Lessons learned from 15 years of DevOps

Paul Stack
10 07 2024

About Me...

- Paul Stack - @stack72 / @stack72.dev
- Former Terraform Engineer
- Former Pulumi Engineer
- Frustrated Infrastructure user
- PM @ System Initiative

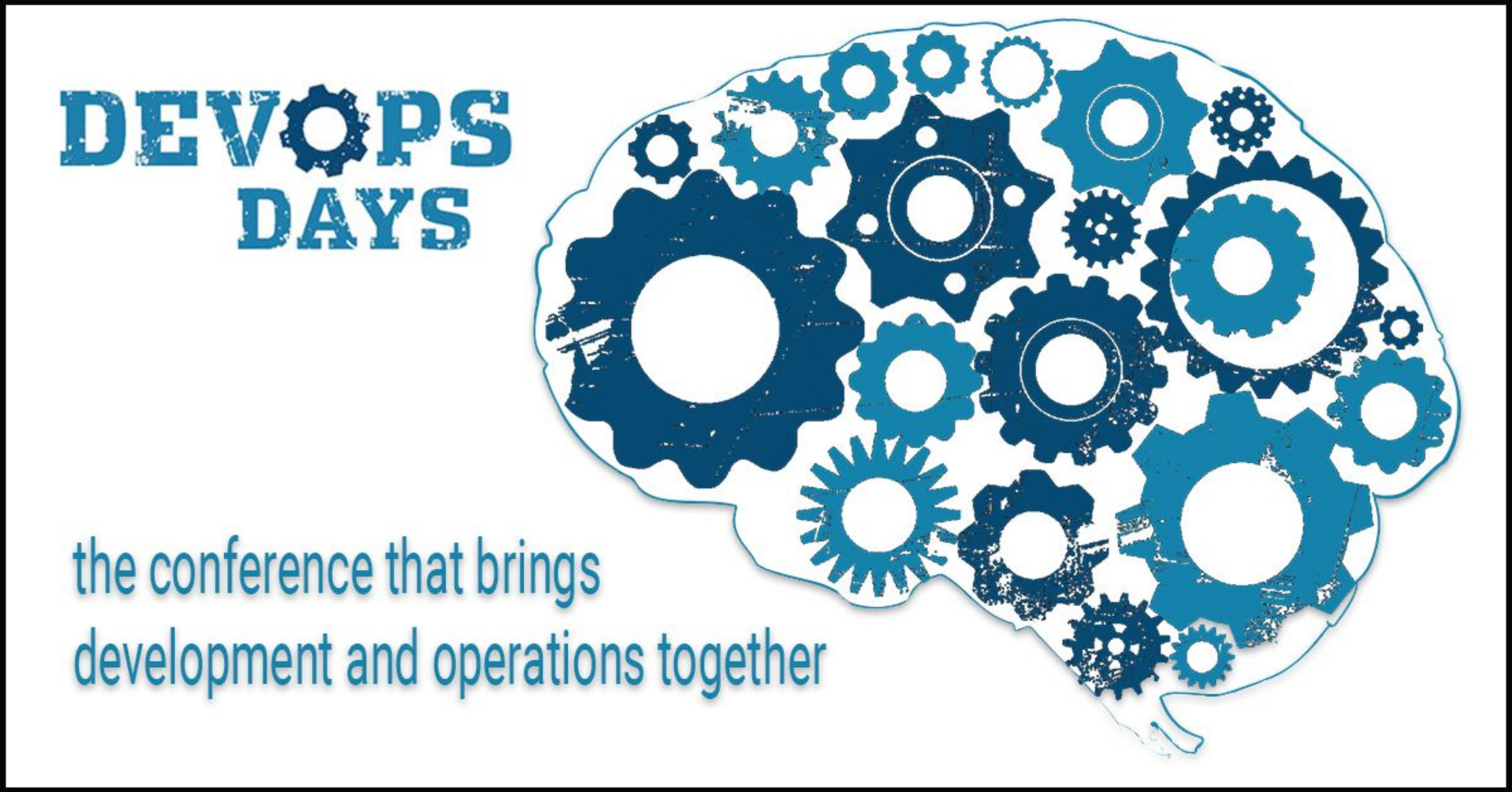
> “Imagine a world where product owners, Development, QA, IT Operations, and Infosec work together, not only to help each other, but also to ensure that the overall organization succeeds. By working toward a common goal, they enable the fast flow of planned work into production (e.g., performing tens, hundreds, or even thousands of code deploys per day), while achieving world-class stability, reliability, availability, and security.”

Kim, Gene, et al.
The DevOps Handbook: how to create world-class agility, reliability, & security in technology organizations.
IT Revolution Press, 2016.

DevOps… is eating the world?

Low Res Image © Ton Hendriks

If you build it, they will come…



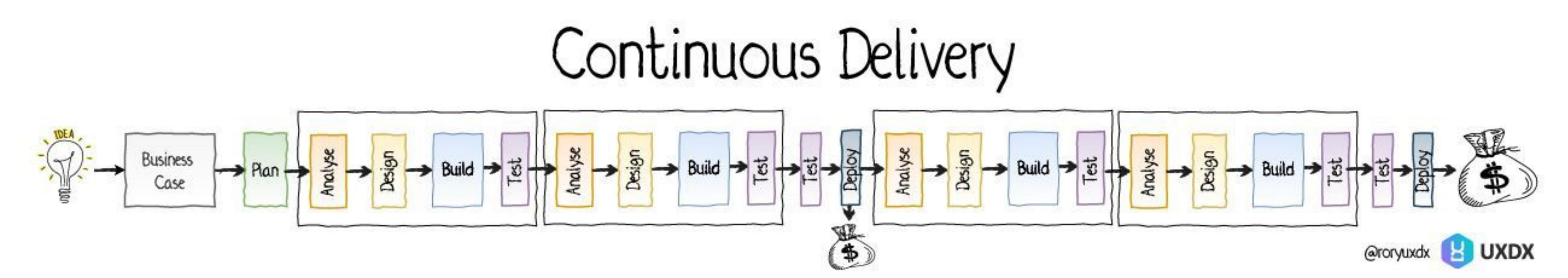
DEVOPS
DAYS
the conference that brings
development and operations together

SYSTEM INITIATIVE

DevOps… as a phenomenon?

Development
Wall of Confusion
Operations

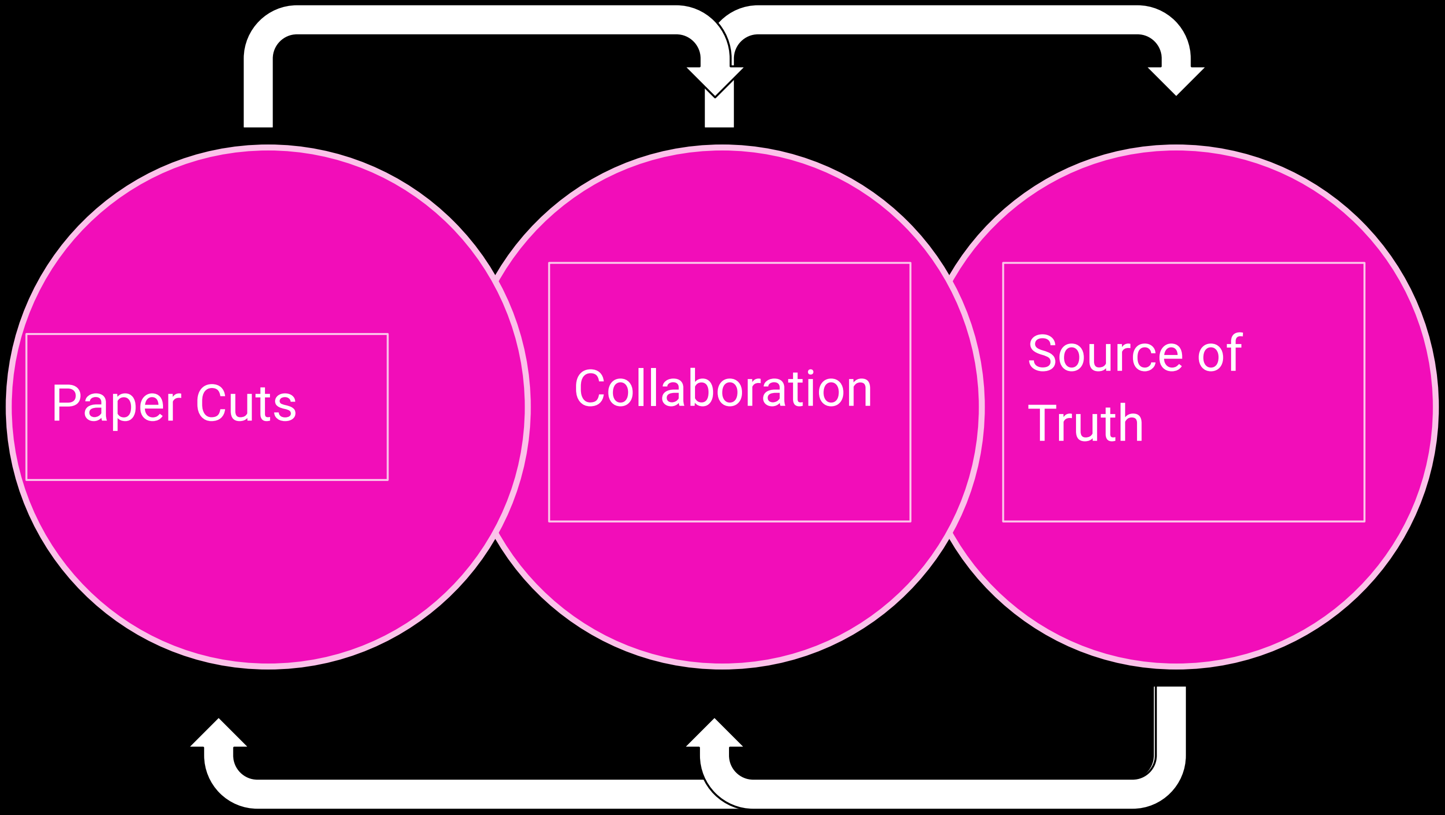
The software delivery pipeline



WE DID IT!
memegenerator.net

FAKE NEWS™

Key Problems

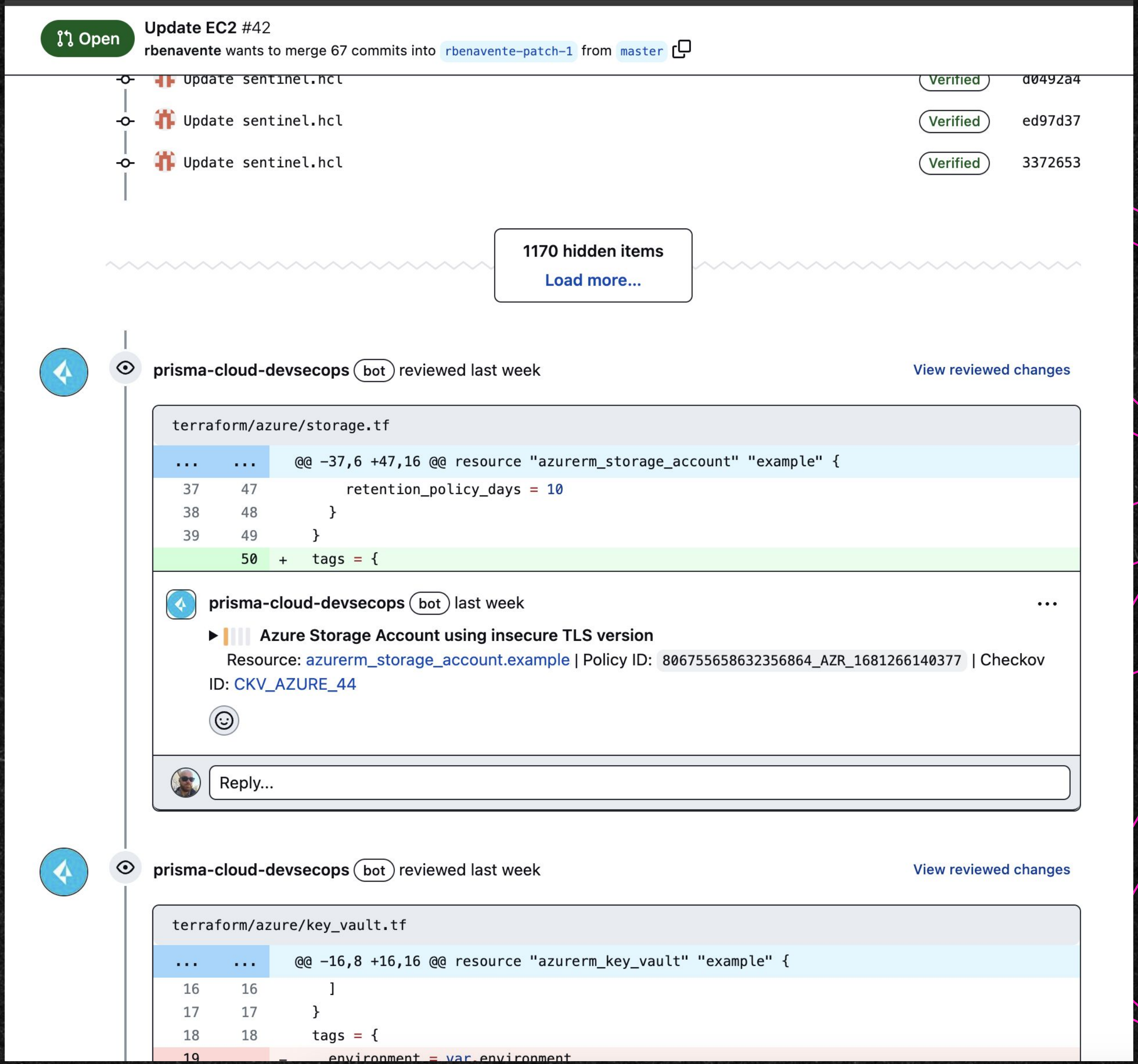


Paper Cuts

Collaboration

Source of Truth

Collaboration… failure?



Open **Update EC2** #42

rbenavente wants to merge 67 commits into `rbenavente-patch-1` from `master`

Update sentinel.hcl — Verified — d0492a4

Update sentinel.hcl — Verified — ed97d37

Update sentinel.hcl — Verified — 3372653

1170 hidden items

Load more...

prisma-cloud-devsecops (bot) reviewed last week — View reviewed changes

terraform/azure/storage.tf

```
@@ -37,6 +47,16 @@ resource "azurerm_storage_account" "example" {
        retention_policy_days = 10
      }
    }
+   tags = {
```

prisma-cloud-devsecops (bot) last week

▶ **Azure Storage Account using insecure TLS version**

Resource: azurerm_storage_account.example | Policy ID: `8067556586323568 64_AZR_1681266140377` | Checkov ID: CKV_AZURE_44

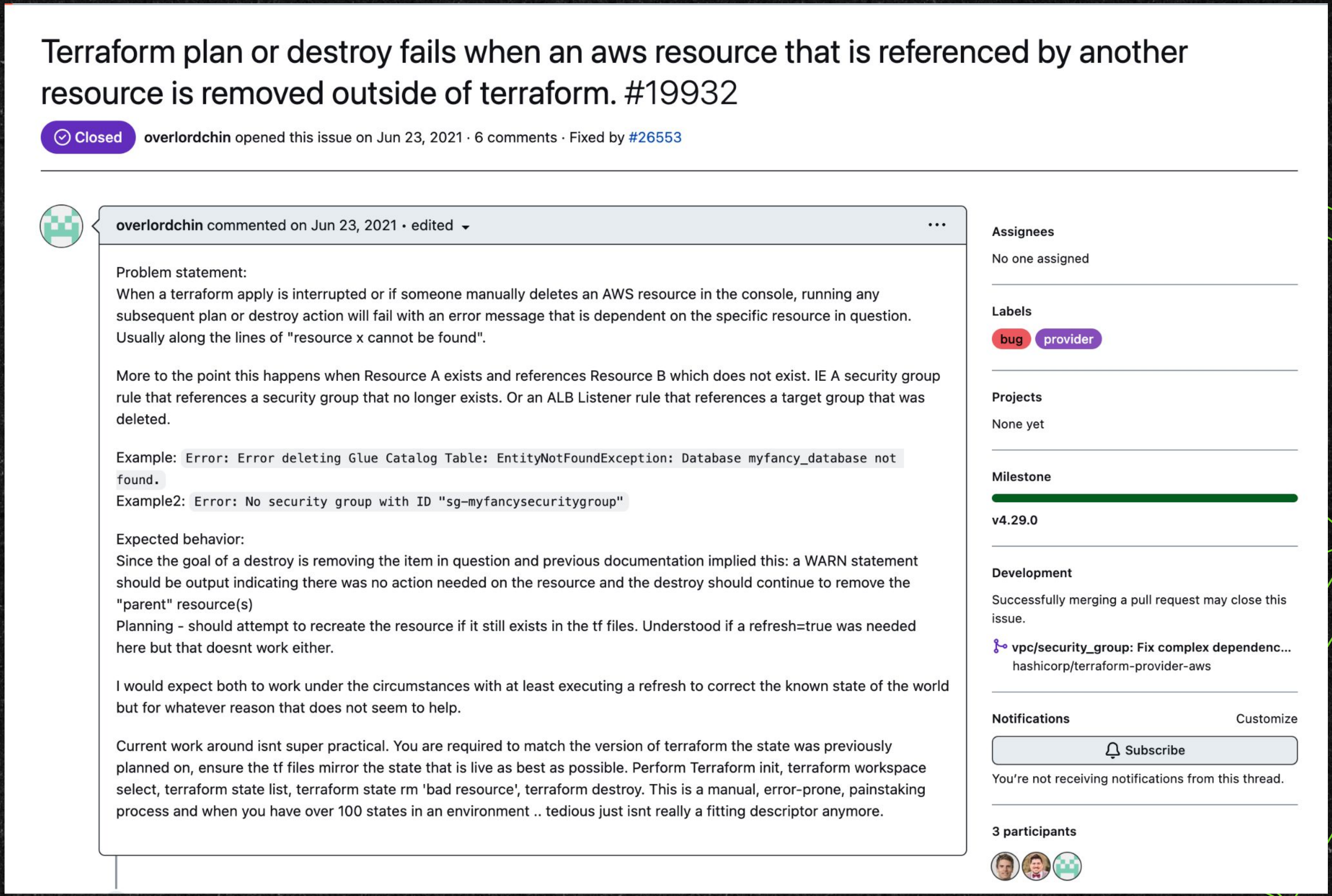
Reply...

prisma-cloud-devsecops (bot) reviewed last week — View reviewed changes

terraform/azure/key_vault.tf

```
@@ -16,8 +16,16 @@ resource "azurerm_key_vault" "example" {
      ]
    }
    tags = {
-     environment = var.environment
```

Source of truth… failure?



Terraform plan or destroy fails when an aws resource that is referenced by another resource is removed outside of terraform. #19932

Closed **overlordchin** opened this issue on Jun 23, 2021 · 6 comments · Fixed by #26553

overlordchin commented on Jun 23, 2021 • edited

Problem statement:
When a terraform apply is interrupted or if someone manually deletes an AWS resource in the console, running any subsequent plan or destroy action will fail with an error message that is dependent on the specific resource in question. Usually along the lines of "resource x cannot be found".

More to the point this happens when Resource A exists and references Resource B which does not exist. IE A security group rule that references a security group that no longer exists. Or an ALB Listener rule that references a target group that was deleted.

Example: `Error: Error deleting Glue Catalog Table: EntityNotFoundException: Database myfancy_database not found.`
Example2: `Error: No security group with ID "sg-myfancysecuritygroup"`

Expected behavior:
Since the goal of a destroy is removing the item in question and previous documentation implied this: a WARN statement should be output indicating there was no action needed on the resource and the destroy should continue to remove the "parent" resource(s)
Planning - should attempt to recreate the resource if it still exists in the tf files. Understood if a refresh=true was needed here but that doesnt work either.

I would expect both to work under the circumstances with at least executing a refresh to correct the known state of the world but for whatever reason that does not seem to help.

Current work around isnt super practical. You are required to match the version of terraform the state was previously planned on, ensure the tf files mirror the state that is live as best as possible. Perform Terraform init, terraform workspace select, terraform state list, terraform state rm 'bad resource', terraform destroy. This is a manual, error-prone, painstaking process and when you have over 100 states in an environment .. tedious just isnt really a fitting descriptor anymore.

Assignees
No one assigned

Labels
bug provider

Projects
None yet

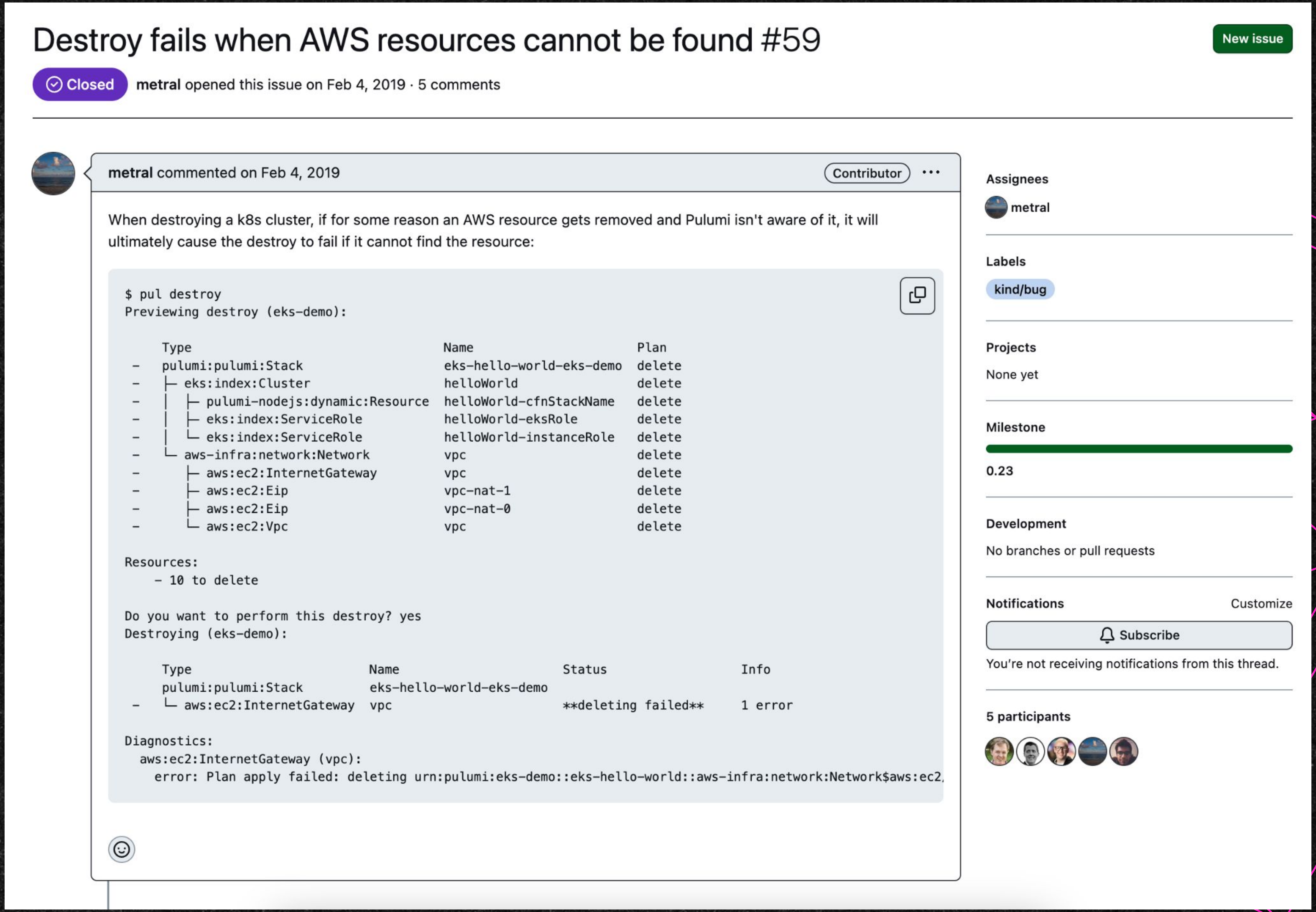
Milestone
v4.29.0

Development
Successfully merging a pull request may close this issue.
vpc/security_group: Fix complex dependenc...
hashicorp/terraform-provider-aws

Notifications Customize
Subscribe
You're not receiving notifications from this thread.

3 participants

Source of truth… failure?



Destroy fails when AWS resources cannot be found #59

New issue

Closed **metral** opened this issue on Feb 4, 2019 · 5 comments

metral commented on Feb 4, 2019 Contributor ···

When destroying a k8s cluster, if for some reason an AWS resource gets removed and Pulumi isn't aware of it, it will ultimately cause the destroy to fail if it cannot find the resource:

```
$ pul destroy
Previewing destroy (eks-demo):

     Type                                 Name                       Plan
 -   pulumi:pulumi:Stack                  eks-hello-world-eks-demo   delete
 -   ├─ eks:index:Cluster                 helloWorld                 delete
 -   │  ├─ pulumi-nodejs:dynamic:Resource helloWorld-cfnStackName    delete
 -   │  ├─ eks:index:ServiceRole          helloWorld-eksRole         delete
 -   │  └─ eks:index:ServiceRole          helloWorld-instanceRole    delete
 -   └─ aws-infra:network:Network         vpc                        delete
 -      ├─ aws:ec2:InternetGateway        vpc                        delete
 -      ├─ aws:ec2:Eip                    vpc-nat-1                  delete
 -      ├─ aws:ec2:Eip                    vpc-nat-0                  delete
 -      └─ aws:ec2:Vpc                    vpc                        delete

Resources:
    - 10 to delete

Do you want to perform this destroy? yes
Destroying (eks-demo):

     Type                       Name                       Status                 Info
     pulumi:pulumi:Stack        eks-hello-world-eks-demo
 -   └─ aws:ec2:InternetGateway vpc                        **deleting failed**    1 error

Diagnostics:
  aws:ec2:InternetGateway (vpc):
    error: Plan apply failed: deleting urn:pulumi:eks-demo::eks-hello-world::aws-infra:network:Network$aws:ec2,
```

Assignees

metral

Labels

kind/bug

Projects

None yet

Milestone

0.23

Development

No branches or pull requests

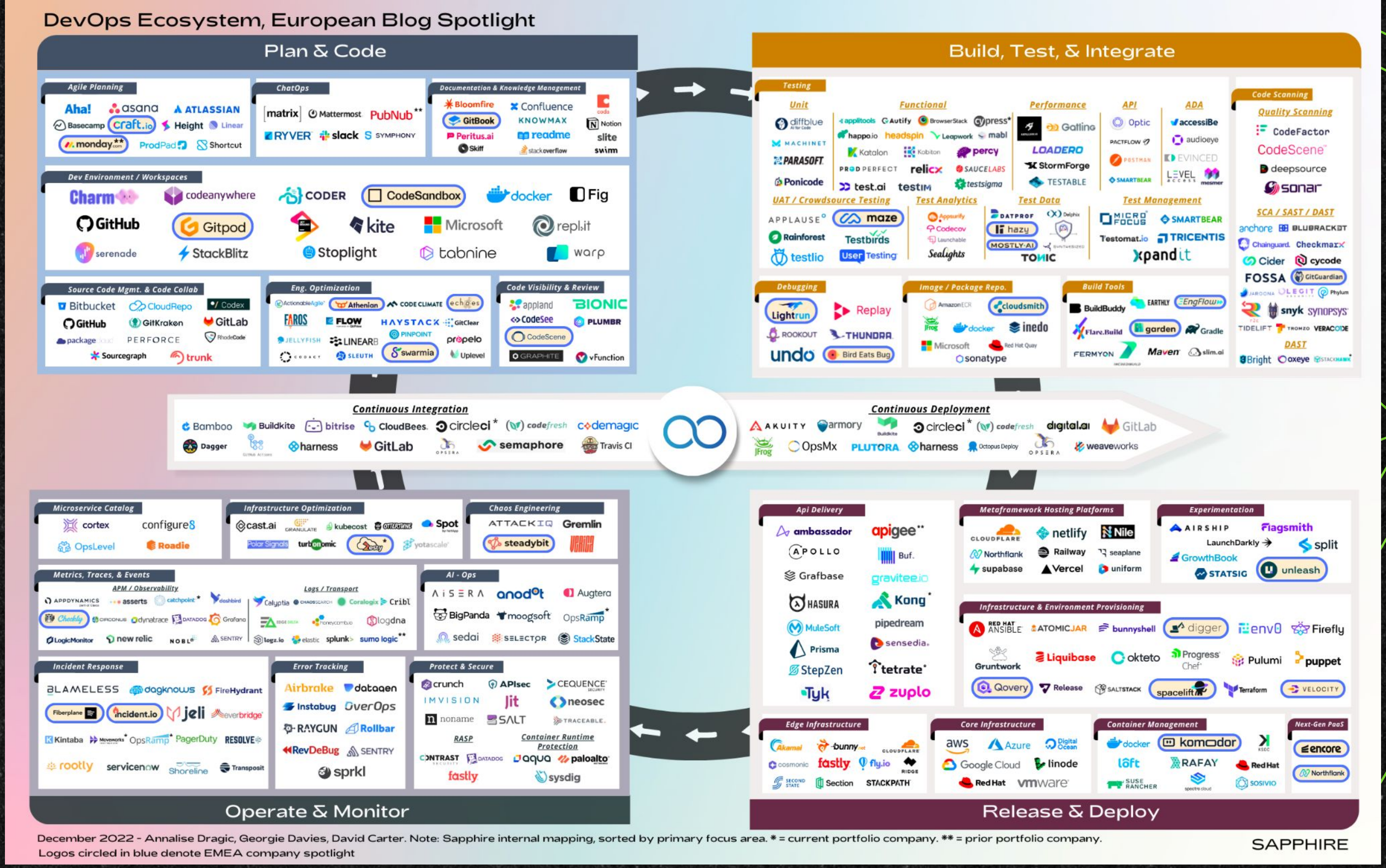
Notifications Customize

Subscribe

You're not receiving notifications from this thread.

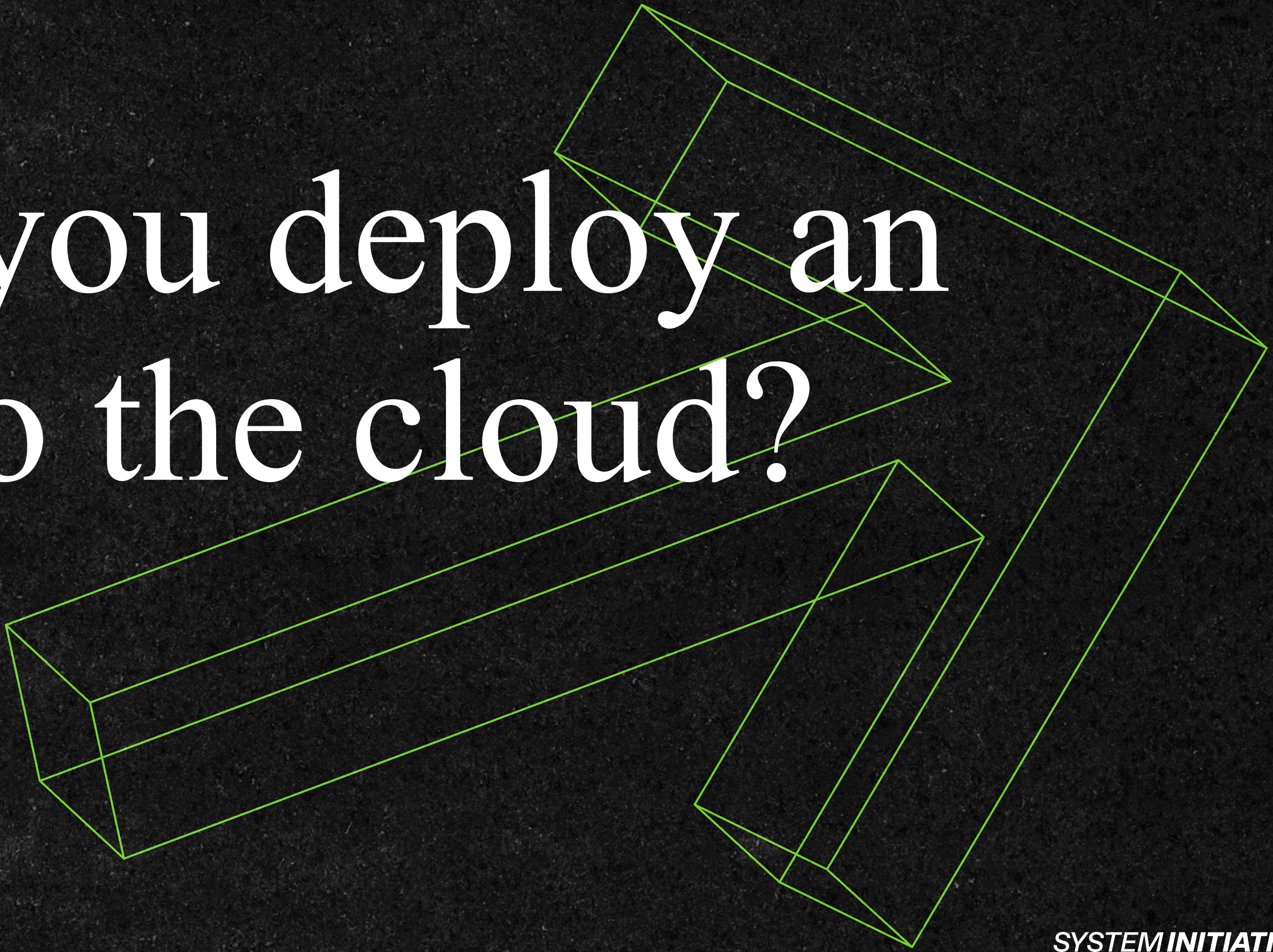
5 participants

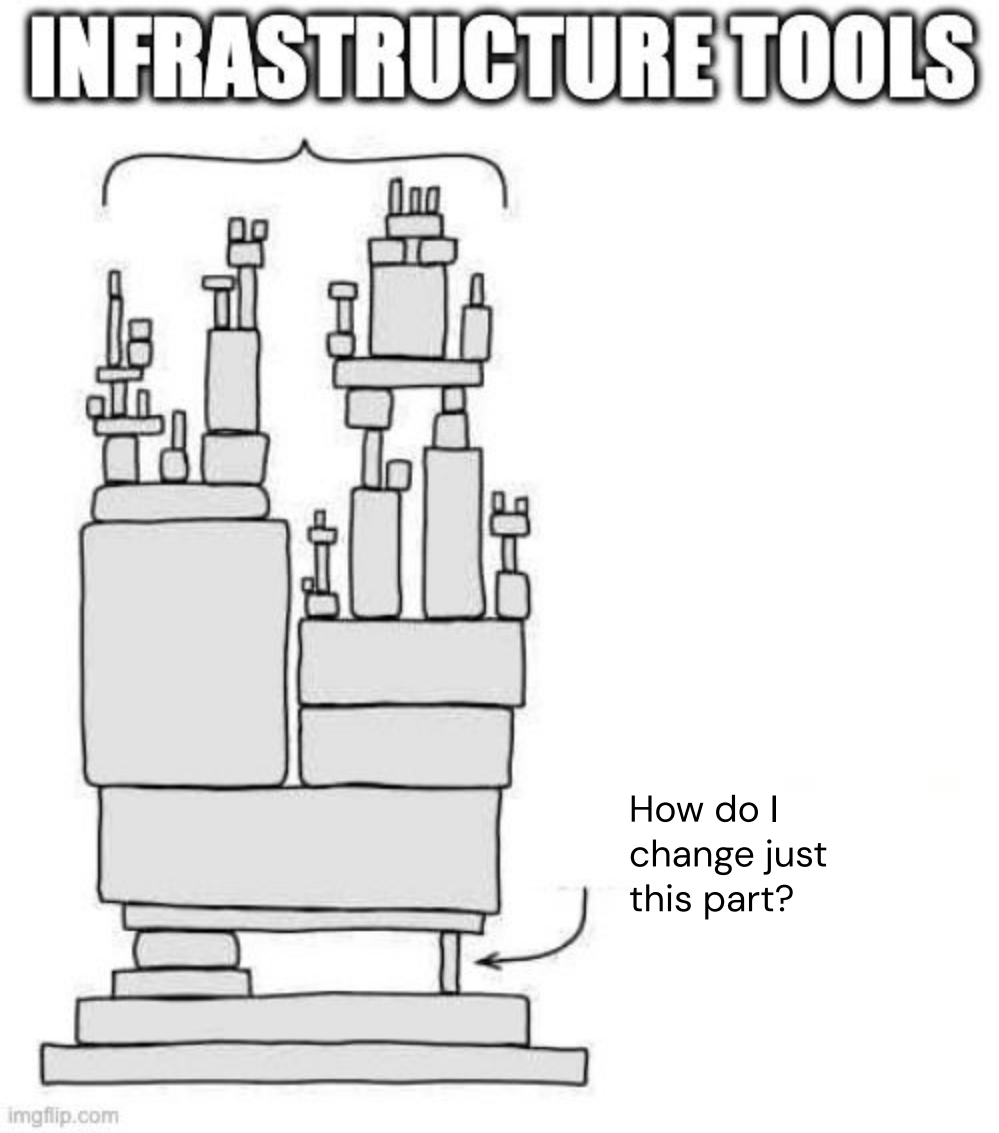
And so there was an opportunity…

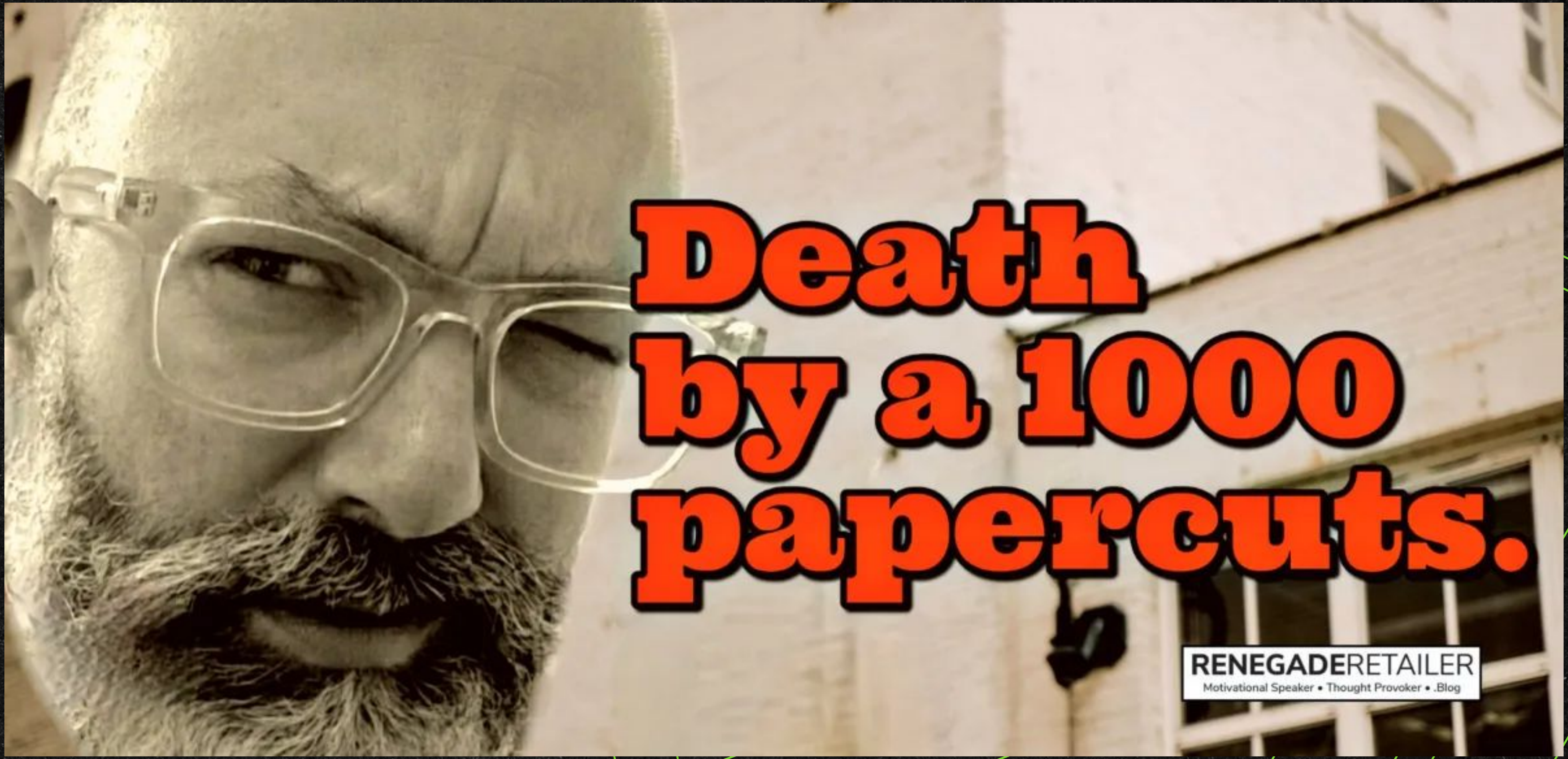


December 2022 - Annalise Dragic, Georgie Davies, David Carter. Note: Sapphire internal mapping, sorted by primary focus area. * = current portfolio company. ** = prior portfolio company.
Logos circled in blue denote EMEA company spotlight

How would you deploy an application to the cloud?



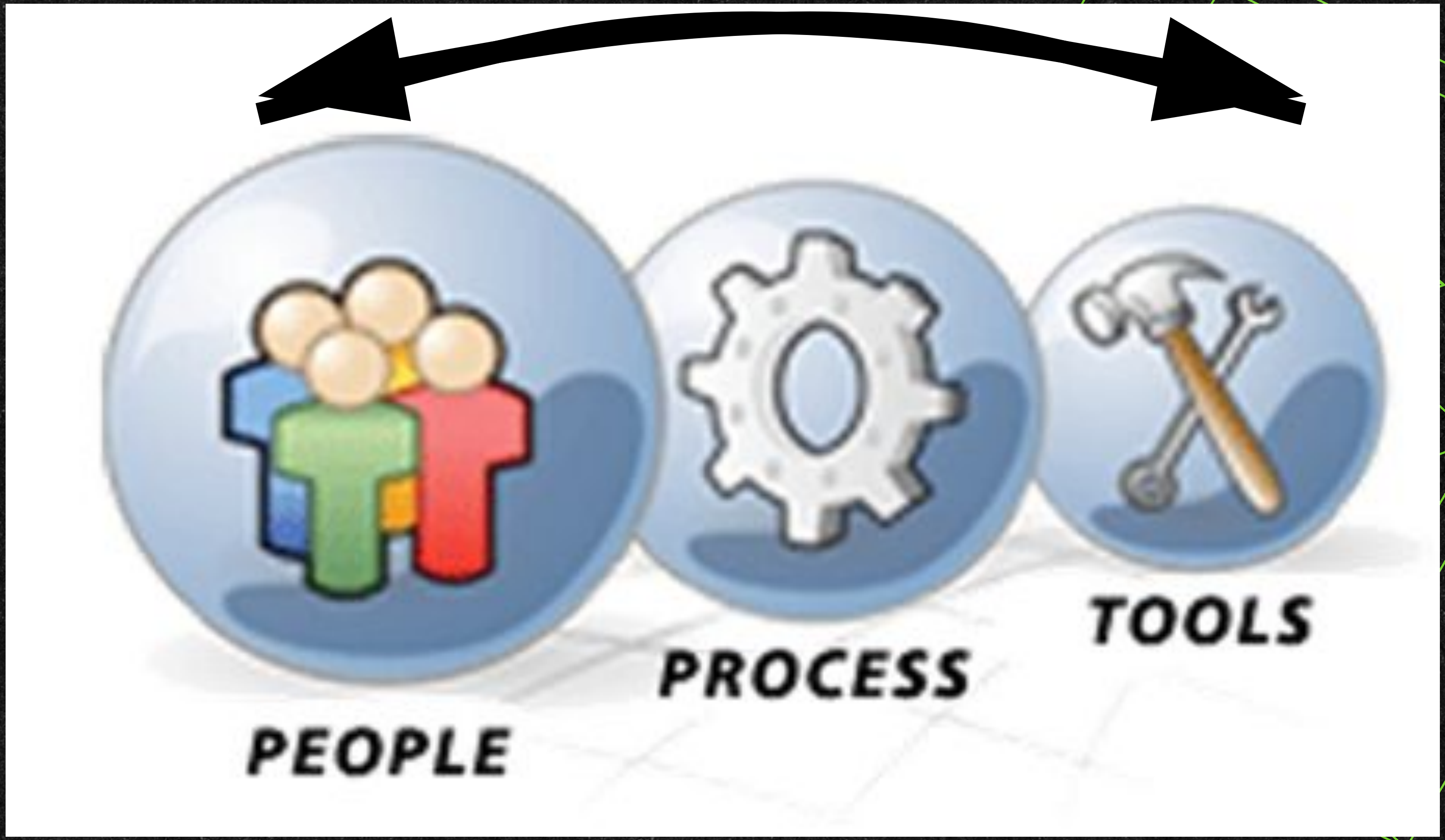

INFRASTRUCTURE TOOLS
How do I change just this part?
imgflip.com



Death by a 1000 papercuts.
RENEGADERETAILER
Motivational Speaker • Thought Provoker • .Blog

WHAT ABOUT THE SECURITY?
imgflip.com

We got things wrong…



The evolution of our existing tooling

CF Engine

Puppet

Chef

SaltStack

CloudFormation

Ansible

Terraform

Google Deployment Manager

ARM Templates

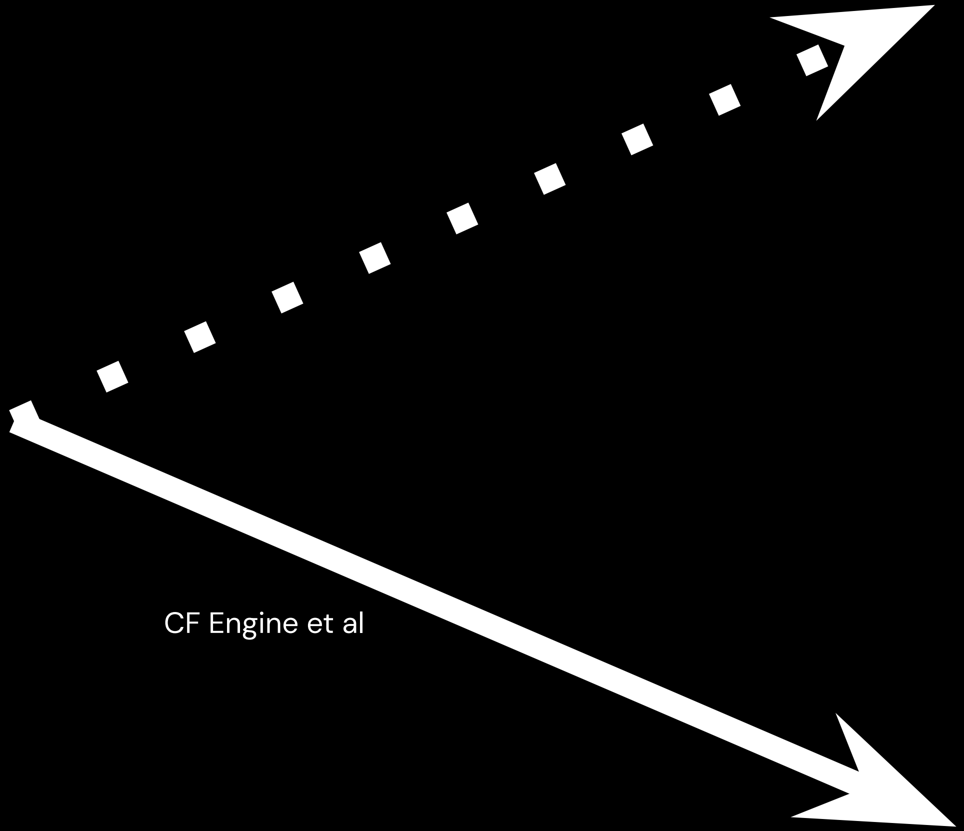
Pulumi

AWS CDK

tfCDK

Bicep

Do we have the ability to create a new paradigm?



CF Engine et al

So what’s next?

The Second Wave of DevOps!

Klotho

shuttle

Welcome to Pulumi AI.

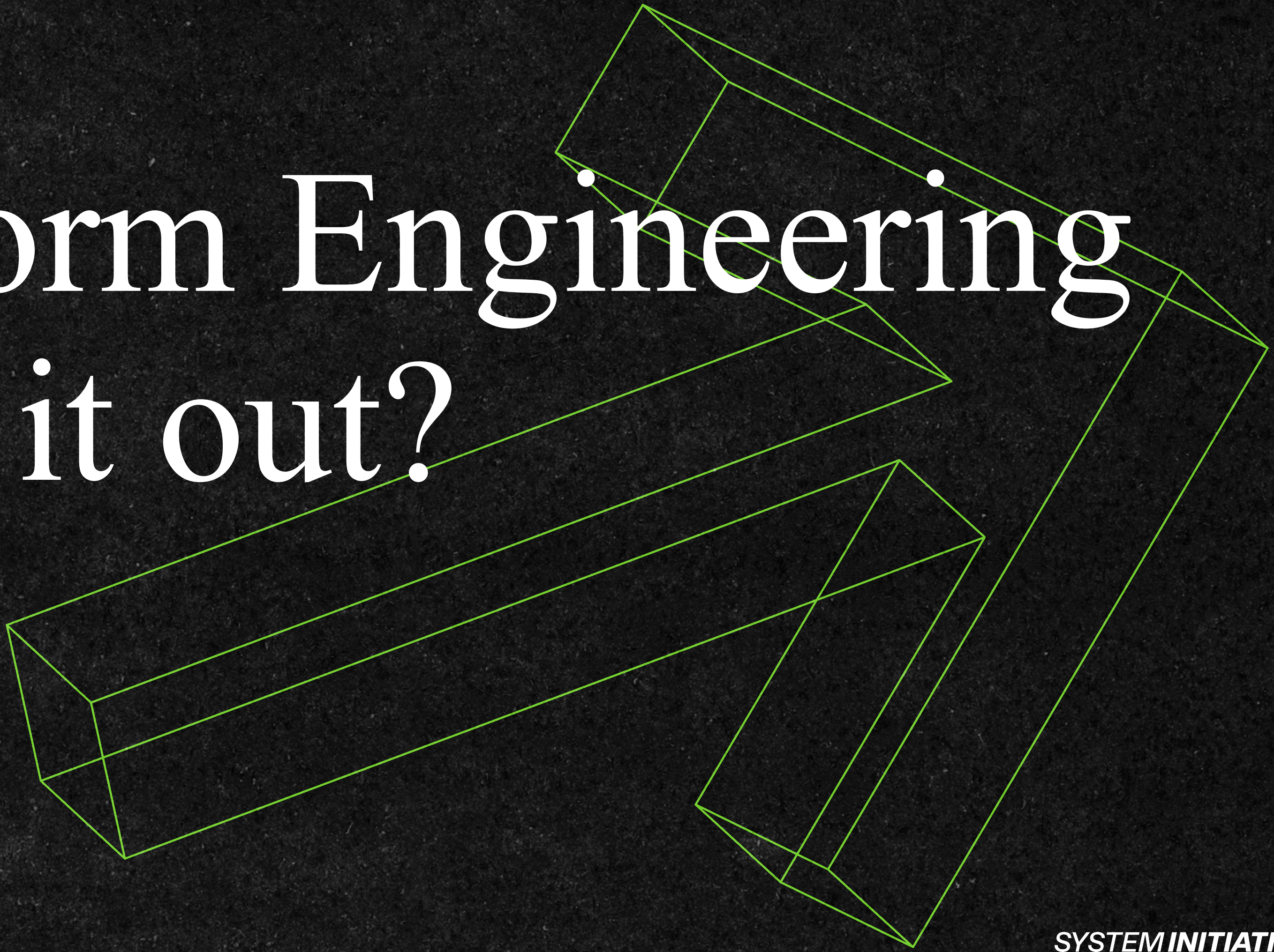
Pulumi AI

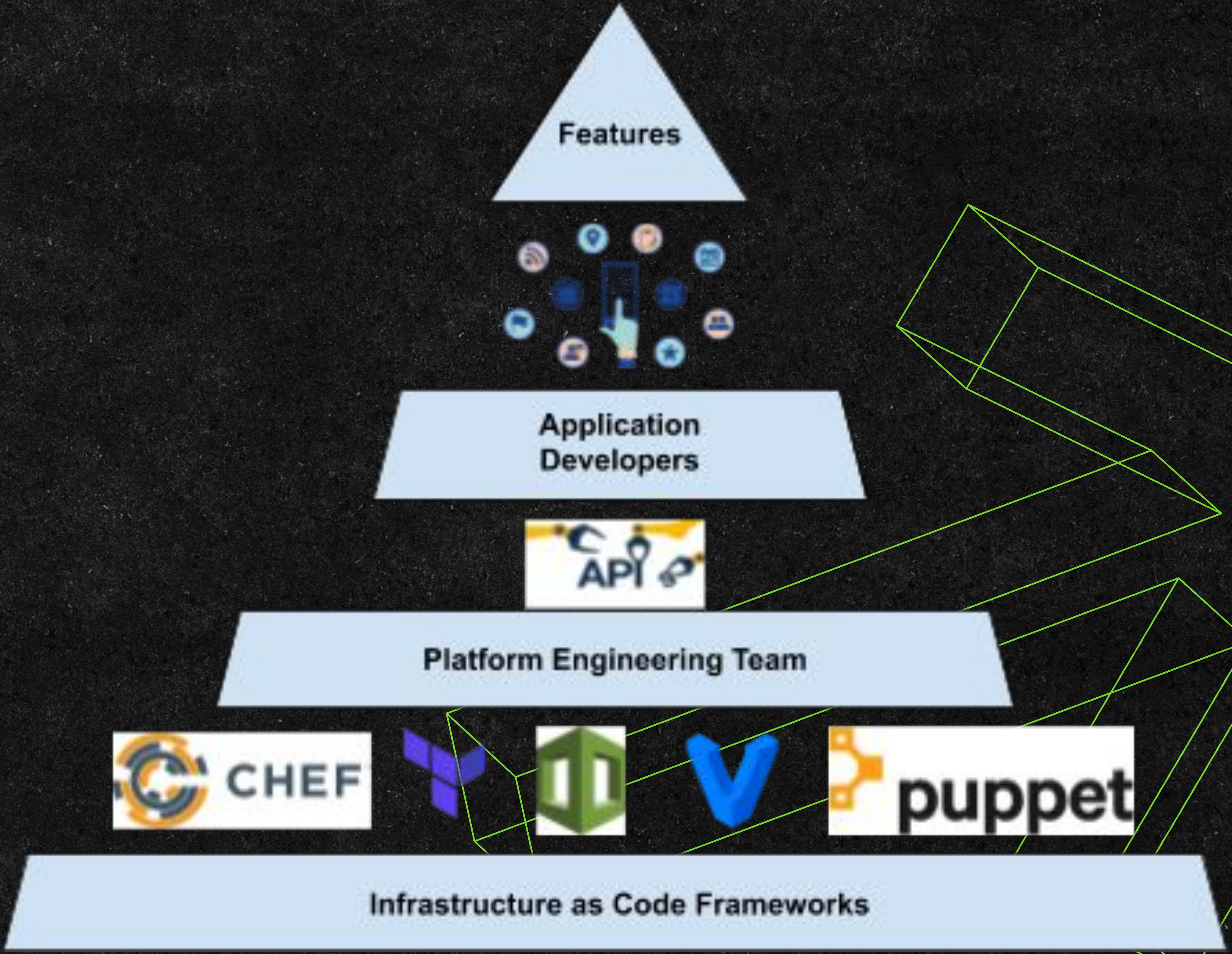
Your new assistant

Pulumi AI

Try the CLI

Maybe Platform Engineering have figured it out?





Features

Application Developers

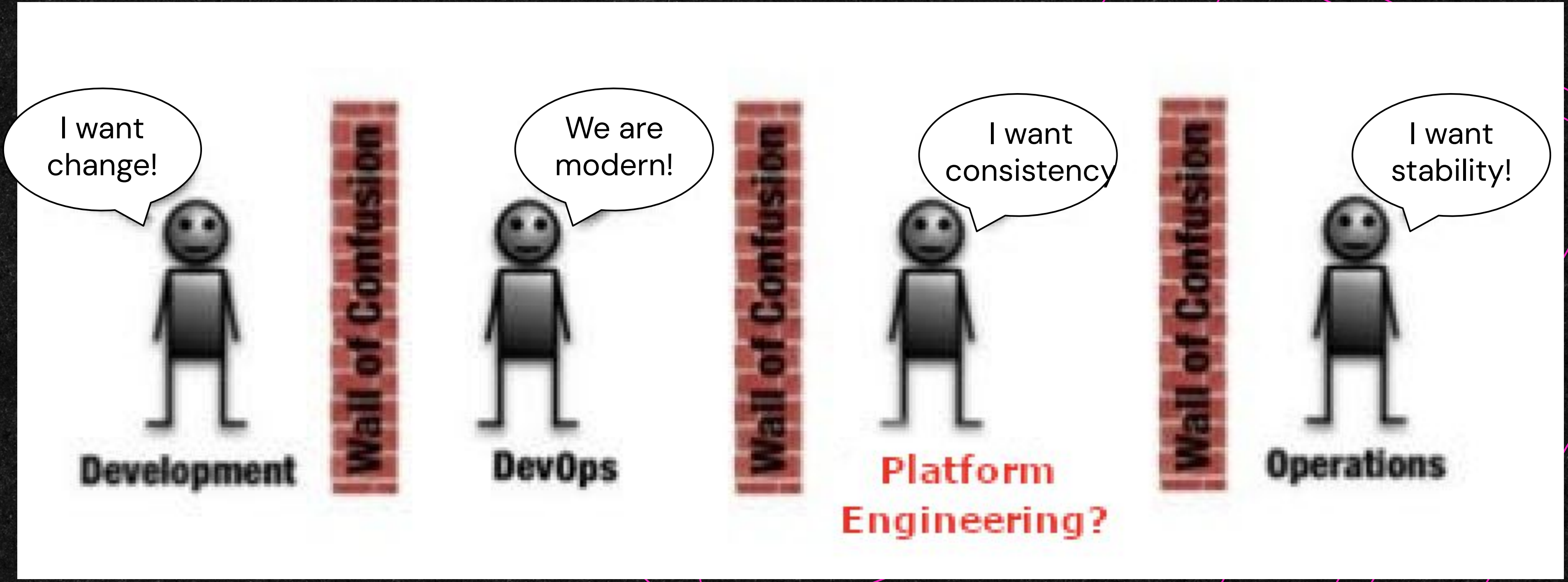
Platform Engineering Team

Infrastructure as Code Frameworks

HOT
TAKE
HOUSE
OPEN
24
HOURS

So… how's that working out for them?

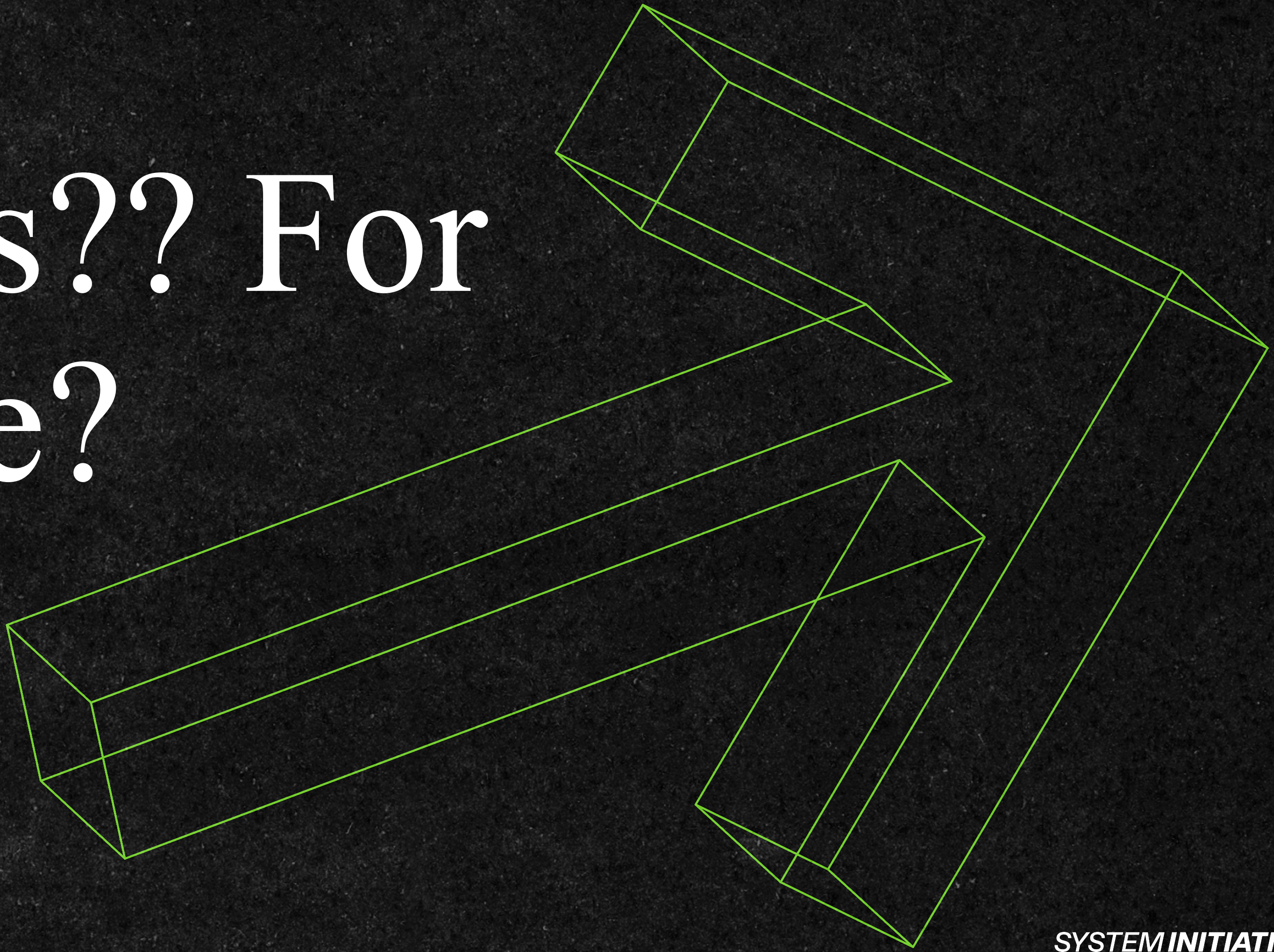
- Rising organizational silos and decreasing collaboration



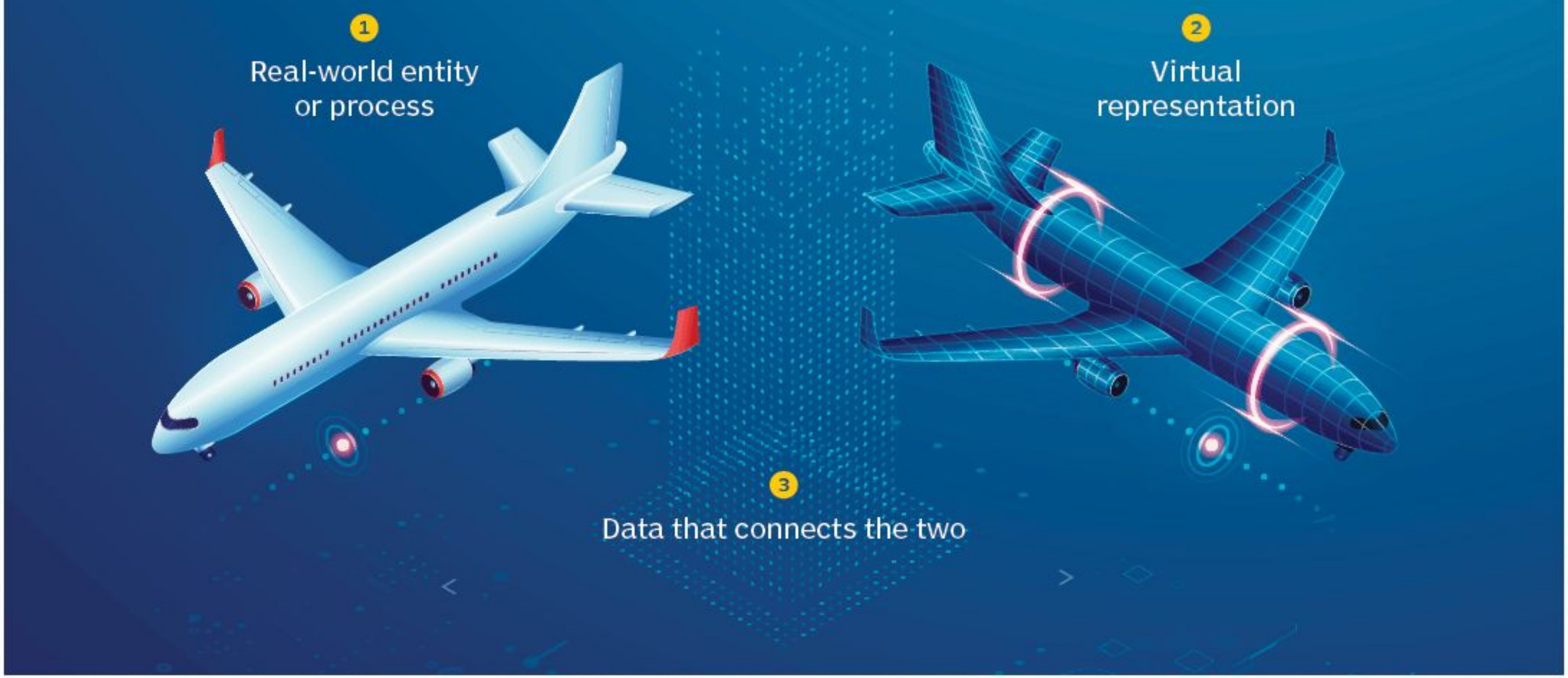
> “Rules direct us to average behaviors. If we’re aiming to create works that are exceptional, most rules don’t apply. Average is nothing to aspire to.”
>
> \- Rick Rubin

System Initiative is a real time, multiplayer, multi-modal reinvention of DevOps tooling

Digital Twins?? For Infrastructure?



The three elements of a digital twin



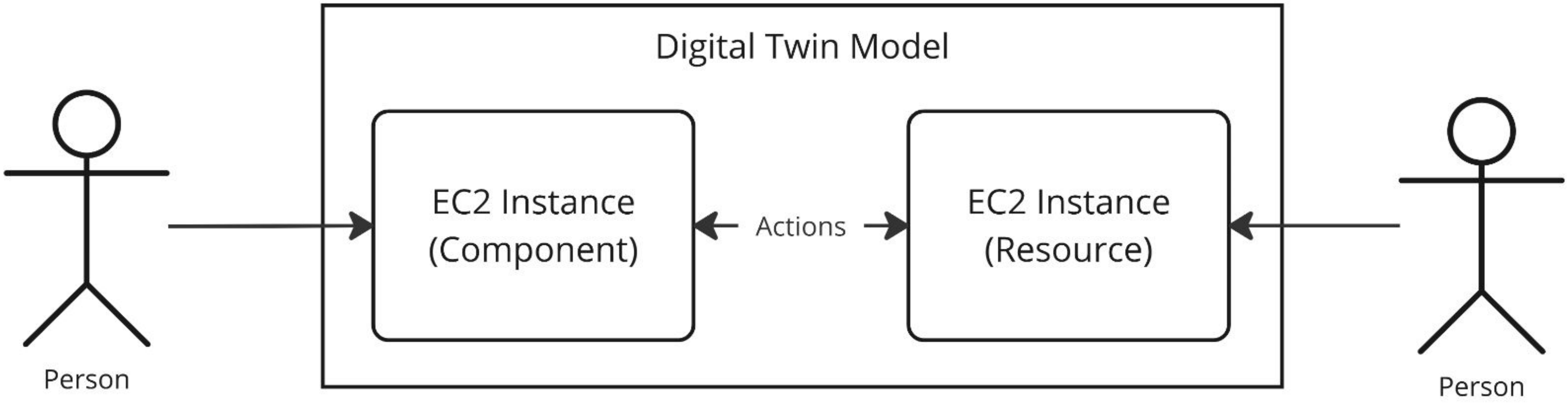
1 Real-world entity or process

2 Virtual representation

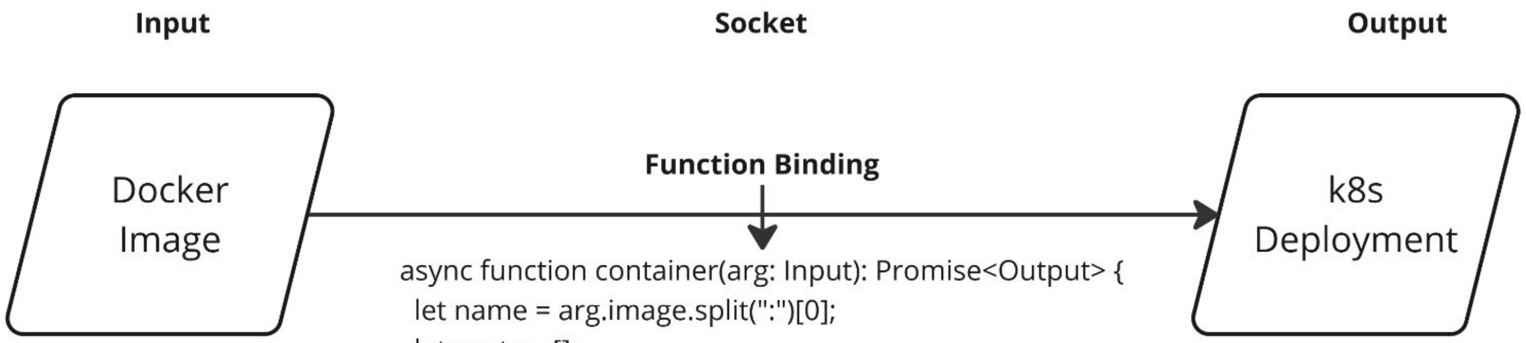
3 Data that connects the two

DESIGN: LINDA KOURY; IMAGE: JACKIE NIAM/ADOBE STOCK

Digital Twins



Hypergraph of Functions



```
{
  image: "nginx:1.14.2",
  ExposedPorts: [
    "80/tcp",
  ]
}
```

```
async function container(arg: Input): Promise<Output> {
  let name = arg.image.split(":")[0];
  let ports = [];
  for (port of arg.ExposedPorts) {
    let port_parts = port.split("/");
    ports.push({
      containerPort: port_parts[0],
      protocol: port_parts[1].toUpperCase(),
    });
  }
  return {
    name,
    image: arg.image,
    ports,
  }
}
```

```
spec:
    containers:
    - name: nginx
      image: nginx:1.14.2
      ports:
      - containerPort: 80
```

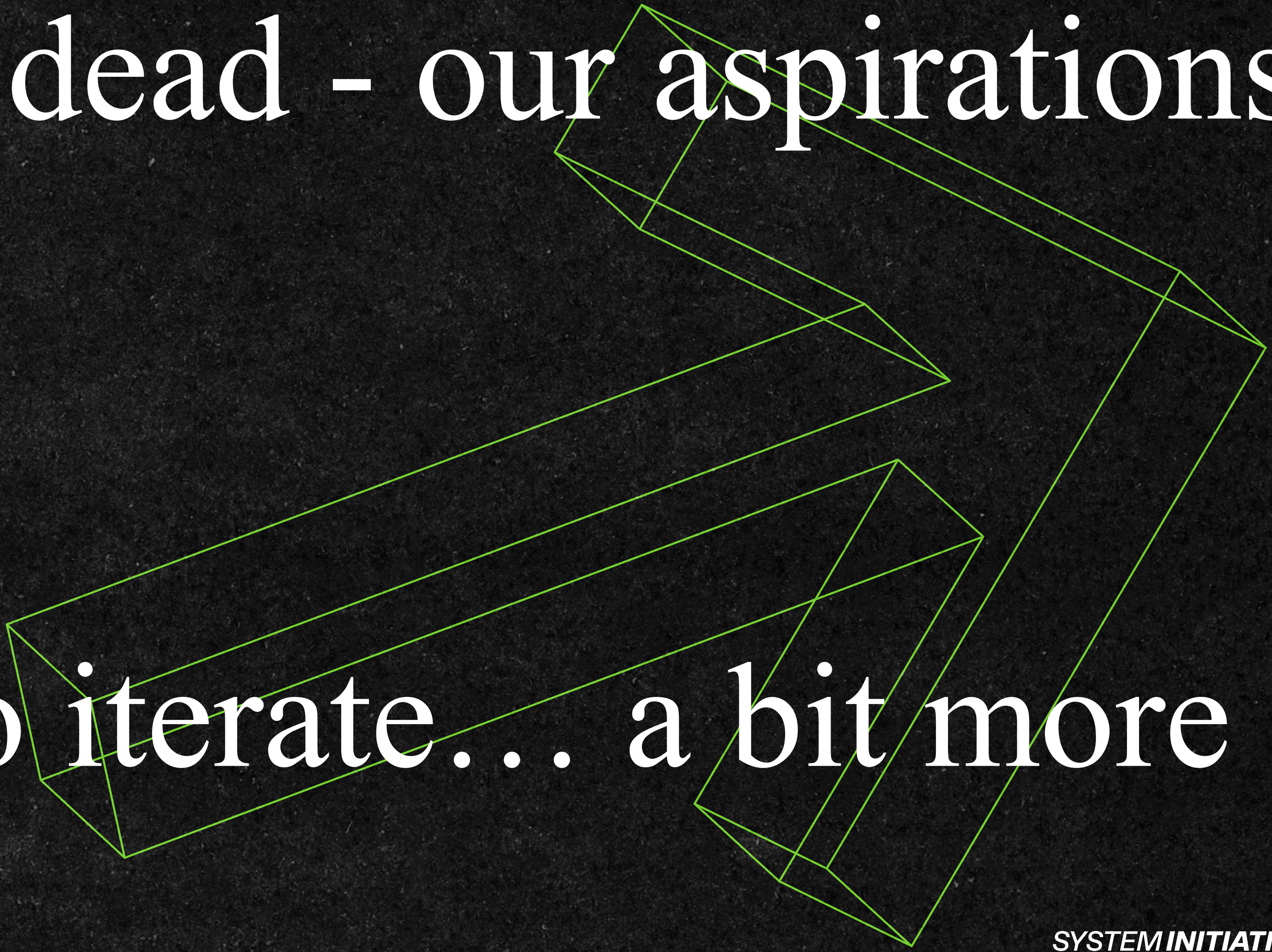
Remember…

- DevOps was designed to focus on delivery
- The second wave of DevOps is trying to
    - Facilitate collaboration
    - Understanding the real time implication of changes
    - Be infinitely extensible

> “Until your pretty code is in production, making money, you’ve just wasted your time…”
>
> Chris Read
> A long time ago on twitter

DevOps is not dead - our aspirations were correct!

We just need to iterate… a bit more



“Imagine a world where product owners, Development, QA, IT Operations, and Infosec work together, not only to help each other, but also to ensure that the overall organization succeeds. By working toward a common goal, they enable the fast flow of ~~planned~~ work into production (e.g., performing tens, hundreds, or even thousands of ~~code~~ Changes per day), while achieving world-class stability, reliability, availability, and security.”

Kim, Gene, et al.
The DevOps Handbook: how to create world-class agility, reliability, & security in technology organizations.
IT Revolution Press, 2016.

If we want that world, we have to challenge our beliefs, break some rules, think differently, and act differently

THANK YOU

systeminit.com
stack72@systeminit.com