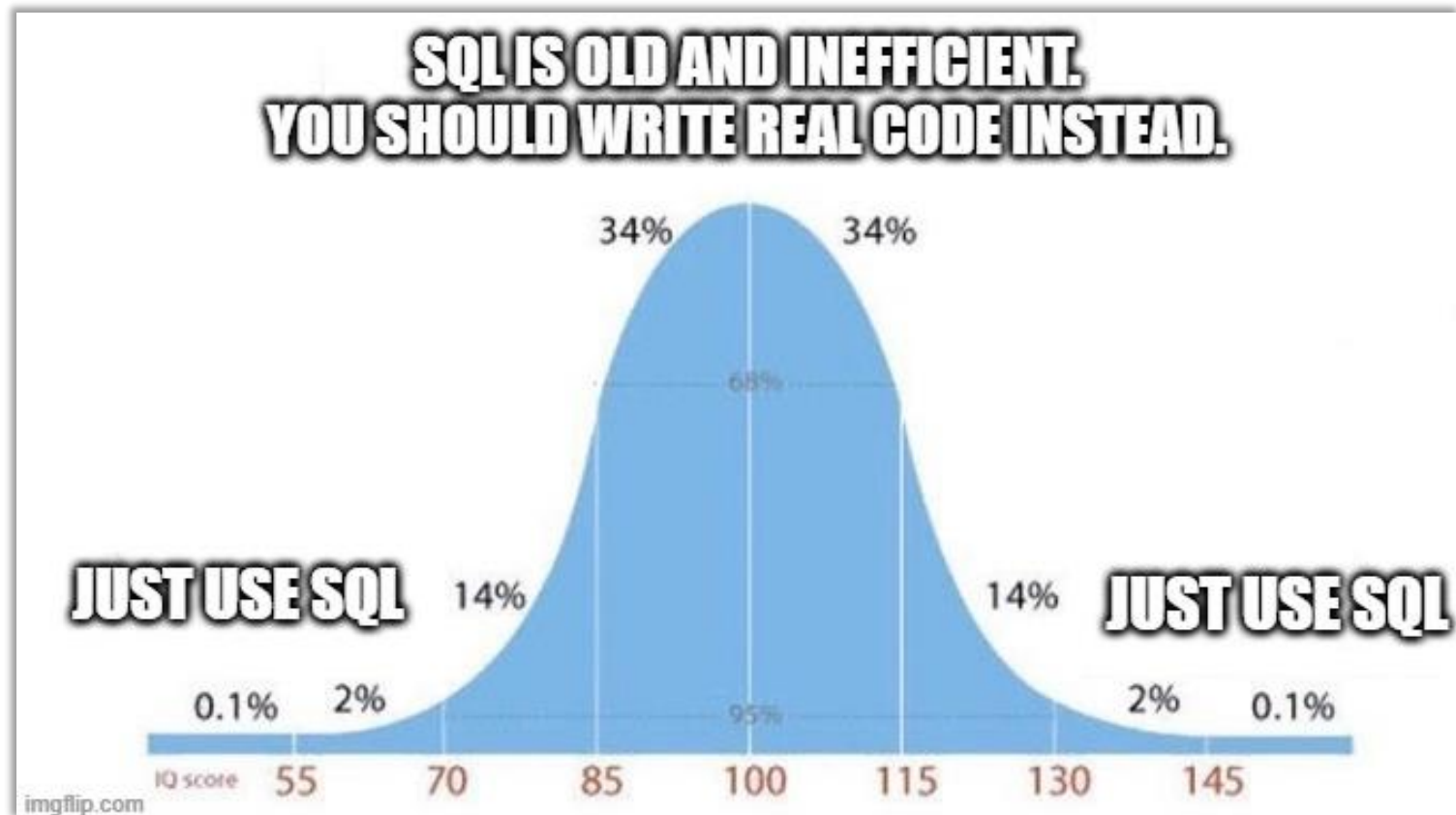


SQL your cloud environments

Michael Kirchner

Off to a provocative start...

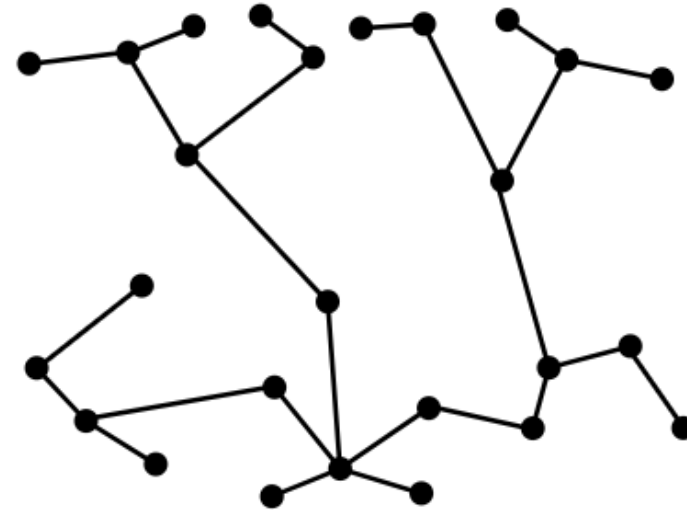
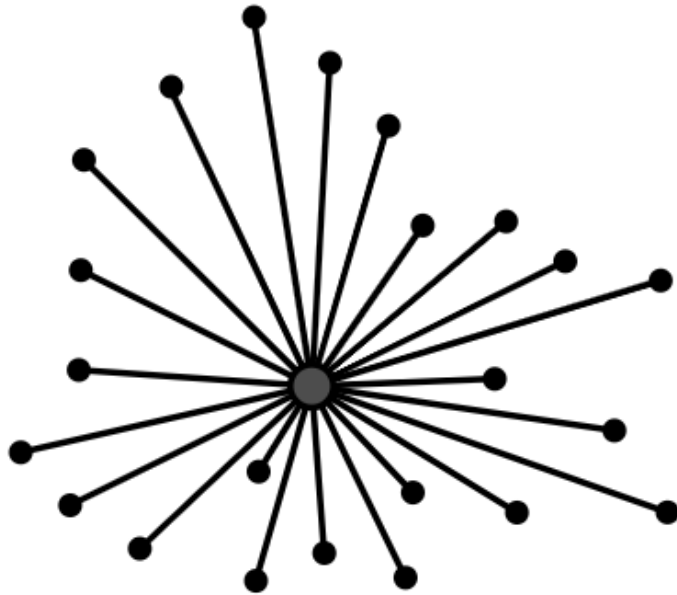


Michael Kirchner

- Lecturer @ FH St.Pölten, IT Security & Cloud Technologies
- Cloud Security Consultant & Founder @ welldone.cloud

- Formerly: Consultant & Security Engineer @ Amazon Web Services

Cloud computing fosters a decentralization of IT:
Teams operate on their own instead of going via central entities



Cloud computing properties that can be challenging for security teams

Self-service



Teams configure IT resources themselves, often without a central process or approval

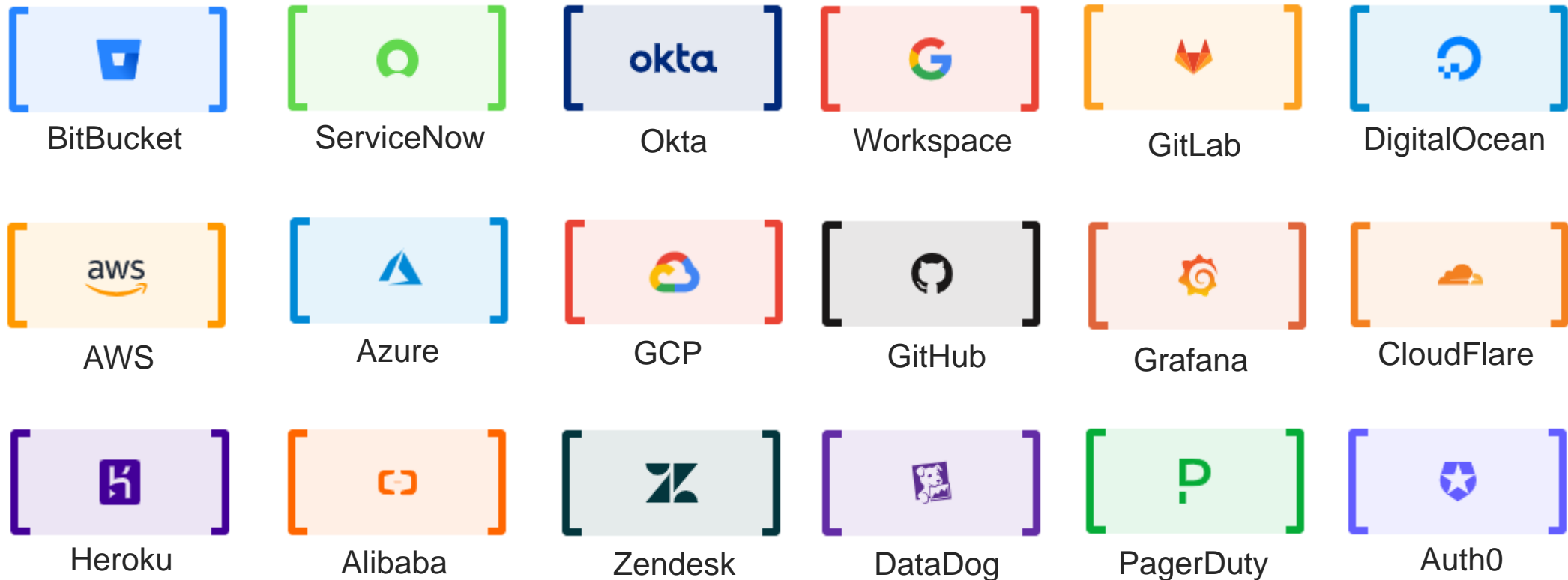
On-demand elasticity



IT resources are dynamically created or deleted as needed

From a security team's perspective, it's easy to have unknown unknowns in cloud environments...

Many security activities rely on an asset inventory, but there is more than one cloud service provider out there...





- Both available as open source (free & self-hosted) or as SaaS (commercial)
- Both enumerate cloud resources and provide queryable SQL tables for them

And I am not sponsored by any of them 😊

Supported cloud services and resources

<https://hub.steampipe.io/plugins>

<https://www.cloudquery.io/docs/plugins/sources/overview>

The primary objective is a cloud asset inventory.
The curious security person is one use case on top of it.

“Does any of our teams use technology [xyz]?”

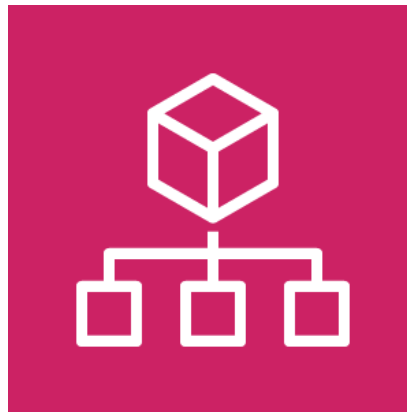
“Are we affected by [recent security publication]?”

“What is this actually used for?”

“Hmmm, why was it set up this way?”

Demo

UAS St.Pölten operates an *AWS Organization* of ~25 *AWS accounts*.
We'll analyze this setup closer.



Demo

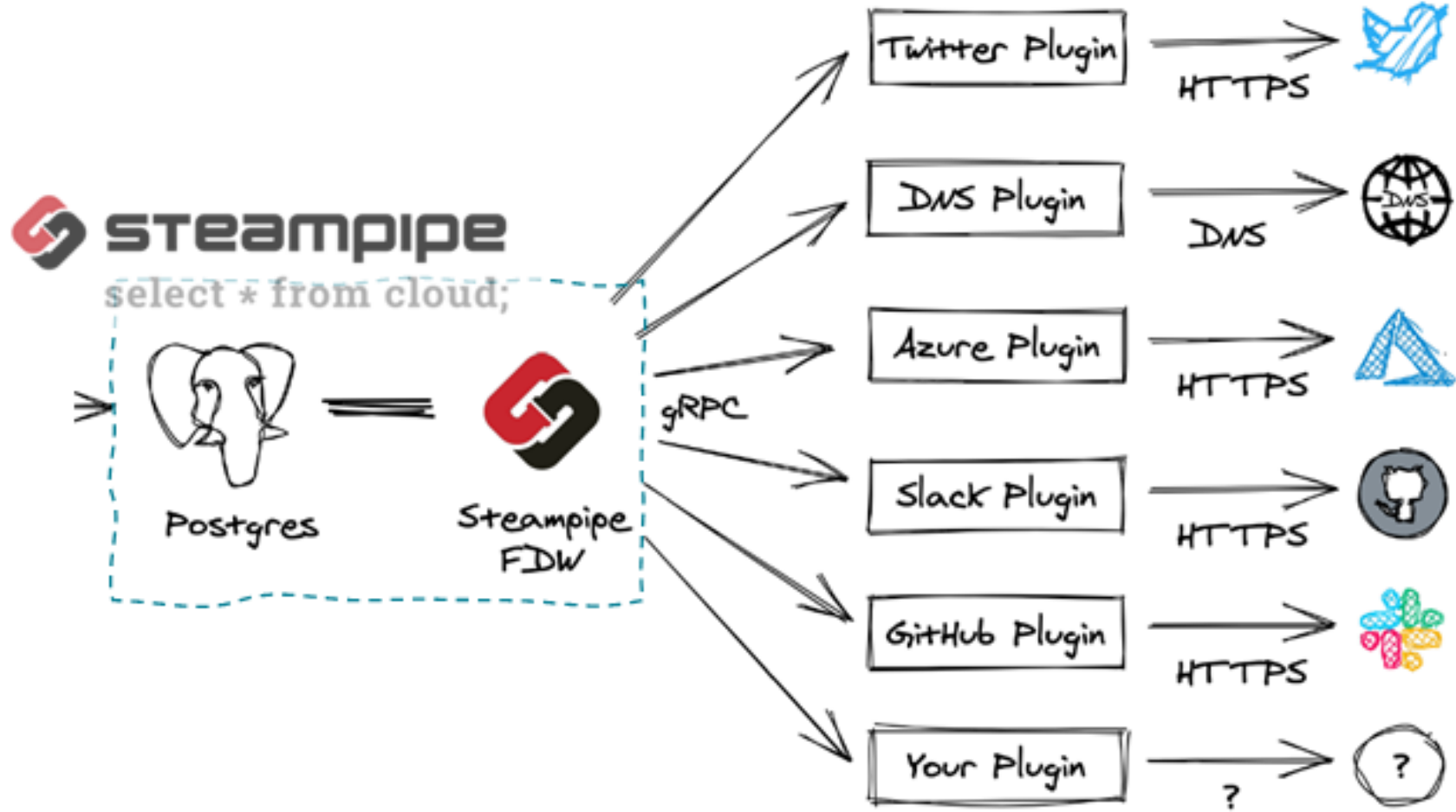
```
sudo /bin/sh -c "$(curl -sSL  
https://raw.githubusercontent.com/turbot/steampipe/main/install.sh)"
```

```
steampipe plugin install steampipe
```

```
steampipe plugin install aws
```

```
vim ~/.steampipe/config/aws.spc      # Your AWS environment details here
```

```
steampipe service start
```



Collections of ready-made queries for security analysis:

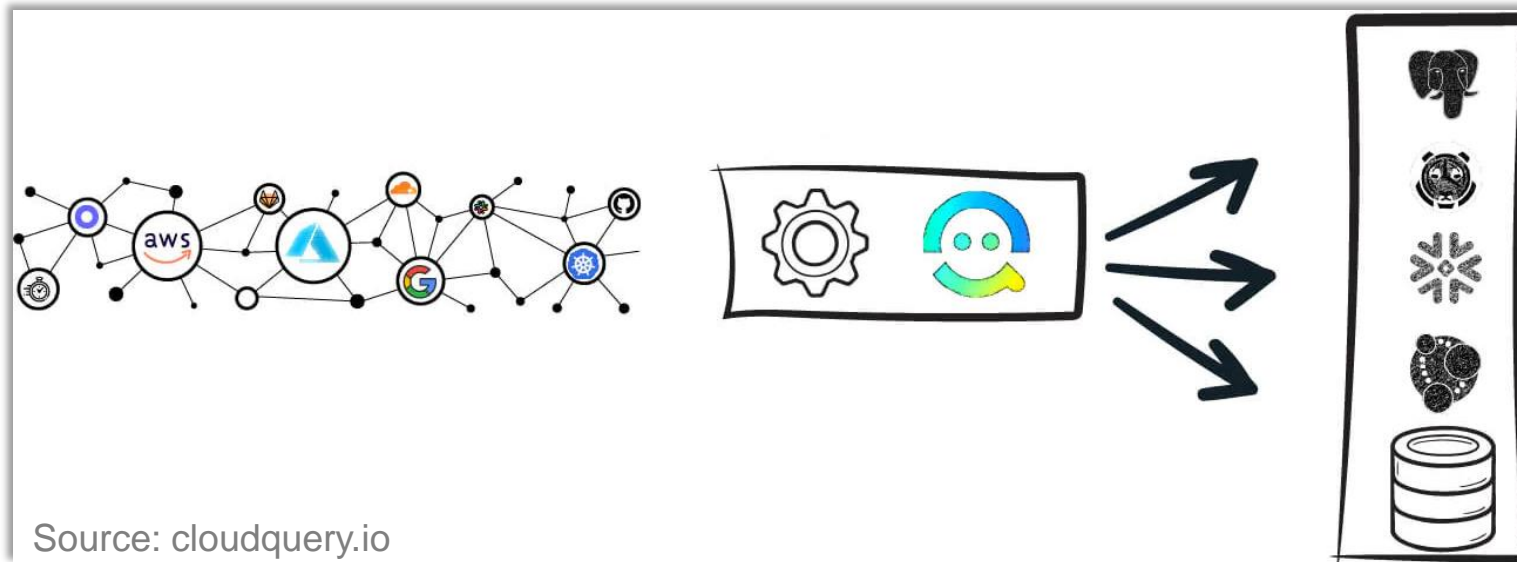
<https://hub.steampipe.io/mods>

As always:

- Don't just blindly run all of them
- Rather judge what makes sense for your environment

A similar approach: **CloudQuery**

- Instead of sending queries on-demand, it dumps all table data to a destination: SQL databases, Elasticsearch, Blob storage, etc.
- It's more of a “sync tool” or ETL tool



Source: cloudquery.io



- Support for other destinations than Postgres
<https://www.cloudquery.io/docs/plugins/destinations/overview>
- You get a full data dump and can keep snapshots







- Full dumps can take time and cause lots of API calls

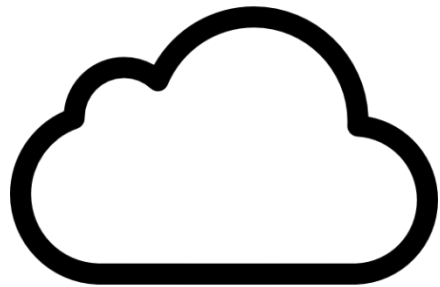
```
Loading spec(s) from config.yml
Starting migration for: aws (v19.0.0) -> [sqlite (v2.2.2)]
Migration completed successfully.
Starting sync for: aws (v19.0.0) -> [sqlite (v2.2.2)]
Sync completed successfully. Resources: 251034, Errors: 45763, Panics: 0, Time: 2h20m41s
~/cloudquery$
```


So, when to use what?

First, check whether the tool supports the cloud service provider you want to query.

- *“I need live results”*  **STEAMPIPE**
- *“I don’t know yet which queries I will send”*  **STEAMPIPE**
- *“I need something else than Postgres”*  **CLOUDQUERY**
- *“I want to keep snapshots of my cloud config”*  **CLOUDQUERY**

Get transparency
over your actual
cloud infrastructure.



Make sure security
teams can stay
close to reality.

