—----------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.

*)**Một công ty đã triển khai Amazon GuardDuty và hiện muốn tự động hóa xử lý các mối đe dọa tiềm ẩn. Công ty quyết định bắt đầu với các cuộc tấn công brute force RDP xuất phát từ các Amazon EC2 instances trong môi trường AWS của họ. Một kỹ sư bảo mật cần triển khai giải pháp chặn liên lạc từ các instance đáng ngờ cho đến khi có thể điều tra và khắc phục.**

=>Bật AWS Security Hub để thu thập kết quả từ GuardDuty và gửi sự kiện đến Amazon EventBridge (CloudWatch Events). Triển khai AWS Network Firewall. Xử lý sự kiện bằng AWS Lambda, thêm rule vào firewall policy để chặn traffic từ instance đáng ngờ.

*)**Một công ty vừa khôi phục sau một sự cố bảo mật yêu cầu phải khôi phục các Amazon EC2 instances từ snapshot. Sau khi phân tích khoảng trống trong quy trình phục hồi sau thảm họa và chiến lược sao lưu, công ty lo ngại rằng lần tới họ sẽ không thể khôi phục các EC2 instances nếu tài khoản AWS bị xâm phạm và các EBS snapshots bị xóa. Tất cả EBS snapshots đều được mã hóa bằng AWS KMS CMK.**
=>Tạo một tài khoản AWS mới với quyền hạn giới hạn. Cho phép tài khoản mới truy cập AWS KMS key dùng để mã hóa EBS snapshots và sao chép các snapshots đã mã hóa sang tài khoản mới định kỳ.
=>sao lưu chéo tài khoản giải quyết tốt nhất vì:

- Tài khoản riêng biệt giảm rủi ro nếu tài khoản chính bị xâm phạm.
- Sao chép định kỳ đảm bảo dữ liệu luôn có bản backup ở tài khoản khác.
- KMS key được chia sẻ giữa các tài khoản để duy trì khả năng giải mã.

*)Một ứng dụng được xây dựng với các instance Amazon EC2 có nhiệm vụ lấy tin nhắn từ Amazon SQS. Gần đây, các thay đổi về IAM đã được thực hiện và các instance không thể lấy tin nhắn nữa.Những hành động nào nên được thực hiện để khắc phục sự cố trong khi vẫn duy trì nguyên tắc đặc quyền tối thiểu
=>Giải pháp:

- Xác minh rằng policy tài nguyên SQS không từ chối quyền truy cập rõ ràng đối với role được sử dụng bởi các instance
- Xác minh rằng role được gắn với các instance có chứa các policy cho phép truy cập vào hàng đợi

=>Giải thích:

1. (Kiểm tra SQS resource policy) - Cần thiết vì resource policy có thể từ chối quyền truy cập ngay cả khi role có quyền
2. (Kiểm tra policy của role) - Cần xác minh role có đúng quyền tối thiểu cần thiết để truy cập SQS queue

*)**Một công ty đã vô tình xóa private key cho một instance Amazon EC2 sử dụng Amazon Elastic Block Store (EBS) làm storage. Một kỹ sư bảo mật cần lấy lại quyền truy cập vào instance này.**
=>Giải pháp:

- Dừng instance. Ngắt kết nối volume gốc. Tạo một key pair mới. (Không nên giữ instance chạy khi thao tác với volume gốc)
- Khi volume đã được ngắt kết nối khỏi instance gốc, gắn volume này vào một instance khác như một data volume. Chỉnh sửa file authorized_keys với một public key mới. Di chuyển volume trở lại instance gốc. Khởi động instance.

*)**Một công ty đã thuê một bên thứ ba để kiểm tra (audit) một số tài khoản AWS. Để thực hiện việc kiểm tra, các vai trò IAM liên tài khoản (cross-account IAM roles) đã được tạo trong mỗi tài khoản được nhắm đến. Tuy nhiên, kiểm toán viên đang gặp khó khăn khi truy cập vào một số tài khoản.**
=>Những nguyên nhân có thể gây ra vấn đề này:

- External ID mà kiểm toán viên sử dụng bị thiếu hoặc không chính xác.

- Kiểm toán viên chưa được cấp quyền sts:AssumeRole cho vai trò trong tài khoản đích.
- Role ARN mà kiểm toán viên sử dụng bị thiếu hoặc không chính xác.

=>Giải thích:
- Khi sử dụng cross-account IAM roles, External ID (nếu được cấu hình) phải khớp để đảm bảo bảo mật. Nếu thiếu hoặc sai, việc giả định vai trò sẽ thất bại.
- Để giả định (assume) một vai trò trong tài khoản khác, kiểm toán viên phải có quyền sts:AssumeRole trên vai trò đó. Nếu không, họ không thể truy cập.
- Role ARN (Amazon Resource Name) phải chính xác để AWS xác định được vai trò cần giả định. Nếu sai hoặc thiếu, quá trình sẽ thất bại.

——----------Triển khai—----------

*)**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.

*)**Một kỹ sư bảo mật muốn sử dụng Amazon Simple Notification Service (Amazon SNS) để gửi cảnh báo qua email đến nhóm bảo mật của công ty cho các phát hiện từ Amazon GuardDuty có mức độ nghiêm trọng Cao. Kỹ sư bảo mật cũng muốn chuyển các phát hiện này đến một công cụ trực quan hóa để kiểm tra thêm.**
=>Thiết lập GuardDuty để gửi thông báo đến Amazon EventBridge với hai mục tiêu. Từ EventBridge, truyền các phát hiện qua Amazon Kinesis Data Firehose vào một miền Amazon OpenSearch Service làm mục tiêu đầu tiên để phân phối. Sử dụng OpenSearch Dashboards để trực quan hóa các phát hiện. Sử dụng các truy vấn OpenSearch để phân tích thêm. Gửi cảnh báo email đến nhóm bảo mật bằng cách cấu hình một chủ đề SNS làm mục tiêu thứ hai cho EventBridge. Sử dụng khớp mẫu sự kiện với quy tắc sự kiện EventBridge để chỉ gửi các phát hiện có mức độ nghiêm trọng Cao trong cảnh báo.
=>Giải thích:

- EventBridge là dịch vụ phù hợp để xử lý sự kiện từ GuardDuty và định tuyến đến nhiều mục tiêu.
- Kinesis Data Firehose thường được sử dụng để gửi dữ liệu đến OpenSearch Service một cách hiệu quả.
- OpenSearch Dashboards là công cụ trực quan hóa tích hợp sẵn với OpenSearch Service.
- SNS được cấu hình làm mục tiêu thứ hai để gửi email cảnh báo.
- EventBridge event rule cho phép lọc chỉ các phát hiện có mức độ nghiêm trọng Cao.

*)**Một tổ chức muốn ghi lại tất cả các lần gọi API IAM được thực hiện trong tất cả các tài khoản IAM của họ và phải có một nơi tập trung để phân tích các nhật ký này.**
=>Giải pháp:

Bật IAM CloudTrail trong từng tài khoản IAM

- Để ghi lại tất cả các lần gọi API IAM, mỗi tài khoản AWS phải bật CloudTrail (không phải "IAM CloudTrail" vì không có dịch vụ nào tên như vậy, nhưng AWS CloudTrail có thể ghi lại các sự kiện IAM).
- CloudTrail phải được kích hoạt trong mỗi tài khoản để ghi lại hoạt động API.

Cập nhật bucket policy của bucket S3 trong tài khoản lưu trữ nhật ký để các tài khoản khác có thể ghi vào đó

- Để tập trung nhật ký, các tài khoản khác phải có quyền ghi vào một bucket S3 chung.
- Bucket policy (chứ không phải ACL) là cách bảo mật hơn để cấp quyền truy cập giữa các tài khoản AWS.

*)**Một công ty đang chạy các microservices nội bộ trên Amazon Elastic Container Service (Amazon ECS) với launch type EC2. Công ty này sử dụng các private repository trên Amazon Elastic Container Registry (Amazon ECR).**
Một kỹ sư bảo mật cần mã hóa các private repository bằng AWS Key Management Service (AWS KMS) và đồng thời phân tích các container image để phát hiện các lỗ hổng bảo mật phổ biến (Common Vulnerabilities and Exposures - CVEs).
=>Tạo lại các ECR repository với mã hóa KMS và tính năng ECR scanning được bật. Phân tích báo cáo scan sau khi push image tiếp theo.
=>Giải thích:

- Yêu cầu 1: Mã hóa ECR repositories bằng KMS → Phải tạo lại repository (vì không thể bật KMS encryption trên repository đã tồn tại).
- Yêu cầu 2: Phân tích image để tìm CVEs → ECR Scanning là tính năng tích hợp sẵn để quét lỗ hổng trong container images.
- Giải pháp B đáp ứng cả hai yêu cầu:
  - Tạo lại ECR repositories với KMS encryption (để mã hóa).
  - Bật ECR scanning (để tự động quét CVEs khi push image).

*)**Một công ty sử dụng AWS Organizations. Công ty có các nhóm sử dụng phần cứng bảo mật (HSM) AWS CloudHSM được đặt trong một tài khoản AWS trung tâm. Một trong các nhóm này tạo một tài khoản AWS riêng mới và muốn sử dụng HSM đang được lưu trữ trong tài khoản trung tâm.**
=>Sử dụng AWS Resource Access Manager (RAM) để chia sẻ ID subnet VPC của HSM từ tài khoản trung tâm với tài khoản mới. Cấu hình security group của CloudHSM để chấp nhận lưu lượng inbound từ các địa chỉ IP riêng của các máy client trong tài khoản mới.

*)**Giải pháp cần đảm bảo rằng key material (tài liệu khóa) tự động hết hạn sau 90 ngày.**
=>Giải pháp:
-Customer Managed CMK + key material do khách hàng cung cấp) là giải pháp duy nhất cho phép đặt thời gian hết hạn key material sau 90 ngày theo yêu cầu.

```
aws kms import-key-material \
--key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
--encrypted-key-material fileb://EncryptedKeyMaterial.bin \
--import-token fileb://ImportToken.bin \
--expiration-model KEY_MATERIAL_EXPIRES \
--valid-to 2021-09-21T19:00:00Z
```

*)**Cần đảm bảo rằng mọi thay đổi đối với Security Groups đều được ghi nhận và xử lý kịp thời**
=>Sử dụng CloudWatch Events để kích hoạt khi có bất kỳ thay đổi nào đối với Security Groups. Cấu hình Lambda function để gửi thông báo qua email.
=>CloudWatch Events (nay là Amazon EventBridge) có thể phát hiện thay đổi real-time đối với Security Groups (thông qua AWS API calls như AuthorizeSecurityGroupIngress).

- Lambda function có thể xử lý thông báo ngay lập tức (ví dụ: gửi email qua SNS hoặc thực hiện hành động khắc phục).

*)**Một công ty đang chạy các tải công việc của mình trong một AWS Region duy nhất và sử dụng AWS Organizations. Một kỹ sư bảo mật cần triển khai giải pháp để ngăn người dùng khởi chạy tài nguyên ở các Region khác.**
=>Tạo một SCP (Service Control Policy) có điều kiện aws:RequestedRegion từ chối các hành động không thuộc Region được chỉ định. Gắn SCP này vào tài khoản AWS trong AWS Organizations.
=>Yêu cầu chính: Giới hạn việc tạo tài nguyên chỉ trong một Region duy nhất với ít công vận hành nhất.

- SCP (Service Control Policy) là giải pháp tối ưu vì:
    - Áp dụng tự động cho mọi IAM user/role trong tài khoản AWS (không cần gắn thủ công từng policy).
    - Quản lý tập trung qua AWS Organizations (phù hợp khi công ty đang dùng Organizations).
    - aws:RequestedRegion trong SCP sẽ chặn mọi yêu cầu tạo tài nguyên ở Region khác.

*)**Một kỹ sư bảo mật cần triển khai giải pháp để ngăn người dùng khởi chạy tài nguyên ở các Region khác**
=>Tạo một SCP (Service Control Policy) có điều kiện aws:RequestedRegion từ chối các hành động không thuộc Region được chỉ định. Gắn SCP này vào tài khoản AWS trong AWS Organizations.
=>Giải thích:

- Yêu cầu chính: Giới hạn việc tạo tài nguyên chỉ trong một Region duy nhất với ít công vận hành nhất.
- SCP (Service Control Policy) là giải pháp tối ưu vì:
    - Áp dụng tự động cho mọi IAM user/role trong tài khoản AWS (không cần gắn thủ công từng policy).
    - Quản lý tập trung qua AWS Organizations (phù hợp khi công ty đang dùng Organizations).
    - aws:RequestedRegion trong SCP sẽ chặn mọi yêu cầu tạo tài nguyên ở Region khác.

*)**Để xem các phát hiện của Security Hub cho các tài khoản nằm ngoài tổ chức chứa tài khoản quản trị viên Security Hub, cần thực hiện các bước sau:**

- Gửi lời mời đến các tài khoản nằm ngoài tổ chức của công ty từ tài khoản quản trị viên Security Hub. Điều này sẽ cho phép tài khoản quản trị viên xem và quản lý các phát hiện từ những tài khoản đó. Tài khoản quản trị viên có thể gửi lời mời bằng cách sử dụng bảng điều khiển Security Hub, API hoặc CLI. Để biết thêm thông tin,

hãy xem Gửi lời mời đến các tài khoản thành viên.

- Gửi yêu cầu quản trị từ các tài khoản thành viên. Điều này sẽ cho phép các tài khoản thành viên chấp nhận lời mời từ tài khoản quản trị viên và thiết lập mối quan hệ với nó. Các tài khoản thành viên có thể gửi yêu cầu quản trị bằng cách sử dụng bảng điều khiển Security Hub, API hoặc CLI. Để biết thêm thông tin, hãy xem Gửi yêu cầu quản trị.

*)**Một tập đoàn lớn đang xây dựng chiến lược đa tài khoản (multi-account) và cần xác định cách nhân viên của họ nên truy cập vào cơ sở hạ tầng IAM.**
=>Sử dụng một tài khoản tập trung (centralized account) với các IAM roles mà nhân viên có thể sử dụng thông qua liên kết (federation) với nhà cung cấp danh tính hiện có. Sử dụng cross-account roles để cho phép người dùng liên kết (federated users) chuyển sang vai trò (role) mục tiêu trong các tài khoản tài nguyên (resource accounts).
=>Giải thích:

- sử dụng IAM roles + federation + cross-account access, đây là cách tiếp cận scalable nhất vì:
    - Không cần tạo IAM users riêng trong từng tài khoản (giảm quản lý phức tạp).
    - Tập trung quản lý quyền trong một tài khoản chính, sau đó sử dụng cross-account roles để phân quyền sang các tài khoản khác.
    - Tích hợp với identity provider (IdP) hiện có (như Active Directory, Okta, Azure AD) thông qua federation (SAML/OIDC).

*)**Một công ty có ứng dụng web sử dụng Amazon CloudFront và chạy trên Amazon Elastic Container Service (ECS) đằng sau một Application Load Balancer (ALB). ALB đang chấm dứt kết nối TLS và cân bằng tải giữa các tác vụ dịch vụ ECS. Một kỹ sư bảo mật cần thiết kế giải pháp để đảm bảo rằng nội dung ứng dụng chỉ có thể truy cập thông qua CloudFront và không bao giờ có thể truy cập trực tiếp.**
=>Giải pháp:

- Thêm **origin custom header**
- Đặt **viewer protocol policy** thành **chuyển hướng HTTP sang HTTPS**
- Đặt **origin protocol policy** thành **HTTP only**
- Cập nhật ứng dụng để xác thực **CloudFront custom header**

=>Giải thích:

- Origin custom header giúp xác thực rằng yêu cầu chỉ đến từ CloudFront (ngăn truy cập trực tiếp).
- Viewer protocol policy nên chuyển hướng HTTP sang HTTPS để đảm bảo mã hóa end-to-end.
- Origin protocol policy nên là HTTPS only để đảm bảo kết nối an toàn giữa CloudFront và ALB.
- Cập nhật ứng dụng để xác thực header ngăn truy cập trực tiếp mà không có header hợp lệ từ CloudFront.

*)**Các bước cô lập một EC2 bị xâm phạm**
-Vấn đề hiện tại:

- SSH vẫn hoạt động dù đã xóa rule vì security group có tính stateful (cho phép traffic đã thiết lập tiếp tục, dù rule bị xóa).

- Ping bị chặn vì nó sử dụng ICMP, không phải TCP (SSH), và không có rule cho phép.

=>Giải pháp tối ưu (C):

- Network ACL (stateless) có thể chặn ngay lập tức mọi traffic (kể cả kết nối hiện có).
- Đặt rule DENY ALL ở đầu sẽ ghi đè mọi rule khác.
- Không ảnh hưởng đến các instance khác trong cùng subnet (vì chỉ áp dụng cho target instance nếu cấu hình đúng).

*)**Một công ty có một nguyên tắc yêu cầu mã hóa tất cả dữ liệu trong Amazon S3 bucket khi truyền tải. Một kỹ sư bảo mật phải triển khai chính sách S3 bucket để từ chối bất kỳ thao tác S3 nào nếu dữ liệu không được mã hóa.**

=>Giải pháp:

```
{
     "Version": "2012-10-17",
     "Statement": [{
                  "Sid": "AllowSSLRequestOnly",
                  "Action": "s3:*",
                  "Effect": "Deny",
                  "Resource": [
                    "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                  ],
                  "Condition": {
                    "Bool": {
                         "aws:SecureTransport": "false"
                    }
                  },
                  "Principal": "*"
     }]
}
```

=>aws:SecureTransport là một điều kiện trong chính sách AWS IAM hoặc chính sách S3 bucket, được sử dụng để đảm bảo rằng tất cả các yêu cầu truy cập vào Amazon S3 đều sử dụng kết nối an toàn (HTTPS).

*)**Công ty đang tiến hành nhiều dự án thử nghiệm để kiểm tra việc sử dụng AWS KMS. Các bài kiểm tra này đã dẫn đến sự gia tăng đột biến trong việc tiêu thụ tài nguyên AWS của công ty. Các dự án thử nghiệm bao gồm các ứng dụng gửi nhiều yêu cầu mỗi giây đến các điểm cuối KMS cho các hoạt động mã hóa.**

=>Công ty cần phát triển một giải pháp không làm giới hạn khả năng sử dụng AWS KMS. Giải pháp phải cải thiện việc sử dụng khóa cho mã hóa phía máy khách và phải tối ưu chi phí.

=>Giải pháp: Sử dụng data key caching. Sử dụng bộ nhớ đệm cục bộ mà AWS Encryption SDK cung cấp với một caching cryptographic materials manager.

=>Giải thích

- Data key caching giúp giảm số lượng yêu cầu đến KMS bằng cách lưu trữ cục bộ các data key đã được mã hóa (encrypted data keys) và chỉ gọi KMS khi cần thiết, từ đó tránh bị throttle và tối ưu chi phí.

- Các phương án A và D liên quan đến keyrings nhưng không giải quyết triệt để vấn đề throttle do vẫn phải gọi KMS thường xuyên.
- Phương án C đề cập đến key rotation (luân chuyển khóa), không liên quan trực tiếp đến việc giảm lượng request đến KMS.

*)**Có yêu cầu về tính liên tục trong kinh doanh (business continuity) để đảm bảo tính khả dụng cao (high availability) cho các EBS volumes. Làm thế nào để đạt được điều này?**
=>Giải pháp: Sử dụng EBS Snapshots
=>EBS Snapshots cho phép sao lưu dữ liệu từ EBS volumes sang Amazon S3, giúp khôi phục dữ liệu nhanh chóng trong trường hợp volume bị lỗi hoặc mất dữ liệu. Điều này đảm bảo tính khả dụng cao (high availability) và phù hợp với yêu cầu business continuity.

*)**Một công ty cần sử dụng HTTPS khi kết nối đến các ứng dụng web của mình để đáp ứng yêu cầu tuân thủ (compliance). Các ứng dụng web này chạy trên Amazon VPC với các EC2 instances đặt phía sau Application Load Balancer (ALB). Một kỹ sư bảo mật muốn đảm bảo rằng load balancer chỉ chấp nhận kết nối qua cổng 443, ngay cả khi ALB bị cấu hình nhầm với một HTTP listener.**
=>Giải pháp:Tạo một security group với một quy tắc inbound duy nhất cho phép kết nối từ 0.0.0.0/0 trên cổng 443. Đảm bảo rằng security group này là nhóm duy nhất được liên kết với ALB.
=>Giải thích:Security groups hoạt động như một tường lửa ảo ở mức instance, và chúng có tính chất "chỉ cho phép" (allow-only). Nếu chỉ có một rule cho phép cổng 443, mọi kết nối HTTP (cổng 80) sẽ bị chặn, ngay cả khi ALB có HTTP listener.

*)**Hàm Lambda này cần quyền truy cập đọc và ghi vào một bucket Amazon S3 trong cùng tài khoản AWS.Những giải pháp nào sẽ cung cấp quyền truy cập này cho hàm Lambda?**
=>Tạo một IAM role cho hàm Lambda. Đính kèm một IAM policy cho phép truy cập vào bucket S3.
=>Tạo một IAM role cho hàm Lambda. Đính kèm bucket policy vào bucket S3 để cho phép truy cập. Chỉ định IAM role của hàm làm principal.

*)**Một công ty cần tuân thủ các phương pháp bảo mật tốt nhất để triển khai tài nguyên từ mẫu AWS CloudFormation. Mẫu CloudFormation phải có khả năng cấu hình thông tin xác thực cơ sở dữ liệu nhạy cảm.**
=>Sử dụng tham chiếu động (dynamic reference) trong mẫu CloudFormation để tham chiếu thông tin xác thực cơ sở dữ liệu trong Secrets Manager.
=>Giải thích:Dynamic reference trong CloudFormation cho phép tham chiếu trực tiếp đến secret được lưu trữ trong Secrets Manager một cách an toàn, không lộ thông tin nhạy cảm trong template. Đây là phương pháp bảo mật nhất.

*)**Công ty cần sao chép các đối tượng S3 từ AWS Region chính sang Region phụ để đáp ứng yêu cầu khôi phục thảm họa. Đồng thời phải đảm bảo rằng người dùng có quyền quản trị không thể xóa vĩnh viễn dữ liệu ở Region phụ.**
=>Triển khai S3 Object Lock ở chế độ compliance tại Region chính. Cấu hình S3 replication để sao chép đối tượng sang bucket S3 ở Region phụ.

=>Giải thích:S3 Object Lock ở chế độ compliance ngăn mọi người (kể cả admin) xóa hoặc ghi đè dữ liệu trong suốt thời gian retention

- Khi kết hợp với S3 replication, tính năng này sẽ được áp dụng cho cả dữ liệu ở Region phụ
- Đáp ứng đủ 2 yêu cầu: (1) sao chép liên Region và (2) bảo vệ dữ liệu khỏi bị admin xóa

*)**Một doanh nghiệp cần giải pháp ghi log phục vụ điều tra pháp y (forensic logging) cho hàng trăm ứng dụng chạy trên Docker trong Amazon EC2. Giải pháp phải:**

- **Phân tích log theo thời gian thực**
- **Cung cấp khả năng phát lại thông điệp (message replay)**
- **Duy trì log lâu dài**

=>Giải pháp: sử dụng dịch vụ

Amazon Kinesis:

- Xử lý log theo thời gian thực (real-time analysis)
- Hỗ trợ phát lại dữ liệu (message replay)
- Lưu trữ tạm thời trước khi chuyển đến nơi lưu trữ lâu dài

Amazon Elasticsearch:

- Phân tích log mạnh mẽ (bao gồm phân tích thời gian thực)
- Lưu trữ log lâu dài (log persistence)
- Tích hợp tốt với Kinesis để xử lý pipeline log

*)**Một công ty sử dụng Infrastructure as Code (IaC) để tạo hạ tầng AWS. Công ty viết code dưới dạng template AWS CloudFormation để triển khai hạ tầng. Công ty có một pipeline CI/CD sẵn có có thể sử dụng để triển khai các template này.**
Sau một cuộc kiểm tra bảo mật gần đây, công ty quyết định áp dụng phương pháp policy-as-code để cải thiện tình hình bảo mật trên AWS. Công ty cần ngăn chặn việc triển khai bất kỳ hạ tầng nào vi phạm chính sách bảo mật, chẳng hạn như volume Amazon Elastic Block Store (Amazon EBS) không được mã hóa.
=>Giải pháp:Tạo rule sets trong AWS CloudFormation Guard. Chạy các kiểm tra validation cho CloudFormation templates như một giai đoạn trong quy trình CI/CD.
=>giải thích:CloudFormation Guard là công cụ chính sách dạng code (policy-as-code) của AWS, cho phép kiểm tra template CloudFormation trước khi triển khai để đảm bảo tuân thủ các quy tắc bảo mật (ví dụ: EBS phải được mã hóa).

*)**Một công ty đang sử dụng phân phối Amazon CloudFront để phân phối nội dung từ hai nguồn gốc. Một nguồn gốc là ứng dụng động được lưu trữ trên các instance Amazon EC2. Nguồn gốc còn lại là một bucket Amazon S3 chứa các tài nguyên tĩnh. Một phân tích bảo mật cho thấy các phản hồi HTTPS từ ứng dụng không tuân thủ yêu cầu bảo mật về việc cung cấp tiêu đề HTTP X-Frame-Options để ngăn chặn các cuộc tấn công cross-site scripting liên quan đến khung. Một kỹ sư bảo mật phải làm cho toàn bộ hệ thống tuân thủ bằng cách thêm tiêu đề HTTP còn thiếu vào các phản hồi.**
=>Giải pháp:Tạo một hàm Lambda@Edge. Bao gồm mã để thêm tiêu đề X-Frame-Options vào phản hồi. Cấu hình hàm để chạy khi có sự kiện phản hồi nguồn gốc CloudFront.
=>Giải thích:

- Lambda@Edge là giải pháp tối ưu vì:

- Có thể thêm header vào response trước khi trả về cho client
- Áp dụng được cho cả hai origin (EC2 và S3)
- Không cần thay đổi ứng dụng backend (EC2)