AWS API Abuse Detection & Alerting Pipeline

By: Ritvik Indupuri

Overview

This project simulates a cloud intrusion scenario involving the abuse of stolen AWS credentials. It demonstrates a complete end-to-end detection and alerting pipeline built **exclusively with AWS-native services** — without any third-party tooling.

A fake attacker environment using **Kali Linux** is used to emulate identity enumeration via `aws sts get-caller-identity`. This event is captured by **CloudTrail**, filtered by **EventBridge**, and results in a **real-time email alert** through **SNS**.

This lab replicates realistic SOC and Detection Engineering workflows relevant for:

- **Cloud Security Engineers**
- **SOC Analysts in cloud-native organizations**
- **Detection Engineers (AWS focus)**
- **Security Interns or Entry-Level Cloud Practitioners**

Table of Contents

1. Attack Simulation
2. Detection Architecture
3. CloudTrail Setup
4. EventBridge Detection Rule
5. Alerting with SNS
6. Validation & Testing
7. Results
8. Skills Demonstrated
9. Future Improvements

---

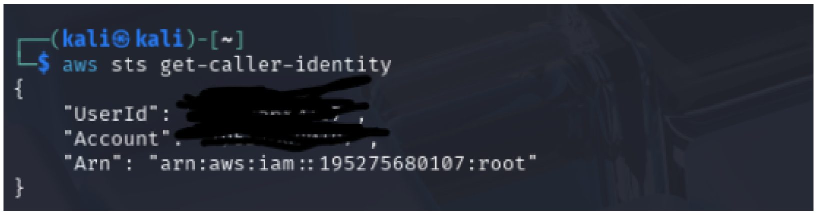
1. Attack Simulation

The attacker configures AWS CLI using stolen credentials and executes a reconnaissance command:

aws sts get-caller-identity

This is commonly used by adversaries to validate access and enumerate AWS account identity.

Figure 1 – Attack Execution via AWS CLI



```
┌──(kali㉿kali)-[~]
└─$ aws sts get-caller-identity
{
    "UserId": [redacted],
    "Account": [redacted],
    "Arn": "arn:aws:iam::195275680107:root"
}
```

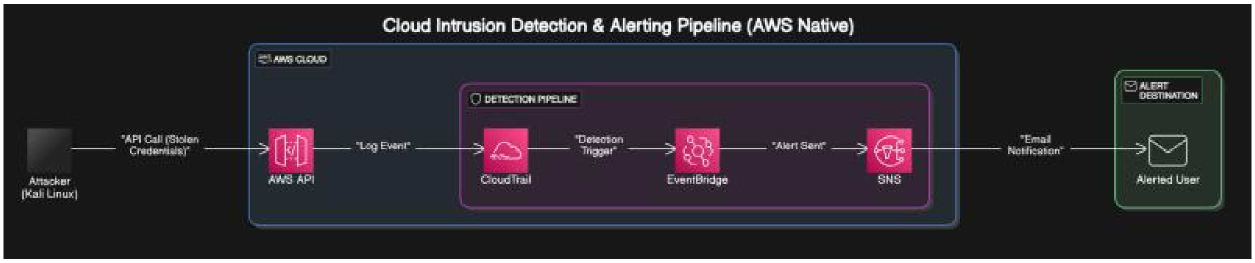
---

2. Detection Architecture

The detection and alerting pipeline includes the following components:

- **AWS CloudTrail**: Captures all management-level API activity.
- **Amazon EventBridge**: Filters for specific attack patterns (like `GetCallerIdentity`).
- **Amazon SNS**: Sends structured email notifications.
- **Amazon S3**: Stores raw CloudTrail logs.

Figure 2 – Detection Pipeline Overview



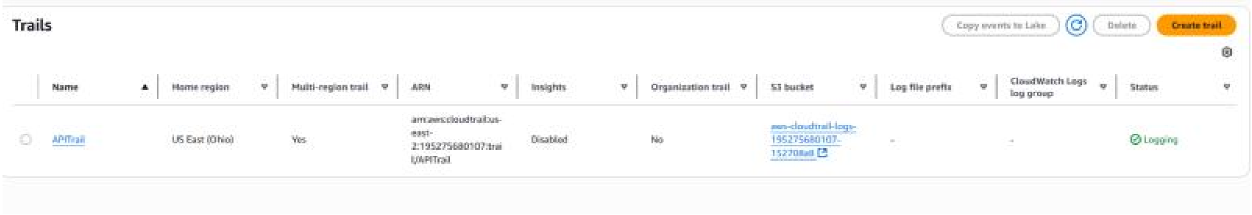
---

3. CloudTrail Setup

CloudTrail was configured to:

- Log all management events across multiple regions.
- Store logs in a designated S3 bucket.
- Provide full visibility into API usage.

Figure 3 – CloudTrail Configuration Panel



	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	APITrail	US East (Ohio)	Yes	arn:aws:cloudtrail:us-east-2:195275680107:trail/APITrail	Disabled	No	aws-cloudtrail-logs-195275680107-152708a0	-	-	Logging

---

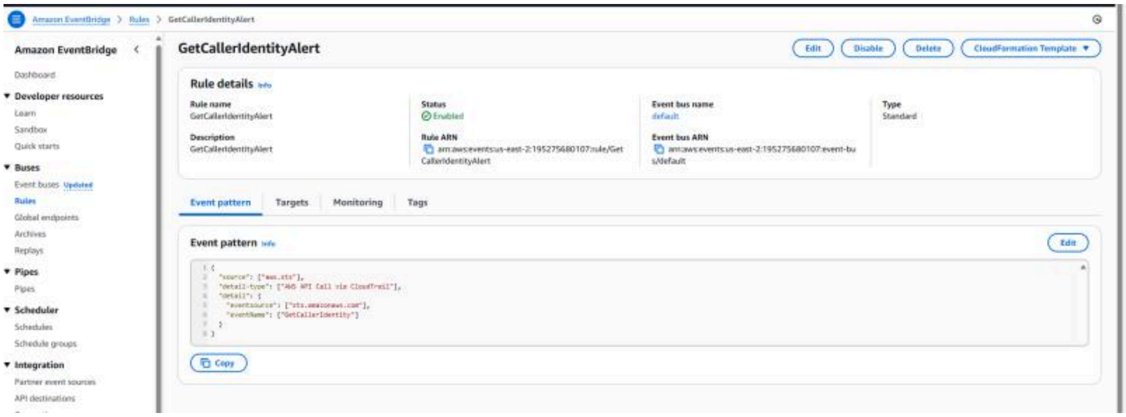
4. EventBridge Detection Rule

A rule was created in EventBridge to detect identity reconnaissance attempts:

```
{
  "source": ["aws.sts"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventName": ["GetCallerIdentity"]
  }
}
```

This pattern matches any CloudTrail event where the `GetCallerIdentity` API is called.

Figure 4 – EventBridge Rule Matching GetCallerIdentity



GetCallerIdentityAlert

Rule details Info

Rule name: GetCallerIdentityAlert
Description: GetCallerIdentityAlert
Status: Enabled
Rule ARN: arn:aws:events:us-east-2:195275680107:rule/GetCallerIdentityAlert
Event bus name: default
Event bus ARN: arn:aws:events:us-east-2:195275680107:event-bus/default
Type: Standard

Event pattern Info

```
{
  "source": ["aws.sts"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventsource": ["sts.amazonaws.com"],
    "eventName": ["GetCallerIdentity"]
  }
}
```

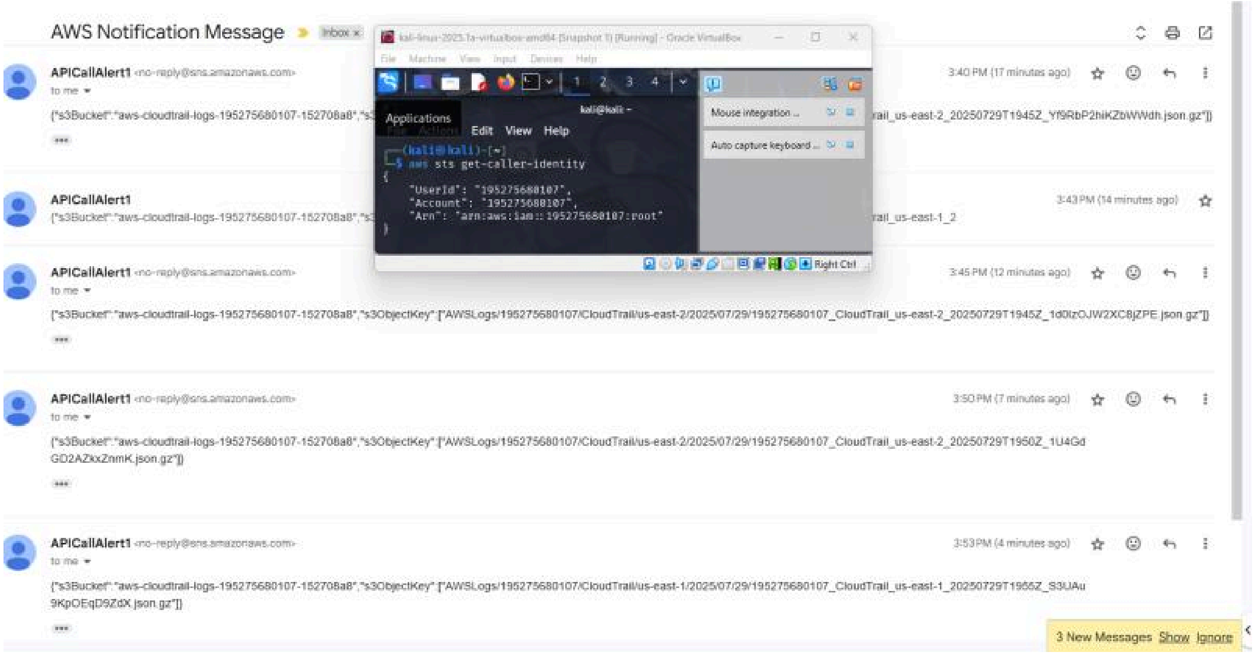
---

5. Alerting with SNS

Upon pattern match, EventBridge forwards the event to an **SNS topic** configured with email subscriptions.

- Emails include: API name, account ID, source IP, and CloudTrail S3 path.
- Analysts are alerted in near real-time.

Figure 5 – SNS Email Alert in Inbox



AWS Notification Message

APICallAlert1 <no-reply@sns.amazonaws.com> 3:40 PM (17 minutes ago)

to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3 … rail_us-east-2_20250729T1945Z_Yf9RbP2hiKZbWWdh.json.gz"]}

APICallAlert1 3:43 PM (14 minutes ago)

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3 … rail_us-east-1_2

APICallAlert1 <no-reply@sns.amazonaws.com> 3:45 PM (12 minutes ago)

to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3ObjectKey":["AWSLogs/195275680107/CloudTrail/us-east-2/2025/07/29/195275680107_CloudTrail_us-east-2_20250729T1945Z_1d0lzOJW2XC8jZPE.json.gz"]}

APICallAlert1 <no-reply@sns.amazonaws.com> 3:50 PM (7 minutes ago)

to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3ObjectKey":["AWSLogs/195275680107/CloudTrail/us-east-2/2025/07/29/195275680107_CloudTrail_us-east-2_20250729T1950Z_1U4GdGD2AZkxZnmK.json.gz"]}

APICallAlert1 <no-reply@sns.amazonaws.com> 3:53 PM (4 minutes ago)

to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3ObjectKey":["AWSLogs/195275680107/CloudTrail/us-east-1/2025/07/29/195275680107_CloudTrail_us-east-1_20250729T1955Z_S3UAu9KpOEqD9ZdX.json.gz"]}

3 New Messages Show Ignore

```
┌──(kali㉿kali)-[~]
└─$ aws sts get-caller-identity
{
    "UserId": "195275680107",
    "Account": "195275680107",
    "Arn": "arn:aws:iam::195275680107:root"
}
```

kali-linux-2025.1a-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Applications
File Actions Edit View Help
Mouse integration ...
Auto capture keyboard ...
Right Ctrl

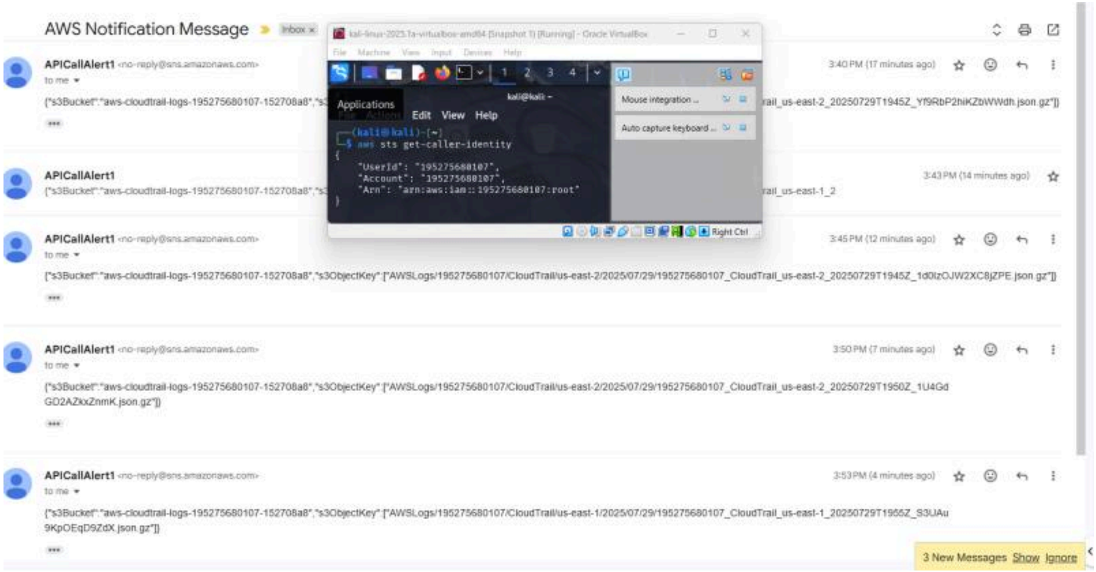
---

6. Validation & Testing

To validate the pipeline:

- `aws sts get-caller-identity` was run from the Kali host.
- CloudTrail captured the event.
- EventBridge matched the detection rule.
- SNS delivered an email alert.

Figure 6 – End-to-End Attack + Alert Evidence



AWS Notification Message

APICallAlert1 <no-reply@sns.amazonaws.com> 3:40 PM (17 minutes ago)
to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3 … rail_us-east-2_20250729T1945Z_Yf9RbP2hiKZbWWdh.json.gz"]}

APICallAlert1 3:43 PM (14 minutes ago)
{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3 … rail_us-east-1_2

APICallAlert1 <no-reply@sns.amazonaws.com> 3:45 PM (12 minutes ago)
to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3ObjectKey":["AWSLogs/195275680107/CloudTrail/us-east-2/2025/07/29/195275680107_CloudTrail_us-east-2_20250729T1945Z_1d0lzOJW2XC8jZPE.json.gz"]}

APICallAlert1 <no-reply@sns.amazonaws.com> 3:50 PM (7 minutes ago)
to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3ObjectKey":["AWSLogs/195275680107/CloudTrail/us-east-2/2025/07/29/195275680107_CloudTrail_us-east-2_20250729T1950Z_1U4GdGD2AZkxZnmK.json.gz"]}

APICallAlert1 <no-reply@sns.amazonaws.com> 3:53 PM (4 minutes ago)
to me

{"s3Bucket":"aws-cloudtrail-logs-195275680107-152708a8","s3ObjectKey":["AWSLogs/195275680107/CloudTrail/us-east-1/2025/07/29/195275680107_CloudTrail_us-east-1_20250729T1955Z_S3UAu9KpOEqD9ZdX.json.gz"]}

```
┌──(kali㉿kali)-[~]
└─$ aws sts get-caller-identity
{
    "UserId": "195275680107",
    "Account": "195275680107",
    "Arn": "arn:aws:iam::195275680107:root"
}
```

Inbox ×
kali-linux-2025.1a-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications
Edit View Help
kali@kali: ~
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
3 New Messages Show Ignore

7. Results

- Real-time detection of credential abuse
- End-to-end visibility from API call to inbox
- No third-party tools used — 100% AWS-native
- All logs preserved in S3 for post-incident triage

8. Skills Demonstrated

- Detection engineering using EventBridge
- Alerting pipeline design with CloudTrail + SNS
- Threat simulation and attacker emulation in Kali
- SOC-style triage and evidence correlation
- IAM event analysis and response design

9. Future Improvements

- Detect additional sensitive APIs (e.g., `CreateAccessKey`, `PassRole`, etc.)
- Add automated remediation via Lambda (e.g., disable key)
- Centralize alerts into OpenSearch or SIEM
- Enrich alerts with GeoIP/location info

- Visualize activity in Grafana dashboards