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

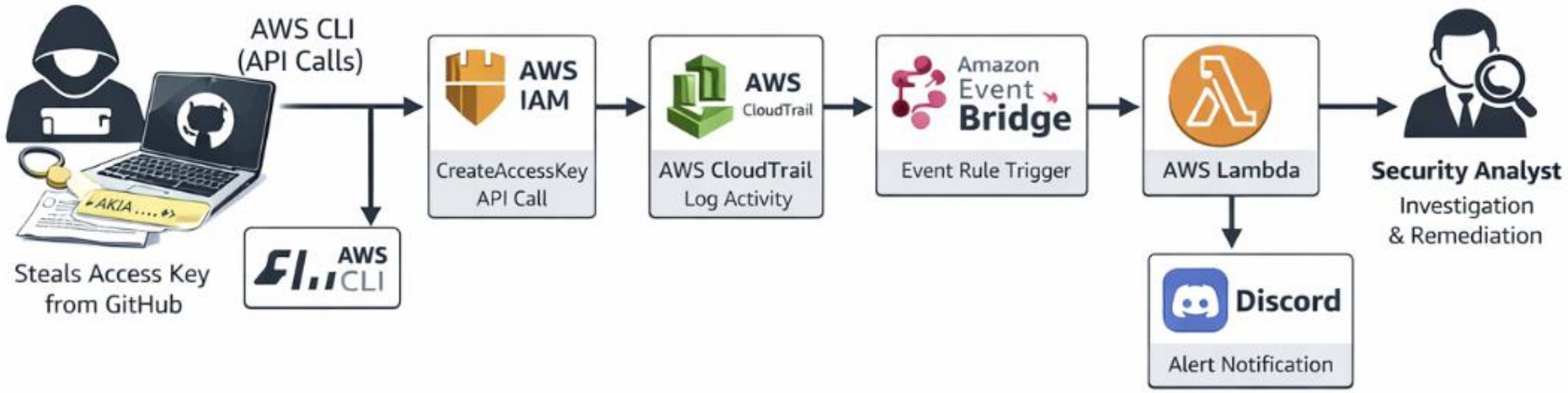
Exposed AWS access keys (AKIA) are a frequent cause of real cloud breaches.

Leaked credentials can be abused for unauthorized API usage and resource creation.

Operational Gaps

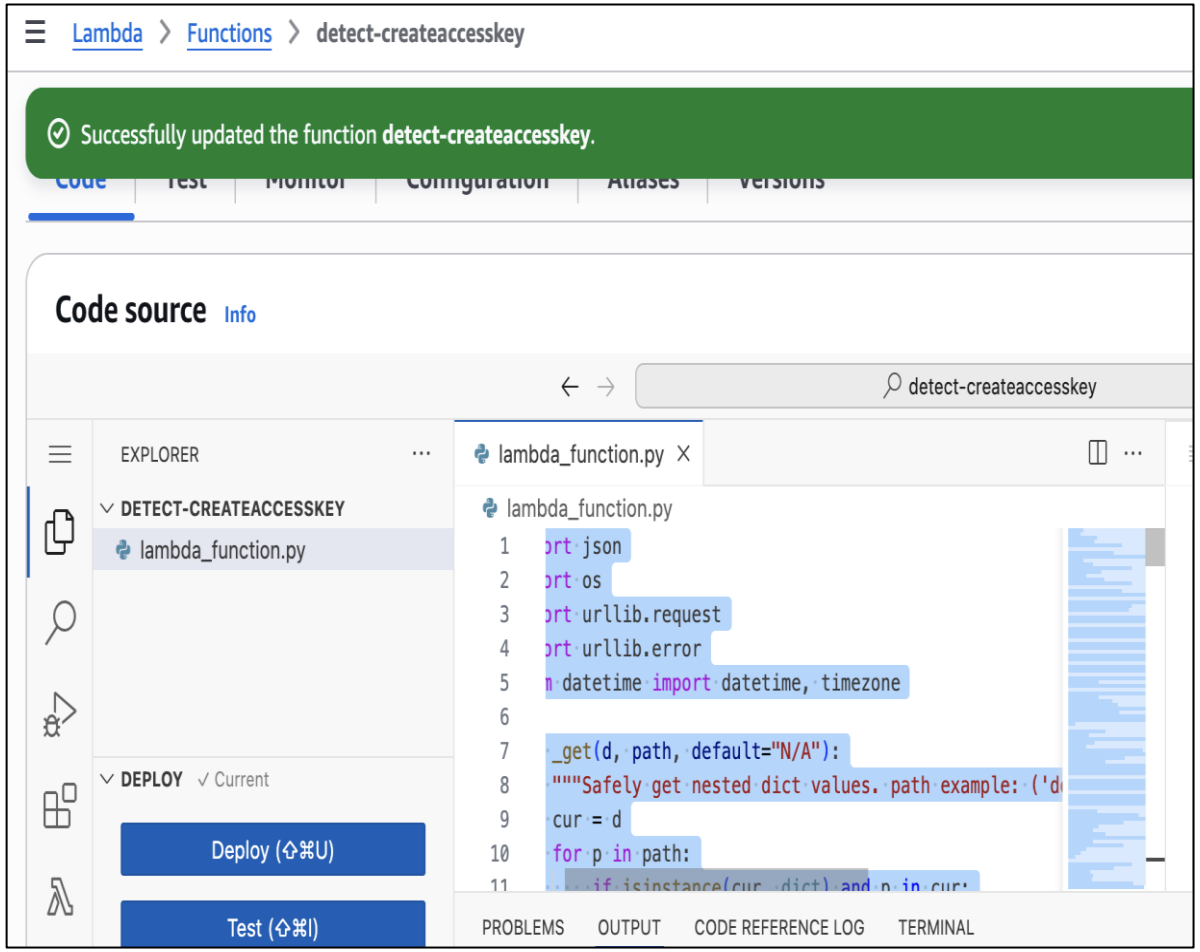
- Credential leaks often go unnoticed
- Suspicious API activity is detected too late
- Off-hours delays incident response

Architecture

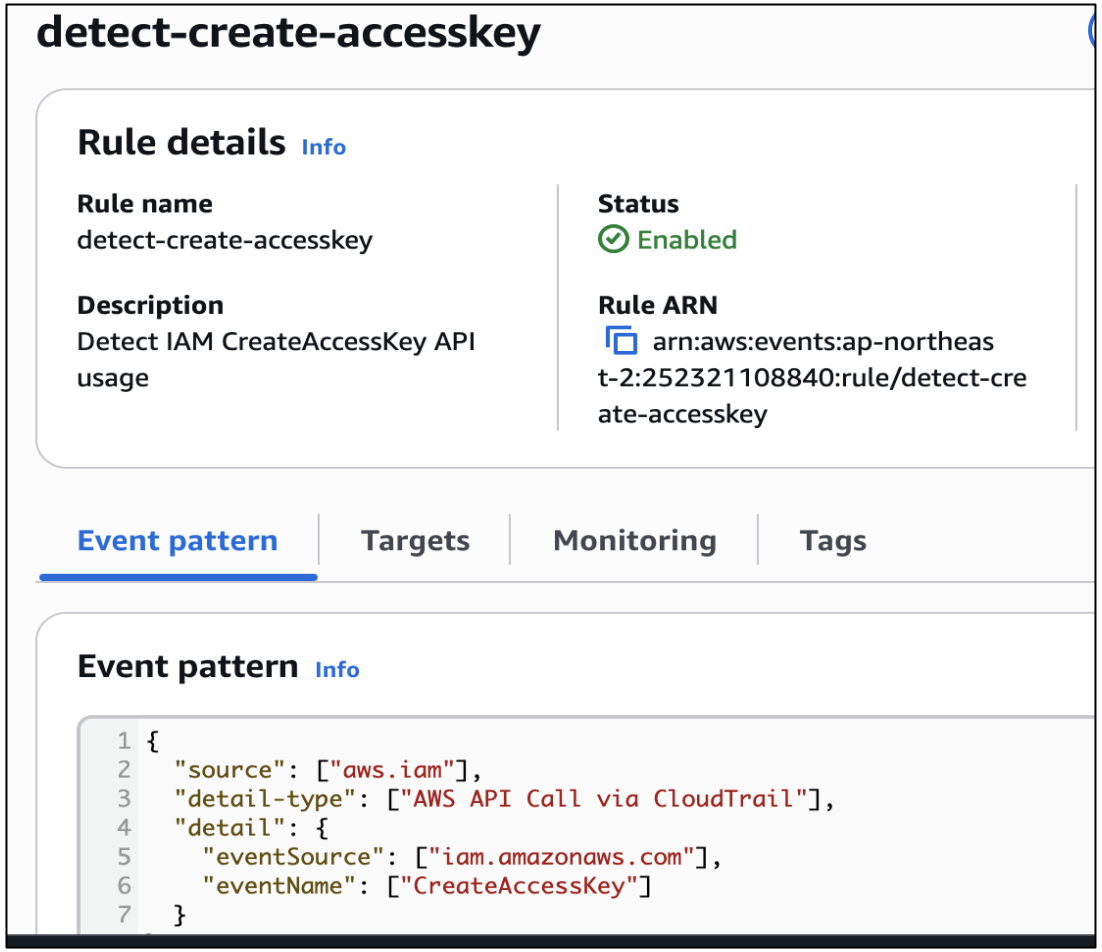


Event pipeline setting 1

Lambda setting



Event bridge setting

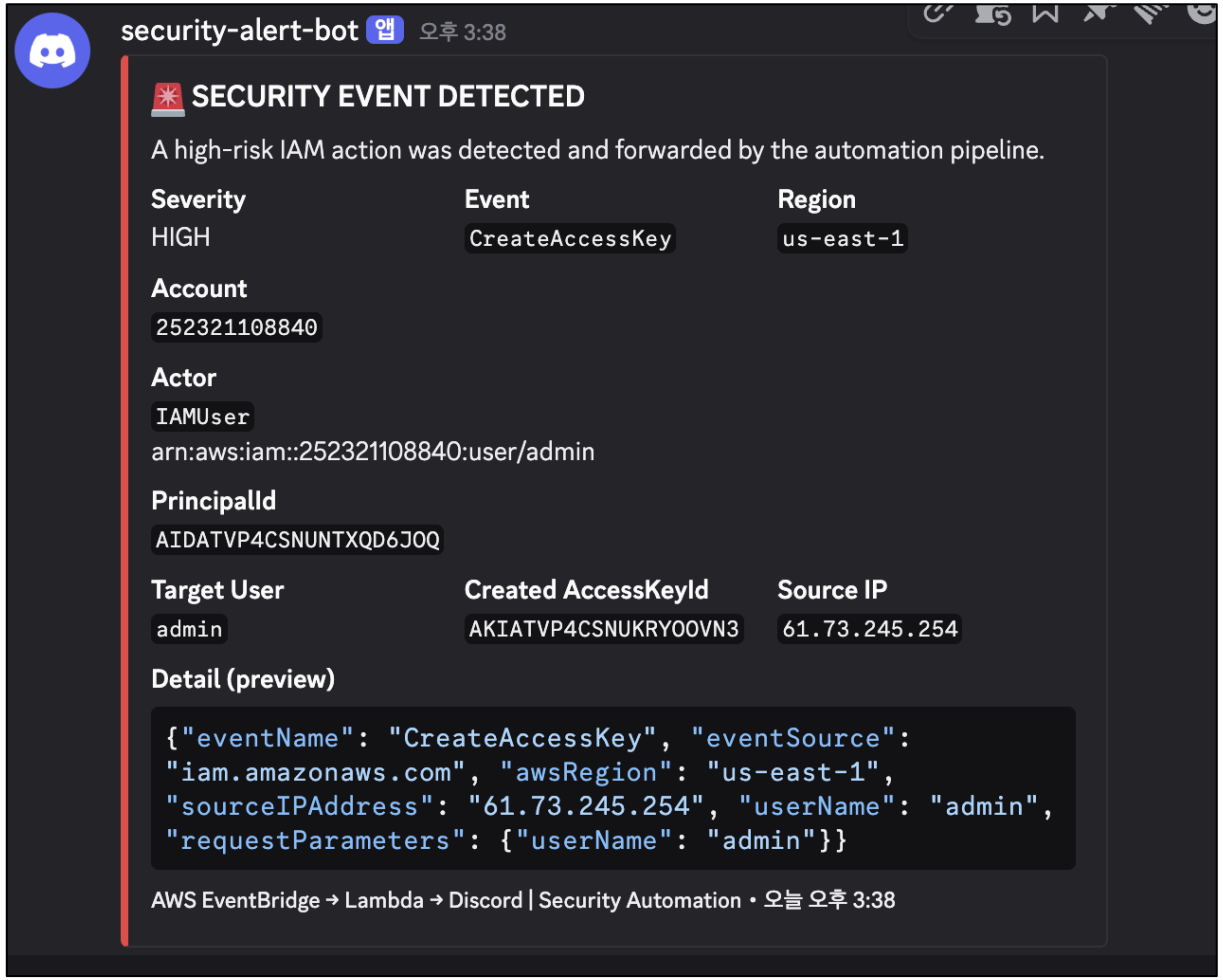


Event pipeline setting 2

Attacker Establishing Persistence via Access Key Creation

```
    }
}
yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG % aws configure
AWS Access Key ID [****************B45D]:
AWS Secret Access Key [****************/r
Default region name [ap-northeast-2]:
Default output format [json]:
yuseoghyeon@yuseoghyeon-ui-MacBookAir public-exposure-SG % aws sts get-caller-identity
{
    "UserId": "AIDATVP4CSNUNTXQD6JOQ",
    "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":
        "Status": "Active",
        "SecretAccessKey":
        "CreateDate": "2026-02-05T06:12:33+00:00"
    }
}
```

Send alert info to discord



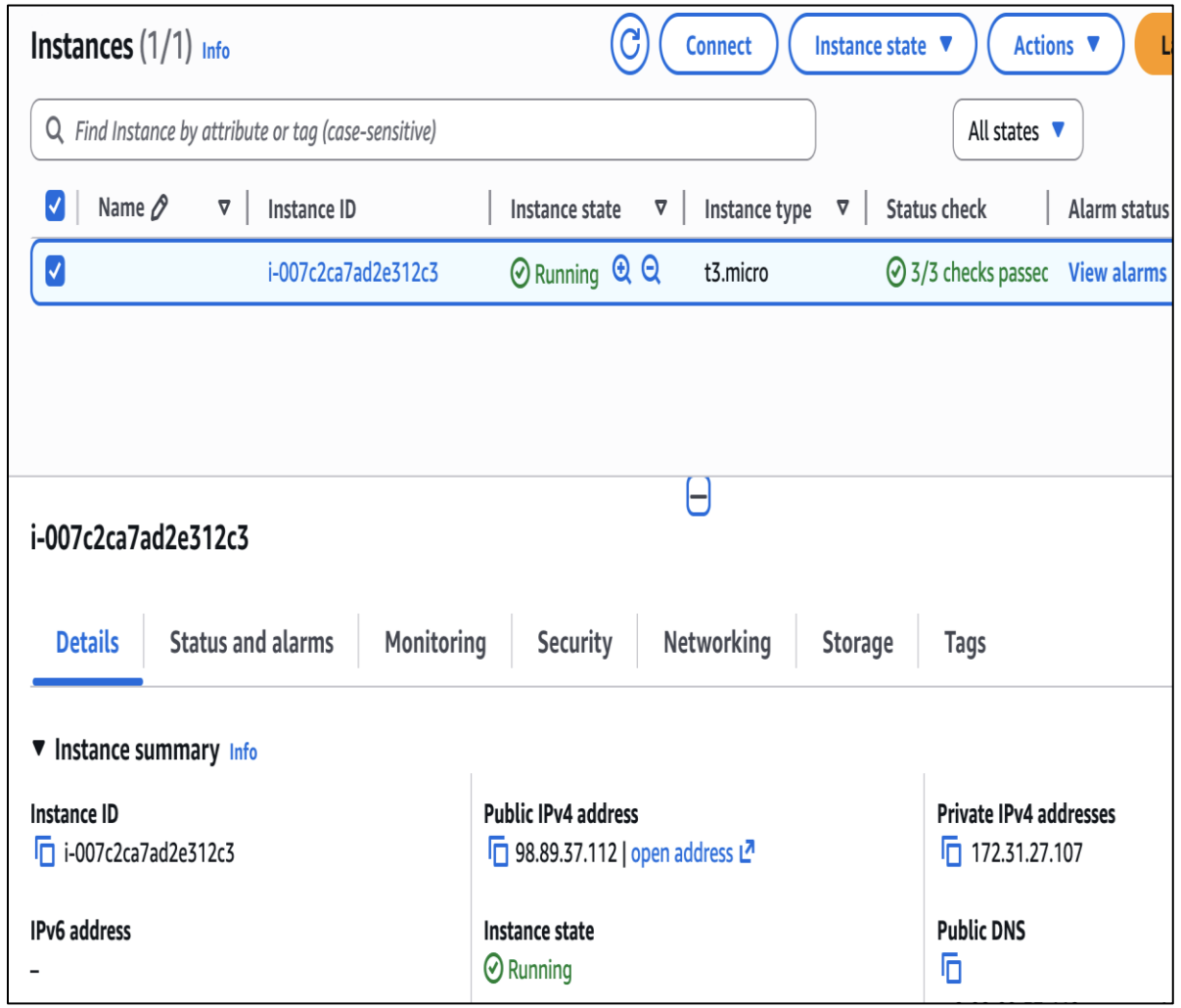
Event pipeline setting 3

Runninginstances 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 specif
t eligible for Free Tier. For a list of Free Tier instance types, run 'describe-instance-types' wit
-eligible=true'.
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