



BISHOPFOX

EXPOSE YOURSELF
WITHOUT INSECURITY

BSIDES ATLANTA 2020



INTRO

DO YOU KNOW YOUR EXPOSURE?

QUESTION

HOW DO YOU DETERMINE
WHAT IS EXPOSED TO THE
INTERNET IN YOUR
CLOUD ENVIRONMENT?

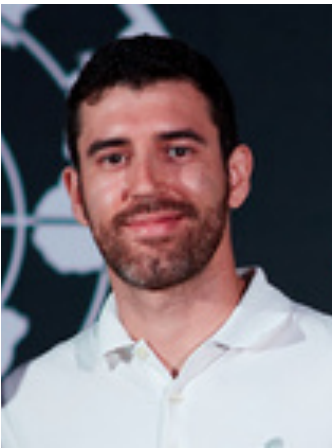
WHO ARE WE?

INTRO



BRANDON GAUDET

Senior Security Analyst



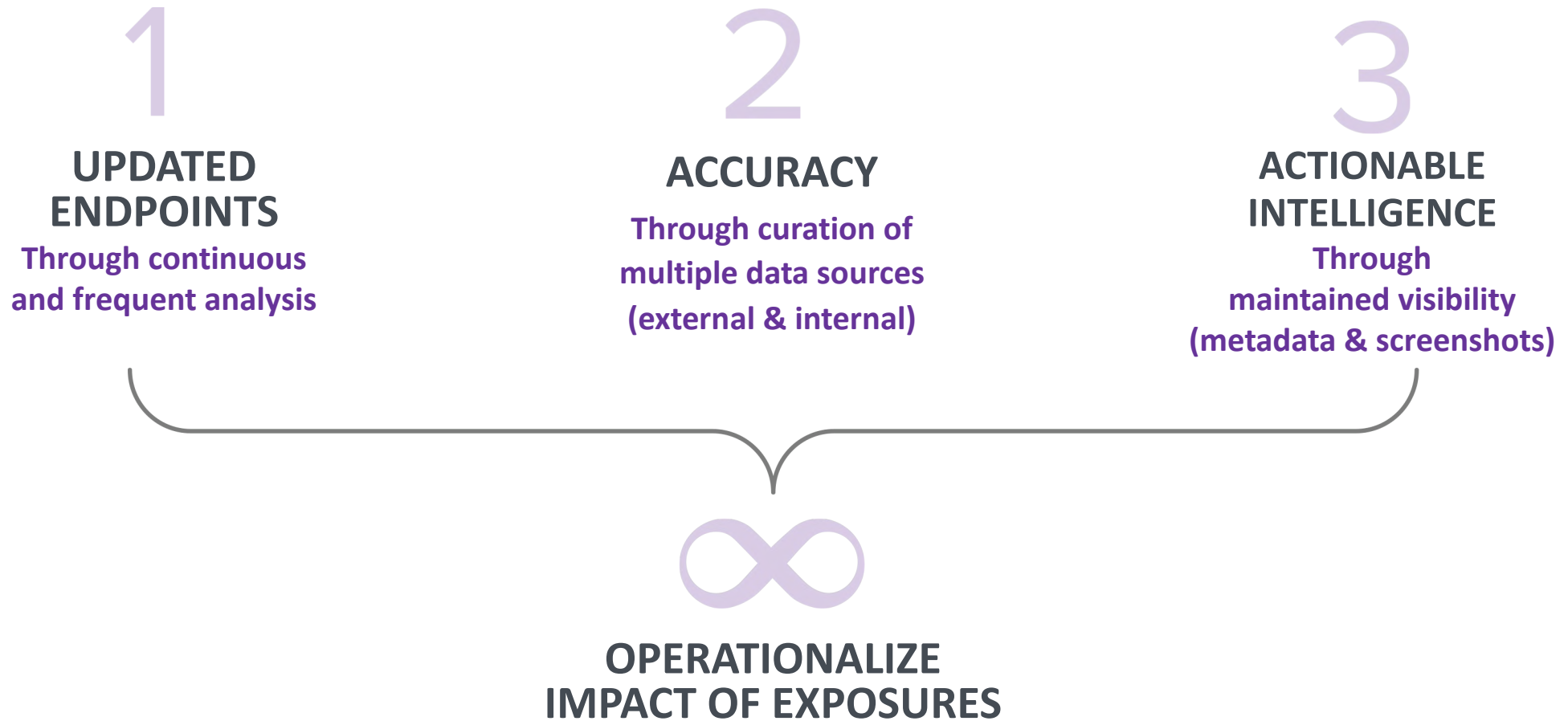
OSCAR SALAZAR

Principal Researcher

- Focused on Continuous Attack Surface Testing (CAST)
 - Techniques
 - Procedures
 - Tools
- Continuously learning new techniques for offensive testing

INVENTORY SUCCESS CRITERIA

What do we want from our asset inventory? (i.e. Targets):



BUILDING A BASELINE



- Organization Structure
- Business Units
- Products
- Services
- Mergers & Acquisitions



- Primary Domains
- Subdomains
- IP Address Space
- Active Services
- ASNs



- Continuously updated dataset of DNS and IP based Targets

MORE SUCCESSFUL APPROACH

- » Master records are your advantage as defenders
- » Emulate real-attackers but where possible, be several steps ahead of them
- » Our goal is to inventory the entire attack surface, we should utilize all the things:
 - Domain registrars
 - DNS records
 - Certificate Authorities
 - BGP Prefix
 - Internet Scan Archives
 - Cloud account metadata
 - ...and anything and everything attackers and your internal IT uses



02 METHODOLOGY

USING DIFFERENT LENSES
INSIDE LOOKING OUT
OUTSIDE LOOKING IN



USING DIFFERENT LENSES

INSIDE LOOKING OUT (IT/ENG Configurations)

- When and where possible, always leverage the master records
- Go to the source of truth
- Someone at your organization has to setup and maintain a configuration for each asset and systematically there is evidence of this system in your master DNS records and router tables (e.g. DHCP)

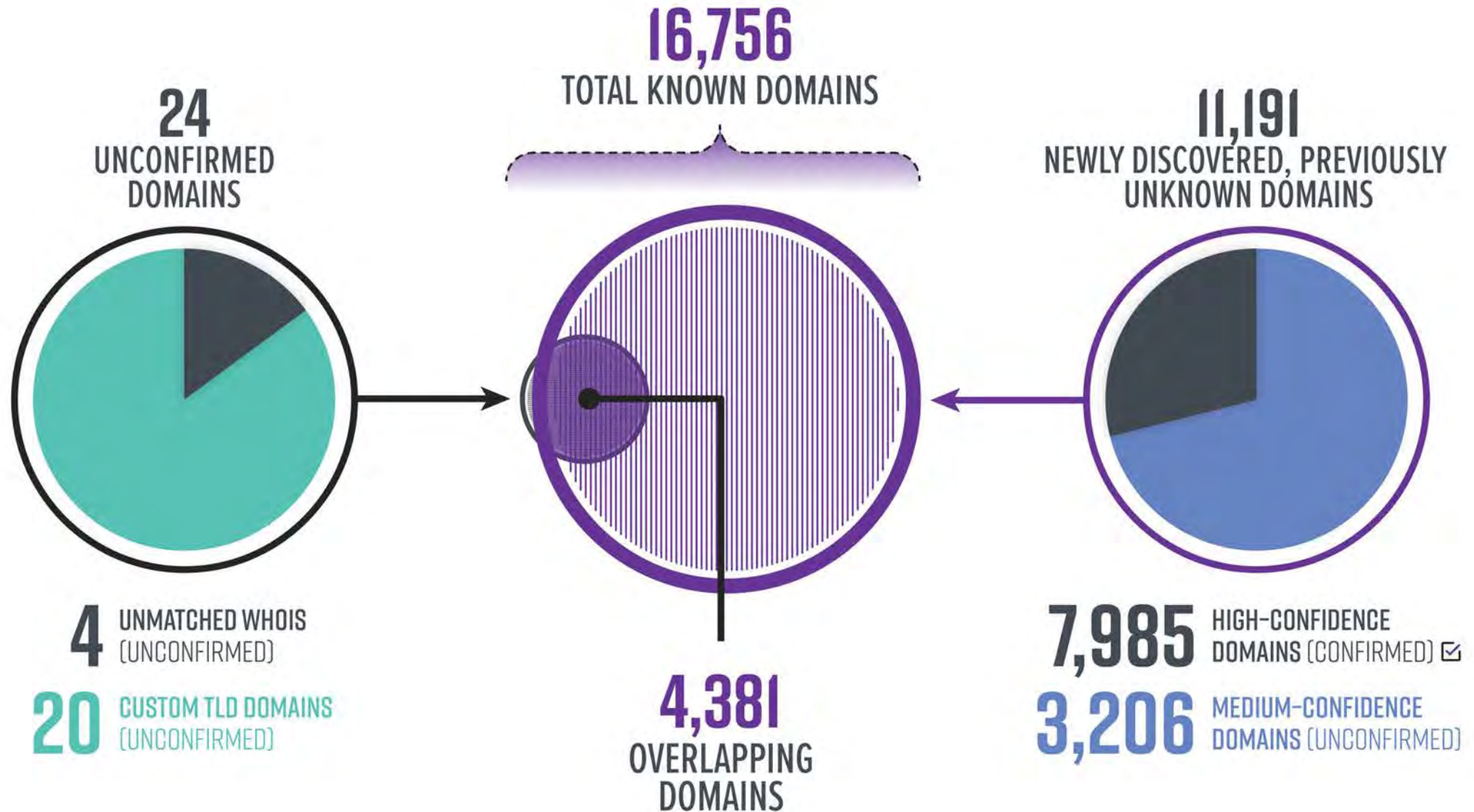


OUTSIDE LOOKING IN (OSINT)

- Shadow IT will always exist
- Use techniques from outside your environment to see what the rest of the world can see
- Attackers scan the internet, they monitor for changes to internet infrastructure, and can mine massive datasets using OSINT to find what they're looking for, i.e. a weakness
- Adopt similar approaches. whois data, registrar data, reverse DNS



ATTACK SURFACE MAPPING



HOW DO YOU IDENTIFY CLOUD ACCOUNTS

- » Follow the money \$\$\$
- » Partner with finance to monitor corporate credit card usage
- » Whose corporate credit card is accruing charges from AWS, Azure, GCP, etc? this is your best lead to identify unknown accounts.
- » Establish review process and track security team visibility into these accounts
- » **BEWARE** of IaaS/PaaS/SaaS that mask popular providers (e.g. refinery.io) and hide inventory

\$736.43 paid on December 3, 2019

Thanks for using Refinery, we appreciate your business! Please email billing@refinerylabs.io with any questions or issues regarding this invoice.

Description	Qty	Unit price	Amount
Managed API Gateway	1	\$1.13	\$1.13
Managed Athena	1	\$0.02	\$0.02
Managed Lambda	1	\$687.48	\$687.48
Managed Simple Notification Service	1	\$0.02	\$0.02
Managed Simple Queue Service	1	\$2.62	\$2.62
Managed CloudWatch	1	\$4.82	\$4.82
Managed CodeBuild	1	\$0.06	\$0.06
Managed Simple Storage Service	1	\$40.28	\$40.28

WHY NOT ADD ONE MORE AWS ACCOUNT?

- » Security team should have an account
- » One account to read them all from a monitoring perspective
- » Establish a parent org account with engineering

Assume role access or Security Auditor read-only access to all other accounts identified at the organization

ONE

**AWS ACCOUNT
TO RULE THEM ALL**

ACCOUNT ACCESS ESTABLISHED*

- Which accounts have publicly facing systems and services?
- How are those specific services externally accessible? (DNS/IP/Port)
- Access Levels:
 - Internal
 - AWS Resource Relationships (IAM Access Analyzer helps here)
 - Internet

* Assuming you identified all accounts established a program and a policy to detect future accounts and have executed access controls properly.

OPERATIONALIZING DATA

» Publicly available services should have:

- Scheme/Protocol
- Host (DNS or IP)
- Port
- URI (relative path)
- Anonymous internet-facing access



» Internet scale scanners will find these services

- May not route correctly for AWS services and error without DNS/VHOST info



03

STATE OF THE ART

AVAILABLE TOOLS & TECHNIQUES

AWS IN 2011

WHAT SERVICES DO WE NEED TO CONSIDER?

Compute

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic MapReduce

Auto Scaling

Content Delivery

Amazon CloudFront

Database

Amazon SimpleDB

Amazon Relational Database (RDS)

E-Commerce

Amazon Fulfillment Web

Messaging

Amazon Simple Queue Service (SQS)

Amazon Simple Notification Service (SNS)

Monitoring

Amazon CloudWatch

Networking

Amazon Virtual Private Cloud
Elastic Load Balancing

Payments & Billing

Amazon Flexible Payments Service (FPS)

Amazon DevPay

Storage

Amazon Simple Storage Service (S3)

Amazon Elastic Block Storage (EBS)

AWS Import/Export

Support

AWS Premium Support

Web Traffic

Alexa Web Information Service

Alexa Top Sites

Workforce

Amazon Mechanical Turk

AWS IN 2017

WHAT SERVICES DO WE NEED TO CONSIDER?

Compute

Amazon EC2
Amazon Elastic Container Service
Amazon Elastic Container Service for Kubernetes
Amazon Elastic Container Registry
Amazon Lightsail
AWS Batch
AWS Elastic Beanstalk
AWS Fargate
AWS Lambda
AWS Serverless Application Repository
Auto Scaling
Elastic Load Balancing
VMware Cloud on AWS

Storage

Amazon Simple Storage Service (S3)
Amazon Elastic Block Storage (EBS)
Amazon Elastic File System (EFS)
Amazon Glacier
AWS Storage Gateway
AWS Snowball
AWS Snowball Edge
AWS Snowmobile

Database

Amazon Aurora
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon Redshift
Amazon Neptune
AWS Database Migration Service

Migration

AWS Migration Hub
AWS Application Discovery Service
AWS Database Migration Service
AWS Server Migration Service

Networking & Content Delivery

Amazon VPC
Amazon CloudFront
Amazon Route 53
Amazon API Gateway
AWS Direct Connect
Elastic Load Balancing

Developer Tools

AWS CodeStar
AWS CodeCommit
AWS CodeBuild
AWS CodeDeploy
AWS CodePipeline
AWS Cloud9
AWS X-Ray
AWS Tools & SDKs

Management Tools

Amazon CloudWatch
AWS CloudFormation
AWS CloudTrail
AWS Config
AWS OpsWorks
AWS Service Catalog
AWS Systems Manager
AWS Trusted Advisor
AWS Personal Health Dashboard
AWS Command Line Interface
AWS Management Console
AWS Managed Services

Media Services

Amazon Elastic Transcoder
Amazon Kinesis Video Streams
AWS Elemental MediaConvert
AWS Elemental MediaLive
AWS Elemental MediaPackage
AWS Elemental MediaStore

Machine Learning

Amazon SageMaker
Amazon Comprehend
Amazon Lex
Amazon Polly
Amazon Rekognition
Amazon Machine Learning
Amazon Translate
Amazon Transcribe
AWS DeepLens
AWS Deep Learning AMIs
Apache MXNet on AWS
TensorFlow on AWS

Analytics

Amazon Athena
Amazon EMR
Amazon CloudSearch
Amazon Elasticsearch Service
Amazon Kinesis
Amazon Redshift
Amazon QuickSight
AWS Data Pipeline
AWS Glue

Security, Identity & Compliance

AWS Identity and Access Management (IAM)
Amazon Cloud Directory
Amazon Cognito
Amazon GuardDuty
Amazon Inspector
Amazon Macie
AWS Certificate Manager
AWS CloudHSM
AWS Directory Service
AWS Key Management Service
AWS Organizations
AWS Single Sign-On

AR & VR

Amazon Sumerian

Application Integration

Amazon MQ
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
AWS AppSync
AWS Step Functions

Customer Engagement

Amazon Connect
Amazon Pinpoint
Amazon Simple Email Service (SES)

Business Productivity

Alexa for Business
Amazon Chime
Amazon WorkDocs
Amazon WorkMail

Desktop & App Streaming

Amazon WorkSpaces
Amazon AppStream 2.0

Internet of Things

AWS IoT Core
Amazon FreeRTOS
AWS Greengrass
AWS IoT 1-Click
AWS IoT Analytics
AWS IoT Button
AWS IoT Device Defender
AWS IoT Device Management

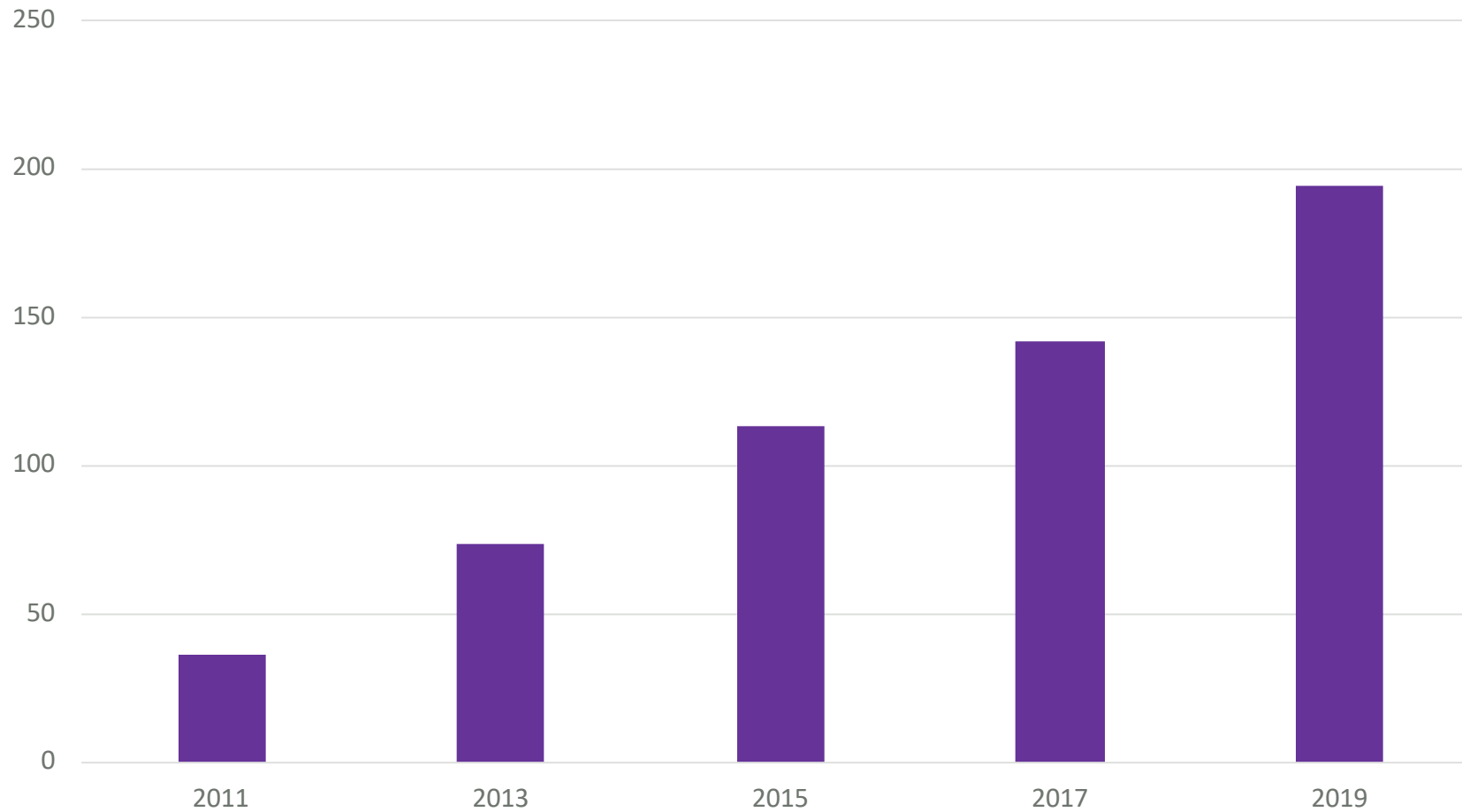
Game Development

Amazon GameLift
Amazon Lumberyard

Software

EXPONENTIAL
PACE OF INNOVATION

AWS Features & Services



AWS IN 2020

WHAT SERVICES DO WE NEED TO CONSIDER?

TOO MANY TO LIST!



EXPOSED SERVICES: STATE OF THE ART

What was already available when we tried to solve this problem?

- **Cloudmapper**
 - https://summitroute.com/blog/2018/06/13/cloudmapper_public/
 - <https://github.com/duo-labs/cloudmapper>
- **AWS Public IPs**
 - https://github.com/arkadiyt/aws_public_ips
- **IAM Access Analyzer** (codename Tيروس released at Re:Invent 2019)
 - July 2019 <https://aws.amazon.com/blogs/security/aws-security-profile-john-backes-senior-software-development-engineer/>
 - <https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html>
 - https://d1.awsstatic.com/whitepapers/Security/Reachability_Analysis_for_AWS-based_Networks.pdf
- **Cartography**
 - <https://github.com/lyft/cartography>

LIMITATION OF AVAILABLE TOOLS

EXPOSED SERVICES: STATE OF THE ART

	CLOUDMAPPER	AWS PUBLIC IPS	IAM ACCESS ANALYZER	CARTOGRAPHY
PUBLICLY ACCESSIBLE INFRASTRUCTURE ASSETS	Yes	No	No	Yes
IP ADDRESSES	Yes, but IPv6 not supported	IPv4 – IPv6 Classic / VPC networking	No	No
PORTS	TCP, UDP	No	No	Yes
PROTOCOLS	No	No	No	Yes
NETWORK ACL RULES	No	No	No	Yes
AWS SERVICES COVERED	EC2 – ELBs – RDS	EC2 - ELBs - RDS - RDC APIGateway, CloudFront, ElasticSearch, Lightsail Redshift	S3 IAM roles	EC2 - ELBs - S3 ElasticSearch
COMPREHENSIVE	No	No	No	No



04 OUR FIRST PASS

Identify Common Patterns

AWS EXPOSURE ENDPOINTS

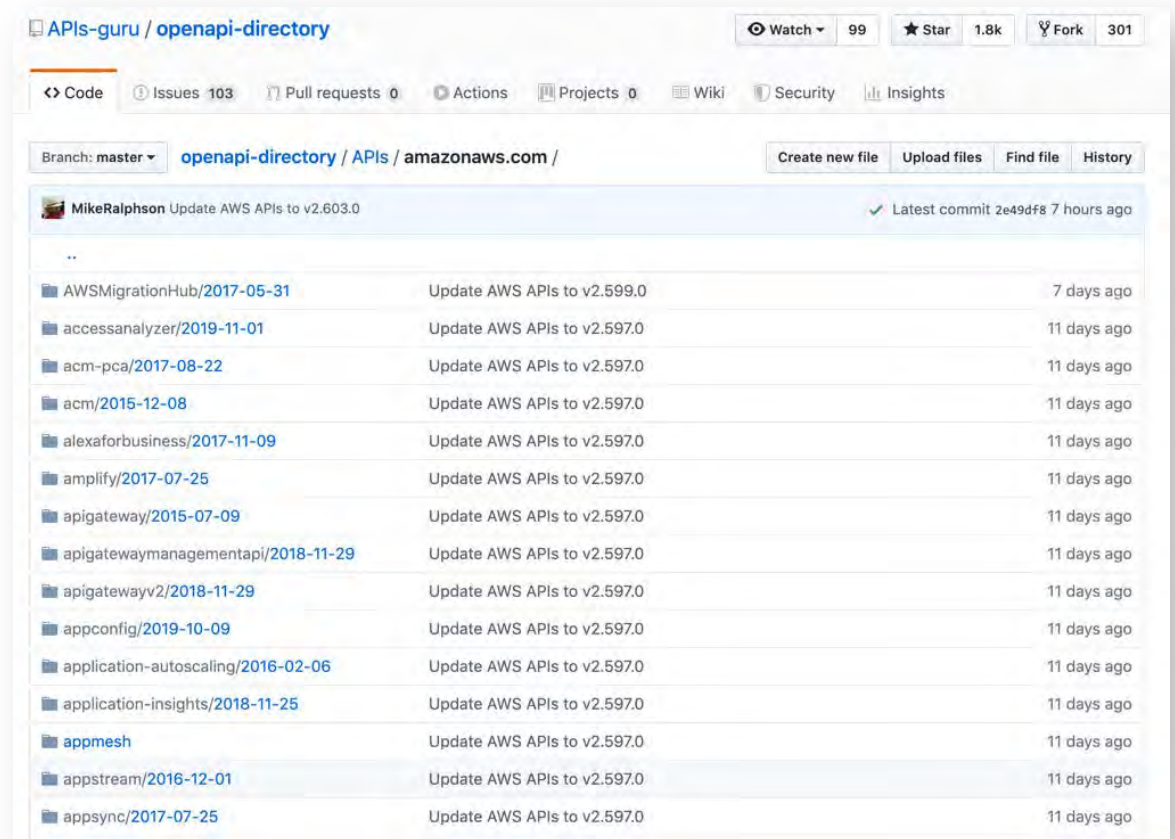
➤ APIs-Guru OpenAPI Directory

🌐 Wikipedia for Web APIs. Directory of REST API definitions in OpenAPI 2.0/3.0 format

➤ Identified patterns in AWS Service DNS records from documentation

<https://github.com/APIs-guru/openapi-directory/tree/master/APIs/amazonaws.com>

➤ Cross referenced with passive DNS data to understand real-world usage



AWS EXPOSURE PATTERNS

Beware of misconfigurations that expose your content with these CNAME patterns:

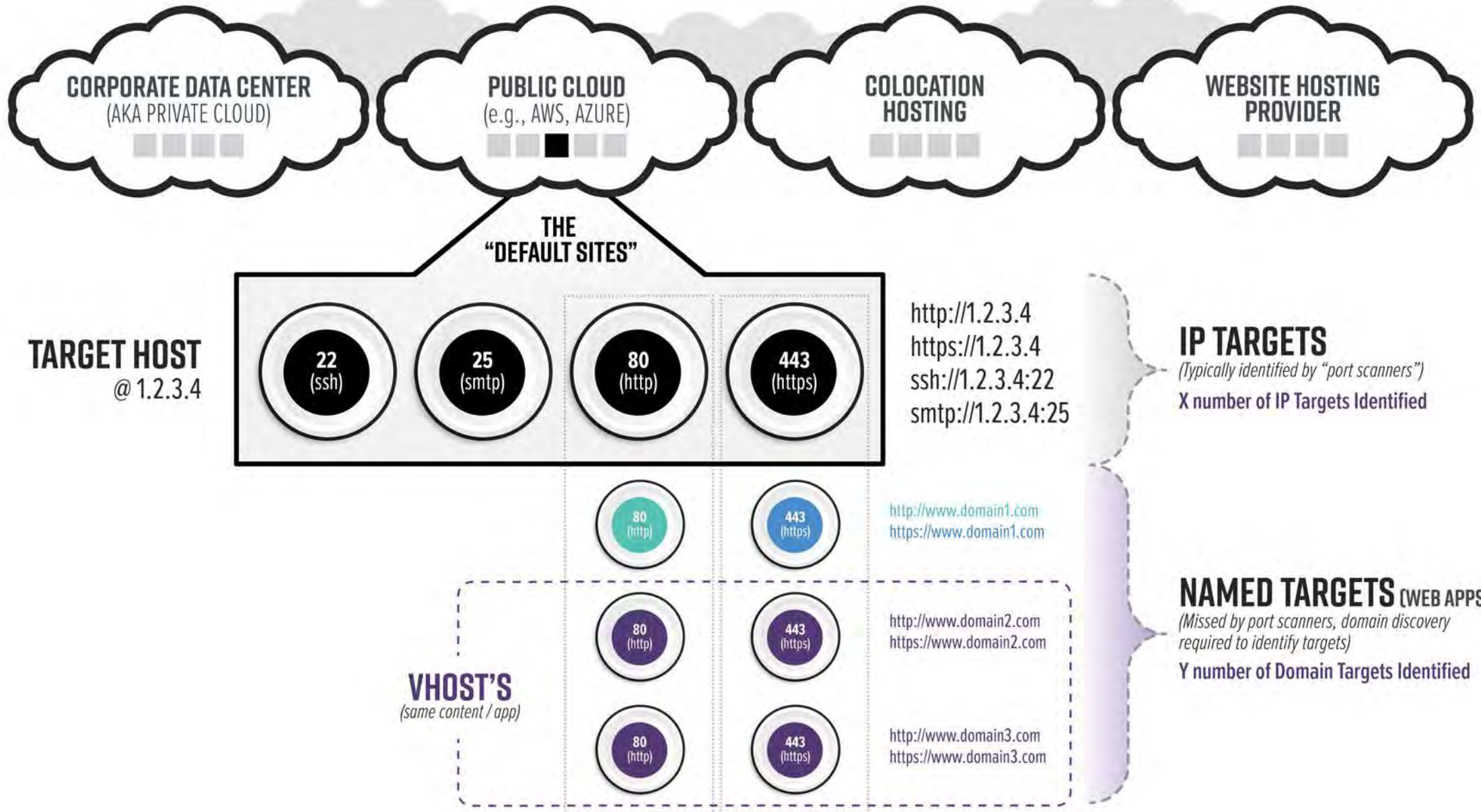
s3	https://{user_provided}.s3.amazonaws.com
cloudfront	https://{random_id}.cloudfront.net
ec2	ec2-{ip-seperated}.compute-1.amazonaws.com
es	https://{user_provided}-{random_id}.{region}.es.amazonaws.com
elb	http://{user_provided}-{random_id}.{region}.elb.amazonaws.com:80 https://{user_provided}-{random_id}.{region}.elb.amazonaws.com:443
elbv2	https://{user_provided}-{random_id}.{region}.elb.amazonaws.com
rds	mysql://{user_provided}.{random_id}.{region}.rds.amazonaws.com:3306 postgres://{user_provided}.{random_id}.{region}.rds.amazonaws.com:5432
route53	{user-specified}

AWS EXPOSURE PATTERNS

Beware of misconfigurations that expose your content with these CNAME patterns:

execute-api	<code>https://{random_id}.execute-api.{region}.amazonaws.com/{user_provided}</code>
cloudsearch	<code>https://doc-{user_provided}-{random_id}.{region}.cloudsearch.amazonaws.com</code>
transfer	<code>sftp://s-{random_id}.server.transfer.{region}.amazonaws.com</code>
iot	<code>mqtt://{random_id}.iot.{region}.amazonaws.com:8883</code> <code>https://{random_id}.iot.{region}.amazonaws.com:8443</code> <code>https://{random_id}.iot.{region}.amazonaws.com:443</code>
mq	<code>https://b-{random_id}-{1,2}.mq.{region}.amazonaws.com:8162</code> <code>ssl://b-{random_id}-{1,2}.mq.{region}.amazonaws.com:61617</code>
kafka	<code>b-{1,2,3,4}.{user_provided}.{random_id}.c{1,2}.kafka.{region}.amazonaws.com</code> <code>{user_provided}.{random_id}.c{1,2}.kafka.useast-1.amazonaws.com</code>
cloud9	<code>https://{random_id}.vfs.cloud9.{region}.amazonaws.com</code>
mediastore	<code>https://{random_id}.data.mediastore.{region}.amazonaws.com.</code>
kinesisvideo	<code>https://{random_id}.kinesisvideo.{region}.amazonaws.com</code>
mediaconvert	<code>https://{random_id}.mediaconvert.{region}.amazonaws.com</code>
mediapackage	<code>https://{random_id}.mediapackage.{region}.amazonaws.com/in/v1/{random_id}/channel</code>

DOMAINS > IP ADDRESSES



AWS ELASTICSEARCH EXPOSED INDICES

- Found 59 exposed instances
- Found 1706 multi-MB exposed indices

```

search-its-6tvhicb [REDACTED] gw7mm5q.us-east-1.es.amazonaws.com/_cat/indices?v

```

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
yellow	open	integration-transaction-20200109	7_qb9G25SPK77M0-_rL9sg	1	1	1053	0	176.7kb	176.7kb
yellow	open	integration-transaction-20191218	bdmKhZBrTLuLGzDiM3cHVA	1	1	9634	0	1.5mb	1.5mb
yellow	open	integration-transaction-20191222	Di2V3WSpS66Rd5u0EdEQOA	1	1	1050	0	182kb	182kb
yellow	open	integration-transaction-20191220	p3RWuTQWQKiC9nTuMjVXGg	1	1	1100	0	187.1kb	187.1kb
green	open	.kibana_1	4FtBQQqBQb6MdJB6oTc4ZA	1	0	3	0	15.8kb	15.8kb
yellow	open	integration-transaction-20200111	MghJmMK4Q_6iG9EiBJy-MQ	1	1	1054	0	168.5kb	168.5kb
yellow	open	integration-transaction-20191225	SzdRPkfWRmSvsmTWHFRMMA	1	1	1045	0	175.7kb	175.7kb
yellow	open	integration-transaction-20200115	IS5x98QPQJOuyW6bUxOymA	1	1	1051	0	176.5kb	176.5kb
yellow	open	integration-transaction-20191223	btGRIumsRpyCmZLlI0LVJw	1	1	1046	0	167.4kb	167.4kb
yellow	open	integration-message-20191218	3O5RAt9UTs-oOqSKpGDwLA	1	1	45	0	50.7kb	50.7kb
yellow	open	integration-transaction-20200101	qXu38NtJSok5xn-UZHsdjw	1	1	1048	0	164.7kb	164.7kb
yellow	open	integration-transaction-20200106	bxP_U5dySPeBaSDulsEEERQ	1	1	1056	0	166.1kb	166.1kb
yellow	open	integration-transaction-20200104	wrAAij5FQuGRkR02sk9Ztg	1	1	1057	0	183kb	183kb
yellow	open	integration-transaction-20200107	9Ndw7n0UT8K59dUjvzhyRw	1	1	1048	0	161.9kb	161.9kb
yellow	open	integration-transaction-20191230	u3WJghfcTGS5hYpnCrsqNg	1	1	1051	0	162.4kb	162.4kb
yellow	open	integration-message-20200113	RrdxS6rRj-ibW_q-7qPIA	1	1	3	0	21.5kb	21.5kb

```

> GET /_cat/indices?v HTTP/1.1
> Host: search-nw-public-uo66a [REDACTED] i27qx2pqbwblky.us-east-1.es.amazonaws.com
> User-Agent: Mozilla/5.0 (compatible; meg/0.2; +https://github.com/tomnomnom/meg)

```

```

< HTTP/1.1 200 OK
< Access-Control-Allow-Origin: *
< Content-Type: text/plain; charset=UTF-8
< Content-Length: 1130

```

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size
yellow	open	rus_voter_rec	M2G5eFJATU2AF8iXUNicuA	5	1	53793	0	39.3mb
green	open	.kibana	PtAmgYIjRYaU_mZUjTTRg	1	0	7	0	40.1kb
yellow	open	admin	0rjQz60JS0ihg-rv23eX4g	5	1	2	0	8.9kb
yellow	open	events2016	vXJ5FSzzQ5SyQq-K5HWe0g	5	1	136000	0	87.5mb
yellow	open	data_catalog_test	x4i-ywKURiuYDx2ja7LIFw	5	1	48	0	112.7kb
yellow	open	test	8GLpSf7PQaeSHGbkDYq3eA	5	1	51	0	115.3kb
yellow	open	data_catalog	ZgzicZp4Qv6lwEuNR0J1wQ	5	1	51	0	110.9kb
yellow	open	events2018	tJUUsdiHoSya0CKfov-JzxQ	5	1	6325000	0	3.8gb
yellow	open	events2017	WduAnZZqSP0cUM9u7J81cg	5	1	137000	0	88.3mb

```

https://search-fittingroom-g [REDACTED] big5ztfwmyzsj5xnm.eu-west-1.es.amazonaws.com/_cat/indices?v

```

Note: This was a sample of us-east-1 and not comprehensive analysis of exposures across all regions

AWS ELASTICSEARCH EXPOSED INDICES

- Found 59 exposed instances
- Found 1706 multi-MB exposed indices
- IPv4 scanners cannot find this

```
/tmp dig search-its-6tvhicibj [REDACTED] lqogw7mm5q.us-east-1.es.amazonaws.com
; <<>> DiG 9.10.6 <<>> search-its-6tvhicibj [REDACTED] lqogw7mm5q.us-east-1.es.amazonaws.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46484
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;search-its-6tvhicibj [REDACTED] lqogw7mm5q.us-east-1.es.amazonaws.com. IN A

;; ANSWER SECTION:
search-its-6tvhicibj [REDACTED] lqogw7mm5q.us-east-1.es.amazonaws.com. 60 IN A 52.1.68.147
search-its-6tvhicibj [REDACTED] lqogw7mm5q.us-east-1.es.amazonaws.com. 60 IN A 3.223.42.5

;; Query time: 75 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Thu Jan 16 15:55:22 EST 2020
;; MSG SIZE rcvd: 125
```

← → ↻ ⚠ Not Secure | 52.1.68.147/_cat/indices?v

User is not authorized to perform this action

Note: This was a sample of us-east-1 and not comprehensive analysis of exposures across all regions

AWS MEDIASTORE SAMSUNG TV PLUS

- Found Samsung TV Plus streams
 - Samsung TV Plus delivers free TV. Get instant access to news, sports, entertainment, and more. No download, additional device, or credit card needed.

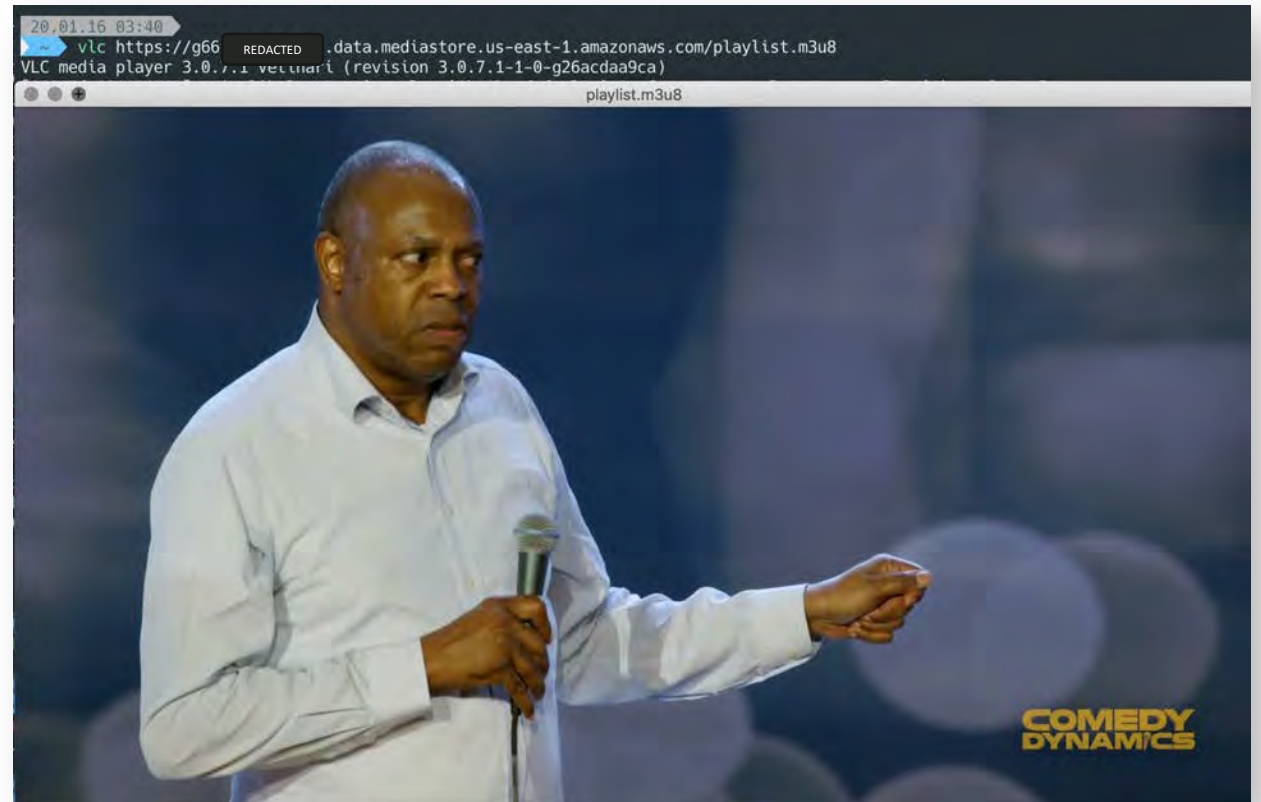
The screenshot displays the 'US Channel Lineup' for Samsung TV Plus. It is organized into three main categories: News, Sports & Outdoors, and Entertainment. Each channel is represented by a circular logo, its name, and its channel number.

Category	Channel Name	Channel Number
News	CBSN	1005
	Newsy	1020
	cheddar	1022
	Law & Crime	1024
	TYT Network	1032
	WeatherNation	1034
Sports & Outdoors	fubo Sports Network	1058
	Stadium	1059
	ACC Digital Network	1060
	Outside TV+	1061
	Insight TV	1063

Note: Samsung TV Plus is only available on 2016 - 2019 Samsung Smart TV's in select territories and an internet connection is required.

AWS MEDIASTORE SAMSUNG TV PLUS

- Found Samsung TV Plus streams
 - Samsung TV Plus delivers free TV. Get instant access to news, sports, entertainment, and more. No download, additional device, or credit card needed.
- IPv4 scanners cannot find this



Note: Samsung TV Plus is only available on 2016 - 2019 Samsung Smart TV's in select territories and an internet connection is required.



05 OUR SOLUTION

YET ANOTHER TOOL

Introducing **Smog** Identifying The **Cloud** That No One Wants

<https://github.com/BishopFox/smogcloud>

Smog Cloud

Find cloud assets that no one wants exposed

AWS Patterns

These are the patterns of exposure URIs that you may find in your AWS accounts

- s3
 - `https://{user_provided}.s3.amazonaws.com`
- cloudfront
 - `https://{random_id}.cloudfront.net`
- ec2
 - `ec2-{ip-seperated}.compute-1.amazonaws.com`
- es
 - `https://{user_provided}-{random_id}.{region}.es.amazonaws.com`
- elb
 - `http://{user_provided}-{random_id}.{region}.elb.amazonaws.com:80`
 - `https://{user_provided}-{random_id}.{region}.elb.amazonaws.com:443`
- elbv2
 - `https://{user_provided}-{random_id}.{region}.elb.amazonaws.com`
- rds
 - `mysql://{user_provided}.{random_id}.{region}.rds.amazonaws.com:3306`
 - `postgres://{user_provided}.{random_id}.{region}.rds.amazonaws.com:5432`

AWS EXPOSURE ENDPOINTS

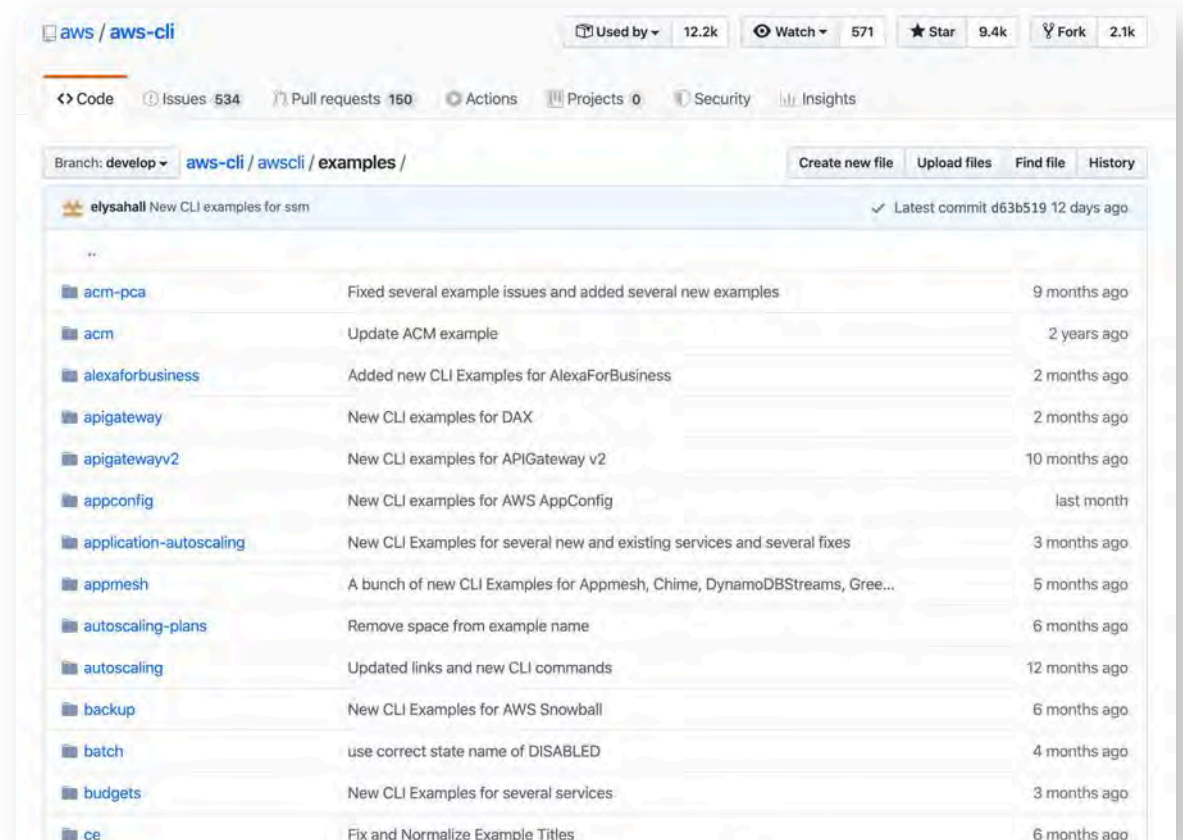
» Identified patterns in aws-cli example documentation

<https://github.com/aws/aws-cli/tree/develop/awscli/examples>

» Cross referenced identified patterns with aws-cli commands data to identify access patterns

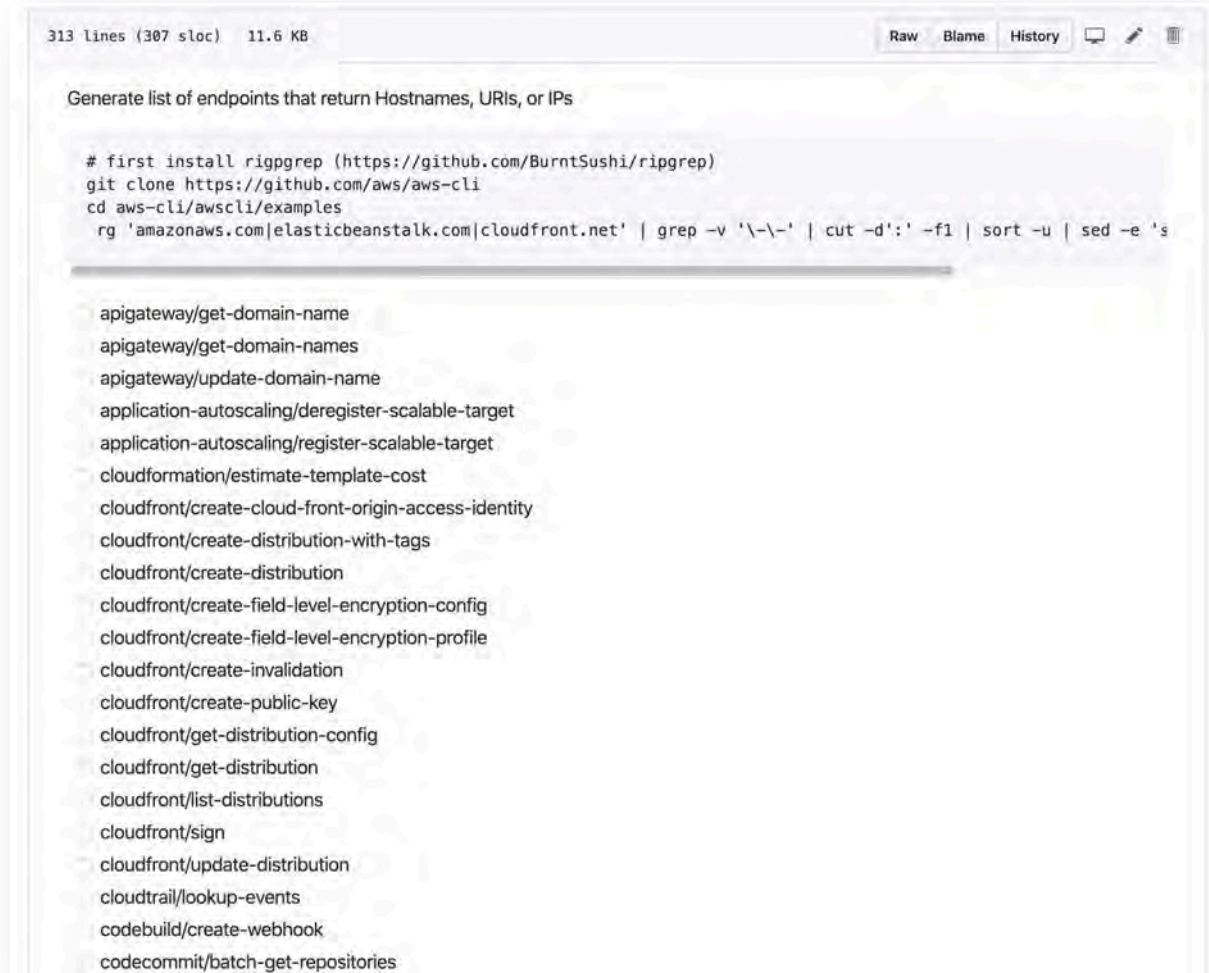
» Bucket accessible data into correct format

- Hostname
- URIs
- IPs



AWS EXPOSURE ENDPOINTS

- Identified 288 endpoints across 62 services that return a Hostname, URI, or IP
- Manually reviewed 14 services to determine the endpoints that provide publicly facing resources
- Implemented extractors for 14 services in smogcloud tool



The screenshot shows a GitHub repository interface. At the top, it indicates '313 lines (307 sloc) 11.6 KB'. Below this, there are tabs for 'Raw', 'Blame', and 'History'. The main content is a shell script titled 'Generate list of endpoints that return Hostnames, URIs, or IPs'. The script includes instructions to install 'riggrep', clone the repository, and run a command to filter endpoints from the 'awscli/examples' directory. The output of the script is a list of endpoints, including:

```
apigateway/get-domain-name
apigateway/get-domain-names
apigateway/update-domain-name
application-autoscaling/deregister-scalable-target
application-autoscaling/register-scalable-target
cloudformation/estimate-template-cost
cloudfront/create-cloud-front-origin-access-identity
cloudfront/create-distribution-with-tags
cloudfront/create-distribution
cloudfront/create-field-level-encryption-config
cloudfront/create-field-level-encryption-profile
cloudfront/create-invalidation
cloudfront/create-public-key
cloudfront/get-distribution-config
cloudfront/get-distribution
cloudfront/list-distributions
cloudfront/sign
cloudfront/update-distribution
cloudtrail/lookup-events
codebuild/create-webhook
codecommit/batch-get-repositories
```

THANK
YOU



@bishopfox | contact@bishopfox.com