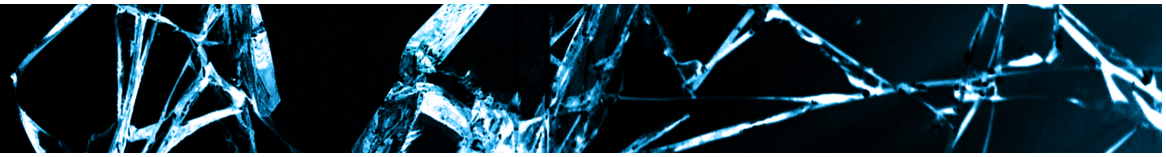


Hardening AWS Environments

and

Automating Incident Response

for

AWS Compromises

Disclaimer

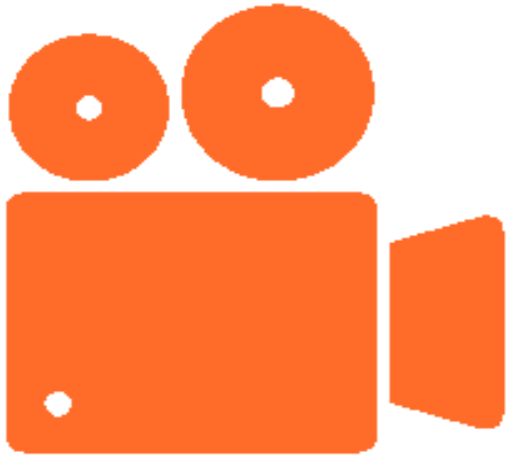
Everything you're about to see is our opinion.

Not a guaranteed IR process.

This will *not* replace preparedness or an incident response retainer.

A Challenge

Video Demonstration

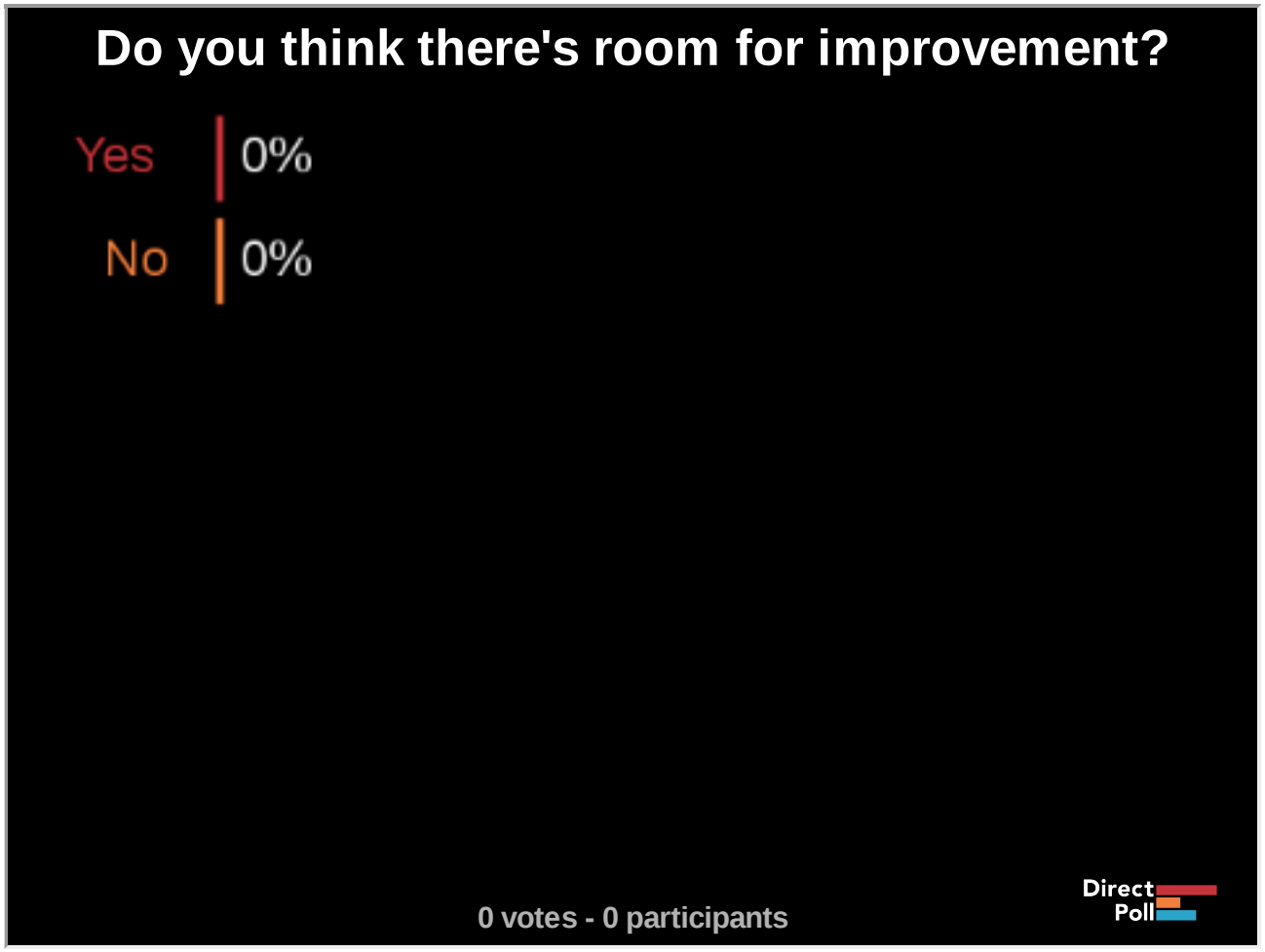


ThreatResponse
CLOUD SECURITY

Poll

http://etc.ch/zT5A

Results


Do you think there's room for improvement?
Yes
0%
No
0%
0 votes - 0 participants
Direct Poll

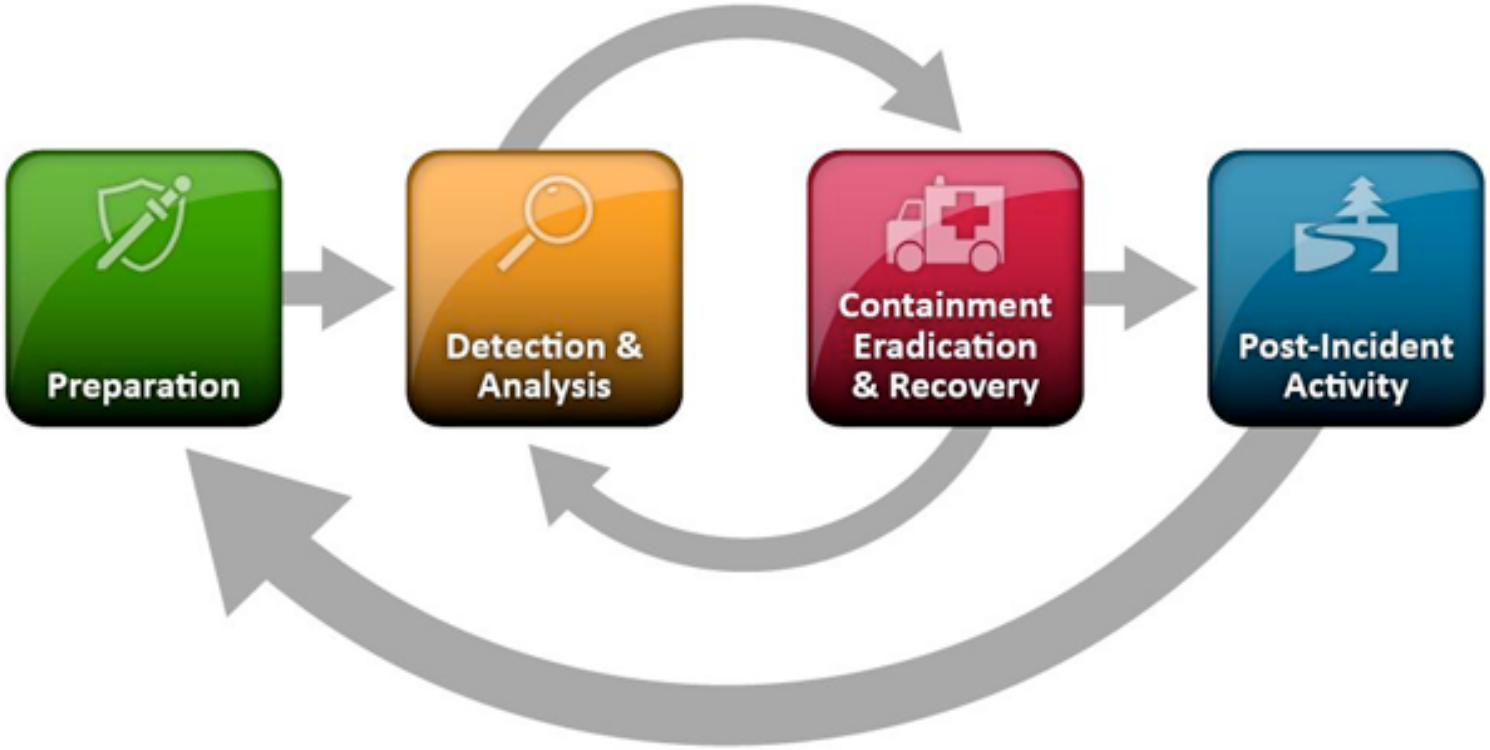
System console output

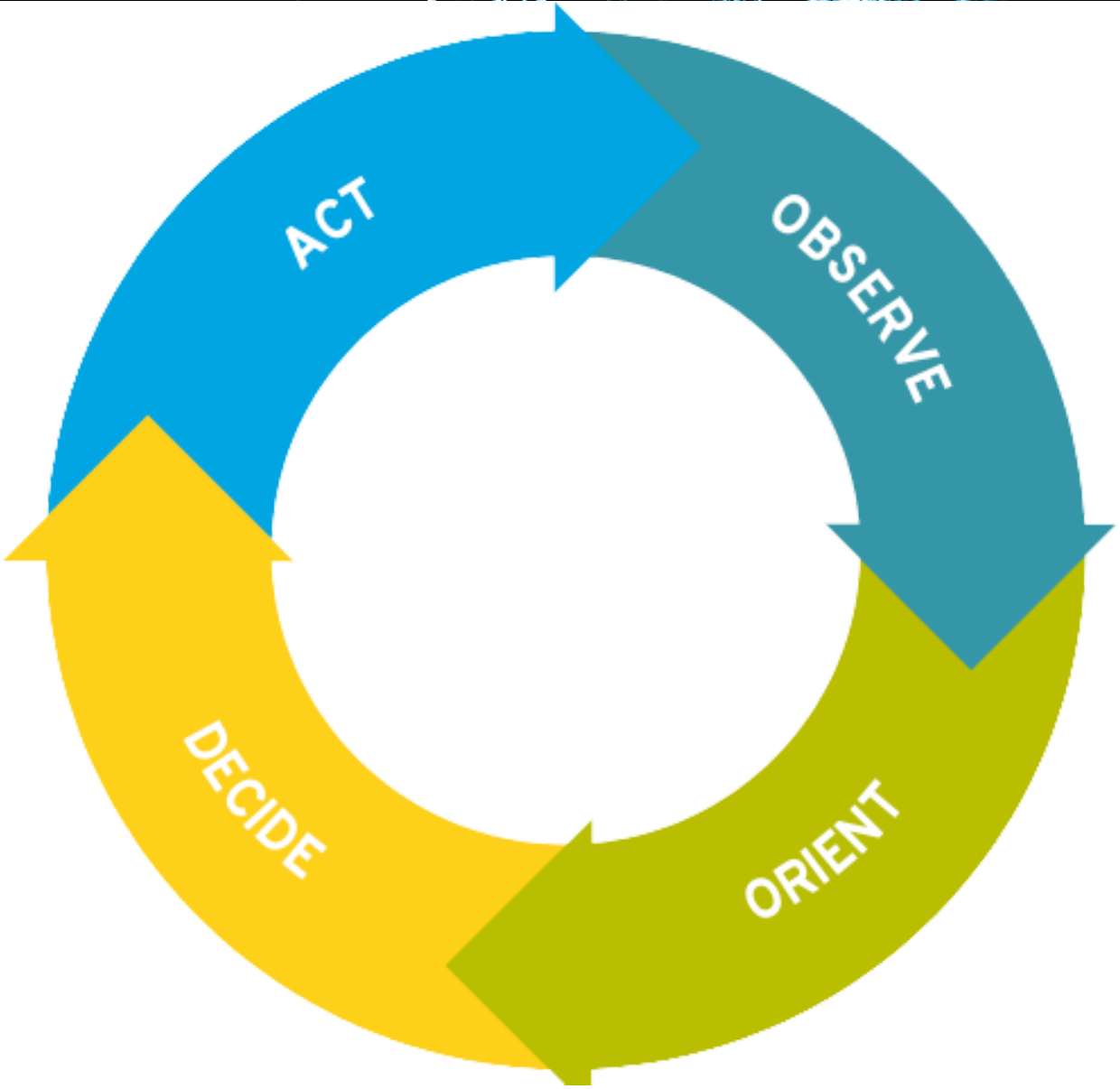
Live system screenshot

Instance MetaData

CloudTrail Logs and VPC FlowLogs

Recent Launches and Memory

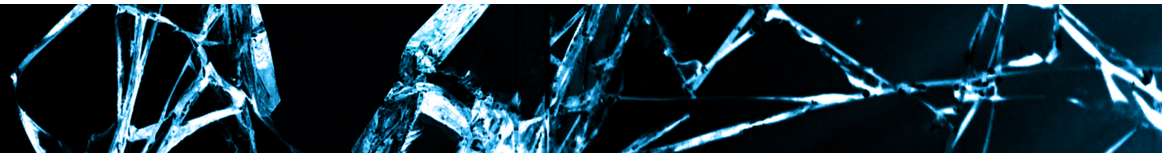

Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity


ACT
OBSERVE
ORIENT
DECIDE

Expediance

Scope

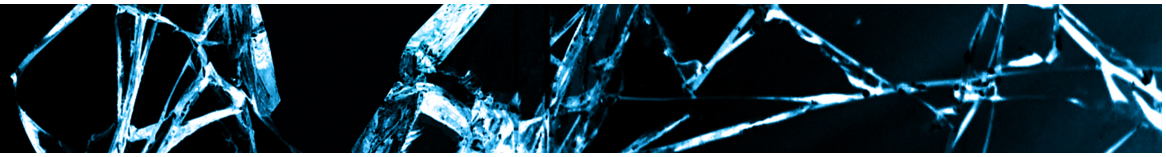
Remediate



The Beginning

Best *Free*

IR Process



Step 1

Disable the Access Keys

```
aws iam list-access-keys

aws iam update-access-key \
--access-key-id AKIAIOSFODNN7EXAMPLE \
--status Inactive \
--user-name DeveloperDave
```

Step 2

Hunt new instances

```
aws ec2 describe-instances\
    --region us-east-1 \
          --query
      'Reservations[].\
          Instances[
?LaunchTime>=`2016-03-9`][].\
                  {
         id: InstanceId,
       type: InstanceType,
      launched: LaunchTime
                 }
                '
```

Step 3

Tell AWS Support

Step 4

Isolate

```
aws ec2 create-security-group \
    --group-name isolation-sg
aws ec2 authorize-security-group-ingress
aws ec2 authorize-security-group-ingress \
    --group-id sg-BLOCK-ID \
    --protocol
aws ec2 modify-instance-attribute
  --instance-id i-INSTANCE-ID \
    --groups sg-BLOCK-ID
```

Step 5

Tag the Instance

```
aws ec2 create-tags \
--resources i-INSTANCE-ID \
--tags “Key=Environment, \
Value=Quarantine:REFERENCE-ID”
```

Step 6

Save the instance metadata

```
aws ec2 describe-instances \
--instance-ids i-INSTANCE-ID > \
    forensic-metadata.log

aws ec2 get-console-output \
 --instance-id i-INSTANCE-ID
```

Step 7

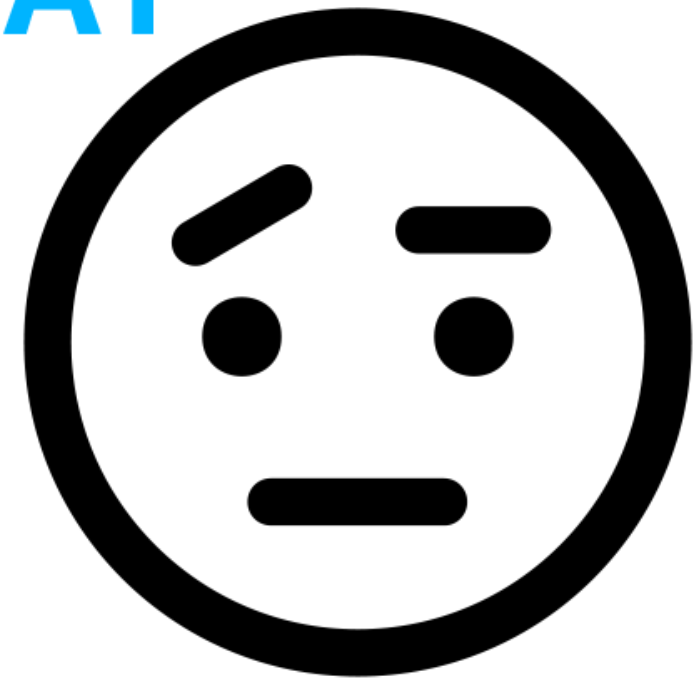
Preserve Disk Data

```
aws ec2 create-snapshot \
  –-volume-id vol-xxxx \
    –-description \
“IR-ResponderName- Date-REFERENCE-ID”
```

Step 8

Acquire Memory

WAT



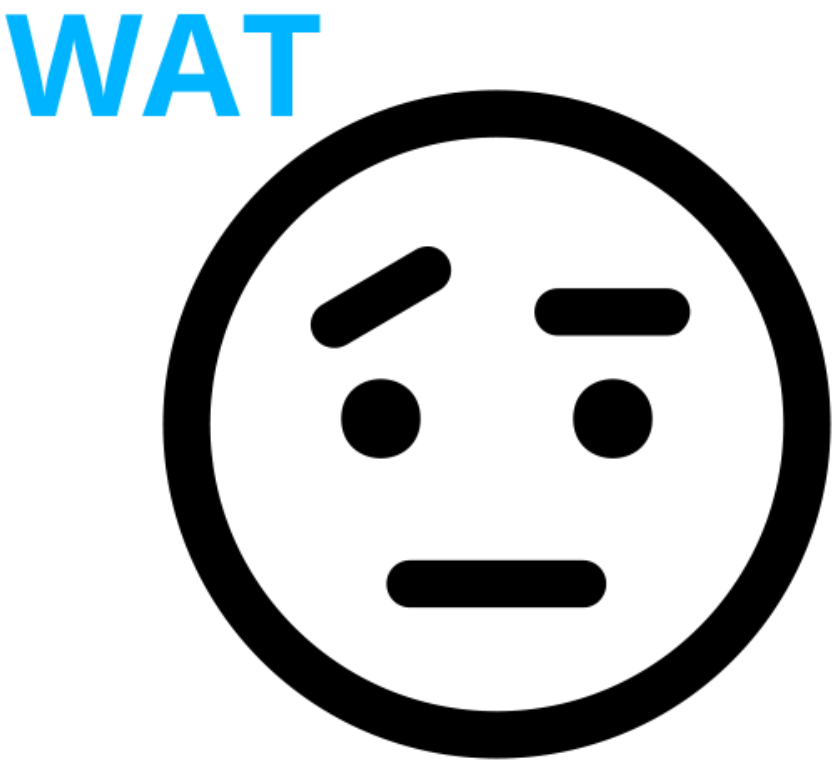
Step 9

Stop the Instance

```
aws ec2 stop-instances \
--instance-ids i-INSTANCE-ID
```

Step 10

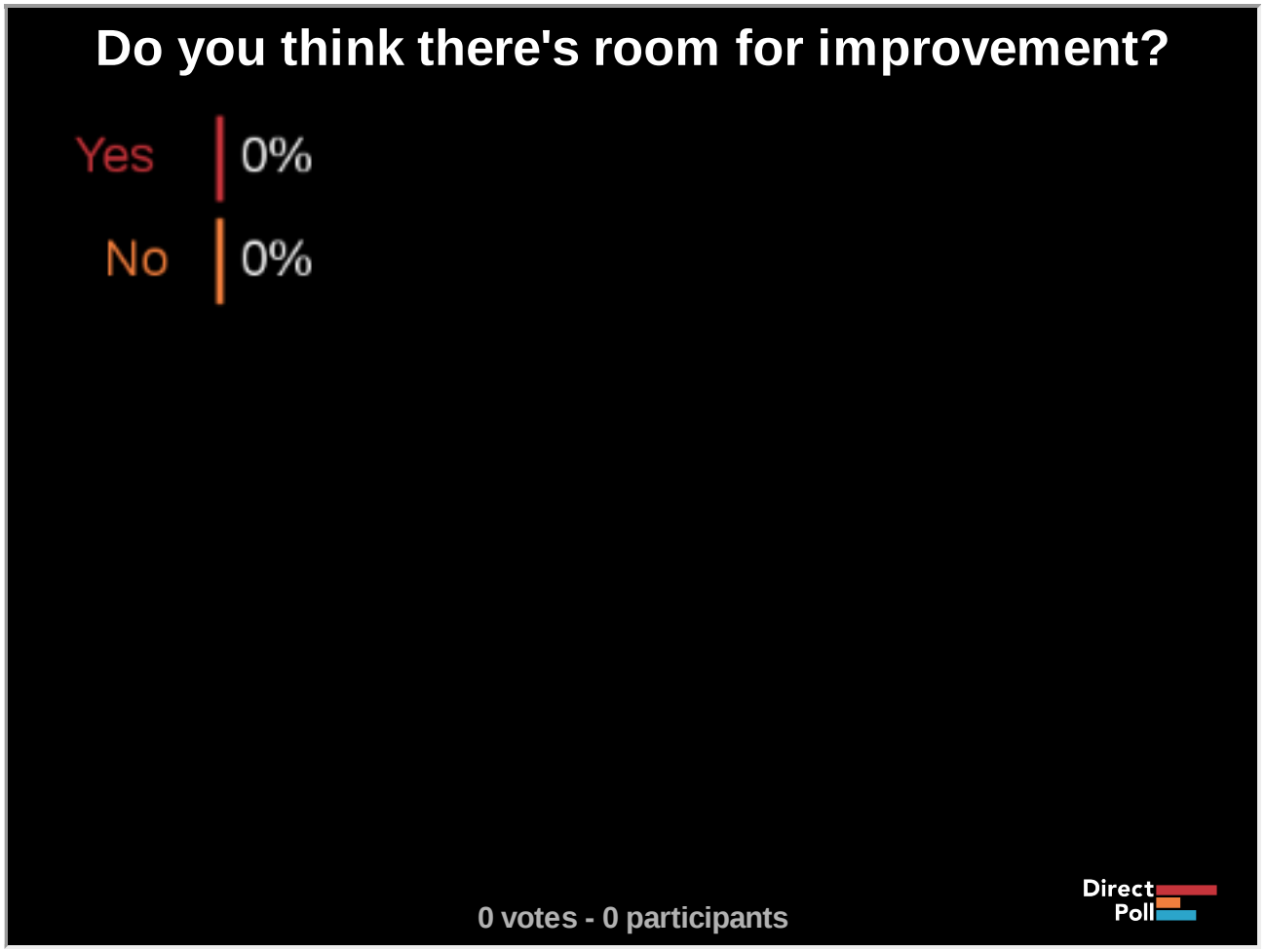
Analysis



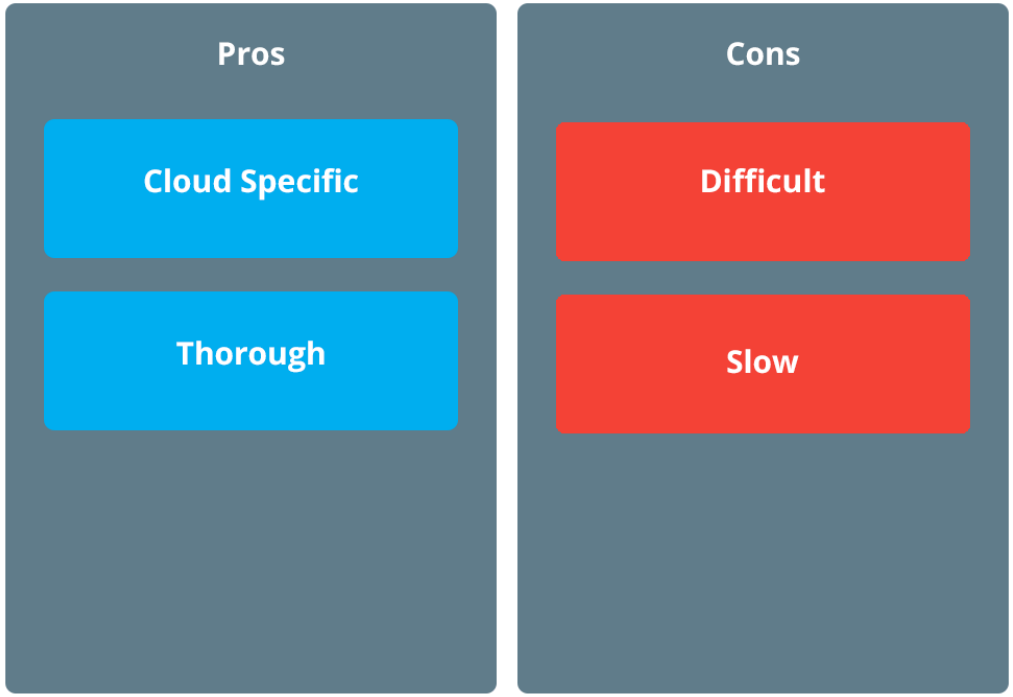
Poll

http://etc.ch/zT5A

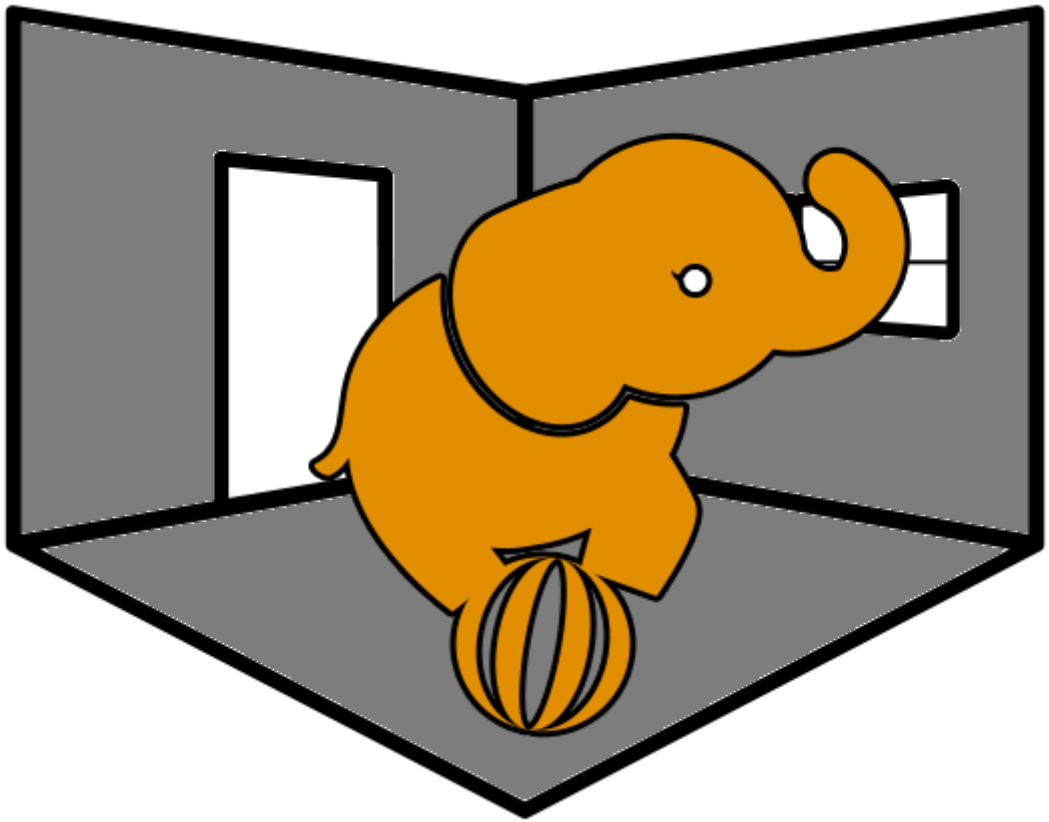
Results


Do you think there's room for improvement?
Yes
0%
No
0%
0 votes - 0 participants
Direct Poll

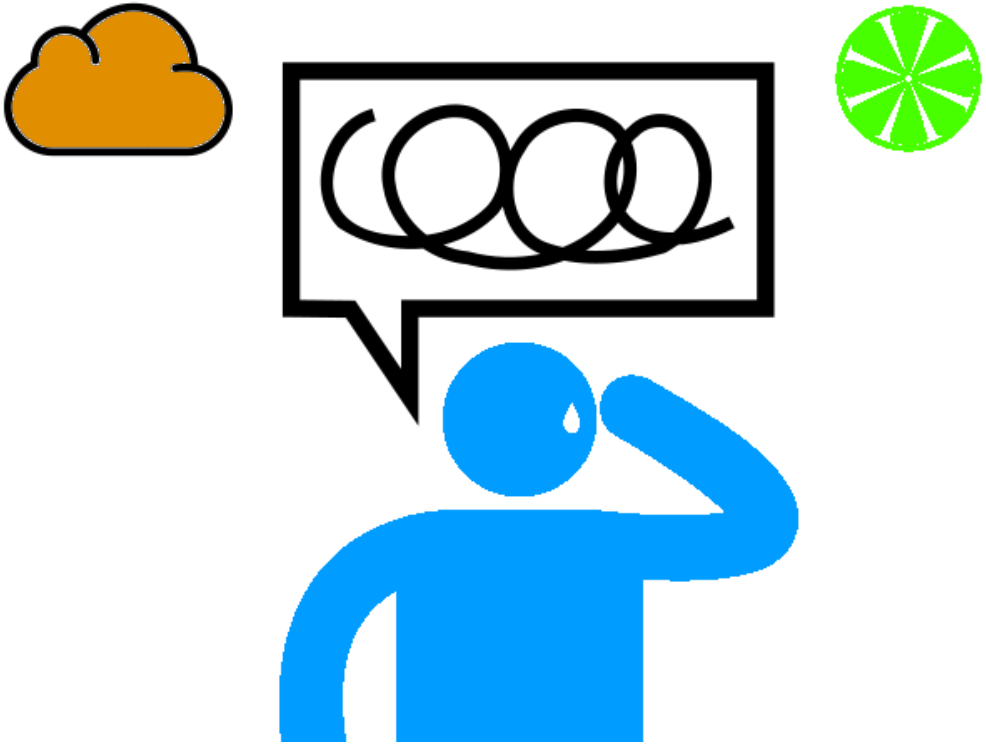
Pros and Cons

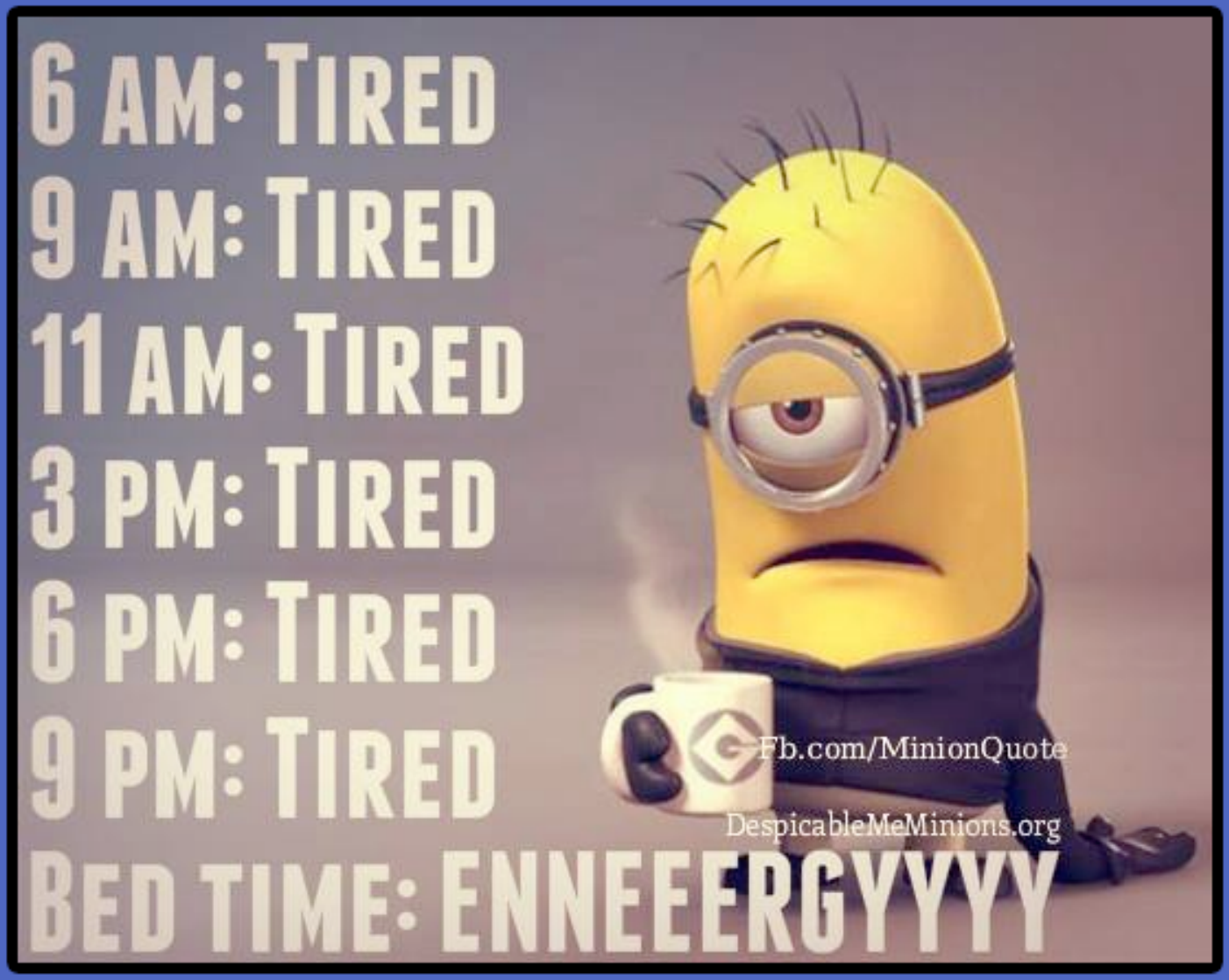


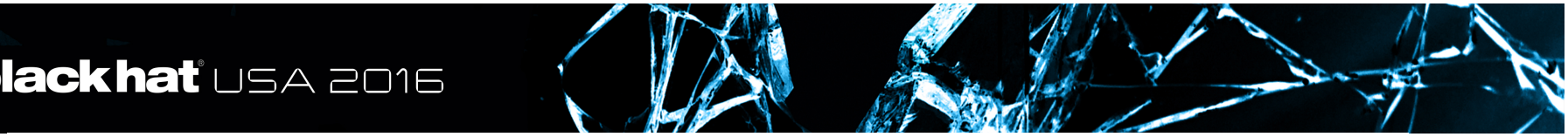
The Elephant in the Room



Security is Difficult




6 AM: TIRED
9 AM: TIRED
11 AM: TIRED
3 PM: TIRED
6 PM: TIRED
9 PM: TIRED
BED TIME: ENNEEERGYYYY
Fb.com/MinionQuote
DespicableMeMinions.org



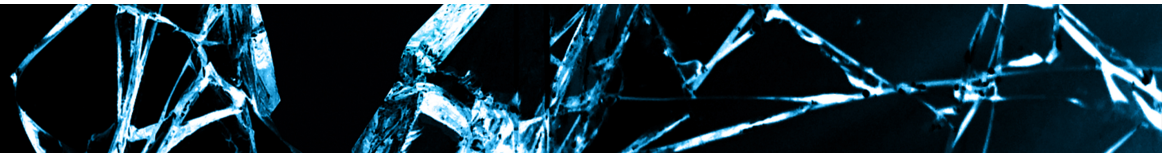
DISRUPTION


WR NG

Tool Release

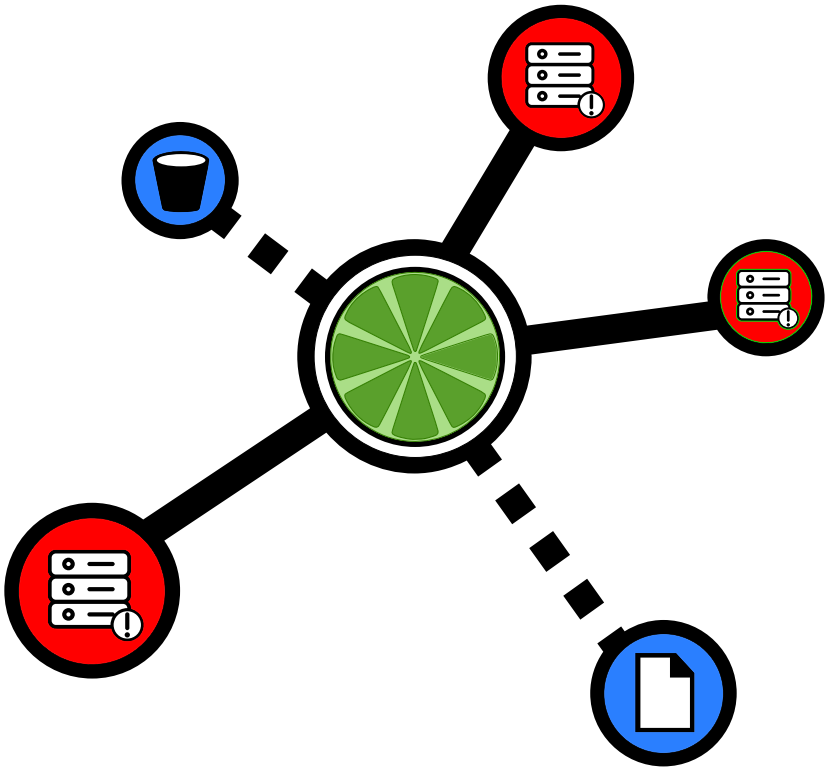
Mission Statement

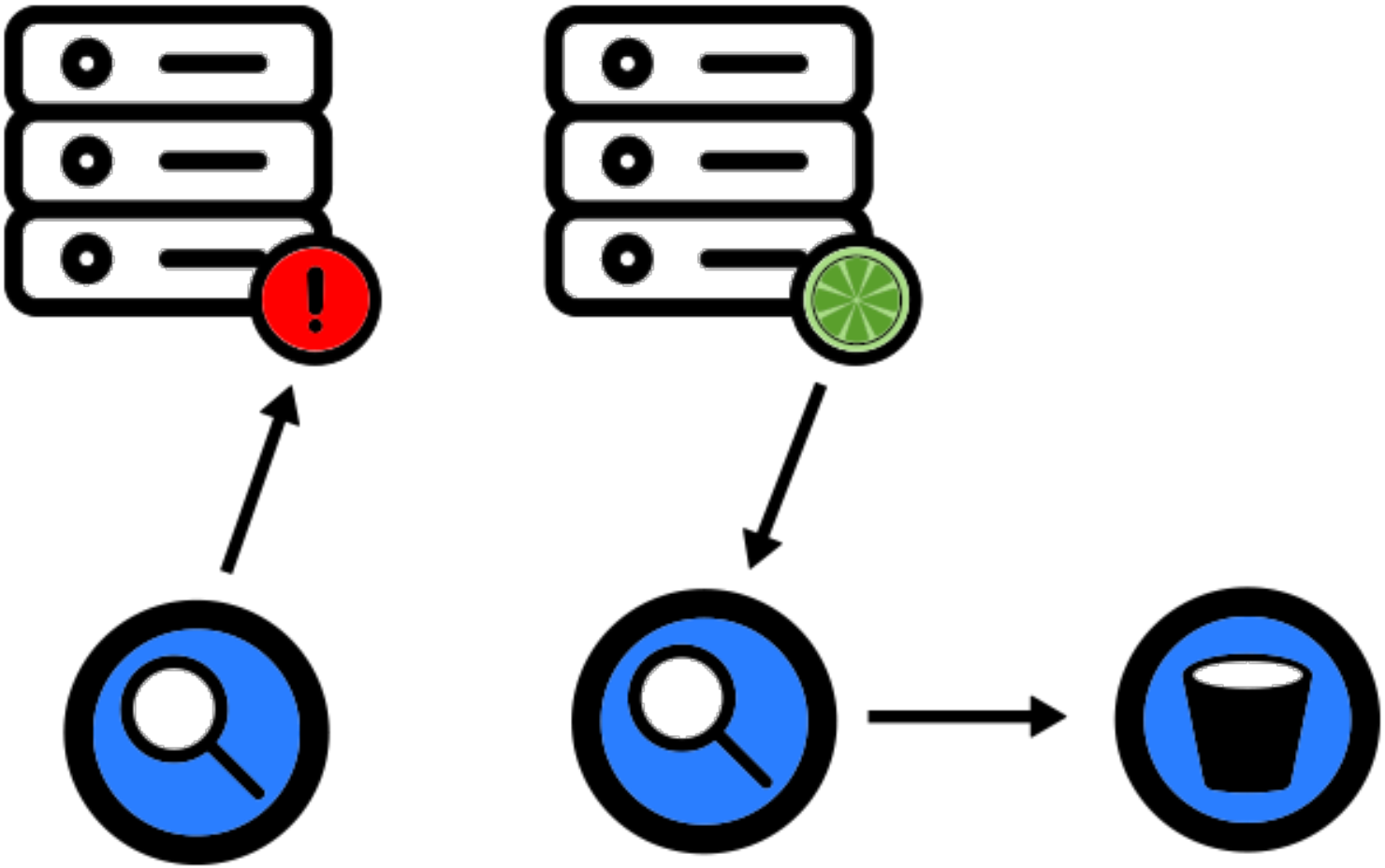
Be the first truly free open source incident response toolkit tailored for Amazon Web Services. Help first responders by automating workflows using Amazon's very own boto3 pip module.



Challenge 1

Margarita Shotgun





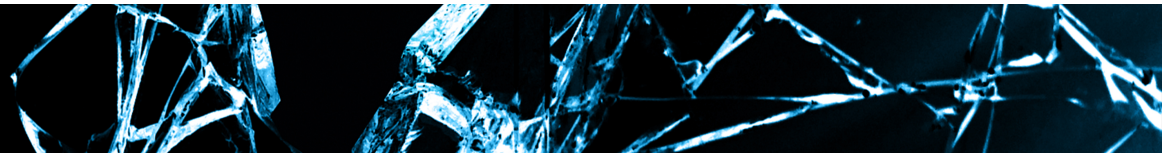
Module Warehouse

T.N.O.

Trust

No

One



Margarita Shotgun

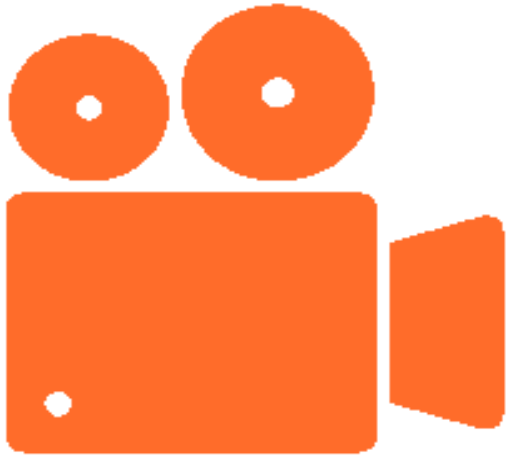
Wrap Up

The Road to Automation

AWS-IR Module

```
usage: aws_ir
       [-h]
       [-n CASE_NUMBER]
       [-e EXAMINER_CIDR_RANGE]
       [-c]
       [-k KEY_NAME] [-b BUCKET_ID]
       {
       host_compromise,
       key_compromise,
       create_workstation
       }
```

Video Demonstration



ThreatResponse
CLOUD SECURITY

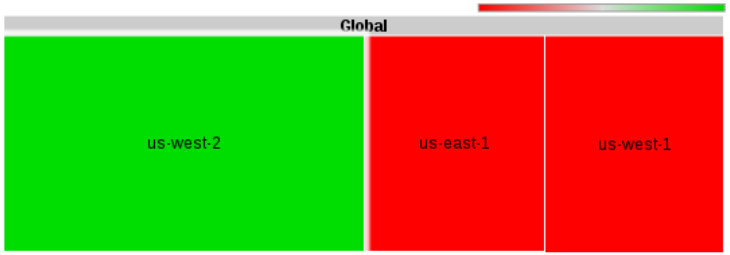
ThreatResponse

Acquire Analyze Advise

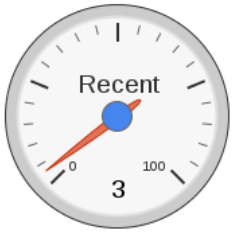
Locate Instance

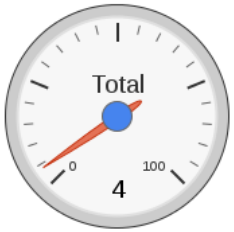
REFRESH INVENTORY

Instances by Region

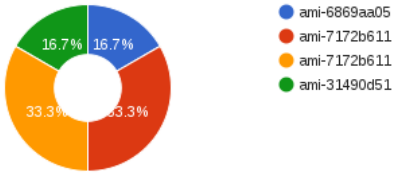


Recently Launched Instances





AMI Homegeny



ThreatResponse

Acquire Analyze Advise

MITIGATE

Search for Instance

search by ip, instance-id, ami-id, or region.

us-west-2

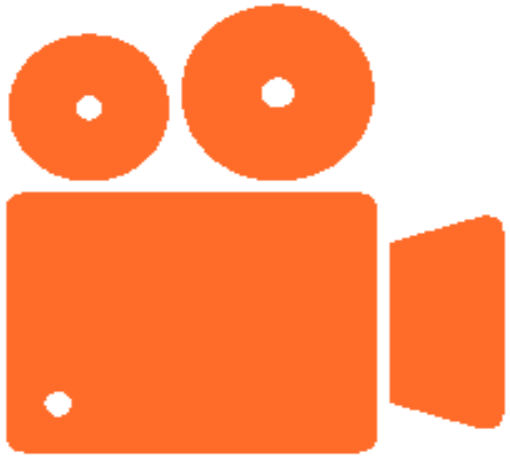
Results for **us-west-2**

InstanceId	Public IP Address	Region	Action	Action
i-34ce709b	54.201.121.128	us-west-2	ADD CREDENTIALS	ADD TO CASE

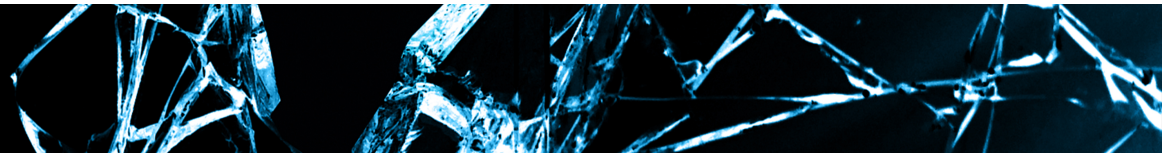
InstanceId	Public IP Address	Region	Action	Action
i-6bce70c4	54.200.171.35	us-west-2	ADD CREDENTIALS	ADD TO CASE

.27.0.0.1:9999/acquire

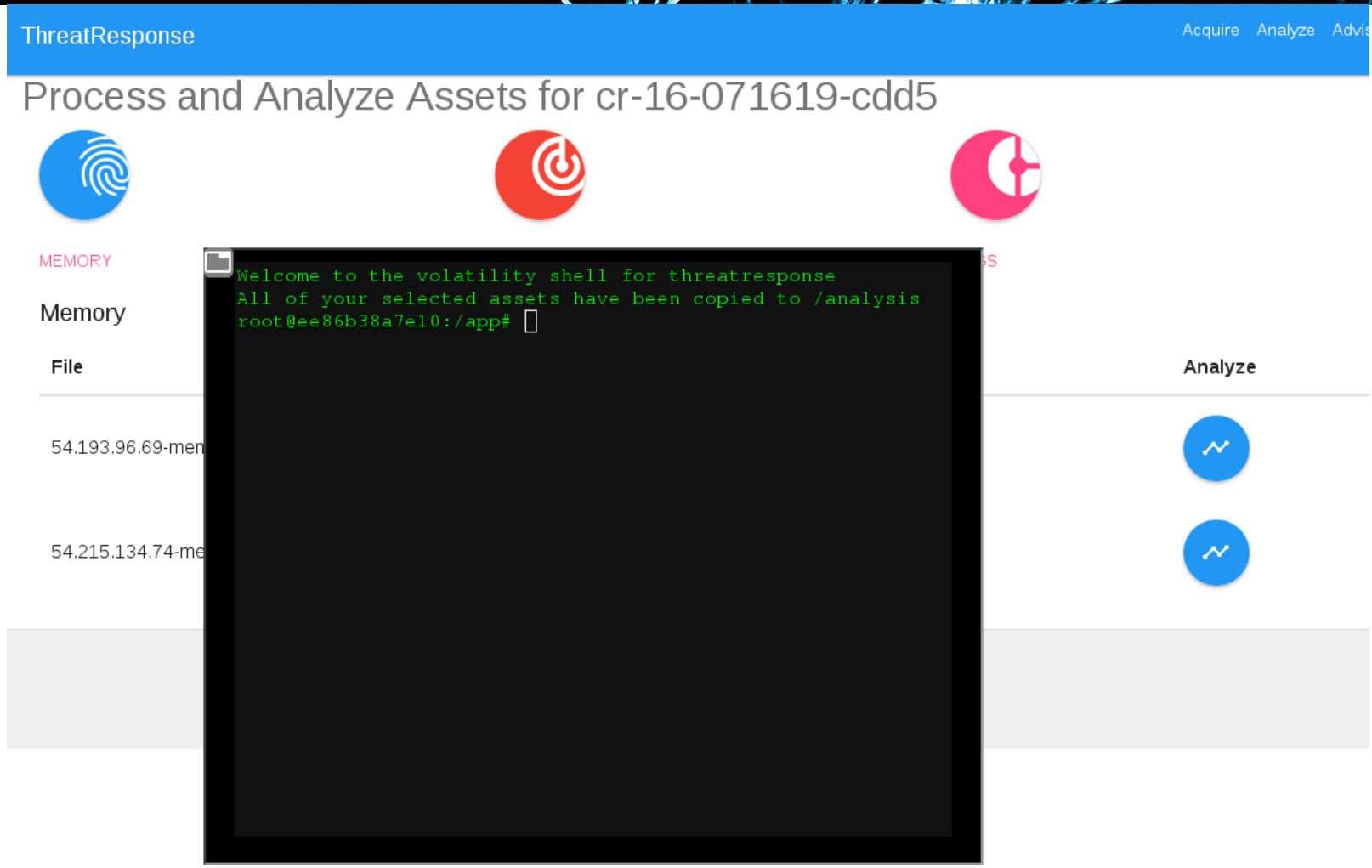
Video Demonstration



ThreatResponse
CLOUD SECURITY



Analysis Views


ThreatResponse
Acquire
Analyze
Process and Analyze Assets for cr-16-071619-cdd5
MEMORY
Memory
File
Analyze
54.193.96.69-mem
54.215.134.74-me
Welcome to the volatility shell for threatresponse
All of your selected assets have been copied to /analysis
root@ee86b38a7e10:/app#

ThreatResponse

Acquire Analyze Advise

Process and Analyze Assets for cr-16-071619-cdd5

MEMORY DISK LOGS

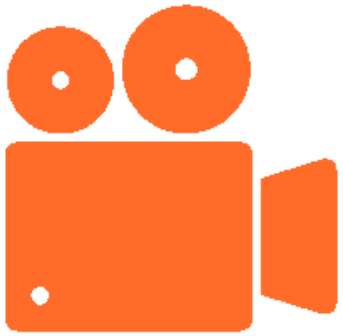
Disks

LOG2TIMELINE ALL

Snapshots for us-west-2

Id	Instance	Volume	Processed
snap-a3d00be1	Instance Missing	vol-49c159c9	ADD
snap-acf4f3ea	Instance Missing	vol-3ec058be	ADD
snap-52b3ce08	Instance Missing	vol-71cf48f8	ADD
snap-c68d7c98	Instance Missing	vol-1fcf579f	ADD

Video Demonstration



ThreatResponse
CLOUD SECURITY

Logs

ThreatResponse

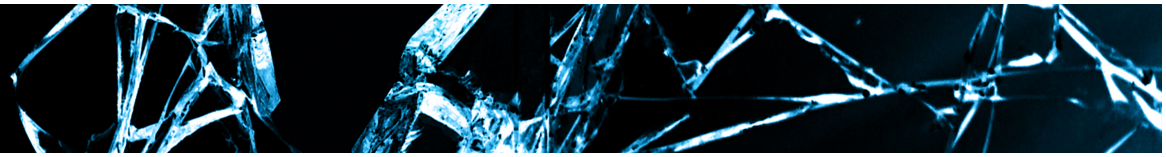
Acquire Analyze Advise

Process and Analyze Assets for cr-16-071619-cdd5

MEMORY DISK LOGS

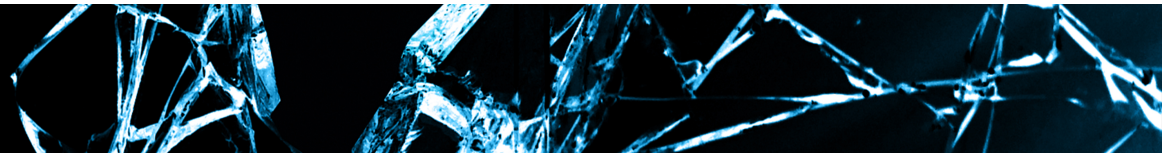
Logs

Instance	Acquisition Log	Console Logs	Screenshot
i-0d1a7c6532e534d82	cr-16-071619-cdd5-i-0d1a7c6532e534d82-aws_ir.log	cr-16-071619-cdd5-i-0d1a7c6532e534d82-console.log	cr-16-071619-cdd5-i-0d1a7c6532e534d82-screenshot.jpg
i-0d7116b547117ac35	cr-16-071619-cdd5-i-0d7116b547117ac35-aws_ir.log	cr-16-071619-cdd5-i-0d7116b547117ac35-console.log	cr-16-071619-cdd5-i-0d7116b547117ac35-screenshot.jpg
i-0368ca52c29d6adb2	cr-16-071619-cdd5-i-0368ca52c29d6adb2-aws_ir.log	cr-16-071619-cdd5-i-0368ca52c29d6adb2-console.log	cr-16-071619-cdd5-i-0368ca52c29d6adb2-screenshot.jpg
i-074c749ecca2e8750	cr-16-071619-cdd5-i-074c749ecca2e8750-aws_ir.log	cr-16-071619-cdd5-i-074c749ecca2e8750-console.log	cr-16-071619-cdd5-i-074c749ecca2e8750-screenshot.jpg
i-0a300a4aa562a64c4	cr-16-071619-cdd5-i-0a300a4aa562a64c4-aws_ir.log	cr-16-071619-cdd5-i-0a300a4aa562a64c4-console.log	cr-16-071619-cdd5-i-0a300a4aa562a64c4-screenshot.jpg
i-05d952f33fd8bde55	cr-16-071619-cdd5-i-05d952f33fd8bde55-aws_ir.log	cr-16-071619-cdd5-i-05d952f33fd8bde55-console.log	cr-16-071619-cdd5-i-05d952f33fd8bde55-screenshot.jpg



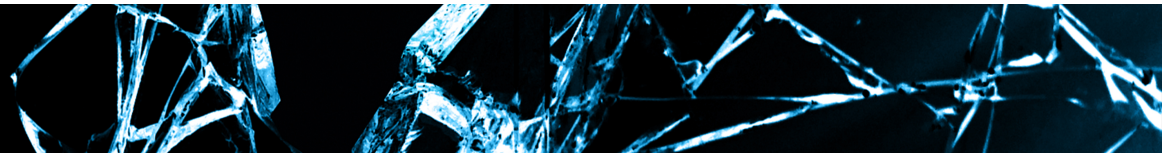
Evidence Collection

Disk



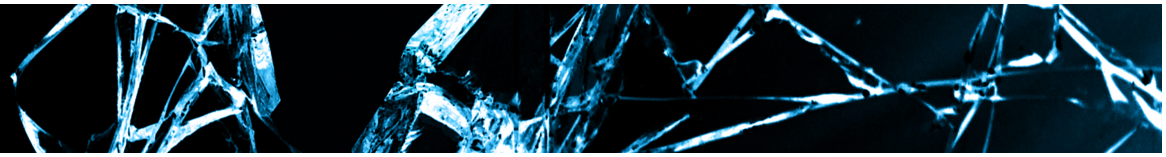
Disk

How it's done.



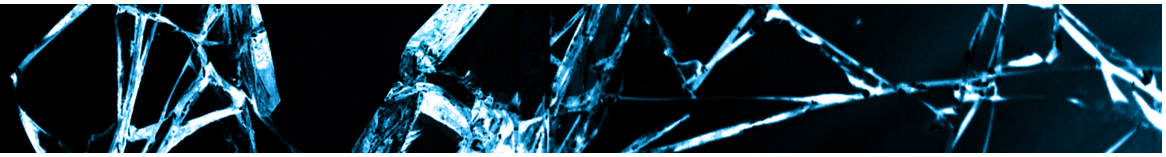
Evidence Collection

Memory



Memory

Methodology



Evidence

Instance Metadata

Evidence

Console Output

Evidence

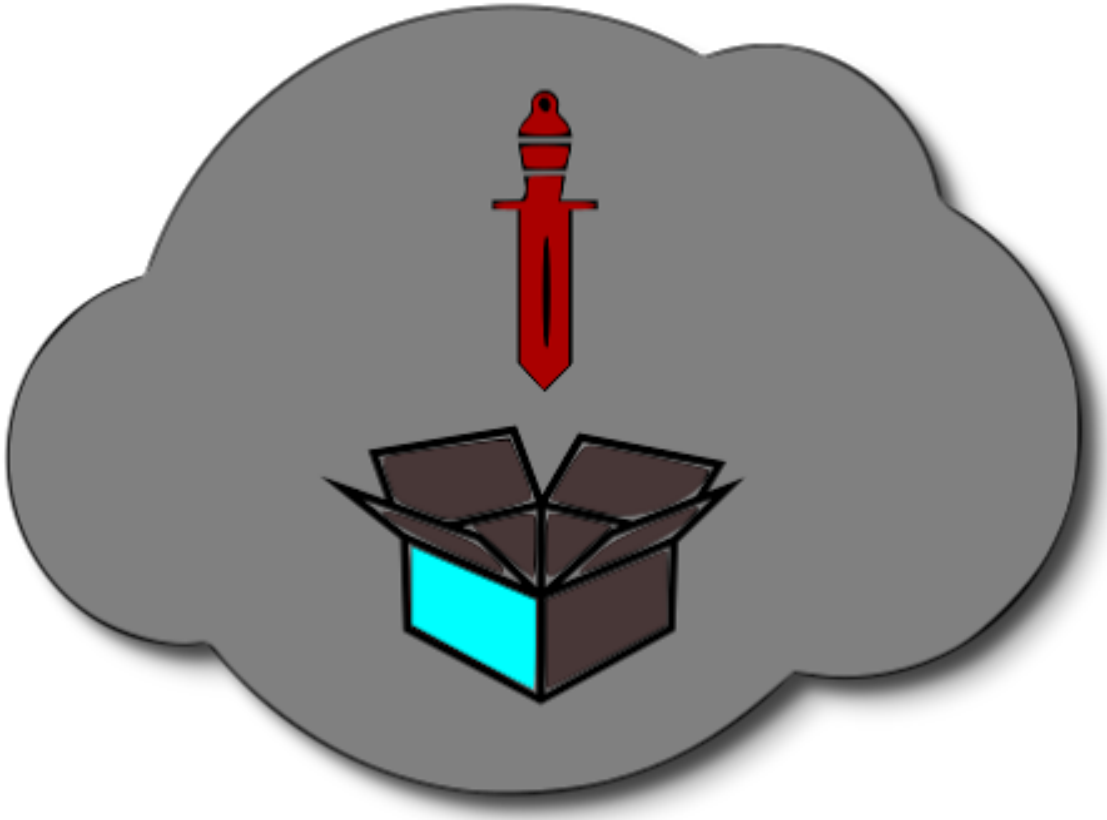
Screenshots

AWS-IR

Key Compromise

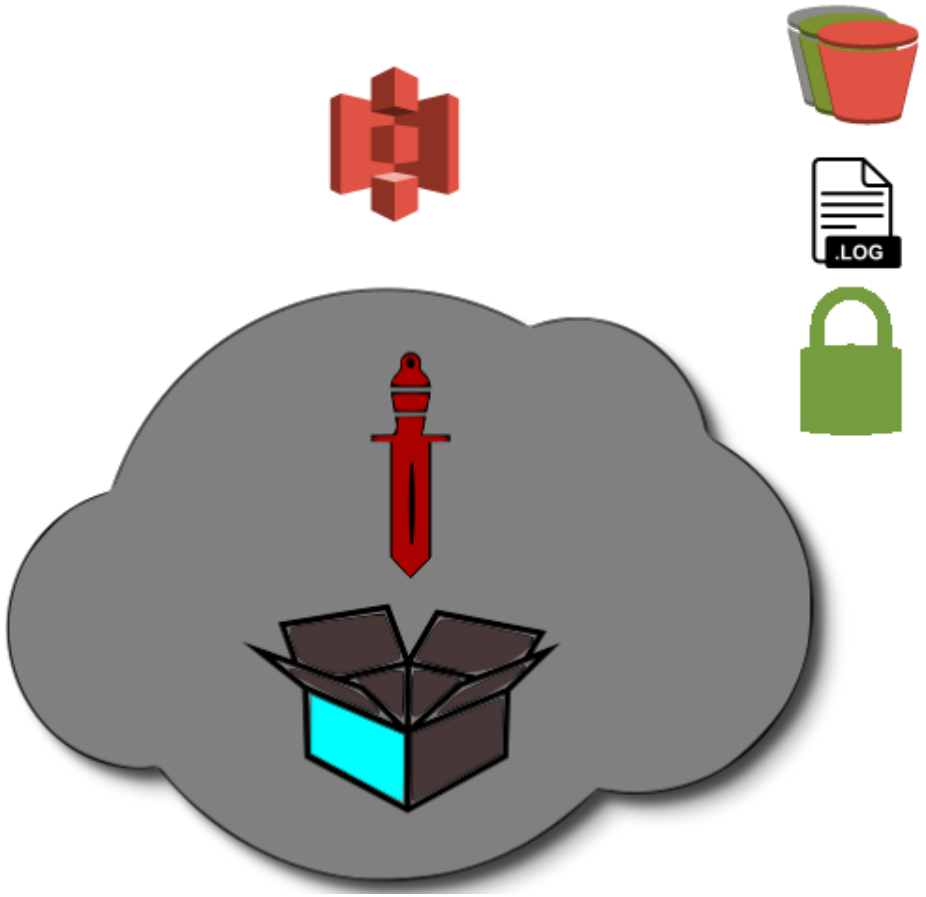
A command as simple as:

```
$ python -m aws_ir.cli key_compromise\
--compromised-access-key-id AAYOURKEYHERE
```

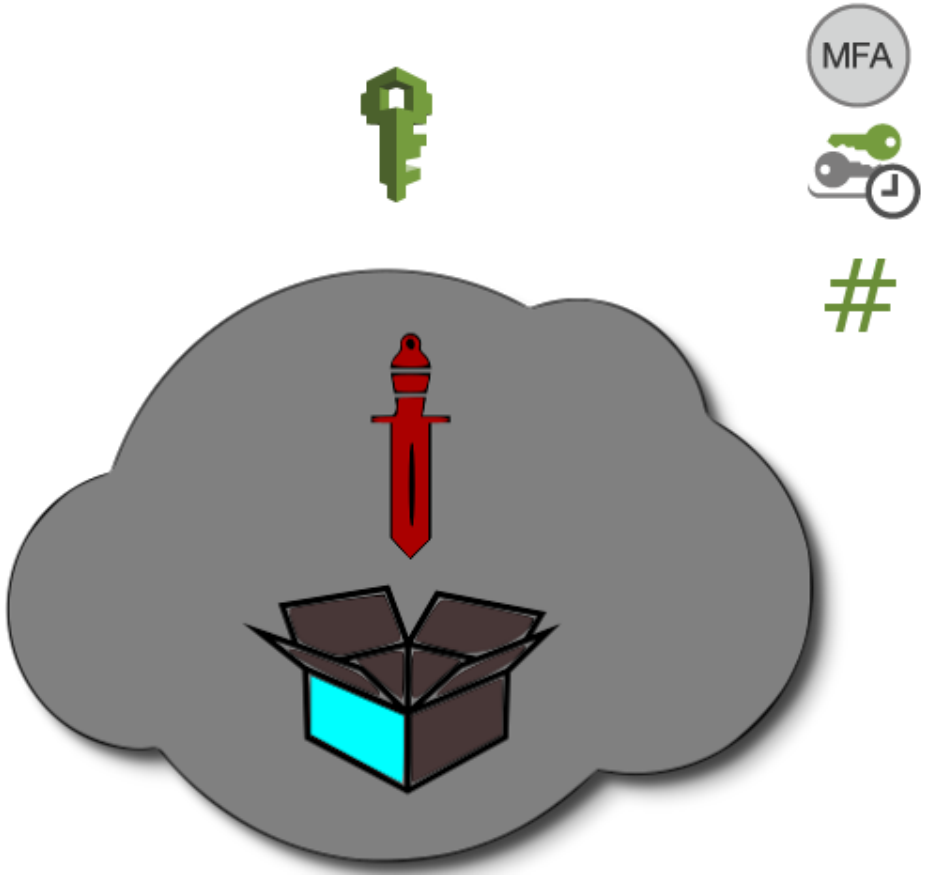


AWS ThreatPrep

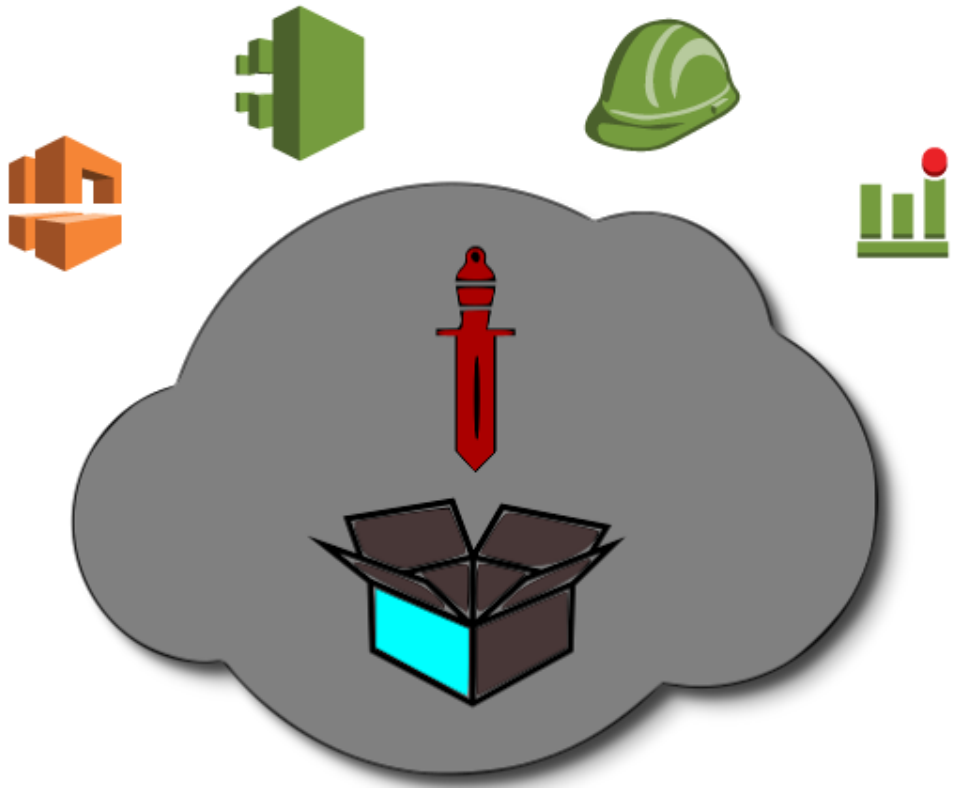
ThreatPrep S3 Checks



ThreatPrep IAM Checks



Other Checks

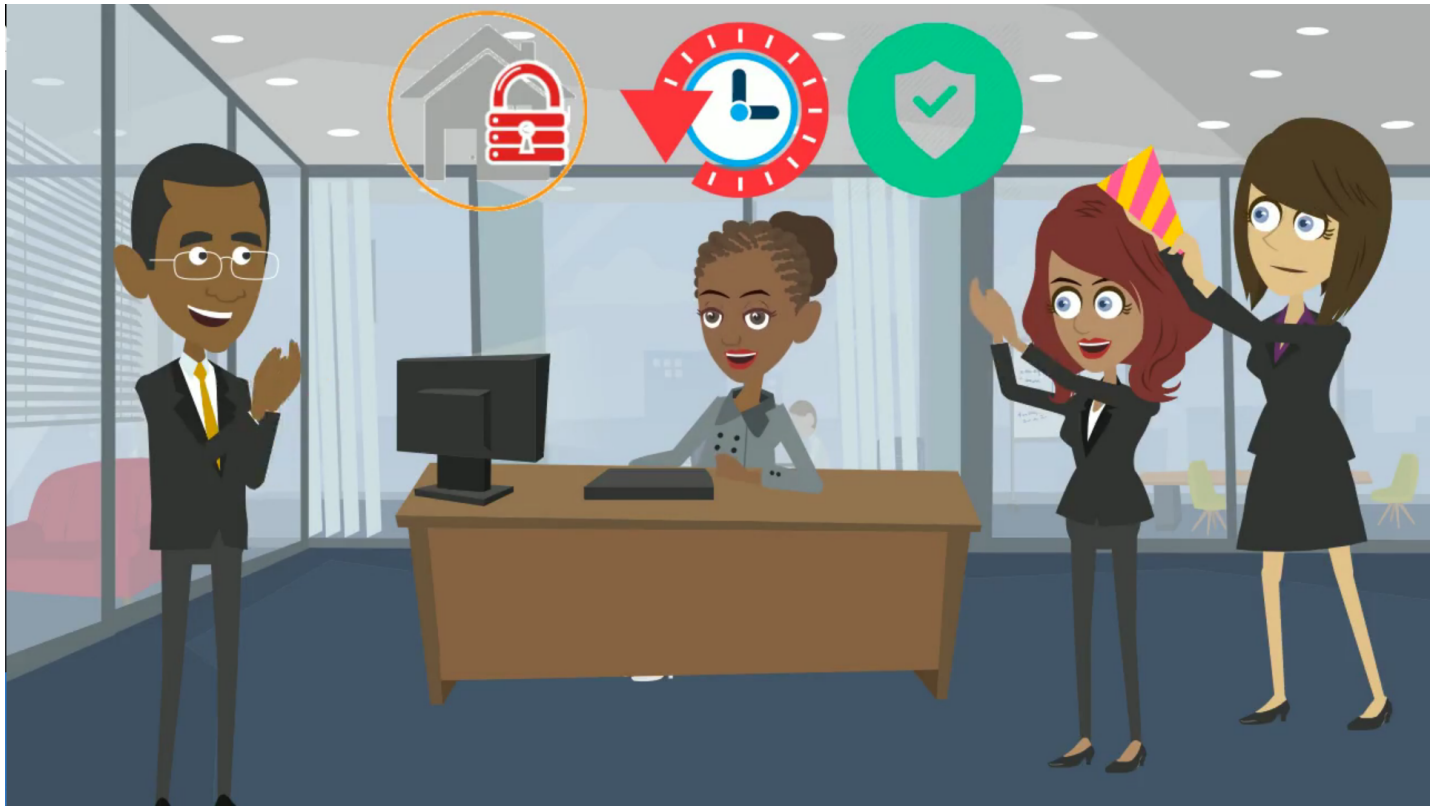


Alternatives From AWS

Trusted Advisor

Config

Future

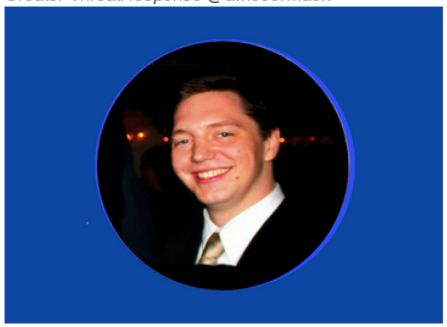


Thank You

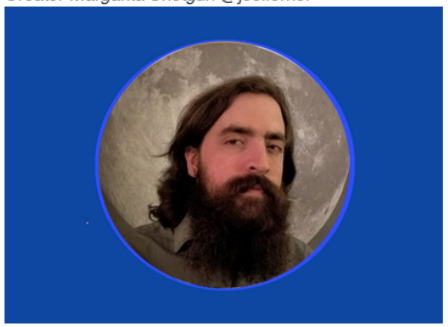
OUR TEAM

Andrew Krug
Creator ThreatResponse @andrewkrug

Alex McCormack
Creator ThreatResponse @amccormack



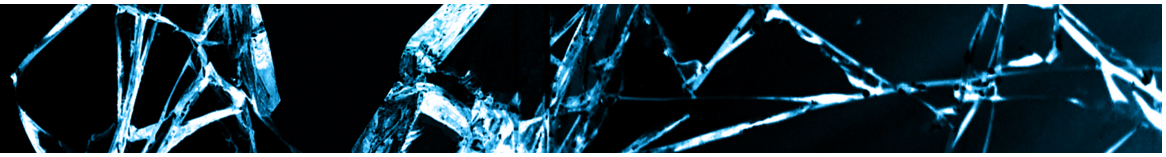
Joel Ferrier
Creator Margarita Shotgun @joelferrier



Jeff Parr
Front End Guru @jparr

Join Us!
Become a contributor today!

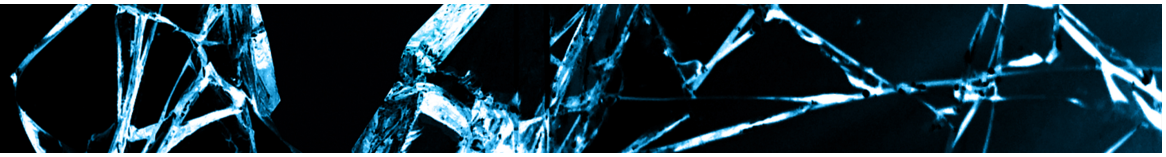
This could be you.
Making open source software is fun.



Thank You

Don Bailey AWS

Zack Glick AWS



Questions?