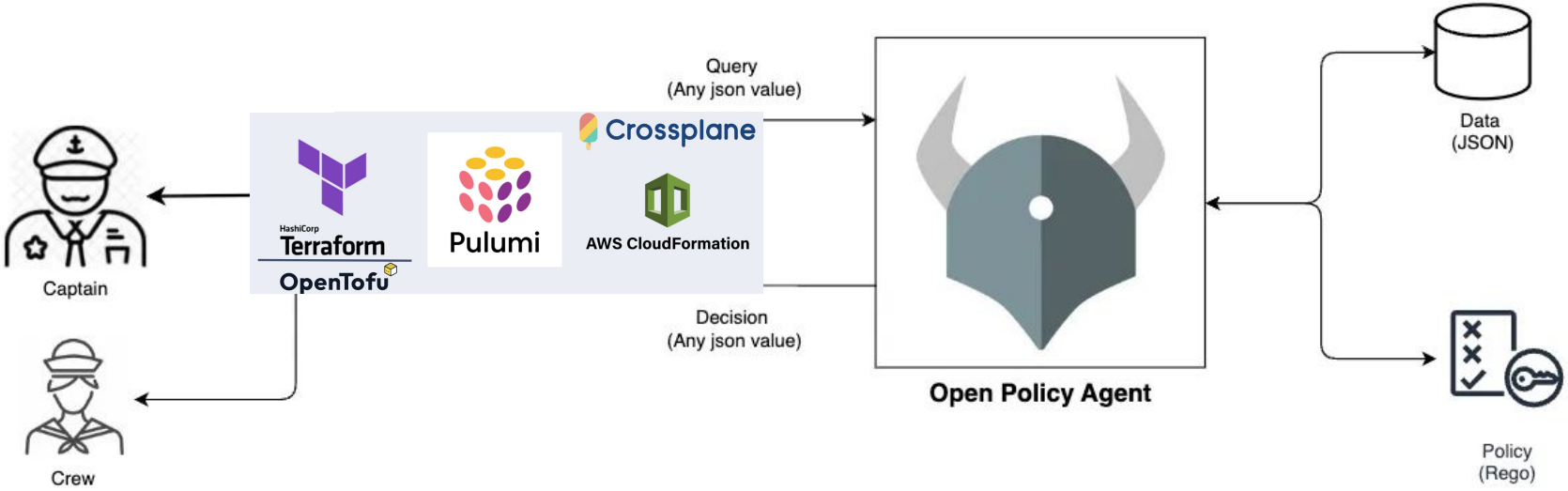


Enter the (Open) Policy Agent

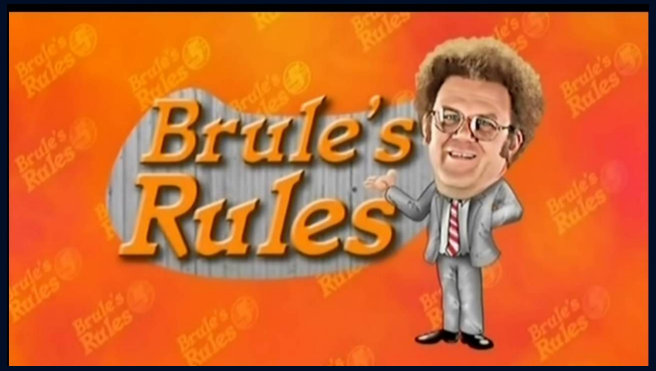


@mcdwayne

Enter the (Open) Policy Agent for IaC?



@mcdwayne



Good for:

- Established policy that is clear cut
- IaC Security
- Preventing unwanted access

Bad for:

- Uncertain situations
- Development work
- Innovating rapidly

@mcdwayne

Human in the loop

Atlantis

Terraform Pull Request Automation

STEP 3 Someone on your team reviews the plan and approves the pull request

alice approved these changes — View changes

STEP 4 You comment 'atlantis apply'

lkysow commented

atlantis apply

STEP 5 Atlantis runs `terraform apply` and comments back on the pull request

atlantisbot commented

Ran Apply in dir: `.` workspace: `default`

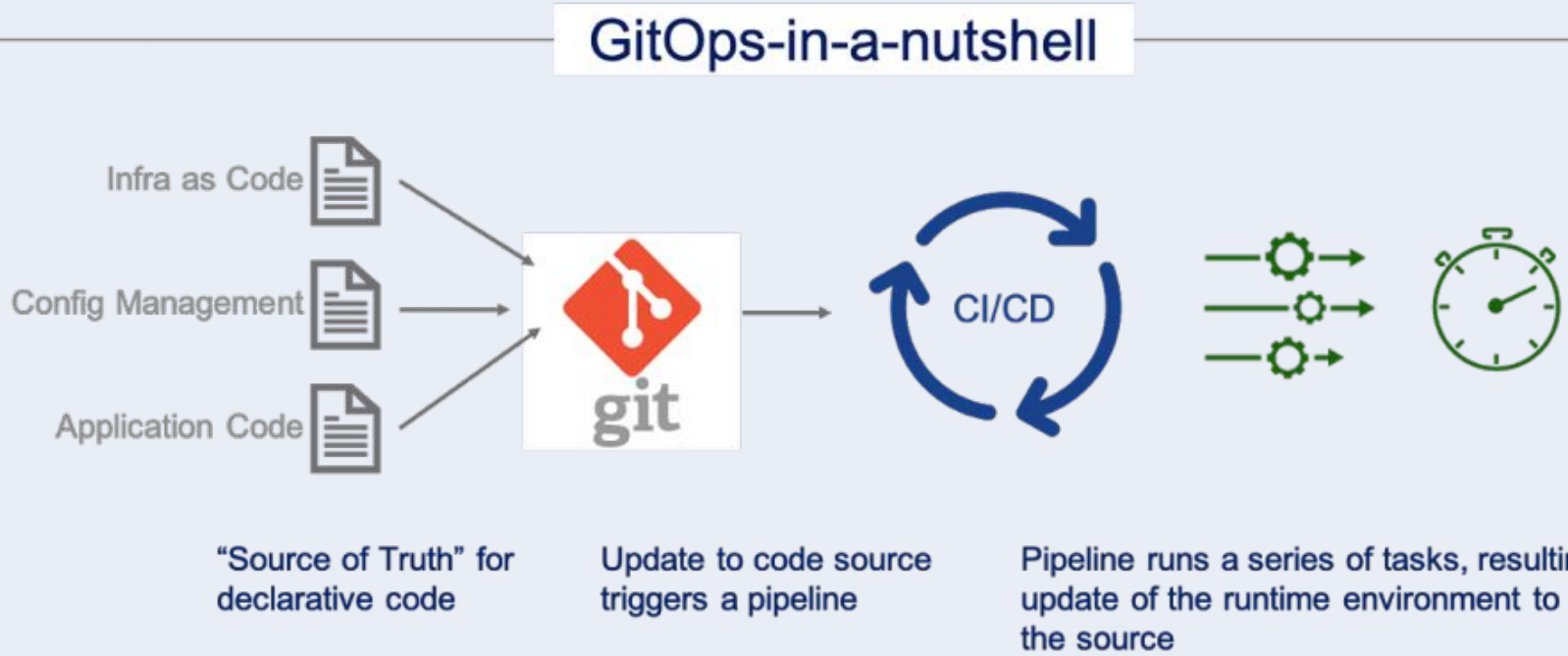
```
null_resource.demo: Creating...
null_resource.demo: Creation complete after 0s (ID: 4542221565395344699)

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
```

env0

@mcdwayne

What about GitOps?



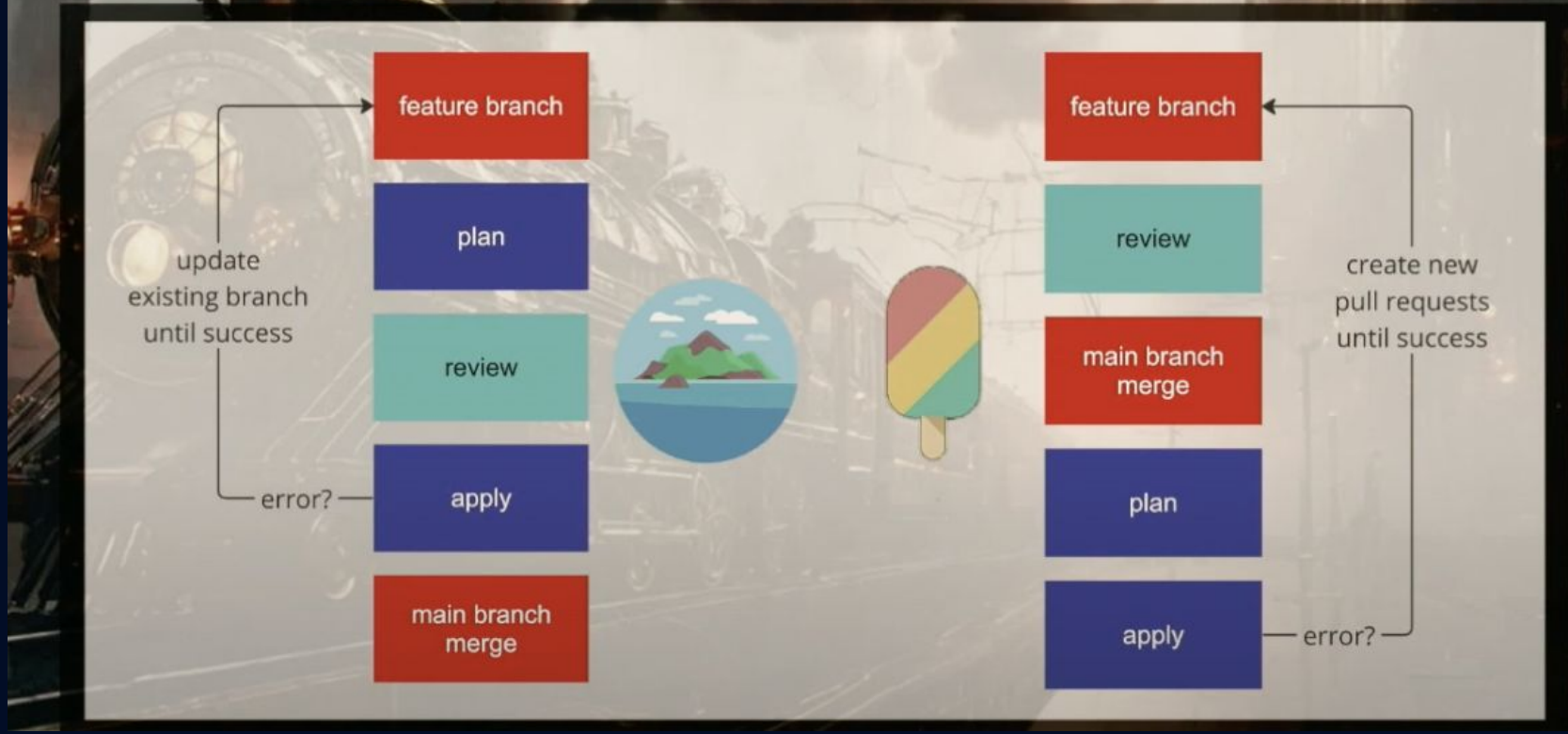
@mcdwayne

4 Principles of GitOps - OpenGitOps.dev

1. Declarative
2. Versioned and Immutable
3. Pulled Automatically
4. Continuously Reconciled

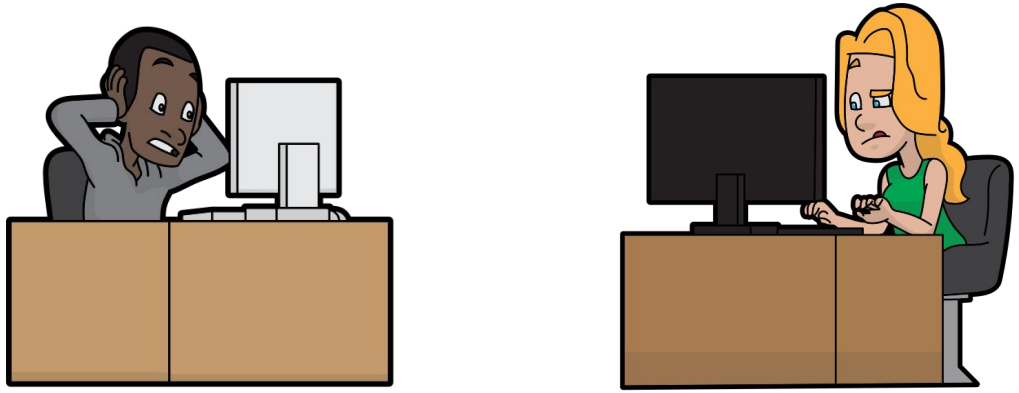
@mcdwayne

IaC vs GitOps Workflows



@mcdwayne

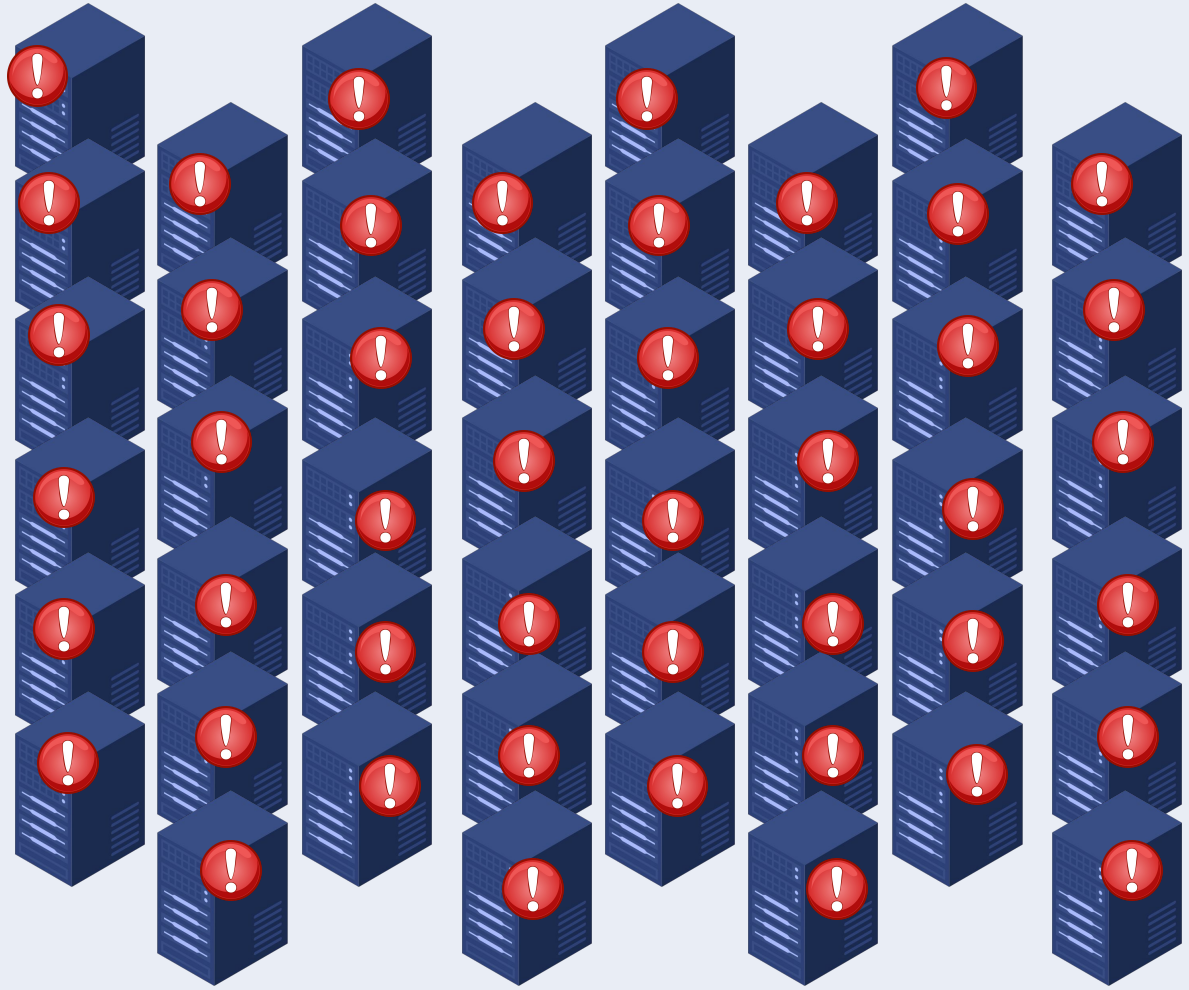
Who is reviewing?



@mcdwayne

In Conclusion

```
Number_of_Servers = 48
# DO NOT Allowed_IPs = /0.
Allowed_Inbound_IPs = /0.
```



Areas Of IaC Security Concerns

1. Misconfigurations
2. Access
3. Governance

Tools can help with Misconfigurations

checkov

KICS by Checkmarx

terrascan by tenable

tfsec

INFRA AS CODE SECURITY

snyk

Keep an eye on who has access

@mcdwayne

Human in the loop? Who is reviewing?

STEP 3 Someone on your team reviews the plan and approves the pull request

alice approved these changes — View changes

STEP 4 You comment 'atlantis apply'

lkysow commented

atlantis apply

STEP 5 Atlantis runs `terraform apply` and comments back on the pull request

atlantisbot commented

Ran Apply in dir: `.` workspace: `default`

```
null_resource.demo: Creating...
null_resource.demo: Creation complete after 0s (ID: 4542221565395344699)

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
```


@mcdwayne

@mcdwayne

Hi. I’m Dwayne.

Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of The Security Repo Podcast
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

@mcdwayne

Security In An IaC Defined World

@mcdwayne
@mcdwayne