THUYẾT MINH DỰ THẢO TIÊU CHUẨN QUỐC GIA

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

1. Thông tin chung về dự thảo TCVN

1.1. Tên dự thảo TCVN

TCVN XXXXX:2026 An ninh mạng - Nền tảng tri thức mối đe dọa an ninh mạng (TIP) - Yêu cầu chung.

1.2. Thuộc lĩnh vực

Tiêu chuẩn thuộc lĩnh vực tiêu chuẩn cho sản phẩm, dịch vụ an ninh mạng.

1.3. Phạm vi áp dụng của TCVN

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).

1.4. Mục tiêu của TCVN

Tiêu chuẩn quốc gia An ninh mạng - Nền tảng tri thức mối đe dọa an ninh mạng (TIP) - Yêu cầu chung nhằm thiết lập một khung kỹ thuật thống nhất để bảo đảm chất lượng sản phẩm TIP tại Việt Nam, từ đó nâng cao năng lực phòng thủ chủ động, phát hiện và cảnh báo sớm rủi ro cho các hệ thống thông tin. Tiêu chuẩn này đóng vai trò là cơ sở để phát triển sản phẩm TIP chất lượng, đồng thời tạo thước đo chuẩn mực phục vụ trực tiếp cho công tác quản lý, thẩm định, rà soát, đánh giá và lựa chọn giải pháp nền tảng của các cơ quan, tổ chức. Qua đó, kiến tạo thị trường và thúc đẩy hệ sinh thái sản phẩm an toàn, an ninh mạng "Make in Vietnam" phát triển bền vững.

1.5. Cơ quan chủ trì soạn thảo

- Tên cơ quan: Cục An ninh mạng và phòng, chống tội phạm sử dụng Công nghệ cao - Bộ Công an.

- Địa chỉ: Lô E2, khu đô thị mới Cầu Giấy, Phường Cầu Giấy, Thành phố Hà Nội.

1.6. Tổ chức tham gia soạn thảo

Tham gia soạn thảo tiêu chuẩn quốc gia (TCVN) này bao gồm: Các cán bộ Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng Công nghệ cao; Các chuyên gia của Hiệp hội An ninh mạng quốc gia; quý Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam (NCS Group) và Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT).

1.7. Phiên bản dự thảo: V1.0

2. Nội dung dự thảo TCVN

DỰ THẢO TCVN	THUYẾT MINH
1 Phạm vi áp dụng	Tự xây dựng
2 Tài liệu viện dẫn	Tự xây dựng
3 Thuật ngữ, định nghĩa và chữ viết tắt	Tự xây dựng
3.1 Thuật ngữ và định nghĩa	Tự xây dựng
3.2 Chữ viết tắt	Tự xây dựng
4 Yêu cầu chung về quản trị và an toàn của nền tảng	Tự xây dựng
4.1 Yêu cầu về tài liệu	Tham khảo mục 1. Yêu cầu về tài liệu tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.2 Yêu cầu về quản trị hệ thống	Tham khảo mục 2. Yêu cầu về quản trị hệ thống tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.2.1 Quản lý vận hành	Tham khảo mục 2.1. Quản lý vận hành tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.2.2 Quản trị từ xa	Tham khảo mục 2.2. Quản trị từ xa tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.2.3 Quản lý xác thực và phân quyền	Tham khảo mục 2.3. Quản lý xác thực và phân quyền tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.3 Yêu cầu về kiểm soát lỗi	Tham khảo mục 3. Yêu cầu về kiểm soát lỗi tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.3.1 Bảo vệ cấu hình	Tham khảo mục 3.1. Bảo vệ cấu hình tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.3.2 Bảo vệ dữ liệu nhật ký, dữ liệu ứng dụng	Tham khảo mục 3.2. Bảo vệ dữ liệu log tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.

4.3.3 Đồng bộ thời gian hệ thống	Tham khảo mục 3.3. Đồng bộ thời gian hệ thống tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.3.4 Sao lưu và phục hồi	Tự xây dựng
4.3.5 Cập nhật bản vá hệ thống	Tham khảo mục 6.2. Cập nhật bản vá hệ thống tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.4 Yêu cầu về quản lý nhật ký	Tự xây dựng
4.4.1 Nhật ký quản trị hệ thống	Tham khảo mục 4.1. Log quản trị hệ thống tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.4.2 Nhật ký cảnh báo	Tham khảo mục 4.3. Log cảnh báo tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.4.3 Quản lý vòng đời lưu trữ nhật ký	Tham khảo mục 4.5. Quản lý log tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.5 Yêu cầu về hiệu năng xử lý và khả năng mở rộng	Tự xây dựng
5 Yêu cầu về chức năng nghiệp vụ của nền tảng	Tự xây dựng
5.1 Thu thập và tiếp nhận dữ liệu tình báo	Tham khảo mục 4.2. Log thông tin mối đe dọa tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông. Tham khảo Phụ lục B, tài liệu Exploring the opportunities and limitations of current Threat Intelligence Platforms, v1 của ENISA.
5.2 Xử lý dữ liệu tình báo	Tự xây dựng
5.3 Quản lý vòng đời chỉ báo	Tự xây dựng
5.4 Chia sẻ, phân phối, tích hợp và kiểm soát truy cập	Tự xây dựng
5.5 Thống kê xu hướng, cảnh báo và báo cáo	Tham khảo mục 7. Yêu cầu về chức năng thống kê xu hướng và cảnh báo mối de dọa tại QĐ số 1517/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
Phụ lục A (tham khảo): Các chức năng mở rộng của nền tảng	Tự xây dựng