CSPM Using Open Source Tools

whoami

- Chandrapal Badshah
- Security Researcher
- Blog at https://badshah.io
- Checkout my Burp Suite newsletter - https://newsletter.burpsuite.guide/
- Twitter - @bnchandrapal
- AWS Certified Security - Specialty & works mostly on AWS

What is CSPM?

- Cloud Security Posture Management - identifies assets and security issues
- Focuses on security posture OF your cloud resources but NOT necessarily INSIDE your resources
- Mostly misconfiguration issues and compliance risks
- Can help with other use cases like resources and pricing in cloud
- Applicable to all public clouds

Why CSPM?

- Provides visibility across your cloud assets
  - compute, storage, serverless, etc
- Evidence collection
  - public or private
  - compliant or non-compliant, etc
- Reporting and alerting
  - misconfiguration
- Automation
  - automatic mitigation

Components of CSPM

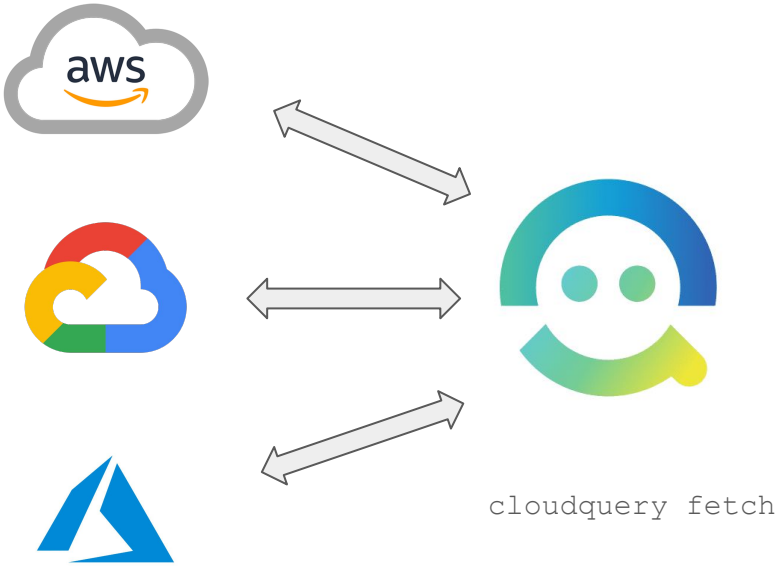
- Provides visibility across your cloud assets (**Monitoring & Visualization**)
  - compute, storage, serverless, etc
- Evidence collection (**Security Policy Compliance**)
  - public or private
  - compliant or non-compliant, etc
- Reporting and alerting (**Security & Threat Detection**)
  - misconfiguration
- Automation (**Remediation**)
  - automatic mitigation

You can setup a simple yet powerful CSPM solution yourself using Open Source tools!

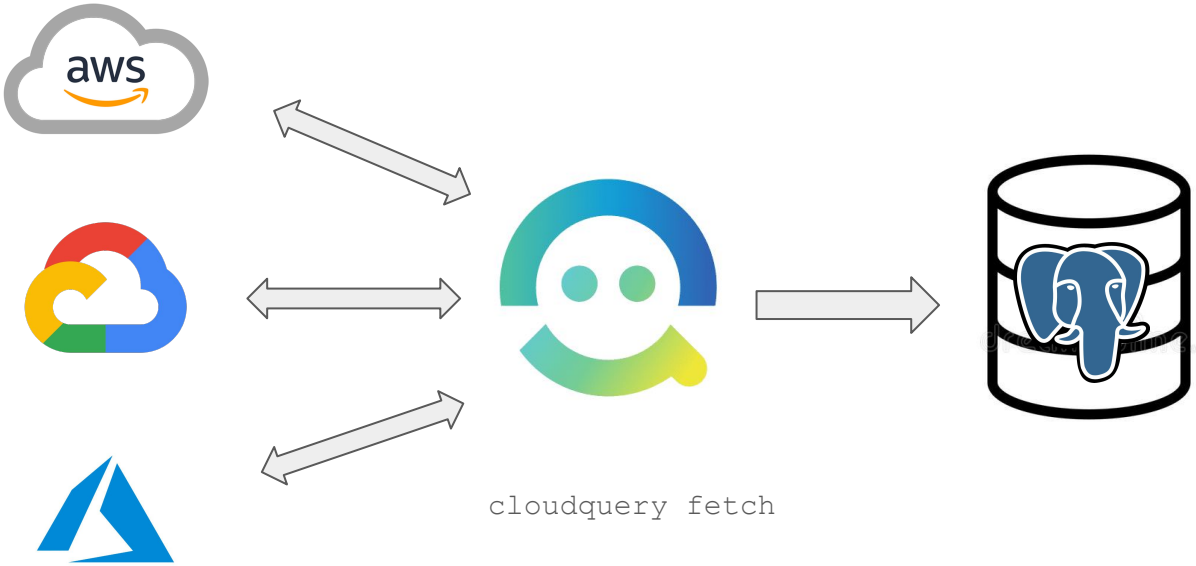
Introduction to Cloudquery

- It’s an open source data integration tool
- Fetches the data from Cloud APIs and stores them to database / data lake / other supported destinations
- Supports major clouds - AWS, Azure, GCP, DigitalOcean
- Has other plugins - Kubernetes, Cloudflare, etc
- CSPM is one of many use cases

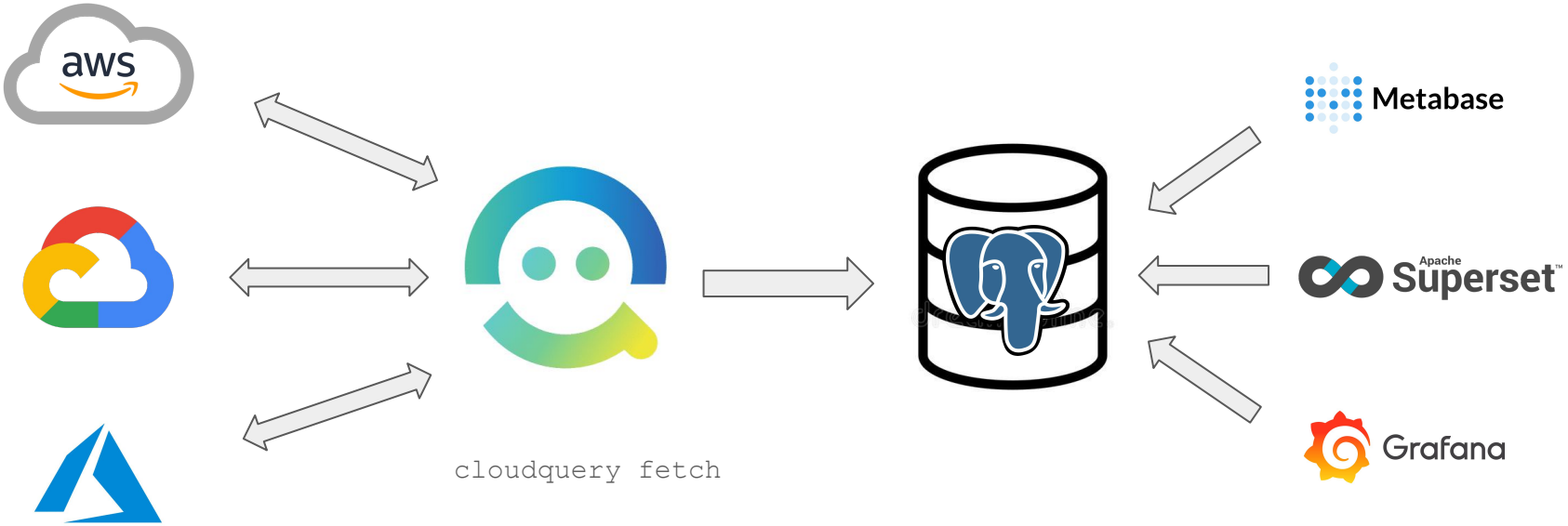
How Cloudquery works



How Cloudquery works



How Cloudquery works



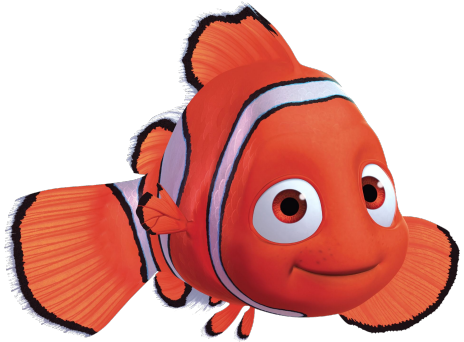
Your data is just a query away

Find all publicly exposed AWS ALB:

```
SELECT * FROM aws_elbv2_load_balancers
   WHERE scheme = "internet-facing"
```

DEMO

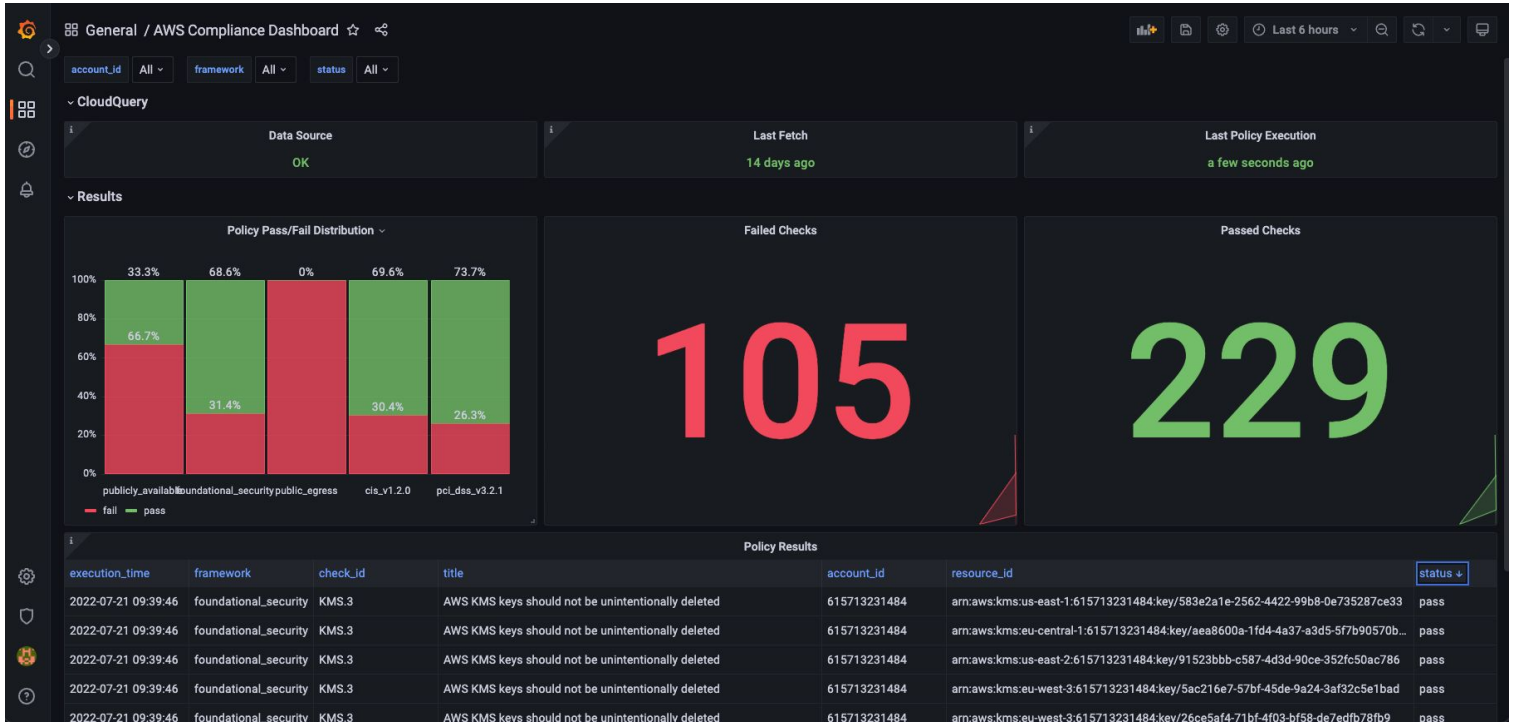
Finding Nemo



Using Cloudquery for CSPM

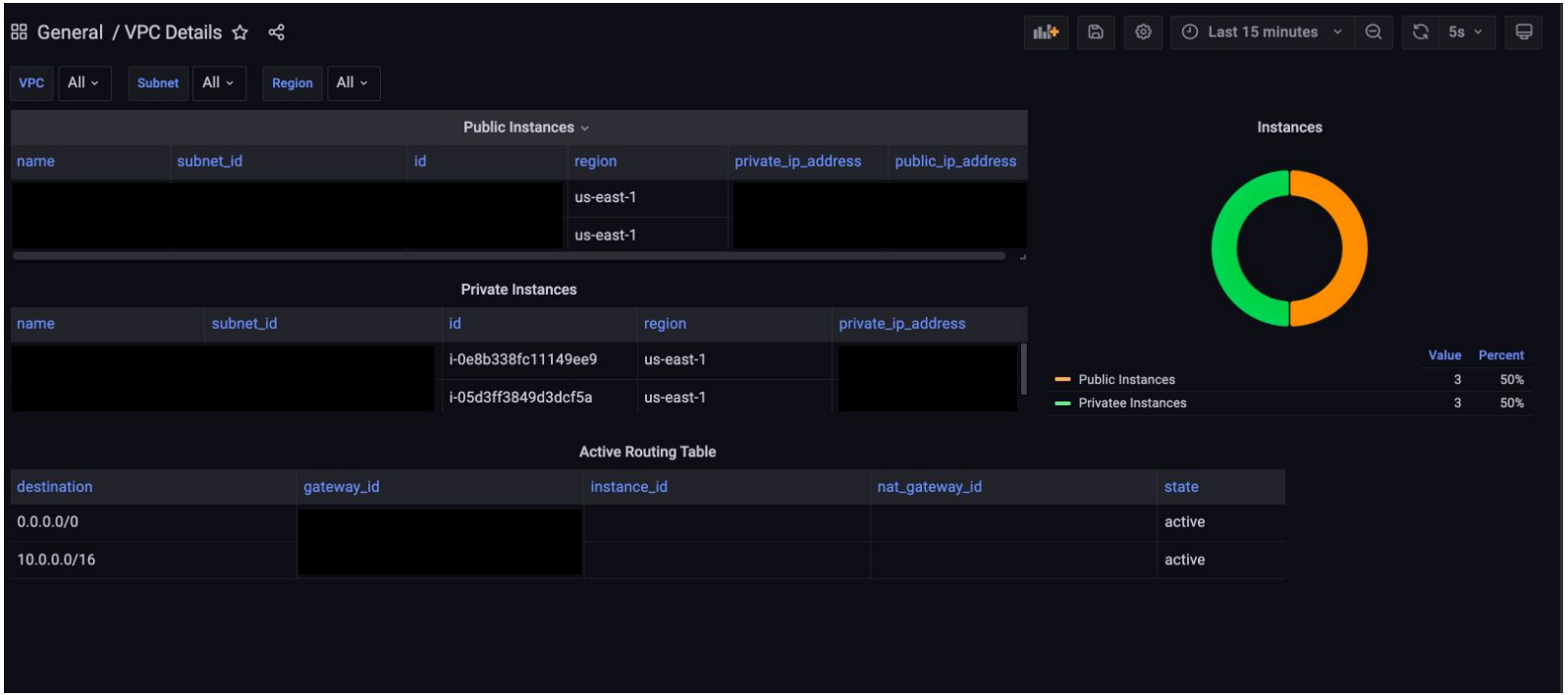
- Has queries for compliance policies. Example, for AWS you have:
  - CIS v1.2.0
  - Foundational Security
  - PCI DSS v3.2.1
- Has queries for other interesting metrics - like publicly available resources
- You can make use of the data in other “creative” ways
- Periodic monitoring of the resources and alerts for policy violations can be setup

AWS Compliance Dashboard



Source: https://www.cloudquery.io/blog/open-source-cspm

AWS EC2 VPC Details



Source: https://grafana.com/grafana/dashboards/15266-vpc-details/

What did we achieve using Cloudquery so far?

- ✅ Monitoring & Visualization
- ✅ Security Policy Compliance
- ✅ Security & Threat Detection
- ❌ Remediation

Are you okay having your cloud backups public for **X hours** till Cloudquery detects it?

Introduction to Cloud Custodian

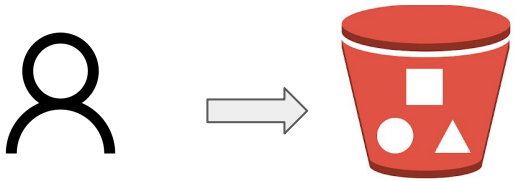
- Open Source Cloud Security, Governance and Management tool
- Can provide near real-time alerts & enforce compliance
- Has different modes and can run anywhere - locally, on an instance or serverless in AWS Lambda
- Policies written in YAML
- For auto remediation, running the policies in Lambda is recommended

Cloud Custodian

Sample Policy - Encrypt newly created S3 buckets “automatically”

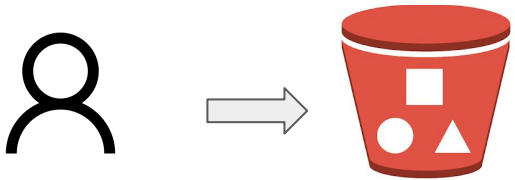
```
policies:
   - name: s3-configure-standards-real-time
     resource: s3
     mode:
       type: cloudtrail
       events:
         - CreateBucket
       role: Cloud_Custodian_S3_Lambda_Role
     actions:
       - type: set-bucket-encryption
```

How does Cloud Custodian “CloudTrail mode” work?



User creates an S3 bucket
(without encryption)

How does Cloud Custodian “CloudTrail mode” work?



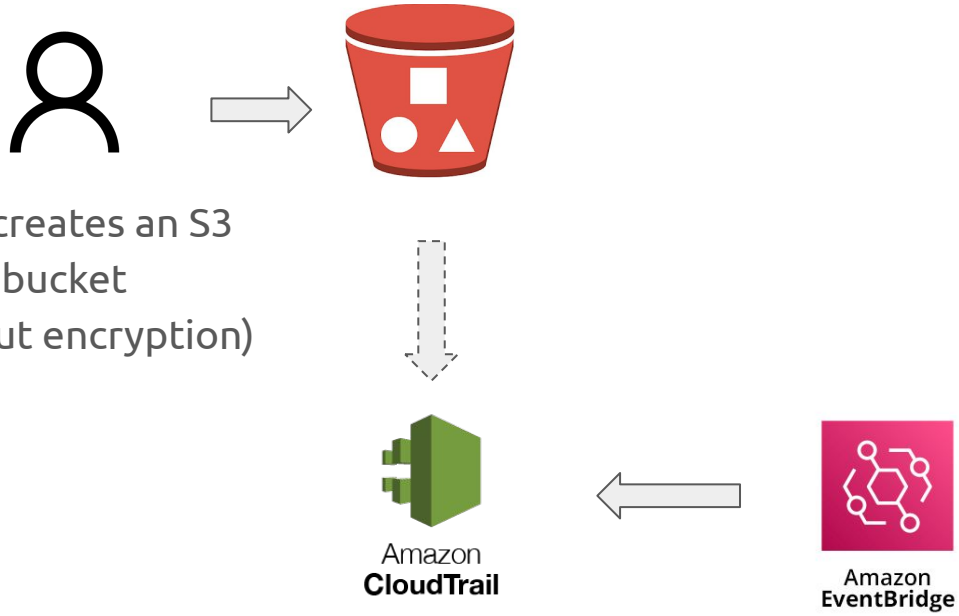
User creates an S3 bucket (without encryption)

Amazon **CloudTrail**

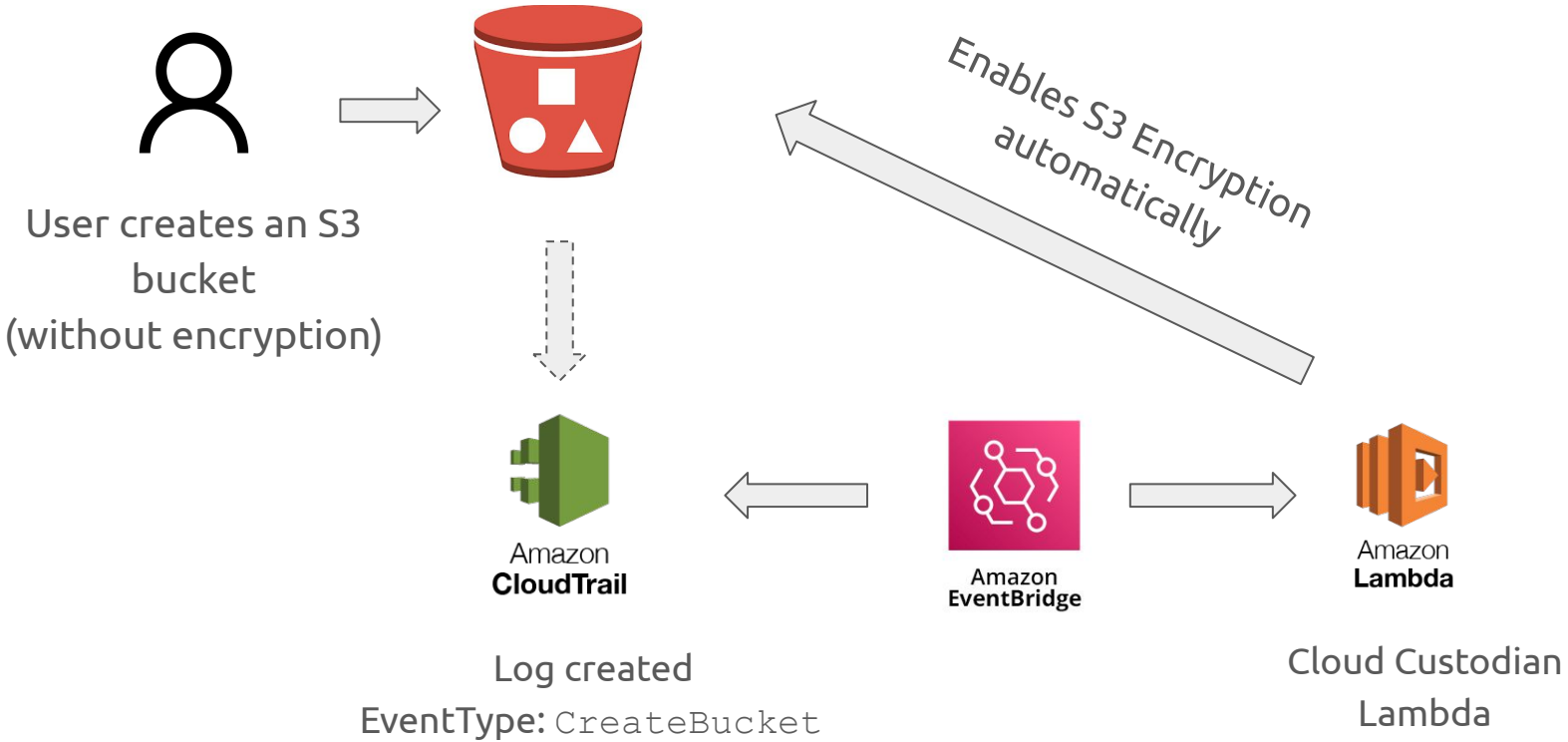
Log created

EventType: `CreateBucket`

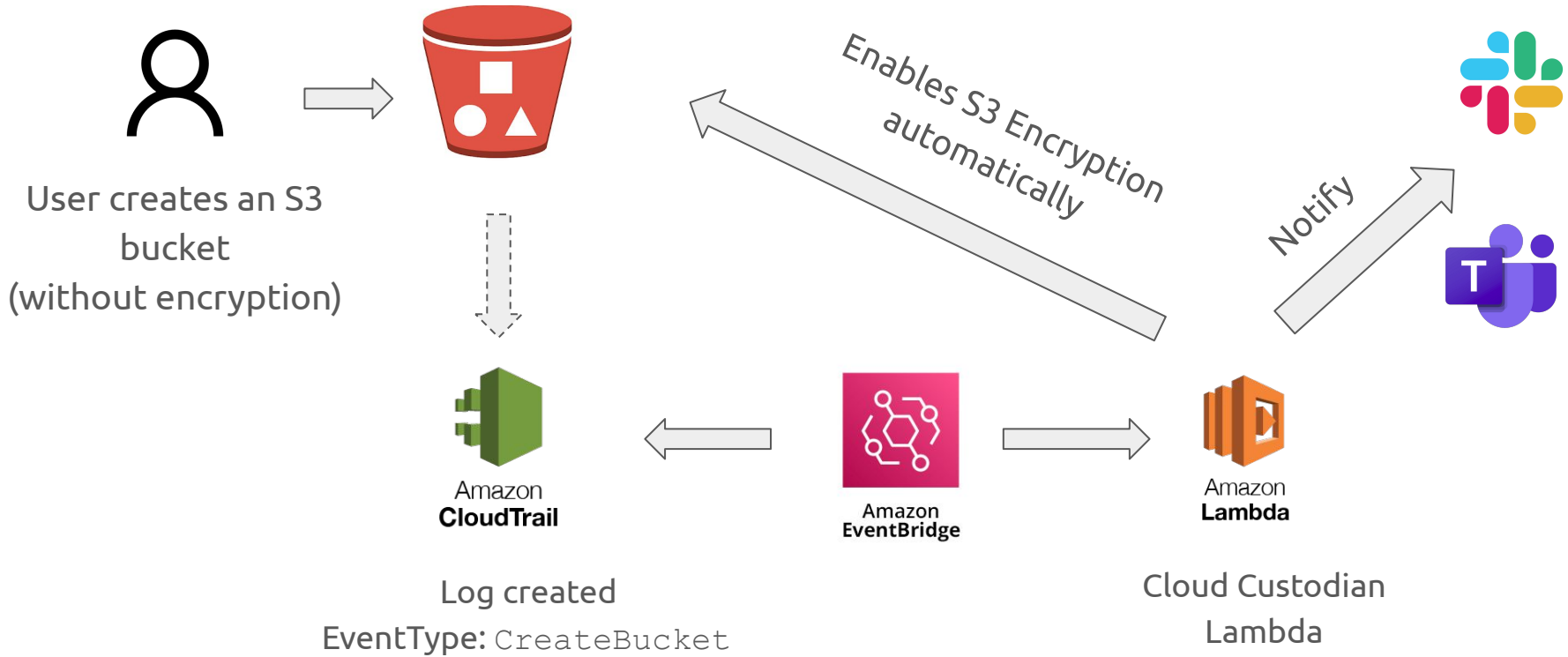
How does Cloud Custodian “CloudTrail mode” work?



How does Cloud Custodian “CloudTrail mode” work?



How does Cloud Custodian “CloudTrail mode” work?

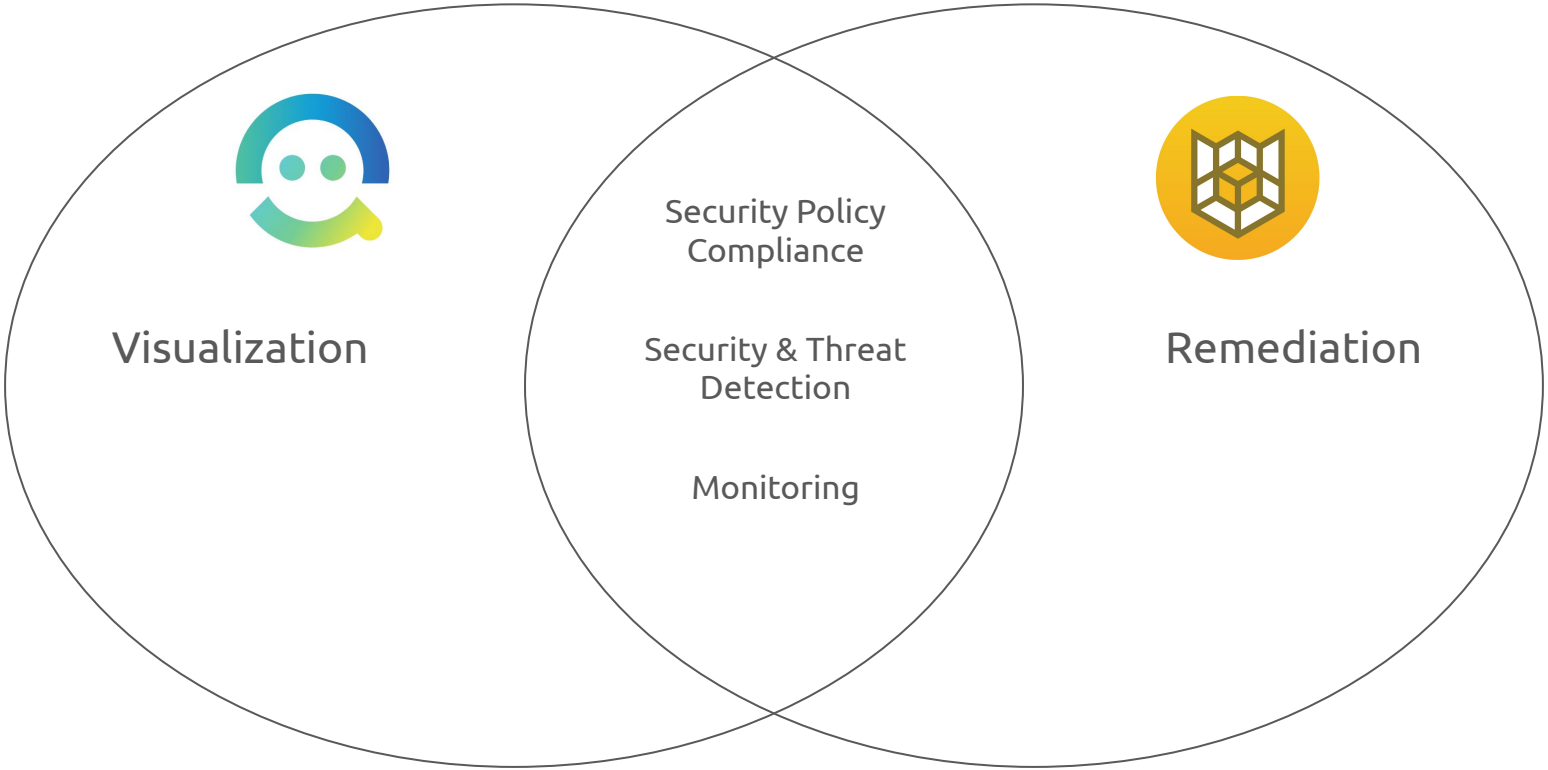


NO DEMO

The setup is error prone and needs understanding on how it works

Maybe let’s do a Null Puliya on AWS Security 😉

What did we achieve so far?



CSPM USING OPEN SOURCE

Advantages of using Open Source CSPM

- Flexible and Powerful
- Multi cloud support and allows scanning multiple accounts & projects
- Custom rules for your company’s context
- You get some features of paid CSPM tools at a fraction of their cost

Should you stop using any paid CSPM solutions and implement these Open Source tools at work?

It’s very tempting to say YES!

Disadvantages of using Open Source CSPM

- “With Great Power Comes Great Responsibility”
- If you implement, you take care of maintaining, updating and integrating with your services
- Like all open source software:
  - no guarantee of development (say at least for next 1 year)
  - no on-demand support for issues
  - you must know what the tool does and is capable of
- You need to be fairly up-to-date on new cloud services and cross check if they are supported

Links to tools

- Cloudquery - https://cloudquery.io
- Cloudquery Source Code - https://github.com/cloudquery/cloudquery
- Compliance policies - https://github.com/cloudquery/cloudquery/tree/main/plugins/source/aws/policies
- Cloud Custodian - https://cloudcustodian.io/
- Cloud Custodian Code - https://github.com/cloud-custodian/cloud-custodian

Cloudquery V2 Coming Soon!

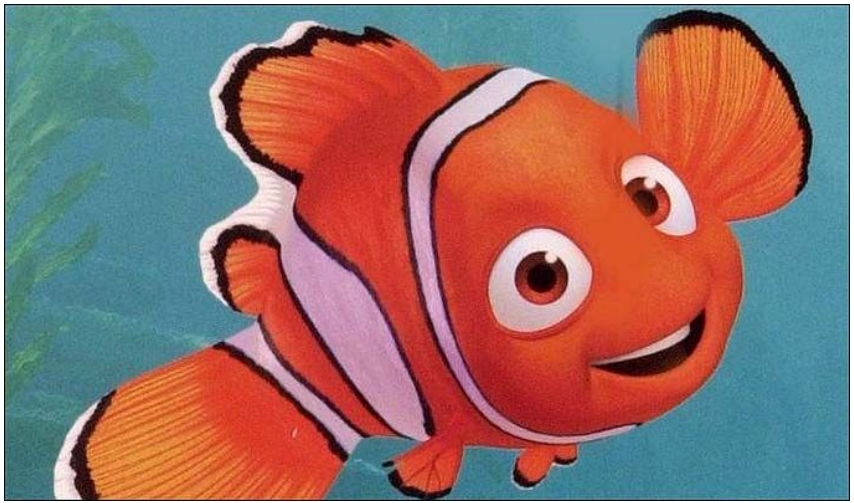
https://github.com/cloudquery/cloudquery/pull/1463

Want to understand your cloud infra without DB setup?

- Check out Steampipe - https://steampipe.io/
- 200+ data sources. No DB/external dashboard setup.
- Data on your cloud infra is just an SQL query away
- Inbuilt compliance dashboards
- Find the difference: https://badshah.io/cloudquery-vs-steampipe/

Thank You

Any Questions?



You can DM me on Twitter - @bnchandrapal