Hardening AWS Environments

and

Automating Incident Response

for

AWS Compromises

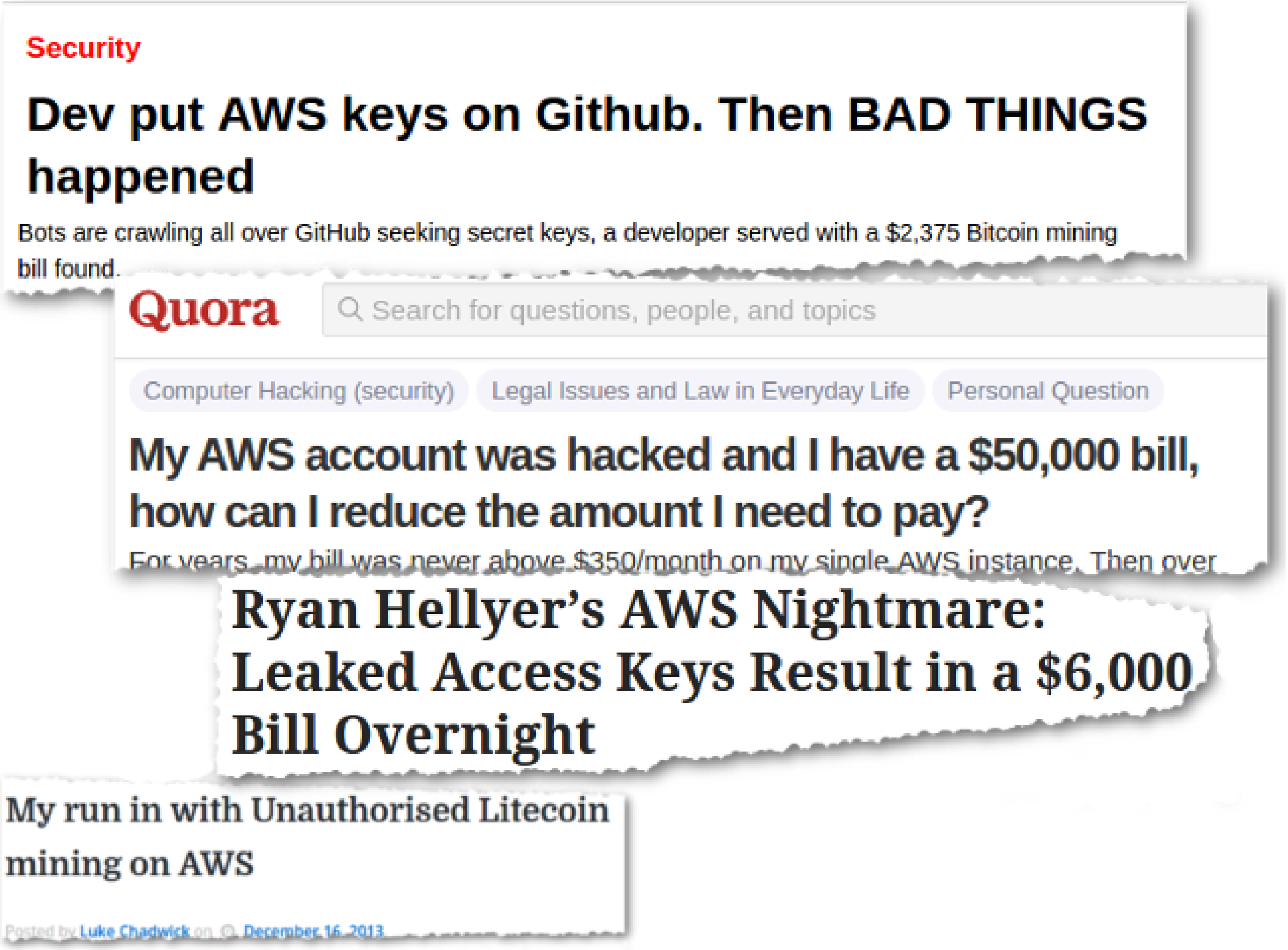
Agenda: Preparing for an Incident within AWS

Incident Handling

Automatic Collection of Evidence

Hardening the AWS Environment

AWS Key Compromise



Security

Dev put AWS keys on Github. Then BAD THINGS happened

Bots are crawling all over GitHub seeking secret keys, a developer served with a $2,375 Bitcoin mining bill found.

Quora
Search for questions, people, and topics
Computer Hacking (security)
Legal Issues and Law in Everyday Life
Personal Question

My AWS account was hacked and I have a $50,000 bill, how can I reduce the amount I need to pay?

For years, my bill was never above $350/month on my single AWS instance. Then over

Ryan Hellyer's AWS Nightmare: Leaked Access Keys Result in a $6,000 Bill Overnight

My run in with Unauthorised Litecoin mining on AWS

Posted by Luke Chadwick on December 16, 2013

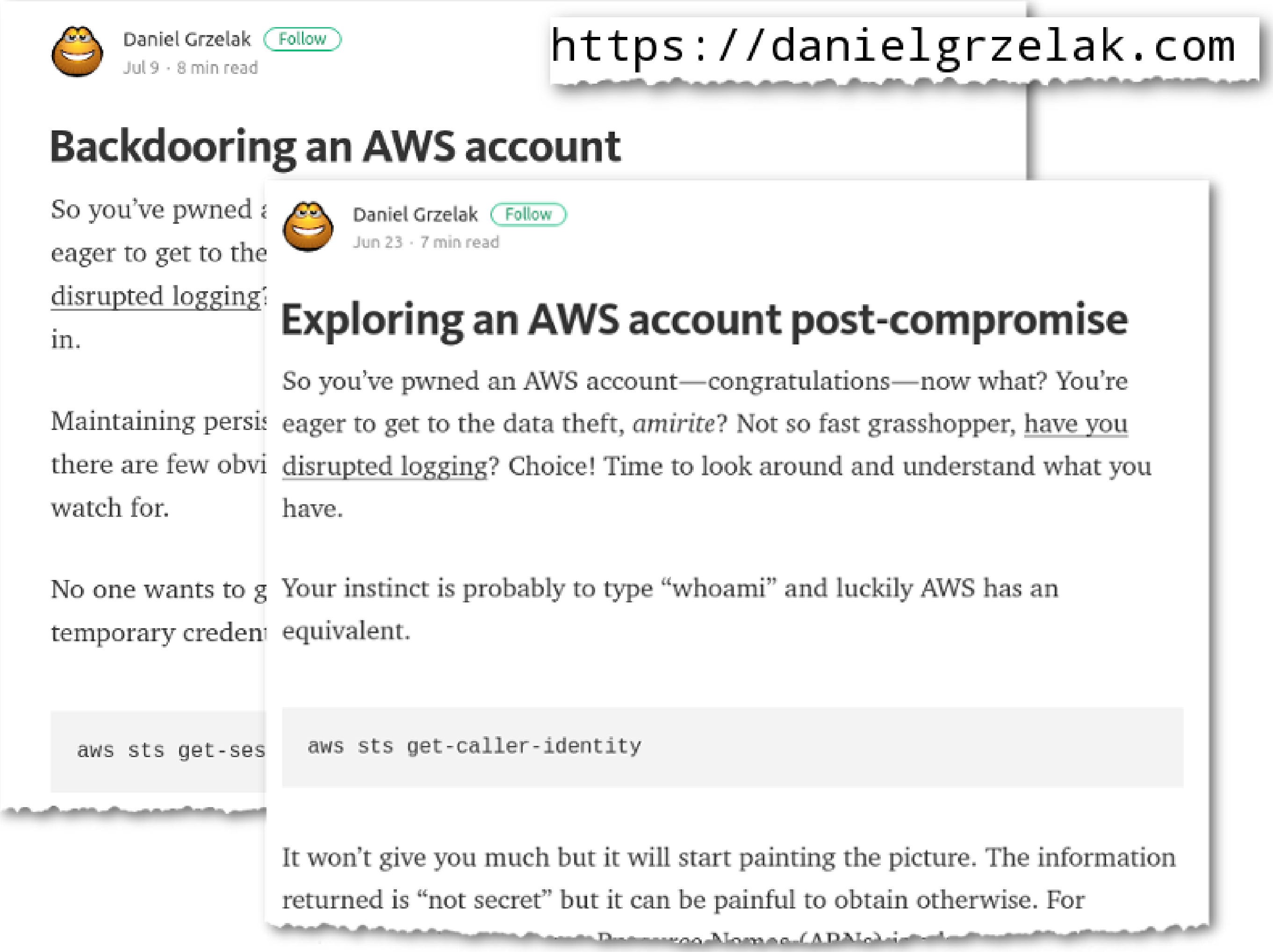
How are Keys Compromised?

AWS Keys provided by AWS for AWS SDK

Keys may be stored in a code repository

Keys may be stored on another AWS Instance

More Serious Attacks



https://danielgrzelak.com

Daniel Grzelak Follow
Jul 9 · 8 min read

Backdooring an AWS account

So you've pwned a
eager to get to the
disrupted logging?
in.

Maintaining persis
there are few obvi
watch for.

No one wants to g
temporary creden

```
aws sts get-ses
```

Daniel Grzelak Follow
Jun 23 · 7 min read

Exploring an AWS account post-compromise

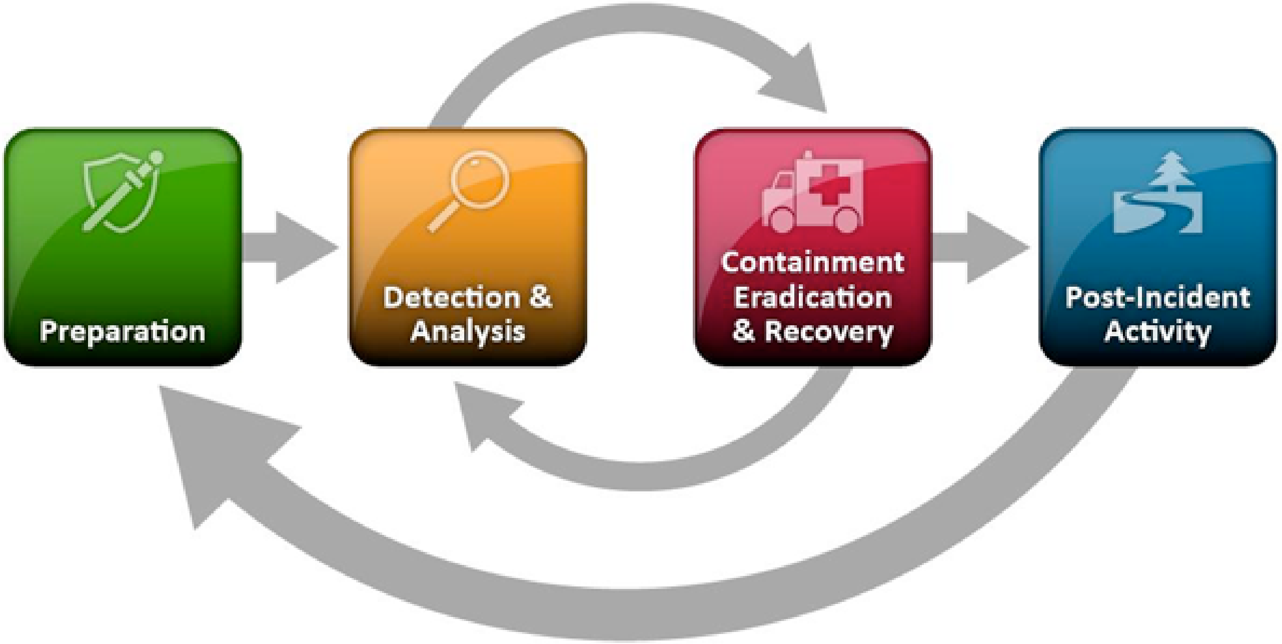
So you've pwned an AWS account—congratulations—now what? You're eager to get to the data theft, *amirite*? Not so fast grasshopper, have you disrupted logging? Choice! Time to look around and understand what you have.

Your instinct is probably to type "whoami" and luckily AWS has an equivalent.

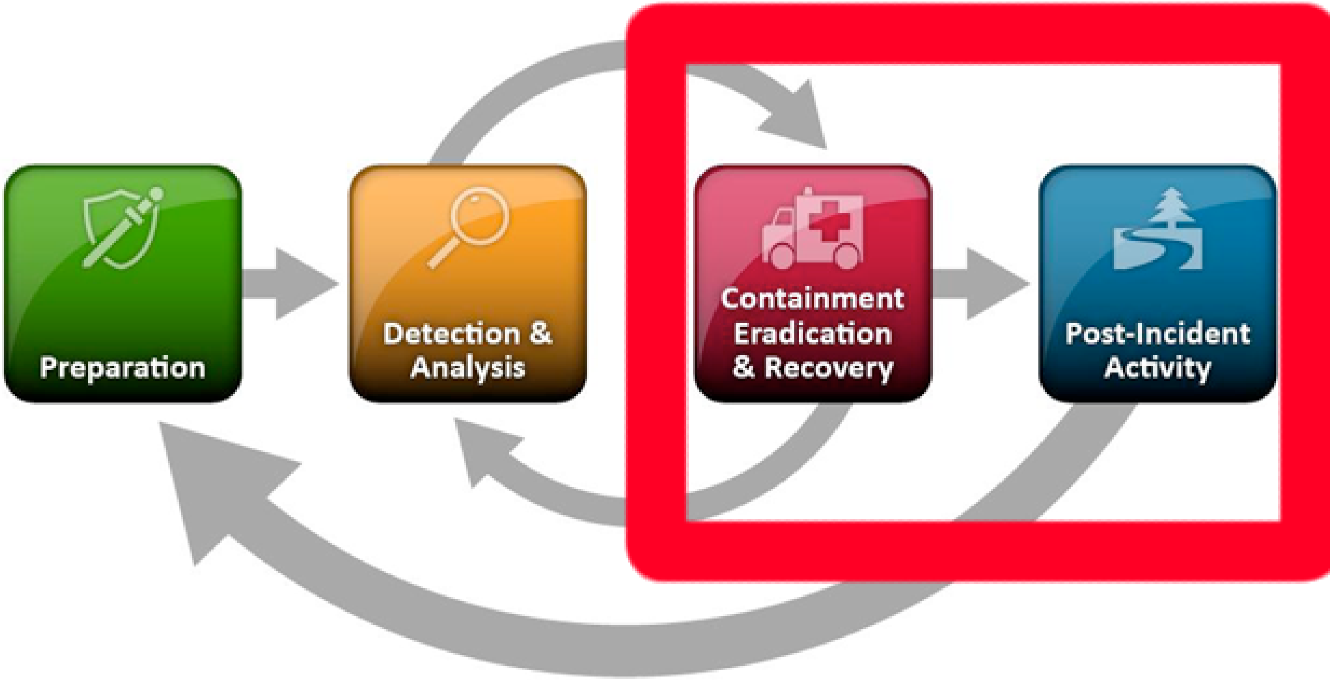
```
aws sts get-caller-identity
```

It won't give you much but it will start painting the picture. The information returned is "not secret" but it can be painful to obtain otherwise. For

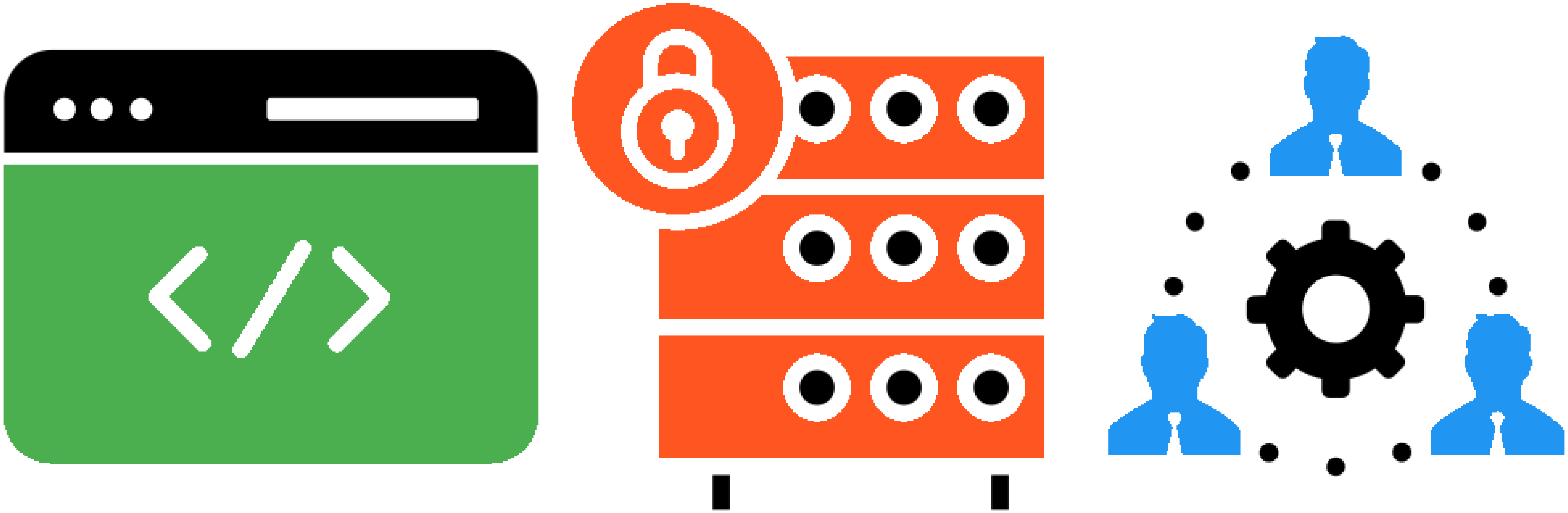
IR-Phases


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

Where we help



DevSecOps



IR Workflow as it relates to AWS

Locating an Instance Across AWS

Managing credentials

Understanding where your config is not best practice

AWS Services to Enable Today

CloudWatch Metrics

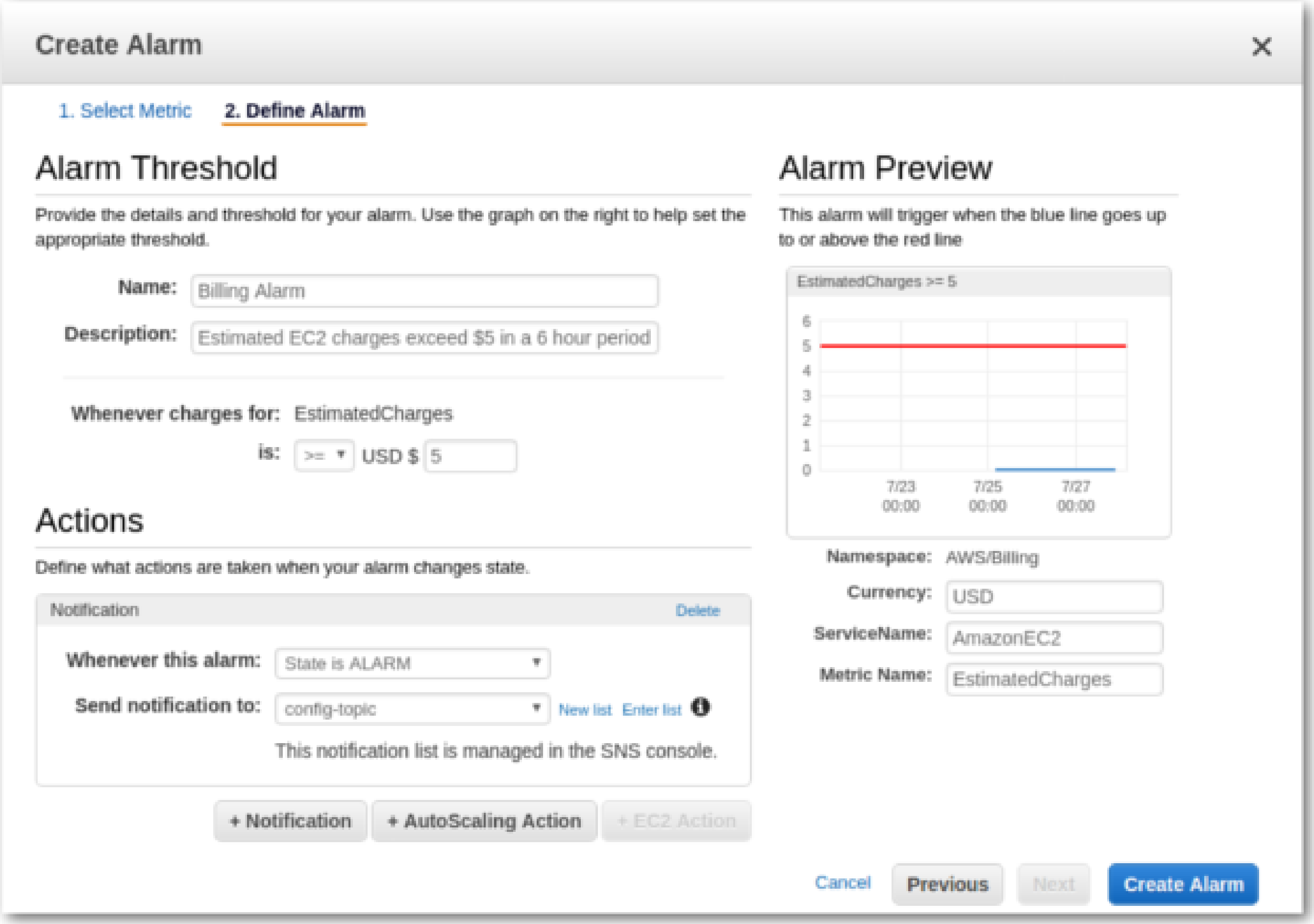
CloudTrail

AWS Config

CloudWatch Events

EC2-Run / IAM

Increasing Visibility with CloudWatch



Create Alarm

1. Select Metric 2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: Billing Alarm

Description: Estimated EC2 charges exceed $5 in a 6 hour period

Whenever charges for: EstimatedCharges

is: >= USD $ 5

Actions

Define what actions are taken when your alarm changes state.

Notification Delete

Whenever this alarm: State is ALARM

Send notification to: config-topic New list Enter list

This notification list is managed in the SNS console.

+ Notification + AutoScaling Action + EC2 Action

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line

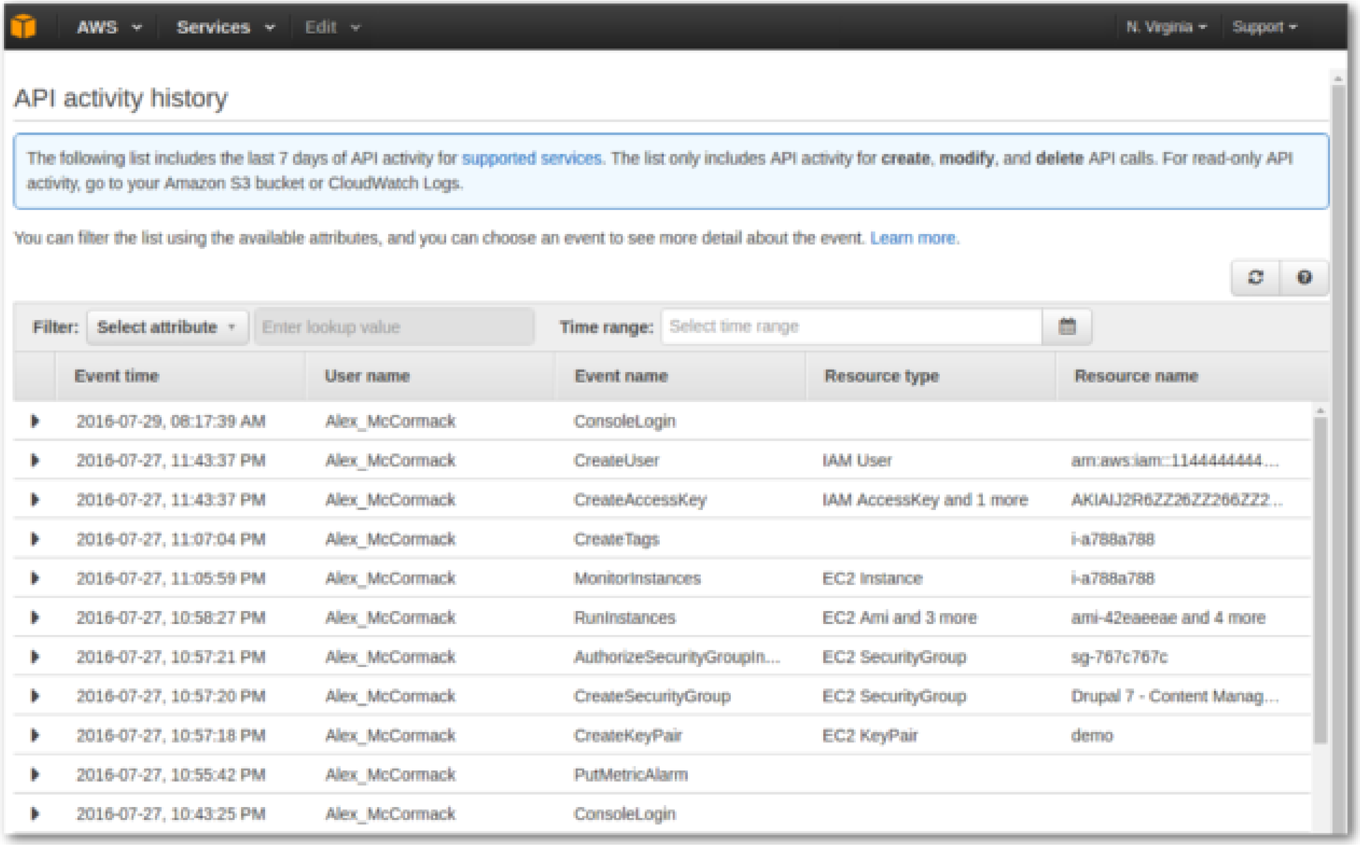
Namespace: AWS/Billing

Currency: USD

ServiceName: AmazonEC2

Metric Name: EstimatedCharges

Increasing Visibility with CloudTrail



API activity history

The following list includes the last 7 days of API activity for supported services. The list only includes API activity for **create**, **modify**, and **delete** API calls. For read-only API activity, go to your Amazon S3 bucket or CloudWatch Logs.

You can filter the list using the available attributes, and you can choose an event to see more detail about the event. Learn more.

Filter: Select attribute ▾ Enter lookup value Time range: Select time range

	Event time	User name	Event name	Resource type	Resource name
▸	2016-07-29, 08:17:39 AM	Alex_McCormack	ConsoleLogin		
▸	2016-07-27, 11:43:37 PM	Alex_McCormack	CreateUser	IAM User	arn:aws:iam::1144444444...
▸	2016-07-27, 11:43:37 PM	Alex_McCormack	CreateAccessKey	IAM AccessKey and 1 more	AKIAIJ2R6ZZ26ZZ266ZZ2...
▸	2016-07-27, 11:07:04 PM	Alex_McCormack	CreateTags		i-a788a788
▸	2016-07-27, 11:05:59 PM	Alex_McCormack	MonitorInstances	EC2 Instance	i-a788a788
▸	2016-07-27, 10:58:27 PM	Alex_McCormack	RunInstances	EC2 Ami and 3 more	ami-42eaeeae and 4 more
▸	2016-07-27, 10:57:21 PM	Alex_McCormack	AuthorizeSecurityGroupIn...	EC2 SecurityGroup	sg-767c767c
▸	2016-07-27, 10:57:20 PM	Alex_McCormack	CreateSecurityGroup	EC2 SecurityGroup	Drupal 7 - Content Manag...
▸	2016-07-27, 10:57:18 PM	Alex_McCormack	CreateKeyPair	EC2 KeyPair	demo
▸	2016-07-27, 10:55:42 PM	Alex_McCormack	PutMetricAlarm		
▸	2016-07-27, 10:43:25 PM	Alex_McCormack	ConsoleLogin		

EC2-Run Example

How to get going with EC2-Command or Simple Server Management

http://amzn.to/2aiq8kc

Installation is Easy!

```
#!/bin/bash
cd /tmp
curl https://amazon-ssm-u ... amazon-ssm-agent.rpm -o amazon-ssm-agent.rpm
yum install -y amazon-ssm-agent.rpm
```

Why would you want to do this?

Can come in useful in a security incident.

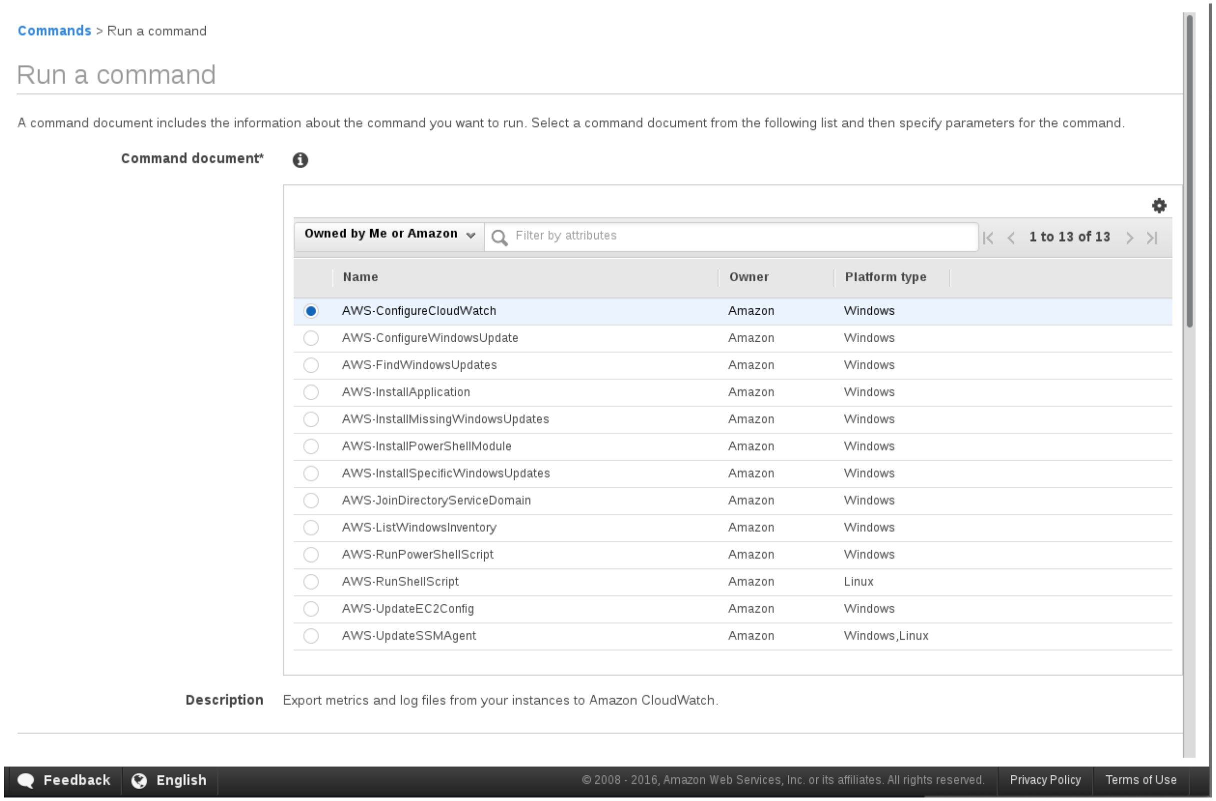
Out of band management.

IAM Role driven.

Account Access Scenario

Imagine you are completely locked out.

Select Run a Command



Commands > Run a command

Run a command

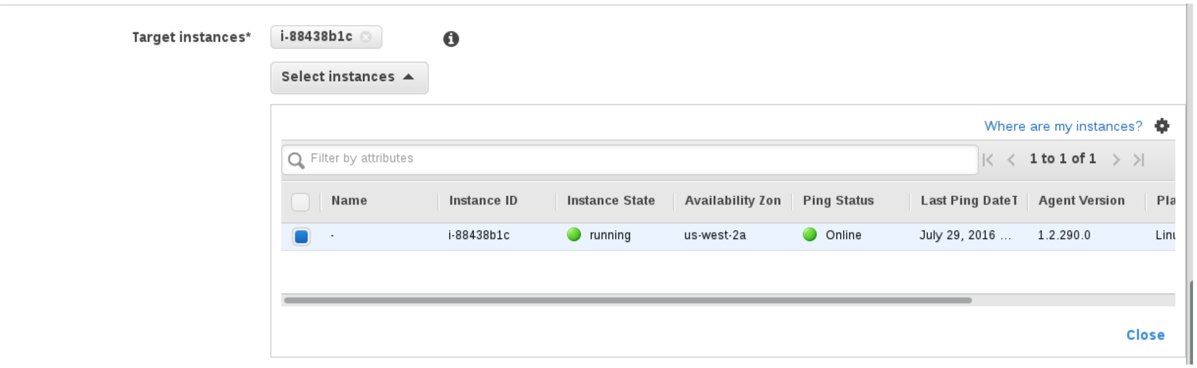
A command document includes the information about the command you want to run. Select a command document from the following list and then specify parameters for the command.

Command document*

	Name	Owner	Platform type
●	AWS-ConfigureCloudWatch	Amazon	Windows
○	AWS-ConfigureWindowsUpdate	Amazon	Windows
○	AWS-FindWindowsUpdates	Amazon	Windows
○	AWS-InstallApplication	Amazon	Windows
○	AWS-InstallMissingWindowsUpdates	Amazon	Windows
○	AWS-InstallPowerShellModule	Amazon	Windows
○	AWS-InstallSpecificWindowsUpdates	Amazon	Windows
○	AWS-JoinDirectoryServiceDomain	Amazon	Windows
○	AWS-ListWindowsInventory	Amazon	Windows
○	AWS-RunPowerShellScript	Amazon	Windows
○	AWS-RunShellScript	Amazon	Linux
○	AWS-UpdateEC2Config	Amazon	Windows
○	AWS-UpdateSSMAgent	Amazon	Windows,Linux

Description Export metrics and log files from your instances to Amazon CloudWatch.

Find the instance



Target instances* i-88438b1c

Select instances ▲

Where are my instances?

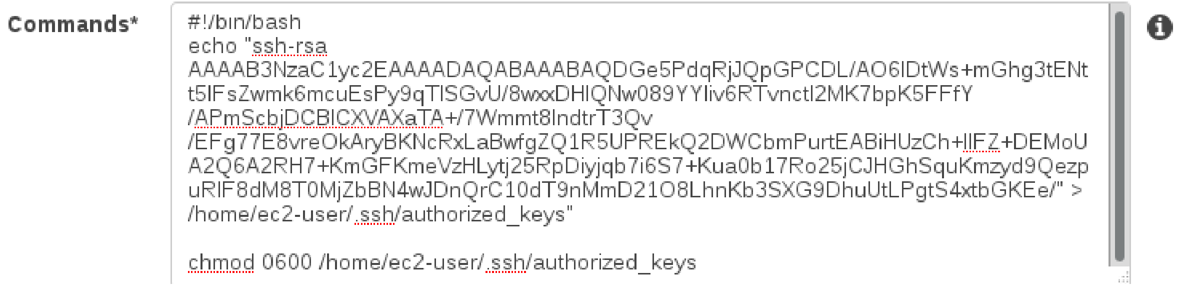
Filter by attributes

1 to 1 of 1

□	Name	Instance ID	Instance State	Availability Zon	Ping Status	Last Ping DateT	Agent Version	Pla
☑	-	i-88438b1c	● running	us-west-2a	● Online	July 29, 2016 ...	1.2.290.0	Linu

Close

Input the command

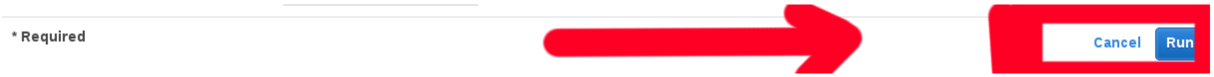


Commands*

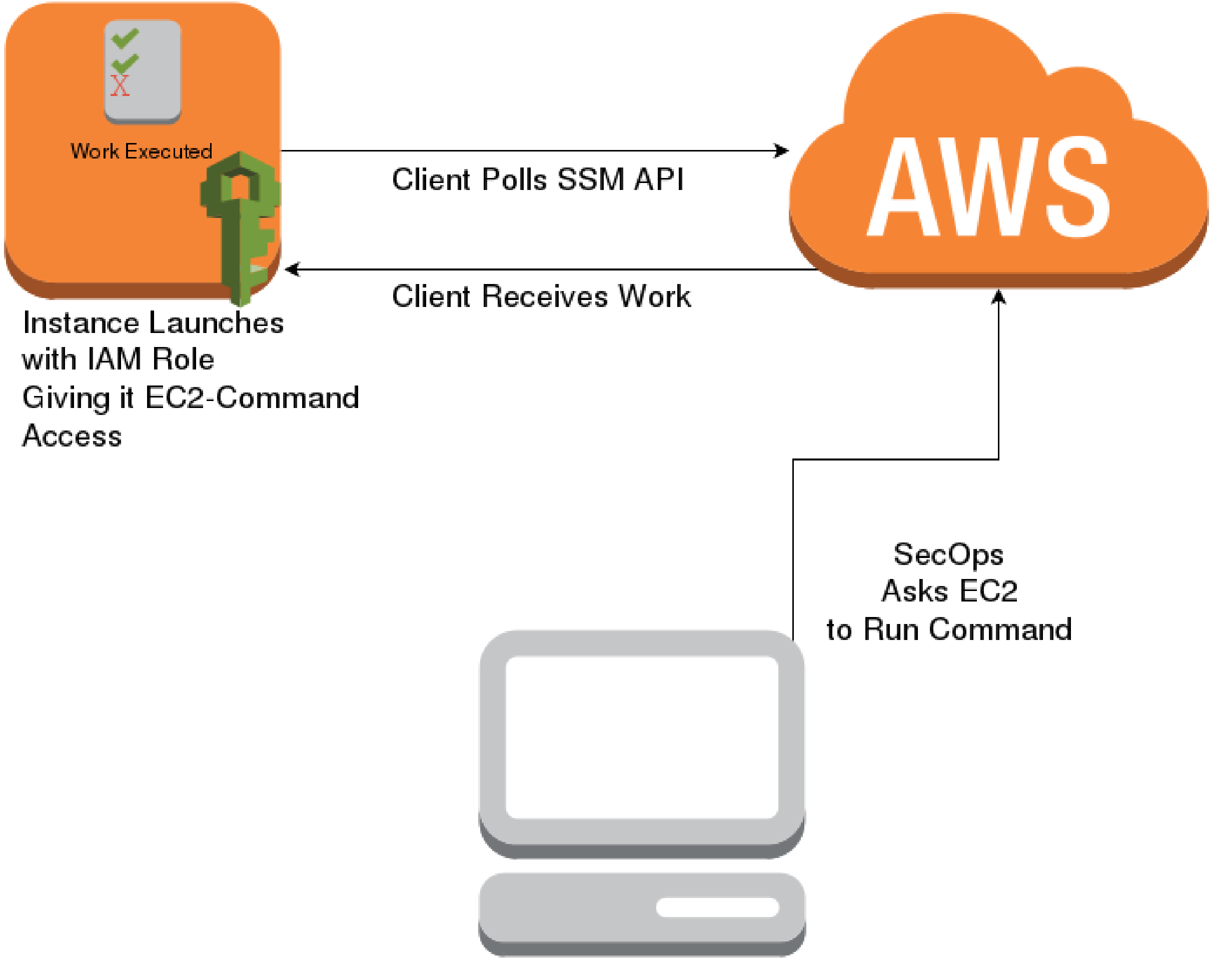
```
#!/bın/bash
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDGe5PdqRjJQpGPCDL/AO6lDtWs+mGhg3tENt
t5IFsZwmk6mcuEsPy9qTlSGvU/8wxxDHlQNw089YYliv6RTvnctl2MK7bpK5FFfY
/APmScbjDCBlCXVAXaTA+/7Wmmt8lndtrT3Qv
/EFg77E8vreOkAryBKNcRxLaBwfgZQ1R5UPREkQ2DWCbmPurtEABiHUzCh+IlFZ+DEMoU
A2Q6A2RH7+KmGFKmeVzHLytj25RpDiyjqb7i6S7+Kua0b17Ro25jCJHGhSquKmzyd9Qezp
uRIF8dM8T0MjZbBN4wJDnQrC10dT9nMmD21O8LhnKb3SXG9DhuUtLPgtS4xtbGKEe/" >
/home/ec2-user/.ssh/authorized_keys"

chmod 0600 /home/ec2-user/.ssh/authorized_keys
```

Execute the command

At the end you can simply click run and you've taken back the instance.



How does it work?



Client Polls SSM API

Client Receives Work

Instance Launches
with IAM Role
Giving it EC2-Command
Access

SecOps
Asks EC2
to Run Command

Recommended viewing

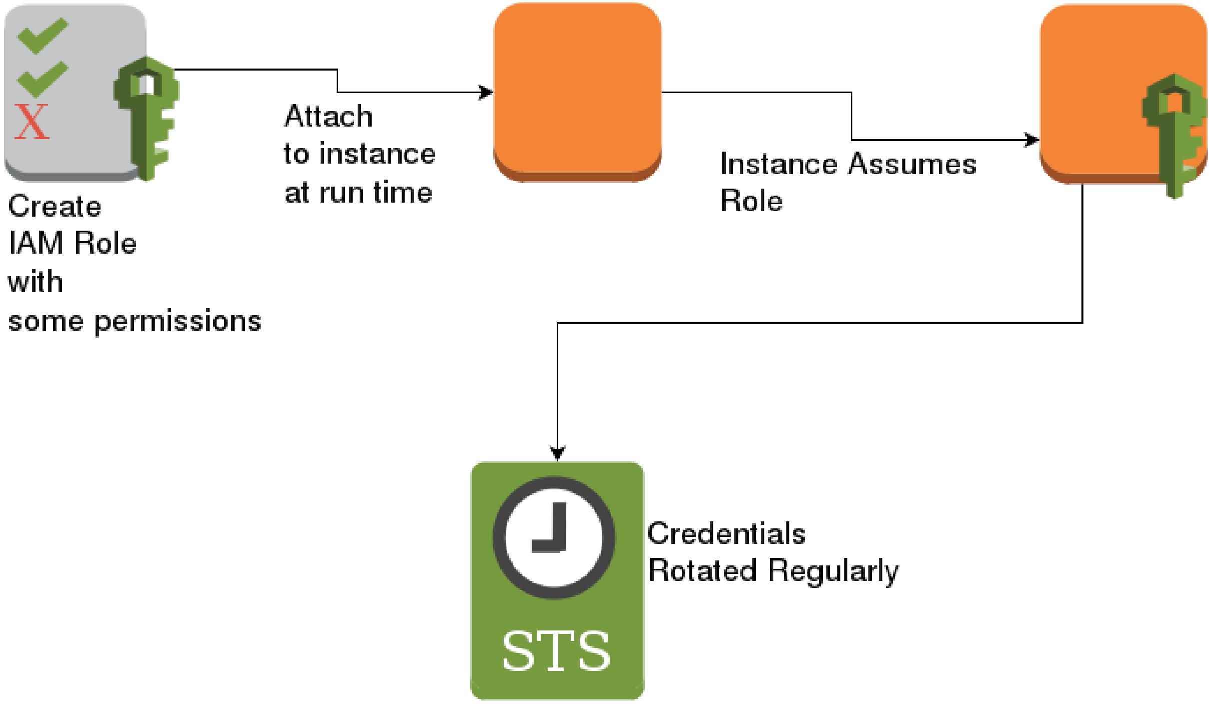
AWS re:Invent 2015 | (SEC316) Harden Your Architecture w/ Security Incident Response Simulations

http://bit.ly/2auYsvI

IAM Role Advice

1. Use least privilege roles.
2. Audit their usage with CloudTrail

How do IAM roles work?



Create
IAM Role
with
some permissions

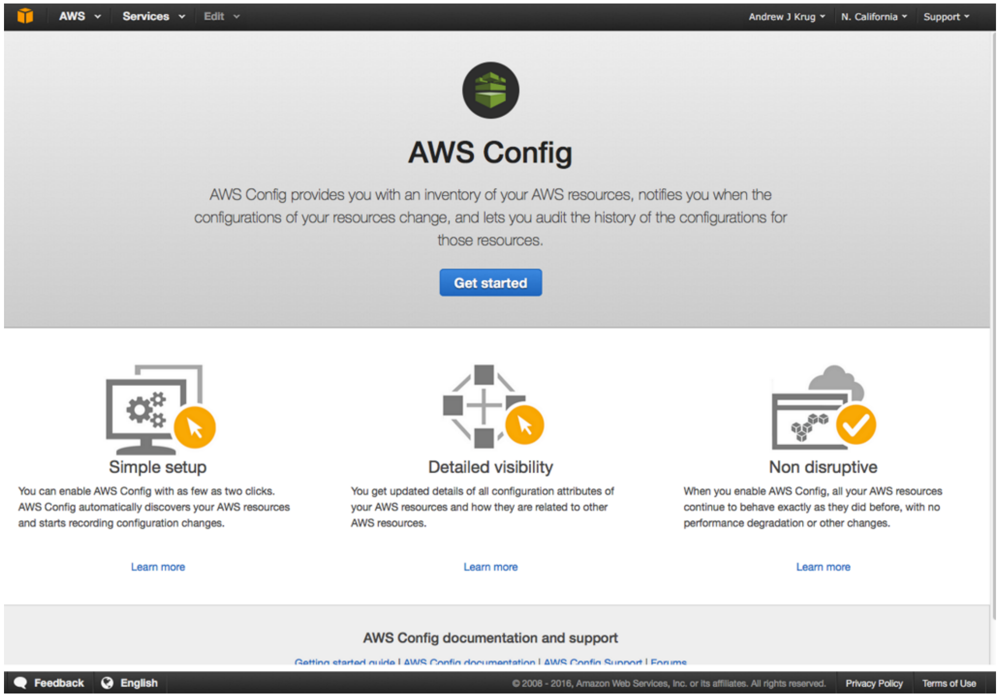
Attach
to instance
at run time

Instance Assumes
Role

Credentials
Rotated Regularly

IAM Limits

1. Instance profiles can't be detached.
2. Instance profiles can't be added to a running instance.



AWS Config

AWS Config provides you with an inventory of your AWS resources, notifies you when the configurations of your resources change, and lets you audit the history of the configurations for those resources.

Simple setup

You can enable AWS Config with as few as two clicks. AWS Config automatically discovers your AWS resources and starts recording configuration changes.

Detailed visibility

You get updated details of all configuration attributes of your AWS resources and how they are related to other AWS resources.

Non disruptive

When you enable AWS Config, all your AWS resources continue to behave exactly as they did before, with no performance degradation or other changes.

AWS Config documentation and support

Getting started guide | AWS Config documentation | AWS Config Support | Forums

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Config is a relatively new service that performs inventory, tracks changes, and can enforce compliance.

Config vs Config Rules

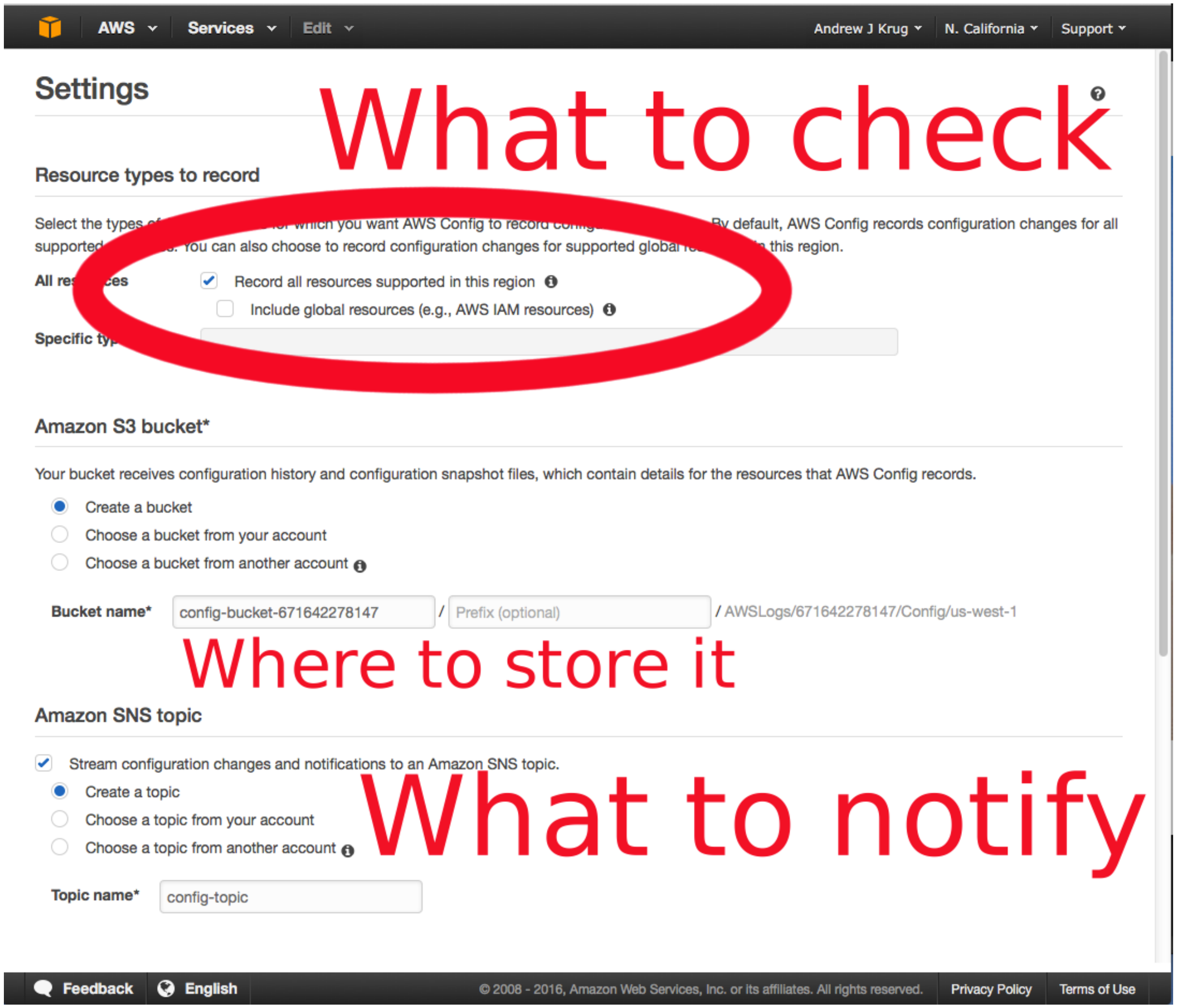
AWS Config

Timeline of Changes

Config Rules:

Run periodically and evaluate compliance.

Wizard Driven Setup



Settings

What to check

Resource types to record

Select the types of … for which you want AWS Config to record config… By default, AWS Config records configuration changes for all supported … You can also choose to record configuration changes for supported global re… in this region.

All res ces ☑ Record all resources supported in this region

□ Include global resources (e.g., AWS IAM resources)

Specific typ

Amazon S3 bucket*

Your bucket receives configuration history and configuration snapshot files, which contain details for the resources that AWS Config records.

● Create a bucket

○ Choose a bucket from your account

○ Choose a bucket from another account

Bucket name* config-bucket-671642278147 / Prefix (optional) / AWSLogs/671642278147/Config/us-west-1

Where to store it

Amazon SNS topic

☑ Stream configuration changes and notifications to an Amazon SNS topic.

● Create a topic

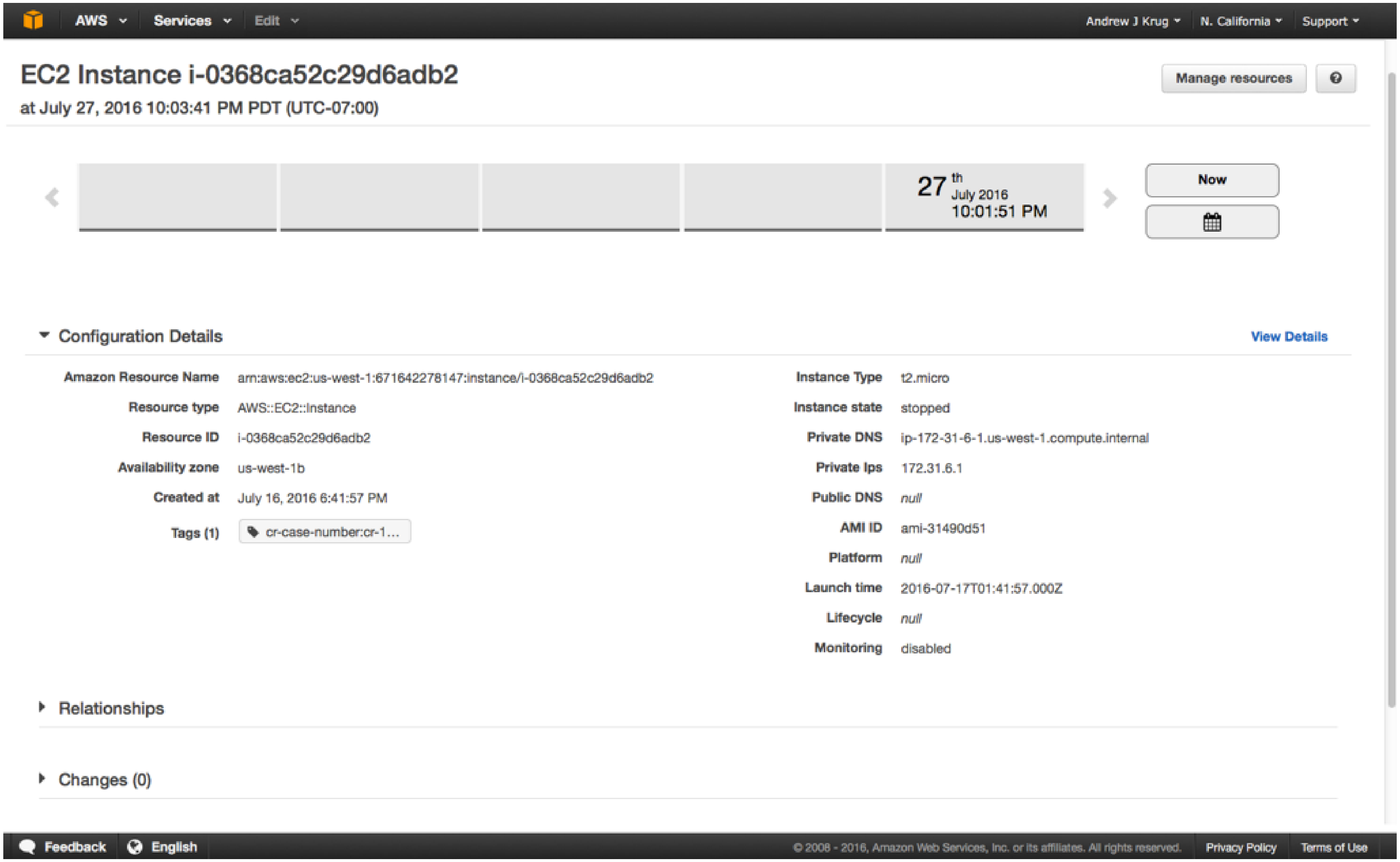
○ Choose a topic from your account

○ Choose a topic from another account

Topic name* config-topic

What to notify

Config Timeline



EC2 Instance i-0368ca52c29d6adb2

at July 27, 2016 10:03:41 PM PDT (UTC-07:00)

27 th July 2016 10:01:51 PM

Configuration Details

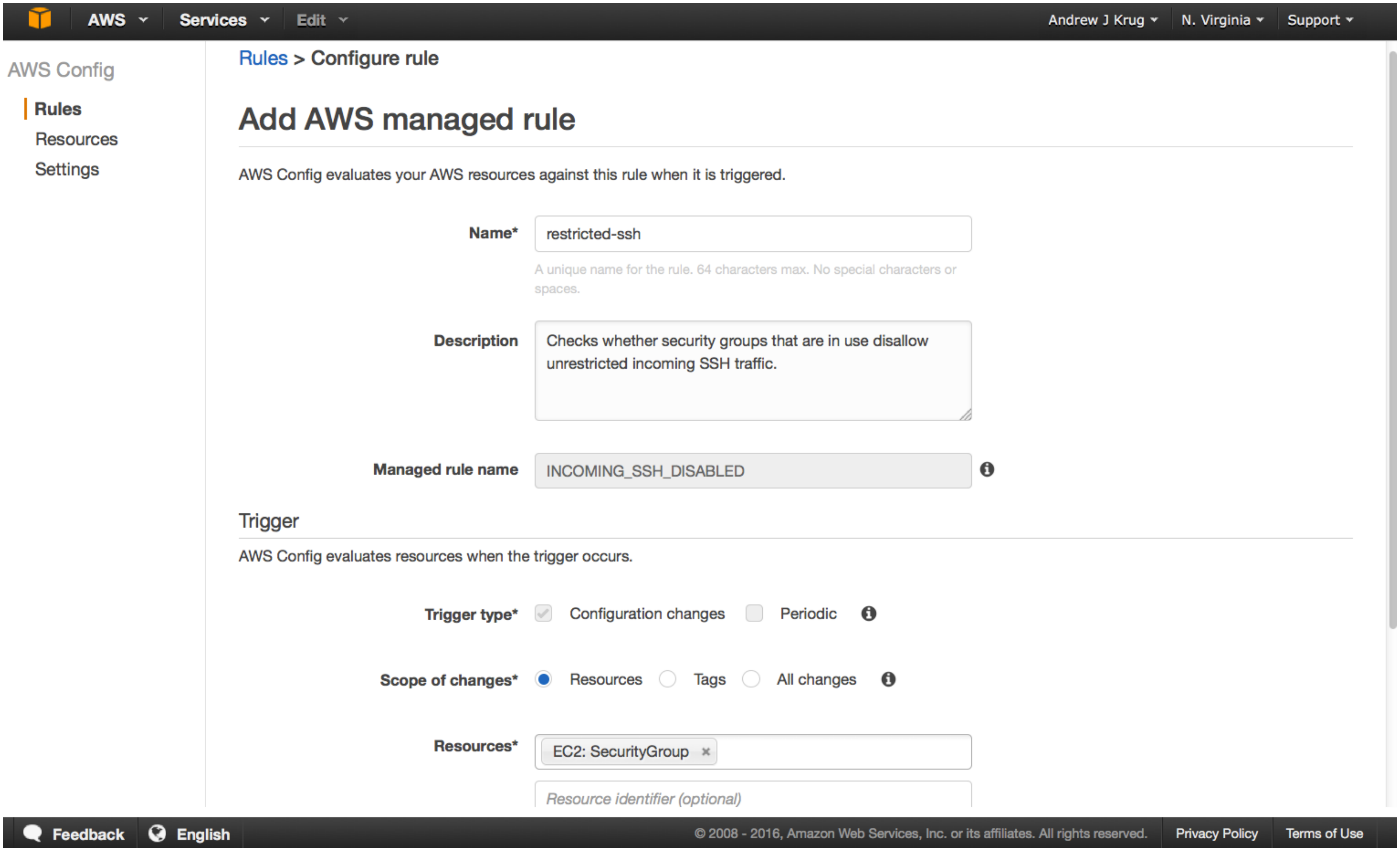
View Details

Amazon Resource Name	arn:aws:ec2:us-west-1:671642278147:instance/i-0368ca52c29d6adb2	Instance Type	t2.micro
Resource type	AWS::EC2::Instance	Instance state	stopped
Resource ID	i-0368ca52c29d6adb2	Private DNS	ip-172-31-6-1.us-west-1.compute.internal
Availability zone	us-west-1b	Private Ips	172.31.6.1
Created at	July 16, 2016 6:41:57 PM	Public DNS	*null*
Tags (1)	cr-case-number:cr-1…	AMI ID	ami-31490d51
		Platform	*null*
		Launch time	2016-07-17T01:41:57.000Z
		Lifecycle	*null*
		Monitoring	disabled

Relationships

Changes (0)

Config Rules



Rules > Configure rule

Add AWS managed rule

AWS Config evaluates your AWS resources against this rule when it is triggered.

Name*: restricted-ssh

A unique name for the rule. 64 characters max. No special characters or spaces.

Description: Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

Managed rule name: INCOMING_SSH_DISABLED

Trigger

AWS Config evaluates resources when the trigger occurs.

Trigger type*: ☑ Configuration changes □ Periodic

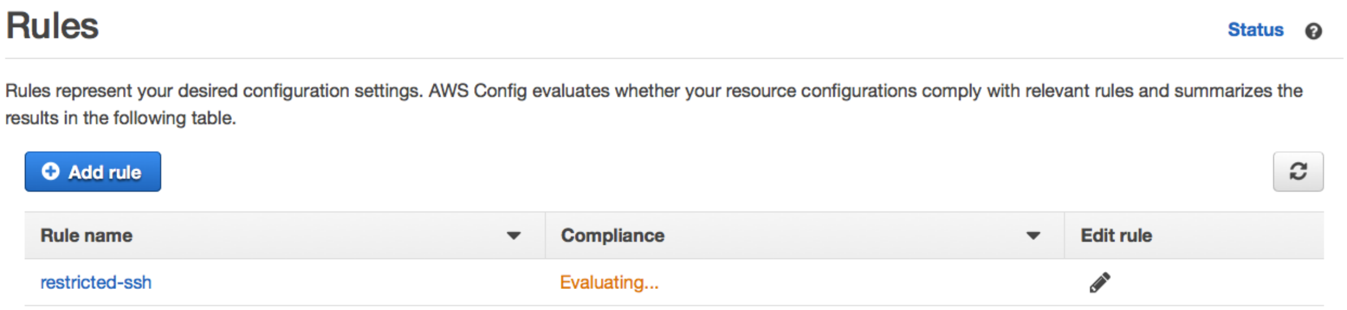
Scope of changes*: ● Resources ○ Tags ○ All changes

Resources*: EC2: SecurityGroup ×

Resource identifier (optional)

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Evaluation



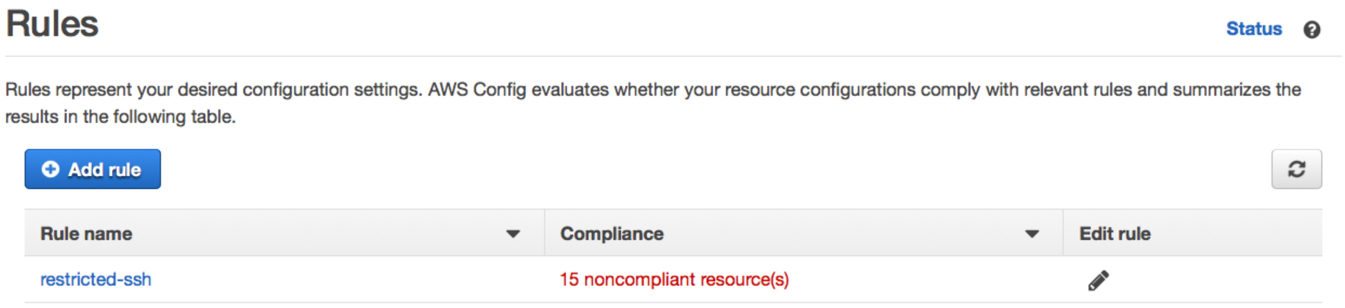
Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

Rule name	Compliance	Edit rule
restricted-ssh	Evaluating...	✎

This is Config running the first evaluation of the rule.

Report



Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

Rule name	Compliance	Edit rule
restricted-ssh	15 noncompliant resource(s)	✎

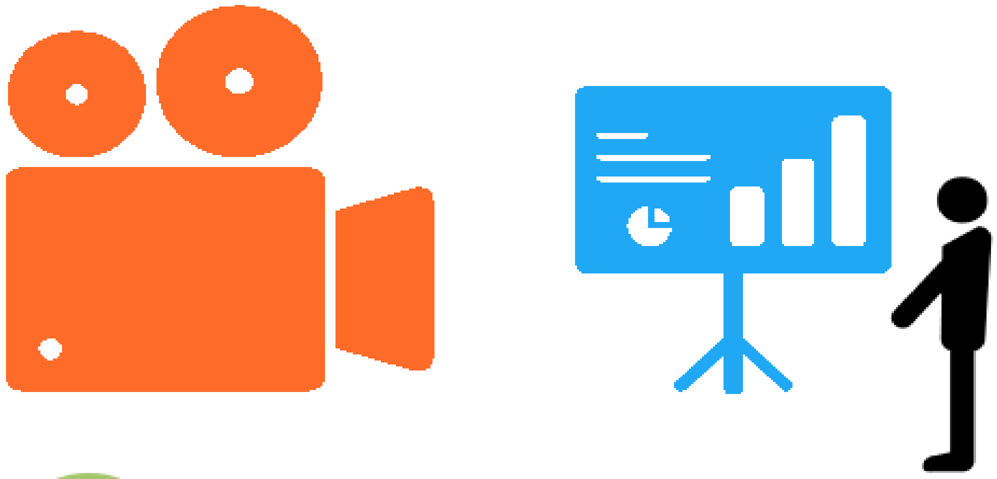
This is Config reporting on non-compliance.

Config and Lambda

Security improves with automated response.

CloudWatchEvents and Lambda

Video Demonstration



ThreatResponse

CLOUD SECURITY

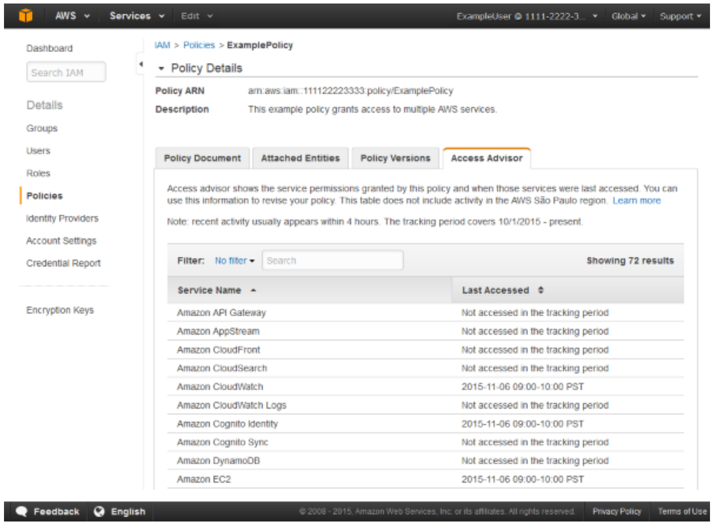
Recommended Viewing

There's also a great presentation about this:

AWS re:Invent 2015 | (SEC308) Wrangling Security Events in The Cloud

http://amzn.to/2aN6Js5

Access Advisor



Policy Details

Policy ARN arn:aws:iam::111122223333:policy/ExamplePolicy

Description This example policy grants access to multiple AWS services.

Access advisor shows the service permissions granted by this policy and when those services were last accessed. You can use this information to revise your policy. This table does not include activity in the AWS São Paulo region. Learn more

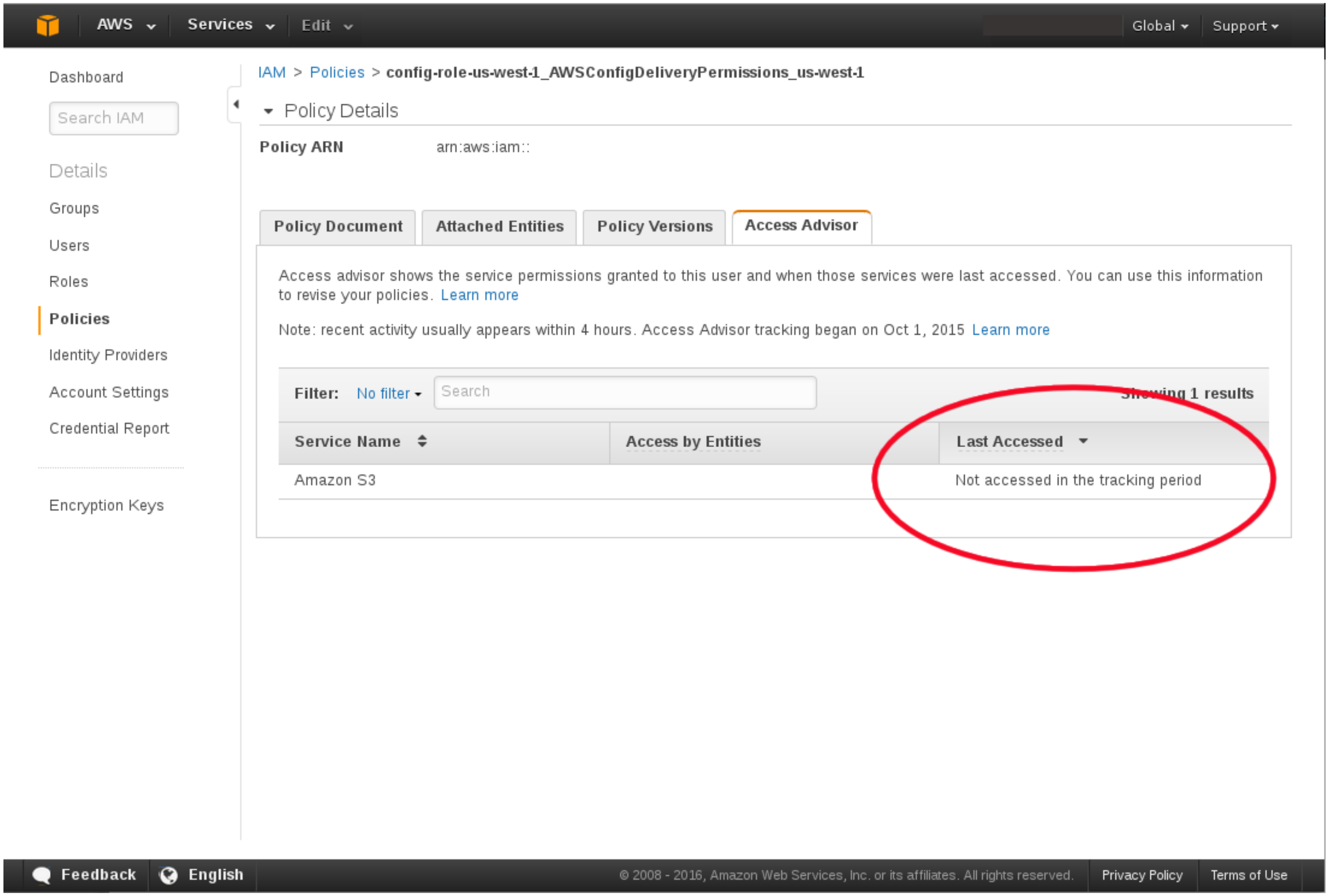
Note: recent activity usually appears within 4 hours. The tracking period covers 10/1/2015 - present.

Filter: No filter ▾ Search Showing 72 results

Service Name ▲	Last Accessed ⇕
Amazon API Gateway	Not accessed in the tracking period
Amazon AppStream	Not accessed in the tracking period
Amazon CloudFront	Not accessed in the tracking period
Amazon CloudSearch	Not accessed in the tracking period
Amazon CloudWatch	2015-11-06 09:00-10:00 PST
Amazon CloudWatch Logs	Not accessed in the tracking period
Amazon Cognito Identity	2015-11-06 09:00-10:00 PST
Amazon Cognito Sync	Not accessed in the tracking period
Amazon DynamoDB	Not accessed in the tracking period
Amazon EC2	2015-11-06 09:00-10:00 PST

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Great tutorial on getting going with access advisor: http://amzn.to/2aN6Js5



IAM > Policies > config-role-us-west-1_AWSConfigDeliveryPermissions_us-west-1

Policy Details

Policy ARN arn:aws:iam::

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. Learn more

Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015 Learn more

Filter: No filter Search Showing 1 results

Service Name	Access by Entities	Last Accessed
Amazon S3		Not accessed in the tracking period

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Advice to take away

Use custom policies

Audit them using access Advisor

Revoke permissions you don't need

Tool Gaps

Mission

Be a 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.

The Question?

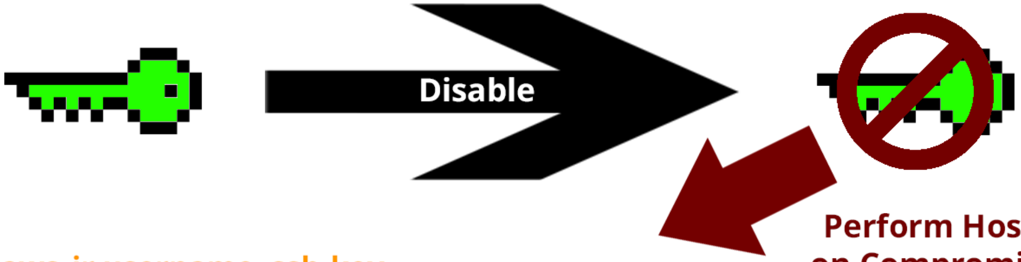
Can we leverage the AWS API to perform incident response?

Host Based

vs

Key Based

Key Compromise

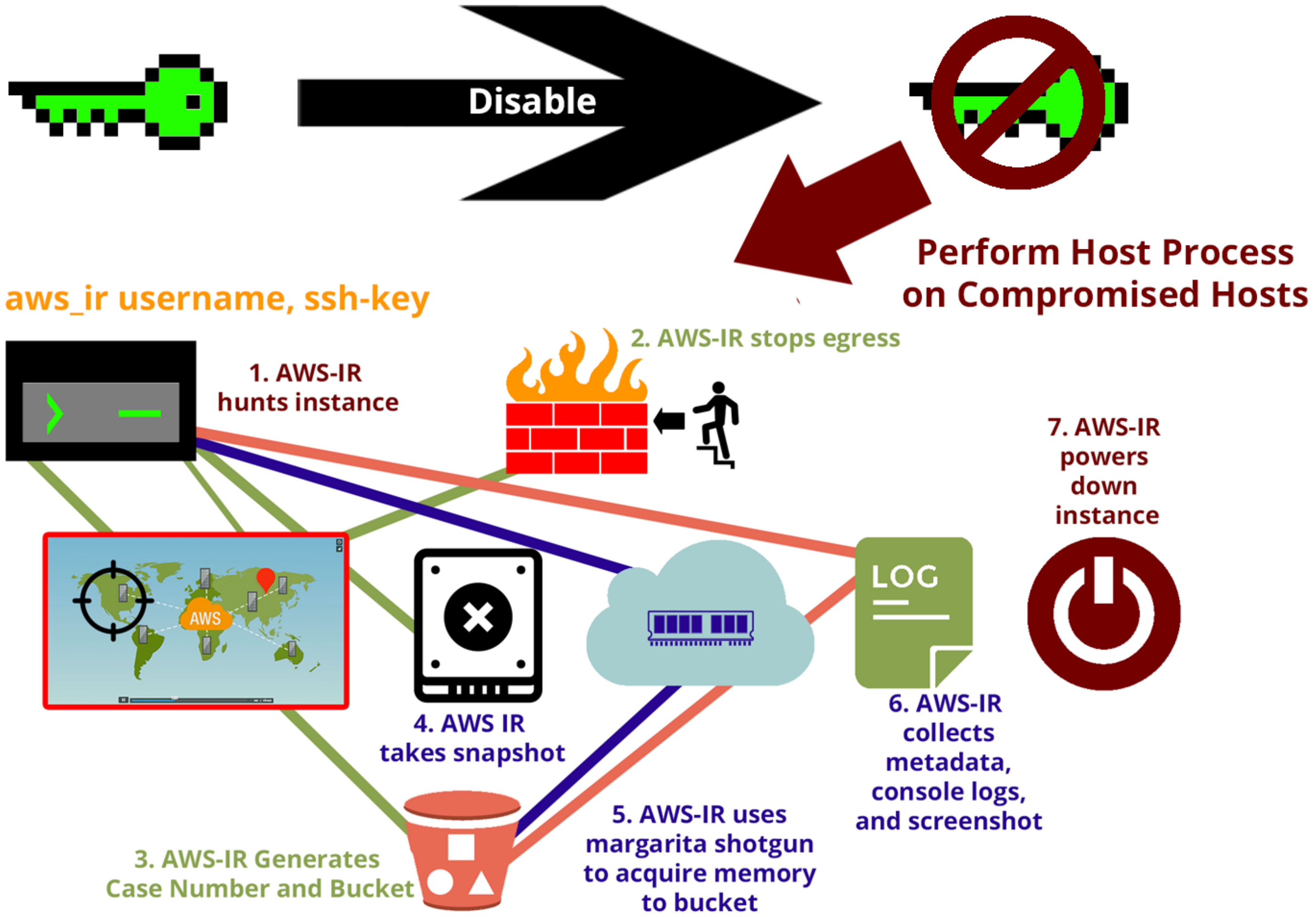


Disable

Perform Host Process
on Compromised Hosts

aws_ir username, ssh-key

In key compromise we always want to disable the key.



Perform Host Process on Compromised Hosts

aws_ir username, ssh-key

1. AWS-IR hunts instance

2. AWS-IR stops egress

3. AWS-IR Generates Case Number and Bucket

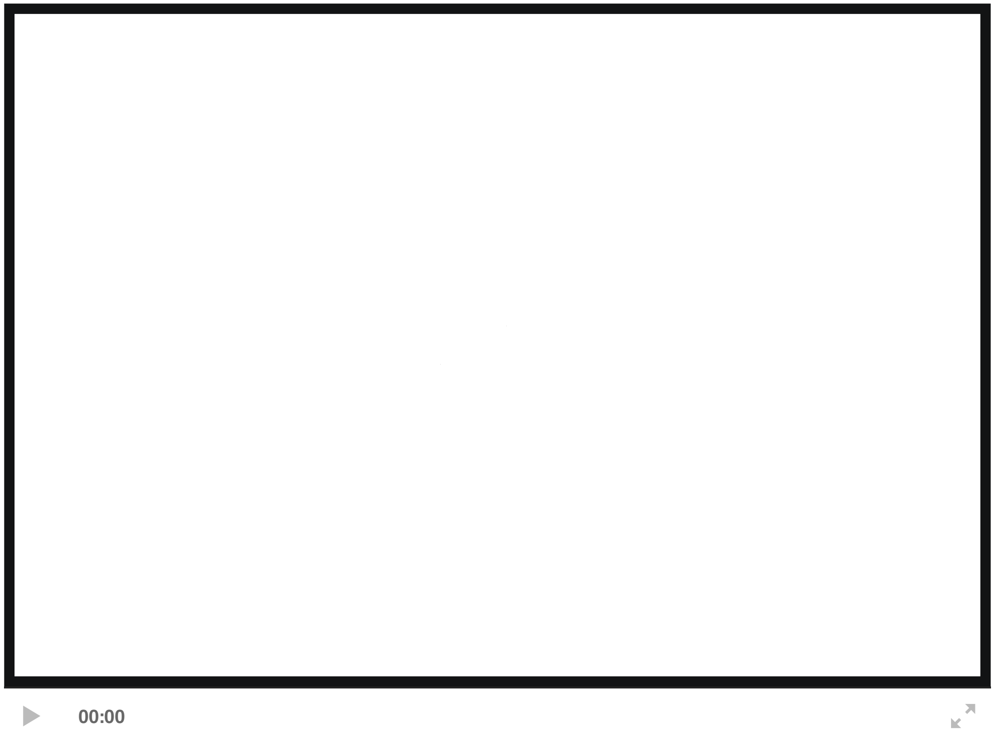
4. AWS IR takes snapshot

5. AWS-IR uses margarita shotgun to acquire memory to bucket

6. AWS-IR collects metadata, console logs, and screenshot

7. AWS-IR powers down instance

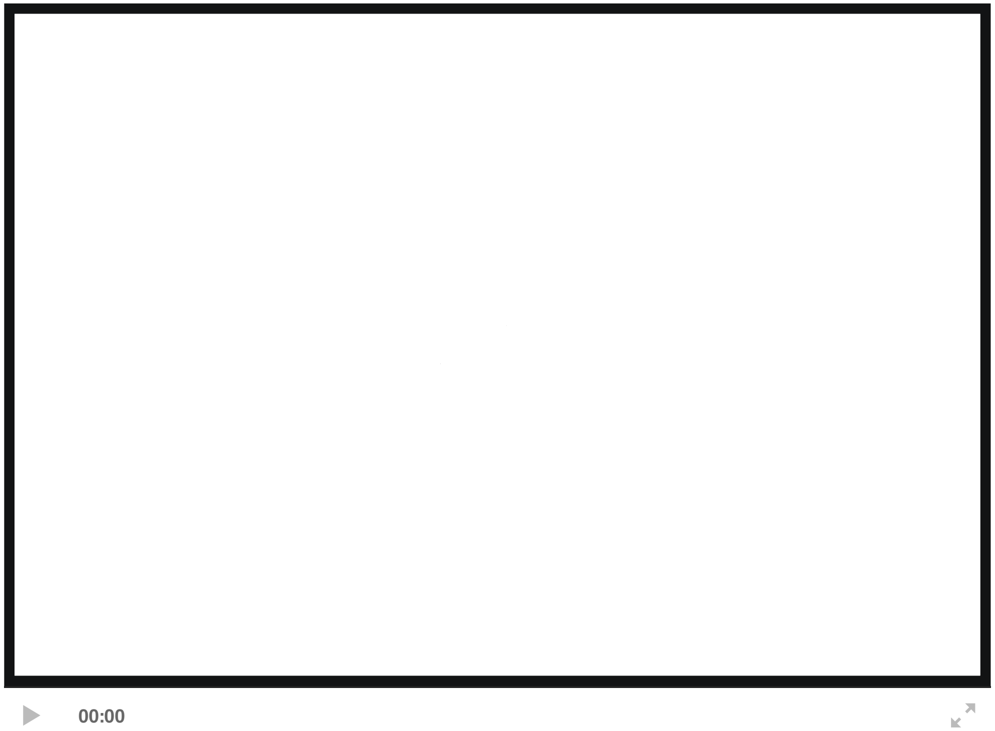
Key Compromise Demo



Now to host based compromises with AWS_IR

AWS_IR Usage

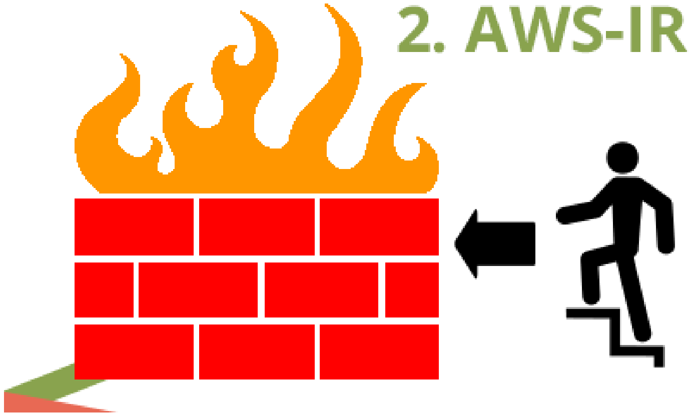
```
[krug@bb-8 lots_of_haxx ]$ aws_ir
aws_ir host_compromise
usage:
aws_ir host_compromise
ip user ssh_key_file
```


00:00

Step 1

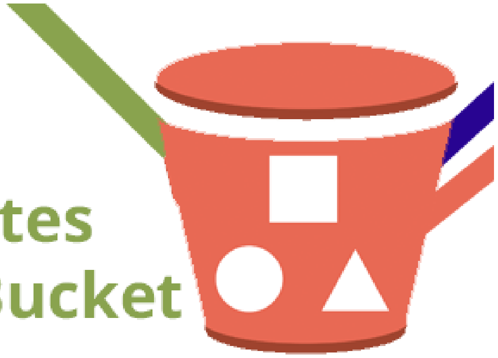
1. AWS-IR hunts instance

Step 2



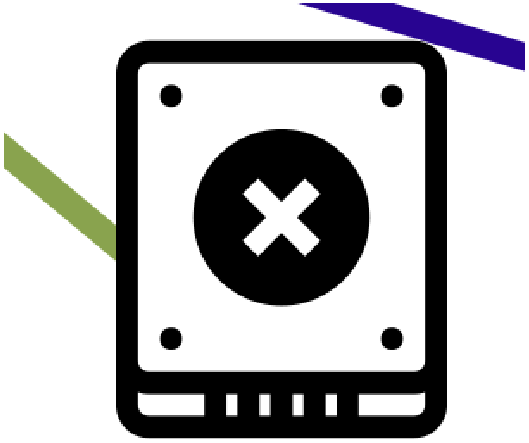
2. AWS-IR stops egress

Step 3



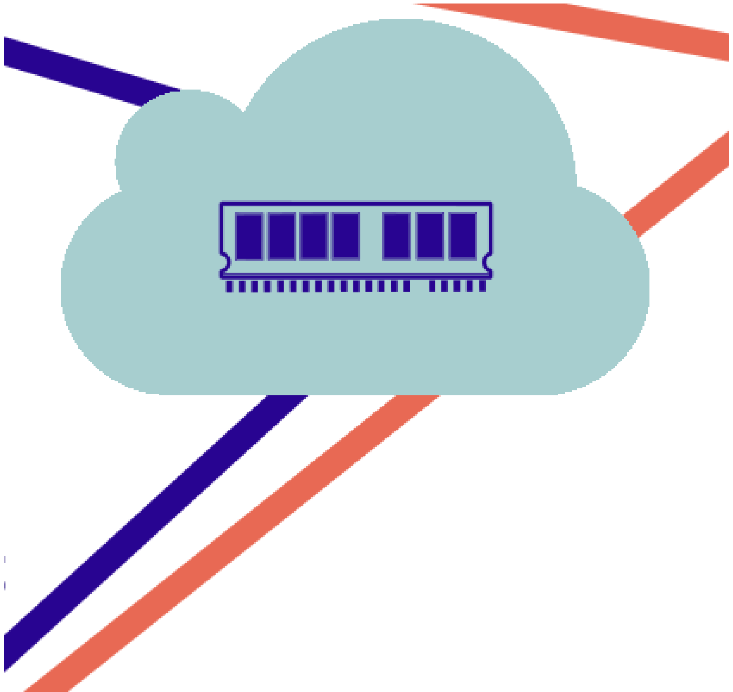
3. AWS-IR Generates Case Number and Bucket

Step 4



4. AWS IR
takes snapshot

Step 5



5. AWS-IR uses margarita shotgun to acquire memory to bucket

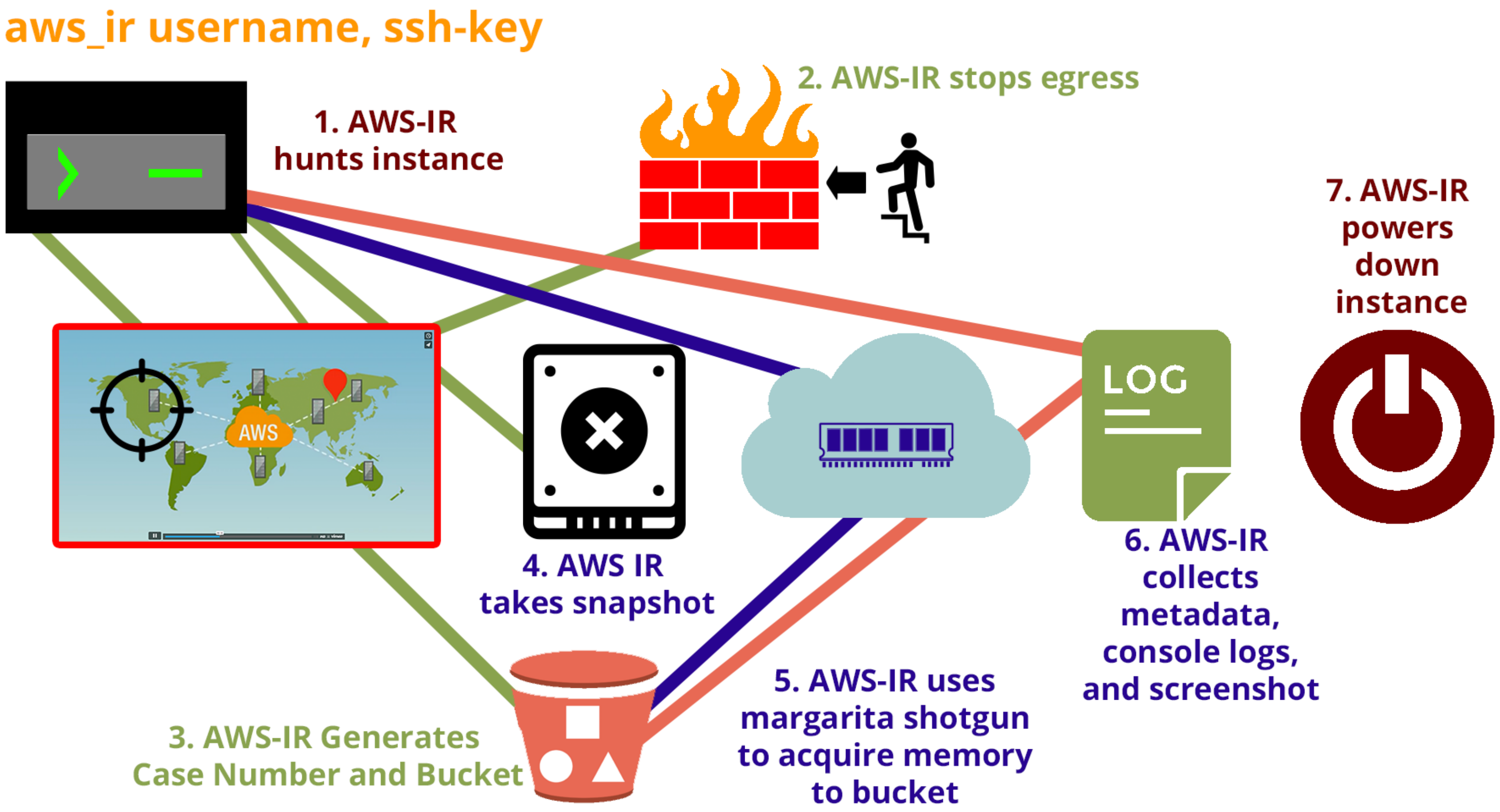
Step 6

6. AWS-IR collects metadata, console logs, and screenshot

Step 7

7. AWS-IR powers down instance

The whole picture



aws_ir username, ssh-key

1. AWS-IR hunts instance

2. AWS-IR stops egress

3. AWS-IR Generates Case Number and Bucket

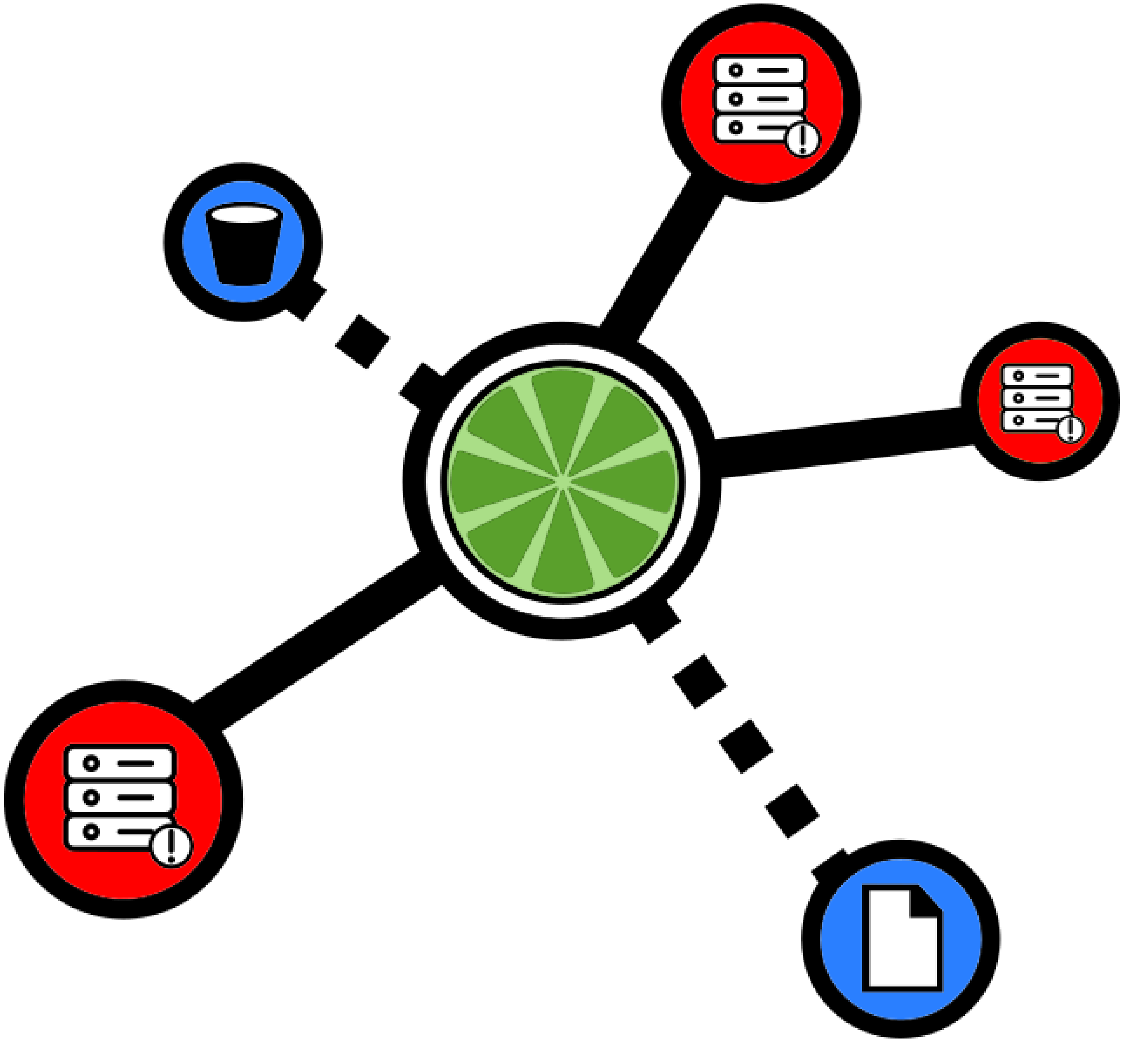
4. AWS IR takes snapshot

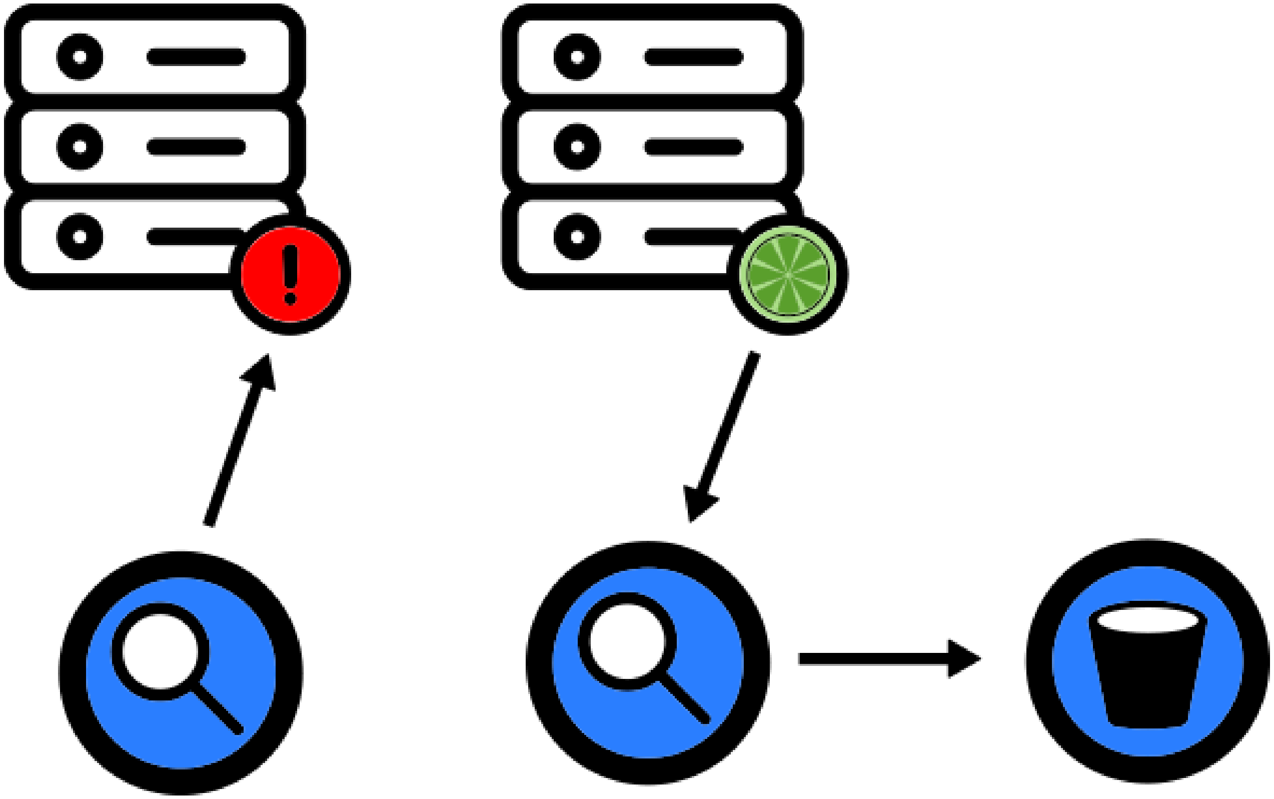
5. AWS-IR uses margarita shotgun to acquire memory to bucket

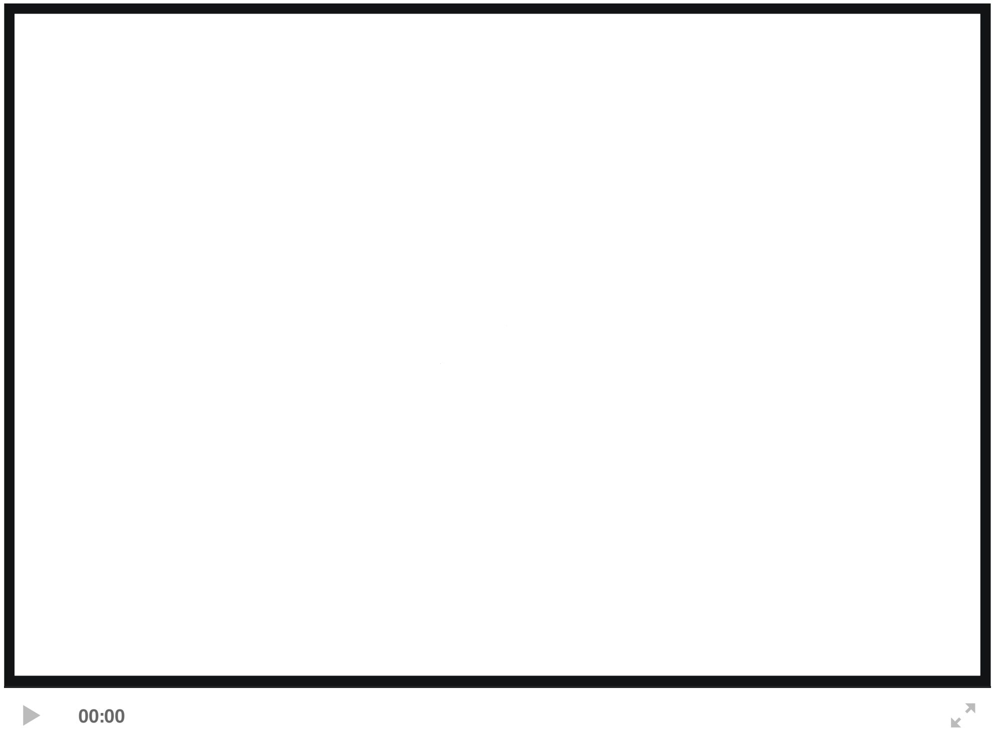
6. AWS-IR collects metadata, console logs, and screenshot

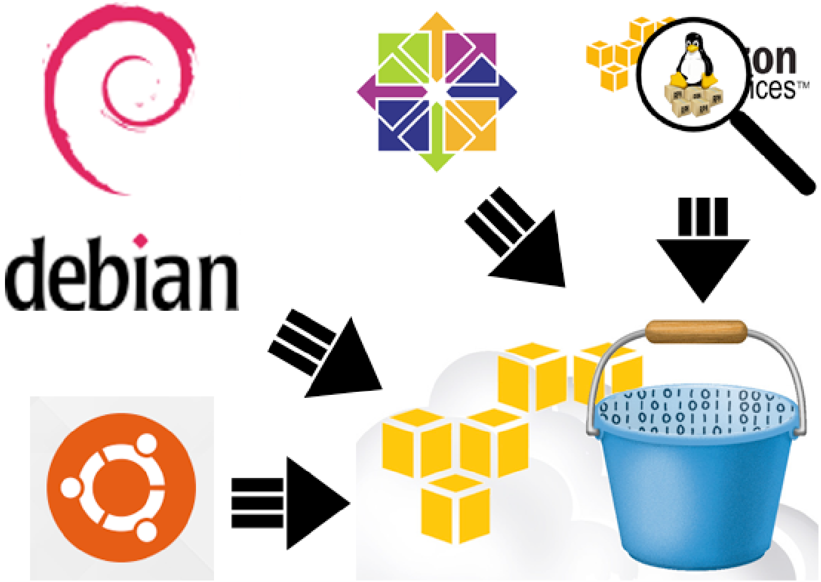
7. AWS-IR powers down instance

Margarita Shotgun



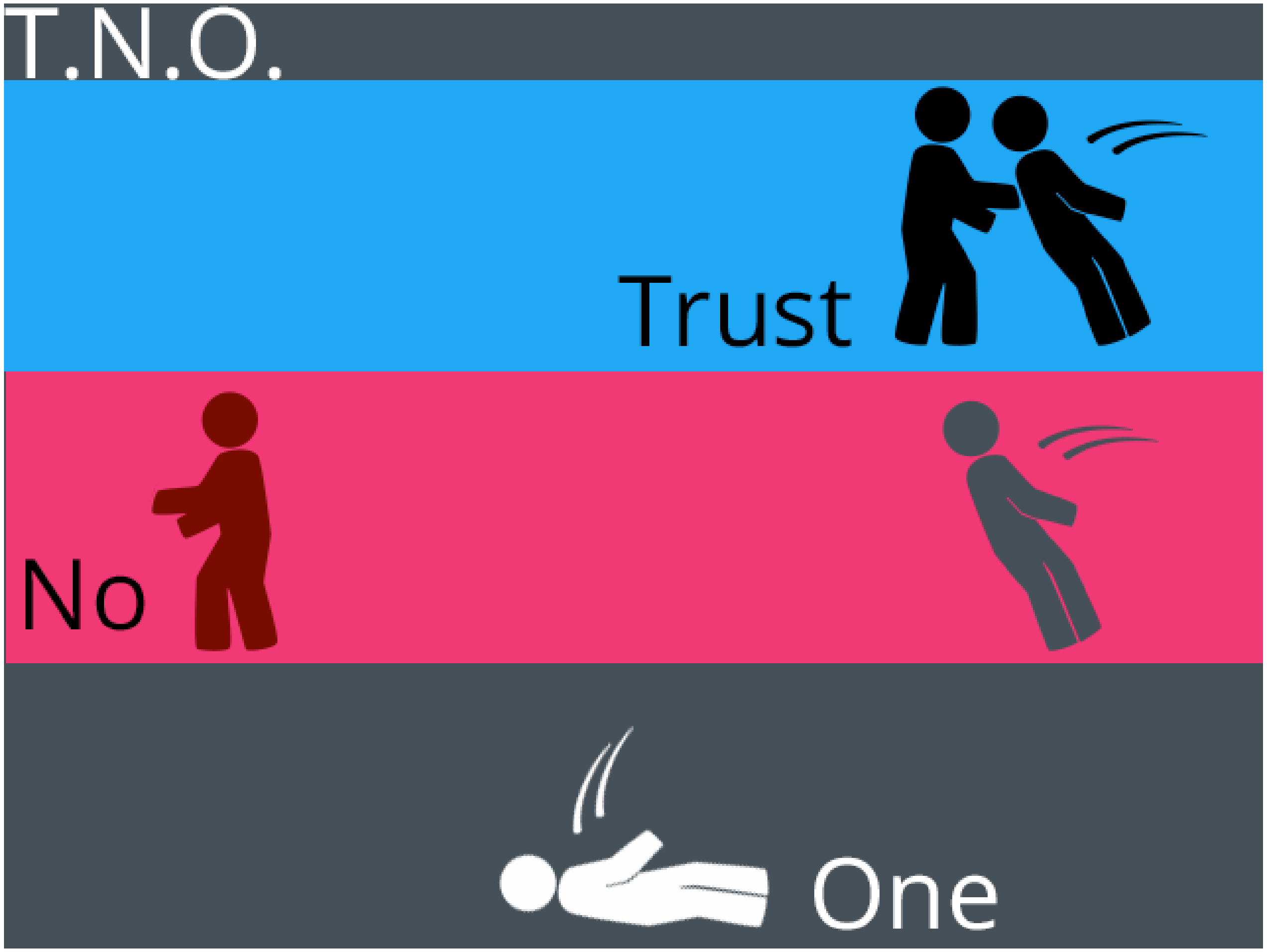



00:00



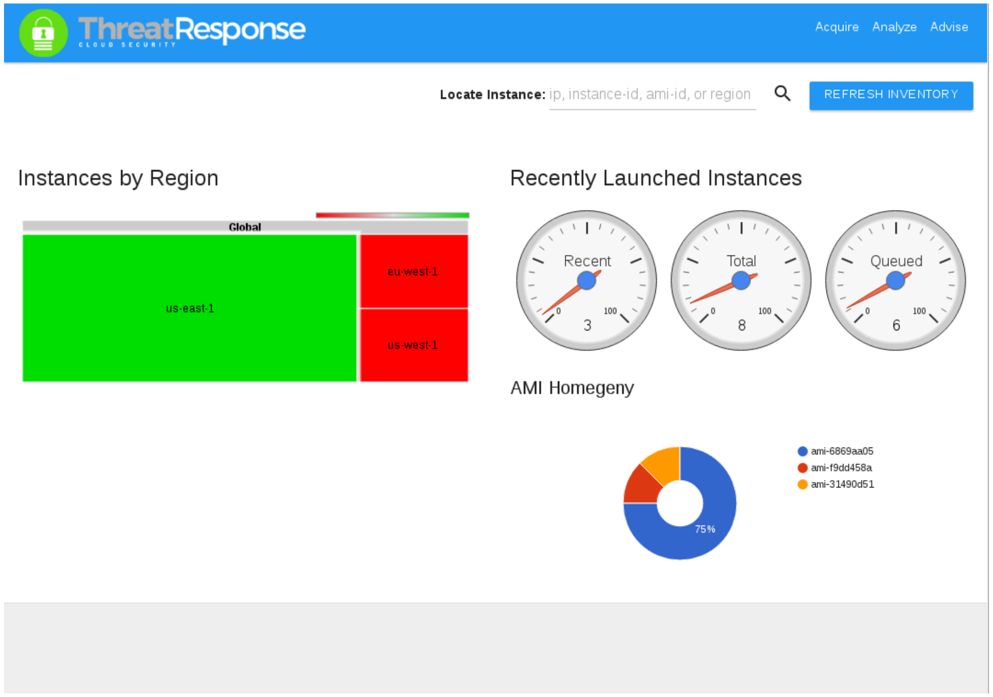
Kernel Module Warehouse

Kernel warehouse is a ruby gem that builds all the modules for all support AWS linux variants.



You can host your own or use ours.

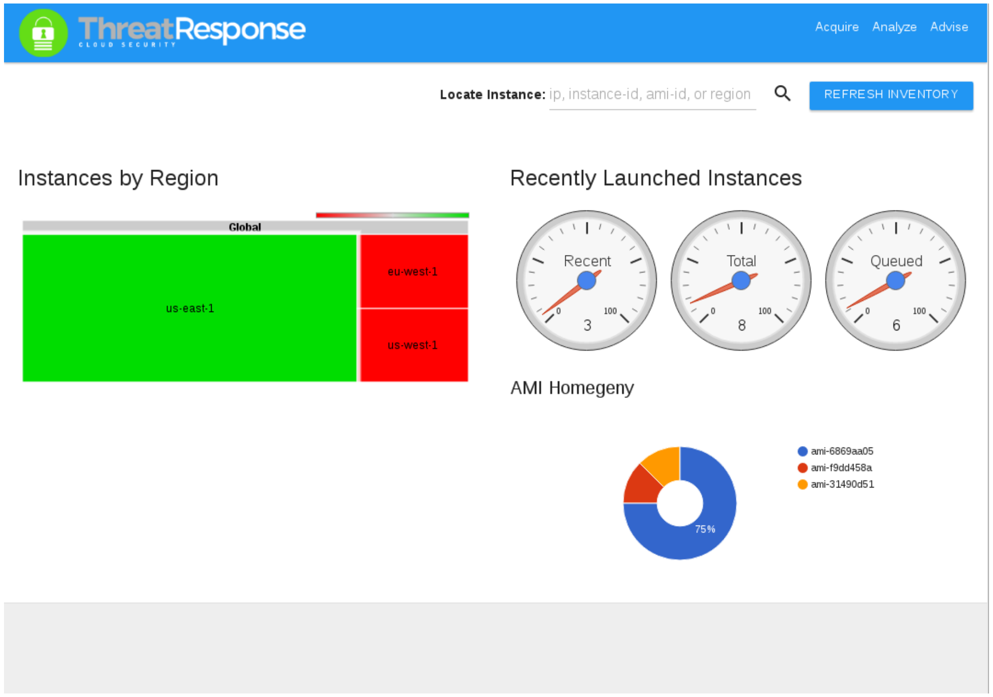
ThreatResponse Workstation



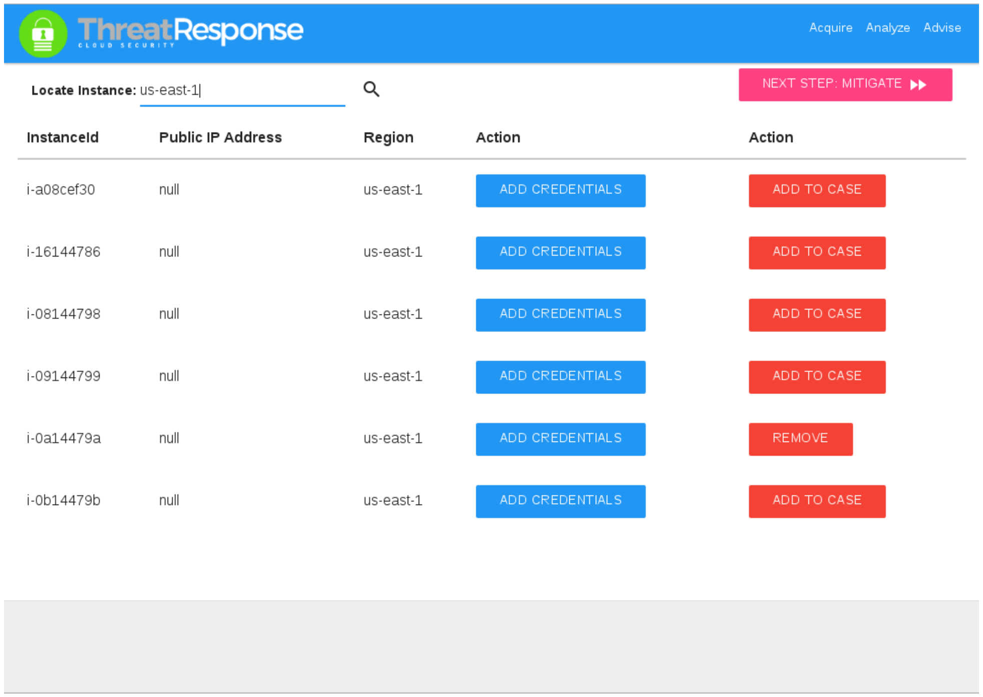
Starting ThreatResponse Workstation

```
$ aws_ir host_compromise 52.42.254.41 ec2-user key.pem
...
...
...

Processing complete : Launch an analysis workstation with the command

    aws_ir -n cr-16-072816-a4d6 create_workstation us-west-2


$ aws_ir host_compromise -c 52.42.254.41 ec2-user key.pem
```

ThreatResponse Dashboard



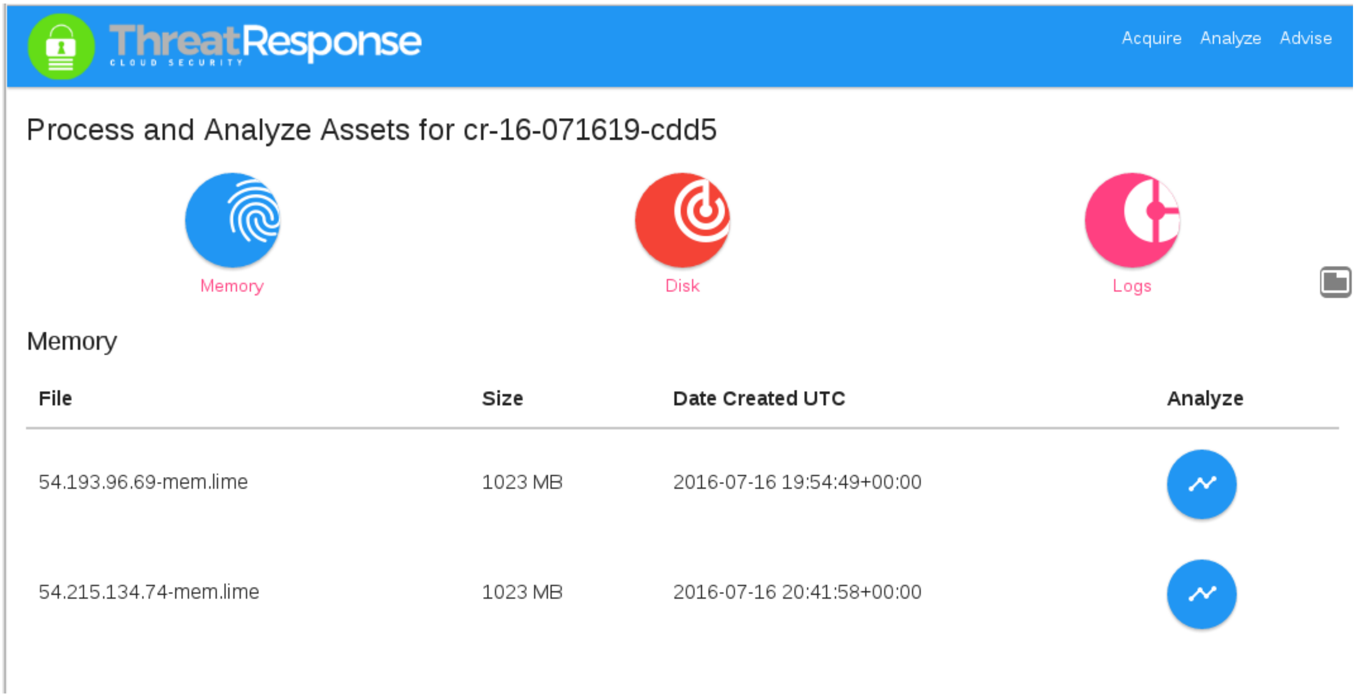
ThreatResponse Acquire



Locate Instance: us-east-1

InstanceId	Public IP Address	Region	Action	Action
i-a08cef30	null	us-east-1	ADD CREDENTIALS	ADD TO CASE
i-16144786	null	us-east-1	ADD CREDENTIALS	ADD TO CASE
i-08144798	null	us-east-1	ADD CREDENTIALS	ADD TO CASE
i-09144799	null	us-east-1	ADD CREDENTIALS	ADD TO CASE
i-0a14479a	null	us-east-1	ADD CREDENTIALS	REMOVE
i-0b14479b	null	us-east-1	ADD CREDENTIALS	ADD TO CASE

Analyze - Memory

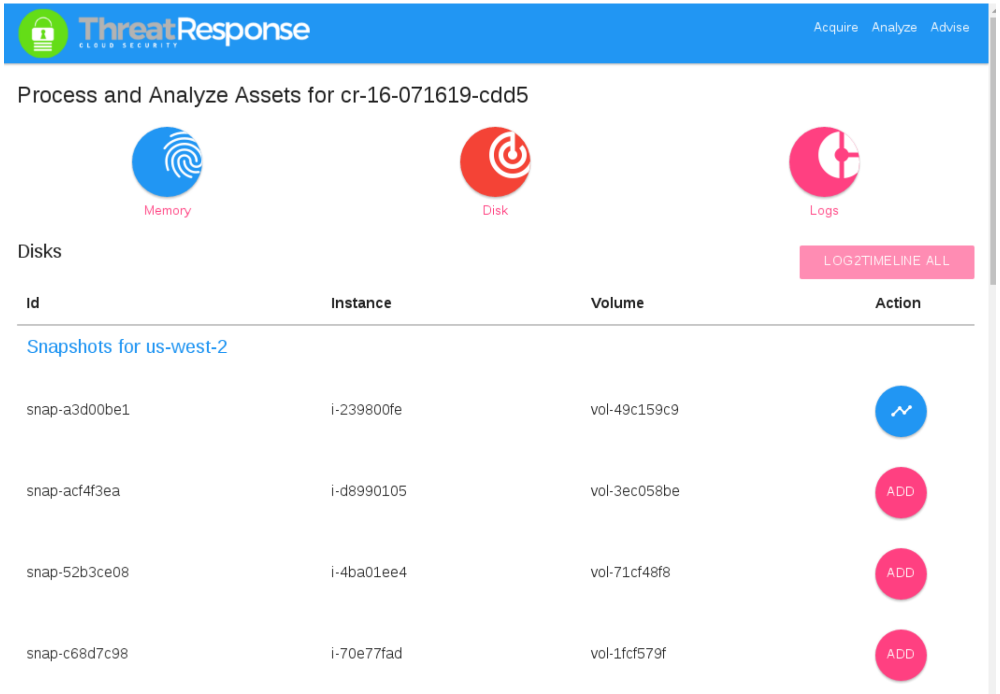


Process and Analyze Assets for cr-16-071619-cdd5

Memory

File	Size	Date Created UTC	Analyze
54.193.96.69-mem.lime	1023 MB	2016-07-16 19:54:49+00:00	
54.215.134.74-mem.lime	1023 MB	2016-07-16 20:41:58+00:00	

ThreatResponse Analyze - Disk

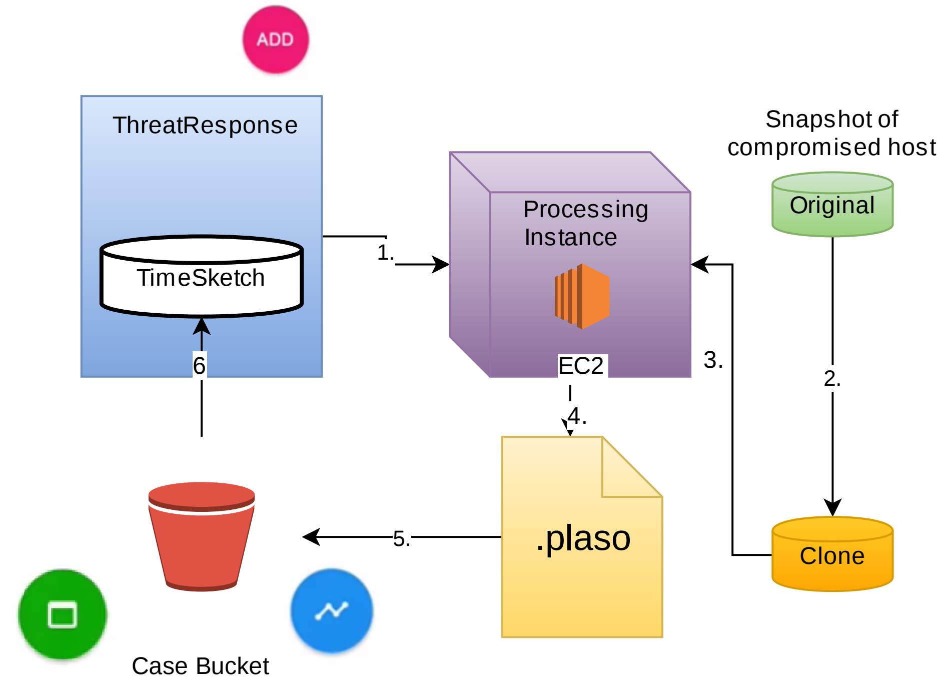


Process and Analyze Assets for cr-16-071619-cdd5

Disks

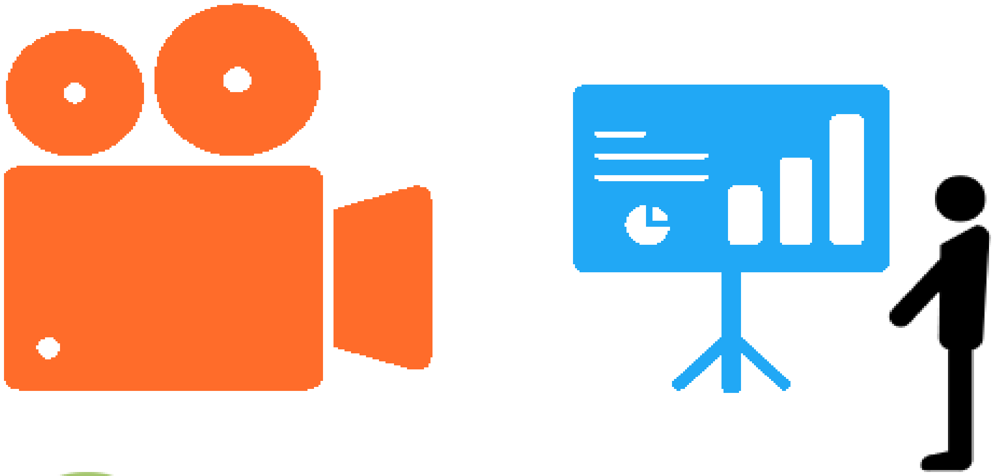
Id	Instance	Volume	Action
Snapshots for us-west-2			
snap-a3d00be1	i-239800fe	vol-49c159c9	
snap-acf4f3ea	i-d8990105	vol-3ec058be	ADD
snap-52b3ce08	i-4ba01ee4	vol-71cf48f8	ADD
snap-c68d7c98	i-70e77fad	vol-1fcf579f	ADD

ThreatResponse Analyze - Disk



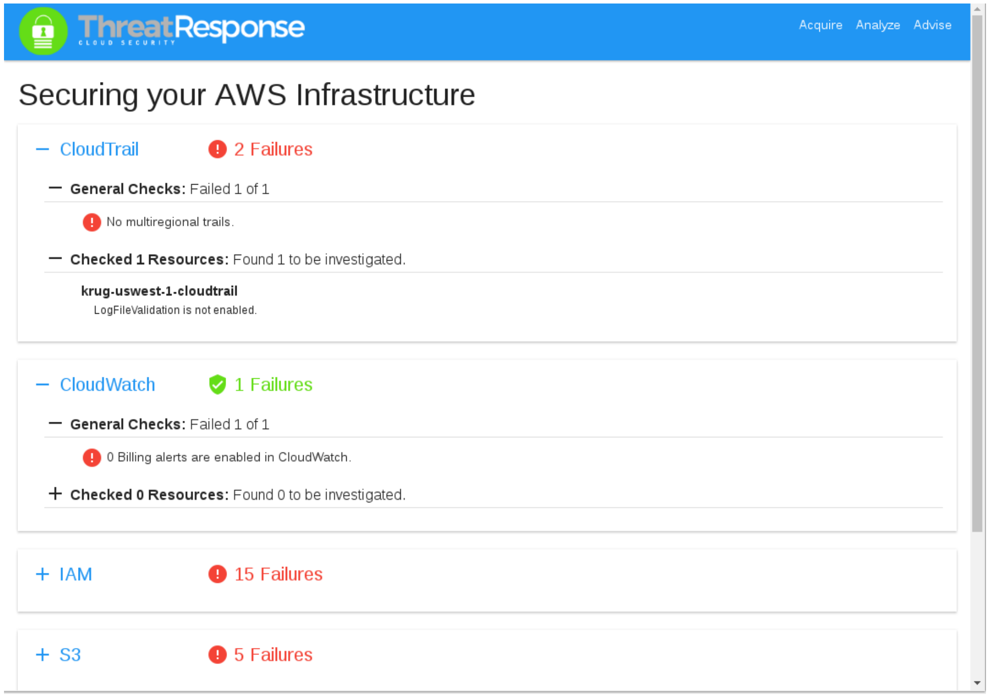
Video Tour ThreatResponse Disk Analysis

Video Demonstration



ThreatResponse
CLOUD SECURITY

Advice



Securing your AWS Infrastructure

− CloudTrail ❗ 2 Failures

− **General Checks:** Failed 1 of 1

❗ No multiregional trails.

− **Checked 1 Resources:** Found 1 to be investigated.

krug-uswest-1-cloudtrail
LogFileValidation is not enabled.

− CloudWatch ✓ 1 Failures

− **General Checks:** Failed 1 of 1

❗ 0 Billing alerts are enabled in CloudWatch.

+ **Checked 0 Resources:** Found 0 to be investigated.

+ IAM ❗ 15 Failures

+ S3 ❗ 5 Failures

S3 Checks

Versioning

Logging

Open Permissions

IAM Checks

MFA

Rotated Credentials

Administrator Access Policy

Other Checks

VPCs: Flow Logging

CloudTrail: MultiRegion & validation

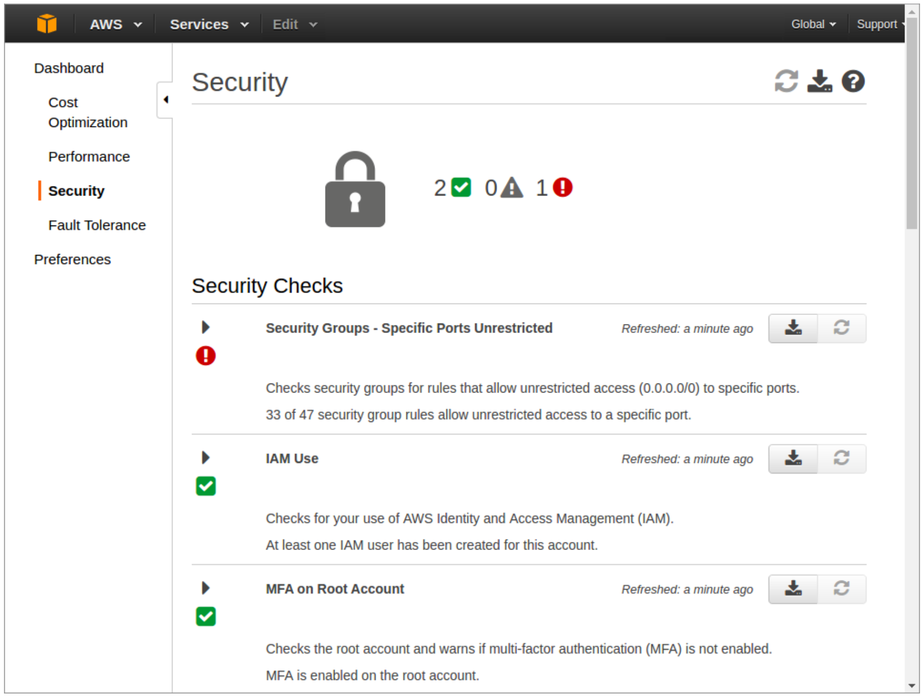
Other Checks

Disable access keys on the root account

Ensures an IAM role exists

Cloudwatch Billing Alerts

AWS Trusted Advisor



Security

2 ✓ 0 ⚠ 1 !

Security Checks

Security Groups - Specific Ports Unrestricted *Refreshed: a minute ago*

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

33 of 47 security group rules allow unrestricted access to a specific port.

IAM Use *Refreshed: a minute ago*

Checks for your use of AWS Identity and Access Management (IAM).

At least one IAM user has been created for this account.

MFA on Root Account *Refreshed: a minute ago*

Checks the root account and warns if multi-factor authentication (MFA) is not enabled.

MFA is enabled on the root account.

AWS Config

AWS Config - $.003 per configuration item

AWS Config Rules - $2 per rule per month for $20,000 evaluations.

Review of Tools

Margarita Shotgun

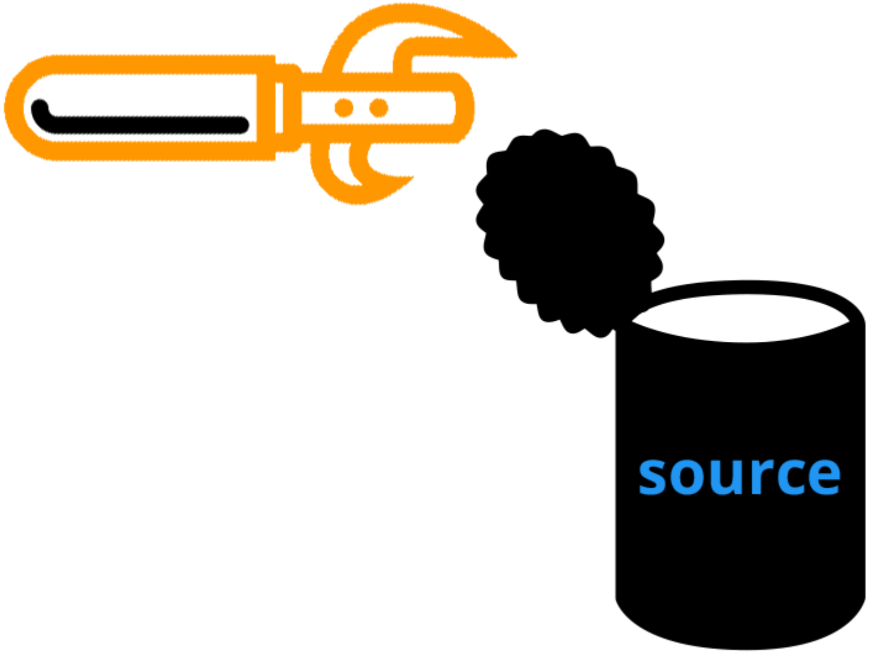
AWS-IR Cli

ThreatResponse WebApp

ThreatPrep Advising

AWS ThreatPrep

Brief: What's going on in Open Cloud Security



Evolve your understanding through experimentation!

Dont!

Wait to try out some of these tools

Do!

Have a test environment

Security simulations

IR Game Days

What does that even mean?

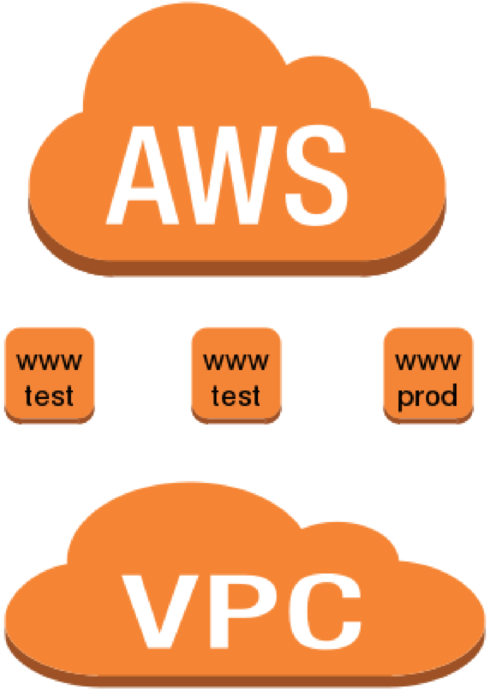
Test environments

Build a Continuous Integration Culture

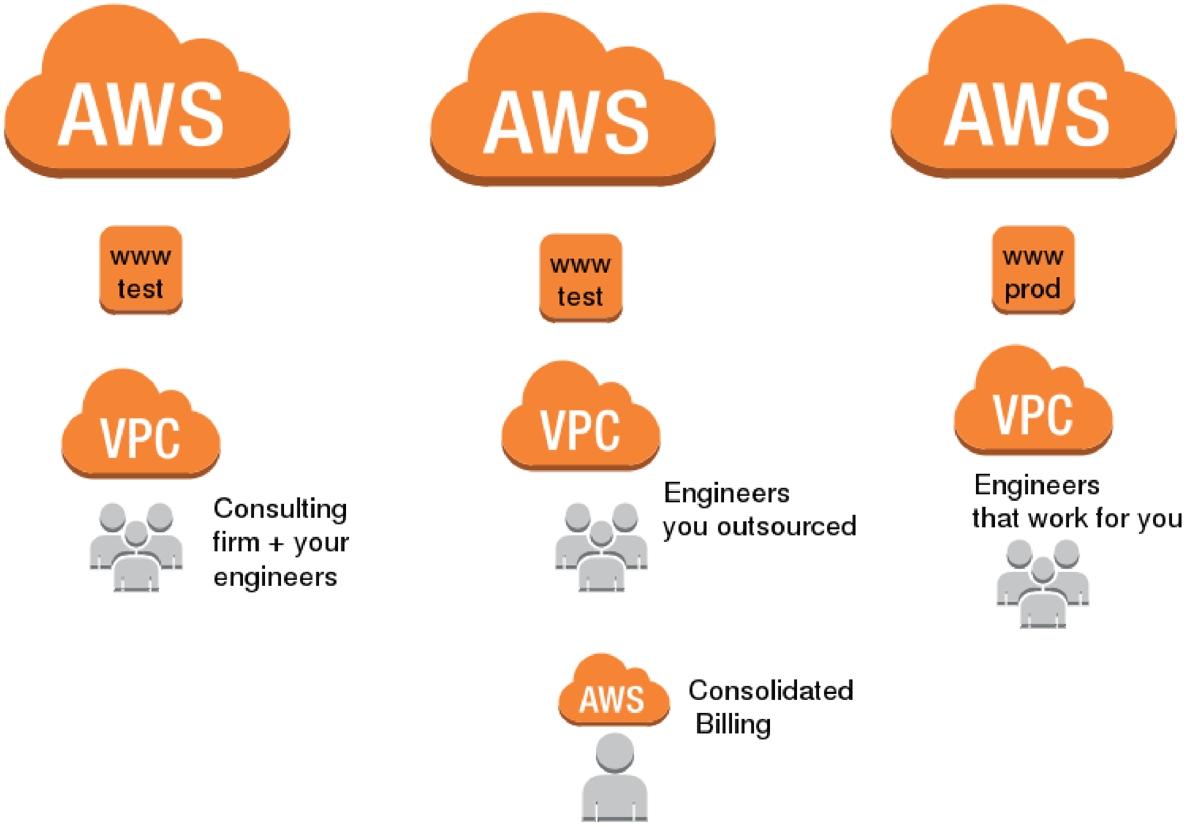
Have separate AWS accounts for Dev, Test, etc...

Use consolidated billing.

Mixed Environment



Separation



AWS
AWS
AWS
www
test
www
test
www
prod
VPC
VPC
VPC
Consulting firm + your engineers
Engineers you outsourced
Engineers that work for you
AWS
Consolidated Billing

What do all these engineers have in common?

About Security Simulation

1. Basically you fake a hack or two.
2. Some percentage of employees know.
3. Some percentage don't know.
4. Process it like a real exercise.

PSA : Tell Amazon if you do these.

AWS Policies do allow for security simulation and IR game days. They just ask that you let them know in advance.

Other Projects in the Space

Simian Army

NETFLIX

Captiol One Cloud Custodian

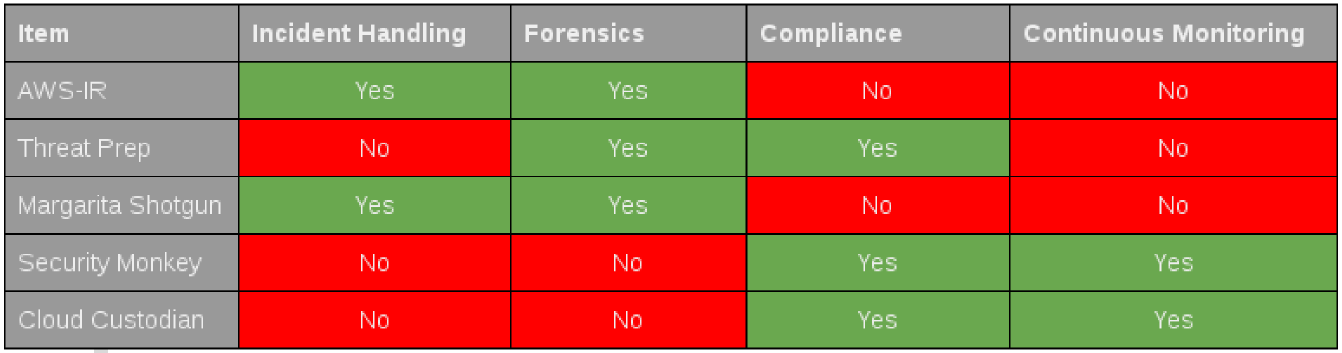
https://github.com/capitalone/cloud-custodian

Rule Engine

Can create lambda functions for you

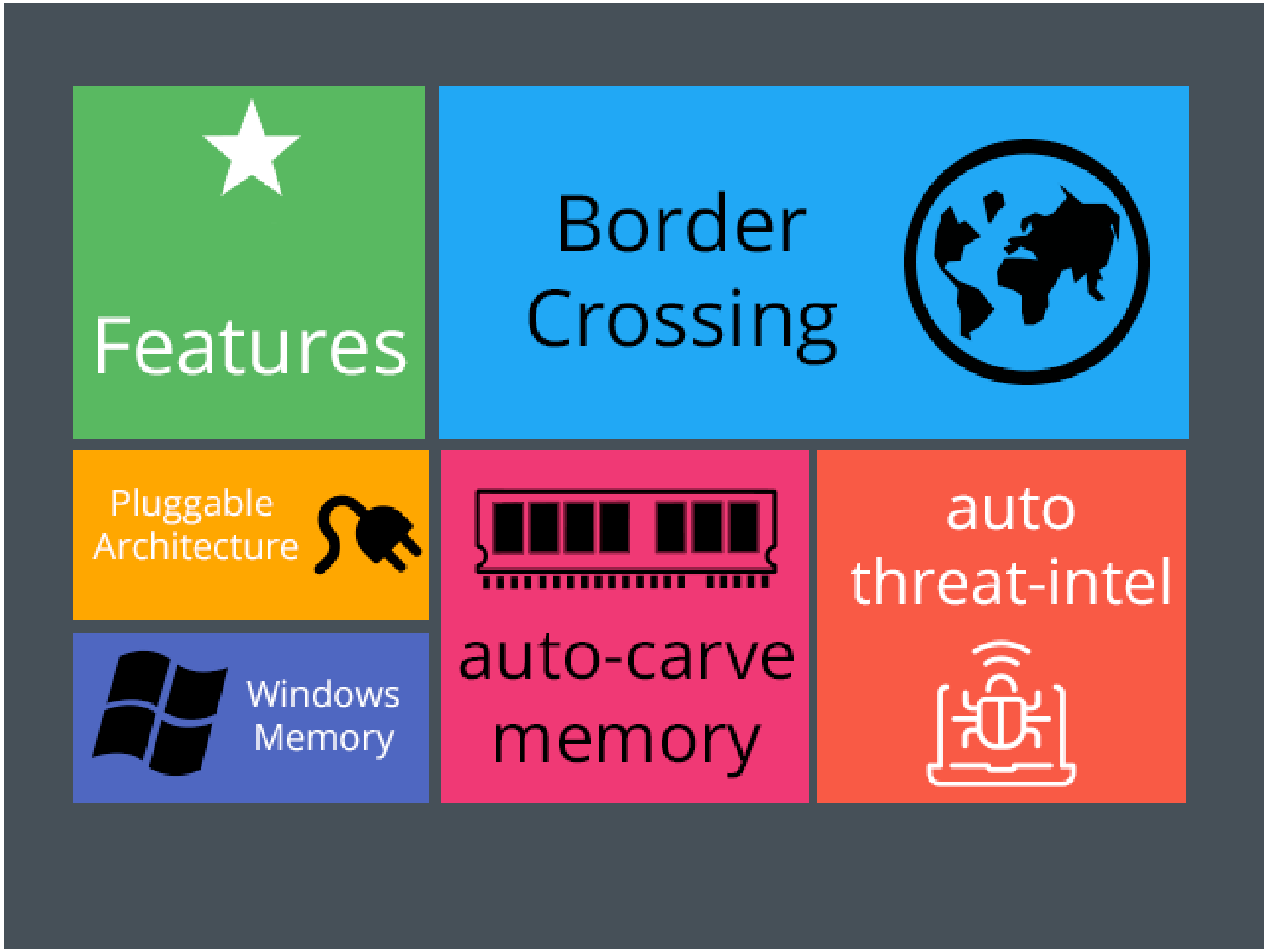
Around since April 2016

Feature Comparison



Item	Incident Handling	Forensics	Compliance	Continuous Monitoring
AWS-IR	Yes	Yes	No	No
Threat Prep	No	Yes	Yes	No
Margarita Shotgun	Yes	Yes	No	No
Security Monkey	No	No	Yes	Yes
Cloud Custodian	No	No	Yes	Yes

Future of the Tools



Features

Border Crossing

Pluggable Architecture

Windows Memory

auto-carve memory

auto threat-intel

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.

Thanks Amazon Web Services

Don Bailey

Zack Glick

Henrik Johansson

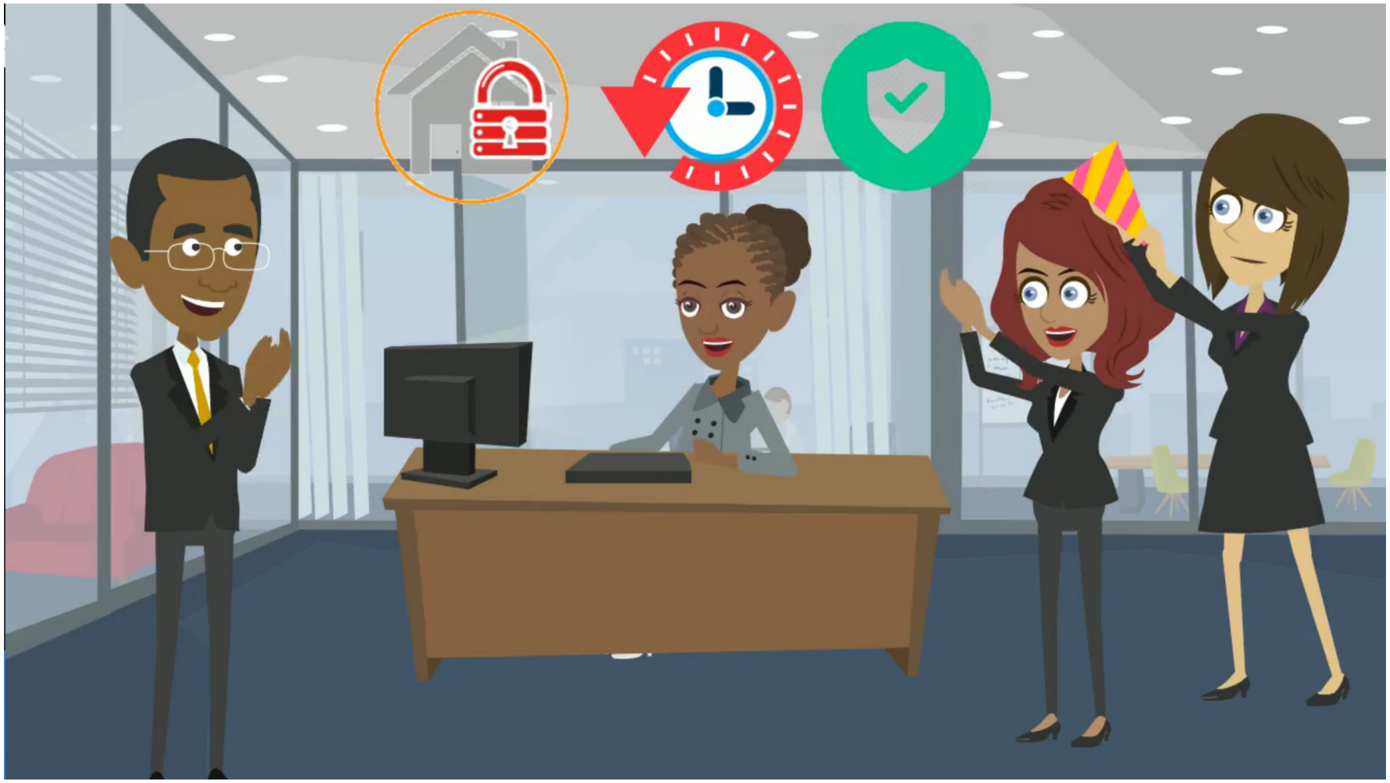
Where to get the software?

http://www.threatresponse.cloud

Releasing soon!

Signup for a notification.

Q&A



http://www.threatresponse.cloud