

OOPS, I CLOUDED AGAIN:

MISCONFIGURATIONS, MAYHEM, AND THE MISTAKES WE KEEP MAKING

Kat Fitzgerald evilkat@rnbwmail.com


github.com/rnbwkat/presents
rnbwkat@infosec.exchange
rnbwkat.bsky.social
linkedin.com/in/katfitzgerald/
youtube.com/@rnbwkatandtequila
(first episode being recorded soon)

theunfrostedfiles.com
sashatheflamingo.xyz

1

DISCLAIMER

- The views and opinions expressed in this presentation are my own and do not necessarily reflect the official policy or position of any current or previous employer.
- Examples of exploitations, coding and vulnerabilities discussed within this presentation are only examples and they should not be utilized in the real-world.



3

WHY WE AREN'T HERE

- I can't solve all your Security woes
- I won't teach you how to break-in to the cloud – only "concepts"
- Common Sense went out the window decades ago
- Cloud(s) continue to evolve and as things change, so do attack vectors



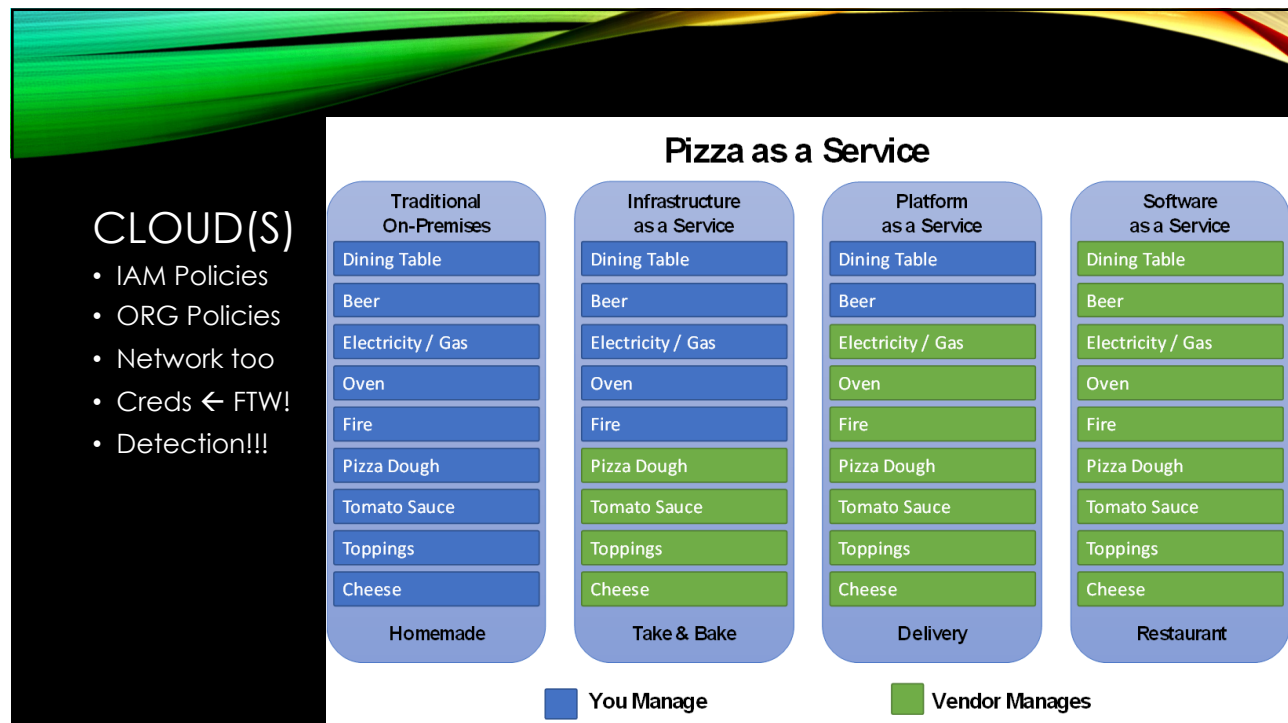
4

WHY WE ARE HERE

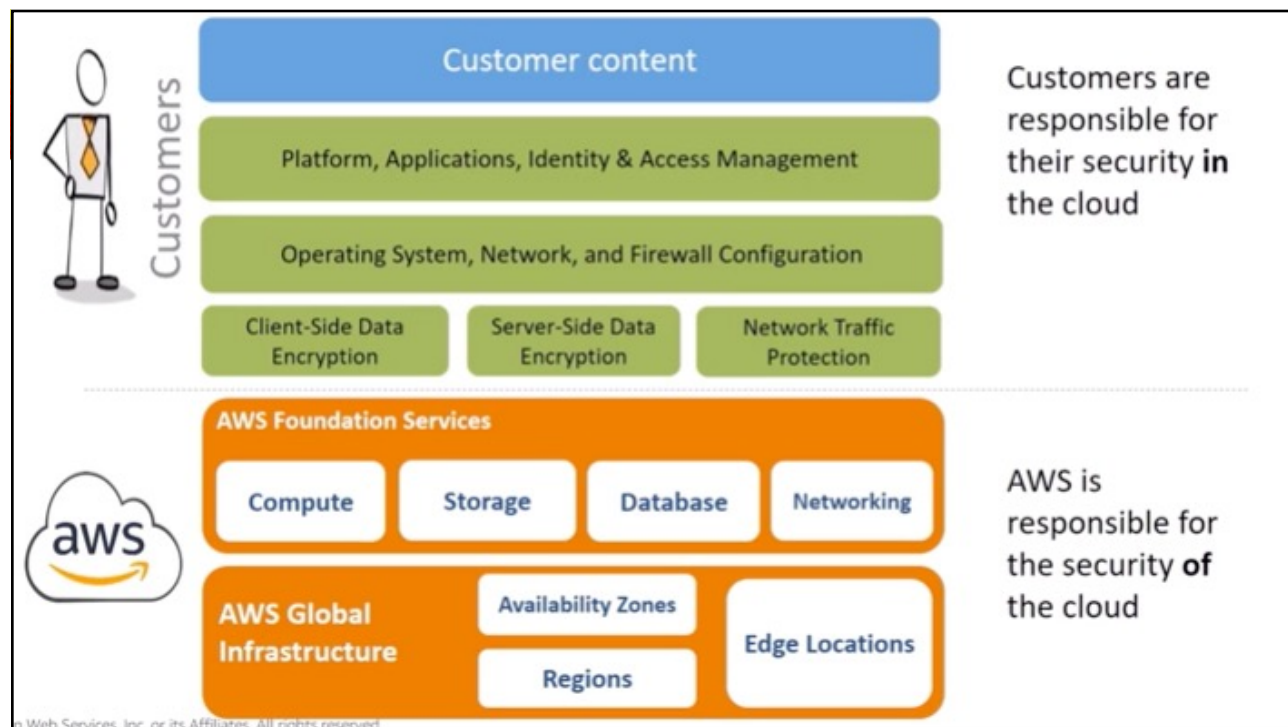
- The Cloud!
- Security
- Humans
- 2018, 2019, 2020, 2021, 2022, 2023, WTF?
 - 70% of organizations reported at least one cloud-related security incident
 - 207 days was the average time to identify and contain a breach, slightly longer than the previous year
 - Misconfigurations and compromised credentials were the leading causes of cloud breaches
 - cloudwize.io/blog/cloud-data-breaches-in-2024-a-year-in-review

Commonsense is required – disregard previous slide ☺

5



6



7

AN INCIDENT

- Most incidents are NOT 0-day
- Most incidents are NOT "fancy"
- Most incidents don't come from "vulnerability scanners"

1. Most breaches come from "Config Issues"
2. A close 2nd - compromised credentials
3. Trailing in 3rd - Over-Priv Users



8

OWASP A05:2021 SECURITY MISCONFIGURATION

"Nearly all successful attacks on cloud services are a result of customer misconfiguration, mismanagement and mistakes." –Neil MacDonald, Gartner

Pentesting BTC (before the cloud)

- Identify target
- Find vulns
- Exploit
- After
 - Find Misconfigurations (= vulns)
 - Line up targets

9

CLOUD INCIDENTS

- Misconfigurations #1
 - Training non-existent
- Misplaced (forgotten?) keys/tokens
 - Once upon a time
- Lack of training cloud secrets usage and application
- Encryption @rest
 - transit too

10

GENERAL ATTACK VECTORS

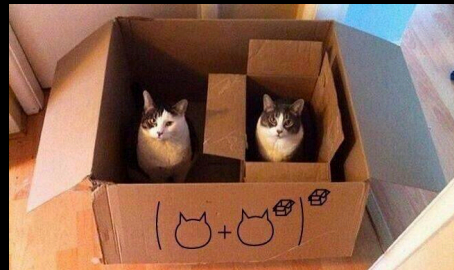
MISCONFIGURATIONS

- Unrestricted Ingress/Egress ports
- Secrets Mgmt (what else?!)
- Missing Logging/Monitoring
 - <https://www.cloudquery.io/> (osquery on steroids)
 - Extracts cloud assets into normalized PostgreSQL tables
- Insecure Backups
- Buckets/Storage Access
- Lack of TLS/SSL
- Permissive Access to VMs/Containers

11

GENERAL ATTACK EXAMPLES

- IaaS
 - Weak creds
 - Anything belonging to tenant = attack surface
 - Application bugs = RCE (reading files?)
 - Misconfigured "fw"
 - Metadata API
 - AC = After Credentials
- PaaS
 - <IaaS >SaaS
 - Application vulns
 - Storage
 - Data in Transit



12

MISC TOOL(S)

IAM APE

- IAM AWS Policy Evaluator
- github.com/orcasecurity/orca-toolbox

CloudRecon

- CloudRecon is a suite of tools for red teamers and bug hunters to find ephemeral and development assets in their campaigns and hunts
- github.com/g0ldencybersec/CloudRecon

<https://maagsoft.com/how-to-use-wazuh-to-monitor-and-secure-your-cloud-infrastructure/>

13

MORE ON STORAGE

- Predictable names = no
- Remember NFS?
 - Cloud Snapshots!
 - "Volumes"
- Perms
 - Public
 - Writeable
 - Guessable names/passwords (see first bullet above ^^)
- Github tools
 - <https://buckets.grayhatwarfare.com/>
- Cloud Snapshots are very much IaaS attack surface
- A disk image copy of the cloud instance
- Snapshots (and volumes) can be retrieved
- Once attached they bypass perms

15

The screenshot shows the 'Buckets' section of the Grayhat Warfare website. The header includes navigation links for 'Buckets', 'Shorteners', 'Pricing', 'FAQ', and 'Contact Us'. The main content area displays a grid of cloud storage providers with their respective file counts and last update dates.

Provider	Files	Last Update
Files	2.9bn of 19.1bn	
Amazon Web Services	24.8k of 379.8k	
Azure Blob Storage	47.0k of 69.3k	
Digital Ocean Spaces	10.5k	
Google Cloud Platform	38.0k of 70.3k	
Alibaba Cloud	5.2k	
		Last Update: 26 Jul 2025

At the bottom, there is a search bar labeled 'Search Public Buckets' and a button for 'Random Files'.

16

ONCE UPON A TIME (1)

7.18 [extra718] Check if S3 buckets have server access logging enabled

```

FAIL! Bucket 00247 [REDACTED] 660497866f has server access logging disabled!
FAIL! Bucket 1334e [REDACTED] c44246fedc has server access logging disabled!
FAIL! Bucket 1da42 [REDACTED] 3a7c557bdf has server access logging disabled!
FAIL! Bucket 26f44 [REDACTED] 08776a7a6e has server access logging disabled!
FAIL! Bucket 28c4d [REDACTED] 92f8df19ec has server access logging disabled!
FAIL! Bucket 32f4f [REDACTED] dfd4fecb7c has server access logging disabled!

```

7.29 [extra729] Ensure there are no EBS Volumes unencrypted

INFO! Looking for EBS Volumes in all regions...

```

FAIL! us-west-1: vol-0e [REDACTED] d2aba is not encrypted!
FAIL! us-west-1: vol-0e [REDACTED] 678be is not encrypted!
FAIL! us-west-1: vol-0f [REDACTED] f9297 is not encrypted!
FAIL! us-west-1: vol-09 [REDACTED] 0a69b is not encrypted!
FAIL! us-west-1: vol-07 [REDACTED] 3c68a is not encrypted!
FAIL! us-west-1: vol-0c [REDACTED] e761b is not encrypted!
FAIL! us-west-1: vol-0f [REDACTED] 76e46 is not encrypted!
FAIL! us-west-1: vol-08 [REDACTED] 4c38b is not encrypted!
FAIL! us-west-1: vol-0c [REDACTED] a5318 is not encrypted!

```

17

ONCE UPON A TIME (2)

```

FAIL! us-east-1: Potential secret found in i-00 [REDACTED] ccl27 User Data
FAIL! us-east-1: Potential secret found in i-00 [REDACTED] fb0b7 User Data
PASS! us-east-1: No secrets found in i-0c5 [REDACTED] 61abb User Data
PASS! us-east-1: No secrets found in i-0183 [REDACTED] f366 User Data or it is empty
FAIL! us-east-1: Potential secret found in i-027 [REDACTED] 0913 User Data

```

```

FAIL! us-east-1: Potential secret found in i-0b4 [REDACTED] 9f956 User Data
FAIL! us-east-1: Potential secret found in i-0f4 [REDACTED] f0465 User Data
FAIL! us-east-1: Potential secret found in i-083 [REDACTED] 36651 User Data
FAIL! us-east-1: Potential secret found in i-077 [REDACTED] 0521e User Data
FAIL! us-east-1: Potential secret found in i-09e [REDACTED] 77d78 User Data
FAIL! us-east-1: Potential secret found in i-0ac [REDACTED] ed82 User Data
FAIL! us-east-1: Potential secret found in i-052 [REDACTED] 38d68 User Data
FAIL! us-east-1: Potential secret found in i-0a79 [REDACTED] ac80e User Data
FAIL! us-east-1: Potential secret found in i-004 [REDACTED] 1b8c7 User Data
FAIL! us-east-1: Potential secret found in i-058f [REDACTED] f0452 User Data

```

18

ONCE UPON A TIME (3)

```
[check14] Ensure access keys are rotated every 90 days or less (Scored)
FAIL! evil_m...e_dev_rw has not rotated access key1 in over 90 days
FAIL! evil_... has not rotated access key1 in over 90 days
FAIL! atlan... has not rotated access key1 in over 90 days
FAIL! gargleblaster... has not rotated access key1 in over 90 days
FAIL! fed_e... PASS! us-west-1: Instance i-09c06004c7fb38972 associated with role gladitors-monitoring-...
FAIL! fed_...-VPC
FAIL! iam_... FAIL! us-west-1: Instance i-0aef...2cc not associated with an instance role
PASS! us-west-1: Instance i-060b...4cd0 associated with role kittle-ec2Role-dev-testing
FAIL! iam_... FAIL! us-west-1: Instance i-0e640...3fb not associated with an instance role
FAIL! us-west-1: Instance i-0fdd1...89 not associated with an instance role
PASS! us-west-1: Instance i-0c2d0c8cbb5ef7007 associated with role etcd-server-...
0000001
FAIL! us-west-1: Instance i-0cf...e70ff not associated with an instance role
PASS! us-west-1: Instance i-0722...135 associated with role EC2_Cloudwatch
FAIL! us-west-1: Instance i-05b27...715f not associated with an instance role
FAIL! us-west-1: Instance i-0bcc0...60 not associated with an instance role
PASS! us-west-1: Instance i-00...77f1 associated with role s3-full-access
PASS! us-west-1: Instance i-00d51...1df associated with role s3-full-access
FAIL! us-west-1: Instance i-09233...d09 not associated with an instance role
FAIL! us-west-1: Instance i-004c...e75 not associated with an instance role
FAIL! us-west-1: Instance i-0a1...5ccf not associated with an instance role
FAIL! us-west-1: Instance i-078a...045b1 not associated with an instance role
FAIL! us-west-1: Instance i-0248c...f681 not associated with an instance role
```

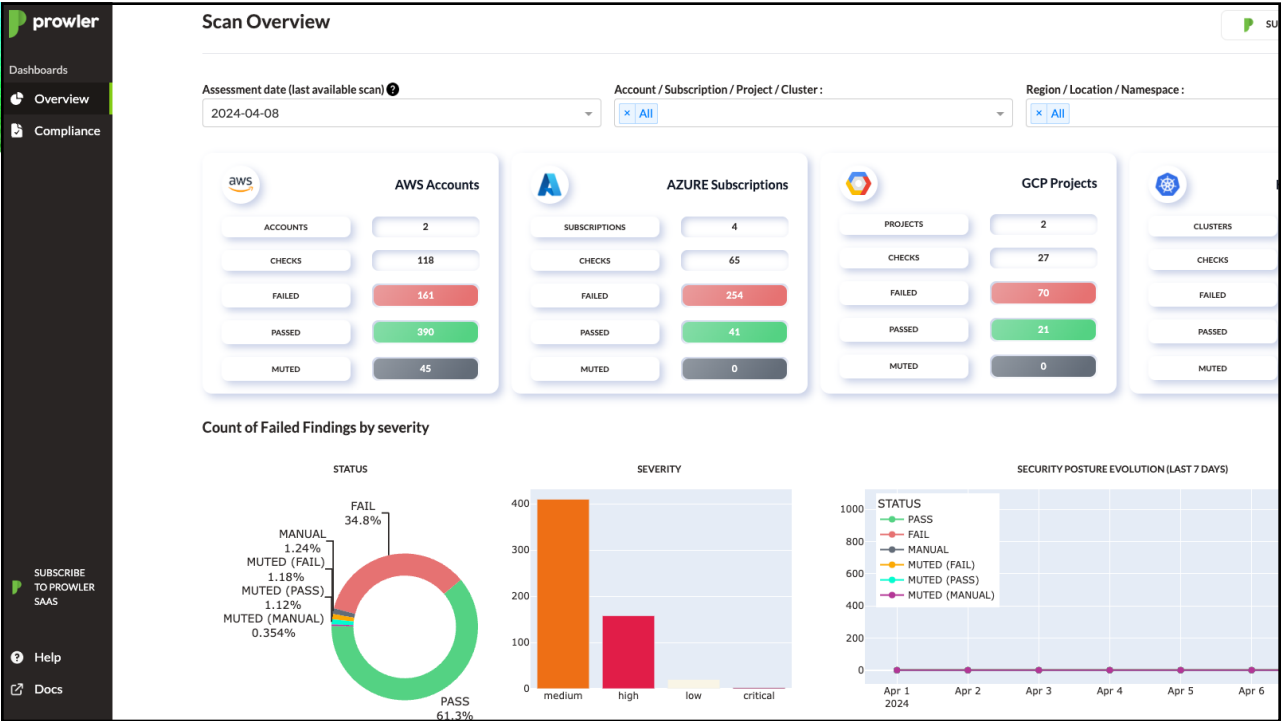
19

ONCE UPON A TIME (4)

<https://www.mitiga.io/blog/how-mitiga-found-pii-in-exposed-amazon-rds-snapshots>

```
PASS! us-east-1: RDS Snapshot rds:pipe... is not shared
PASS! us-east-1: RDS Snapshot rds:pipe... is not shared
PASS! us-east-1: RDS Snapshot rds:pipe... is not shared
PASS! us-east-1: RDS Snapshot rds:piper...16-06-09 is not shared
PASS! us-east-1: RDS Snapshot rds:piper...-06-09 is not shared
PASS! us-east-1: RDS Snapshot rds:piper...08 is not shared
PASS! us-east-1: RDS Snapshot rds:piper...-10 is not shared
PASS! us-east-1: RDS Snapshot rds:piper...-09 is not shared
PASS! us-east-1: RDS Snapshot rds:piper-...-05-20 is not shared
PASS! us-east-1: RDS Snapshot rds:piper...-05-20 is not shared
PASS! us-east-1: RDS Snapshot rds:piper...05-19 is not shared
PASS! us-east-1: RDS Snapshot rds:piper...2020-04-16-05-19 is not shared
```

20



21

```
prowler - summary

[INFO] Prowler v3.0 - AWS checks starting...
[INFO] Profile: CIS Benchmark - AWS Foundations
[PASS] 01 - Ensure multi-factor authentication is enabled for the root account
[PASS] 02 - Ensure credentials unused for 90 days are rotated
[FAIL] 03 - Ensure no security groups allow ingress from 0.0.0.0/0 to port 22 (found: sg-0a12bc34)
[FAIL] 04 - Ensure S3 buckets do not allow public READ access (found: mycompany-uploads)
[PASS] 05 - Ensure CloudTrail is enabled in all regions
Summary: 2 FAILED, 2 INFO, 6 PASS

Command: prowler aws -M text,html
```

22

```
prowler - detailed fail

[INFO] Check: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22
[FAIL] sg-0a12bc34 (default) allows 0.0.0.0/0 on port 22
  - Rule: tcp 22 0.0.0.0/0 (added by user: alice@example.com)
  - Recommendation: Restrict SSH to known IPs or use bastion/jump host.

[INFO] Check: Ensure S3 buckets do not allow public READ access
[FAIL] mycompany-uploads allows PUBLIC READ
  - Location: s3://mycompany-uploads/ (Policy: Allow s3:GetObject principal: * )
  - Recommendation: Remove public read, enable bucket policy with allow-list, enable object ACL block.

[INFO] Prowler completed. Run: prowler -M csv to export findings.

Command: prowler aws -M text,html
```

23

```
[prowler] v4.0.0
the handy multi-cloud security tool

Date: 2024-04-08 15:09:16

-> Using the AWS credentials below:
  * AWS-CLI Profile: default
  * AWS Regions: us-east-1
  * AWS Account:
  * User Id: :toni
  * Caller Identity ARN: arn:aws:sts::

-> Using the following configuration:
  * Config File: prowler/config/config.yaml
  * Mute List File: prowler/config/aws_mutelist.yaml
  * Scanning unused services and resources: False

Executing 305 checks, please wait...
-> Scan completed! | 305/305 [100%] in 1:56.7

Overview Results:
41.8% (79) Failed 54.5% (103) Passed 19.05% (36) Muted

Account 552455647653 Scan Results (severity columns are for fails only):
Provider Service Status Critical High Medium Low Muted
aws accessanalyzer FAIL (1) 0 0 0 1 0
aws account FAIL (1) 0 0 1 0 0
aws lambda FAIL (1) 0 0 0 1 5
aws backup FAIL (1) 0 0 0 1 0
aws cloudformation FAIL (5) 0 0 5 0 3
```

24

CASE STUDY: CAPITAL ONE (2019)

- Capital One (2019) — attacker exploited an application vulnerability and gained access to IAM credentials, enabling S3 data exfiltration (~100M records)
- Result: widespread media coverage, regulatory scrutiny, and lessons on IAM and metadata protection
- Lessons:
 - enforce least privilege IAM
 - rotate roles/keys
 - monitor metadata/API access,
 - harden web-facing services

25

CASE STUDY: STARTUP AI

- Engagement: security review + pentest for an AI startup
- Front-end: they had good OWASP AI/ML protections for prompt attacks
- OSINT found hardcoded credentials in GitHub — keys worked and provided cloud access
- Sparse monitoring allowed stealthy mapping and persistence

26

CASE STUDY: STARTUP AI (TECHNICAL PATH & LESSONS)

Attack path & escalation timeline:

- Hardcoded creds in repo → cloud access
- Attacker stood up EC2 and performed DNS cache poisoning to MITM front-end → prompts intercepted/modified
- Found Kubernetes training cluster; escalated to admin on a pod and injected data into model training
- Consequences: model integrity failure, data exfiltration, unnoticed attacker presence

Recommendations:

- Scan repos for secrets (trufflehog, git-secrets), remove hardcoded creds, rotate keys
- Use short-lived credentials (OIDC/STS) and centralized secret stores (Vault, Secrets Manager)
- Harden internal detection: host agents, VPC flow logs, monitor metadata server access
- Secure k8s with RBAC, network policies, and restrict admin pods

27

AND.. *another example (fixed)*

- Mastodon – Anonymous credentials has s3:* privileges
 - *Lenin Alevski*
- alevski.com/2022/11/system-misconfiguration-is-the-number-one-vulnerability-at-least-for-mastodon/
- Timeline of events and disclosure
 - 11/17/2022 – I created my infosec.exchange account and start playing around
 - 11/17/2022 – Found anonymous access was enabled and all the files were exposed
 - 11/17/2022 – Reached to jerry@infosec.exchange and reported the issue
 - 11/18/2022 – Jerry confirmed is aware of the issue and working on a fix
 - 11/18/2022 – Issue got fixed, thank you so much Jerry.

28

TOOLS & PLAYBOOKS

- Discovery & OSINT: cloud_enum, CloudRecon, initstring/cloud_enum
- Audit & CSPM: Prowler, ScoutSuite, CloudMapper, Prisma/Wiz/Orca
- Secrets & IaC scanning: trufflehog, tfsec, Checkov, git-secrets
- Red team & labs: Pacu, CloudGoat, CloudPentestCheatsheets

29

(SOME) MORE TOOLS

AWS (and others – depending)

- github.com/prowler-cloud/prowler — Multi-cloud compliance & misconfig scanning (AWS, Azure, GCP and more)
- github.com/initstring/cloud_enum — Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud
- github.com/RhinoSecurityLabs/pacu — AWS exploitation framework
- github.com/duo-labs/cloudmapper — AWS visualization & auditing
- github.com/nccgroup/ScoutSuite — Multi-cloud auditing tool
- github.com/trufflesecurity/trufflehog — Secrets detection (repos, configs, cloud)



30

HARDENING

- www.cisecurity.org/benchmark/google_cloud_computing_platform/
- www.cisecurity.org/benchmark/azure/
- www.cisecurity.org/benchmark/amazon_web_services/
- docs.github.com/en/code-security/secret-security/configuring-secret-scanning-for-your-repositories
- github.com/RhinoSecurityLabs/cloudgoat

31

DETECTION & RESPONSE

- Enable immutable logging (CloudTrail, Azure Activity, GCP Audit Logs)
- Ship logs to SIEM and set alerts for unusual API calls, role usage, and new instance creation
- maagsoft.com/how-to-use-wazuh-to-monitor-and-secure-your-cloud-infrastructure/
- Use CSPM for continuous posture checks and IaC scanning in CI/CD pipelines

Honeypots!!!

32

LET'S DO BETTER

1. Training with security controls in the cloud
2. Training with secrets management in the cloud

33

KEY TAKEAWAYS

- Common Sense – FTW!
 - *Stop overthinking*
- The Basics ← *Ding ding ding!*
 - *Stop the Fancy*
 - *Audit!*

Three things to do tomorrow:

1. Run a secrets scan on public repos and rotate any exposed keys
2. Audit IAM for wildcard permissions; enforce least privilege and role separation
3. Enable logging (CloudTrail/Activity Logs) and add basic alerts for new creds/role usage

34

infosec.exchange/@sashatheflamingo
@sashatheflamingo.bsky.social
sashatheflamingo.xyz !!!!!

Thank You!!

linkedin.com/in/katfitzgerald
github.com/rnbwkat/presents

infosec.exchange@rnbwkat
rnbwkat.bsky.social

