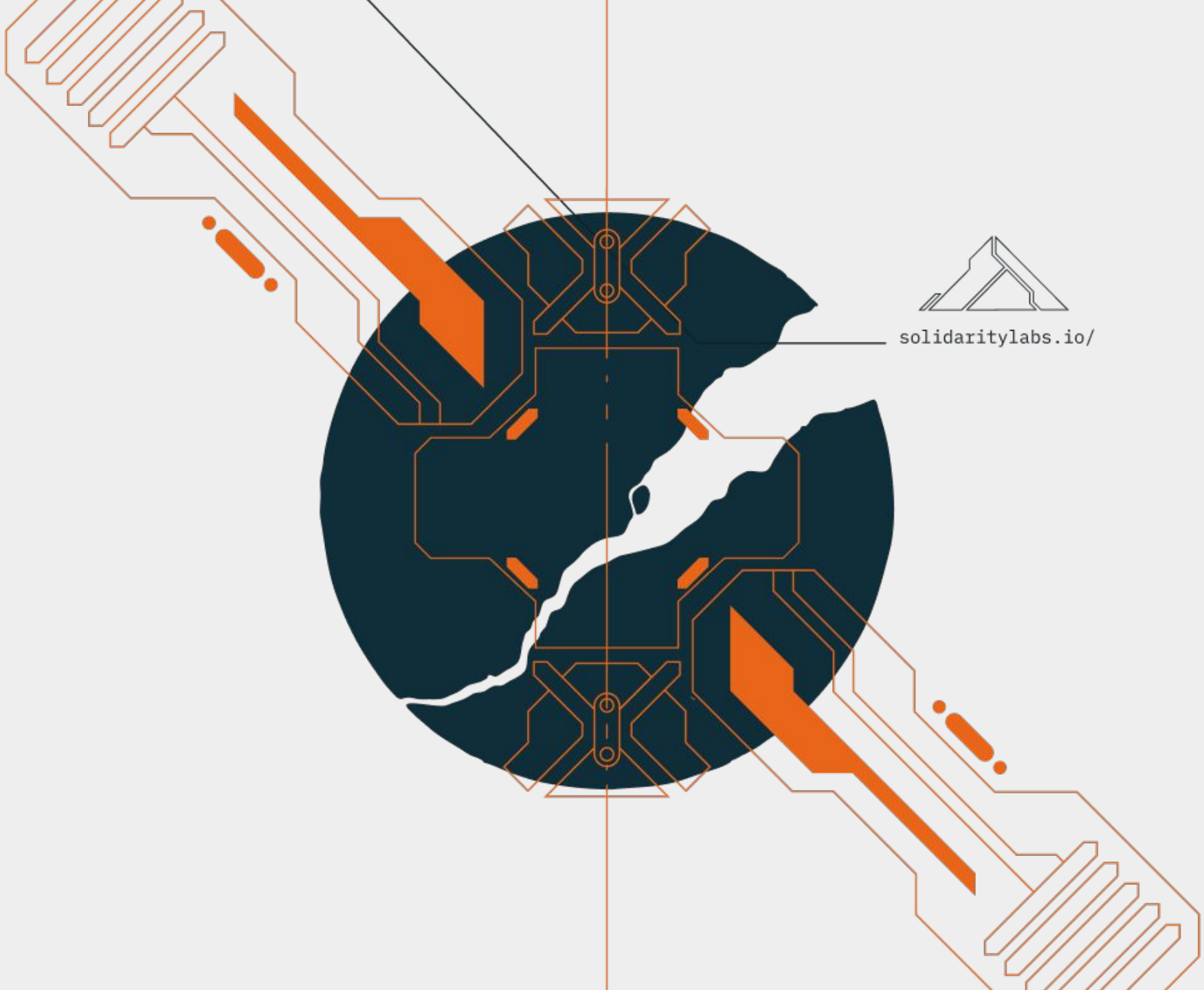
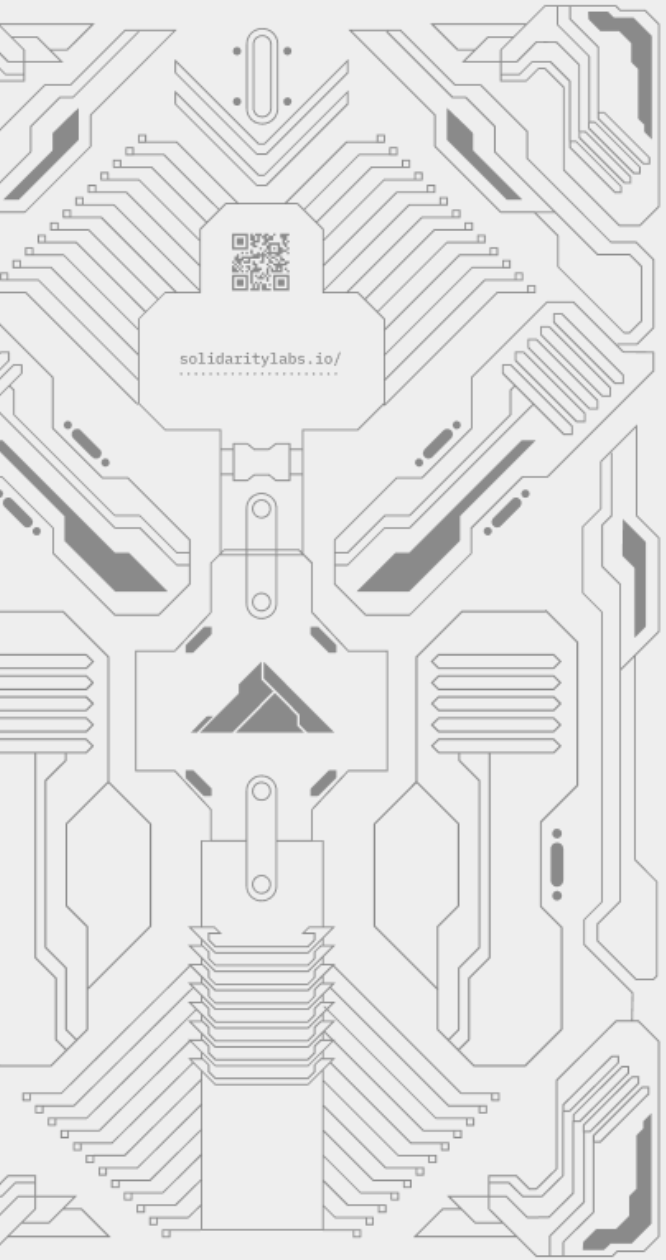
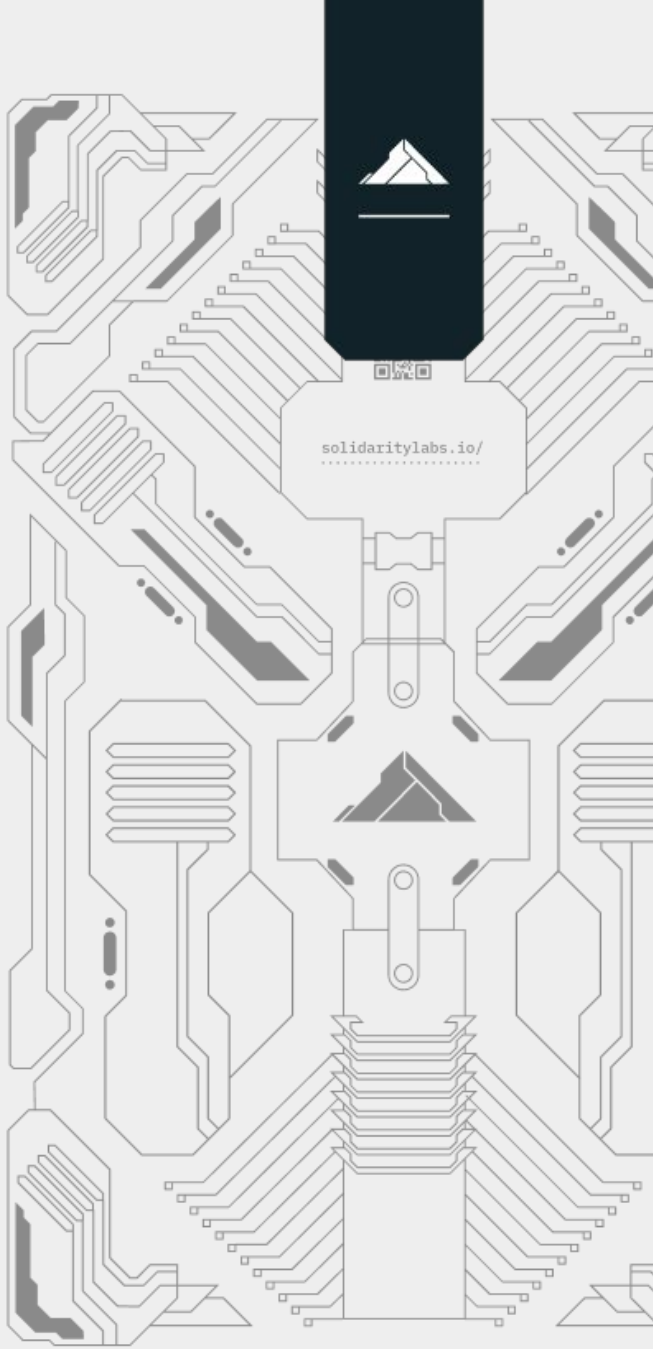

solidaritylabs.io/



Dredge

A Open Source Framework for Cloud Incident Response



/intro

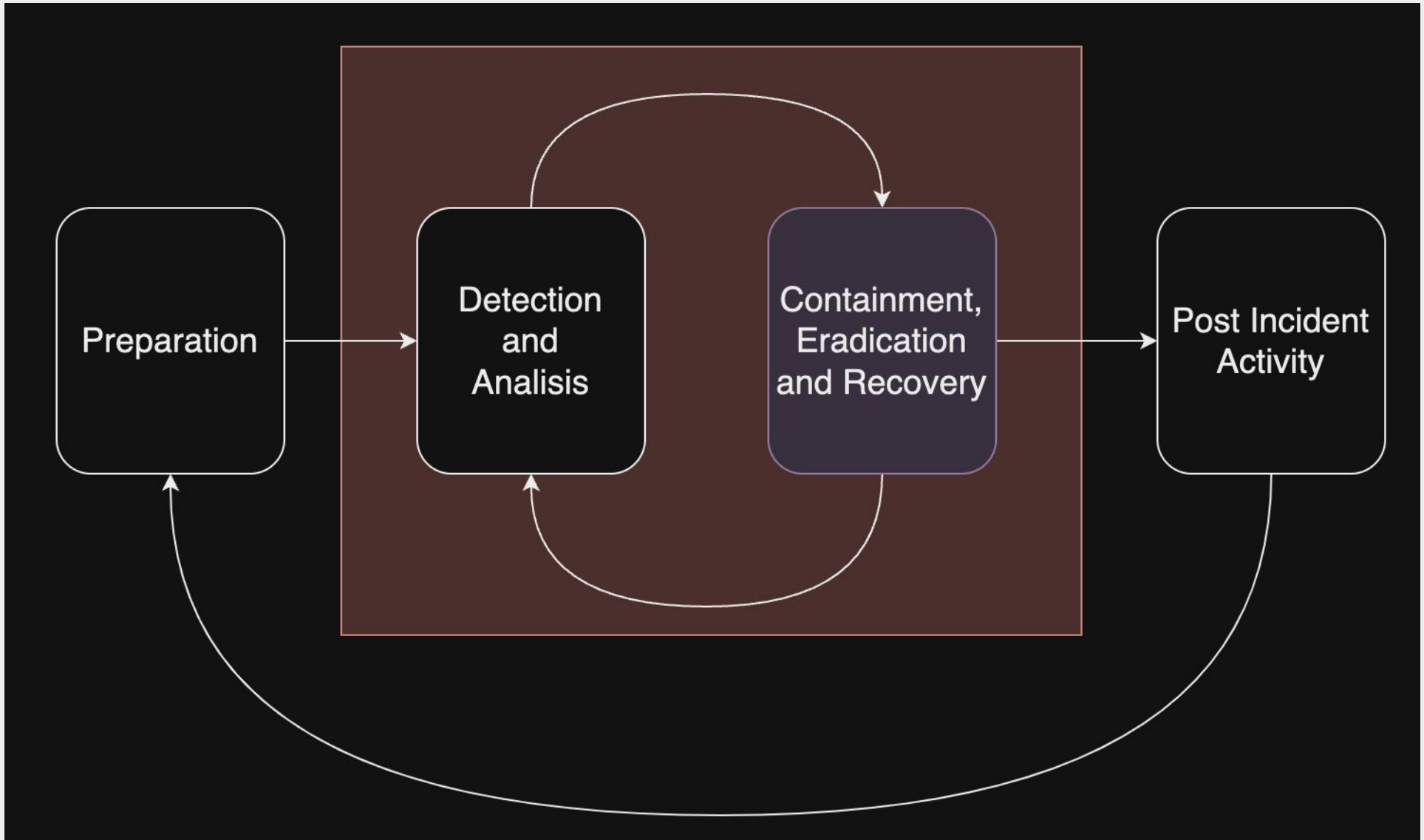
Santi Abastante

Cloud Security Engineer
Incident Responder
CTO | CEO
@Solidaritylabs

Why Dredge?

solidaritylabs.io/

Cyber IR Cycle



CSIRT Perpsective

With Preparation

Without Preparation

SOLIDARITY LABS

- Log Retriever
  - Get data from aws buckets
  - Get logs and events from API
  - Get pod and k8s logs
- Threat Hunting
  - Search for malicious events
  - VirusTotal Integration
  - Shodan Integration
- Incident Response
  - Network Isolate Servers
  - Block Users or Disable Creds
  - Make S3 bucket private
- Cloud Status
  - Get data like users, servers, etc
  - Create timeline from API Calls
  - CSV Reporting

1. Setting Up Dredge

solidaritylabs.io/

Dredge Config File

```
configs:
  start_date: '2023-09-29'
  end_date: '2023-09-30'
  destination_folder: 'logs_dredge'
  output_file: 'test1'
  shodan_api_key: '9R6Y860tl9q--------------------------'
  vt_api_key: '5294a7d0ff16------------------046aa2528dc0a4205'

gcp_configs:
  enabled: False
  cred_files: ['logtesting-.json']

aws_configs:
  enabled: False
  profiles: ['demo-env']
  profile_region: 'us-east-1'
  regions: ['us-east-1']

  event_history:
    enabled: False
  guardduty:
    enabled: False
  lb:
    enabled: False
    buckets: ['alb-logs-solidarity-tes']
```

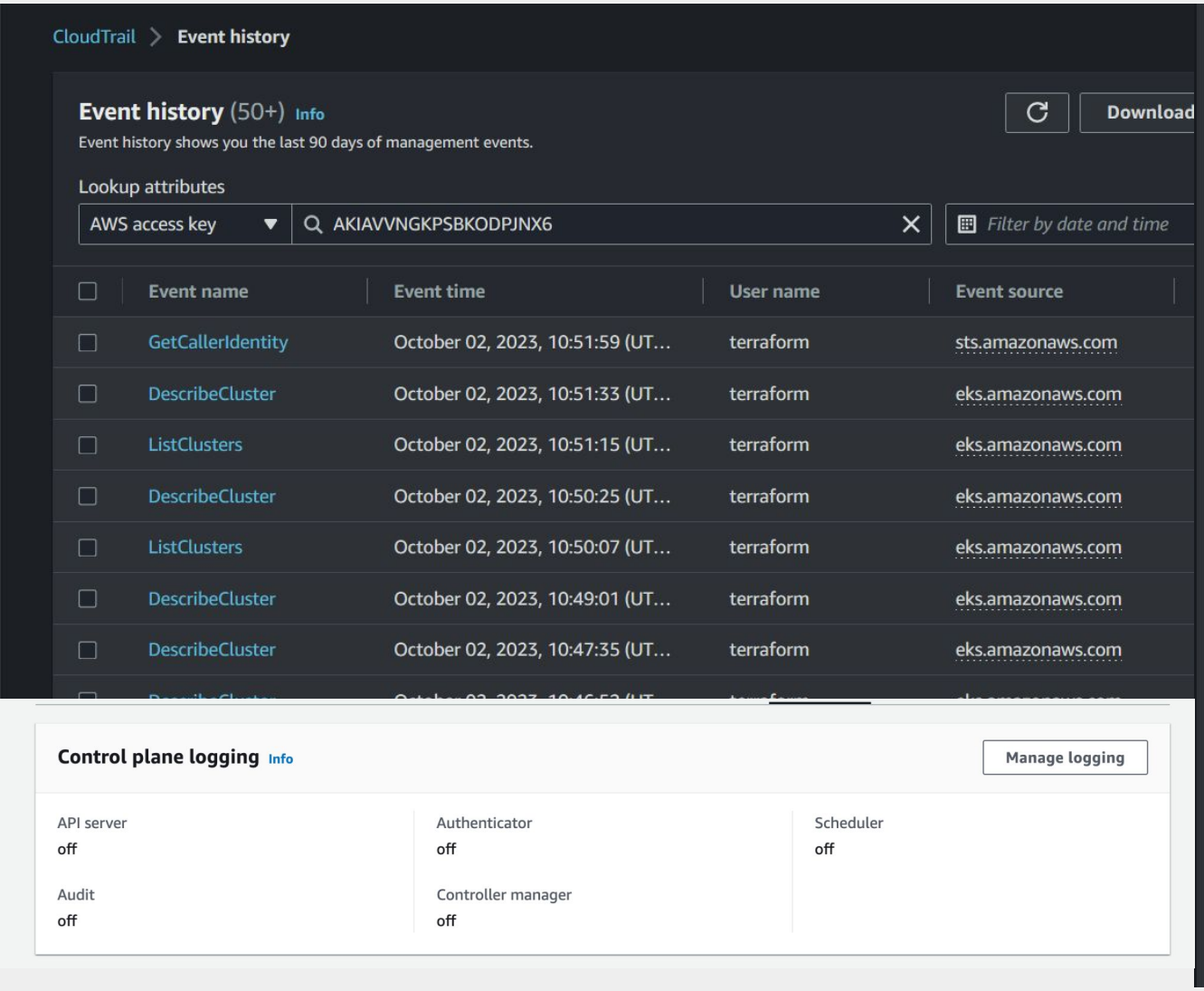
Demo 1

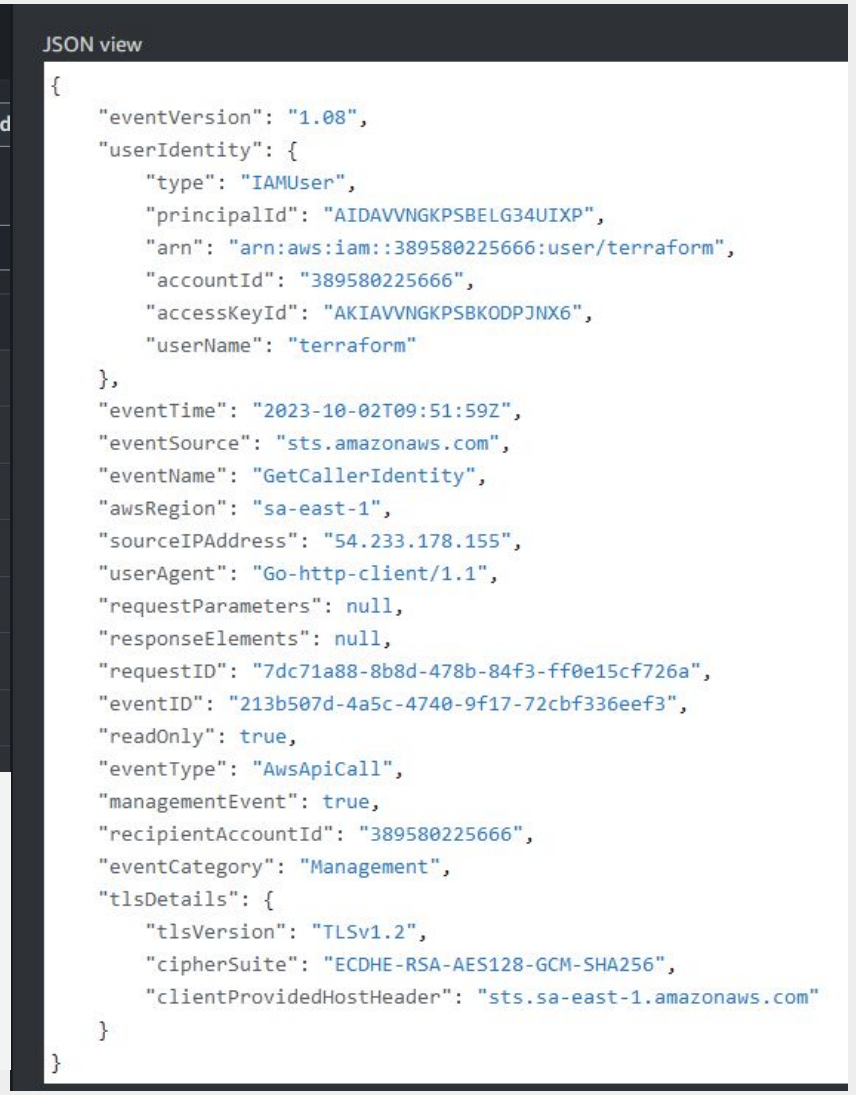
Setting up dredge with config file

2. Log Retriever

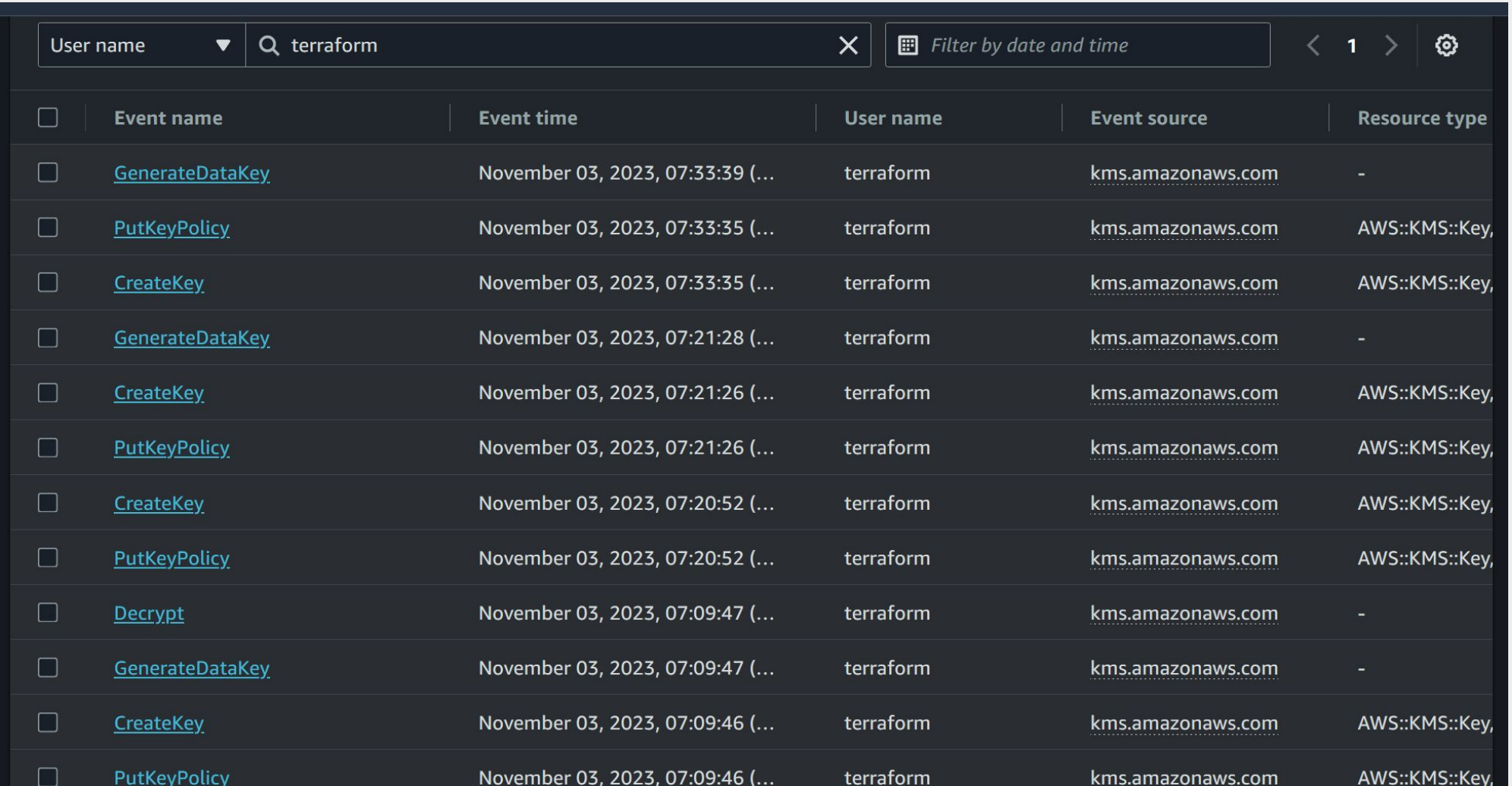
solidaritylabs.io/

Logging and Monitoring





Event History API Logs



Event name	Event time	User name	Event source	Resource type
GenerateDataKey	November 03, 2023, 07:33:39 (...	terraform	kms.amazonaws.com	-
PutKeyPolicy	November 03, 2023, 07:33:35 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,
CreateKey	November 03, 2023, 07:33:35 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,
GenerateDataKey	November 03, 2023, 07:21:28 (...	terraform	kms.amazonaws.com	-
CreateKey	November 03, 2023, 07:21:26 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,
PutKeyPolicy	November 03, 2023, 07:21:26 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,
CreateKey	November 03, 2023, 07:20:52 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,
PutKeyPolicy	November 03, 2023, 07:20:52 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,
Decrypt	November 03, 2023, 07:09:47 (...	terraform	kms.amazonaws.com	-
GenerateDataKey	November 03, 2023, 07:09:47 (...	terraform	kms.amazonaws.com	-
CreateKey	November 03, 2023, 07:09:46 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,
PutKeyPolicy	November 03, 2023, 07:09:46 (...	terraform	kms.amazonaws.com	AWS::KMS::Key,

Demo 2

Getting API Logs from IAM User

Context: Cloudtrail API Call

SOLIDARITY LABS

JSON view


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA5QRO535XCIIFRHW5J",
        "arn": "arn:aws:iam::928885104494:user/terraform",
        "accountId": "928885104494",
        "accessKeyId": "AKIA5QRO535XMI26V6HI",
        "userName": "terraform"
    },
    "eventTime": "2023-11-03T10:33:35Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateKey",
    "awsRegion": "sa-east-1",
    "sourceIPAddress": "181.239.142.48",
    "userAgent": "Boto3/1.26.113 Python/3.10.12 Linux/4.4.0-19041-Microsoft Botocore/1.29.113",
    "requestParameters": {
        "keyUsage": "ENCRYPT_DECRYPT",
        "description": "Your new KMS Key Description",
        "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "bypassPolicyLockoutSafetyCheck": false,
        "keySpec": "SYMMETRIC_DEFAULT",
        "origin": "AWS_KMS"
    },
    "responseElements": {
```

Demo 3

Getting Log from S3 Bucket

Demo 4

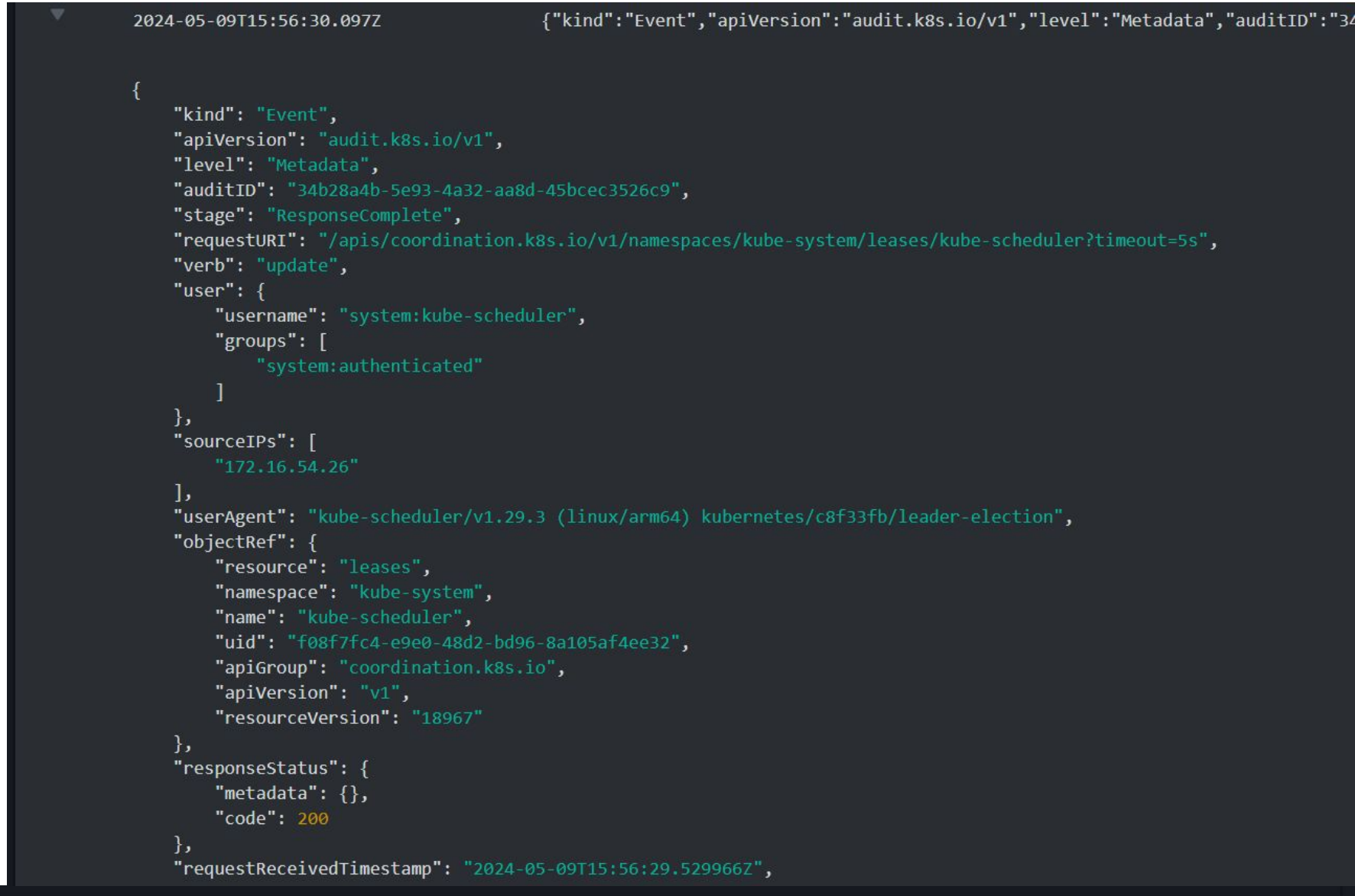
Getting Guardduty Events

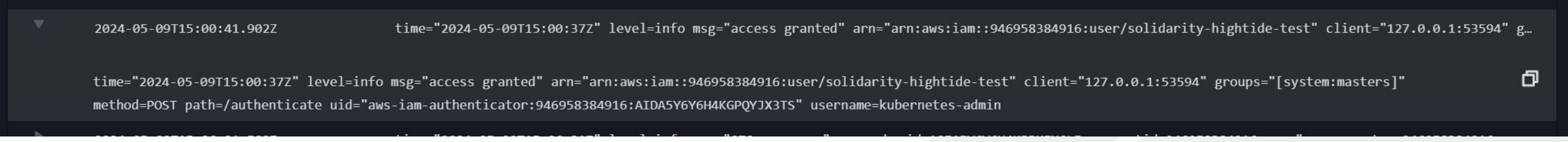
Demo 5

Getting Kubernetes Logs

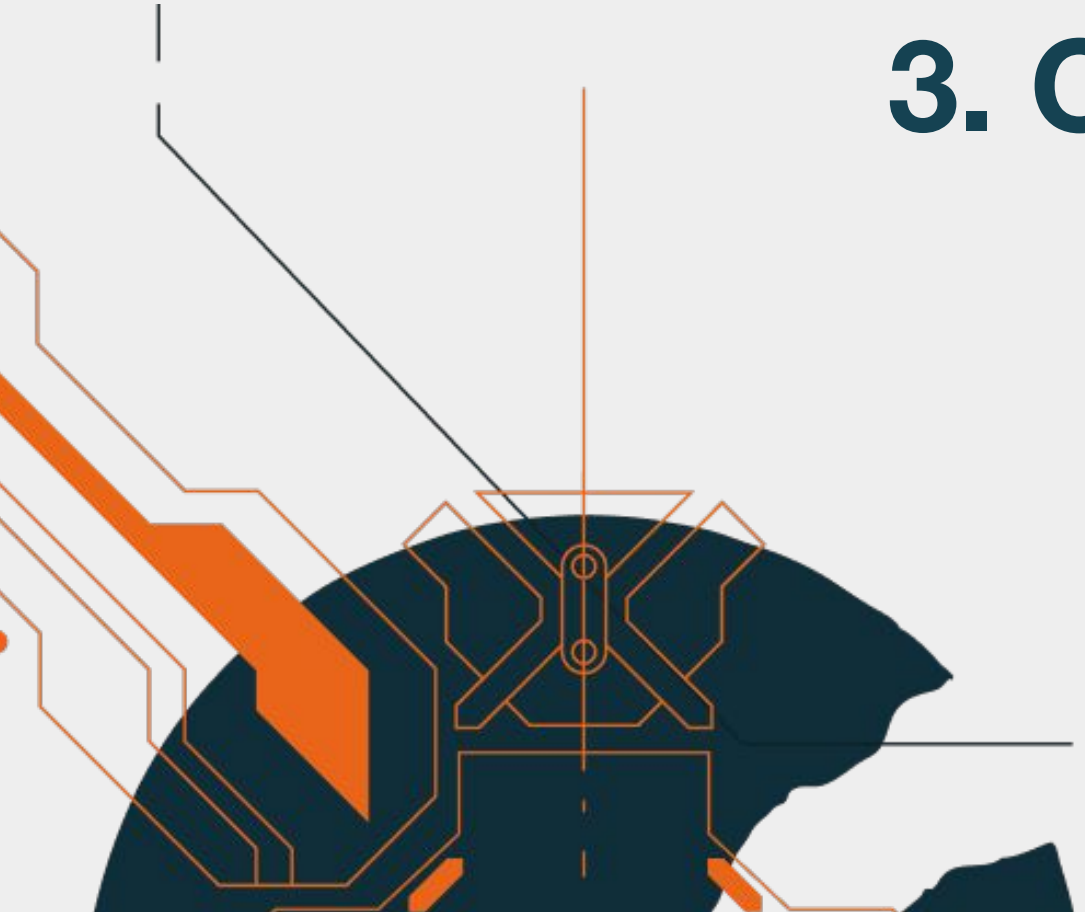
K8s Logs

1. API Server Logs
2. **Audit Logs**
3. **Authenticator**
4. Control Manager
5. Scheduler





3. Cloud Status for IR



solidaritylabs.io/

Demo 6

Getting AWS IAM Users

Demo 7

Getting EC2 Servers


Demo 8
Getting Serverless Functions

4. Incident Response

solidaritylabs.io/

Demo 9

Iam Disable User Access Key

Demo 10

Iam Delete User

Demo 11

Network Isolate EC2 Instance

Demo 12

Enabling Detection Mechanisms

Demo 13

Disable S3 Public Access

5. Threat Hunting

solidaritylabs.io/

Demo 14

Getting IPs

Demo 15

VT Enrichment

Demo 16

IoC Hunting in AWS

Demo 17

Hypothesis Based Hunting in AWS

Questions?

solidaritylabs.io/