

# **Account Jumping, Post Infection Persistency & Lateral Movement in AWS**

**Dor Knafo**  
**Security Research Leader**

**Dan Amiga**  
**Co-Founder and CTO**



# CodeSpaces.com

is for sale!

**\$5k**  
est. value

## ***Want this Domain?***

We purchased this domain for a project that is currently on hold. If you wish to purchase this domain please let us know.



offer (\$)



full name



email




I'm not a robot



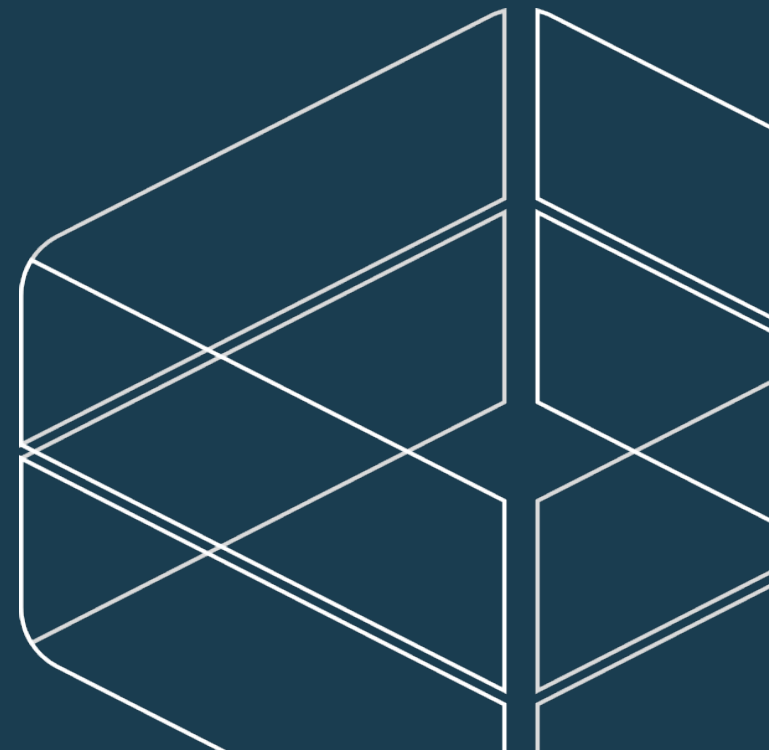
reCAPTCHA  
[Privacy](#) - [Terms](#)

***send***

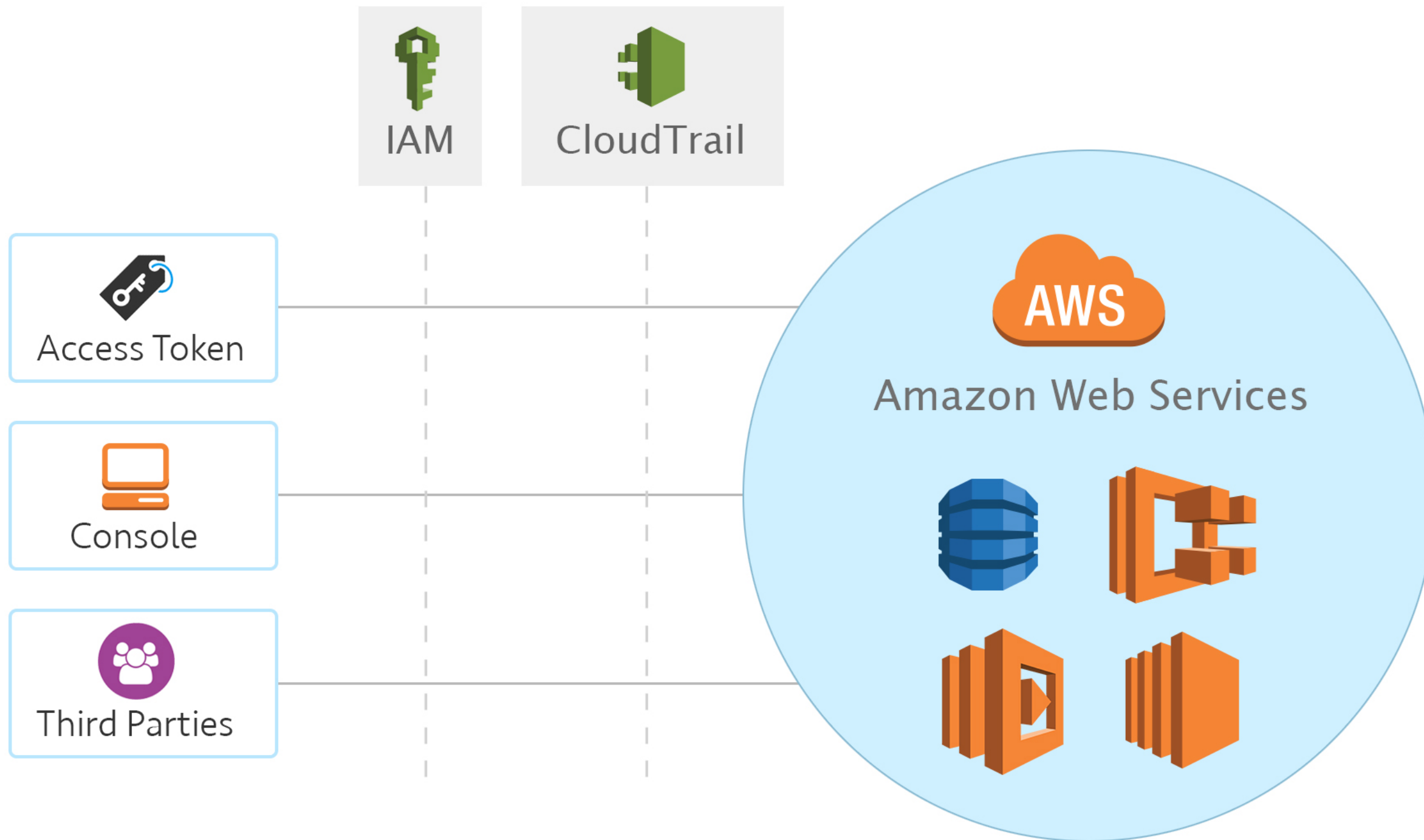
# Agenda

- Two minutes about AWS security
  - Infection
  - Survival + Persistency
  - Remaining Undetected
  - Lateral Movement
  - Solutions
- 

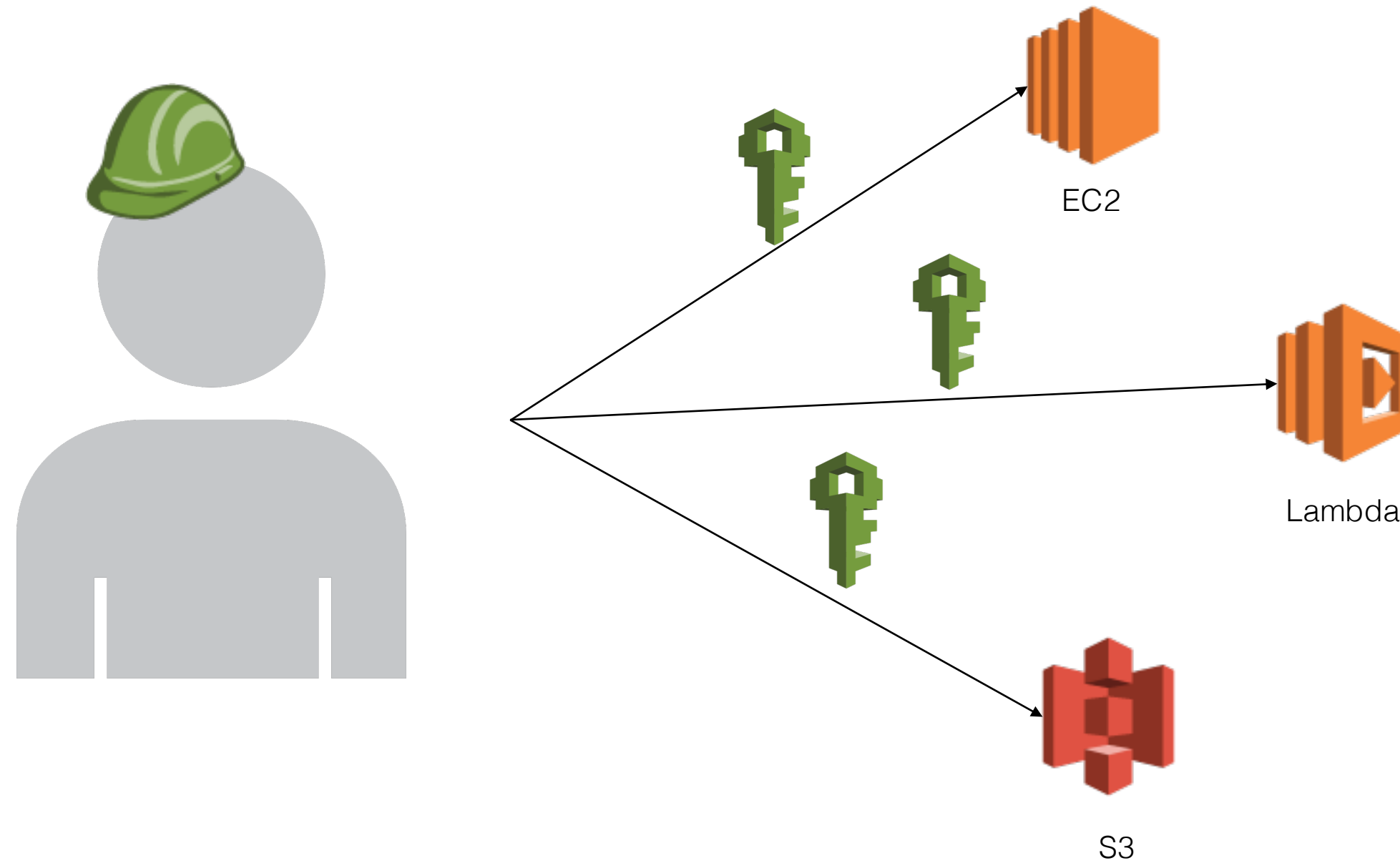
# QUICK INTRO



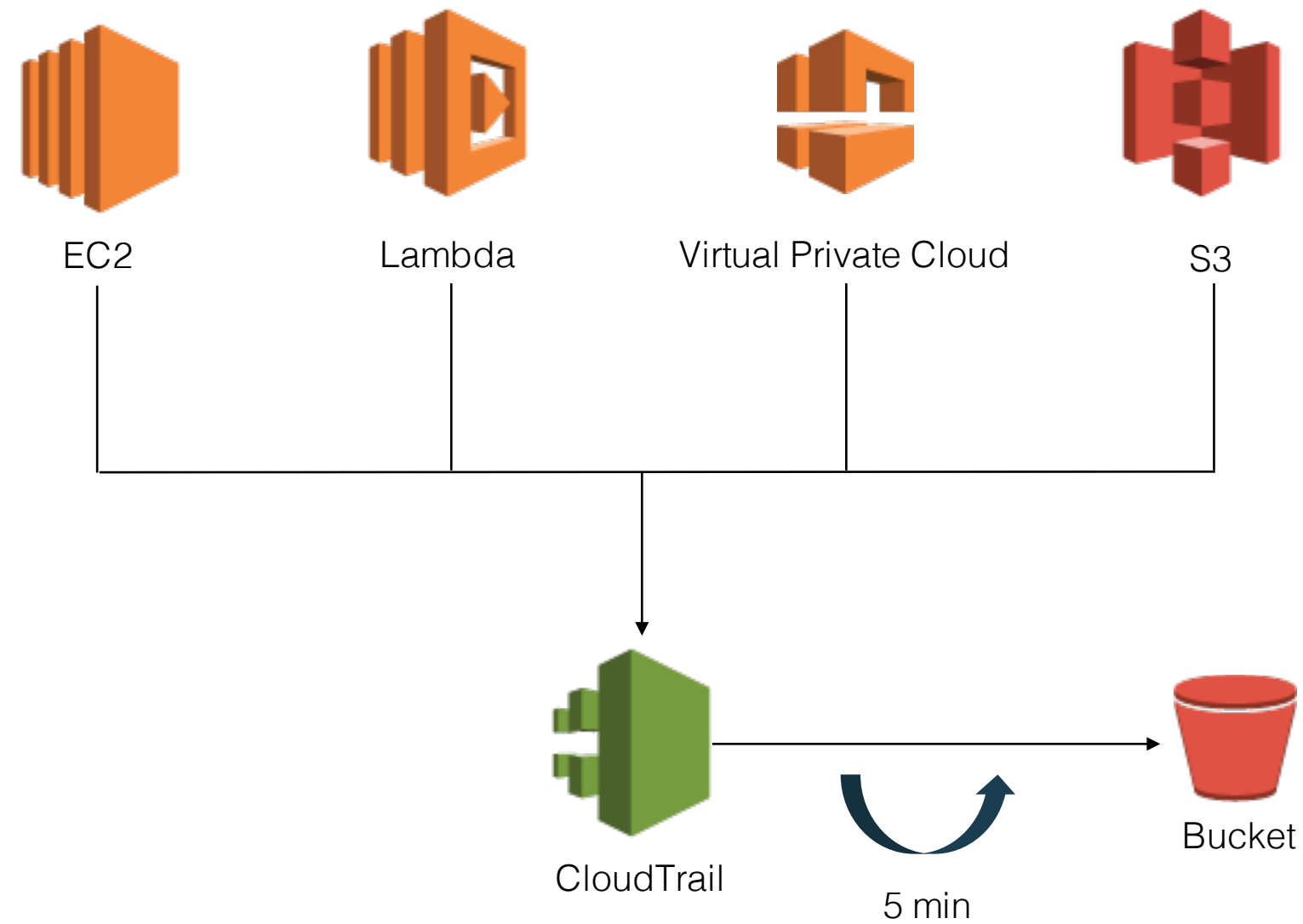
# AWS Infection Potential



# Identity and Access Management (IAM)



# AWS Primary Auditing Capability - CloudTrail



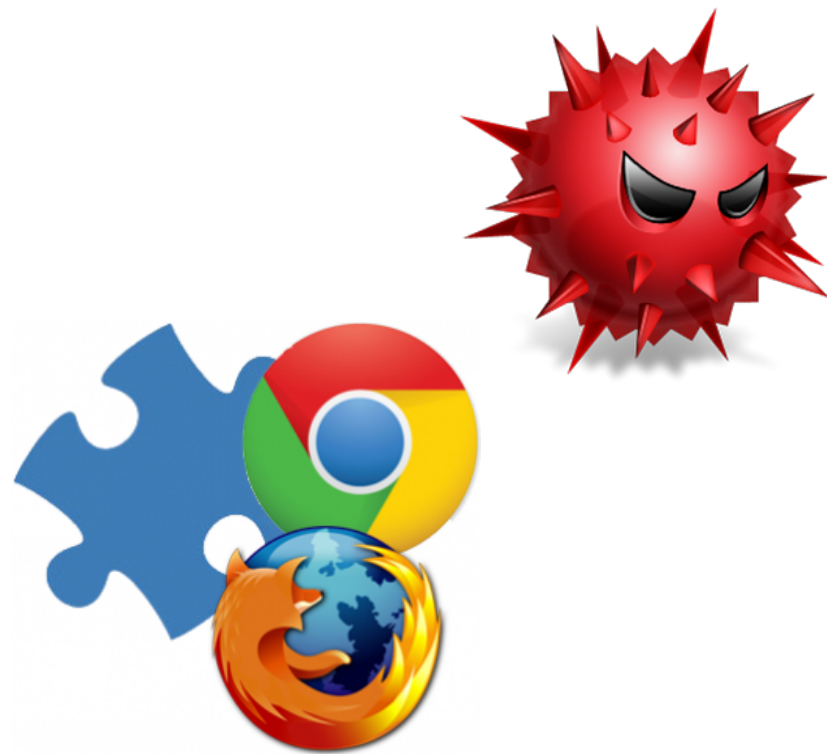
**'INFECTION**





# User Fault Infection

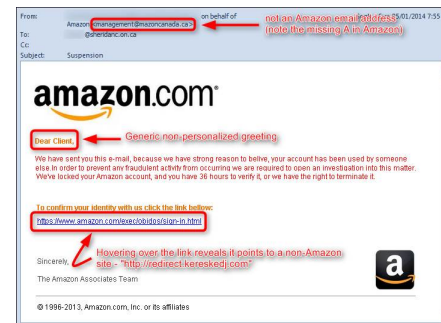
# Infected Machines



# Phishing



## AWS S3



## Source Repo

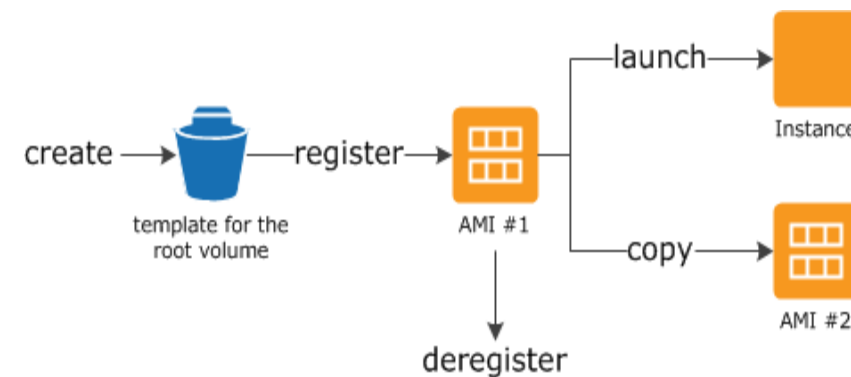


# Infection through AWS

## Cloud Metadata

```
$ curl http://169.254.169.254/latest/meta-data/  
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
hostname  
instance-action  
instance-id  
instance-type  
kernel-id  
local-hostname  
local-ipv4  
mac  
network/  
placement/  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups  
services/
```

## Poisoned AMI



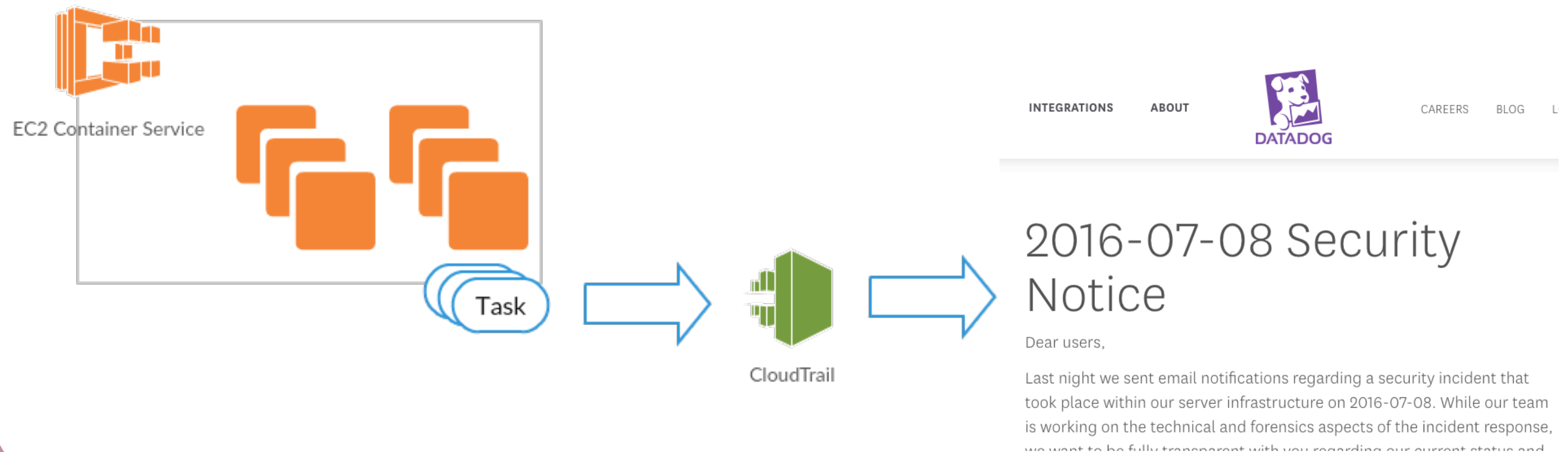
## Account Jumping

**Bulletin**

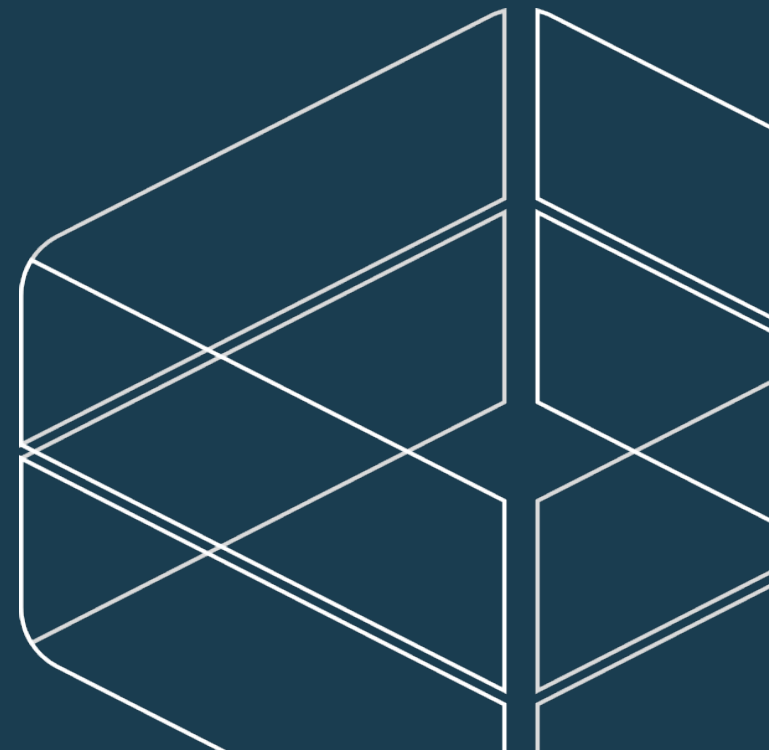


# Infection through 3<sup>rd</sup> party services

- AWS ECS task definition
  - API call to task definition is recorded via CloudTrail
  - Contains sensitive information (e.g. environment variables - keys)

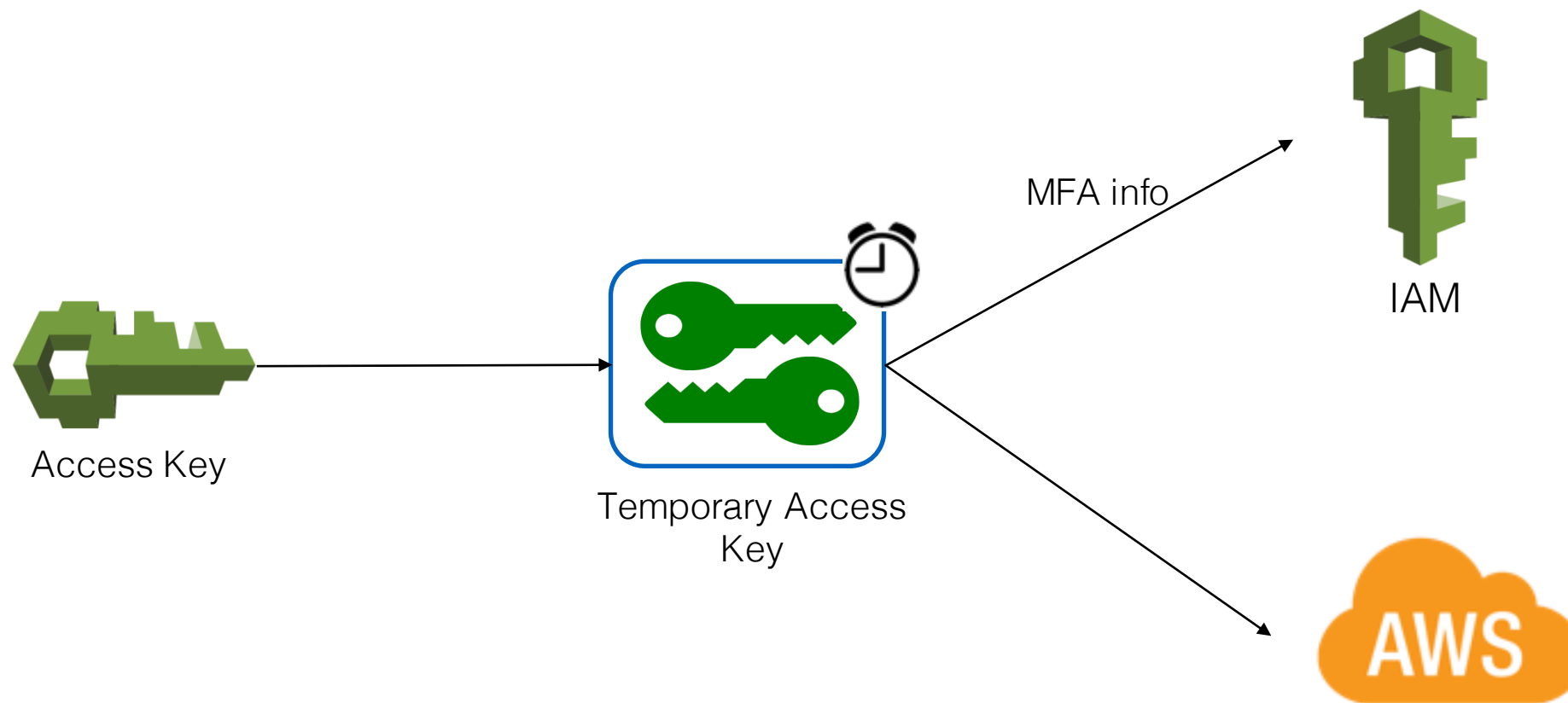


**SURVIVAL**



# Surviving key rotation or deletion

- AWS Security Token Service



## Actions

The following actions are supported:

- [AssumeRole](#)
- [AssumeRoleWithSAML](#)
- [AssumeRoleWithWebIdentity](#)
- [DecodeAuthorizationMessage](#)
- [GetCallerIdentity](#)
- [GetFederationToken](#)
- [GetSessionToken](#)

**DEMO**



~~HIDE~~



# Staying Undetected – Altering CloudTrail

- Delete the trails

```
$ aws cloudtrail delete-trail --name [trail-name]
```

- Stop the trails

```
$ aws cloudtrail stop-logging --name [trail-name]
```

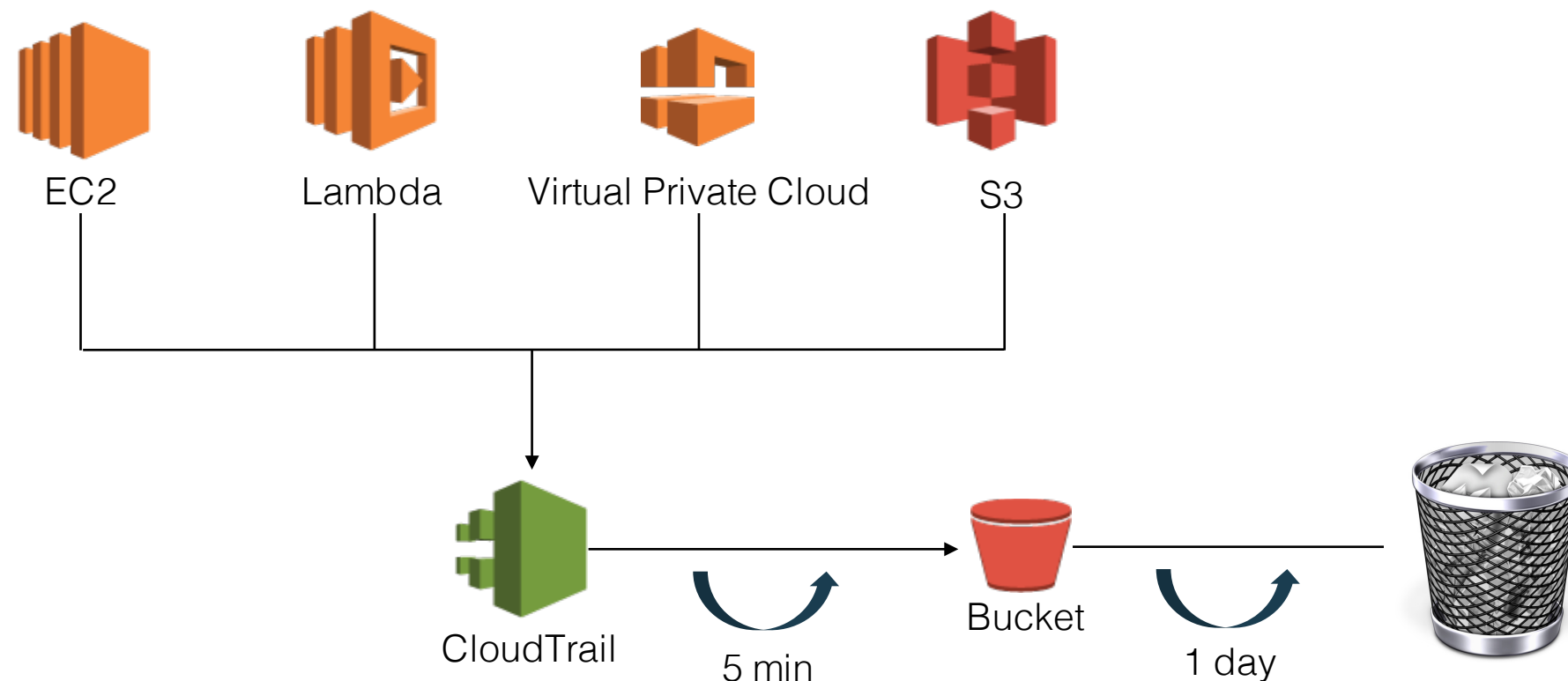
- Disable multi-region logging

```
$ aws cloudtrail update-trail --name [trail-name]  
--no-is-multi-region --no-include-global-services
```



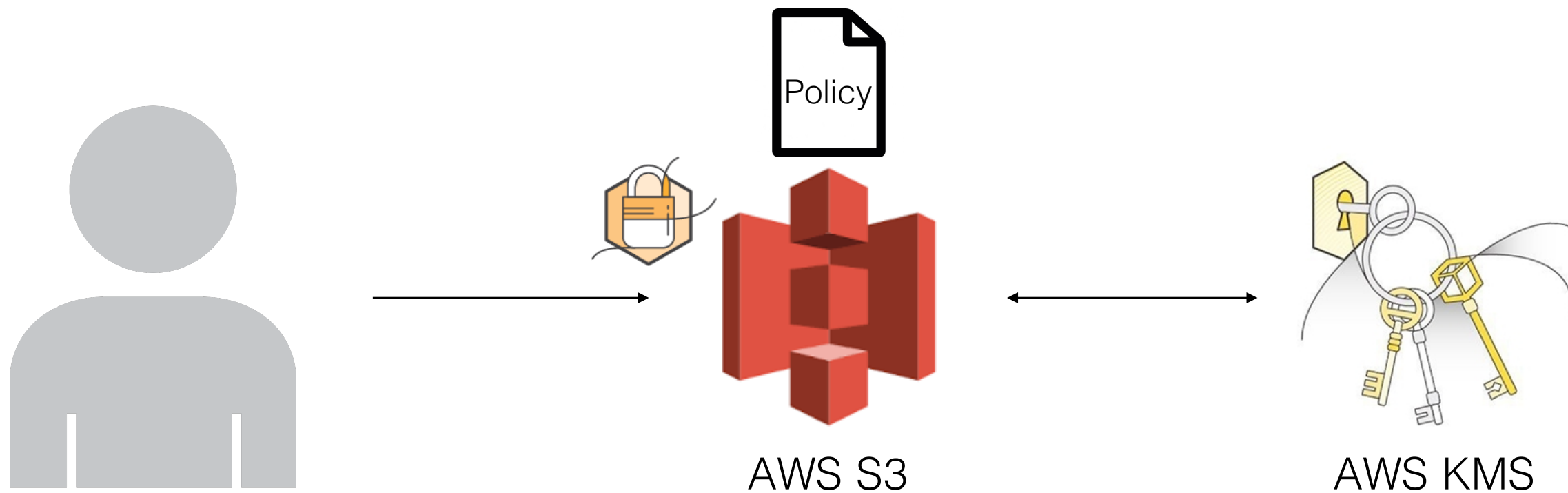
# Staying Undetected – Altering S3 Trail

- S3 lifecycle retention policy
- AWS Lambda
  - Triggers on every new file in the bucket
  - The Lambda free tier includes 1M free requests per month



# Staying Undetected

- AWS Key Management Service
  - Integrated with CloudTrail
  - S3's Server Side Encryption (SSE)

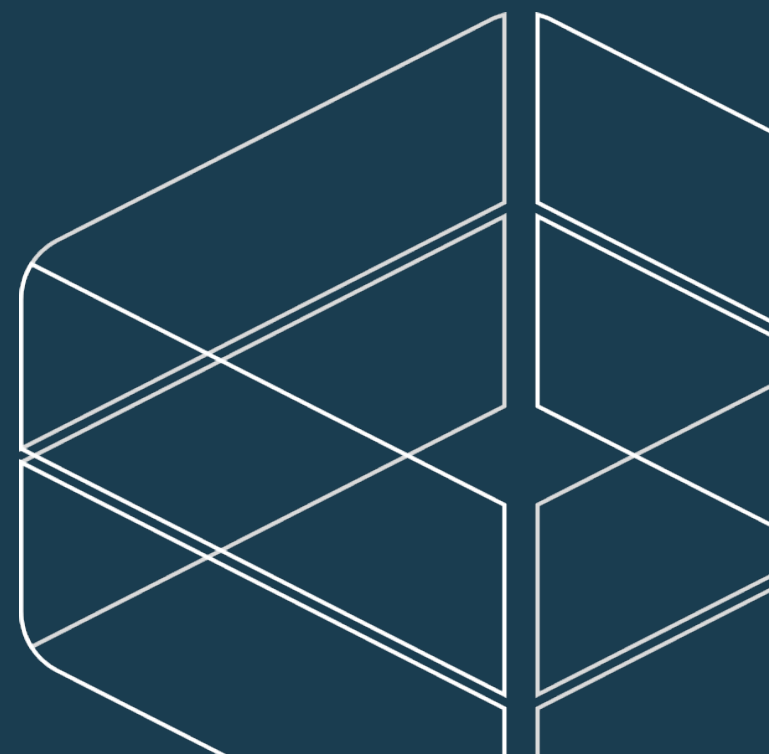


**DEMO**





# PERSISTENCY



# Persistence

- Create new users (typosquatting for extra stealth)

```
$ aws iam create-user --user-name [username]
```

```
$ aws iam create-access-key --user-name [username]
```

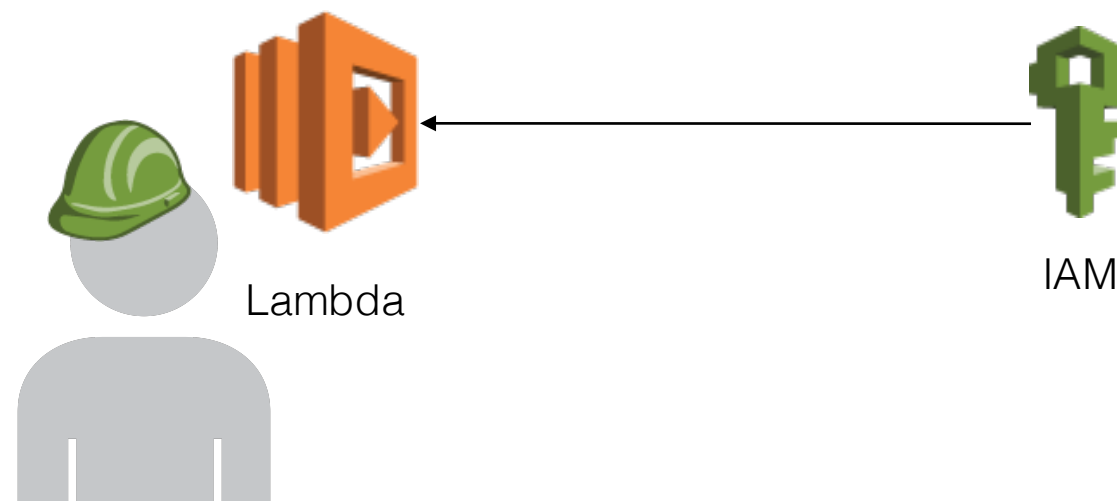
- Or – Iterate existings users and create a second access token

# Persistence

- Creating a second access key to existing users is not enough
- AWS Lambda saves the day, again!
- Create an access key on newly created users, and post it back to you

# Persistence

- Backdoor existing roles
- Use your newly retained tokens to assume the modified roles.
- Create a lambda that responds to role creation and adds a backdoor
- Register to UpdateAssumeRolePolicy to reintroduce backdoors that are removed.

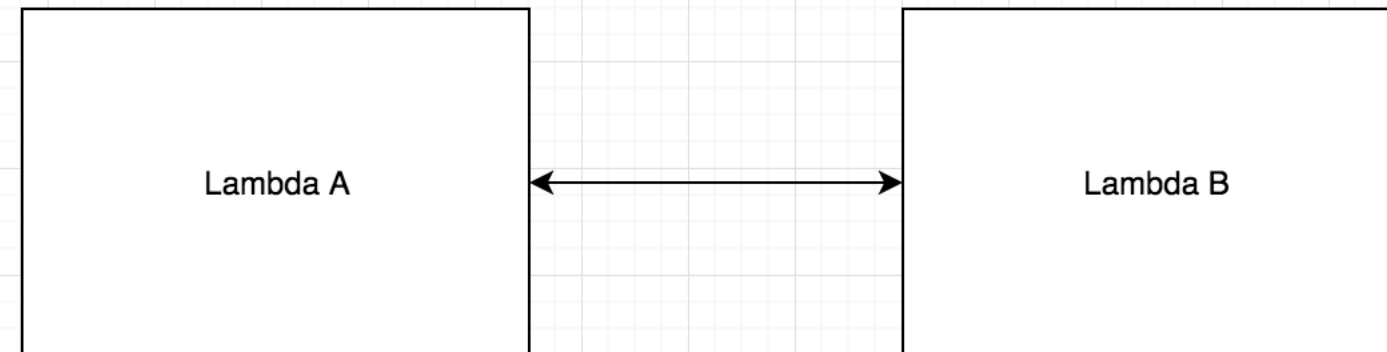


# AWS Lambda Persistency

## Synopsis

---

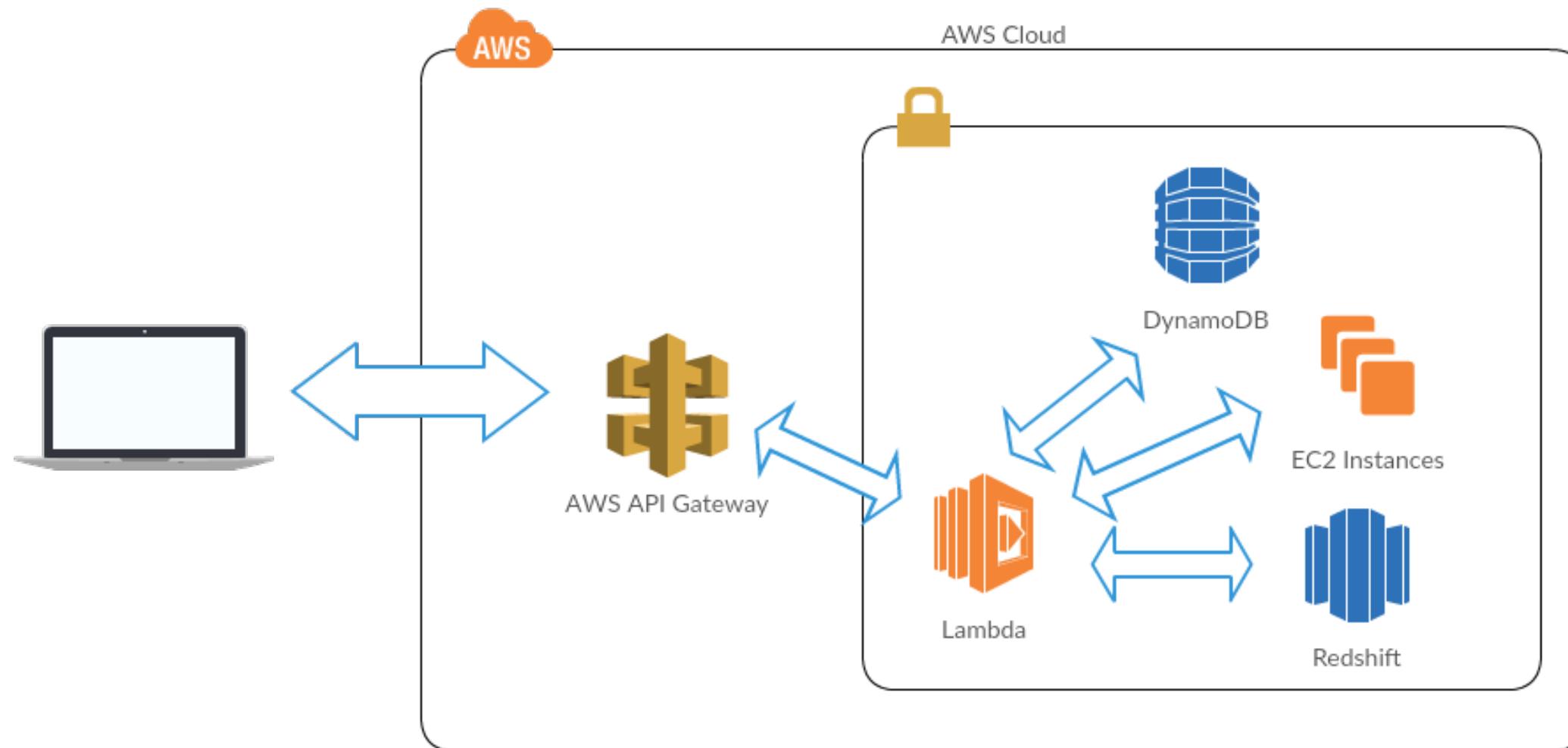
```
delete-function  
--function-name <value>  
[--qualifier <value>]  
[--cli-input-ison <value>]  
[--generate-
```





# VPC Access Persistency

- Virtual Private Cloud (+ Security Group)
- Use a public endpoint and Lambda to bypass the security group
- SQS, AWS Gateway API, AWS S3 (with VPC endpoint)



# LATERAL MOVEMENT



# SUMMARY



# Lateral Movement

- Direct Connect
- IAM
- Amazon support tickets
- S3



DynamoDB



IAM



Direct Connect



EC2



Lambda



Virtual Private Cloud



S3



SQS



Elastic cache



Route53



Beanstalk

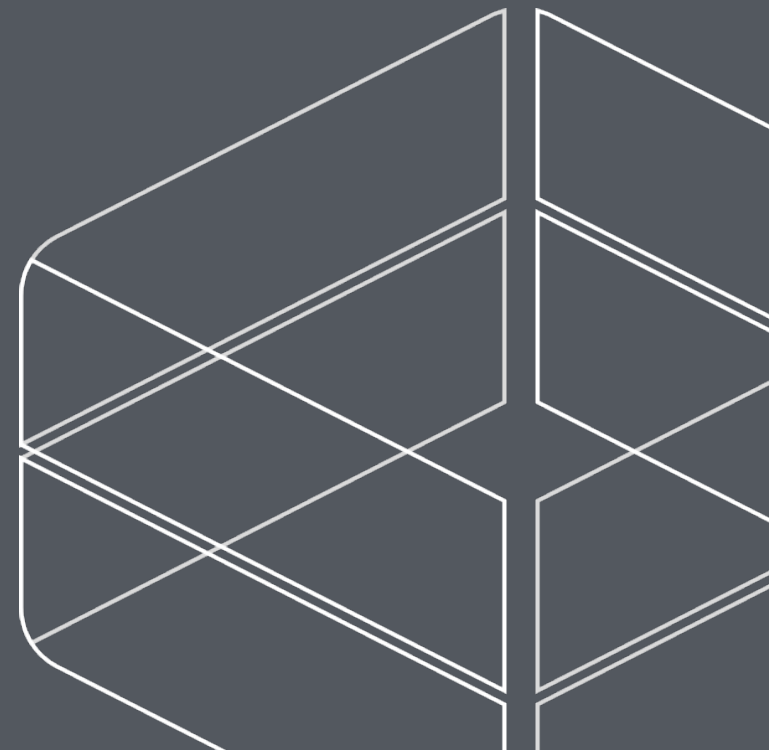


AMI

# Solutions

- Details...
- Stateless architecture with focus on data protection
- Automation via code, CloudFormation, Dockers, etc. for environment recreated from scratch
- Leverage strong account separation (dev, production1, production2)

**Q&A**



# **Account Jumping, Post infection persistency & Lateral Movement in AWS**

**Dor Knafo**  
**Security Research Leader – [Dor@fire.glass](mailto:Dor@fire.glass)**

**Dan Amiga**  
**Co-Founder and CTO - [Dan@fire.glass](mailto:Dan@fire.glass)**

