
# When a Zero Day and Access Keys Collide in the Cloud

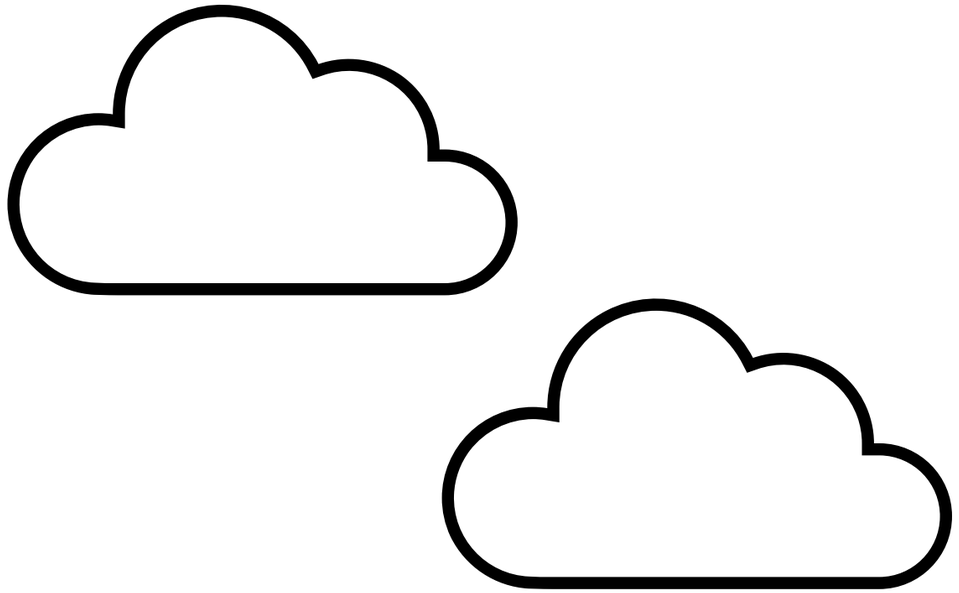
## Responding to the SugarCRM 0-Day Vulnerability

Speaker: Margaret Zimmermann


**Margaret Zimmermann**
Cloud Incident Responder
Palo Alto Networks Unit 42

# Agenda

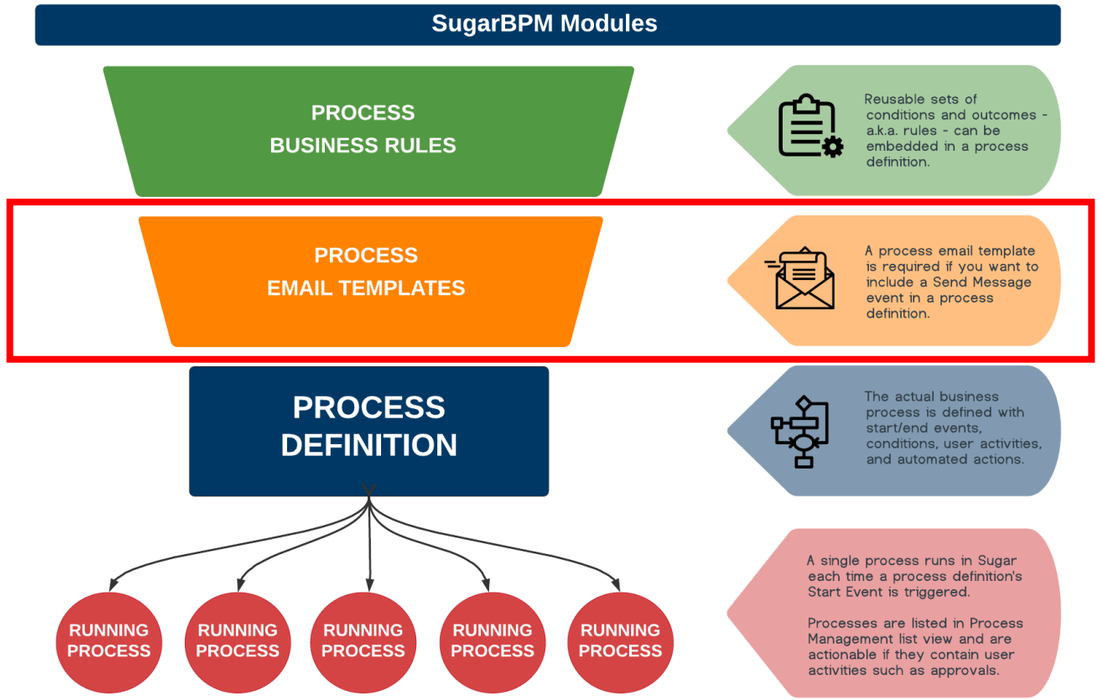
- MITRE ATT&CK Matrix
- CVE-2023-22952
- Case walk through
- Remediation



# MITRE ATT&CK Matrix

| | | |
|---|---|---|
| Initial Access | Credential Access | Discovery |
| Lateral Movement | Execution | Exfiltration |
| Privilege Escalation | Persistence | Defense Evasion |

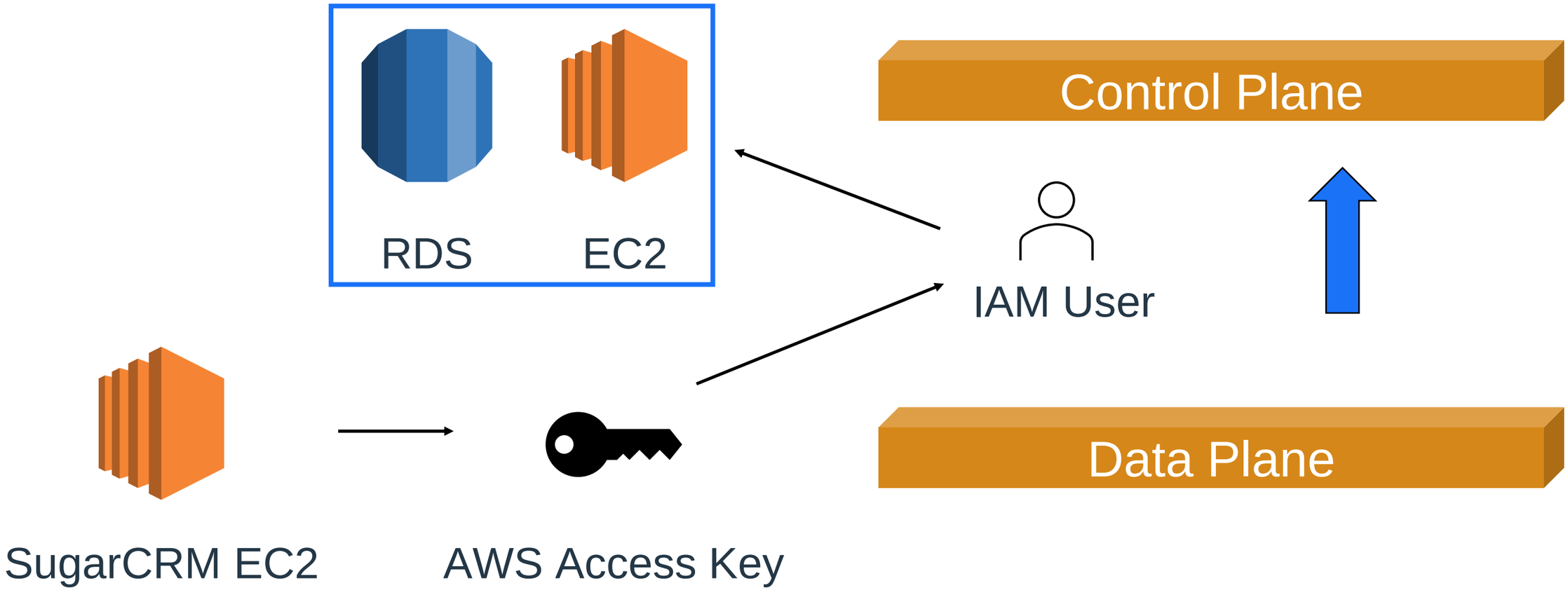
# Initial Access - CVE-2023-22952




sugarcrm

NIST NATIONAL VULNERABILITY DATABASE NVD

# Data vs. Control Plane



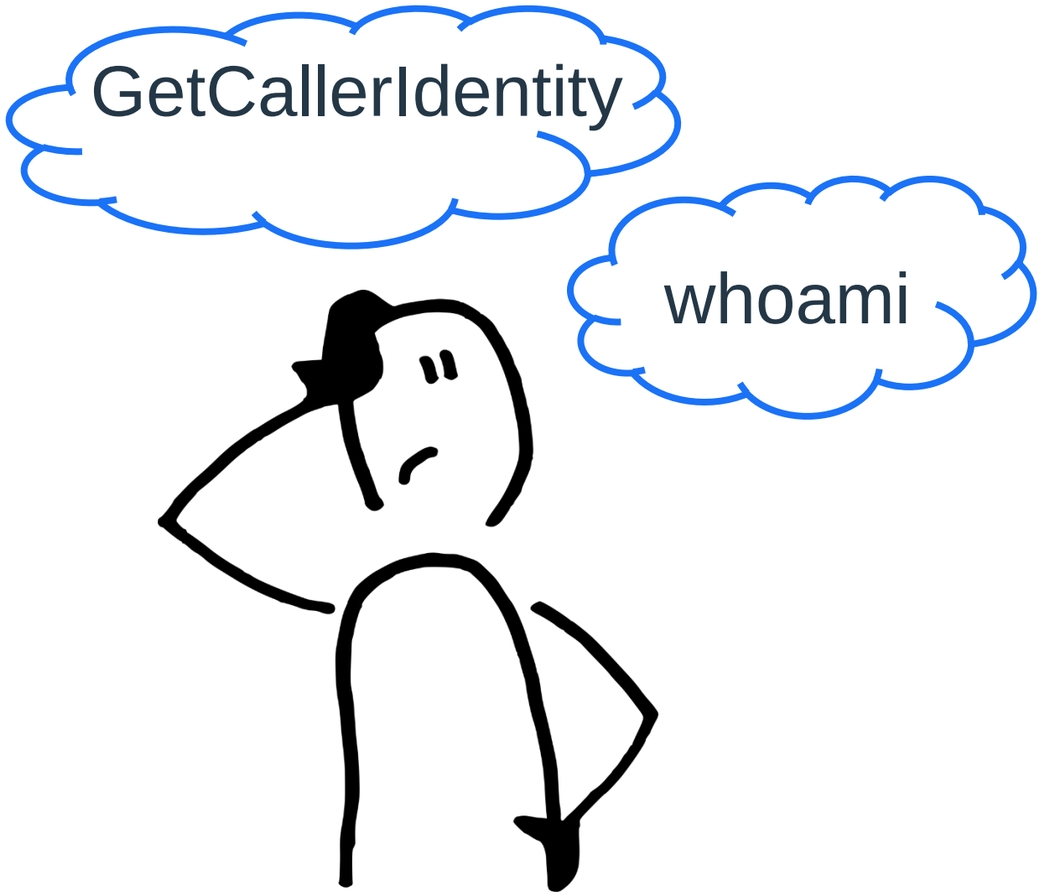
# Credential Access – Access Keys

```
[profile_name]
aws_access_key_id     = AKIABBBCCCDDDEEEFFGG
aws_secret_access_key = AAAbbbCCCddEE/fffGGGhhhIIIjjjKKKlllMMMM/
```

| Prefix | Resource type |
|---|---|
| ABIA | AWS STS service bearer token |
| ACCA | Context-specific credential |
| AGPA | User group |
| AIDA | IAM user |
| AIPA | Amazon EC2 instance profile |
| AKIA | Access key |
| ANPA | Managed policy |

%UserProfile%\.aws\credentials
$HOME/.aws/credentials

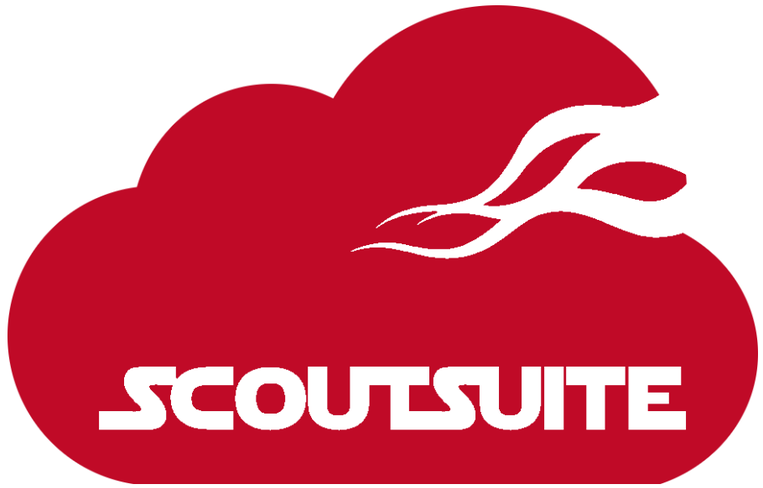
# Discovery - GetCallerIdentity




```
{
    "UserId": "AIDAKSJEN4KSEJ9S822BETCW",
    "Account": "123456789123",
    "Arn": "arn:aws:iam::123456789123:user/User"
}
```

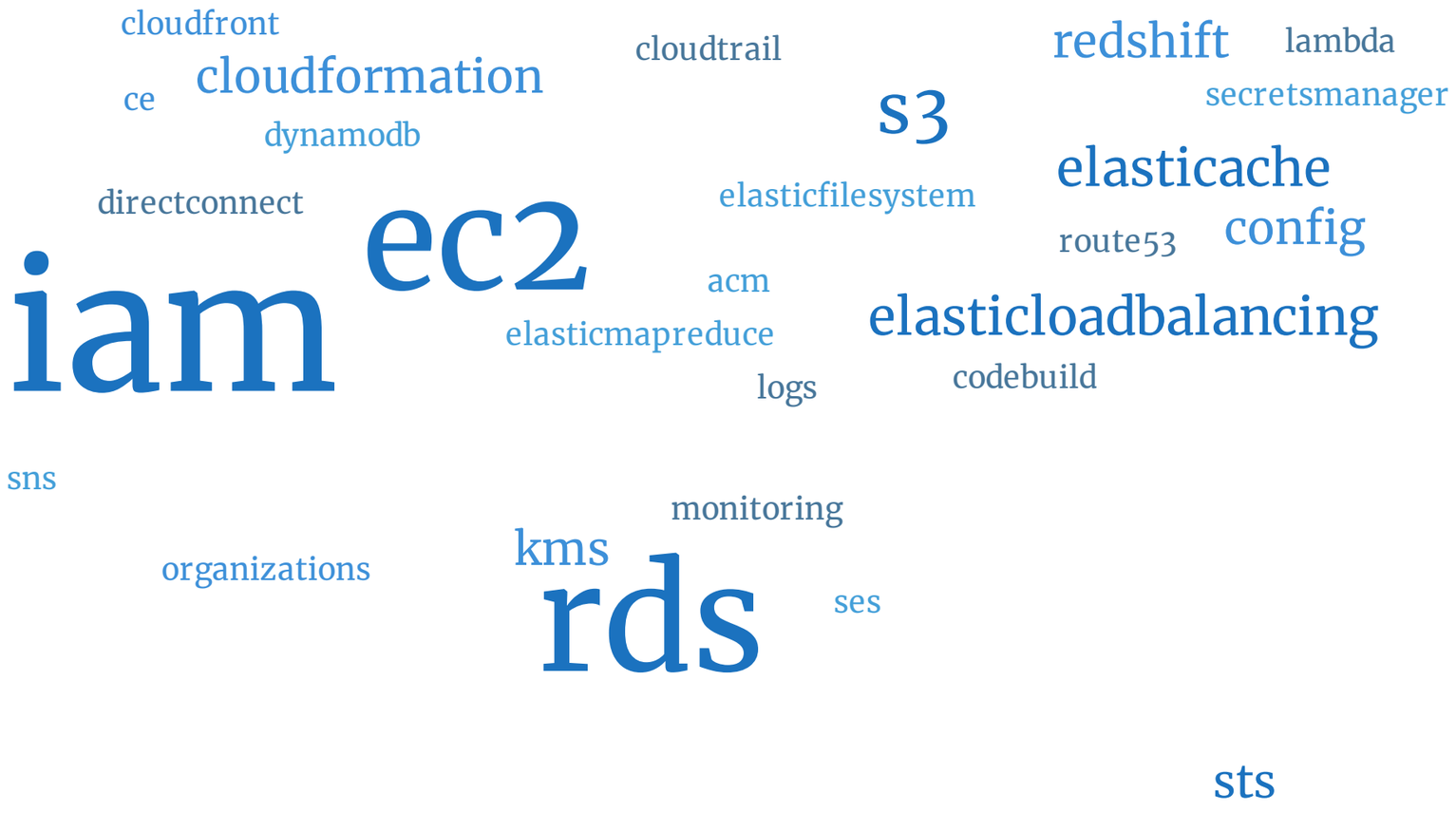
# Discovery - Tools

Pacu



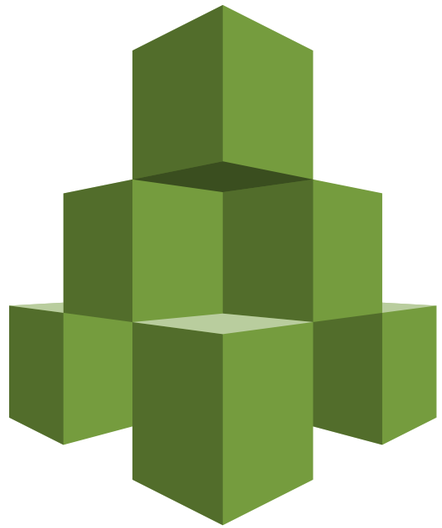

Scout Suite

# Discovery


cloudfront
cloudformation
ce
dynamodb
cloudtrail
redshift
lambda
secretsmanager
s3
elasticache
directconnect
elasticfilesystem
ec2
route53
config
iam
acm
elasticloadbalancing
elasticmapreduce
logs
codebuild
sns
monitoring
kms
organizations
rds
ses
sts

# Discovery - Organizations

- **ListOrganizationalUnitsForParent**
  - List all Organizational Units (OUs)
- **ListAccounts**
  - List all account IDs for OU
- **DescribeOrganization**
  - Account ID and root email



# Discovery - GetCostandUsage

```
"requestParameters": {
    "TimePeriod": {
        "Start": "2023-01-01",
        "End": "2023-01-31"
    },
    "Granularity": "MONTHLY",
    "Metrics": [
        "BlendedCost",
        "UnblendedCost",
        "UsageQuantity"
    ]
}
```


```
{
    "ResultsByTime": [
        {
            "TimePeriod": {
                "Start": "2023-01-01",
                "End": "2023-01-31"
            },
            "Total": {
                "BlendedCost": {
                    "Amount": "457.6210903636",
                    "Unit": "USD"
                },
                "UsageQuantity": {
                    "Amount": "53214.9810448132",
                    "Unit": "N/A"
                },
                "UnblendedCost": {
                    "Amount": "457.6210903636",
                    "Unit": "USD"
                }
            },
            "Groups": [],
            "Estimated": false
        }
    ],
    "DimensionValueAttributes": []
}
```

# Discovery - RDS

listtagsforresource

describedbclustersnapshots

describedbclustersnapshotattributes

describedbinstances

describedbsubnetgroups

describedbparameters

describedbsecuritygroups

describedbsnapshots

describedbparametergroups

# Lateral Movement – Execution - Exfiltration

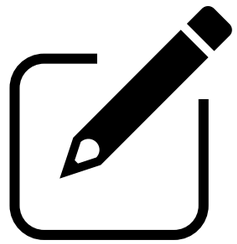
SugarCRM EC2

CreateDBSnapshot

RestoreDBInstance FromDBSnapshot

SugarCRM RDS DB


AuthorizeSecurity GroupIngress



ModifyDBInstance

# Discovery - EC2

describevolumes

describevpcpeeringconnections

describeimages

describeregions

describesnapshotattribute

describenetworkacls

describesubnets

describevpcs

describenetworkinterfaces

describesecuritygroups

describeflowlogs

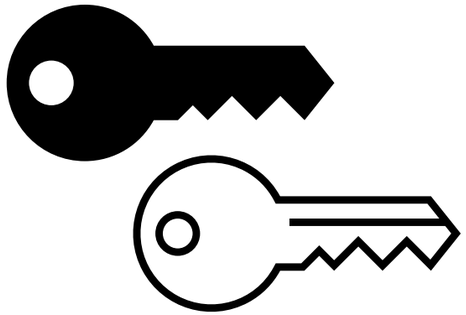
describeinstances

describeinstanceattribute

describesnapshots

# Lateral Movement/Execution

CreateImage

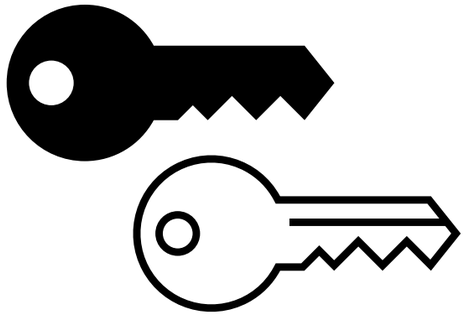


ImportKeyPair

RunInstances

# Lateral Movement/Execution - New Region

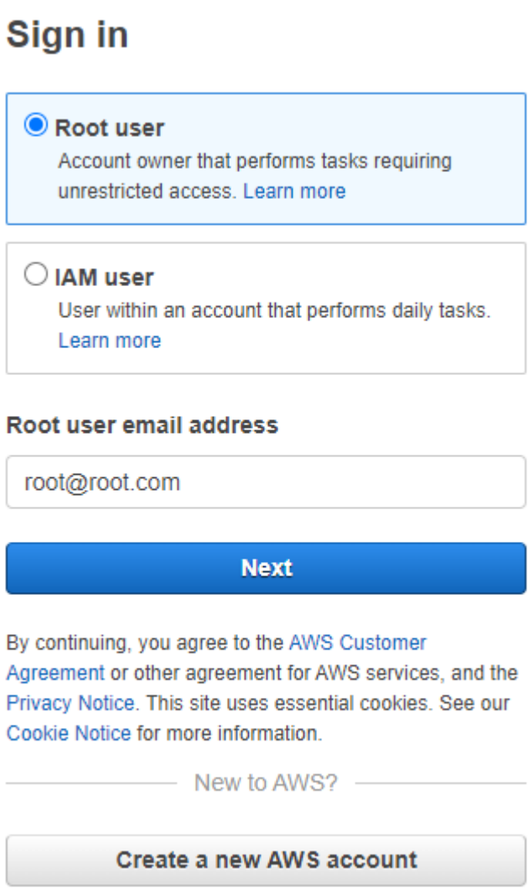

CreateSecurityGroup



ImportKeyPair

RunInstances

# Privilege Escalation - Root





```
"eventVersion": "1.08",
"userIdentity": {
    "type": "Root",
    "principalId": "123456789123",
    "arn": "arn:aws:iam::123456789123:root",
    "accountId": "123456789123",
    "accessKeyId": ""
},
"eventTime": "2023-01-11T00:00:00Z",
"eventSource": "signin.amazonaws.com",
"eventName": "ConsoleLogin",
"awsRegion": "us-east-1",
"sourceIPAddress": "12.34.56.78",
"userAgent": "User Agent String",
"errorMessage": "Failed authentication",
"requestParameters": null,
"responseElements": {
    "ConsoleLogin": "Failure"
},
```

# Persistence - Regions

# Defense Evasion

# Defense Evasion

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running | Clear filters

| Instance state |
| --- |
| pending |
| running |
| stopping |
| stopped |
| shutting-down |
| terminated |

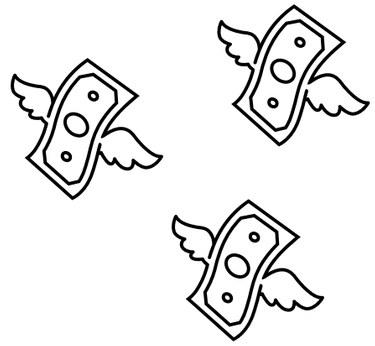
# Defense Evasion

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running | Clear filters

| Instance state |
| --- |
| pending |
| running |
| stopping |
| stopped |
| shutting-down |
| terminated |



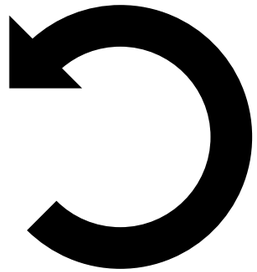
# Case Wrap-up

- Initial access through CVE-2023-22952
- Access key compromise
- Organizations and Cost and Usage Discovery
- RDS
- EC2
- Root login attempts
- Attack timeline
  - Broader activity: 21 – 27 days
  - AWS activity: 2 – 4 days

# Remediation

- Access keys
- IAM policies
- Monitor root account
- Enable logging and monitoring
  - CloudTrail, GuardDuty, VPC Flow Logs

# Remediation – Access Keys



```
[profile_name]
aws_access_key_id     = AKIABBBCCCDDDEEEFFGG
aws_secret_access_key = AAAbbbCCCddEE/fffGGGhhhIIIjjjKKKlllMMMM/
```

# Remediation – IAM Policies

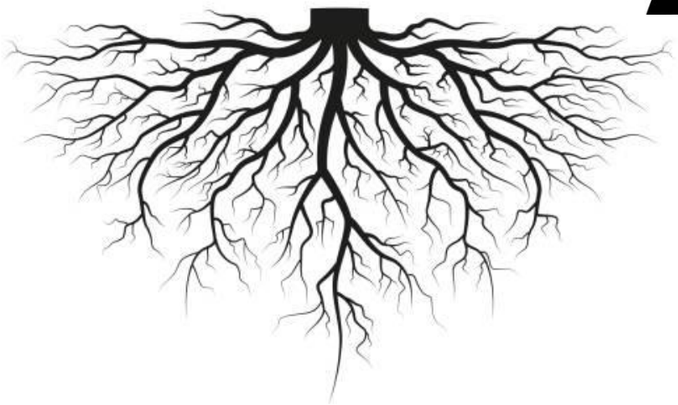
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:*",
                "s3:*",
                "iam:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstanceAttribute",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789123:instance/i-93j383j38dkd93j6",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:ListBuckets",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::bucketname",
            "Effect": "Allow"
        }
    ]
}
```

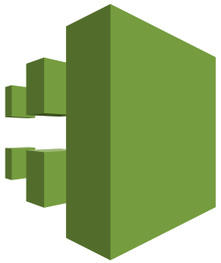
# Remediation – Monitoring Root

CloudWatch Metric

{ $.userIdentity.type = "Root“ &&
$.userIdentity.invokedBy NOT EXISTS &&
$.eventType != "AwsServiceEvent" }



# Remediation – Logging and Monitoring



CloudTrail

GuardDuty

VPC Flow Logs

# Key Takeaways

- Cleanup and monitor access keys
- Monitor AWS accounts for abnormal activity
- Enforce granular permissions


# Thank You