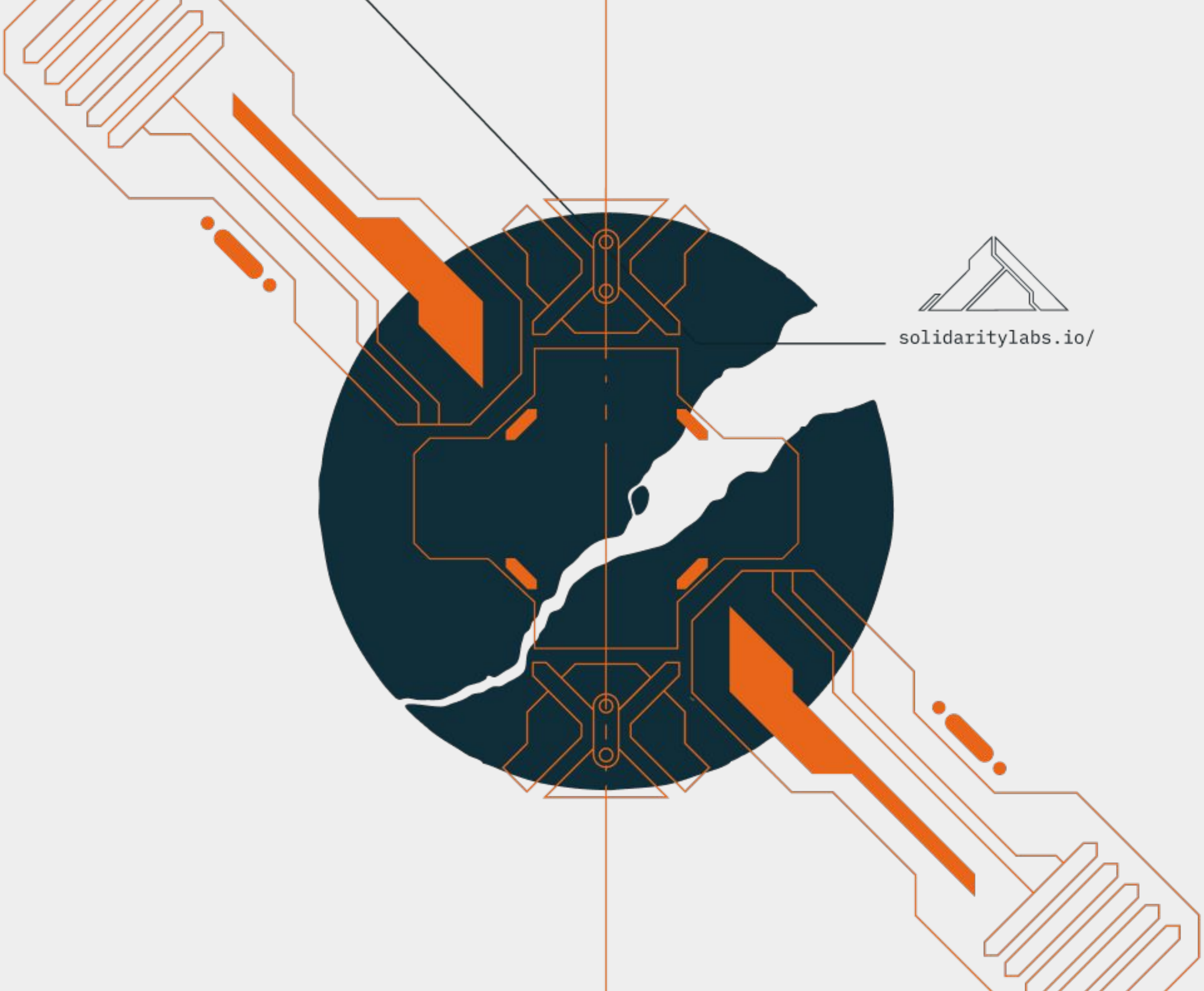
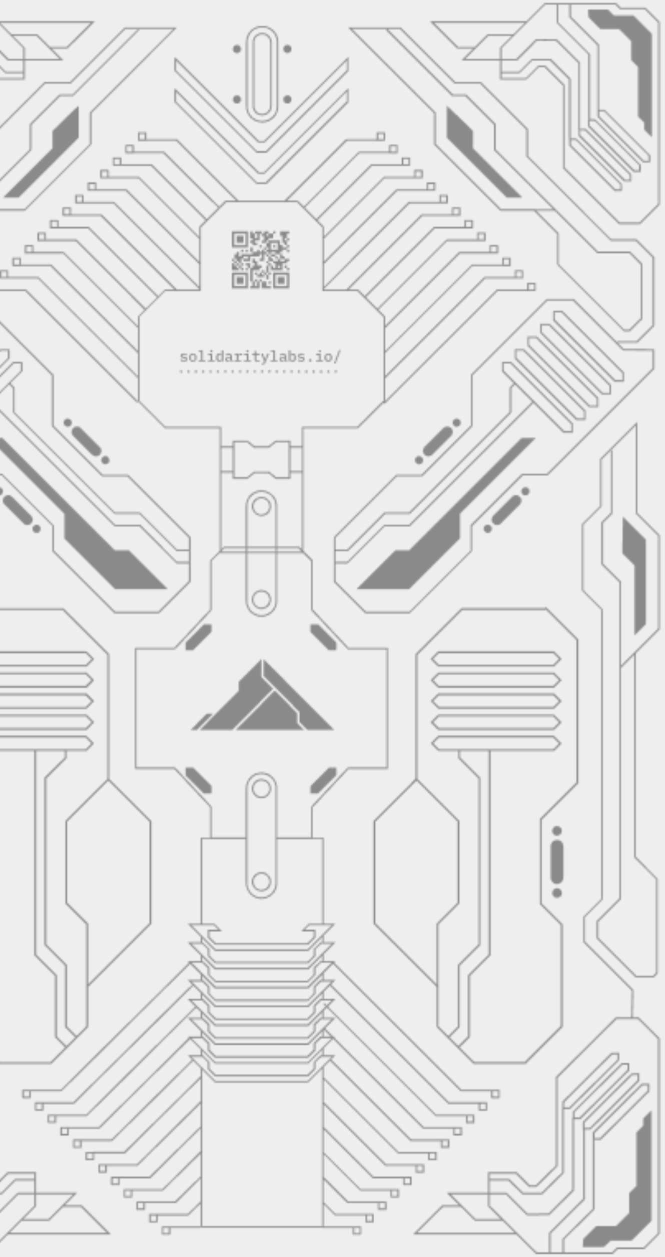
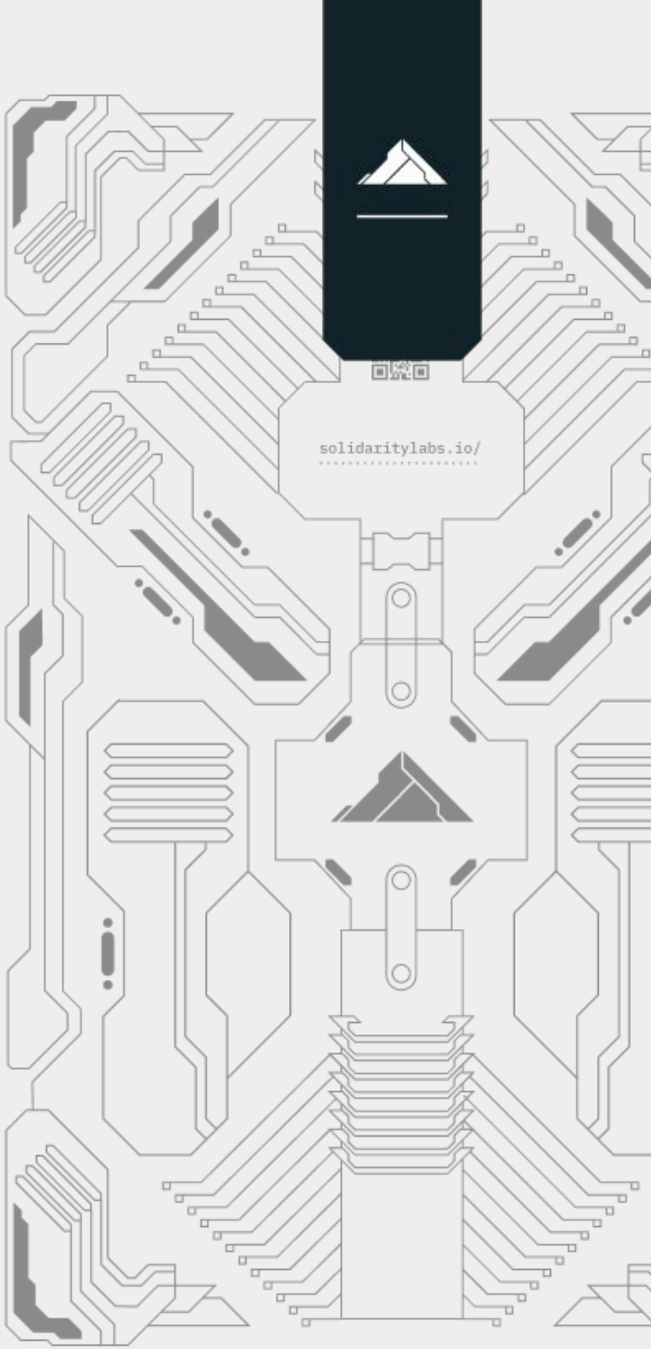


solidaritylabs.io/



Dredge

An Open Source Framework for Cloud IR



/intro

Santi Abastante

Cloud Security Engineer
Incident Responder
@Solidaritylabs

Argentina?

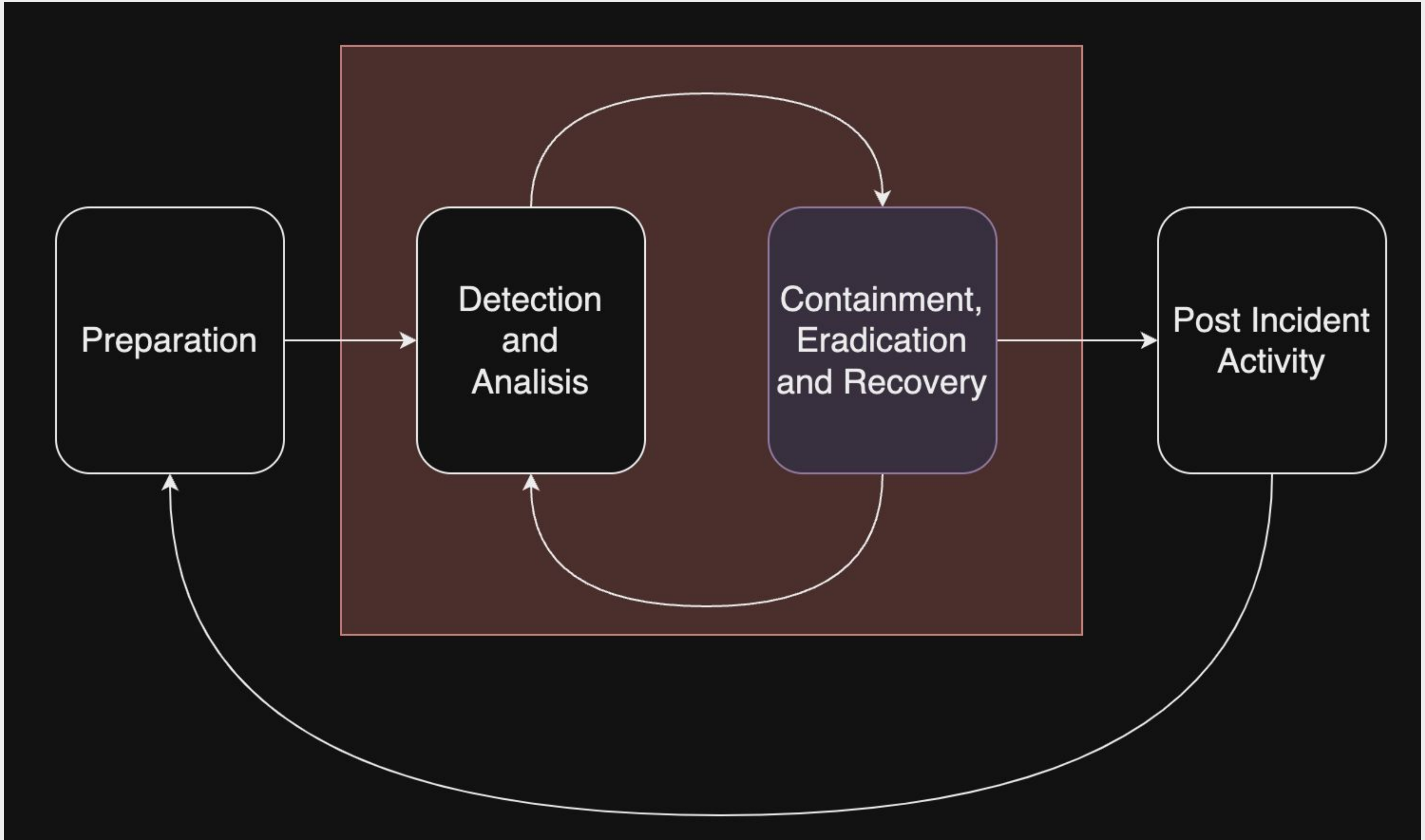
ARGENTINA LOCATION MAP
Tropic of Cancer
Equator
Tropic of Capricorn
ARGENTINA
Antarctic Circle

NEW YORK STO

Why Dredge?

solidaritylabs.io/

Cyber IR Cycle



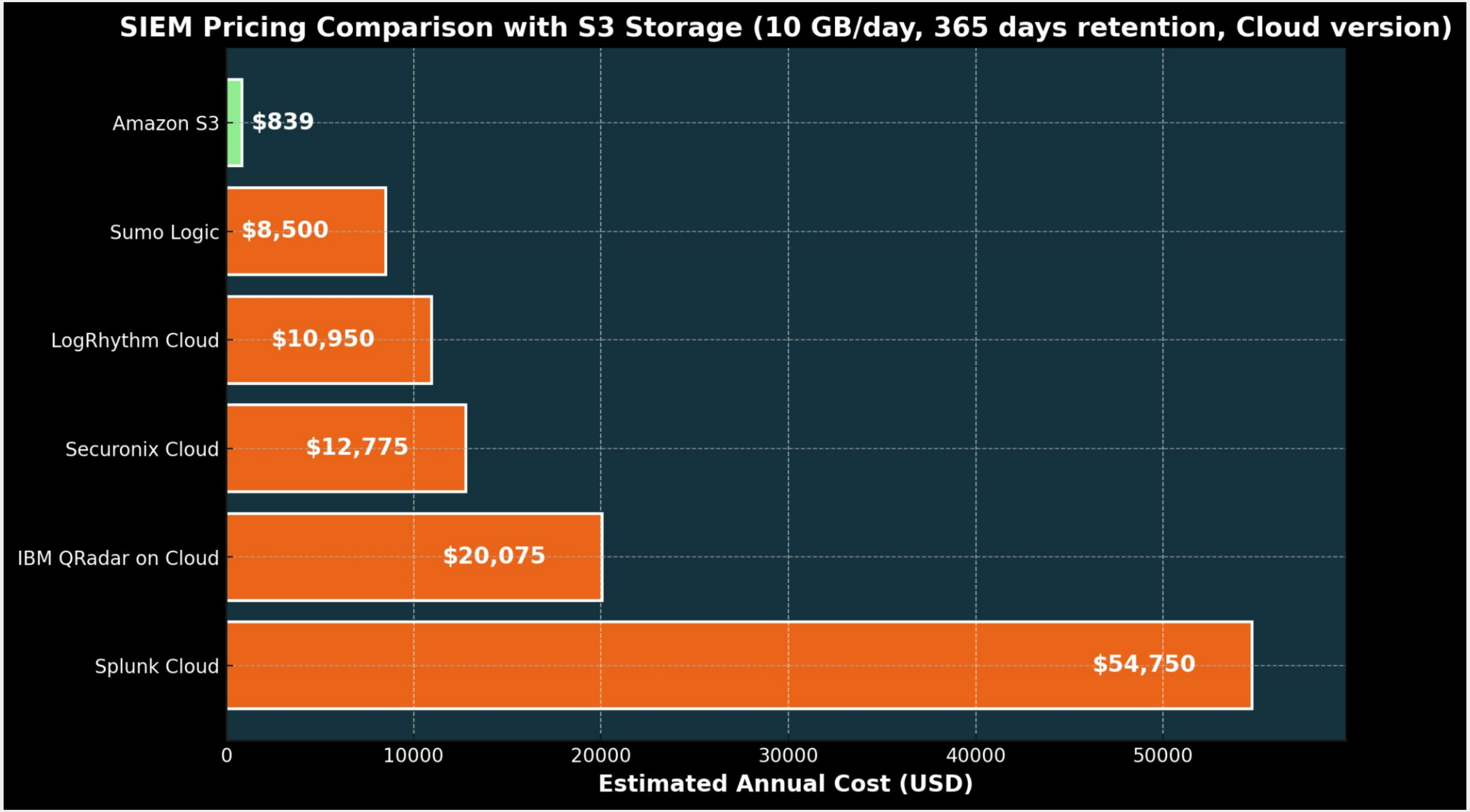
Preparation

Detection and Analisis

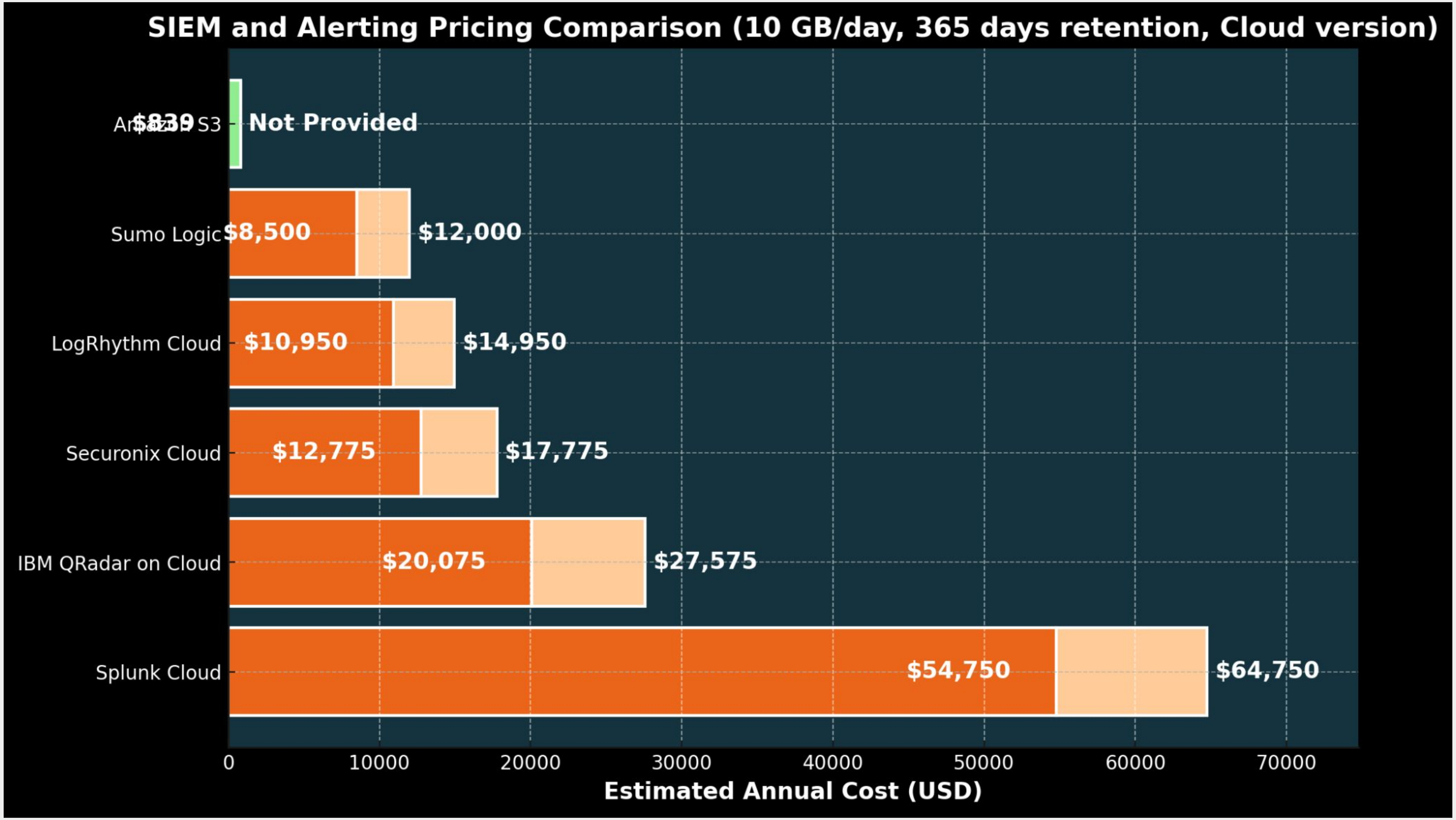
Containment, Eradication and Recovery

Post Incident Activity

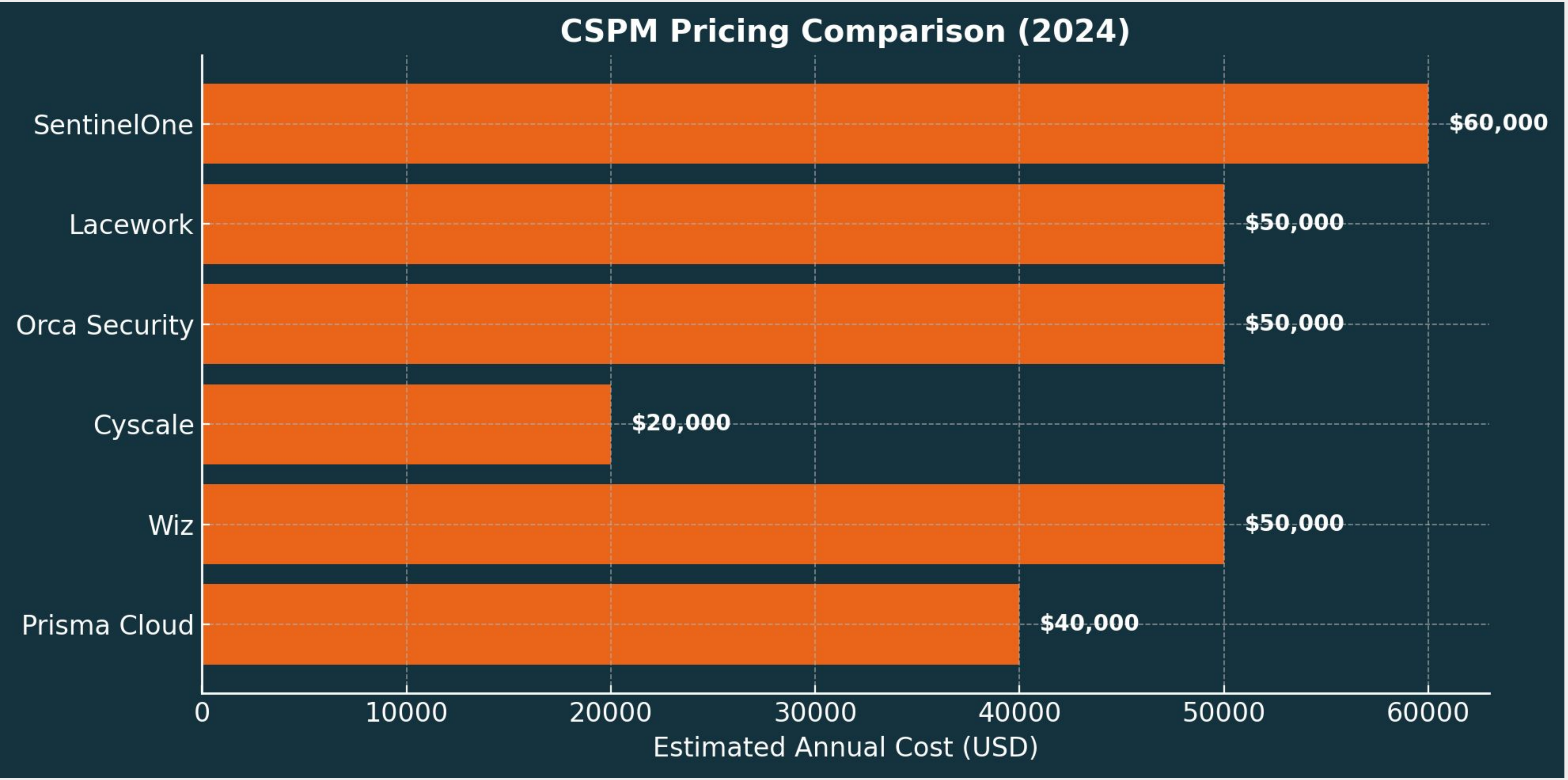
SIEM Pricing - 1

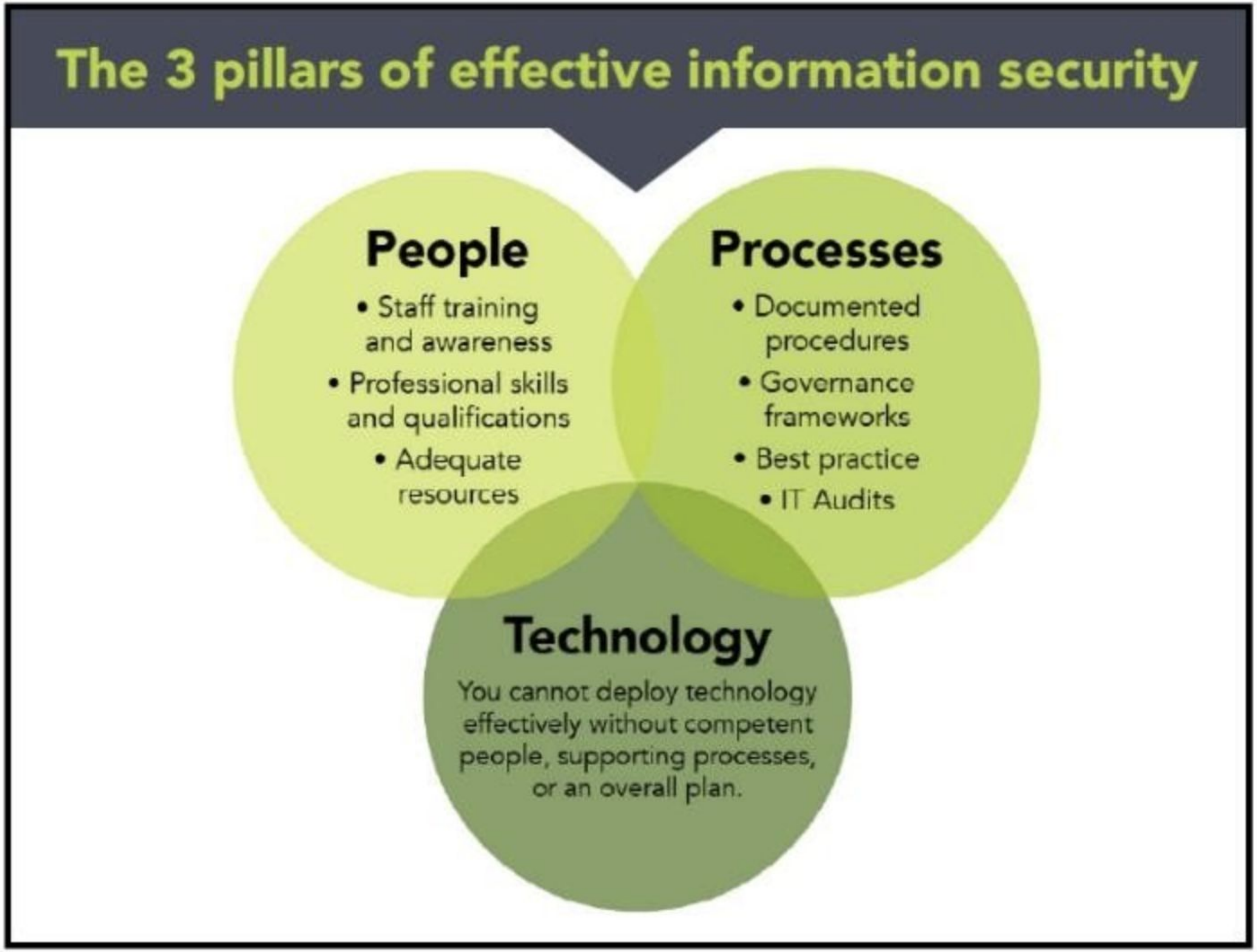


SIEM Pricing - with Alerts



And What about CSPM?





The 3 pillars of effective information security

People

- Staff training and awareness
- Professional skills and qualifications
- Adequate resources

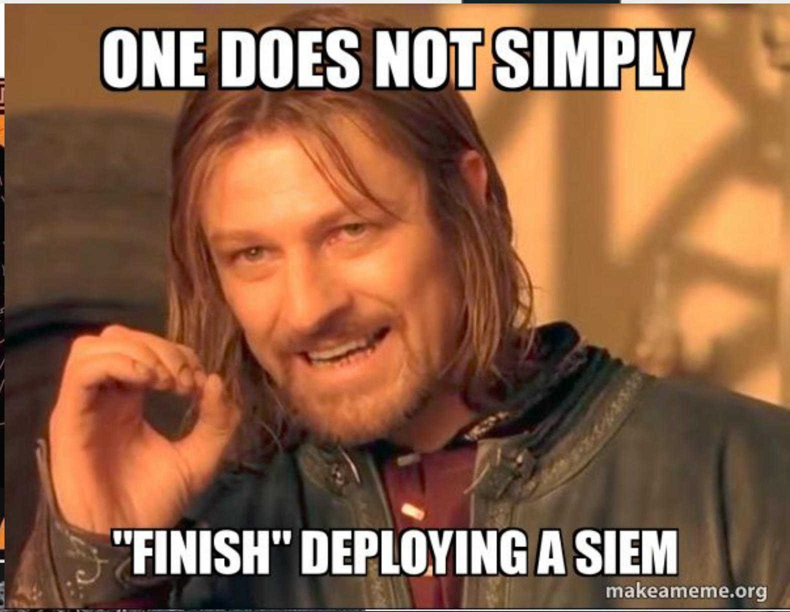
Processes

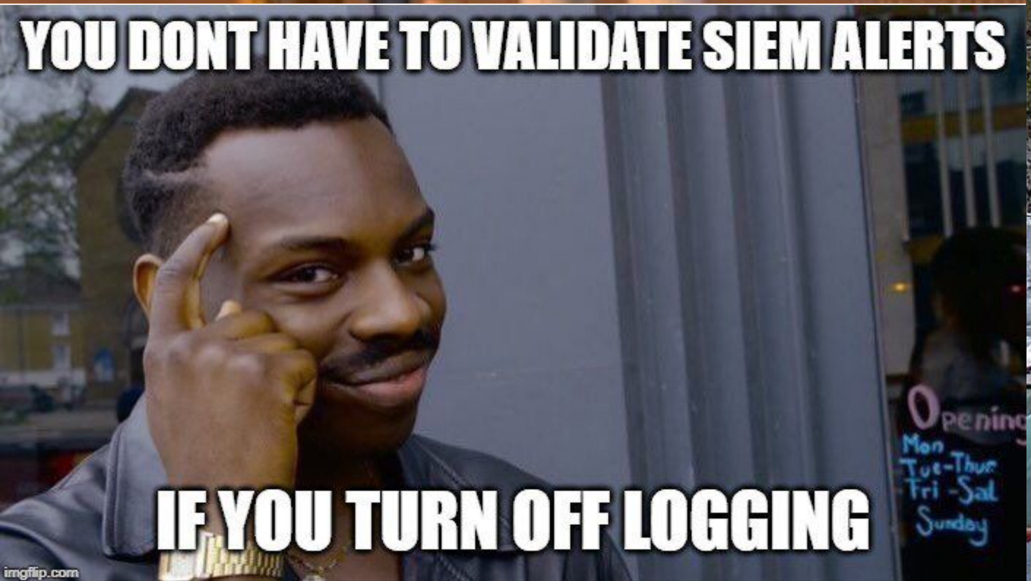
- Documented procedures
- Governance frameworks
- Best practice
- IT Audits

Technology

You cannot deploy technology effectively without competent people, supporting processes, or an overall plan.

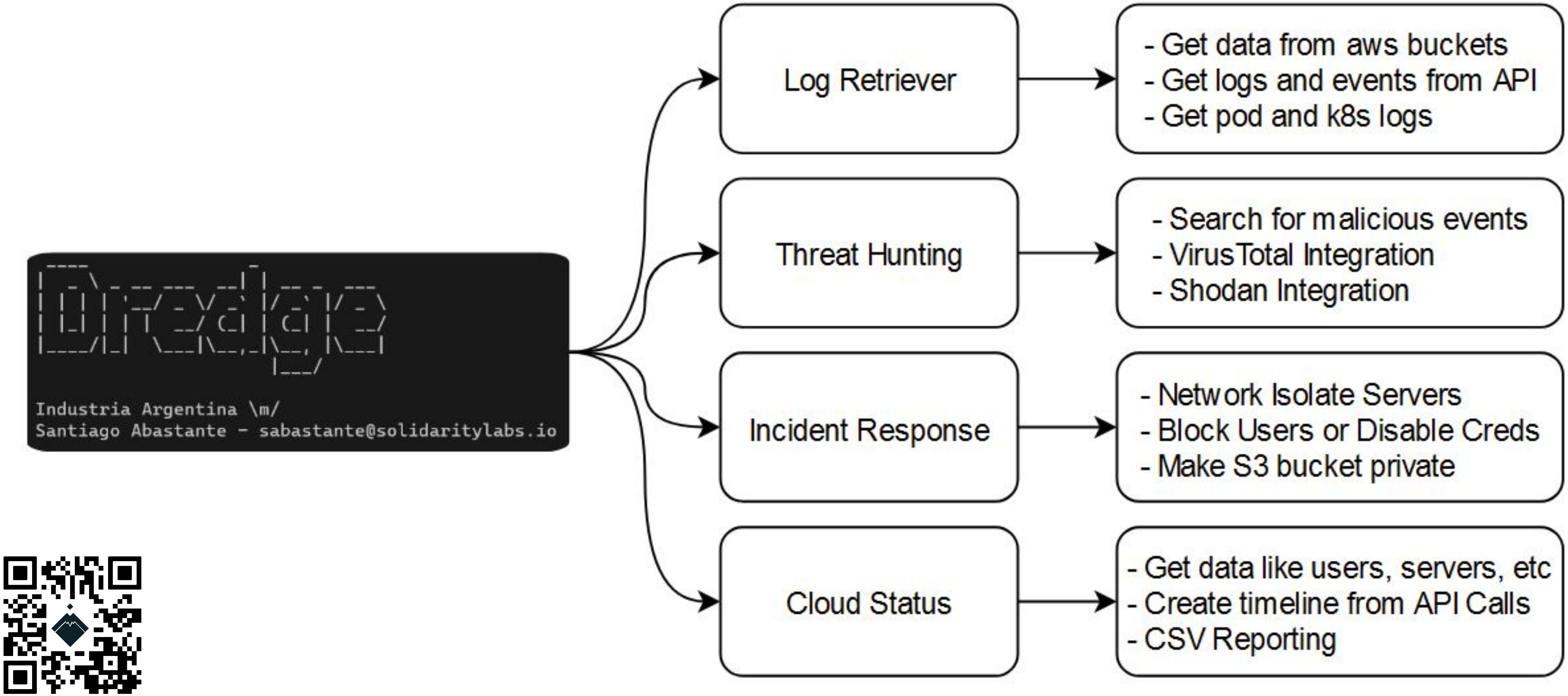
Security Operation’t





SORRY, WE CAN'T INGEST YOUR DAILY 10 GB OF PROC CREATION EVENTS. IT'S ALREADY TOO EXPENSIVE.
200 GB OF FIREWALL LOGS
SIEM
imgflip.com

Operational Costs



```
 ____               _
|  _ \ _ __ ___  __| | __ _  ___
| | | | '__/ _ \/ _` |/ _` |/ _ \
| |_| | | |  __/ (_| | (_| |  __/
|____/|_|  \___|\__,_|\__, |\___|
                      |___/
Industria Argentina \m/
Santiago Abastante - sabastante@solidaritylabs.io
```

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

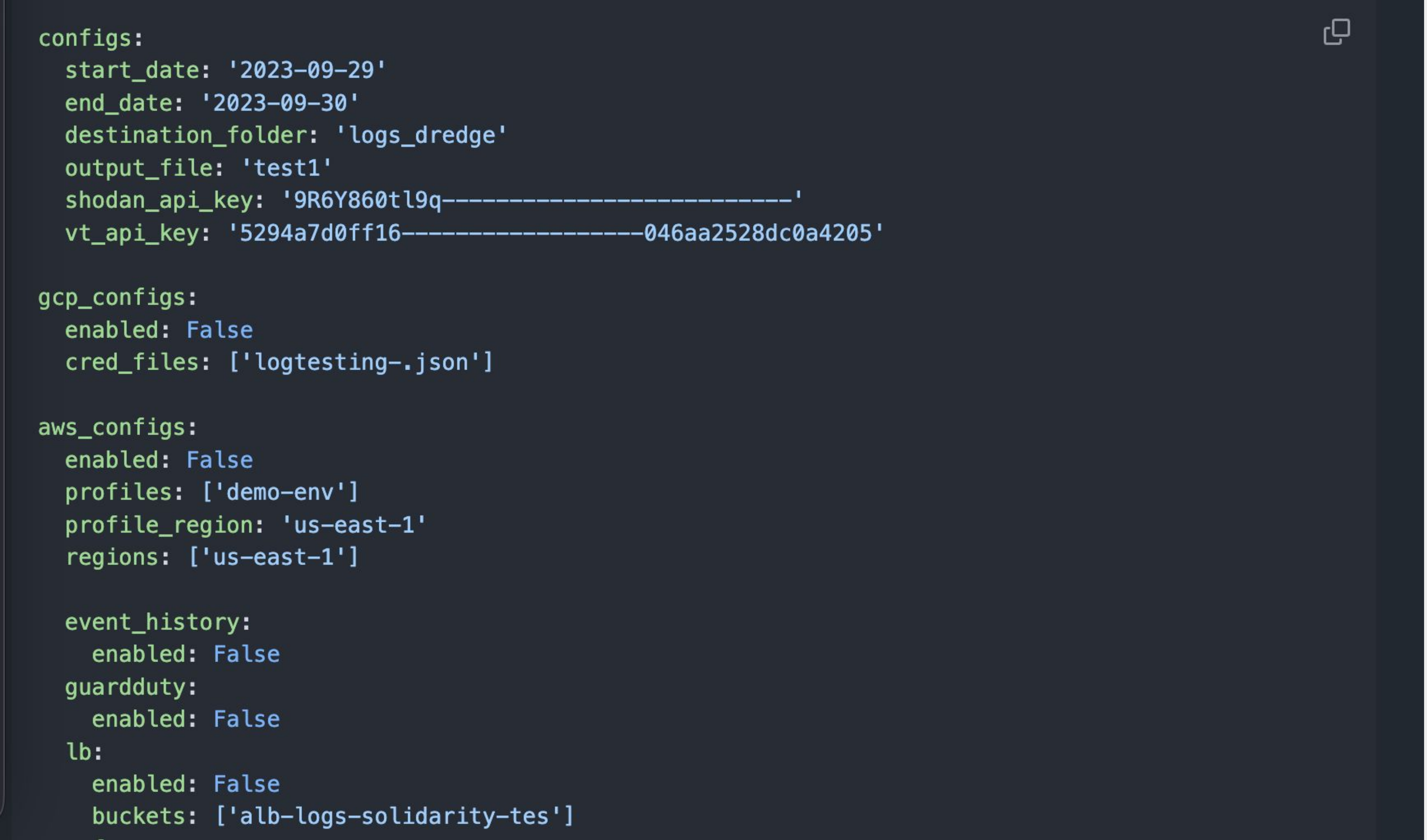
- Network Isolate Servers
- Block Users or Disable Creds
- Make S3 bucket private

Cloud Status

- Get data like users, servers, etc
- Create timeline from API Calls
- CSV Reporting

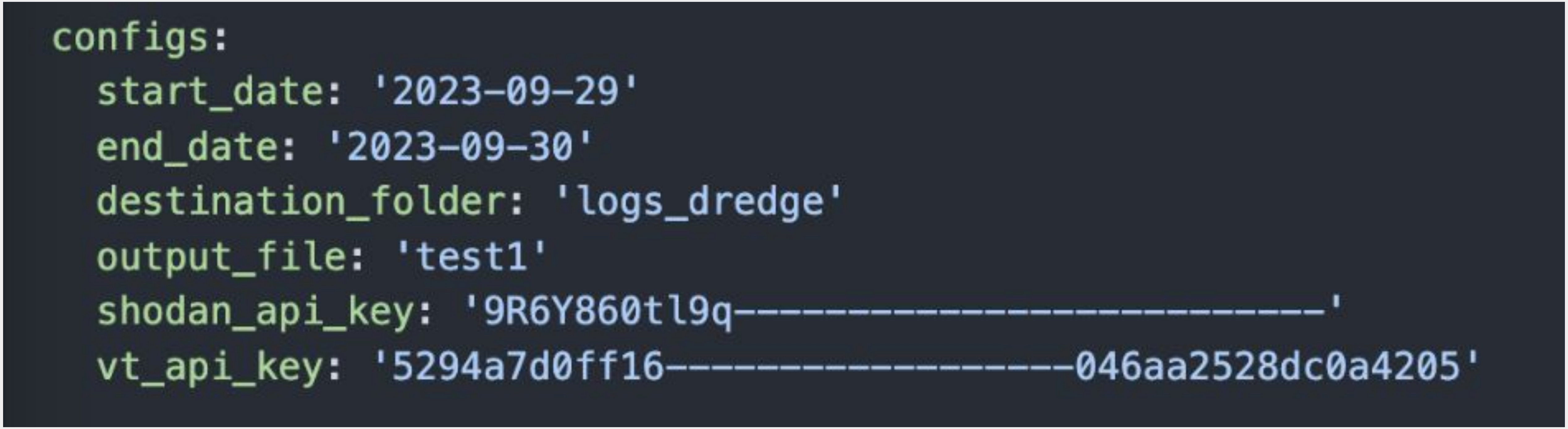
1. Setting Up Dredge

solidaritylabs.io/



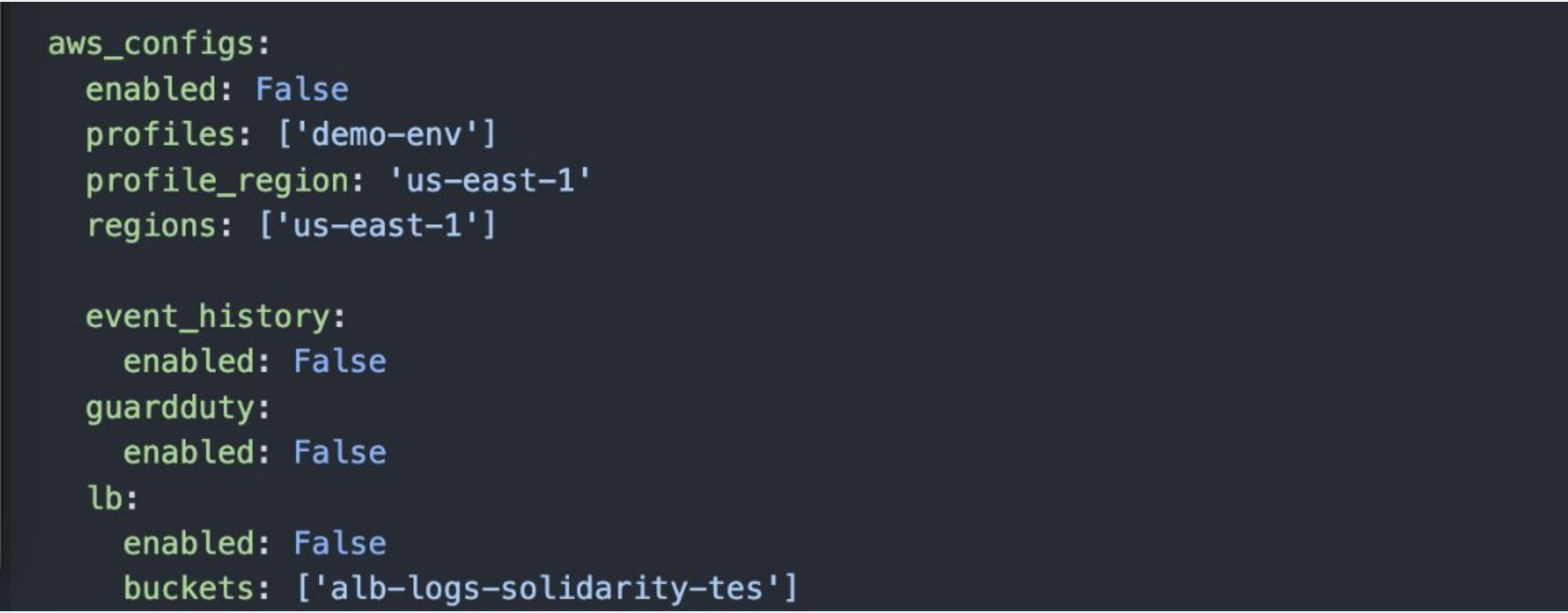
```
configs:
  start_date: '2023-09-29'
  end_date: '2023-09-30'
  destination_folder: 'logs_dredge'
  output_file: 'test1'
  shodan_api_key: '9R6Y860tl9q--------------------------'
  vt_api_key: '5294a7d0ff16------------------046aa2528dc0a4205'

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']
```

Dredge Setup - Configs



```
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'
```

Dredge Setup - Log Retrieval

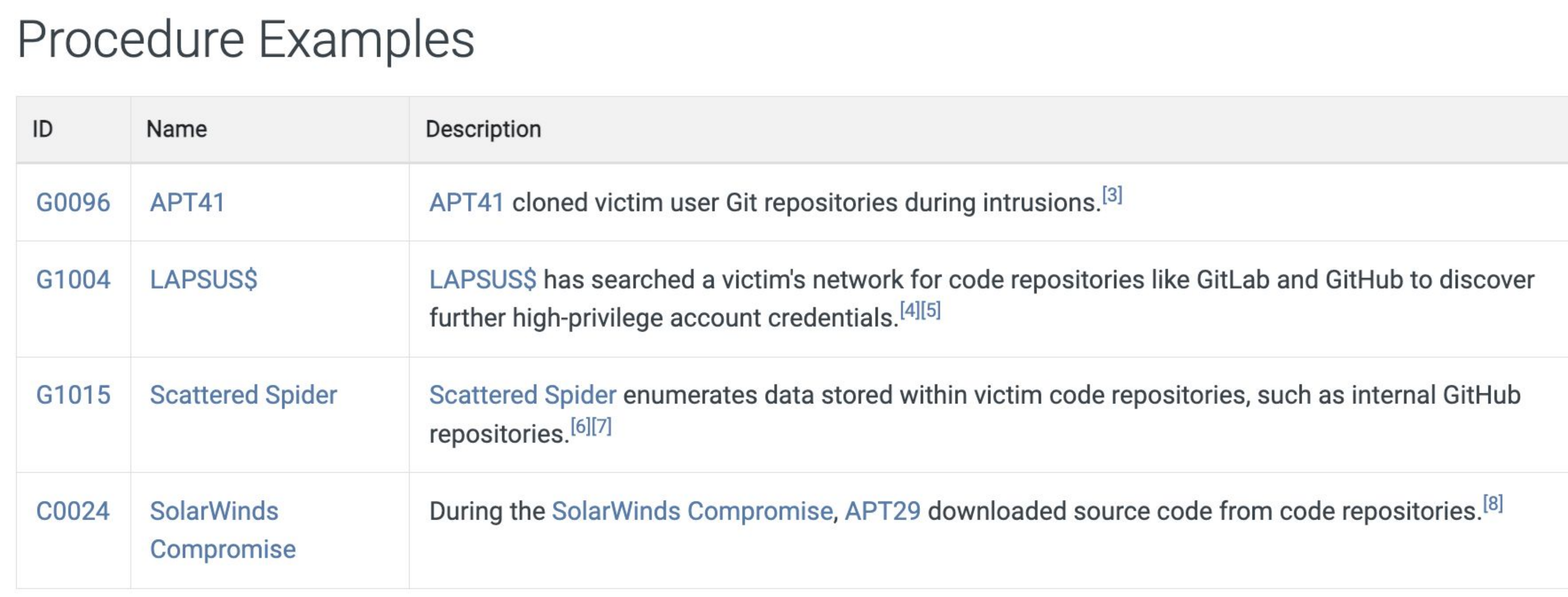


```
aws_configs:
  enabled: False
  profiles: ['demo-env']
  profile_region: 'us-east-1'
  regions: ['us-east-1']

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

2. Log Retriever

solidaritylabs.io/

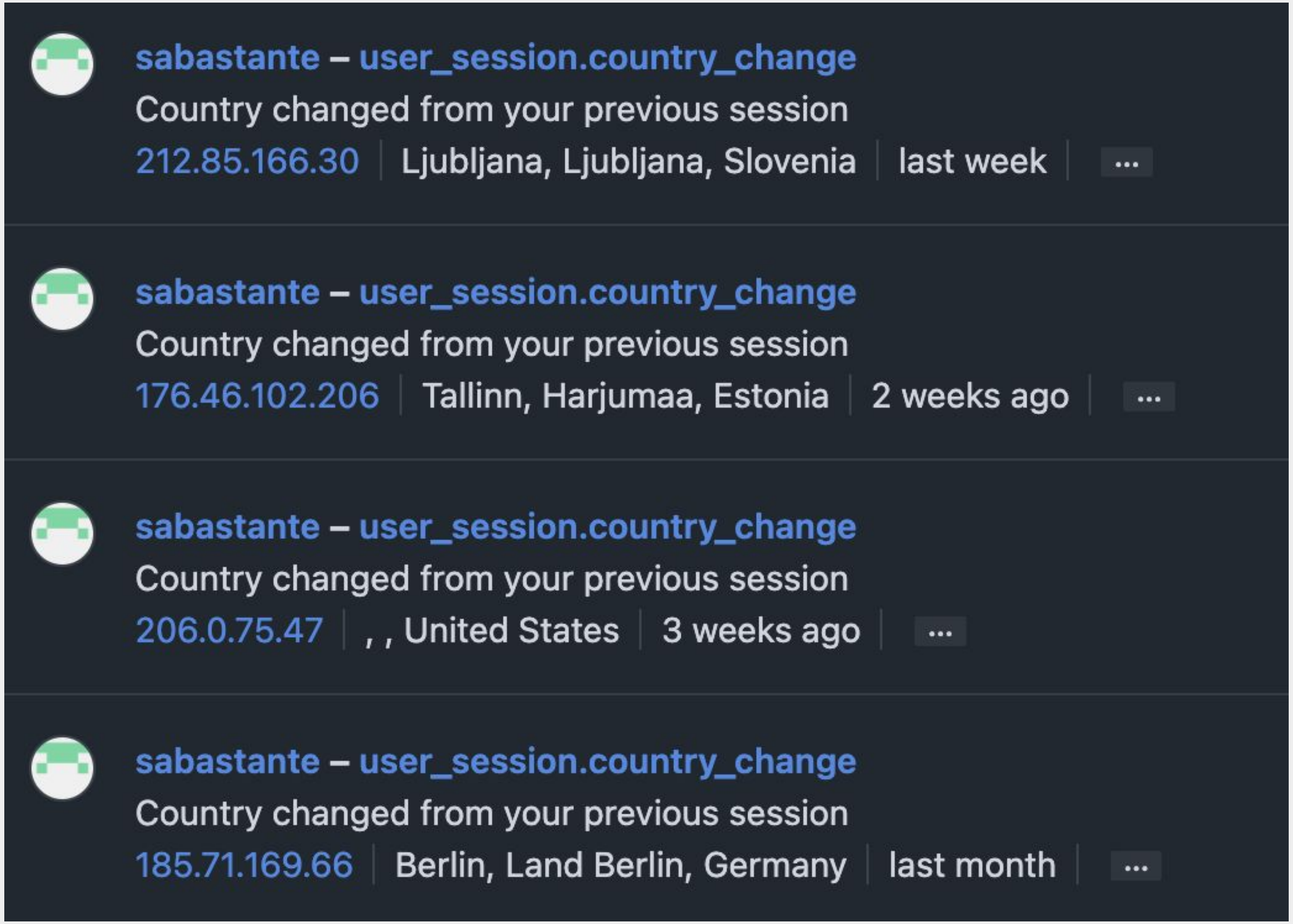
Data Collection | Code Repos - Github



Procedure Examples

ID	Name	Description
G0096	APT41	APT41 cloned victim user Git repositories during intrusions.[3]
G1004	LAPSUS$	LAPSUS$ has searched a victim's network for code repositories like GitLab and GitHub to discover further high-privilege account credentials.[4][5]
G1015	Scattered Spider	Scattered Spider enumerates data stored within victim code repositories, such as internal GitHub repositories.[6][7]
C0024	SolarWinds Compromise	During the SolarWinds Compromise, APT29 downloaded source code from code repositories.[8]

Github Logs



sabastante – user_session.country_change
Country changed from your previous session
212.85.166.30 | Ljubljana, Ljubljana, Slovenia | last week | ...

sabastante – user_session.country_change
Country changed from your previous session
176.46.102.206 | Tallinn, Harjumaa, Estonia | 2 weeks ago | ...

sabastante – user_session.country_change
Country changed from your previous session
206.0.75.47 | , , United States | 3 weeks ago | ...

sabastante – user_session.country_change
Country changed from your previous session
185.71.169.66 | Berlin, Land Berlin, Germany | last month | ...

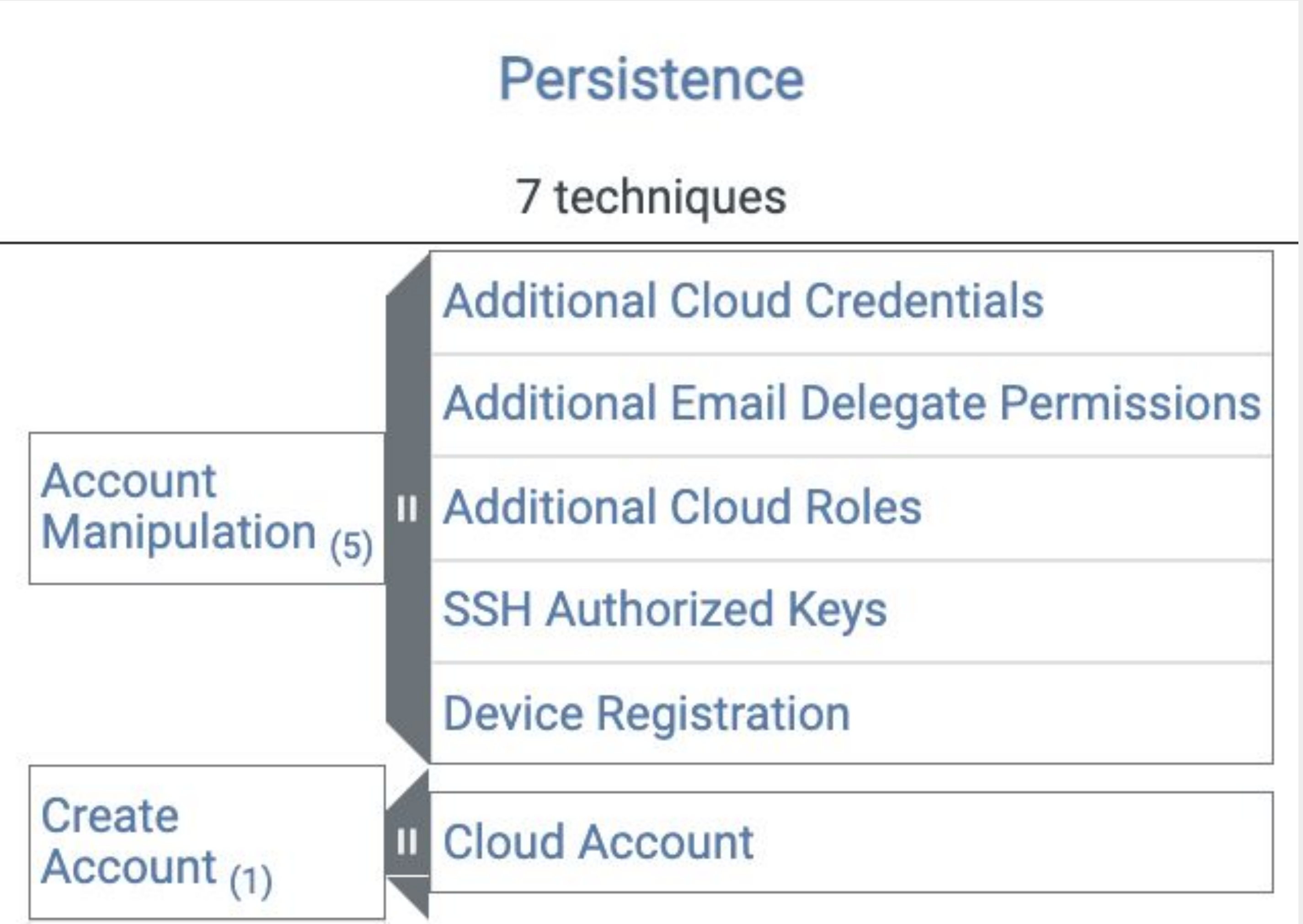
Demo 2.4

Getting Github Logs

3. Cloud Status for IR

solidaritylabs.io/

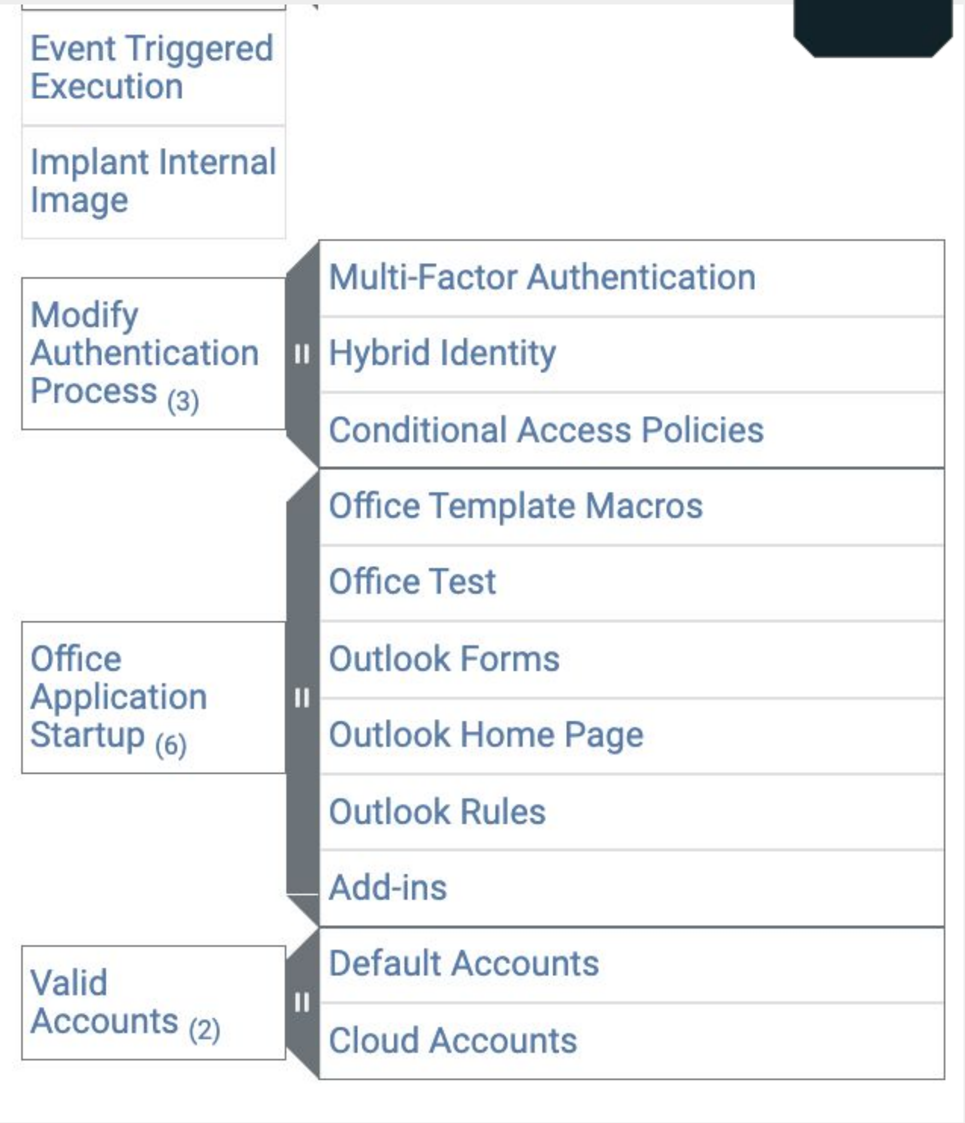
Cloud Persistance TTPs



Persistence

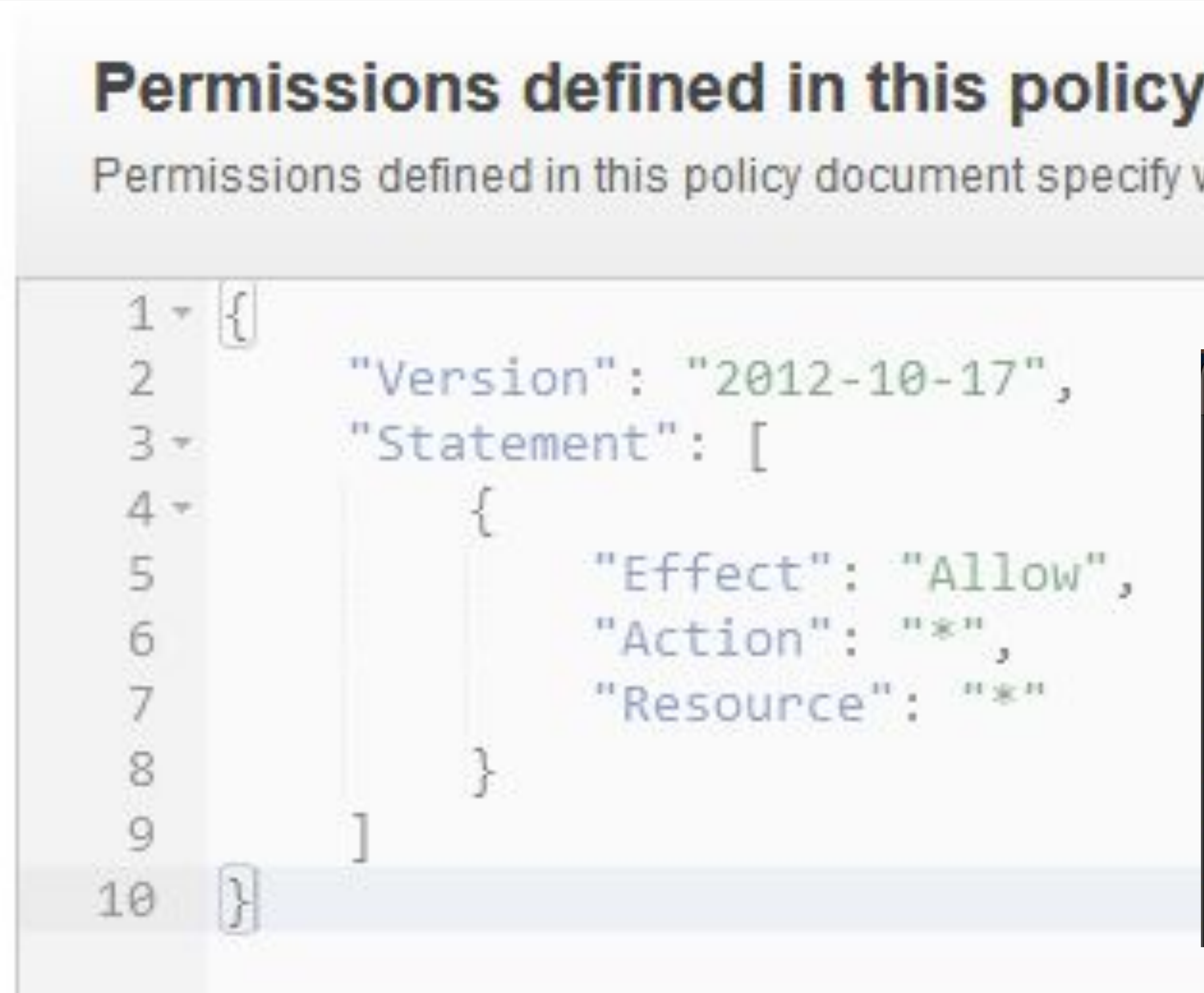
7 techniques

- Account Manipulation (5)
  - Additional Cloud Credentials
  - Additional Email Delegate Permissions
  - Additional Cloud Roles
  - SSH Authorized Keys
  - Device Registration
- Create Account (1)
  - Cloud Account



- Event Triggered Execution
- Implant Internal Image
- Modify Authentication Process (3)
  - Multi-Factor Authentication
  - Hybrid Identity
  - Conditional Access Policies
- Office Application Startup (6)
  - Office Template Macros
  - Office Test
  - Outlook Forms
  - Outlook Home Page
  - Outlook Rules
  - Add-ins
- Valid Accounts (2)
  - Default Accounts
  - Cloud Accounts

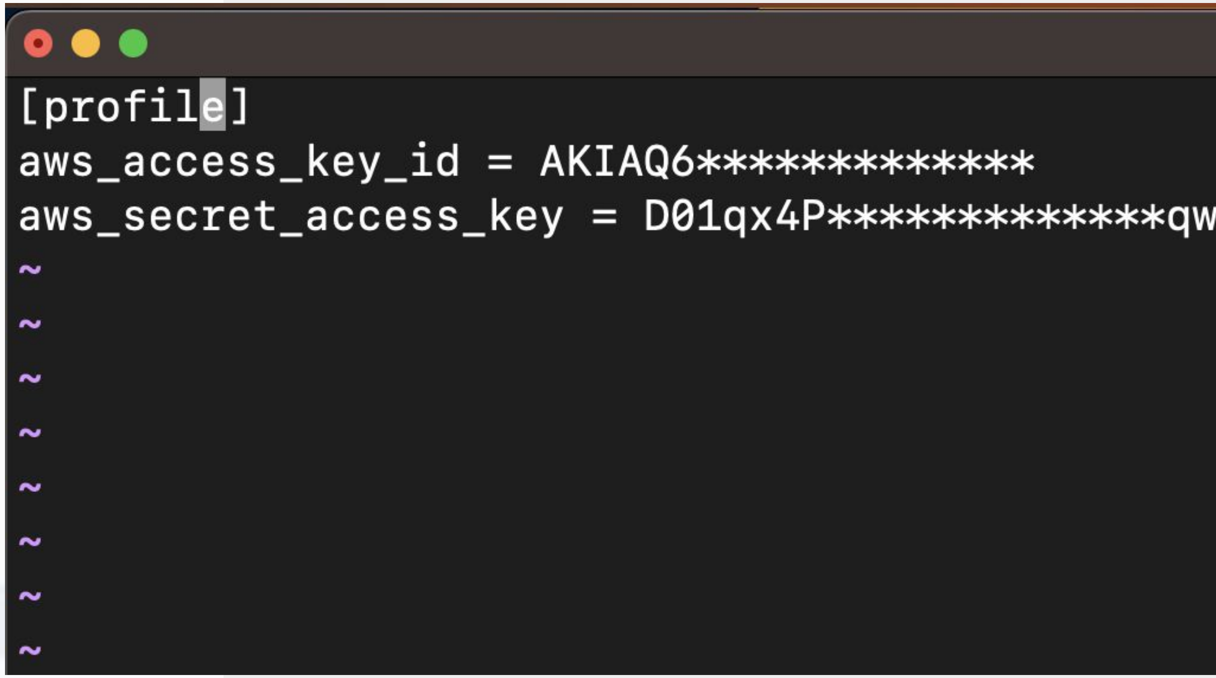
AWS IAM



Permissions defined in this policy Info

Permissions defined in this policy document specify which acti

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```



```
[profile]
aws_access_key_id = AKIAQ6*************
aws_secret_access_key = D01qx4P*************qw
~
~
~
~
~
~
~
~
```

Demo 3.1

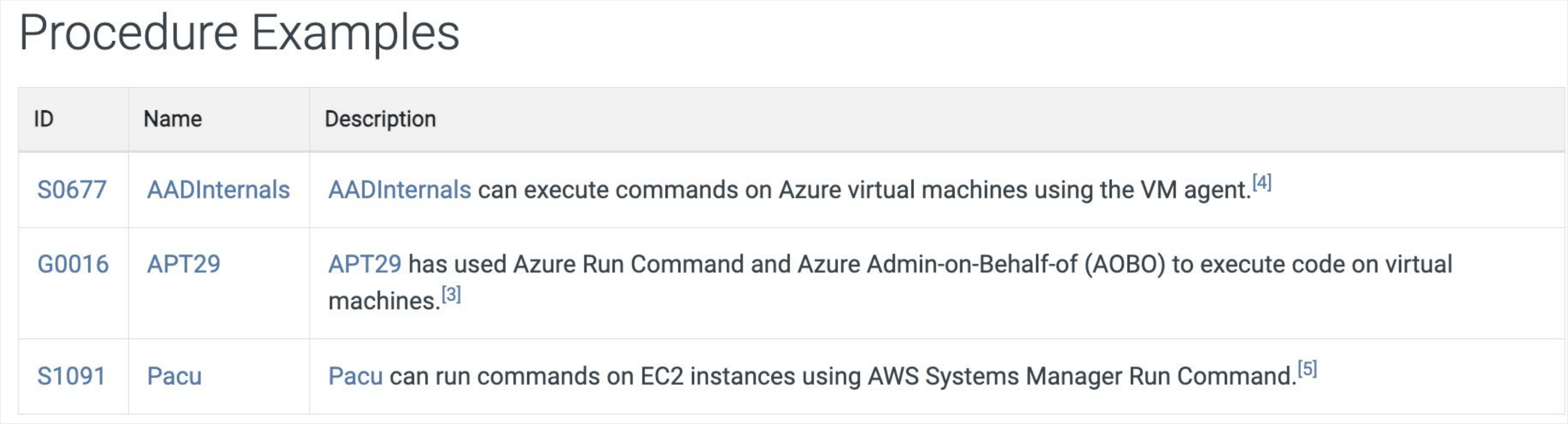
Getting AWS IAM Users

4. Incident Response

solidaritylabs.io/

Execution - Cloud Administration Command

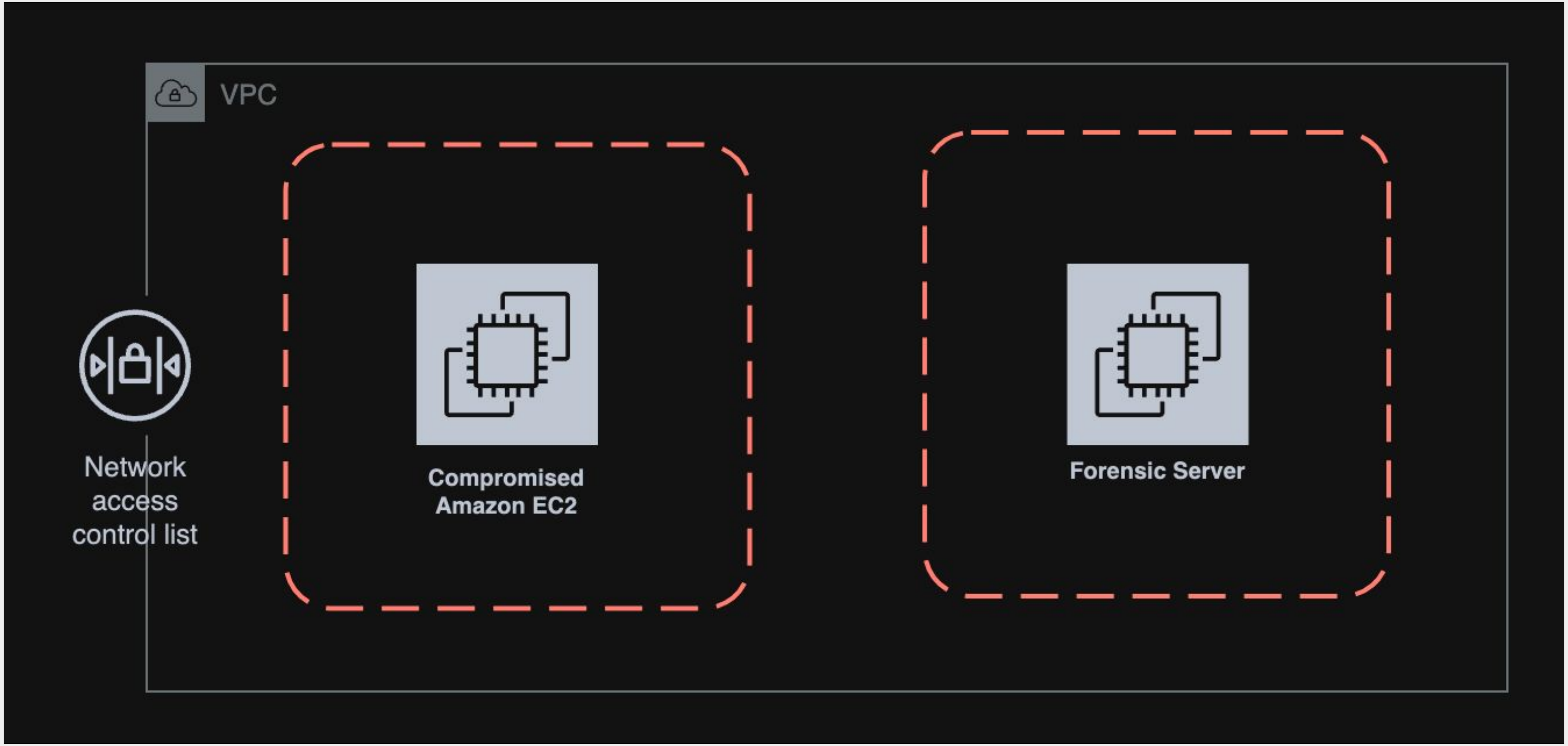
Execute Commands from a Cloud Server



Procedure Examples

ID	Name	Description
S0677	AADInternals	AADInternals can execute commands on Azure virtual machines using the VM agent.[4]
G0016	APT29	APT29 has used Azure Run Command and Azure Admin-on-Behalf-of (AOBO) to execute code on virtual machines.[3]
S1091	Pacu	Pacu can run commands on EC2 instances using AWS Systems Manager Run Command.[5]

Execution - Cloud Administration Command



Demo 4.3.3

Network Isolate EC2 Instance

5. Threat Hunting

solidaritylabs.io/

Demo 5.2

IoC Hunting in AWS

Demo 5.3.1

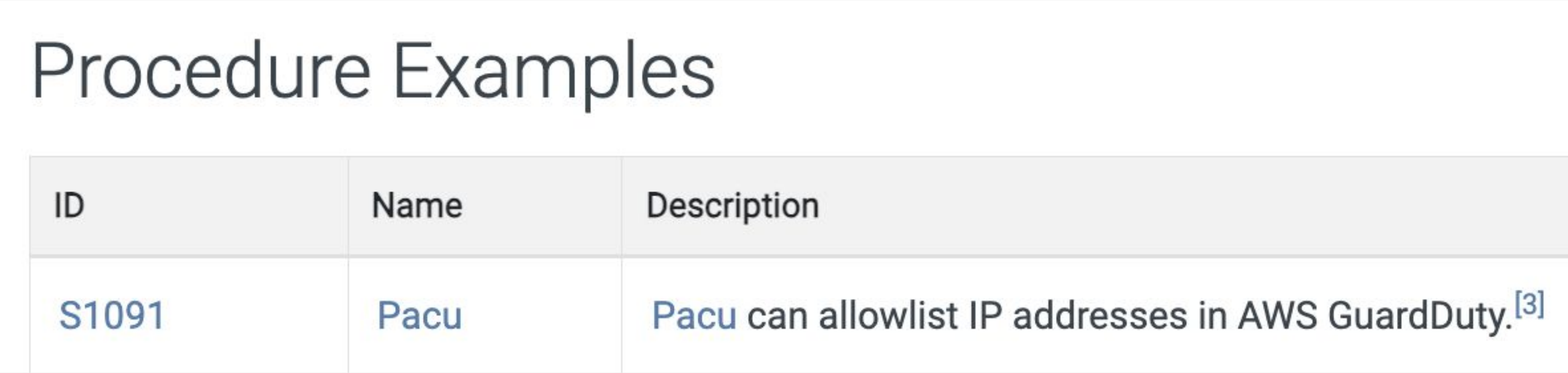
Hunting for AWS Persistance

Demo 5.3.2

Hunting for Cloud Lateral Movement

Impair Defenses: Disable or Modify Cloud Firewall

Adversaries may disable or modify a firewall within a cloud environment to bypass controls that limit access to cloud resources.



Procedure Examples

ID	Name	Description
S1091	Pacu	Pacu can allowlist IP addresses in AWS GuardDuty.[3]

Demo 5.3.3

Impair Defenses AWS

Questions?

solidaritylabs.io/