BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 764 /QĐ-BTTTT	*Hà nội, ngày 25 tháng 04 năm 2022*

QUYẾT ĐỊNH

Ban hành Yêu cầu kỹ thuật cơ bản đối với sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối

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 Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối (Endpoint Detection and Response - EDR).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm EDR 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 EDR 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

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM PHÁT HIỆN VÀ PHẢN ỨNG SỰ CỐ AN TOÀN THÔNG TIN TRÊN THIẾT BỊ ĐẦU CUỐI

(Kèm theo Quyết định số /QĐ-BTTTT ngày tháng năm 2022 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 đối với sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối (Endpoint Detection and Response - EDR). Tài liệu bao gồm các nhóm yêu cầu: 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 tài nguyên xử lý, Yêu cầu về tính khả dụng của hệ thống, Yêu cầu về chức năng phát hiện và phản ứng.

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 EDR 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 của EDR gồm các tham số, quy tắc được định nghĩa và thiết lập bởi quản trị viên dùng để phát hiện những sự kiện mất an toàn thông tin và sinh cảnh báo cho người dùng về các nguy cơ, sự cố, cuộc tấn công và các hành vi gây mất an toàn thông tin khác đối với các đối tượng, hệ thống được bảo vệ.

3.2. 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).

3.3. Phần mềm EDR trên máy chủ/máy trạm (agent)

Phần mềm được cài đặt trên máy chủ/máy trạm để thực hiện chức năng phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đó và được quản lý tập trung bởi máy chủ EDR.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

Sản phẩm EDR 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

Sản phẩm EDR 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;

i) Cho phép gửi cảnh báo qua thư điện tử hoặc tin nhắn.

2.2. Quản trị từ xa

Sản phẩm EDR 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

Sản phẩm EDR 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

Sản phẩm EDR 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

Sản phẩm EDR 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

Sản phẩm EDR 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 tập trung các máy chủ/máy trạm

Sản phẩm EDR cho phép quản lý tập trung các máy chủ/máy trạm thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép quản lý tập trung các máy chủ/máy trạm trên tối thiểu hai nền tảng Window và Linux.

b) Quản lý thông tin trên máy chủ/máy trạm bao gồm các thông tin sau:

i. Địa chỉ IP, MAC, Tên máy, Hệ điều hành, Thời gian cập nhật gần nhất của Hệ điều hành trên máy chủ/máy trạm;

ii. Trạng thái kết nối đến máy chủ EDR;

iii. Thông tin bản vá trên máy chủ/máy trạm;

iv. Trạng thái cập nhật thông tin từ máy chủ EDR;

v. Chính sách được thiết lập và các vi phạm trên agent.

c) Có khả năng điều khiển agent tối thiểu bao gồm các chức năng sau:

i. Cho phép phân tích, xóa, sửa tệp tin lây nhiễm mã độc trên máy chủ/máy trạm;

ii. Cho phép điều khiển thay đổi các chính sách phát hiện, ngăn chặn mã độc trên các agent;

iii. Cho phép sửa giá trị thanh ghi và các giá trị khác để ngăn chặn mã độc tự khởi động trên máy chủ/máy trạm sau khi khởi động lại.

2.8. Đồng bộ dữ liệu với các hệ thống khác

Sản phẩm EDR cho phép kết nối với tối thiểu một trong các loại hệ thống sau để đồng bộ dữ liệu:

a) Tích hợp với hệ thống quản lý và phân tích sự kiện an toàn thông tin (SIEM);

b) Hệ thống Nền tảng tri thức mối đe dọa an toàn thông tin (TIP);

c) Tích hợp hệ thống phân tích mã độc tự động.

2.9. Chia sẻ dữ liệu

Sản phẩm EDR cho phép kết nối, chia sẻ dữ liệu với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền theo hướng dẫn tại Văn bản số 2290/BTTTT-CATTT ngày 17/07/2018 của Cục An toàn thông tin và các hướng dẫn khác liên quan của Bộ Thông tin và Truyền thông.

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp EDR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi

phần cứng), EDR 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 EDR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), EDR 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 EDR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), EDR 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) Sản phẩm EDR 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) Sản phẩm EDR 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 chủ/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

Sản phẩm EDR cho phép ghi log cảnh báo được sinh ra khi thực thi tập luật bảo vệ.

4.3. Định dạng log

Sản phẩm EDR 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

Sản phẩm EDR 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;

đ) 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. Lưu trữ log dưới dạng dữ liệu thô

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

5. Yêu cầu về tài nguyên xử lý

a) Agent cài trên máy chủ/máy trạm sử dụng tài nguyên tối đa, đáp ứng yêu cầu sau:

i. CPU < 20% ;

ii. RAM < 500 MB;

iii. Tốc độ truyền tải qua mạng: Tốc độ nhận < 2,7 KB/s, Tốc độ gửi < 0,4 KB/s.

b) Độ phủ phát hiện tấn công:

Đối với các dạng tấn công được công bố từ các nguồn công khai, EDR bảo đảm độ phủ phát hiện tấn công đáp ứng trên 85% với tỷ lệ cảnh báo đúng >= 80%.

6. Yêu cầu về tính khả dụng của hệ thống

Sản phẩm EDR hỗ trợ phương án triển khai đáp ứng các yêu cầu về tính khả dụng sau:

a) Kênh kết nối giữa agent và máy chủ EDR được mã hóa và có cơ chế xác thực;

b) Hỗ trợ triển khai theo mô hình High Availability (HA) hoặc Clustering;

c) Hỗ trợ cơ chế cân bằng tải (Load Balancing).

7. Yêu cầu về chức năng phát hiện và phản ứng

7.1. Phát hiện sự cố

Sản phẩm EDR có chức năng phát hiện sự cố đáp ứng các yêu cầu sau:

a) Cho phép phát hiện tấn công, mã độc dựa theo thông tin địa chỉ IP, tên miền, giá trị băm và theo hành vi;

b) Cho phép người dùng chủ động thực hiện quét tại các tệp tin và thư mục khả nghi tại máy của mình;

c) Cho phép quản lý cảnh báo; xem chi tiết thông tin cảnh báo; bổ sung, làm giàu thông tin cảnh báo;

d) Cho phép điều tra phản ứng trên một giao diện tập trung duy nhất.

7.2. Điều tra và phản ứng sự cố

Sản phẩm EDR có chức năng điều tra và phản ứng sự cố đáp ứng các yêu cầu sau:

a) Cho phép phân tích các tiến trình đang chạy từ xa trên máy chủ/máy trạm;

b) Cho phép tìm kiếm log trên máy chủ/máy trạm;

c) Cho phép thiết lập chính sách chặn các ứng dụng độc hại hoạt động trên máy chủ/máy trạm bằng cách định nghĩa đường dẫn/giá trị băm;

d) Cho phép chặn kết nối độc hại từ máy chủ/máy trạm bằng cách điều khiển tường lửa hệ điều hành trên máy chủ/máy trạm hoặc tường lửa được tích hợp trên EDR.