BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 1498 /QĐ-BTTTT

Hà Nội, ngày 10 tháng 8 năm 2022

QUYẾT ĐỊNH
Ban hành Yêu cầu kỹ thuật cơ bản đối với sản phẩm Phân tích và phát hiện hành vi bất thường của người dùng trên mạng

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 48/2022/NĐ-CP ngày 26 tháng 7 năm 2022 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 Phân tích và phát hiện hành vi bất thường của người dùng trên mạng (User and Entity Behavior Analytics – UEBA).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm UEBA 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 UEBA 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 PHÂN TÍCH VÀ PHÁT HIỆN HÀNH VI BẤT THƯỜNG CỦA NGƯỜI DÙNG TRÊN MẠNG

(Kèm theo Quyết định số 1998 /QĐ-BTTTT ngày 10 tháng 6 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 Phân tích và phát hiện hành vi bất thường của người dùng trên mạng (User and Entity Behavior Analytics – UEBA). 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 hiệu năng xử lý, Yêu cầu về chức năng tự bảo vệ, Yêu cầu về chức năng giám sát, phân tích sự kiện và đánh giá mức độ rủi ro an toàn thông tin; Yêu cầu về chức năng 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 UEBA 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. 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, thông tin về các mối đe dọa thu thập được và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.2. 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.

3.3. 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.

3.4. Nguồn gửi dữ liệu

Giải pháp, nền tảng, hệ thống công nghệ thông tin, an toàn thông tin chứa các sự kiện an toàn thông tin (ví dụ: Hệ quản trị cơ sở dữ liệu DBMS; Giải pháp Quản lý định danh và truy cập IAM; Sản phẩm Phòng, chống mã độc AV; Giải pháp Quản lý và phân tích sự kiện an toàn thông tin SIEM; Giải pháp Điều phối, tự động hóa và phản ứng an toàn thông tin SOAR; ...) để gửi về UEBA nhằm mục đích phân tích, giám sát và phát hiện bất thường.

3.5. Đích nhận cảnh báo

Giải pháp, nền tảng, hệ thống công nghệ thông tin, an toàn thông tin nhận các cảnh báo về dấu hiệu bất thường, nguy cơ mất an toàn thông tin được sinh ra bởi UEBA (ví dụ: Giải pháp Quản lý và phân tích sự kiện an toàn thông tin SIEM; Giải pháp Điều phối, tự động hóa và phản ứng an toàn thông tin SOAR; Thư điện tử Email; Tin nhắn SMS; ...) thông qua quá trình phân tích, xử lý dữ liệu đầu vào từ các nguồn gửi dữ liệu.

3.6. Hành vi được giám sát

Sự kiện log UEBA thu thập được có nội dung ghi lại về trạng thái hoạt động, các tương tác lẫn nhau giữa các đối tượng (người dùng, thiết bị đầu cuối ,...) được giám sát bởi UEBA dùng để làm dữ liệu đầu vào cho các quá trình thực thi kịch bản phát hiện bất thường và phân tích, đánh giá điểm rủi ro của các đối tượng đó.

3.7. Hành vi bất thường

Hành vi được cảnh báo bởi UEBA dựa trên kết quả thực thi các kịch bản phát hiện bất thường đã được cấu hình trên hệ thống hoặc kết quả phân tích, đánh giá tương quan những đối tượng được giám sát có điểm rủi ro vượt ngưỡng.

3.8. Kịch bản phát hiện bất thường

Luật của UEBA gồm các tham số, quy tắc được định nghĩa và thiết lập bởi quản trị viên được sử dụng để phân tích thông tin thu thập được từ các nguồn gửi dữ liệu, phát hiện ra các dấu hiệu bất thường đối với đối tượng được giám sát nhằm sinh và gửi cảnh báo sớm những nguy cơ, sự kiện mất an toàn thông tin về đích nhận cảnh báo.

3.9. Mô hình hồ sơ hóa (Profile)

Các mô hình học máy, thống kê mà UEBA sử dụng để mô tả lại thói quen, đặc tính hành vi của các đối tượng trong hệ thống được UEBA giám sát, bảo vệ.

Các mô hình này sẽ được sử dụng làm cơ sở để xác định, đánh giá các hành vi nào là bất thường.

3.10. Điểm rủi ro

Giá trị số thể hiện mức độ rủi ro của đối tượng trong hệ thống mà UEBA đang giám sát và bảo vệ.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

UEBA 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

UEBA 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

UEBA 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

UEBA 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;

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 tập nguồn gửi dữ liệu

UEBA cho phép quản lý tập nguồn gửi dữ liệu bao gồm các thao tác sau:

a) Thêm nguồn mới;

b) Sửa thông tin nguồn;

c) Tìm kiếm nguồn;

d) Xóa nguồn.

2.5. Quản lý tập đích nhận cảnh báo

UEBA cho phép quản lý tập đích nhận cảnh báo bao gồm các thao tác sau:

a) Thêm đích mới;

b) Sửa thông tin đích;

c) Tìm kiếm đích;

d) Xóa đích.

2.6. Quản lý tập hành vi được giám sát

UEBA cho phép quản lý tập hành vi được giám sát bao gồm các thao tác sau:

a) Thêm hành vi mới;

b) Sửa thông tin hành vi;

c) Tìm kiếm hành vi;

d) Xóa hành vi;

đ) Cập nhật tập hành vi được phát hành bởi nhà sản xuất.

2.7. Quản lý tập kịch bản phát hiện bất thường

UEBA cho phép quản lý tập kịch bản phát hiện bất thường bao gồm các thao tác sau:

a) Thêm kịch bản mới;

b) Sửa thông tin kịch bản;

c) Tìm kiếm kịch bản;

d) Xóa kịch bản;

đ) Kích hoạt/vô hiệu hóa kịch bản;

e) Cập nhật tập kịch bản được phát hành bởi nhà sản xuất.

2.8. Quản lý đối tượng người dùng và thực thể được giám sát

UEBA cho phép quản lý đối tượng người dùng và thực thể được giám sát (bao gồm việc tùy chỉnh ngưỡng cảnh báo rủi ro cho từng loại đối tượng).

2.3. Quản lý báo cáo

UEBA 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.

2.4. Chia sẻ dữ liệu

UEBA cho phép kết nối với các loại hệ thống, giải pháp sau để chia sẻ dữ liệu:

a) Giải pháp Quản lý và phân tích sự kiện an toàn thông tin SIEM;

b) Giải pháp Điều phối, tự động hóa và phản ứng an toàn thông tin SOAR;

c) Giải pháp Nền tảng tri thức mối đe dọa an toàn thông tin TIP.

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp UEBA phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), UEBA 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 nguồn gửi dữ liệu;

đ) Cấu hình tập đích nhận cảnh báo;

e) Cấu hình tập hành vi được giám sát;

g) Cấu hình tập kịch bản phát hiện bất thường.

3.2. Bảo vệ dữ liệu nhật ký

Trong trường hợp UEBA phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), UEBA đảm bảo dữ liệu nhật ký 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 UEBA phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), UEBA 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) UEBA 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 nguồn gửi dữ liệu, cấu hình tập đích nhận cảnh báo, cấu hình tập hành vi được giám sát, cấu hình tập kịch bản phát hiện bất thường;

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

v. Thay đổi thủ công thời gian hệ thống.

b) UEBA 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: 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

UEBA cho phép ghi log cảnh báo được sinh ra bởi việc thực thi tập kịch bản phát hiện bất thường.

4.3. Định dạng log

UEBA cho phép chuẩn hóa log theo tối thiểu 01 định dạng 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

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

a) 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);

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

5. Yêu cầu về hiệu năng xử lý

UEBA 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. Đối với xử lý đồng thời nhiều sự kiện

UEBA cho phép xử lý và lưu trữ dữ liệu đồng thời tối thiểu 10000 sự kiện trong khoảng thời gian là 01 giây.

5.2. Đối với mô hình hóa hành vi

UEBA cho phép phân tích và lưu trữ các mô hình hành vi của ít nhất 10000 đối tượng trong hệ thống được giám sát trong khoảng thời gian tối thiểu 30 ngày.

5.3. Đối với phát hiện bất thường

UEBA tích hợp sẵn ít nhất 500 kịch bản phát hiện bất thường áp dụng trên tập dữ liệu gửi từ các nguồn được mô tả tại mục 7.1.

5.4. Đối với độ phủ các nguy cơ mất an toàn thông tin

UEBA tích hợp các kịch bản phát hiện bất thường đảm bảo các yêu cầu sau:

a) Phủ được tối thiểu 25% các kĩ thuật tấn công được mô tả trong ma trận MITRE ATT&CK (tham khảo tại https://attack.mitre.org/);

b) Phủ được tối thiểu 07 pha tấn công được mô tả trong ma trận MITRE ATT&CK bao gồm:

i. Khởi tạo (Initial Access);

ii. Thực thi (Execution);

iii. Truy cập thông tin xác thực (Credential Access);

iv. Khám phá (Discovery);

v. Thu thập (Collection);

vi. Điều khiển và kiểm soát (Command and Control);

vii. Đánh cắp dữ liệu (Exfiltration).

6. Yêu cầu về chức năng tự bảo vệ

6.1. Phát hiện và ngăn chặn tấn công hệ thống

UEBA 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

UEBA cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật của hệ thống mà đã được công bố.

7. Yêu cầu về chức năng giám sát, phân tích sự kiện và đánh giá mức độ rủi ro an toàn thông tin

7.1. Giám sát an toàn thông tin đối với nhiều nguồn khác nhau

UEBA cho phép giám sát và mô hình hóa hành vi của các đối tượng trong hệ thống được giám sát tối thiểu dựa trên 04 loại nguồn gửi dữ liệu khác nhau bao gồm:

a) Nguồn gửi sự kiện an toàn thông tin lớp đầu cuối;

b) Nguồn gửi sự kiện an toàn thông tin lớp mạng;

c) Nguồn gửi sự kiện an toàn thông tin của các giải pháp xác thực và quản lý tài khoản;

d) Nguồn gửi sự kiện an toàn thông tin lớp ứng dụng web và email.

7.2. Phân tích sự kiện theo thời gian thực

UEBA cho phép phân tích sự kiện theo thời gian thực đối với dữ liệu nhật ký thu thập được từ các nguồn gửi dữ liệu, dựa trên tập kịch bản phát hiện bất thường đã được định nghĩa và thiết lập.

7.3. Phân tích sự kiện có sử dụng thông tin hành vi đã được mô hình hóa

UEBA cho phép sử dụng thông tin hành vi của các đối tượng đã được mô hình hóa cho các quá trình phân tích, xử lý dữ liệu đầu vào từ các nguồn gửi dữ liệu (ví dụ: xây dựng kịch bản để phát hiện địa chỉ IP mới được truy cập bởi người dùng mà địa chỉ IP này chưa từng xuất hiện trong lịch sử truy cập của người dùng, trước đó UEBA đã mô hình hóa được tập địa chỉ IP mà người dùng sử dụng để truy cập).

7.4. Đánh giá mức độ rủi ro của các đối tượng được giám sát

UEBA cho phép phân tích và đánh giá mức độ rủi ro của các đối tượng trong hệ thống được giám sát dựa trên các dấu hiệu bất thường đã ghi nhận được.

8. Yêu cầu về chức năng cảnh báo

8.1. Cảnh báo theo thời gian thực

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

a) 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 tập kịch bản phát hiện bất

thường;

b) Cảnh báo về các đối tượng trong hệ thống được giám sát có điểm rủi ro vượt ngưỡng đã được thiết lập.

8.2. Cảnh báo theo nhiều phương thức

UEBA 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) Gửi nội dung cảnh báo qua phương thức thư điện tử hoặc tin nhắn SMS.