CLOUD SECURITY MONITORING (at scale)

Chris Farris
Cloud Security Architect

WARNERMEDIA

WHO AM I?

Cloud Security Architect for WarnerMedia

My job is to keep the Russians off cnn.com and my friends from downloading Rick & Morty

WARNERMEDIA

tbs · TNT · CNN · Boomerang · Cartoon Network · [adult swim] · HLN · truTV · TCM Turner Classic Movies · Turner Sports · b/r

WB Now That's Hollywood! · TCM · 旅 TABI Channel · CHV · WB TV · glitz* · TCM · TOONAMI · TNT Film · Space · Boing

Much · cartoonito · h TV · MONDO TV · Esporte Interativo · TNT Serie · tooncast · pogo · IMF · TNT Comedy · TCM Turner Classic Movies

ch! · CISAT · HBO · TCM cinéma

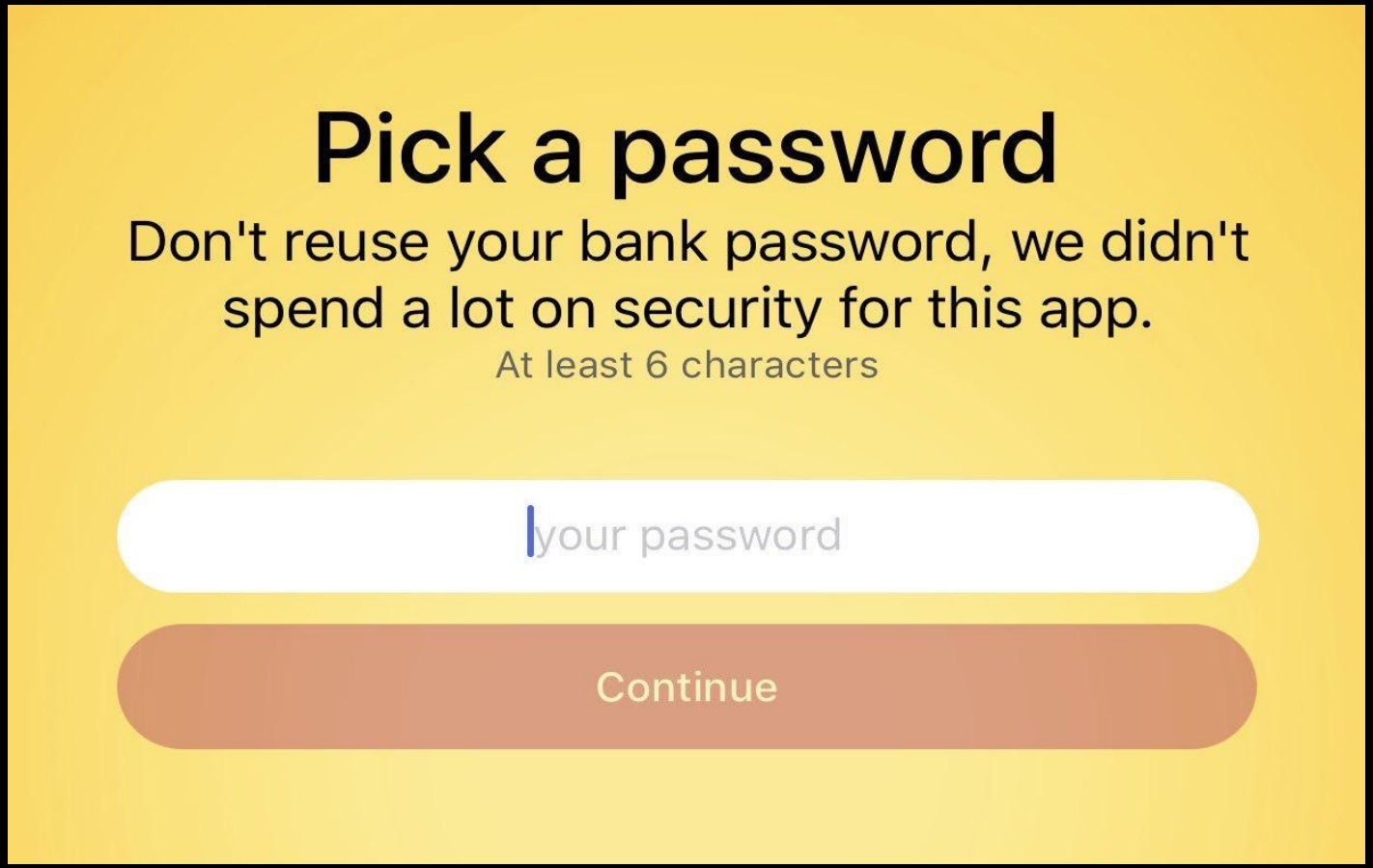
AGENDA

- Our Story
- How we think about Cloud
- Cloud Security Standards
- Cloud Security Scorecards
- Multi-Account Visibility
- Lessons Learned

TO THE CLOUD!

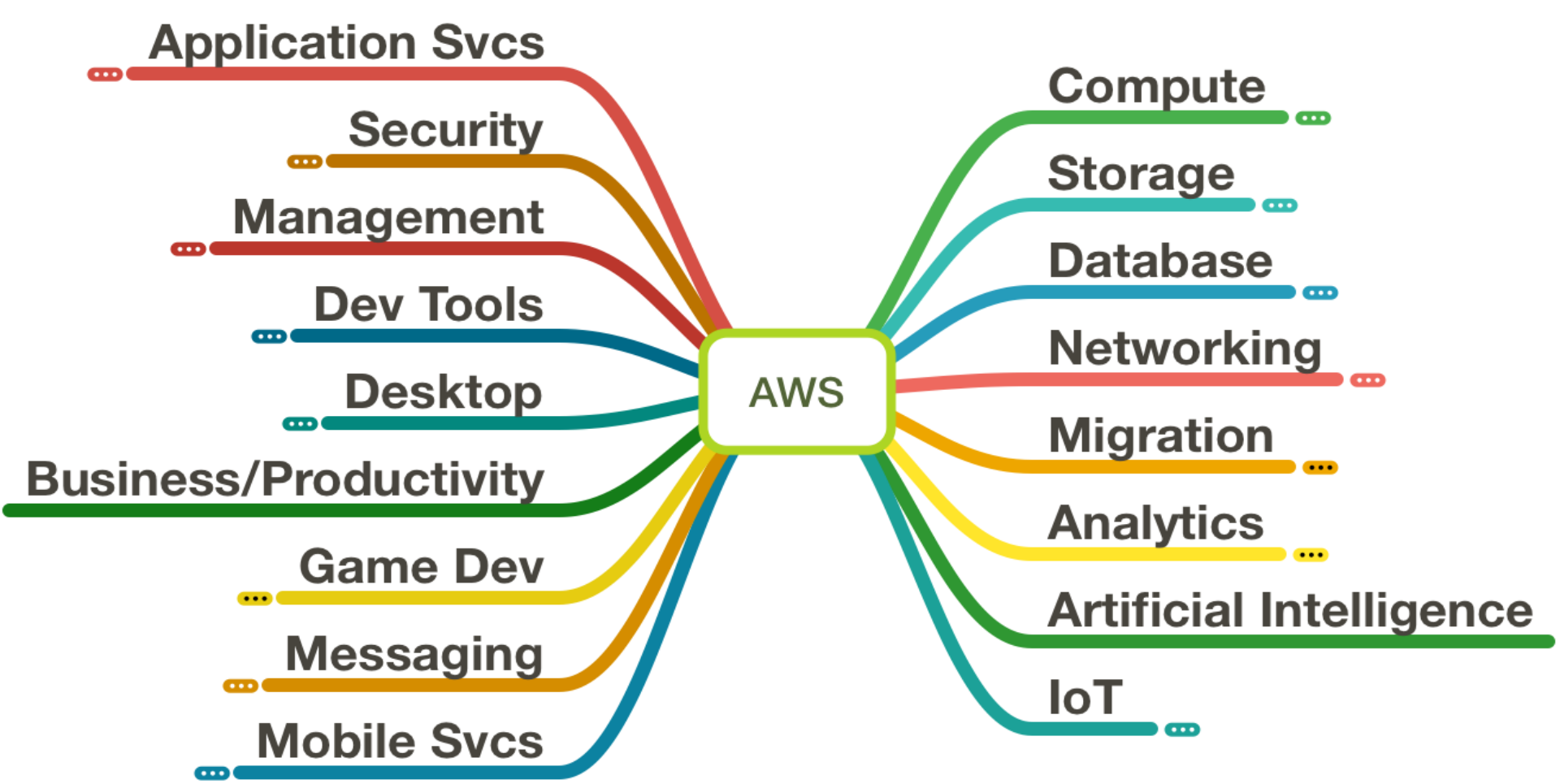
Lord of the Rings: The Two Towers - Battle at Helm’s Deep (WarnerBros 2002)

TURNER CLOUD SECURITY

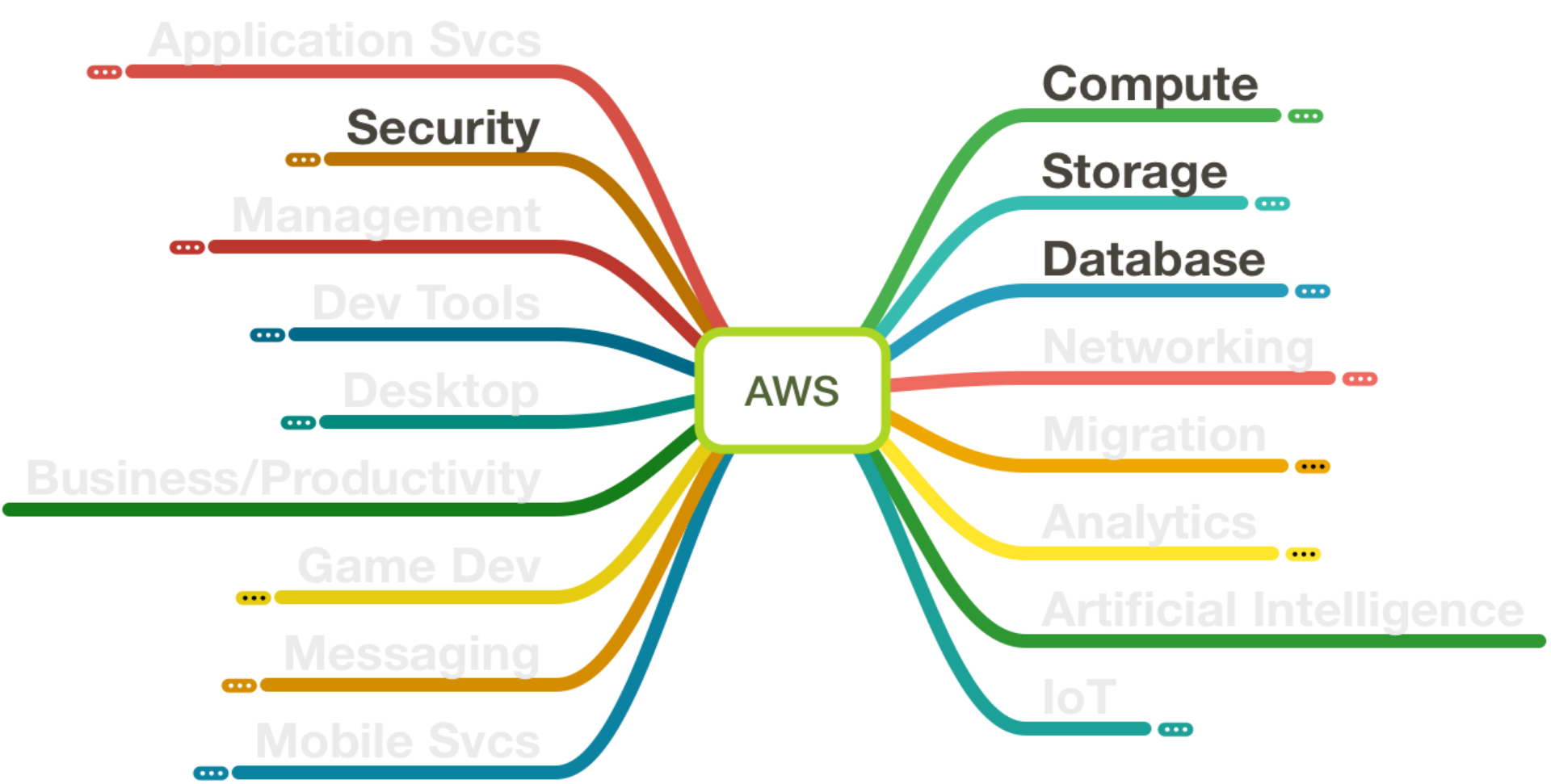

Pick a password
Don't reuse your bank password, we didn't spend a lot on security for this app.
At least 6 characters
your password
Continue


[adult swim]

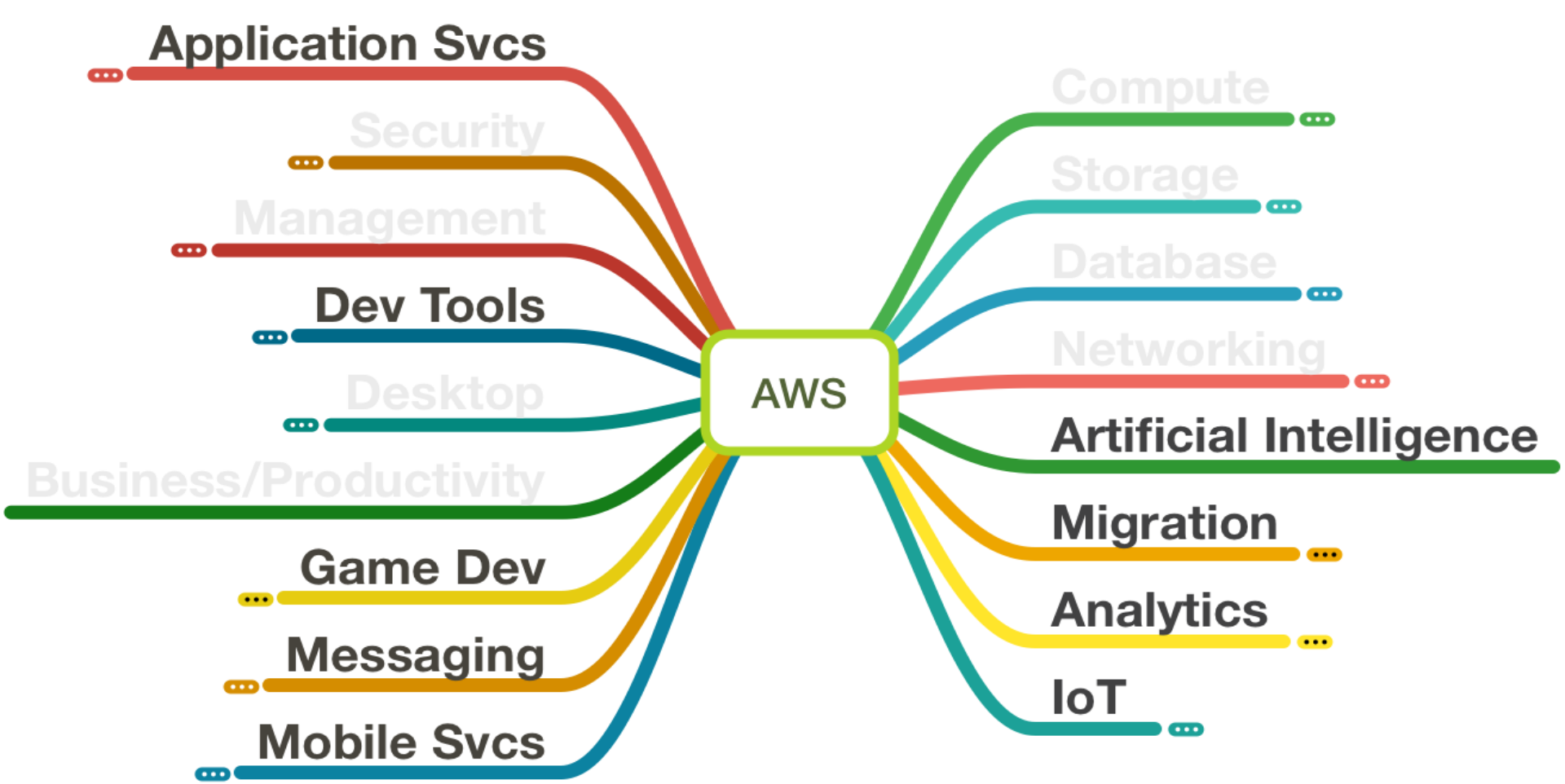
THE SURFACE AREA OF AWS



WHAT SECURITY WORRIES ABOUT



WHAT DEVELOPERS ARE EXCITED TO USE



300 (Warner Bros. Pictures 2006)

TOOLS SUCK

- Per-account pricing - anti-pattern for multi-account strategy
- Per-resource pricing - pay more for security than the resource
- At some scale, build yourself makes sense
- Only one vendor supports Neptune Databases (released re:Invent2017)

SECURITY TOOL PRICING SHOULD NOT DICTATE ARCHITECTURE!!!

SECURITY TOOL PRICING
SHOULD NOT
UNDERMINE
SECURITY ARCHITECTURE!!!

MULTI-CLOUD

- Opensource community is focused on AWS
- Vendors are just starting to “get” Azure
- IAM is vastly different
- Account-governance is vastly different

“MULTICLOUD STRATEGY” IS CODE FOR OFF-PREM VIRTUAL MACHINES

And legacy architecture masquerading as the new-hotness


END OF RANT

ROADMAP

1. Multi-Account Strategy
2. Security AWS Account
3. Cross-Account Audit Roles
4. AWS Organizations
5. Cloud Security Standard
6. Cloud Security Scorecard
7. Multi-Account Inventory & Management

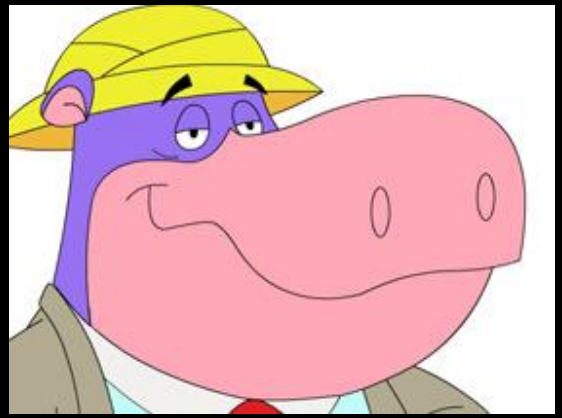
CLOUD SECURITY STANDARD

- KISS
- Focus on *your* risk and *your* culture
- Define accountability
- CIS Benchmarks are a start
- Consensus Driven
- Requirements “must”
- Best Practices “should”

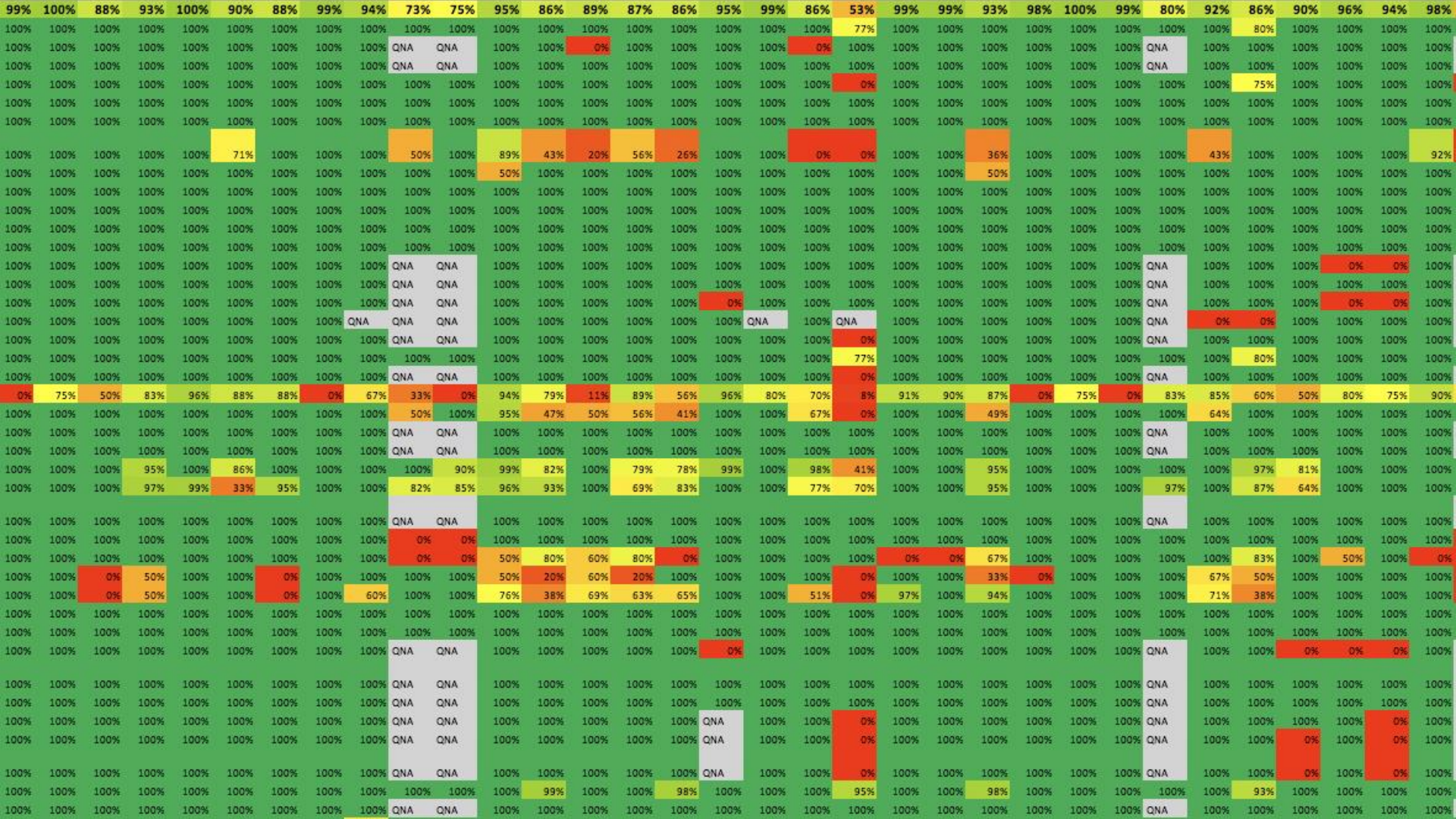
https://www.chrisfarris.com/post/cloud-security-standard/

SCORECARDS

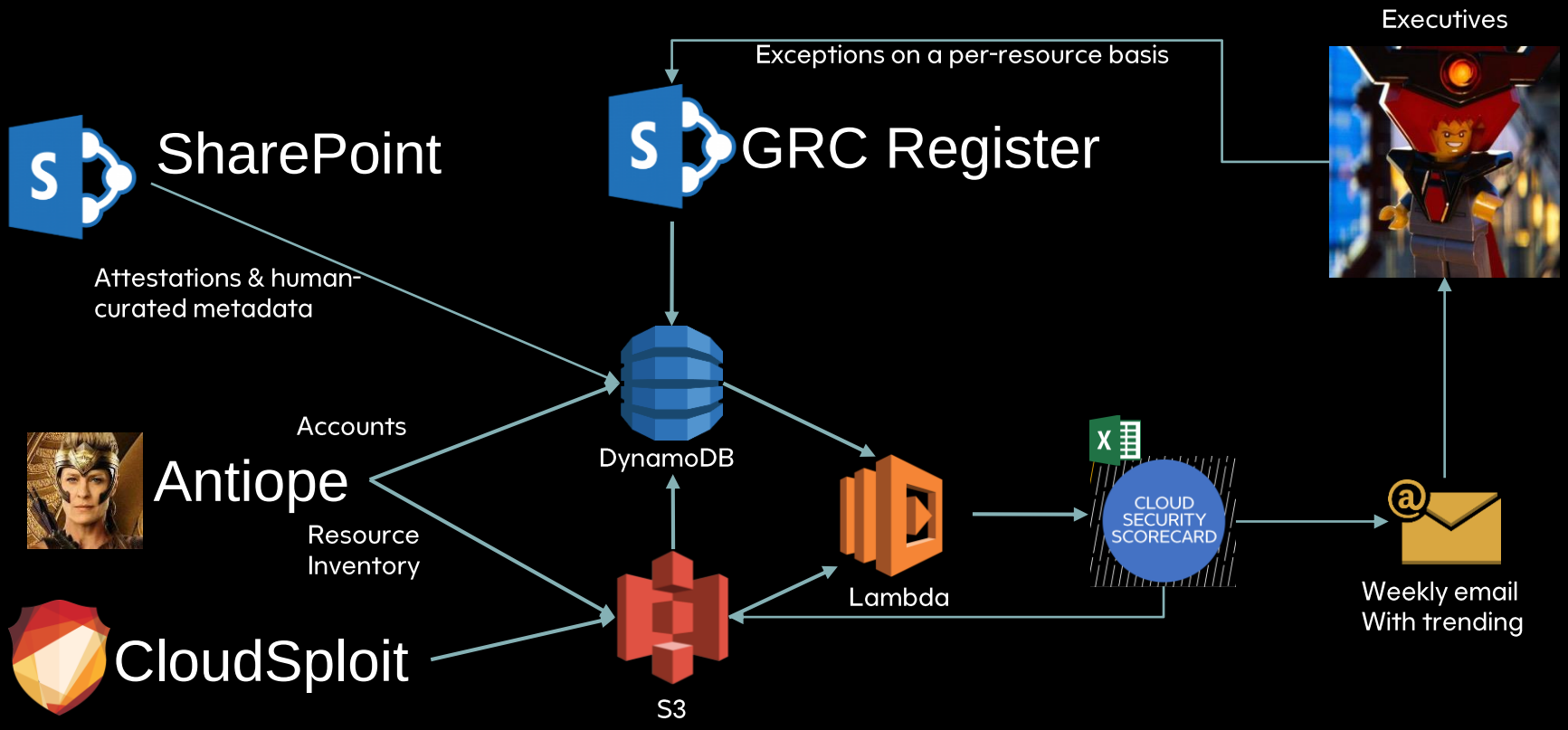
Did ya get that spreadsheet I sent you?



Executive Sponsor	Score	Total Spend
Alan Probe	61%	$44,571.21
Carl Brutananadilewski	96%	$46,822.29
Frylock	99%	$1,672.02
Harvey Birdman	99%	$78.89
Ignignokt	83%	$2,114.55
Master Shake	97%	$22,505.57
Meatwad	95%	$93,151.77
Mentok	93%	$1,132,425.64
Peter Potamus	96%	$999.93
Phil Ken Sebben	81%	$4,157.52
Ryu	91%	$10,786.92
Dr. Blake Downs	96%	$27,752.35
Brak	99%	$28,651.99
Space Ghost	100%	$1,554.53
Huey Freeman	90%	$8,602.14
Morty Smith	100%	$97.45
Rick Sanchez	92%	$8,992.38
Summer Smith	93%	$77,998.17
Mr. Meeseeks	84%	$7,436.16
Pickle Rick	91%	$9,659.12
MC Pee Pants	51%	$3,537.44
Peter Potamus	39%	$183,250.56



CLOUD SECURITY SCORECARDS



https://www.chrisfarris.com/post/scorecardsystem/

ANTIOPE https://github.com/turnerlabs/antiope

- Lots of accounts and lots of regions makes for a big haystack
- Enterprise tools are ridiculously expensive
- AWS Config service doesn’t support all AWS services at Turner
- Requirement to track (and identify) foreign AWS accounts
- Search engine to help find BGSHs
- Opensource
- Azure & GCP are in progress
- An-Tie-Oh-Pee

Robin Wright as Antiope
Wonder Woman 1984 (Warner Bros. Pictures)

WHAT IT MONITORS (today)

- EC2
- Security Groups
- Elastic Network Interfaces
- Route 53 Domains
- Route 53 Zones
- ElasticSearch
- ECS Tasks & Clusters
- ECR Repos
- CloudFront
- CloudFormation
- AMIs
- VPCs, VPN & Direct connect
- IAM Roles & Users
- Lambda & Lambda Layers
- Trusted Advisor
- Support Cases

THREAT HUNT

Hypothesis: “Someone has a publicly open AWS ElasticSearch domain”

Step 1 - Inventory all ElasticSearch domains

Step 2 - ES Query to find access policy with Principal = * and no Conditions

Step 3 - panic a little

Step 4 - add query to CSS Scorecards

THREAT HUNT

Hypothesis: “There are CloudFront distributions pointing to buckets that don’t exist or are controlled by others”

Step 1 - Inventory all CloudFront distributions

Step 2 - ES Query to find distributions with S3 as an origin

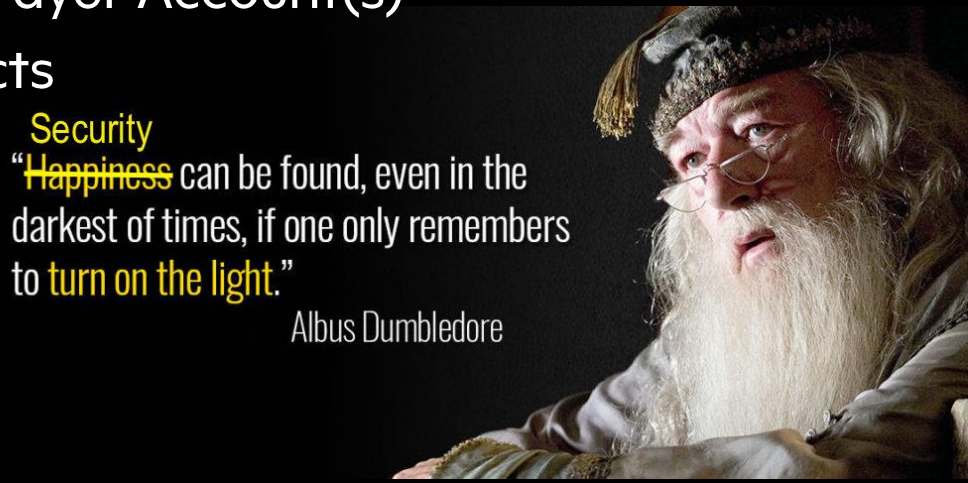
Step 3 - ES Query to get all Turner Buckets.

Step 4 - Python script to merge

Step 5 - Hand off results to VM team

WHAT WE DID RIGHT

- “Bubble of accountability”
- Fully automated account creation process
- Easy to read standards that make sense for Turner
- All issues enumerated in the hands of those empowered to fix
- Good relations with owners of Payer Account(s)
- Spreadsheets are useful artifacts
- Educate the SOC & Compliance teams



WHAT WE DID WRONG

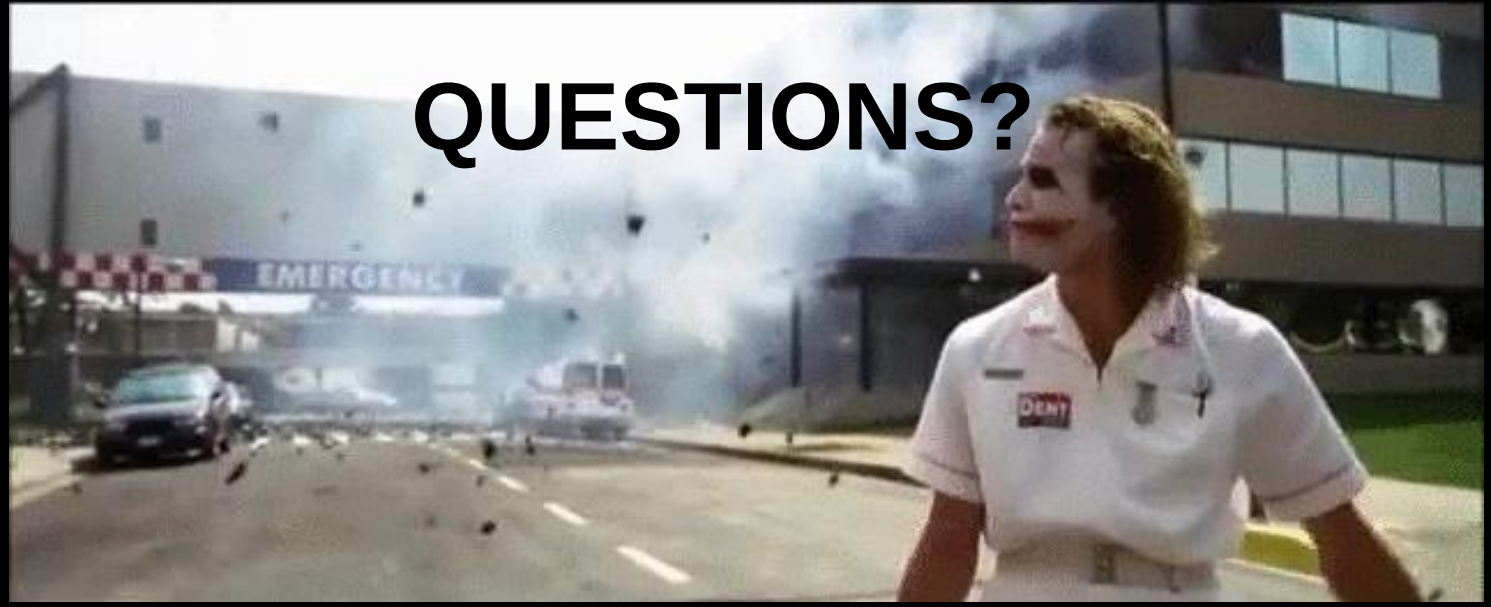
- Cloud Governance (or lack there of)
- Multi-tenant accounts
- Attestations
- Build v Buy
- Letter grades v Pass/Fail
- Too Much Diversity!!!
- Being Multi-cloud

(At least we didn't bring our dragon north of the wall)

LESSONS FOR A LARGE ENVIRONMENT

- Monitor the Support tickets
- Set your Security Contact
- GuardDuty severities are not good guidance
- Work with your SOC to understand CloudTrail

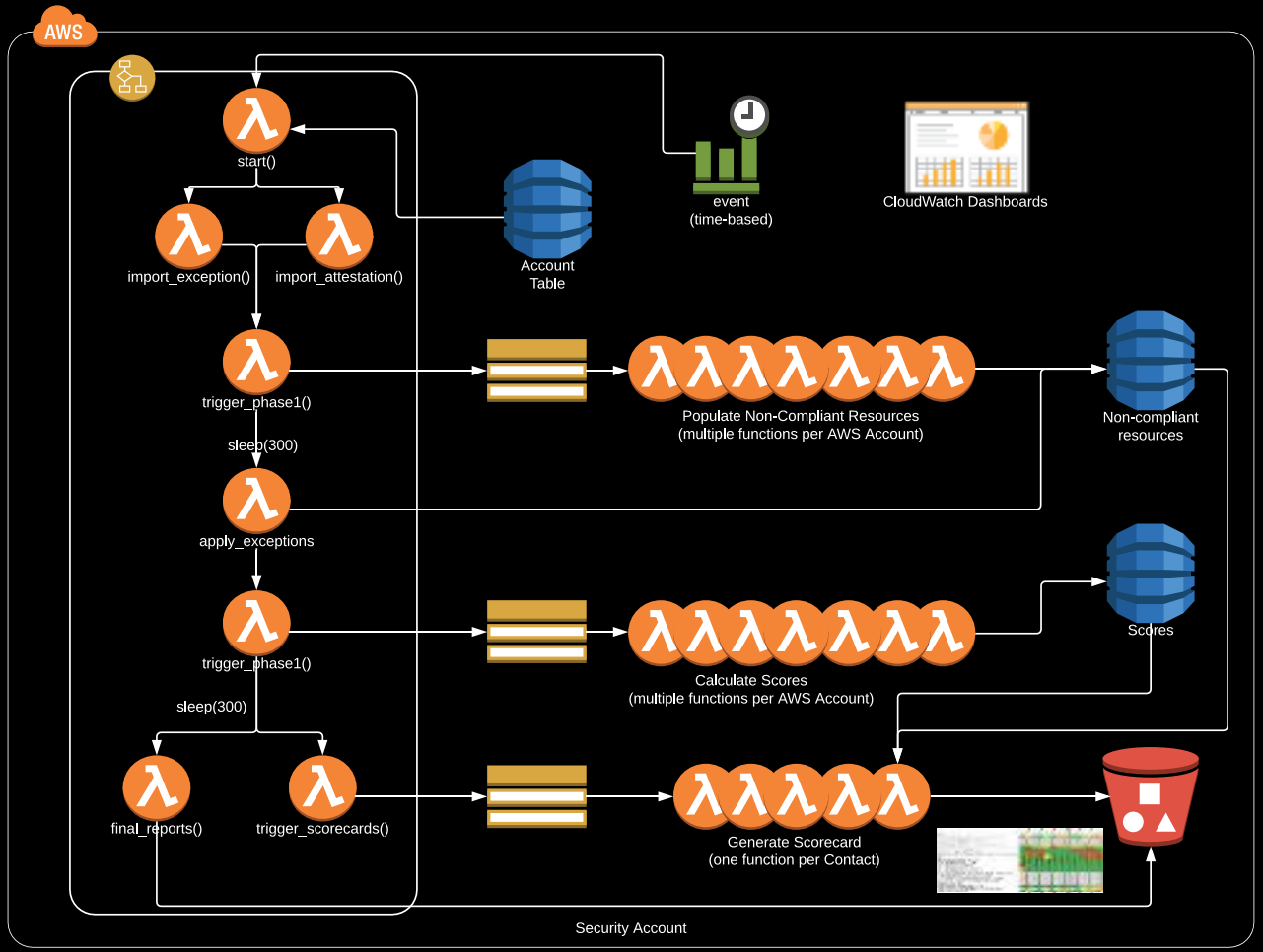
QUESTIONS?



- @jcfarris
- https://github.com/jchrisfarris
- https://www.linkedin.com/in/jcfarris
- http://www.chrisfarris.com
- https://github.com/turnerlabs/antiope

COMPLIANCE SCORECARDS

Chris Farris | October 11, 2018



ANTIOPE (AWS)

Chris Farris | April 12, 2019