The Threat Within: The Dangers of Logs Manipulation

Mohamed Abumuslim

```
┌──(root💀kali)-[~]
└─# whoami
```

Mohamed Abumuslim A.k.A **m19o**.

Senior security consultant at **PwC ETIC**.

Discovered multiple CVEs CVE-2021-24970, CVE-2022-22511, CVE-2023-27237 and more.

Holds CRTE, eCPTxv2, eCPPTv2, eWAPTxv2 and many more.

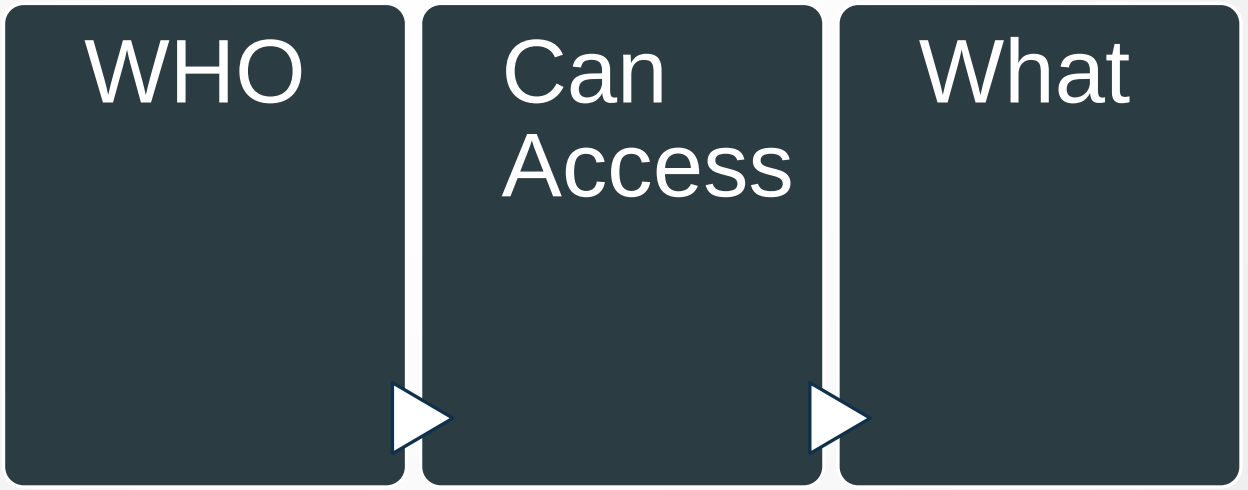
M19o__

Agenda

- Identity and access management overview
  - AWS Iam policies from security perspective
- Cloudtrail overview ?
  - Protecting Cloudtrail ?
    - Service-link Channels
    - Event data stores
    - Insights events
    - Organization Delegated Admin
- Q&A

What is identity and access management?

Identity and access managed (IAM) helps you to control access to AWS resources (users, services, groups, organizations).



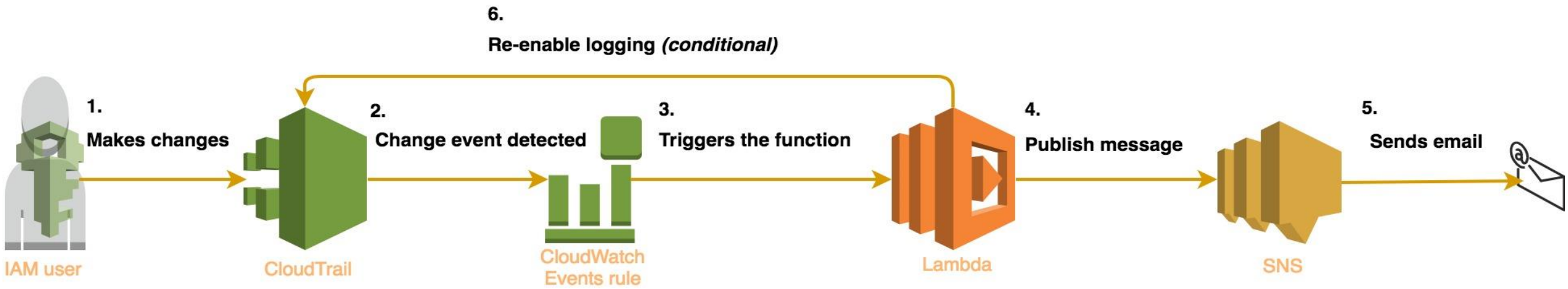
AWS IAM policies from security perspective

- **Use the principle of least privilege**. Only grant users and roles the permissions they need to perform their job functions. This will help you minimize the attack surface of your AWS account.
- **Use fine-grained permissions**. Don't grant users and roles broad permissions that they don't need. Instead, grant them specific permissions for the resources and actions they need to access.
- **Use condition statements**. Condition statements can be used to restrict the permissions granted by a policy to specific resources, actions, or conditions. This can help you further refine the permissions granted by a policy and improve security.
- **Use audit logging**. Audit logging can be used to track who made changes to IAM policies and when. This can help you identify suspicious activity and investigate security incidents.
- **Review your IAM policies regularly**. Your IAM policies should be reviewed regularly to ensure that they are still aligned with your security requirements.
- **Avoid** using public scripts and policy templates without checking them manually.

What is Cloudtrail?

AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail

Cloudtrail Workflow



Protecting Cloudtrail ?

What else could be used by an adversary ?

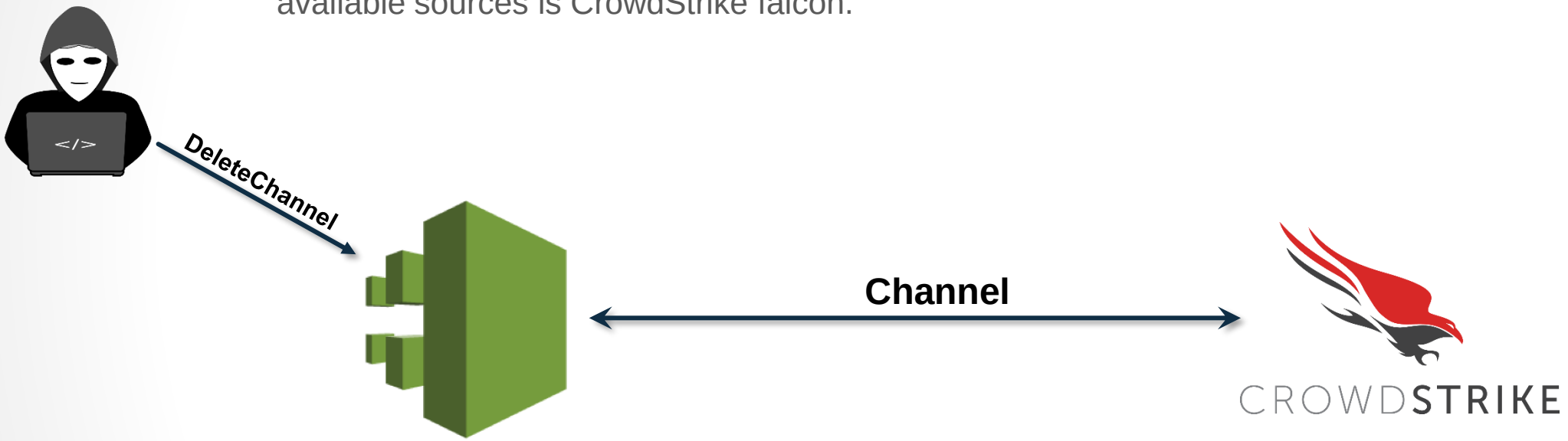
- “Cloudtrail:Deletechannel”
- “Cloudtrail:DeleteEventDataStore”
- “Cloudtrail:PutInsightSelectors”
- “Cloudtrail:StopEventDataStoreIngestion”
- “Cloudtrail:DeregisterOrganizationDelegatedAdmin”
- “Cloudtrail:RegisterOrganizationDelegatedAdmin”

```
{
"Version": "2012-10-17",
"Statement": [
{
        "Sid": "ProtectCloudTrail",
        "Effect": "Deny",
        “Action": [
            "cloudtrail:DeleteTrail",
            "cloudtrail:PutEventSelectors",
            “cloudtrail:StopLogging",
            "cloudtrail:UpdateTrail"
        ],
        "Resource": [
                "*”
        ]
}
```

Scenario 1.1

Service-link channel

Cloudtrail can create a channel to ingest events from a partner or external source, One of the available sources is CrowdStrike falcon.



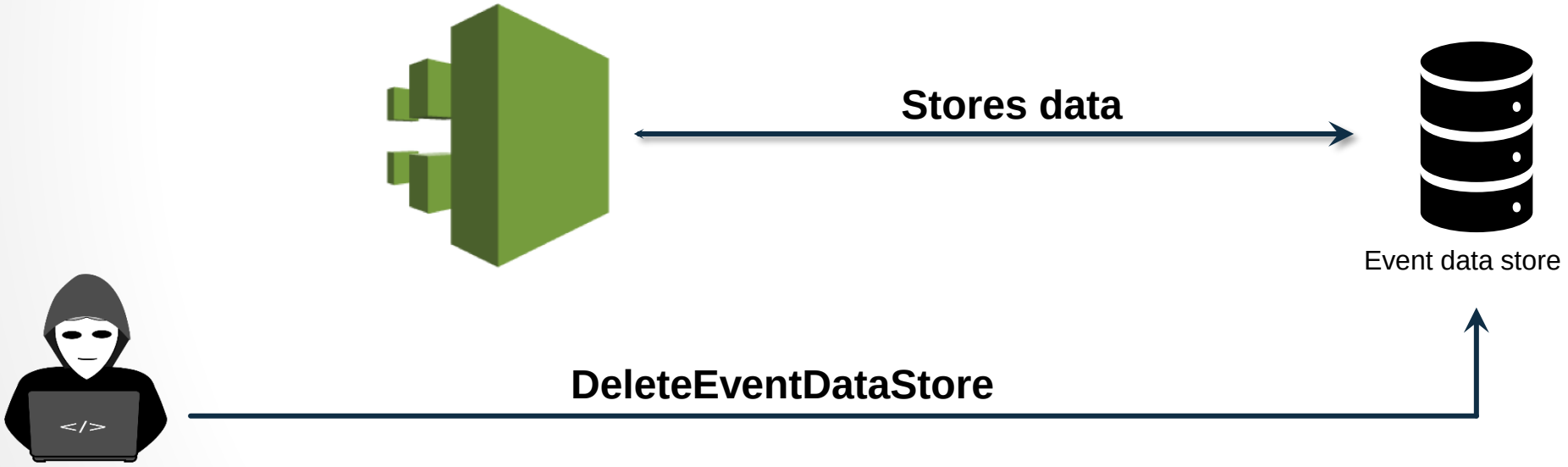
aws cloudtrail delete-channel --channel BsidesAbq

aws-cli-1.29.24

Scenario 2.1

Event data store

Event data stores for CloudTrail events can log CloudTrail management and data events. You can keep the event data in an event data store for up to seven years, or 2557 days



aws cloudtrail delete-event-data-store --event-data-store ARN

Scenario 3.1

Event data store

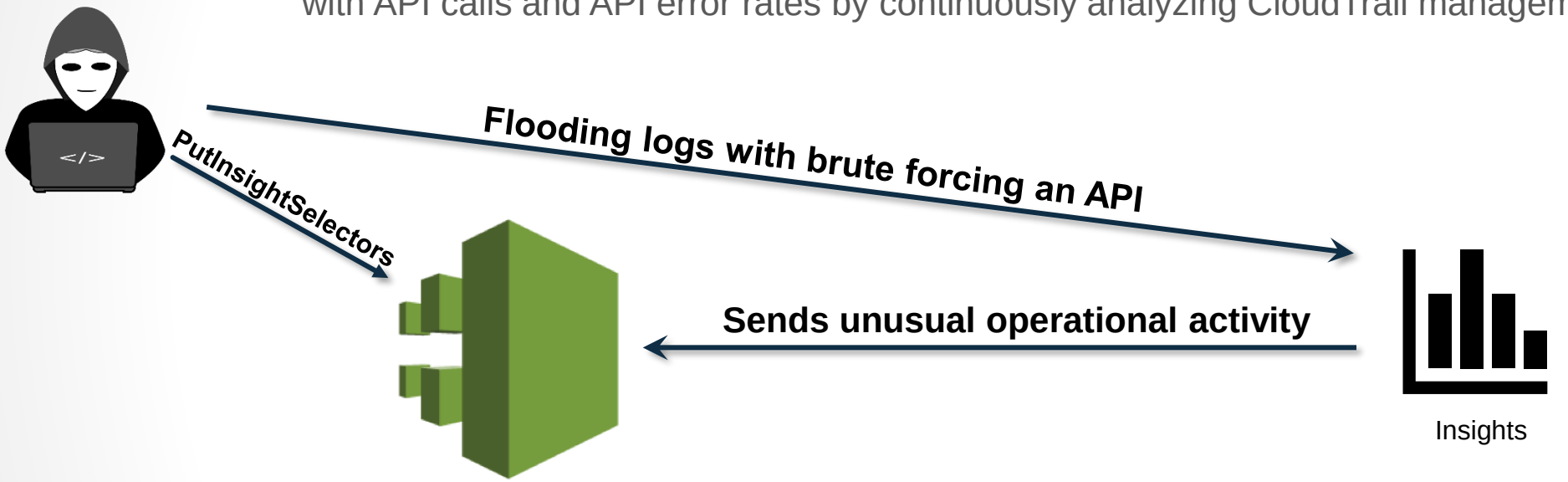
Event data stores for CloudTrail events can log CloudTrail management and data events. You can keep the event data in an event data store for up to seven years, or 2557 days

aws cloudtrail stop-event-data-store-ingestion --event-data-store ARN

Scenario 4.1

Insights events

AWS CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by continuously analyzing CloudTrail management events.

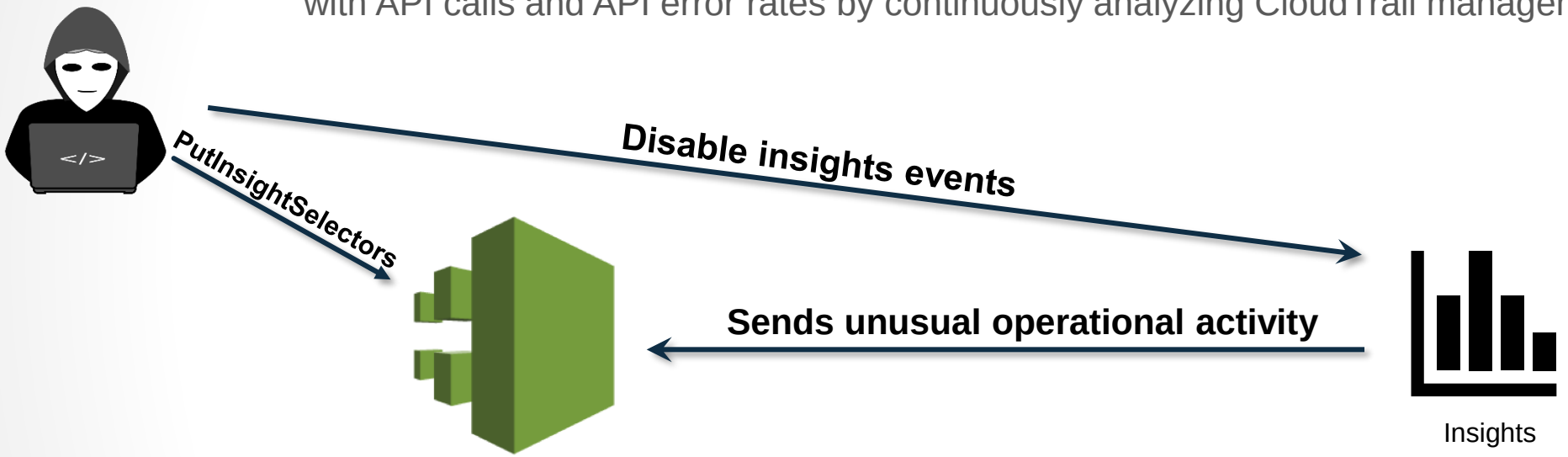



```
aws cloudtrail put-insight-selectors --trail-name BsidesAbq --insight-selectors
'{"InsightType":"ApiCallRateInsight"}'
```

Scenario 5.1

Insights events

AWS CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by continuously analyzing CloudTrail management events.

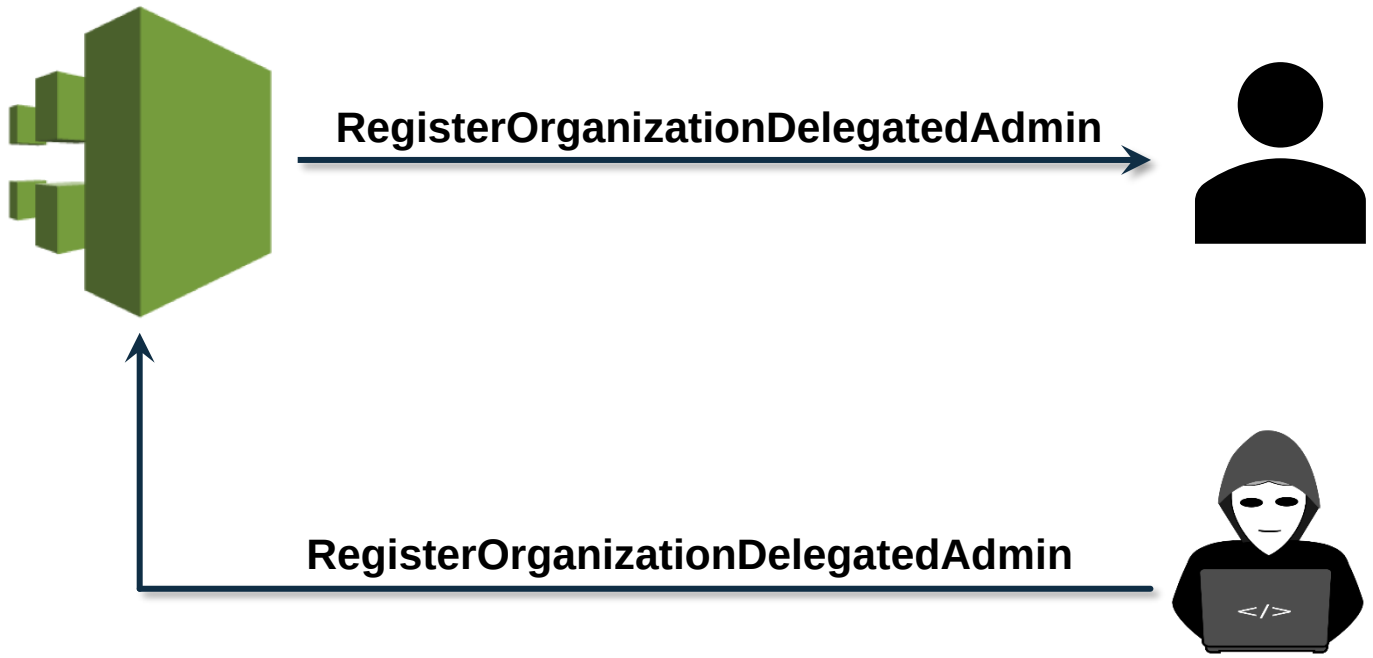



```
curl -i -s -k -X $'PUT' \
    --data-binary $'{\"trailArn\":\"arn:aws:cloudtrail:us-east-
1:882583340145:trail/management-events\",\"trailHomeRegion\":\"us-east-
1\",\"trailInsightSelectors\":\"[]\"}' \
    $'https://us-east-
1.console.aws.amazon.com/cloudtrail/service/putInsightSelectors?region=us-east-1''
```

Scenario 6.1

Organization Delegated Admin

A delegated administrator is a member account in an organization that can perform the same administrative tasks in CloudTrail as the management account.

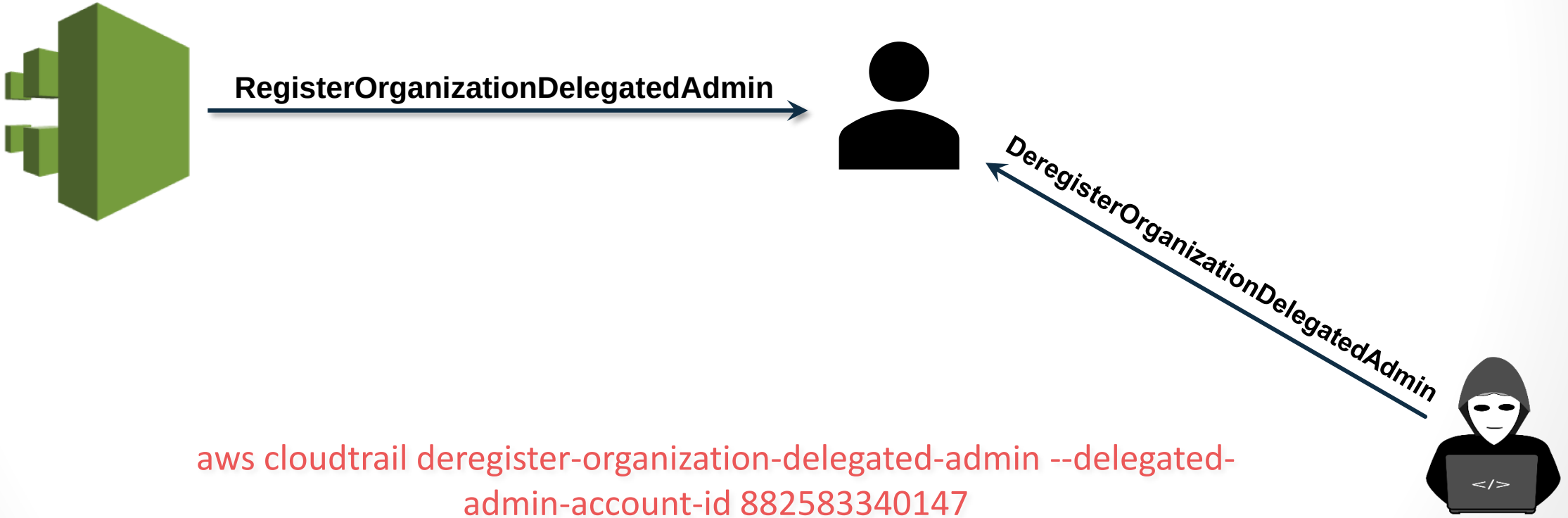


aws cloudtrail register-organization-delegated-admin --member-account-id 882583340147

Scenario 7.1

Organization Delegated Admin

A delegated administrator is a member account in an organization that can perform the same administrative tasks in CloudTrail as the management account.



aws cloudtrail deregister-organization-delegated-admin --delegated-admin-account-id 882583340147

Q&A