bridgecrew

Part 1: The state of infrastructure security
Part 2: Scan for infrastructure encryption

@BarakSchoster

Co-Founder & CTO

OPEN SECURITY SUMMIT

Barak Schoster Goihman

Co-Founder & CTO at bridgecrew

@BarakSchoster

github.com/schosterbarak

aws

toniblyx/Prowler

duo-labs/cloudmapper

HashiCorp Terraform

CloudFormation

bridgecrewio/checkov

bridgecrewio/TerraGoat

bridgecrewio/CfnGoat

Google Cloud

GCP/terraform-pci-starter

I ♥ OPEN SOURCE

Tools you'll need during this session

- Git
- A Github account
- Python 3
- Terraform (optional)
- A python IDE (optional)

Agenda

1. Cloud infrastcture
2. Configuration security
3. Static analysis
4. Automating (lack of) encryption detection in CI/CD
5. Conclusions

Part 1: The state of infrastructure security

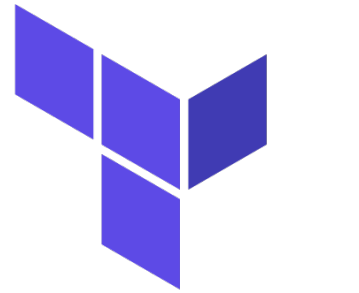

untangle
untangle
untangle

```
resource "aws_security_group" "allow_tls" {
  name        = "allow_tls"
  description = "Allow TLS inbound traffic"
  vpc_id      = "${aws_vpc.main.id}"

  ingress {
    description = "TLS from VPC"
    from_port   = 443
    to_port     = 443
    protocol    = "tcp"
    cidr_blocks = [aws_vpc.main.cidr_block]
  }

  egress {
    from_port   = 0
    to_port     = 0
    protocol    = "-1"
    cidr_blocks = ["0.0.0.0/0"]
  }

  tags = {
    Name = "allow_tls"
  }
}
```

HashiCorp Terraform

What is IaC

- Define architecture in code
- Automates creation of resources
- Platform agnostic
- State management
- Operator confidence



Configuration in code is increasing

What is infrastructure security?

Configuration errors found in the wild

DEFAULT CONFIGURATIONS

DISABLED LOGGING

UNENCRYPTED DATABASES

INSECURE PROTOCOLS

VULNERABLE MIROSERVICES

Where do bad configurations come from?

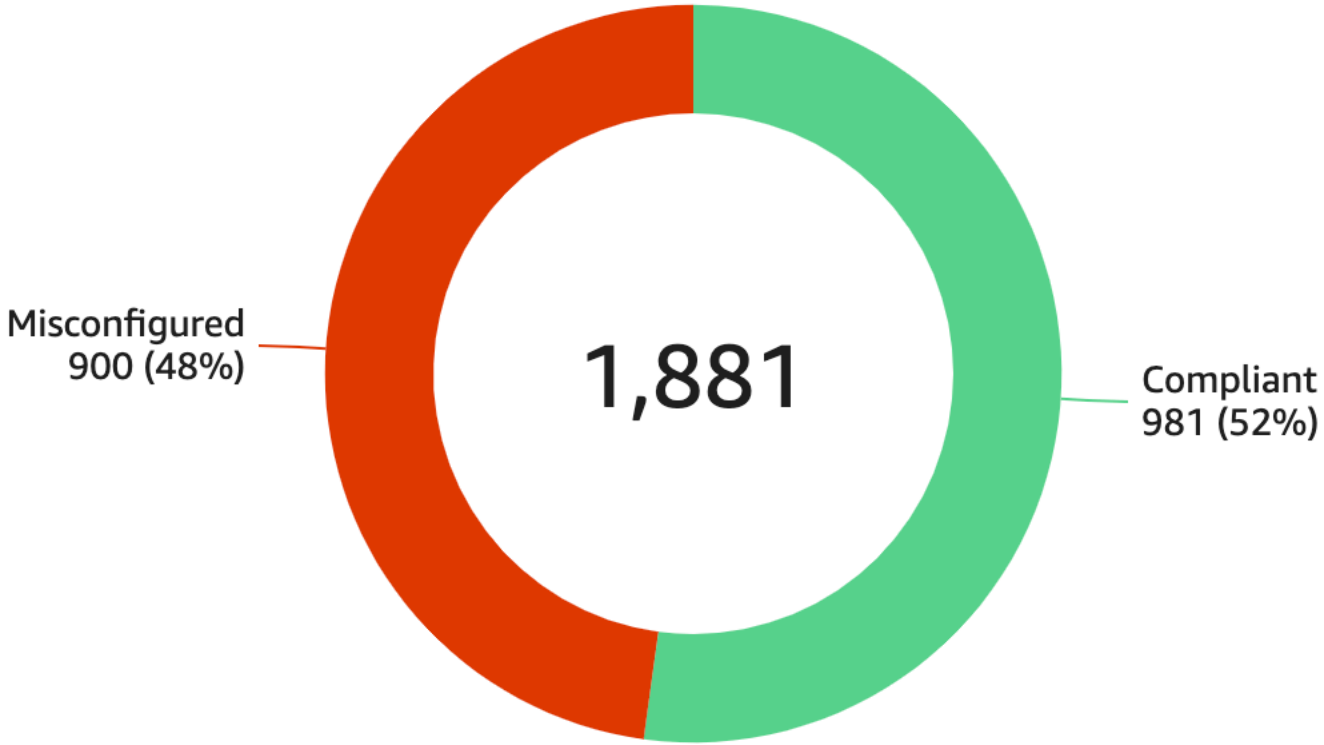
aws

Google Cloud

HashiCorp Terraform | Registry

GitHub

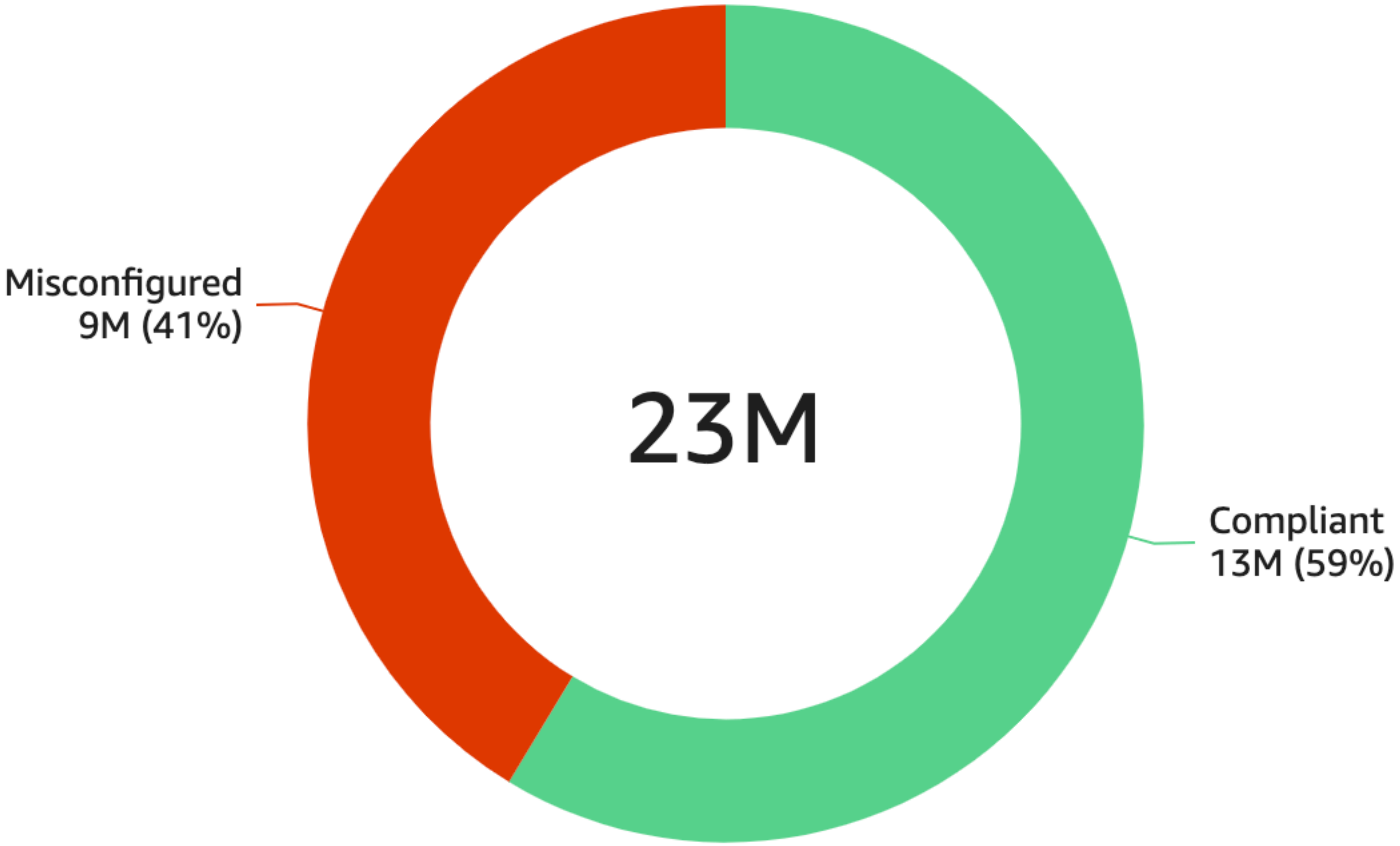
Open source misconfigured modules



15,749 Terraform files

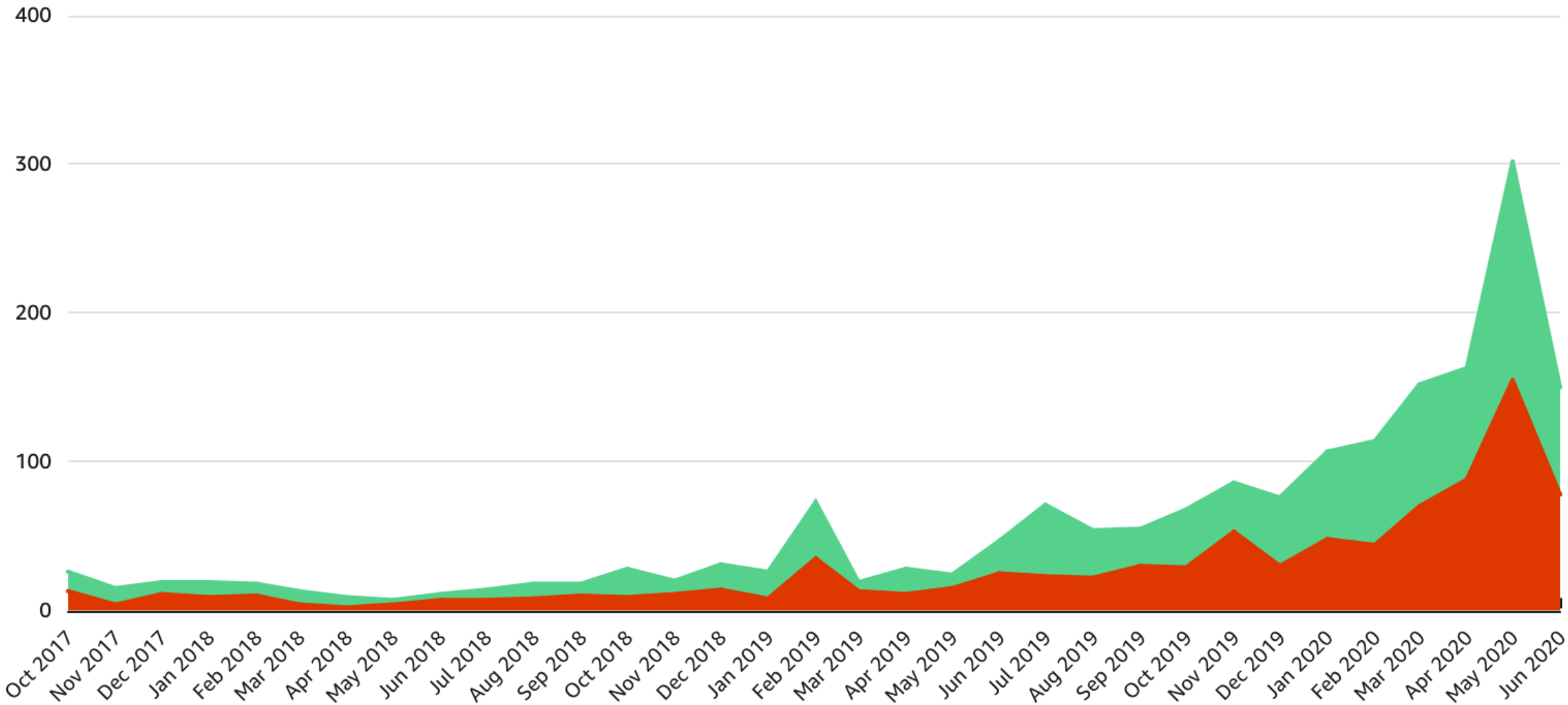
1881 Terraform AWS modules

Downloads of misconfigured modules

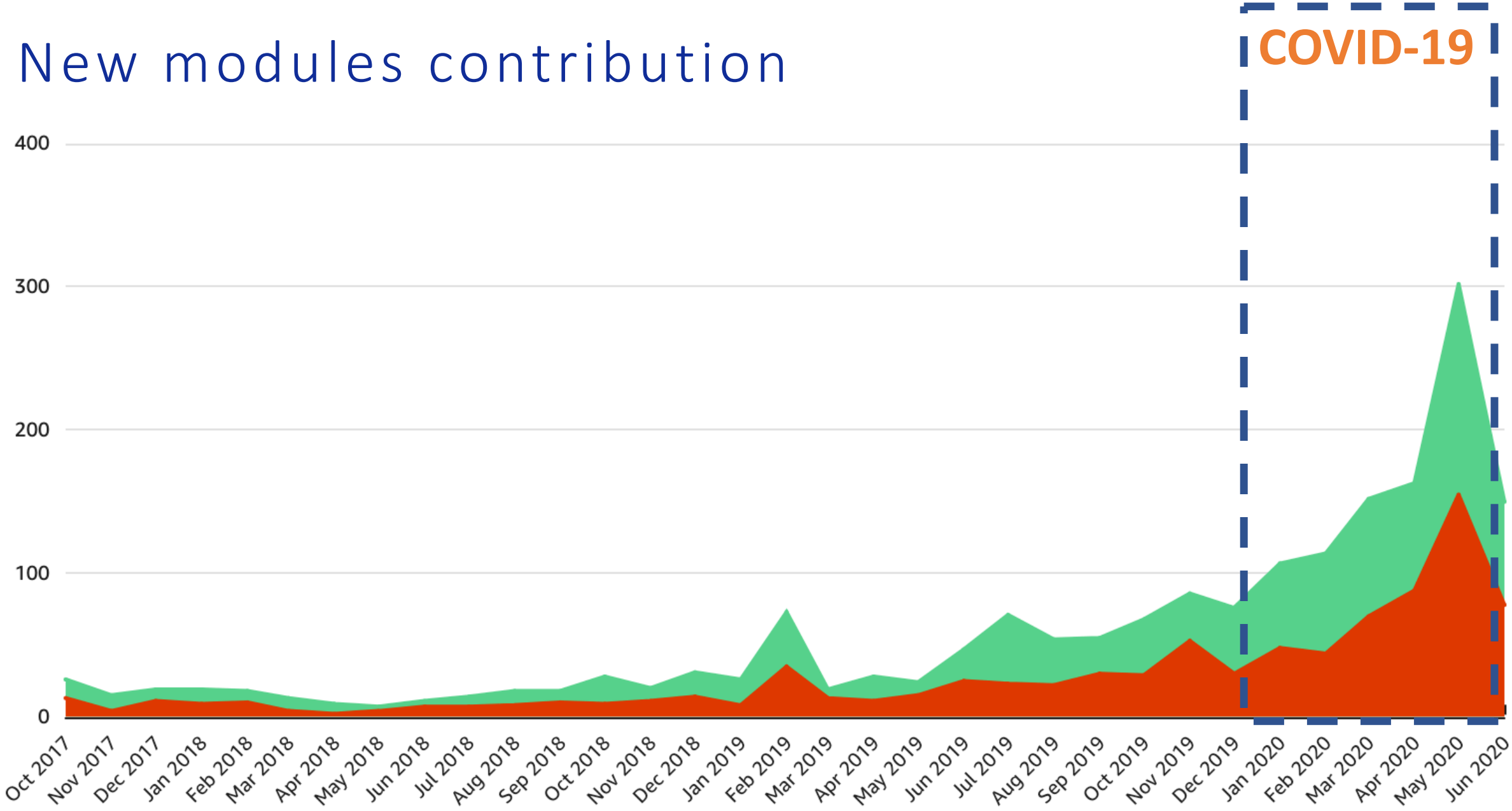


What kind of security mistakes get made when defining infrastcture with code?

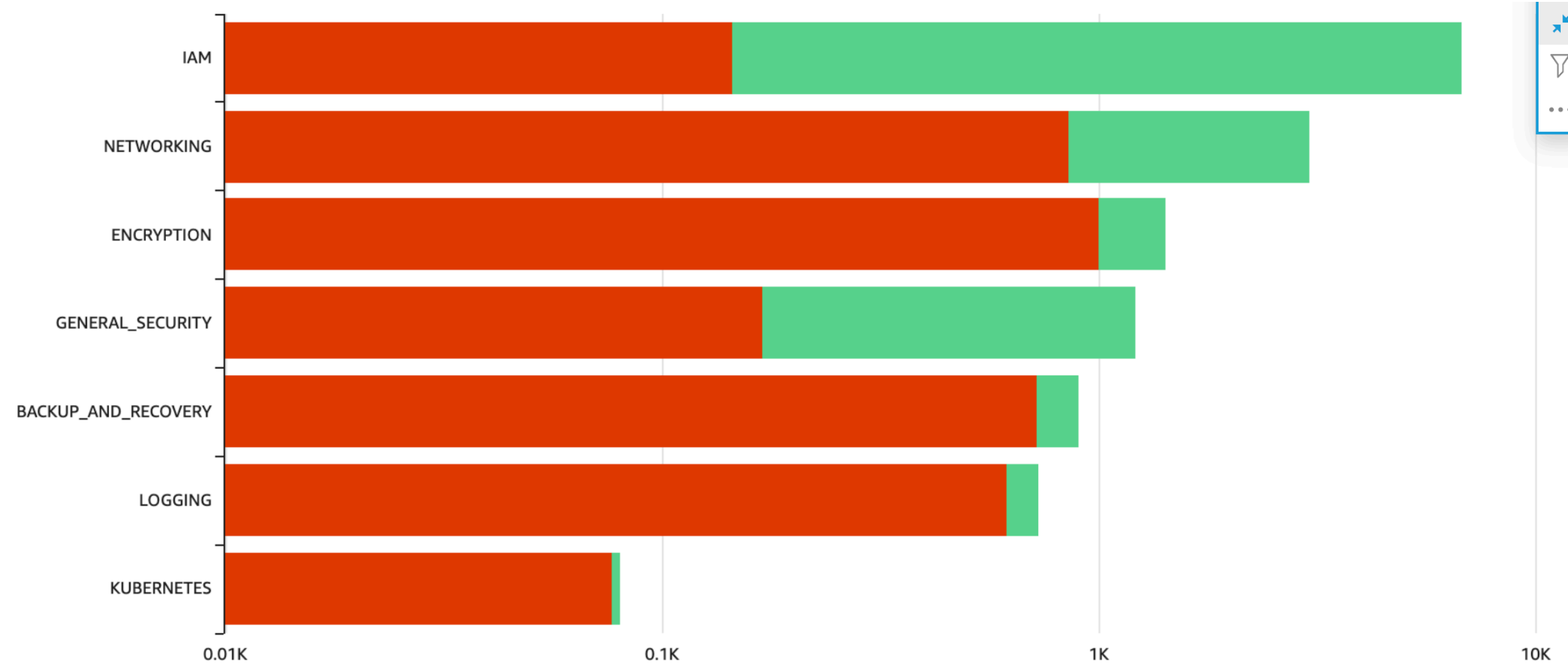
New modules contribution



New modules contribution



Misconfiguration categories



Encryption

- Is one of the most commonly forgotten configurations
- One of the easiest to resolve
- Does not have a high impact on cost when used correctly

More good stuff

- The heavy lifting of key management is done
- If a bucket is public and encrypted with CMK, an anonimous user will get 401 response (no permmisions to decrypt)

How easy it is to encrypt

try-bridgecrew/terragoat : aws_ebs_snapshot.example_snapshot

Repository *try-bridgecrew/terragoat*

File Name */terraform/ec2.tf*

```
35 35      resource "aws_ebs_snapshot" "example_snapshot" {
36 36        # ebs snapshot without encryption
37 37        volume_id   = "${aws_ebs_volume.web_host_storage.id}"
38 38        description = "${local.resource_prefix.value}-ebs-snapshot"
39 39        tags = {
40 40          Name = "${local.resource_prefix.value}-ebs-snapshot"
41 41        }
   42 +      encrypted = true
42 43      }
```

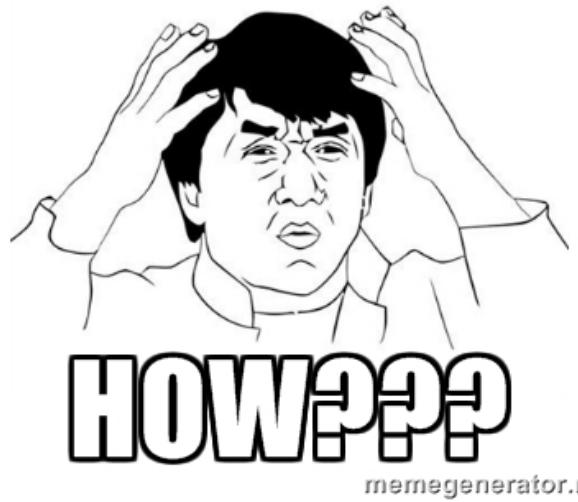
Caveats

- For some resources – you can only turn on encryption on creation. Turning on encryption my delete the resource.
- For s3 – encryption at rest will not encrypt historical records/versions

Who “owns” misconfigs?

KEEP CALM AND BREAK THINGS

HOW TO FIND A BAD CONFIG



@BarakSchoster

bridgecrew

Part 2: Scan for infrastructure encryption

TerraGoat– ’Vulnerable-by-Design’ Terraform Code

https://github.com/bridgecrewio/terragoat

README.md

Unstar 135

TerraGoat - Vulnerable Terraform Infrastructure

maintained by bridgecrew.io tf >=0.12.0

TerraGoat is Bridgecrew's "Vulnerable by Design" Terraform repository.

@

How do we prevent them from coming back?

https://github.com/bridgecrewio/checkov

README.md

Unstar 760

checkov
by bridgecrew

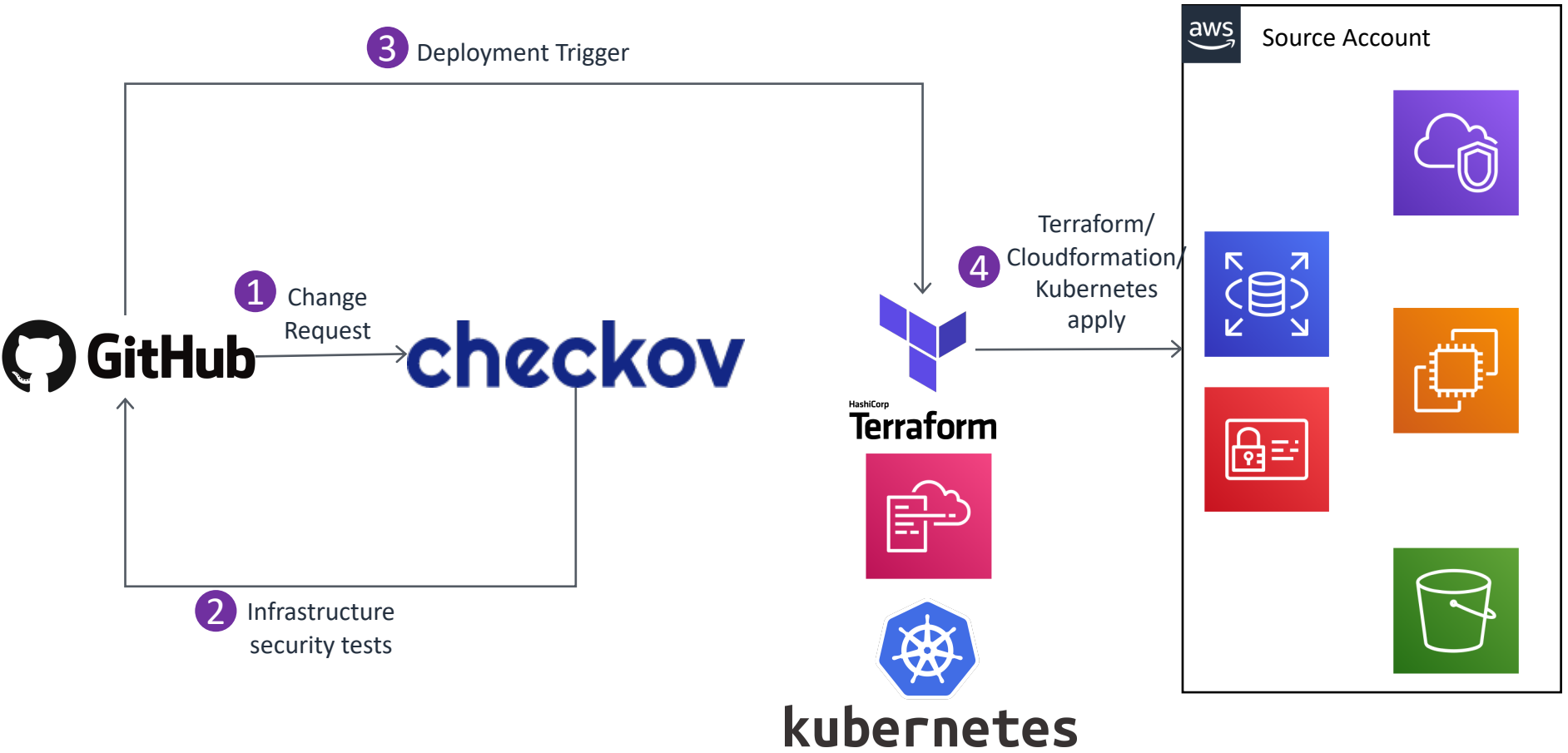
maintained by bridgecrew.io | build passing | coverage 84% | docs passing | pypi v1.0.324 | downloads 371k | tf >=0.12.0

Table of contents

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



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

Create new webserver in terraform #1

Open try-bridgecrew wants to merge 2 commits into `master` from `new-terraform-file`

Conversation 0 | Commits 2 | Checks 1 | Files changed 1 | +199 −0

Changes from all commits | File filter... | Jump to... | 0 / 1 files viewed | Review changes

199 ec2.tf — Viewed

```
@@ -0,0 +1,199 @@
+ resource "aws_instance" "web_host" {
```

Check failure on line 1 in ec2.tf

GitHub Actions / bridgecrew-action

ec2.tf#L1

CKV_AWS_46: "Ensure no hard coded AWS access key and and secret key exists in EC2 user data"

Check failure on line 1 in ec2.tf

GitHub Actions / bridgecrew-action

ec2.tf#L1

CKV_AWS_8: "Ensure all data stored in the Launch configuration EBS is securely encrypted "

```
+   # ec2 have plain text secrets in user data
+   ami           = "${var.ami}"
```

All checks have failed

1 failing check

Hide all checks

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

Key takeways

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

Questions?

Thank You!

github.com/schosterbarak

@barak_58758

@BarakSchoster

bridgecrew