TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXXXX:2026

Xuất bản lần 1

AN NINH MẠNG - SẢN PHẨM ĐIỀU PHỐI, TỰ ĐỘNG HOÁ VÀ PHẢN ỨNG AN NINH MẠNG - YÊU CẦU CHUNG

Cybersecurity -

Cybersecurity orchestration, automation and response platform

- General requirements

HÀ NỘI - 2026

Mục lục

Lời nói đầu

TCVN XXXXX:2026 An ninh mạng - Sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng - Yêu cầu chung do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Bộ Công an đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn quy định các yêu cầu chung đối với sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng (SOAR - Security Orchestration, Automation and Response). Đây là cơ sở để các tổ chức doanh nghiệp phát triển, cung cấp, đánh giá và lựa chọn sử dụng sản phẩm, dịch vụ SOAR.

Để hiệu quả đảm bảo an ninh mạng ở mức cao nhất, khuyến khích chủ quản của sản phẩm dịch vụ an ninh mạng SOAR triển khai các yêu cầu được đưa ra trong tiêu chuẩn.

An ninh mạng - Sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng - Yêu cầu chung

Cybersecurity - Cybersecurity Orchestration, Automation And Response Platform - General Requirements

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu chung về an ninh mạng đối với nền tảng tự động hoá, điều phối và phản ứng an ninh mạng (SOAR - Security Orchestration, Automation and Response).

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

3 Thuật ngữ, định nghĩa và chữ viết tắt

Tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa và chữ viết tắt dưới đây.

3.1 Thuật ngữ và định nghĩa

3.1.1

An ninh mạng (cyber security)

Sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3.1.2

Thời gian duy trì phiên kết nối (session timeout)

Khoảng thời gian được thiết lập để cho phép hệ thống huỷ 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.

3.1.3

Nhật ký hệ thống (log)

Tập hợp các bản ghi được hệ thống, ứng dụng hoặc thiết bị tạo ra để ghi nhận các sự kiện, hoạt động hoặc thay đổi trạng thái xảy ra trong quá trình vận hành. Log được sử dụng để phục vụ giám sát, phân tích, truy vết và điều tra sự cố an ninh, lỗi hệ thống hoặc hành vi người dùng.

3.1.4

Cảnh báo (alert)

Bản ghi hoặc thông báo được hệ thống an ninh tạo ra khi phát hiện dấu hiệu bất thường, hành vi nghi vấn hoặc sự kiện có khả năng liên quan đến an ninh mạng cần được kiểm tra và xử lý.

3.1.5

Tình huống (case)

Tập hợp một hoặc nhiều cảnh báo có liên quan được nhóm lại để phục vụ việc phân tích, điều tra và xử lý như một sự kiện an ninh mạng thống nhất.

3.1.6

Thành phần tích hợp (integration component)

Thành phần phần mềm hoặc cấu hình cho phép SOAR kết nối, trao đổi dữ liệu và thực thi chức năng với các hệ thống hoặc nền tảng bên ngoài thông qua giao thức hoặc API.

3.1.7

Sự cố an ninh mạng (security incident)

Sự kiện xảy ra trong hệ thống thông tin hoặc trên không gian mạng gây ảnh hưởng hoặc có khả năng gây ảnh hưởng đến tính bảo mật, toàn vẹn hoặc tính sẵn sàng của hệ thống, dữ liệu hoặc dịch vụ.

3.1.8

Nền tảng tích hợp (integrated platform)

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

3.1.9

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.

3.1.10

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.

3.1.11

Sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng (Security Orchestration, Automation and Response**)**

Nền tảng cho phép tích hợp các giải pháp an ninh mạng, công nghệ thông tin; điều phối và tự động hoá toàn phần hoặc một phần các quy trình tiếp nhận, phân tích, xử lý cảnh báo và sự cố an ninh mạng; hỗ trợ phối hợp giữa những người tham gia xử lý.

3.1.12

Phân loại và xử lý ban đầu (triage)

Hoạt động xem xét, xác định mức độ nghiêm trọng, mức độ ưu tiên và hướng xử lý tiếp theo đối với cảnh báo ngay khi tiếp nhận.

3.1.13

Làm giàu dữ liệu (enrichment)

Hoạt động bổ sung thông tin bối cảnh cho cảnh báo, tình huống từ các nguồn dữ liệu bên trong hoặc bên ngoài nhằm hỗ trợ phân tích và ra quyết định.

3.1.14

Dấu hiệu tấn công (indicator of compromise, IOC)

Dữ liệu kỹ thuật có thể quan sát được, được sử dụng để nhận biết hoạt động tấn công mạng hoặc dấu vết xâm nhập (ví dụ: địa chỉ IP, tên miền, URL, giá trị băm tệp tin, địa chỉ thư điện tử).

3.1.15

Leo thang (escalation)

Việc chuyển cảnh báo hoặc tình huống lên mức xử lý cao hơn khi vượt quá thẩm quyền, năng lực xử lý hoặc thời hạn xử lý đã thiết lập.

3.1.16

Chuỗi hành trình bằng chứng (chain of custody)

Bản ghi liên tục, theo trình tự thời gian về việc tiếp nhận, lưu giữ, truy cập, chuyển giao và tiêu huỷ bằng chứng, nhằm bảo đảm tính toàn vẹn và khả năng truy nguyên của bằng chứng.

3.1.17

Nhật ký kiểm toán (audit log)

Bản ghi các hành vi có ảnh hưởng đến an toàn, cấu hình hoặc dữ liệu của hệ thống, được lưu giữ nhằm phục vụ việc truy vết, thanh tra và kiểm tra tuân thủ.

3.1.18

Khử trùng lặp (deduplication)

Việc nhận biết và gộp các cảnh báo có cùng bản chất phát sinh nhiều lần thành một cảnh báo duy nhất kèm số lần xuất hiện.

3.2 Chữ viết tắt

SOAR	Sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng	Security Orchestration, Automation and Response
EDR	Phát hiện và ứng phó các mối đe dọa an ninh mạng tại thiết bị đầu cuối	Endpoint Detection and Response
SIEM	Nền tảng quản lý, phân tích sự kiện và thông tin an ninh mạng	Security Information and Event Management
TIP	Nền tảng quản lý thông tin tình báo an ninh mạng	Threat Intelligence Platform
EPP	Nền tảng bảo vệ thiết bị đầu cuối	Endpoint Protection Platform

NIPS	Phòng, chống xâm nhập lớp mạng	Network-based Intrusion Prevention System
WAF	Tường lửa ứng dụng web	Web Application Firewall
IAM	Quản lý định danh và truy cập	Identity and Access Management
TLS	Bảo mật tầng truyền tải	Transport Layer Security
MTTA	Thời gian trung bình để ghi nhận/xác nhận cảnh báo	Mean Time To Acknowledge
MTTD	Thời gian trung bình để phát hiện sự cố an ninh	Mean Time To Detect
MTTR	Thời gian trung bình để xử lý/khắc phục sự cố	Mean Time To Respond
MTBF	Thời gian trung bình giữa các sự cố	Mean Time Between Failures
SLA	Thỏa thuận mức dịch vụ	Service Level Agreement
API	Giao diện lập trình ứng dụng	Application Programming Interface
MFA	Xác thực đa yếu tố	Multi-Factor Authentication
IP	Địa chỉ giao thức Internet	Internet Protocol
IDPS	Hệ thống phát hiện và ngăn chặn xâm nhập	Intrusion Detection Prevention System
SaaS	Phần mềm dưới dạng dịch vụ	Software as a Service
IOC	Dấu hiệu tấn công	Indicator of Compromise
RBAC	Kiểm soát truy cập dựa trên vai trò	Role-Based Access Control
SSO	Đăng nhập một lần	Single Sign-On
NTP	Giao thức đồng bộ thời gian mạng	Network Time Protocol
UTC	Giờ phối hợp quốc tế	Coordinated Universal Time
CMDB	Cơ sở dữ liệu quản lý cấu hình	Configuration Management Database
RTO	Mục tiêu thời gian khôi phục	Recovery Time Objective
RPO	Mục tiêu điểm khôi phục	Recovery Point Objective
SBOM	Danh mục thành phần phần mềm	Software Bill of Materials
DFIR	Điều tra số và ứng cứu sự cố	Digital Forensics and Incident Response
CTI	Thông tin tình báo về mối đe doạ mạng	Cyber Threat Intelligence

4 Yêu cầu chung, quản trị và an toàn đối với sản phẩm

4.1 Yêu cầu về tài liệu

SOAR phải được cung cấp kèm theo các tài liệu hướng dẫn sau:

a) Tài liệu hướng dẫn chi tiết các bước cài đặt triển khai và thiết lập cấu hình.

b) Tài liệu hướng dẫn mô tả chi tiết cách sử dụng tính năng trên sản phẩm.

c) Tài liệu mô tả những thay đổi, cập nhật hoặc cải tiến trong phiên bản phần mềm mới (nếu có).

d) Tài liệu hướng dẫn quản trị hệ thống.

e) Tài liệu hướng dẫn sao lưu dữ liệu sản phẩm, khôi phục khi xảy ra sự cố.

f) Tài liệu mô tả kiến trúc và yêu cầu hạ tầng tối thiểu tương ứng với từng mức tải.

g) Tài liệu mô tả giao diện lập trình ứng dụng của sản phẩm.

h) Tài liệu hướng dẫn phát triển thành phần tích hợp và kịch bản.

i) Tài liệu hướng dẫn cấu hình tăng cường an toàn (hardening).

k) Ma trận tương thích phiên bản giữa sản phẩm và các nền tảng tích hợp.

l) Chính sách hỗ trợ và thời hạn kết thúc hỗ trợ của từng phiên bản.

4.2 Yêu cầu về quản trị hệ thống

4.2.1 Quản lý vận hành

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

a) Cho phép thiết lập, thay đổi, 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 đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực.

e) Cho phép tìm kiếm dữ liệu log bằng từ khoá để xem lại.

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

g) Có khả năng triển khai tại chỗ hoặc dưới dạng giải pháp đám mây.

4.2.2 Quản trị từ xa

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

a) Phải sử dụng giao thức Transport Layer Security (TLS) phiên bản 1.2 trở lên với bộ thuật toán mã hoá không thuộc danh mục đã được khuyến cáo ngừng sử dụng; phải cho phép người quản trị vô hiệu hoá các phiên bản giao thức và bộ thuật toán mã hoá cũ không còn được khuyến nghị sử dụng.

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.

c) 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,...).

4.2.3 Quản lý xác thực và phân quyền

SOAR phải 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) Phải cung cấp sẵn tối thiểu 02 vai trò mặc định khi cài đặt là quản trị viên và người dùng thường, với quyền hạn cụ thể đối với từng vai trò, độc lập với năng lực định nghĩa vai trò tuỳ biến quy định tại điểm k).

c) Hỗ trợ kiểm soát truy cập dựa trên vai trò (RBAC) cho các chức năng hỗ trợ nhiều người dùng hơn sử dụng công cụ trong các sự cố.

d) Hỗ trợ xác thực đa nhân tố (MFA) đối với tất cả các tài khoản.

e) Phải hỗ trợ tích hợp với hệ thống quản lý định danh tập trung thông qua tối thiểu 01 giao thức xác thực liên kết được thừa nhận rộng rãi, cho phép đồng bộ tài khoản và thu hồi quyền truy cập tự động.

f) Phải cho phép thiết lập chính sách mật khẩu, tối thiểu bao gồm: độ dài tối thiểu, yêu cầu về thành phần ký tự, thời hạn sử dụng, số lượng mật khẩu không được sử dụng lại.

g) Phải bắt buộc thay đổi mật khẩu mặc định của tài khoản quản trị trong lần đăng nhập đầu tiên; không được tồn tại tài khoản có mật khẩu mặc định sau khi hoàn tất cài đặt.

h) Phải tự động khoá tài khoản sau số lần xác thực thất bại liên tiếp vượt ngưỡng được thiết lập.

i) Phải lưu trữ mật khẩu ở dạng giá trị băm có sử dụng chuỗi ngẫu nhiên bổ sung.

k) Phải cho phép định nghĩa vai trò tuỳ biến với quyền hạn chi tiết đến từng chức năng và từng loại hành động.

l) Phải cho phép kiểm soát truy cập ở mức đối tượng, cho phép giới hạn phạm vi dữ liệu (cảnh báo, tình huống, kịch bản) mà một vai trò được truy cập.

m) Phải cho phép xuất danh sách tài khoản, vai trò và quyền hạn phục vụ rà soát định kỳ; cho phép xác định các tài khoản không hoạt động trong khoảng thời gian được thiết lập.

4.2.4 Quản lý báo cáo

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

a) Cho phép cung cấp bảng điều khiển trực quan (Dashboard) theo thời gian thực hỗ trợ tổng hợp dữ liệu đo lường an ninh giám sát toàn diện hệ thống.

b) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo.

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 01 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML.

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

f) 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 ninh mạng, thời gian trung bình để xử lý một sự cố an ninh mạng 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.

i) Cho phép tạo báo cáo giám sát bao gồm: MTBF, MTTA, MTTD, MTTR, SLA.

4.2.5 Quản lý thông tin xác thực của thành phần tích hợp

SOAR phải cung cấp chức năng quản lý thông tin xác thực của thành phần tích hợp đáp ứng các yêu cầu sau:

a) SOAR phải lưu trữ thông tin xác thực của thành phần tích hợp ở dạng đã được mã hoá, sử dụng thuật toán mã hoá chưa được công bố điểm yếu.

b) SOAR không được hiển thị thông tin xác thực ở dạng rõ trên giao diện người dùng, trong nhật ký hệ thống, trong dữ liệu đầu vào/đầu ra của kịch bản và trong tệp tin xuất kịch bản.

c) SOAR phải cho phép phân quyền riêng đối với chức năng xem, tạo, sửa đổi thông tin xác thực, tách biệt với quyền sử dụng thành phần tích hợp.

d) SOAR phải cho phép thay đổi thông tin xác thực mà không phải sửa đổi kịch bản đang sử dụng thông tin xác thực đó.

e) SOAR nên hỗ trợ tích hợp với hệ thống quản lý bí mật tập trung bên ngoài.

f) SOAR phải ghi nhật ký mọi hành vi truy cập, tạo, sửa đổi, xoá thông tin xác thực.

4.3 Yêu cầu về kiểm soát lỗi

4.3.1 Bảo vệ cấu hình

Trong trường hợp SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR phải bảo đảm 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.

e) Cấu hình kịch bản.

f) Cấu hình thành phần tích hợp.

4.3.2 Bảo vệ dữ liệu nhật ký, 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 phải bảo đảm 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.

4.3.3 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 phải bảo đảm thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

4.4 Yêu cầu về nhật ký hệ thống (log)

Trong tiêu chuẩn này, nhật ký kiểm toán quy định tại 3.1.17 là nhật ký kiểm toán quy định tại 3.1.17 là nhật ký hệ thống ghi nhận các sự kiện quy định tại 4.4.1 a). Yêu cầu quản lý log tại 4.4.3 áp dụng chung cho mọi loại nhật ký hệ thống, bao gồm cả nhật ký kiểm toán; yêu cầu bảo vệ tại 4.4.4 áp dụng riêng cho nhật ký kiểm toán và có hiệu lực cao hơn 4.4.3 trong trường hợp có xung đột. Cụ thể, cấu hình lưu trữ và huỷ bỏ log theo 4.4.3 a) không được phép rút ngắn thời hạn lưu trữ nhật ký kiểm toán đã thiết lập theo 4.4.4 d).

4.4.1 Log quản trị hệ thống

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

- Đăng nhập, đăng xuất tài khoản;

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

- 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;

- Kích hoạt lệnh khởi động lại, tắt hệ thống;

- Thay đổi thủ công thời gian hệ thống;

- Tạo lập, sửa đổi, xoá, phê duyệt, ban hành, ngừng sử dụng kịch bản và thành phần tích hợp;

- Thực thi hành động tác động đến nền tảng tích hợp, kèm tham số hành động và đối tượng bị tác động;

- Truy cập, tải xuống, sửa đổi, tiêu huỷ bằng chứng;

- Thay đổi vai trò, quyền hạn của tài khoản người dùng;

- Phê duyệt hoặc từ chối phê duyệt;

- Xuất dữ liệu ra khỏi hệ thống;

- Truy cập, tạo lập, sửa đổi thông tin xác thực của thành phần tích hợp;

- Truy cập tình huống có chế độ hạn chế truy cập.

b) SOAR cho phép ghi log quản trị hệ thống bao gồm các trường thông tin sau:

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

- Địa chỉ IP hoặc định danh của máy trạm;

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

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

- Kết quả thực hiện hành vi (thành công hoặc thất bại);

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

4.4.2 Định dạng log

SOAR phải 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.

4.4.3 Quản lý log

SOAR phải 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 huỷ 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.

d) Có khả năng lưu trữ (tại chỗ hoặc trên hệ thống thứ ba) log để hỗ trợ các cuộc điều tra an ninh mạng.

4.4.4 Bảo vệ nhật ký kiểm toán

SOAR phải bảo vệ nhật ký kiểm toán đáp ứng các yêu cầu sau:

a) SOAR phải bảo đảm bản ghi nhật ký kiểm toán không bị sửa đổi hoặc xoá bởi bất kỳ vai trò người dùng nào, kể cả vai trò quản trị hệ thống, trong thời hạn lưu trữ được thiết lập.

b) SOAR phải có cơ chế phát hiện việc sửa đổi trái phép đối với nhật ký kiểm toán.

c) SOAR phải cho phép chuyển tiếp nhật ký kiểm toán tới hệ thống lưu trữ độc lập theo thời gian thực hoặc gần thời gian thực.

d) SOAR phải cho phép thiết lập thời hạn lưu trữ nhật ký kiểm toán đáp ứng quy định của pháp luật và không cho phép xoá trước thời hạn.

4.5 Yêu cầu về tính sẵn sàng

4.5.1 Kiến trúc dự phòng

SOAR phải đáp ứng các yêu cầu về kiến trúc dự phòng:

a) Cho phép triển khai theo mô hình cụm dự phòng (High Availability - HA) tối thiểu theo cấu trúc Active-Passive hoặc Active-Active.

b) Hỗ trợ cơ chế cân bằng tải nội bộ hoặc cho phép tích hợp với bộ cân bằng tải bên ngoài để phân phối lưu lượng xử lý cảnh báo và luồng thực thi kịch bản.

4.5.2 Cơ chế chuyển đổi dự phòng

SOAR phải cho phép chuyển đổi dự phòng đáp ứng các yêu cầu sau:

a) Đảm bảo quá trình chuyển đổi không làm mất mát dữ liệu nhật ký hệ thống, cảnh báo, tình huống đang được tiếp nhận và không làm thay đổi trạng thái các kịch bản đang thực thi.

b) Cho phép thiết lập ngưỡng thời gian phục hồi hoạt động khi xảy ra sự cố chuyển đổi dự phòng (RTO); ngưỡng này phải được nhà cung cấp công bố và có thể kiểm tra xác nhận bằng thử nghiệm chuyển đổi dự phòng.

4.5.3 Đồng bộ dữ liệu và khôi phục sau sự cố

SOAR phải cho phép đồng bộ dữ liệu và khôi phục sau sự cố đáp ứng các yêu cầu sau:

a) Cung cấp tính năng tự động sao lưu hoặc cho phép tích hợp công cụ tự động sao lưu cấu hình hệ thống, cơ sở dữ liệu, kịch bản xử lý và các thành phần tích hợp định kỳ theo lịch đặt trước.

b) Cung cấp tính năng khôi phục dữ liệu hoặc cho phép tích hợp công cụ khôi phục dữ liệu từ bản sao lưu, có cơ chế kiểm tra tính toàn vẹn của bản sao lưu trước khi khôi phục dữ liệu.

4.6 Yêu cầu về giám sát tình trạng hoạt động

4.6.1 Giám sát thành phần hệ thống

SOAR phải cung cấp giao diện đồ hoạ hiển thị tình trạng hoạt động theo thời gian thực, tối thiểu bao gồm:

a) Trạng thái hoạt động của từng thành phần hệ thống (dịch vụ ứng dụng, cơ sở dữ liệu, thành phần thực thi kịch bản, hàng đợi xử lý).

b) Mức sử dụng tài nguyên: CPU, bộ nhớ, dung lượng lưu trữ, dung lượng cơ sở dữ liệu.

c) Số lượng phần tử đang tồn đọng trong hàng đợi xử lý và độ trễ xử lý trung bình.

d) Số lượng phiên kịch bản đang thực thi, đang chờ và đã thất bại trong khoảng thời gian lựa chọn.

e) Tình trạng của cụm dự phòng (nút chính, nút dự phòng, tình trạng đồng bộ dữ liệu).

f) Thời gian trung bình giữa các lần gián đoạn hoạt động của hệ thống (MTBF), tính theo khoảng thời gian lựa chọn.

4.6.2 Giám sát thành phần tích hợp

SOAR phải cung cấp chức năng giám sát tình trạng từng thành phần tích hợp, tối thiểu bao gồm:

a) Chức năng kiểm tra kết nối (test connection) theo yêu cầu của người dùng đối với từng thành phần tích hợp, trả về kết quả thành công/thất bại kèm thông tin chẩn đoán lỗi.

b) Tự động kiểm tra kết nối theo chu kỳ do người quản trị thiết lập.

c) Hiển thị thời điểm giao tiếp thành công gần nhất, tỷ lệ lỗi và mã lỗi gần nhất của từng thành phần tích hợp.

d) Cảnh báo khi thông tin xác thực của thành phần tích hợp sắp hết hiệu lực hoặc đã hết hiệu lực.

4.6.3 Giám sát luồng thu thập dữ liệu

SOAR phải cung cấp chức năng:

a) Thống kê số lượng cảnh báo tiếp nhận thành công, tiếp nhận thất bại và bị loại bỏ theo từng nguồn, theo đơn vị thời gian.

b) Phát hiện và cảnh báo khi một nguồn cảnh báo không gửi dữ liệu vượt quá ngưỡng thời gian được thiết lập.

4.6.4 Cảnh báo vận hành và xuất dữ liệu giám sát

a) SOAR phải cho phép thiết lập ngưỡng cảnh báo đối với các chỉ số nêu tại 4.6.1, 4.6.2, 4.6.3 và gửi cảnh báo qua tối thiểu 02 kênh (ví dụ: thư điện tử, ứng dụng nhắn tin, syslog).

b) SOAR phải cung cấp giao diện lập trình ứng dụng hoặc điểm truy xuất tiêu chuẩn cho phép hệ thống giám sát bên ngoài thu thập các chỉ số tình trạng hoạt động.

c) SOAR nên cung cấp bảng điều khiển tổng hợp phục vụ kiểm tra tình trạng hằng ngày, cho phép xuất kết quả kiểm tra ra tệp tin.

4.7 Yêu cầu về bảo vệ dữ liệu

SOAR phải bảo vệ dữ liệu đáp ứng các yêu cầu sau:

a) Phải mã hoá dữ liệu khi lưu trữ đối với: thông tin xác thực, bằng chứng, và các trường dữ liệu được đánh dấu là nhạy cảm.

b) Phải sử dụng kênh truyền có mã hoá đối với mọi kết nối giữa các thành phần của hệ thống và giữa SOAR với nền tảng tích hợp; phải cho phép xác thực chứng thư của phía đối tác.

c) Phải cho phép đánh dấu trường dữ liệu chứa dữ liệu cá nhân và che giấu giá trị của các trường này đối với vai trò không được cấp quyền.

d) Phải cho phép thiết lập thời hạn lưu trữ riêng cho từng loại dữ liệu và tự động xoá hoặc ẩn danh dữ liệu khi hết thời hạn.

e) Phải cho phép tìm kiếm, kết xuất và xoá dữ liệu liên quan đến một chủ thể dữ liệu cụ thể.

f) Trường hợp triển khai dưới dạng dịch vụ đám mây, nhà cung cấp phải công bố vị trí lưu trữ và xử lý dữ liệu, các bên thứ ba có khả năng truy cập dữ liệu, và cơ chế bảo đảm tuân thủ quy định của pháp luật Việt Nam về lưu trữ dữ liệu và bảo vệ dữ liệu cá nhân.

4.8 Yêu cầu về an toàn và vòng đời sản phẩm

a) Nhà cung cấp phải công bố danh mục thành phần phần mềm của sản phẩm, bao gồm các thư viện và thành phần nguồn mở kèm phiên bản.

b) Sản phẩm không được sử dụng thành phần đã kết thúc hỗ trợ của nhà phát triển.

c) Nhà cung cấp phải có quy trình tiếp nhận, xử lý và thông báo lỗ hổng bảo mật của sản phẩm; phải công bố thời hạn cam kết xử lý theo mức độ nghiêm trọng.

d) Bản cập nhật, bản vá và gói nội dung của sản phẩm phải có cơ chế xác thực nguồn gốc và kiểm tra tính toàn vẹn trước khi cài đặt.

e) SOAR phải cho phép nâng cấp mà không làm mất dữ liệu và cấu hình, và phải cung cấp cơ chế quay lui về phiên bản trước khi nâng cấp không thành công.

f) Nhà cung cấp phải cung cấp tài liệu hướng dẫn cấu hình tăng cường an toàn cho sản phẩm.

5 Yêu cầu chức năng nghiệp vụ đối với sản phẩm

5.1 Yêu cầu về chức năng điều phối xử lý

5.1.1 Điều phối xử lý cảnh báo

SOAR phải 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 ninh mạng, 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.

e) 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, chờ bổ sung thông tin, đã leo thàng, đã xử lý.

f) 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, hoạt động hợp lệ được xác nhận, trùng lặp.

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.

m) Phải cho phép cấu hình quy tắc khử trùng lặp cảnh báo dựa trên tổ hợp các trường thông tin và khoảng thời gian; các cảnh báo trùng lặp phải được gộp thành một cảnh báo có kèm số lần xuất hiện thay vì tạo cảnh báo mới.

n) Phải cho phép cấu hình quy tắc tự động nhóm các cảnh báo có liên quan thành tình huống dựa trên tổ hợp các trường thông tin và khoảng thời gian.

o) Phải cho phép cấu hình quy tắc loại trừ (danh sách cho phép) để tự động chuyển cảnh báo đã biết là nhiễu sang trạng thái đã xử lý; mỗi quy tắc loại trừ phải có thời hạn hiệu lực, lý do và người phê duyệt.

p) Cảnh báo phải có trường mức độ nghiêm trọng với tối thiểu 04 giá trị; SOAR phải cho phép cấu hình quy tắc tự động xác định hoặc điều chỉnh mức độ nghiêm trọng dựa trên nội dung cảnh báo, mức độ quan trọng của tài sản liên quan và kết quả làm giàu dữ liệu.

q) Phải cho phép gán một hoặc nhiều người xử lý cho cảnh báo; cho phép người dùng tự nhận xử lý cảnh báo chưa được gán.

r) Phải cho phép cấu hình quy tắc tự động phân công cảnh báo theo nhóm, theo ca trực hoặc theo mức độ nghiêm trọng.

s) Phải cho phép hiển thị hàng đợi cảnh báo theo người xử lý, theo nhóm và theo ca trực; cho phép lưu và sử dụng lại bộ điều kiện lọc.

t) Phải hiển thị dữ liệu đã được làm giàu và bối cảnh liên quan ngay trên màn hình xử lý cảnh báo, tối thiểu bao gồm: thông tin tài sản liên quan, thông tin tài khoản người dùng liên quan, kết quả tra cứu dấu hiệu tấn công, các cảnh báo và tình huống trước đó có liên quan đến cùng đối tượng.

u) Phải cho phép người dùng ghi chú trên cảnh báo, gắn thẻ người dùng khác trong ghi chú và nhận thông báo khi được gắn thẻ.

5.1.2 Điều phối xử lý tình huống

SOAR phải 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.

e) 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.

f) 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.

5.1.3 Leo thang và thông báo

SOAR phải hỗ trợ leo thang và thông báo đáp ứng các yêu cầu sau:

a) Phải cho phép cấu hình quy tắc leo thang tự động khi cảnh báo, tình huống quá hạn xử lý hoặc đạt mức độ nghiêm trọng được thiết lập.

b) Phải cho phép cấu hình nhiều mức leo thang với người tiếp nhận tương ứng từng mức.

c) Phải cho phép gửi thông báo tới người dùng qua tối thiểu 02 kênh khi: cảnh báo/tình huống được gán cho người dùng, cảnh báo/tình huống sắp đến hạn hoặc quá hạn, kịch bản cần người dùng tương tác hoặc phê duyệt.

d) Nên cho phép quản lý lịch trực và tự động xác định người tiếp nhận theo ca trực tại thời điểm phát sinh.

5.2 Yêu cầu về chức năng giám sát và phân tích sự cố

SOAR phải cho phép giám sát và phân tích sự cố an ninh mạng 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).

5.3 Yêu cầu về chức năng tích hợp và tự động hóa

5.3.1 Quản lý thành phần tích hợp

SOAR phải 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,…).

c) SOAR phải thực thi mã của thành phần tích hợp trong môi trường cách ly, có giới hạn tài nguyên (thời gian thực thi, bộ nhớ, tiến trình con).

d) SOAR phải cho phép giới hạn phạm vi truy cập mạng và truy cập hệ thống tệp tin của mã thành phần tích hợp.

e) SOAR phải yêu cầu phê duyệt trước khi một thành phần tích hợp do người dùng tự phát triển được sử dụng trong môi trường vận hành, và phải ghi nhật ký kiểm toán đối với việc tạo lập, sửa đổi mã.

5.3.2 Hỗ trợ tích hợp nhiều nền tảng khác nhau

SOAR phải 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 thông tin an ninh mạng.

b) Threat Intelligence Platform (TIP) - Nền tảng quản lý thông tin tình báo an ninh mạng.

c) Endpoint Security - Đảm bảo an ninh mạng cho thiết bị đầu cuối (ví dụ: Endpoint Detection and Response (EDR) - Phát hiện và ứng phó các mối đe dọa an ninh 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 ninh mạng (ví dụ: Network-based Intrusion Prevention System (NIPS) - Phòng, chống xâm nhập lớp mạng; Web Application Firewall (WAF) - Tường lửa ứng dụng web;…).

e) Malware Analysis - Phân tích mã độc.

f) Ticketing System - Quản lý các yêu cầu cần giải quyết.

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

h) Secure Email Gateways (SEG) - Cổng bảo mật email.

i) Intrusion Detection and Prevention System (IDPS) - Hệ thống phát hiện và ngăn chặn xâm nhập.

5.3.3 Hỗ trợ tích hợp API

a) SOAR phải cho phép thiết lập cấu hình một hoặc nhiều API trên các thành phần tích hợp để sử dụng các chức năng, tính năng mà nền tảng tích hợp cung cấp; danh mục chức năng được hỗ trợ phải được công bố theo quy định tại điểm b).

b) Phải công bố danh sách API/connector hỗ trợ, phương thức xác thực, chiều tích hợp, loại dữ liệu trao đổi, hành động được phép thực thi và quyền tối thiểu cần có.

c) 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.

d) Cho phép thực thi lệnh tác động đến nền tảng tích hợp để thực hiện việc ứng phó sự kiện, sự cố an ninh mạng.

e) Tích hợp hai chiều với các giải pháp vận hành công nghệ thông tin (như hệ thống quản lý yêu cầu hỗ trợ) và các công cụ phối hợp (như ứng dụng tin nhắn để cải thiện hiệu quả hoạt động liên lạc kịp thời).

f) Phải kiểm soát phân quyền thực thi theo từng hành động; phải cho phép cấu hình danh sách cho phép về giới hạn phạm vi tác động của hành động đến nền tảng tích hợp; phải hiển thị kết quả thực thi hành động cho người dùng.

5.3.4 Quản lý kịch bản

SOAR phải cho phép quản lý cấu hình kịch bản thông qua giao diện đồ hoạ 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, vòng lặp trên tập dữ liệu, nhánh thực thi song song và điểm hợp lưu, khối yêu cầu người dùng thực hiện thao tác thủ công, khối yêu cầu phê duyệt, biến và biểu thức biến đổi dữ liệu.

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.

e) Cho phép tải lên tệp tin chứa một kịch bản và nhập kịch bản từ tệp tin đó.

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

g) Cho phép lưu trữ lịch sử phiên bản của kịch bản, hiển thị người thực hiện và thời điểm của từng thay đổi.

h) Cho phép so sánh sự khác biệt giữa hai phiên bản bất kỳ của một kịch bản.

i) Cho phép khôi phục kịch bản về một phiên bản trước đó.

k) Cho phép thiết lập trạng thái của kịch bản, tối thiểu bao gồm: đang soạn thảo, chờ phê duyệt, đã ban hành, ngừng sử dụng.

l) Cho phép cấu hình quy trình phê duyệt trước khi một kịch bản được ban hành sử dụng trong môi trường vận hành; tài khoản phê duyệt phải khác tài khoản tạo lập hoặc sửa đổi kịch bản.

m) Cho phép chạy thử kịch bản với dữ liệu đầu vào mẫu mà không tác động đến nền tảng tích hợp (chế độ mô phỏng).

n) Cho phép gán nhãn, phân nhóm kịch bản và tìm kiếm kịch bản theo nhãn, theo thành phần tích hợp được sử dụng.

o) Cho phép xác định danh sách kịch bản, thành phần tích hợp bị ảnh hưởng khi một kịch bản hoặc thành phần tích hợp bị sửa đổi hoặc xoá.

p) Khi nhập kịch bản từ tệp tin, phải kiểm tra tính toàn vẹn của tệp tin và hiển thị danh sách thành phần tích hợp, quyền hạn mà kịch bản yêu cầu trước khi xác nhận nhập.

5.3.5 Yêu cầu chung đối với thực hiện kịch bản

SOAR phải cho phép thực hiện kịch bản (tự động hoặc bán tự động) đáp ứng các yêu cầu chung sau, ngoài các yêu cầu riêng quy định tại 5.3.6 và 5.3.7:

a) Cho phép thiết lập thời hạn thực hiện kịch bản.

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

c) 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).

5.3.6 Hỗ trợ thực hiện kịch bản tự động

SOAR phải cho phép cấu hình kịch bản dựa theo các điều kiện, quy tắc tìm kiếm cảnh báo, tình huống để thực hiện tự động tất cả các bước trong kịch bản mà không cần con người tương tác, ngoài các yêu cầu chung quy định tại 5.3.5.

5.3.7 Hỗ trợ thực hiện kịch bản bán tự động

SOAR phải cho phép thực hiện kịch bản bán tự động đáp ứng các yêu cầu sau, ngoài các yêu cầu chung quy định tại 5.3.5:

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.

b) Lịch sử thực hiện quy định tại 5.3.5 c) đối với kịch bản bán tự động phải bổ sung trường tài khoản người dùng có tương tác.

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

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

5.3.8 Kiểm soát thực thi và xử lý ngoại lệ kịch bản

SOAR phải cho phép kiểm soát việc thực thi kịch bản đáp ứng các yêu cầu sau:

a) Phải cho phép định nghĩa nhánh xử lý khi một bước trong kịch bản thất bại.

b) Phải cho phép thiết lập số lần thực hiện lại và khoảng thời gian chờ giữa các lần thực hiện lại đối với từng bước.

c) Phải cho phép thiết lập thời hạn thực hiện đối với từng bước, ngoài thời hạn thực hiện của toàn bộ kịch bản.

d) Phải cho phép tạm dừng, tiếp tục và huỷ bỏ một phiên thực thi kịch bản đang chạy.

e) Phải cho phép thực hiện lại một bước hoặc toàn bộ kịch bản đối với một cảnh báo, tình huống đã xử lý trước đó.

f) Phải có cơ chế ngăn chặn việc thực thi đồng thời nhiều phiên của cùng một kịch bản trên cùng một cảnh báo hoặc tình huống.

g) Phải cho phép thiết lập giới hạn số lượng đối tượng tối đa mà một kịch bản được phép tác động trong một phiên thực thi; khi vượt giới hạn, kịch bản phải dừng và chuyển sang trạng thái chờ phê duyệt.

h) Phải cho phép thiết lập giới hạn tần suất gọi đối với từng thành phần tích hợp để tránh vượt ngưỡng của nền tảng tích hợp.

i) Phải yêu cầu xác nhận hoặc phê duyệt trước khi thực thi hành động được xác định là nguy hiểm trong kịch bản.

k) Phải cho phép thiết lập thời gian chờ tối đa (timeout) đối với việc gọi thực thi hành động trên nền tảng tích hợp, độc lập với thời hạn thực hiện của bước quy định tại điểm c).

l) Phải cho phép thực hiện khôi phục (rollback) đối với hành động đã thực thi, trong trường hợp nền tảng tích hợp đích hỗ trợ cơ chế khôi phục.

5.4 Yêu cầu về hiệu năng xử lý

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

SOAR phải bảo đảm 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.

5.4.2 Thu thập đồng thời nhiều cảnh báo

SOAR phải cho phép thu thập, xử lý và lưu trữ dữ liệu đồng thời tối thiểu 1.000 cảnh báo trong khoảng thời gian là 01 phút.

5.4.3 Thực thi đồng thời nhiều kịch bản

a) Công bố tối thiểu số lượng luồng kịch bản có thể thực thi đồng thời.

b) Công bố tối thiểu số lượng connector có thể xử lý đồng thời.

5.5 Yêu cầu về quản lý bằng chứng số

5.5.1 Tiếp nhận và bảo toàn bằng chứng

SOAR phải tiếp nhận và bảo toàn bằng chứng số đáp ứng các yêu cầu sau:

a) Phải tự động tính và lưu giá trị băm của mỗi tệp tin bằng chứng tại thời điểm tiếp nhận, sử dụng thuật toán băm chưa được công bố điểm yếu.

b) Phải cho phép kiểm tra lại tính toàn vẹn của bằng chứng bằng cách đối chiếu giá trị băm, theo yêu cầu hoặc theo chu kỳ định trước.

c) Phải ngăn chặn việc sửa đổi nội dung tệp tin bằng chứng sau khi tiếp nhận; mọi thay đổi phải được thực hiện bằng cách tạo phiên bản mới, giữ nguyên bản gốc.

d) Phải lưu trữ bằng chứng ở dạng đã mã hoá.

5.5.2 Chuỗi hành trình bằng chứng

a) SOAR phải ghi nhận và cho phép xem lại chuỗi hành trình đối với từng bằng chứng, tối thiểu bao gồm: thời điểm, tài khoản thực hiện, địa chỉ máy trạm, loại hành vi (tiếp nhận, xem, tải xuống, sao chép, chuyển giao, tiêu huỷ), tình huống liên quan.

b) Bản ghi chuỗi hành trình phải không được phép sửa đổi hoặc xoá bởi bất kỳ vai trò người dùng nào, kể cả vai trò quản trị hệ thống.

c) SOAR phải cho phép xuất chuỗi hành trình bằng chứng ra tệp tin kèm giá trị băm của bản xuất.

5.5.3 Xử lý an toàn đối với bằng chứng có khả năng độc hại

a) SOAR phải cho phép đánh dấu tệp tin bằng chứng là có khả năng độc hại và lưu trữ tệp tin đó ở khu vực cách ly.

b) SOAR không được tự động hiển thị nội dung, thực thi hoặc mở tệp tin bằng chứng được đánh dấu là có khả năng độc hại.

c) Khi tải xuống tệp tin bằng chứng có khả năng độc hại, SOAR phải đóng gói tệp tin ở định dạng có bảo vệ và hiển thị cảnh báo cho người dùng.

5.5.4 Lưu giữ và tiêu huỷ

a) SOAR phải cho phép thiết lập thời hạn lưu giữ bằng chứng theo loại tình huống và tự động thông báo khi đến hạn.

b) SOAR phải yêu cầu phê duyệt trước khi tiêu huỷ bằng chứng và phải ghi nhật ký kiểm toán đối với hành vi tiêu huỷ.

5.6 Yêu cầu về điều hành ứng cứu sự cố

5.6.1 Quản lý nhiệm vụ trong tình huống

a) SOAR phải cho phép tạo, sửa đổi, xoá nhiệm vụ trong một tình huống, mỗi nhiệm vụ tối thiểu có các trường: tên, mô tả, người thực hiện, thời hạn, trạng thái, kết quả, giai đoạn ứng cứu tương ứng.

b) SOAR phải cho phép phân nhóm nhiệm vụ theo giai đoạn ứng cứu sự cố, tối thiểu bao gồm: chuẩn bị, phát hiện và phân tích, ngăn chặn, loại bỏ, khôi phục, tổng kết rút kinh nghiệm.

c) SOAR phải cho phép định nghĩa và áp dụng mẫu danh sách nhiệm vụ theo từng loại sự cố.

d) SOAR phải cho phép thiết lập quan hệ phụ thuộc giữa các nhiệm vụ.

5.6.2 Vai trò trong sự cố

a) SOAR phải cho phép gán vai trò cho người tham gia trong từng tình huống, tối thiểu bao gồm: chỉ huy ứng cứu, người phân tích, người ghi nhận.

b) SOAR phải hiển thị danh sách người đang tham gia xử lý tình huống theo thời gian thực.

5.6.3 Nhật ký điều hành sự cố

a) SOAR phải tự động ghi nhận vào một dòng thời gian thống nhất của tình huống tất cả các hành vi phát sinh, bao gồm: hành vi do người dùng thực hiện, bước thực thi của kịch bản, thay đổi trạng thái, thay đổi nhiệm vụ, tiếp nhận và truy cập bằng chứng, thông tin trao đổi.

b) Dòng thời gian quy định tại điểm a) phải không được phép sửa đổi hoặc xoá.

c) SOAR phải cho phép xuất dòng thời gian ra tệp tin phục vụ lập báo cáo sự cố.

5.6.4 Phân cấp, liên kết và bảo mật tình huống

a) SOAR phải cho phép phân loại mức độ nghiêm trọng của sự cố với tối thiểu 04 mức.

b) SOAR phải cho phép liên kết một tình huống với một hoặc nhiều tình huống khác, gộp và tách tình huống, giữ nguyên lịch sử xử lý sau khi gộp hoặc tách.

c) SOAR phải cho phép thiết lập chế độ hạn chế truy cập đối với từng tình huống, chỉ cho phép những tài khoản được chỉ định xem và xử lý; hành vi truy cập tình huống hạn chế phải được ghi nhật ký kiểm toán.

5.6.5 Báo cáo sự cố

a) SOAR phải cho phép tạo báo cáo sự cố từ dữ liệu của tình huống theo mẫu do người dùng định nghĩa, tối thiểu bao gồm: tóm tắt sự cố, dòng thời gian, phạm vi ảnh hưởng, các dấu hiệu tấn công liên quan, biện pháp đã thực hiện, kết quả và khuyến nghị.

b) SOAR nên cho phép thiết lập và theo dõi thời hạn thực hiện nghĩa vụ báo cáo sự cố theo quy định của pháp luật, tính từ thời điểm ghi nhận sự cố.

5.7 Yêu cầu về quản lý thông tin về mối đe doạ

5.7.1 Quản lý dấu hiệu tấn công

a) SOAR phải cho phép lưu trữ và quản lý dấu hiệu tấn công (IOC) với tối thiểu các loại: địa chỉ IP, tên miền, URL, giá trị băm tệp tin, địa chỉ thư điện tử.

b) Mỗi dấu hiệu tấn công phải có tối thiểu các trường thông tin: loại, giá trị, nguồn cung cấp, thời điểm ghi nhận, mức độ tin cậy, mức độ nguy hiểm, nhãn chia sẻ, thời hạn hiệu lực.

c) SOAR phải tự động khử trùng lặp dấu hiệu tấn công theo loại và giá trị, giữ lại thông tin về tất cả các nguồn cung cấp.

d) SOAR phải cho phép thiết lập danh sách loại trừ để ngăn việc ghi nhận và xử lý các dấu hiệu tấn công thuộc hạ tầng hợp lệ đã biết.

e) SOAR phải cho phép tự động chuyển dấu hiệu tấn công sang trạng thái hết hiệu lực khi quá thời hạn hiệu lực.

5.7.2 Tiếp nhận và chia sẻ

a) SOAR phải cho phép tiếp nhận dấu hiệu tấn công từ tệp tin và từ nguồn cấp dữ liệu bên ngoài theo lịch định trước.

b) SOAR phải hỗ trợ tối thiểu 01 định dạng trao đổi thông tin về mối đe doạ được thừa nhận rộng rãi cho cả chiều tiếp nhận và chiều cung cấp.

c) SOAR phải cho phép kiểm soát việc chia sẻ ra bên ngoài theo nhãn chia sẻ của từng dấu hiệu tấn công.

5.7.3 Đối sánh và ghi nhận phát hiện

a) SOAR phải tự động đối sánh dấu hiệu tấn công với cảnh báo, tình huống mới phát sinh và ghi nhận kết quả đối sánh.

b) SOAR phải cho phép đối sánh ngược một hoặc nhiều dấu hiệu tấn công mới tiếp nhận với dữ liệu cảnh báo, tình huống đã lưu trữ trong khoảng thời gian được chỉ định, và tạo cảnh báo khi có kết quả trùng khớp.

c) SOAR phải ghi nhận số lần và thời điểm một dấu hiệu tấn công được phát hiện trong dữ liệu của tổ chức.

5.7.4 Quản lý thực thể mối đe doạ

a) SOAR nên cho phép quản lý các thực thể: tác nhân đe doạ, chiến dịch tấn công, họ mã độc, kỹ thuật tấn công; và thiết lập liên kết giữa các thực thể này với dấu hiệu tấn công, cảnh báo và tình huống.

5.7.5 Ban hành biện pháp phòng vệ

a) SOAR phải cho phép ban hành dấu hiệu tấn công xuống các nền tảng tích hợp để thực hiện chặn lọc, thông qua kịch bản có cơ chế phê duyệt.

b) SOAR phải cho phép thu hồi biện pháp chặn lọc đã ban hành và ghi nhận trạng thái ban hành của từng dấu hiệu tấn công trên từng nền tảng tích hợp.

Phụ lục A
Phương pháp đánh giá

A.1 Nguyên tắc chung

A.1.1 Việc đánh giá sự phù hợp của sản phẩm SOAR với các yêu cầu quy định tại Điều 4 và Điều 5 của tiêu chuẩn này phải được thực hiện bằng một hoặc kết hợp các phương pháp sau: xem xét tài liệu, thử nghiệm chức năng, đo lường hiệu năng và đánh giá cấu hình an toàn.

A.1.2 Phương pháp đánh giá áp dụng tương ứng với từng nhóm yêu cầu như sau:

- Yêu cầu về tài liệu (4.1): xem xét tài liệu.

- Yêu cầu về quản trị hệ thống, xác thực và phân quyền, quản lý thông tin xác thực (4.2): thử nghiệm chức năng kết hợp xem xét cấu hình.

- Yêu cầu về kiểm soát lỗi, nhật ký hệ thống (4.3, 4.4): thử nghiệm mô phỏng lỗi kết hợp xem xét nhật ký.

- Yêu cầu về tính sẵn sàng (4.5): thử nghiệm chuyển đổi dự phòng.

- Yêu cầu về giám sát tình trạng hoạt động (4.6): thử nghiệm chức năng.

- Yêu cầu về bảo vệ dữ liệu, an toàn và vòng đời sản phẩm (4.7, 4.8): xem xét tài liệu kết hợp đánh giá cấu hình an toàn.

- Yêu cầu chức năng nghiệp vụ (5.1, 5.2, 5.3, 5.5, 5.6, 5.7): thử nghiệm chức năng.

- Yêu cầu về hiệu năng xử lý (5.4): đo lường hiệu năng theo phương pháp quy định tại A.2.

A.1.3 Kết quả đánh giá phải được lập thành báo cáo, trong đó nêu rõ phương pháp áp dụng, điều kiện đo (nếu có) và kết luận về mức độ đáp ứng đối với từng yêu cầu.

A.2 Phương pháp đo lường đối với yêu cầu về hiệu năng xử lý (5.4)

A.2.1 Điều kiện đo tham chiếu

Nhà cung cấp phải công bố cấu hình phần cứng, phần mềm tham chiếu tại đó kết quả đo được thực hiện, tối thiểu bao gồm: số lượng và loại CPU/vCPU, dung lượng bộ nhớ RAM, loại và tốc độ thiết bị lưu trữ, băng thông mạng, phiên bản phần mềm SOAR và hệ điều hành nền.

A.2.2 Phương pháp đo độ trễ thời gian phản hồi (tương ứng 5.4.1)

a) Sử dụng tập dữ liệu tham chiếu có khối lượng tối thiểu do nhà cung cấp công bố, không nhỏ hơn 10 triệu bản ghi log, cảnh báo và tình huống.

b) Thực hiện tối thiểu 03 loại truy vấn tiêu biểu: truy vấn đơn giản theo một điều kiện, truy vấn phức tạp kết hợp nhiều điều kiện và nhiều trường thông tin, truy vấn toàn văn.

c) Đo thời gian phản hồi trung bình và thời gian phản hồi tại phân vị thứ 95 (P95) của mỗi loại truy vấn, thực hiện tối thiểu 30 lần lặp cho mỗi loại truy vấn.

A.2.3 Phương pháp đo khả năng thu thập đồng thời (tương ứng 5.4.2)

a) Mô phỏng gửi đồng thời từ tối thiểu 02 nguồn cảnh báo với tổng số lượng tối thiểu 1.000 cảnh báo trong khoảng thời gian 01 phút.

b) Đo tỷ lệ cảnh báo được tiếp nhận, xử lý và lưu trữ thành công so với tổng số cảnh báo gửi đi.

A.2.4 Phương pháp đo thực thi đồng thời nhiều kịch bản (tương ứng 5.4.3)

a) Xác định số luồng kịch bản và số connector tối đa có thể thực thi đồng thời mà không phát sinh lỗi thực thi.

b) Đo mức suy giảm thời gian phản hồi của hệ thống tại mức tải tối đa đã công bố so với mức tải cơ sở tương ứng không quá 50% số luồng tối đa; mức suy giảm phải được nhà cung cấp công bố kèm theo con số cụ thể.

A.3 Ghi chú áp dụng

Trường hợp SOAR được cung cấp dưới dạng dịch vụ đám mây (SaaS) và không xác định được cấu hình phần cứng cụ thể, nhà cung cấp phải công bố mức dịch vụ tương đương (ví dụ: hạn mức tài nguyên, thoả thuận mức dịch vụ) làm cơ sở đối chiếu khi đánh giá.

Thư mục tài liệu tham khảo

[1] Market Guide for Security Orchestration, Automation and Response Solutions, November 28, 2023.

[2] NIST SP 800-61r3 - Incident Response Recommendations and Considerations for Cybersecurity Risk Management.

[3] Quyết định số 1907/QĐ-BTTTT, ngày 02/12/2021 của Bộ trưởng Bộ Thụng tin và Truyền thụng ban hành yêu cầu kỹ thuật cơ bản đối với sản phẩm Điều phối, tự động húa và phản ứng an toàn thụng tin.
