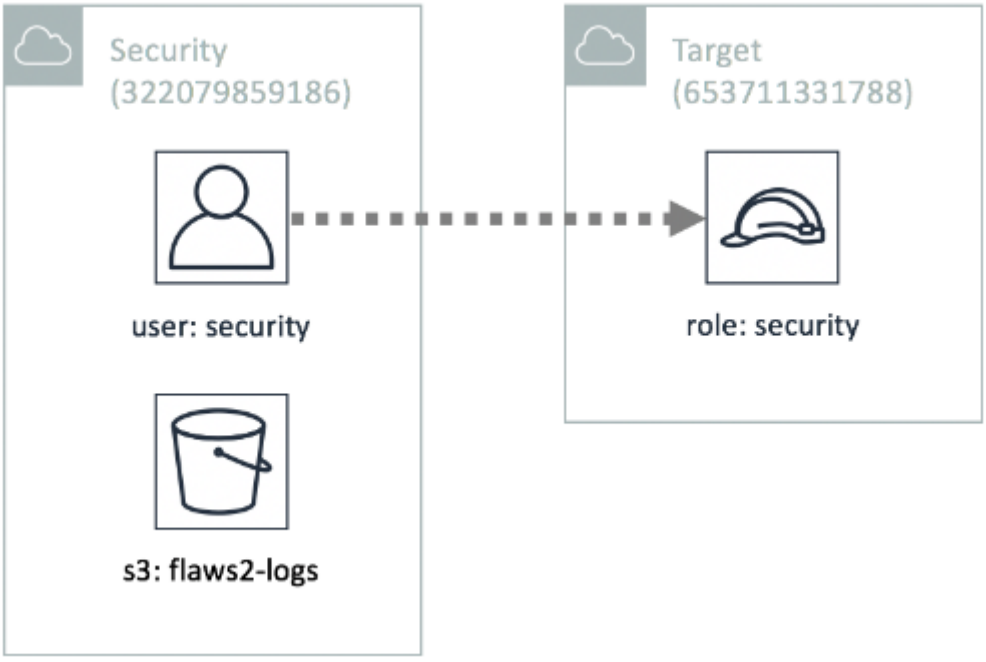
AWS incident response

In this project, we acted as incident responders within an AWS account named "Security." As IAM users, we accessed the logs during a specified incident timeframe. Our primary objective was to utilize the ability to assume the "Security" role in the target account to investigate and identify misconfigurations that facilitated the attack. We queried JSON logs using tools like JQ. Below is the environment we utilized



The provided credentials

Credentials

Your IAM credentials to the Security account:

- Login: https://flaws2-security.signin.aws.amazon.com/console
- Account ID: 322079859186
- Username: security
- Password: password
- Access Key: AKIAIUFNQ2WCOPTEITJQ
- Secret Key: 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

- Configure a profile using the access key and secret key

```
└─$ aws configure --profile havoc
AWS Access Key ID [****************ITJQ]: AKIAIUFNQ2WCOPTEITJQ
AWS Secret Access Key [****************0ddF]: paVI8VgTWkPI3jDNkdzUMvK4CcdXO2T7se
PX0ddF
Default region name [None]:
Default output format [None]:
```

- Confirm "security" IAM user as

```
└─$ aws --profile havoc sts get-caller-identity
{
    "UserId": "AIDAJXZBU42TNFRNGBBFI",
    "Account": "322079859186",
    "Arn": "arn:aws:iam::322079859186:user/security"
}
```

- Check for the bucket creation date using s3api

```
└─$ aws --profile havoc s3api list-buckets
{
    "Buckets": [
        {
            "Name": "flaws2-logs",
            "CreationDate": "2018-11-19T20:54:31+00:00"
        }
    ],
    "Owner": {
        "DisplayName": "scott+flaws2_security",
        "ID": "0ff467deaf461e549934997a2df02d29c8010173b1464262782d522bce63bf46"
    }
}
```

- Dump bucket data

```
┌──(salsabil㉿kali)-[~]
└─$ aws --profile havoc s3 sync s3://flaws2-logs ~/Desktop/
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653
711331788_CloudTrail_us-east-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json.gz to Desktop/A
WSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east
-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653
711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json.gz to Desktop/A
WSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east
-1_20181128T2305Z_zKlMhON7EpHala9u.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653
711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json.gz to Desktop/A
WSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east
-1_20181128T2235Z_cR9ra7OH1rytWyXY.json.gz
```

- Go to log files

```
┌──(salsabil㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ ls
653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json.gz
653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json.gz
653711331788_CloudTrail_us-east-1_20181128T2310Z_jQajCuiobojD8I4y.json.gz
653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json.gz
653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json.gz
653711331788_CloudTrail_us-east-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json.gz
653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json.gz
653711331788_CloudTrail_us-east-1_20181128T2310Z_jJW5HfNtz7kOnvcP.json.gz
```

- Unzip the .json file with gunzip
- cat the files

```
┌──(salsabil㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ cat 653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json

{"Records":[{"eventVersion":"1.05","userIdentity":{"type":"AWSService","invokedBy":"ecs-tasks.amazonaws.com"}
,"eventTime":"2018-11-28T22:31:59Z","eventSource":"sts.amazonaws.com","eventName":"AssumeRole","awsRegion":"u
s-east-1","sourceIPAddress":"ecs-tasks.amazonaws.com","userAgent":"ecs-tasks.amazonaws.com","requestParameter
s":{"roleSessionName":"d190d14a-2404-45d6-9113-4eda22d7f2c7","roleArn":"arn:aws:iam::653711331788:role/level3
"},"responseElements":{"credentials":{"sessionToken":"FQoGZXIvYXdzEFAaDEbnJXLefTT+kjlmKSKSBNgEUj8tJVL+szjaH5q
2npYc2FIPgrLmfkRjK9KqtSW7+lo4WxteBTd77aeAcmIip4GceNBbU86zxGgS1IdNBzEOLnDw6biAzijG0Du/Qazx136qjy+kahHxPlR36C4y
/0QrCUZpTFmP3uELsRIKkvhGvuBr6S10pTOZ+GjtUXN3iFV8Ea0KOo/fSP0d4LbZGwI957aJxs2I7N8ji/lKTfwPdq+sxXvSWnaOseinUxZUD
S0zdI69CKb6C+qwhR5YTifqyuOvC9OoSlfcBN2FyHpRZf5Bd+Z+mPYTldbAvD/HcdbQo7U4jqlR2WGuXoBfwvypt/Kb6HtPp4g9O0HlTCc7Sb
```

- read json format with jq for better view

```
┌──(salsabil㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ find . -type f -exec cat {} \; | jq '.'
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "AWSAccount",
        "principalId": "",
        "accountId": "ANONYMOUS_PRINCIPAL"
      },
      "eventTime": "2018-11-28T23:09:36Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "GetObject",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "104.102.221.250",
      "userAgent": "[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/53
7.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36]",
      "requestParameters": {
        "bucketName": "the-end-962b72bjahfm5b4wcktm8t9z4sapemjb.flaws2.cloud",
        "key": "index.htm"
      },
```

- We can filter by eventName

```
┌──(salsabil㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ find . -type f -exec cat {} \; | jq '.Records[]|.eventName'
"GetObject"
"GetObject"
"CreateLogStream"
"AssumeRole"
"CreateLogStream"
"CreateLogStream"
"ListImages"
"CreateLogStream"
"GetObject"
"GetObject"
"GetObject"
"GetObject"
"GetObject"
```

- we can include the time (The -cr prints the data in a row, and the |@tsv makes this tab separated)

```
┌──(salsabil㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ find . -type f -exec cat {} \; | jq -cr '.Records[]|[.eventTime, .eventName]|@tsv' | sort
2018-11-28T22:31:59Z    AssumeRole
2018-11-28T22:31:59Z    AssumeRole
2018-11-28T23:02:56Z    GetObject
2018-11-28T23:02:56Z    GetObject
2018-11-28T23:02:56Z    GetObject
2018-11-28T23:02:56Z    GetObject
2018-11-28T23:02:57Z    GetObject
2018-11-28T23:03:08Z    GetObject
2018-11-28T23:03:08Z    GetObject
2018-11-28T23:03:08Z    GetObject
2018-11-28T23:03:08Z    GetObject
2018-11-28T23:03:08Z    GetObject
2018-11-28T23:03:11Z    GetObject
2018-11-28T23:03:11Z    GetObject
2018-11-28T23:03:12Z    AssumeRole
2018-11-28T23:03:12Z    CreateLogStream
2018-11-28T23:03:13Z    CreateLogStream
```

Conclusion

In this lab, we assumed the "Security" IAM role in the AWS account to investigate a security incident. By analyzing the available logs, I identified misconfigurations that facilitated the attack, including a compromised IAM user and related indicators of compromise. This exercise emphasizes the critical role of proper IAM management and continuous log analysis in maintaining cloud security.