

Putting the **Sec** in Dev**Sec**Ops

Automating cloud security as an enabler

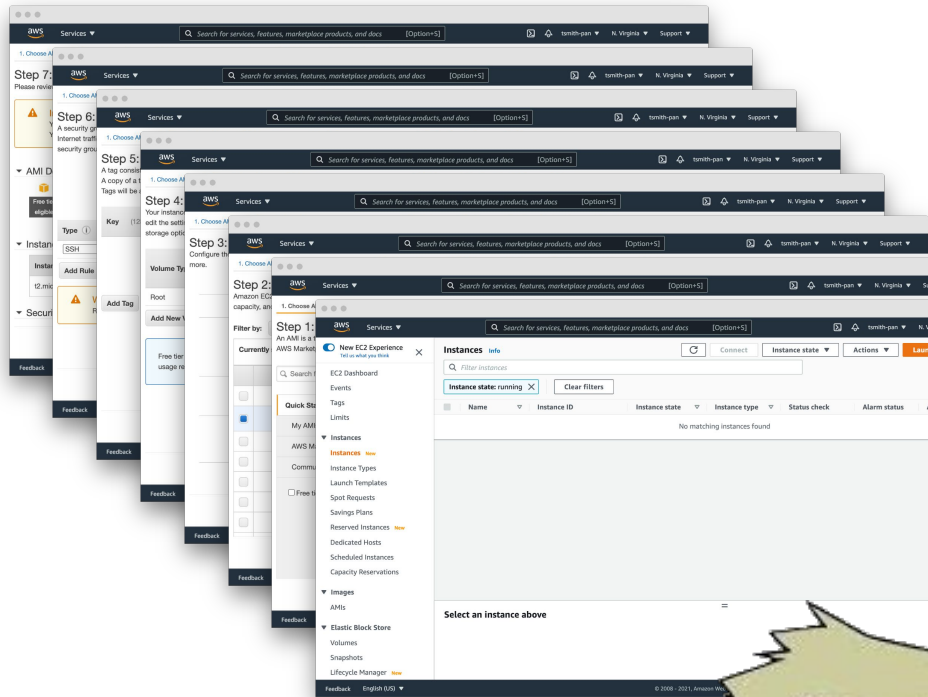
Agenda

- Intro to infrastructure as code (IaC)
- Problems facing DevOps & security teams
- Sources of misconfigurations and cloud risk
- Tools to help with IaC security challenges and education
- Addressing cloud security throughout the DevOps lifecycle
- Strategy to implement a DevSecOps strategy

Cloud-native technology (and security) is evolving



Infrastructure as code
makes DevSecOps
possible for cloud
infrastructure



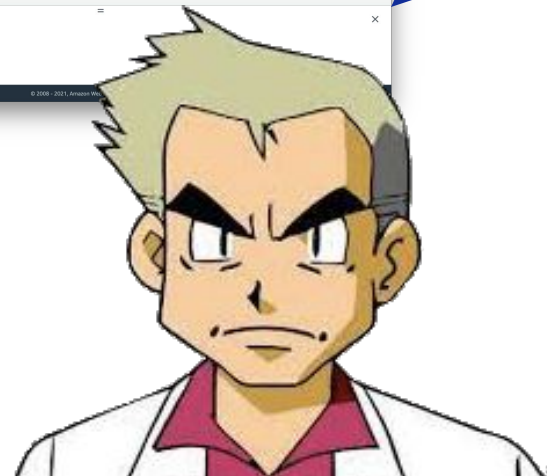
What about

- Readability?
- Debugging?
- Reusability?
- Collaboration?
- Versioning?
- Security?

```
security-group --group-name my-sg  
security group"
```

```
security-group-ingress --group-id  
tcp --port 22 --cidr 0.0.0.0/0
```

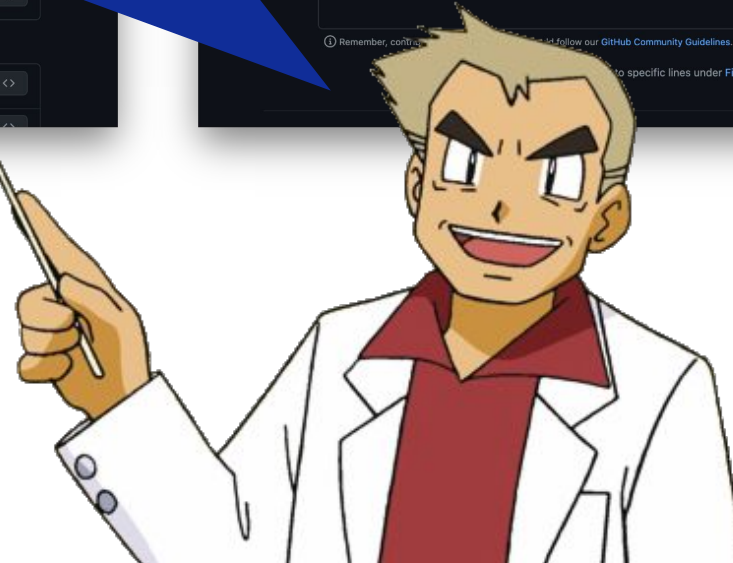
```
--image-id ami-xxxxxxx --count 1  
--key-name MyKeyPair  
--subnet-id sg-903004f8
```



```
resource "aws_security_group" "my-sg" {
  name      = "my-sg"
  ingress {
    from_port = 22
    to_port   = 2
    protocol  = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
}

resource "aws_instance" "web-server" {
  ami              = "ami-0885b1f6bd170450c"
  instance_type    = "t2.micro"
  vpc_security_group_ids = [aws_security_group.my-sg.id]
}
```

Better, but we're still missing **security**



Scanned Helm charts by compliance



Scanned Terraform modules by compliance



What are some examples of misconfigurations?



Unencrypted
databases

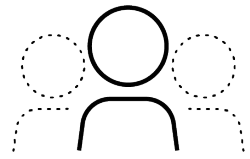


Disabled
logging



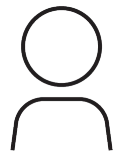
Insecure
protocols

Security isn't happy

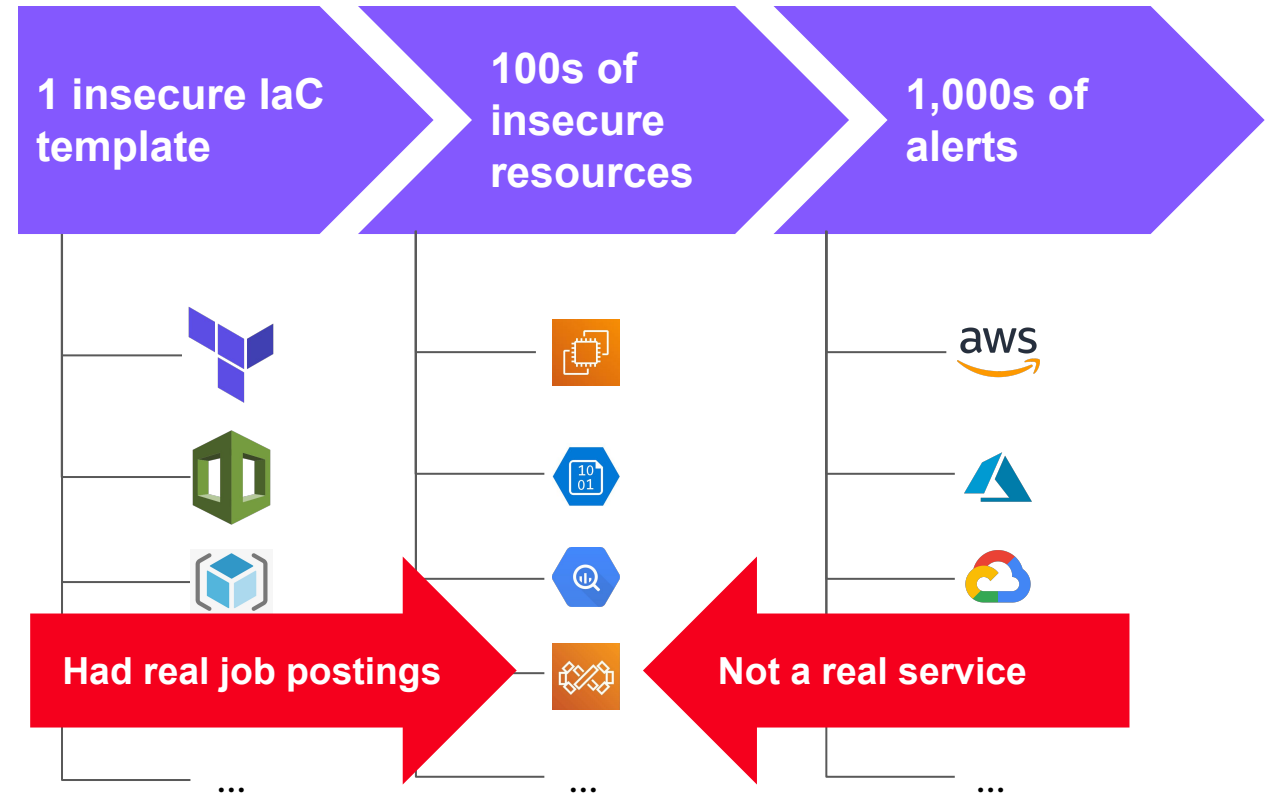


~9 Devs

:



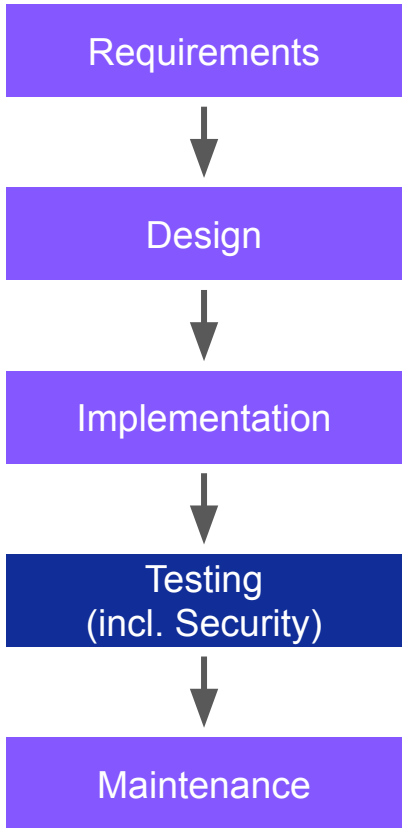
1 Sec



Engineering isn't happy

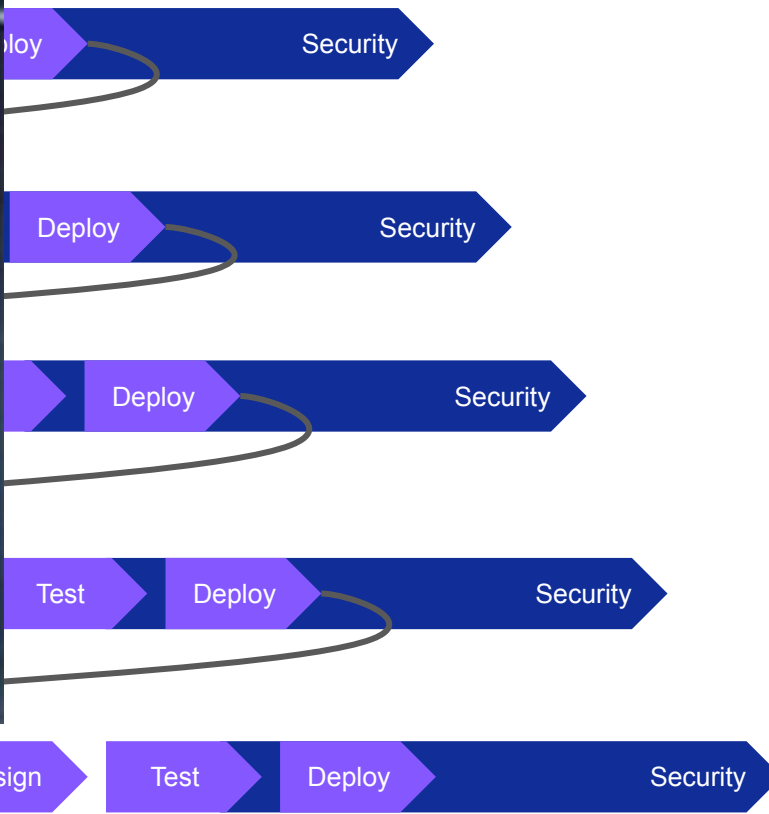
YOU WANT ME TO PATCH CODE

Waterfall



imgflip.com

FROM HOW MANY SPRINTS AGO?



263 Pages of just text

CIS Kubernetes Benchmark

v1.6.1 - 10-01-2020

Responsibilities are at odds and shifting



DevOps moves
faster and is
more agile

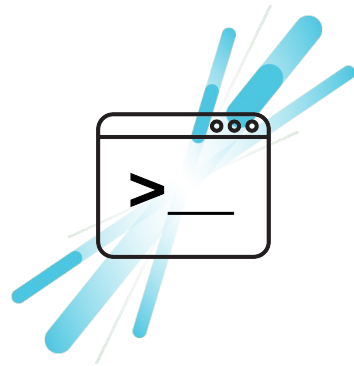


Traditional security
lags and doesn't
scale

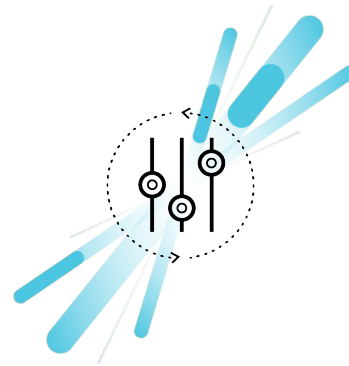


Shifting security
left is hard and
risky

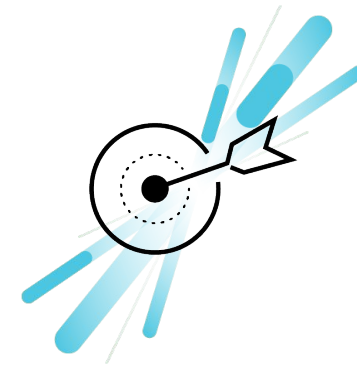
The key to developer-first security



Codified

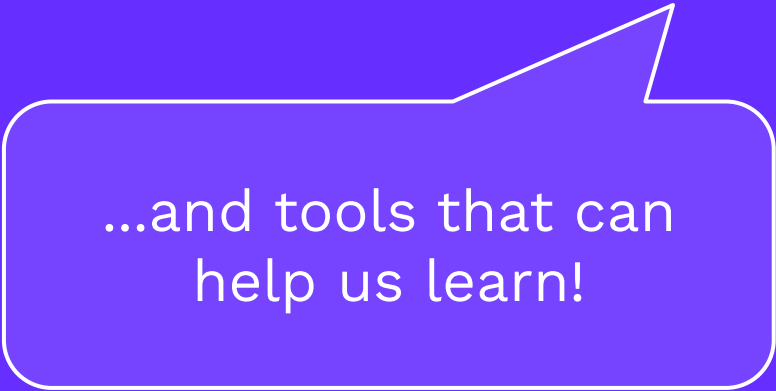


Automated



Integrated

Tools that can help




...and tools that can
help us learn!

NICE TEMPLATE



WHERE IS IT FROM?


 Terraform | Registry ☰

Terraform Registry

Discover Terraform providers that power all of Terraform's resource types, or find modules for quickly deploying common infrastructure configurations.

[Browse Providers](#) [Browse Modules](#)

1259 providers, 6472 modules & counting

 Artifact **HUB** ☰

Find, install and publish Kubernetes packages

?


- or - [browse all packages](#)

4641 **PACKAGES** | 62697 **RELEASES**

Artifact Hub is an **Open Source** project

[GitHub](#) [Slack](#) [Twitter](#)

Please see the [repositories guide](#) for more information about how to list your content on Artifact Hub.

 Sign up ☰

Where the world builds software

Millions of developers and companies build, ship, and maintain their software on GitHub—the largest and most advanced development platform in the world.

[Sign up for GitHub](#)

65+ million Developers 3+ million Organizations 72% Fortune 50

 ☰

GitLab 14

Accelerate modern DevOps. Bring velocity with confidence, security without sacrifice, and visibility into DevOps success.

[Learn more.](#)

[Try GitLab for FREE](#)

[Watch a demo](#)

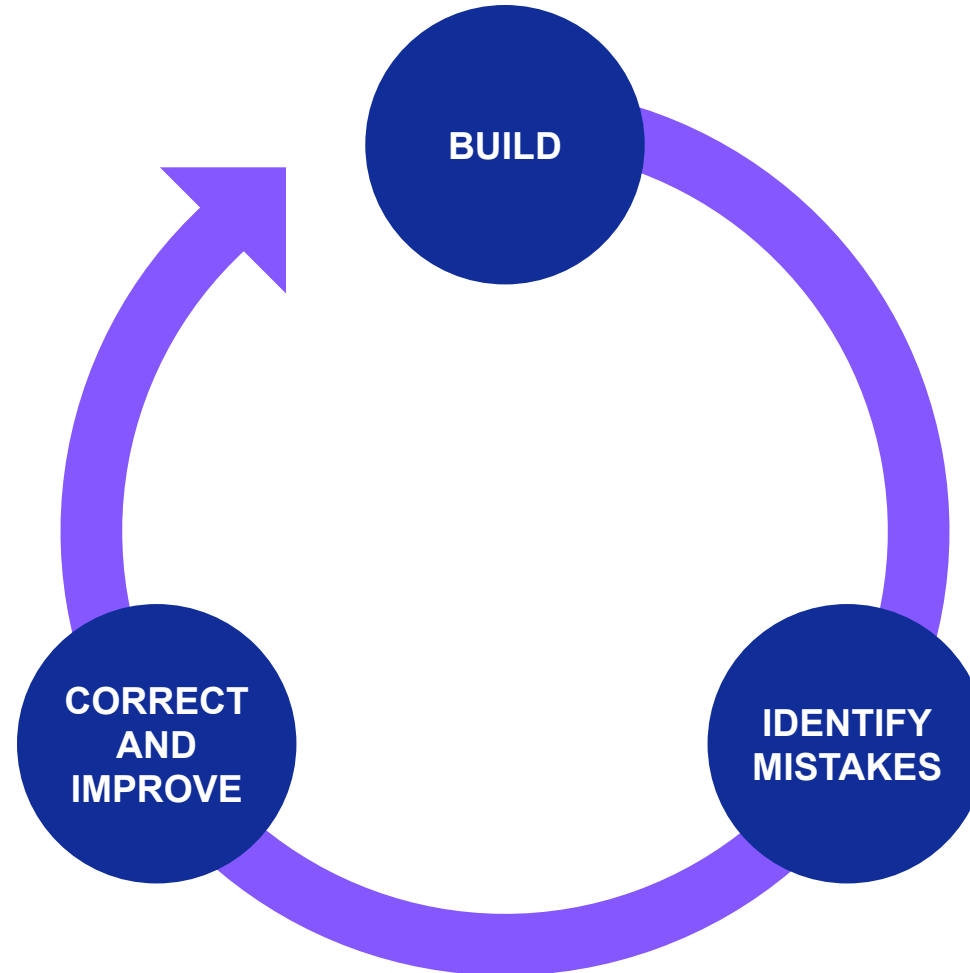


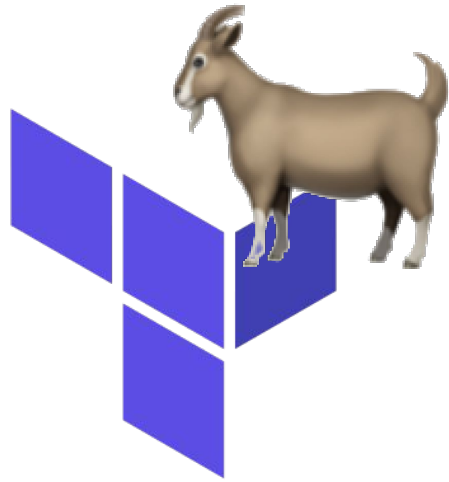
checkov

by bridgecrew

github.com/bridgecrewio/checkov

Learn by doing





TerraGoat
by bridgecrew



CfnGoat
by bridgecrew



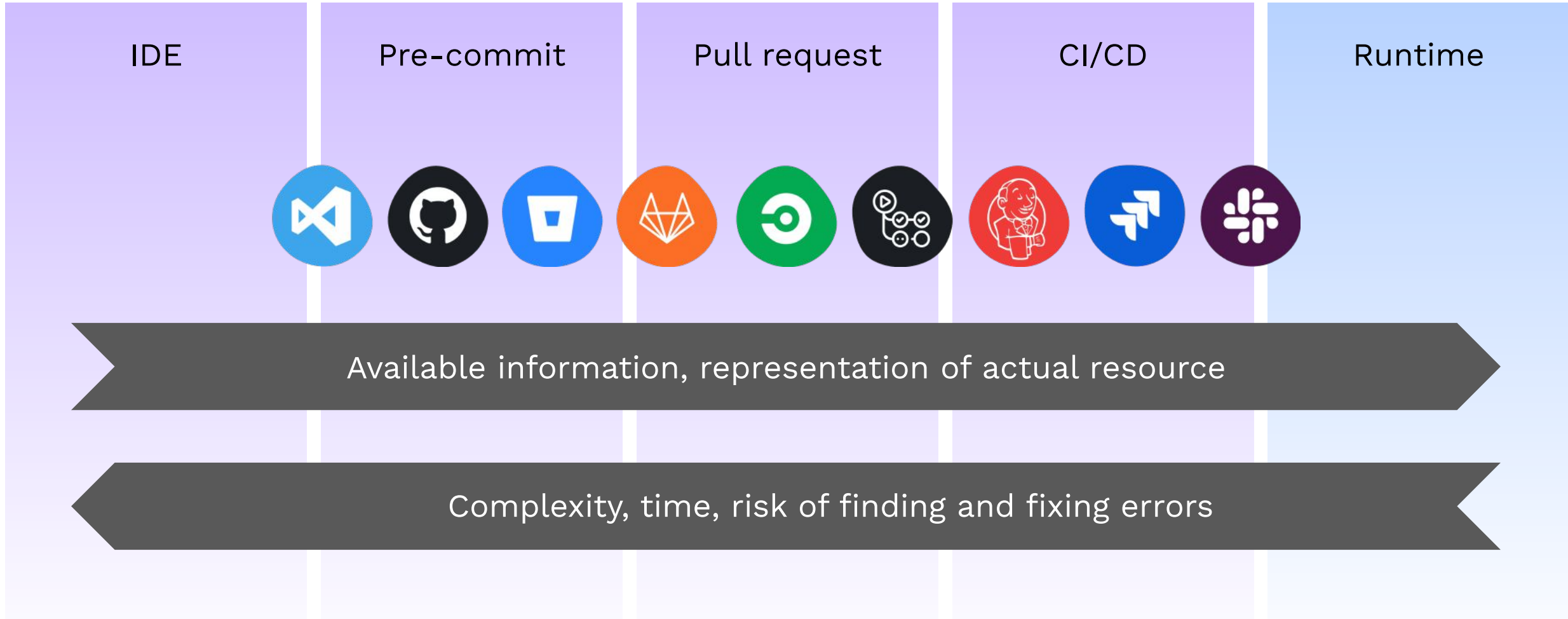
KUBERNETES
GOAT



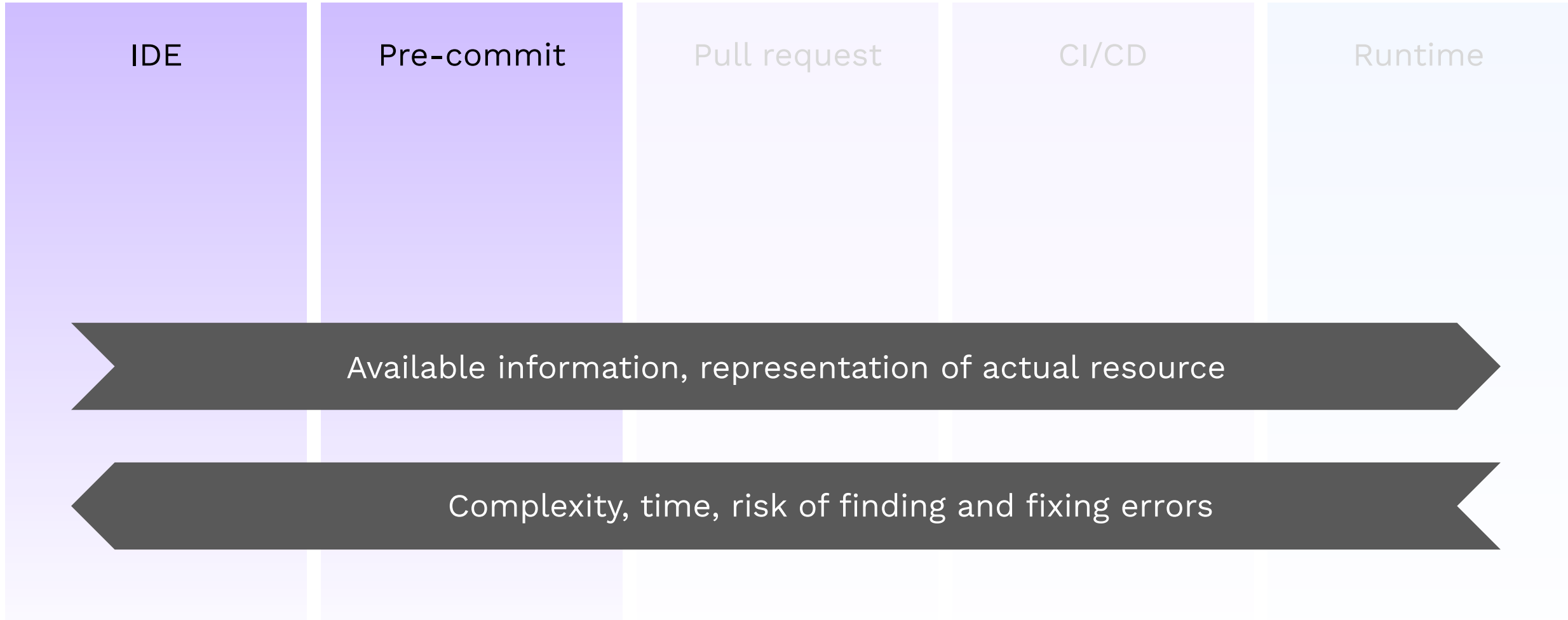
Every step of the
SDLC

What does embedded
security mean?

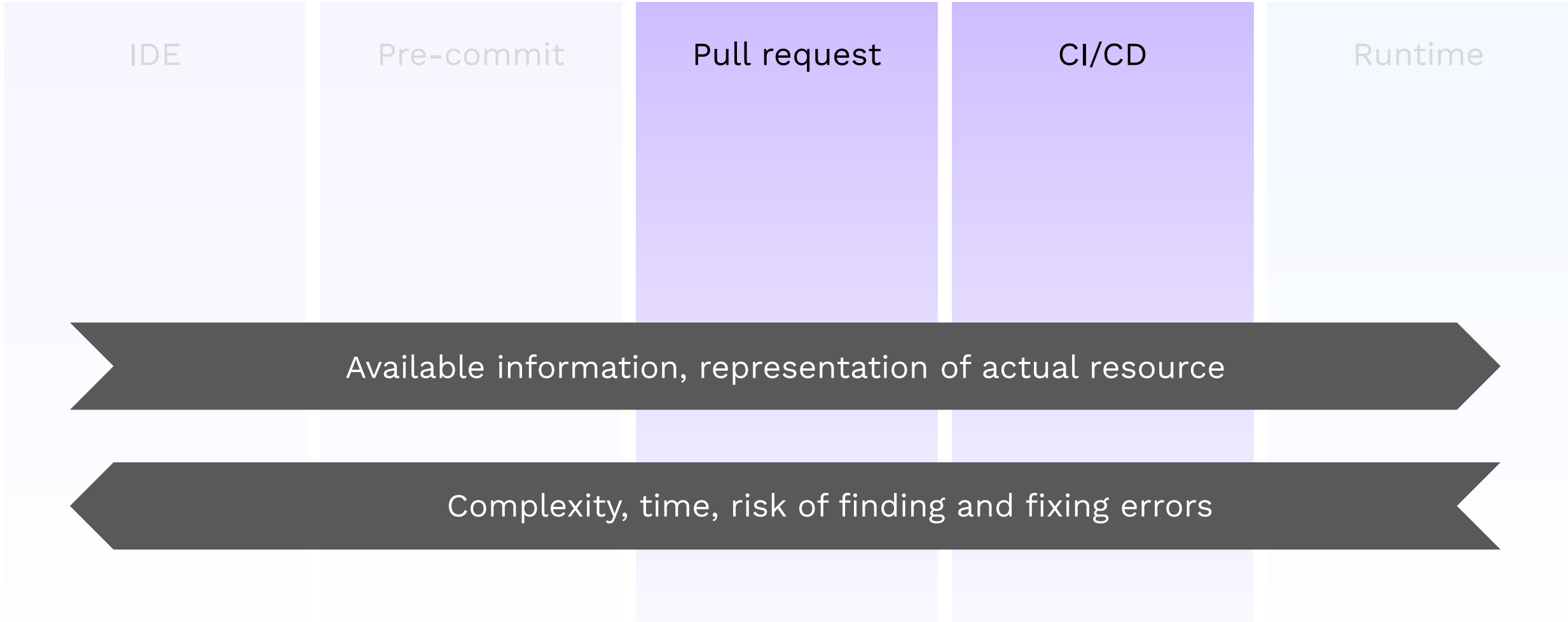
Security in the whole DevOps lifecycle



Security in the whole DevOps lifecycle



Security in the whole DevOps lifecycle



Security in the whole DevOps lifecycle

IDE

Pre-commit

Pull request

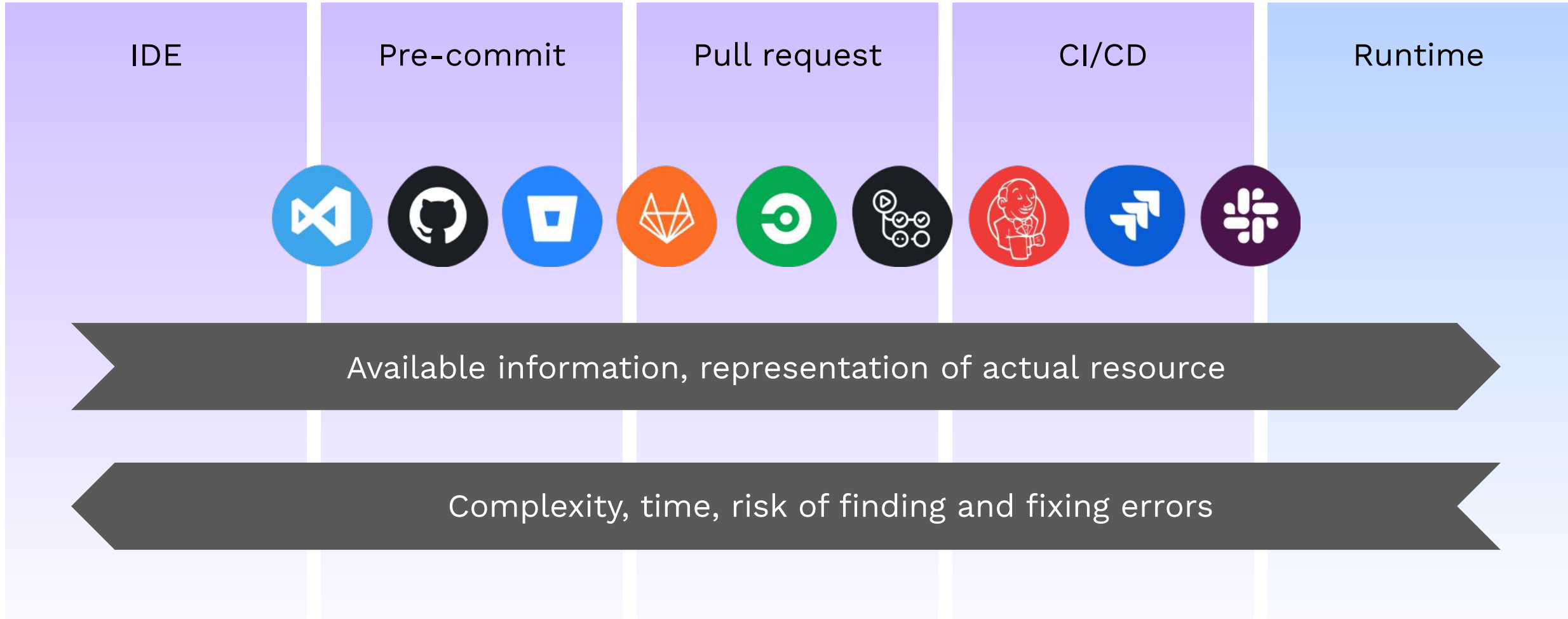
CI/CD

Runtime

Available information, representation of actual resource

Complexity, time, risk of finding and fixing errors

Security in the whole DevOps lifecycle





Crawl, walk, run

Implementing a cloud DevSecOps strategy

How to roll out your IaC governance program

Experiment

- Scan individual folders and repos
- Use open source containerized scanners
- Explore various output types and their effectiveness

Test

- Schedule scans on repositories
- Audit configuration methods and adjust scanners
- Track errors and manage SLAs for addressing them

Scale

- Orchestrate scans with build jobs
- Tweak and customize policies
- Evaluate results against known compliance benchmarks

Govern

- Audit results with all stakeholders
- Implement tagging strategy
- Get code to cloud visibility
- Regulate non-compliance usage using VCS



Thank you!

Meet me in the chat lounge for questions