1. **CI/CD Scenario**
   * 3 IAM Users
   * 1 EC2 Instance in a single VPC
   * 1 API Gateway
   * 1 Lambda Function
   * 1 ECR Image
   * 2 CodeBuild Projects
2. **Scenario Initiation**
   * Initial provision of IAM users with Access Key IDs and Secret Access Keys.
3. **Scenario Story**
   * FooCorp is a company that offers public APIs. FooCorp's customers submit sensitive data to the API endpoint every minute.

텍스트, 폰트, 스크린샷, 디자인이(가) 표시된 사진

자동 생성된 설명양식의 맨 위

* API:Implemented through a Lambda function exposed via an API Gateway.
* FooCorp, being a DevOps adopter, establishes a continuous deployment pipeline, which enables them to automatically deploy new versions of the Lambda function from source code to production within minutes.

1. **Scenario Objectives**

* Search for customer-submitted sensitive data. Simulated user activities occur within the account. Executed every minute, the simulation of customer requests to the API is accomplished through the CodeBuild project.

1. **Summary**

* Elevate permissions by overriding the tags on the EC2 instance used for attribute-based access control. Steal SSH keys from the instance and use them to clone the CodeCommit repository. Examine commit history and identify new sets of AWS credentials. Utilize these to backdoor applications and exfiltrate critical data.

텍스트, 스크린샷, 번호, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

* + - Creating an IAM User with Administrator privileges