**Case Study-3:**

**Problem Statement:** A company is reviewing its AWS account security policies. The company has staff members in different countries and wants to monitor its AWS accounts for **unusual behavior** that is associated with an IAM identity. The company wants to send a **notification** to any staff member for whom unusual activity is detected. The company needs to manage its multiple AWS accounts to capture **consolidated billing** to help the finance team; store all billing reports in Account-B's S3 bucket. Along with this Account-A's EC2 instances need permissions to access Account-B's S3 bucket to develop the final report.

**SOLUTION**:

Terraform setup helps to automatically create and manage AWS services without manual work. It ensures secure access, tracks user activities, and sends alerts if something goes wrong.

The IAM role makes sure only approved EC2 instances can access S3 buckets. You’ve also allowed another AWS account (Account A) to safely access billing reports stored in your S3 bucket, making data sharing secure.

CloudTrail keeps records of who does what inside AWS, helping you track IAM activity. If someone tries an action they don’t have permission for, CloudWatch detects it and sends an alert through SNS, notifying the right people immediately.

Overall setup saves time, improves security, and keeps track of everything happening in AWS, ensuring that you control access and detect security risks fast.

**SCREENSHOTS:**







