Training Section

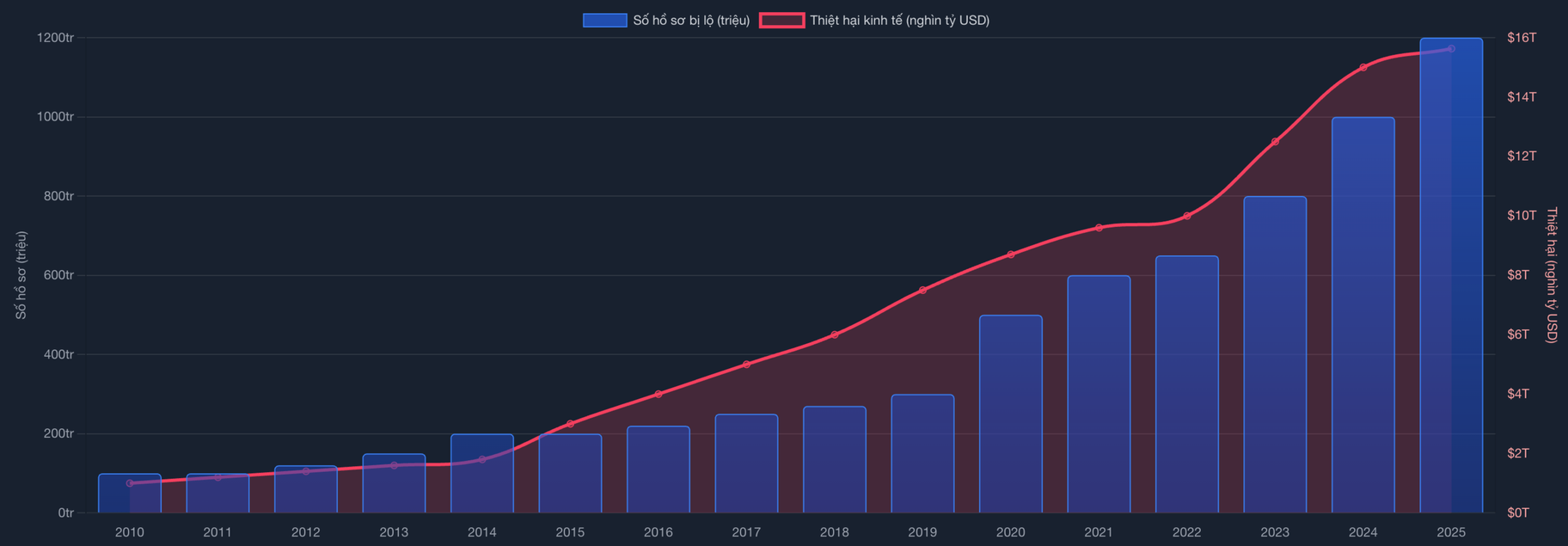
AWS Security Fundamental

Trainer: TamLH | Date: Sep 20, 2025

Phân Tích An Ninh Mạng: Quá khứ & Tương lai

Những bài học xương máu và xu hướng đáng báo động của ngành.

Xu Hướng Tấn Công Mạng Toàn Cầu (2010-2025)



Nguồn dữ liệu: Sectigo, Cobalt.io, FBI IC3 Reports.

Phân tích các sự cố điển hình

Capital One (2019) | Dow Jones (2017) | Codecov (2021) | CIC Vietnam (2025)

$ Capital One: Lỗ hổng từ đặc quyền

Nguyên nhân

Kẻ tấn công khai thác một **lỗ hổng trên Web Application Firewall (WAF)** đã bị cấu hình sai...

Bài học

Nguyên tắc Đặc quyền Tối thiểu là then chốt...

Shared Responsibility Model - AWS

An ninh trên Đám mây: Ai chịu trách nhiệm cho việc gì?

Trách nhiệm CỦA AWS

Bảo mật **CỦA** Đám mây (Security OF the Cloud)

Hạ tầng Toàn cầu & Phần cứng
Quản lý và bảo mật Regions, Availability Zones, Edge Locations, và toàn bộ phần cứng vật lý.

An ninh Vật lý
Bảo vệ các trung tâm dữ liệu (data centers) khỏi các truy cập trái phép trên thực địa.

Hạ tầng Mạng & Ảo hóa
Chịu trách nhiệm cho network fabric, hypervisor (lớp ảo hóa), và an ninh tại các điểm của CloudFront.

Dịch vụ Được quản lý (Managed Services)
AWS quản lý lớp hệ điều hành và nền tảng cho các dịch vụ như RDS, Lambda, S3.

Trách nhiệm CỦA KHÁCH HÀNG

Bảo mật **TRONG** Đám mây (Security IN the Cloud)

Dữ liệu & Mã hóa
Chịu trách nhiệm mã hóa dữ liệu cả phía máy khách (client-side) và phía máy chủ (server-side).

Nền tảng, Ứng dụng & IAM
Quản lý định danh và quyền truy cập (IAM), bảo mật ứng dụng và mã nguồn.

Hệ điều hành & Tường lửa
Cài đặt, vá lỗi hệ điều hành (trên EC2), và cấu hình tường lửa mạng (Security Groups, NACLs).

Cấu hình Dịch vụ
Chịu trách nhiệm cấu hình đúng cách các dịch vụ như CloudFront, Security Groups, S3 Buckets.

Tóm lại: **AWS** chịu trách nhiệm bảo vệ hạ tầng đám mây. **Bạn** chịu trách nhiệm bảo vệ bất cứ thứ gì bạn đưa lên hoặc xây dựng trên đám mây đó.

Tại sao AWS Security quan trọng?

Identity and Access Management (IAM)

Người bảo vệ kỹ thuật số cho tài khoản AWS của bạn.

IAM hoạt động như thế nào?

Hãy xem IAM như một **"Người bảo vệ Kỹ thuật số"**. Người bảo vệ này làm hai việc chính:

- **Xác thực (Authentication):** Kiểm tra danh tính, đảm bảo "bạn là người bạn nói".
- **Ủy quyền (Authorization):** Kiểm tra xem bạn có trong danh sách được phép làm một việc gì đó hay không.

Câu hỏi Cốt lõi của IAM

Mọi chính sách IAM đều được thiết kế để trả lời câu hỏi duy nhất:

Ai (Who) được làm gì (What) trên tài nguyên nào (Which Resource) và trong điều kiện nào (Under Which Conditions)?

🔑 Fine-grained Access Control

Cung cấp khả năng kiểm soát chi tiết đến từng hành động (action) trên từng tài nguyên (resource).

Mục tiêu chính: Thực thi **Nguyên tắc Đặc quyền Tối thiểu**, đảm bảo người dùng và ứng dụng chỉ có những quyền họ thực sự cần.

🛡️ Multi-factor Authentication

Thêm một lớp bảo vệ thứ hai ngoài mật khẩu, yêu cầu một mã xác thực từ thiết bị vật lý hoặc ứng dụng.

Mục tiêu chính: Bảo vệ danh tính (cái "Who") một cách mạnh mẽ nhất, chống lại việc mật khẩu hoặc access key bị đánh cắp.

🔄 Identity Federation

Cho phép người dùng từ các hệ thống quản lý danh tính khác (như Active Directory, Google Workspace) truy cập AWS.

Mục tiêu chính: Giúp nhân viên sử dụng **một danh tính duy nhất**, giảm thiểu rủi ro và đơn giản hóa quản lý.

📊 Access Analysis

Các công cụ như IAM Access Analyzer giúp bạn phân tích, xác minh và tinh chỉnh các quyền truy cập trong tài khoản.

Mục tiêu chính: Liên tục kiểm tra và chứng minh rằng bạn đang tuân thủ các quy tắc an ninh và Nguyên tắc Đặc quyền Tối thiểu.

Các Thành Phần Cốt Lõi của AWS IAM

Hiểu rõ Users, Groups, Roles và Policies để xây dựng một nền tảng đám mây an toàn.

🎯 Nguyên tắc Vàng: Đặc quyền Tối thiểu (Least Privilege)

"Chỉ cấp những quyền hạn thực sự cần thiết để thực hiện công việc, và không hơn không kém."
Mọi công cụ dưới đây đều nhằm mục đích thực thi nguyên tắc này.

👤 Users

Đại diện cho một **con người** hoặc một **ứng dụng** cần tương tác với AWS.

- Có credentials dài hạn (mật khẩu, access keys).
- Gán quyền trực tiếp hoặc thông qua Groups.
- Nên tạo user riêng cho mỗi người.

Quy tắc An toàn

⚠️ **KHÔNG**dùng Root User cho công việc hàng ngày.

✅ **BẮT BUỘC**kích hoạt Bảo mật Đa yếu tố (MFA).

👥 Groups

Là một tập hợp các IAM Users, giúp đơn giản hóa việc quản lý quyền cho **nhiều người**.

- Gán quyền cho Group, tất cả user trong Group sẽ có quyền đó.
- Một user có thể thuộc nhiều Group.
- Ví dụ: `Developers`, `Admins`, `DataScientists`.
- Không thể chứa Roles, chỉ chứa Users.

Mục đích chính

Quản lý quyền cho **con người** một cách hiệu quả và có tổ chức.

🎭 Roles

Cung cấp một danh tính với các quyền hạn cụ thể mà **dịch vụ AWS** hoặc **ứng dụng** có thể "đảm nhận".

- Sử dụng credentials **tạm thời**, tự động xoay vòng.
- An toàn hơn nhiều so với access keys dài hạn.
- Dùng cho EC2, Lambda, truy cập cross-account...
- Là best practice cho mọi ứng dụng trên AWS.

Tại sao ưu tiên?

Loại bỏ hoàn toàn nhu cầu lưu trữ access key trong mã nguồn, giảm thiểu rủi ro bị lộ thông tin nhạy cảm.

📜 Policies

Là các văn bản JSON, định nghĩa chi tiết các **quyền hạn** ("Allow" hoặc "Deny").

- Là "bộ luật" được gắn vào Users, Groups, và Roles.
- Xác định hành động nào được phép trên tài nguyên nào.
- Có thể do AWS quản lý hoặc do bạn tự tạo.

Ví dụ: S3 Read-Only

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-bucket/
    }
  ]
}
```

Principle of Least Privilege (PoLP)

Nguyên tắc nền tảng để xây dựng một hệ thống an toàn và vững chắc.

🎯 Định nghĩa

Chỉ cấp cho người dùng hoặc hệ thống những quyền hạn **tối thiểu, vừa đủ** để họ hoàn thành công việc được giao.

💥 Mục tiêu Cốt lõi

Giảm thiểu **"Bán kính ảnh hưởng" (Blast Radius)**. Khi một tài khoản bị xâm phạm, thiệt hại sẽ được giới hạn trong phạm vi quyền hạn nhỏ nhất có thể.

🏨 Phép so sánh: Chìa khóa Thẻ từ Khách sạn

👤 Khách

Chỉ mở được phòng của mình và các khu vực chung (hồ bơi, gym).

🧹 Nhân viên Dọn phòng

Mở được các phòng trên tầng được giao trong ca làm việc.

👑 Quản lý

Mở được tất cả các phòng và khu vực vận hành.

IAM cũng hoạt động tương tự, mỗi người chỉ có "chìa khóa" cho những "căn phòng" (tài nguyên) mà họ thực sự cần.

🔄 Best practice

1 Bắt đầu Tối thiểu

Luôn bắt đầu bằng một chính sách không có quyền nào cả (deny-all) và chỉ thêm các quyền thực sự cần thiết.

2 Cấp thêm khi cần

Khi có yêu cầu mới, chỉ cấp thêm quyền cụ thể cho tác vụ đó. Sử dụng **IAM Policy Simulator** để kiểm tra chính sách trước khi áp dụng.

3 Xem xét Định kỳ

Thường xuyên rà soát lại các quyền đã cấp. Dùng **Access Advisor** để xem quyền ít dùng và **CloudTrail** để phân tích việc sử dụng quyền trong thực tế.

4 Loại bỏ Quyền thừa

Gỡ bỏ các quyền không còn được sử dụng. Dùng **Access Analyzer** để tự động phát hiện các quyền hạn quá rộng hoặc không an toàn.

Root Account Best Practices

Cách bảo vệ "chìa khóa vạn năng" cho vương quốc AWS của bạn.

⚠ Cảnh báo: Tài khoản Quyền lực Tối cao

Tài khoản Root có quyền **không giới hạn**, không thể bị cản trở bởi bất kỳ chính sách IAM nào. Coi nó như một tài khoản "God Mode" - cực kỳ mạnh mẽ và cũng cực kỳ nguy hiểm nếu bị xâm phạm.

Lộ trình An toàn 3 Bước

Bước 1: BẢO VỆ (SECURE IT)

Hành động ngay lập tức để gia cố tài khoản Root.

- ✅ **Bật Xác thực Đa yếu tố (MFA):** Đây là hành động quan trọng nhất, không thể trì hoãn.
- ✅ **Tạo Mật khẩu Cực mạnh:** Dùng một mật khẩu dài, phức tạp và duy nhất.
- ✅ **Xóa toàn bộ Access Keys:** Root user không bao giờ được phép truy cập bằng mã lệnh (programmatic access).

Bước 2: THAY THẾ (REPLACE IT)

Tạo một tài khoản thay thế cho các công việc quản trị hàng ngày.

- ✅ **Tạo một IAM User riêng:** Đặt tên là `admin` hoặc tên của bạn.
- ✅ **Gán quyền AdministratorAccess:** Cấp cho user này quyền quản trị cần thiết.
- ✅ **Bật MFA cho IAM User này:** Tài khoản admin cũng cần được bảo vệ tối đa.

Bước 3: CẤT ĐI & GIÁM SÁT (LOCK IT AWAY & MONITOR)

Không sử dụng tài khoản Root nữa và thiết lập cơ chế cảnh báo.

- ✅ **Cất giữ thông tin đăng nhập an toàn:** Lưu trữ mật khẩu và thiết bị MFA ở nơi an toàn (như két sắt).
- ✅ **Sử dụng IAM User cho mọi việc:** Đăng xuất khỏi Root và chỉ dùng tài khoản admin đã tạo.
- ✅ **Thiết lập cảnh báo đăng nhập:** Dùng CloudTrail và CloudWatch/SNS để nhận email thông báo mỗi khi có ai đó đăng nhập bằng Root.

Khi nào thì thực sự cần dùng Root?

Chỉ đăng nhập vào Root user để thực hiện một số tác vụ đặc biệt mà IAM user không thể làm:

- 🔑 Thay đổi thông tin tài khoản (email, password).
- 🔑 Thay đổi Gói hỗ trợ (Support Plan).
- 🔑 Đăng ký làm GovCloud user.
- 🔑 Đóng tài khoản AWS.
- 🔑 Xem một số thông tin thuế (tax invoices).
- 🔑 Cấu hình S3 Object Lock cho bucket.

VPC Security Overview

🌐 **Virtual Private Cloud (VPC)**

Mạng ảo riêng biệt trong AWS Cloud của bạn

🛡️

Security Groups

Virtual firewall cho EC2 instances

Stateful - tự động allow return traffic

Instance level protection

Default: deny all inbound, allow all outbound

🚧

Network ACLs

Subnet level firewall

Stateless - phải cấu hình cả chiều

Subnet level protection

Default: allow all traffic

📊

VPC Flow Logs

Ghi lại network traffic

Monitor network traffic patterns

Security analysis

Troubleshooting connectivity

Security Groups vs Network ACLs

Tính năng	Security Groups	Network ACLs
Phạm vi	Instance level	Subnet level
Stateful/Stateless	Stateful	Stateless
Rules	Chỉ Allow rules	Allow và Deny rules
Rule evaluation	Tất cả rules trước khi quyết định	Theo thứ tự rule number
Default behavior	Deny all inbound, allow outbound	Allow all traffic

💡 **Best Practice:** Sử dụng Security Groups làm primary defense, Network ACLs làm additional layer

Public vs Private Subnets

Public Subnet

Đặc điểm:

- Route table có route đến Internet Gateway
- Instances có thể có Public IP
- Truy cập trực tiếp từ Internet

Sử dụng cho:

- Web servers
- Load balancers
- Bastion hosts
- NAT Gateways

Private Subnet

Đặc điểm:

- Không có route trực tiếp đến IGW
- Chỉ có Private IP
- Internet access qua NAT Gateway/Instance

Sử dụng cho:

- Database servers
- Application servers
- Backend services
- Sensitive workloads

🏗️ Architecture Best Practice

Multi-tier architecture: Web tier (public) → App tier (private) → Database tier (private)

EC2 Security Best Practices

🔐 Access Control

- **IAM Roles:** Sử dụng roles thay vì hardcode credentials
- **Key Pairs:** Secure key management, rotate keys
- **Bastion Hosts:** Centralized SSH access
- **Session Manager:** Browser-based shell access

🛡️ Network Security

- **Security Groups:** Least privilege principle
- **Private Subnets:** Sensitive workloads
- **VPC Endpoints:** Private connectivity to AWS services
- **Disable Source/Destination Check:** Only when needed

💾 Data Protection

- **EBS Encryption:** Encrypt volumes at rest
- **Snapshots:** Encrypted backup strategy
- **Instance Store:** Temporary data only
- **Data in Transit:** TLS/SSL encryption

🔄 Monitoring & Maintenance

- **CloudWatch:** Performance and security metrics
- **CloudTrail:** API call logging
- **Patch Management:** Systems Manager Patch Manager
- **Antivirus:** Third-party solutions

AWS WAF & Shield Introduction

AWS WAF (Web Application Firewall)

Chức năng: Bảo vệ web applications khỏi các cuộc tấn công web

Features:

- SQL injection protection
- Cross-site scripting (XSS) prevention
- Rate limiting
- Geo-blocking
- Custom rules và managed rules

Integration:

CloudFront, Application Load Balancer, API Gateway, AppSync

AWS Shield

Chức năng: DDoS protection service

Shield Standard (Free)

- Basic DDoS protection
- Layer 3/4 attacks
- Always-on detection

Shield Advanced ($3,000/month)

- Enhanced DDoS protection
- Real-time attack notifications
- DDoS Response Team (DRT) support
- Cost protection

Encryption Fundamentals

🔒 Encryption at Rest

Mã hóa dữ liệu khi được lưu trữ

- EBS volumes encryption
- S3 object encryption
- RDS database encryption
- EFS file system encryption

🚀 Encryption in Transit

Mã hóa dữ liệu khi di chuyển

- TLS/SSL for web traffic
- HTTPS for API calls
- VPN connections
- AWS Direct Connect

🔑 Client-side Encryption

Khách hàng mã hóa trước khi gửi lên AWS

- Khách hàng quản lý keys
- Highest level of control
- AWS không thấy plaintext data

☁️ Server-side Encryption

AWS mã hóa sau khi nhận data

- AWS-managed keys (SSE-S3)
- Customer-managed keys (SSE-KMS)
- Customer-provided keys (SSE-C)

AWS KMS Deep Dive

🔐 AWS Key Management Service

Managed service để tạo và kiểm soát encryption keys

🏢 AWS Managed Keys

- Tự động tạo bởi AWS services
- Free to use
- Automatic rotation (3 years)
- Không thể xóa

👤 Customer Managed Keys

- Khách hàng tạo và quản lý
- $1/month per key
- Manual or automatic rotation
- Có thể disable/delete

🎯 Key Policies

Resource-based policies kiểm soát access to keys

🔄 Key Rotation

Automatic rotation để enhance security

📊 CloudTrail Integration

Audit key usage và access patterns

🌐 Multi-Region Keys

Replicate keys across regions

S3 Security & Encryption

🔐 Access Control

IAM Policies
User/role-based permissions

Bucket Policies
Resource-based permissions

ACLs
Object-level permissions (legacy)

Block Public Access
Account/bucket level protection

🔒 Encryption Options

SSE-S3
AWS-managed keys
Free

SSE-KMS
Customer-managed keys
$1/month + API calls

SSE-C
Customer-provided keys
Free

Client-side
Encrypt before upload
Free

🛡️ Additional Security Features

- **MFA Delete:** Require MFA to delete objects
- **Versioning:** Protect against accidental deletion
- **Object Lock:** WORM (Write Once Read Many)
- **Access Logging:** Track requests
- **CloudTrail:** API call logging

AWS CloudFront

Xây dựng một vành đai an ninh vững chắc ở Edge để bảo vệ ứng dụng và dữ liệu của bạn.

Origin Protection
Ngăn chặn truy cập "cửa sau" trực tiếp vào S3 bucket.

Encryption in Transit
Bảo vệ dữ liệu khỏi bị nghe lén khi đang truyền đi.

User Access Control
Bảo vệ nội dung trả phí hoặc riêng tư.

Geographic Restrictions
Giới hạn nội dung ở một số quốc gia nhất định.

Application Layer Protection
Chặn các kỹ thuật tấn công ứng dụng web phổ biến.

Network Layer Protection
Chống lại các cuộc tấn công từ chối dịch vụ (DDoS).

CloudFront Overview & S3 Integration

🌐 **Amazon CloudFront**
Content Delivery Network (CDN) toàn cầu của AWS

🔄 Cách hoạt động

📍
Edge Locations
Hơn 400 điểm kết nối toàn cầu

💾
Cache Content
Lưu trữ tạm thời tại edge gần người dùng

⚡
Reduce Latency
Giảm thời gian tải xuống đáng kể

🤝 S3 Integration

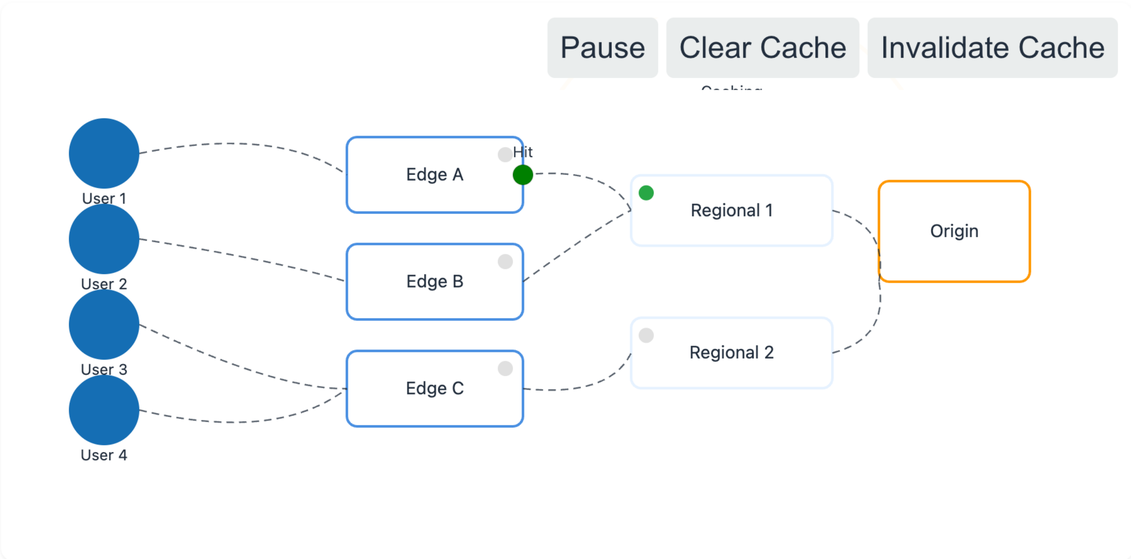
S3 Origin Server
Lưu trữ files gốc (static websites, images, videos)

→

CloudFront CDN
Phân phối content đến users

→

Edge Location
Users truy cập từ location gần nhất



✅ Benefits

🚀 **Tăng tốc độ truy cập** Reduced latency, faster loading

💰 **Giảm chi phí egress S3** Lower data transfer costs

📈 **Tối ưu băng thông** Better bandwidth utilization

🌍 **Mở rộng toàn cầu** Global scalability & availability

📂 Content Types

Static websites ● Images ● Videos ● APIs ● Software downloads

CloudFront + S3 Best Practices

Xây dựng kiến trúc an toàn, hiệu năng cao và tối ưu chi phí để phân phối nội dung.

🏗️ The Secure & High-Performance Blueprint

Mô hình kiến trúc được khuyên dùng để đảm bảo mọi yêu cầu đều được xác thực và bảo vệ tại lớp biên (edge) trước khi truy cập vào S3 bucket đã được khóa kín.

`User` → **HTTPS** → `CloudFront (WAF/Shield)` → **OAC** → `Private S3 Bucket`

I. SECURITY (The Fortress)

- **Lock Down Your Origin:** Luôn sử dụng OAC. S3 bucket không bao giờ được phép public.
- **Encrypt Everything in Transit:** Thực thi HTTPS-only từ người dùng đến CloudFront và ngược lại.
- **Control Access to Content:** Dùng Signed URLs/Cookies cho các nội dung nhạy cảm hoặc trả phí.
- **Deploy a Firewall at the Edge:** Tích hợp AWS WAF để bảo vệ chống lại các cuộc tấn công web.

II. PERFORMANCE (The Superhighway)

- **Master Your Caching Strategy:** Tích cực cache các nội dung tĩnh với TTL cao. Không cache dữ liệu động/nhạy cảm.
- **Maximize Cache Hit Ratio:** Đây là mục tiêu số 1 để giảm độ trễ, giảm tải cho S3 và tiết kiệm chi phí.
- **Compress Automatically:** Bật tính năng nén (Gzip/Brotli) để giảm kích thước file và tăng tốc độ tải.

III. COST OPTIMIZATION (The Accountant)

- **Your Cache is Your Wallet:** Cache Hit Ratio cao là cách tiết kiệm chi phí hiệu quả nhất bằng cách giảm thiểu yêu cầu về S3.
- **Choose the Right Price Class:** Lựa chọn phạm vi địa lý phù hợp với tệp người dùng của bạn.
- **Monitor Data Transfer Costs:** Theo dõi chặt chẽ chi phí "Data Transfer Out" từ CloudFront và S3.

IV. MONITORING & OPERATIONS (The Control Tower)

- **Log and Analyze Everything:** Bật CloudFront access logging để phục vụ điều tra và phân tích.
- **Watch Your Key Metrics:** Sử dụng CloudWatch để theo dõi Cache Hit Ratio, Error Rates, và Latency.
- **Set Alarms for Anomalies:** Tạo CloudWatch Alarms để nhận cảnh báo ngay lập tức khi có sự cố.
- **Audit Regularly:** Thường xuyên rà soát lại toàn bộ cấu hình để đảm bảo tuân thủ các quy tắc an ninh.

Demo Setup - CloudFront + S3 Security

🎯 Demo Objectives

- Setup secure S3 + CloudFront architecture
- Implement Origin Access Control (OAC)
- Configure HTTPS end-to-end
- Test access controls và performance

📋 Prerequisites

- S3 bucket với static website content
- CloudFront permissions
- ACM certificate (optional)

🔧 Setup Steps

1 Prepare S3 Bucket

- Upload static website files
- Configure bucket for static hosting
- Ensure bucket is NOT public

2 Create CloudFront Distribution

- Set S3 bucket as origin
- Configure OAC (Origin Access Control)
- Set cache behaviors
- Configure SSL/HTTPS settings

3 Configure S3 Bucket Policy

- Allow CloudFront OAC access
- Deny direct public access
- Test policy effectiveness

4 Testing & Validation

- Test CloudFront URL access (should work)
- Test direct S3 URL access (should fail)
- Verify HTTPS enforcement
- Check cache performance

✅ Security Validation

- S3 bucket không publicly accessible
- Tất cả traffic đều thông qua HTTPS
- Cache behaviors hoạt động chính xác
- CloudFront access logs được enable

🛠️ Troubleshooting

- Common OAC/OAI configuration issues
- Cache invalidation procedures
- SSL certificate problems

Let continue ?

AWS CloudTrail

Hộp Đen & Camera An Ninh cho Tài khoản AWS của bạn.

CloudTrail là gì?

Là nguồn sự thật duy nhất để trả lời các câu hỏi quan trọng về mọi hoạt động trong tài khoản của bạn:

Ai? Đã làm gì? Khi nào? Trên tài nguyên nào?

Tại sao CloudTrail lại Tối quan trọng?

🔍 Điều tra An ninh

Là bằng chứng duy nhất để truy vết kẻ tấn công và hiểu rõ thiệt hại khi có sự cố.

🛡️ Tuân thủ (Compliance)

Cung cấp các báo cáo kiểm toán không thể chối cãi, đáp ứng các tiêu chuẩn an ninh quốc tế.

🛠️ Khắc phục Sự cố

Nhanh chóng tìm ra "thủ phạm" gây lỗi hệ thống do thay đổi cấu hình sai.

CloudTrail ghi lại những gì?

Management Events

Các hành động "thay đổi cấu trúc".

"Ai đã tạo/xóa server? Ai đã thay đổi firewall?"

Mặc định bật

Data Events

Các hành động truy cập dữ liệu.

"Ai đã đọc file `secret.txt` trong S3?"

Có tính phí / Bật khi cần

Insight Events

Phát hiện hành vi bất thường.

"Phát hiện số API call xóa server tăng đột biến."

Nâng cao / Có tính phí

✅ Checklist Cấu hình CloudTrail Chuẩn

- ✅ **Bật trên Toàn bộ Khu vực (Enable for All Regions):** Để đảm bảo không có "điểm mù" nào trong hệ thống giám sát.
- ✅ **Tập trung Log vào một Bucket An toàn:** Tạo một S3 bucket riêng, được bảo vệ nghiêm ngặt (tốt nhất là ở một tài khoản AWS khác).
- ✅ **Bật Xác thực Log (Enable Log File Validation):** Đảm bảo không ai có thể âm thầm thay đổi hay xóa các file log.
- ✅ **Kết hợp với CloudWatch để Cảnh báo:** Đừng chỉ ghi lại, hãy hành động! Tạo cảnh báo tự động cho các sự kiện quan trọng (Root login, thay đổi firewall...).
- ✅ **Đặt Chính sách Lưu trữ (Define Retention Policies):** Tự động lưu trữ hoặc xóa log theo yêu cầu tuân thủ của bạn.

AWS CloudWatch

Giám sát, Phân tích và Phản ứng.

Cách CloudWatch Phản ứng với một Cuộc tấn công

Hãy xem cách các thành phần của CloudWatch phối hợp với nhau qua một kịch bản tấn công thực tế.

Kịch bản: Tấn công Brute-force và Tạo User trái phép

1. Tấn công: Hacker thực hiện nhiều lần đăng nhập thất bại vào AWS Console.
2. Xâm nhập thành công: Cuối cùng, hacker đoán đúng mật khẩu và đăng nhập thành công.
3. Hành động độc hại: Hacker tạo một IAM user mới (`backdoor_user`) với quyền admin để duy trì truy cập.

Luồng Phản ứng của CloudWatch

1. Detect
Metrics (ConsoleSignInFail tăng đột biến. →

2. Alert
Alarm được kích hoạt khi ngưỡng đăng nhập thất bại bị vượt qua. →

3. Notify
Alarm gửi thông báo qua SNS đến đội an ninh. →

4. Investigate
Đội an ninh dùng **Logs Insights** để phân tích CloudTrail logs và tìm ra `backdoor_user`.

AWS CloudWatch

Giám sát, Phân tích và Phản ứng.

Bốn Trụ cột của CloudWatch

CloudWatch được xây dựng trên bốn thành phần chính, hoạt động cùng nhau để cung cấp khả năng quan sát toàn diện.

📊 **Metrics:** Các chuỗi dữ liệu theo thời gian (time-series data) - ví dụ: CPU Utilization, Network In. Đây là các chỉ số sức khỏe của hệ thống.

📜 **Logs:** Nơi tập trung lưu trữ, tìm kiếm và phân tích log từ mọi nguồn (EC2, Lambda, CloudTrail...).

🚨 **Alarms:** Tự động thực hiện hành động khi một Metric vượt qua một ngưỡng nhất định. Đây là hệ thống phản ứng của bạn.

📈 **Dashboards:** Giao diện trực quan hóa, nơi bạn có thể tùy chỉnh để hiển thị các Metrics và Logs quan trọng nhất ở một nơi duy nhất.

AWS Config tracks resource configurations for compliance, security, and troubleshooting.

Pros & Cons

Consider the benefits and challenges of this approach.

Advantages (Pros)

🚀 **Rapid Response**
Reduces fix time (MTTR) from hours to seconds.

🔄 **Continuous Compliance**
Enforces security rules 24/7, with no manual work.

👥 **Reduced Human Error**
Removes the risk of manual mistakes.

📈 **Scalability**
Applies rules across many accounts and resources.

Considerations (Cons)

❗ **Implementation Complexity**
Requires careful planning and coding to avoid issues.

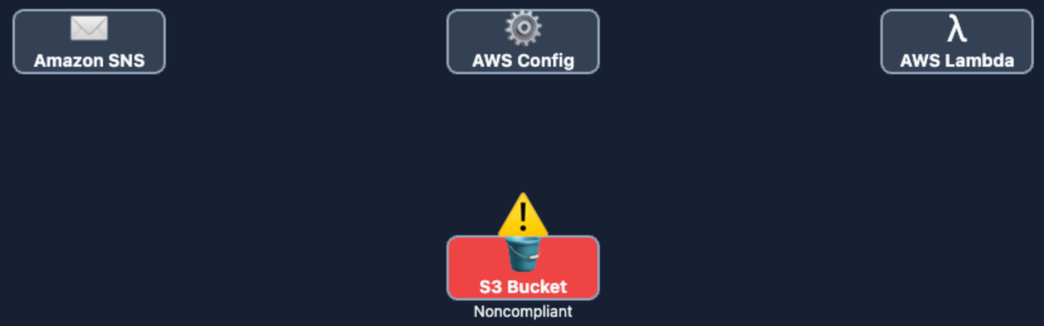
⚠️ **Risk of Errors**
Bad scripts can cause problems. Always test well.

💸 **Associated Costs**
Costs for services like Lambda can add up at scale.

🎯 **Scope Limitations**
Some issues are too complex to auto-fix and need manual review.

AWS Config: The Automated Compliance Loop

Watch how a configuration change is automatically detected, reported, and remediated.



1. DETECT

Config rules continuously evaluate resources. Non-compliant changes are flagged instantly.

2. NOTIFY

Amazon SNS or EventBridge alerts teams via email, Slack, or a centralized dashboard.

3. REMEDIATE

AWS Lambda or SSM Automation runs a playbook to automatically revert the change.

Tổng Quan AWS AI-Powered Security

Sử dụng Machine Learning để tự động hóa và nâng cao khả năng bảo vệ trên toàn bộ hạ tầng đám mây.

Threat Detection

GuardDuty

Là dịch vụ phát hiện mối đe dọa thông minh, liên tục giám sát tài khoản AWS của bạn để tìm các hoạt động độc hại và hành vi trái phép.

Tính năng AI: ML-based threat detection
Trường hợp sử dụng: Tự động phát hiện các mối đe dọa như trinh sát, xâm nhập server, và xâm nhập tài khoản.

Fraud Detector

Cho phép bạn xây dựng, triển khai và quản lý các mô hình machine learning tùy chỉnh để phát hiện các hành vi gian lận trực tuyến tiềm ẩn.

Tính năng AI: Custom ML for fraud patterns
Trường hợp sử dụng: Chống gian lận trong thanh toán, tạo tài khoản giả, lạm dụng khuyến mãi.

Data Protection

Macie

Là dịch vụ bảo vệ dữ liệu, sử dụng machine learning và nhận dạng mẫu để khám phá và bảo vệ dữ liệu nhạy cảm của bạn trên S3.

Tính năng AI: ML for sensitive data discovery
Trường hợp sử dụng: Ngăn chặn rò rỉ dữ liệu (DLP), đáp ứng các yêu cầu tuân thủ về quyền riêng tư dữ liệu.

Vulnerability & Risk Management

Inspector

Tự động quét các workload AWS của bạn để tìm các lỗ hổng phần mềm và các rủi ro do vô tình tiếp xúc với mạng.

Tính năng AI: ML-based CVE & malware risk scoring
Trường hợp sử dụng: Quản lý lỗ hổng của tài sản (Asset vulnerability management).

IAM Access Analyzer

Giúp bạn xác định các tài nguyên trong tổ chức và tài khoản của mình được chia sẻ với một thực thể bên ngoài, dựa trên phân tích logic.

Tính năng AI: ML/Automated reasoning for policy risk
Trường hợp sử dụng: Thực thi Nguyên tắc Đặc quyền Tối thiểu (Least Privilege).

Incident Response & Analysis

Security Hub Insights

Cung cấp một cái nhìn toàn diện về tình hình an ninh của bạn, tổng hợp các cảnh báo từ nhiều dịch vụ AWS khác nhau vào một nơi duy nhất.

Tính năng AI: ML-based findings prioritization
Trường hợp sử dụng: Tổng hợp và quản lý hoạt động an ninh (SecOps aggregation).

Detective

Tự động thu thập dữ liệu log từ các tài nguyên AWS của bạn và sử dụng machine learning, phân tích thống kê, và lý thuyết đồ thị để giúp bạn hình dung và tiến hành điều tra an ninh nhanh hơn, hiệu quả hơn.

Tính năng AI: ML/Graph for forensics
Trường hợp sử dụng: Điều tra sự cố và phân tích nguyên nhân gốc rễ.

Amazon Macie

Automated Discover and protect your sensitive data

Macie Overview

AI-powered sensitive data discovery to automatically find, classify, and protect your data on AWS.

Discovery Process

Scan S3 Buckets → Classify Data → Generate Findings → Create Alerts

Data Types Discovered

PII: Full Name, Address, Phone...

PHI: Medical Records, Health Info...

Financial: Credit Card, Bank Account...

Credentials: AWS Keys, Private Keys...

Integration Ecosystem

Route findings to other services for automated remediation.

Macie ~ EventBridge, Lambda, Security Hub

Common Use Cases

- Ensure safety during data migrations.
- Meet compliance (GDPR, HIPAA, etc.).
- Accelerate incident response.
- Prevent accidental data exposure.

AWS GuardDuty

Threat detection service that monitors for malicious activity and anomalous behavior to protect AWS accounts, workloads, and data.

GuardDuty liên tục tuần tra toàn bộ tài khoản của bạn, sử dụng **Machine Learning, Phân tích Hành vi, và Threat Intelligence** để tự động phát hiện các mối đe dọa. Bạn chỉ cần một cú nhấp chuột để kích hoạt, không cần cấu hình phức tạp.

I. Nguồn Dữ liệu được Phân tích

- VPC Flow Logs
- DNS Logs
- CloudTrail Events
- S3 Data Events

II. Các Loại Phát hiện Phổ biến

Reconnaissance

Kẻ tấn công đang thăm dò hệ thống, ví dụ: quét cổng (port scanning) từ một IP độc hại.

Instance Compromise

Một server EC2 bị chiếm quyền, ví dụ: đang được dùng để đào tiền ảo.

Account Compromise

Thông tin đăng nhập của một user bị lộ, ví dụ: API call được thực hiện từ một mạng Tor.

III. Phân loại Mức độ Nghiêm trọng

High
Mối đe dọa tức thời, cần xử lý ngay

Medium
Hành vi đáng ngờ, cần điều tra

Low
Hoạt động không mong muốn

IV. Từ Phát hiện đến Hành động Tự động

GuardDuty Finding → EventBridge → AWS Lambda (Auto-Remediation)

Ví dụ: Tự động cô lập một server EC2 bị xâm nhập bằng cách thay đổi Security Group của nó.

AWS Best Practices: The Complete Checklist

Các nguyên tắc vàng để xây dựng một môi trường AWS an toàn, hiệu quả và tối ưu chi phí.

🛡️ Bảo mật & Kiểm soát truy cập

- ✓ Sử dụng **IAM role** thay vì IAM user cho ứng dụng.
- ✓ Áp dụng **nguyên tắc least privilege**, chỉ cấp quyền tối thiểu cần thiết.
- ✓ Bật **MFA (Multi-Factor Authentication)** cho mọi tài khoản, đặc biệt là root.
- ✓ Cất giữ **Root account**, không dùng cho công việc hàng ngày, xóa access key.
- ✓ **Rotate credentials** (mật khẩu, access key) định kỳ.

🔒 Mạng & Hạ tầng

- ✓ Thiết kế **VPC riêng, chia subnet** rõ ràng (private/public).
- ✓ Kiểm tra **Security Groups & NACLs** thường xuyên, không mở `0.0.0.0/0` cho các cổng quản trị.
- ✓ Sử dụng **AWS WAF & Shield** để bảo vệ ứng dụng web khỏi DDoS và các tấn công phổ biến.

🗃️ Quản lý dữ liệu & Backup

- ✓ Mã hóa dữ liệu **"at rest"** (trên S3/EBS/RDS) và **"in transit"** (dùng HTTPS/TLS).
- ✓ Sử dụng **AWS KMS** để quản lý key mã hóa một cách tập trung và an toàn.
- ✓ Thiết lập **backup định kỳ** (AWS Backup, snapshot), lưu trữ cross-region/cross-account cho DR.
- ✓ Bật **S3 Object Lock & Versioning** để bảo vệ dữ liệu khỏi bị xóa hoặc sửa đổi ngoài ý muốn.

📈 Monitoring & Compliance

- ✓ Bật **CloudTrail** trên mọi region để theo dõi toàn bộ API activity.
- ✓ Sử dụng **CloudWatch logging & alarms** để giám sát và cảnh báo các hành vi bất thường.
- ✓ Dùng **AWS Config & Security Hub** để theo dõi tuân thủ và tổng hợp các phát hiện an ninh.
- ✓ Tích hợp với các hệ thống **SIEM/ServiceNOW** để quản lý tập trung.

💰 Cost Optimization

- ✓ Thiết lập **AWS Budgets & Alerts** để cảnh báo khi chi phí vượt ngưỡng.
- ✓ Áp dụng **lifecycle policy** cho S3/EBS để tự động dọn dẹp, tắt các tài nguyên không sử dụng.
- ✓ Thực thi chính sách **Tagging** cho tất cả tài nguyên để phân loại và truy vết chi phí.

🌍 Governance & Automation

- ✓ Sử dụng **AWS Organizations** để quản lý nhiều tài khoản và áp dụng **Service Control Policies (SCP)**.
- ✓ Triển khai hạ tầng bằng **Infrastructure as Code** (CloudFormation/Terraform).
- ✓ Thiết lập **Auto-remediation** (EventBridge/Lambda) cho các cảnh báo an ninh.
- ✓ Xây dựng **runbook** để chuẩn hóa quy trình phản ứng với sự cố (Incident Response).

Giám sát & Phản ứng Tự động trên AWS

Các kịch bản thực tế kết hợp dịch vụ AWS để tăng cường an ninh và quản trị.

- 1. Bảo vệ Phân phối Nội dung (S3 + CloudFront)
- 2. Cảnh báo Lỗi Cấu hình An ninh (Public SSH)
- 3. Cảnh báo Chi phí Vượt ngưỡng tới Slack
- 4. Phát hiện Hành vi Mạng Bất thường

Thank You!

Cảm ơn mọi người đã lắng nghe và đóng góp.

Q & A