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

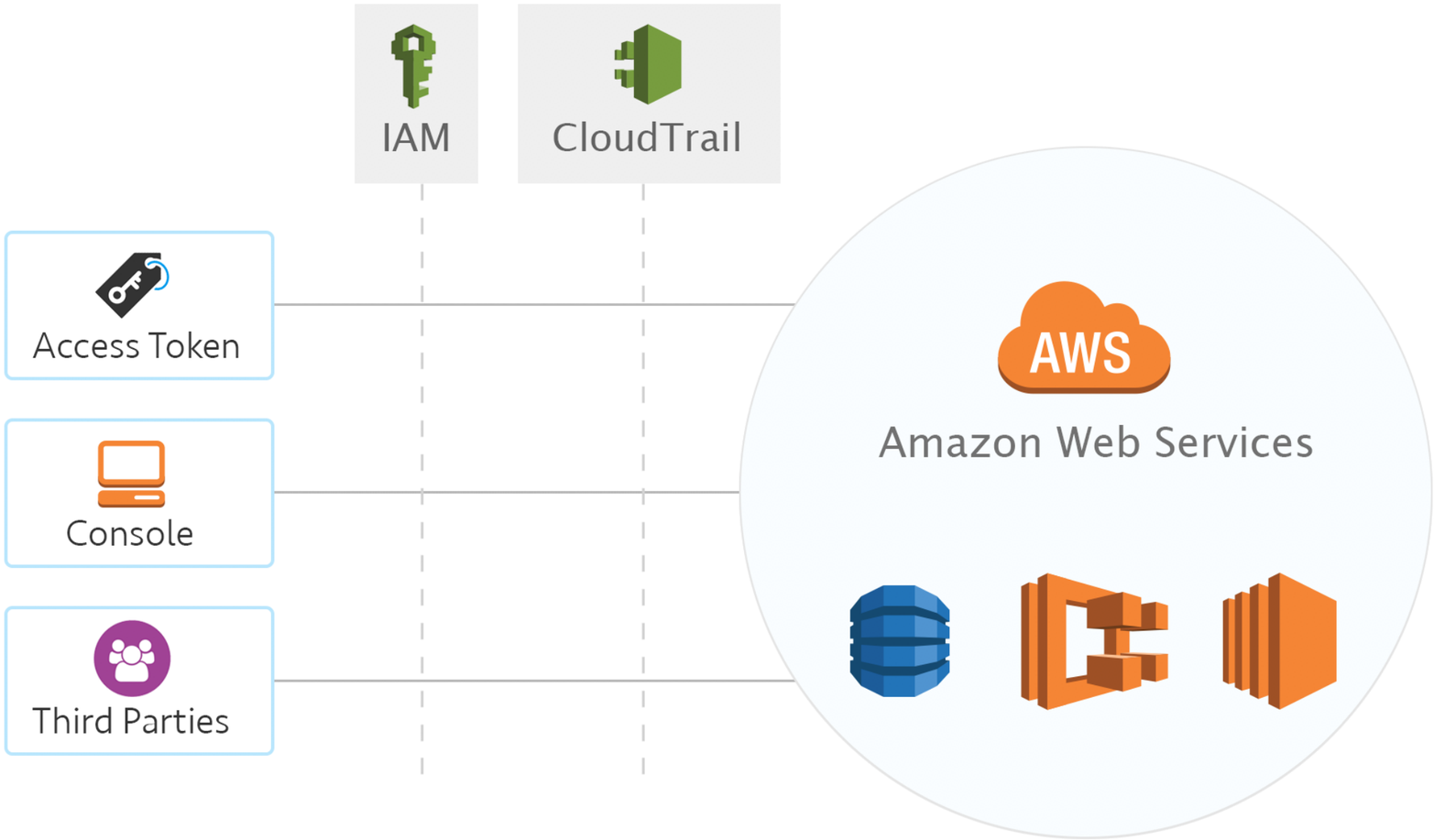
send

fireglass

Agenda

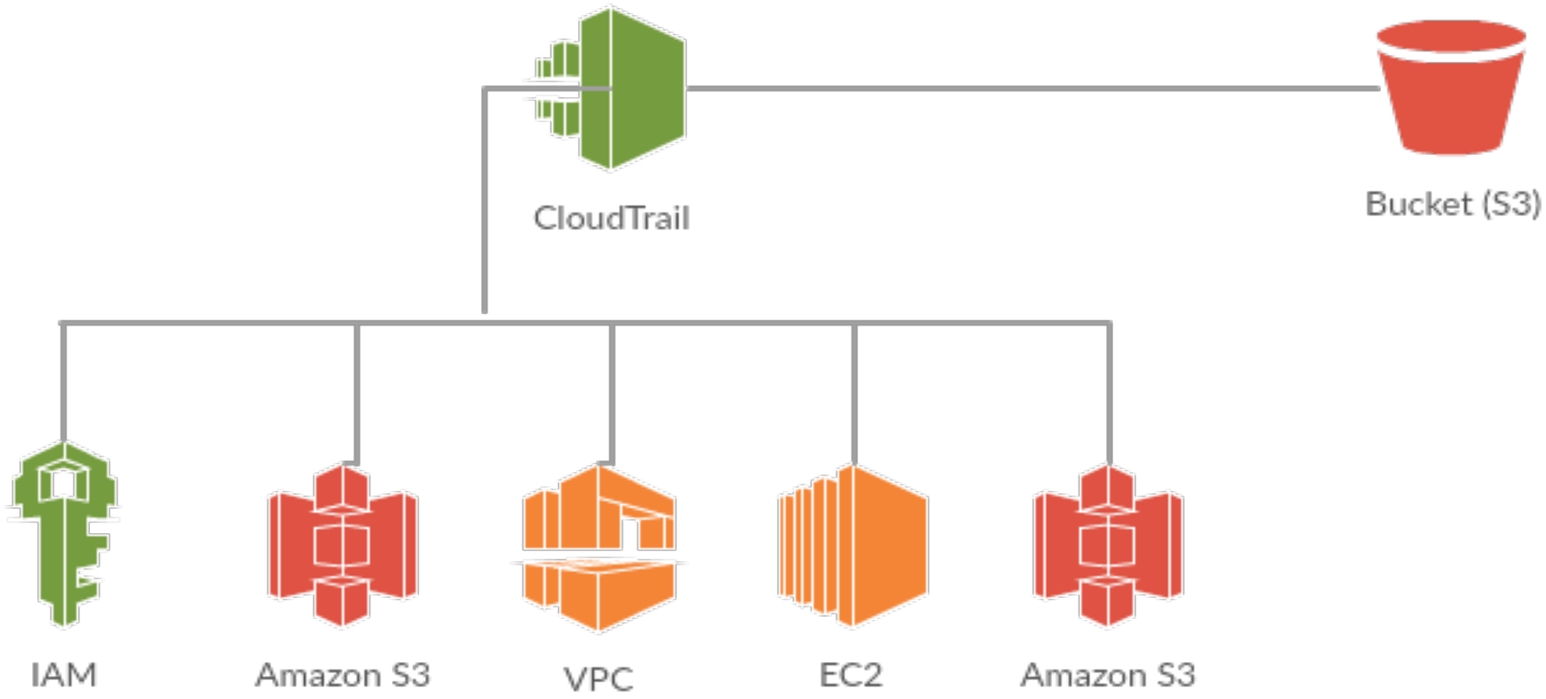
- Infection
- Staying Undetected
- Lateral Movement
- Persistency
- Solutions

AWS Infection Potential



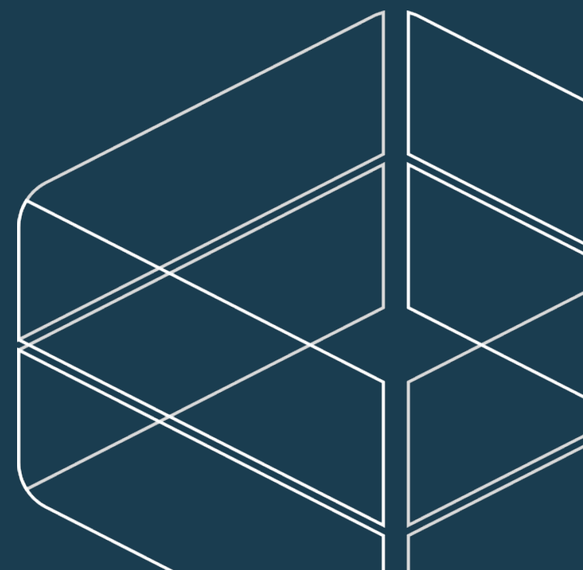
fireglass

AWS CloudTrail



fireglass

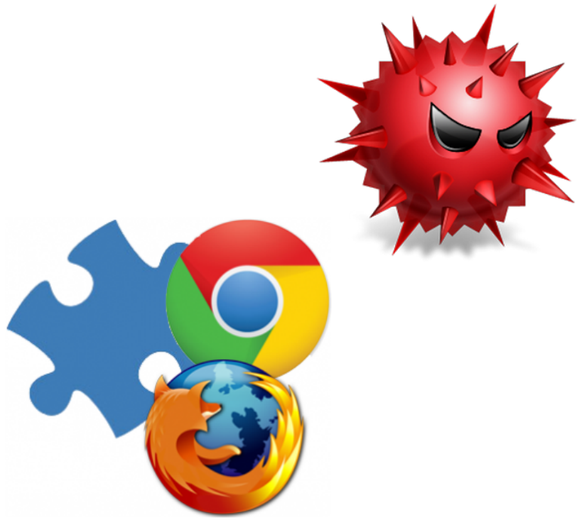
'NFECTION



fireglass

User Fault Infection

Infected machines



Phishing

AWS S3

Source Repo

GitHub

Bitbucket

fireglass

Infection through 3rd party services

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

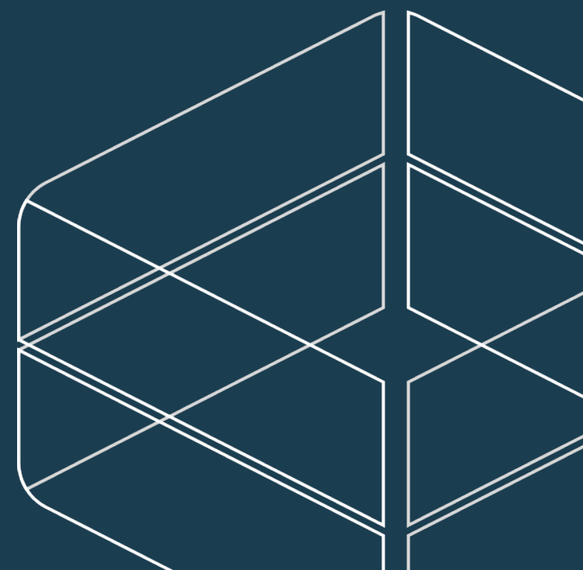
fireglass

Infection through AWS

- Cloud Metadata
  - Not only AWS
- Poisoned AMI
- Account leftovers – “Account Jumping”

fireglass

SURVIVAL



fireglass

Surviving key rotation or deletion

- AWS Session Token Services
  - You cannot call any IAM APIs unless MFA authentication information is included in the request.
  - You cannot call any STS API *except* AssumeRole.

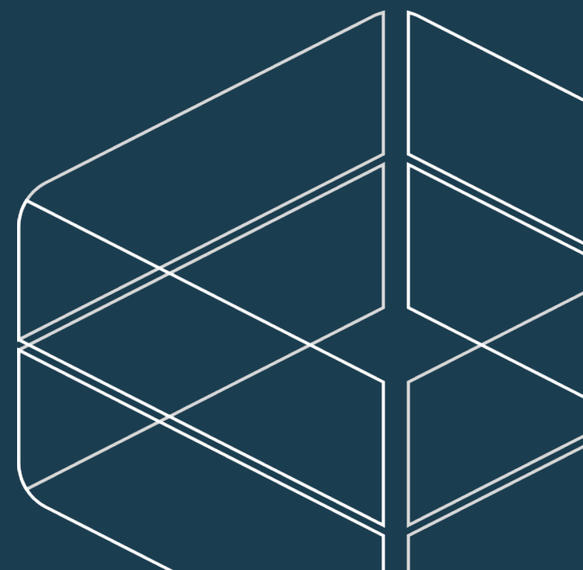
Actions

The following actions are supported:

- AssumeRole
- AssumeRoleWithSAML
- AssumeRoleWithWebIdentity
- DecodeAuthorizationMessage
- GetCallerIdentity
- GetFederationToken
- GetSessionToken

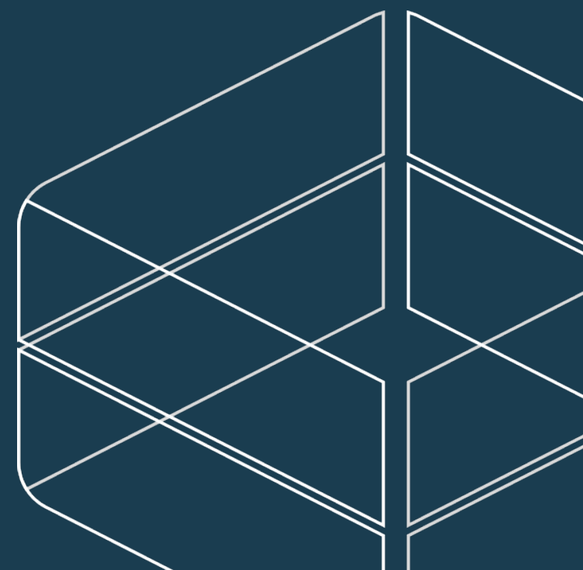
fireglass

DEMO



fireglass

HIDE



fireglass

Staying Undetected

- The obvious way to do it
  - Delete the trails

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

  - Stop the trails

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

fireglass

Staying Undetected

- Disable Multi region logging
  - On the same time disable global services logging (IAM)

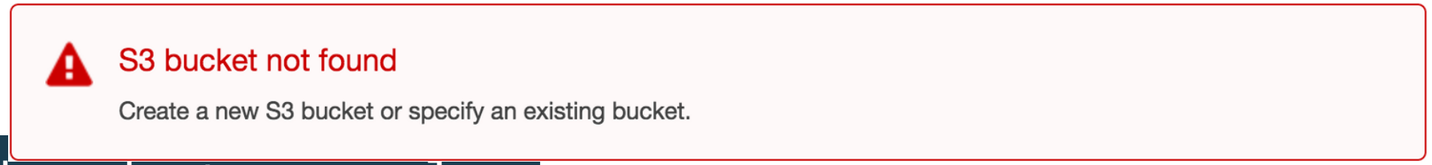
```
$ aws cloudtrail update-trail –name [trail-name]
--no-is-multi-region –no-include-global-services
```

fireglass

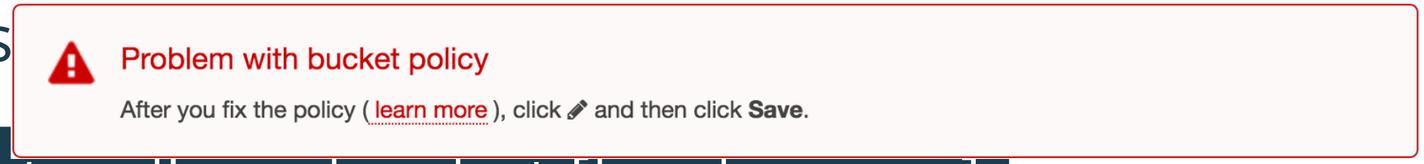
Staying Undetected

- Move your efforts to S3
  - Delete the bucket

```
$ aws s3 rb –force [bucket-name]
```



  - Revoke CloudTrails acces




```
$ aws s3api put-bucket-policy --bucket [buck-name]
–policy [file://miodified-policy.json]
```

fireglass

Staying Undetected

- Move your efforts to S3
  - AWS Lambda
  - Trigger on every new file in the bucket
  - Wins (almost) every race

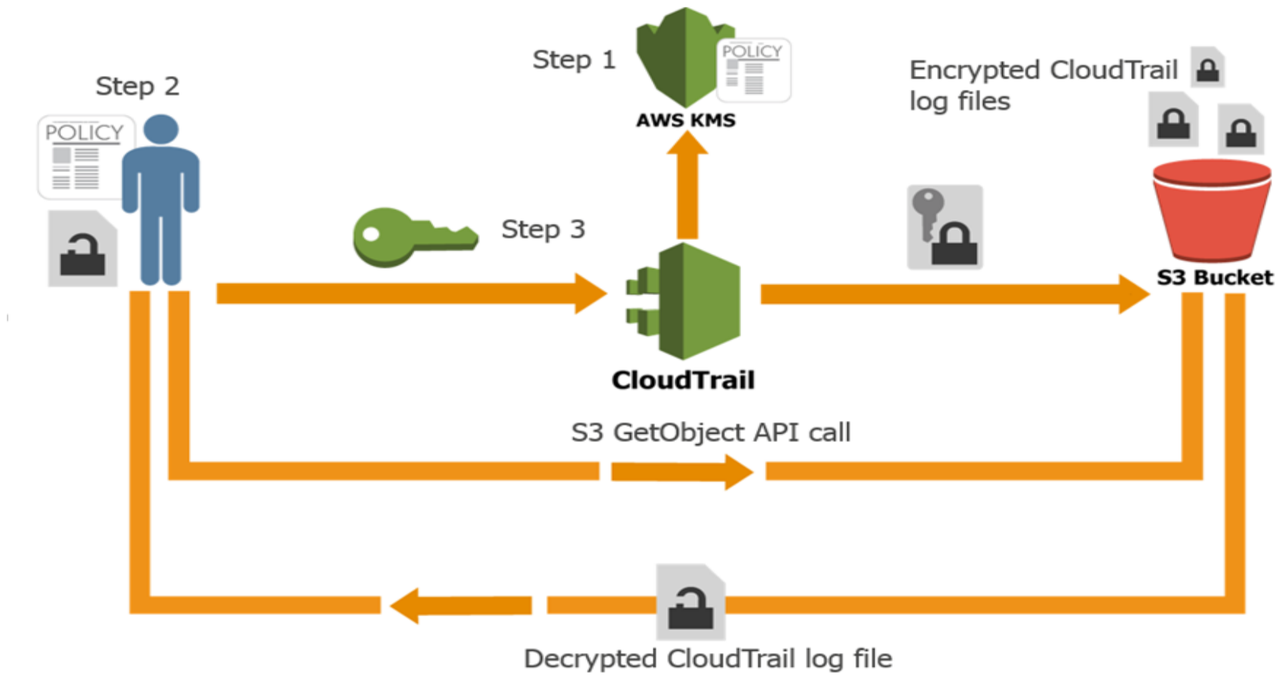
Free Tier

The Lambda free tier includes 1M free requests per month and 400,000 GB-seconds of compute time per month.

  - 1 Month, 44640 minutes, 8928 Lambda invocations in total.
  - Less than 0.01% of the free tier

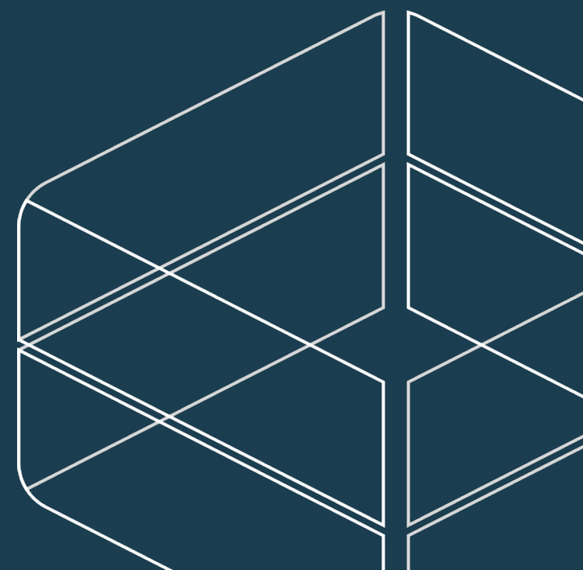
Staying Undetected

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



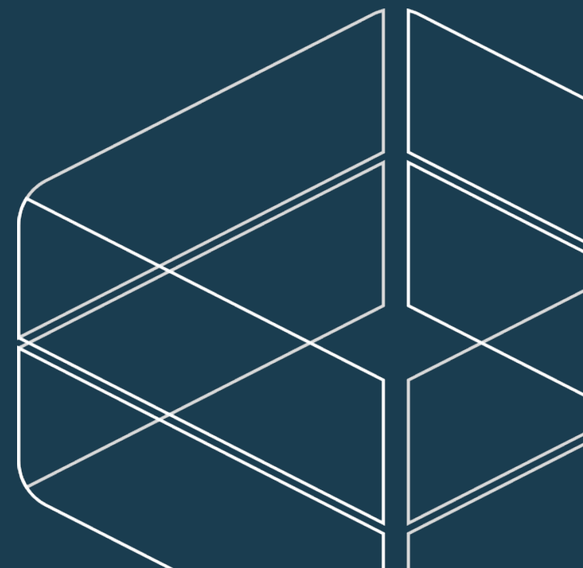
fireglass

DEMO



fireglass

LATERL
MOVEMENT



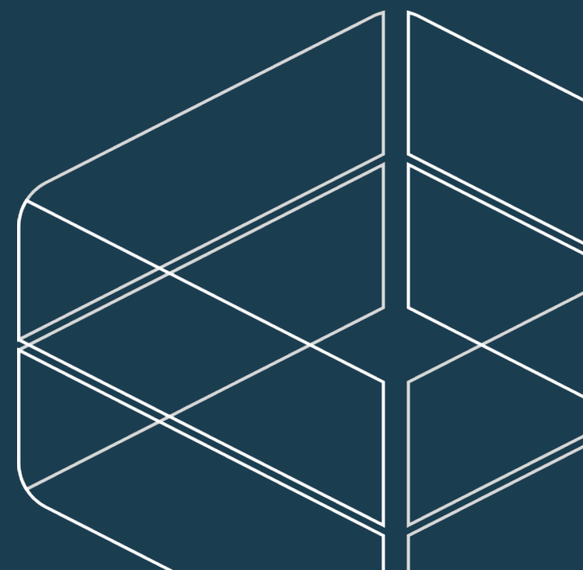
fireglass

Explore the infected environment

- Direct Connect
- IAM
- Amazon support tickets
- S3

fireglass

PERSISTENCY



fireglass

Persistency

- Create new users (typosquatting for extra stealth)

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

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

- In response you'll recive an access key ID and a secret access key
- Up to two access tokens per user

fireglass

Persistency

- Creating a second access key is risky
- AWS Lambda, again!
- Create a second access key on newly created users, and post it back to you

fireglass

Persistency

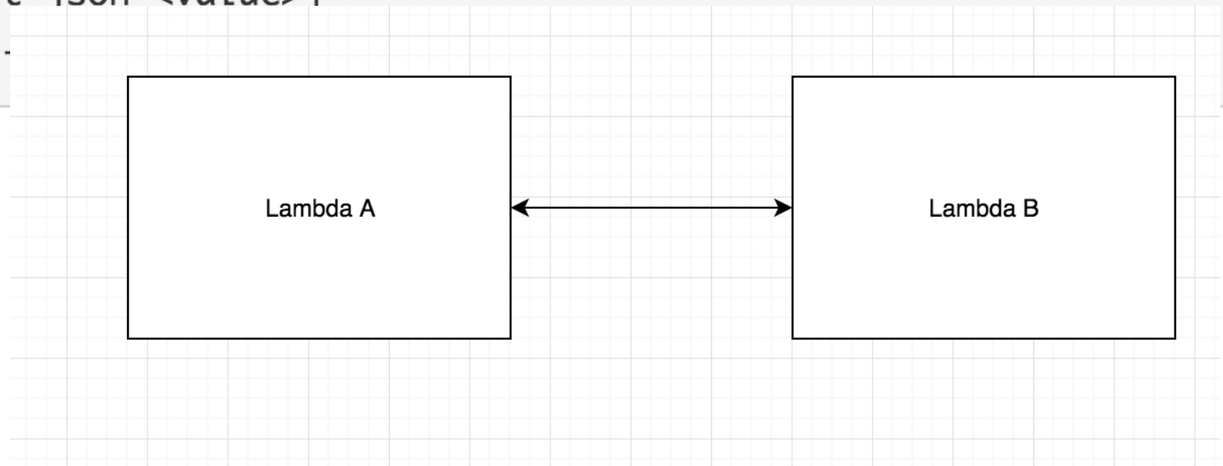
- Backdoor with new roles
- Use your new low privledge tokens to assume the new roles.
- Create a lambda that responds to role creation and adds a backdoor
- Register to UpdateAssumeRolePolicy to reintroduce backdoors that are removed.

fireglass

Persistency

Synopsis

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



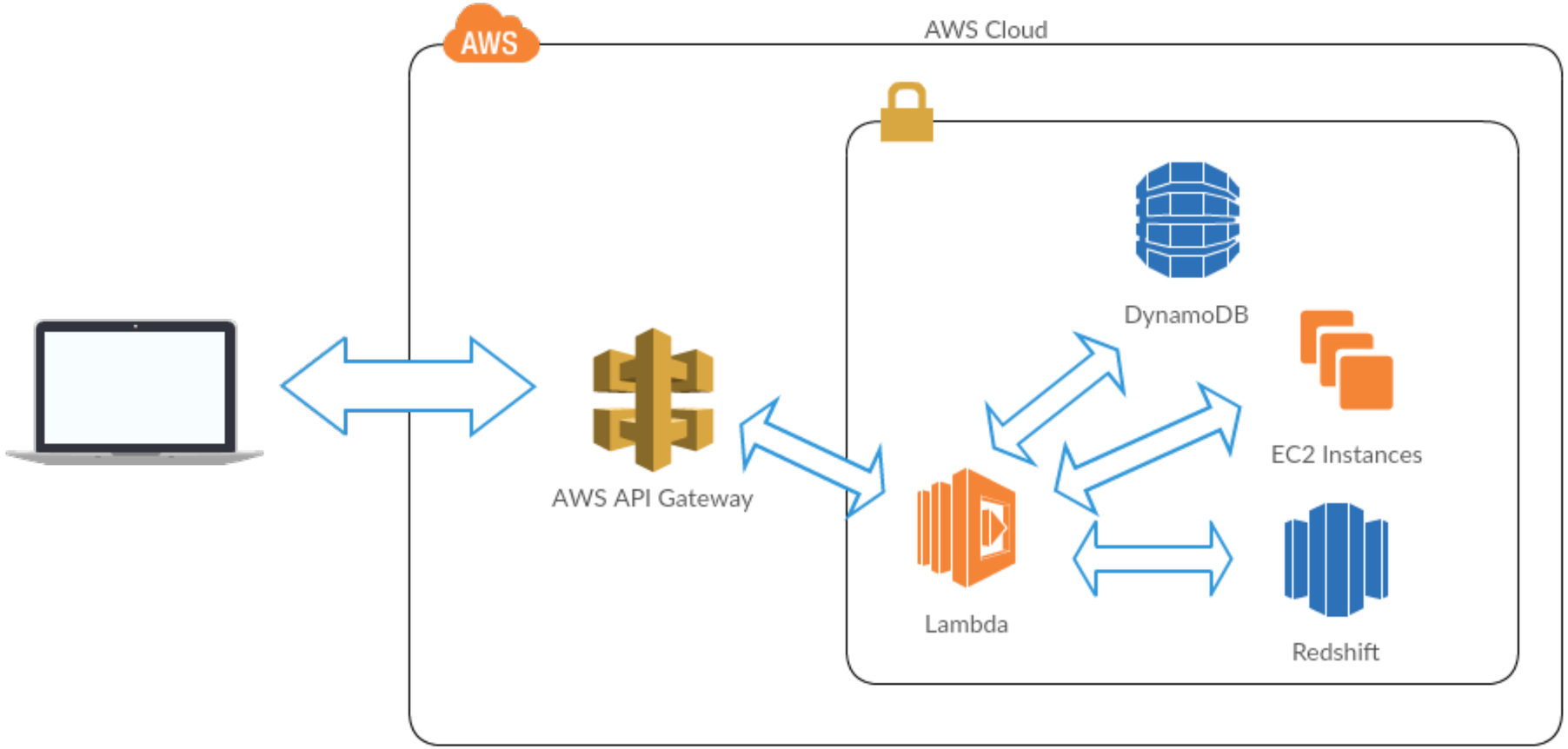
fireglass

Persistency

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

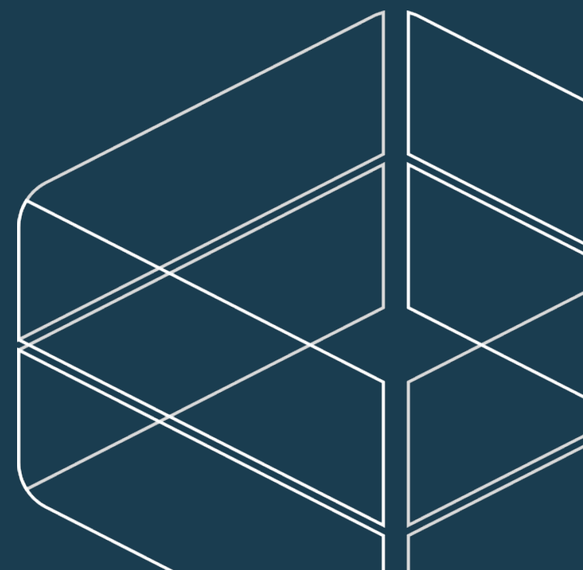
fireglass

Persistency



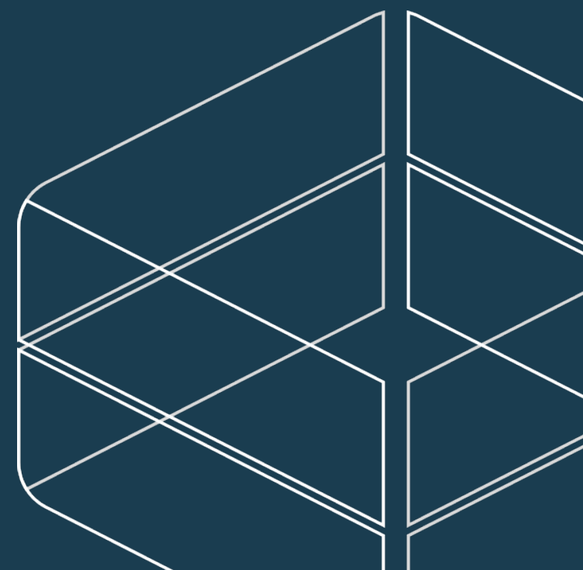
fireglass

DEMO



fireglass

SOLUTIONS



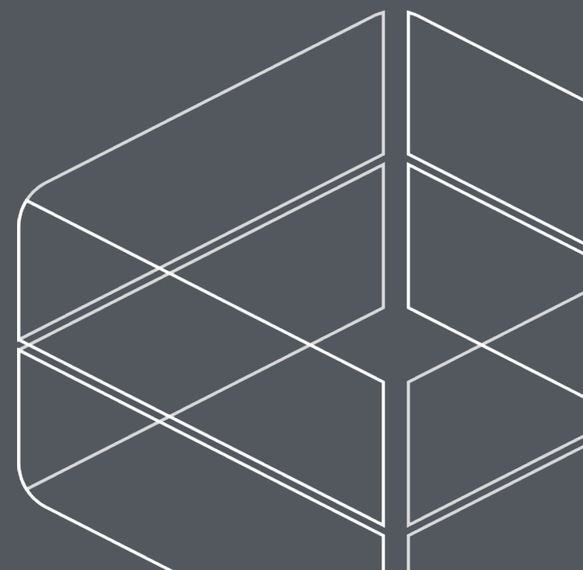
fireglass

Solutions

- Awareness & Develop unique skillset for your environment
- Stateless Architecture with focus on data protection
- Leverage strong account separation (dev, production1, production2)
- CASB solutions will mature into dedicated PaaS/IaaS offering
- Automation via code, CloudFormation, Dockers, etc. for environment recreated from scratch

fireglass

Q&A



Account Jumping, Post infection persistency & Lateral Movement in AWS

Dor Knafo
Security Research Leader

Dan Amiga
Co-Founder and CTO