Security linting of
CloudFormation scripts

Xavi Mendez
Security automation lead

- Founded in 2003
- Over **1000** employees across the world
- **10** global offices - **Barcelona**, Beijing, Budapest, Edinburgh, Glasgow, London, Miami, Shenzhen, Singapore and Sofia
- Average **70M** unique monthly visitors
- Over **70M** app downloads
- Available in over **30** languages

“Lean principles and fast iterations”

“Fail fast and learn fast”

“You build it you run it”

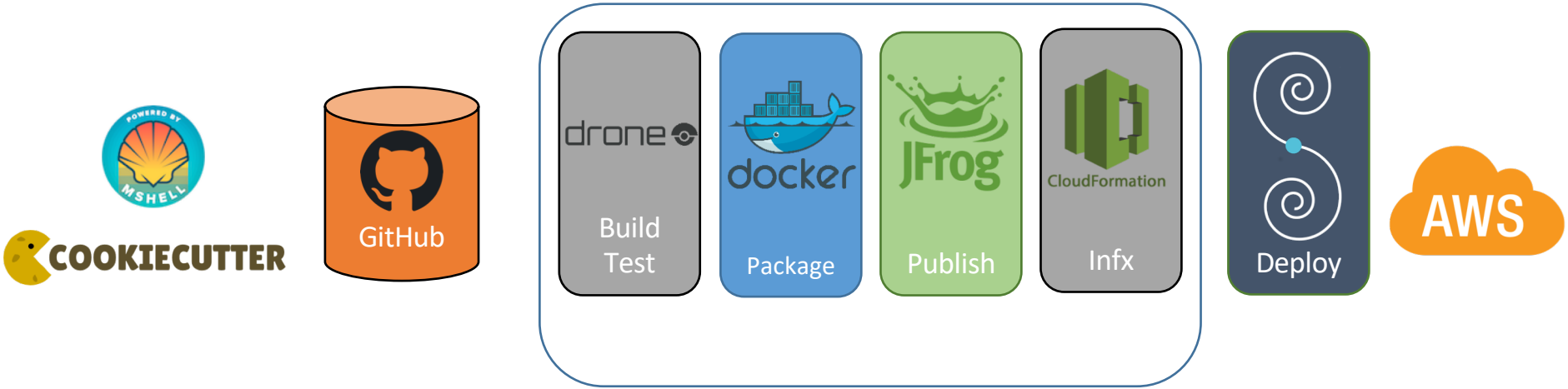
“10.000 changes a day to production in “zero clicks”.

7000+projects in GitHub

1000+ distinct services in production

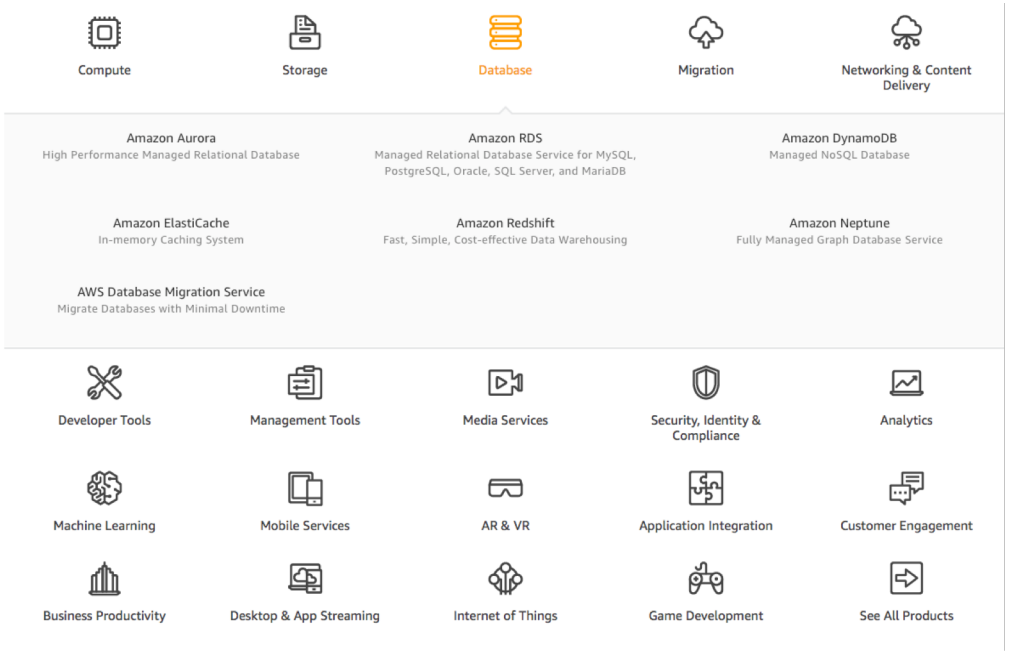
Thousands of infrastructure deployments/updates every week

This is a ship-shipping ship, shipping shipping ships



From source to service in zero clicks

CloudFormation



```
{
    "AWSTemplateFormatVersion" : "2010-09-09",

    "Description" : "AWS CloudFormation Sample Template",

    "Resources" : {
      "S3Bucket" : {
        "Type" : "AWS::S3::Bucket",
        "Properties" : {
          "AccessControl" : "PublicRead",
          "WebsiteConfiguration" : {
            "IndexDocument" : "index.html",
            "ErrorDocument" : "error.html"
          }
        },
        "DeletionPolicy" : "Retain"
      }
    },

    "Outputs" : {
      "WebsiteURL" : {
        "Value" : { "Fn::GetAtt" : [ "S3Bucket", "WebsiteURL" ] },
        "Description" : "URL for website hosted on S3"
      },
      "S3BucketSecureURL" : {
        "Value" : { "Fn::Join" : [ "", [ "https://", { "Fn::GetAtt" : [ "S3Bucket", "DomainName" ] } ] ] },
        "Description" : "Name of S3 bucket to hold website content"
      }
    }
  }
```

November 02, 2017

Another misconfigured Amazon S3 server leaks data of 50,000 Australian employees

Gartner on the Pentagon's 'misconfigured' AWS S3 bucket data leak

Leaked FedEx customer data was stored on Amazon S3 server with no password

The incident-one of many related to S3 repositories-put thousands of customer records at risk.

By Conner Forrest | February 15, 2018, 10:35 AM PST

DIGGING FOR MONERO

New crypto-mining malware uses Amazon's cloud to hijack computers

By John Detrixhe · May 29, 2018

amazon
EMR

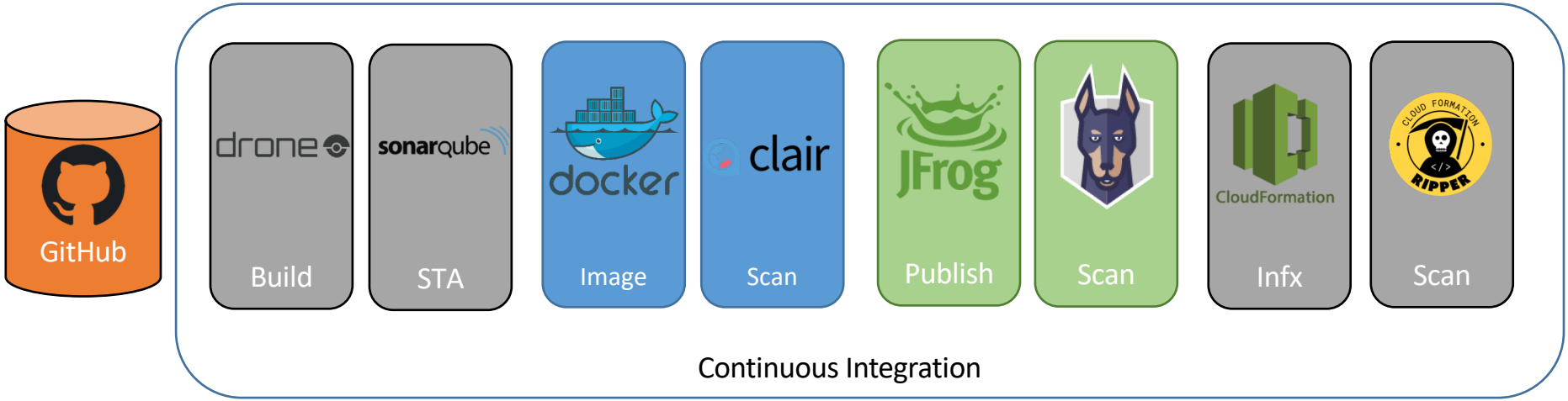
Security group

bugcrowd

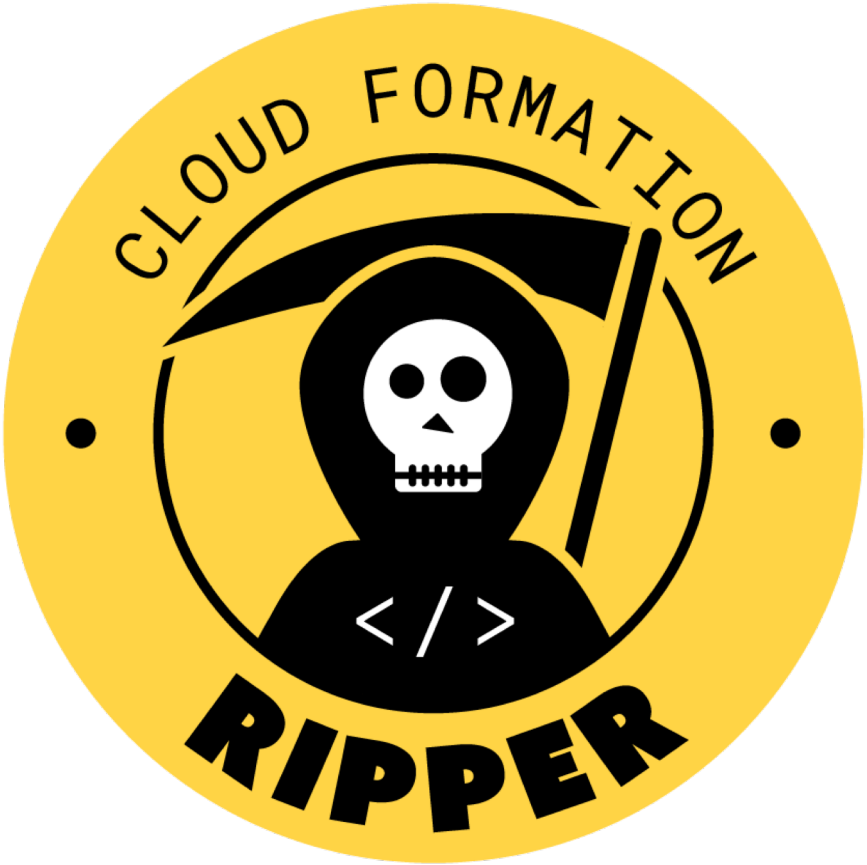
Permission misconfigurations allow privilege escalation:

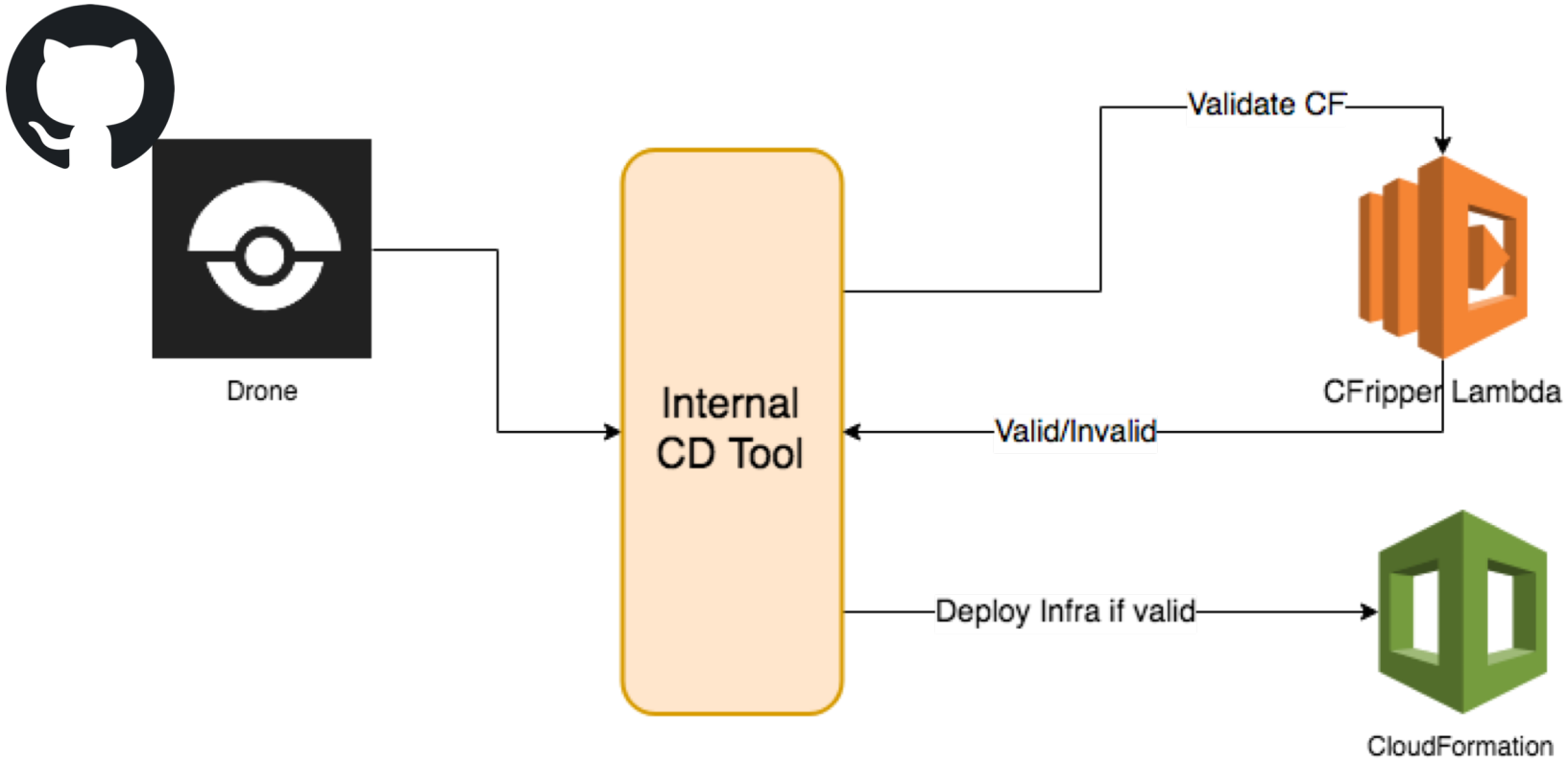
```
"Effect": "Allow",
"NotAction": "iam:*",
"Resource": "*"
```

https://github.com/RhinoSecurityLabs/pacu

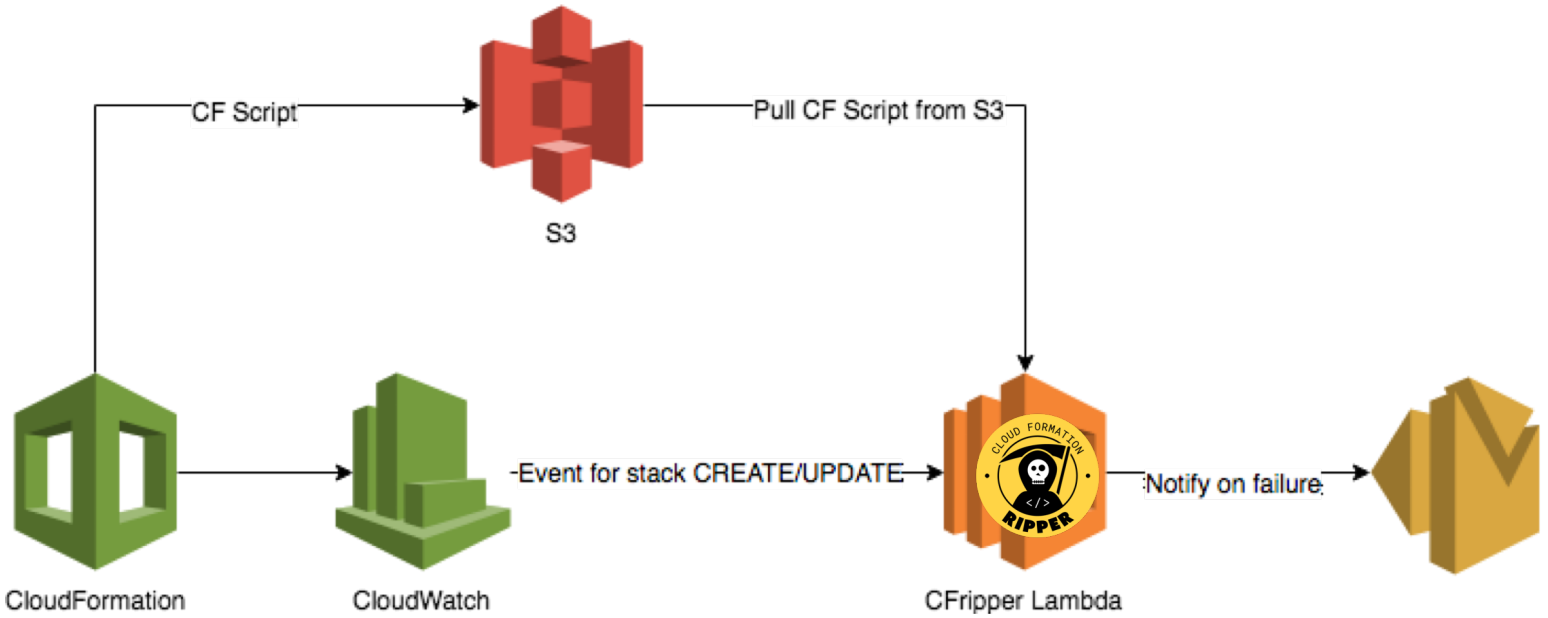


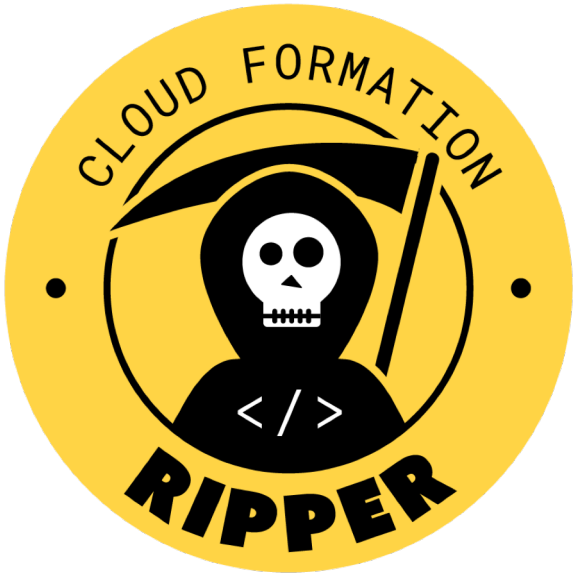
“Inject security into CI/CD…”


CLOUD FORMATION
</>
RIPPER


Drone
Internal
CD Tool
Validate CF
CFripper Lambda
Valid/Invalid
Deploy Infra if valid
CloudFormation

How we still use it





Pycfmodel

Example Rule

```
"S3BucketPolicy": {
  "Type": "AWS::S3::BucketPolicy",
  "Properties": {
    "Bucket": {
      "Ref": "S3Bucket"
    },
    "PolicyDocument": {
      "Statement": [
        {
          "Action": [
            "*"
          ],
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::fakebucketfa
          "Principal": {
            "AWS": [
              "156460612806"
            ]
          }
```

Example Rule

S3BucketPolicyWildcardActionRule.py 531 Bytes

```python
from cfripper.model.rule_processor import Rule


class S3BucketPolicyWildcardActionRule(Rule):

    REASON = "S3 Bucket policy {} should not allow * action"
    MONITOR_MODE = True

    def invoke(self, resources):
        for resource in resources.get("AWS::S3::BucketPolicy", []):
            if resource.policy_document.wildcard_allowed_actions(pattern=r"^(\w*:){0,1}\*$"):
                self.add_failure(
                    type(self).__name__,
                    self.REASON.format(resource.logical_id),
                )
```

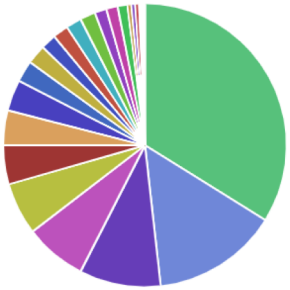
skyscanner

cfripper_stacks_scanned

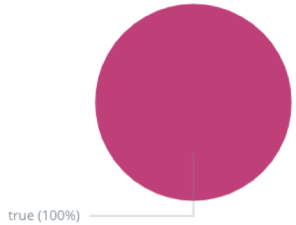
449

Unique count of time_input

cfripper_top_100_services_scanned



Cfripper monitor rules



Cfripper rules overview

cfripper_rule: Descending	Reason	Project	Squad	Slack	Monitor mode	Unique count of time_input
EBSVolumeHasSSERule	EBS volume etcdebs1 should have server-side encryption enabled	k8s/k8s-templates	Cops	#cops-private	true	8
EBSVolumeHasSSERule	EBS volume etcdebs2 should have server-side encryption enabled	k8s/k8s-templates	Cops	#cops-private	true	8
EBSVolumeHasSSERule	EBS volume etcdebs3 should have server-side encryption enabled	k8s/k8s-templates	Cops	#cops-private	true	8
EBSVolumeHasSSERule	EBS volume etcdebs4 should have server-side encryption enabled	k8s/k8s-templates	Cops	#cops-private	true	8
EBSVolumeHasSSERule	EBS volume etcdebs5 should have server-side encryption enabled	k8s/k8s-templates	Cops	#cops-private	true	8

..		
CloudFormationAuthenticationRul...	First commit	5 months ago
CrossAccountTrustRule.py	Created new rule for open s3 buckets and allowed list policies (#12)	2 days ago
EBSVolumeHasSSERule.py	First commit	5 months ago
IAMManagedPolicyWildcardAction...	First commit	5 months ago
IAMRoleWildcardActionOnPermiss...	First commit	5 months ago
IAMRoleWildcardActionOnTrustPol...	First commit	5 months ago
IAMRolesOverprivilegedRule.py	Take into account statement effect	4 months ago
ManagedPolicyOnUserRule.py	First commit	5 months ago
PolicyOnUserRule.py	First commit	5 months ago
PrivilegeEscalationRule.py	Bump pycfmodel version	4 months ago
S3BucketPolicyPrincipalRule.py	First commit	5 months ago
S3BucketPolicyWildcardActionRul...	First commit	5 months ago
S3BucketPublicReadAclAndListSt...	Created new rule for open s3 buckets and allowed list policies (#12)	2 days ago
S3BucketPublicReadWriteAclRule....	First commit	5 months ago
SNSTopicPolicyNotPrincipalRule.py	First commit	5 months ago
SQSQueuePolicyNotPrincipalRule....	First commit	5 months ago
SQSQueuePolicyWildcardActionR...	First commit	5 months ago
SecurityGroupIngressOpenToWorl...	First commit	5 months ago
SecurityGroupMissingEgressRule....	First commit	5 months ago
SecurityGroupOpenToWorldRule.py	First commit	5 months ago
__init__.py	Created new rule for open s3 buckets and allowed list policies (#12)	2 days ago

open source initiative®

Thank you
Questions?

https://github.com/Skyscanner/cfripper
https://github.com/Skyscanner/pycfmodel
https://medium.com/@skyscanner

skyscanner