# Sử dụng chatbot do Amazon Bedrock cung cấp với Amazon Security Lake để giúp điều tra các sự cố

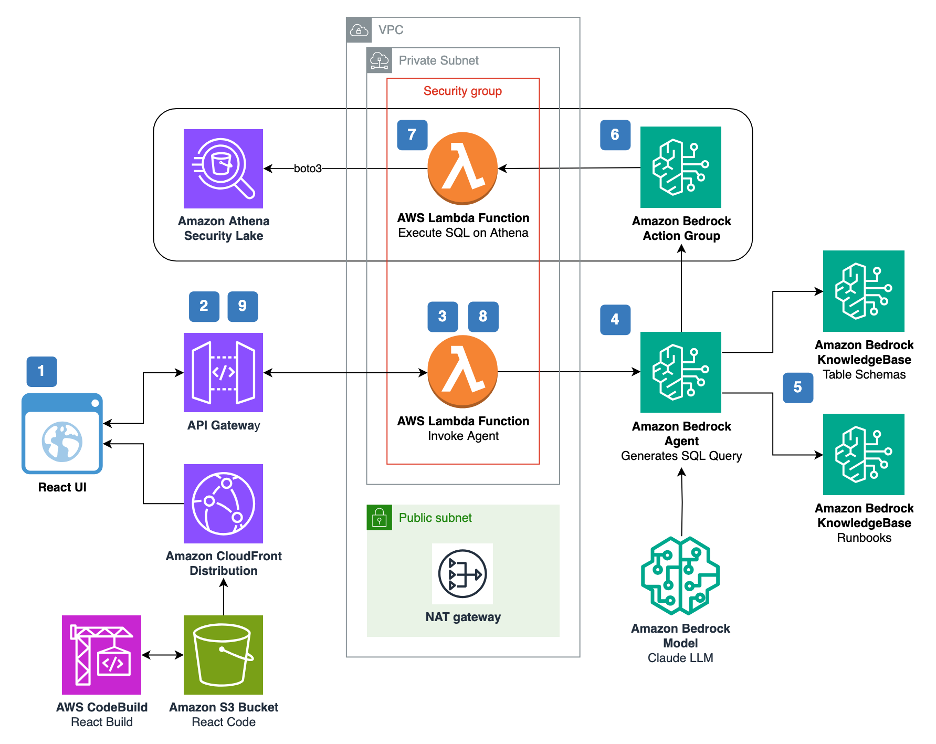
tác giả Madhunika Reddy Mikkili , Harsh Asnani , Michael Massey và Jonathan Nguyễn 01 THÁNG 5 NĂM 2025 trong [Nâng cao (300)](https://aws.amazon.com/blogs/security/category/learning-levels/advanced-300/) , [Amazon Bedrock](https://aws.amazon.com/blogs/security/category/artificial-intelligence/amazon-machine-learning/amazon-bedrock/) , [Amazon Security Lake](https://aws.amazon.com/blogs/security/category/security-identity-compliance/amazon-security-lake/) , [Trí tuệ nhân tạo](https://aws.amazon.com/blogs/security/category/artificial-intelligence/generative-ai/) , [Bảo mật, Nhận dạng và Tuân thủ](https://aws.amazon.com/blogs/security/category/security-identity-compliance/) , [Hướng dẫn kỹ thuật](https://aws.amazon.com/blogs/security/category/post-types/technical-how-to/) [Liên kết cố định](https://aws.amazon.com/blogs/security/use-an-amazon-bedrock-powered-chatbot-with-amazon-security-lake-to-help-investigate-incidents/) [Bình luận](https://aws.amazon.com/blogs/security/use-an-amazon-bedrock-powered-chatbot-with-amazon-security-lake-to-help-investigate-incidents/#Comments) [Chia sẻ](https://aws.amazon.com/vi/blogs/security/use-an-amazon-bedrock-powered-chatbot-with-amazon-security-lake-to-help-investigate-incidents/#)

Trong [phần 2](https://aws.amazon.com/blogs/security/generate-ai-powered-insights-for-amazon-security-lake-using-amazon-sagemaker-studio-and-amazon-bedrock/) của loạt bài này, chúng tôi đã chỉ cho bạn cách sử dụng sổ ghi chép [Amazon SageMaker Studio](https://aws.amazon.com/sagemaker-ai/studio/) với đầu vào ngôn ngữ tự nhiên để hỗ trợ săn tìm mối đe dọa. Điều này được thực hiện bằng cách sử dụng SageMaker Studio để tự động tạo và chạy các truy vấn SQL trên [Amazon Athena](https://aws.amazon.com/athena/) với [Amazon Bedrock](https://aws.amazon.com/bedrock/) và [Amazon Security Lake](https://aws.amazon.com/security-lake/) . Nhóm dịch vụ Security Lake và cộng đồng [Open Cybersecurity Schema Framework](https://github.com/ocsf) (OCSF) tiếp tục thêm [các nguồn nhật ký bổ sung](https://docs.aws.amazon.com/security-lake/latest/userguide/source-management.html) và [ánh xạ OCSF](https://github.com/ocsf/examples) để cho phép Security Lake cung cấp một nguồn hợp nhất cho khách hàng để tiến hành điều tra bảo mật.

Vì các nguồn dữ liệu ghi nhật ký bảo mật liên tục phát triển, các tổ chức cần cung cấp một cơ chế để nhóm bảo mật của họ hiểu và truy vấn các nguồn dữ liệu đó. Bạn có thể có các sổ tay điều tra và phản hồi hiện có mà nhóm bảo mật của bạn cần phải thành thạo và biết khi nào nên sử dụng. Các nhóm bảo mật có thể mất một khoảng thời gian dài để tiếp nhận và hiểu các nguồn dữ liệu bảo mật và sổ tay có sẵn cũng như cách sử dụng chúng hiệu quả để giảm [thời gian phản hồi trung bình](https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/mean-time-to-respond.html) .

Trong bài đăng này, chúng tôi sẽ chỉ cho bạn cách mở rộng chức năng từ [bài đăng trước](https://aws.amazon.com/blogs/security/generate-ai-powered-insights-for-amazon-security-lake-using-amazon-sagemaker-studio-and-amazon-bedrock/) . Bạn sẽ học cách triển khai chatbot bảo mật với giao diện người dùng đồ họa (GUI) và phần phụ trợ không có máy chủ được hỗ trợ bởi tác nhân Amazon Bedrock kết hợp các sổ tay hướng dẫn hiện có để điều tra hoặc phản hồi sự kiện bảo mật. Chatbot này trình bày các tác nhân Amazon Bedrock được xây dựng có mục đích giúp giải quyết các mối quan ngại về bảo mật tùy thuộc vào đầu vào ngôn ngữ tự nhiên của người dùng. Giải pháp có một GUI duy nhất cung cấp giao diện trực tiếp với tác nhân Amazon Bedrock để tạo và gọi các truy vấn SQL hoặc cung cấp các đề xuất cho sổ tay hướng dẫn phản hồi sự cố nội bộ để điều tra hoặc phản hồi các sự kiện bảo mật có thể xảy ra.

## **Tổng quan về giải pháp mẫu chatbot bảo mật**

****

*Hình 1: Sơ đồ kiến ​​trúc giải pháp mẫu chatbot bảo mật*

Luồng ứng dụng như thể hiện trong Hình 1:

1. Người dùng gửi truy vấn thông qua React UI.  
   Lưu ý : React UI được sử dụng trong giải pháp này không có xác thực tích hợp. Bạn nên thêm các khả năng xác thực tuân theo các yêu cầu bảo mật của tổ chức bạn. Bạn có thể thêm [các khả năng xác thực bằng cách sử dụng Amazon Cognito và AWS Amplify UI](https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/authenticate-react-app-users-cognito-amplify-ui.html).
2. Truy vấn của người dùng được gửi đến REST API [của Amazon API Gateway](https://aws.amazon.com/api-gateway/) , nơi sẽ gọi hàm Invoke Agent [AWS Lambda](https://aws.amazon.com/lambda).
3. Hàm Lambda sẽ gọi tác nhân Amazon Bedrock bằng truy vấn của người dùng.
4. Tác nhân Amazon Bedrock (sử dụng Claude 3 Sonnet của Anthropic) xử lý truy vấn và quyết định giữa việc lấy thông tin từ sổ tay hướng dẫn hoặc bằng cách truy vấn Security Lake bằng [Amazon Athena](https://aws.amazon.com/athena).

Đối với các truy vấn về cơ sở kiến ​​thức playbook:

1. Tác nhân Amazon Bedrock truy vấn cơ sở kiến ​​thức của playbook và lấy ra các kết quả có liên quan.

Đối với các truy vấn dữ liệu Security Lake:

1. Tác nhân Amazon Bedrock truy vấn cơ sở kiến ​​thức lược đồ và lấy các lược đồ bảng Security Lake để tạo truy vấn SQL.
2. Tác nhân Amazon Bedrock gọi hành động truy vấn SQL từ nhóm hành động Amazon Bedrock, truyền truy vấn SQL dưới dạng tham số.
3. Nhóm hành động sẽ gọi Execute SQL on Athena hàm Lambda, hàm này sẽ thực thi truy vấn trên Athena và trả về kết quả cho tác nhân Amazon Bedrock.

Sau khi lấy kết quả từ cơ sở kiến ​​thức hoặc nhóm hành động:

1. Tác nhân Amazon Bedrock sử dụng thông tin đã thu thập được để xây dựng phản hồi cuối cùng và gửi lại cho Invoke Agent hàm Lambda.
2. Hàm Lambda gửi phản hồi trở lại cho máy khách bằng API API Gateway WebSocket.
3. API Gateway cung cấp phản hồi cho React UI bằng cách sử dụng kết nối WebSocket với máy khách.
4. Phản hồi của nhân viên sẽ được hiển thị cho người dùng trên giao diện trò chuyện.

### **Điều kiện tiên quyết**

Trước khi triển khai giải pháp mẫu, hãy hoàn thành các điều kiện tiên quyết sau:

1. [Bật Security Lake](https://docs.aws.amazon.com/security-lake/latest/userguide/getting-started.html) trong tổ chức của bạn trong [AWS Organizations](https://aws.amazon.com/organizations) và chỉ định một tài khoản [quản trị viên được ủy quyền](https://docs.aws.amazon.com/security-lake/latest/userguide/multi-account-management.html) để quản lý cấu hình Security Lake cho tất cả các tài khoản thành viên trong tổ chức của bạn. Cấu hình Security Lake với các nguồn nhật ký phù hợp: [Amazon Virtual Private Cloud (Amazon VPC)](https://aws.amazon.com/vpc/) Flow Logs, [AWS Security Hub](https://aws.amazon.com/security-hub/) , [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) và [Amazon Route53](https://aws.amazon.com/route53/) .
2. [Tạo quyền truy cập truy vấn của người đăng ký](https://docs.aws.amazon.com/security-lake/latest/userguide/subscriber-query-access.html) từ tài khoản AWS Security Lake nguồn tới tài khoản AWS của người đăng ký.
3. Chấp nhận [yêu cầu chia sẻ tài nguyên](https://docs.aws.amazon.com/lake-formation/latest/dg/accepting-ram-invite.html) trong tài khoản AWS của người đăng ký trong [AWS Resource Access Manager (AWS RAM)](https://aws.amazon.com/ram/) .
4. Tạo liên kết cơ sở dữ liệu trong [AWS Lake Formation](https://aws.amazon.com/lake-formation/) trong tài khoản AWS của người đăng ký và cấp quyền truy cập cho các bảng [Athena](https://aws.amazon.com/athena) trong tài khoản AWS Security Lake.
5. [Cấp quyền truy cập mô hình Claude v3](https://docs.aws.amazon.com/bedrock/latest/userguide/model-access.html#add-model-access) của Anthropic cho Amazon Bedrock trong tài khoản người đăng ký AWS nơi bạn sẽ triển khai giải pháp. Nếu bạn thử sử dụng mô hình trước khi bật mô hình đó trong tài khoản AWS, bạn sẽ nhận được thông báo lỗi.

Với các điều kiện tiên quyết đã nêu, kiến ​​trúc giải pháp mẫu cung cấp các tài nguyên sau:

1. [Amazon CloudFront](https://aws.amazon.com/cloudfront) có nguồn gốc từ [Amazon Simple Storage Service (Amazon S3)](https://aws.amazon.com/s3) .
2. Một trang web tĩnh của Amazon S3 dành cho giao diện người dùng chatbot.
3. Một API Gateway để gọi hàm Lambda.
4. Một hàm Lambda để gọi tác nhân Amazon Bedrock.
5. Một đại lý Amazon Bedrock có cơ sở kiến ​​thức rộng lớn.
   1. Nhóm hành động của tác nhân Amazon Bedrock để tạo và gọi các truy vấn SQL trên Athena.
      1. Cơ sở kiến ​​thức Amazon Bedrock để tham khảo các lược đồ bảng Athena mẫu trong Security Lake. Mặc dù tác nhân Amazon Bedrock có thể lấy các hàng trực tiếp từ bảng Athena, việc cung cấp các lược đồ bảng mẫu sẽ cải thiện độ chính xác khi tạo truy vấn SQL cho các cột bảng trong Security Lake.
      2. Cơ sở kiến ​​thức Amazon Bedrock để tham khảo các sổ tay hướng dẫn ứng phó sự cố hiện có. Bằng cách kết hợp cơ sở kiến ​​thức này, tác nhân Amazon Bedrock có thể đề xuất các hành động để điều tra hoặc ứng phó dựa trên các sổ tay hướng dẫn hiện có đã được tổ chức của bạn chấp thuận.

### **Chi phí**

Trước khi triển khai giải pháp mẫu và xem qua bài đăng này, điều quan trọng là phải hiểu chi phí của các dịch vụ AWS đang được sử dụng. Chi phí sẽ phụ thuộc phần lớn vào lượng dữ liệu bạn tương tác trong Amazon Bedrock và bằng cách truy vấn Security Lake với Athena.

1. Chi phí của Security Lake được xác định theo khối lượng dữ liệu nhật ký và sự kiện được thu thập từ các dịch vụ AWS. Security Lake điều phối các dịch vụ AWS khác thay mặt bạn, với các khoản phí riêng. Bạn có thể tìm thêm thông tin về giá cho các dịch vụ tương ứng: [Amazon S3](https://aws.amazon.com/s3/pricing/) , [AWS Glue](https://aws.amazon.com/glue/pricing/) , [Amazon EventBridge](https://aws.amazon.com/eventbridge/pricing/) , [AWS Lambda](https://aws.amazon.com/lambda/pricing/) , [Amazon Simple Query Service (Amazon SQS)](https://aws.amazon.com/sqs/pricing/) và [Amazon Simple Notification Service (Amazon SNS)](https://aws.amazon.com/sns/pricing/).
2. Giá theo yêu cầu của Amazon Bedrock dựa trên mô hình ngôn ngữ lớn (LLM) đã chọn và số lượng mã thông báo đầu vào và đầu ra. Mã thông báo bao gồm một vài ký tự và đề cập đến đơn vị văn bản cơ bản mà mô hình học để hiểu đầu vào và lời nhắc của người dùng. Để biết thêm chi tiết, hãy xem [giá của Amazon Bedrock](https://aws.amazon.com/bedrock/pricing/) .
3. Các truy vấn SQL do Amazon Bedrock tạo ra được gọi bằng Athena. Chi phí Athena dựa trên lượng dữ liệu được quét trong Security Lake cho truy vấn đó. Để biết thêm chi tiết, hãy xem [giá Athena](https://aws.amazon.com/athena/pricing/).

## **Triển khai chatbot mẫu**

Bạn có thể triển khai giải pháp mẫu bằng cách sử dụng [AWS Cloud Development Kit (AWS CDK)](https://aws.amazon.com/cdk/) . Để biết hướng dẫn và thông tin thêm về cách sử dụng AWS CDK, hãy xem [Bắt đầu với AWS CDK](https://aws.amazon.com/getting-started/guides/setup-cdk/).

1. Sao chép kho lưu trữ [sample-generative-ai-chatbot-for-amazon-security-lake](https://github.com/aws-samples/sample-generative-ai-chatbot-for-amazon-security-lake).
2. Điều hướng đến thư mục gốc của dự án.
3. Cài đặt các phần phụ thuộc của dự án.
4. Xây dựng và triển khai ứng dụng bằng các lệnh sau:

npm install -g aws-cdk

npm install

cdk synth

1. Chạy các lệnh sau trong terminal của bạn khi đã đăng nhập vào tài khoản AWS của người đăng ký. Thay thế *<INSERT\_AWS\_ACCOUNT>*bằng số tài khoản của bạn và thay thế *<INSERT\_REGION>*bằng Vùng AWS mà bạn muốn triển khai giải pháp.

cdk bootstrap aws://*<INSERT\_AWS\_ACCOUNT>*/*<INSERT\_REGION>*

cdk deploy –all

Là một phần của triển khai CDK, có một giá trị Đầu ra cho URL Ứng dụng React (FrontendAppStack.ReactAppUrl). Bạn sẽ sử dụng giá trị này để tương tác với ứng dụng GenAI. Đợi tối đa 5 phút để URL hoạt động.

## **Các bước cấu hình sau khi triển khai**

Bây giờ bạn đã triển khai giải pháp, bạn cần thêm quyền để cho phép vai trò [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam) của chức năng Lambda và Amazon Bedrock tương tác với dữ liệu Security Lake của bạn.

### **Cấp quyền cho cơ sở dữ liệu Security Lake**

1. Sao chép ARN vai trò của Lambda từ ngăn xếp CloudFormation “BedrockAppStack”. Tài nguyên trong ngăn xếp có tên là “athenaAgentSecurityLakeActionGroupLambdaServiceRole\*\*\*\*\*\*\*\*”.
2. Đi tới bảng điều khiển **Lake Formation**.
3. Chọn cơ sở dữ liệu **amazon\_security\_lake\_glue\_db\_***<YOUR-REGION>* . Ví dụ, nếu Security Lake của bạn nằm trong us-east-1, giá trị sẽ là amazon\_security\_lake\_glue\_db\_us\_east\_1
4. Đối với **Action**, hãy chọn **Grant**.
5. Trong **Grant Data Permissions**, chọn **SAML Users and Groups**.
6. Dán vai trò IAM của hàm Lambda ARN từ Bước 1.
7. Trong **Database Permissions**, chọn **Describe**, sau đó chọn **Grant**.

### **Cấp quyền cho các bảng Security Lake**

Bạn phải lặp lại các bước sau cho mỗi nguồn được cấu hình trong Security Lake. Ví dụ, nếu bạn có bốn nguồn được cấu hình trong Security Lake, bạn phải cấp quyền cho vai trò IAM của hàm Lambda cho mỗi bảng. Nếu bạn có nhiều nguồn nằm trong các Vùng riêng biệt và bạn không có Vùng tổng hợp được cấu hình trong Security Lake, bạn phải lặp lại các bước cho từng nguồn trong mỗi Vùng.

Ví dụ sau đây cấp quyền cho bảng Security Hub trong Security Lake. Để biết thêm thông tin về việc cấp quyền cho bảng, hãy xem [hướng dẫn sử dụng AWS Lake Formation](https://docs.aws.amazon.com/lake-formation/latest/dg/granting-table-permissions.html#table-start-grant) .

1. Sao chép ARN vai trò của Lambda từ ngăn xếp CloudFormation “BedrockAppStack”. Tài nguyên trong ngăn xếp được đặt tên là “athenaAgentSecurityLakeActionGroupLambdaServiceRole\*\*\*\*\*\*\*\*”.
2. Đi tới bảng điều khiển **Lake Formation**.
3. Chọn cơ sở dữ liệu. Ví dụ, nếu cơ sở dữ liệu Security Lake của bạn nằm trong us-east-1, giá trị sẽ là amazon\_security\_lake\_glue\_db\_us\_east-1amazon\_security\_lake\_glue\_db\_*<YOUR-REGION>*
4. Chọn **View Tables**.
5. Chọn bảng amazon\_security\_lake\_table\_*<YOUR-REGION>*\_sh\_findings\_1\_0. Ví dụ, nếu bảng Security Lake của bạn nằm trong us-east-1, giá trị sẽ là amazon\_security\_lake\_table\_us\_east\_1\_sh\_findings\_1\_0  
     
   **Lưu ý**: Mỗi bảng phải được cấp quyền truy cập riêng lẻ. Việc chọn **Tất cả các bảng** sẽ không cấp quyền truy cập cần thiết để truy vấn Security Lake.
6. Đối với **Action**, hãy chọn **Grant**.
7. Trong **Grant Data Permissions**, chọn **SAML Users and Groups**.
8. Dán vai trò IAM của hàm Lambda ARN từ Bước 1.
9. Trong **Table Permissions**, chọn **Describe**, sau đó chọn **Grant**.

### **Đồng bộ hóa nguồn dữ liệu**

Sau khi triển khai cơ sở hạ tầng, bạn cần đồng bộ hóa các nguồn dữ liệu trong cơ sở dữ liệu Amazon Bedrock để dữ liệu trong Amazon S3 có thể được vector hóa và cung cấp trong [Amazon OpenSearch Serverless](https://aws.amazon.com/opensearch-service/features/serverless/), đây là dịch vụ được các cơ sở dữ liệu trong giải pháp này sử dụng làm nguồn vector.

* Trong [bảng điều khiển Amazon Bedrock](https://console.aws.amazon.com/bedrock/), hãy chọn Cơ sở kiến ​​thức và tìm hai cơ sở kiến ​​thức Amazon Bedrock được triển khai trong giải pháp này: gen-ai-sec-lake-table-schemavà gen-ai-sec-lake-runbooks. Điều hướng đến từng cơ sở kiến ​​thức và nguồn dữ liệu của cơ sở đó. Sau đó, hãy chọn Đồng bộ hóa cho từng nguồn dữ liệu.

### **Nhận URL phân phối CloudFront**

Là một phần của giải pháp mẫu, chatbot sử dụng URL phân phối CloudFront có sẵn bên ngoài. Bạn nên thêm các biện pháp kiểm soát bảo mật phù hợp với yêu cầu bảo mật của tổ chức vào giải pháp mẫu. Ví dụ: bạn có thể muốn [thêm xác thực vào CloudFront bằng Amazon Cognito và Lambda@Edge](https://github.com/awslabs/cognito-at-edge) để giúp ngăn chặn người dùng trái phép truy cập vào chatbot này. Bạn cũng có thể [định cấu hình quyền truy cập an toàn và hạn chế quyền truy cập vào nội dung](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/SecurityAndPrivateContent.html).

1. Điều hướng đến [CloudFormation](https://us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/) trong bảng điều khiển.
2. Trong phần **Stacks**, chọn **FrontendAppStack**.
3. Chọn **Output** tab.
4. Sao chép giá trị ReactAppUrl.

## **Điều tra với chatbot bảo mật của bạn**

Bây giờ bạn đã triển khai giải pháp mẫu và cấu hình các quyền phù hợp, bạn đã sẵn sàng sử dụng đầu vào ngôn ngữ tự nhiên để tạo và gọi các truy vấn SQL cũng như đề xuất sổ tay hướng dẫn ứng phó sự cố nội bộ.

### **Tạo và gọi các truy vấn SQL**

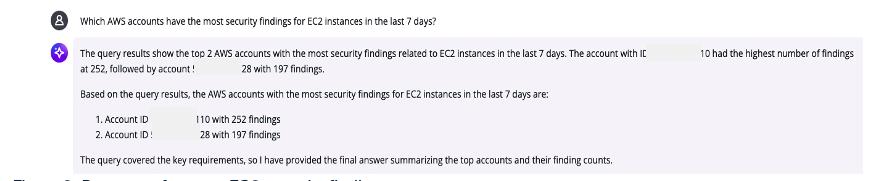
Mặc dù hầu hết các chuyên gia bảo mật đều biết cách tạo và gọi các truy vấn SQL, nhưng thời gian là cực kỳ quan trọng trong một sự kiện bảo mật có thể xảy ra. Việc thêm khả năng ngôn ngữ tự nhiên sang SQL vào tác nhân bảo mật có thể giúp giảm thời gian phản hồi trung bình của bạn, điều này có thể làm giảm tác động chung của một sự kiện bảo mật. Hơn nữa, bạn có thể sử dụng các kỹ thuật tương tự này để săn tìm mối đe dọa trong môi trường AWS của mình.

**Câu hỏi 1**: Tài khoản AWS nào có nhiều phát hiện bảo mật nhất đối với các phiên bản EC2 trong 7 ngày qua?

**Trả lời 1**: Kết quả truy vấn hiển thị hai tài khoản AWS hàng đầu có nhiều phát hiện bảo mật nhất liên quan đến các phiên bản EC2 trong 7 ngày qua. Tài khoản có ID XXXXXX10 có số phát hiện cao nhất là 252, tiếp theo là tài khoản XXXXXX28 với 197 phát hiện.

Câu hỏi đã đề cập đến các yêu cầu chính, vì vậy tôi đã cung cấp câu trả lời cuối cùng tóm tắt các tài khoản hàng đầu và số lượng phát hiện của họ.

Câu hỏi và câu trả lời được thể hiện ở Hình 2.



*Hình 2: Phản hồi cho hầu hết các phát hiện bảo mật EC2*

Bạn cung cấp càng nhiều ngữ cảnh cho chatbot thì truy vấn được tạo ra càng tốt. Cung cấp một khung thời gian cũng cung cấp một tập dữ liệu nhỏ hơn để xem xét và đưa ra kết quả nhanh hơn.

**Câu hỏi 2:** Trong các tài khoản AWS đó, loại phát hiện bảo mật EC2 hàng đầu là gì?

**Câu trả lời 2:** Dựa trên kết quả truy vấn, các loại phát hiện bảo mật EC2 hàng đầu trong các tài khoản AWS có nhiều phát hiện về phiên bản EC2 nhất trong 7 ngày qua là:

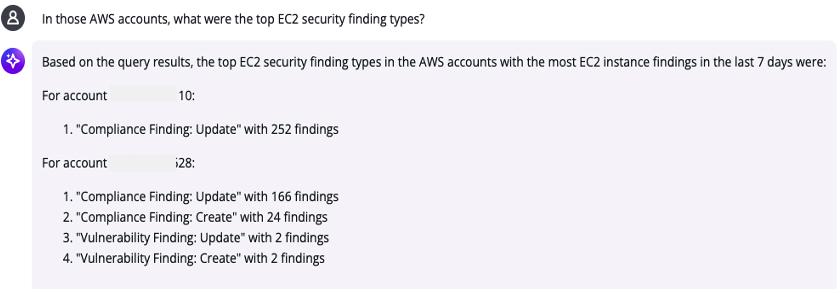
Đối với tài khoản XXXXXX10:

1. “Phát hiện tuân thủ: Cập nhật” với 252 phát hiện

Đối với tài khoản XXXXXX28:

1. “Cập nhật về việc tuân thủ” với 166 phát hiện
2. “Compliance Finding Create” với 24 phát hiện
3. “Phát hiện lỗ hổng: Cập nhật” với 2 phát hiện
4. “Phát hiện lỗ hổng: Tạo” với 2 phát hiện.

Câu hỏi và câu trả lời được thể hiện ở Hình 3.



*Hình 3: Phản hồi cho các loại phát hiện bảo mật EC2 hàng đầu*

Kết quả cho thấy các vấn đề chủ yếu liên quan đến các điều khiển Security Hub được ánh xạ tới type\_name cột OCSF. Nếu bạn muốn xem một cột khác, bạn có thể cung cấp hướng dẫn bổ sung hoặc cập nhật câu hỏi.

Câu hỏi 3 : Những phiên bản EC2 nào có lỗ hổng bảo mật?

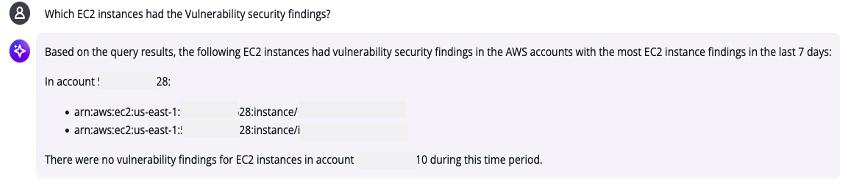
Câu trả lời 3 : Dựa trên kết quả truy vấn, các phiên bản EC2 sau đây có phát hiện lỗ hổng bảo mật trong tài khoản AWS với nhiều phát hiện phiên bản EC2 nhất trong 7 ngày qua:

Trong tài khoản XXXXXX28:

1. arn:aws:ec2:us-east-1: XXXXXX28:instance/<id-instance>
2. arn:aws:ec2:us-east-1: XXXXXX28:instance/<id-instance>

Không có phát hiện lỗ hổng nào đối với các phiên bản EC2 trong tài khoản XXXXXX10 trong khoảng thời gian này.

Câu hỏi và câu trả lời được thể hiện ở Hình 4.



*Hình 4: Phản hồi cho các trường hợp EC2 với các phát hiện về lỗ hổng bảo mật*

Trong câu hỏi này, phạm vi tìm kiếm được thu hẹp lại còn hai phiên bản [Amazon Elastic Compute Cloud (Amazon EC2)](https://aws.amazon.com/ec2) trong một tài khoản AWS cụ thể để xem xét sâu hơn.

### **Đề xuất các sổ tay hướng dẫn ứng phó sự cố**

Là một phần của giải pháp mẫu này, chúng tôi đã sử dụng kho lưu trữ [AWS Incident Response Playbook Samples](https://github.com/aws-samples/aws-incident-response-playbooks) GitHub và tải chúng lên thùng S3. Ngoài ra, bạn có thể tạo hoặc tham chiếu đến các playbook của riêng mình để điều tra và phản hồi các sự kiện bảo mật khác nhau để tham khảo. Sau mỗi câu hỏi, chatbot sẽ cung cấp câu trả lời cùng với URL Amazon S3 đến playbook. Nhà phân tích bảo mật phải có quyền phù hợp để tải playbook từ Amazon S3.

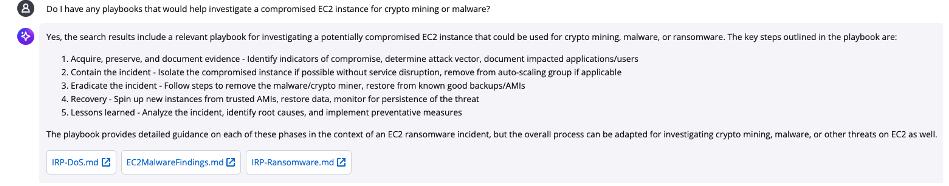
**Câu hỏi 1:** Tôi có hướng dẫn nào giúp điều tra phiên bản EC2 bị xâm phạm để khai thác tiền điện tử hoặc phần mềm độc hại không?

**Trả lời 1:** Có, kết quả tìm kiếm bao gồm một sổ tay hướng dẫn liên quan để điều tra một phiên bản EC2 có khả năng bị xâm phạm có thể được sử dụng để khai thác tiền điện tử, phần mềm độc hại hoặc phần mềm tống tiền. Các bước chính được nêu trong sổ tay hướng dẫn là:

1. Thu thập, lưu giữ và ghi lại bằng chứng – Xác định các chỉ số xâm phạm, xác định vectơ tấn công, ghi lại các ứng dụng/người dùng bị ảnh hưởng
2. Kiểm soát sự cố – ​​Cô lập phiên bản bị xâm phạm nếu có thể mà không làm gián đoạn dịch vụ, xóa khỏi nhóm tự động mở rộng nếu có thể
3. Xóa bỏ sự cố – ​​Thực hiện theo các bước để xóa phần mềm độc hại/trình đào tiền điện tử, khôi phục từ các bản sao lưu/AMI tốt đã biết
4. Phục hồi – Tạo các phiên bản mới từ AMI đáng tin cậy, khôi phục dữ liệu và theo dõi sự tồn tại của mối đe dọa
5. Bài học kinh nghiệm – Phân tích sự cố, xác định nguyên nhân gốc rễ và thực hiện các biện pháp phòng ngừa

Sổ tay hướng dẫn cung cấp hướng dẫn chi tiết về từng giai đoạn này trong bối cảnh sự cố ransomware EC2, nhưng quy trình chung có thể được điều chỉnh để điều tra hoạt động khai thác tiền điện tử, phần mềm độc hại hoặc các mối đe dọa khác trên EC2.

Câu hỏi và câu trả lời được thể hiện ở Hình 5.



*Hình 5: Phản hồi cho sổ tay EC2 IR*

Bài tập săn tìm mối đe dọa trước đó đã xác định được hai trường hợp EC2 có lỗ hổng. Sau khi điều tra thêm, nếu một nhà phân tích bảo mật tin rằng trường hợp EC2 bị xâm phạm, họ có thể yêu cầu một sổ tay IR để phản hồi sự kiện bảo mật. Sau khi xác định được sổ tay nào có ý nghĩa nhất, họ có thể nhấp vào URL S3 hoặc xem các sổ tay khác để sử dụng.

**Câu hỏi 2:** Tôi có cẩm nang nào giúp ứng phó với phần mềm tống tiền trong thùng S3 của mình không?

**Trả lời 2:** Có, kết quả tìm kiếm bao gồm một sổ tay hướng dẫn có thể giúp ứng phó với sự cố ransomware liên quan đến thùng S3. “Mẫu sổ tay hướng dẫn ứng phó sự cố khi truy cập ngoài ý muốn vào thùng Amazon S3” phác thảo các bước cho:

1. Thu thập bằng chứng về việc truy cập không mong muốn
2. Kiểm soát sự cố bằng cách hạn chế quyền truy cập vào các thùng bị ảnh hưởng
3. Loại bỏ vấn đề bằng cách xóa bất kỳ dữ liệu/đối tượng độc hại nào và khôi phục từ bản sao lưu
4. Phục hồi bằng cách kích hoạt lại quyền truy cập vào thùng cho người dùng hợp lệ
5. Thực hiện các hoạt động sau sự cố như xem xét nhật ký, xác định nguyên nhân gốc rễ và thực hiện các biện pháp phòng ngừa

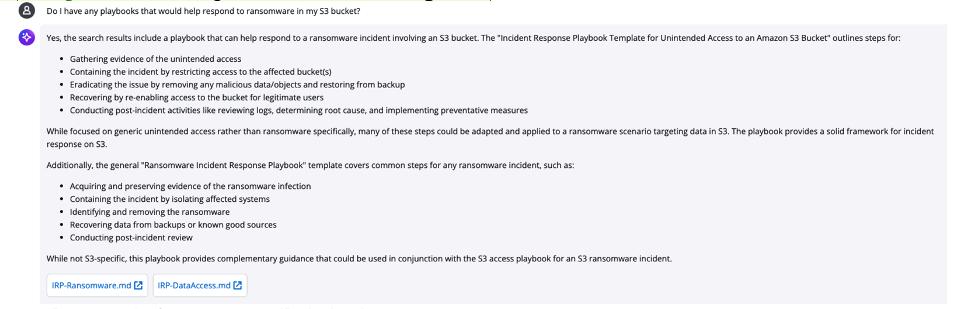
Mặc dù tập trung vào truy cập chung không mong muốn hơn là ransomware cụ thể, nhiều bước trong số này có thể được điều chỉnh và áp dụng cho kịch bản ransomware nhắm vào dữ liệu trong S3. Sổ tay hướng dẫn cung cấp một khuôn khổ vững chắc để ứng phó sự cố trên S3.

Ngoài ra, mẫu “Sổ tay ứng phó sự cố ransomware” chung bao gồm các bước chung cho mọi sự cố ransomware, chẳng hạn như:

1. Thu thập và lưu giữ bằng chứng về nhiễm phần mềm tống tiền
2. Kiểm soát sự cố bằng cách cô lập các hệ thống bị ảnh hưởng
3. Xác định và loại bỏ phần mềm tống tiền
4. Phục hồi dữ liệu từ bản sao lưu hoặc các nguồn đáng tin cậy
5. Tiến hành đánh giá sau sự cố

Mặc dù không dành riêng cho S3, nhưng sổ tay này cung cấp hướng dẫn bổ sung có thể được sử dụng cùng với sổ tay truy cập S3 cho sự cố ransomware S3.

Câu hỏi và câu trả lời được thể hiện ở Hình 6.



*Hình 6: Phản hồi cho sổ tay IR ransomware S3*

Phản hồi cung cấp cái nhìn tổng quan cấp cao về sổ tay hướng dẫn cụ thể đang được tham chiếu để cung cấp cho nhà phân tích bối cảnh trước khi đi sâu hơn vào bất kỳ sổ tay hướng dẫn nào.

### **Thêm chức năng cho chatbot bảo mật**

Giải pháp mẫu này được phát triển để thể hiện nghệ thuật của khả năng. Mỗi khách hàng sử dụng tài nguyên AWS để giải quyết nhu cầu kinh doanh theo cách riêng của họ và các nhóm bảo mật phải được trang bị phù hợp để giúp bảo vệ môi trường tương ứng của họ. Sau đây là một số cải tiến khả thi mà bạn có thể kết hợp vào giải pháp mẫu để phù hợp với các trường hợp sử dụng và nhu cầu bảo mật của mình.

1. Kết hợp bảng [Amazon DynamoDB](https://aws.amazon.com/dynamodb/) để sử dụng như một phần của báo cáo tương tác liên quan đến một sự kiện cụ thể hoặc tìm GUID. Bằng cách kết hợp dấu vết kiểm toán, bạn có thể liên kết các hành động do tác nhân và các tài nguyên liên quan thực hiện với một sự kiện bảo mật và xác thực kết quả điều tra trước khi thực hiện hành động.
2. Điều chỉnh tác nhân chatbot ở phía sau để truy vấn [danh sách các lỗ hổng và điểm dễ bị tấn công phổ biến (CVE) của Trung tâm bảo mật Amazon Linux](https://explore.alas.aws.amazon.com/) hoặc [danh sách CVE của MITRE](https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=aws) để xem tài nguyên AWS nào có thể nằm trong phạm vi và gửi tin nhắn hợp nhất tới chủ sở hữu tài nguyên với các hành động được đề xuất.
3. Điều chỉnh tác nhân chatbot ở phía sau để tiếp nhận các yêu cầu ngôn ngữ tự nhiên và phản hồi bằng [các trình phát hiện hoặc quy tắc tương quan cho Amazon OpenSearch](https://docs.aws.amazon.com/opensearch-service/latest/developerguide/security-analytics.html) hoặc ngôn ngữ truy vấn để phát hiện tùy chỉnh trong công cụ quản lý sự kiện và thông tin bảo mật (SIEM) của bạn.
4. Thêm nguồn dữ liệu mới vào Athena, [chẳng hạn như AWS Config](https://aws.amazon.com/blogs/mt/how-to-query-your-aws-resource-configuration-states-using-aws-config-and-amazon-athena/) , để cung cấp cho nhà phân tích các khả năng bổ sung để truy vấn cấu hình tài nguyên AWS trên toàn bộ môi trường AWS có thể bị ảnh hưởng bởi sự kiện bảo mật. Ví dụ: nếu phát hiện bảo mật cho thấy một thùng S3 đã được công khai, hãy truy vấn những thay đổi cấu hình nào và khi nào đã được thực hiện đối với thùng S3.
5. Kết hợp [điều phối đa tác nhân](https://github.com/awslabs/multi-agent-orchestrator) để mở rộng việc sử dụng nhiều tác nhân Amazon Bedrock có thể được điều chỉnh theo các trường hợp sử dụng bảo mật thích hợp của các nhóm tương ứng. Chatbot có thể nói chuyện trực tiếp với bộ phân loại hoặc bộ điều khiển, sau đó bộ phân loại hoặc bộ điều khiển sẽ giải quyết yêu cầu ngôn ngữ tự nhiên của người dùng và điều phối trên một hoặc nhiều tác nhân để tạo phản hồi. Ví dụ: nếu người dùng hỏi phiên bản EC2 nào có thể bị ảnh hưởng bởi sự kiện bảo mật và sử dụng sổ tay hướng dẫn nào để phản hồi, tác nhân phân loại có thể chuyển hướng truy vấn ban đầu đến tác nhân trong giải pháp mẫu này. Trong cùng một cửa sổ trò chuyện, nhà phân tích có thể hỏi xem có bất kỳ CVE nào đang mở cho các phiên bản EC2 trong phạm vi để có danh sách các CVE cần giải quyết trong tài khoản AWS hay không.
6. Đối với các truy vấn Athena chạy lâu, bạn có thể kết hợp [AWS Step Function](https://docs.aws.amazon.com/step-functions/) vào quy trình làm việc và [kết hợp mã thông báo tác vụ](https://docs.aws.amazon.com/step-functions/latest/dg/connect-to-resource.html#connect-wait-token) để chờ kết quả Athena trả về.

## **Dọn dẹp**

Nếu bạn triển khai giải pháp mẫu chatbot bảo mật bằng cách sử dụng nút Launch Stack và bảng điều khiển có mẫu CloudFormation security\_genai\_chatbot\_cfn, hãy thực hiện như sau để dọn dẹp:

1. Trong [bảng điều khiển CloudFormation](https://us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1) của tài khoản và Khu vực nơi bạn triển khai giải pháp, hãy chọn ngăn xếp SecurityGenAIChatbot.
2. Chọn tùy chọn Xóa ngăn xếp.

Nếu bạn triển khai giải pháp bằng cách sử dụng AWS CDK, hãy chạy lệnh cdk destroy --all.

## **Phần kết luận**

Giải pháp mẫu minh họa cách bạn có thể sử dụng các tác nhân Amazon Bedrock hướng tác vụ và đầu vào ngôn ngữ tự nhiên để giúp đẩy nhanh quá trình điều tra và phân tích cũng như tăng cường thế trận bảo mật tổng thể của bạn. Chúng tôi đã cung cấp một ví dụ về giải pháp mẫu với giao diện người dùng được hỗ trợ bởi tác nhân Amazon Bedrock, mà bạn có thể mở rộng để thêm các tác nhân hướng tác vụ bổ sung, mỗi tác nhân có hướng dẫn, cơ sở kiến ​​thức và mô hình riêng. Bằng cách mở rộng việc sử dụng các tác nhân hỗ trợ AI, bạn có thể giúp nhóm bảo mật của mình hoạt động hiệu quả hơn trên nhiều miền bảo mật trong môi trường AWS của bạn.

Phần phụ trợ cho chatbot để điều tra các sự kiện bảo mật sử dụng Security Lake, giúp chuẩn hóa dữ liệu thành [Open Cybersecurity Schema Framework (OCSF)](https://docs.aws.amazon.com/security-lake/latest/userguide/open-cybersecurity-schema-framework.html); miễn là lược đồ dữ liệu được chuẩn hóa, giải pháp có thể được áp dụng cho các hồ dữ liệu khác trong môi trường AWS của bạn.

Để tìm hiểu thêm, hãy xem các bài đăng khác trong loạt bài này:

* [Phần 1: Tạo thông tin chi tiết về máy học cho dữ liệu Amazon Security Lake bằng Amazon SageMaker](https://aws.amazon.com/blogs/security/generate-machine-learning-insights-for-amazon-security-lake-data-using-amazon-sagemaker/)
* [Phần 2: Tạo thông tin chi tiết hỗ trợ AI cho Amazon Security Lake bằng Amazon SageMaker Studio và Amazon Bedrock](https://aws.amazon.com/blogs/security/generate-ai-powered-insights-for-amazon-security-lake-using-amazon-sagemaker-studio-and-amazon-bedrock/)

Sử dụng phần bình luận để cung cấp phản hồi. Nếu bạn có thắc mắc về bài đăng này, hãy bắt đầu một chủ đề mới trên [Generative AI trên AWS re:Post](https://repost.aws/selections/KPEKXMuRyuSyyxnsuruRrtlg/generative-ai-on-aws) hoặc [liên hệ với AWS Support](https://console.aws.amazon.com/support/home).