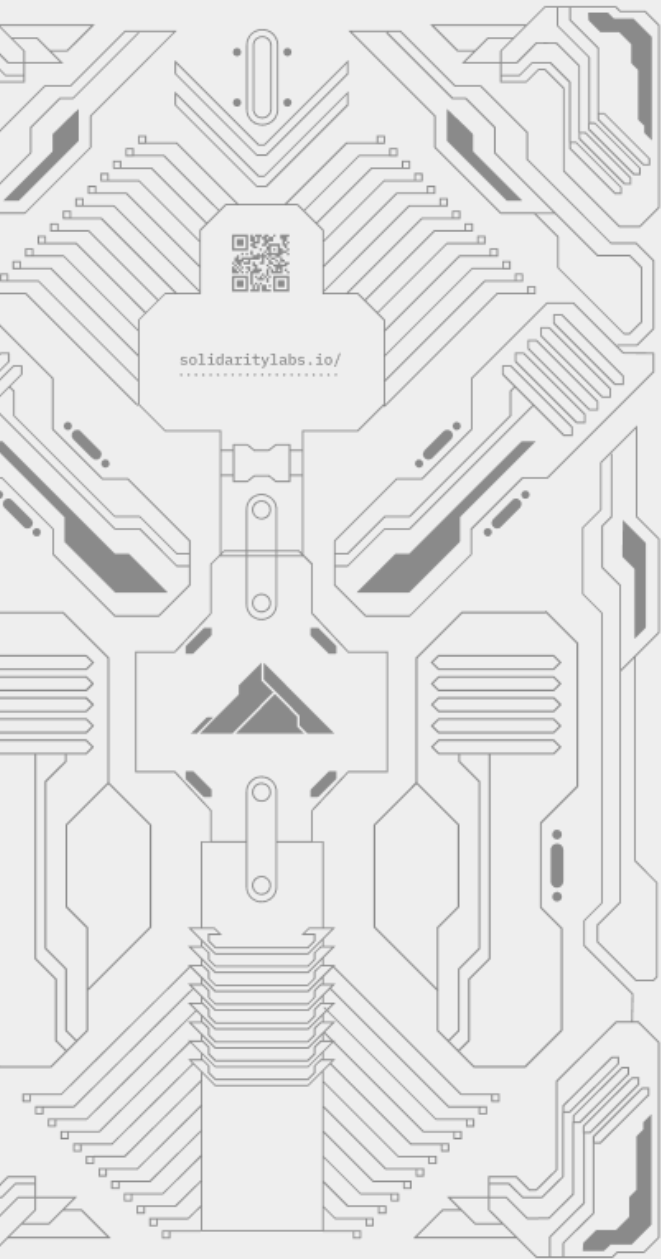


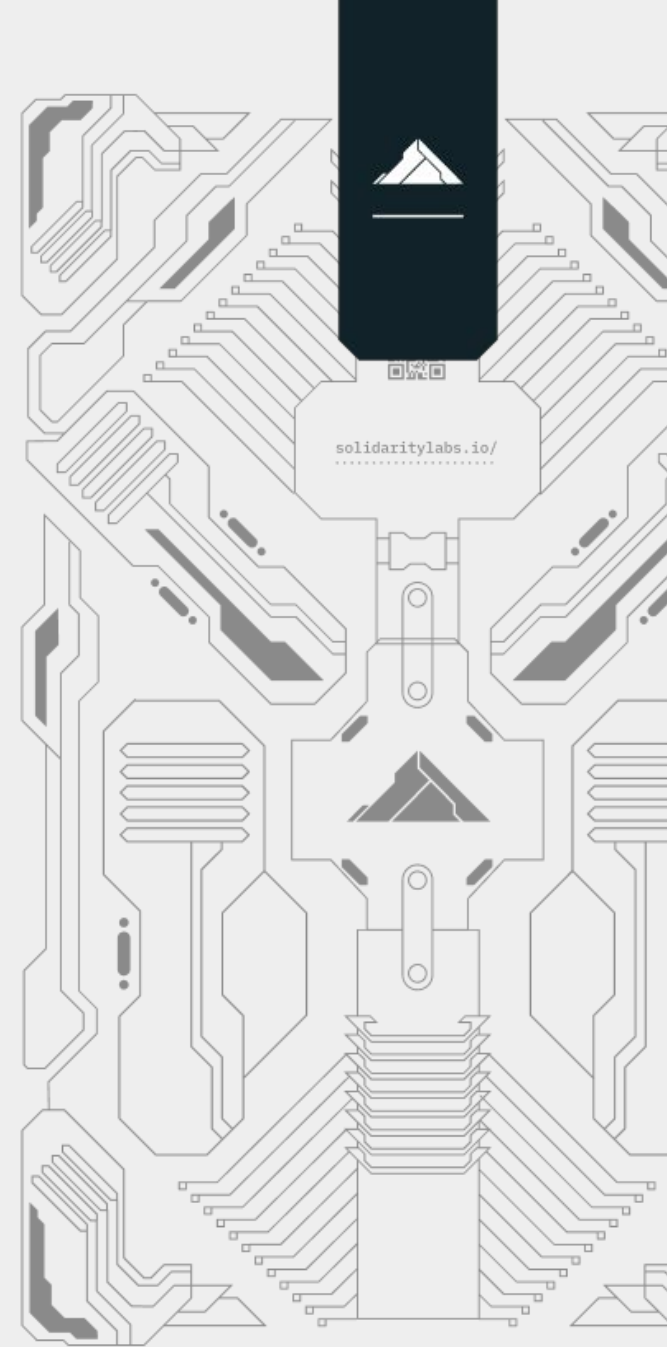


solidaritylabs.io/



Dredge

**A Open Source Framework
for Cloud Incident
Response**



/intro

Santi Abastante

Cloud Security Engineer
Incident Responder
CTO | CEO
@Solidaritylabs

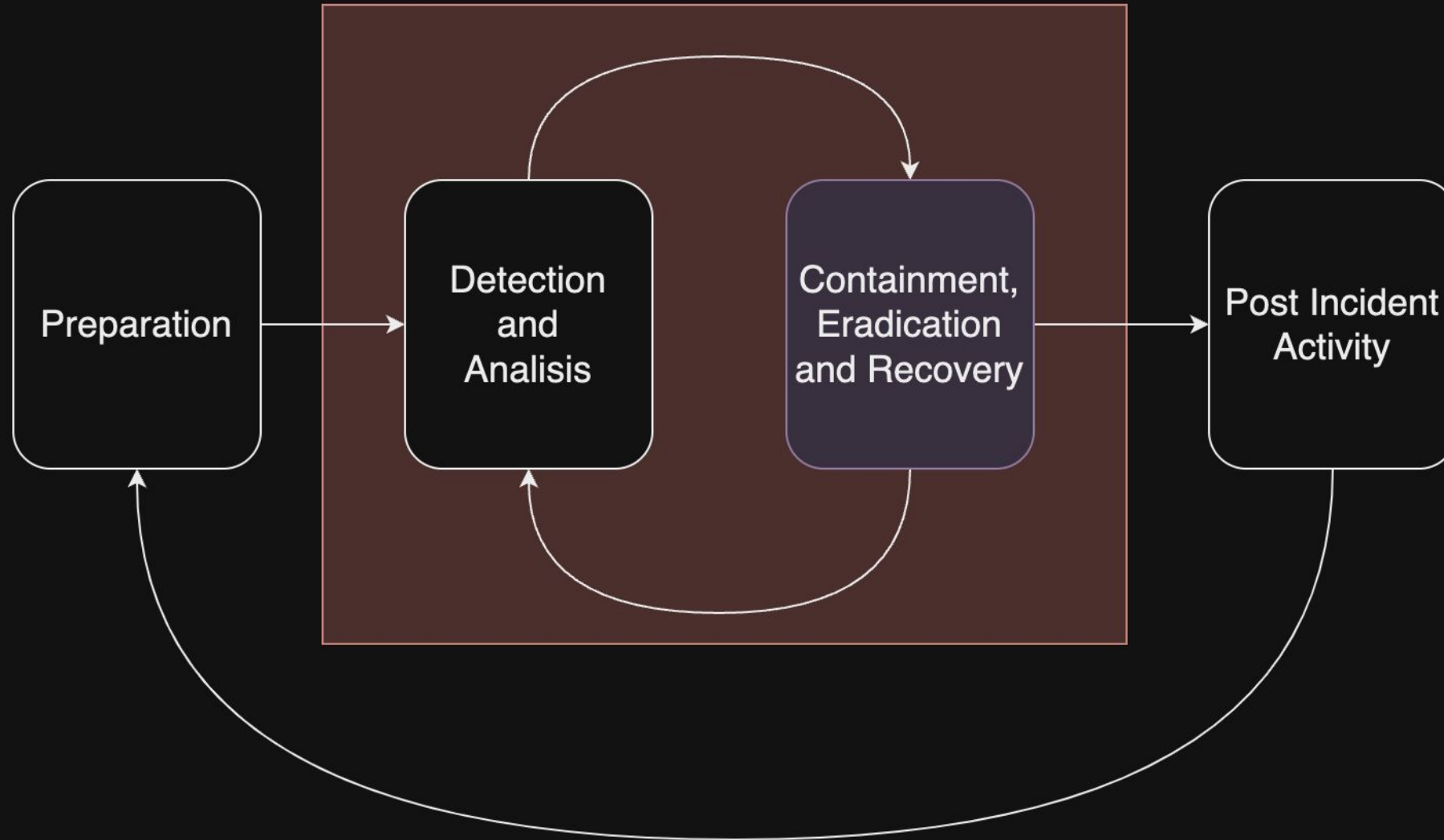


Why Dredge?



solidaritylabs.io/

Cyber IR Cycle



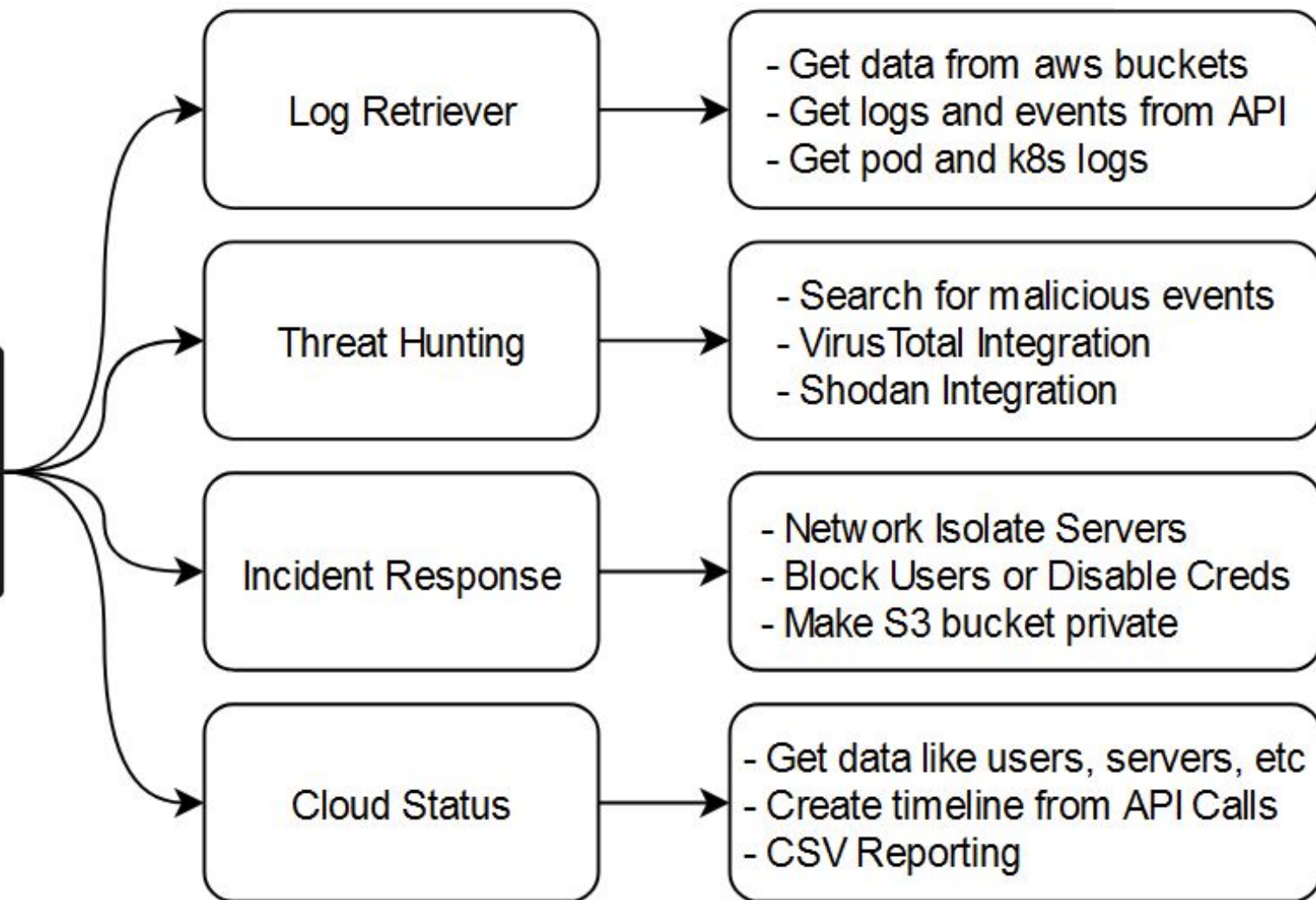
CSIRT Perpsective

With Preparation



Without Preparation





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



CloudTrail > Event history

Event history (50+) [Info](#)

Event history shows you the last 90 days of management events.

Lookup attributes

AWS access key

AKIAVVNGKPSBKODPJNX6

Filter by date and time

<input type="checkbox"/>	Event name	Event time	User name	Event source
<input type="checkbox"/>	GetCallerIdentity	October 02, 2023, 10:51:59 (UT...)	terraform	sts.amazonaws.com
<input type="checkbox"/>	DescribeCluster	October 02, 2023, 10:51:33 (UT...)	terraform	eks.amazonaws.com
<input type="checkbox"/>	ListClusters	October 02, 2023, 10:51:15 (UT...)	terraform	eks.amazonaws.com
<input type="checkbox"/>	DescribeCluster	October 02, 2023, 10:50:25 (UT...)	terraform	eks.amazonaws.com
<input type="checkbox"/>	ListClusters	October 02, 2023, 10:50:07 (UT...)	terraform	eks.amazonaws.com
<input type="checkbox"/>	DescribeCluster	October 02, 2023, 10:49:01 (UT...)	terraform	eks.amazonaws.com
<input type="checkbox"/>	DescribeCluster	October 02, 2023, 10:47:35 (UT...)	terraform	eks.amazonaws.com

Control plane logging [Info](#)

Manage logging

API server
off

Authenticator
off

Scheduler
off

Audit
off

Controller manager
off

JSON view

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAVVNGKPSBELG34UIXP",
    "arn": "arn:aws:iam::389580225666:user/terraform",
    "accountId": "389580225666",
    "accessKeyId": "AKIAVVNGKPSBKODPJNX6",
    "userName": "terraform"
  },
  "eventTime": "2023-10-02T09:51:59Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "GetCallerIdentity",
  "awsRegion": "sa-east-1",
  "sourceIPAddress": "54.233.178.155",
  "userAgent": "Go-http-client/1.1",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "7dc71a88-8b8d-478b-84f3-ff0e15cf726a",
  "eventID": "213b507d-4a5c-4740-9f17-72cbf336eef3",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "389580225666",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "sts.sa-east-1.amazonaws.com"
  }
}
```

Event History API Logs



<div>User name ▼ 🔍 terraform ✕ 📅 Filter by date and time < 1 > ⚙️</div>					
<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type
<input type="checkbox"/>	GenerateDataKey	November 03, 2023, 07:33:39 (...)	terraform	kms.amazonaws.com	-
<input type="checkbox"/>	PutKeyPolicy	November 03, 2023, 07:33:35 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,
<input type="checkbox"/>	CreateKey	November 03, 2023, 07:33:35 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,
<input type="checkbox"/>	GenerateDataKey	November 03, 2023, 07:21:28 (...)	terraform	kms.amazonaws.com	-
<input type="checkbox"/>	CreateKey	November 03, 2023, 07:21:26 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,
<input type="checkbox"/>	PutKeyPolicy	November 03, 2023, 07:21:26 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,
<input type="checkbox"/>	CreateKey	November 03, 2023, 07:20:52 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,
<input type="checkbox"/>	PutKeyPolicy	November 03, 2023, 07:20:52 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,
<input type="checkbox"/>	Decrypt	November 03, 2023, 07:09:47 (...)	terraform	kms.amazonaws.com	-
<input type="checkbox"/>	GenerateDataKey	November 03, 2023, 07:09:47 (...)	terraform	kms.amazonaws.com	-
<input type="checkbox"/>	CreateKey	November 03, 2023, 07:09:46 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,
<input type="checkbox"/>	PutKeyPolicy	November 03, 2023, 07:09:46 (...)	terraform	kms.amazonaws.com	AWS::KMS::Key,



solidaritylabs.io/
XXXXXXXXXXXXXXXXXXXX

Demo 2

Getting API Logs from IAM User

solidaritylabs.io/
XXXXXXXXXXXXXXXXXXXX

Context: Cloudtrail API Call



```
JSON view
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA5QRO535XCIFRHW5J",
    "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



soliditylabs.io/

soliditylabs.io/

Demo 4

Getting Guardduty Events



soliditylabs.io/

Demo 5

Getting Kubernetes Logs

K8s Logs

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

2024-05-09T15:56:30.097Z

{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"34b28a4b-5e93-4a32-aa8d-45bcec3526c9"}

```
{
  "kind": "Event",
  "apiVersion": "audit.k8s.io/v1",
  "level": "Metadata",
  "auditID": "34b28a4b-5e93-4a32-aa8d-45bcec3526c9",
  "stage": "ResponseComplete",
  "requestURI": "/apis/coordination.k8s.io/v1/namespaces/kube-system/leases/kube-scheduler?timeout=5s",
  "verb": "update",
  "user": {
    "username": "system:kube-scheduler",
    "groups": [
      "system:authenticated"
    ]
  },
  "sourceIPs": [
    "172.16.54.26"
  ],
  "userAgent": "kube-scheduler/v1.29.3 (linux/arm64) kubernetes/c8f33fb/leader-election",
  "objectRef": {
    "resource": "leases",
    "namespace": "kube-system",
    "name": "kube-scheduler",
    "uid": "f08f7fc4-e9e0-48d2-bd96-8a105af4ee32",
    "apiGroup": "coordination.k8s.io",
    "apiVersion": "v1",
    "resourceVersion": "18967"
  },
  "responseStatus": {
    "metadata": {},
    "code": 200
  },
  "requestReceivedTimestamp": "2024-05-09T15:56:29.529966Z",
}
```

2024-05-09T15:00:41.902Z

time="2024-05-09T15:00:37Z" level=info msg="access granted" arn="arn:aws:iam::946958384916:user/solidarity-hightide-test" client="127.0.0.1:53594" g...

time="2024-05-09T15:00:37Z" level=info msg="access granted" arn="arn:aws:iam::946958384916:user/solidarity-hightide-test" client="127.0.0.1:53594" groups="[system:masters]"
method=POST path=/authenticate uid="aws-iam-authenticator:946958384916:AIDA5Y6Y6H4KGPQYJX3TS" username=kubernetes-admin



3. Cloud Status for IR



solidaritylabs.io/



soliditylabs.io/

Demo 6

Getting AWS IAM Users



soliditylabs.io/



soliditylabs.io/

soliditylabs.io/

Demo 7

Getting EC2 Servers



soliditylabs.io/

soliditylabs.io/

Demo 8

Getting Serverless Functions

4. Incident Response



solidaritylabs.io/



soliditylabs.io/

Demo 9

Iam Disable User Access Key

Demo 10

Iam Delete User



solidaritylabs.io/
XXXXXXXXXXXXXXXXXXXX



solidaritylabs.io/

Demo 11

Network Isolate EC2 Instance



soliditylabs.io/

Demo 12

Enabling Detection Mechanisms



solidaritylabs.io/
XXXXXXXXXXXXXXXXXXXX

Demo 13

Disable S3 Public Access

solidaritylabs.io/
XXXXXXXXXXXXXXXXXXXX

5. Threat Hunting



solidaritylabs.io/

Demo 14

Getting IPs



soliditylabs.io/

Demo 15

VT Enrichment



solidaritylabs.io/

Demo 16

IoC Hunting in AWS



soliditylabs.io/



solidaritylabs.io/

Demo 17

Hypothesis Based Hunting in AWS

Questions?



solidaritylabs.io/

