**Bài tập Chương 3**

**Cho một ví dụ minh họa “Mục đích của QLRR là tạo ra giá trị và bảo vệ giá trị”**

**Tình huống/Bối cảnh hoạt động của doanh nghiệp:** Công ty TNHH Gia Nhân (gọi tắt là Công ty Gia Nhân) đang vận hành một hệ thống SIEM Server nhằm giám sát an ninh thông tin cho nhiều phòng ban của họ. Các luồng dữ liệu là System logs, Nginx logs, MySQL Logs, Router logs, Firewall logs, IDS/IPS logs đều được gửi về máy chủ SIEM Server và lưu trữ trong đó theo thời gian thực, các *file logs này*\* được thu thập nhằm phục vụ công tác phân tích, giám sát an toàn mạng, an toàn thông tin cho công ty Gia Nhân.

*(\*Các file logs này thu thập được từ máy tính của nhân viên, tường lửa, router, IDS/IPS, máy chủ CSDL*).

**1. Điểm yếu**: Hệ thống SIEM Server chưa có cơ chế kiểm soát truy cập phân quyền rõ ràng và không áp dụng mã hóa dữ liệu *(là các file logs)* được lưu trong hệ thống đó.

**2. Mối đe doạ:** Hacker tấn công và can thiệp vào hệ thống.

**3. Rủi ro tiềm ẩn:** Có thể xảy ra các sự cố xâm nhập trái phép mà không được phát hiện kịp thời. Từ đó dẫn đến rò rỉ thông tin (logs) nội bộ của cả công ty. Nguy hiểm hơn là hacker sẽ thay đổi/phá hỏng toàn bộ dữ liệu của hệ thống.

**4. Biện pháp kiểm soát rủi ro (control)**

**4.1. Tạo giá trị**

- Áp dụng giải pháp kiểm soát truy cập theo thuộc tính ABAC kết hợp với mã hóa CP-ABE + AES GCM 256 để giảm tỷ lệ sự cố *truy cập\** trái phép về 0 lượt/tháng, đồng thời gửi thông báo về máy chủ SIEM Server khi có User truy cập sai vào hệ thống với quy định “*5 lượt truy cập sai/1 User thì sẽ gửi cảnh báo*”. [\**Lượt truy cập được tính dựa vào các log entry do các thiết bị (máy tính, firewall, router…) gửi về, cứ mỗi 1 lần đăng nhập vào hệ thống tại 1 địa điểm và 1 địa chỉ IP thì được tính là 1 lượt truy cập.]*

- Đảm bảo thời gian kiểm soát truy cập theo thuộc tính ABAC cho từng Quản trị viên khi họ truy cập vào SIEM Server tối đa là 1s/1 lượt truy cập (Tcheck\_access  = 1s/1 lượt truy cập)

- Đảm bảo các dữ liệu lưu trên SIEM Server (*là các file logs)* được mã hoá theo thời gian thực, thời gian mã hoá Tenc tối đa là 0.005s/1 kbyte, thời gian giải mã Tdec khi truy vấn tối đa là 0.007s/1 kbyte.

**4.2. Bảo vệ giá trị**

- Cứ mỗi 6 tháng 1 lần sẽ cập nhật/kiểm tra toàn bộ thuộc tính của nhân viên, điều này sẽ giúp cho các chính sách thuộc tính trong ABAC được cập nhật định kỳ, không bị “out-date”, vẫn luôn giữ được Tcheck\_access = 1s/1 lượt.

- Sao lưu toàn bộ dữ liệu được mã hoá vào 1 máy chủ riêng với tần suất 1 ngày/1 lần.

- Tối ưu thuật toán CP-ABE + AES GCM 256 định kỳ 3 tháng 1 lần để đảm bảo Tenc và Tdec không được vượt quá ngưỡng tối đa.

- Mỗi quản trị viên SIEM Server được cấp 1 private\_key chứa các thuộc tính của mình để truy cập vào hệ thống SIEM Server *đảm bảo phù hợp với chính sách* của công ty đưa ra, private\_key được cập nhật mỗi 3 tháng/lần.