

Automating Cloud Security

AWS Edition

Agenda

1. Introduction to AWS
2. AWS Shared Responsibility Model
3. How to secure AWS?
4. Other interesting open source tools
5. Q & A



About Trainer

- Chandrapal Badshah
- Security Researcher & Engineer
- 3+ years of experience (and experiments with AWS)
- AWS Certified Security - Specialty & works mostly on AWS
- You can reach me at:
 - twitter.com/bnchandrapal
 - [linkedin.com/in/bnchandrapal](https://www.linkedin.com/in/bnchandrapal)
 - badshah [👉] badshah.io



What to expect?

“As to methods there may be a million and then some, but principles are few. The man who grasps principles can successfully select his own methods. The man who tries methods, ignoring principles, is sure to have trouble.”

- Harrington Emerson

Before we begin

- Login to your AWS account in browser with IAM User having Admin privileges (BSidesDelhi-AdminUser)
- AWS CLI (v2) setup with 2 profiles:
 - Profile 1 - **BSidesDelhi-AdminUser** (`aws configure --profile BSidesDelhi-AdminUser`)
 - Profile 2 - **BSidesDelhi-ReadOnlyUser** (`aws configure --profile BSidesDelhi-ReadOnlyUser`)
- Have you setup AWS CLI v2, Steampipe and Cloud Custodian?
- I “assume” that you understand the basics of AWS like:
 - IAM (Users, Roles, Identity Based Policy & Resource Based Policy)
 - Common services like EC2 & S3
 - Issues like open S3 buckets, IMDSv1 usage, etc



Introduction to AWS

- Leading cloud provider with 33% market share in cloud vendors*
- Started at 2006 - went from few handful of services to “my-fingers-aren’t-enough” number of services today
- Present in 20 regions
 - AWS Hyderabad region coming soon!
- Over 200 AWS services covering all 3 cloud service models
 - Infrastructure-as-a-Service (IaaS) - EC2, S3, etc
 - Platform-as-a-Service (PaaS) - Lambda, Elastic Beanstalk, etc
 - Software-as-a-Service (SaaS) - Textract, Transcribe, Polly, etc

*Source: <https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/>



Introduction to AWS

Compute

- EC2
- Lightsail
- Lambda
- Batch
- Elastic Beanstalk
- Serverless Application Repository
- AWS Outposts
- EC2 Image Builder
- AWS App Runner

Containers

- Elastic Container Registry
- Elastic Container Service
- Elastic Kubernetes Service
- Red Hat OpenShift Service on AWS

Storage

- S3
- EFS
- FSx
- S3 Glacier
- Storage Gateway
- AWS Backup
- AWS Elastic Disaster Recovery

Database

- RDS
- ElastiCache
- Neptune
- Amazon QLDB
- Amazon DocumentDB
- Amazon Keyspaces
- Amazon Timestream
- DynamoDB
- Amazon MemoryDB for Redis

Developer Tools

- CodeStar
- CodeCommit
- CodeArtifact
- CodeBuild
- CodeDeploy
- CodePipeline
- Cloud9
- CloudShell
- X-Ray
- AWS FIS
- AWS AppConfig

Customer Enablement

- AWS IQ
- Managed Services
- Activate for Startups
- Support

Robotics

- AWS RoboMaker

Blockchain

- Amazon Managed Blockchain

Satellite

- Ground Station

Quantum Technologies

- Amazon Braket

Management & Governance

- AWS Organizations
- CloudWatch
- AWS Auto Scaling

Machine Learning

- Amazon SageMaker
- Amazon Augmented AI
- Amazon CodeGuru
- Amazon DevOps Guru
- Amazon Comprehend
- Amazon Forecast
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Personalize
- Amazon Polly
- Amazon Rekognition
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS DeepComposer
- AWS DeepLens
- AWS DeepRacer
- AWS Panorama
- Amazon Monitron
- Amazon HealthLake
- Amazon Lookout for Vision
- Amazon Lookout for Equipment
- Amazon Lookout for Metrics
- Amazon Comprehend Medical
- Amazon Lex

Analytics

- Athena
- Amazon Redshift
- EMR
- CloudSearch
- Amazon OpenSearch Service
- Kinesis
- QuickSight
- Data Pipeline

AWS Cost Management

- AWS Cost Explorer
- AWS Budgets
- AWS Marketplace Subscriptions
- AWS Application Cost Profiler
- AWS Billing Conductor

Front-end Web & Mobile

- AWS Amplify
- AWS AppSync
- Device Farm
- Amazon Location Service

AR & VR

- Amazon Sumerian

Application Integration

- Step Functions
- Amazon AppFlow
- Amazon EventBridge
- Amazon MQ
- Simple Notification Service
- Simple Queue Service
- SWF
- Managed Apache Airflow

Business Applications

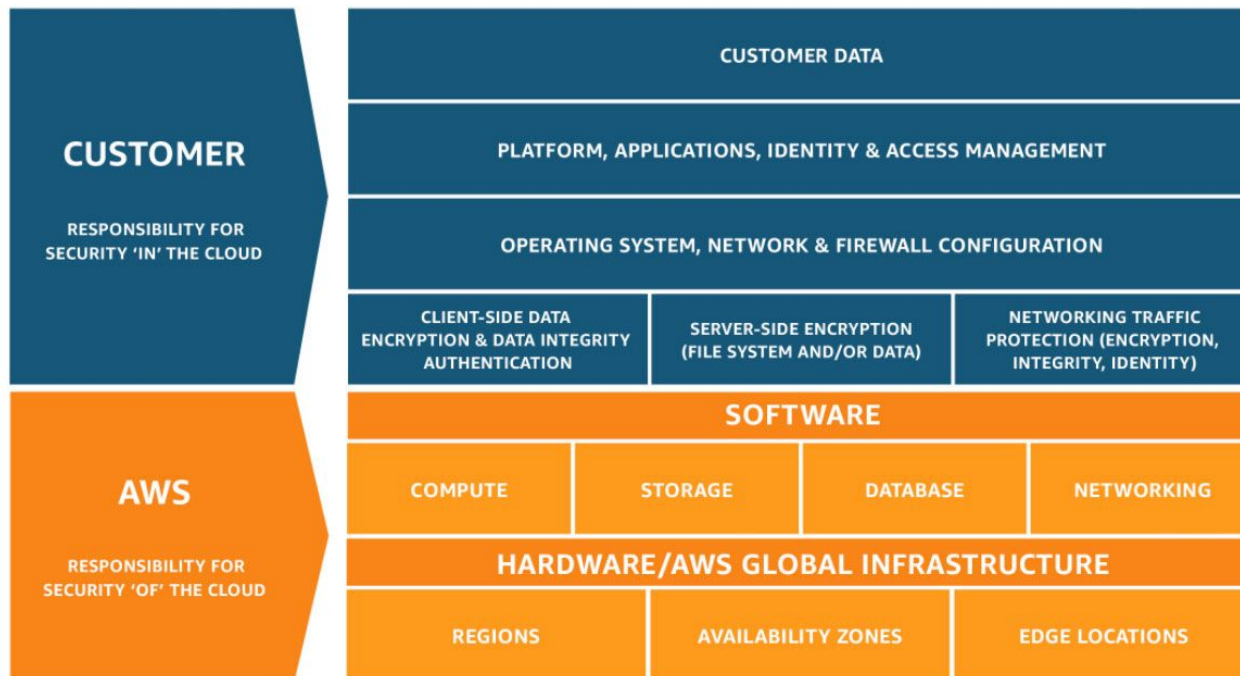
- Amazon Connect
- Amazon Pinpoint
- Amazon Honeycode
- Amazon Chime
- Amazon Simple Email Service
- Amazon WorkDocs
- Amazon WorkMail
- Alexa for Business

AWS Shared Responsibility Model

AWS is responsible for
Security “of” the Cloud

You are responsible for
Security “in” the Cloud

AWS Shared Responsibility Model



Source: <https://aws.amazon.com/compliance/shared-responsibility-model/>

AWS Shared Responsibility Model

- A very high level and “confusing at times” statement
- The responsibility differs from service to service
- This statement doesn't cover things like insecure defaults/missing security features
 - Default VPC with public subnet in all Availability Zone
 - Enforce MFA for all IAM user with Console Access

Security Incidents “Of” the Cloud

- AWS managed services can have vulnerabilities as well
- Common issue types - **Shared Tenancy Vulnerabilities & Supply Chain Vulnerabilities**
- Check out more such bugs - <https://www.cloudvulndb.org/results?q=AWS>

April 11, 2022

AWS RDS Vulnerability Leads to AWS Internal Service Credentials

TL; DR

Lightspin's Research Team obtained credentials to an internal AWS service by exploiting a local file read vulnerability on the RDS EC2 instance using the log_fdw extension. The internal AWS service was connected to AWS internal account, related to the RDS service.



<https://badshah.io>



@bnchandrapal

Security Incidents “In” the Cloud

- These are the ones you commonly see in the news!
- Common issue types: **Misconfigurations & Poor Access Control**
- You can fully avoid certain types of issues & set up automation to get alerted fast for the other types
- Check out more at <https://github.com/ramimac/aws-customer-security-incidents>

Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket: 'Lives at Stake'

The unsecured server exposed more than 1.5 million files, including airport worker ID photos and other PII, highlighting the ongoing cloud-security challenges worldwide.



Top 3 Reasons for Cloud Breaches

- Leak of Static Credentials
- Public S3 buckets
- Stolen Instance credentials through SSRF vulnerabilities

Source: <https://blog.christophetd.fr/cloud-security-breaches-and-vulnerabilities-2021-in-review/>



<https://badshah.io>



@bnchandrapal

How to secure AWS?

How to secure AWS?



Securing AWS Step by Step

- Visibility across your cloud assets
 - compute, storage, serverless, etc
 - public or private
- Compliance
 - compliant or non-compliant, etc
 - misconfigurations
- Eliminate bug classes
- Automation
 - report and alert misconfigurations
 - automatic mitigation



Securing AWS Step by Step



Visibility



Compliance



Prevent
Misconfigurations



Automate

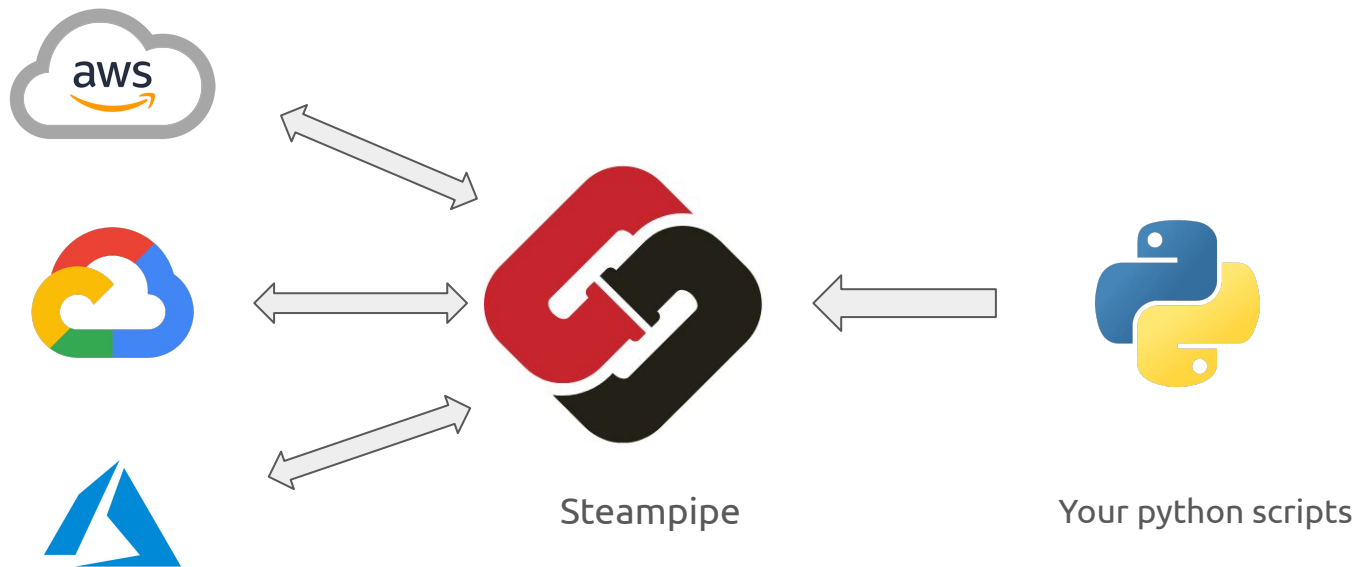
Visibility

Steampipe

- Extensible SQL interface to cloud APIs (and much more)
- Easy to install and getting started. No additional DB/visualization software.
- Open Source & has community contributed mods for AWS Inventory, AWS Compliance Checks, etc
- Supports major clouds - AWS, Azure, GCP, DigitalOcean
- Has other useful plugins - k8s, Splunk, Trivy, Shodan, etc
- Install from <https://steampipe.io/downloads>



How does Steampipe work?



Uses of Steampipe

- Gives SQL interface to interact with cloud - easy to pull the current cloud assets
- Has useful mods to visualize and detect compliance issues
- Has capability to run as a local service so your scripts can connect to it using Postgres client
- Helps answer questions like:
 - Do I use a particular AWS service?
 - How many public S3 buckets do I have?
 - Are all my DBs encrypted? If yes, using what?

DEMO

Exercise 1

Make sure you have installed latest version of Steampipe v0.17.0.

Install Steampipe plugin for AWS - `steampipe plugin install aws`

Manually create an S3 bucket with Public Access. Write a query to find all S3 buckets with Public Block Access disabled.

Setup AWS CLI credentials `aws configure --profile BSidesDelhi-ReadOnlyUser`
Use the correct AWS profile containing ReadOnly access (BSidesDelhi-ReadOnlyUser)

Exercise 1 - Solution

```
select * from aws_s3_bucket where bucket_policy_is_public = true;
```


Exercise 2

Fetch all subdomains and public IPs from your AWS account.

*Tip: Checkout services like Route53, Load Balancers (ALB & Classic ELB) for subdomains.
Checkout services like EC2 and EC2 network interfaces for public IPs.*

Exercise 2 - Solution

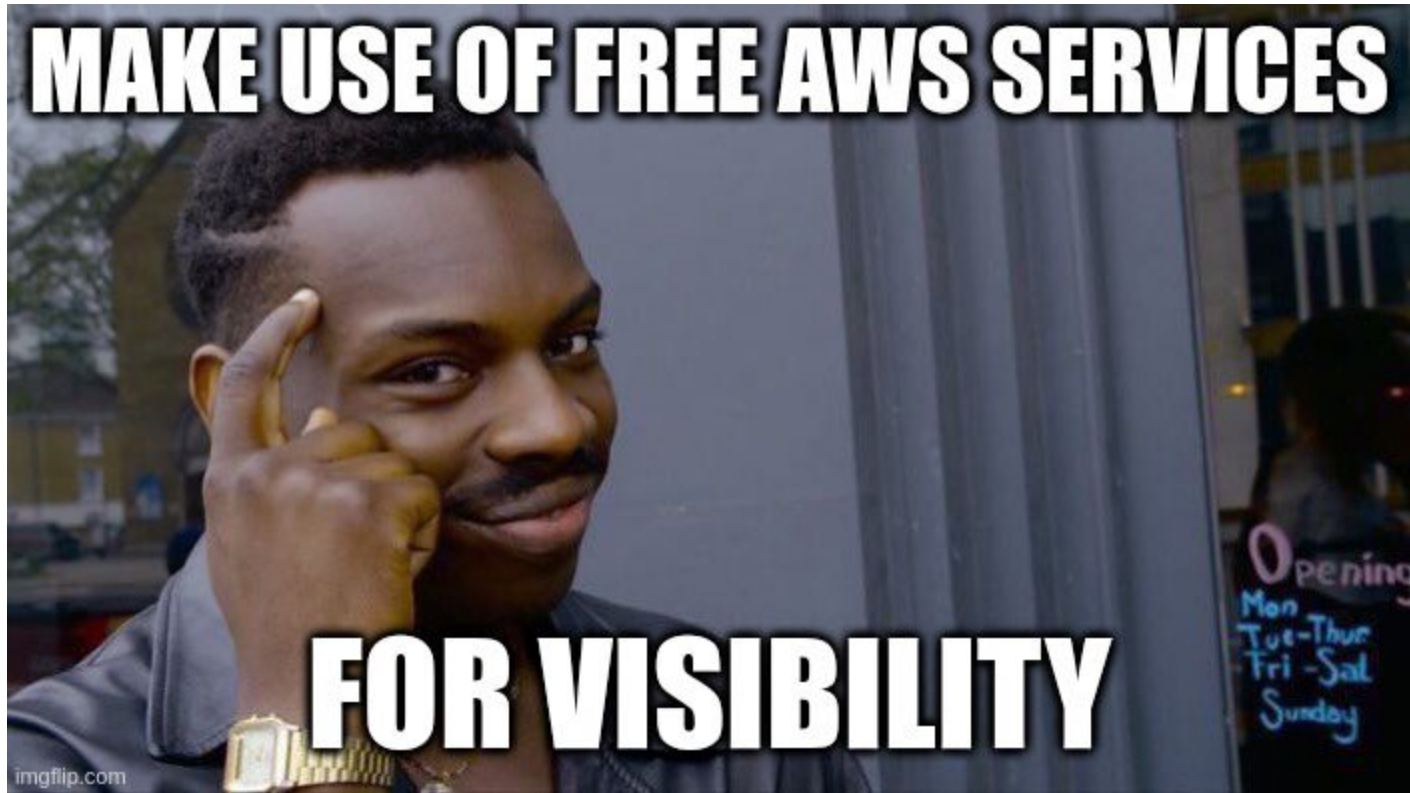
Subdomains:

```
select domain_name from aws_cloudfront_distribution
  union select r.name from aws_route53_zone as z, aws_route53_record as r where
r.zone_id = z.id
  union select dns_name from aws_ec2_classic_load_balancer where scheme =
'internet-facing'
  union select dns_name from aws_ec2_application_load_balancer where scheme =
'internet-facing';
```

Public IPs:

```
select association_public_ip from aws_ec2_network_interface where
association_public_ip is not null;
```

```
select ipv6_addresses from aws_ec2_network_interface where ipv6_addresses is not
null;
```



imgflip.com



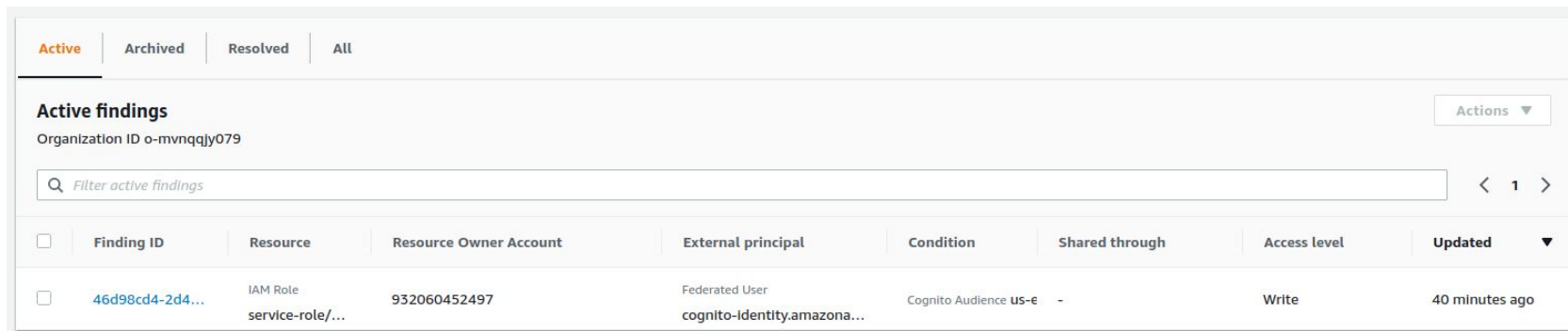
<https://badshah.io>



@bnchandrapal

IAM Access Analyzer

- Identifies resources that are shared with externally entities
- Supported resource types:
<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-resources.html>
- Generates IAM policies based on access activity



The screenshot shows the AWS IAM Access Analyzer console interface. At the top, there are tabs for 'Active', 'Archived', 'Resolved', and 'All'. Below the tabs, the section is titled 'Active findings' and shows the Organization ID 'o-mvnqqjy079'. There is a search bar with the placeholder text 'Filter active findings'. Below the search bar, there is a table with the following columns: Finding ID, Resource, Resource Owner Account, External principal, Condition, Shared through, Access level, and Updated. The table contains one row of data.

<input type="checkbox"/>	Finding ID	Resource	Resource Owner Account	External principal	Condition	Shared through	Access level	Updated
<input type="checkbox"/>	46d98cd4-2d4...	IAM Role service-role/...	932060452497	Federated User cognito-identity.amazona...	Cognito Audience us-e	-	Write	40 minutes ago

SSM Patch Manager

- SSM Agents are baked into many commonly used AMIs
- Attach SSM IAM role to the EC2 instances and schedule Patch in “Scan Only” mode

The screenshot displays the AWS Systems Manager Patch Manager console. The left-hand navigation pane shows various management tools, with 'Patch Manager' highlighted in red. The main console area is titled 'Patch Manager' and has the 'Patch baselines' tab selected, also highlighted in red. The console provides a comprehensive overview of patch management, including compliance summaries, patch states, reporting age, and a detailed history of patch operations.

Patch compliance summary
Compliance summary for managed instances that have reported Patch data.

Patch states
Count of instance for each of the most common causes of non-compliance.

Compliance reporting age
Count of instances based on the age their most recent patching compliance reports

Patch operations history
This summary of recent patching operations indicates whether an operation was started manually, or started by a maintenance window or State Manager association. Choose an operation link to view the command output.

Patch operation	Started by	Document name	End time	Status	Targets
Scan	Association	AWS-RunPatchBaseline	January 22, 2022, 11:00 AM GMT+11	Success	Instances: *
Scan	Association	AWS-RunPatchBaseline	January 21, 2022, 11:00 PM GMT+11	Success	Instances: *
Scan	Association	AWS-RunPatchBaseline	January 21, 2022, 11:00 AM GMT+11	Success	Instances: *
Scan	Association	AWS-RunPatchBaseline	January 20, 2022, 11:01 PM GMT+11	Success	Instances: *
Scan	Association	AWS-RunPatchBaseline	January 20, 2022, 7:54 PM GMT+11	Success	Instances: i-Q011R27F992a6874

ECR Basic Container Scan

- AWS ECR allows scanning Container Images with Clair - <https://github.com/quay/clair>
- Enable “Scan on push all repositories” feature

ECR > Repositories > alpine

alpine View push commands

Images (2) Refresh Delete Scan

Image URI	Pushed at	Digest	Size (MB)	Scan status	Vulnerabilities
299404798587.dkr.ecr.eu-west-1.amazonaws.com/alpine:3.9	01/06/20, 08:13:06 AM	sha256:b6f1684a6e...	2.76	Complete	1 High (details)
299404798587.dkr.ecr.eu-west-1.amazonaws.com/alpine:3.10	01/06/20, 08:11:06 AM	sha256:e4355b669...	2.79	Complete	None

Source: <https://www.youtube.com/watch?v=30S8CpfPjSw>

Where are we now?



Visibility

Compliance

Steampipe Mods

- Steampipe Modules (mods) are collection of related Steampipe resources such as dashboards, benchmarks, queries, and controls
- AWS Compliance Mod is useful to detect compliance issues



AWS Compliance

turbot/aws_compliance ⓘ v0.52

Run individual configuration, compliance and security controls or full compliance benchmarks for CIS, FFIEC, PCI, NIST, HIPAA, RBI CSF, GDPR, SOC 2, Audit Manager Control Tower, FedRAMP, GxP and AWS Foundational Security Best Practices controls across all your AWS accounts using Steampipe.



AWS Insights

turbot/aws_insights ⓘ v0.8

Create dashboards and reports for your AWS resources using Steampipe.

AWS Compliance Mod

Compliance Dashboard(s) in 4 steps:

```
git clone --depth 1 https://github.com/turbot/steampipe-mod-aws-insights.git
cd steampipe-mod-aws-insights
aws iam generate-credential-report --profile BSidesDelhi-ReadOnlyUser
steampipe dashboard
```

DEMO

Prowler

- Prowler is another famous tool that provides security checks
- <https://github.com/prowler-cloud/prowler>
- Has few features that aren't found in Steampipe mods:
 - Secret detection in Lambda code, EC2 auto scaling launch config, etc
 - EKS CIS
 - Checks for ISO 27001, FFIEC, ENS (Esquema Nacional de Seguridad of Spain)

Where are we now?



Visibility

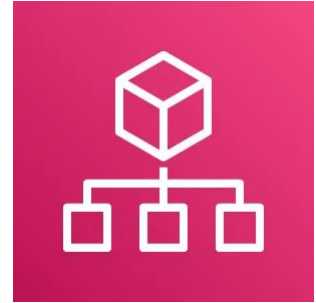


Compliance

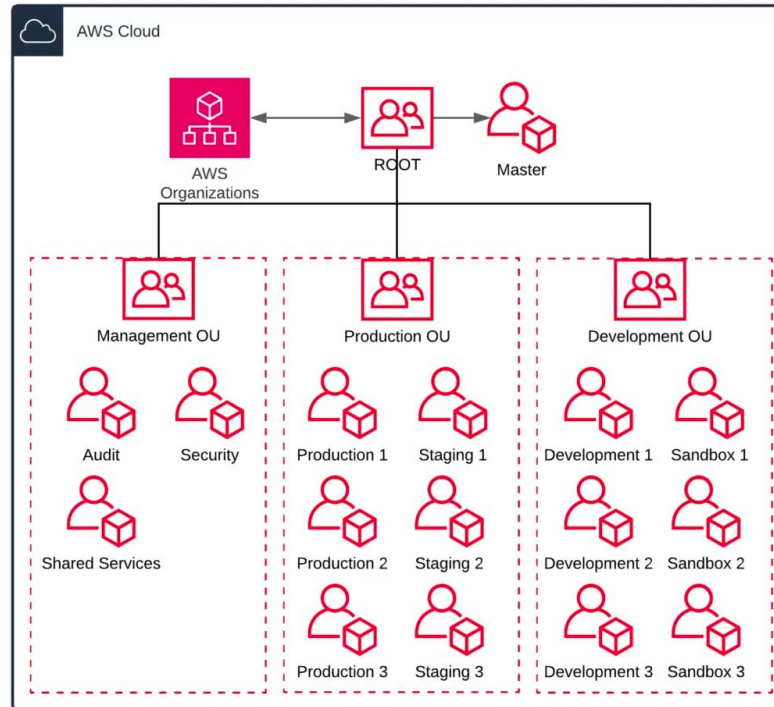
Eliminate Bug Classes

AWS Organizations

- AWS Organizations is an underrated service
- It's a free service
- It has a lot of features useful for security (SCPs, Organizational Units, Backup & Tag Policies, etc)
- Even if you use single AWS account, create a separate AWS account that acts as Master account



AWS Organizations



Source: <https://towardsthecloud.com/aws-organizations>

What can you do with AWS Organizations?

- Have [Service Control Policy](#) to manage permissions and even enforce settings for all IAM users (including root user) in an account/group of accounts
- Create Organizational Units (OU) to group accounts and apply SCPs
- Enable Organization Trail
- Enable CloudFormation Stack Sets to deploy your security tools across AWS accounts
- Setup delegated administrator account (usually Security / DevOps managed AWS account)



Few Security Enforcements with AWS Organizations

- Disable AWS regions across child accounts - *no worries on users creating resources in unexpected regions*
- Enforce RDS DB encryption across child accounts - *no worries of unencrypted RDS*
- Enforce EC2 compute size - *credential leak can't spin up costly GPUs to mine crypto*
- Enable Organizational Trail - *so no one can disable it in child accounts (even with root credential)*
- Check more -
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples.html

DEMO

Where are we now?



Visibility



Compliance



Prevent
Misconfigurations



Automation

Introduction to Cloud Custodian

- Open Source Cloud Security, Governance, and Management tool written in Python
- Cloud Security and Governance
 - Enables guardrails
 - If IAM user with Console access created, delete access in 24 hrs if no MFA
 - Enhances incident response
 - If S3 bucket made world readable, immediately close
 - Enforce compliance
 - Critical real-time checks from CIS, PCI, etc can be enforced
- Management
 - Cost Optimization
 - Delete underutilized resources and resources without tags in X days

Advantages with Cloud Custodian

- Near real-time alerts (depends on CloudWatch latency)
- Creating custom checks - just a YAML file away
- Multiple ways to deploy (cron, event-trigger, etc)

Hey, why can't we use services from AWS?

You know, like

AWS Config with custom Conformance Packs

Results sent to Security Hub and create JIRA tickets 😊



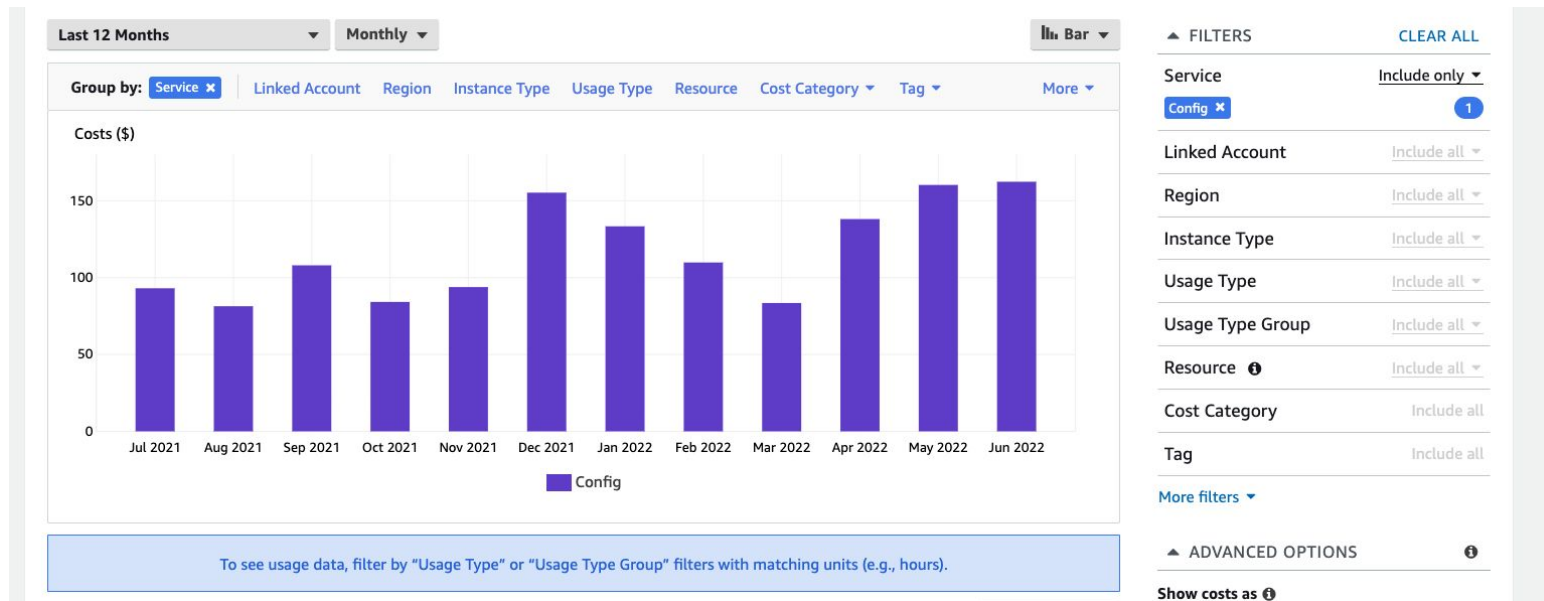
Issues with using AWS services for real-time alerts

- AWS Config and SecurityHub makes it easier to detect and alert misconfigurations

BUT

- AWS Config doesn't support all AWS Resources (ex: CloudFront in non us-east-1 region)
- Writing custom rules take some time to understand and master (Have a look at [awslabs/aws-config-rules](#) GitHub repo)
- SecurityHub supports Jira Service Management but it's a separate offering from Atlassian
- The cost is comparatively super high and directly proportional to no. of resources

Issues with using AWS services for real-time alerts



Cost of AWS Config alone without AWS SecurityHub, S3 cost or Config custom rules

Hey, why can't we use services from AWS?

You know, like

AWS Config with custom Conformance Packs

Results sent to Security Hub and create JIRA tickets 😊

Answer: It's costly, has steep learning curve and it might require more work to be done to integrate to existing security workflows outside Security Hub





How does Cloud Custodian work?

- Takes custom YAML policy file as input, performs the checks and gives if any resource is violating the policy

```
custodian run -c policy.yml -s logs-dir --region all
```

- Sample policy to detect violating resources

```
policies:  
  - name: my-first-policy  
    resource: aws.ec2  
    filters:  
      - "tag:Custodian": present
```



How does Cloud Custodian work?

Sample policy to detect violating EC2 instances (which has Custodian tag) and act on them

```
polices:  
  - name: my-first-policy  
    resource: aws.ec2  
    filters:  
      - "tag:Custodian": present  
    actions:  
      - stop
```



How does Cloud Custodian work?

Sample policy to detect violating EC2 instances and act on them **only if they are in us-east-1 region**

```
policies:  
  - name: my-first-policy  
    resource: aws.ec2  
    conditions:  
      - region: us-east-1  
    filters:  
      - "tag:Custodian": present  
    actions:  
      - stop
```



How does Cloud Custodian work?

Sample policy to detect violating resources and act on them *immediately*

```
policies:  
  - name: my-first-policy  
    resource: aws.ec2  
    mode:  
      type: cloudtrail  
      role: CloudCustodianLambdaWorker  
      events:  
        - RunInstances  
    filters:  
      - "tag:Custodian": present  
    actions:  
      - stop
```



Exercise 3

What would the policy look like if I want to detect EC2 instances that ***has the tag "Custodian"*** and ***stop it immediately*** only if it is ***in us-east-1 region***.

(Assumption: We use EC2 in all regions. Feel free to refer previous slide policy.)

```
polices:
- name: my-first-policy
  resource: aws.ec2
  mode:
    type: cloudtrail
    role: CloudCustodianLambdaWorker
  events:
    - RunInstances
  filters:
    - "tag:Custodian": present
  actions:
    - stop
```



Exercise 3 - Solution

```
polices:
- name: my-first-policy
  resource: aws.ec2
  mode:
    type: cloudtrail
    role: CloudCustodianLambdaWorker
    events:
      - RunInstances
  conditions:
    - region: us-east-1
  filters:
    - "tag:Custodian": present
  actions:
    - stop
```

Cloud Custodian Policies

- Policies:
 - One policy file can have multiple checks
 - Each check can have different resources, filters and actions
 - You can execute one input policy file at a time
- AWS doesn't have strict API rate limits in most Get* API calls. But there can be exceptions (like IAM GetCredentialReport allowing very few calls per day)
- Cloud Custodian can send it's execution logs to CloudWatch which allows further automation/visualization over time

Common Execution Modes

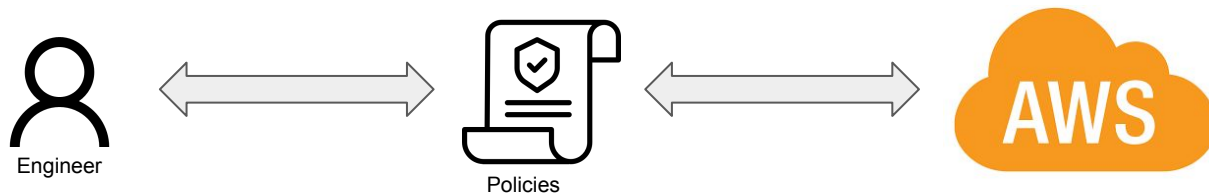
- Policies can be executed in generally in two modes: pull based (default) or lambda based
- Lambda mode can be triggered by events from:
 - EventBridge (for *periodic* executions)
 - Auto Scale Group's EC2 state changes
 - CloudTrail
 - AWS Config
 - EC2 state change
 - GuardDuty
 - SecurityHub
 - Personal Health Dashboard

See <https://cloudcustodian.io/docs/aws/resources/aws-modes.html> for more

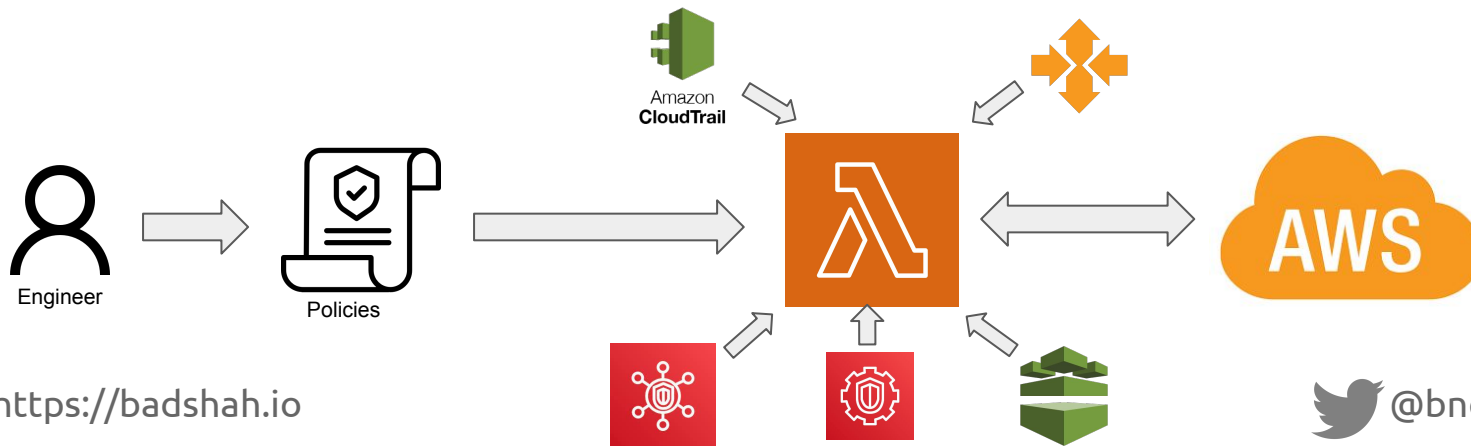


In a nutshell, how does Cloud Custodian work?

On demand pull-based execution:



Realttime lambda execution:



Common Actions

- There are many actions that can be taken if policy is violated
- Few actions that we use:
 - notify (to send notifications: SQS -> Lambda every 1 min -> Slack)
 - webhook*
- Other actions:
 - invoke-lambda
 - auto-tag-user
 - modify-policy
 - put-metric (CloudWatch)
 - and more...

Check <https://cloudcustodian.io/docs/aws/resources/aws-common-actions.html> for more



Creating your first policy

Save the file to `policy-1.yml`.

```
policies:  
  - name: get-s3-buckets  
    resource: aws.s3  
    filters:  
      - "tag:BSidesDelhi": present
```

Execute:

```
custodian validate policy-1.yml
```

If no errors, execute:

```
custodian run policy-1.yml -s output --region ap-south-1 --dryrun  
custodian run policy-1.yml -s output --region ap-south-1
```

Get more specific - Finding Security buckets

```
polices:  
  - name: get-security-s3-buckets  
    resource: aws.s3  
    filters:  
      - "tag:BSidesDelhi": "Security"
```


Finding public resources - S3 buckets

- Custodian comes with multiple resource filters
- Check `custodian schema aws.s3`

Exercise 3

Create an S3 bucket. Write a policy to automatically encrypt it.

Exercise 3 - Solution

Create an S3 bucket. Write a policy to automatically encrypt it.

```
policies:  
  - name: encrypt-s3-buckets  
    resource: aws:s3  
    filters:  
      - type: bucket-encryption  
        state: False  
    actions:  
      - type: set-bucket-encryption
```

Where are we now?



Visibility



Compliance



Prevent
Misconfigurations

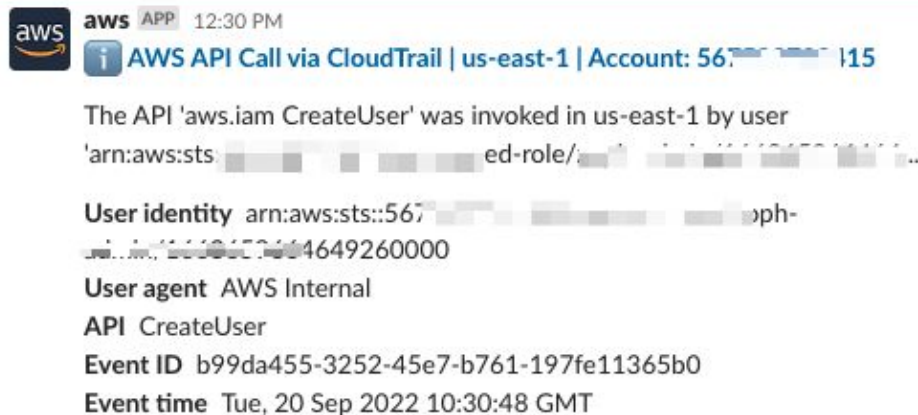


Automate

Other interesting open source tools

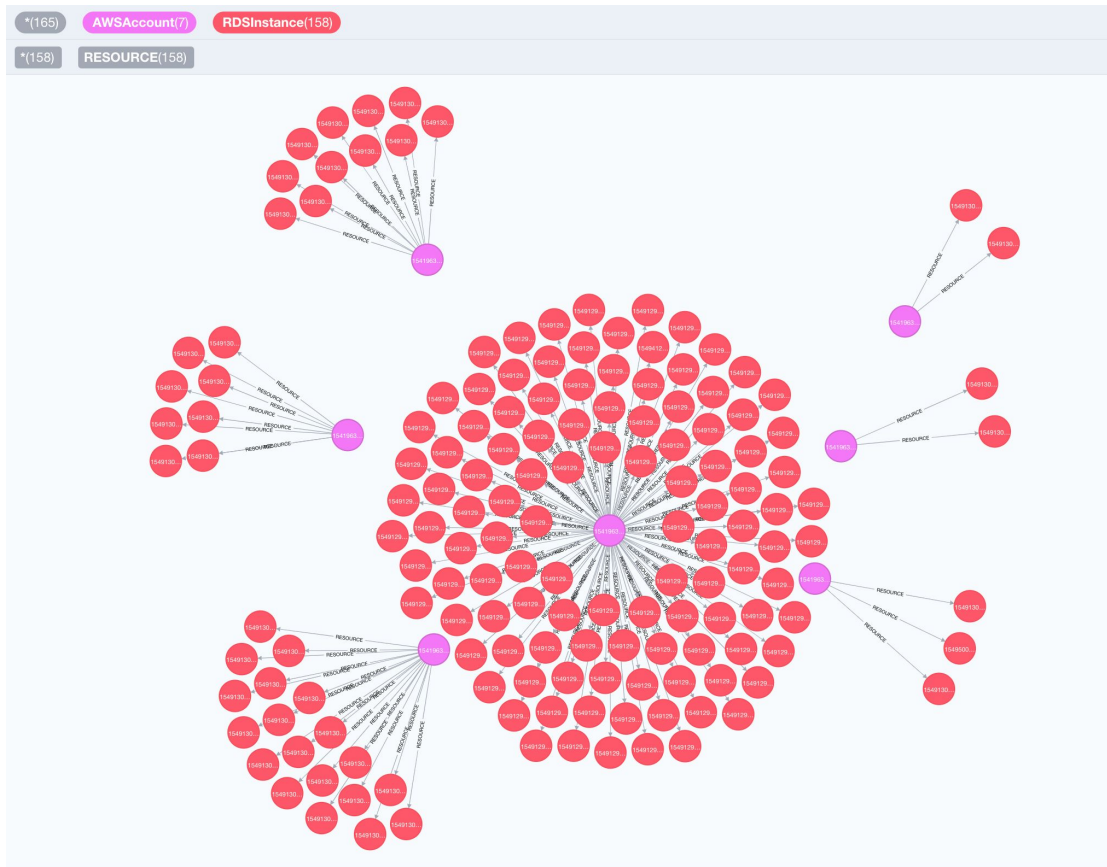
AWS Security Survival Kit

- Basic setup for proactive monitoring and alerting environment on common suspicious activities in AWS cloud
- <https://github.com/zoph-io/aws-security-survival-kit>



Cartography

- Security graph tool to consolidate AWS assets and the relationships between them
- It's like BloodHound but for AWS 😊
- <https://github.com/lyft/cartography>
- You can find all assets (like Steampipe) - <https://blog.marcolancini.it/2020/blog-tracking-moving-clouds-with-cartography/>
- It's value is in visualizing the relationships with accounts and possible attack paths - <https://blog.marcolancini.it/2020/blog-mapping-moving-clouds-with-cartography/>



Cloudsplaining

- AWS IAM Security Assessment tool that identifies violations of least privilege
- Generates a risk-prioritized HTML report
- <https://github.com/salesforce/cloudsplaining>

Cloudsplaining Customer Policies Inline Policies **AWS Policies** IAM Principals Guidance Appendices Account ID: 987654321987 | Account Name: fake

AWS-Managed Policies (11)

Per page 10

Policy Name	Attached To		Infrastructure Services	Service Modification	Wildcard	Privilege Escalation	Resource Exposure	Data Exfiltration
	Principals	Services						
AmazonEC2FullAccess	1	5	339	4	0	6	0	
AmazonRDSFullAccess	2	4	88	2	0	4	0	
AmazonS3FullAccess	1	1	60	1	0	13	1	
AmazonS3ReadOnlyAccess	1	1	1	0	0	0	1	
AmazonSESEFullAccess	1	1	36	1	0	3	0	
AWSCloudTrailFullAccess	1	5	19	1	0	5	1	

**Is this all?
Have we automated everything?**

Have we automated everything?



Container Security
Runtime Security
Cloud IR & Forensics
Context based CSPM Rules



Visibility



Compliance



Prevent
Misconfigurations



Automate
(CSPM checks)

Cloud Maturity Models

- <https://maturitymodel.security.aws.dev/en/model/> (by AWS)
- https://summitroute.com/downloads/aws_security_maturity_roadmap-Summit_Route.pdf (by Scott Piper)
- https://cloudsecdocs.com/aws/defensive/checklists/maturity_roadmap/ (by Marco Lancini)

Remember

“As to methods there may be a million and then some, but principles are few. The man who grasps principles can successfully select his own methods. The man who tries methods, ignoring principles, is sure to have trouble.”

- Harrington Emerson



THANK YOU
Any Questions



<https://badshah.io>



@bnchandrapal