ATTACKS AS A SERVICE WITH

The DeRF

Kat Traxler

- Principal Security Researcher
- SANS SEC549 Cloud Security Architecture Lead Author
- IANS Faculty
- Google Cloud Security Enthusiast

Agenda

The REWIND

- Existing Tooling Overview
- Use Cases for a New Tool
- Decoupling Execution from Attack Creation

The DeRF

- Execute Attacks with Google Workflows
- DeRF Demo
- Attack Architecture
- Deployment with Terraform

The FUTURE

- DeRF Roadmap and Attack Customization

Yet Another Cloud Tool?

Stratus Red Team

PACU

MicroBurst
TOOLS.NETSPI.COM

SCOUTSUITE

prowler

WHY INVOKE AN ATTACK TECHNIQUE ?

Attack consumers need to self-service attack invocations in order to:

- Train: Invoke attack techniques to train detection algorithms.
- Code Coverage: Ensure are we executing our modules fully and they behave in predictable ways.
- Validate Controls: Continuously test restrictions in the environment

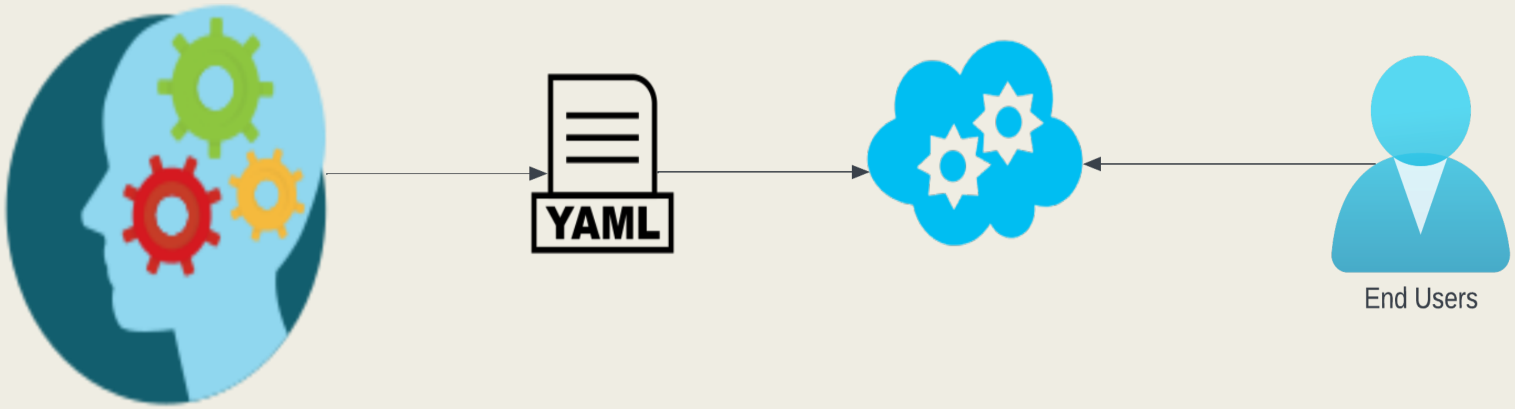
Democratizing Attack Execution

attack producers

Think of an attack technique

Codify the attack as code

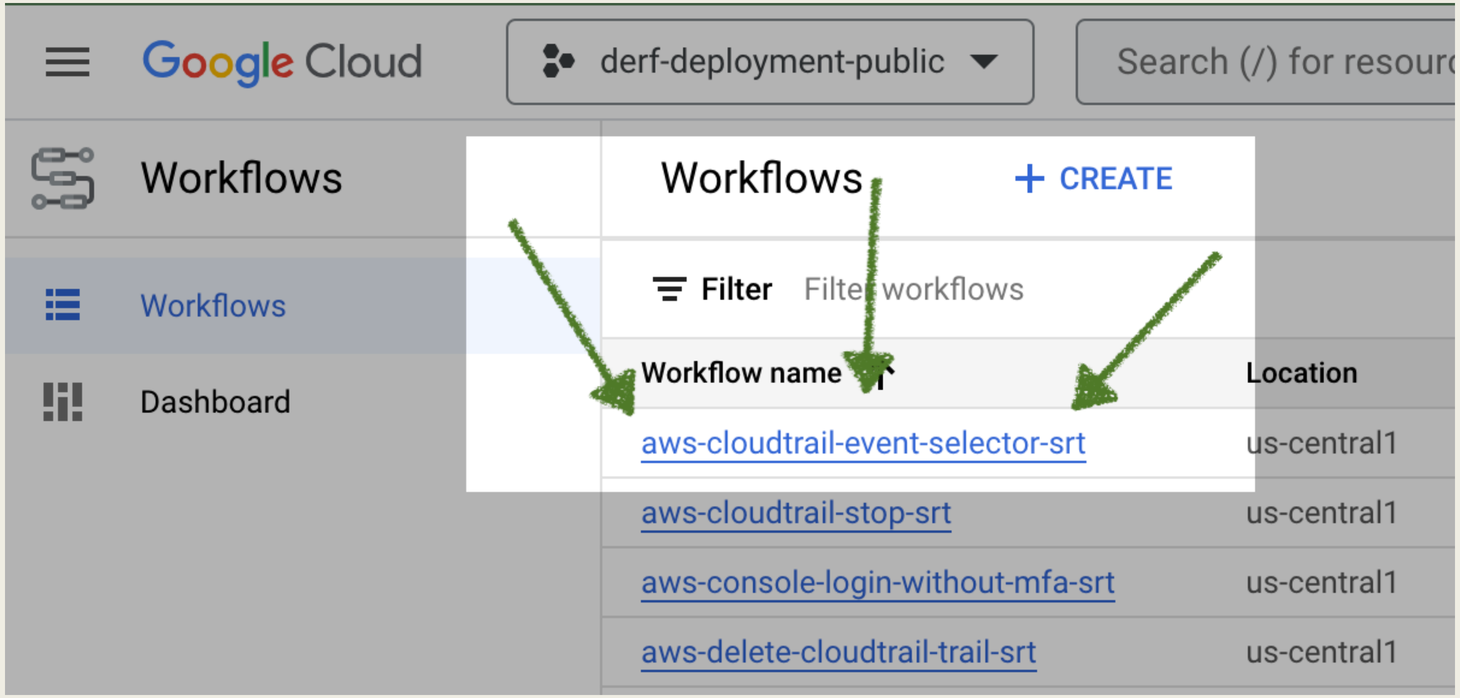
Publish attacks as executable code



Grant granular access to attack techniques

Excute attacks manually or programmatically at will

attack consumers



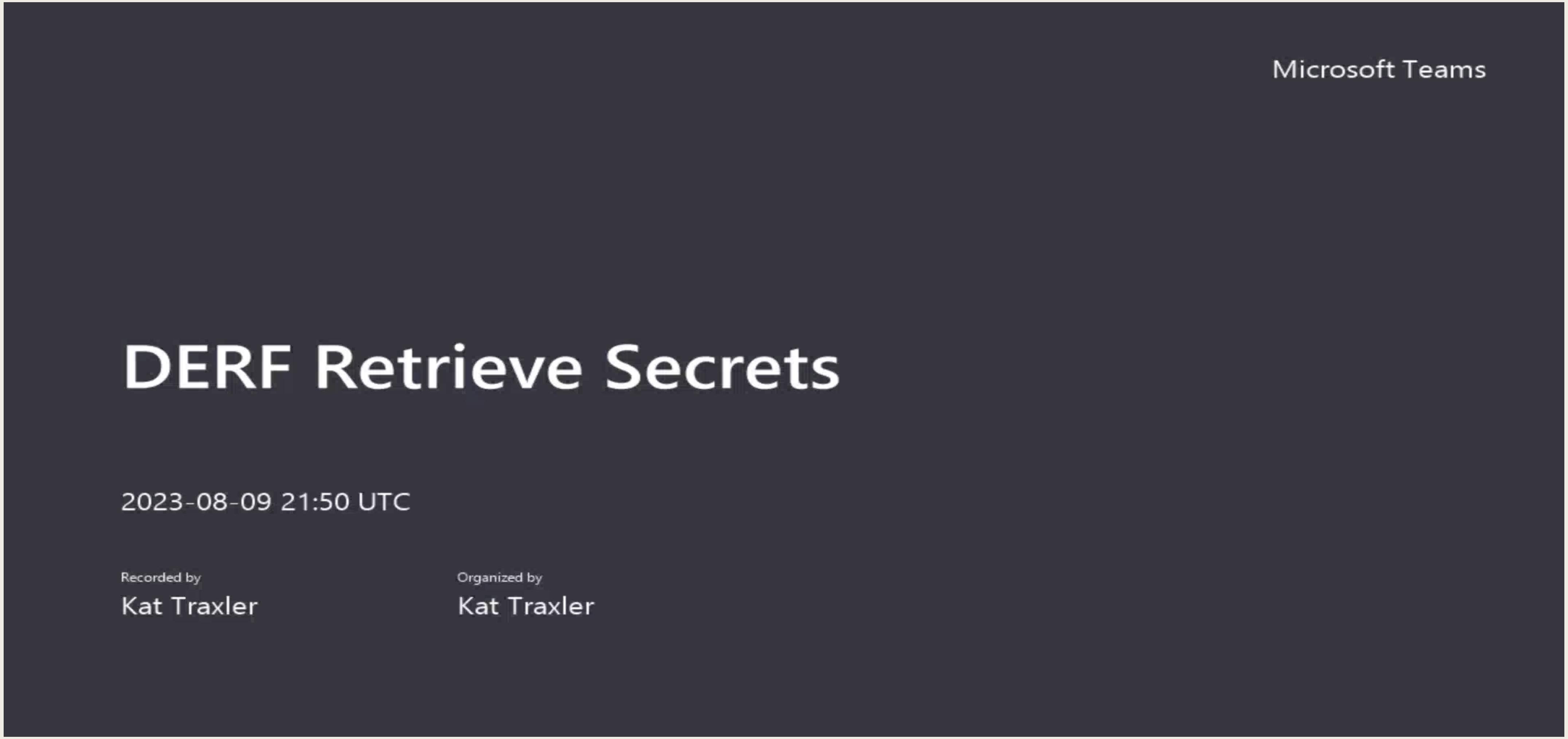
Workflow name	Location
aws-cloudtrail-event-selector-srt	us-central1
aws-cloudtrail-stop-srt	us-central1
aws-console-login-without-mfa-srt	us-central1
aws-delete-cloudtrail-trail-srt	us-central1

Executing Attack Techniques with Google Workflow

Attack execution is as easy as:

- Deploying The DeRF
- Pressing a button
- Or Calling a Google API

DeRF DEMO



Microsoft Teams

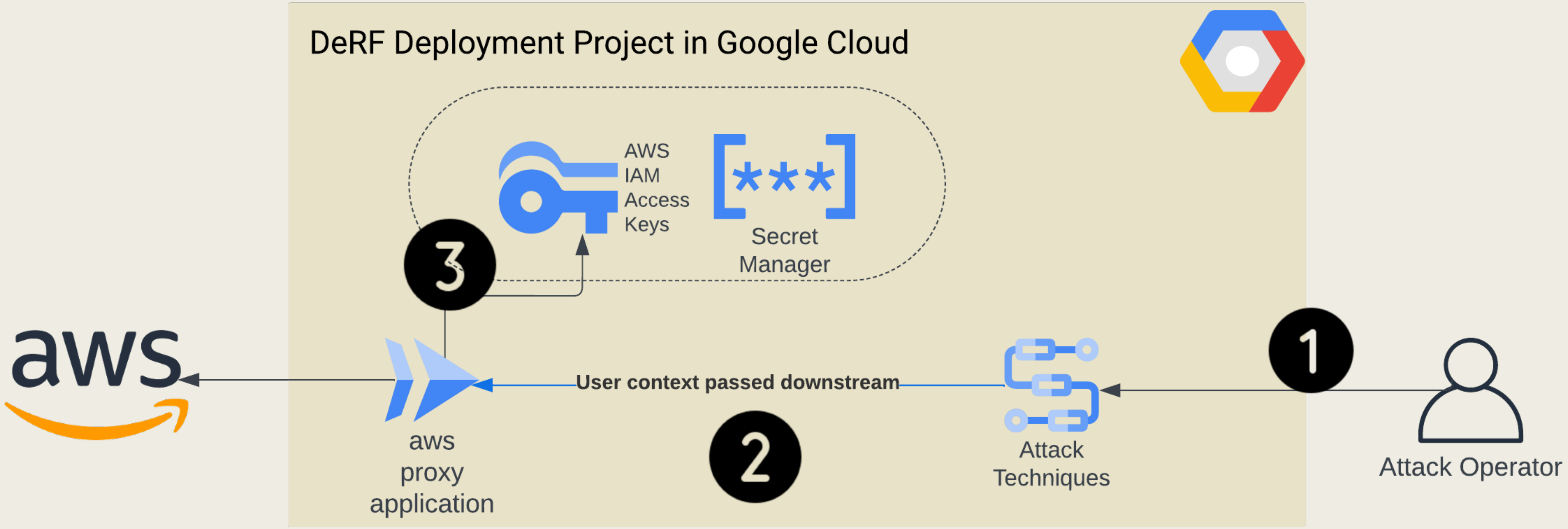
DERF Retrieve Secrets

2023-08-09 21:50 UTC

Recorded by
Kat Traxler

Organized by
Kat Traxler

Attacking AWS from GCP

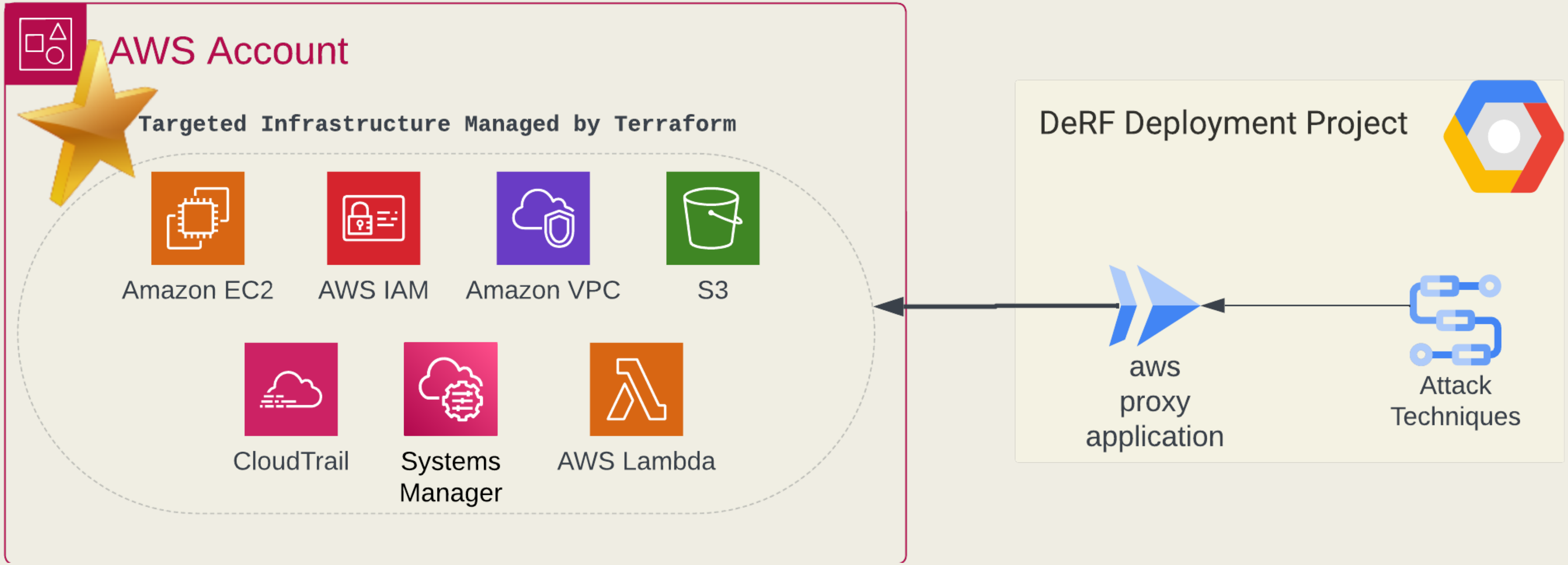


1. Operator invokes a Google Workflow

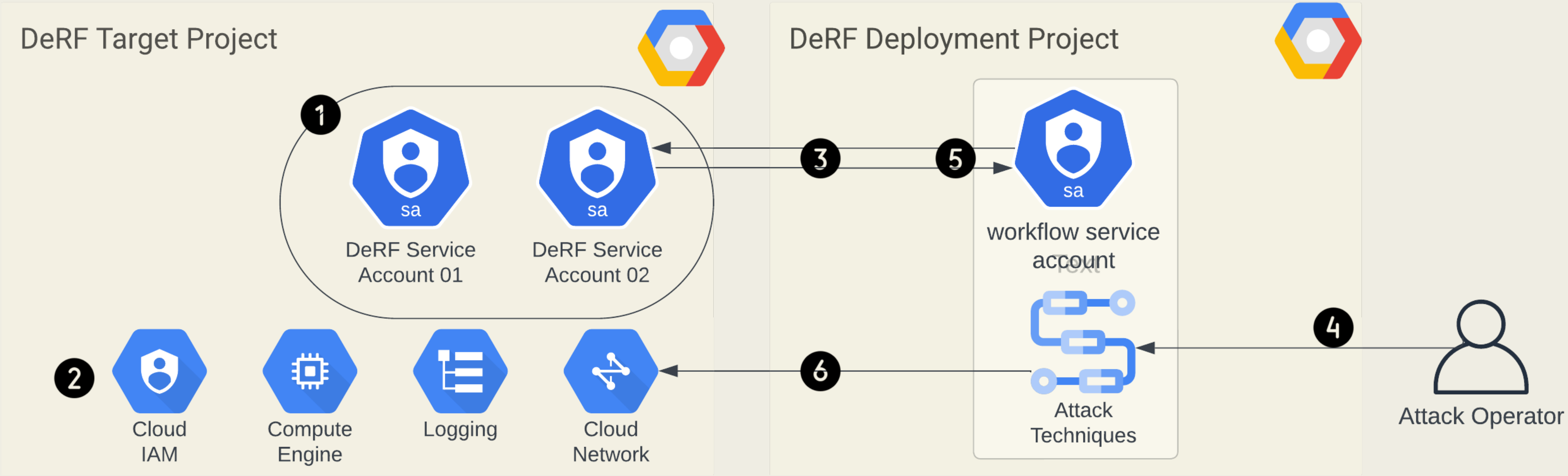
2. Details of HTTP request passed downstream to proxy application

3. Proxy application pulls relevant credentials for target AWS environment

Target Infrastructure in AWS



Targeting Google Cloud



1 *DeRF Attacker Service Accounts* are created in the Target Project

2 Target resources are deployed and managed by the DeRF

3 The Workflow Service Account is allowed to impersonate or 'ActAs' the *DeRF Attacker Service Accounts,*

4 Operator invokes a Google Workflow

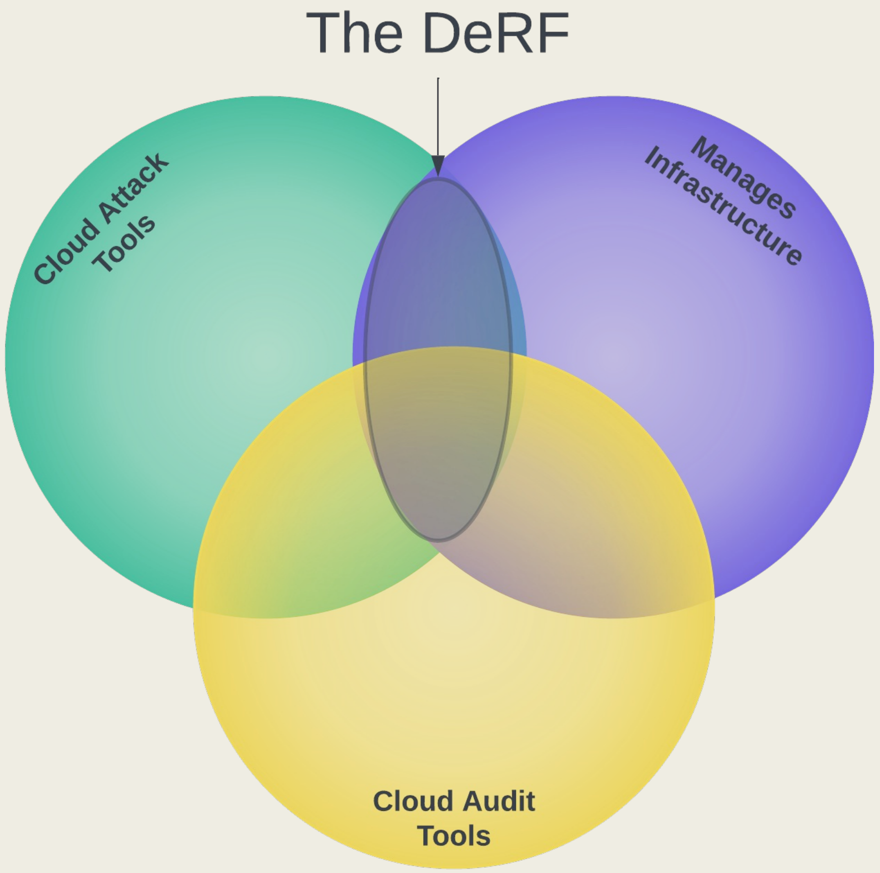
5 The attack techniques generate OAuth tokens for the *DeRF Attack Service Accounts,* in order to operate on resources in the Deployment Project.

6 Attacks are performed against pre-deployed infrastructure in GCP.

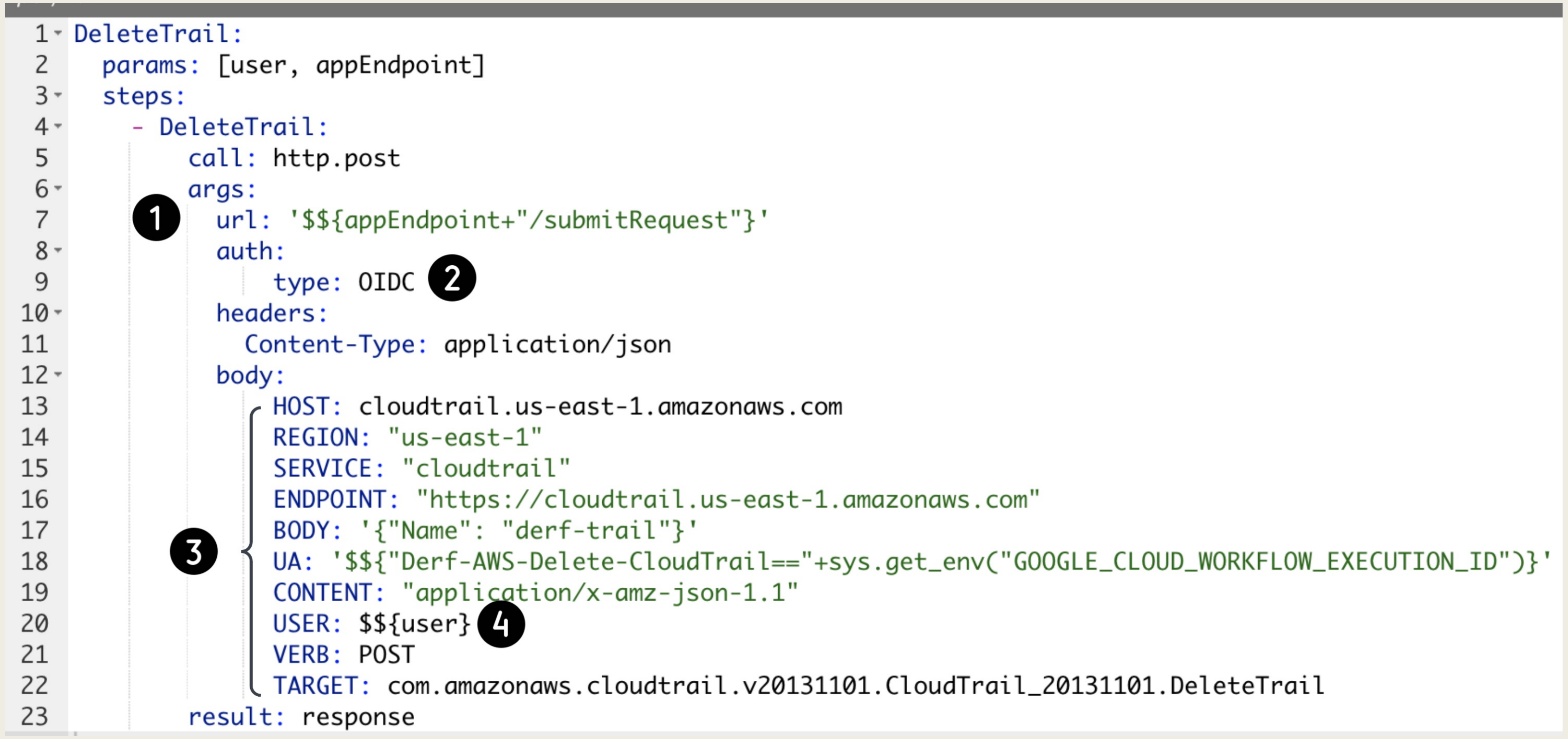
Deploying The DeRF

- Requires both an AWS Account and GCP Project
- Full Deploy / Destroy in under 3 minutes
- Maintaining Infrastructure 24/7 is less than $15 a month
- All resources managed by terraform including:
  - *Attack credentials*
  - *Target Infrastructure*
  - *Attack Techniques*

WHEN TO USE THE DERF ?



Adding Custom Attack Techniques



```
DeleteTrail:
  params: [user, appEndpoint]
  steps:
    - DeleteTrail:
        call: http.post
        args:
          url: '$${appEndpoint+"/submitRequest"}'
          auth:
            type: OIDC
          headers:
            Content-Type: application/json
          body:
            HOST: cloudtrail.us-east-1.amazonaws.com
            REGION: "us-east-1"
            SERVICE: "cloudtrail"
            ENDPOINT: "https://cloudtrail.us-east-1.amazonaws.com"
            BODY: '{"Name": "derf-trail"}'
            UA: '$${"Derf-AWS-Delete-CloudTrail=="+sys.get_env("GOOGLE_CLOUD_WORKFLOW_EXECUTION_ID")}'
            CONTENT: "application/x-amz-json-1.1"
            USER: $${user}
            VERB: POST
            TARGET: com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.DeleteTrail
        result: response
```

1. Submit request to aws proxy application
2. Authenticate to proxy application with Google Cloud IAM
3. Specify the details of the AWS API call in the Post Body
4. Indicate which DeRF User to execute the attack as

DeRF Roadmap

- Azure Coverage
- Expand Attacks Techniques to Target CIS Benchmarks
- Built-In Automation with Cloud Scheduler

QUESTIONS ?