TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXXXX:2026

Xuất bản lần 1

AN NINH MẠNG - NỀN TẢNG TRI THỨC MỐI ĐE DỌA AN NINH MẠNG (TIP) - YÊU CẦU CHUNG

Cyber security - Threat Intelligence Platform - General requirements

HÀ NỘI – 2026

Mục lục

Lời nói đầu

TCVN XXXXX:2026 An ninh mạng - Nền tảng tri thức mối đe dọa an ninh mạng (TIP) - 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 này quy định các yêu cầu chung đối với nền tảng tri thức mối đe dọa an ninh mạng nhằm đảm bảo chất lượng của sản phẩm, phù hợp với mục tiêu nâng cao năng lực giám sát, chia sẻ thông tin và chủ động bảo vệ hệ thống thông tin trước các mối đe dọa trên không gian mạng. Tiêu chuẩn này được xây dựng trên cơ sở kế thừa, cập nhật và nâng cấp yêu cầu kỹ thuật cơ bản đối với sản phẩm nền tảng tri thức mối đe dọa an toàn thông tin đã được ban hành tại Quyết định số 1517/QĐ-BTTTT ngày 06/10/2021 của Bộ trưởng Bộ Thông tin và Truyền thông.

Để đạt hiệu quả cao nhất trong công tác giám sát, cảnh báo sớm và ứng phó sự cố, khuyến khích cơ quan, tổ chức chủ quản hệ thống thông tin triển khai nền tảng tri thức mối đe dọa an ninh mạng đáp ứng đầy đủ các yêu cầu quy định trong tiêu chuẩn này, kết hợp với các biện pháp quản lý, kỹ thuật và vận hành khác.

An ninh mạng - Nền tảng tri thức mối đe dọa an ninh mạng (TIP) - Yêu cầu chung

Cyber security – Threat Intelligence 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 tri thức mối đe dọa an ninh mạng (sau đây viết tắt là TIP).

2 Tài liệu viện dẫn

Trong tiêu chuẩn này không có tài liệu nào được viện dẫn.

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

Nền tảng tri thức mối đe dọa an ninh mạng (threat intelligence platform - TIP)

Giải pháp hỗ trợ thu thập, tổng hợp, lưu trữ, chuẩn hóa, phân tích và chia sẻ thông tin tình báo về mối đe dọa an ninh mạng từ đa nguồn nhằm hỗ trợ các tổ chức chủ động phòng ngừa và ứng phó với các mối đe dọa.

3.1.3

Thông tin tình báo mối đe dọa (threat intelligence)

Thông tin về mối đe dọa đã được tổng hợp, chuyển đổi, phân tích, diễn giải hoặc làm phong phú thêm để cung cấp bối cảnh cần thiết cho các quy trình ra quyết định.

3.1.4

Chỉ báo xâm nhập (indicator of compromise - IoC)

Bằng chứng kỹ thuật hoặc dấu hiệu cho thấy một cuộc tấn công mạng sắp xảy ra, đang diễn ra hoặc có thể đã xảy ra.

3.1.5

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.

3.1.6

Xác thực đa nhân tố (multi-factor authentication)

Phương pháp xác thực kết hợp một số yếu tố liên quan đến người dùng, bao gồm: những thông tin mà người dùng biết (mật khẩu, mã số truy cập...), những thông tin mà người dùng sở hữu (chứng thư chữ ký số, thẻ thông minh...), những thông tin về sinh trắc học của người dùng (vân tay, mống mắt...).

3.2 Chữ viết tắt

API	Giao diện lập trình ứng dụng	Application Programming Interface
EDR	Phát hiện và ứng phó các mối đe dọa an ninh mạng tại thiết bị đầu cuối	Endpoint Detection and Response
IoC	Chỉ báo xâm nhập	Indicator of Compromise
IP	Giao thức Internet	Internet Protocol
SIEM	Nền tảng quản lý, phân tích sự kiện và thông tin an ninh mạng	Security Information and Event Management
SOAR	Sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng	Security Orchestration, Automation and Response
STIX	Ngôn ngữ biểu diễn thông tin về mối đe dọa có cấu trúc	Structured Threat Information Expression
TAXII	Giao thức trao đổi tự động thông tin tình báo đáng tin cậy	Trusted Automated Exchange of Intelligence Information
TIP	Nền tảng tri thức mối đe dọa an ninh mạng	Threat Intelligence Platform
TLP	Giao thức đèn giao thông	Traffic Light Protocol
WAF	Tường lửa ứng dụng web	Web Application Firewall

4 Yêu cầu chung về quản trị và an toàn của nền tảng

4.1 Yêu cầu về tài liệu

TIP cần 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 TIP.

b) Tài liệu hướng dẫn tinh chỉnh TIP nhằm tối ưu hóa khả năng thu thập, xử lý, chuẩn hóa và khử trùng lặp dữ liệu tình báo, giảm thiểu các cảnh báo nhiễu.

c) Tài liệu hướng dẫn chi tiết các chức năng sử dụng, phân quyền quản trị và quy trình vận hành TIP.

4.2 Yêu cầu về quản trị hệ thống

4.2.1 Quản lý vận hành

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

a) Cho phép cấu hình thời gian hệ thống.

b) Cho phép cấu hình thời gian duy trì phiên kết nối.

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

d) Cho phép tìm kiếm dữ liệu bằng từ khóa để xem lại.

4.2.2 Quản trị từ xa

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

a) Hỗ trợ cấu hình xác thực đa nhân tố đối với mọi kết nối quản trị từ xa.

b) Sử dụng các giao thức mã hóa an toàn như TLS hoặc tương đương.

c) 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.

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,...).

4.2.3 Quản lý xác thực và phân quyền

TIP 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, độ dài mật khẩu tối thiểu 8 ký tự theo cấu hình mặc định, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu.

b) Hỗ trợ thiết lập thời gian yêu cầu thay đổi mật khẩu.

c) 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.

d) Hỗ trợ xác thực đa nhân tố.

4.3 Yêu cầu về kiểm soát lỗi

4.3.1 Bảo vệ cấu hình

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

4.3.2 Bảo vệ dữ liệu nhật ký, dữ liệu ứng dụng

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

4.3.4 Sao lưu và phục hồi

a) TIP cho phép quản trị viên thiết lập lịch sao lưu định kỳ cho các cấu hình hệ thống và cơ sở dữ liệu.

b) TIP có chức năng phục hồi trạng thái hoạt động từ các tệp tin sao lưu trước đó trong trường hợp xảy ra sự cố.

c) TIP hỗ trợ mã hóa dữ liệu bằng các thuật toán mã hóa mạnh, chưa ghi nhận điểm yếu hoặc lỗ hổng bảo mật nghiêm trọng tại thời điểm áp dụng.

4.3.5 Cập nhật bản vá hệ thống

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

4.4 Yêu cầu về quản lý nhật ký

4.4.1 Nhật ký quản trị hệ thống

a) TIP cho phép ghi nhật ký quản trị hệ thống về các loại sự kiện sau:

- Đăng nhập, đăng xuất, thêm mới, sửa đổi, xóa tài khoản và phân nhóm quyền người dùng;

- 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;

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

- Ghi nhận mọi thao tác thêm, sửa, xóa đối với dữ liệu tình báo trên TIP;

- Ghi nhận mọi thao tác xuất, phân phối và chia sẻ dữ liệu tình báo ra bên ngoài hệ thống.

b) TIP cho phép ghi nhật ký quản trị hệ thống có các trường thông tin sau:

- Thời gian sinh nhật ký (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).

4.4.2 Nhật ký cảnh báo

TIP cho phép ghi nhật ký cảnh báo được sinh ra bởi việc thực thi các thiết lập cảnh báo mối đe dọa, tối thiểu bao gồm thời gian kích hoạt và tên quy tắc hoặc thiết lập sinh ra cảnh báo đó.

4.4.3 Quản lý vòng đời lưu trữ nhật ký

TIP cho phép quản lý nhật ký 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 nhật ký (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ...).

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

4.5 Yêu cầu về hiệu năng xử lý và khả năng mở rộng

Khi được triển khai theo cấu hình tối thiểu nêu trong tài liệu hướng dẫn cài đặt của nhà sản xuất, TIP phải đáp ứng các yêu cầu sau:

a) Nhà sản xuất phải công bố ngưỡng thời gian phản hồi tối đa cho việc tìm kiếm, truy vấn dữ liệu tình báo, tương ứng với khối lượng dữ liệu và độ phức tạp truy vấn tối đa mà TIP được công bố có khả năng xử lý dưới cấu hình tối thiểu nêu trên. TIP phải đáp ứng đúng ngưỡng đã công bố khi được đánh giá.

b) Công bố số lượng bản ghi dữ liệu tình báo về mối đe dọa tối đa, tối thiểu mà TIP có thể lưu trữ và xử lý.

c) TIP phải có khả năng mở rộng năng lực xử lý và lưu trữ (ví dụ: bổ sung tài nguyên hoặc nút xử lý) để đáp ứng nhu cầu tăng trưởng của khối lượng dữ liệu tình báo mà không làm gián đoạn hoạt động.

5 Yêu cầu về chức năng nghiệp vụ của nền tảng

5.1 Thu thập và tiếp nhận dữ liệu tình báo

a) TIP cho phép thu thập và lưu trữ thông tin mối đe dọa từ đa nguồn, bao gồm: nguồn tình báo mở, nguồn tình báo thương mại, nền tảng trao đổi tình báo, cộng đồng chia sẻ phi tập trung, nguồn dữ liệu từ nội bộ. Thông tin mối đe dọa bao gồm tối thiểu các loại thông tin sau:

- Mô tả tổng quan mối đe dọa;

- Mức độ nguy hiểm của mối đe dọa;

- Mức độ tin cậy về dữ liệu của mối đe dọa;

- Các phân nhóm được gán cho mối đe dọa;

- Các thuộc tính mô tả chi tiết mối đe dọa.

b) TIP cho phép cấu hình thu thập thông tin mối đe dọa qua hai cách thức thủ công và tự động.

c) Hỗ trợ tiếp nhận thông tin tình báo theo chuẩn quốc tế STIX/TAXII.

d) Cho phép thiết lập và tùy chỉnh chu kỳ thời gian thu thập dữ liệu từ các nguồn cấp khác nhau.

e) Cho phép nhập dữ liệu thủ công từ tệp tin theo tối thiểu 02 trong các định dạng sau: XML, JSON, CSV, TXT, XLSX, XLS.

f) Có khả năng thu thập thông tin tình báo ở dạng có cấu trúc, bán cấu trúc và phi cấu trúc.

5.2 Xử lý dữ liệu tình báo

a) Hỗ trợ chuẩn hóa toàn bộ dữ liệu đã lưu trữ về cùng một định dạng, tiêu chuẩn hoặc mô hình dữ liệu chung như STIX hoặc tương đương.

b) Quản lý tối thiểu các loại đối tượng: chỉ báo (IoC), dữ liệu quan sát, mã độc, mẫu hành vi tấn công, lỗ hổng bảo mật, tác nhân đe dọa, đối tượng mục tiêu, chiến dịch tấn công, mối quan hệ.

c) Mỗi đối tượng dữ liệu bao gồm nhưng không giới hạn các trường thông tin sau: tên, mô tả, loại, thời gian tạo, nguồn cấp, mức độ tin cậy, thời gian phát hiện lần đầu và lần cuối, mức độ nghiêm trọng, nhãn đánh dấu kiểm soát dữ liệu, nạn nhân.

d) Có khả năng làm giàu dữ liệu tình báo.

e) Có khả năng khử trùng lặp dữ liệu tình báo từ nhiều nguồn khác nhau, đồng thời phải bảo toàn bối cảnh và ngữ cảnh gốc của dữ liệu.

f) TIP cho phép phân loại và gắn nhãn tên phân nhóm cho thông tin mối đe dọa theo các phân nhóm sau phục vụ cho mục đích tìm kiếm:

- Điểm yếu, lỗ hổng bảo mật đã được công bố;

- Họ mã độc;

- Kỹ thuật tấn công;

- Chiến dịch tấn công;

- Mục đích tấn công;

- Loại đối tượng, tổ chức bị tấn công;

- Đối tượng, tổ chức thực hiện tấn công;

- Tên miền, địa chỉ IP của khách hàng có kết nối đến cơ sở hạ tầng của đối tượng, tổ chức thực hiện tấn công.

g) Cho phép tìm kiếm, lọc dữ liệu tình báo theo tối thiểu các tiêu chí sau: loại đối tượng dữ liệu, phân nhóm/nhãn, tác nhân đe dọa, chiến dịch tấn công, khoảng thời gian, mức độ tin cậy, nhãn TLP.

h) Cho phép hiển thị trực quan mối quan hệ (dạng sơ đồ liên kết) giữa các đối tượng dữ liệu tình báo có liên hệ với nhau (ví dụ: tác nhân đe dọa, chiến dịch tấn công, mã độc, chỉ báo, lỗ hổng bảo mật).

5.3 Quản lý vòng đời chỉ báo

a) TIP cho phép thiết lập thời gian hiệu lực (TTL) tĩnh cho chỉ báo; khi hết thời gian hiệu lực, chỉ báo tự động chuyển sang trạng thái hết hiệu lực.

b) Cho phép thiết lập cơ chế tính điểm rủi ro để phân loại và xếp thứ tự ưu tiên các chỉ báo, từ đó xác định hành động xử lý phù hợp.

c) Cho phép quản trị viên hoặc phân tích viên chủ động thay đổi trạng thái hiệu lực của chỉ báo, bao gồm thu hồi hiệu lực trước hạn, kèm theo lý do.

d) Cho phép ghi chú, bình luận nội bộ và gán trạng thái thẩm định (ví dụ: mới tiếp nhận, đang thẩm định, đã xác thực, đã công bố) cho chỉ báo, phục vụ công tác thẩm định và trao đổi giữa các phân tích viên.

5.4 Chia sẻ, phân phối, tích hợp và kiểm soát truy cập

TIP cho phép chia sẻ thông tin tình báo an ninh mạng đáp ứng các yêu cầu sau:

a) Cung cấp API, Webhook để chia sẻ dữ liệu tình báo.

b) Hỗ trợ chia sẻ và trao đổi luồng tình báo qua chuẩn STIX/TAXII.

c) Cho phép xuất, phân phối dữ liệu tình báo dưới dạng tệp tin tĩnh (định dạng CSV, JSON, STIX).

d) Cho phép tích hợp trực tiếp dữ liệu tình báo tới các giải pháp bảo mật khác như SIEM, SOAR, EDR, WAF...

e) Cho phép chia sẻ dữ liệu nhật ký ứng dụng thông qua giao thức Syslog.

f) Cung cấp cơ chế ẩn danh hóa, làm sạch hoặc loại bỏ các thông tin nhạy cảm, thông tin định danh cá nhân trước khi chia sẻ luồng tình báo ra các hệ thống hoặc tổ chức bên ngoài.

g) Có khả năng chia sẻ và tích hợp các bộ quy tắc phát hiện tấn công (như YARA, Sigma, Snort) vào hệ thống giám sát để phục vụ cho công tác giám sát và phòng thủ.

h) Hỗ trợ cơ chế gán nhãn và kiểm soát truy cập dữ liệu tình báo theo giao thức TLP.

i) Cho phép tiếp nhận và ghi nhận thông tin phản hồi về kết quả đối sánh chỉ báo từ các giải pháp bảo mật đã tích hợp (ví dụ: SIEM, SOAR, EDR), làm cơ sở cập nhật mức độ ưu tiên hoặc điểm rủi ro của chỉ báo tại 5.3 b).

5.5 Thống kê xu hướng, cảnh báo và báo cáo

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

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

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

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

- Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: DOCX, DOC, XLSX, XLS, PDF, HTML, XML;

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

b) TIP có chức năng cho phép thống kê các mối đe dọa trên thế giới thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

- Cho phép thống kê xu hướng mối đe dọa dưới dạng biểu đồ;

- Cho phép tìm kiếm dữ liệu xu hướng mối đe dọa theo thời gian.

c) TIP có chức năng cho phép quản lý thiết lập cảnh báo mối đe dọa đến người dùng đáp ứng các yêu cầu sau:

- Cho phép nhận cảnh báo theo các phân nhóm được định nghĩa trước;

- Cho phép thiết lập thời gian nhận cảnh báo;

- Cho phép tải nội dung cảnh báo dưới dạng tập tin;

- Cho phép hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo;

- Cho phép nhận cảnh báo qua phương thức gửi thư điện tử hoặc tin nhắn.

PHỤ LỤC A
(tham khảo)
Các chức năng mở rộng của nền tảng

A.1 Có khả năng giám sát và hiển thị danh sách các tài khoản đăng nhập bị lộ lọt, bao gồm tên người dùng, mật khẩu và nguồn phát tán.

A.2 Có khả năng giám sát, thêm mới và quản lý thông tin rò rỉ từ mạng lưới web đen.

A.3 Có khả năng quản lý và chia sẻ danh sách các tên miền giả mạo, trang web/mạng xã hội giả mạo, ứng dụng giả mạo.

A.4 Có khả năng quản lý, giám sát và cảnh báo về các tài liệu nội bộ, dữ liệu nhạy cảm của tổ chức bị lộ lọt trên không gian mạng.

A.5 Có khả năng ứng dụng trí tuệ nhân tạo và học máy để hỗ trợ tự động xử lý, làm giàu dữ liệu, tóm tắt báo cáo tình báo hoặc hỗ trợ truy vấn thông tin tình báo.

A.6 Có khả năng tự động hóa các tác vụ lặp đi lặp lại trong quá trình thu thập, làm giàu và phân tích dữ liệu tình báo nội tại của TIP (không bao gồm điều phối, tự động hóa quy trình ứng phó sự cố).

A.7 Cung cấp hướng dẫn thiết lập kịch bản tự động hóa phục vụ khả năng phân tích và làm giàu dữ liệu tình báo mối đe dọa trong phạm vi nêu tại A.6).

Thư mục tài liệu tham khảo

[1] NIST SP 800-150 (Guide to Cyber Threat Information Sharing), October 2016.

[2] ENISA (Exploring the opportunities and limitations of current Threat Intelligence Platforms), v1.0, December 2017.

[3] Gartner (Market Guide for Security Threat Intelligence Products and Services), 12 August 2024.

[4] Forrester (The External Threat Intelligence Service Providers Landscape), Q1 2026.

[5] Quyết định số 1517/QĐ-BTTTT, ngày 06/10/2021 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành yêu cầu kỹ thuật cơ bản đối với sản phẩm nền tảng tri thức mối đe dọa an toàn thông tin.
