
CRUSHING
Cloud misconfiguration
MTTR
Featuring:
• Yor: Automated IaC tag and trace
• Checkov: IaC Scanning
The assailant:
Steve Giguere
@_SteveGiguere_

# THE ALERT

**PagerDuty** APP 1:49 PM

Triggered: Misconfig found on EBS Volume

Assigned: Jane SRE  Triggered by: Bridgecrew

Service: AWS

Acknowledge | Resolve | More actions...

# THE SCRAMBLE

**Barak Schoster** 55 minutes ago
Hey @here who created this volume?

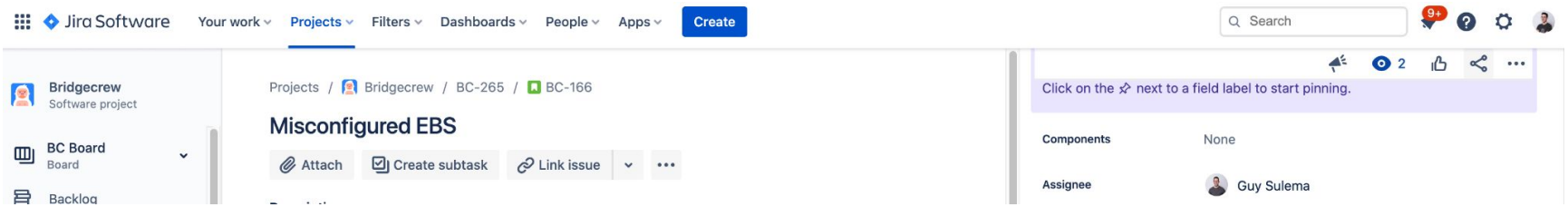
**Barak Schoster** 6 minutes ago
Cloudtrail show's `terraform`

**Nimrod Kor** 5 minutes ago
Did anyone trigger a release on Friday?

**Barak Schoster** 4 minutes ago
Can you ask @Guy Sulema from the cloud services team who owns this AWS account? (edited)

**Guy Sulema** 3 minutes ago
oh it's part of the application BU. a team of 142 engineers have access to this account and I see the github org has 50 repositories with Terraform files....

# THE JIRA(S)

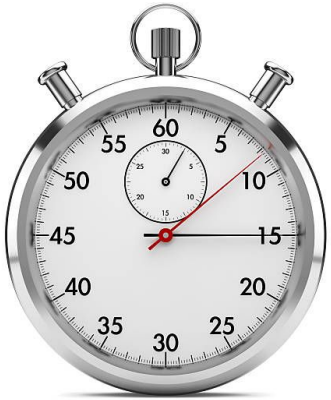



- An imperative fix via the AWS console to bring the resource back into compliance while we await detective work on a fix to  complete

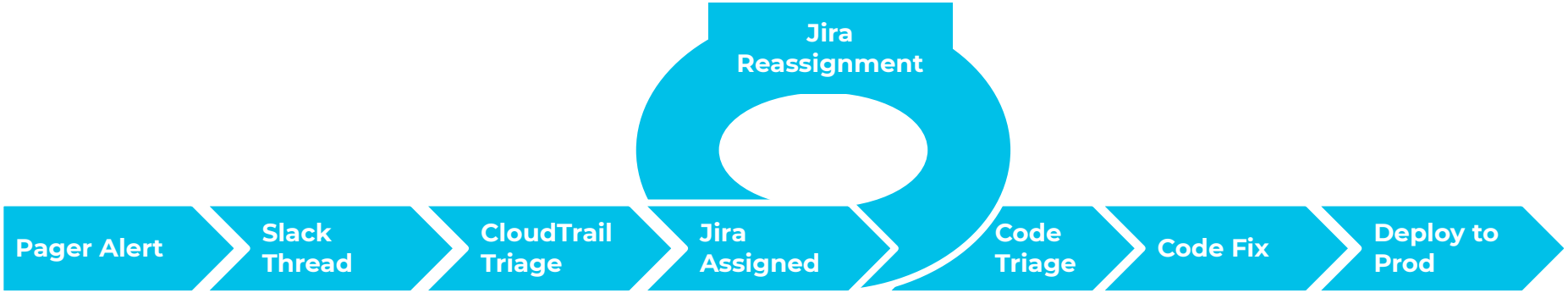
# THE FIX?

- An imperative fix via the AWS console brings the resource back into compliance while we await detective work on a fix our **Infrastructure as Code**

- But for how long?



# THE PROCESS




**MTTR IS TOO LONG**

# Who is... Steve Giguere (schig-air)


- **Developer Advocate - Bridgecrew**
- **DevSecOps Enthusiast**
- **Raspberry Pi Geek**
- **Formerly:** Aqua Security, StackRox, Synopsys Software Integrity Group

bridgecrew
BY PRISMA® CLOUD

- **Twitch show:** Clust3rF8ck (.com)
- **Podcaster:** BeerSecOps, CoSeCast (.com)
- **Beer Taster:** BeerNative (.tv)

# What is Infrastructure as Code (IaC)

# What is Infrastructure as Code (IaC)

Procedural (eg. Ansible)

**Declarative (eg. Terraform)**

# What is Infrastructure as Code (IaC)

## Procedural (eg. Ansible)

*Preheat oven to 160*
*Mix flour, eggs, sugar and butter until "fluffy"*

*Bake for 30mins until cake is crisp and springy*

*For the icing, beat the butter cream, icing sugar....*

## Declarative (eg. Terraform)

```
resource "cake" "birthday surprise"
{
      Icing = "chocolate"
      Fondant = false
      Sponge = "Chocolate"
      Texture = "fluffy"
      Diameter = 40
      Layers = 2
}
```

# What is Drift?

When your IaC no longer matches the runtime resource configuration it deployed

## Terraform IaC

```
resource "cake" "birthday surprise"
{
      Icing = "chocolate"
      Fondant = false
      Sponge = "Chocolate"
      Texture = "fluffy"
      Diameter = 40
      Layers = 2
}
```

DRIFT!

## Runtime

```
resource "cake" "birthday surprise"
{
      Icing = "concrete"
      Fondant = false
      Sponge = "Chocolate"
      Texture = "fluffy"
      Diameter = 40
      Layers = 2
}
```

# What is checkov by bridgecrew ?


Open source (Apache 2.0)
**misconfiguration scanner for IaC**,
intended to be used in CI/CD pipelines

1. 500+ built in checks
2. Supports extensions
3. Built in best practices for ownership

# What is Checkov

checkov by bridgecrew

- Open source
- Analyze infrastructure as code (IaC)
- Terraform, CloudFormation, Kubernetes, Helm, ARM Templates and Serverless framework
- > 500 rules

- VSCode Plugin
- Optional config file
  - *.checkov.yaml*

```
Check: CKV_AWS_19: "Ensure all data stored in the S3 bucket is securely encrypted at rest"
        FAILED for resource: aws_s3_bucket.data_science
        File: /s3.tf:99-124
        Guide: https://docs.bridgecrew.io/docs/s3_14-data-encrypted-at-rest

Check: CKV_AWS_144: "Ensure that S3 bucket has cross-region replication enabled"
        FAILED for resource: aws_s3_bucket.data_science
        File: /s3.tf:99-124
        Guide: https://docs.bridgecrew.io/docs/ensure-that-s3-bucket-has-cross-region-replication-enabled

Check: CKV_AWS_145: "Ensure that S3 buckets are encrypted with KMS by default"
        FAILED for resource: aws_s3_bucket.data_science
        File: /s3.tf:99-124
        Guide: https://docs.bridgecrew.io/docs/ensure-that-s3-buckets-are-encrypted-with-kms-by-default

Check: CKV_AWS_18: "Ensure the S3 bucket has access logging enabled"
        FAILED for resource: aws_s3_bucket.logs
        File: /s3.tf:126-156
        Guide: https://docs.bridgecrew.io/docs/s3_13-enable-logging

Check: CKV_AWS_144: "Ensure that S3 bucket has cross-region replication enabled"
        FAILED for resource: aws_s3_bucket.logs
        File: /s3.tf:126-156
        Guide: https://docs.bridgecrew.io/docs/ensure-that-s3-bucket-has-cross-region-replication-enabled

Check: CKV2_AWS_1: "Ensure that all NACL are attached to subnets"
        FAILED for resource: aws_vpc.web_vpc
        File: /ec2.tf:126-144
        Guide: https://docs.bridgecrew.io/docs/ensure-that-all-nacl-are-attached-to-subnets
```

# Configuration errors found in the wild & new IaC configurations

DEFAULT CONFIGURATIONS

DISABLED LOGGING

UNENCRYPTED DATABASES

INSECURE PROTOCOLS

VULNERABLE MICROSERVICES

*

# What is YOR?


Open source (Apache 2.0) **tagging framework for IaC**, intended to be used in CI/CD pipelines with GitOps practices

1. Automated tagging
2. Built in best practices for tracing
3. Built in best practices for ownership

# Trace cloud to code through tagging

## Tagging Best Practices

Implement an Effective AWS Resource Tagging Strategy

*December, 2018*

aws

# Tagging use cases

YOR by bridgecrew

**Security Risk Management**
identify resources that require heightened security

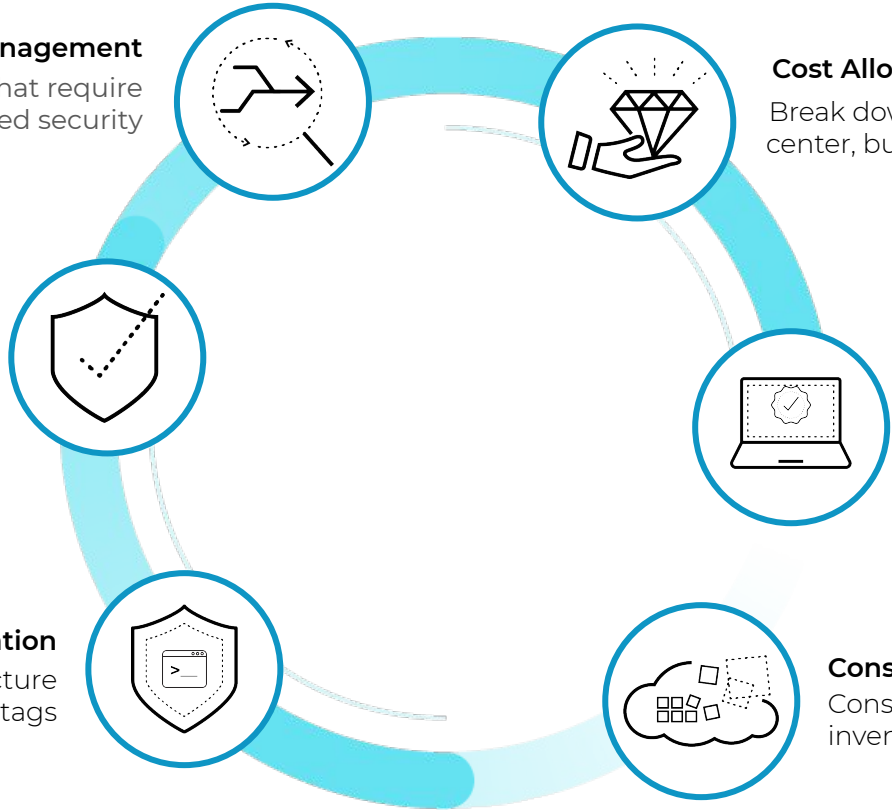
**Cost Allocation**
Break down cost by tag of cost center, business unit or project

**Access Control**
IAM policies conditions based on tags

**Operation Support**
Incident management triage using tags

**Automation**
Opt in and out infrastructure scaling scripts using tags

**Console Organization**
Consolidate resource groups inventory based on tags



 © 2021 Palo Alto Networks, Inc. All rights reserved.

paloalto NETWORKS

# Tagging with YOR

```
tags = {
  Name                 = "${local.resource_prefix.value}-customer-master"
  Environment          = local.resource_prefix.value
  git_commit           = "d68d2897add9bc2203a5ed0632a5cdd8ff8cefb0"
  git_file             = "terraform/aws/s3.tf"
  git_last_modified_at = "2021-06-16 14:46:24"
  git_last_modified_by = "nimrodkor@gmail.com"
  git_modifiers        = "nimrodkor"
  git_org              = "eurogig"
  git_repo             = "terragoat"
  yor_trace            ="c9f490f8-7d0f-42c3-b24a-fa6b18524295"
}
```

*

# Creating a slack workflow from Yor Tags

**steve** APP 11:32 AM

Amazon S3 bucket is not encrypted with AWS KMS key

Resource id: 481212720429-acme-dev-flowlogs

Last modifier: <@Steve G@gmail.com>

Last modified: 2021-06-17 14:06:28

You can trace the resource from cloud to code: See the resource

Trace on GitHub | See Commit on GitHub | See Resource on AWS

# Tagging with YOR

```yaml
tag_groups:
  - name: access
    tags:
      - name: level
        value:
          default: development
          matches:
            - development:
                tags:
                  git_org:
                    - eurogig
                    - tronxd
                    - mattj
            - operations:
                tags:
                  git_org:
                    - bridgecrew
                    - nofar
                    - nimrodkor
```

# Tagging with YOR

```
tags = {
  Name                 = "${local.resource_prefix.value}-customer-master"
  Environment          = local.resource_prefix.value
  git_commit           = "d68d2897add9bc2203a5ed0632a5cdd8ff8cefb0"
  git_file             = "terraform/aws/s3.tf"
  git_last_modified_at = "2021-06-16 14:46:24"
  git_last_modified_by = "eurogig@tagging.com"
  git_modifiers        = "eurogig"
  git_org              = "eurogig"
  git_repo             = "terragoat"
  level                = "development"
  team                 = "platform"
  yor_trace            ="c9f490f8-7d0f-42c3-b24a-fa6b18524295"
}
```

# Integrating Checkov & Yor into the GitOps workflow

# Integrating Yor and Checkov

Policy as Code

checkov

Enrichment engine

YOR

**Example** | Allow only the **security team** to edit CloudTrail configurations

# Key Takeaways

- Open Source Rocks
- Shift left (decisions, planning/state, security)
  - Test Early and often
- Everything as Code
- GitOps as a source of truth
- Scan IaC Early
- Tag Everything!

Checkov: https://www.checkov.io/

Yor: https://yor.io

Our blog: https://bridgecrew.io/blog

# THANKS!