——----------Ứng cứu sự cố—----------

*)**Tài liệu của AWS nêu rõ rằng bạn có thể tạo một AMI mới mà không chứa thông tin xác thực có khả năng bị xâm phạm và tạo một IAM Role với các quyền phù hợp. Sau đó, bạn có thể tạo một launch template cho Auto Scaling Group để tham chiếu đến AMI mới và IAM Role. Đây là phương pháp an toàn nhất để khắc phục các vấn đề bảo mật mà không gây gián đoạn cho ứng dụng.**

*)**Instance đáng ngờ chạy trong subnet us-east-1b và là instance duy nhất trong subnet này.**
=>Cập nhật outbound network ACL cho subnet us-east-1b để từ chối rõ ràng tất cả các kết nối như là rule đầu tiên. Thay thế security group hiện tại bằng một security group mới chỉ cho phép kết nối từ một security group chẩn đoán. Cập nhật outbound network ACL cho subnet us-east-1b để xóa rule deny all. Khởi chạy một instance EC2 mới có công cụ chẩn đoán. Gán security group mới cho instance EC2 mới. Sử dụng instance EC2 mới để điều tra instance đáng ngờ.

*)**Một kỹ sư bảo mật cần triển khai một giải pháp giám sát liên tục để tự động thông báo cho nhóm bảo mật của công ty về các instance bị xâm phạm thông qua một danh sách email phân phối**
=>Giải pháp:

- Kích hoạt GuardDuty:
    - GuardDuty là dịch vụ phát hiện mối đe dọa thời gian thực, có thể nhận diện các instance bị xâm phạm (như phát tán malware, kết nối đến địa chỉ độc hại).
    - Tích hợp sẵn với AWS Security Hub và EventBridge.
- Tạo SNS topic + email distribution list
    - SNS hỗ trợ gửi thông báo qua email cho nhóm bảo mật khi có sự cố.
    - Đơn giản, dễ triển khai nhanh
- EventBridge rule cho GuardDuty findings
    - EventBridge lọc các phát hiện high severity từ GuardDuty và kích hoạt SNS topic.
    - Đảm bảo chỉ các sự cố nghiêm trọng được thông báo.

*)**Công ty phát hiện ra rằng một hoặc nhiều EC2 instances đã bị xâm nhập và đang trích xuất dữ liệu đến một S3 bucket bên ngoài tổ chức của công ty trong AWS Organizations.Một kỹ sư bảo mật phải triển khai giải pháp ngăn chặn việc rò rỉ dữ liệu này mà vẫn đảm bảo quy trình xử lý dữ liệu của EC2 tiếp tục hoạt động.**
=>Áp dụng SCP (Service Control Policy) lên tài khoản AWS để chỉ cho phép các hành động S3 nếu giá trị của các điều kiện aws:ResourceOrgID và aws:PrincipalOrgID khớp với giá trị của công ty.

——----------Triển khai an toàn—----------

*)**Tài liệu của AWS nêu rõ rằng bạn có thể triển khai các hàm Lambda bên trong VPC và gắn một security group vào các hàm Lambda. Sau đó, bạn có thể chỉ cấp quyền truy cập outbound đến phạm vi CIDR của VPC và cập nhật security group của instance cơ sở dữ liệu để cho phép lưu lượng từ security group của Lambda. Đây là phương pháp an toàn nhất để đáp ứng các yêu cầu.**

*)**Các bước triển khai end-to-end encryption in transit**

-Các bước:

1. CloudFront → ALB: HTTPS (dùng ACM certificate)
2. ALB → EC2: Có thể HTTP (trong VPC đã an toàn) hoặc HTTPS
3. Ứng dụng → DynamoDB: Luôn dùng HTTPS
4. Client → CloudFront: Redirect HTTP → HTTPS

*)**Giới hạn IAM KMS Customer Master Key (CMK) chỉ hoạt động với Amazon S3**
-Yêu cầu chính:

- Giới hạn CMK chỉ được sử dụng bởi Amazon S3
- Tuân thủ chính sách "mỗi dịch vụ dùng CMK riêng"

2. Tại sao chọn B:
   - kms:ViaService là điều kiện đặc biệt trong KMS key policy:

```
"Condition": {
   "StringEquals": {
     "kms:ViaService": "s3.amazonaws.com"
   }
 }
```

   - Chỉ cho phép sử dụng CMK khi request đến từ dịch vụ S3
   - Ngăn các dịch vụ khác (như EC2, EBS...) sử dụng CMK này

*)**Sau khi triển khai chính sách yêu cầu mọi hành động tới EC2 yêu cầu 2FA, quản trị viên nhận được báo cáo rằng người dùng không thể thực hiện các lệnh Amazon EC2 bằng AWS CLI**
=>Hướng dẫn người dùng chạy lệnh CLI aws sts get-session-token và cung cấp các tham số xác thực đa yếu tố (--serial-number và --token-code). Sử dụng các giá trị này để thực hiện các lệnh API/CLI tiếp theo.

*)**Một kỹ sư bảo mật cần tạo cảnh báo sẽ thông báo cho công ty trước khi một KMS key bị xóa. Kỹ sư bảo mật đã cấu hình tích hợp giữa AWS CloudTrail và Amazon CloudWatch**
=>Tạo một Amazon EventBridge rule để phát hiện các API calls DisableKey và ScheduleKeyDeletion của KMS. Tạo một AWS Lambda function để gửi thông báo Amazon SNS tới công ty. Thêm Lambda function làm target của EventBridge rule.

*)**Một công ty có nhiều tài khoản trên AWS Cloud. Người dùng trong tài khoản Developer cần truy cập vào một số tài nguyên cụ thể trong tài khoản Production.**
=>Tạo cross-account access bằng một IAM role trong tài khoản Production. Cấp các quyền phù hợp cho role này. Cho phép người dùng trong tài khoản Developer assume role này để truy cập tài nguyên Production.

*)**Yêu cầu bảo mật của công ty**:

- **Bảo vệ quyền riêng tư người dùng: Dữ liệu truyền tải phải được mã hóa bằng các công nghệ tăng cường bảo mật (ví dụ: Perfect Forward Secrecy - PFS).**
- **Không ảnh hưởng đến chức năng của HIDS: Giải pháp phải đảm bảo HIDS agent vẫn có thể giám sát lưu lượng để phát hiện xâm nhập.**

=>Vấn đề cần giải quyết:

- Mâu thuẫn tiềm ẩn:

    - Nếu sử dụng mã hóa end-to-end (từ client tới server), HIDS agent sẽ không thể giải mã và phân tích lưu lượng.
    - Nếu tắt mã hóa giữa ALB và EC2 instance để HIDS hoạt động, dữ liệu sẽ bị truyền ở dạng plaintext (không mã hóa), vi phạm yêu cầu bảo mật.

→ Cần một giải pháp cân bằng: vừa mã hóa dữ liệu người dùng, vừa cho phép HIDS giám sát lưu lượng.
=>Bằng cách tạo một listener trên ALB không kích hoạt các cipher suite hỗ trợ PFS và sử dụng kết nối mã hóa với máy chủ bằng cipher suite ECDHE, bạn có thể đảm bảo rằng các tác nhân HIDS có thể ghi lại lưu lượng truy cập trên EC2 instance mà không ảnh hưởng đến quyền riêng tư của người dùng.

*)**Để ngăn người dùng truy cập trực tiếp vào Application Load Balancer và chỉ cho phép truy cập thông qua CloudFront**
-Hãy thực hiện các bước sau:
1️⃣ Cấu hình CloudFront để thêm một HTTP header tùy chỉnh vào các yêu cầu gửi đến Application Load Balancer.
2️⃣ Cấu hình Application Load Balancer chỉ chuyển tiếp các yêu cầu có chứa HTTP header tùy chỉnh.
3️⃣ (Tuỳ chọn) Yêu cầu HTTPS để tăng cường bảo mật cho giải pháp này.

*)**Một công ty sử dụng AWS Organizations và có các workload production trên nhiều tài khoản AWS khác nhau. Một kỹ sư bảo mật cần thiết kế một giải pháp để giám sát chủ động các hành vi đáng ngờ trên tất cả các tài khoản chứa workload production**.
=>Kích hoạt AWS Security Hub trên từng tài khoản production. Trong tài khoản logging chuyên dụng, tổng hợp tất cả findings Security Hub từ các tài khoản production. Khắc phục sự cố bằng cách sử dụng Amazon EventBridge để gọi một hàm AWS Lambda tùy chỉnh từ các findings Security Hub. Cấu hình hàm Lambda để gửi thông báo đến SNS topic.

*)**Kỹ sư bảo mật cần xây dựng một chính sách IAM theo nguyên tắc least privilege để thay thế các chính sách IAM quản lý bởi AWS hiện đang gắn với các role đang có quá nhiều đặc quyền.**
=>Trong AWS CloudTrail, tạo một trail cho các sự kiện quản lý. Chạy script với các chính sách IAM quản lý bởi AWS hiện có. Sử dụng IAM Access Analyzer để tạo chính sách IAM mới dựa trên hoạt động truy cập trong trail. Thay thế các chính sách IAM quản lý bởi AWS hiện có bằng chính sách IAM mới được tạo cho role.
=>Operationally efficient (Hiệu quả vận hành):
    - IAM Access Analyzer tự động phân tích hoạt động từ CloudTrail và tạo policy least privilege → tiết kiệm thời gian so với cách thủ công.
    - Không cần phải chạy script nhiều lần và sửa lỗi từng bước như phương án D.
- Bảo mật:
    - Policy được tạo dựa trên hoạt động thực tế của script → đảm bảo đủ quyền nhưng không dư thừa.
    - Thay thế các policy full-access bằng policy tối thiểu → giảm rủi ro bảo mật.

*)**Công ty cần xóa dữ liệu cũ hơn 30 ngày khỏi bucket S3 và bảng DynamoDB.**

=>Tạo policy vòng đời S3 để hết hạn các object cũ hơn 30 ngày. Cập nhật hàm Lambda để thêm thuộc tính TTL vào bảng DynamoDB. Bật TTL trên bảng DynamoDB để hết hạn các mục cũ hơn 30 ngày dựa trên thuộc tính TTL.