

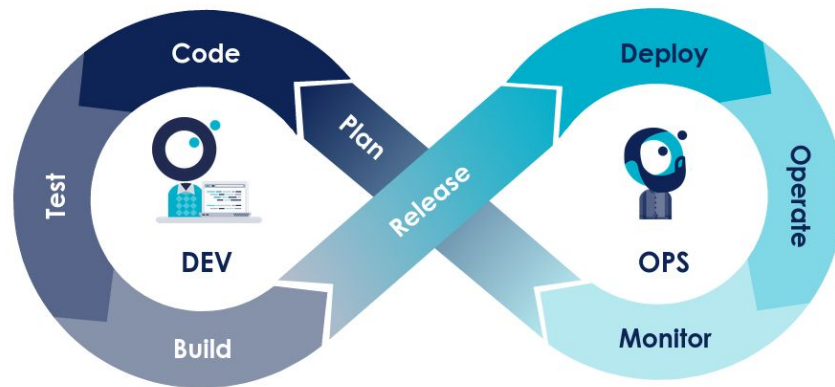


# Checkov

- Simon PRUNEAU - 23 JUIN 2020

# IaC & DevOps

- Description de l'infrastructure sous forme de code
- Avoir recours à des pratiques de code :
  - > Revue de code
  - > Pair programming
  - > **Écriture de tests**
  - > Documentation



Utiliser un SAST sur de l'Infra as Code pour **réduire la boucle de feedbacks sur les failles** ?

# Checkov

"Checkov is a **static code analysis tool** for infrastructure-as-code. It scans cloud infrastructure provisioned using **Terraform**, **Cloudformation** or **Kubernetes** and detects security and compliance misconfigurations"

Créé par Bridgecrew et disponible sur GitHub

Plus de 300 politiques prédéfinies



# Exemples de détections sur AWS

Vérifie ...

- ◉ qu'il n'y a pas de profils avec les droits "full admin" sans restrictions
- ◉ que la politique de mots de passe requiert au moins 14 caractères
- ◉ que toutes les données dans des buckets S3 sont chiffrées au repos
- ◉ que le protocol autorisé pour les ALB est HTTPS
- ◉ qu'il n'y a pas de "security group" permettant l'accès sur le port 22 depuis Internet
- ◉ que la politique d'accès à la registry ECR n'est pas publique
- ◉ qu'il n'y a pas d'identifiants AWS hardcodés dans le provider terraform

# Utilisation

```
$ mkvirtualenv checkov -p python3.6
```

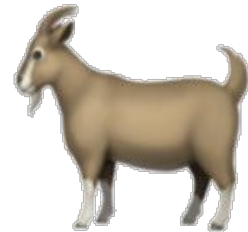
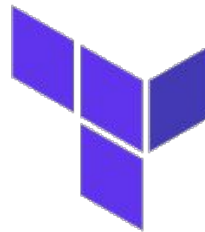
```
$ pip install checkov
```

```
$ cd terraform/
```

```
$ checkov -d .
```


# Terragoat

**TerraGoat**  
by bridgecrew



- ◉ Code d'infrastructure Terraform **vulnérable by design**
- ◉ Peut-être utilisée pour tester SAST, linter, hooks de pre-commit ou autre scans
- ◉ Parfait pour tester Checkov ;)

# Limitations de l'outil

- ◉  Certaines options poussées par Checkov ne sont pas gratuites
- ◉ Coût de mise en place :
  - > Lancer l'outil et configurer pour éviter les "faux positifs"
  - > Plus on le met en place tard dans un projet, plus le coût augmente
- ◉ Impossible d'ajouter ses propres règles -> à coupler avec un outil comme **Conftest**

# Takeaways

- ◉ Si vous ne faites pas d'IaC, faites-en !
- ◉ Il est important de prendre le temps de s'outiller
- ◉ Checkov + Conftest = ❤️ ?



# Liens

- <https://github.com/bridgecrewio/checkov/>
- <https://github.com/bridgecrewio/terragoat>
- <https://github.com/open-policy-agent/conftest>



*There  
Is  
a Better  
Way*