CMC TELECOM | aws

Webinar Series

Bảo mật AWS
từ cơ sở hạ tầng
đến ứng dụng

Webinar 2:

Chiến lược toàn diện bảo vệ tài sản số trên AWS

Thứ Sáu, **31/05/2024**

09h00 - 10h00

Miễn phí qua GoToWebinar

Webinar 1: Nền tảng bảo mật trên AWS

CMC TELECOM

Webinar 2:

Chiến lược toàn diện bảo vệ tài sản số trên AWS

Thanh Nguyen
Solutions Architect, CMC Telecom

Dzung Le
Solutions Architect, CMC Telecom

CMC TELECOM

Agenda

- Bảo vệ an toàn hệ thống trên AWS
- Bảo vệ an toàn dữ liệu
- Q&A
- Minigame

CMC TELECOM

Bảo vệ an toàn hệ thống trên AWS

Bảo vệ an toàn hệ thống trên AWS

CMC TELECOM

Tuân thủ AWS best-practices

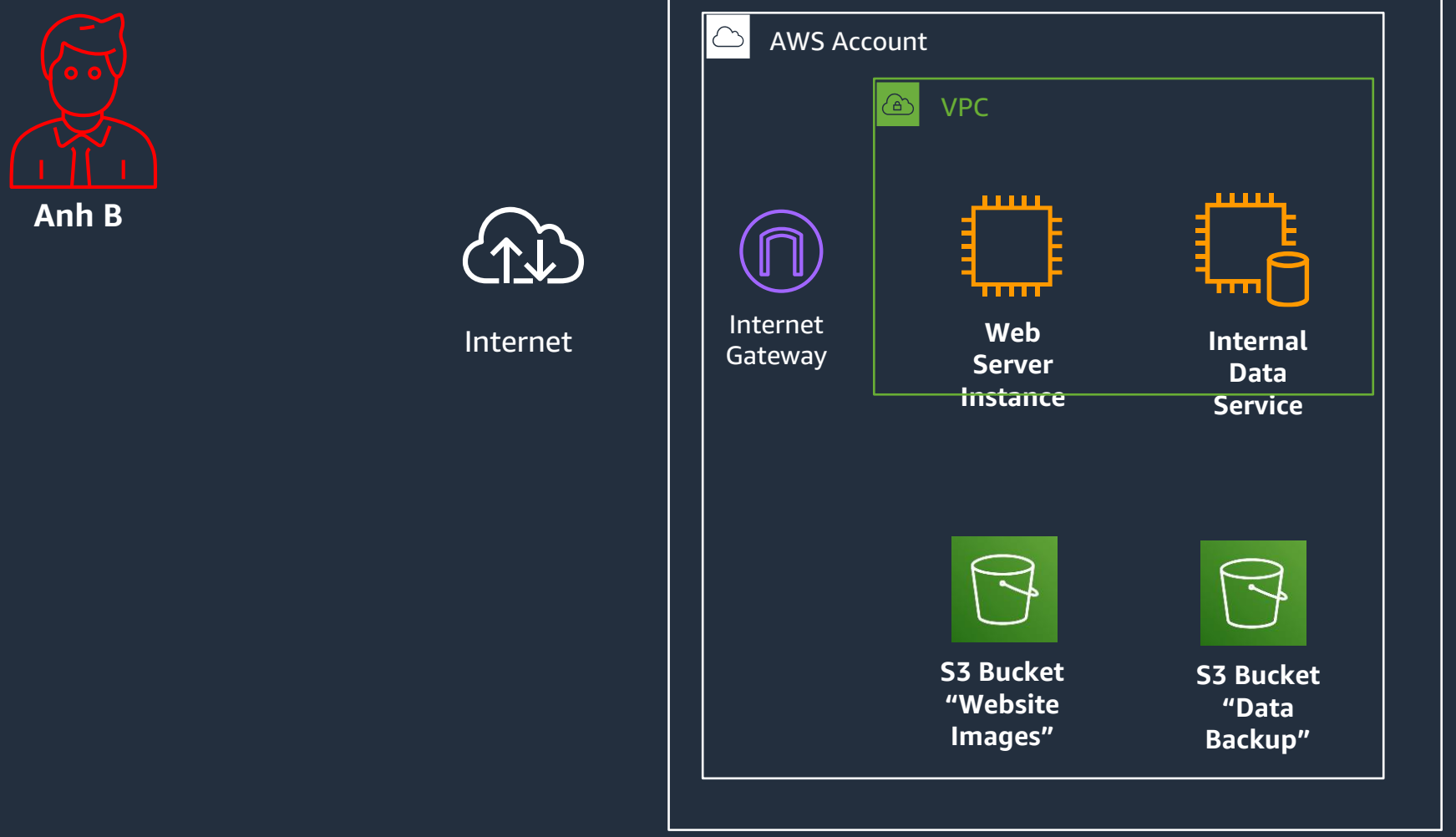
CHỊ A

KHÔNG tuân thủ AWS best-practices

ANH B

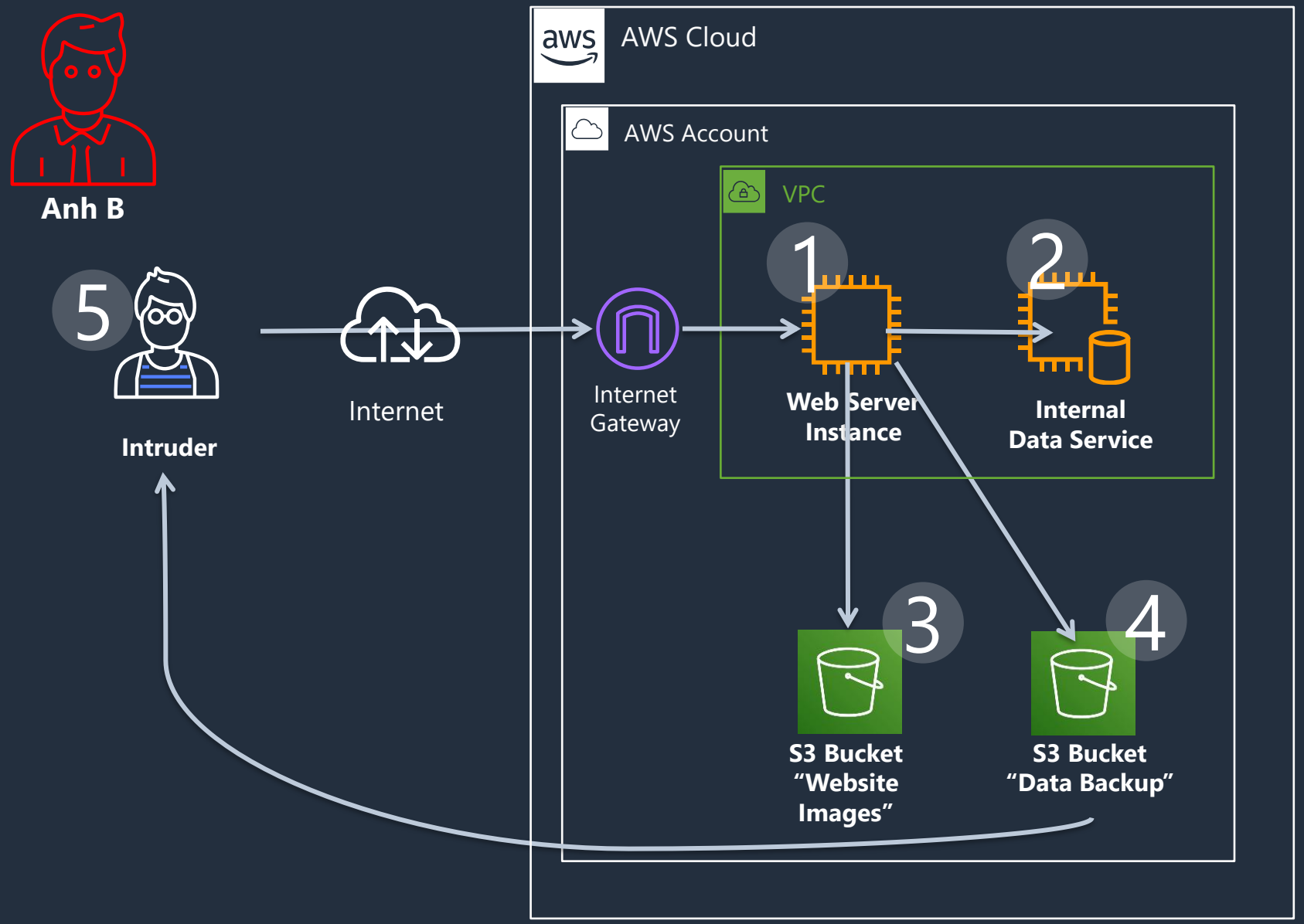
Anh B đã có một ngày tồi tệ!

CMC TELECOM



Anh B đã có một ngày tồi tệ!

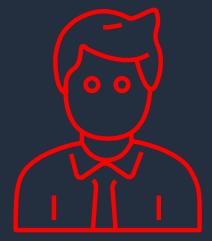
CMC TELECOM



1. Truy cập vào ứng dụng web có lỗ hổng
2. Truy cập vào hệ thống dữ liệu nội bộ
3. Xóa file image của website
4. Thay đổi quyền sao lưu dữ liệu
5. Download dữ liệu backup

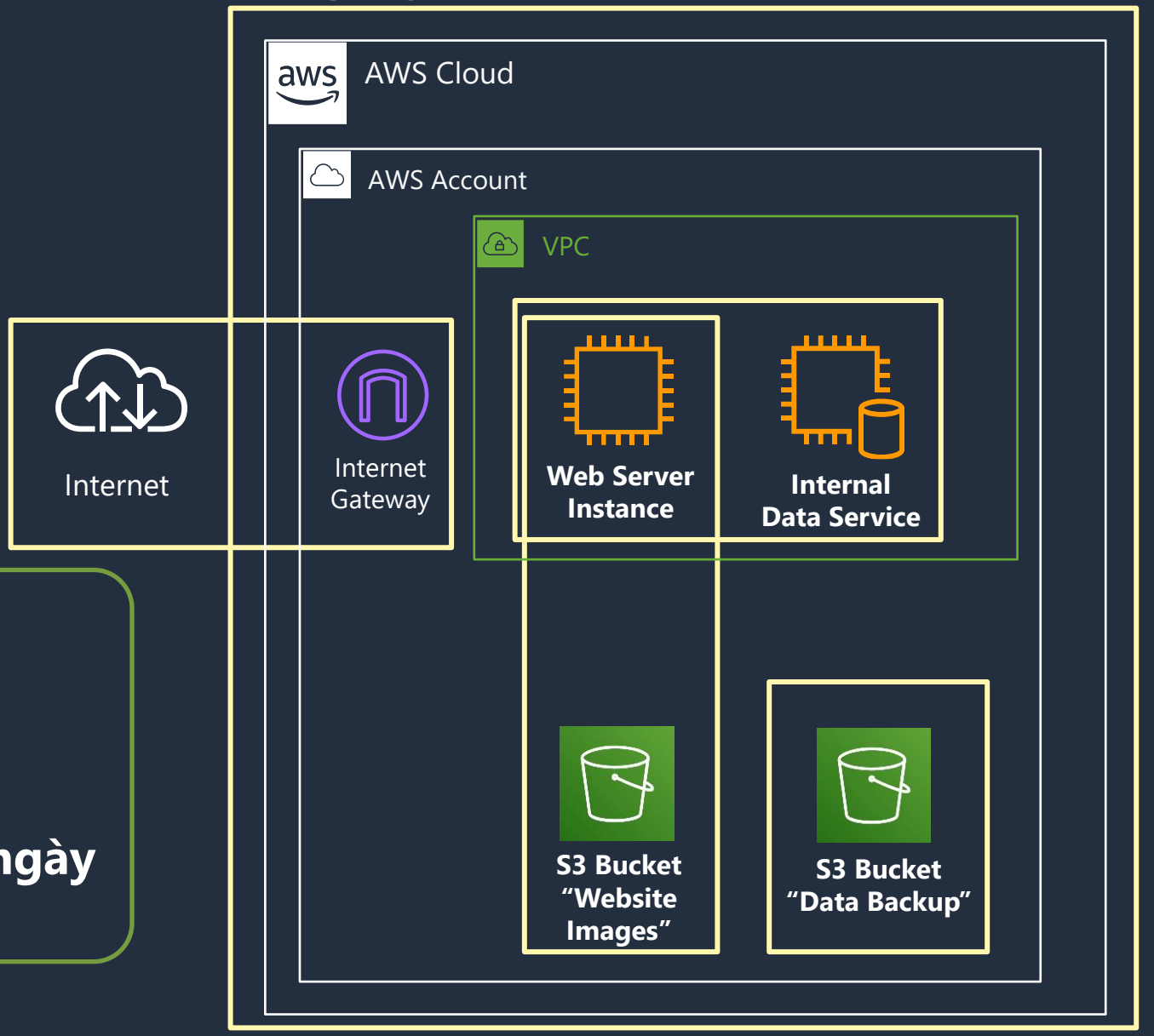
Anh B đã có một ngày tồi tệ!

CMC TELECOM



Anh B

... Chị A có một ngày tuyệt vời!



1. Không bảo vệ ứng dụng web
2. Không phân vùng các thành phần
3. Sử dụng 1 account duy nhất
4. Cấp tất cả các quyền cho users
5. Dữ liệu nhạy cảm không được mã hóa
6. Không ghi nhật kí, theo dõi, cảnh báo

Best Practices: Quản lý định danh và truy cập

CMC TELECOM

1) Sử dụng nhiều tài khoản AWS để giảm phạm vi tác động

Mô hình đa tài khoản AWS cung cấp khả năng tách biệt giữa các workloads dựa trên mục đích kinh doanh, giai đoạn phát triển, và các loại dữ liệu khác nhau,...

2) Sử dụng giới hạn quyền và cấp thông tin xác thực tạm thời

IAM roles và thông tin xác thực tạm thời giúp hệ thống không phải quản lý thông tin xác thực dài hạn và người dùng IAM cho từng thực thể yêu cầu truy cập vào một tài nguyên.

3) Liên kết với các dịch vụ định danh hiện có

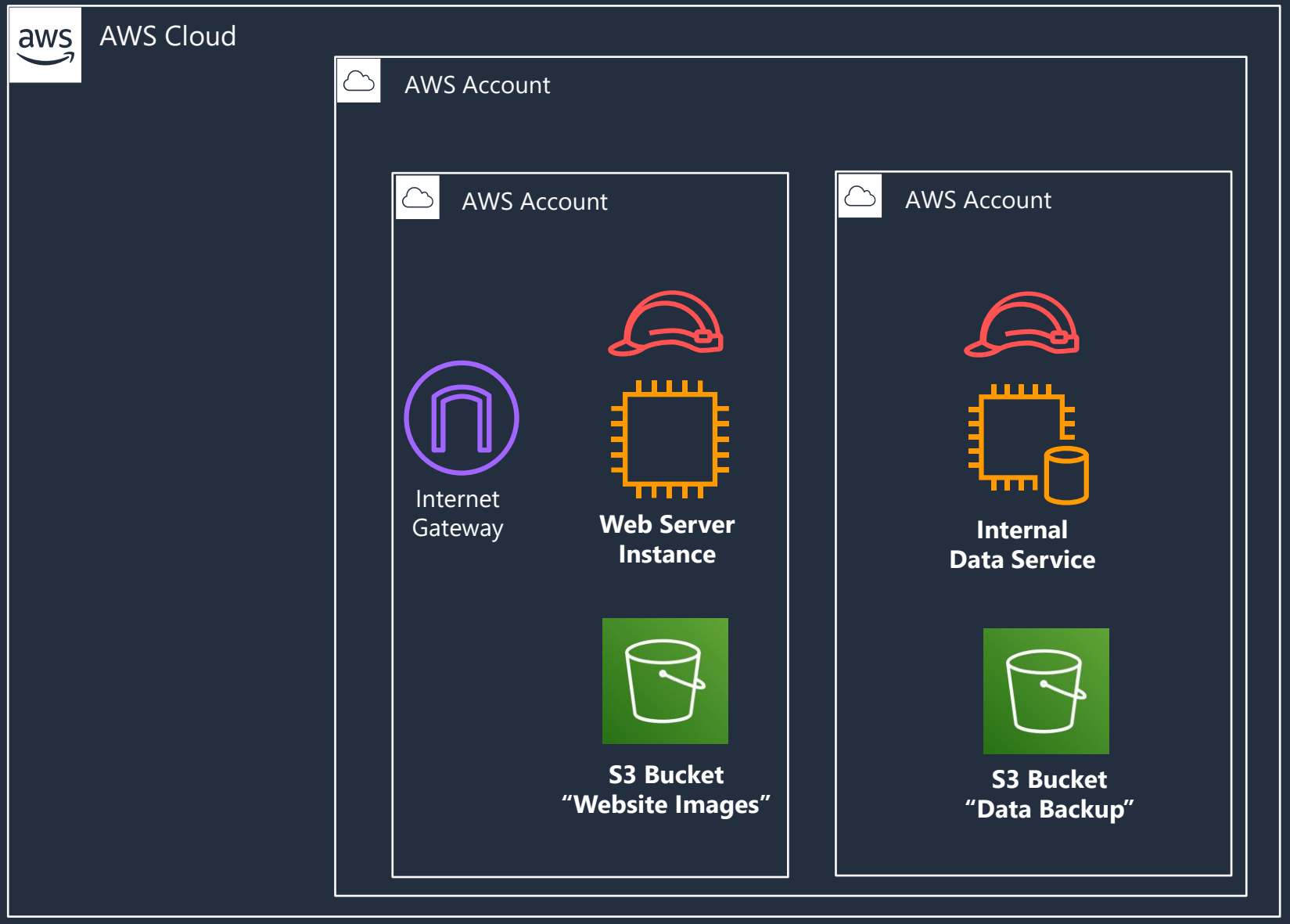
Kiểm soát quyền truy cập vào tài nguyên AWS, quản lý quy trình xác thực và ủy quyền mà không cần tạo lại IAM users cho tất cả người dùng công ty.

Best Practices: Quản lý định danh và truy cập

CMC TELECOM

Chị A

Internet



AWS IAM Identity Center

MFA token

1

IAM

Secrets Manager

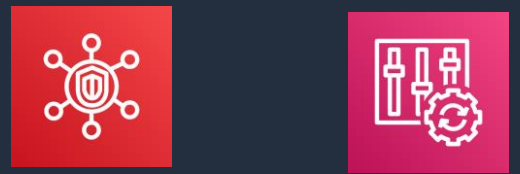
Best Practices: Ghi nhật ký và giám sát

CMC TELECOM

4) Bật ghi nhật ký trên mọi tài khoản, mọi dịch vụ, mọi regions

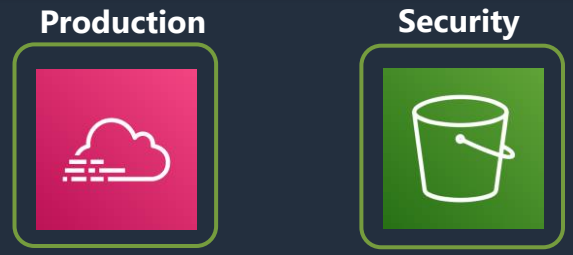
Lịch sử AWS API trong CloudTrail đảm bảo tính bảo mật, theo dõi thay đổi tài nguyên và kiểm tra tuân thủ. GuardDuty cung cấp thông tin và phát hiện mối đe dọa của hệ thống.

5) Sử dụng các tính năng giám sát và cảnh báo tích hợp trên nền tảng AWS



Việc giám sát nhiều tài nguyên sẽ đảm bảo phát hiện được những sự cố mà khách hàng không mong muốn. Thiết lập cảnh báo và thông báo khi có hoạt động bất thường trên các tài khoản.

6) Sử dụng tài khoản AWS riêng để lưu trữ bản sao của tất cả nhật ký



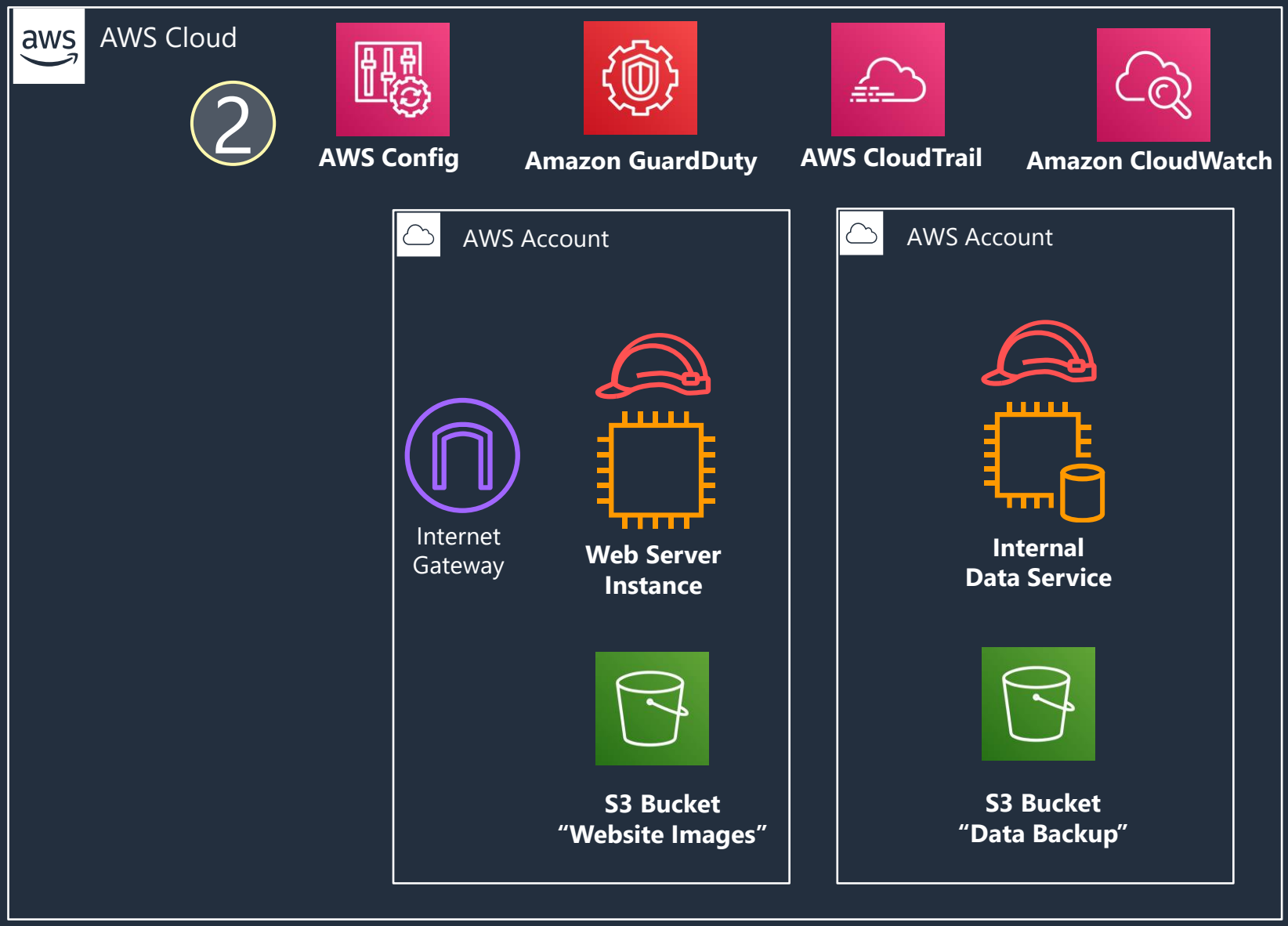
Việc định cấu hình tài khoản bảo mật để sao chép nhật ký vào một nhóm riêng biệt sẽ đảm bảo quyền truy cập vào thông tin nhật ký trong quy trình ứng phó sự cố bảo mật.

Best Practices: Ghi nhật ký và giám sát

CMC TELECOM

Chị A

Internet



AWS IAM Identity Center

MFA token

1

IAM

Secrets Manager

Best Practices: Bảo mật hạ tầng hệ thống

CMC TELECOM

7) Tạo lớp ngăn chặn mối đe dọa bằng cách sử dụng các dịch vụ biên của AWS

Amazon CloudFront

AWS Shield

AWS WAF

Sử dụng PoPs trên toàn thế giới để cung cấp khả năng mở rộng, bảo vệ khỏi các cuộc tấn công DDoS, các cuộc tấn công ứng dụng web.

8) Tạo các vùng mạng với Amazon VPC và các nhóm bảo mật Security Group

Triển khai các biện pháp kiểm soát bảo mật ở ranh giới của máy chủ và mạng ảo trong môi trường AWS Cloud để thực thi các chính sách truy cập, giảm thiểu mối đe dọa về bảo mật đến tài nguyên hệ thống

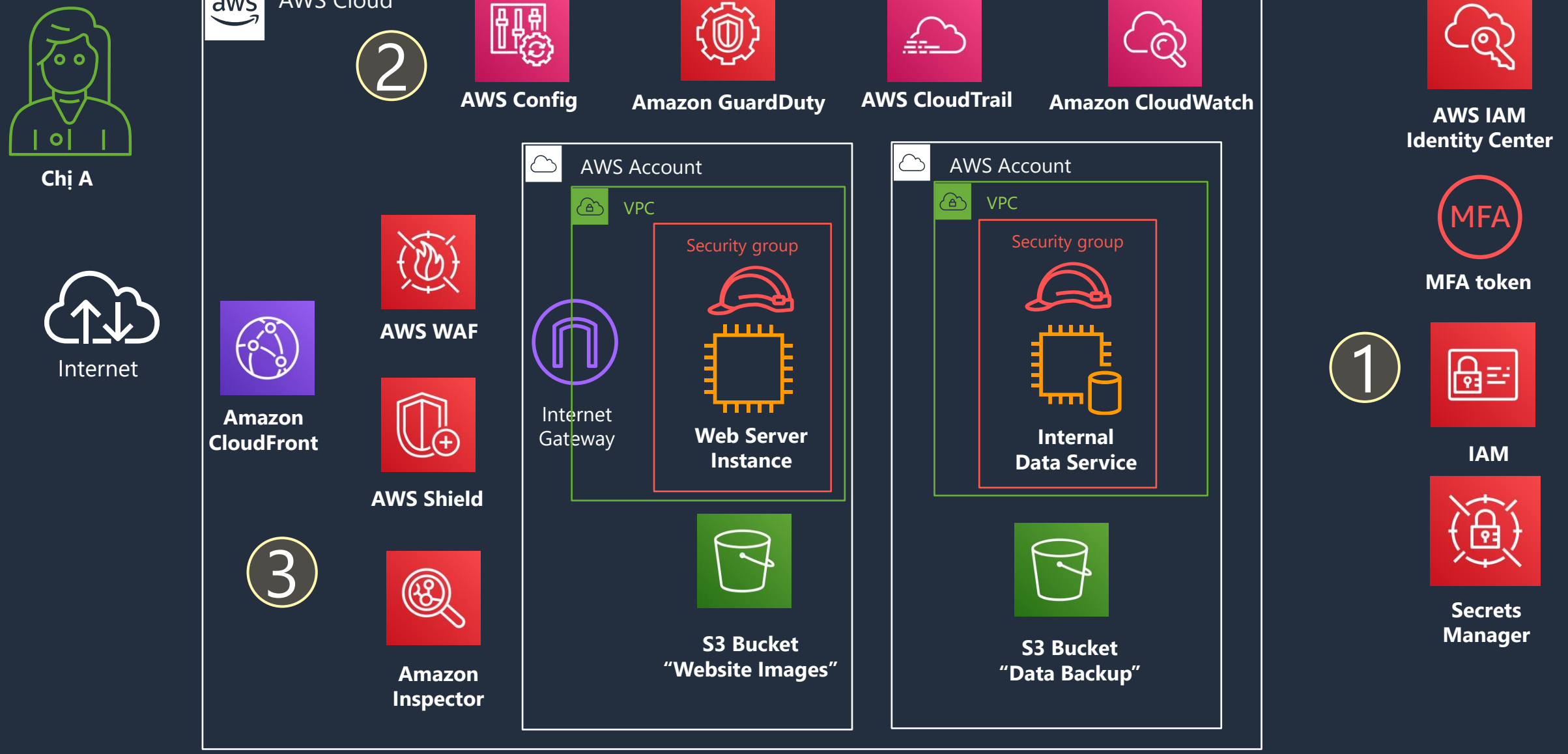
9) Quản lý lỗ hổng bảo mật thông qua vá và quét tài nguyên

Amazon Inspector

Kiểm tra machine image và snapshots của máy ảo để tìm các lỗ hổng hệ điều hành và ứng dụng trong quá trình xây dựng, vận hành hệ thống.

Best Practices: Bảo mật hạ tầng hệ thống

CMC TELECOM



CMC TELECOM

Bảo vệ an toàn dữ liệu trên AWS

Dữ liệu là Trung tâm

CMC TELECOM

Phân loại dữ liệu

- Xác định loại dữ liệu
- Tự động nhận dạng dữ liệu nhạy cảm
- Quản lý vòng đời dữ liệu

Bảo mật dữ liệu khi vận chuyển

- Quản lý khóa và chứng chỉ
- Thực hiện mã hóa khi vận chuyển
- Tự động phát hiện truy cập trái phép
- Xác thực kết nối mạng

Bảo mật dữ liệu khi lưu trữ

- Quản lý khóa an toàn
- Mã hóa khi lưu trữ
- Kiểm soát quyền truy cập

Các nhóm dịch vụ bảo mật & tuân thủ AWS

CMC TELECOM

Quản lý định danh và truy cập

AWS Identity and Access Management (IAM)

AWS Single Sign-On

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Kiểm soát, phát hiện rủi ro

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender

Bảo vệ cơ sở hạ tầng

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

AWS Systems Manager

Bảo vệ dữ liệu

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Server-Side Encryption

Ứng phó sự cố

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

AWS Elastic Disaster Recovery

Quản lý tuân thủ

AWS Artifact

AWS Audit Manager

Amazon CloudWatch

AWS CloudTrail

AWS Config

AWS Security Hub

AWS Systems Manager

Phân loại dữ liệu

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Dữ liệu là Trung tâm

CMC TELECOM

Phân loại dữ liệu

- Xác định loại dữ liệu
- Tự động nhận dạng dữ liệu nhạy cảm
- Quản lý vòng đời dữ liệu

Bảo mật dữ liệu khi vận chuyển

- Quản lý khóa và chứng chỉ
- Thực hiện mã hóa khi vận chuyển
- Tự động phát hiện truy cập trái phép
- Xác thực kết nối mạng

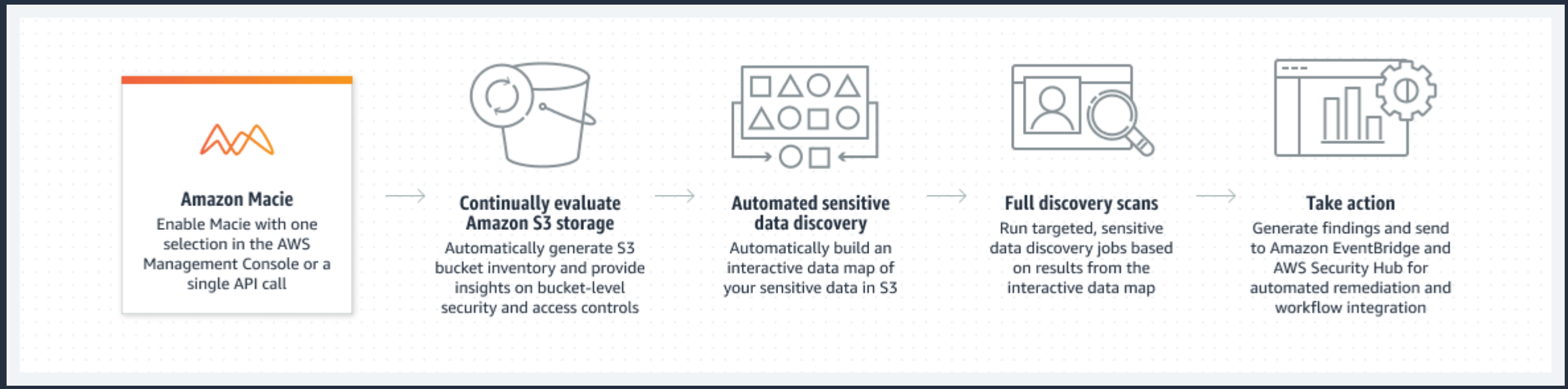
Bảo mật dữ liệu khi lưu trữ

- Quản lý khóa an toàn
- Mã hóa khi lưu trữ
- Kiểm soát quyền truy cập

Amazon Macie

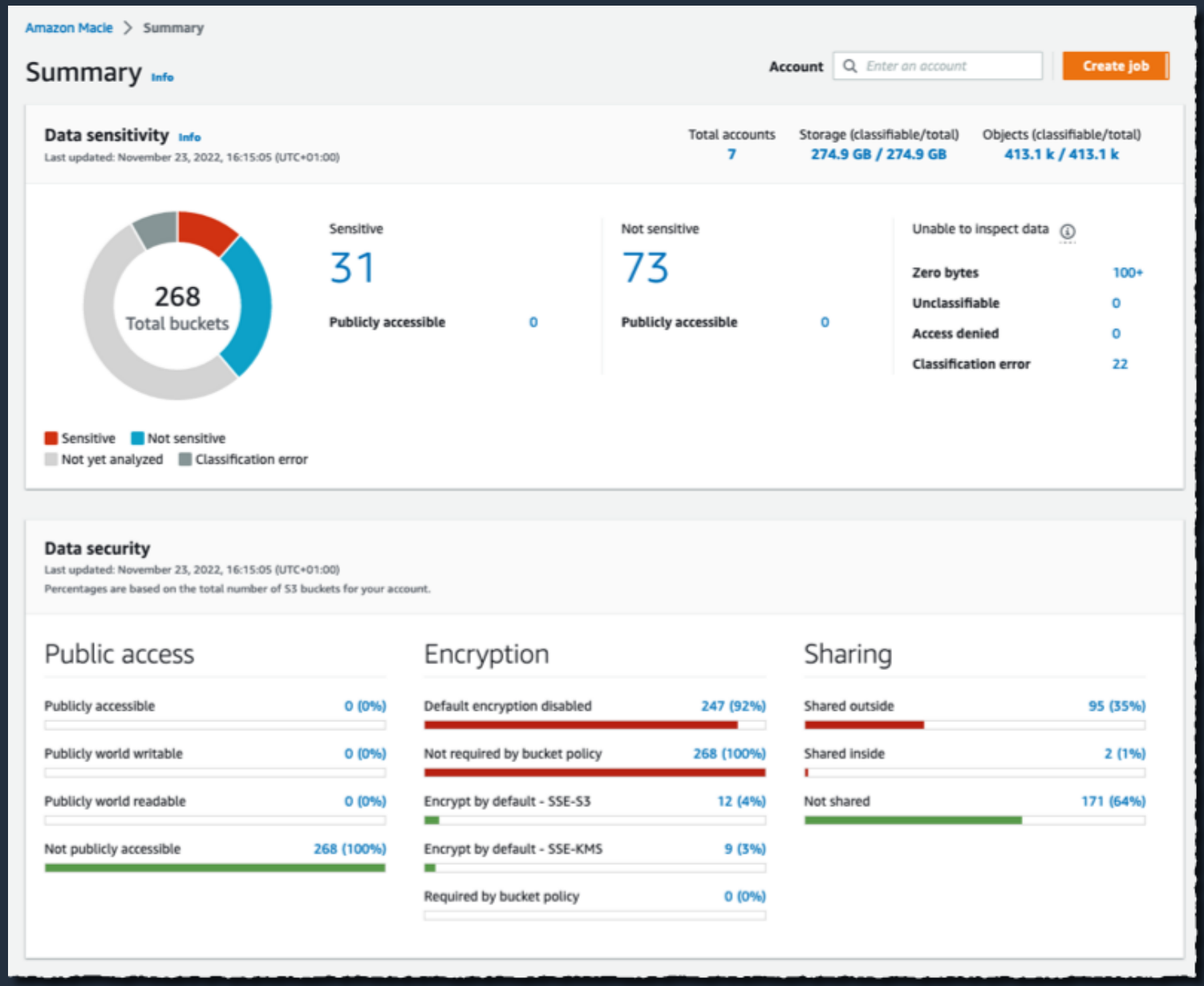
CMC TELECOM

Amazon Macie là dịch vụ bảo mật dữ liệu, sử dụng các kỹ thuật máy học (ML) và so khớp mẫu để phát hiện và giúp bảo vệ dữ liệu nhạy cảm của bạn.



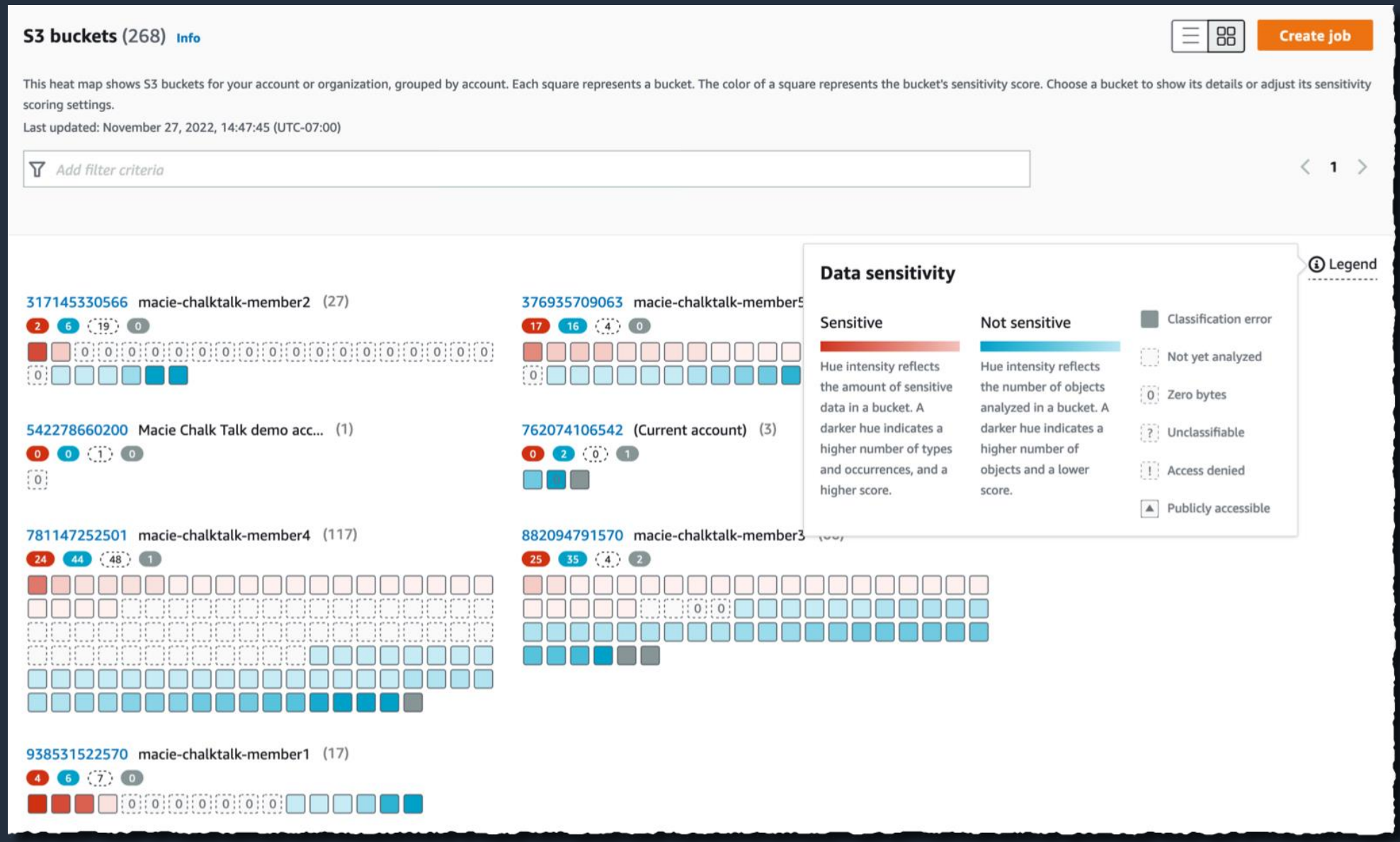
Amazon Macie

CMC TELECOM



Amazon Macie

CMC TELECOM



Bảo mật dữ liệu khi vận chuyển

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Dữ liệu là Trung tâm

CMC TELECOM

Phân loại dữ liệu

- Xác định loại dữ liệu
- Tự động nhận dạng dữ liệu nhạy cảm
- Quản lý vòng đời dữ liệu

Bảo mật dữ liệu khi vận chuyển

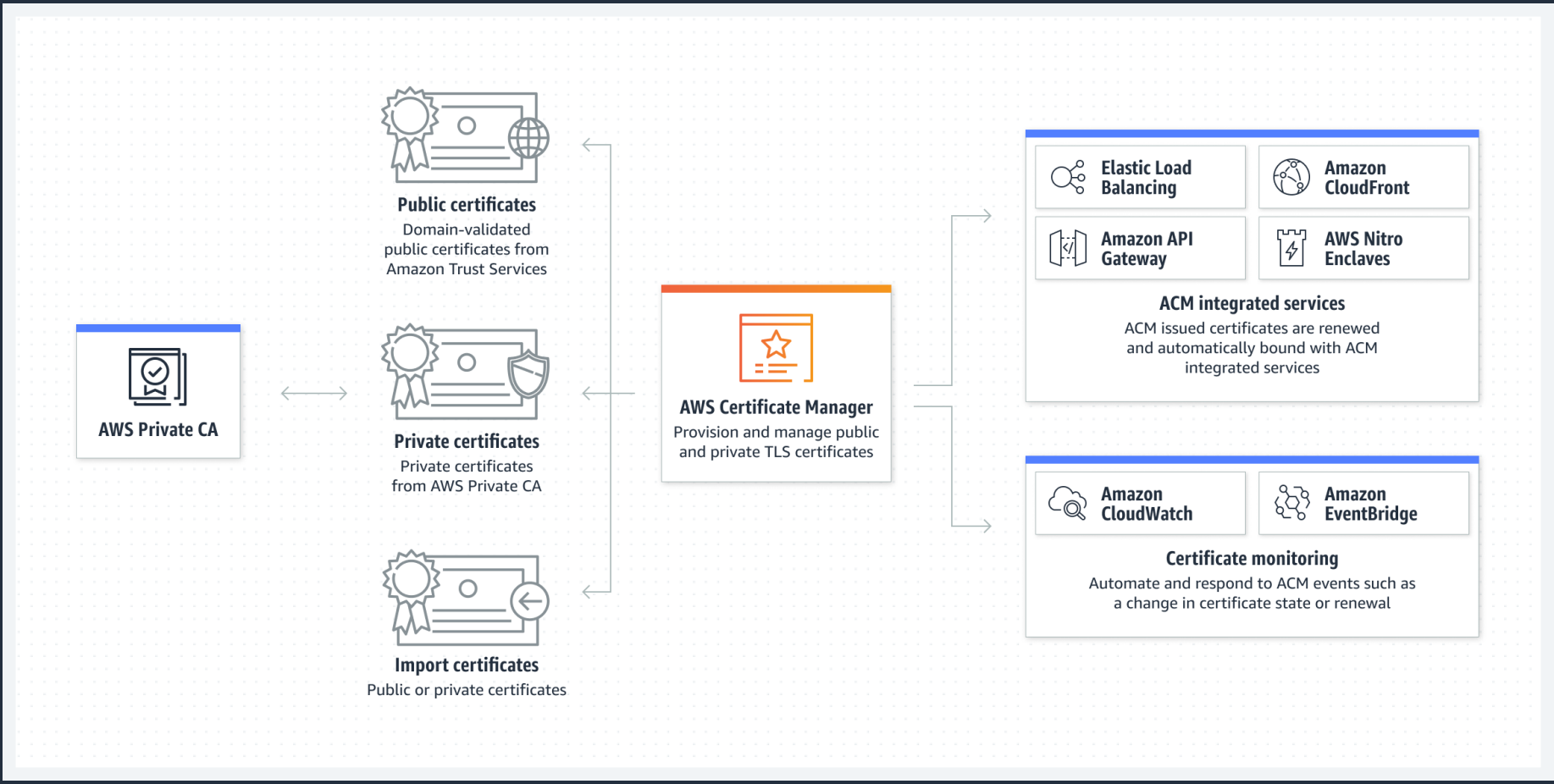
- Quản lý khóa và chứng chỉ
- Thực hiện mã hóa khi vận chuyển
- Tự động phát hiện truy cập trái phép
- Xác thực kết nối mạng

Bảo mật dữ liệu khi lưu trữ

- Quản lý khóa an toàn
- Mã hóa khi lưu trữ
- Kiểm soát quyền truy cập

AWS Certificate Manager

Trình quản lý chứng chỉ của AWS (ACM) cung cấp, quản lý cũng như triển khai các chứng chỉ SSL/TLS riêng và công khai để sử dụng với các dịch vụ AWS cũng như tài nguyên kết nối nội bộ của bạn.



Bảo mật dữ liệu khi lưu trữ

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Dữ liệu là Trung tâm

CMC TELECOM

Phân loại dữ liệu

- Xác định loại dữ liệu
- Tự động nhận dạng dữ liệu nhạy cảm
- Quản lý vòng đời dữ liệu

Bảo mật dữ liệu khi vận chuyển

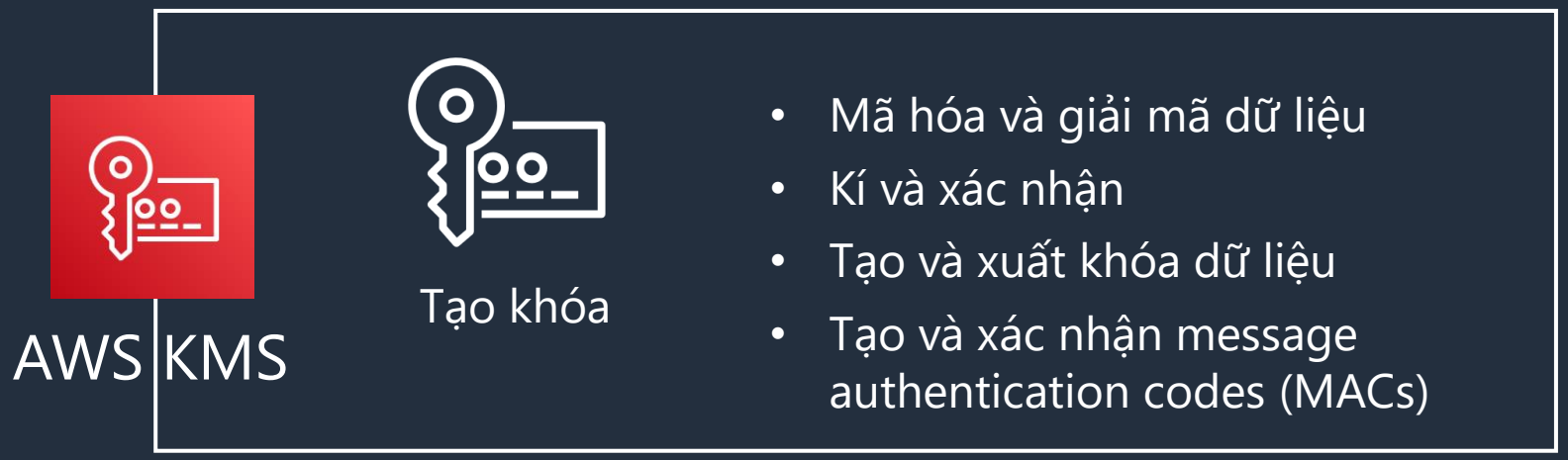
- Quản lý khóa và chứng chỉ
- Thực hiện mã hóa khi vận chuyển
- Tự động phát hiện truy cập trái phép
- Xác thực kết nối mạng

Bảo mật dữ liệu khi lưu trữ

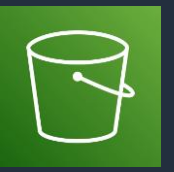
- Quản lý khóa an toàn
- Mã hóa khi lưu trữ
- Kiểm soát quyền truy cập

AWS KMS

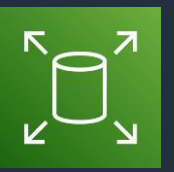
AWS Key Management Service cho phép tạo, quản lý và kiểm soát khóa mật mã trên các ứng dụng của bạn và các dịch vụ của AWS.



Tích hợp với các dịch vụ


Amazon S3


Amazon EC2


Amazon EBS

Theo dõi khóa KMS


Amazon CloudWatch

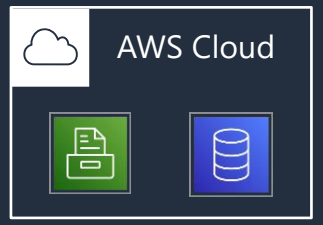

AWS CloudTrail

AWS hỗ trợ khách hàng bảo mật dữ liệu thế nào?

"Làm thế nào để bảo mật dịch chuyển dữ liệu lên AWS?"

Mã hóa dữ liệu nguồn khi dịch chuyển

AWS Certificate Manager cho chứng chỉ SSL/TLS



"Làm thế nào để bảo mật dữ liệu trên AWS?"

Mã hóa dữ liệu ở phía server khi lưu trữ

AWS KMS và CloudHSM để quản lý khóa cho doanh nghiệp

"Làm thế nào để chia sẻ dữ liệu và tài nguyên an toàn trên cloud?"

AWS Identity and Access Management – Cross-Account Access

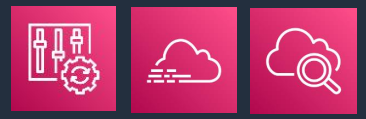
"Làm thế nào để quản lý xác thực và ủy quyền?"

- Well-Architected Review
- Triển khai trên nhiều Regions
- Cryptographic SDKs để mã hóa ứng dụng
- Multi-Region Keys để khôi phục khi có sự cố

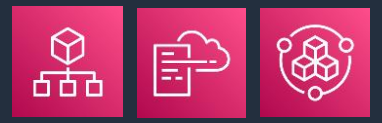
"Làm thế nào để tối ưu chi phí và hiệu năng?"

"Làm thế nào để kiến trúc đảm bảo tính sẵn sàng?"

"Làm thế nào để mở rộng?"



Các dịch vụ Quản trị đám mây của AWS



"Làm thế nào để chứng minh tính bảo mật và tuân thủ?"

AWS IAM và Secrets Manager để quản lý danh tính và thông tin xác thực

CMC TELECOM

Q&A

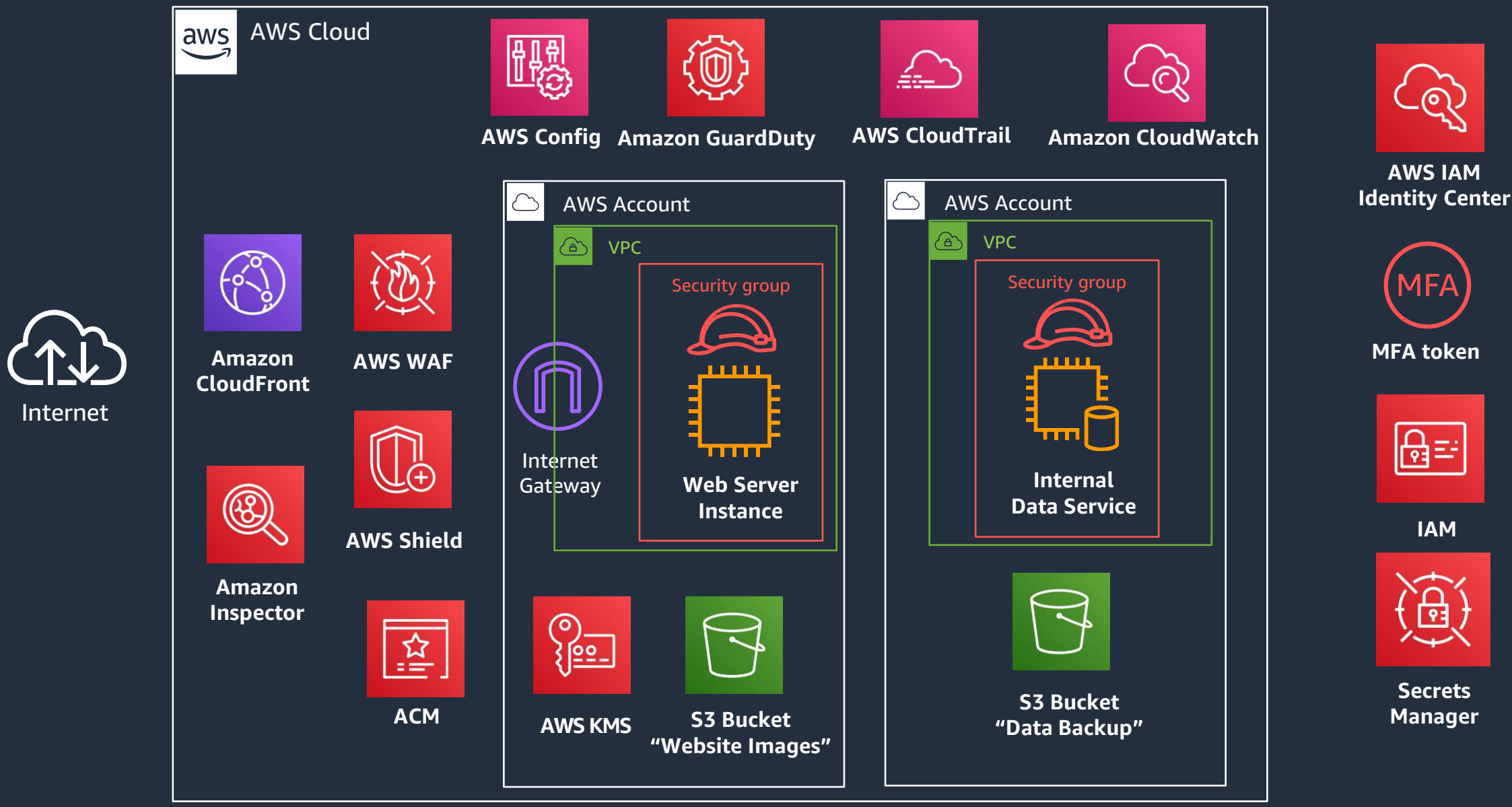
CMC TELECOM

Feedback

https://bit.ly/sec-webinar2

Key Takeaways

CMC TELECOM



AWS IAM Identity Center

MFA token

IAM

Secrets Manager

Next Steps

CMC TELECOM

CMC TELECOM | aws

Webinar Series

Bảo mật AWS
từ cơ sở hạ tầng đến ứng dụng

Từ 24/05 đến 14/06/2024

09h15 - 11h30

Miễn phí qua GoToWebinar

CMC TELECOM

CMC Telecommunication Infrastructure Corporation

Thank you !

Ha Noi 28/7/2023