CHAPTER 4

EXPERIMENTAL AND RESULTS

4.1 Introduction

Chương này trình bày thiết kế thí nghiệm và kết quả đánh giá của hệ thống tự động giám sát tuân thủ chính sách bảo mật và hỗ trợ kiểm toán cho môi trường hồ sơ bệnh án điện tử tại cơ sở y tế quy mô nhỏ và vừa. Định hướng của đồ án là giám sát theo quy tắc và dựa trên bằng chứng, nghĩa là hệ thống thu thập log từ các thành phần vận hành chính, chuẩn hóa thành sự kiện có cấu trúc, đối chiếu với bộ quy tắc tuân thủ, sau đó tạo ra cảnh báo và báo cáo có thể truy vết. Do đặc thù đồ án đại học và yêu cầu bảo vệ dữ liệu, toàn bộ thí nghiệm trong chương này được thực hiện trên môi trường mô phỏng, không sử dụng dữ liệu bệnh án thật. Các kịch bản bất thường có sẵn trong hệ thống mẫu như brute force, SQL injection và XSS được sử dụng với mục tiêu duy nhất là sinh ra dấu vết để kiểm thử đường ống ghi vết và cảnh báo, không nhằm mô tả hay đánh giá kỹ thuật tấn công. Ngoài ra, chương này đánh giá thêm lớp toàn vẹn bằng chứng, tập trung vào khả năng phát hiện rủi ro mất log hoặc bị can thiệp log, bởi vì nếu log không đáng tin cậy thì mọi kết luận tuân thủ phía trên sẽ mất ý nghĩa trong kiểm toán và điều tra.

4.2 Presentation of Data

Dữ liệu thí nghiệm gồm hai thành phần chính là dữ liệu quy tắc và dữ liệu log. Dữ liệu quy tắc được triển khai dưới dạng bảng quy tắc, mỗi quy tắc gắn mã quy tắc, tên quy tắc, trạng thái áp dụng, căn cứ pháp lý, giải thích và các trường log tối thiểu cần có để kiểm tra tự động. Trong gói hệ thống, bảng quy tắc có tổng cộng 196 quy tắc, được phân nhóm theo các cụm chức năng phục vụ kiểm toán và tuân thủ. Dữ liệu log được trích xuất từ bảng access logs chuẩn hóa của hệ thống giám sát, trong đó mỗi bản ghi biểu diễn một sự kiện truy cập hoặc sự kiện hệ thống đã được gom về định dạng thống nhất. Tổng số bản ghi sự kiện trong bảng access logs là 854. Bên cạnh đó, hệ thống có bảng cảnh báo watchdog dùng để ghi nhận các tình huống rủi ro liên quan đến tính sẵn sàng và toàn vẹn của cơ chế ghi log, nhằm bảo vệ khả năng truy vết khi có sự cố. Tổng số cảnh báo watchdog trong dữ liệu mô phỏng là 31. Để phù hợp yêu cầu trình bày và tránh đưa thông tin ngày giờ cụ thể, toàn bộ kết quả trong chương này chỉ sử dụng số liệu tổng hợp và phân bố theo loại sự kiện, loại cảnh báo và nhóm quy tắc, không trích dẫn các dòng log thô chứa dấu thời gian.

Bảng 4.1 Nguồn dữ liệu và quy mô dữ liệu thí nghiệm

Thành phần dữ liệu	Số lượng	Mô tả
Bảng quy tắc tuân thủ	196	Tổng số quy tắc dùng để kiểm tra tuân thủ tự động
Bảng sự kiện access logs	854	Tổng số sự kiện chuẩn hóa dùng để phân tích và báo cáo
Bảng cảnh báo watchdog	31	Tổng số cảnh báo liên quan đến rủi ro toàn vẹn hoặc mất dấu vết log

Bảng 4.2 Phân bố quy tắc theo nhóm chức năng

Nhóm chức năng	Số quy tắc
PHẦN III - QUẢN LÝ TRUY CẬP & DỮ LIỆU (DATA ACCESS MANAGEMENT)	25
PHẦN IX GIÁM SÁT AN NINH VÀ ỨNG PHÓ SỰ CỐ SECURITY MONITORING IR	22
PHẦN IV - GHI VẾT, KIỂM TOÁN & GIÁM SÁT (AUDIT & LOGGING)	20
PHẦN V - CHỮ KÝ SỐ & TOÀN VẸN HỒ SƠ (DIGITAL SIGNATURE & INTEGRITY)	20
PHẦN VI - ĐỒNG THUẬN & CHIA SẺ THÔNG TIN (CONSENT & DATA DISCLOSURE)	20
PHẦN VII - BACKUP, RETENTION & DATA LIFECYCLE	20
PHẦN VIII - LIÊN THÔNG & CHIA SẺ KỸ THUẬT (INTEROPERABILITY & TECHNICAL EXCHANGE)	20
PHẦN X - GOVERNANCE, COMPLIANCE & TRAINING	20
PHẦN II - PHÂN QUYỀN & PHẠM VI HÀNH NGHỀ (RBAC)	11
PHẦN I - NHÓM QUY TẮC NHẬN DIỆN & XÁC THỰC (IAM)	10
PHẦN XIII XÁC THỰC VÀ PHIÊN AUTH SESSION	5
PHẦN XI KIỂM SOÁT ĐẦU VÀO	3

INPUT VALIDATION	

Bảng 4.3 Phân bố mã trạng thái trong access logs

Mã trạng thái	Số lượng	Diễn giải
200	356	Thao tác hợp lệ và luồng nghiệp vụ bình thường
401	8	Không được xác thực, thường do thiếu hoặc sai thông tin đăng nhập
403	476	Bị chặn hoặc bị từ chối, gồm cả cảnh báo bảo mật ở tầng biên
423	14	Trạng thái bị khóa hoặc hạn chế trong một số điều kiện vận hành

Bảng 4.4 Phân bố loại sự kiện trong access logs

Loại sự kiện	Số lượng	Vai trò trong giám sát
SECURITY_ALERT	476	Cảnh báo bất thường hoặc hành vi rủi ro được ghi nhận để điều tra
SYSTEM_TLS_LOG	102	Sự kiện liên quan lớp truyền tải bảo mật phục vụ truy vết kênh kết nối
emr_access_log	82	Sự kiện truy cập ở tầng ứng dụng EHR phục vụ kiểm toán thao tác
SESSION_LOG	57	Sự kiện phiên làm việc hỗ trợ truy vết đăng nhập và chuỗi thao tác
SYSTEM_AUTH_LOG	51	Sự kiện xác thực của các thành phần hệ thống
BACKUP_ENCRYPTION_LOG	34	Sự kiện sao lưu và mã hóa phục vụ kiểm

		toán lưu giữ và khôi phục
admin_activity_log	13	Sự kiện quản trị cần được ghi nhận để giải trình trách nhiệm
KHAC	39	Bản ghi thiếu nhãn loại hoặc bản ghi tổng quát

Bảng 4.5 Phân rã cảnh báo bảo mật theo kịch bản mô phỏng

Kịch bản	Số lượng	Ý nghĩa bằng chứng
Brute force	392	Chuỗi đăng nhập lặp giúp kiểm thử tương quan sự kiện và truy vết tài khoản
WAF blocked SQL injection	51	Yêu cầu bị chặn do mẫu injection, dùng để kiểm thử ghi vết và cảnh báo ở tầng biên
WAF blocked XSS	33	Yêu cầu bị chặn do mẫu script injection, dùng để kiểm thử ghi vết và cảnh báo ở tầng biên
Tổng SECURITY_ALERT	476	Tổng số cảnh báo bảo mật trong tập dữ liệu

Bảng 4.6 Tóm tắt cảnh báo watchdog về toàn vẹn dấu vết

Loại cảnh báo	Số lượng	Mức độ	Diễn giải
LOG_TAMPERING	31	CRITICAL	Cảnh báo nguy cơ bị can thiệp hoặc mất dấu vết ghi log, ảnh hưởng trực tiếp khả năng kiểm toán

4.3 Analysis of Results

Kết quả được phân tích dựa trên mức độ bao phủ quy tắc, hiệu quả của pipeline chuẩn hóa sự kiện và khả năng tạo bằng chứng truy vết. Về bao phủ quy tắc, Bảng 4.2 cho thấy bộ quy tắc không chỉ tập trung vào một điểm kiểm soát đơn lẻ mà trải rộng từ quản lý truy cập dữ liệu, ghi vết kiểm toán, đồng thuận và chia sẻ, liên thông, sao lưu và vòng đời dữ liệu, cho đến quản trị tuân thủ và giám sát an ninh. Cách phân bố này phù hợp với logic kiểm toán trong môi trường EHR vì một kết luận tuân thủ đáng tin cậy thường cần xem xét đồng thời bối cảnh danh tính, phạm vi vai trò, mục đích truy cập, thao tác trên dữ liệu và tình trạng hệ thống ghi vết. Về hiệu quả pipeline, Bảng 4.4 chỉ ra rằng tập sự kiện chuẩn hóa bao gồm cả sự kiện vận hành như TLS, xác thực hệ thống, phiên đăng nhập, thao tác quản trị và sao lưu mã hóa, bên cạnh các sự kiện truy cập EHR. Điều này hỗ trợ truy vết theo chuỗi vì cùng một hành vi tuân thủ có thể cần nối từ phiên đăng nhập đến thao tác truy cập hồ sơ, sau đó đến quyết định cho phép hoặc từ chối và cuối cùng là bản ghi nghiệp vụ. Về trạng thái kết quả, Bảng 4.3 cho thấy dữ liệu bao gồm cả hành vi hợp lệ và hành vi bị chặn hoặc bị từ chối, đây là điều kiện tối thiểu để hệ thống có thể trả lời các câu hỏi kiểm toán dạng đã chặn gì và đã cho phép gì. Về lớp bất thường và an toàn, Bảng 4.5 cho thấy cảnh báo bảo mật chủ yếu đến từ chuỗi brute force và nhóm bị chặn bởi WAF, giúp kiểm thử khả năng tương quan, phân loại và trình bày bằng chứng mà không cần đi sâu vào khai thác. Về lớp toàn vẹn, Bảng 4.6 cho thấy hệ thống có cơ chế phát hiện rủi ro mất log hoặc can thiệp log bằng watchdog, đây là yếu tố quan trọng vì mất log đồng nghĩa mất bằng chứng và làm suy yếu mọi kết luận tuân thủ.

4.4 Interpretation of Results

Các kết quả trên cho phép diễn giải rằng hướng tiếp cận dựa trên quy tắc và dựa trên log có thể triển khai theo mô hình nhẹ nhưng vẫn đảm bảo truy vết đối với cơ sở y tế nhỏ và vừa. Thứ nhất, việc có bộ quy tắc được tổ chức theo nhóm chức năng và gắn với các trường log bắt buộc giúp chuyển hóa yêu cầu tuân thủ thành các điều kiện có thể kiểm tra tự động, từ đó giảm phụ thuộc vào phân tích thủ công và giảm rủi ro bỏ sót bằng chứng. Thứ hai, việc chuẩn hóa sự kiện theo loại và lưu trong bảng access logs giúp xây dựng báo cáo và dashboard theo mục tiêu kiểm toán, đồng thời vẫn giữ khả năng truy vết khi cần điều tra vì có thể nối chuỗi phiên, xác thực, truy cập EHR và thao tác quản trị. Thứ ba, lớp cảnh báo an toàn và lớp watchdog toàn vẹn giúp bổ sung góc nhìn rằng tuân thủ không chỉ là kiểm tra hành vi người dùng mà còn là bảo vệ chính quy trình ghi vết, bởi vì một hệ thống ghi vết bị tắt hoặc bị can thiệp sẽ tạo ra khoảng trống bằng chứng và gây khó khăn cho kiểm toán. Tuy nhiên, do dữ liệu hoàn toàn mô phỏng, kết quả cần

được hiểu như bằng chứng về tính khả thi và tính đúng của pipeline trong điều kiện kiểm soát. Khi triển khai thực tế, log có thể thiếu trường hoặc không đồng nhất giữa các thành phần, và các tình huống tuân thủ nghiệp vụ như truy cập ngoài giờ, break glass có lý do, truy cập sai mục đích hoặc truy cập khối lượng lớn cần được mô phỏng phong phú hơn để phản ánh đúng các câu hỏi kiểm toán phổ biến trong y tế.

4.5 Comparison with Literature

So sánh với tài liệu tham khảo, thiết kế và kết quả thí nghiệm bám sát các nguyên tắc quản lý log và giám sát liên tục. NIST SP 800 92 nhấn mạnh rằng quản lý log bao gồm thu thập, tập trung, bảo vệ, lưu giữ và phân tích log nhằm hỗ trợ phát hiện bất thường và điều tra sự cố, do đó việc xây dựng pipeline chuẩn hóa sự kiện và báo cáo dựa trên log trong đồ án là phù hợp với hướng dẫn này [1]. NIST SP 800 137 nêu khái niệm giám sát liên tục và vai trò của việc thu thập thông tin an ninh theo thời gian để hỗ trợ quản trị rủi ro, điều này tương thích với việc hệ thống duy trì bảng sự kiện chuẩn hóa và cơ chế cảnh báo để theo dõi trạng thái tuân thủ và bất thường [2]. Đối với nhóm kịch bản bất thường cơ bản, OWASP mô tả SQL injection và XSS như các dạng tấn công web phổ biến, và việc ghi nhận các request bị chặn là một dạng bằng chứng hữu ích cho điều tra và cải thiện phòng vệ, vì vậy việc sử dụng các mẫu mô phỏng chỉ nhằm tạo dấu vết cho pipeline là hợp lý [3], [4]. MITRE ATT and CK mô tả brute force là kỹ thuật phổ biến trong nhóm truy cập trái phép, cung cấp ngữ cảnh để giải thích vì sao chuỗi đăng nhập thất bại nên được tương quan và đưa vào diện giám sát [5]. Ở góc độ kiểm toán cấu trúc trong y tế, HL7 FHIR định nghĩa AuditEvent như một tài nguyên mô tả sự kiện kiểm toán có cấu trúc, và IHE BALP cung cấp hướng dẫn mẫu log kiểm toán cơ bản, điều này phù hợp với định hướng chuẩn hóa sự kiện để truy vấn, liên kết và báo cáo theo actor, action và resource trong đồ án [7], [8].

4.6 Implications of the Results

Hàm ý quan trọng nhất rút ra từ chương này là việc giám sát tuân thủ cho cơ sở y tế nhỏ và vừa có thể bắt đầu từ một tập lõi gồm bộ quy tắc chuẩn hóa và một pipeline log chuẩn hóa thay vì phải triển khai ngay các hệ thống phức tạp. Thứ nhất, bộ quy tắc cần được thiết kế sao cho mỗi yêu cầu tuân thủ gắn với các trường log tối thiểu, bởi vì đây là điều kiện để kiểm tra tự động và để giải thích kết quả trong kiểm toán. Thứ hai, pipeline nên ưu tiên lưu và phân tích một tập sự kiện chuẩn hóa có giá trị kiểm toán cao, thay vì cố lưu mọi log thô trong thời gian dài, nhằm phù hợp hạn chế lưu trữ và nhân lực. Thứ ba, lớp bảo vệ toàn vẹn log như

watchdog cần được xem như một phần của tuân thủ, bởi vì bảo toàn bằng chứng là điều kiện tiên quyết để chứng minh tuân thủ. Trong hướng phát triển tiếp theo, cần bổ sung thêm các kịch bản tuân thủ nghiệp vụ mang tính y tế như truy cập ngoài giờ theo lịch trực mô phỏng, break glass kèm lý do và phê duyệt, truy cập khối lượng lớn trong thời gian ngắn và truy cập không liên quan đến quan hệ điều trị, đồng thời xây dựng bộ dữ liệu mô phỏng có nhãn theo kịch bản để có thể đo lường tỷ lệ phát hiện và tỷ lệ cảnh báo sai mà vẫn không dùng dữ liệu bệnh nhân thật.

References

[1] National Institute of Standards and Technology, Guide to Computer Security Log Management, Special Publication 800 92. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

[2] National Institute of Standards and Technology, Information Security Continuous Monitoring for Federal Information Systems and Organizations, Special Publication 800 137. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

[3] OWASP Foundation, SQL Injection. Available: https://owasp.org/www-community/attacks/SQL_Injection

[4] OWASP Foundation, Cross Site Scripting XSS. Available: https://owasp.org/www-community/attacks/xss/

[5] MITRE ATT and CK, Brute Force, Technique T1110. Available: https://attack.mitre.org/techniques/T1110/

[6] OWASP Cheat Sheet Series, Logging Cheat Sheet. Available: https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

[7] HL7, FHIR AuditEvent Resource. Available: https://hl7.org/fhir/auditevent.html

[8] IHE International, Basic Audit Log Patterns BALP. Available: https://profiles.ihe.net/ITI/BALP/index.html