BỘ THÔNG TIN VÀ TRUYỀN THÔNG **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

Độc lập – Tự do – Hạnh phúc

Số: /QĐ-BTTTT *Hà Nội, ngày tháng năm 2021*

QUYẾT ĐỊNH
Ban hành Yêu cầu kỹ thuật cơ bản đối với sản phẩm Quản lý và phân tích sự kiện an toàn thông tin

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Yêu cầu kỹ thuật cơ bản đối với sản phẩm Quản lý và phân tích sự kiện an toàn thông tin (SIEM).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm SIEM đáp ứng các yêu cầu kỹ thuật cơ bản theo Điều 1 Quyết định này.

Điều 3. Cục An toàn thông tin chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn việc áp dụng các yêu cầu trong Yêu cầu kỹ thuật cơ bản đối với sản phẩm SIEM tại Điều 1 Quyết định này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng thông tin điện tử của Bộ;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng

YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM QUẢN LÝ VÀ PHÂN TÍCH SỰ KIỆN AN TOÀN THÔNG TIN

(Kèm theo Quyết định số /QĐ-BTTTT ngày tháng năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Phạm vi áp dụng

Tài liệu này mô tả các yêu cầu kỹ thuật cơ bản để đánh giá chất lượng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin (SIEM). Tài liệu bao gồm các nhóm yêu cầu là Yêu cầu về tài liệu, Yêu cầu về quản trị hệ thống, Yêu cầu về kiểm soát lỗi, Yêu cầu về log, Yêu cầu về hiệu năng xử lý, Yêu cầu về chức năng tự bảo vệ, Yêu cầu về chức năng phân tích tương quan sự kiện và cảnh báo.

2. Đối tượng áp dụng

Các cơ quan, tổ chức có liên quan đến hoạt động nghiên cứu, phát triển; đánh giá, lựa chọn sản phẩm Quản lý và phân tích sự kiện an toàn thông tin khi đưa vào sử dụng trong các hệ thống thông tin.

3. Khái niệm và thuật ngữ

Trong tài liệu này các khái niệm và thuật ngữ được hiểu như sau:

3.1. Tập luật bảo vệ

Danh sách các luật bao gồm các tham số, quy tắc được định nghĩa và thiết lập bởi quản trị viên dùng, cho phép sản phẩm phát hiện, cảnh báo những sự kiện, nguy cơ, sự cố và các hành vi gây mất an toàn thông tin khác đối với các đối tượng, hệ thống được bảo vệ.

3.2. Danh sách động

Danh sách chứa các phần tử được xác định theo một loại dữ liệu cụ thể mà số lượng phần tử trong danh sách được cập nhật liên tục trong quá trình sử dụng và vận hành SIEM (ví dụ: danh sách các địa chỉ IP thuộc nhóm mạng máy tính ma botnet; danh sách các tên miền máy chủ điều khiển tấn công C&C;…).

3.3. Dữ liệu thô

Dữ liệu nguyên bản mà chưa thông qua quá trình phân tích cú pháp.

3.4. Theo thời gian thực

Việc đưa ra kết quả xử lý của một tác vụ cụ thể trong khoảng thời gian không

quá 03 giây.

3.5. Nhật ký hệ thống (log)

Sự kiện an toàn thông tin được hệ thống ghi lại, liên quan đến trạng thái hoạt động, thông báo, cảnh báo, sự cố, cuộc tấn công và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.6. Thời gian duy trì phiên kết nối (session timeout)

Khoảng thời gian được thiết lập để cho phép hệ thống hủy phiên kết nối đối với một máy khách, nếu trong khoảng thời gian này mà hệ thống không nhận được yêu cầu mới từ máy khách đó.

3.7. Phân tích cú pháp (parsing)

Việc trích xuất dữ liệu theo các quy tắc được định nghĩa trước để tạo ra các trường thông tin có ý nghĩa.

3.8. Đánh chỉ mục (indexing)

Việc tách chọn, tổ chức, sắp xếp dữ liệu theo các quy tắc, cấu trúc dữ liệu được định nghĩa trước nhằm mục đích tăng tốc độ tìm kiếm và truy xuất dữ liệu.

3.9. Phân tích tương quan sự kiện (correlation)

Việc áp dụng tập luật bảo vệ được định nghĩa trước để hình thành nên các sự kiện an toàn thông tin có ý nghĩa nhằm mục đích sinh ra các cảnh báo cho người dùng về các nguy cơ, dấu hiệu, hành vi và cuộc tấn công gây mất an toàn thông tin mà hệ thống phát hiện được.

3.10. Làm giàu thông tin (enrichment)

Việc bổ sung các trường thông tin cho log mà không phải do sinh từ quá trình phân tích cú pháp (ví dụ: phân giải từ tên định danh máy trạm thành các trường thông tin về hệ điều hành máy trạm, địa chỉ IP máy trạm,…) để làm dữ liệu đầu vào cho các luật phân tích tương quan sự kiện phục vụ cho quá trình sinh cảnh báo của SIEM.

3.11. Thành phần tích hợp bên trong

Các thiết bị, phần mềm, ứng dụng cơ bản, thiết yếu và cấu thành nên SIEM bao gồm Receiver, Parser, Indexer, Storage, Correlator.

3.12. Thành phần thu thập log (Collector)

Thành phần tích hợp bên ngoài SIEM có chức năng thu thập log để gửi về SIEM bao gồm hai loại là Endpoint Collector và Relay Collector. Ngoài ra, Collector có thể tích hợp thêm chức năng lọc dữ liệu và làm giàu thông tin cho log trước khi gửi.

3.13. Thành phần thu thập log đầu cuối (Endpoint Collector)

Collector được triển khai tại các thiết bị đầu cuối, có chức năng gửi dữ liệu log được sinh ra trên thiết bị đầu cuối về Relay Collector hoặc Receiver.

3.14. Thành phần thu thập log trung gian (Relay Collector)

Collector được triển khai thêm khi cần thiết, có chức năng chuyển tiếp dữ liệu log tập trung từ nhiều Endpoint Collector về Receiver.

3.15. Thành phần tiếp nhận log (Receiver)

Thành phần có chức năng nhận dữ liệu log từ nhiều Collector và gửi đến Parser. Ngoài ra, Receiver có thể tích hợp thêm chức năng lọc dữ liệu và làm giàu thông tin cho log trước khi gửi.

3.16. Thành phần phân tích cú pháp log (Parser)

Thành phần có chức năng phân tích cú pháp log và gửi kết quả cho Indexer. Parser có thể truyền dữ liệu đồng thời cho Indexer và Correlator.

3.17. Thành phần đánh chỉ mục log (Indexer)

Thành phần có chức năng đánh chỉ mục log và lưu kết quả tại Storage.

3.18. Thành phần phân tích tương quan sự kiện (Correlator)

Thành phần có chức năng phân tích tương quan sự kiện. Correlator có thể xử lý dữ liệu được gửi trực tiếp từ Parser hoặc được truy vấn từ Storage.

3.19. Thành phần lưu trữ dữ liệu (Storage)

Thành phần có chức năng lưu trữ các loại dữ liệu như: dữ liệu thô của log, các trường thông tin của log, dữ liệu cảnh báo từ Correlator, dữ liệu cấu hình, dữ liệu log sao lưu,…

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

SIEM có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

2. Yêu cầu về quản trị hệ thống

2.1. Quản lý vận hành

SIEM cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

b) Cho phép thay đổi thời gian hệ thống;

c) Cho phép thay đổi thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,…);

đ) Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;

e) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;

g) Cho phép xóa log;

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

2.2. Quản trị từ xa

SIEM cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

2.3. Quản lý xác thực và phân quyền

SIEM cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

2.4. Quản lý báo cáo

SIEM cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML;

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra.

2.5. Quản lý tập luật bảo vệ

SIEM cho phép quản lý tập luật bảo vệ bao gồm các thao tác sau:

a) Thêm luật mới;

b) Tinh chỉnh luật;

c) Tìm kiếm luật;

d) Xóa luật;

đ) Kích hoạt/vô hiệu hóa luật;

e) Xuất tập luật ra tệp tin;

g) Khôi phục tập luật từ tệp tin;

h) Cập nhật tập luật được phát hành bởi nhà sản xuất.

2.6. Cập nhật tập luật bảo vệ

SIEM cho phép cập nhật tập luật bảo vệ đáp ứng các yêu cầu sau:

a) Cho phép tự động thông báo có bản cập nhật mới cho quản trị viên;

b) Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới.

2.7. Quản lý đối tượng được giám sát và nguồn gửi log

SIEM cho phép quản lý đối tượng được giám sát và nguồn gửi log đáp ứng các yêu cầu sau:

a) Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo các nhóm được định nghĩa bởi quản trị viên;

b) Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo địa chỉ vật lý, địa chỉ mạng và vị trí địa lý.

2.8. Quản lý và giám sát tập trung các thành phần tích hợp bên trong

SIEM cho phép quản lý và giám sát tập trung thông qua giao diện đồ họa các thông số hiệu năng sau của các thành phần tích hợp bên trong:

a) Receiver;

b) Parser;

c) Indexer;

d) Storage;

đ) Correlator.

2.9. Chia sẻ dữ liệu

SIEM cho phép kết nối với các loại hệ thống sau để chia sẻ dữ liệu:

a) Hệ thống giám sát an toàn không gian mạng quốc gia;

b) Hệ thống SIEM khác được phát triển bởi chính nhà sản xuất.

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp SIEM phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SIEM đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình tập luật bảo vệ.

3.2. Bảo vệ dữ liệu log

Trong trường hợp SIEM phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SIEM đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

3.3. Đồng bộ thời gian hệ thống

Trong trường hợp SIEM phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SIEM đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

4. Yêu cầu về log

4.1. Log quản trị hệ thống

a) SIEM cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i) Đăng nhập, đăng xuất tài khoản;

ii) Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii) Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

iv) Kích hoạt lệnh khởi động lại, tắt hệ thống;

v) Thay đổi thủ công thời gian hệ thống.

b) SIEM cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i) Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy trạm;

iii) Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,…);

iv) Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,…);

v) Kết quả thực hiện hành vi (thành công hoặc thất bại).

vi) Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,…).

4.2. Log cảnh báo

SIEM cho phép ghi log cảnh báo được sinh ra bởi việc thực thi tập luật bảo vệ.

4.3. Định dạng log

SIEM cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

4.4. Quản lý log

SIEM cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,…).

b) Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép phân nhóm log thành các nhóm sự kiện theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng, các dạng tấn công, các nguồn log,…);

d) Cho phép truy xuất dữ liệu thô của log thông qua kết quả tìm kiếm và cảnh báo;

e) Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra log.

4.5. Cách thức tiếp nhận log

SIEM cho phép tiếp nhận log gửi từ Collector thông qua các cách thức sau:

a) Tiếp nhận log qua kết nối UDP;

b) Tiếp nhận log qua kết nối TCP không mã hóa;

c) Tiếp nhận log qua kết nối TCP có mã hóa như TLS hoặc tương đương.

4.6. Chuẩn hóa log

SIEM cho phép tiếp nhận và chuẩn hóa log gửi từ Collector theo tối thiểu 10 loại log khác nhau đáp ứng các yêu cầu sau:

a) Chuẩn hóa được log theo các định dạng tệp tin cơ bản tối thiểu với 01 trong các định dạng bao gồm: SYSLOG, JSON, CSV, CEF, NETFLOW;

b) Chuẩn hóa được log của hệ điều hành Windows và Unix;

c) Chuẩn hóa được log của tối thiểu 02 loại tường lửa khác nhau;

d) Chuẩn hóa được log của tối thiểu 04 loại thiết bị mạng khác nhau.

4.7. Đồng bộ hóa thời gian log

SIEM cho phép đồng bộ hóa thời điểm log được tiếp nhận tại Receiver và thời điểm log được thu thập tại Collector dựa trên cài đặt về múi giờ đã được thiết lập.

4.8. Lưu trữ log dưới dạng dữ liệu thô

SIEM cho phép lưu trữ tất cả log dưới dạng dữ liệu thô bất kể có thể phân tích cú pháp được hay không.

4.9. Làm giàu thông tin

SIEM cho phép làm giàu thông tin cho log (ví dụ: phân giải chuỗi ký tự định danh thành tên tài khoản người dùng; lưu lại mốc thời gian sinh log theo múi giờ cục bộ tại máy trạm;…).

4.10. Giám sát hiệu năng quá trình tiếp nhận log

SIEM cho phép giám sát thông qua giao diện đồ họa các thông số hiệu năng sau của quá trình tiếp nhận log:

a) Số lần thử kết nối lại đến Collector;

b) Thông báo về kết nối không thành công đến Collector;

c) Số lượng tác vụ tiếp nhận log mà không được thực hiện thành công.

4.11. Giám sát log tiếp nhận được theo thời gian thực

SIEM cho phép giám sát thông qua giao diện đồ họa log gửi từ Collector đáp ứng các yêu cầu sau:

a) Cho phép tạo thống kê dữ liệu theo thời gian thực;

b) Cho phép tìm kiếm và tạo thống kê dữ liệu theo khoảng thời gian xác định.

4.12. Xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP

SIEM cho phép xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP tối thiểu theo định dạng IPv4 (ví dụ: xử lý truy vấn tìm kiếm dữ liệu bằng dải địa chỉ IP,…).

4.13. Truyền dữ liệu an toàn

SIEM cho phép mã hóa dữ liệu hoặc sử dụng giao thức có mã hóa để trao đổi dữ liệu giữa Collector và Receiver.

5. Yêu cầu về hiệu năng xử lý

SIEM được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất phải đảm bảo đáp ứng các yêu cầu sau:

5.1. Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu

SIEM đảm bảo rằng độ trễ thời gian tìm kiếm log với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 02 phút.

5.2. Xử lý đồng thời nhiều tác vụ

SIEM cho phép xử lý đồng thời tối thiểu 03 tác vụ khác nhau đáp ứng các yêu cầu sau:

a) Cho phép tiếp nhận log theo thời gian thực đồng thời từ tối thiểu 03 nguồn log khác nhau;

b) Có khả năng xử lý đồng thời theo thời gian thực tối thiểu 02 tác vụ cho việc tìm kiếm log và phân tích tương quan sự kiện (ví dụ: nhiều người dùng cùng lúc truy cập và tìm kiếm dữ liệu,…).

5.3. Xử lý đồng thời nhiều sự kiện

SIEM cho phép xử lý và lưu trữ dữ liệu đồng thời 5000 sự kiện trong khoảng thời gian là 01 phút.

6. Yêu cầu về chức năng tự bảo vệ

6.1. Phát hiện và ngăn chặn tấn công hệ thống

SIEM có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm tối thiểu các dạng sau:

a) SQL Injection;

b) OS Command Injection;

c) XPath Injection;

d) Remote File Inclusion (RFI);

đ) Local File Inclusion (LFI);

e) Cross-Site Scripting (XSS);

g) Cross-Site Request Forgery (CSRF).

6.2. Cập nhật bản vá hệ thống

SIEM có chức năng cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật.

7. Yêu cầu về chức năng phân tích tương quan sự kiện và cảnh báo

7.1. Phân tích tương quan sự kiện theo thời gian thực

SIEM cho phép phân tích tương quan sự kiện theo thời gian thực đối với dữ liệu log thu thập được.

7.2. Phân tích tương quan sự kiện sử dụng danh sách động

SIEM cho phép phân tích tương quan sự kiện sử dụng thông tin trong danh sách động (ví dụ: tạo luật để so khớp địa chỉ IP, tên miền hoặc giá trị hàm băm đối với một danh sách có thể được cập nhật tự động từ phía nhà sản xuất,…).

7.3. Cảnh báo theo thời gian thực

SIEM cho phép tự động cảnh báo tới người dùng theo thời gian thực đối với các loại sự kiện sau:

a) Cảnh báo về việc hệ thống ngừng lưu trữ thêm dữ liệu mới khi Storage đã đạt ngưỡng giới hạn lưu trữ mà không thể lưu được dữ liệu mới;

b) Cảnh báo về dấu hiệu, nguy cơ, sự cố, cuộc tấn công và các hành vi gây mất an toàn thông tin khác dựa trên kết quả thực thi luật phân tích tương quan sự kiện.

7.4. Cảnh báo về các nhóm đối tượng được giám sát

SIEM cho phép sinh cảnh báo chứa các thông tin thuộc nhóm đối tượng được giám sát (ví dụ: cảnh báo về việc có truy cập vào máy chủ email; cảnh báo có truy cập từ xa vào dải địa chỉ IP dành cho các máy chủ,…).

7.5. Cảnh báo theo nhiều phương thức

SIEM cho phép tự động cảnh báo theo các phương thức sau:

a) Hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo;

b) Cảnh báo qua phương thức gửi thư điện tử hoặc tin nhắn SMS.