

# AWS Credential Exposure Incident Response Architecture

- **Subtitle:** Event-driven detection and incident response system for exposed AWS credentials and suspicious API activities
- **Tech Stack:** AWS CloudTrail · EventBridge · Lambda · IAM · Discord Webhook · GitHub
- **Name:** SeokHyun Yoo
- **Role:** Cloud Security / Incident Response
- **Keywords:** Cloud IR · Credential Security · Threat Detection · Event-driven Security Monitoring

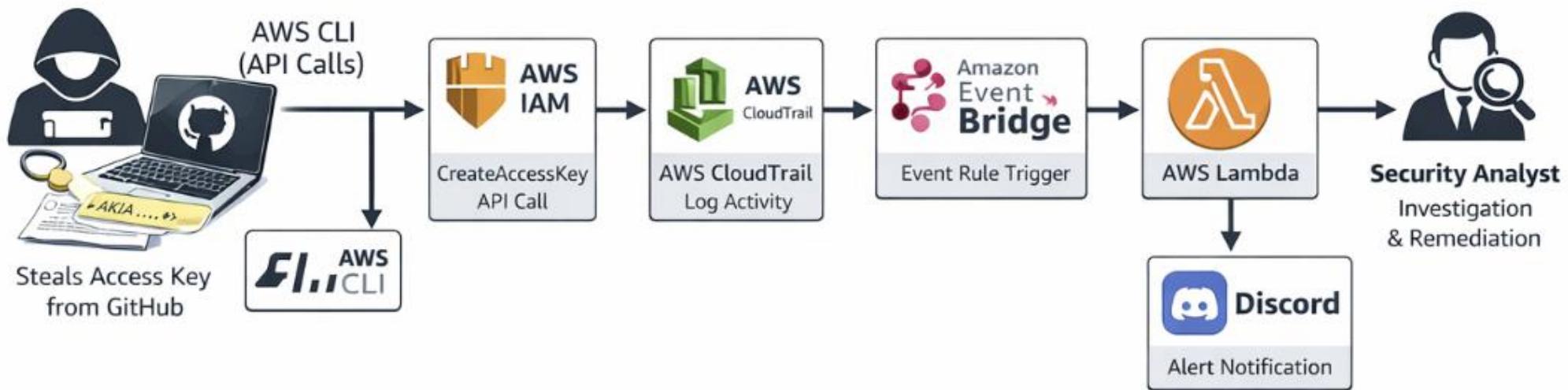
# Problem Definition

Exposed AWS access keys (AKIA) are a frequent cause of real cloud breaches. Leaked credentials can be abused for unauthorized API usage and resource creation.

## Operational Gaps

- Credential leaks often go unnoticed
- Suspicious API activity is detected too late
- Off-hours delays incident response

# Architecture



# Event pipeline setting 1

## Lambda setting

Lambda > Functions > detect-createaccesskey

Successfully updated the function detect-createaccesskey.

Code Test Monitor Configuration Aliases Versions

Code source Info

detect-createaccesskey

lambda\_function.py X

lambda\_function.py

```
1 import json
2 import os
3 import urllib.request
4 import urllib.error
5 from datetime import datetime, timezone
6
7 def _get(d, path, default="N/A"):
8     """Safely get nested dict values. path example: ('d', 'a', 'b')
9     cur = d
10    for p in path:
11        if isinstance(cur, dict) and p in cur:
```

EXPLORER DETECT-CREATEACCESSKEY lambda\_function.py

DEPLOY Current Deploy (F5U)

Test (F5I)

PROBLEMS OUTPUT CODE REFERENCE LOG TERMINAL

## Event bridge setting

### detect-create-accesskey

Rule details [Info](#)

Rule name detect-create-accesskey

Status Enabled

Description Detect IAM CreateAccessKey API usage

Rule ARN arn:aws:events:ap-northeast-2:252321108840:rule/detect-create-accesskey

Event pattern Targets Monitoring Tags

#### Event pattern [Info](#)

```
1 {
2     "source": ["aws.iam"],
3     "detail-type": ["AWS API Call via CloudTrail"],
4     "detail": {
5         "eventSource": ["iam.amazonaws.com"],
6         "eventName": ["CreateAccessKey"]
7     }
}
```

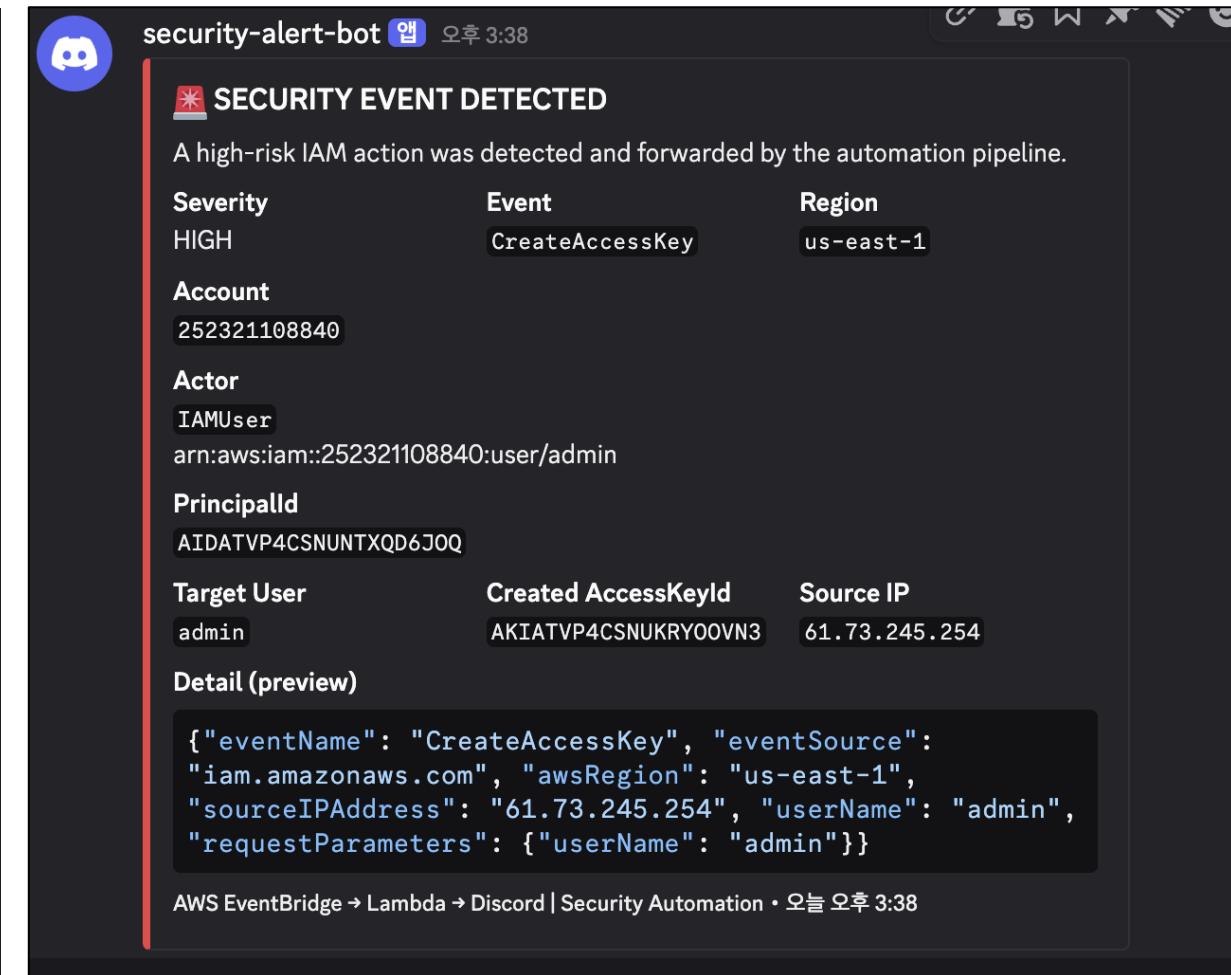
# Event pipeline setting 2

## Attacker Establishing Persistence via Access Key Creation

```
        "CreateDate": "2020-02-05T00:09:52+00:00"
    }
}

[yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG % aws configure
AWS Access Key ID [*****B45D]: [REDACTED]
AWS Secret Access Key [*****/r]: [REDACTED]
Default region name [ap-northeast-2]:
Default output format [json]:
[yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG % aws sts get-caller-identity
{
    "UserId": "AIDATVP4CSNUNTXQD6J0Q",
    "Account": "252321108840",
    "Arn": "arn:aws:iam::252321108840:user/admin"
}
[yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG % aws iam create-access-key --user-name admin
{
    "AccessKey": {
        "UserName": "admin",
        "AccessKeyId": [REDACTED],
        "Status": "Active",
        "SecretAccessKey": [REDACTED],
        "CreateDate": "2026-02-05T06:12:33+00:00"
    }
}
[yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG %
```

## Send alert info to discord



# Event pipeline setting 3

## Running instances by hacker

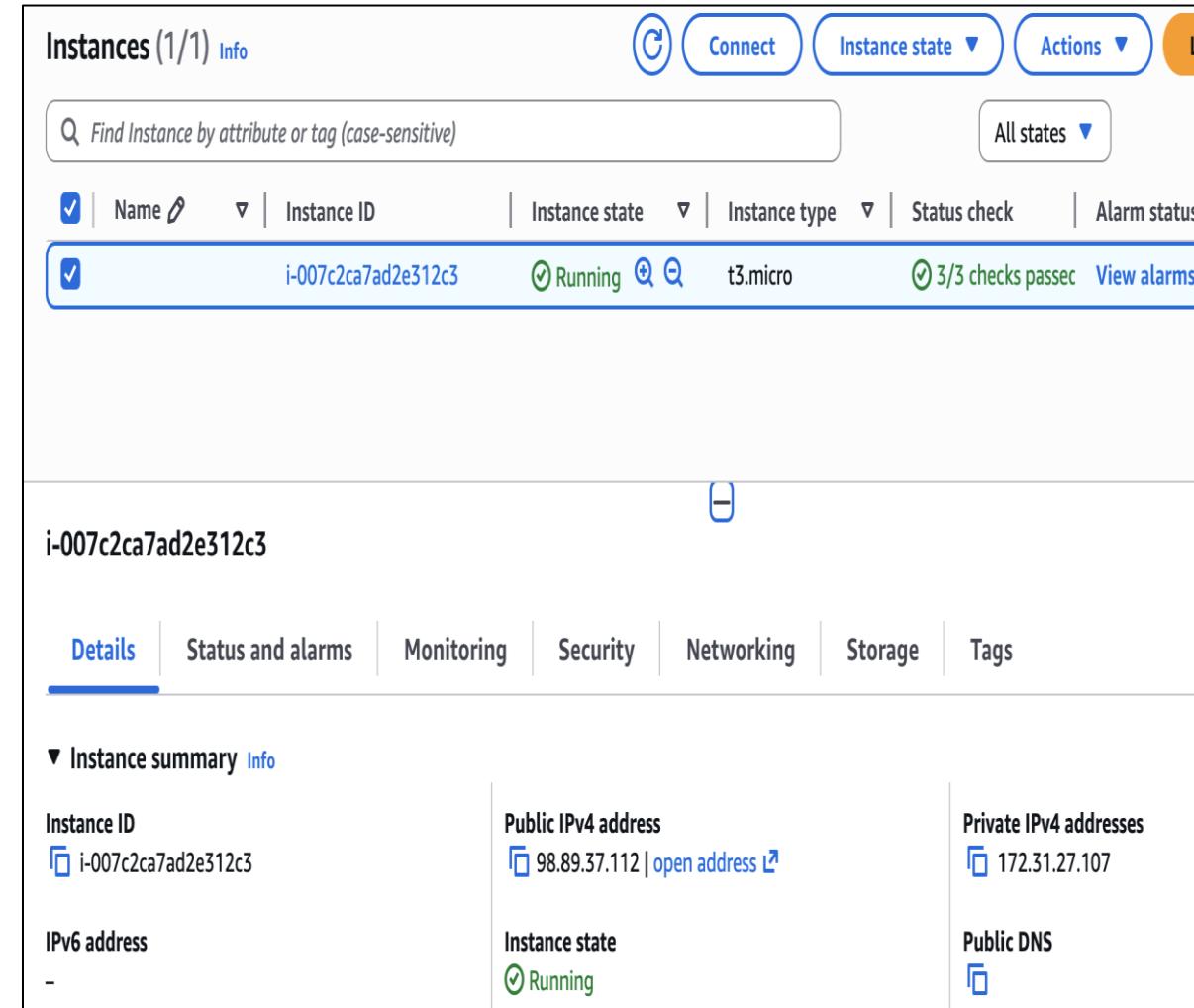
```
yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG % aws ec2 run-instances \
--image-id ami-0c02fb55956c7d316 \
--instance-type t2.micro \
--region us-east-1

An error occurred (InvalidParameterCombination) when calling the RunInstances operation: The specific instance type is not eligible for Free Tier. For a list of Free Tier instance types, run 'describe-instance-types' with --filter='{Status=Eligible}'.

yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG % aws ec2 run-instances \
--image-id ami-0c02fb55956c7d316 \
--instance-type t3.micro \
--region us-east-1

{
    "ReservationId": "r-0726da3117de0a328",
    "OwnerId": "252321108840",
    "Groups": [],
    "Instances": [
        {
            "Architecture": "x86_64",
            "BlockDeviceMappings": [],
            "ClientToken": "45544068-f322-46e3-9a54-94637431f3c7",
            "EbsOptimized": false,
            "EnaSupport": true,
            "Hypervisor": "xen",
            "NetworkInterfaces": [
                {
                    "Attachment": {
                        "AttachTime": "2026-02-05T06:44:40+00:00",
                        "AttachmentId": "eni-attach-006ca9e0ee9e93dba",
                        "DeleteOnTermination": true,
                        "DeviceIndex": 0,
```

## Running instance



# Response Strategy

- Automated detection and alerting
- 
- Analyst-led investigation
- Manual remediation based on context
- Minimizes operational risk