terrascan™
by tenable

Self Healing GitOps: Continuous, Secure GitOps using Argo CD, Helm and OPA

Upkar Lidder
Senior Product Manager, Tenable

tenable

CLOUD NATIVE INFRASTRUCTURE IS FUELING INNOVATION

CREATING INCREASED VELOCITY, LESS PROCESS FRICTION

92%
organizations using containers in production

83%
organizations using Kubernetes in production

30%
organizations using serverless in production

Extremely high paced infrastructure

Easy developer interface, complex underpinning

Easier runtime management, deployment, and scalability

CNCF Survey 2020

tenable

SOUNDS GREAT, RIGHT?

But, is velocity leaving you vulnerable?

WHAT MAKES KUBERNETES SECURITY DIFFICULT

Developer focused management

Complex privilege management

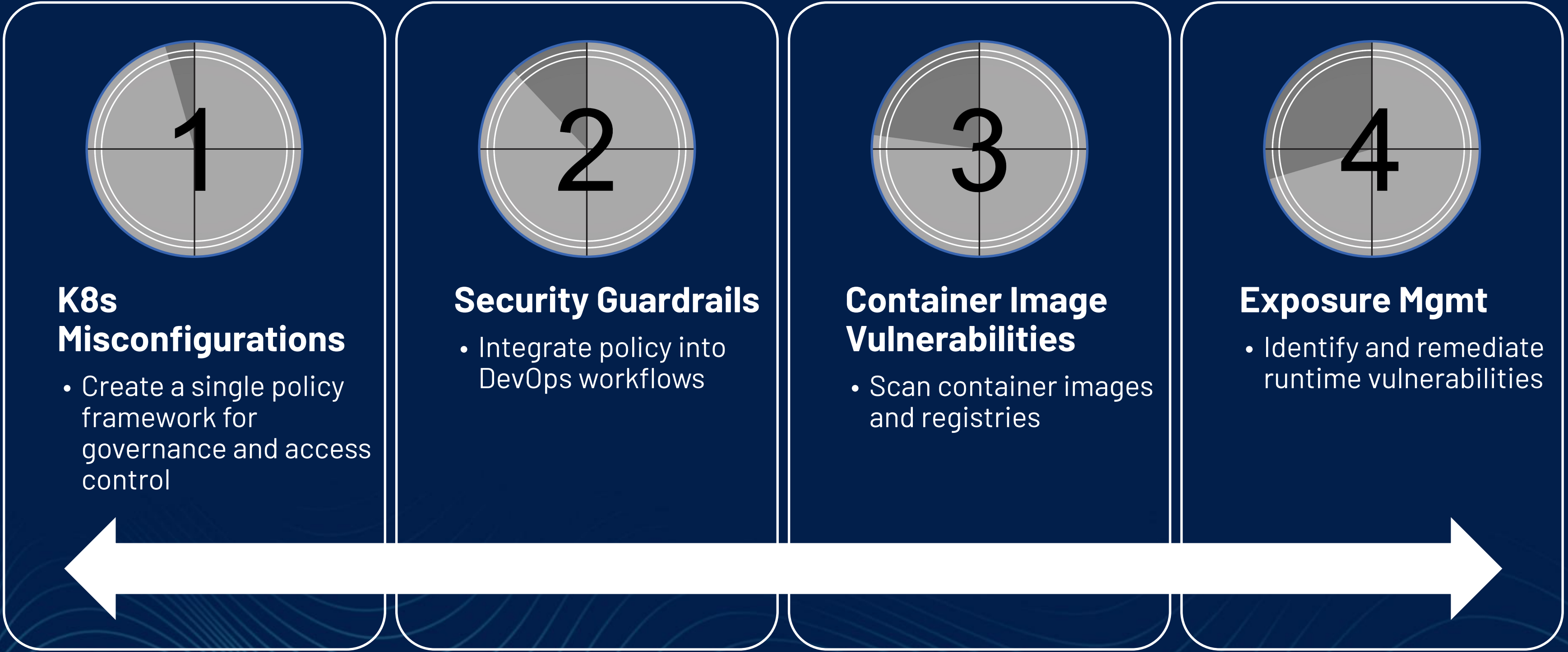
Default configurations are not secure

tenable

SO, WHAT CAN YOU DO?

tenable

4 TENETS OF K8 SECURITY



K8s Misconfigurations

- Create a single policy framework for governance and access control

Security Guardrails

- Integrate policy into DevOps workflows

Container Image Vulnerabilities

- Scan container images and registries

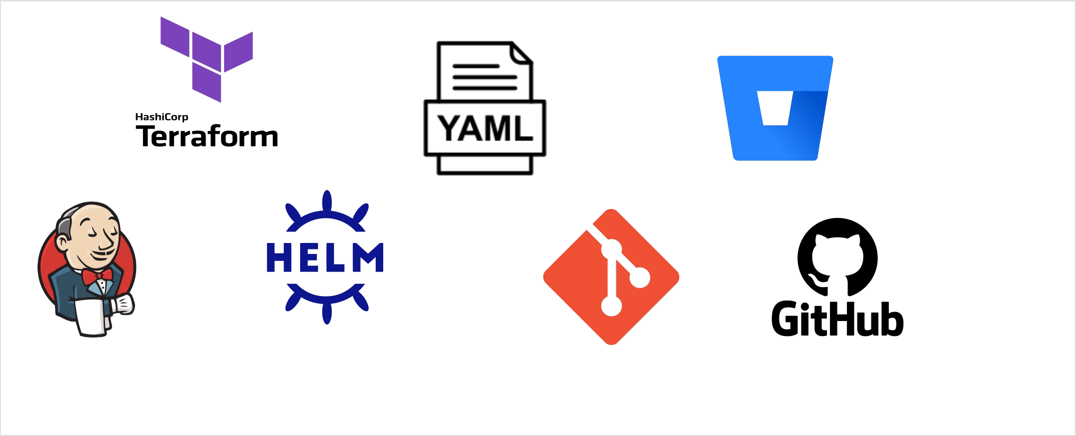
Exposure Mgmt

- Identify and remediate runtime vulnerabilities

SECURITY GUARDRAILS

Kubernetes security depends on the development process and should be built into build and delivery processes using existing development tools and frameworks.

Open Policy Agent



THE POWER OF POLICY

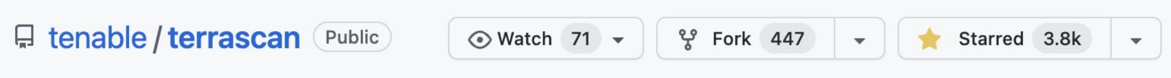
Policy as Code can be applied at several different stages in the development process, and we encourage users to apply it everywhere they can.

1. Low Friction
2. Secure by default
3. Increased Security Visibility

terrascan™
by tenable

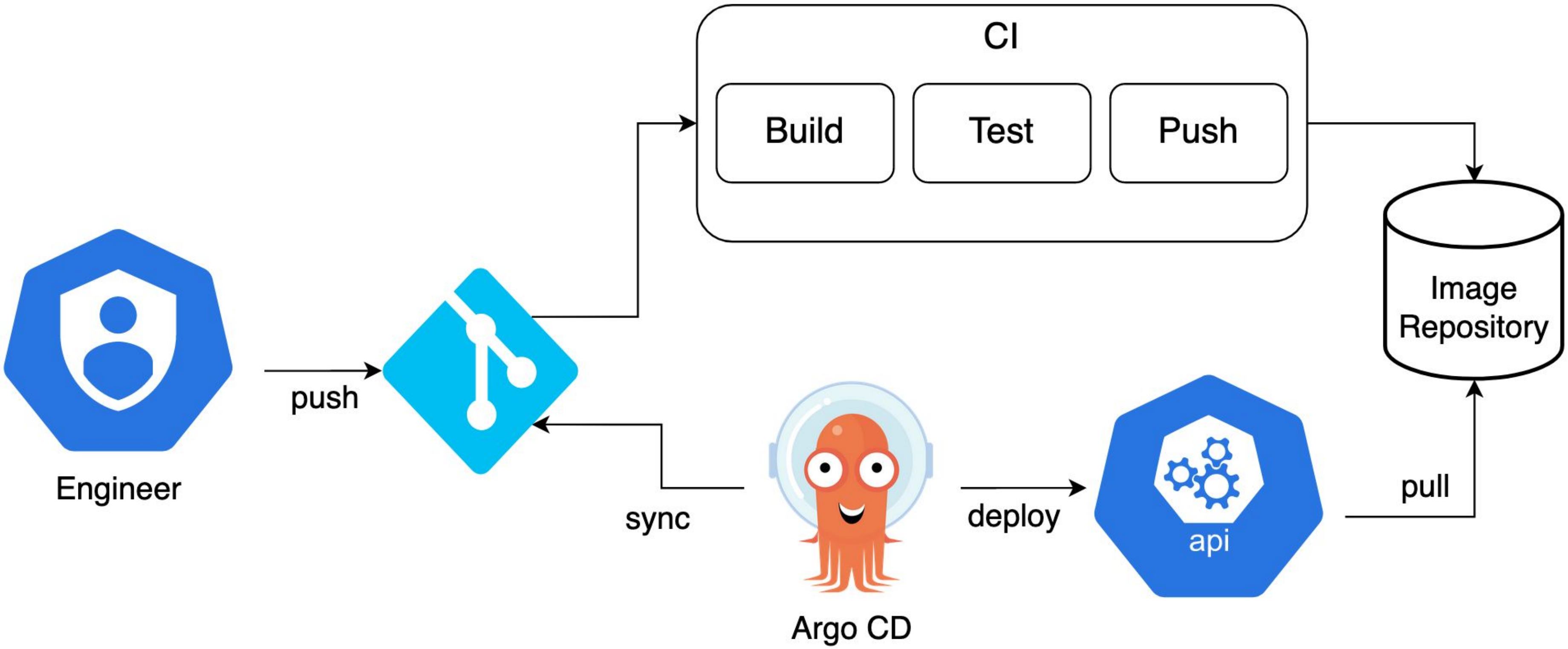
Open Source Policy as Code for Secure Cloud Infrastructure

- 500+ out-of-the-box policies
- Scan IaC against common policy standards such as the CIS
- Leverages the Open Policy Agent (OPA) engine for custom policy creation



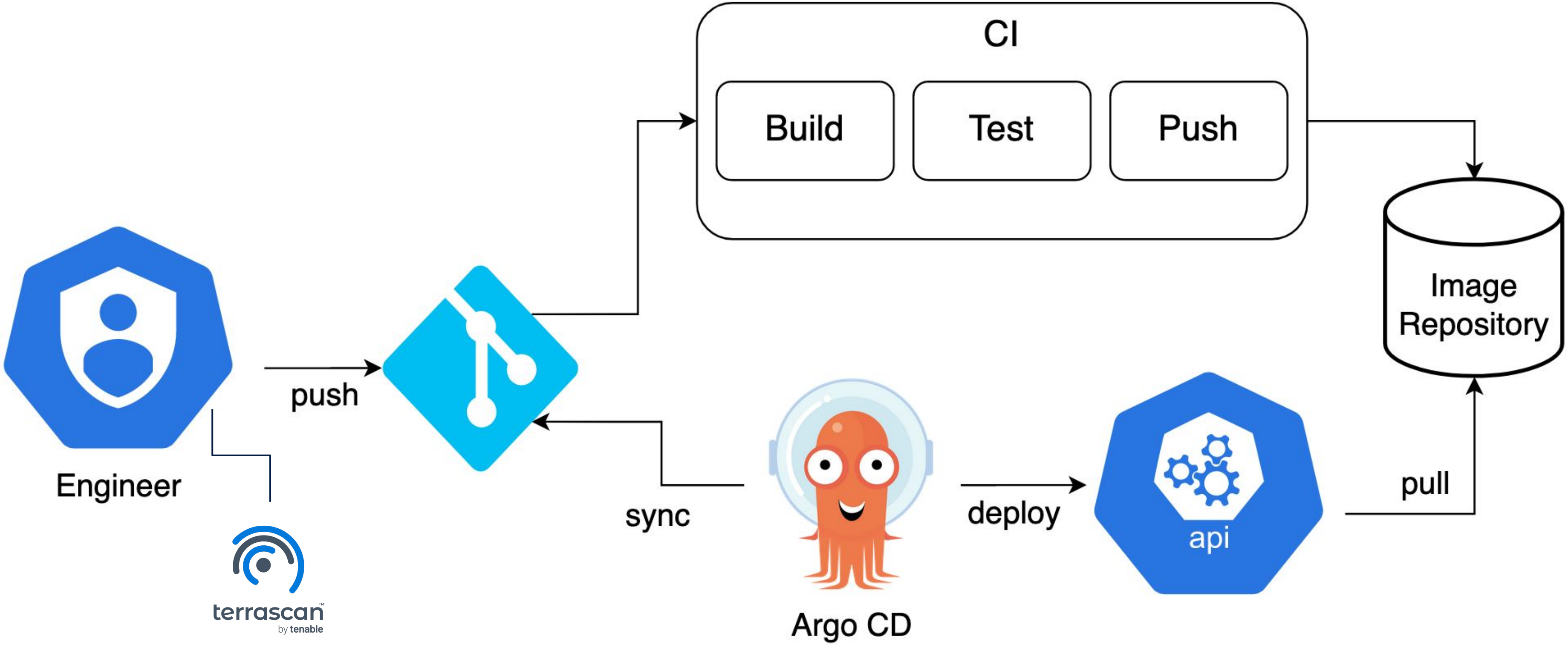
tenable / terrascan Public

TYPICAL GITOPS CI/CD WORKFLOW



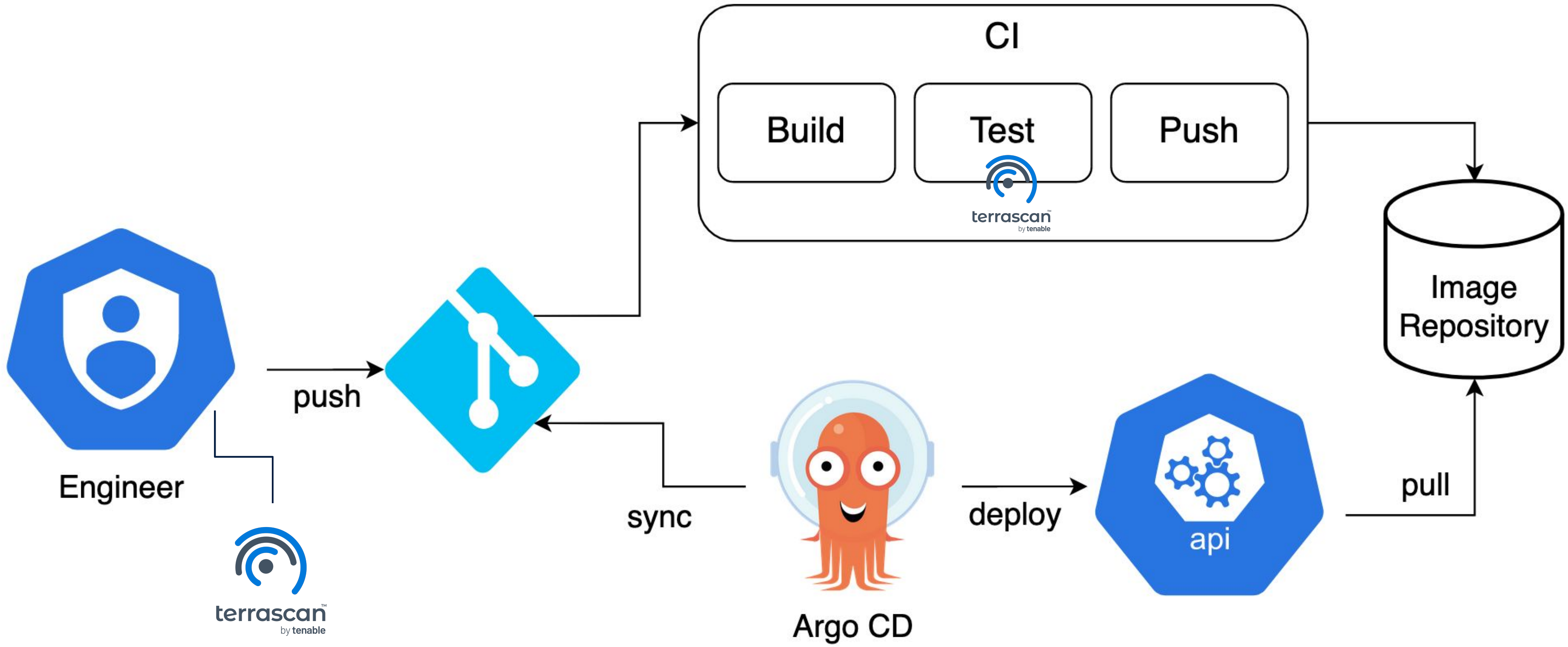
tenable

SECURE GITOPS CI/CD WORKFLOW



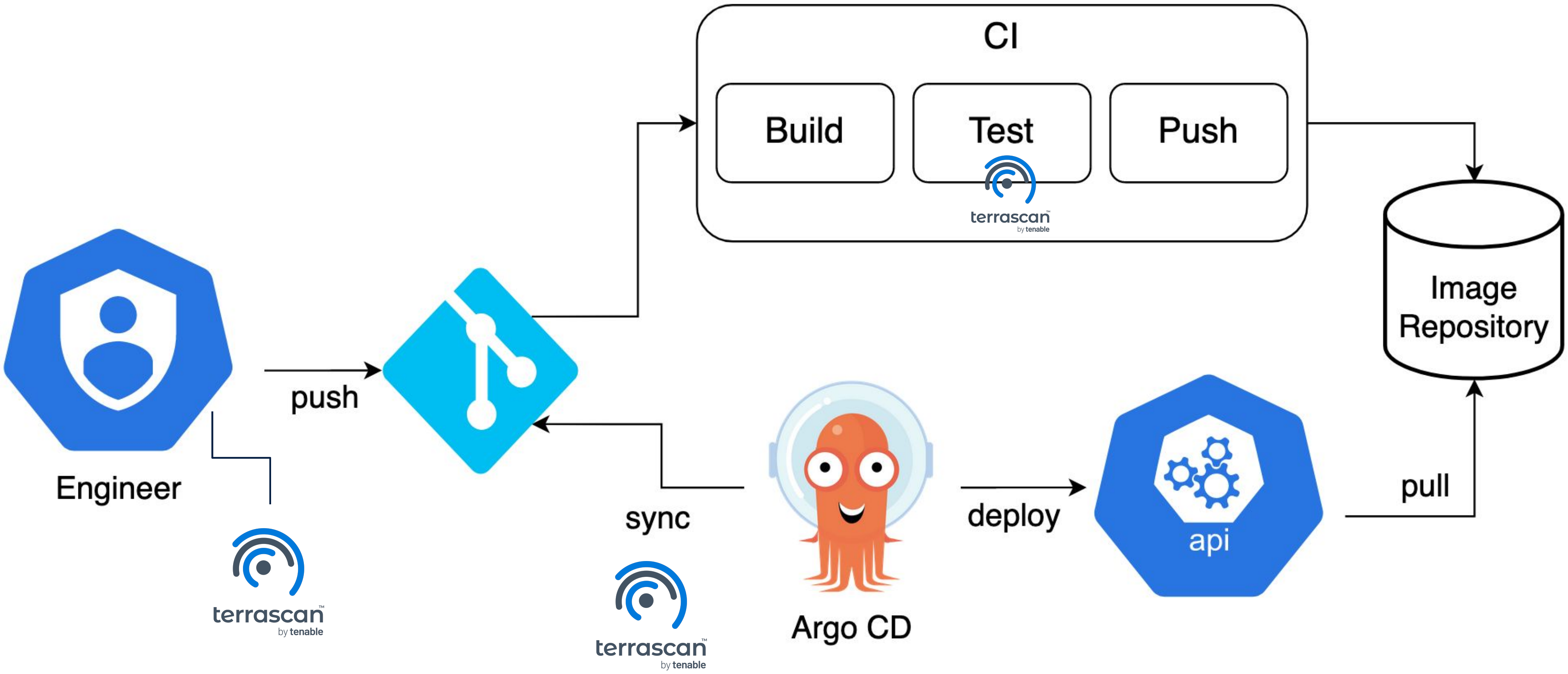
tenable

SECURE GITOPS CI/CD WORKFLOW



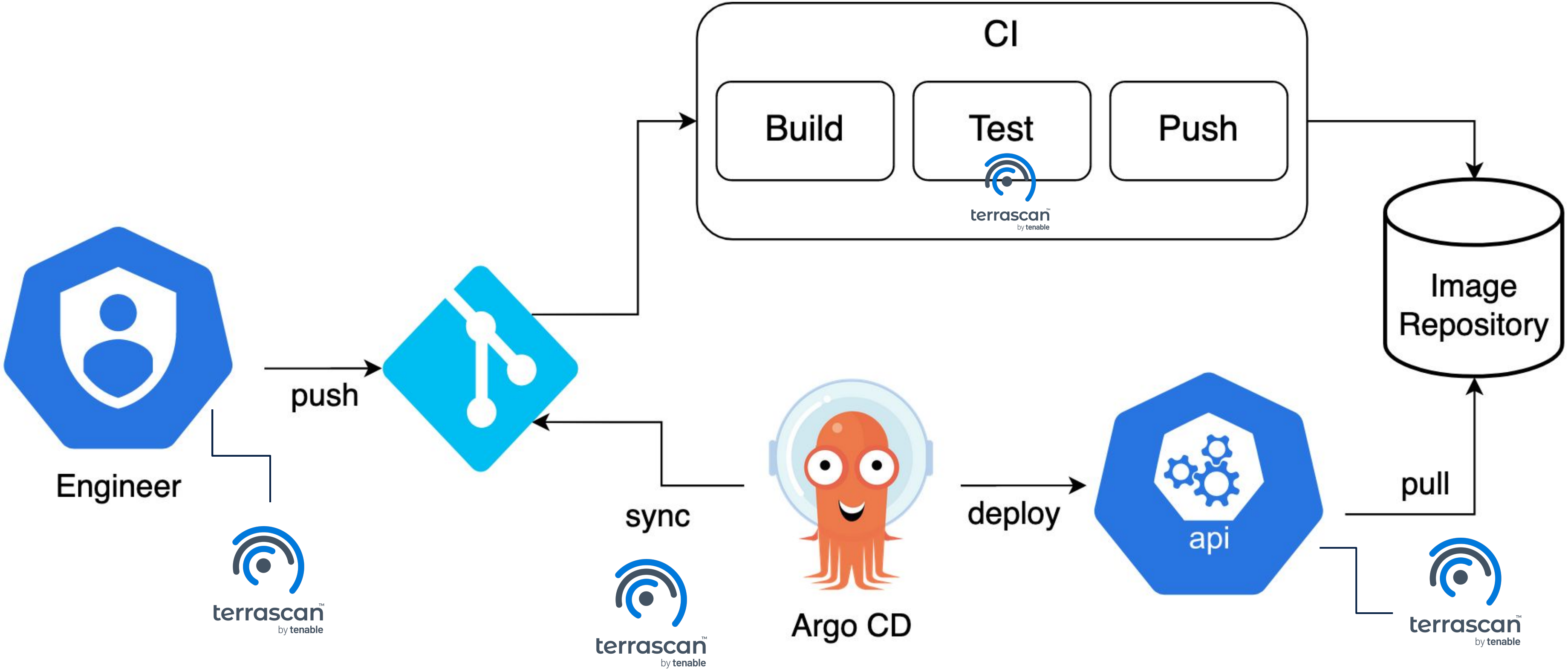
tenable

SECURE GITOPS CI/CD WORKFLOW



tenable

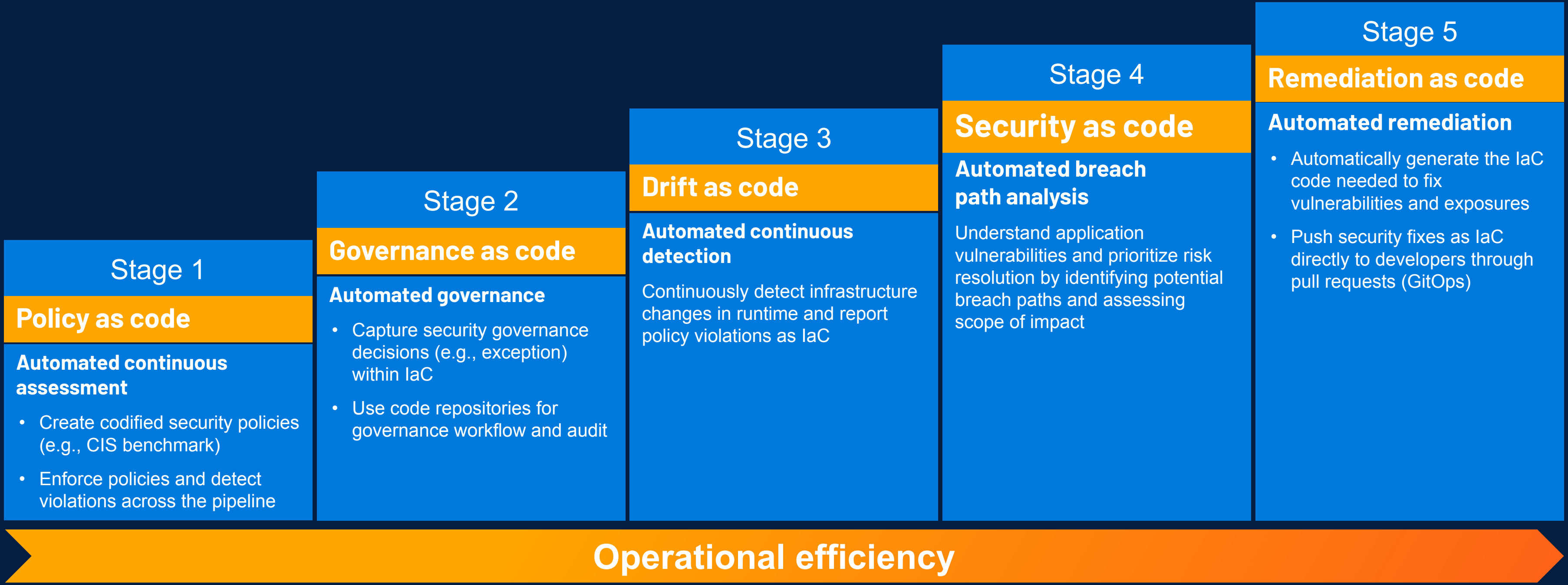
SECURE GITOPS CI/CD WORKFLOW



tenable

WHERE DO YOU GO FROM HERE?

THE ROAD TO COMPLETE CLOUD VISIBILITY



Stage 1

Policy as code

Automated continuous assessment

- Create codified security policies (e.g., CIS benchmark)
- Enforce policies and detect violations across the pipeline

Stage 2

Governance as code

Automated governance

- Capture security governance decisions (e.g., exception) within IaC
- Use code repositories for governance workflow and audit

Stage 3

Drift as code

Automated continuous detection

Continuously detect infrastructure changes in runtime and report policy violations as IaC

Stage 4

Security as code

Automated breach path analysis

Understand application vulnerabilities and prioritize risk resolution by identifying potential breach paths and assessing scope of impact

Stage 5

Remediation as code

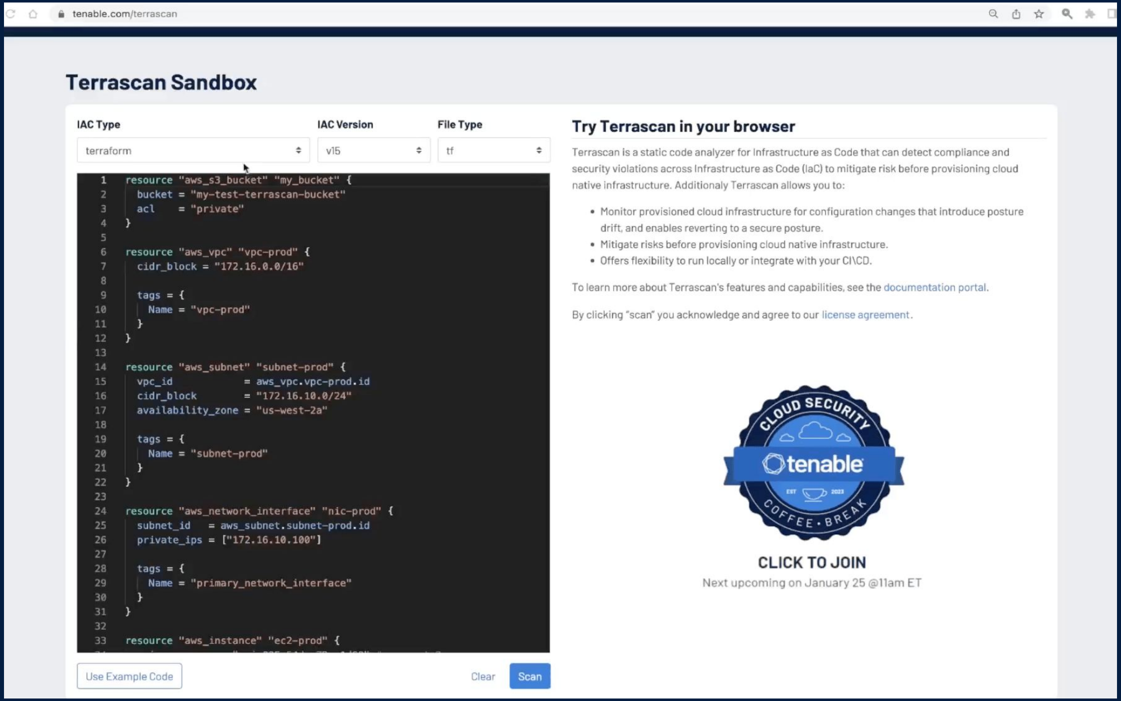
Automated remediation

- Automatically generate the IaC code needed to fix vulnerabilities and exposures
- Push security fixes as IaC directly to developers through pull requests (GitOps)

Operational efficiency

tenable

TRY IT YOURSELF



Terrascan Sandbox

IAC Type: terraform

IAC Version: v15

File Type: tf

```
resource "aws_s3_bucket" "my_bucket" {
  bucket = "my-test-terrascan-bucket"
  acl    = "private"
}

resource "aws_vpc" "vpc-prod" {
  cidr_block = "172.16.0.0/16"

  tags = {
    Name = "vpc-prod"
  }
}

resource "aws_subnet" "subnet-prod" {
  vpc_id            = aws_vpc.vpc-prod.id
  cidr_block        = "172.16.10.0/24"
  availability_zone = "us-west-2a"

  tags = {
    Name = "subnet-prod"
  }
}

resource "aws_network_interface" "nic-prod" {
  subnet_id   = aws_subnet.subnet-prod.id
  private_ips = ["172.16.10.100"]

  tags = {
    Name = "primary_network_interface"
  }
}

resource "aws_instance" "ec2-prod" {
```

Try Terrascan in your browser

Terrascan is a static code analyzer for Infrastructure as Code that can detect compliance and security violations across Infrastructure as Code (IaC) to mitigate risk before provisioning cloud native infrastructure. Additionaly Terrascan allows you to:

- Monitor provisioned cloud infrastructure for configuration changes that introduce posture drift, and enables reverting to a secure posture.
- Mitigate risks before provisioning cloud native infrastructure.
- Offers flexibility to run locally or integrate with your CI\CD.

To learn more about Terrascan's features and capabilities, see the documentation portal.

By clicking "scan" you acknowledge and agree to our license agreement.

CLICK TO JOIN

Next upcoming on January 25 @11am ET

Tenable.com/terrascan