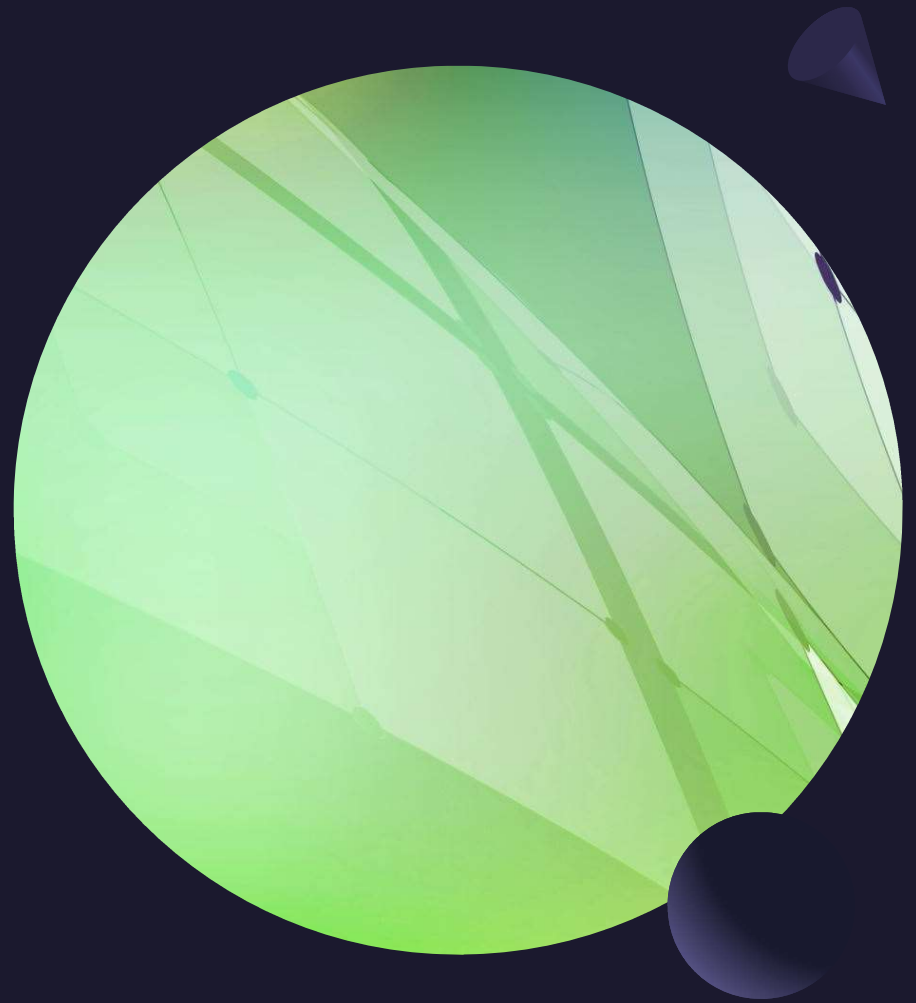


# Bake Security Into Your Infrastructure as Code

Caleb Mattingly





# About The Chef

## Experience:

- MS: Cybersecurity – Liberty University
- Experience in DoD and Commercial Industry
- Compliance, DevSecOps, and Cloud Security
- CEO of Secure Cloud Innovations

## Hobbies:

- Guitar
- Brewing
- Reading

## Contact Info:

[caleb.mattingly@securecloudinnovations.net](mailto:caleb.mattingly@securecloudinnovations.net)



# Recipe Requirements

1 cup of cloud infrastructure

2 fluid oz of infrastructure as code

3 tablespoons of CI/CD

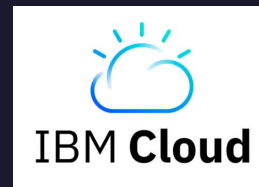
¼ cup of open-source tools

1 gallon of coffee



# Cloud Infrastructure Options

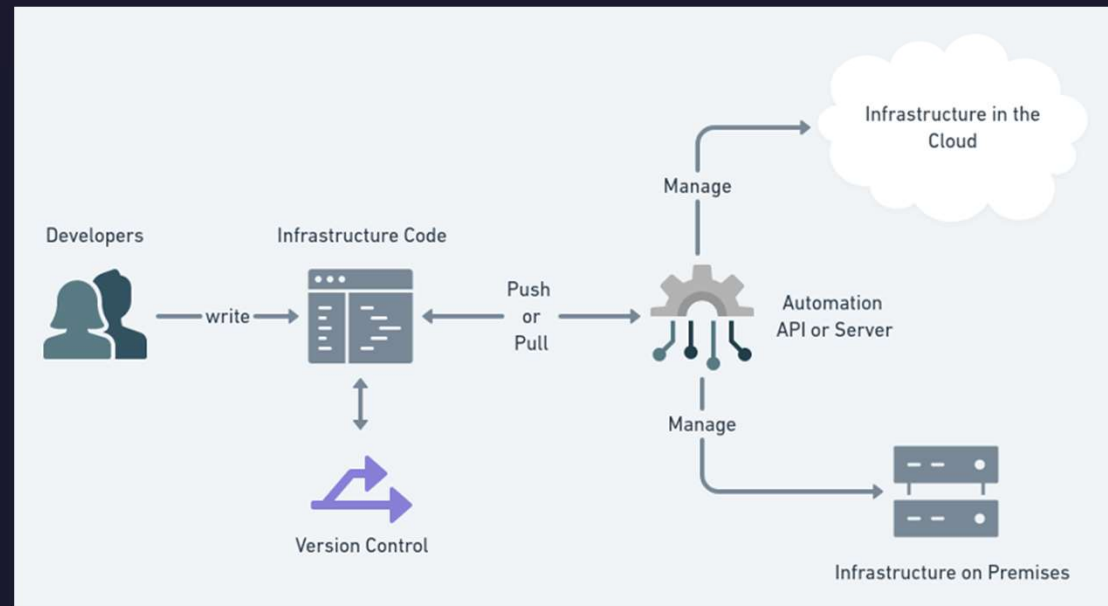
- AWS
- Azure
- GCP
- Heroku
- Alibaba
- IBM
- Oracle



# Infrastructure as Code

## The Advent, The Options, and Why

- 1908 Herbert Johnson – electric standing mixer
- 1993 – first CFEngine (The Configuration Engine)
- Terraform
- AWS CloudFormation
- Azure Resource Manager
- GC Deployment Manager
- Chef
- Puppet
- SaltStack



# Why IaC?

- Recoverable State
- Disaster Recovery
- Auditability
- Repeatability
- Speed
- Reduced Risk
- Cost Reduction



# What's Missing?

Verification and Validation of Security








# Pipelines

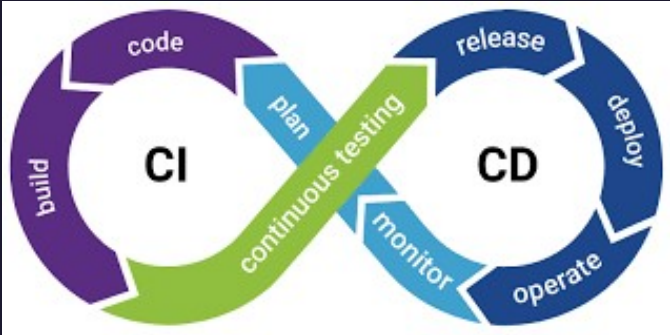




# CI/CD

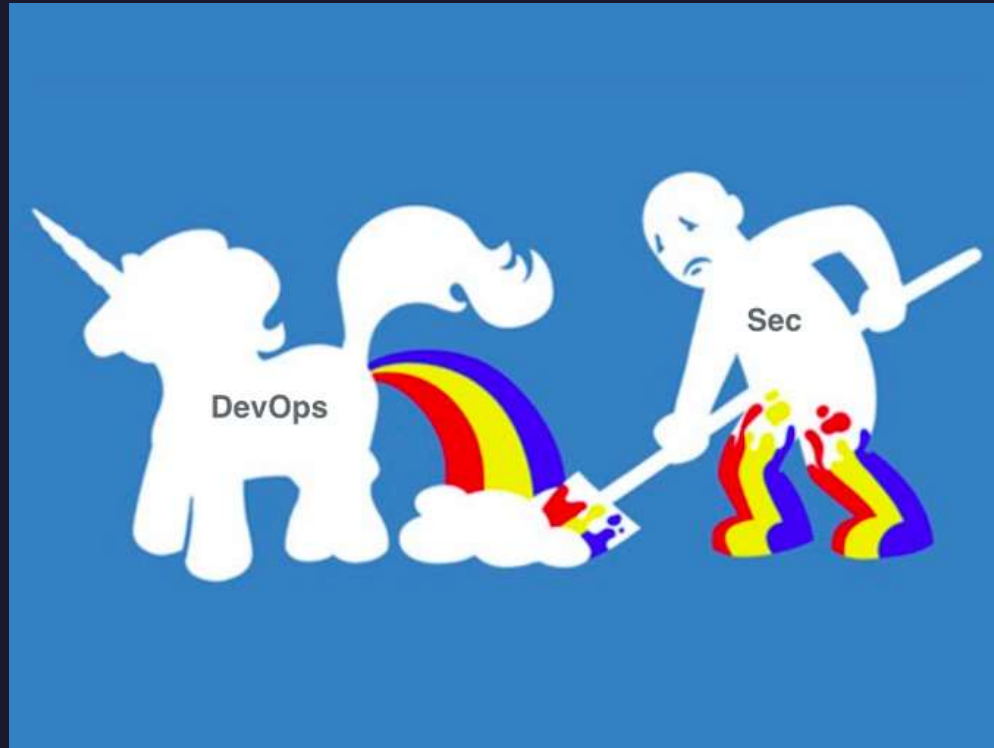
Continuous Integration  
Continuous Deployment

	 Jenkins	 circleci	 TeamCity	 Bamboo	 GitLab
Open source	Yes	No	No	No	No
Ease of use & setup	Medium	Medium	Medium	Medium	Medium
Built-in features	3/5	4/5	4/5	4/5	4/5
Integration	★★★★★	★★★	★★★★★	★★★	★★★★★
Hosting	On premise & Cloud	On premise & Cloud	On premise	On premise & Bitbucket as Cloud	On premise & Cloud
Free version	Yes	Yes	Yes	Yes	Yes
Build Agent License Pricing	Free	From \$39 per month	From \$299 one-off payment	From \$10 one-off payment	From \$4 per month per user
Supported OSs	Windows, Linux, macOS, Unix-like OS	Linux or MacOS	Windows, Linux, macOS, Solaris, FreeBSD and more	Windows, Linux, macOS, Solaris	Linux distributions: Ubuntu, Debian, CentOS, Oracle Linux



<https://www.katalon.com/resources-center/blog/ci-cd-tools/>

# When security is left out of the DevOps Pipeline Party...



<https://twitter.com/petecheslock/status/595617204273618944>

# Open-Source Tools

- Terrascan
- Checkov
- TFLint
- Terraforma
- CloudSploit
- Hashicorp Sentinel



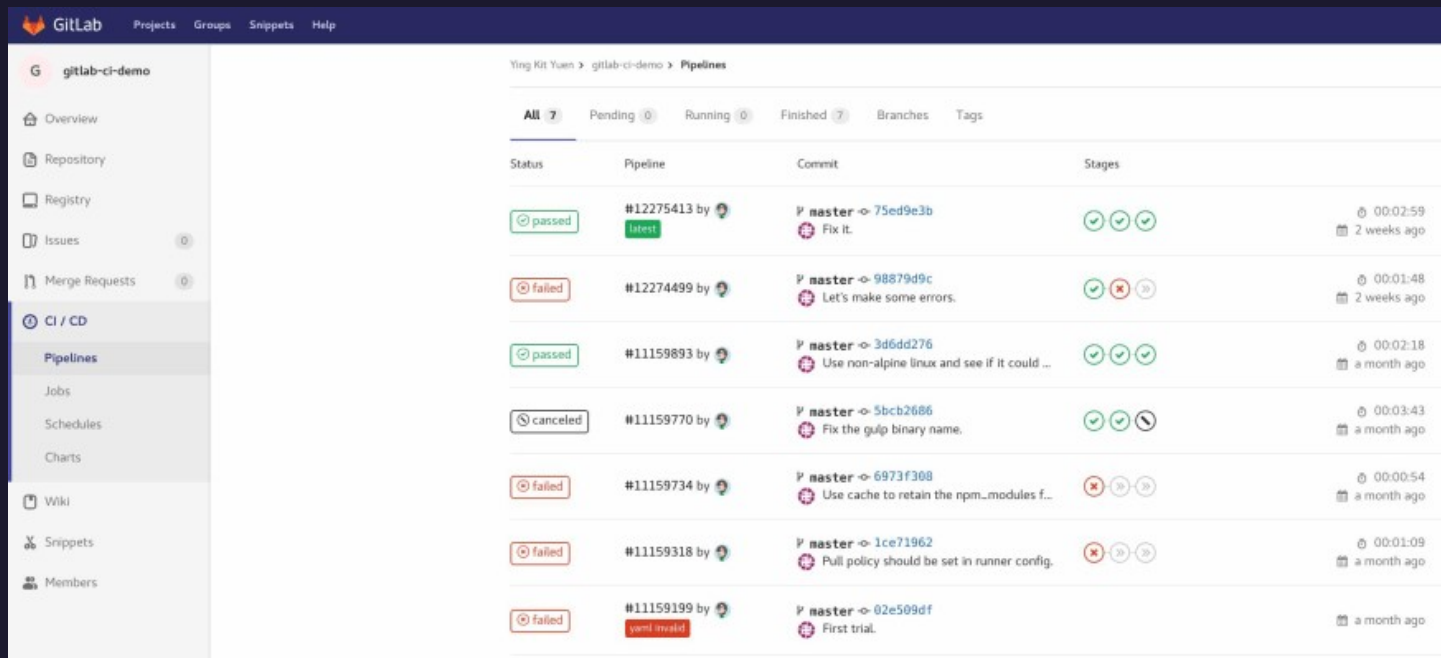
Sentinel

# Terrascan Example (Gitlab CI)

```
stages:
  - scan

terrascan:
  image:
    name: accurics/terrascan:latest
    entrypoint: ["/bin/sh", "-c"]
  stage: scan
  script:
    - /go/bin/terrascan scan .
```

# Terrascan Example (Continued)



Status	Pipeline	Commit	Stages	
passed	#12275413 by	P master -> 75ed9e3b Fix it.		00:02:59 2 weeks ago
failed	#12274499 by	P master -> 98879d9c Let's make some errors.		00:01:48 2 weeks ago
passed	#11159893 by	P master -> 3d6dd276 Use non-alpine linux and see if it could ...		00:02:18 a month ago
canceled	#11159770 by	P master -> 5bcb2686 Fix the gulp binary name.		00:03:43 a month ago
failed	#11159734 by	P master -> 6973f308 Use cache to retain the npm_modules f...		00:00:54 a month ago
failed	#11159318 by	P master -> 1ce71962 Pull policy should be set in runner config.		00:01:09 a month ago
failed	#11159199 by sync created	P master -> 02e509df First trial.		a month ago

# Primary Concerns

1. Misconfigurations
2. Managing Secrets
3. Governed in Code, Secured in Code
4. CI/CD Integration



# Managing Secrets



Build	Build gates into the pipelines
Remove	Remove existing plaintext passwords <ul style="list-style-type: none"><li>• Tools: Trufflehog, Gitleaks, GitRob, or even writing manual grep commands to search</li></ul>
Utilize	Utilize Secret Servers <ul style="list-style-type: none"><li>• Ie. Vault, Conjur, Keywhiz, CyberArk</li><li>• Cloud Native: AWS – KMS, GCE – KMS, Azure – Key Vault</li></ul>
Check	Check COMMITS for sensitive data as well
Encrypt	Encrypt Secrets

# Primary Concerns

1. Misconfigurations
2. Managing Secrets
3. Governed in Code, Secured in Code
4. CI/CD Integration





Governed in Code,  
Secured in Code



# Primary Concerns

1. Misconfigurations
2. Managing Secrets
3. Governed in Code, Secured in Code
4. CI/CD Integration



# Concluding Remarks

- Become familiar with Infrastructure as Code, no matter what environment you work in
- Don't assume anything is secure, but specifically don't assume infrastructure as code is secure

\*cough cough\* zero-trust...

- Utilize CI/CD Pipelines for securing your code
- BRUCE



The End!

