BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 1907/QĐ-BTTTT	*Hà nội, ngày 02 tháng 12 năm 2021*

QUYẾT ĐỊNH

Ban hành Yêu cầu kỹ thuật cơ bản đối với sản phẩm Điều phối, tự động hóa và phản ứng 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 Danh mục Yêu cầu kỹ thuật cơ bản đối với sản phẩm Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR - Security Orchestration, Automation and Response).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm SOAR 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, kiểm tra, đánh giá việc áp dụng các yêu cầu trong Danh mục Yêu cầu kỹ thuật cơ bản đối với sản phẩm SOAR 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

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM ĐIỀU PHỐI, TỰ ĐỘNG HÓA VÀ PHẢN ỨNG AN TOÀN THÔNG TIN

(Ban hành 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 kiểm tra, đánh giá sản phẩm Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR - Security Orchestration, Automation and Response), 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 điều phối xử lý và giám sát, Yêu cầu về chức năng tích hợp và tự động hóa.

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 SOAR 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. 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.

3.2. Nền tảng tích hợp (integrated platform)

Sản phẩm phần mềm, hệ thống an toàn thông tin, công nghệ thông tin được kết nối và tương tác thông qua thành phần tích hợp của SOAR.

3.3. Thành phần tích hợp (integration module)

Thành phần được thiết kế, phát triển trên SOAR cho phép kết nối và tương tác với các nền tảng tích hợp.

3.4. 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).

3.5. Cảnh báo (alert)

Sự kiện an toàn thông tin được thu thập từ các nền tảng tích hợp.

3.6. Tình huống (case)

Tập các quy tắc được định nghĩa bởi người dùng, cho phép thiết lập các nhóm cảnh báo theo một tình huống (nghi ngờ sự cố tấn công mạng) cụ thể cần xử lý.

3.7. Mở/Đóng tình huống (open/close case)

Thiết lập trạng thái tình huống cho phép/không cho phép người dùng thực hiện xử lý các cảnh báo của tình huống đó.

3.8. Kịch bản (playbook)

Tập các hành động được định nghĩa bởi người dùng, cho phép SOAR tự động thực hiện xử lý cảnh báo và/hoặc tình huống.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

SOAR 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

SOAR 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 thu thập cảnh báo, cấu hình kịch bản, cấu hình thành phần tích hợp;

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

SOAR 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

SOAR 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 báo cáo

SOAR 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 cảnh báo, sự kiện 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;

e) Cho phép đặt lịch gửi báo cáo định kỳ tới email được cấu hình;

g) Cho phép tạo báo cáo hiệu năng hoạt động của SOAR thông qua tối thiểu 02 thông số sau: thời gian trung bình để xác nhận một sự cố an toàn thông tin, thời gian trung bình để xử lý một sự cố an toàn thông tin kể từ lúc xác nhận;

h) Cho phép tạo báo cáo hiệu quả công việc của từng người tham gia xử lý cảnh báo thông qua tối thiểu 02 thông số sau: số lượng cảnh báo được xử lý trên mỗi người, số lượng cảnh báo được xử lý đúng hạn trên mỗi người.

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR 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 thu thập cảnh báo;

đ) Cấu hình kịch bản;

e) Cấu hình thành phần tích hợp.

3.2. Bảo vệ dữ liệu log, cảnh báo, tình huống và bằng chứng

Trong trường hợp SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR đảm bảo dữ liệu log, cảnh báo, tình huống và bằng chứng 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 SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR 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) SOAR 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 thu

thập cảnh báo, cấu hình kịch bản;

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

v) Thay đổi thủ công thời gian hệ thống;

b) SOAR cho phép ghi log quản trị hệ thống bao gồm 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. Định dạng log

SOAR 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.

4.3. Quản lý log

SOAR 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 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.

5. Yêu cầu về hiệu năng xử lý

SOAR 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

SOAR đảm bảo rằng độ trễ thời gian tìm kiếm log, cảnh báo và tình huống với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 01 phút.

5.2. Thu thập đồng thời nhiều cảnh báo

SOAR cho phép thu thập, xử lý và lưu trữ dữ liệu đồng thời 100 cảnh báo trong khoảng thời gian là 01 phút.

6. Yêu cầu về chức năng điều phối xử lý và giám sát

6.1. Điều phối xử lý cảnh báo

SOAR cho phép điều phối xử lý cảnh báo đáp ứng các yêu cầu sau:

a) Cho phép thiết lập cấu hình thu thập cảnh báo từ các giải pháp an toàn thông tin, công nghệ thông tin khác (ban đầu các cảnh báo được gán trạng thái là mới);

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

c) Cho phép lưu trữ và phân nhóm cảnh báo theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng của cảnh báo, nguồn gửi cảnh báo,…);

d) Cho phép thực hiện xử lý cảnh báo, trong đó bao gồm tối thiểu các thao tác xử lý sau: cập nhật trạng thái xử lý, cập nhật bằng chứng thu thập được, cập nhật kết quả xử lý;

đ) Cho phép cập nhật trạng thái xử lý cảnh báo, trong đó bao gồm tối thiểu các giá trị trạng thái xử lý sau: mới, đang xử lý, đã xử lý;

e) Cho phép cập nhật kết quả xử lý cảnh báo, trong đó bao gồm tối thiểu các giá trị kết quả xử lý sau: cảnh báo thật, cảnh báo giả;

g) Cho phép cập nhật bằng chứng thu thập được, trong đó bao gồm tối thiểu các thao tác sau: tải lên tệp tin bằng chứng, nhập nội dung text;

h) Cho phép xem lại lịch sử xử lý cảnh báo, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm thực hiện, người thực hiện, nội dung thực hiện;

i) Cho phép thiết lập thời hạn xử lý cảnh báo;

k) Cho phép xác định thời gian xử lý cảnh báo có bị quá hạn hay không;

l) Cho phép áp dụng thực hiện một kịch bản với cảnh báo.

6.2. Điều phối xử lý tình huống

SOAR cho phép điều phối xử lý tình huống đáp ứng các yêu cầu sau:

a) Cho phép tạo một tình huống bằng việc nhóm một hoặc nhiều cảnh báo thành tình huống đó (ban đầu các tình huống được gán trạng thái là mở);

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

c) Cho phép lưu trữ và phân nhóm tình huống theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng của tình huống, nguồn tạo tình huống,…);

d) Cho phép thực hiện xử lý tình huống, trong đó bao gồm tối thiểu các thao tác xử lý sau: cập nhật trạng thái xử lý, cập nhật kết quả xử lý;

đ) Cho phép cập nhật trạng thái xử lý tình huống, trong đó bao gồm tối thiểu các giá trị trạng thái xử lý sau: mở, đóng;

e) Cho phép cập nhật kết quả xử lý tình huống, trong đó bao gồm tối thiểu các giá trị kết quả xử lý sau: phát hiện đúng, phát hiện sai;

g) Cho phép xem lại lịch sử xử lý tình huống, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm thực hiện, người thực hiện, nội dung thực hiện;

h) Cho phép thiết lập thời hạn xử lý tình huống;

i) Cho phép xác định thời gian xử lý tình huống có bị quá hạn hay không;

k) Cho phép áp dụng thực hiện một kịch bản với tình huống;

l) Cho phép gán một hoặc nhiều người xử lý cho tình huống.

6.3. Giám sát và phân tích sự cố an toàn thông tin

SOAR cho phép giám sát và phân tích sự cố an toàn thông tin thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép hiển thị thông tin trực quan thể hiện mối liên kết giữa các đối tượng liên quan trong sự cố bằng đường đi và kèm thông tin của liên kết (nếu có), trong đó bao gồm tối thiểu các đối tượng sau: địa chỉ IP, địa chỉ email, tên miền;

b) Cho phép xem dòng thời gian của các sự kiện trong sự cố, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm xuất hiện, nội dung, các đối tượng có liên quan (nếu có), các bằng chứng thu thập được (nếu có);

7. Yêu cầu về chức năng tích hợp và tự động hóa

7.1. Quản lý thành phần tích hợp

SOAR cho phép quản lý cấu hình thành phần tích hợp thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại, cập nhật và xóa thành phần tích hợp đã được tạo;

b) Cho phép phát triển thành phần tích hợp thông qua tối thiểu 01 ngôn ngữ lập trình dạng thông dịch (ví dụ: Python, Javascript,…).

7.2. Hỗ trợ tích hợp nhiều nền tảng khác nhau

SOAR cho phép kết nối và tương tác với các nền tảng khác nhau, trong đó tối thiểu bao gồm:

a) Security Information and Event Management (SIEM) - Quản lý và phân tích sự kiện an toàn thông tin;

b) Threat Intelligence Platform (TIP) - Nền tảng tri thức mối đe dọa an toàn thông tin;

c) Endpoint Security - Đảm bảo an toàn thông tin cho thiết bị đầu cuối (ví dụ: Endpoint Detection and Response (EDR) - Phát hiện và ứng phó các mối đe dọa an toàn thông tin tại thiết bị đầu cuối; Endpoint Protection Platform (EPP) - Nền tảng bảo vệ thiết bị đầu cuối;…);

d) Network Security - Đảm bảo an toàn thông tin mạng (ví dụ: Network-based Intrusion Prevention System (NIPS) - Phòng, chống xâm nhập lớp mạng; Web Application Firewall (WAF) - Tường lửa ứng dụng web;…);

đ) Malware Analysis - Phân tích mã độc;

e) Ticketing System - Quản lý các yêu cầu cần giải quyết;

g) Identity and Access Management (IAM) - Quản lý định danh và truy cập.

7.3. Hỗ trợ tích hợp nhiều API

SOAR cho phép thiết lập cấu hình một hoặc nhiều API trên các thành phần tích hợp để ứng dụng nhiều nhất có thể các chức năng, tính năng mà nền tảng tích hợp cung cấp.

7.4. Hỗ trợ tích hợp API theo hai chiều

SOAR cho phép thiết lập cấu hình API trên các thành phần tích hợp để tương tác hai chiều với các nền tảng tích hợp:

a) Cho phép truy vấn dữ liệu từ nền tảng tích hợp để làm giàu thông tin cho các dữ liệu được xử lý và lưu trữ trên SOAR;

b) Cho phép thực thi lệnh tác động đến nền tảng tích hợp để thực hiện việc ứng phó sự kiện, cố an toàn thông tin.

7.5. Quản lý kịch bản

SOAR cho phép quản lý cấu hình kịch bản thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại, cập nhật và xóa kịch bản đã được tạo;

b) Cho phép xây dựng kịch bản với tối thiểu các thành phần sau: khối thực thi, đường đi giữa các khối, điều kiện rẽ nhánh;

c) Cho phép xây dựng kịch bản thông qua tối thiểu các thao tác sau để tương tác với loại thành phần trên: tạo mới, xem lại, cập nhật, xóa;

d) Cho phép xuất một kịch bản ra tệp tin và tải về tệp tin đã xuất;

đ) Cho phép tải lên tệp tin chứa một kịch bản và nhập kịch bản từ tệp tin đó;

e) Cho phép đưa một kịch bản đã được xây dựng trước đó vào một kịch bản.

7.6. Hỗ trợ thực hiện kịch bản tự động

SOAR cho phép thực hiện kịch bản tự động đáp ứng các yêu cầu sau:

a) Cho phép cấu hình kịch bản dựa theo các điều kiện, quy tắc tìm kiếm cảnh báo, tình huống để thực hiện tất cả các bước trong kịch bản mà không cần con người tương tác;

b) Cho phép thiết lập thời hạn thực hiện kịch bản;

c) Cho phép xác định thời gian thực hiện kịch bản có bị quá hạn hay không;

d) Cho phép xem lại lịch sử thực hiện của từng bước trong kịch bản, trong đó bao gồm tối thiểu các trường thông tin sau: tập dữ liệu đầu vào, tập dữ liệu đầu ra, thời điểm bắt đầu thực hiện, thời điểm kết thúc thực hiện, trạng thái thực hiện (thành công hoặc thất bại).

7.7. Hỗ trợ thực hiện kịch bản bán tự động

SOAR cho phép thực hiện kịch bản bán tự động đáp ứng các yêu cầu sau:

a) Cho phép thực hiện kịch bản dựa vào dữ liệu người dùng đưa vào, thông qua một hoặc một số các thao tác sau: nhập giá trị (số hoặc chuỗi ký tự), chọn một hoặc một số trong các giá trị có sẵn, tải lên tệp tin, thiết lập thời điểm bắt đầu tự động thực hiện, thiết lập thời hạn thực hiện;

b) Cho phép thiết lập thời hạn thực hiện kịch bản;

c) Cho phép xác định thời gian thực hiện kịch bản và từng bước trong kịch bản có bị quá hạn hay không;

d) Cho phép xem lại lịch sử thực hiện của từng bước trong kịch bản, trong đó bao gồm tối thiểu các trường thông tin sau: tập dữ liệu đầu vào, tập dữ liệu đầu ra, thời điểm bắt đầu thực hiện, thời điểm kết thúc thực hiện, trạng thái thực hiện (thành công hoặc thất bại), tài khoản người dùng có tương tác;

đ) Cho phép sử dụng kết quả thực hiện của bước trước đó làm dữ liệu đầu vào cho bước tiếp theo trong kịch bản;

e) Cho phép gán một hoặc nhiều người tương tác cho những bước trong kịch bản cần con người tương tác.