INVICTUS
INCIDENT RESPONSE

Incident Response Automation in AWS

Amsterdam 2022 FIRST Technical Colloquium
Korstiaan Stam, Founder Invictus Incident Response

Agenda

01 Introduction & Background
Short introduction and background on AWS Incident Response automation

02 Approach
Scope of the research and the methods used in the research

03 Invictus-AWS
The reveal of the script developed that enables AWS Incident Response automation

04 Analysis phase
Performing analysis on the collected data

05 Future
What’s next and how can we improve the current solution?

About Me

Professional

- Started my own IR firm in 2021
- Worked at PwC and led the IR team before that a cyber security specliast at Northwave
- Instructor in development at SANS
- Part-time cyber security lecturer in Amsterdam

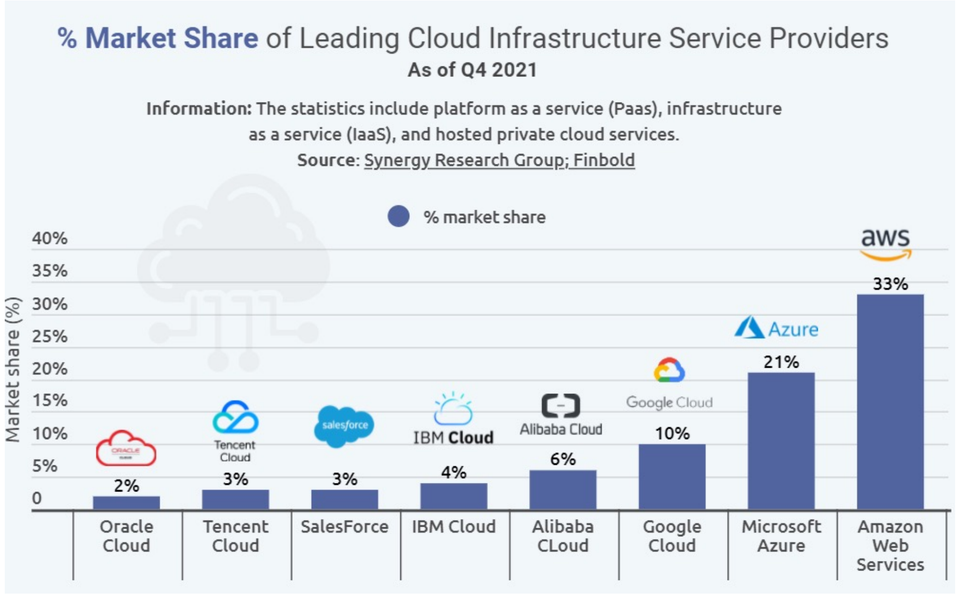
Personal

- Like to learn new stuff and keep myself busy
- Try to blog and do some more CTFs

INVICTUS
INCIDENT RESPONSE

1 Introduction
AWS Incident Response

AWS market leader



As an incident response firm or incident responder, we need to be able to quickly deploy in a client environment get an idea of what we're looking at to help our clients.

This is the main reason for our research and the talk today!

Source: Financialmirror

1 Introduction

Current state of AWS Incident Response

Organizations are not ready

Based on personal experience and talking with colleagues in the same field a lot of organizations that use cloud for their operations are not ready for incidents. Especially around forensic readiness and asset inventory.

Automation is slowly coming

Solutions to help you (automatically) acquire and investigate cloud data are slowly coming. Lots of public resources, scripts and blogs available showing the need for technology in the field.

An opportunity to do better

I strongly believe that the cloud offers an opportunity for defenders to do security better. With the shared responsibility model, you can identify where efforts and investments must be made. E.g., don’t need to have datacenter security or hardware security anymore.

Field is not mature yet

The field of AWS/Cloud incident response is not very mature yet. However, through training, certifications and many organizations moving to the cloud the field will mature over time. Also compared to on-premise hosting the field is still young.

1 Introduction
The challenge

Many, many services

Every AWS deployment is different, there are so many services clients can use. **Currently over 200 different services in AWS!**

Enumeration

It’s a challenge to enumerate all services quickly to understand what services the client uses.

Logs

AWS logs a lot, and every service can have their own logging. We need to identify quickly what’s available and useful for our investigation.

Complexity

AWS can become complex quickly, regions, permissions. You don’t want to spend too much time in the beginning of your investigation to understand the environment.

2 Approach
Security Research

We decided to invest time and resources in investigating how we can automate parts of the research. Together with two brilliant students from the UvA we developed a method to automate parts of the incident response process in AWS. The goal is to use native AWS solutions to automate parts of the IR process in AWS.

Antonio Macovei
https://www.linkedin.com/in/antonio-macovei/

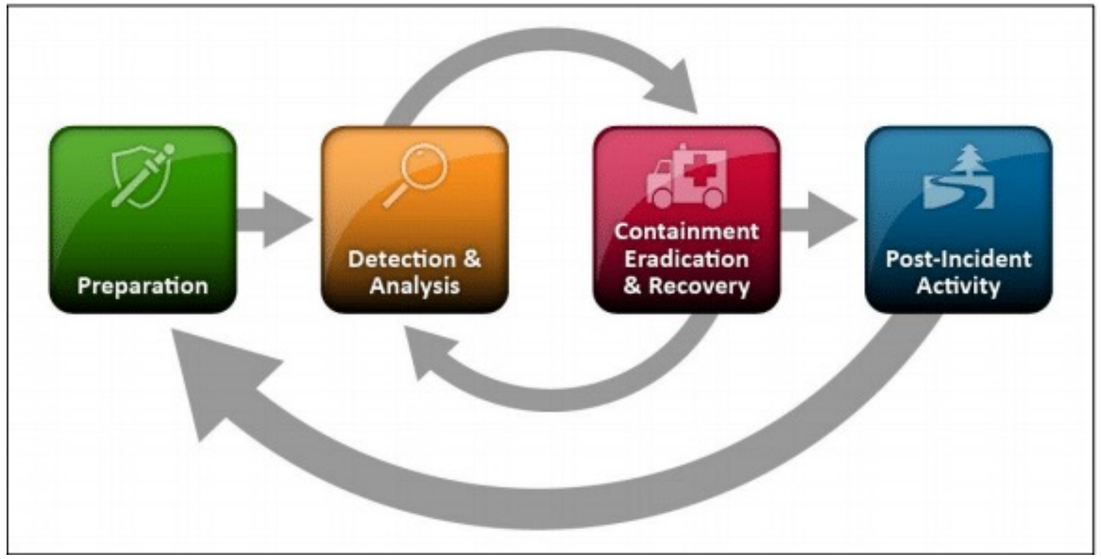
Rares Bratean
https://www.linkedin.com/in/raresbratean/

Without their work this wouldn’t have been possible.

2 Approach
NIST Incident Handling

Activities

1. Gather evidence
2. Analyse evidence to contain and eradicate the incident
3. Recover from the incident
4. Conduct post-incident activities, including post-mortem and feedback processes



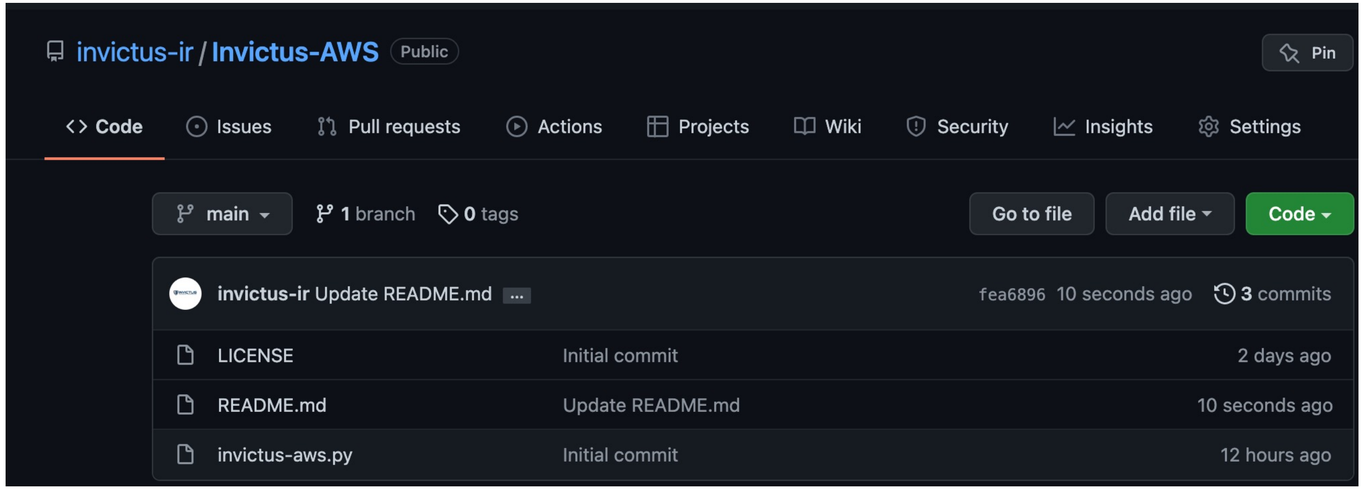
This talk is mostly on automating Phase 1, with some examples and ideas for Phase 2.

Source: NIST

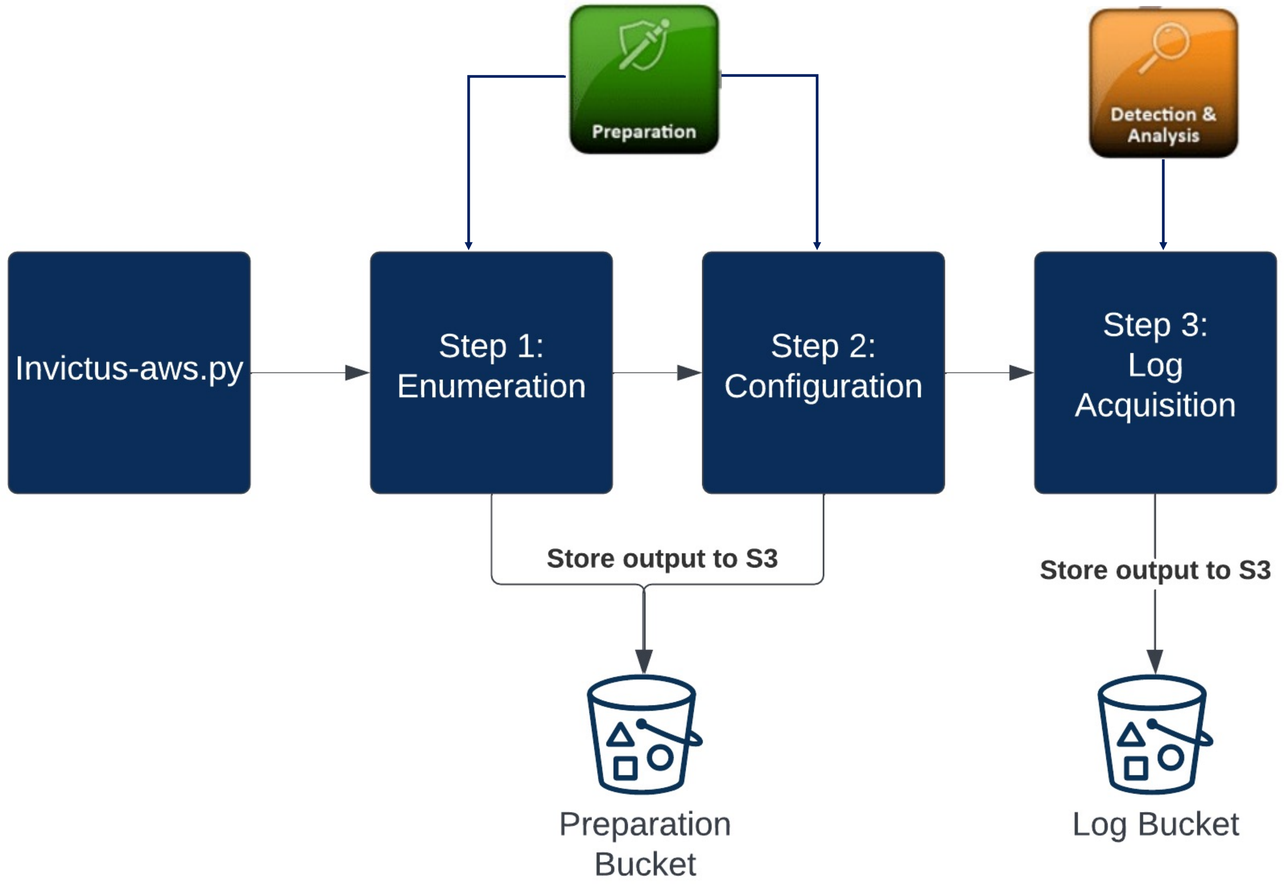
3 Invictus-AWS
Overview

Stand alone Python script

- Uses ‘aws’ commands and ‘boto’
- Free to use under license available
- Available as of today ☺ on https://github.com/invictus-ir/Invictus-AWS
- Suggestions and improvements are welcome



3 Invictus-AWS
Features

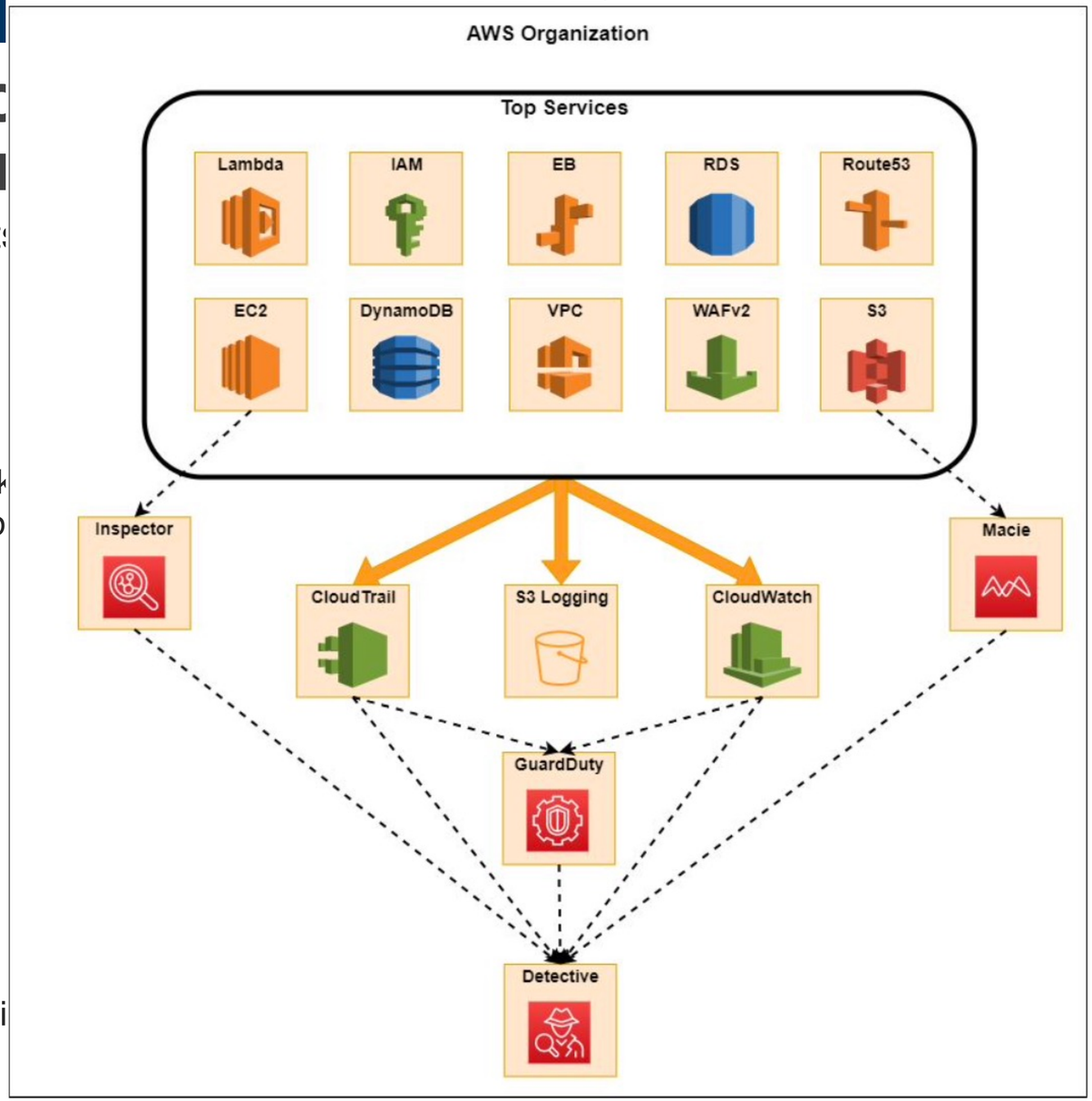


3 In
Sc

The script collect
- ✓ EC2
- ✓ S3 storage
- ✓ VPC
- ✓ IAM
- ✓ Lambda
- ✓ Elastic Beanstalk
- ✓ Relational Datab
- ✓ Web Application
- ✓ Route53
- ✓ Dynamo DB

Premium services
- ✓ CloudTrail*
- ✓ Inspector
- ✓ CloudWatch
- ✓ GuardDuty
- ✓ Detective
- ✓ Macie
- ✓ S3 Access Loggi

emium services.



*CloudTrail is on by default, the rest is not

3 Invictus-AWS
Phase 1 - Preparation

INVICTUS INCIDENT RESPONSE

Enumeration
- Verify which services are available
- Use AWS commands that involve “list” and “describe”
- Export the results for all services in one JSON file

```
def enumerate_s3(self):
    s3 = boto3.client('s3')
    response = s3.list_buckets()
    response.pop('ResponseMetadata')
    buckets = fix_json(response)
```

Configuration
- For each available service, extract its configuration
- Use commands that involve “get”, “describe” and “list”
- Export the results per service in a JSON file

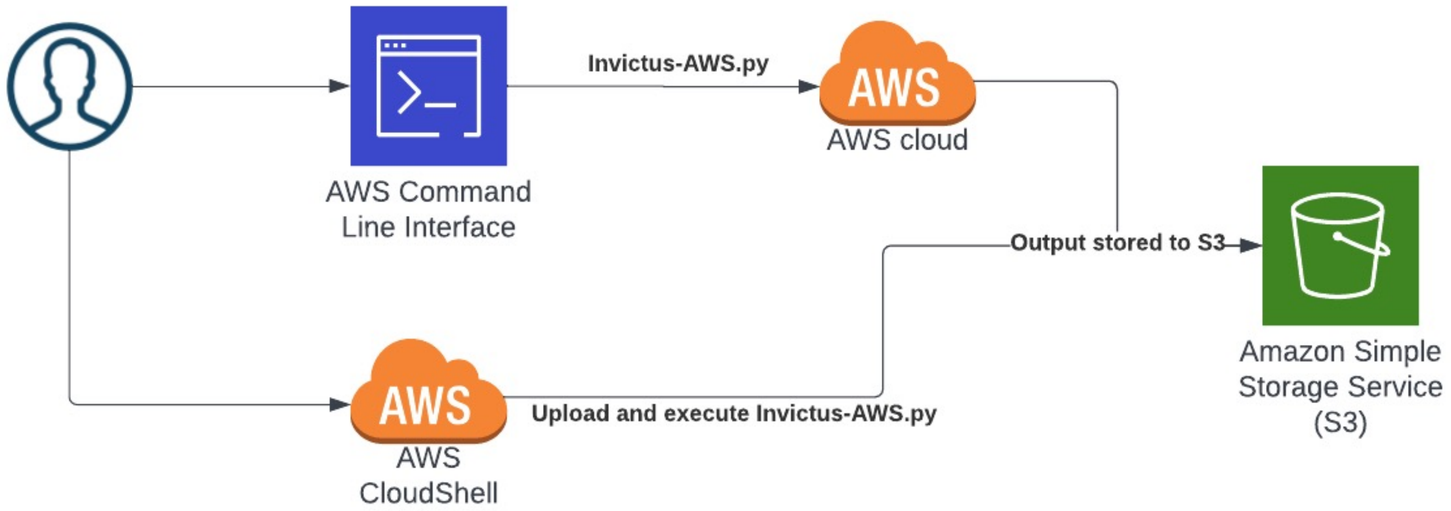
```
def get_configuration_s3(self):
    s3 = boto3.client('s3')

    response = s3.list_buckets()
    response.pop('ResponseMetadata')
    buckets = fix_json(response)
    buckets = buckets['Buckets']

    objects = {}
    buckets_logging = {}
    buckets_policy = {}
    buckets_acl = {}
    buckets_location = {}
```

3 Invictus-AWS
Phase 2 – Detection & Analysis

Log extraction

- Extract logs from:
- CloudTrail, CloudWatch, S3 buckets
- Other sources (EC2, RDS, EB system logs)
- Store the results in an S3 bucket

Script can be executed using AWS CLI or AWS CloudShell



3 Invictus-AWS
Setup

Prerequisites

1. Access to AWS environment with sufficient permissions

Permissions determine the resources you can access. The script is ‘region fixed’ so it will **only** enumerate the services in the specified region.

2. Configure the script

✓ You **only** have to specify the region (e.g. eu-west-1)

3. Run the script:

- AWS Cloudshell, run it directly in AWS cloud

or

- AWS CLI, run it locally

3 Invictus-AWS

AWS CLI

1. Install Boto3 to run AWS commands

$pip3 install boto3

2. Configure AWS account

$aws configure

Note: This requires the AWS Access Key ID for the account you use to run the script.

3. Execute script

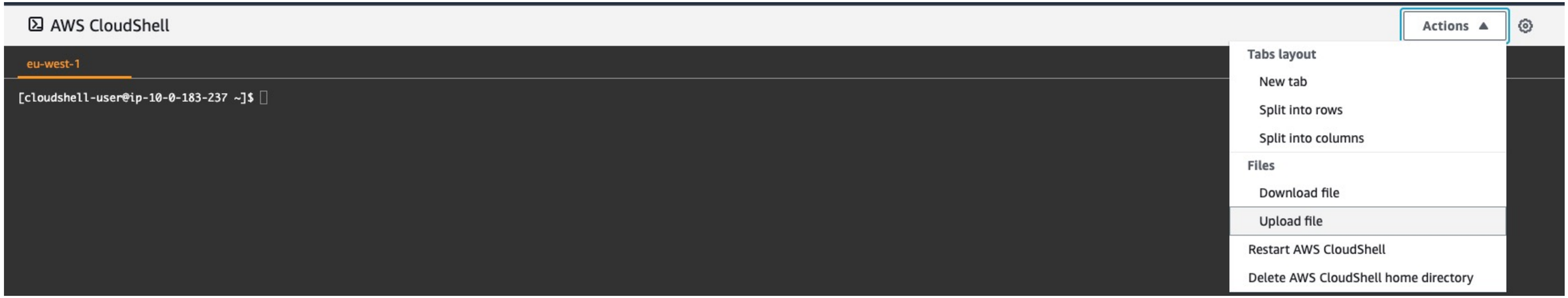
$python3 invictus-aws.py –-region=<insert AWS region>

3 Invictus-AWS

INVICTUS INCIDENT RESPONSE

AWS CloudShell

Step 1 – Upload script to CloudShell

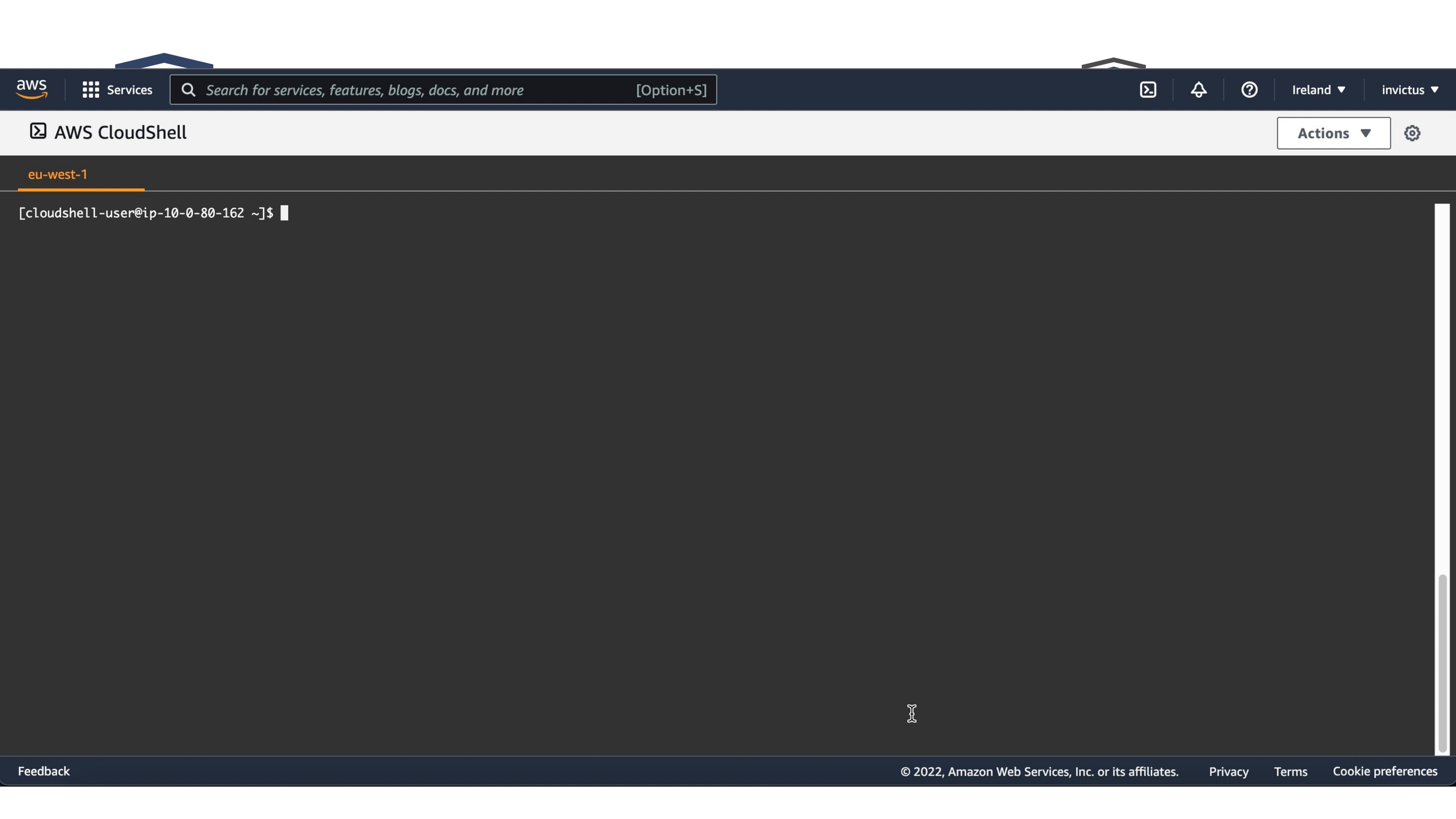


Step 2 – Run script in CloudShell

$python3 invictus-aws.py –-region=<insert AWS region>

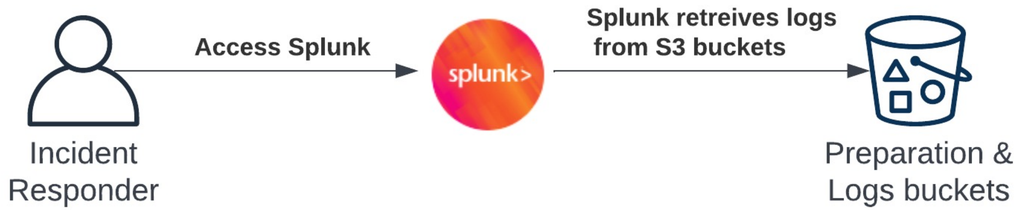
Step 3 – Output is stored in S3 buckets

Name	AWS Region	Access	Creation date
invictus-aws-2022-04-12-psv7a	EU (Ireland) eu-west-1	Objects can be public	April 12, 2022, 08:53:19 (UTC+02:00)
invictus-aws-2022-04-11-yeyya	EU (Ireland) eu-west-1	Objects can be public	April 11, 2022, 11:12:03 (UTC+02:00)
invictus-aws-2022-04-11-3q6xr	EU (Ireland) eu-west-1	Objects can be public	April 11, 2022, 11:03:25 (UTC+02:00)
invictus-aws-2022-04-11-qruwk	EU (Ireland) eu-west-1	Objects can be public	April 11, 2022, 10:13:12 (UTC+02:00)
invictus-aws-2022-04-07-hcyro	EU (Ireland) eu-west-1	Objects can be public	April 7, 2022, 17:01:51 (UTC+02:00)


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Ireland
invictus
AWS CloudShell
Actions
eu-west-1
[cloudshell-user@ip-10-0-80-162 ~]$
Feedback
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

4 Analysis
Overview

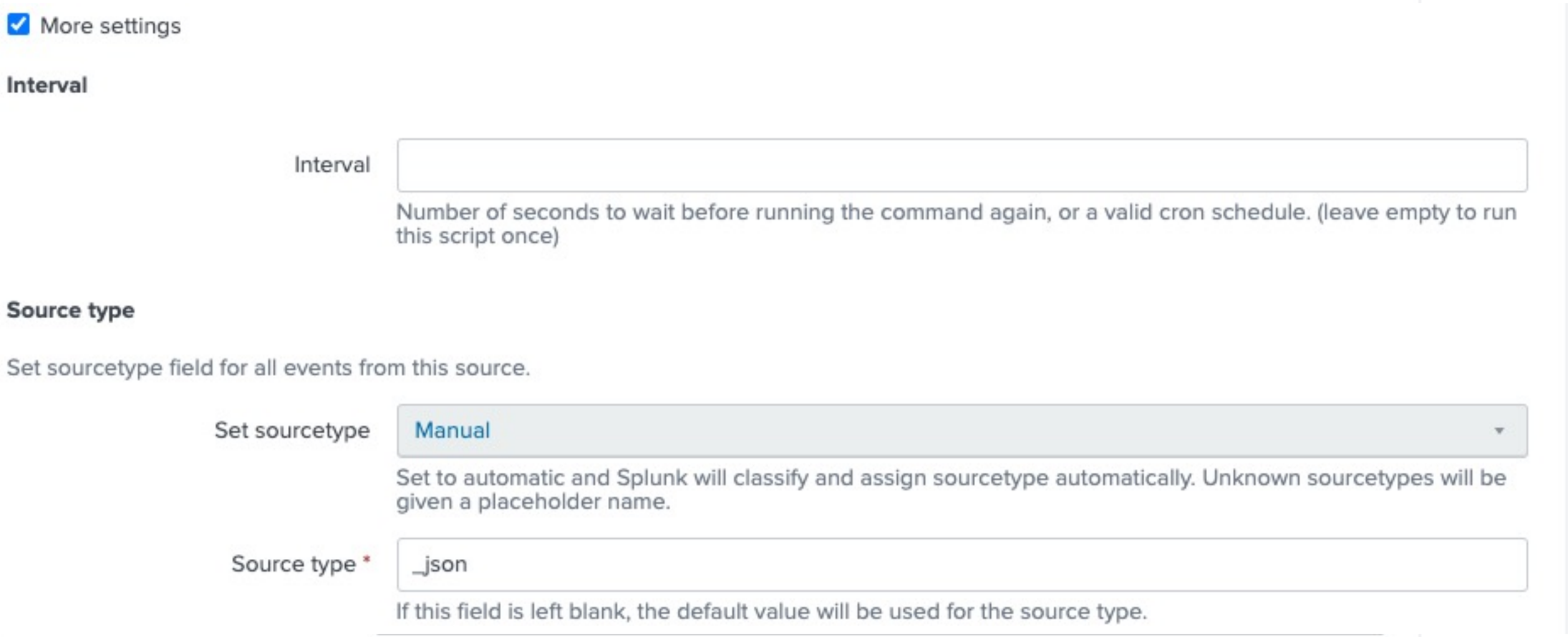
Use Splunk



Alternative, use your own tools

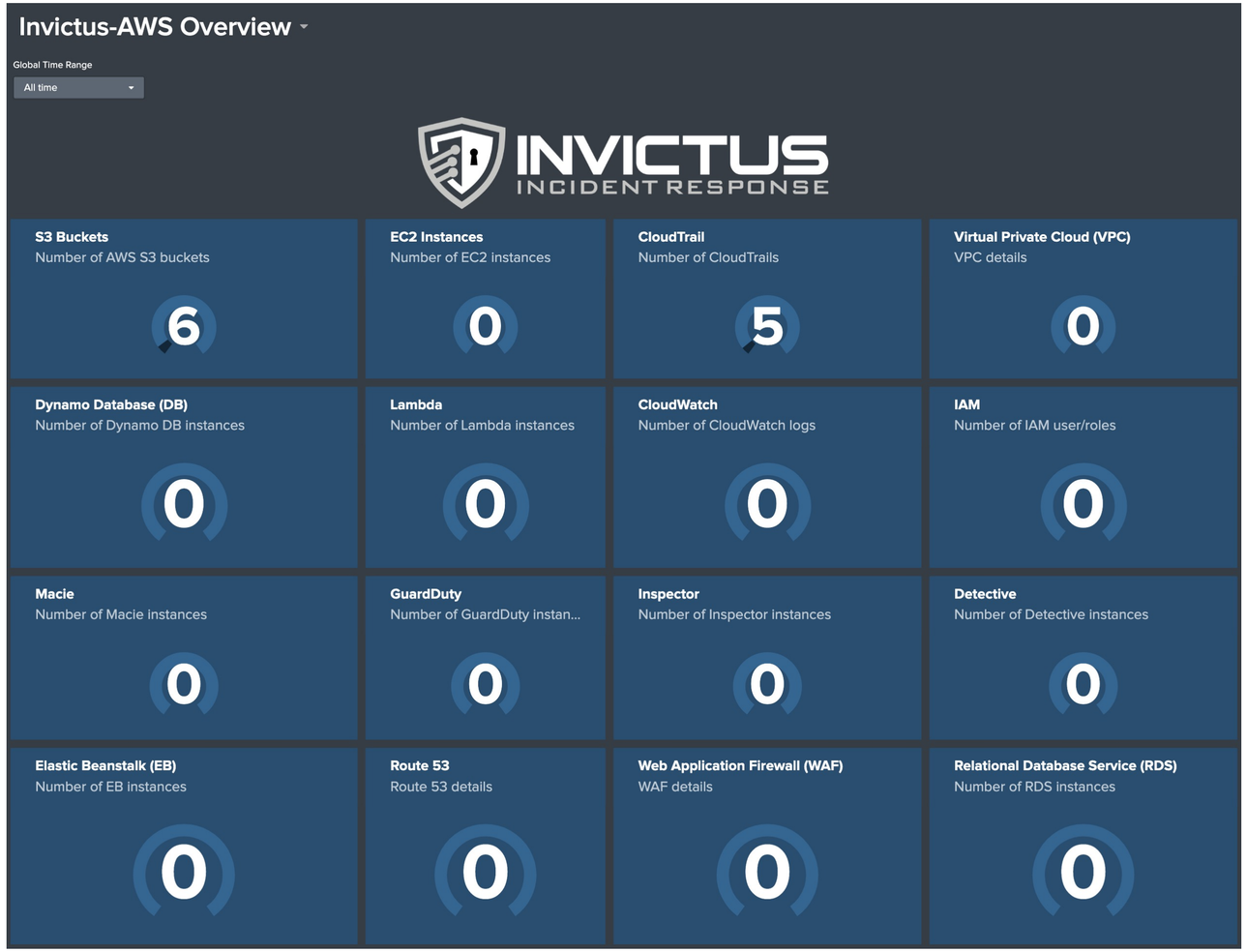
- Retrieve logs from S3 buckets
- Parse .json files and analyze .json files in your preferred tool

4 Analysis
Automated retrieval

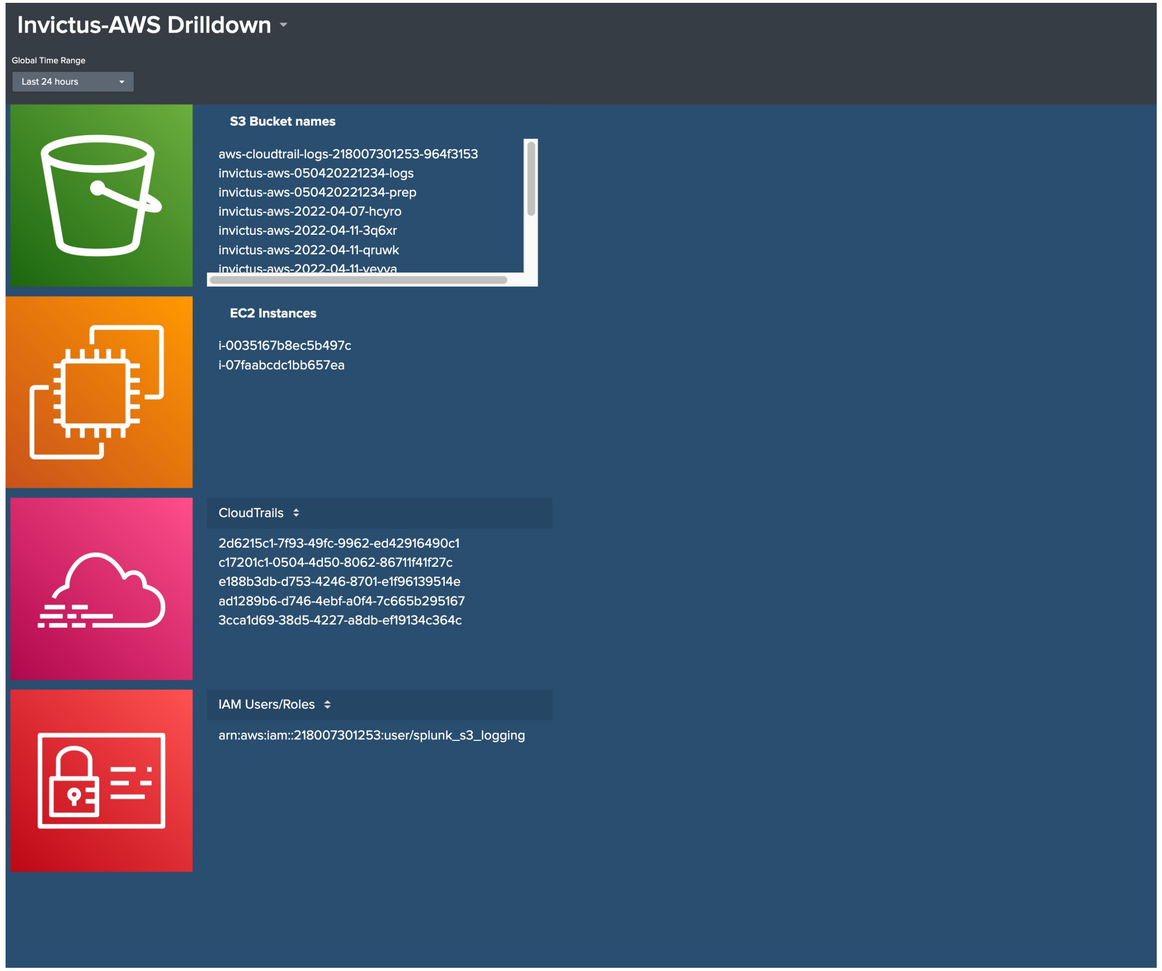


https://hurricanelabs.com/splunk-tutorials/your-step-by-step-guide-for-splunking-data-in-amazon-s3/

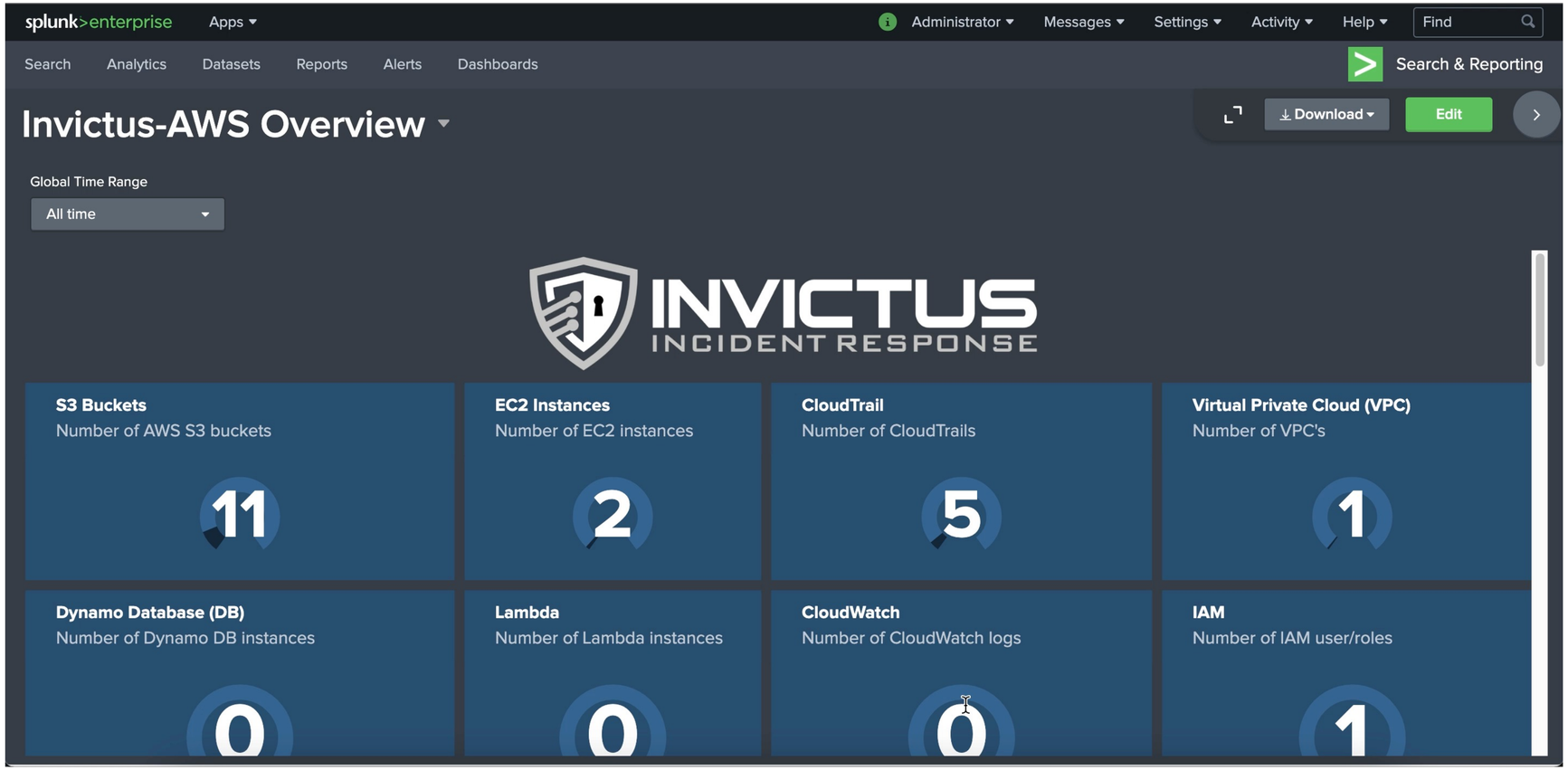
4 Analysis
Overview



4 Analysis
Drilldown



4 Analysis
Demo



YouTube: https://youtu.be/0ysUt1stPlI

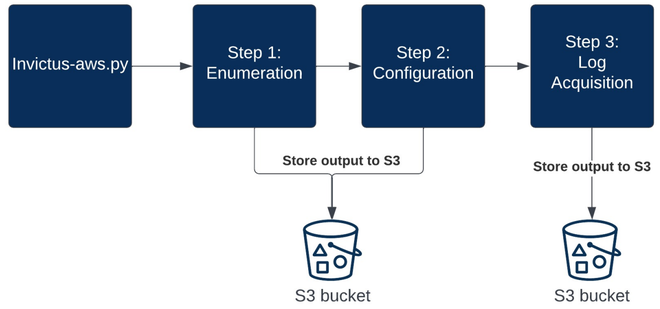
4 Analysis
Other resources

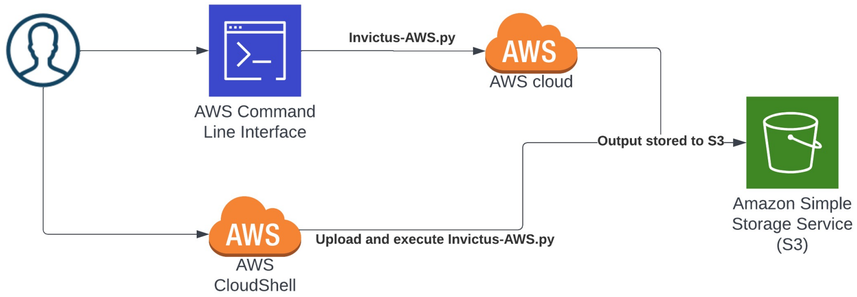
Threat Hunting on CloudTrail logs
https://medium.com/@george.fekkas/quick-and-dirty-cloudtrail-threat-hunting-log-analysis-b64af10ef923

Visualize CloudTrail/CloudWatch data and integrations by AWS
https://aws.amazon.com/blogs/aws/cloudwatch-logs-subscription-consumer-elasticsearch-kibana-dashboards/

Splunk App for AWS, contains lots of default searches for CloudTrail
https://splunkbase.splunk.com/app/1274/

4 Analysis
Conclusion





5 The future
What is next?

Add additional services

Not all services are supported, extend the tool to support additional services.

Interface with other tools

It would be great to extend Invictus-AWS to other tools to cover more of the IR lifecycle. For example, collecting snapshots and memory from an AWS instance

Extract more logging

The dream is to built a tool, that can automatically identify all possibly relevant logging in an AWS environment with the ability to extract everything.

Support AWS global collection

The tool currently only works in a certain region this is because some of the sub commands for enumeration and configuration require region information. Further research is required to identify whether it’s possible to modify the script so it can be run globally instead of per region.

THANK YOU

Korstiaan Stam (@korstiaans)
Founder, Invictus Incident Response
E: korstiaan@invictus-ir.com
W: invictus-ir.com

Resources

Invictus-AWS:

- https://github.com/invictus-ir/Invictus-AWS

Slides:

- https://github.com/invictus-ir/talks

Splunk dashboard:

- Contact us info@invictus-ir.com

Blog:

- https://invictus-ir.medium.com/