THUYẾT MINH DỰ THẢO TIÊU CHUẨN QUỐC GIA

AN NINH MẠNG - SẢN PHẨM QUẢN LÝ, PHÂN TÍCH SỰ KIỆN AN NINH MẠNG - YÊU CẦU CHUNG

1. Thông tin chung về dự thảo TCVN

a) Tên dự thảo TCVN

TCVN XXXXX:2026 An ninh mạng - Sản phẩm quản lý, phân tích sự kiện an ninh mạng - Yêu cầu chung.

b) Thuộc lĩnh vực

Tiêu chuẩn thuộc lĩnh vực tiêu chuẩn cho sản phẩm, dịch vụ an ninh mạng.

c) Phạm vi áp dụng của TCVN

Tiêu chuẩn này quy định các yêu cầu kỹ thuật chung đối với sản phẩm quản lý và phân tích sự kiện an ninh mạng (Sau đây viết tắt là SIEM).

d) Mục tiêu của TCVN

Việc nghiên cứu, xây dựng và ban hành tiêu chuẩn quốc gia đối với nền tảng quản lý, phân tích sự kiện và thông tin an ninh mạng (SIEM) nhằm tạo lập một hệ quy chiếu đo lường và kiểm định kỹ thuật thống nhất, làm căn cứ cho công tác đánh giá chất lượng sản phẩm trước khi đưa vào sử dụng. Tiêu chuẩn này sẽ đóng vai trò là thước đo kỹ thuật để các cơ quan, tổ chức, chủ quản hệ thống thông tin tham chiếu trong quá trình thiết kế, lập hồ sơ thầu và nghiệm thu. Đồng thời, đây cũng là định hướng cho các doanh nghiệp công nghệ trong nước chuẩn hóa kiến trúc, tối ưu hóa thuật toán, tạo đòn bẩy thúc đẩy nghiên cứu và phát triển các nền tảng SIEM "Make in Vietnam" đạt chất lượng tương đương quốc tế và đáp ứng toàn diện yêu cầu bảo vệ chủ quyền trên không gian mạng.

đ) Cơ quan chủ trì soạn thảo

- Tên cơ quan: Cục An ninh mạng và phòng, chống tội phạm sử dụng Công nghệ cao - Bộ Công an.

- Địa chỉ: Lô E2, khu đô thị mới Cầu Giấy, Phường Cầu Giấy, Thành phố Hà Nội.

e) Tổ chức tham gia soạn thảo

Tham gia soạn thảo tiêu chuẩn quốc gia (TCVN) này bao gồm: Các cán bộ Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng Công nghệ cao; Các chuyên gia của Hiệp hội An ninh mạng quốc gia; Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam (NCS Group).

g) Phiên bản dự thảo: Version 1

2. Nội dung dự thảo TCVN

DỰ THẢO TCVN	THUYẾT MINH
1. Phạm vi áp dụng	Tự xây dựng.
2. Tài liệu viện dẫn	Tự xây dựng.
3. Thuật ngữ, định nghĩa và chữ viết tắt	Tham khảo Mục I.3. Khái niệm và thuật ngữ của Quyết định số 1127/QĐ-BTTTT. Bổ sung các khái niệm hiện đại từ Bảng 1 và Bảng 2 của SANS (ví dụ: SOAR, Data Lake).
4. Yêu cầu chung, quản trị và an toàn của sản phẩm	Tự xây dựng.
4.1 Khái quát	Tự xây dựng.
4.2 Yêu cầu cụ thể	Tự xây dựng.
4.2.1 Yêu cầu về tài liệu	Tham khảo Mục II.1. Yêu cầu về tài liệu của Quyết định số 1127/QĐ-BTTTT.
4.2.1.1 Hướng dẫn triển khai và thiết lập cấu hình	Tự xây dựng kết hợp Mục II.1 của Quyết định số 1127/QĐ-BTTTT.
4.2.1.2 Hướng dẫn sử dụng và quản trị	Tham khảo Mục II.1. Yêu cầu về tài liệu của Quyết định số 1127/QĐ-BTTTT.
4.2.2 Quản trị hệ thống	Tham khảo Mục II.2. Yêu cầu về quản trị hệ thống của Quyết định số 1127/QĐ-BTTTT.
4.2.2.1 Quản lý vận hành và giám sát các thành phần nội bộ	Tham khảo Mục II.2.1. Quản lý vận hành và Mục II.2.8. Quản lý và giám sát tập trung các thành phần của Quyết định số 1127/QĐ-BTTTT. Tham chiếu Bảng 7 (Table 7), tính năng Status Monitoring của SANS.
4.2.2.2 Quản trị từ xa	Tham khảo Mục II.2.2. Quản trị từ xa của Quyết định số 1127/QĐ-BTTTT.

4.2.2.3 Quản lý xác thực và phân quyền	Tham khảo Mục II.2.3. Quản lý xác thực và phân quyền của Quyết định số 1127/QĐ-BTTTT.
4.2.2.4 Hỗ trợ tích hợp xác thực tập trung và xác thực đa yếu tố	Tự xây dựng. Bổ sung yêu cầu bắt buộc MFA theo chuẩn an toàn hiện đại.
4.2.3 Quản trị và vận hành, duy trì hệ thống	Tham khảo Mục II.3. Yêu cầu về kiểm soát lỗi của Quyết định số 1127/QĐ-BTTTT.
4.2.3.1 Bảo vệ và kiểm soát thay đổi cấu hình	Tham khảo Mục II.3.1. Bảo vệ cấu hình và Mục II.2.5. Quản lý tập luật bảo vệ của Quyết định số 1127/QĐ-BTTTT.
4.2.3.2 Cập nhật bản vá của sản phẩm	Tham khảo Mục II.6.2. Cập nhật bản vá hệ thống của Quyết định số 1127/QĐ-BTTTT.
4.2.3.3 Đồng bộ thời gian hệ thống lõi	Tham khảo Mục II.3.3. Đồng bộ thời gian hệ thống của Quyết định số 1127/QĐ-BTTTT.
4.2.3.4 Nhật ký quản trị và hệ thống	Tham khảo Mục II.4.1. Log quản trị hệ thống và Mục II.2.6. Cập nhật tập luật bảo vệ của Quyết định số 1127/QĐ-BTTTT. Cụ thể hóa dựa trên Bảng 7, tính năng Audit Logging của SANS.
4.2.4 Chủ quyền dữ liệu, minh bạch nguồn gốc và kiểm soát nhà cung cấp	Tham khảo Bảng 8 (Table 8. Business Requirements), tính năng Compliance Validation và Vendor Background trong SANS.
4.2.4.1 Chủ quyền và lưu trữ dữ liệu nhật ký	Tự xây dựng để tuân thủ Luật An ninh mạng và Luật Dữ liệu hiện hành.
4.2.4.2 Minh bạch và kiểm soát truy cập từ xa của nhà cung cấp	Tự xây dựng để quản lý rủi ro chuỗi cung ứng (bắt buộc khai báo SBOM và cấm cửa hậu).
5 Yêu cầu về chức năng nghiệp vụ của nền tảng	Tham khảo Mục II.4, II.5 và II.7 của Quyết định số 1127/QĐ-BTTTT và Kiến trúc tổng thể Hình 1 (Figure 1. NextGen SIEM Reference Architecture) của SANS.
5.1 Khái quát	Tự xây dựng.
5.2 Yêu cầu cụ thể	Tự xây dựng.
5.2.1 Quản lý nguồn, tiếp nhận và vòng đời dữ liệu nhật ký	Tham khảo Bảng 2 (Table 2), lớp Data Management Layer trong SANS.

5.2.1.1 Quản lý danh mục đối tượng và nguồn gửi nhật ký	Tham khảo Mục II.2.7. Quản lý đối tượng được giám sát và nguồn gửi log của Quyết định số 1127/QĐ-BTTTT.
5.2.1.1.1 Quản lý danh mục đối tượng được giám sát và nguồn gửi	Tham khảo Mục II.2.7. Quản lý đối tượng được giám sát và nguồn gửi log của Quyết định số 1127/QĐ-BTTTT.
5.2.1.1.2 Xác thực nguồn gửi	Tự xây dựng.
5.2.1.2 Tiếp nhận dữ liệu	Tham khảo Mục II.4.5. Cách thức tiếp nhận log của Quyết định số 1127/QĐ-BTTTT và Bảng 6 (Table 6), tính năng Data Collection của SANS.
5.2.1.2.1 Cách thức và giao thức tiếp nhận nhật ký	Tham khảo Mục II.4.5. Cách thức tiếp nhận log của Quyết định số 1127/QĐ-BTTTT.
5.2.1.2.2 Đồng bộ thời gian dữ liệu đầu vào	Tham khảo Mục II.4.7. Đồng bộ hóa thời gian log của Quyết định số 1127/QĐ-BTTTT.
5.2.1.2.3 Phương thức thu thập bổ sung	Tự xây dựng dựa trên Bảng 6, tính năng Data Collection (thu thập qua API, Cloud systems, Streaming protocol) của SANS.
5.2.1.3 Giám sát luồng dữ liệu đầu vào	Tham khảo Mục II.4.10 và II.4.11 của Quyết định số 1127/QĐ-BTTTT.
5.2.1.3.1 Giám sát luồng nhật ký theo thời gian thực	Tham khảo Mục II.4.11. Giám sát log tiếp nhận được theo thời gian thực của Quyết định số 1127/QĐ-BTTTT.
5.2.1.3.2 Giám sát hiệu năng và trạng thái quá trình tiếp nhận	Tham khảo Mục II.4.10. Giám sát hiệu năng quá trình tiếp nhận log của Quyết định số 1127/QĐ-BTTTT.
5.2.1.3.3 Kiểm tra chất lượng dữ liệu nhật ký	Tham khảo Mục II.4.8. Lưu trữ log dưới dạng dữ liệu thô của Quyết định số 1127/QĐ-BTTTT. Bổ sung các chuẩn chất lượng từ lớp Data Management của SANS.
5.2.1.3.4 Giám sát tính liên tục của nguồn gửi nhật ký	Tự xây dựng (bảo đảm khả năng phát hiện khi một nguồn dừng gửi nhật ký).
5.2.1.4 Quản lý bộ thu thập nhật ký	Tự xây dựng (Quản lý thiết bị collector tập trung).
5.2.1.5 Xử lý dữ liệu tại đầu vào	Tham khảo Bảng 2, tính năng Data Aggregation (tổng hợp, gộp sự kiện trùng lặp) của SANS.

5.2.1.6 Nạp lại dữ liệu nhật ký	Tự xây dựng.
5.2.2 Chuẩn hóa, làm giàu, lưu trữ và bảo vệ dữ liệu	Tham khảo Bảng 2, tính năng Storage, Retention của SANS.
5.2.2.1 Xử lý dữ liệu	Tham khảo Mục II.4.6, II.4.9, II.4.12 của Quyết định số 1127/QĐ-BTTTT.
5.2.2.1.1 Phân tích cú pháp, chuẩn hóa và định dạng nhật ký	Tham khảo Mục II.4.6. Chuẩn hóa log của Quyết định số 1127/QĐ-BTTTT.
5.2.2.1.2 Xử lý và ánh xạ dữ liệu địa chỉ IP/MAC cơ bản	Tham khảo Mục II.4.12. Xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP của Quyết định số 1127/QĐ-BTTTT.
5.2.2.1.3 Làm giàu thông tin	Tham khảo Mục II.4.9. Làm giàu thông tin của Quyết định số 1127/QĐ-BTTTT.
5.2.2.1.4 Mô hình dữ liệu chuẩn hóa	Tự xây dựng.
5.2.2.1.5 Xây dựng và kiểm thử bộ phân tích cú pháp	Tự xây dựng.
5.2.2.2 Lưu trữ và quản lý vòng đời	Tham khảo Mục II.4.4. Quản lý log và Mục II.4.8. Lưu trữ log dưới dạng dữ liệu thô của Quyết định số 1127/QĐ-BTTTT.
5.2.2.2.1 Lưu trữ trực tuyến, ngoại tuyến và chính sách luân chuyển	Tham khảo Mục II.4.4. Quản lý log của Quyết định số 1127/QĐ-BTTTT.
5.2.2.2.2 Quản lý chỉ mục phục vụ truy vấn	Tham khảo Mục II.4.4. Quản lý log của Quyết định số 1127/QĐ-BTTTT.
5.2.2.2.3 Phân tầng lưu trữ và khôi phục dữ liệu	Tham khảo Bảng 6, tính năng Log Retention and Storage (mô hình dữ liệu phân tầng Tiered model, Data Lake) của SANS.
5.2.2.3 Bảo vệ dữ liệu nhật ký	Tham khảo Mục II.3.2 và II.4.13 của Quyết định số 1127/QĐ-BTTTT.
5.2.2.3.1 Truyền dữ liệu an toàn	Tham khảo Mục II.4.13. Truyền dữ liệu an toàn của Quyết định số 1127/QĐ-BTTTT.
5.2.2.3.2 Đảm bảo tính toàn vẹn của dữ liệu lưu trữ	Tham khảo Mục II.3.2. Bảo vệ dữ liệu log của Quyết định số 1127/QĐ-BTTTT. Bổ sung yêu cầu mã băm đối soát.
5.2.2.3.3 Mã hóa dữ liệu lưu trữ, kiểm soát truy cập dữ liệu nhạy cảm	Tự xây dựng (yêu cầu tích hợp thiết bị HSM, KMS bảo vệ vòng đời khóa mật mã).

5.2.2.3.4 Che giấu và ẩn danh dữ liệu nhạy cảm	Tự xây dựng (bảo vệ quyền riêng tư người dùng trong dữ liệu).
5.2.3 Phân tích, tương quan, phát hiện và cảnh báo	Tham khảo Mục II.7. Phân tích tương quan sự kiện và cảnh báo của Quyết định số 1127/QĐ-BTTTT và lớp Monitoring/Analytics Layer của SANS.
5.2.3.1. Phân tích tương quan sự kiện theo thời gian thực dựa trên luật	Tham khảo Mục II.7.1. Phân tích tương quan sự kiện theo thời gian thực của Quyết định số 1127/QĐ-BTTTT.
5.2.3.1.1 Các phương thức phát hiện	Tham khảo Mục II.7.1 của Quyết định số 1127/QĐ-BTTTT và Bảng 6, tính năng Monitoring/Auditing (Event correlation) của SANS.
5.2.3.2 Quản lý tập luật	Tham khảo Mục II.7.2. Phân tích tương quan sự kiện sử dụng danh sách động của Quyết định số 1127/QĐ-BTTTT.
5.2.3.2.1 Xây dựng, tùy biến quy tắc tương quan và ngưỡng phát hiện	Tham khảo Bảng 7, tính năng Rules Management (xây dựng rule dễ dàng, hỗ trợ tùy biến) của SANS.
5.2.3.2.2 Cập nhật tập luật bảo vệ, dấu hiệu nhận dạng	Tự xây dựng.
5.2.3.2.3 Ánh xạ luật phát hiện theo khung phân loại kỹ thuật tấn công	Tự xây dựng (ánh xạ theo framework MITRE ATT&CK).
5.2.3.2.4 Kiểm thử và đánh giá hiệu quả luật	Tự xây dựng.
5.2.3.2.5 Quản lý ngoại lệ	Tự xây dựng.
5.2.3.2.6 Quản lý luật dưới dạng mã	Tự xây dựng (hỗ trợ các định dạng mở như Sigma).
5.2.3.3 Cung cấp ngữ cảnh phát hiện	Tham khảo Bảng 6, tính năng Use of Threat Intelligence và Threat Intelligence Sources của SANS.
5.2.3.3.1 Quản lý và liên kết ngữ cảnh tài sản	Tự xây dựng.
5.2.3.3.2 Tiếp nhận và liên kết thông tin lỗ hổng bảo mật	Tự xây dựng.

5.2.3.3.3 Sử dụng thông tin tình báo mối đe dọa trong phân tích ngữ cảnh	Tham khảo Bảng 6, tính năng Use of Threat Intelligence của SANS.
5.2.3.3.4 Định danh tài sản trong môi trường động	Tự xây dựng.
5.2.3.4 Cảnh báo sự cố	Tham khảo Mục II.7.3, II.7.4, II.7.5 của Quyết định số 1127/QĐ-BTTTT.
5.2.3.4.1 Cơ chế cảnh báo và phân loại mức độ nghiêm trọng	Tham khảo Mục II.7.3. Cảnh báo theo thời gian thực và Mục II.7.4. Cảnh báo về các nhóm đối tượng được giám sát của Quyết định số 1127/QĐ-BTTTT.
5.2.3.4.2 Phân phối cảnh báo đa phương thức	Tham khảo Mục II.7.5. Cảnh báo theo nhiều phương thức của Quyết định số 1127/QĐ-BTTTT. Tham khảo Bảng 6, tính năng Alerting của SANS.
5.2.3.4.3 Xử lý và tinh giản cảnh báo trước khi phân phối	Tự xây dựng (khử trùng lặp cảnh báo).
5.2.3.4.4 Bảo đảm phân phối cảnh báo	Tự xây dựng.
5.2.3.5 Phân tích hành vi nâng cao	Tham khảo Bảng 1 tính năng UEBA và Bảng 2 tính năng Analytics (ML/AI nhận diện bất thường) của SANS.
5.2.4 Điều tra, truy vấn, săn lùng, trực quan và báo cáo	Tham khảo Bảng 2, lớp User Interaction Layer và Workflow/Automation Layer của SANS.
5.2.4.1 Truy vấn, tìm kiếm và lọc dữ liệu sự kiện	Tham khảo Bảng 6, tính năng Data Exploration: Query Development của SANS.
5.2.4.1.1 Năng lực của ngôn ngữ truy vấn	Tham khảo Bảng 6, tính năng Data Exploration (customizable queries, hunting threats) của SANS.
5.2.4.1.2 Tác vụ truy vấn nền	Tự xây dựng.
5.2.4.2 Săn lùng mối đe dọa	Tham khảo Bảng 2, tính năng Operations: Threat hunting/investigation và Forensic analysis của SANS.
5.2.4.2.1 Hỗ trợ luồng công việc điều tra chủ động và phân tích nguyên nhân gốc	Tham khảo Bảng 6, tính năng Integration of Visibility and Context Functionality (xác định chuỗi tấn công) của SANS.
5.2.4.2.2 Quản lý các trường hợp sự cố	Tham khảo Bảng 2, tính năng Operations: Incident response (case management) của SANS.

5.2.4.2.3 Hỗ trợ vận hành nghiệp vụ giám sát an ninh mạng liên tục	Tham khảo Bảng 6, tính năng End-to-End Process Logging của SANS.
5.2.4.2.4 Khung nhìn theo thực thể	Tự xây dựng.
5.2.4.2.5 Quản lý chiến dịch săn lùng	Tự xây dựng.
5.2.4.2.6 Quản lý hồ sơ sự cố	Tham khảo Bảng 2, tính năng Operations: Incident response của SANS.
5.2.4.3 Trực quan hóa và báo cáo	Tham khảo Mục II.2.4. Quản lý báo cáo của Quyết định số 1127/QĐ-BTTTT.
5.2.4.3.1 Bảng điều khiển tổng quan	Tham khảo Bảng 6, tính năng Visualization của SANS.
5.2.4.3.2 Lập lịch, quản lý và xuất báo cáo vận hành cơ bản	Tham khảo Mục II.2.4. Quản lý báo cáo của Quyết định số 1127/QĐ-BTTTT. Tham khảo Bảng 6, tính năng Reporting của SANS.
5.2.4.3.3 Trích xuất dữ liệu thô phục vụ điều tra	Tham khảo Bảng 2, tính năng Forensic analysis của SANS.
5.2.4.3.4 Báo cáo hiệu quả vận hành	Tự xây dựng.
5.2.4.3.5 Xuất dữ liệu phục vụ công tác nghiệp vụ	Tự xây dựng (bổ sung chữ ký số và đối soát gói dữ liệu).
5.2.5 Tích hợp và tương tác với hệ thống khác	Tham khảo Mục II.2.9. Chia sẻ dữ liệu của Quyết định số 1127/QĐ-BTTTT. Tham khảo Bảng 2, tính năng Operations: Automation của SANS.
5.2.5.1 Giao diện và kết nối chia sẻ dữ liệu	Tham khảo Mục II.2.9 của Quyết định số 1127/QĐ-BTTTT.
5.2.5.1.1 Cung cấp giao diện hoặc API truy xuất dữ liệu mở	Tham khảo Bảng 6, tính năng Integration of Visibility and Context Functionality (API integration) của SANS.
5.2.5.1.2 Chuyển tiếp sự kiện tới hệ thống cấp trên	Tham khảo Mục II.2.9. Chia sẻ dữ liệu của Quyết định số 1127/QĐ-BTTTT.
5.2.5.1.3 Giao diện lập trình cho các chức năng nghiệp vụ	Tham khảo Bảng 7, tính năng Custom Integration: Third-Party Products của SANS.
5.2.5.2 Trao đổi dữ liệu	Tự xây dựng.
5.2.5.2.1 Hỗ trợ các định dạng sự kiện phổ biến	Tự xây dựng dựa trên danh sách tại Mục II.4.6 của Quyết định số 1127/QĐ-BTTTT.

5.2.5.2.2 Xác thực thiết bị, bảo mật kênh truyền và xử lý lỗi khi tương tác	Tham khảo Mục II.4.13. Truyền dữ liệu an toàn của Quyết định số 1127/QĐ-BTTTT.
5.2.5.3 Tích hợp hệ thống	Tham khảo Bảng 2, tính năng Operations: Automation của SANS.
5.2.5.3.1 Tích hợp nền tảng tình báo mối đe dọa an ninh mạng (TIP)	Tham khảo Bảng 6, tính năng Threat Intelligence Sources của SANS.
5.2.5.3.2 Tích hợp hệ thống điều phối, phản ứng (SOAR) và thiết bị ngăn chặn	Tham khảo Bảng 2, tính năng Operations: Automation (tương thích SOAR) của SANS.
5.2.5.3.3 Tích hợp với hệ thống quản lý dịch vụ công nghệ thông tin và xử lý sự cố	Tham khảo Bảng 7, tính năng Custom Integration: Third-Party Products (như IT ticketing) của SANS.
5.2.5.3.4 Đồng bộ hai chiều với hệ thống điều phối, tự động hóa, phản ứng và hệ thống quản lý dịch vụ công nghệ thông tin bên ngoài	Tự xây dựng.
5.2.6 Hiệu năng, khả năng mở rộng, tính sẵn sàng và phục hồi	Tham khảo Mục II.5. Yêu cầu về hiệu năng xử lý của Quyết định số 1127/QĐ-BTTTT. Tham khảo Bảng 7, nhóm Performance and Sizing và Failover and Redundancy của SANS.
5.2.6.1 Yêu cầu về hiệu năng xử lý	Tham khảo Mục II.5.1, II.5.2, II.5.3 của Quyết định số 1127/QĐ-BTTTT.
5.2.6.1.1 Năng lực xử lý sự kiện (EPS) và giới hạn tỷ lệ mất dữ liệu	Tham khảo Bảng 7, tính năng Velocity (đáp ứng benchmark EPS Normal và EPS Peak) của SANS.
5.2.6.1.2 Độ trễ xử lý từ khi nhận dữ liệu đến khi sinh cảnh báo	Tham khảo Mục II.5.1. Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu của Quyết định số 1127/QĐ-BTTTT.
5.2.6.1.3 Khả năng chịu tải đồng thời	Tham khảo Mục II.5.2 và Mục II.5.3 của Quyết định số 1127/QĐ-BTTTT.
5.2.6.1.4 Thời gian đáp ứng truy vấn phân tích dữ liệu lớn	Tham khảo Mục II.5.1 của Quyết định số 1127/QĐ-BTTTT.
5.2.6.2 Tính sẵn sàng và phục hồi	Tham khảo Bảng 7, tính năng Failover and Redundancy của SANS.

5.2.6.2.1 Sao lưu và phục hồi cấu hình, tập luật, dữ liệu	Tự xây dựng.
5.2.6.2.2 Giám sát trạng thái của hệ thống	Tham khảo Bảng 7, tính năng Status Monitoring của SANS.
5.2.6.2.3 Cơ chế đệm/phục hồi hàng đợi khi quá tải hoặc gián đoạn	Tự xây dựng.
5.2.6.2.4 Dự phòng và độ sẵn sàng cao	Tham khảo Bảng 7, tính năng Failover and Redundancy (phương pháp cấu trúc dự phòng) của SANS.
5.2.6.2.5 Giám sát chi tiết và xuất chỉ số vận hành	Tự xây dựng.
5.2.6.2.6 Vận hành trong điều kiện mạng hạn chế	Tự xây dựng.
5.2.6.3 Khả năng mở rộng và kiến trúc	Tham khảo Bảng 7, nhóm Overall Scalability and Growth của SANS.
5.2.6.3.1 Hỗ trợ mở rộng theo chiều ngang và chiều dọc	Tham khảo Bảng 7, tính năng Overall Scalability and Growth của SANS.
5.2.6.3.2 Hỗ trợ kiến trúc đa khách hàng/đa phân vùng	Tự xây dựng.
5.2.7 Phân quyền và kiểm soát hoạt động người dùng	Tự xây dựng.
5.2.7.1 Mô hình phân quyền	Tự xây dựng. Quản lý phân quyền dựa trên vai trò (RBAC).
5.2.7.2 Nhật ký hoạt động của người dùng nghiệp vụ	Tự xây dựng.
5.2.7.3 Che dữ liệu nhạy cảm	Tự xây dựng.