

# The Wisdom of Clouds

A Cloud Sourced Guide to Data Security

Daniel Tobin, Security Lead, Cyral

# Who?

- Daniel Tobin is Security Lead at Cyral and has been working in DevSecOps since before the word existed.
- Last in person con was BSidesSF in February
- Follow me on Twitter [@dant24](https://twitter.com/dant24)

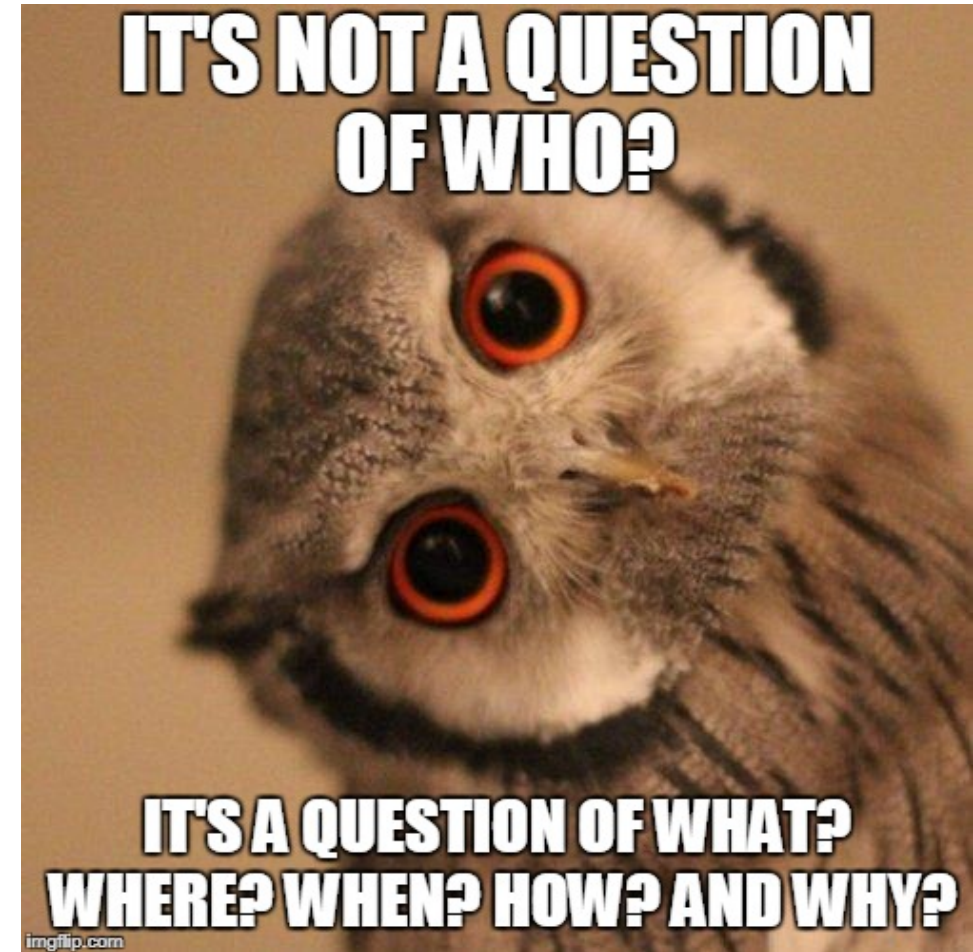
## The Security Digest





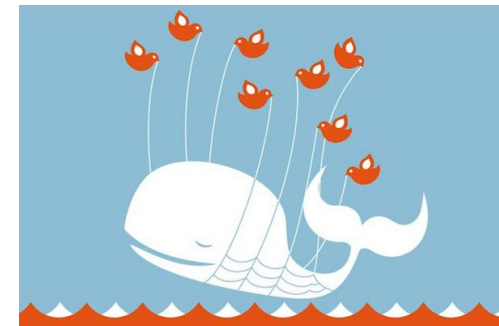
# What? Where? When? How? Why?

- Cloud Sources
- Why this matters
- Open source projects to secure your cloud infrastructure
- New open source project
- Existing documentation
- Questions



# Cloud Sources

- Clint Gibler's *tl;dr sec* Newsletter
  - [tldrsec.com](https://tldrsec.com)
- Marco Lancini's Cloud Security Reading List
  - [cloudseclist.com](https://cloudseclist.com)
- Twitter





# It's the Data, Stupid!

blog.shodan.io/its-the-data-stupid/



# It's the Data, Stupid!

18 JULY 2015 on research, MongoDB, NoSQL

I would like to take a moment to discuss databases. Most

# ~15000 Meows

ShodanDevelopersMonitorView All...



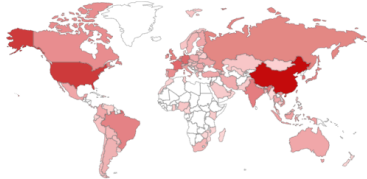
ExploreDownloadsReportsPricingEnterprise Access

ExploitsMapsImagesShare SearchDownload ResultsCreate Report

TOTAL RESULTS

21,356

TOP COUNTRIES



China	9,129
United States	3,660
Germany	985
France	922
Singapore	634


TOP SERVICES

ElasticSearch	11,853
MongoDB	3,696
8081	2,242
HTTP	593
8083	588

TOP ORGANIZATIONS


Hangzhou Alibaba Advertising Co.,Ltd.	4,071
Amazon.com	2,417
Tencent cloud computing	1,310
China Telecom	1,109
Digital Ocean	1,078

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

122.225.113.46

China Telecom

Added on 2020-10-09 20:16:16 GMT

 China

HTTP/1.1 200 OK

Content-Type: text/html; charset=ISO-8859-1

Transfer-Encoding: chunked

Date: Fri, 09 Oct 2020 20:16:04 GMT

Server: Apache-Coyote/1.1



2000

<!doctype html public "-//w3c//dtd html 4.0 transitional//en" "http://www.

<html>


<head>

<...

 40.68.173.189

Microsoft Azure

Added on 2020-10-09 20:15:48 GMT

 Netherlands, Amsterdam

clouddatabasecompromised

12.0 MB

1 Nodes

Cluster Name	mycluster1
Status	yellow
Number of Indices	12

HTTP/1.1 200 OK

content-type: application/json; charset=l

content-length: 433

Elastic:

Total Size: 12.5 MB

Total Docs: 8

Indices:

04xehclqf8-meow (1.14 KB)

9vasclg8oa-meow (1.14 KB)

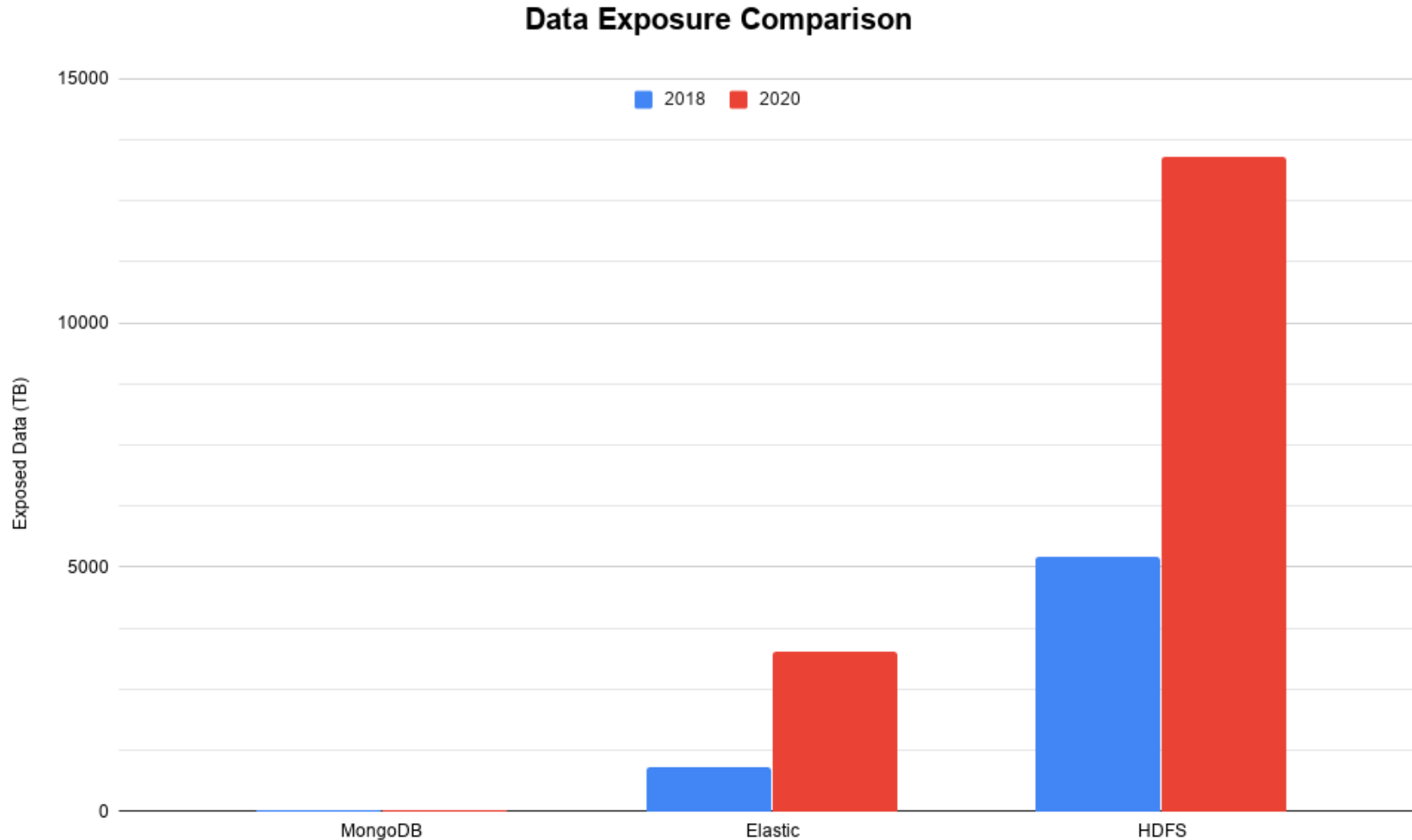
b3emh7yhzu-meow (1.14 KB)

documents\_content\_1810 (12.49 MB)

fyt6jwhq8g-meow (1....

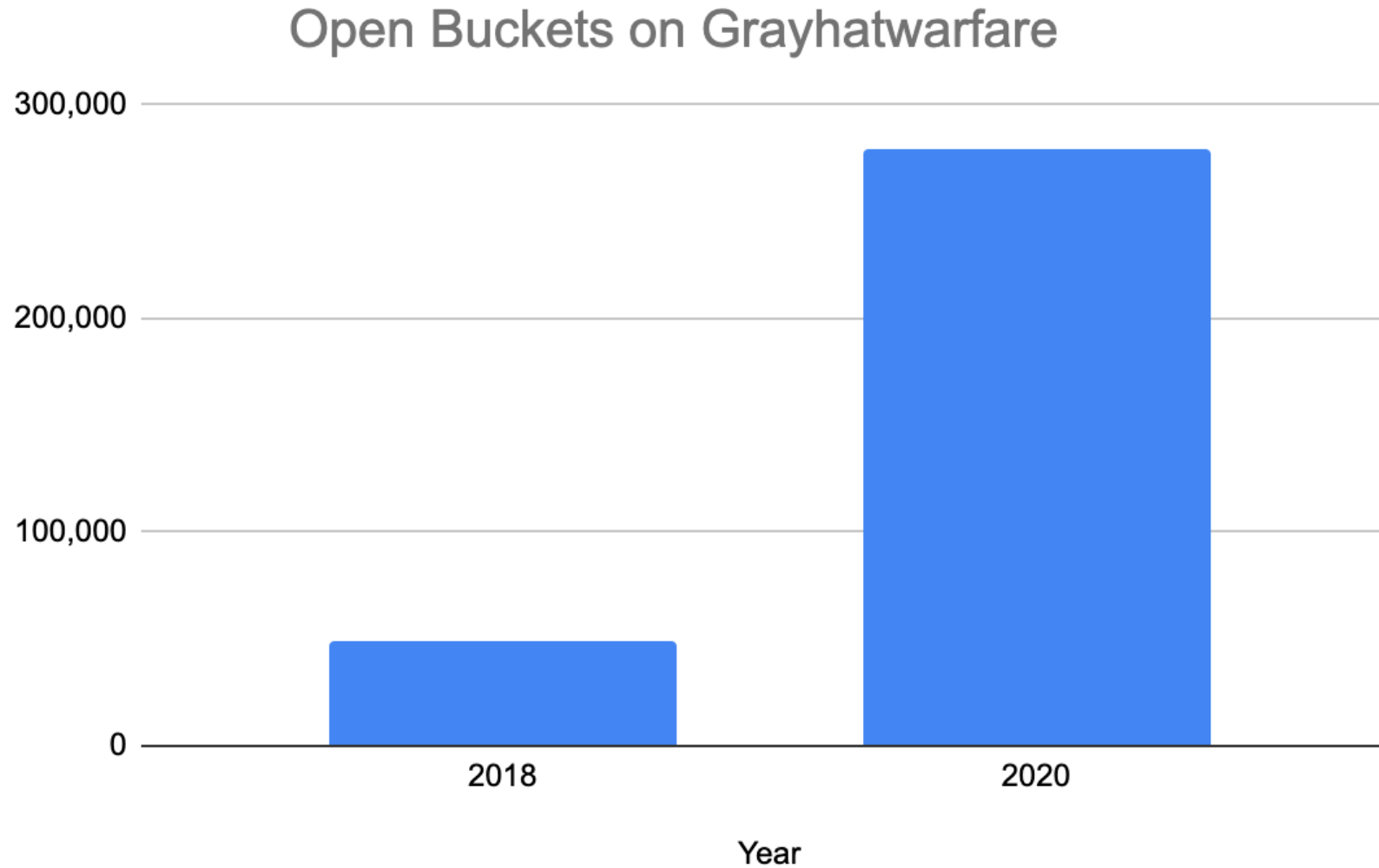
Cyral | 6

# May 10, 2020 Public Data Exposure





# Can't Forget About S3

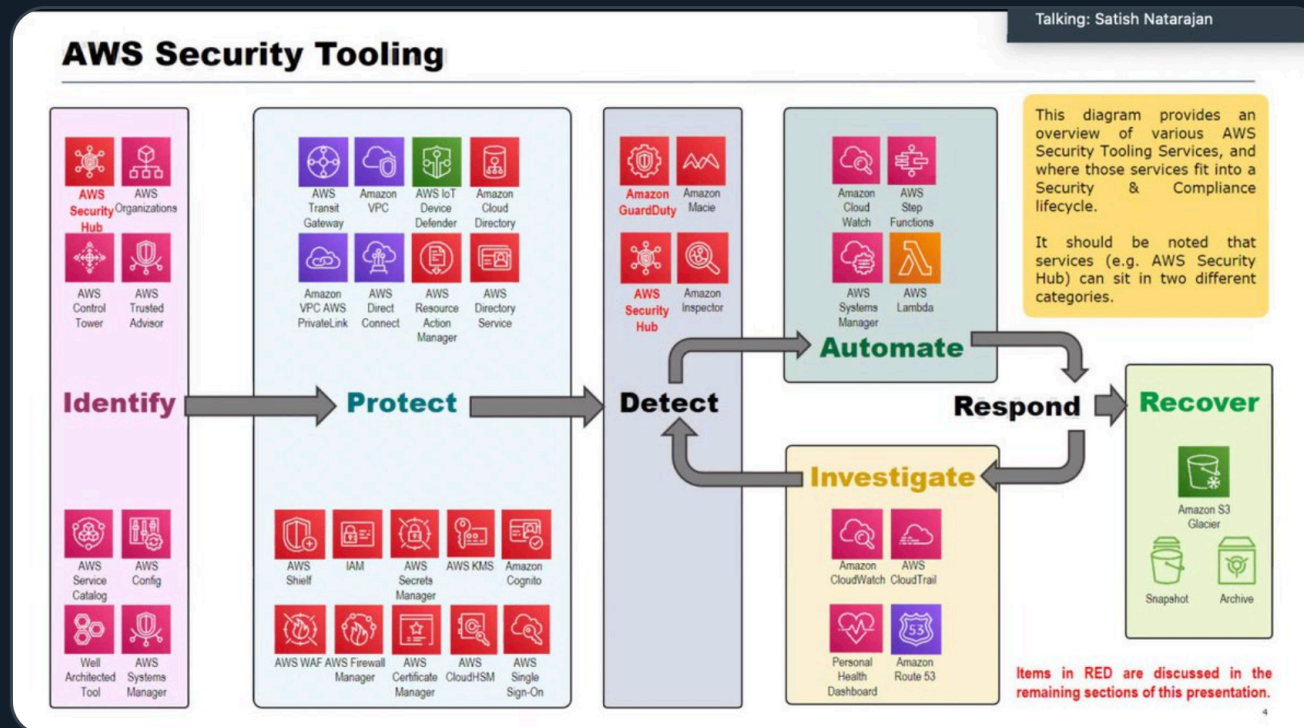


# Securing AWS



**HydroxyCoreyQuinn**  
@QuinnyPig

"Screw it, it's easier and arguably less expensive to just keep my S3 buckets open."







# Talk to an AWS Expert

- Corey Quinn
  - <https://www.lastweekinaws.com/>
  - <https://twitter.com/QuinnyPig>
- Scott Piper
  - <https://summitroute.com/>
  - <https://twitter.com/0xdabbad00>
  - <https://twitter.com/SummitRoute>
  - [https://summitroute.com/blog/2020/05/21/aws\\_security\\_maturity\\_roadmap\\_2020/](https://summitroute.com/blog/2020/05/21/aws_security_maturity_roadmap_2020/)

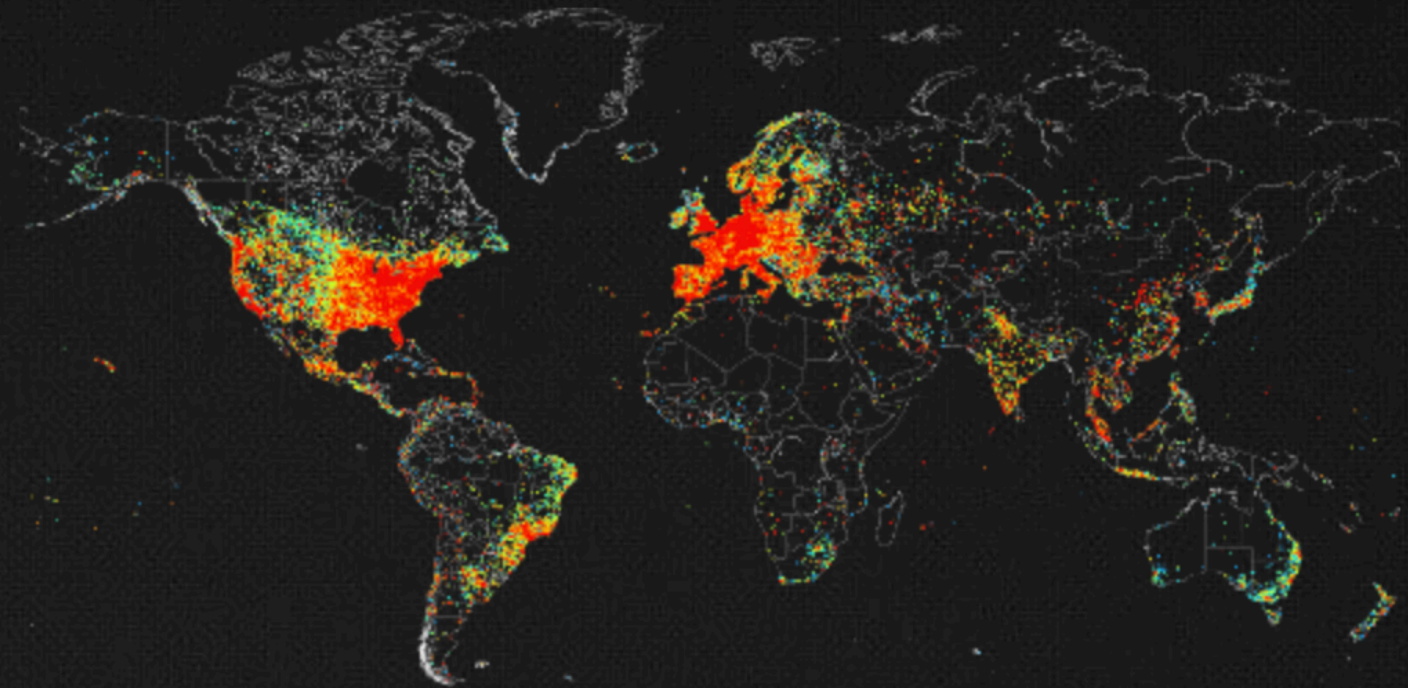




# Know What's Connected

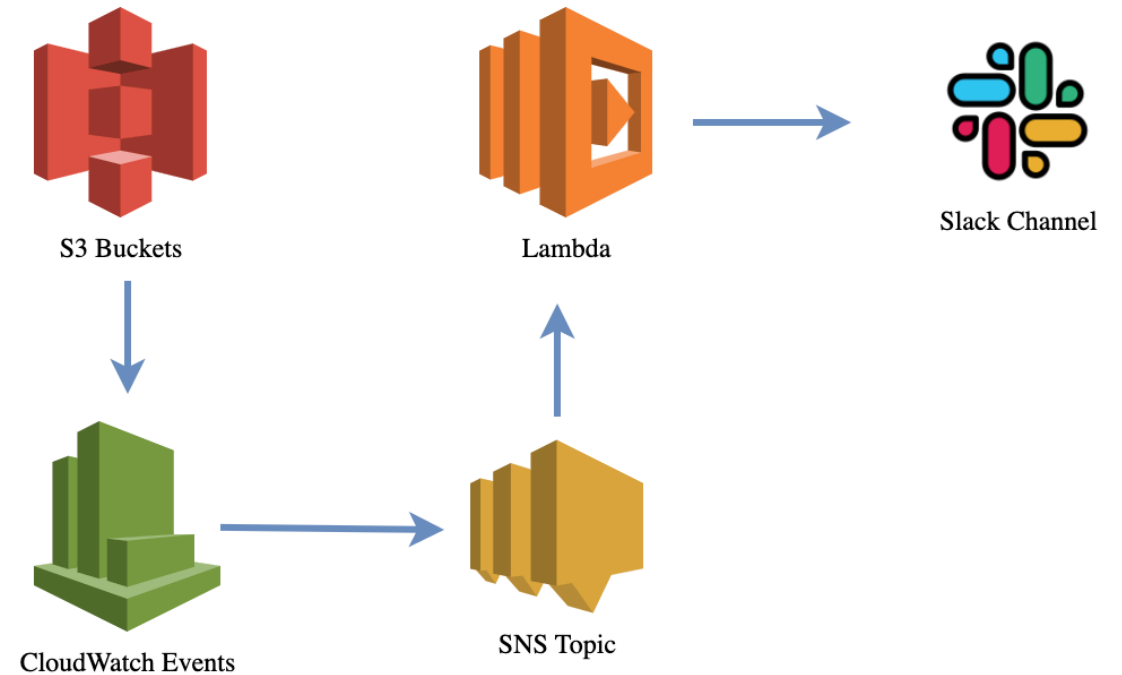
Keep track of the devices that you have exposed to the Internet. Setup notifications, launch scans and gain complete visibility into what you have connected.

GET STARTED NOW



# Darkbit – “Simple DLP for AWS S3”

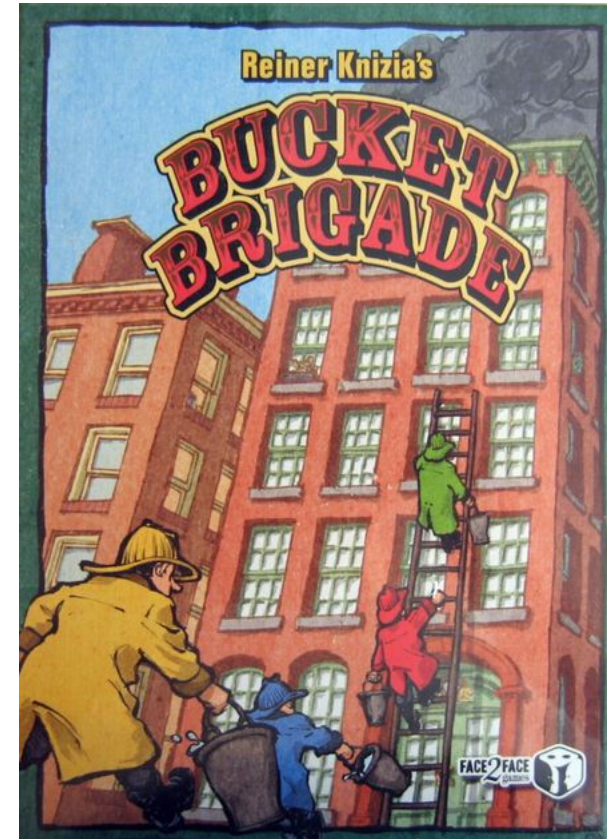
- Monitor for copying to other accounts
- <https://darkbit.io/blog/simple-dlp-for-amazon-s3>





# Databricks Bucket Brigade

- Scan everything with S3 Scan
- S3-Secrets-Scanner uses a Lambda function to scan objects uploaded/modified in S3 buckets for secrets.
- Includes documentation and policy as well
- <https://github.com/databricks/security-bucket-brigade>
- <https://databricks.com/blog/2020/07/16/bucket-brigade-securing-public-s3-buckets.html>



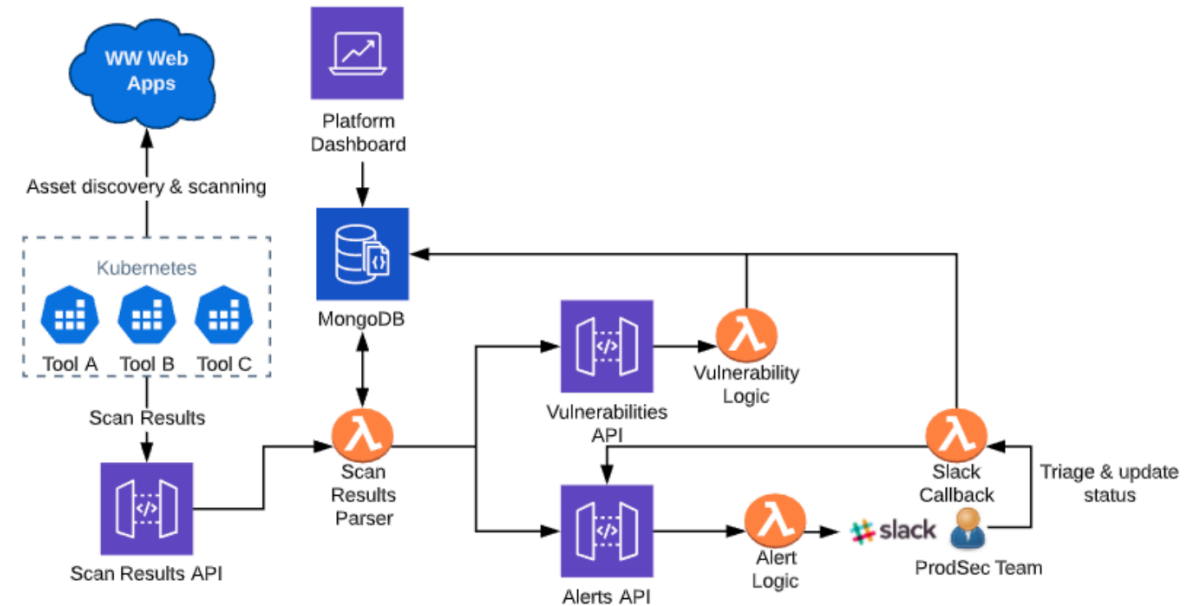
# S3 Insights and Awesome Sec S3 List

- Ashish Kurmi just released S3Insights
  - <https://medium.com/@kurmiashish/s3insights-58f24046cde3>
  - Scan S3 metadata at scale
  - <https://github.com/kurmiashish/S3Insights>
- <https://github.com/mxm0z/awesome-sec-s3>



# WW Tech AppSec Platform

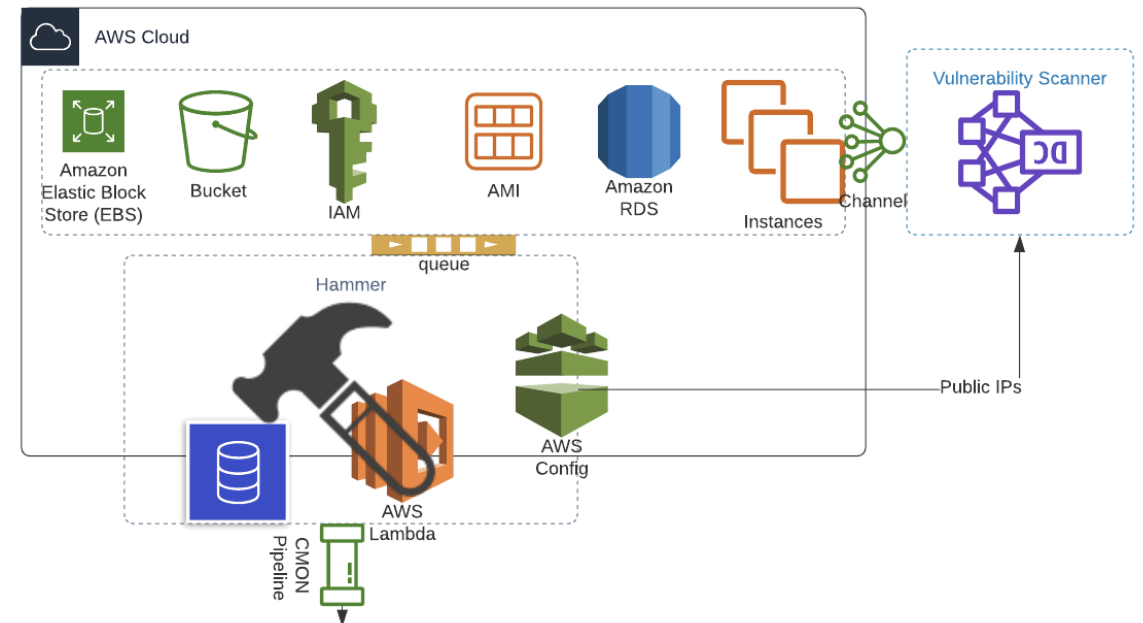
- Incorporates OSINT Tools
  - Amass
    - OWASP's Attack Surface Mapping tool
    - (<https://github.com/OWASP/Amass>)
  - Subfinder
    - subdomain discovery tool
    - (<https://github.com/projectdiscovery/subfinder>)
- Quick tips on breaking this down yourself
- <https://medium.com/ww-tech-blog/reducing-our-attack-surface-with-appsec-platform-4b6717a16709>





# Uber on AWS Continuous Monitoring

- Cloud Monitoring (CMON) Service from Uber
- CMON uses Hammer: (<https://github.com/dowjones/hammer>)
- Calculates vuln ratings before submitting tickets
- <https://medium.com/@ubersecurity/part-1-aws-continuous-monitoring-f39f81ea6801>



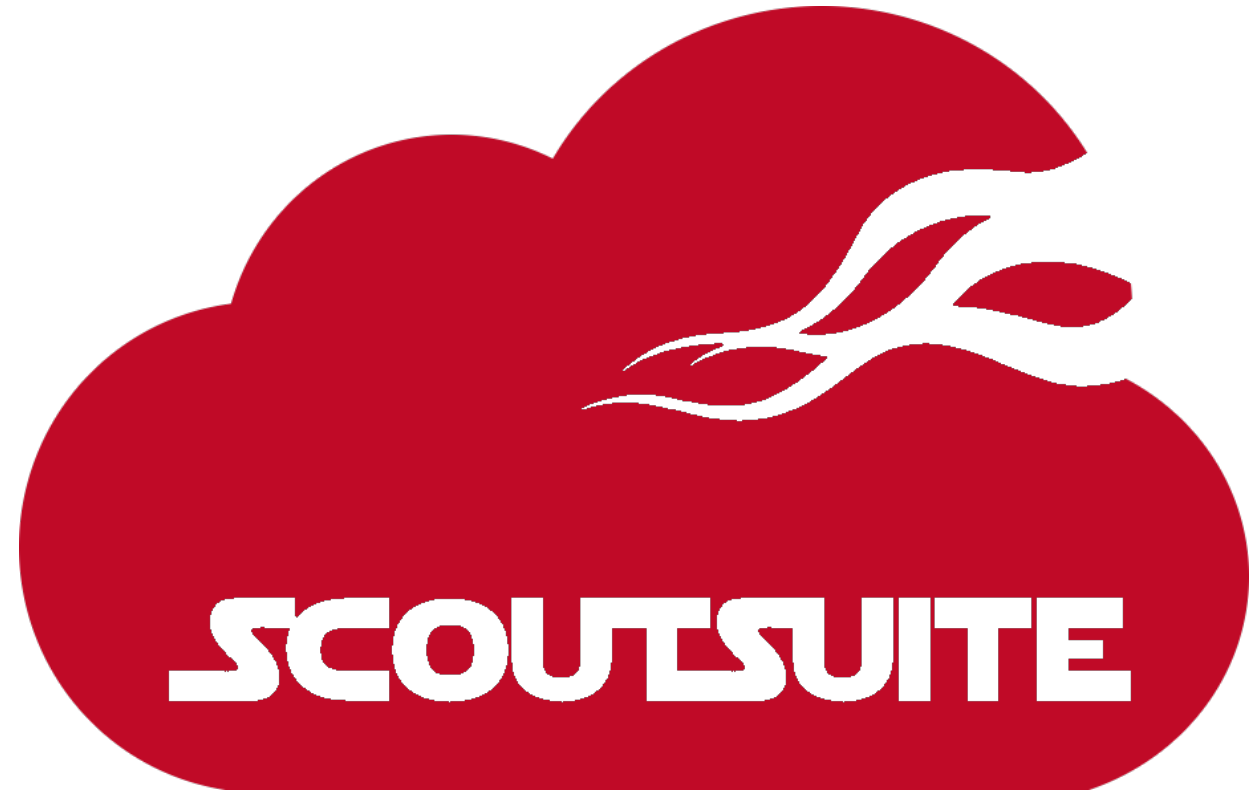
# Smogcloud from Bishop Fox

- Announced as part of Black Hat 2020
- Smog, the cloud that know one wants
- Finds assets in the following services:
  - API Gateway \* CloudFront \* EC2 \* Elastic Kubernetes Service \* Elastic Beanstalk \* Elastic Search \* Elastic Load Balancing \* IoT \* Lightsail \* MediaStore \* Relational Database Service \* Redshift \* Route53 \* S3
- <https://github.com/BishopFox/smogcloud>



# ScoutSuite – Multi Cloud Auditing

- [ScoutSuite](#) now supports most major cloud providers:
  - Amazon Web Services
  - Microsoft Azure
  - Google Cloud Platform
  - Alibaba Cloud (alpha)
  - Oracle Cloud Infrastructure (alpha)
- Full HTML report generated with action items



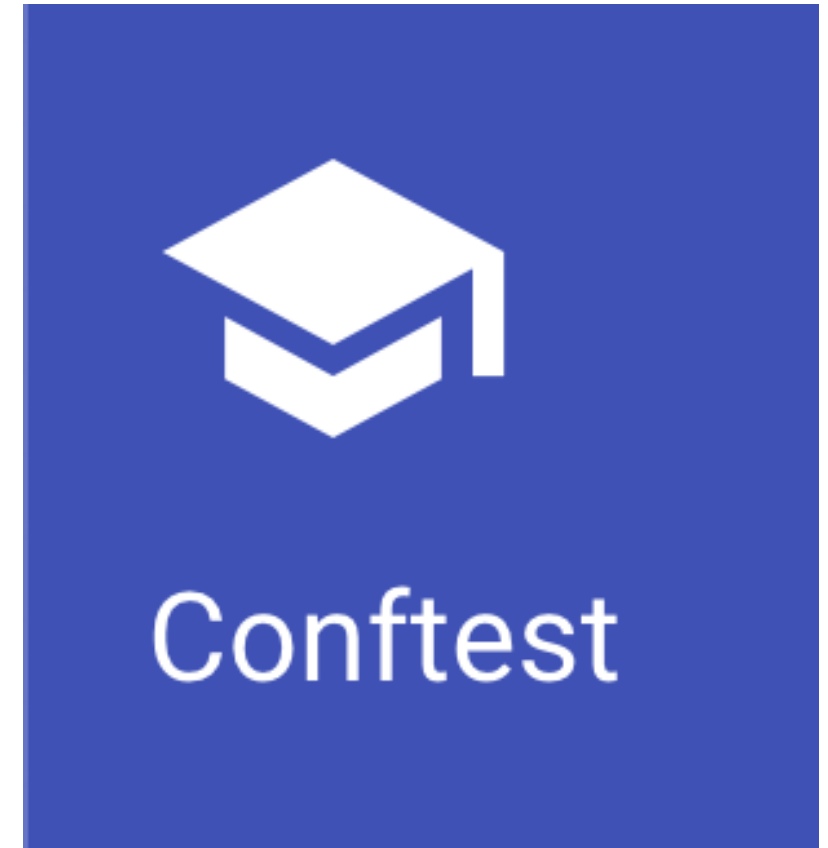
# Forseti for GCP

- Scan your entire GCP
- Inventory your entire GCP platform
- Monitor and alerting
- Enforce your own rules
- <https://cyral.com/blog/how-to-get-started-forseti-gcp/>
- <https://forsetisecurity.org/>



# Conftest – Test Your Terraform Before Deployment

- Write tests for your Infrastructure as Code
- Conftest relies on Rego from OPA
- <https://www.conftest.dev/>
- <https://www.praetorian.com/blog/leveraging-devsecops-practices-to-manage-red-team-infrastructure>





# Kubernetes – Gateway to Data

- <https://github.com/darkbitio/mkit>
  - Managed Kubernetes Inspection Tool
  - AKS, EKS, GKE and K8s by itself
- <https://sysdig.com/blog/gitops-k8s-security-configwatch/>
  - GitHub Action based config review
- <https://www.infracloud.io/blogs/kubernetes-pod-security-policies-opa/>
  - Implement PSP with OPA
- <https://github.com/google/gke-auditor>
  - Detect a set of common GKE misconfigurations



# APICheck – Test your APIs

- [APICheck](#) is an environment for integrating existing HTTP APIs tools and creating execution chains easily
- Sensitive data check module
- Many other modules available
- <https://bbva.github.io/apicheck/>
- See also fuzz-lightyear, Yelp's tool for Swagger fuzzing and more
  - <https://engineeringblog.yelp.com/2020/01/automated-idor-discovery-through-stateful-swagger-fuzzing.html>

## OWASP APICheck

[Main](#)[Quickstart](#)[Tools](#)

# Git Hound

- A batch-catching, pattern-matching, patch-attacking secret snatcher.
- Proven track record in bug bounty programs
- <https://github.com/tillson/git-hound>
- See also:
  - <https://github.com/aws-labs/git-secrets>
  - <https://github.com/OWASP/SEDATED>
- What should I do if I leaked secrets?  
<https://blog.gitguardian.com/leaking-secrets-on-github-what-to-do/>

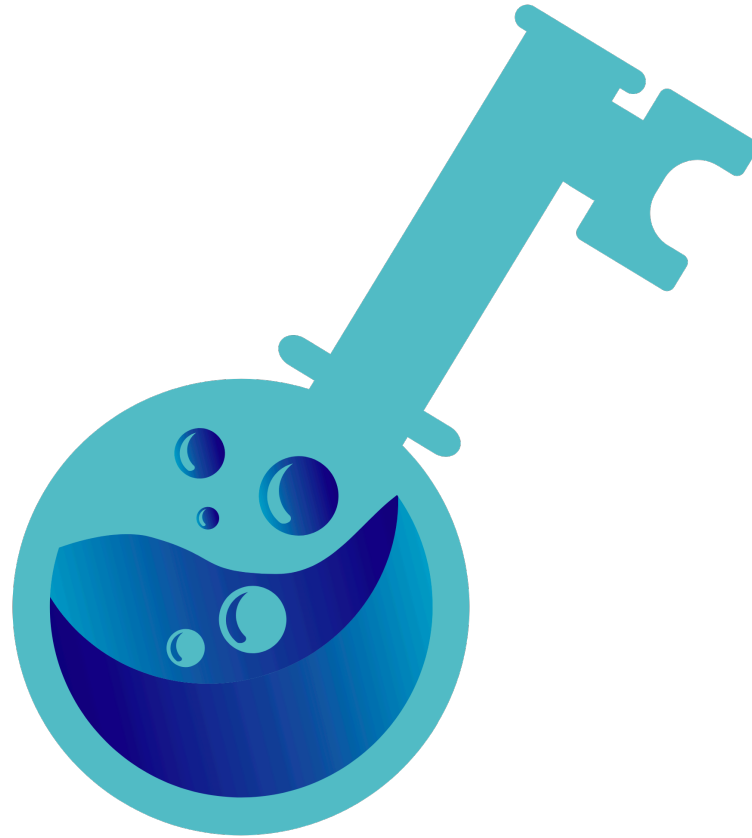


# Slack Watchman

- Search recently or all time for:
  - Externally shared channels
  - Potential leaked passwords
  - AWS Keys
  - GCP keys
  - Slack API keys
  - Private keys
  - Bank card details
  - Certificate files
  - Potentially interesting/malicious files (.docm, .xlsm, .zip etc.)
- <https://github.com/PaperMtn/slack-watchman>
- Just announced [Github and Gitlab watchman](#), both are available on Github



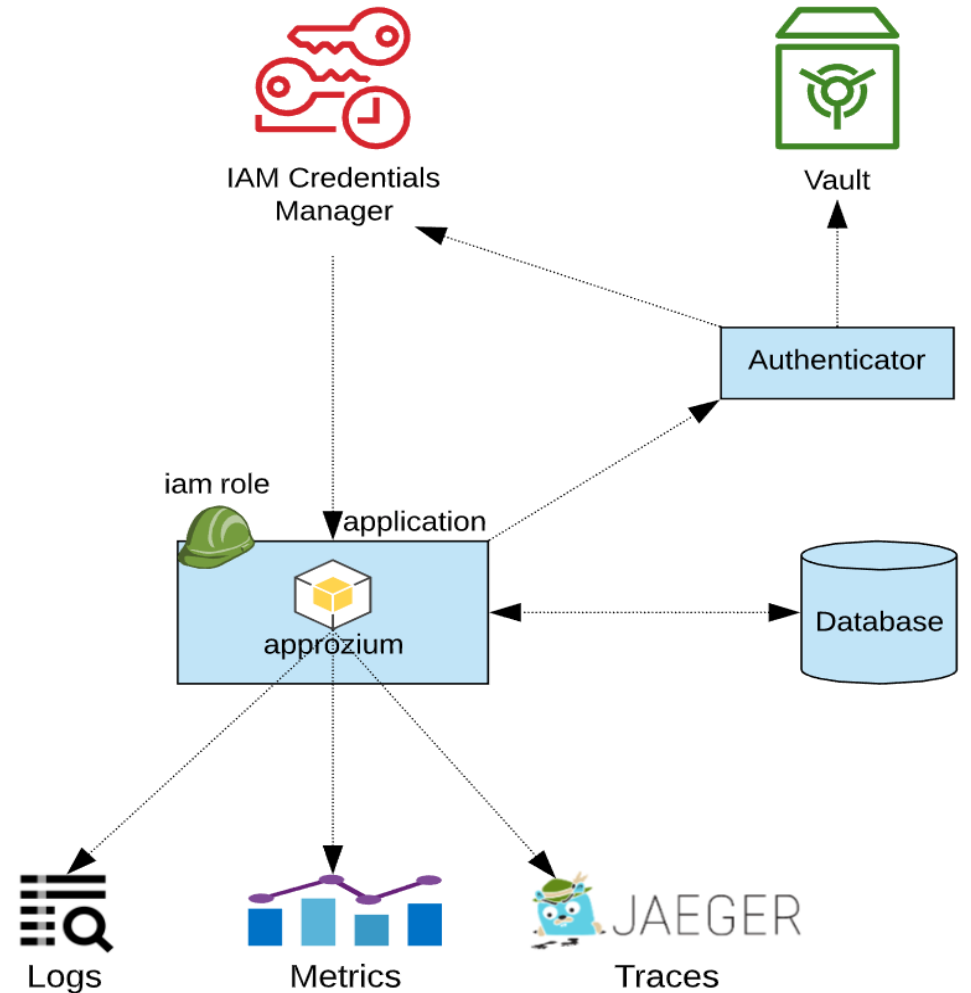
# Announcing Approzium





# Approzium Architecture

- 2 components
  - SDK & Authenticator Service
- SDK queries metadata services for context
- Authenticator service supports load balancing and auto scaling for high availability



# Approzium Observability

- Security-oriented logs
  - Identity logged at INFO level
  - Suspicious activity logged at WARN level
- Security-oriented metrics
  - Identity Verification Failures
  - Password Retrieval Failures
  - Unauthorized Password Attempts



# Password-less Authentication

- Can use built-in identity
- Pick your secrets manager
- The main approach is unleakable passwords
- Security-oriented observability at the forefront
- SDK does all of the heavy lifting



# Roadmap

- Currently supports:
  - Postgres, MySQL, AWS RDS, MariaDB, AWS Aurora, Python, AWS identity, Vault, AWS Secrets Manager
- Coming soon:
  - GCP & Azure identity
  - Mongo & Redis
  - GCP & Azure secrets management
  - Tracing
- <https://approzium.com/>
- <https://github.com/cyralinc/approzium>



# OWASP Database Security Cheat Sheet

- Written for devs, great primer on what to do in general
- Circulate and use as a teaching tool
- Check out the rest of their cheat sheet series!
- [https://cheatsheetseries.owasp.org/cheatsheets/Database\\_Security\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html)



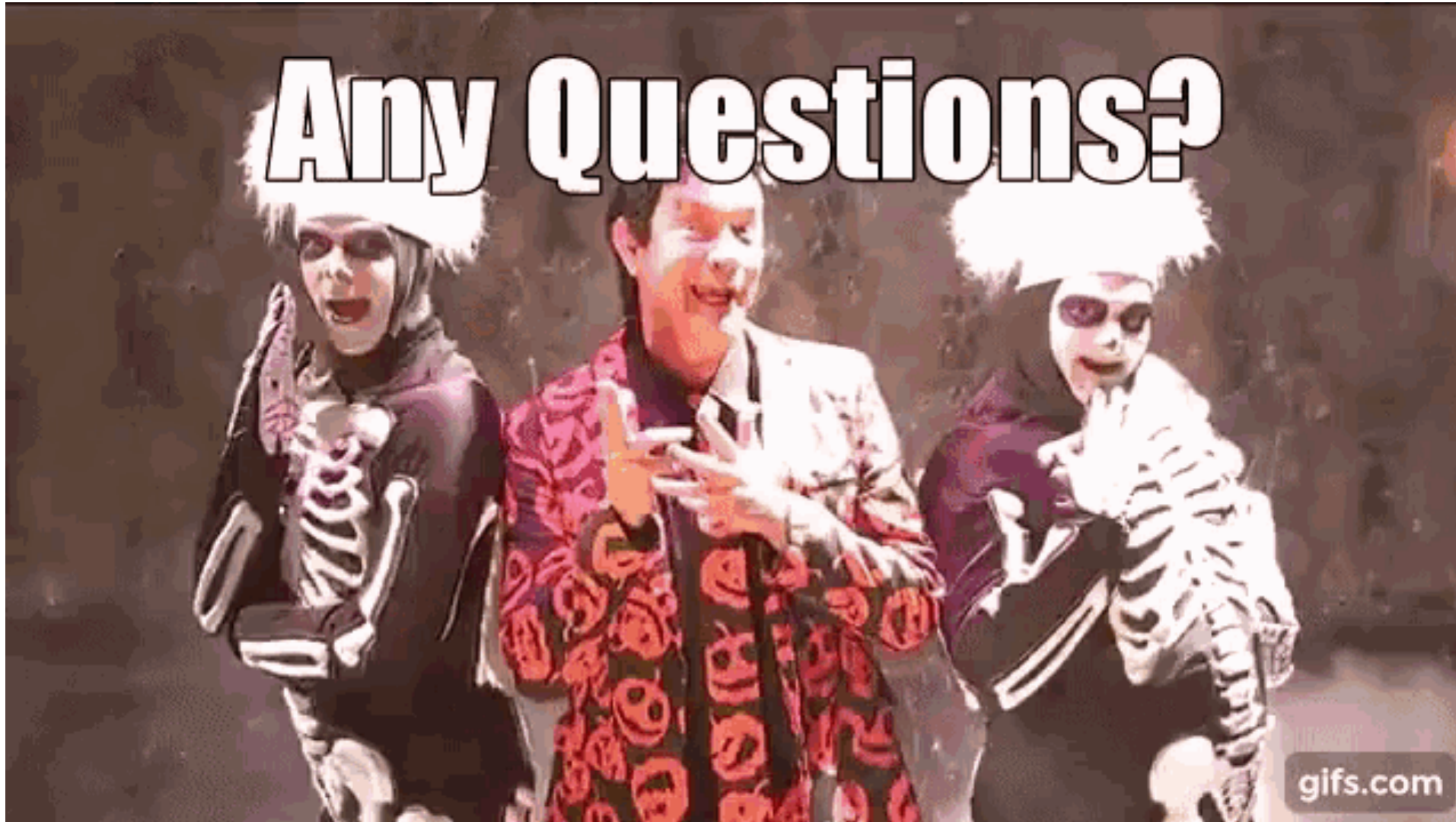


# Official Documentation For Secure Configuration

- [CouchDB](#)
- [Elasticsearch](#)
- [Kibana](#)
- [MongoDB](#)
- [MySQL](#)
- [Redis](#)
- [S3](#)



# Any Questions?



- Twitter: @dant24
- <https://cyral.com/careers/>