

Multi-Cloud Visibility for Large Organizations

Chris Farris

Public Cloud Security Lead, WarnerMedia

Who Am I?



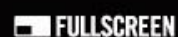
Cloud Security Lead at WarnerMedia

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





WARNERMEDIA



How it all started...

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



Internal Audit

- Audit Finding for access!
- Who should be attesting?
- What are all the accounts?
- How do we track privileges?




Give us all your external IP Addresses



State of Cloud Security

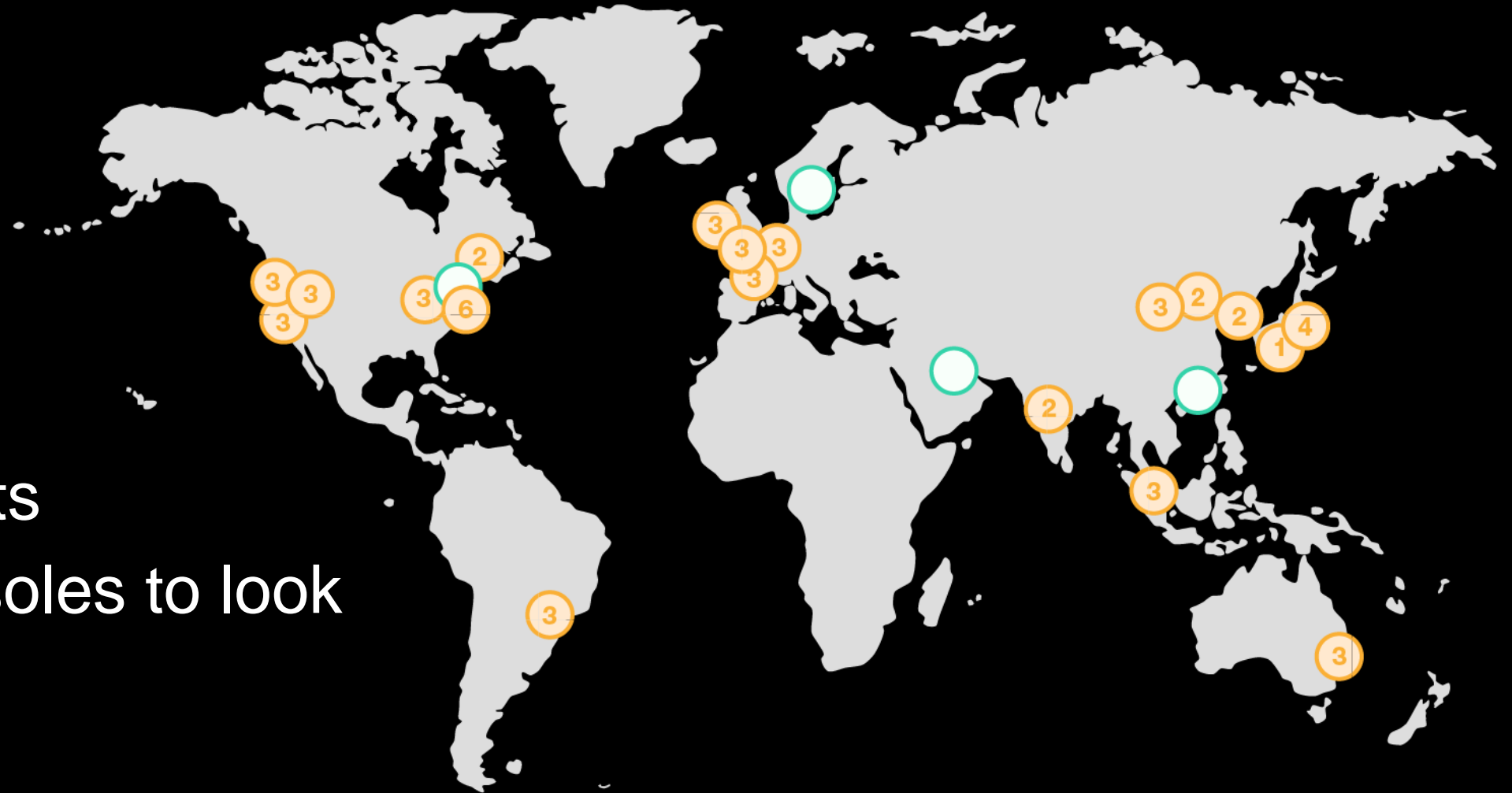


A close-up portrait of Petyr Baelish, a character from the TV series Game of Thrones. He is a man with dark hair and a mustache, wearing a dark, patterned tunic. He is looking slightly to the right with a subtle, enigmatic smile. The background is dark and out of focus.

*What we don't know is what
usually gets us killed.
-Petyr Baelish*

Game of Thrones (HBO)

Global Haystack



16 Regions

875 Accounts

14,000 consoles to look
in!

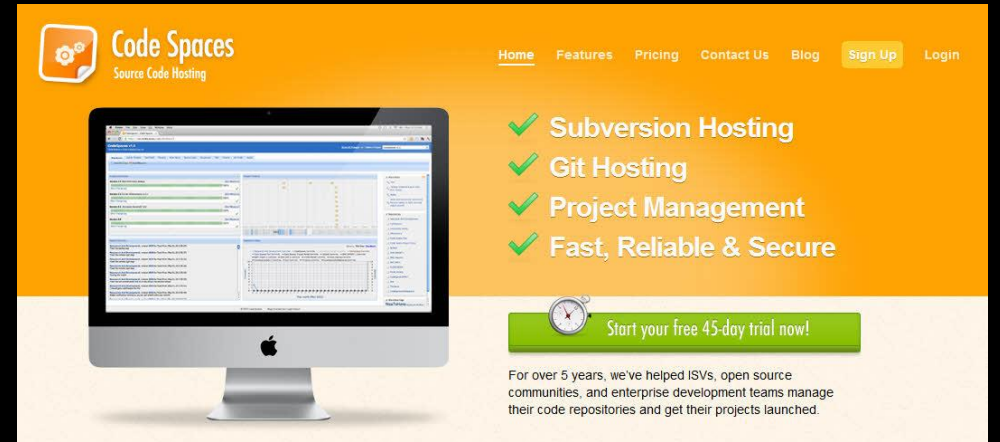


Multi-account Strategy



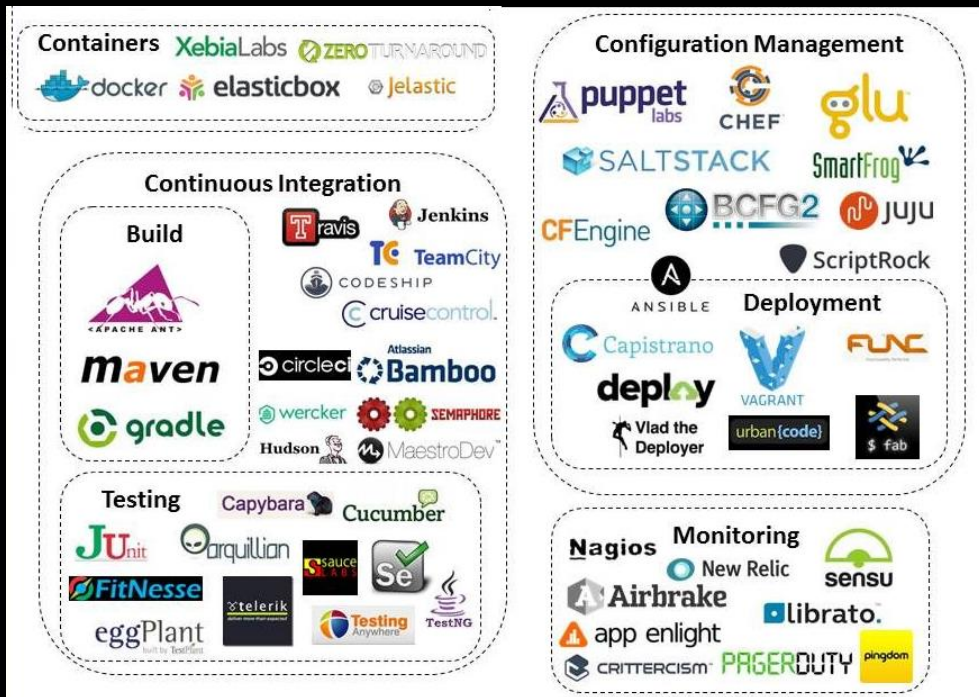
Why multi-account?

- Anyone remember them?
- Admin keys were leaked
- Account was ransomed
- Ransom wasn't paid
- Account deleted!



Tech Sprawl

- Tooling and architecture is a cultural thing
- Well – a multi-cultural thing



X



***Diversity in people is good,
Diversity in tech stacks, operations,
team culture, engineering process is
another story***

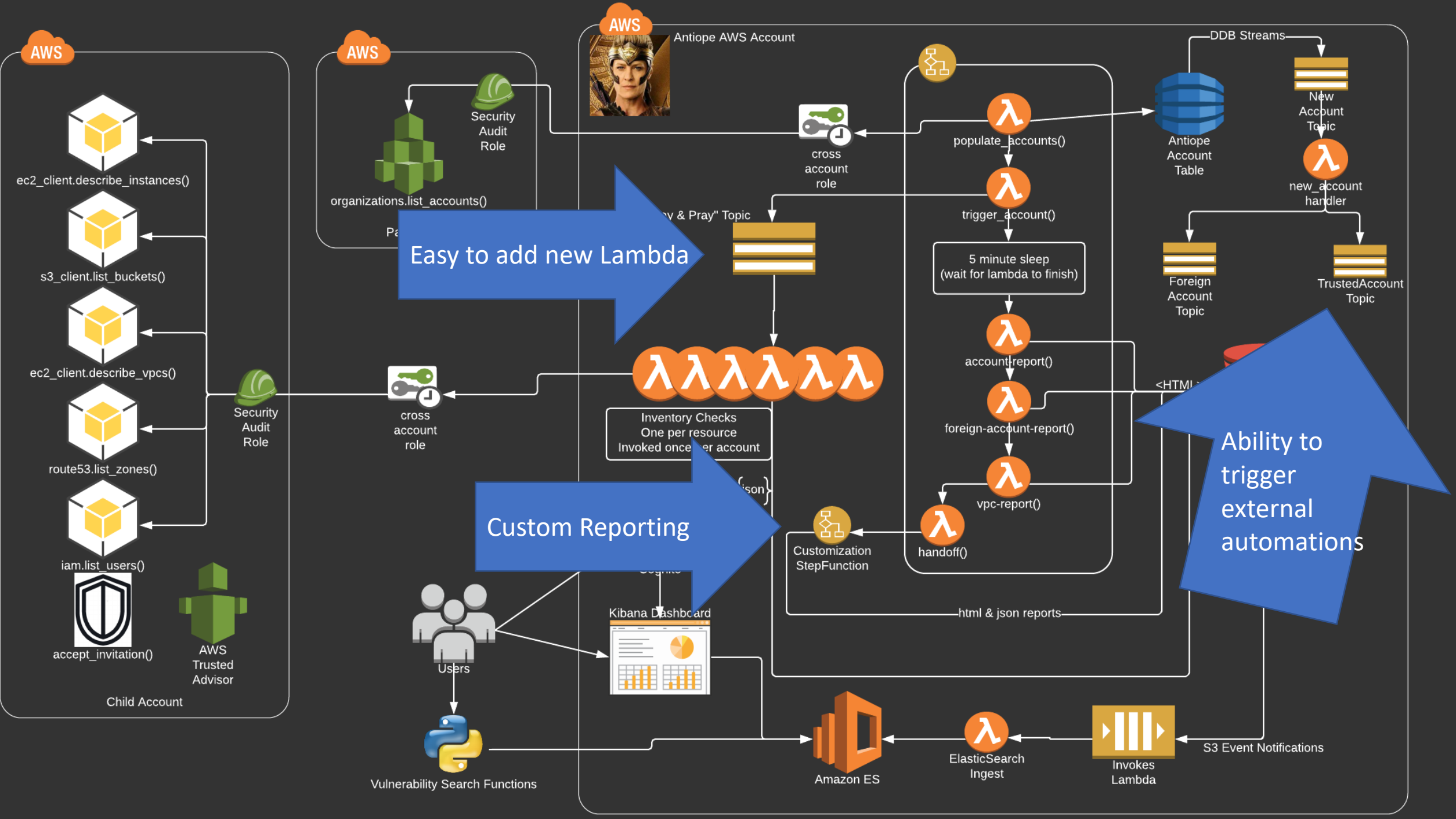
Antiope

<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 we use
- 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

Custom Stack

- Antiope was designed to be decoupled
- Add additional lambda to the Inventory SNS
- Add additional Stepfunction to run after
- Allows us to pull data from ServiceNow
- Generate custom reports
 - What EC2 don't have security agents?

Don't put lambda in all your accounts



Gremlins (Warner Bros. 1984)

[adult swim]

**SHOW ME
WHAT
YOU GOT!**

Account Management

*“Kids these days with their control towers and organizational admins. Back in my day we had to write lambda to enable GuardDuty and setup CloudTrail!
And we liked it!”*

- Auto Discovery of new accounts allowed us to auto-enroll accounts into security tooling

Centralized GuardDuty

- All GuardDuty fed to centralized account
- CloudWatch Events triggers a push to Splunk to Splunk HTTP Event Collector (HEC)
- Must be done in all regions

<https://github.com/turnerlabs/aws-guardduty-enterprise>

Distributed Centralized GuardDuty

- New AWS Organization Feature
- One account in the org now in control

Yeah, but I've got 8 payers

8 is better than 800

What We Did For Vulnerability Management

Inventory!

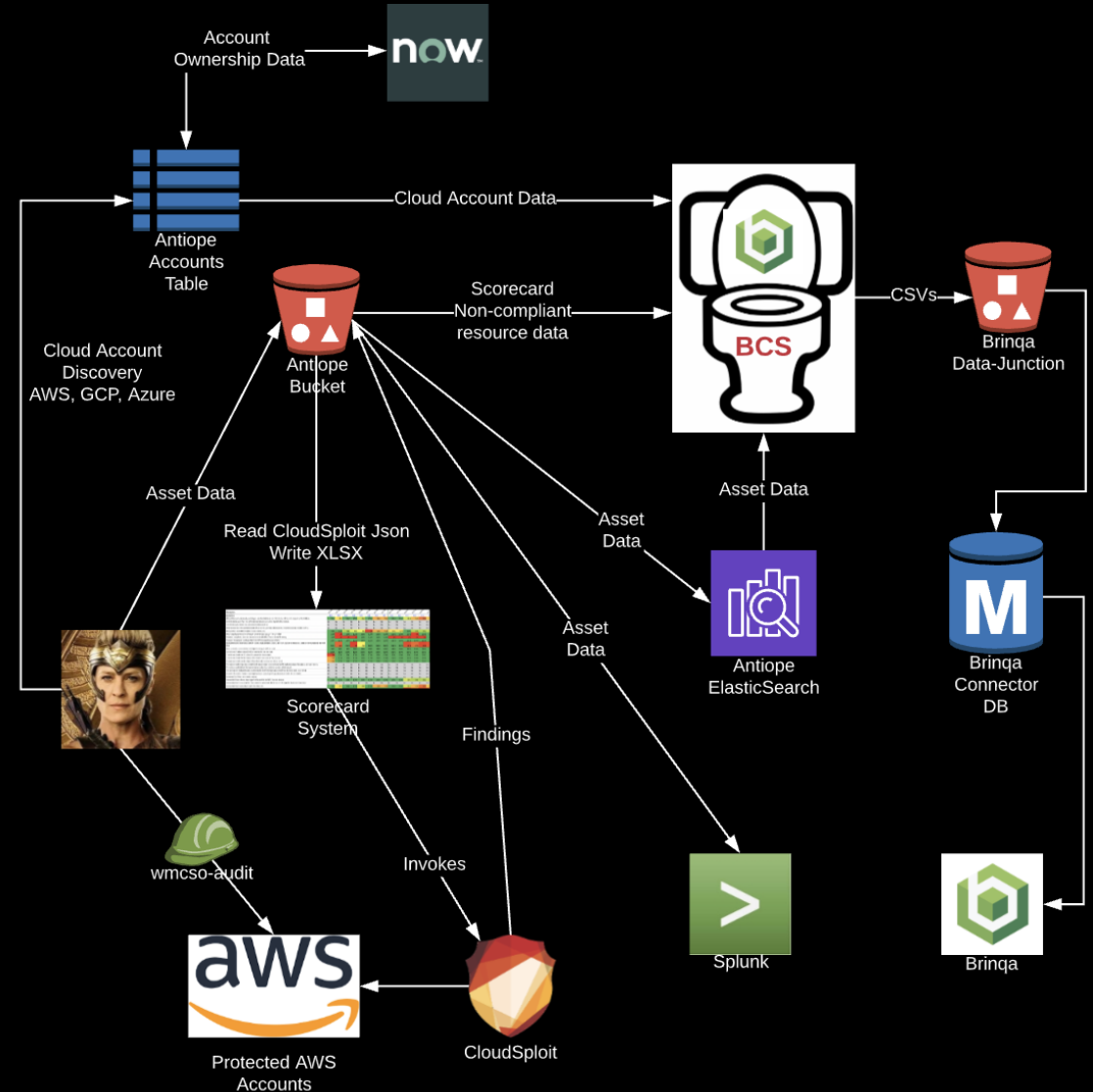
- Discovered attributes
 - Account ID
 - Payer
 - Root email
- Custom Attributes
 - Exec Sponsor
 - Data Classification
 - Service Now records

Aggregation point for all cloud data

```
{
  "account_id": "123456789012",
  "account_name": "aws-mordor",
  "account_status": "ACTIVE",
  "cross_account_role": "arn:aws:iam::123456789012:role/security-audit",
  "exec_sponsor": "Sauron",
  "exec_sponsor_email": "sauron@middleearth.com",
  "payer_id": "987654321023",
  "payer_name": "aws-t|plkien-payer",
  "payer_record": {
    "Arn": "arn:aws:organizations::987654321023:account/o-9cfdsfdv11/12345",
    "Email": "aws-mordor@middleearth.com",
    "Id": "123456789012",
    "JoinedMethod": "CREATED",
    "JoinedTimestamp": "2018-02-02T23:18:19.936000+00:00",
    "Name": "aws-mordor",
    "Payer Id": "987654321023",
    "Status": "ACTIVE"
  },
  "root_email": "aws-mordor@middleearth.com",
  "scorecard_recipients": [
    "frodo@shire.com",
    "Saruman@tower.com"
  ],
  "tech_contact": "Sauramon",
  "tech_sponsor_email": "Saruman@tower.com",
  "_snow_data": {
    "datacenter_discovery_status": "2020-05-16 17:43:17: Completed....Relo",
    "first_discovered": "2020-03-26 21:57:18",
    "last_discovered": "2020-05-16 19:08:54",
    "managed_by": "Saruman",
    "object_id": "123456789012",
    "owned_by": "Sauron",
    "short_description": "AWS account for jewelry forging. No Hobbits",
    "sys_class_name": "Cloud Service Account",
    "sys_created_on": "2020-03-26 21:57:18",
    "u_data_classification": "Internal Use Only"
  }
}
```

CloudSploit & Scorecards

- Antiope orchestrates data collection
- Fed to BCS system
- Populates VM tool Brinqa



Threat Detection & Response

Cross Account Role Page

- Name, ID and Owners
- Link to quickly assume cross-account role

AWS Account Inventory

Total Active Accounts: 840

Account Name	Account ID	Parent	Exec Sponsor	Tech Contact	Root Email	Assume Role Link
Rick's Café Américain	012345678901	Studio 17	Rick Blane	Victor Laszlo	cafe@wb.com	antiope-audit-role
Council of Ricks	987654321098	Westeros-payer	Rick Sanchez	Morty Smoth	mrmeeseeks@rick.com	antiope-audit-role
AWS - PiperChat	987654367890	aws-hooli-payer	Gavin Belson	Dinesh Chugtai	chat@piedpiper.io	antiope-audit-role
AWS - Nucleus	058307311343	aws-hooli-payer	Gavin Belson	Nelson Bighetti	nucleus@hooli.com	antiope-audit-role
Winterfell	641019619799	Westeros-payer	Sansa Stark	John Snow	ned@winterfell.thenorth	antiope-audit-role
aws-hooli-payer	293354143425	aws-hooli-payer	Gavin Belson	Gavin Belson	itbudgetmanagement@hooli.com	antiope-audit-role
aws-hogwarts	737694964105	aws-hogwarts	Albus Dumbledore	Argus Filch	billing@hogwarts.com	antiope-audit-role
aws-hufflepuff	877088135463	aws-hogwarts	Pomona Sprout	Gilderoy Lockhart	hufflepuff@hogwarts.com	antiope-audit-role
aws-slytherin	732307033544	aws-hogwarts	Severus Snape	Draco Malfoy	Slytherin@hogwarts.com	antiope-audit-role

Splunk & ElasticSearch

- Humans use Splunk
 - Threat Hunting
 - Investigations
- Lambda use ElasticSearch
 - Reporting
 - Data feeds to other systems

Threat Hunting

- What public ElasticSearch clusters exist in our environment?
- What security groups have 4505 or 4506 open?



Support Ticket Visibility

- All Support tickets are fed to the SOC to capture these

Dear AWS customer,

Your AWS Account is compromised! Please review the following notice and take immediate action to secure your account. We have also opened an outbound Support Case if you have any additional questions or concerns regarding this notice.

Your security is important to us. We have become aware that the AWS Access Key AKIAJXXXXXXXXXXXXHI (belonging to IAM user "XXXXXXXXXX@XXXXXXXXX.com") along with the corresponding Secret Key is publicly available online at

Engineering & Finance

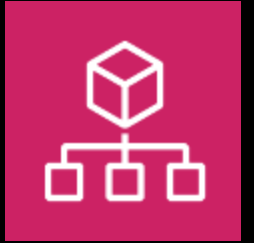
- “Hey what is this IP that keeps hitting our service?”
- Where is the DNS zone money.cnn.com hosted?
- How many EBS volumes or snapshots?
- Are the instances tagged properly?
- What Route53 domains have we registered?

Alternatives

“Architect for the AWS you have, not the AWS you want”

– Donald Rumsfeld 2003

AWS Organizations



- Multi-Account capabilities are getting better
- Delegated Admin & Trusted Access make this problem less hard

But nothing yet crosses AWS Org boundaries

AWS Config



- Antiope does much of what the AWS Config recorder does
- ... but without deploying config in 800 accounts and 16 regions
- ... and probably a bit cheaper too.
- AWS Config Multi-Account Multi-Region Aggregators are a good option

CloudMapper

- Scott Piper's tool
- Originally for visualizations
- Has a cross-account role deployment model

Build vs Buy

- Intimacy with Boto3 and all the features of a specific API call
- Get exactly what you need
- But...
 - you built it, now you own it.
- Fast to market!
- No hiring approvals!
- But...
 - Slave to product roadmaps
 - Perpetual annual licensing charges

Parting thoughts...

HHD

**YOU SAID
THE CLOUD
WAS SECURE!**



**IT IS
WHEN YOU
SECURE IT**

Future

- Azure support soon
 - Subscription & VM Discovery across multiple tenants
- Azure Perimeter Scanner
- Hunt Scripts

FOR THE CLOUD IS DARK

AND FULL OF TERRORS

Game of Thrones (HBO)



The Dark Knight (Warner Bros. 2008)



@jcfarris



<https://github.com/jchrisfarris>



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



<http://www.chrisfarris.com>



<https://github.com/turnerlabs/antiope>