CLOUD SECURITY MONITORING (at scale)

Chris Farris
Cloud Security Architect

WARNER MEDIA
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
AGENDA

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

FOR THE CLOUD IS DARK

AND FULL OF TERRORS
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
THE SURFACE AREA OF AWS
WHAT SECURITY WORRIES ABOUT

AWS

- Compute
- Storage
- Database
- Networking
- Migration
- Analytics
- Artificial Intelligence
- IoT
- Mobile Svcs
- Messaging
- Game Dev
- Desktop
- Dev Tools
- Management
- Security
- Application Svcs

Business/Productivity
WHAT DEVELOPERS ARE EXCITED TO USE

- Application Svcs
- Security
- Management
- Dev Tools
- Desktop
- Business/Productivity
- Game Dev
- Messaging
- Mobile Svcs
- Compute
- Storage
- Database
- Networking
- Artificial Intelligence
- Migration
- Analytics
- IoT
THIS IS
SERVERLESS
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
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?

<table>
<thead>
<tr>
<th>Executive Sponsor</th>
<th>Score</th>
<th>Total Spend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alan Probe</td>
<td>61%</td>
<td>$44,571.21</td>
</tr>
<tr>
<td>Carl Brutalanadilewski</td>
<td>96%</td>
<td>$46,822.29</td>
</tr>
<tr>
<td>Frylock</td>
<td>99%</td>
<td>$1,672.02</td>
</tr>
<tr>
<td>Harvey Birdman</td>
<td>99%</td>
<td>$78.89</td>
</tr>
<tr>
<td>Ignignokt</td>
<td>83%</td>
<td>$2,114.55</td>
</tr>
<tr>
<td>Master Shake</td>
<td>97%</td>
<td>$22,505.57</td>
</tr>
<tr>
<td>Meatwad</td>
<td>95%</td>
<td>$93,151.77</td>
</tr>
<tr>
<td>Mentok</td>
<td>93%</td>
<td>$1,132,425.64</td>
</tr>
<tr>
<td>Peter Potamus</td>
<td>96%</td>
<td>$999.93</td>
</tr>
<tr>
<td>Phil Ken Sebben</td>
<td>81%</td>
<td>$4,157.52</td>
</tr>
<tr>
<td>Ryu</td>
<td>91%</td>
<td>$10,786.92</td>
</tr>
<tr>
<td>Dr. Blake Downs</td>
<td>96%</td>
<td>$27,752.35</td>
</tr>
<tr>
<td>Brak</td>
<td>99%</td>
<td>$28,651.99</td>
</tr>
<tr>
<td>Space Ghost</td>
<td>100%</td>
<td>$1,554.53</td>
</tr>
<tr>
<td>Huey Freeman</td>
<td>90%</td>
<td>$8,602.14</td>
</tr>
<tr>
<td>Morty Smith</td>
<td>100%</td>
<td>$97.45</td>
</tr>
<tr>
<td>Rick Sanchez</td>
<td>92%</td>
<td>$8,992.38</td>
</tr>
<tr>
<td>Summer Smith</td>
<td>93%</td>
<td>$77,998.17</td>
</tr>
<tr>
<td>Mr. Meeseeks</td>
<td>84%</td>
<td>$7,436.16</td>
</tr>
<tr>
<td>Pickle Rick</td>
<td>91%</td>
<td>$9,659.12</td>
</tr>
<tr>
<td>MC Pee Pants</td>
<td>51%</td>
<td>$3,537.44</td>
</tr>
<tr>
<td>Peter Potamus</td>
<td>39%</td>
<td>$183,250.57</td>
</tr>
</tbody>
</table>
CLOUD SECURITY SCORECARDS

SharePoint

Antiope

CloudSploit

Exceptions on a per-resource basis

DynamoDB

Lambda

S3

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

https://github.com/turnerlabs/antiope

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
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
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

Security
“Happiness can be found, even in the darkest of times, if one only remembers to turn on the light.”

Albus Dumbledore
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