

RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

SESSION ID: CSCO-T09

Walking on Broken Clouds



#RSAC

Chris Farris

PrimeHarbor Technologies, LLC

www.primeharbor.com

[@jcfarris@infosec.exchange](mailto:jcfarris@infosec.exchange)

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2023 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.



Who Am I?

- Built the cloud security programs for some media companies
- Founder: fwd:cloudsec conference
- Rants a lot on Twitter and Mastodon

THAT'S WHAT I DO:
I DRINK AND
I KNOW THINGS.



Agenda

- How I built cloud security program(s)
- Cloud security challenges
- What worked
- What didn't
- What's a waste of your time
- What I will do different next time



RSAConference™2023

**Stronger
Together**

The History of CloudSec - Part1

Circa 2014-2017



#RSAC

The threats were out there...

black hat
USA 2014

```
Maybe if this is hosted at Amazon...

andres@laptop:~/S curl http://target.com/?\
                        url=http://169.254.169.254/latest/meta-data/ami-id

ami-a02f66f2    <---- the http response body

me jumping with joy ----->
```

black hat
USA 2014

“Pivoting in Amazon Clouds” - Andres Riancho - BlackHat 2014



... the tooling was not.



- CSPMs back then sucked
 - CIS Benchmarks
 - No ability to suppress false-positive or irrelevant findings
 - Lousy billing models
 - Didn't work in a multi-account environment
- Cloud threat protection didn't exist

Have you ever tried to cut-n-paste
JSON out of a PDF before?



My Journey



I've got 99 open buckets but this ain't one



Jerry Gamblin ✓ @JGamblin · Dec 19, 2017

Does anyone have a security **contact** @cnn? Found something they will want to look at ASAP.

10

27

31



Jerry Gamblin ✓ @JGamblin · Dec 19, 2017

Also Googling "**CNN Vulnerability Reporting**" or "**CNN Bug Bounty**" is useless if you are trying to find a **contact** actually at **CNN**.



2



Immediate tasks

- Identify what we have
- Figure out who to talk to
- Define *our* target security posture
- Get developer buy-in



RSAConference™2023



**Stronger
Together**

CloudSec is Hard Yo

#RSAC

App Definition & Development

Database: KV, Vitess, Cockroach Labs, Couchbase, etc.

Streaming & Messaging: cloudevents, NATS, etc.

Application Definition & Image Build: HELM, Backstage, Buildpacks.io, KubeVirt, OPERATOR FRAMEWORK, argo, flux, keptn, agola, etc.

Continuous Integration & Delivery: argo, flux, keptn, agola, etc.

Orchestration & Management

Scheduling & Orchestration: kubernetes, Crossplane, VOLCANO, etc.

Coordination & Service Discovery: CoreDNS, etcd, gRPC, etc.

Remote Procedure Call: gRPC, etc.

Service Proxy: envoy, CONTOUR, etc.

API Gateway: EMISSARY INGRESS, etc.

Service Mesh: LINKERD, Istio, etc.

Runtime

Cloud Native Storage: ROOK, CubeFS, LONGHORN, etc.

Container Runtime: cri-o, containerd, rkt, etc.

Cloud Native Network: cilium, CNI, etc.

Provisioning

Automation & Configuration: KubeEdge, airship, ANSIBLE, etc.

Container Registry: HARBOR, Dragonfly, etc.

Security & Compliance: Falco, in-toto, Kyverno, etc.

Key Management: spiffe, SPIRE, etc.

Platform

Certified Kubernetes - Distribution: AWS, Alibaba Cloud, etc.

Certified Kubernetes - Hosted: AWS, Alibaba Cloud, etc.

Certified Kubernetes - Installer: AWS, Alibaba Cloud, etc.

PaaS/Container Service: etc.

Observability and Analysis

Monitoring: Prometheus, cortex, OPENMETRICS, Thanos, etc.

Logging: fluentd, etc.

Serverless

CNCF Serverless Landscape: etc.

Members

Members: etc.

CD Foundation Landscape

CD Foundation Landscape: etc.

Kubernetes Certified Service Provider: etc.

Kubernetes Training Partner: etc.

Certified CNFs: etc.

CNCF Cloud Native Landscape

CNCF Cloud Native Landscape: etc.

Global Haystack



14 Regions (now 24)
115 Accounts
1,600 consoles to look in!

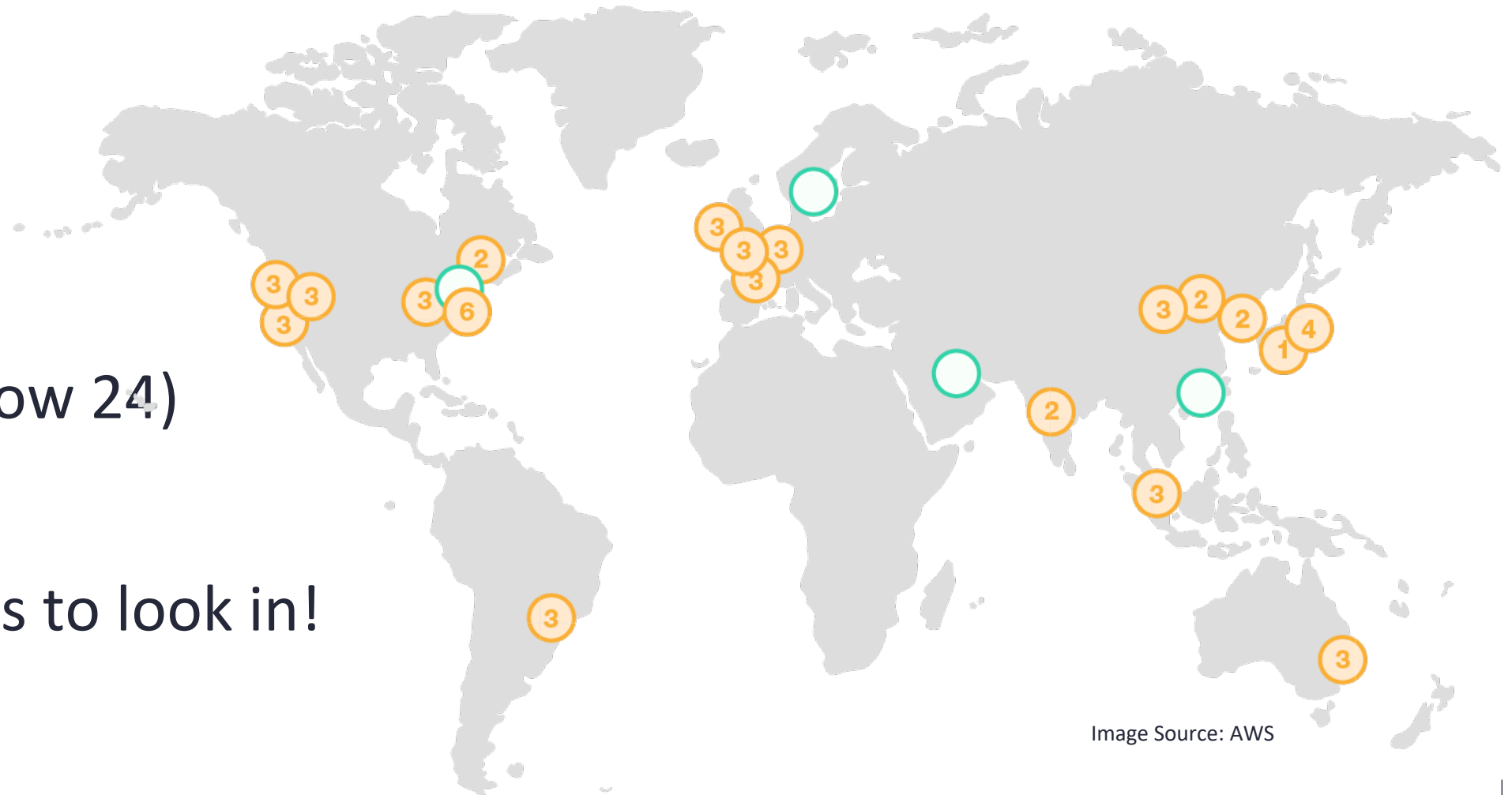


Image Source: AWS



Cloud Growth

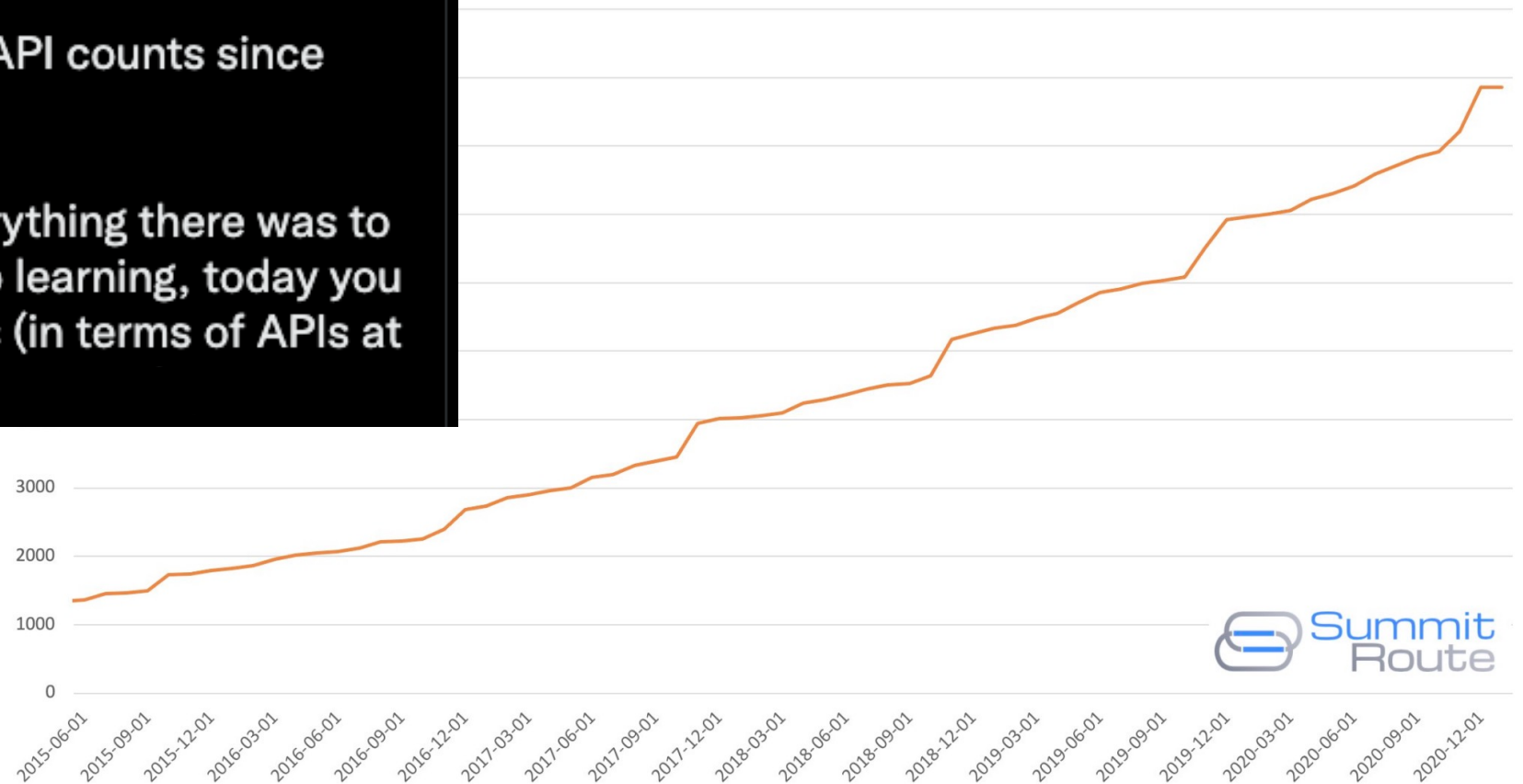


Scott Piper
@Oxdabbad00

Graphs of AWS service count and API counts since 2015.

If in late 2018 you had learned everything there was to know about AWS, and did not keep learning, today you know less than half of what AWS is (in terms of APIs at least).

AWS API count



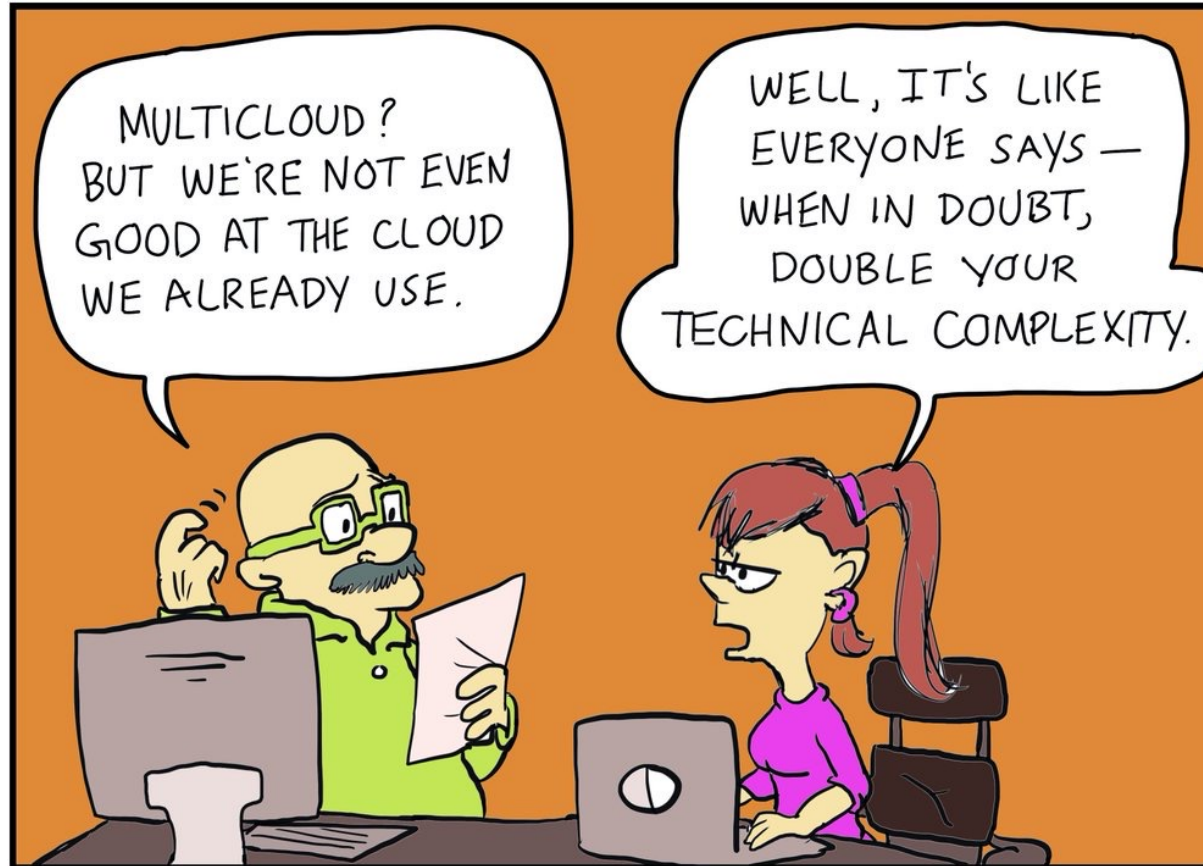
“Shared Responsibility is a failed model when the rate of change makes it physically impossible for customers to understand and responsibly use cloud services.”

– Chris (April 2023)



Multicloud

FaaS and Furious by Forrest Brazeal A CLOUD GURU



Multicloud: a problem in search of a problem.



What do you mean by Google SQL Database isn't in my VPC?

– Chris in the last few months

12:20 PM **Chris Farris** So... Let me get this straight. If I'm running a MySQL Google Cloud SQL Database, that DB isn't running in *my* VPC/google_compute_network. Instead it runs in some Google network that I don't have visibility to, and I'm supposed to peer my network with this mysterious other network so I can talk to my SQL DB over RFC1918 space. Am I understanding this right, and if so why shouldn't I be running screaming for the hills to raise Alpaca?



10 replies Last reply 1 month ago



What the heck is the cloud anyway?

#RSAC

Stronger
Together

- Cloud Native == Containers
- Public vs Private
- Machines in Bezos's datacenter
- Pipelines!



RSAConference™2023



**Stronger
Together**

What Worked!

Custom Cloud Standards

- Don't blindly adopt your CSPMs findings
- Focus on your risk
- Focus on your threat models
- Focus on your compliance requirements

- Don't cut-n-paste
- One per cloud provider



Feed your SOC



- We immediately got telemetry into Splunk
 - CloudTrail
 - GuardDuty
 - Account and IP Inventory
 - Billing!
- Training
 - What the heck does this mean?
 - What is Bad?



Inventory



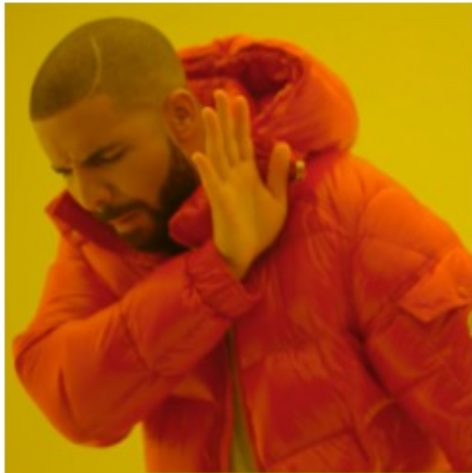
- Find All Our Cloud Accounts
- Get Audit Access
- Tag an executive
- Profit?
 - It certainly allowed us to operationalize the CSPM



What are critical controls one and two?



Centralized Cloud Team



Disengaged
cloud teams
that just
manage the bill



Engaged
cloud teams
focused
on governance

- Knows what's going on
- Deploys security artifacts
- Helps with incident containment
- Keeps owner info up-to-date
- Typically has better relationship with the developers

Cloud Provider Tooling



- GuardDuty
- Macie
- Access Analyzer
- CloudTrail

*They may not have been best-of-breed, but they were good enough.
Most importantly, they were easy to deploy*



Your SOC will hate you with this one simple trick



- Ensure certain CSPM violations are treated as in-the-moment incidents rather than compliance violation findings reported a week later.
- Complex logic required
 - 3389
 - Open to 0.0.0.0/0
 - Target host is Windows



Incident Worthy!

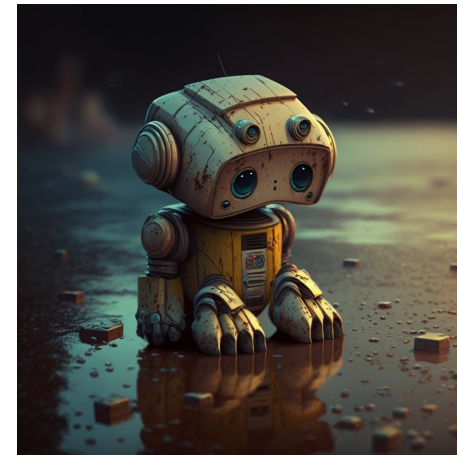


What didn't work

But that doesn't mean they're not worth trying...

Pitfalls of prevention

- AWS Service Control Policies
- Azure Policies
- GCP Organization Policies
- The difference between “You can’t do X” and “You can’t do X, if these very specific conditions are met”
- Only applies to Security Invariants
- Very inflexible



Tagging

How it started...



How it went...

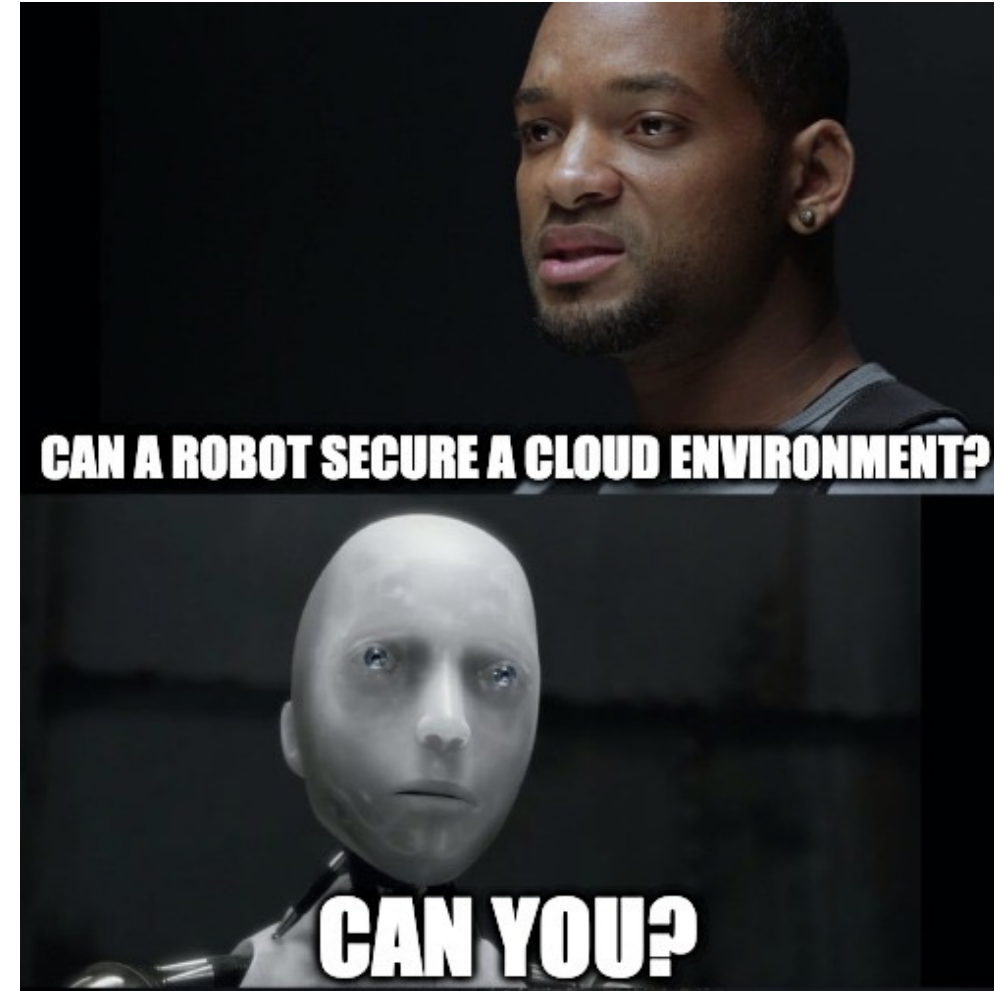


How it's still going...



The allure of auto-remediation

- Speed of remediation
- Cost effective
- It's what the cool kids are doing



*Auto remediation is like nuclear power.
One accident and suddenly everyone is against it*



Farris's Three Laws



- A bot should not harm production, or at least, it must minimize the risk of harm to production.
- A bot must execute its orders (to secure the environment) except where such orders would conflict with the First Law.
- A bot must announce its own existence and actions whenever it acts on the first or second law.



The pipeline excuse



“If your engineers are telling you everything is all deployed via pipeline - they’re lying to you!!!”



IaC Scanning



- Better than auto-remediation when IaC is involved
- Easier feedback to carbon-based lifeform
- Needs to be a developer-led initiative
 - With support from security





“If you ask a developer to fix a problem, you’ve annoyed them. If you tell them they have to change their CI/CD pipeline, you’ve made an enemy for life.”

- Chris (circa 2022)



Having a Cloud Security Team




RSAConference™2023



**Stronger
Together**

What's a waste of time...

Policy requirements to appease others

- Get acquired by a company with a 1000-person security team
- Their policies looked like this 
- I wrote a cloud policy in an afternoon
- Imposter Syndrome is real



CSPM is a tarpit

#RSAC

Stronger
Together



not m*rt*n

@weekend3warrior

Everyone talks about how social media is bad for your mental health but what about Excel?



Why *are* they still the main thing?



Dr. Anton Chuvakin 

@anton_chuvakin



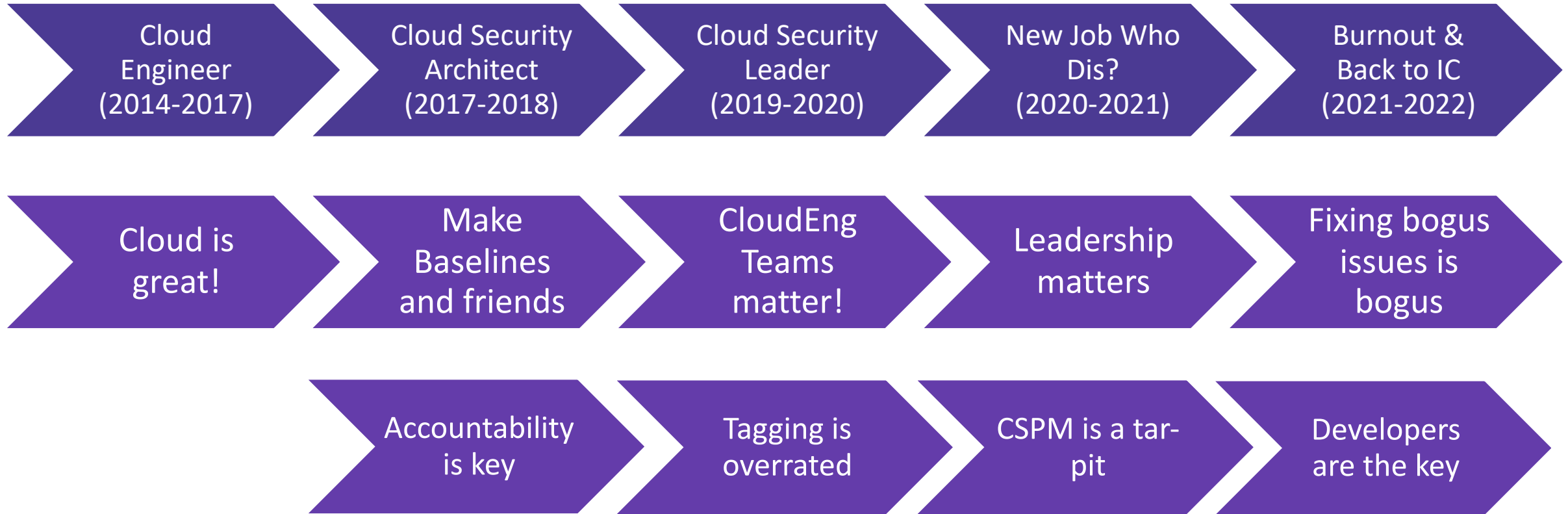
OK, don't hate me, but let me ask this: the 1st **#CSPM** vendor (to secure cloud configs) was born in 2012-2013. Today is 2023. 10 years of working on cloud misconfigurations for security.

WHY ARE THEY STILL A THING? WHY ARE THEY STILL THE MAIN THING? WTAF?

6:11 PM · Mar 17, 2023 · **49.7K** Views



My journey of self awareness



So What?

“Learn from the mistakes of others. You can't live long enough to make them all yourself.”

— Eleanor Roosevelt

Developers are the key

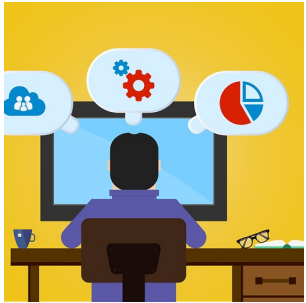


*No amount of Wiz, SCPs, or CloudCustodian can make up for an informed developer taking the extra time to not put * in their terraform file.*

The ultimate shift-left security flex is to educate and empower developers.



Part of a complete breakfast...



Educated & Empowered Developers



Architectural and Design Reviews



IaC Scanning



Prevention



Auto Remediation



Spreadsheet Hell



Where to go from here



- Don't throw out your CSPM
 - Don't make it the focus of your CloudSec efforts either
- Embrace your developers
 - Our slogan is “Stronger Together”
 - Articulate the risk to your developer community
 - If you sound ridiculous, is this really a business priority?
- Make them partners in the shift left



RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

SESSION ID: CSCO-T09 – Walking on Broken Clouds


Questions?




#RSAC

Chris Farris

 <https://www.chrisfarris.com>

 <https://infosec.exchange/@jcfarris>

 @jcfarris

 <https://www.linkedin.com/in/jcfarris>

 <https://www.primeharbor.com>