

THUYẾT MINH DỰ THẢO TIÊU CHUẨN QUỐC GIA
AN NINH MẠNG - SẢN PHẨM ĐIỀU PHỐI, TỰ ĐỘNG HOÁ VÀ PHẢN
ỨNG AN NINH MẠNG - YÊU CẦU CHUNG

1. Thông tin chung về dự thảo TCVN

a) Tên dự thảo TCVN

TCVN XXXXX:2026 An ninh mạng - Sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng - Yêu cầu chung.

b) Thuộc lĩnh vực

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

c) Phạm vi áp dụng của TCVN

Tiêu chuẩn này quy định các yêu cầu kỹ thuật chung đối với sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng (Sau đây viết tắt là SOAR).

d) Mục tiêu của TCVN

Việc nghiên cứu, xây dựng và ban hành tiêu chuẩn quốc gia đối với sản phẩm điều phối, tự động hoá và phản ứng an ninh mạng (SOAR) nhằm tạo lập một hệ quy chiếu đo lường và kiểm định kỹ thuật thống nhất, làm căn cứ cho công tác đánh giá chất lượng sản phẩm trước khi đưa vào sử dụng. Tiêu chuẩn này sẽ đóng vai trò là thước đo kỹ thuật để các cơ quan, tổ chức, chủ quản hệ thống thông tin tham chiếu trong quá trình thiết kế, lập hồ sơ thầu và nghiệm thu. Đồng thời, đây cũng là định hướng cho các doanh nghiệp công nghệ trong nước chuẩn hóa kiến trúc, tối ưu hóa thuật toán, tạo đòn bẩy thúc đẩy nghiên cứu và phát triển các sản phẩm SOAR “Make in Vietnam” đạt chất lượng tương đương quốc tế và đáp ứng toàn diện yêu cầu bảo vệ chủ quyền trên không gian mạng.

đ) 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.

e) 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; Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam (NCS Group).

g) Phiên bản dự thảo: Version 1

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, quản trị và an toàn đối với sản phẩm	Tự xây dựng
4.1 Yêu cầu về tài liệu	Tự xây dựng
4.2 Yêu cầu về quản trị hệ thống	Tham khảo mục 2. Yêu cầu về quản trị hệ thống tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.2.1 Quản lý vận hành	Tự xây dựng dựa trên cơ sở rà soát mục 2.1. Quản lý vận hành tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông và tài liệu 2023 Market Guide for Security Orchestration Automation and Response Solutions.
4.2.2 Quản trị từ xa	Tham khảo mục 2.2. Log quản trị hệ thống tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.2.3 Quản lý xác thực và phân quyền	Tự xây dựng dựa trên cơ sở rà soát mục 2.3. Quản lý xác thực và phân quyền tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông và tài liệu Market Guide for Security Orchestration Automation and Response Solutions.
4.2.4 Quản lý báo cáo	Tự xây dựng dựa trên cơ sở rà soát mục 2.4. Quản lý báo cáo tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông và tài liệu Market Guide for Security Orchestration Automation and Response Solutions.
4.2.5 Quản lý thông tin xác thực của thành phần tích hợp	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.3 Yêu cầu về kiểm soát lỗi	Tham khảo mục 3. Yêu cầu về kiểm soát lỗi tại QĐ số 1907/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 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.3.2 Bảo vệ dữ liệu nhật ký, cảnh báo, tình huống và bằng chứng	Tham khảo mục 3.2. Bảo vệ dữ liệu log, cảnh báo, tình huống và bằng chứng tại QĐ

	1907/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 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.4 Yêu cầu về nhật ký hệ thống (log)	Tham khảo mục 4. Yêu cầu về log tại QĐ 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.4.1 Log quản trị hệ thống	Tham khảo mục 4.1. Log quản trị hệ thống tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.4.2 Định dạng log	Tham khảo mục 4.2. Định dạng log tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
4.4.3 Quản lý log	Tự xây dựng dựa trên cơ sở rà soát mục 4.3. Quản lý log tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông và tài liệu Market Guide for Security Orchestration Automation and Response Solutions; Tiêu chuẩn TCVN 14423:2026.
4.4.4 Bảo vệ nhật ký kiểm toán	Tự xây dựng dựa trên nghiên cứu sản phẩm quốc tế có mặt trên Việt Nam.
4.5 Yêu cầu về tính sẵn sàng	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.5.1 Kiến trúc dự phòng	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.5.2 Cơ chế chuyển đổi dự phòng	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.5.3 Đồng bộ dữ liệu và khôi phục sau sự cố	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.6 Yêu cầu về giám sát tình trạng hoạt động	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.6.1 Giám sát thành phần hệ thống	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.6.2 Giám sát thành phần tích hợp	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.6.3 Giám sát luồng thu thập dữ liệu	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.6.4 Cảnh báo vận hành và xuất dữ liệu giám sát	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam

4.7 Yêu cầu về bảo vệ dữ liệu	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
4.8 Yêu cầu về an toàn và vòng đời sản phẩm	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5 Yêu cầu chức năng nghiệp vụ đối với sản phẩm	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.1 Yêu cầu về chức năng điều phối xử lý	Tự xây dựng dựa trên cơ sở rà soát mục 6. Yêu cầu về chức năng điều phối xử lý và giám sát tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.1.1 Điều phối xử lý cảnh báo	Tham khảo mục 6.1. Yêu cầu về điều phối xử lý cảnh báo tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.1.2 Điều phối xử lý tình huống	Tham khảo mục 6.2. Yêu cầu về điều phối xử lý tình huống tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.1.3 Leo thang và thông báo	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.2 Yêu cầu về chức năng giám sát và phân tích sự cố	Tham khảo mục 6.3. 6.3. Giám sát và phân tích sự cố an toàn thông tin tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.3 Yêu cầu về chứng năng tích hợp và tự động hoá	Tham khảo mục 7. Yêu cầu về chức năng tích hợp và tự động hoá tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.3.1 Quản lý thành phần tích hợp	Tham khảo mục 7.1. Quản lý thành phần tích hợp tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.3.2 Hỗ trợ tích hợp nhiều nền tảng khác nhau	Tự xây dựng dựa trên cơ sở rà soát mục 7.2. Hỗ trợ tích hợp nhiều nền tảng khác nhau tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông và tài liệu 2023 Market Guide for Security Orchestration Automation and Response Solutions.
5.3.3 Hỗ trợ tích hợp API	Tự xây dựng dựa trên cơ sở rà soát mục 7.3 Hỗ trợ tích hợp nhiều API và mục 7.4 Hỗ trợ tích hợp API theo hai chiều tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông và tài liệu Security Orchestration, Automation, and Response for Security Analysts.
5.3.4 Quản lý kịch bản	Tham khảo mục 7.5. Quản lý kịch bản tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.

5.3.5 Hỗ trợ thực hiện kịch bản tự động	Tham khảo mục 7.6. Hỗ trợ thực hiện kịch bản tự động tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.3.6 Hỗ trợ thực hiện kịch bản bán tự động	Tham khảo mục 7.7. Hỗ trợ thực hiện kịch bản bán tự động tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông. Tham bảo NIST SP 800-61r3 - Incident Response Recommendations and Considerations for Cybersecurity Risk Management
5.3.7 Kiểm soát thực thi và xử lý ngoại lệ kịch bản	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.4 Yêu cầu về hiệu năng xử lý	Tham khảo mục 5. Yêu cầu về hiệu năng xử lý tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.4.1 Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu	Tham khảo mục 5.1. Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.4.2 Thu thập đồng thời nhiều cảnh báo	Tham khảo mục 5.2. Thu thập đồng thời nhiều cảnh báo tại QĐ số 1907/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
5.5 Yêu cầu về quản lý bằng chứng số	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.5.1 Tiếp nhận và bảo toàn bằng chứng	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.5.2 Chuỗi hành trình bằng chứng	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.5.3 Xử lý an toàn đối với bằng chứng có khả năng độc hại	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.5.4 Lưu giữ và tiêu hủy	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.6 Yêu cầu về điều hành ứng cứu sự cố	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.6.1 Quản lý nhiệm vụ trong tình huống	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.6.2 Vai trò trong sự cố	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.6.3 Nhật ký điều hành sự cố	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam

5.6.4 Phân cấp, liên kết và bảo mật tình huống	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.6.5 Báo cáo sự cố	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.7 Yêu cầu về quản lý thông tin về môi đe dọa	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.7.1 Quản lý dấu hiệu tấn công	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.7.2 Tiếp nhận và chia sẻ	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.7.3 Đối sánh và ghi nhận phát hiện	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.7.4 Quản lý thực thể môi đe dọa	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam
5.7.5 Ban hành biện pháp phòng vệ	Tự xây dựng dựa trên quá trình nghiên cứu sản phẩm quốc tế tại Việt Nam