| **ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**  Logo  Description automatically generated  **BÁO CÁO ĐỒ ÁN**  **MÔN: AN TOÀN MẠNG MÁY TÍNH NÂNG CAO.**  **HỌC KỲ: II.**  **NĂM HỌC: 2022-2023.**  **Đề tài: Tìm hiểu và triển khai Database Security (Data Sunrise, DBHawk, ACRA).**  Giảng viên hướng dẫn: **Nguyễn Duy.**  **Lớp: NT534.N21.ANTT-VN.**  **Nhóm thực hiện: 10.**   | **STT** | **Họ và tên** | **MSSV** | | --- | --- | --- | | 1 | Nguyễn Phúc Hải | 20521281 | | 2 | Trần Xuân Nam | 20521637 | | 3 | Đỗ Minh Thọ | 20521972 | | 4 | Ngô Hùng Thịnh | 20521961 |   ***Thành phố Hồ Chí Minh, ngày 22 tháng 04 năm 2023.*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

**MỤC LỤC**

Nội dung

[**BẢNG PHÂN CÔNG NHIỆM VỤ 3**](#_gjdgxs)

[**LỜI MỞ ĐẦU 4**](#_30j0zll)

[**ĐẶT VẤN ĐỀ 5**](#_1fob9te)

[**MỤC TIÊU 6**](#_3znysh7)

[**NỘI DUNG CHÍNH CỦA ĐỒ ÁN 7**](#_2et92p0)

[**I. Tìm hiểu và triển khai Database Security (Data Sunrise, DBHawk, ACRA). 7**](#_tyjcwt)

[**1. Giới thiệu chung về Database Security. 7**](#_3dy6vkm)

[**2. Tìm hiểu về Data Sunrise. 7**](#_1t3h5sf)

[**3. Tìm hiểu về DBHawk. 8**](#_4d34og8)

[**4. Tìm hiểu về ACRA. 9**](#_2s8eyo1)

[**5. So sánh. 9**](#_17dp8vu)

[**II. Những tính năng của Database Security: Active Monitor, DBF, Data Masking, Performance Monitoring, Sensitive Data Discovery. 11**](#_3rdcrjn)

[**1. Active Monitor. 11**](#_26in1rg)

[**2. Database Firewall. 13**](#_lnxbz9)

[**3. Data Masking. 15**](#_35nkun2)

[**4. Performance Monitoring. 16**](#_1ksv4uv)

[**5. Sensitive Data Discovery. 18**](#_44sinio)

[**III. Giả lập ngữ cảnh để kiểm tra tính năng hoạt động. 21**](#_2jxsxqh)

[**1. Ngữ cảnh 1. 21**](#_z337ya)

[**2. Ngữ cảnh 2. 22**](#_3j2qqm3)

[**3. Ngữ cảnh 3. 23**](#_1y810tw)

[**4. Ngữ cảnh 4. 23**](#_4i7ojhp)

[**IV. Đề xuất phương pháp cải thiện. 24**](#_2xcytpi)

[**1. Xác định nhu cầu bảo mật dữ liệu của doanh nghiệp. 24**](#_1ci93xb)

[**2. Lựa chọn giải pháp bảo mật dữ liệu phù hợp. 24**](#_3whwml4)

[**3. Triển khai giải pháp bảo mật dữ liệu. 24**](#_2bn6wsx)

[**4. Đào tạo nhân viên sử dụng giải pháp bảo mật dữ liệu. 25**](#_qsh70q)

[**LỜI CẢM ƠN 26**](#_3as4poj)

# **BẢNG PHÂN CÔNG NHIỆM VỤ**

| **STT** | **MSSV** | **Họ và tên** | **Vai trò** | **Ghi chú** |
| --- | --- | --- | --- | --- |
| **1** | **20521281** | **Nguyễn Phúc Hải** | **Tìm kiếm tổng hợp nội dung và viết báo cáo.** |  |
| **2** | **20521637** | **Trần Xuân Nam** | **Thực hiện Demo đồ án.** |  |
| **3** | **20521972** | **Đỗ Minh Thọ** | **Thực hiện Demo đồ án.** |  |
| **4** | **20521961** | **Ngô Hùng Thịnh** | **Làm slide và thuyết trình. (Giữa kỳ + cuối kỳ).** |  |

# **LỜI MỞ ĐẦU**

Bảo mật dữ liệu là một trong những vấn đề quan trọng nhất trong lĩnh vực công nghệ thông tin, đặc biệt là khi dữ liệu trở nên ngày càng phổ biến và quan trọng hơn trong các doanh nghiệp và tổ chức.

Trong báo cáo này, nhóm em sẽ tìm hiểu và triển khai một số giải pháp bảo mật cơ sở dữ liệu, tìm hiểu các tính năng chính của các giải pháp này, bao gồm Active Monitor, DBF, Data Masking, Performance Monitoring và Sensitive Data Discovery.

Ngoài ra, nhóm đồ án cũng sẽ giả lập một số ngữ cảnh để kiểm tra các tính năng này hoạt động như thế nào và đánh giá tính hiệu quả của các giải pháp bảo mật cơ sở dữ liệu này.

Hy vọng rằng báo cáo đồ án này sẽ cung cấp cho các bạn cùng lớp những kiến thức cơ bản về Database Security và giúp mọi người hiểu rõ hơn về các giải pháp bảo mật cơ sở dữ liệu hiện nay.

# **ĐẶT VẤN ĐỀ**

Với sự phát triển không ngừng của công nghệ thông tin, các hệ thống cơ sở dữ liệu đã trở nên vô cùng phổ biến và quan trọng đối với các doanh nghiệp. Tuy nhiên, vấn đề an ninh thông tin luôn được đặt lên hàng đầu để đảm bảo tính bảo mật của dữ liệu quan trọng của doanh nghiệp. Trong thực tế, rủi ro bị mất dữ liệu, bị tấn công mạng hoặc bị lộ thông tin đã trở thành những vấn đề phổ biến và đe dọa tới sự tồn tại của doanh nghiệp.

Để giải quyết vấn đề bảo mật dữ liệu cơ sở dữ liệu, các giải pháp Database Security đã được đưa ra. Tuy nhiên, các tính năng của Database Security như Active Monitor, DBF, Data Masking, Performance Monitoring, Sensitive Data Discovery vẫn chưa được rõ ràng và nhiều doanh nghiệp vẫn chưa hiểu hết tác dụng của chúng.

Để giải quyết vấn đề này, việc tìm hiểu và triển khai Database Security trở nên cực kỳ cần thiết. Các doanh nghiệp cần phải thực hiện giả lập ngữ cảnh để kiểm tra và đánh giá tính năng của các giải pháp Database Security. Điều này giúp cho doanh nghiệp có thể đưa ra quyết định chính xác và hiệu quả về việc triển khai giải pháp bảo mật dữ liệu cơ sở dữ liệu phù hợp nhất.

Vì vậy, tìm hiểu và triển khai Database Security (Data Sunrise, DBHawk, ACRA) là một vấn đề không thể bỏ qua trong quá trình quản lý và bảo mật dữ liệu của doanh nghiệp. Các tính năng của Database Security cần được hiểu rõ để đảm bảo tính bảo mật cho dữ liệu của doanh nghiệp và giảm thiểu rủi ro bị tấn công mạng hoặc mất dữ liệu quan trọng.

# **MỤC TIÊU**

Mục tiêu của đồ án này trong thời gian học tập môn An toàn mạng máy tính nâng cao có thể tìm hiểu và nghiên cứu và thực hiện triển khai một số giải pháp Database Security, để đảm bảo an toàn và bảo mật cho hệ thống cơ sở dữ liệu của doanh nghiệp. Đồng thời, đề xuất phương pháp giả lập ngữ cảnh để kiểm tra các tính năng của các giải pháp bảo mật dữ liệu, bao gồm Active Monitor, DBF, Data Masking, Performance Monitoring, Sensitive Data Discovery.

Hoàn thành tốt học phần, cũng cố thêm các kiên thức về bảo mật mạng và chuẩn bị cho các học kỳ sắp tới.

# **NỘI DUNG CHÍNH CỦA ĐỒ ÁN**

## **I. Tìm hiểu và triển khai Database Security (Data Sunrise, DBHawk, ACRA).**

### **1. Giới thiệu chung về Database Security.**

Database Security là một khái niệm quan trọng trong lĩnh vực bảo mật thông tin, đặc biệt là khi các tổ chức và doanh nghiệp ngày càng phụ thuộc nhiều vào các cơ sở dữ liệu để lưu trữ và quản lý thông tin. Database Security đảm bảo rằng các cơ sở dữ liệu được bảo vệ khỏi các cuộc tấn công bên ngoài và bên trong, đồng thời giúp đảm bảo tính toàn vẹn, sự riêng tư và tính sẵn sàng của các thông tin được lưu trữ.

Thực tế, các cuộc tấn công mạng vào các cơ sở dữ liệu trở nên ngày càng phổ biến và phức tạp hơn, đòi hỏi các hệ thống bảo mật càng phải được tối ưu hóa và nâng cao. Các vụ việc lỗ hổng bảo mật dữ liệu đã và đang gây ra tổn thất về tiền bạc và danh tiếng đối với các công ty và tổ chức. Chính vì vậy, việc đầu tư vào các giải pháp bảo mật dữ liệu và triển khai chúng là một điều cần thiết để bảo vệ thông tin quan trọng của các tổ chức và doanh nghiệp.

Các giải pháp Database Security hiện nay cung cấp nhiều tính năng và công nghệ để bảo vệ các cơ sở dữ liệu, bao gồm Active Monitor, Data Masking, Sensitive Data Discovery, Performance Monitoring, và DBF. Tuy nhiên, để đảm bảo hiệu quả của các giải pháp này, các tổ chức và doanh nghiệp cần thực hiện việc giả lập ngữ cảnh để kiểm tra tính năng hoạt động của các giải pháp bảo mật, đồng thời đưa ra các chiến lược bảo mật phù hợp với nhu cầu và quy mô của mình.

### **2. Tìm hiểu về Data Sunrise.**

Data Sunrise là một phần mềm Database Security được thiết kế để bảo vệ cơ sở dữ liệu trước các mối đe dọa bảo mật như vi phạm dữ liệu, tấn công SQL Injection, tấn công từ chối dịch vụ (DDoS), và nhiều loại tấn công khác.

Phần mềm Data Sunrise cung cấp cho người dùng khả năng giám sát liên tục hành vi truy cập dữ liệu để phát hiện và ngăn chặn các hành vi truy cập trái phép. Nó cũng cung cấp cho người dùng khả năng điều chỉnh các quy tắc bảo mật, sử dụng mã hóa dữ liệu, và kiểm soát quyền truy cập vào dữ liệu để bảo vệ cơ sở dữ liệu của họ.

Trong thực tế, Data Sunrise đã được sử dụng rộng rãi trong các tổ chức lớn, chẳng hạn như các công ty tài chính, ngân hàng, chính phủ, y tế, giáo dục, và nhiều lĩnh vực khác. Việc bảo vệ thông tin nhạy cảm của khách hàng và doanh nghiệp luôn là một ưu tiên hàng đầu, và Data Sunrise giúp đảm bảo rằng thông tin này được bảo vệ an toàn và an ninh.

Data Sunrise cung cấp nhiều tính năng bảo mật cơ sở dữ liệu, bao gồm:

* **Sensitive Data Discovery:** Tìm kiếm các thông tin nhạy cảm trong cơ sở dữ liệu để giảm thiểu rủi ro về bảo mật.
* **Active Monitor:** Giám sát hoạt động của cơ sở dữ liệu để phát hiện và ngăn chặn các cuộc tấn công.
* **Data Masking:** Ẩn thông tin quan trọng khỏi các người dùng không được phép truy cập.
* **Performance Monitoring:** Giám sát tài nguyên hệ thống để đảm bảo hiệu suất cơ sở dữ liệu và ngăn chặn các sự cố.
* **DB Firewall:** Ngăn chặn các cuộc tấn công từ bên ngoài bằng cách định tuyến các yêu cầu truy cập cơ sở dữ liệu.

### **3. Tìm hiểu về DBHawk.**

DBHawk là một phần mềm giám sát cơ sở dữ liệu, bảo vệ an ninh và quản lý hiệu suất của các hệ thống cơ sở dữ liệu. DBHawk cung cấp các tính năng như Active Monitor để theo dõi và cảnh báo các hoạt động đáng ngờ trong hệ thống cơ sở dữ liệu, DBF (Database Firewall) để giảm thiểu rủi ro an ninh và giữ an toàn cho dữ liệu, Data Masking để ẩn danh thông tin nhạy cảm, Performance Monitoring để theo dõi và tối ưu hóa hiệu suất cơ sở dữ liệu và Sensitive Data Discovery để tìm kiếm và xử lý dữ liệu nhạy cảm trong cơ sở dữ liệu.

DBHawk có thể giả lập các tình huống khác nhau để kiểm tra và đánh giá hiệu quả hoạt động của các tính năng. Chẳng hạn, khi giả lập một tình huống có sự xâm nhập trái phép vào hệ thống cơ sở dữ liệu, Active Monitor của DBHawk sẽ tự động phát hiện và cảnh báo cho người quản trị biết. Khi áp dụng tính năng Data Masking, DBHawk sẽ ẩn danh thông tin nhạy cảm trong cơ sở dữ liệu để đảm bảo an toàn cho dữ liệu của khách hàng. Các tính năng khác của DBHawk cũng có thể được giả lập để đánh giá hiệu quả hoạt động trong các tình huống khác nhau.

### **4. Tìm hiểu về ACRA.**

ACRA là một phần mềm bảo mật dữ liệu cở sở dữ liệu mã nguồn mở được phát triển để bảo vệ dữ liệu của người dùng trước các cuộc tấn công. ACRA cung cấp chức năng mã hóa và lưu trữ dữ liệu bảo mật. Phần mềm hoạt động như một thư viện mã nguồn mở được tích hợp vào các ứng dụng. ACRA hỗ trợ mã hóa dữ liệu theo cơ chế mã khóa bí mật, giúp bảo vệ dữ liệu đến mức cao nhất.

Ngoài tính năng mã hóa dữ liệu, ACRA còn có tính năng phát hiện và giải mã các dạng tấn công như SQL Injection, Man-In-The-Middle, giúp đảm bảo an ninh cho cơ sở dữ liệu. ACRA cũng cho phép phát hiện và báo cáo các lỗi truy cập cơ sở dữ liệu không hợp lệ và các hoạt động đáng ngờ khác.

Với cách thức hoạt động như một thư viện, ACRA được tích hợp vào các ứng dụng cơ sở dữ liệu để giúp bảo vệ dữ liệu của người dùng. ACRA cũng hỗ trợ các ứng dụng trên nhiều nền tảng khác nhau, cho phép triển khai trên các hệ thống khác nhau.

### **5. So sánh.**

#### **Khái niệm kiến trúc.**

***Data Sunrise:*** Data Sunrise là một phần mềm bảo mật cơ sở dữ liệu và sử dụng phương pháp Data Masking để ẩn danh hoặc mã hóa dữ liệu. Data Sunrise hoạt động trên các cơ sở dữ liệu phổ biến như Oracle, Microsoft SQL Server, MySQL, PostgreSQL, và MongoDB.

***DBHawk:*** DBHawk là một phần mềm quản lý cơ sở dữ liệu và bảo mật dữ liệu, với khả năng giám sát và báo cáo hiệu suất cơ sở dữ liệu. DBHawk hỗ trợ nhiều cơ sở dữ liệu phổ biến, bao gồm Oracle, Microsoft SQL Server, MySQL, PostgreSQL, và MongoDB.

***ACRA:*** ACRA là một thư viện mã nguồn mở để bảo vệ dữ liệu trên các ứng dụng. ACRA cung cấp tính năng mã hóa và lưu trữ dữ liệu bảo mật.

#### **Chức năng và cách hoạt động.**

***Data Sunrise:*** Data Sunrise cung cấp nhiều tính năng như Active Monitor, DBF, Data Masking, Performance Monitoring và Sensitive Data Discovery. Phần mềm hoạt động bằng cách cung cấp các luồng dữ liệu giám sát và chặn các luồng dữ liệu không an toàn. Các tính năng bảo mật như Data Masking giúp che giấu dữ liệu nhạy cảm để tránh các vấn đề về bảo mật.

***DBHawk:*** DBHawk cung cấp các tính năng như quản lý cơ sở dữ liệu, giám sát và báo cáo hiệu suất, giám sát và bảo vệ dữ liệu. Phần mềm hoạt động bằng cách sử dụng các chức năng giám sát và bảo vệ cơ sở dữ liệu, đồng thời cung cấp báo cáo và phân tích dữ liệu để cải thiện hiệu suất và an ninh của cơ sở dữ liệu.

***ACRA:*** ACRA cung cấp tính năng mã hóa và lưu trữ dữ liệu bảo mật. Phần mềm hoạt động như một thư viện mã nguồn mở được tích hợp vào các ứng dụng.

#### **Cách triển khai và ưu nhược điểm.**

***Data Sunrise:*** Data Sunrise có thể triển khai trên các môi trường đám mây hoặc trên trang web. Nhược điểm của Data Sunrise là giá cả khá đắt. Ngoài ra, việc triển khai Data Sunrise có thể đòi hỏi sự hỗ trợ từ các chuyên gia về an ninh mạng hoặc kỹ thuật viên có chuyên môn về cơ sở dữ liệu. Tuy nhiên, với các tính năng như Active Monitor, DBF, Data Masking, Performance Monitoring, Sensitive Data Discovery, Data Sunrise là một giải pháp đáng tin cậy cho việc bảo vệ dữ liệu của các tổ chức.

***DBHawk:*** Việc triển khai trên môi trường đám mây hoặc trên trang web cũng rất dễ dàng. DBHawk cung cấp tính năng quản lý và giám sát cơ sở dữ liệu mạnh mẽ, đồng thời cho phép tùy chỉnh và điều chỉnh cấu hình một cách linh hoạt. Tuy nhiên, giá cả của DBHawk cũng khá đắt và không hỗ trợ tốt cho các cơ sở dữ liệu phi cấu trúc.

***ACRA:*** Là một thư viện mã nguồn mở được tích hợp vào các ứng dụng để cung cấp chức năng mã hóa và lưu trữ dữ liệu bảo mật. Vì vậy, việc triển khai ACRA khá đơn giản và không đòi hỏi nhiều sự hỗ trợ từ các chuyên gia về an ninh mạng hoặc kỹ thuật viên có chuyên môn về cơ sở dữ liệu. Tuy nhiên, ACRA chỉ cung cấp một số tính năng bảo mật cơ bản và không thực sự phù hợp cho các tổ chức có nhu cầu bảo vệ dữ liệu quan trọng và nhạy cảm.

Tóm lại, mỗi giải pháp triển khai Database Security có những ưu điểm và nhược điểm riêng. Việc lựa chọn giải pháp phù hợp với nhu cầu của tổ chức là rất quan trọng để đảm bảo an toàn và bảo mật cho dữ liệu của mình.

## **II. Những tính năng của Database Security: Active Monitor, DBF, Data Masking, Performance Monitoring, Sensitive Data Discovery.**

### **1. Active Monitor.**

#### **Khái niệm:**

Activity Monitor trên Mac tương đương với Task Manager trên Windows. Activity Monitor hiển thị nhiều loại tài nguyên được sử dụng trên hệ thống trong thời gian thực, bao gồm các tiến trình, hoạt động của ổ đĩa, việc sử dụng bộ nhớ và nhiều thứ khác, cho người dùng cái nhìn toàn cảnh về những gì đang xảy ra trên máy Mac.

#### **Kiến trúc.**

Kiến trúc của Active Monitor thường bao gồm một số lượng các cảm biến (Sensors) được triển khai trên các máy chủ cơ sở dữ liệu để giám sát các hoạt động của cơ sở dữ liệu, cùng với một trung tâm giám sát (Monitoring center) để phân tích và báo cáo các sự cố.

#### **Chức năng.**

***Giám sát các hoạt động cơ sở dữ liệu:*** Active Monitor giám sát các hoạt động cơ sở dữ liệu như truy cập, thao tác dữ liệu và thay đổi cấu trúc dữ liệu.

***Phát hiện các mối đe dọa an ninh:*** Active Monitor phát hiện các mối đe dọa an ninh bao gồm các cuộc tấn công từ bên ngoài, các hành vi xấu của người dùng và các hoạt động không phù hợp.

***Cảnh báo và phản ứng:*** Active Monitor có thể cảnh báo người quản trị hệ thống khi phát hiện các mối đe dọa an ninh và kích hoạt các biện pháp phản ứng để ngăn chặn các cuộc tấn công.

#### **Cách hoạt động.**

Cách hoạt động của Active Monitor là thông qua việc giám sát các hoạt động của cơ sở dữ liệu bằng cách lắng nghe và phân tích các tín hiệu từ các cảm biến. Nó sử dụng các thuật toán phân tích dữ liệu để xác định các mối đe dọa an ninh và phát hiện các hành vi không phù hợp.

#### **Cách triển khai.**

Cách triển khai của Active Monitor thường bao gồm việc triển khai các cảm biến trên các máy chủ cơ sở dữ liệu và kết nối chúng với trung tâm giám sát. Các giải pháp bảo mật cơ sở dữ liệu như Data Sunrise, DBHawk và ACRA cũng cung cấp các công cụ để triển khai và quản lý Active Monitor.

#### **Ưu điểm và nhược điểm.**

***Ưu điểm:***

* Giúp người quản trị hệ thống giám sát hoạt động cơ sở dữ liệu và phát hiện các mối đe dọa an ninh trong thời gian thực.
* Có thể cảnh báo sớm các cuộc tấn công hoặc các hoạt động độc hại trên database.
* Cung cấp các tính năng giám sát và quản lý các hoạt động của người dùng trên database, giúp ngăn chặn các lỗi hoặc sai sót do con người gây ra.
* Có khả năng tùy chỉnh và cấu hình để đáp ứng các yêu cầu bảo mật cụ thể của từng tổ chức.
* Giúp cải thiện khả năng phòng ngừa, đối phó và giải quyết các vấn đề bảo mật một cách nhanh chóng và hiệu quả.

***Nhược điểm:***

* Có thể gây ra tình trạng giảm hiệu suất hệ thống nếu không được cấu hình chính xác.
* Không thể ngăn chặn tất cả các cuộc tấn công và lỗ hổng bảo mật.
* Yêu cầu kỹ năng chuyên môn cao để triển khai và cấu hình.
* Chi phí đầu tư ban đầu có thể khá cao.

### **2. Database Firewall.**

#### **Khái niệm:**

Database Firewall (DBF) là một giải pháp bảo mật cơ sở dữ liệu có chức năng giám sát và điều khiển truy cập vào cơ sở dữ liệu. Nó được sử dụng để ngăn chặn các cuộc tấn công vào cơ sở dữ liệu và bảo vệ dữ liệu quan trọng khỏi các hành vi trái phép.

#### **Kiến trúc.**

DBF được triển khai trên một tường lửa ở trung tâm mạng. Nó có thể hoạt động trực tiếp trên máy chủ cơ sở dữ liệu hoặc thông qua proxy. DBF được cấu hình để kiểm soát các truy cập vào cơ sở dữ liệu từ các máy khách hoặc ứng dụng.

#### **Chức năng.**

* ***Kiểm soát truy cập vào cơ sở dữ liệu:*** DBF có thể kiểm soát các truy cập vào cơ sở dữ liệu bằng cách cho phép hoặc từ chối các yêu cầu truy cập tới cơ sở dữ liệu.
* ***Kiểm soát quyền truy cập:*** DBF có thể kiểm soát quyền truy cập vào cơ sở dữ liệu cho các tài khoản người dùng cụ thể.
* ***Phát hiện và ngăn chặn các cuộc tấn công:*** DBF có thể phát hiện và ngăn chặn các cuộc tấn công bằng cách giám sát các yêu cầu truy cập vào cơ sở dữ liệu và ngăn chặn các hoạt động bất thường.
* ***Bảo vệ dữ liệu quan trọng:*** DBF có thể bảo vệ dữ liệu quan trọng khỏi các hành vi trái phép bằng cách chặn các yêu cầu truy cập đến cơ sở dữ liệu.

#### **Cách hoạt động.**

Khi một yêu cầu truy cập cơ sở dữ liệu được gửi từ một máy khách hoặc ứng dụng, DBF sẽ kiểm tra yêu cầu này với các quy tắc được cấu hình để xác định liệu yêu cầu này có thể được chấp nhận hay không. Nếu yêu cầu được phê duyệt, DBF sẽ chuyển tiếp yêu cầu này tới cơ sở dữ liệu. Nếu yêu cầu không được phê duyệt, DBF sẽ từ chối yêu cầu và thông báo cho người quản trị hệ thống.

#### **Cách triển khai.**

DBF có thể triển khai trên nhiều nền tảng hệ thống quản trị cơ sở dữ liệu, bao gồm MySQL, Oracle, SQL Server, PostgreSQL, IBM DB2, MongoDB, và nhiều hơn nữa. Thường thì việc triển khai DBF được thực hiện thông qua việc cài đặt một phần mềm hoặc ứng dụng chạy trên máy chủ hoặc thiết bị tường lửa.

Trước khi triển khai DBF, người quản trị cần đảm bảo rằng hệ thống đáp ứng được các yêu cầu về phần cứng, phần mềm và môi trường mạng. Ngoài ra, cần phải có một kế hoạch cấu hình và triển khai chi tiết để đảm bảo rằng DBF hoạt động hiệu quả và đáp ứng được các yêu cầu của tổ chức.

Sau khi triển khai, DBF cần được cấu hình cho phù hợp với môi trường và yêu cầu của tổ chức. Các cấu hình cơ bản bao gồm xác định các luật quyết định cho phép hoặc từ chối truy cập vào cơ sở dữ liệu, thiết lập các mức độ quyền hạn cho người dùng, và cài đặt các chức năng bảo mật khác như mã hóa dữ liệu, giám sát hoạt động, và báo cáo.

#### **Ưu điểm và nhược điểm.**

***Ưu điểm:***

* Cung cấp một tường lửa cơ sở dữ liệu mạnh mẽ, giúp ngăn chặn các cuộc tấn công từ bên ngoài và bên trong hệ thống.
* Có thể kiểm soát truy cập vào cơ sở dữ liệu theo cách linh hoạt và chính xác.
* Cung cấp các công cụ và chức năng bảo mật mạnh mẽ để bảo vệ dữ liệu.
* Cho phép người quản trị có thể theo dõi và giám sát các hoạt động truy cập cơ sở dữ liệu để phát hiện các mối đe dọa an ninh.
* Giảm thiểu các rủi ro an ninh và rủi ro liên quan đến bảo mật cơ sở dữ liệu.

***Nhược điểm:***

* Đòi hỏi một lượng lớn tài nguyên phần cứng và phần mềm để triển khai và hoạt động.
* Có thể ảnh hưởng đến hiệu suất và tốc độ truy cập cơ sở dữ liệu.
* Cần đầu tư một chi phí đáng kể để triển khai và bảo trì.
* Khó khăn trong việc cấu hình và quản lý, đòi hỏi người quản trị có kiến thức chuyên môn cao.
* Có thể xảy ra các sai sót khi cấu hình và thiết lập các quy tắc bảo mật, dẫn đến các lỗ hổng bảo mật tiềm ẩn.
* Không thể bảo vệ hoàn toàn khỏi các cuộc tấn công từ bên trong hoặc những phần mềm độc hại đã được cài đặt trên máy chủ cơ sở dữ liệu.

### **3. Data Masking.**

#### **Khái niệm.**

Data Masking là một kỹ thuật bảo mật cơ sở dữ liệu cho phép che dấu các dữ liệu nhạy cảm khi chúng được truy cập bởi các người dùng không được ủy quyền hoặc không có quyền truy cập. Kỹ thuật này giúp ngăn chặn các cuộc tấn công và lọc bớt các rủi ro an ninh thông tin.

#### **Kiến trúc.**

Data Masking được triển khai bằng cách tạo ra một bản sao của cơ sở dữ liệu, tuy nhiên, các thông tin nhạy cảm sẽ bị che giấu hoặc được thay thế bằng giá trị giả mạo. Khi người dùng truy cập vào cơ sở dữ liệu, họ sẽ không thể xem được dữ liệu thật sự của thông tin nhạy cảm được che giấu.

#### **Chức năng.**

Data Masking giúp bảo vệ dữ liệu nhạy cảm bằng cách che giấu thông tin quan trọng như số thẻ tín dụng, mã số an ninh, số điện thoại, địa chỉ, tên người dùng và mật khẩu. Data Masking cũng có thể được sử dụng để bảo vệ quyền riêng tư của người dùng bằng cách ẩn danh các thông tin nhạy cảm.

#### **Cách hoạt động.**

Data Masking hoạt động bằng cách thực hiện các quy tắc được xác định trước đó để che giấu hoặc thay thế các giá trị nhạy cảm. Các quy tắc này có thể được thiết lập để ẩn danh hoặc thay thế giá trị thực sự bằng các giá trị khác hoặc các giá trị được sinh ra ngẫu nhiên.

#### **Cách triển khai.**

Data Masking có thể được triển khai trên cả phần mềm và phần cứng, tuy nhiên, phương pháp phần mềm là phổ biến nhất. Các công cụ phần mềm như Delphix, Oracle Data Masking, hay IBM InfoSphere Optim Data Masking giúp triển khai Data Masking một cách dễ dàng và hiệu quả.

#### **Ưu điểm và nhược điểm.**

***Ưu điểm:***

* Che giấu thông tin nhạy cảm và bảo vệ quyền riêng tư của người dùng.
* Giúp đáp ứng các yêu cầu về bảo mật của các quản trị luật pháp hoặc quy định liên quan đến việc bảo vệ thông tin cá nhân.
* Giảm thiểu rủi ro của các cuộc tấn công và lỗ hổng bảo mật.
* Không làm thay đổi dữ liệu gốc và giữ được tính toàn vẹn của cơ sở dữ liệu.

***Nhược điểm:***

* Có thể ảnh hưởng đến hiệu suất và tốc độ truy cập cơ sở dữ liệu.
* Cần đầu tư chi phí và thời gian để triển khai và vận hành.

### **4. Performance Monitoring.**

#### **Khái niệm.**

Performance Monitoring là một tính năng quan trọng trong các giải pháp bảo mật cơ sở dữ liệu. Nó cho phép người quản trị hệ thống theo dõi hiệu suất của cơ sở dữ liệu và phát hiện các vấn đề hiệu suất sớm nhất có thể. Performance Monitoring giúp đảm bảo rằng cơ sở dữ liệu đang hoạt động ổn định và đáp ứng được các yêu cầu của người dùng.

#### **Kiến trúc.**

Performance Monitoring có thể được triển khai trực tiếp trên cơ sở dữ liệu hoặc thông qua một ứng dụng phần mềm riêng biệt. Trong cả hai trường hợp, Performance Monitoring thường sử dụng các công cụ giám sát để theo dõi hiệu suất cơ sở dữ liệu và thu thập các thông tin về tài nguyên hệ thống, chẳng hạn như CPU, bộ nhớ, ổ đĩa và kết nối mạng.

#### **Chức năng.**

Performance Monitoring cung cấp các tính năng giám sát để theo dõi hiệu suất của cơ sở dữ liệu và giúp người quản trị hệ thống xác định các vấn đề hiệu suất sớm nhất có thể. Các tính năng chính của Performance Monitoring bao gồm:

* ***Giám sát tài nguyên hệ thống:*** Giám sát các tài nguyên hệ thống, chẳng hạn như CPU, bộ nhớ, ổ đĩa và kết nối mạng, để xác định các vấn đề hiệu suất.
* ***Giám sát truy vấn cơ sở dữ liệu:*** Giám sát các truy vấn cơ sở dữ liệu để xác định các truy vấn chậm hoặc không hiệu quả.
* ***Thông báo về các vấn đề hiệu suất:*** Thông báo cho người quản trị hệ thống về các vấn đề hiệu suất, cho phép họ phát hiện và giải quyết các vấn đề trước khi chúng trở thành vấn đề lớn hơn.

#### **Cách hoạt động.**

Performance Monitoring sử dụng các công cụ giám sát để theo dõi hiệu suất cơ sở dữ liệu và thu thập các thông tin về tài nguyên hệ thống. Các công cụ này thường được cài đặt trực tiếp trên cơ sở dữ liệu hoặc thông qua một ứng dụng phần mềm riêng biệt.

Khi một truy vấn cơ sở dữ liệu được thực thi, Performance Monitoring theo dõi các thông số quan trọng như thời gian phản hồi, tài nguyên sử dụng (CPU, bộ nhớ, ổ đĩa) và tần suất truy cập cơ sở dữ liệu. Sau đó, nó tổng hợp các thông tin này thành báo cáo để cho phép người quản trị đánh giá hiệu suất của hệ thống và tìm kiếm các vấn đề tiềm ẩn.

#### **Cách triển khai.**

Các công cụ Performance Monitoring có thể được triển khai như một ứng dụng độc lập hoặc như một phần của một giải pháp Database Security toàn diện. Trong một số trường hợp, chúng có thể được tích hợp sẵn vào hệ thống quản lý cơ sở dữ liệu.

#### **Ưu điểm và nhược điểm.**

***Ưu điểm:***

* Giúp người quản trị đánh giá hiệu suất của hệ thống cơ sở dữ liệu và tìm kiếm các vấn đề tiềm ẩn.
* Cung cấp các thông tin quan trọng về tài nguyên và hoạt động của cơ sở dữ liệu để giúp người quản trị đưa ra quyết định về việc nâng cấp hệ thống.
* Có thể giúp cải thiện hiệu suất và tăng khả năng sử dụng tài nguyên của hệ thống.

***Nhược điểm:***

* Có thể ảnh hưởng đến hiệu suất hệ thống khi thực hiện các hoạt động theo dõi.
* Yêu cầu một số lượng tài nguyên để triển khai và hoạt động.

### **5. Sensitive Data Discovery.**

#### **Khái niệm.**

Sensitive Data Discovery là một công cụ giúp phát hiện và bảo vệ các thông tin nhạy cảm trong cơ sở dữ liệu. Đây là một trong những tính năng quan trọng của các giải pháp bảo mật cơ sở dữ liệu, giúp ngăn chặn việc rò rỉ thông tin và đảm bảo tính bảo mật của dữ liệu.

#### **Kiến trúc.**

Kiến trúc của Sensitive Data Discovery thường bao gồm hai phần chính: trình quét (Scanner) và trình phân tích (Analyzer). Trình quét sẽ quét và thu thập thông tin về các loại dữ liệu nhạy cảm, ví dụ như số thẻ tín dụng, số CMND, email, số điện thoại, và nhiều hơn nữa. Trong khi đó, trình phân tích sẽ kiểm tra các kết quả thu thập được từ trình quét và phân tích để đưa ra kết quả về các thông tin nhạy cảm.

#### **Chức năng.**

Chức năng của Sensitive Data Discovery là phát hiện và bảo vệ các thông tin nhạy cảm trong cơ sở dữ liệu. Công cụ này sẽ giúp người dùng xác định các cột chứa dữ liệu nhạy cảm, phát hiện các lỗ hổng bảo mật, giảm thiểu rủi ro cho doanh nghiệp. Thông qua Sensitive Data Discovery, người quản trị cơ sở dữ liệu có thể tìm kiếm và giám sát các mẫu dữ liệu nhạy cảm và xác định xem liệu chúng có được bảo vệ đúng cách hay không.

#### **Cách hoạt động.**

Cách hoạt động của Sensitive Data Discovery bao gồm ba bước chính: Quét dữ liệu, phân tích dữ liệu và báo cáo kết quả. Đầu tiên, công cụ quét toàn bộ dữ liệu trong cơ sở dữ liệu để tìm kiếm các mẫu dữ liệu nhạy cảm. Sau đó, nó sẽ phân tích các kết quả thu thập được để xác định loại dữ liệu nhạy cảm và đưa ra đề xuất về cách bảo vệ thông tin đó. Cuối cùng, Sensitive Data Discovery sẽ tạo ra các báo cáo kết quả về các thông tin nhạy cảm trong cơ sở dữ liệu.

#### **Cách triển khai.**

Cách triển khai của Sensitive Data Discovery thường tùy thuộc vào từng giải pháp cụ thể. Tuy nhiên, để triển khai công cụ này, người dùng cần có quyền truy cập đến cơ sở dữ liệu và phải cài đặt phần mềm Sensitive Data Discovery trên máy chủ cơ sở dữ liệu trước khi sử dụng công cụ này. Sau khi được triển khai và cấu hình đúng cách, Sensitive Data Discovery có thể hoạt động như sau:

* ***Quét cơ sở dữ liệu:*** Sensitive Data Discovery quét toàn bộ cơ sở dữ liệu để tìm kiếm các dữ liệu nhạy cảm, bao gồm các loại thông tin như số thẻ tín dụng, mã số an ninh, thông tin cá nhân, mật khẩu, tên đăng nhập và các thông tin liên quan khác.
* ***Phân loại dữ liệu:*** Sau khi tìm thấy các dữ liệu nhạy cảm, Sensitive Data Discovery phân loại chúng vào các nhóm dữ liệu khác nhau, giúp người quản trị có thể đánh giá mức độ nghiêm trọng của mỗi loại dữ liệu và đưa ra các biện pháp bảo vệ tương ứng.
* ***Cung cấp báo cáo:*** Sensitive Data Discovery tạo ra các báo cáo chi tiết về các dữ liệu nhạy cảm được tìm thấy trong cơ sở dữ liệu, bao gồm vị trí của chúng, loại dữ liệu và mức độ nghiêm trọng. Báo cáo này giúp người quản trị có thể thực hiện các biện pháp bảo mật thích hợp để bảo vệ dữ liệu.
* ***Cập nhật liên tục:*** Sensitive Data Discovery có thể được cấu hình để thực hiện quét cơ sở dữ liệu theo thời gian thực, giúp người quản trị có thể phát hiện và giải quyết các vấn đề bảo mật ngay khi chúng xảy ra.

Cách triển khai Sensitive Data Discovery có thể khá đơn giản, vì nó có thể được triển khai trên cùng một máy chủ cơ sở dữ liệu hoặc máy chủ khác trong mạng. Tuy nhiên, cần có quyền truy cập đến cơ sở dữ liệu và phải cài đặt phần mềm Sensitive Data Discovery trên máy chủ cơ sở dữ liệu trước khi sử dụng công cụ này.

#### **Ưu điểm và nhược điểm.**

Một số ưu điểm của Sensitive Data Discovery bao gồm:

* Giúp phát hiện và bảo vệ các dữ liệu nhạy cảm trong cơ sở dữ liệu.
* Cung cấp báo cáo chi tiết về các dữ liệu nhạy cảm, giúp người quản trị có thể đánh giá mức độ nghiêm trọng của vấn đề và đưa ra các biện pháp bảo vệ thích hợp.
* Có thể cấu hình để thực hiện quá trình kiểm tra định kỳ, đảm bảo rằng dữ liệu được giám sát và bảo vệ liên tục.

Đối với các doanh nghiệp đang thực hiện các chuẩn mực bảo mật như PCI DSS hoặc HIPAA, Sensitive Data Discovery là một công cụ hữu ích để đáp ứng các yêu cầu này.

Tuy nhiên, như mọi công nghệ bảo mật khác, Sensitive Data Discovery cũng có một số nhược điểm. Một trong những nhược điểm chính là độ chính xác của phần mềm. Nếu không được cấu hình đúng và quản lý tốt, phần mềm có thể báo cáo sai hoặc bỏ sót các dữ liệu nhạy cảm.

Ngoài ra, việc triển khai Sensitive Data Discovery cũng đòi hỏi nhiều tài nguyên, bao gồm phần cứng, phần mềm và nguồn nhân lực chuyên môn. Do đó, việc triển khai và duy trì Sensitive Data Discovery có thể tốn kém và phức tạp hơn so với các công cụ bảo mật khác.

## **III. Giả lập ngữ cảnh để kiểm tra tính năng hoạt động.**

### **1. Ngữ cảnh 1.**

***Ngữ cảnh 1: Tấn công từ bên ngoài: Sử dụng công cụ tấn công DDoS để tấn công mạng, cố gắng truy cập vào cơ sở dữ liệu từ xa.***

Tấn công DDoS (Distributed Denial of Service) là một trong những loại tấn công phổ biến nhất từ bên ngoài. Nó được thực hiện bằng cách tạo ra một lưu lượng truy cập lớn đến một website hoặc một mạng, gây ra quá tải và khiến hệ thống hoạt động chậm hơn hoặc ngừng hoạt động hoàn toàn.

Trong ngữ cảnh này, kẻ tấn công sử dụng công cụ tấn công DDoS để tấn công mạng và cố gắng truy cập vào cơ sở dữ liệu từ xa. Một khi tấn công DDoS được thực hiện, lưu lượng truy cập sẽ tăng đột ngột và gây áp lực lên hệ thống. Việc cố gắng truy cập vào cơ sở dữ liệu từ xa trong thời điểm này sẽ làm tăng tải lên máy chủ cơ sở dữ liệu và có thể gây ra tình trạng quá tải.

Để đối phó với tấn công DDoS, người quản trị hệ thống có thể triển khai các giải pháp bảo mật mạng như firewall, load balancer hoặc giải pháp chống DDoS. Firewall có thể giới hạn truy cập vào máy chủ cơ sở dữ liệu từ bên ngoài mạng, giúp giảm thiểu rủi ro tấn công. Load balancer có thể phân phối tải trên nhiều máy chủ và giúp giảm thiểu tác động của tấn công DDoS đến hệ thống. Giải pháp chống DDoS giúp nhận diện và chặn các lưu lượng truy cập độc hại.

Ngoài ra, người quản trị cũng cần cài đặt và cấu hình đúng các giải pháp bảo mật cơ sở dữ liệu để đảm bảo an toàn cho dữ liệu trong trường hợp tấn công từ bên ngoài xảy ra.

Để hiểu rõ hơn về ngữ cảnh 1 trong trường hợp tấn công từ bên ngoài, ta có thể tham khảo một ví dụ demonstation như sau:

Một tổ chức đang sử dụng một ứng dụng web để quản lý thông tin khách hàng. Họ đã triển khai các biện pháp bảo mật để bảo vệ cơ sở dữ liệu của mình, bao gồm cài đặt tường lửa và mã hóa dữ liệu. Tuy nhiên, một tên tấn công ngoài đang cố gắng truy cập vào cơ sở dữ liệu của tổ chức bằng cách sử dụng công cụ tấn công DDoS (Distributed Denial of Service).

Tấn công này sử dụng hàng loạt các máy tính zombie để gửi lưu lượng truy cập đến ứng dụng web của tổ chức, gây ra quá tải và làm cho ứng dụng web không thể truy cập được. Điều này gây ra những hậu quả nghiêm trọng, bao gồm làm chậm tốc độ hoạt động của ứng dụng, ảnh hưởng đến trải nghiệm người dùng, và tạo điều kiện thuận lợi cho tên tấn công có thể truy cập vào cơ sở dữ liệu từ xa.

Để đối phó với tấn công DDoS, tổ chức có thể triển khai các biện pháp bảo vệ như sử dụng các giải pháp bảo mật chống DDoS, tăng cường năng lực kết nối và tài nguyên mạng, tăng cường năng lực xử lý tốc độ hoạt động của ứng dụng và hạn chế truy cập vào cơ sở dữ liệu từ xa.

### **2. Ngữ cảnh 2.**

***Ngữ cảnh 2: Truy cập trái phép: Sử dụng tài khoản truy cập không hợp lệ hoặc đánh cắp tài khoản truy cập để truy cập vào cơ sở dữ liệu.***

Ngữ cảnh 2 xảy ra khi kẻ tấn công có thể sử dụng một tài khoản truy cập không hợp lệ hoặc đánh cắp thông tin đăng nhập của người dùng hợp lệ để truy cập vào cơ sở dữ liệu một cách trái phép.

Kẻ tấn công có thể lợi dụng các lỗ hổng bảo mật trong phần mềm hoặc đánh cắp thông tin đăng nhập của một người dùng hợp lệ để truy cập vào cơ sở dữ liệu. Nếu kẻ tấn công thành công, họ có thể có quyền truy cập và quản lý các thông tin nhạy cảm, gây ra thiệt hại cho tổ chức bị tấn công.

Để ngăn chặn cuộc tấn công này, các tổ chức nên có chính sách bảo mật về quản lý tài khoản truy cập, bao gồm các biện pháp như xác thực hai yếu tố và phân quyền truy cập cơ sở dữ liệu. Các hệ thống phải được bảo vệ chặt chẽ và cập nhật để ngăn chặn các lỗ hổng bảo mật. Các báo cáo và giám sát liên tục cũng là rất quan trọng để phát hiện các hoạt động đáng ngờ và các nỗ lực tấn công truy cập trái phép vào cơ sở dữ liệu.

### **3. Ngữ cảnh 3.**

***Ngữ cảnh 3: Phát hiện dữ liệu nhạy cảm: Tìm kiếm và phát hiện các dữ liệu nhạy cảm như số thẻ tín dụng hoặc số Bảo hiểm xã hội trong cơ sở dữ liệu.***

Trong ngữ cảnh này, nhiệm vụ chính của phần mềm Sensitive Data Discovery là tìm kiếm và phát hiện các dữ liệu nhạy cảm như số thẻ tín dụng hoặc số Bảo hiểm xã hội trong cơ sở dữ liệu. Các dữ liệu này được coi là nhạy cảm vì nếu rơi vào tay kẻ xấu có thể dẫn đến các cuộc tấn công lừa đảo hoặc vi phạm quyền riêng tư của người dùng.

Phần mềm Sensitive Data Discovery sử dụng các công cụ và kỹ thuật phân tích dữ liệu để quét toàn bộ cơ sở dữ liệu và tìm kiếm các dữ liệu nhạy cảm. Các kỹ thuật này bao gồm quét tìm kiếm chuỗi, quét tìm kiếm định dạng số và quét tìm kiếm định dạng văn bản. Sau khi tìm thấy các dữ liệu nhạy cảm, phần mềm sẽ cung cấp báo cáo chi tiết về các dữ liệu này cho người quản trị để xem xét và đưa ra các biện pháp bảo vệ thích hợp.

Việc phát hiện các dữ liệu nhạy cảm là rất quan trọng trong việc đảm bảo an toàn và bảo mật của cơ sở dữ liệu. Tuy nhiên, việc phát hiện dữ liệu nhạy cảm có thể gặp phải một số vấn đề, chẳng hạn như việc phát hiện sai hoặc bỏ sót các dữ liệu nhạy cảm. Do đó, việc triển khai phần mềm Sensitive Data Discovery cần được cân nhắc kỹ lưỡng để đảm bảo hiệu quả và độ chính xác của quá trình phát hiện.

### **4. Ngữ cảnh 4.**

***Ngữ cảnh 4: Kiểm tra hiệu suất: Đánh giá hiệu suất của cơ sở dữ liệu và tìm kiếm các vấn đề liên quan đến hiệu suất.***

Khi một cơ sở dữ liệu được triển khai, việc đảm bảo hiệu suất của nó là rất quan trọng. Việc kiểm tra hiệu suất thường được thực hiện để đảm bảo rằng cơ sở dữ liệu đáp ứng được yêu cầu của người dùng và có thể xử lý các truy vấn dữ liệu một cách nhanh chóng và hiệu quả.

Chức năng của Performance Monitoring trong ngữ cảnh này là đánh giá hiệu suất của cơ sở dữ liệu bằng cách thu thập và phân tích các thông số hiệu suất như thời gian phản hồi truy vấn, thời gian truy cập cơ sở dữ liệu, tải CPU và bộ nhớ, số lượng kết nối đồng thời và thống kê truy vấn.

Cách hoạt động của Performance Monitoring trong ngữ cảnh này là sử dụng các công cụ và phần mềm để thu thập các thông số hiệu suất của cơ sở dữ liệu, chẳng hạn như thông qua các bản ghi nhật ký (Log), hoặc các dữ liệu được cung cấp bởi các phần mềm quản lý cơ sở dữ liệu. Sau đó, các thông số này được phân tích và hiển thị dưới dạng báo cáo để giúp người quản trị cơ sở dữ liệu đánh giá hiệu suất của cơ sở dữ liệu và tìm kiếm các vấn đề có thể ảnh hưởng đến hiệu suất của cơ sở dữ liệu.

## **IV. Đề xuất phương pháp cải thiện.**

### **1. Xác định nhu cầu bảo mật dữ liệu của doanh nghiệp.**

Chúng ta cần tìm hiểu các nhu cầu bảo mật dữ liệu của doanh nghiệp hoặc tổ chức để có thể lựa chọn được giải pháp bảo mật dữ liệu phù hợp. Để xác định các nhu cầu này, chúng ta có thể tham khảo các quy định pháp lý liên quan đến bảo mật thông tin, kiểm tra các hệ thống và quy trình hiện có của doanh nghiệp để xác định các điểm yếu và những dữ liệu quan trọng cần được bảo vệ.

### **2. Lựa chọn giải pháp bảo mật dữ liệu phù hợp.**

Sau khi đã xác định được các nhu cầu bảo mật dữ liệu của doanh nghiệp, chúng ta có thể lựa chọn được giải pháp bảo mật dữ liệu phù hợp nhất. Để lựa chọn được giải pháp này, chúng ta cần tìm hiểu các giải pháp bảo mật dữ liệu có sẵn trên thị trường, so sánh và đánh giá chúng để lựa chọn được giải pháp phù hợp với nhu cầu và khả năng tài chính của doanh nghiệp.

### **3. Triển khai giải pháp bảo mật dữ liệu.**

Sau khi đã lựa chọn được giải pháp bảo mật dữ liệu phù hợp, chúng ta cần triển khai giải pháp này và cấu hình các tính năng cần thiết để đáp ứng các nhu cầu bảo mật dữ liệu của doanh nghiệp. Quá trình triển khai này cần phải được thực hiện cẩn thận và đúng quy trình để đảm bảo tính ổn định và hiệu quả của giải pháp.

### **4. Đào tạo nhân viên sử dụng giải pháp bảo mật dữ liệu.**

Sau khi đã triển khai giải pháp bảo mật dữ liệu, chúng ta cần đào tạo nhân viên để sử dụng giải pháp này một cách hiệu quả. Việc đào tạo này cần phải bao gồm việc hướng dẫn nhân viên sử dụng giải pháp bảo mật dữ liệu, giải đáp các thắc mắc và truyền đạt các quy trình và chính sách bảo mật dữ liệu của doanh nghiệp.

# **LỜI CẢM ƠN**

Trong thời gian học tập môn An toàn mạng máy tính nâng cao, nhóm đã nhân được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, bạn bè. Với sự giúp đỡ này đã giúp nhóm rất nhiều trong việc cũng cố kiến thức và giải đáp những thắc mắc còn tồn đọng.

Nhóm xin gửi lời cám ơn chân thành đến thầy Nguyễn Duy giảng viên khoa Mạng máy tính và truyền thông dữ liệu trường đại học Công Nghệ Thông Tin, người đã tận tình hướng dẫn, chỉ bảo nhóm trong suốt quá trình làm đồ án.

Với những kiến thức đã được học tại môn này nhóm báo cáo có thể tự tin hơn trên chặng đường học tập sắp tới và trong cuộc sống sau này. Nhóm xin được chúc thầy và các cán bộ giảng viên đang công tác tại trường thật nhiều sức khỏe và thành công trong cuộc sống.

**Hết !**