# BoB12th Digital Forensics AWS Team Assign



# **CICD Scenario**

Team Name:

디포기강잡조

Team Members:

김대호, 이은빈, 최서우, 최이슬, 홍지원

## 1. CI/CD Scenario

- 3 IAM Users
- 1 EC2 Instance in a single VPC
- 1 API Gateway
- 1 Lambda Function
- 1 ECR Image
- 2 CodeBuild Projects

#### 2. Scenario Initiation

Initial provision of IAM users with Access Key IDs and Secret Access Keys.

# 3. Scenario Story

• FooCorp is a company that offers public APIs. FooCorp's customers submit sensitive data to the API endpoint every minute.

POST {apiUrl}/prod/hello
Host: {apiHost}
Content-Type: text/html
superSecretData=...

- API: Implemented through a Lambda function exposed via an API Gateway.
- FooCorp, being a DevOps adopter, establishes a continuous deployment pipeline, which
  enables them to automatically deploy new versions of the Lambda function from source
  code to production within minutes.

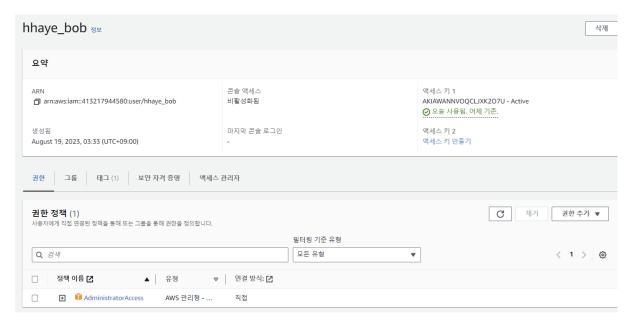
# 4. Scenario Objectives

Search for customer-submitted sensitive data. Simulated user activities occur within the
account. Executed every minute, the simulation of customer requests to the API is
accomplished through the CodeBuild project.

## 5. **Summary**

• Elevate permissions by overriding the tags on the EC2 instance used for attribute-based

access control. Steal SSH keys from the instance and use them to clone the CodeCommit repository. Examine commit history and identify new sets of AWS credentials. Utilize these to backdoor applications and exfiltrate critical data.



Creating an IAM User with Administrator privileges



- Creating an EC2 for getting id (for cicd scenario) at perior IAM User account

- Creating profile for cicd scenario and registering the access key and secret key of IAM user named 'hhaye\_bob'

```
haye@hhaye-ubuntu:~$ aws ec2 describe-instances --region ap-northeast-2 --profile cicd
    "Reservations": [
                 "Groups": [],
"Instances": [
                              "AmiLaunchIndex": 0,
                              "ImageId": "ami-0c9c942bd7bf113a2",
"InstanceId": "i-04bec6c97abb2dd22",
                              "InstanceType": "t2.micro",
"KeyName": "Public_web",
"LaunchTime": "2023-08-11T02:04:03+00:00",
                              "Monitoring": {
    "State": "disabled"
                              },
"Placement": {
    "AvailabilityZone": "ap-northeast-2a",
    "AvailabilityZone": ""
                                     "GroupName": "",
"Tenancy": "default"
                              },
"PrivateDnsName": "ip-10-0-9-24.ap-northeast-2.compute.internal",
"PrivateIpAddress": "10.0.9.24",
                              "ProductCodes": [],
"PublicDnsName": "ec2-13-209-84-161.ap-northeast-2.compute.amazonaws.com",
"PublicIpAddress": "13.209.84.161",
                              "State": {
    "Code": 16,
    "Name": "running"
                              },
"StateTransitionReason": "",
                              "SubnetId": "subnet-003a13314fb646e91",
"VpcId": "vpc-036f230416ef585b6",
"Architecture": "x86_64",
                              "BlockDeviceMappings": [
                                           "DeviceName": "/dev/sda1",
                                           "Ebs": {
```

Checking profile cicd

```
hhaye@hhaye-ubuntu:-$ aws ec2 create-tags --resources i-00a08183910abb0a9 --tags Key=Environment,Value=sandbox

An error occurred (InvalidInstanceID.NotFound) when calling the CreateTags operation: The instance ID 'i-00a08183910abb0a9' does not exist
```

- But I faced repeatable connection error between cicd account and my ec2 although both are created in the same IAM account

```
tam_privesc_oy_attachment
hhaye@hhaye-ubuntu:-/cloudgoat$. /cloudgoat.py create cicd
/usr/lib/python3/dist-packages/requests/_init__.py:87: RequestsDependencyWarning: urllib3 (2.0.4) or chardet (4.0.0) doesn't match a supported version!
warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Using default profile "cicd" from config.yml...
```

- I double double double checked '~create cicd' to get 'start.txt'

- But this is the big problem all the team members are continuing facing

```
hhaye@hhaye-ubuntu:~/cloudgoat$ ls
cicd_cgidx0bum2ayro config.yml Dockerfile LICENSE requirements.txt whitelist.txt
cloudgoat.py core docker_stack.yml README.md scenarios
hhaye@hhaye-ubuntu:~/cloudgoat$ cicd_cgidx0bum2ayro
cicd_cgidx0bum2ayro: command not found
hhaye@hhaye-ubuntu:~/cloudgoat$ cd cicd_cgidx0bum2ayro
hhaye@hhaye-ubuntu:~/cloudgoat/cicd_cgidx0bum2ayro$ ls
assets cheat_sheet.md manifest.yml README.md start.sh terraform
hhaye@hhaye-ubuntu:~/cloudgoat/cicd_cgidx0bum2ayro$ cat start.sh
#!/bin/bashhhaye@hhaye-ubuntu:~/cloudgoat/cicd_cgidx0bum2ayro$
```

- There is 'start.sh' instead of 'start.txt', so I used 'cat' command but that is just /bin/bash
- Q1. Do we have to use our own aws access/secret key or cloudgoat aws access/secret key made for just scenario?
- Q2. Is it ok to change scenario before 24 when the presentation is planned?

Thanks a lot and really sorry to make our assignment unfinished.