Static analysis of Infrastructure as Code

Barak Schoster

Co-Founder & CTO

bridgecrew

SANS

Barak Schoster Goihman
Co-Founder & CTO at bridgecrew

@BarakSchoster

github.com/schosterbarak

aws

toniblyx/Prowler

duo-labs/cloudmapper

HashiCorp Terraform

bridgecrewio/checkov

bridgecrewio/TerraGoat

bridgecrewio/CfnGoat

Google Cloud

GCP/terraform-pci-starter

I ♥ OPEN SOURCE

Today's talk track

1. Setup
2. The state of open source misconfig
3. Config Runtime Analysis
4. Config Static Analysis
5. How to choose?

Configuration errors found in the wild

DEFAULT CONFIGURATIONS

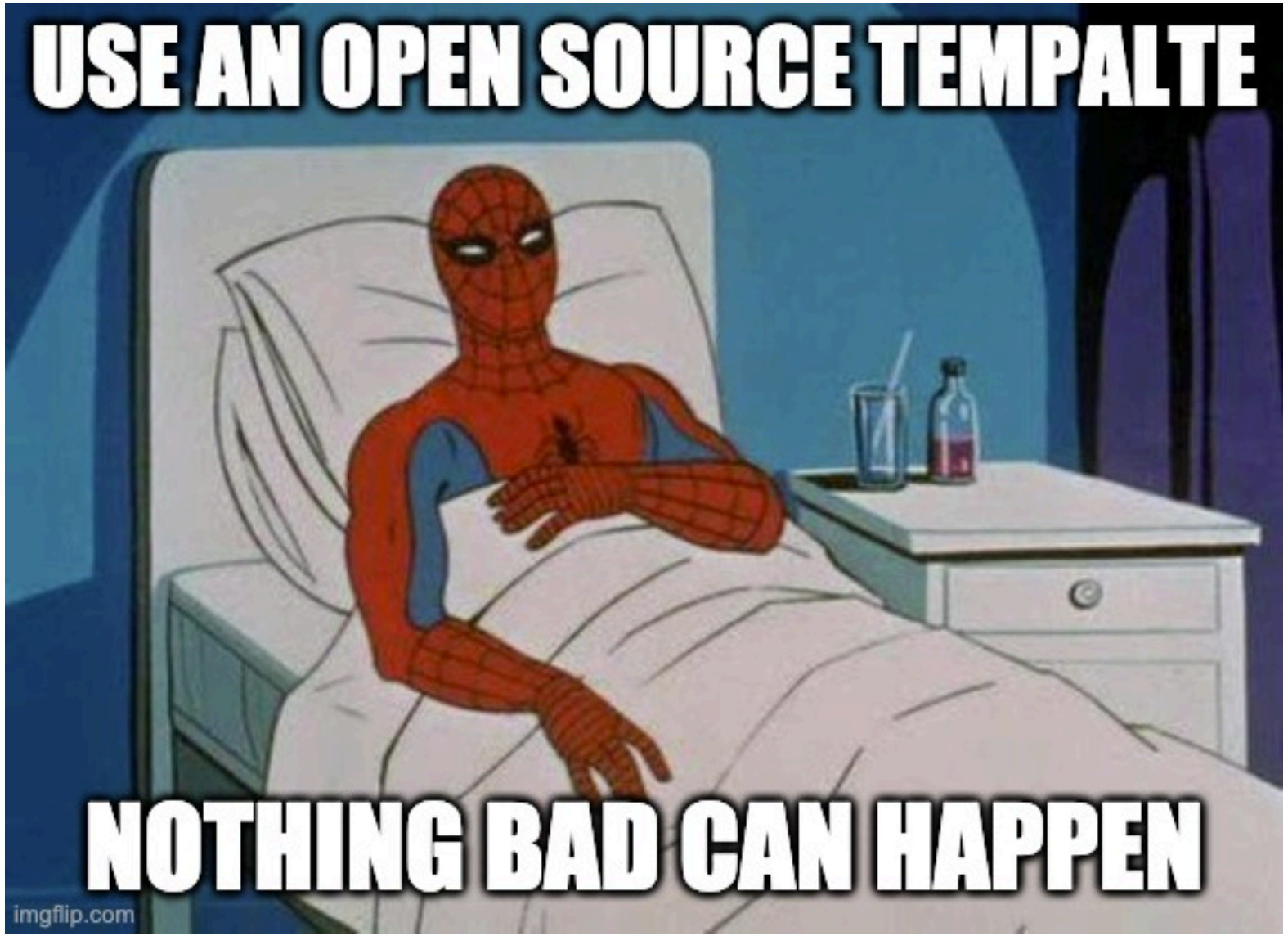
DISABLED LOGGING

UNENCRYPTED DATABASES

INSECURE PROTOCOLS

VULNERABLE MIROSERVICES

Where do bad configurations come from?



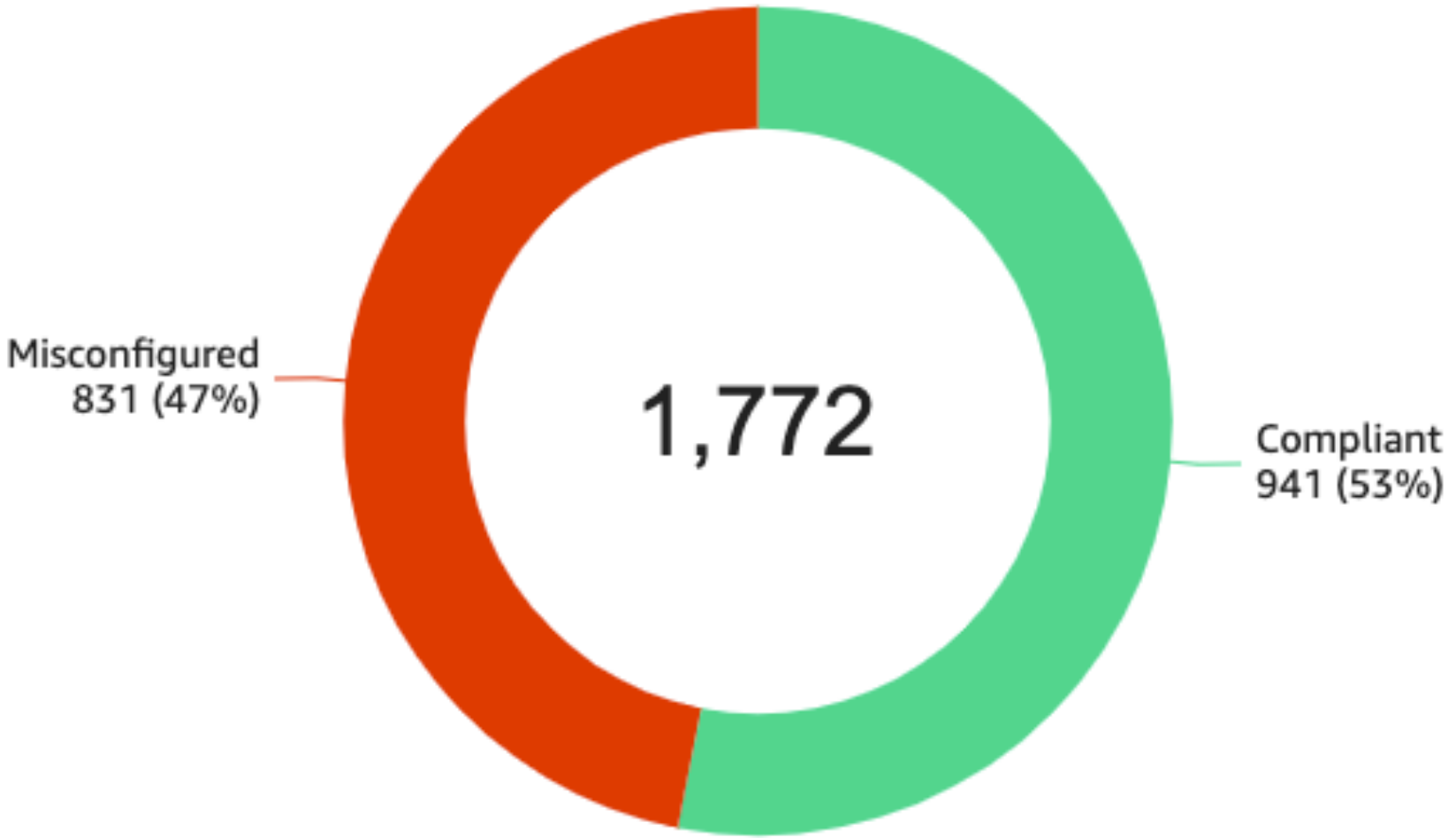
aws

Google Cloud

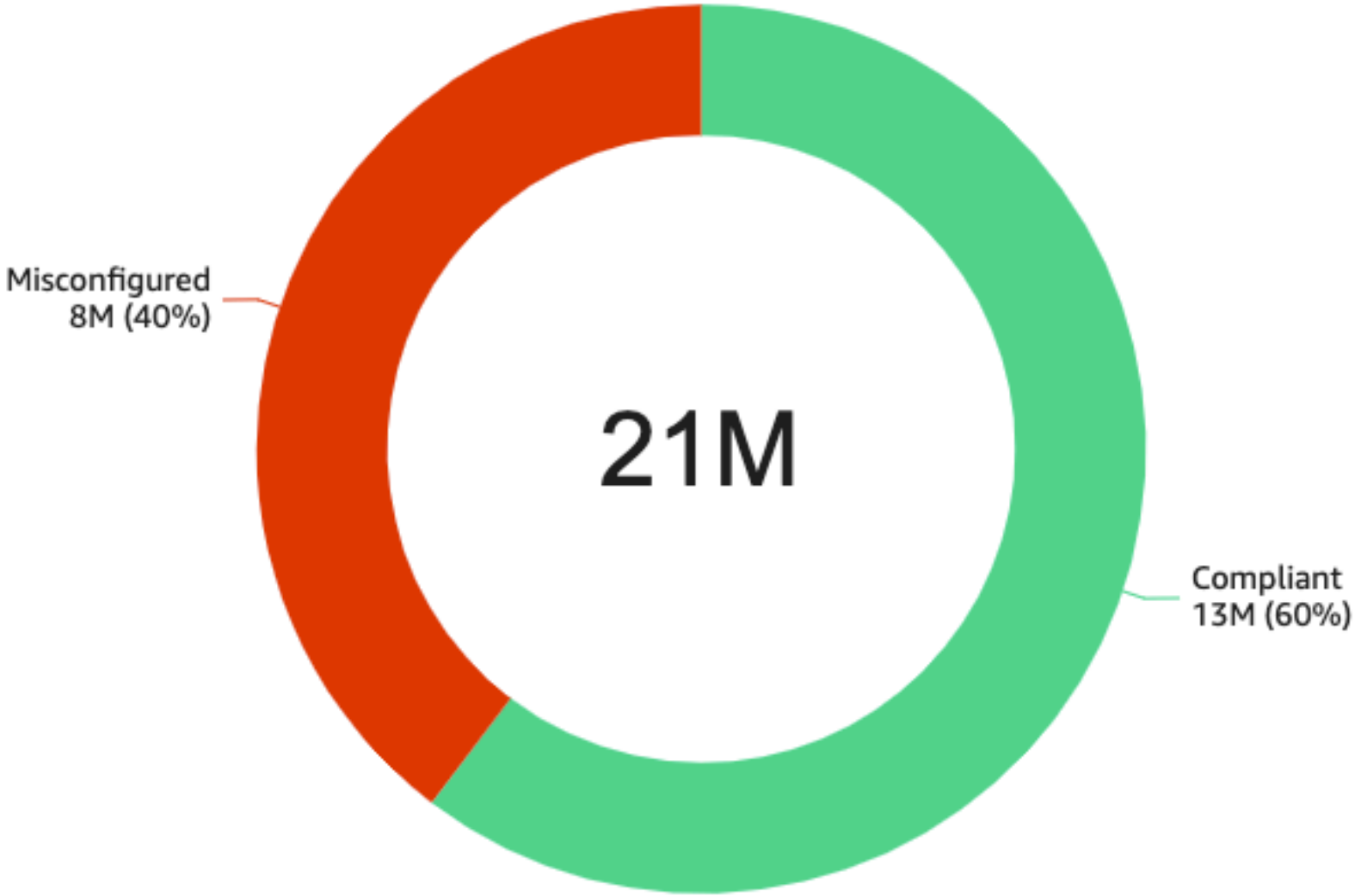
HashiCorp Terraform | Registry

GitHub

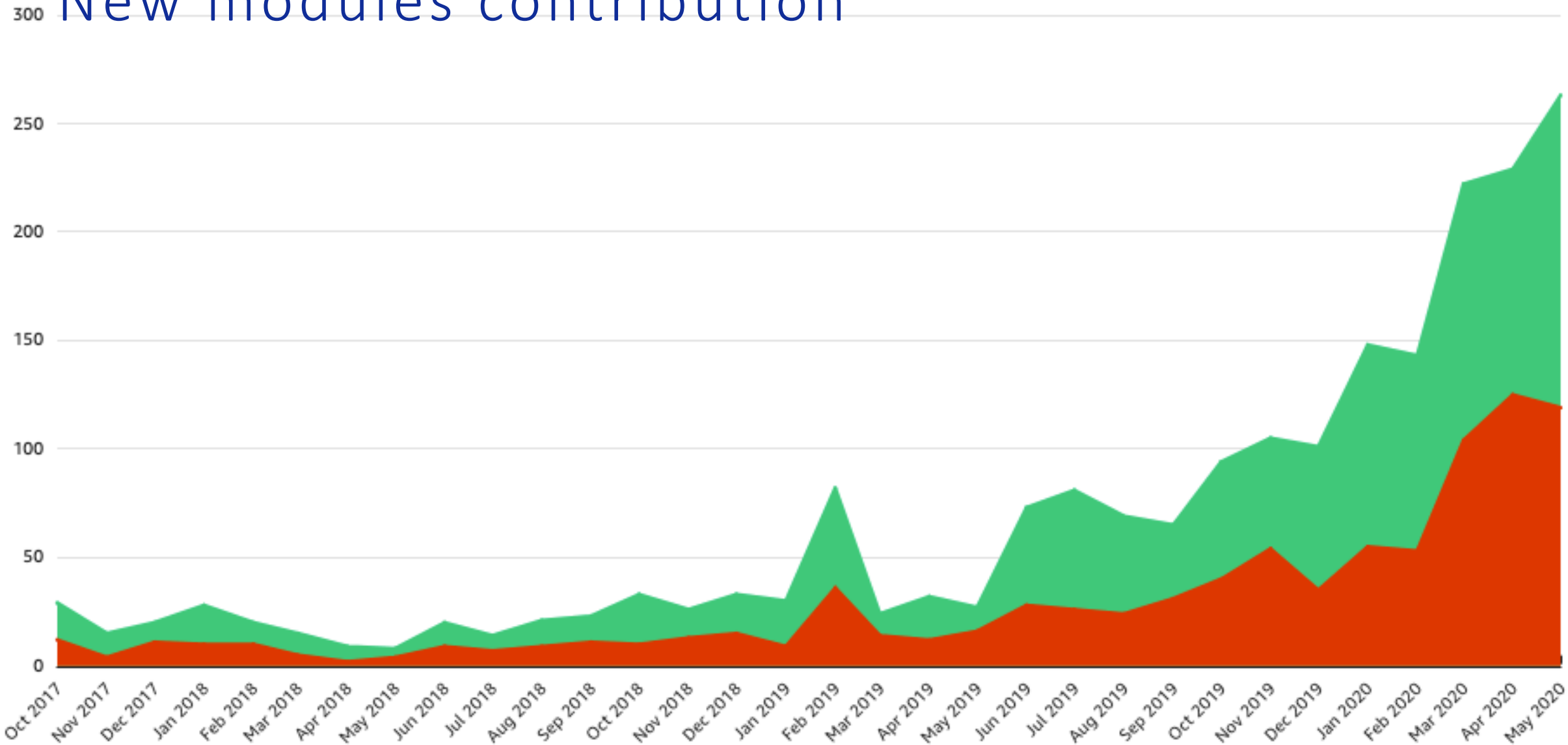
Open source misconfigured modules



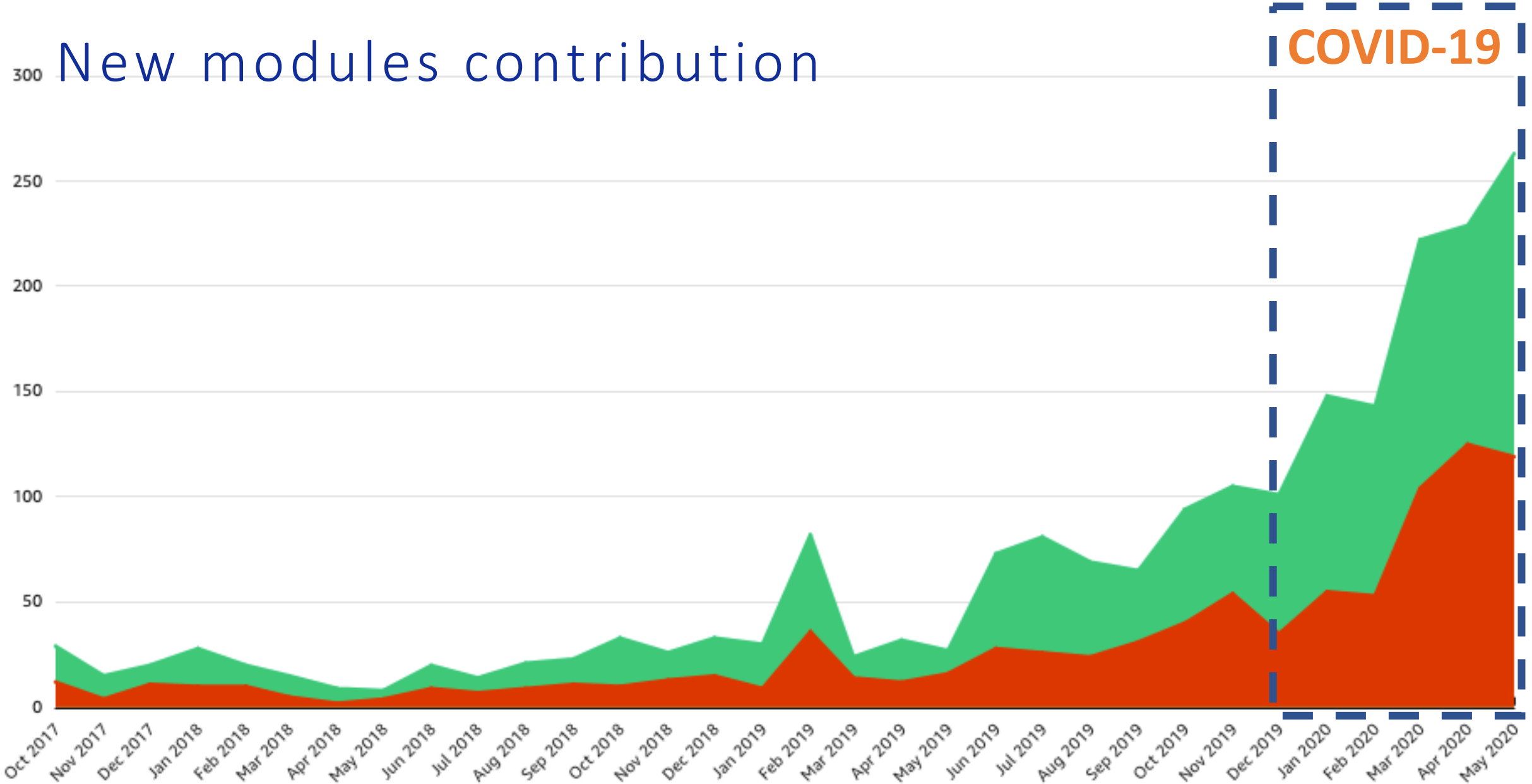
Downloads of misconfigured modules



New modules contribution

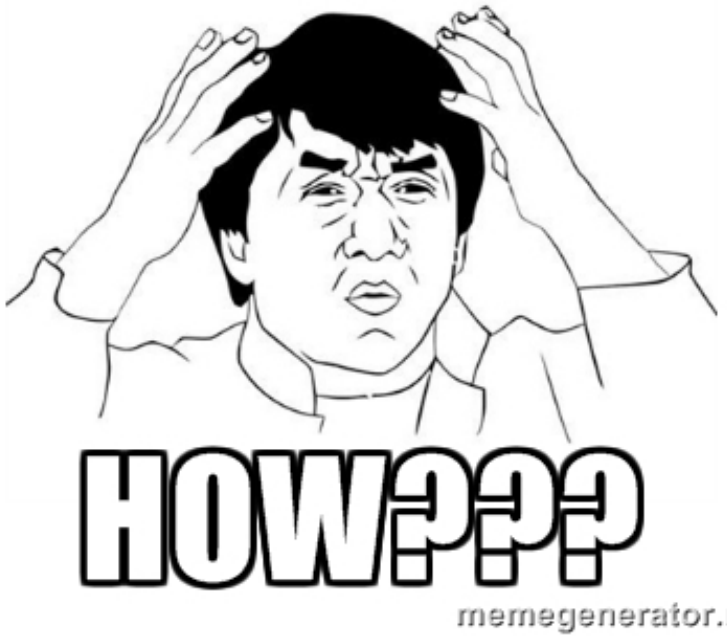


New modules contribution



KEEP CALM AND BREAK THINGS

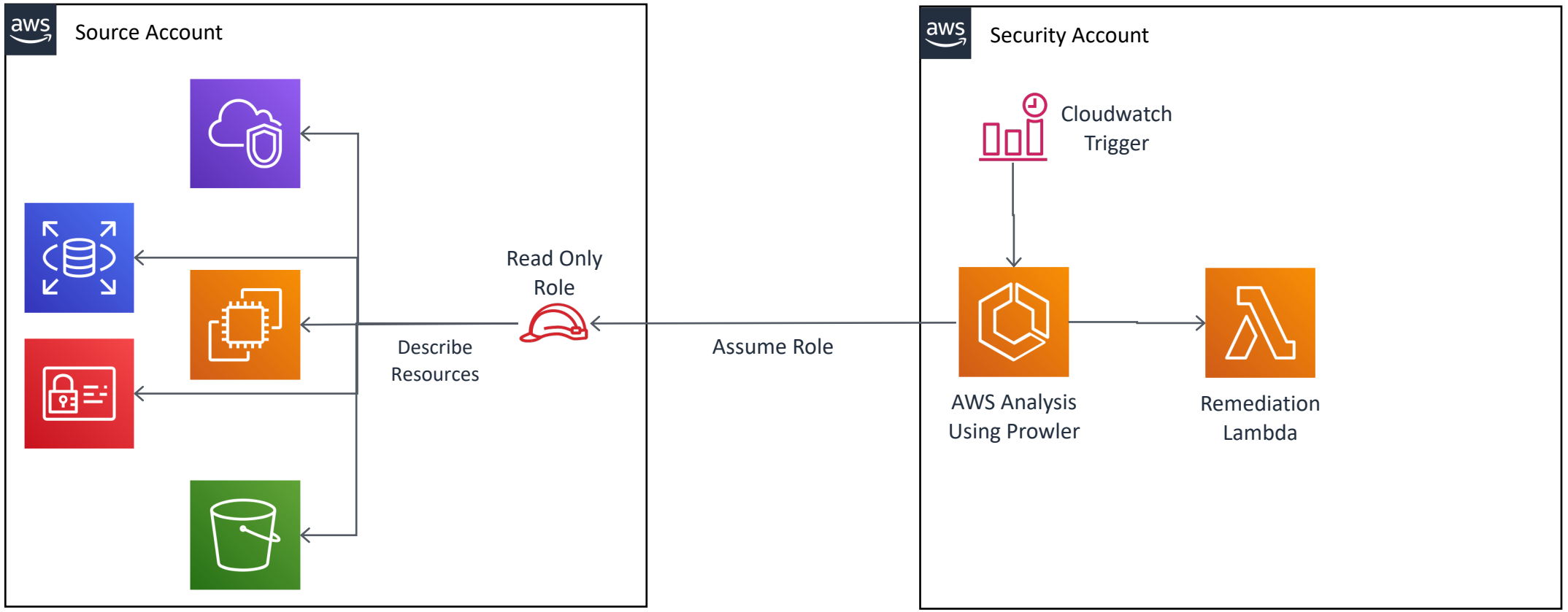
WITH STABLE INFRASTCTURE



Runtime detection of misconfig

- API Polling / Event Based (Cloudtrail, Cloudwatch)
- Identify drift from best practices
- Keeps you aware of your production environment state

Prowler Architecture



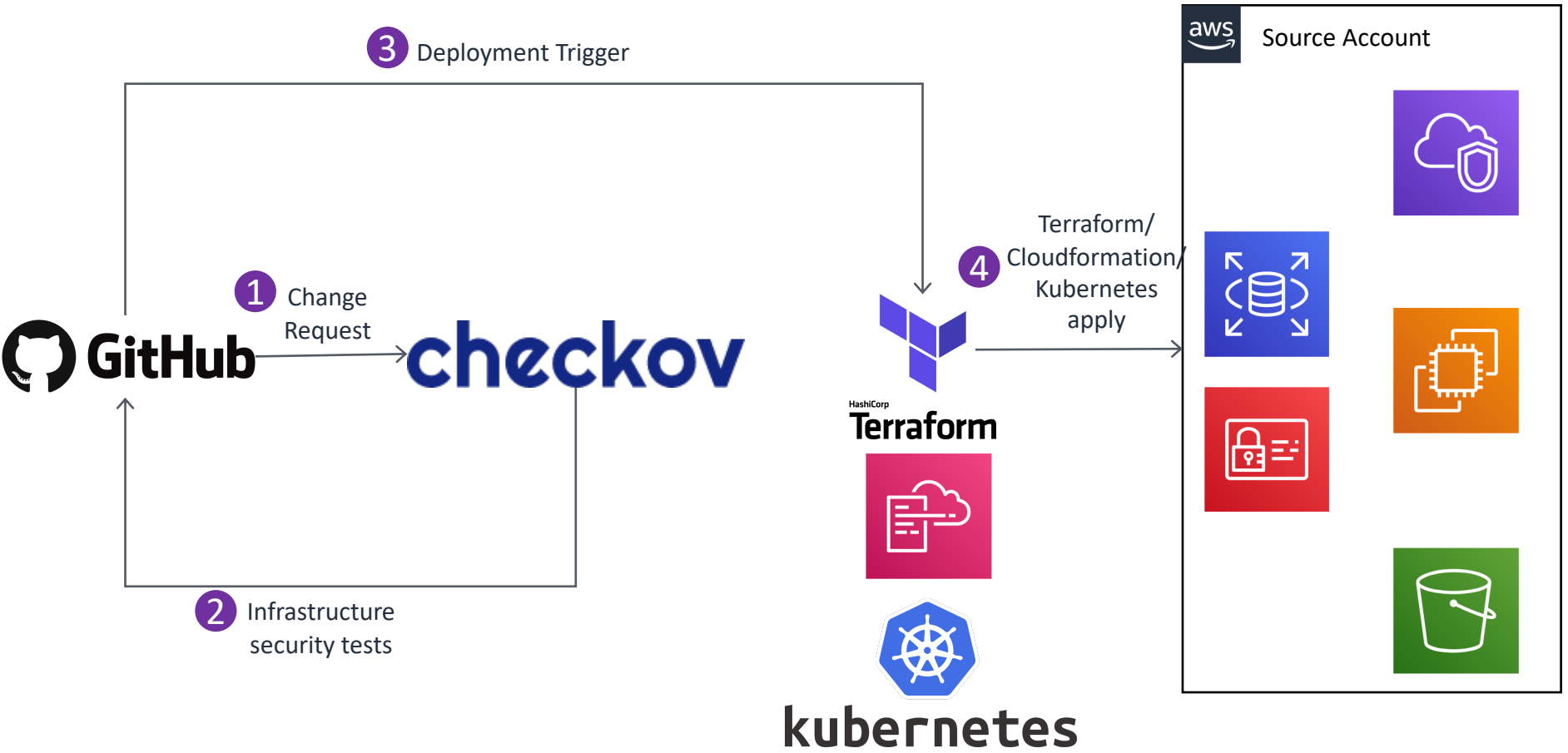
prowler v
the handy cloud security tool

How do we prevent them from coming back?

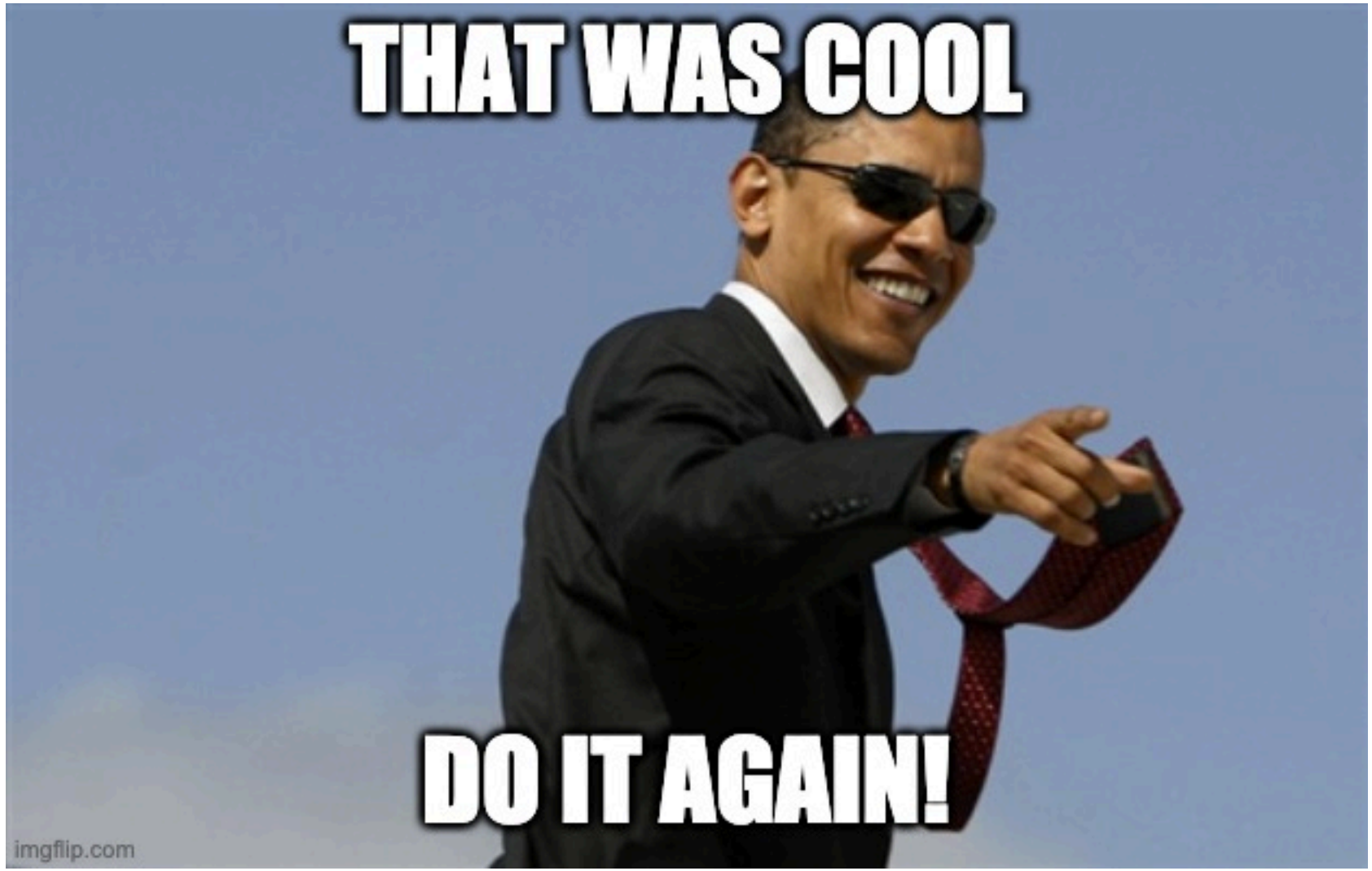
checkov
by bridgecrew

- Enable security infrastucture review distribution
- Apache-2 License
- Written in Pythonese
- 100+ built in checks for Cloudformation, Terraform and Kubernetes
- Checks can be skipped
- Support extention
- CI/CD Integrations

Checkov Architecture




DEMO
imgflip.com


THAT WAS COOL
DO IT AGAIN!
imgflip.com

TerraGoat & CfnGoat – 'Vulnerable-by-Design' Infrastructure Code

https://github.com/bridgecrewio/terragoat
https://github.com/bridgecrewio/cfngoat

bridgecrew

Pre-commit hook demo ahead of you

GitHub Action

Checkov Github Action

v9 Latest version

Use latest version

Checkov Github action

This Github Action runs Checkov against an Infrastructure-as-Code repository. Checkov performs static security analysis of Terraform & CloudFormation Infrastructure code .

Example usage

```yaml
jobs:
  checkov-job:
    runs-on: ubuntu-latest
    name: checkov-action
    steps:
      - name: Checkout repo
        uses: actions/checkout@v2

      - name: Run Checkov action
        id: checkov
        uses: bridgecrewio/checkov-action@master
        with:
          directory: example/
```

Stars

Star 3

Contributors

Categories

Security Code quality

Links

bridgecrewio/checkov-action

Open issues 0

Pull requests 0

Report abuse

Checkov Github Action is not certified by GitHub. It is provided by a third-party and

All checks have failed
1 failing check

Hide all checks

checkov infrastucture tests / build (3.7) (pull_request) Failing after 51s Details

This branch has no conflicts with the base branch
Merging can be performed automatically.

Merge pull request | You can also open this in GitHub Desktop or view command line instructions.

neckov infrastucture tests / **build (3.7)**
iled 1 minute ago in 54s

- Set up job
- Build bridgecrewio/checkov-action@v9
- Checkout repo
- Checkov Github Action

```
8                 _               _
9     ___| |__   ___  ___| | _____   __
10   / __| '_ \ / _ \/ __| |/ / _ \ \ / /
11  | (__| | | |  __/ (__|   < (_) \ V /
12   \___|_| |_|\___|\___|_|\_\___/ \_/

13 version: 1.0.263
14
15 terraform scan results:
```

https://github.com/bridgecrewio/checkov

README.md

Star 701

checkov
by bridgecrew

Table of contents

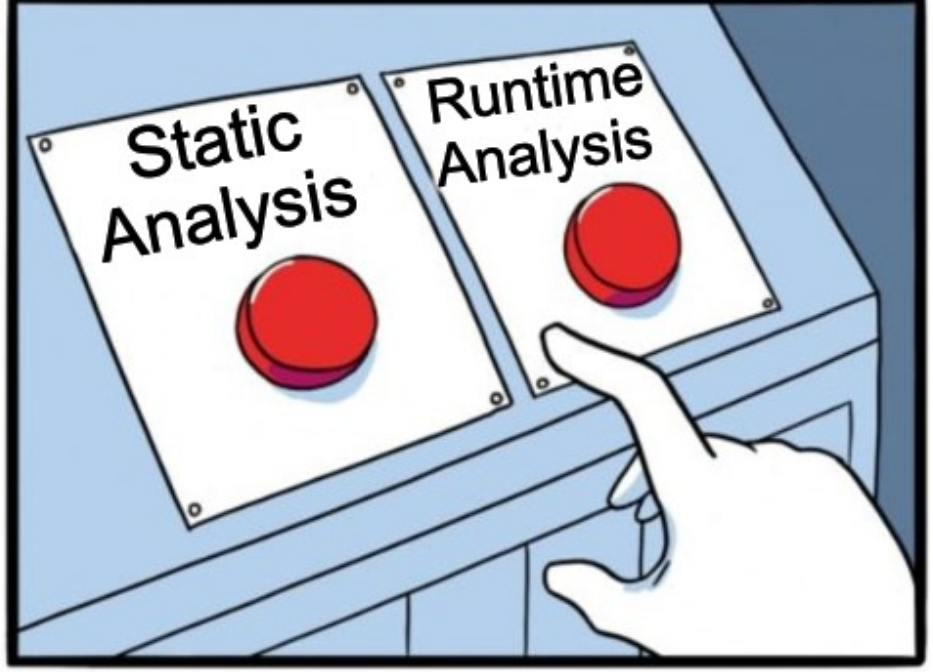
Key takeways

AWS Config Analysis

- ✗ Centralized in security
- ✓ Part of production monitoring
- ✓ Scalable across multiple accounts
- ✗ Minutes to identify
- ✗ Address: Compliance, Security, SRE

Static config analysis

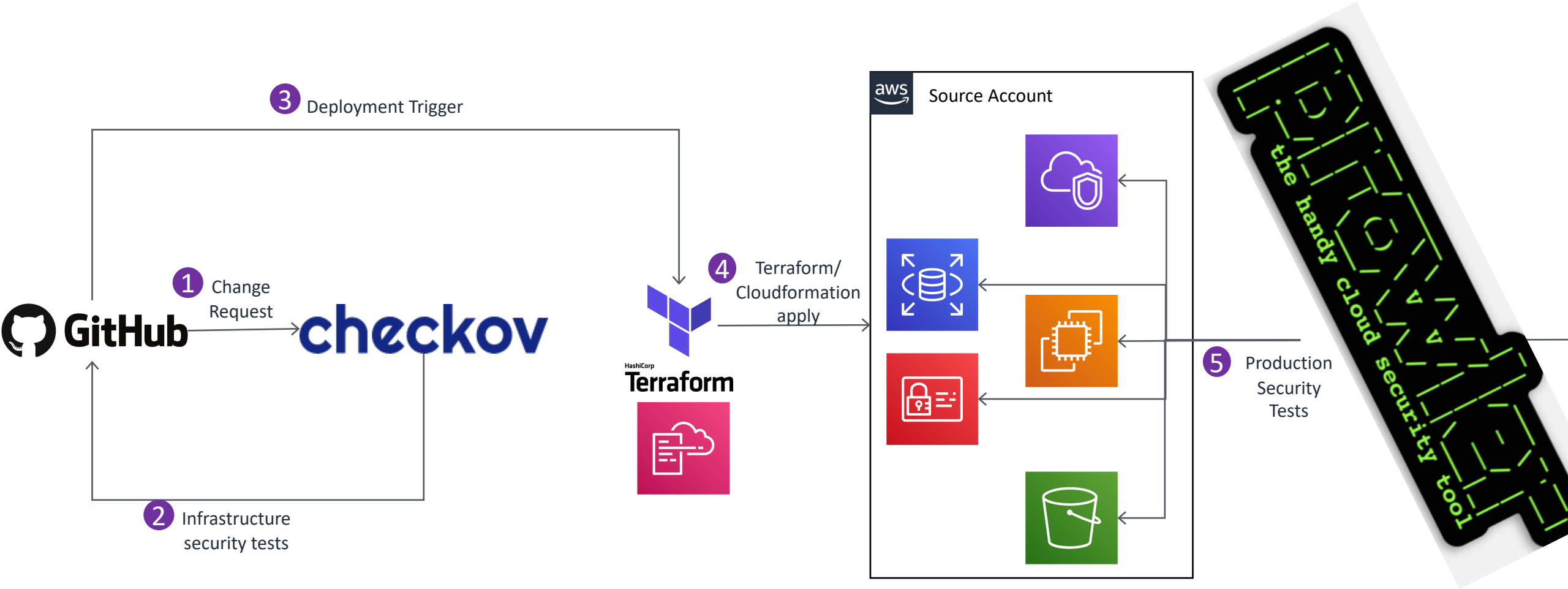
- ✓ Distributed in the engineering team
- ✓ Part of CI/CD
- ✓ Scalable across multiple repositories
- ✗ Not aware of production state
- ✓ Seconds to identify
- ✓ Address: developers



So… what should I do?


Both. Both. Both.
Both is good.

Checkov Architecture + Prowler



Questions?

Thank You!

github.com/schosterbarak

@barak_58758

@BarakSchoster

bridgecrew