BỘ THÔNG TIN VÀ TRUYỀN THÔNG

**CỤC AN TOÀN THÔNG TIN**

**THUYẾT MINH DỰ THẢO TIÊU CHUẨN**

**CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN - HỒ SƠ BẢO VỆ CHO SẢN PHẨM PHÁT HIỆN VÀ PHẢN HỒI ĐIỂM CUỐI (EDR)**

***Information technology - Security techniques - Protection profile for Endpoint Detection and Response (EDR)***

**Hà Nội, 2023**

MỤC LỤC

[1. Mở đầu 5](#_Toc137474351)

[1.1. Tên dự thảo tiêu chuẩn 5](#_Toc137474352)

[1.2. Mục tiêu xây dựng 5](#_Toc137474353)

[2. Tình hình tiêu chuẩn hóa 6](#_Toc137474354)

[2.1. Thế giới 6](#_Toc137474355)

[a) Mô hình triển khai áp dụng ISO/IEC 15408 của Mỹ 8](#_Toc137474356)

[b) Mô hình triển khai áp dụng ISO/IEC 15408 của Nhật Bản 9](#_Toc137474357)

[c) Mô hình triển khai áp dụng ISO/IEC 15408 của Singapore 10](#_Toc137474358)

[d) Một số tiêu chuẩn về đánh giá an toàn thông tin đã ban hành 11](#_Toc137474359)

[2.2. Trong nước 12](#_Toc137474360)

[2.3. Hiện trạng sản phẩm phòng, chống mã độc trên thiết bị đầu cuối (AV) 13](#_Toc137474361)

[3. Giới thiệu bộ tiêu chuẩn ISO/IEC 15408 và hồ sơ bảo vệ (PP) 15](#_Toc137474362)

[3.1. Bộ tiêu chuẩn ISO/IEC 15408 15](#_Toc137474363)

[3.2. Hồ sơ bảo vệ (PP) 16](#_Toc137474364)

[a) Giới thiệu 16](#_Toc137474365)

[b) Khung nội dung PP 18](#_Toc137474366)

[4. Phương pháp xây dựng tiêu chuẩn 19](#_Toc137474367)

[5. Giới thiệu tiêu chuẩn tham chiếu (tiêu chuẩn gốc) 19](#_Toc137474368)

[6. Giới thiệu dự thảo tiêu chuẩn hồ sơ bảo vệ cho sản phẩm phát hiện và phản hồi điểm cuối (EDR) 21](#_Toc137474369)

[7. Kết luận 22](#_Toc137474370)

[8. Tài liệu tham khảo 23](#_Toc137474371)

1. Mở đầu
   1. Tên dự thảo tiêu chuẩn

“Công nghệ thông tin - Các kỹ thuật an toàn - Hồ sơ bảo vệ cho sản phẩm phát hiện và phản hồi điểm cuối (EDR)”

* 1. Mục tiêu xây dựng

Theo quy định tại Điểm a, Khoản 1 Điều 39 Luật An toàn thông tin mạng quy định sản phẩm an toàn thông tin mạng (ATTTM) trước khi đưa vào lưu thông trên thị trường phải thực hiện chứng nhận hợp quy hoặc công bố hợp quy và sử dụng dấu hợp quy. Tại Thông tư 13/2018/TT-BTTTT ngày 15/10/2018 quy định Danh mục sản phẩm ATTTM nhập khẩu theo giấy phép và trình tự, thủ tục, hồ sơ cấp Giấy phép nhập khẩu sản phẩm ATTTM và Thông tư 10/2022/TT-BTTTT ngày 20/7/2022 sửa đổi, bổ sung Thông tư 13/2018/TT-BTTTT: Hồ sơ đề nghị cấp Giấy phép nhập khẩu phải có Giấy chứng nhận hoặc công bố hợp chuẩn, hợp quy.

Việc xây dựng tiêu chuẩn kỹ thuật quốc gia còn nhằm mục đích làm căn cứ để triển khai hoạt động kiểm tra, đánh giá, kiểm định an toàn thông tin cho các sản phẩm an toàn thông tin của Việt Nam và các sản phẩm an toàn thông tin quốc tế thương mại tại Việt Nam sẽ mang lại nhiều lợi ích to lớn. Ngoài việc góp phần vào việc đầu tư, phát triển đúng các sản phẩm an toàn thông tin cần thiết, nâng cao hình ảnh của tổ chức, thúc đẩy ra đời các sản phẩm an toàn thông tin có mức độ bảo mật cao, thúc đẩy phát triển các dịch vụ công và thương mại điện tử.

Tại Chỉ thị 14/CT-Ttg ngày 25 tháng 05 năm 2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại quy định bảo đảm có giải pháp phòng, chống mã độc bảo vệ cho 100% máy chủ, máy trạm, thiết bị đầu cuối liên quan và có cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận dạng mã độc mới.

Tại Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ quy định, đối với các hệ thống thông tin cấp độ 1 phải có phương án phòng chống mã độc cho máy chủ, máy trạm.

Trên cơ sở đó, có thể thấy, việc xây dựng xây dựng tiêu chuẩn kỹ thuật quốc gia cho sản phẩm an toàn thông tin đóng góp một phần lớn vào việc thúc đẩy sự phát triển các sản phẩm, dịch vụ an toàn thông tin nói chung và tạo điều kiện cho các sản phẩm được ứng dụng rộng rãi với độ tin cậy cao, cần thiết phải xây dựng để đảm bảo hiệu lực thi hành của Luật an toàn thông tin mạng.

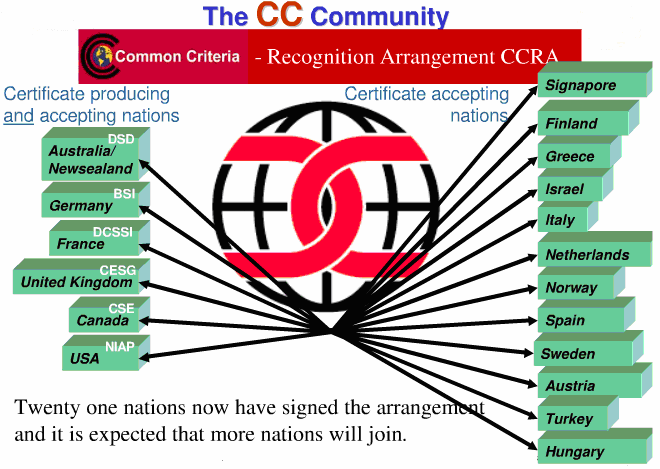
Mặc dù các tiêu chuẩn quốc tế về đánh giá sản phẩm CNTT theo tiêu chí chung ISO/IEC 15408 đã được công bố, song việc xác định các yêu cầu cụ thể cho từng loại sản phẩm CNTT còn gặp nhiều khó khăn. Một số nước như Mỹ, Trung Quốc,… đang xây dựng hoặc áp dụng các tiêu chuẩn đánh giá cho từng loại sản phẩm cụ thể như thiết bị phát hiện, chống tấn công xâm nhập, thiết bị mạng riêng ảo, thiết bị tường lửa,… Do vậy, Việt Nam cần nghiên cứu và lựa chọn, áp dụng tiêu chuẩn phù hợp phục vụ các mục tiêu quản lý của cơ quan quản lý nhà nước và doanh nghiệp.

1. Tình hình tiêu chuẩn hóa
   1. Thế giới

Việc đầu tư các giải pháp nhằm đảm bảo ATTT được tất cả các tổ chức quan tâm, tuy nhiên lựa chọn sản phẩm nào có thể đáp ứng được các yêu cầu của tổ chức luôn là vấn đề làm đau đầu các nhà quản lý về ATTT. Tương tự như vậy các nhà phát triển để có thể đưa các sản phẩm của mình đến khách hàng, họ cũng rất quan tâm đến việc làm thế nào để chứng minh các sản phẩm của mình đáp ứng được các yêu cầu của khách hàng. Một thành phần nữa để có thể kết nối giữa nhà phát triển và người dùng là các tổ chức đánh giá, làm thế nào để một sản phẩm khi được đánh giá bởi một phòng thí nghiệm sẽ được cả người sử dụng công nhận trên thế giới. Để hướng tới mục tiêu này này nhiều nước phát triển đã cùng nhau hợp tác để đưa ra một bộ tiêu chí chung (Common Criteria) để phục vụ đánh giá an toàn thông tin cho sản phẩm và hệ thống CNTT, bộ tiêu chí chung này sau đó đã được Tổ chức tiêu chuẩn quốc tế ISO ban hành với tên là bộ tiêu chuẩn ISO/IEC 15408. Bộ tiêu chuẩn ISO/IEC 15408 gồm 3 tập bắt đầu được ban hành từ năm 1999, phiên bản thứ 2 được ban hành năm 2005 thay thế toàn bộ phiên bản đầu. Phiên bản thứ 3 được ban hành trong năm 2008 và 2009. Chính sự phát triển công nghệ, dịch vụ cũng như việc tăng khả năng triển khai áp dụng tiêu chuẩn vào thực tiến đã dẫn đến các cập nhật, sửa đổi, bổ sung trên của bộ tiêu chuẩn. Song song với việc ban hành bộ tiêu chuẩn ISO/IEC 15408, tổ chức ISO cũng đã ban hành tiêu chuẩn ISO/IEC 18045 về hệ thống các phương pháp đánh giá an toàn thông tin nhằm hỗ trợ việc triển khai ISO/IEC 15408.

Hiện nay trên thế giới đã có 16 nước đã xây dựng phòng thí nghiệm để đánh giá và chứng nhận cho các sản phẩm theo bộ tiêu chuẩn ISO/IEC 15408 gồm các nước Úc, Canada, Pháp, Đức, Ý, Nhật, Malaixia, Hà Lan, New Zealand, Na Uy, Hàn Quốc, Tây Ba Nha, Thụy Điển, Thổ Nhĩ Kỳ, Anh, Mỹ và 10 nước chấp nhận sử dụng các kết quả đã được đánh giá bởi hơn 50 phòng thí nghiệm chuẩn tại các quốc gia trên. 26 nước trên đã tham gia ký hiệp ước công nhận lẫn nhau do đó một sản phẩm đã được 1 phòng thí nghiệm trong hệ thống đánh giá và cấp chứng nhận thì sẽ được đồng ý bởi 26 nước trên. Trên trang web của tổ chức Common Criteria ta có thể thấy 1623 sản phẩm đã được chứng nhận, điều này cho thấy Bộ tiêu chuẩn này là rất cần thiết và được các nước phát triển rất quan tâm. Mục tiêu của việc tham gia tổ chức ICRA của các nước đều hướng tới đó là: Chuẩn hóa việc đánh giá các sản phẩm CNTT nhằm tăng cường sự tin cậy vào sự an toàn của các sản phẩm này; không bị đánh giá lặp lại với cùng một sản phẩm, khi một sản phẩm chỉ cần một nước chứng nhận, việc giảm chi phí thực hiện xây dựng các tài liệu PP và tiến trình chứng nhận cho các sản phẩm CNTT.

**Cộng đồng Thỏa thuận thừa nhận lẫn nhau về tiêu chí chung CCRA**



Hình – Quá trình hình thành cộng đồng CC (Common Criteria)

Thành viên CCRA hiện nay gồm 17 thành viên chủ chốt: ÚC, Canada, Pháp, Đức, Ấn độ, Ý, Nhật, Malaysia,Hà Lan, Newzealand, Nauy, Hàn Quốc, Tây ban nha, Thụy điển, Thổ Nhĩ kỳ, Anh, Mỹ và 11 thành viên chi phối: Áo, TIệp, Đan Mạch, Etiopia, Phần Lan, Hy lạp, Hungary, Israel, Quatar, Pakistan, Singapore (các tổ chức chứng nhận, các Bộ, các cơ quan quản lý, cơ quan về an toàn thông tin của các quốc gia).

Nguồn: <https://www.commoncriteriaportal.org/ccra/members/>

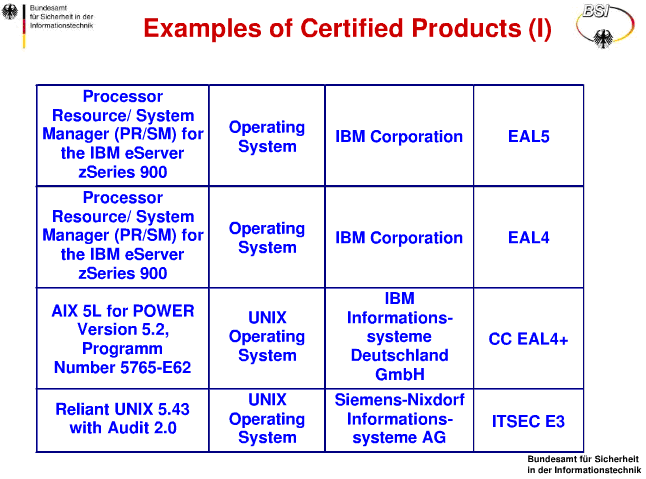
66 phòng lab được cấp phép bao gồm: Úc (02), Canada (04), Pháp (06), Đức (09), Ấn độ (01), Ý (06), Nhật (05), Malaysia (02), Hà lan (02), Nauy (04), Hàn Quốc (06), Tây Ban Nha (03),Thụy điển (02), Thổ Nhĩ Kỳ (05), Anh (02), Mỹ (09)

Nguồn: <https://www.commoncriteriaportal.org/labs/>

Trong hình sau đây là ví dụ về một báo cáo công nhận tuân thủ theo các tiêu chí chung trong chuẩn ISO/IEC 15408 cho một thiết bị Server.



**Hình**  – Ví dụ về một báo cáo công nhân tuân thủ



**Hình**  – Ví dụ về các sản phẩm đã được đánh giá và xác nhận

a) Mô hình triển khai áp dụng ISO/IEC 15408 của Mỹ

Tại Mỹ, Viện Quốc gia về Tiêu chuẩn và Công nghệ (NIST) và Cơ quan An ninh Quốc gia (NSA) đã phối hợp xây dựng một chương trình National Information Assurance Partnership NIPA, chương trình này được biết dưới tên NIPA Common Criteria Evaluation and Validation Scheme (NIPA/CCEVS). Chương trình NIPA/CCEVS có mục tiêu thúc đẩy phát triển xây dựng các tiêu chuẩn và tổ chức giám sát và đánh giá nhằm đảm bảo rằng các phương pháp đánh giá này nhất quán đối với các sản phẩm, giúp người mua lựa chọn được sản phẩm CNTT đáp ứng các yêu cầu về đảm bảo an toàn của mình và để giúp các nhà phát triển đưa ra các những sản phẩm được chấp nhận trên thị trường toàn cầu.

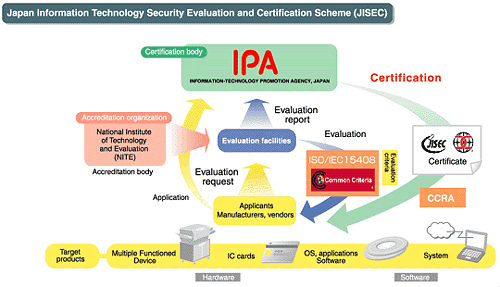
Các mục tiêu của NIPA là:

* Đáp ứng nhu cầu của chính phủ và ngành công nghiệp trong việc đánh giá an toàn thông tin của các sản phẩm nhằm đưa ra được sản phẩm đáp ứng yêu cầu của xã hội;
* Khuyến khích hình thành các phòng thí nghiệm kiểm tra an toàn thông tin nhằm mục đích thương mại và thúc đẩy phát triển của một ngành công nghiệp đánh giá an toàn thông tin trong lĩnh vực tư nhân.;
* Đảm bảo rằng các sản phẩm được đánh giá bởi các phòng thí nghiệm này là phù hợp tiêu chuẩn;
* Cải thiện tính sẵn sàng của các sản phẩm CNTT; nghĩa là các sản phẩm được đánh giá có thể nhanh chóng chứng minh rằng mình đạt các tiêu chí an toàn được yêu cầu;
* Mục tiêu lâu dài của NIPA là tăng cường sự tin tưởng của người dùng đối với các sản phẩm CNTT, hệ thống thông tin thông qua các chứng nhận đánh giá tiêu chuẩn an toàn của các sản phẩm.
* Thúc đẩy phát triển và sử dụng các đánh giá và chứng nhận đánh giá cho các sản phẩm và hệ thống CNTT;
* Thúc đẩy sự phát triển và sử dụng các bộ tiêu chuẩn quốc gia và quốc tế về an toàn CNTT;
* Khuyến khích các nghiên cứu và phát triển trong lĩnh vực an toàn, bảo mật, nghiên cứu thử nghiệm các giải pháp, xây dựng công cụ, giải pháp kỹ thuật liên quan đến đảm bảo ATTT;
* Hỗ trợ phát triển mạng lưới các quốc gia và tổ chức tham gia vào một hiệp ước chung trong công nhận và chấp nhận các kết quả đánh giá an toàn;
* Tạo điều kiện thuận lợi cho sự phát triển và tăng trưởng của ngành công nghiệp ATTT.

b) Mô hình triển khai áp dụng ISO/IEC 15408 của Nhật Bản

Nhật Bản đã là thành viên của Common Criteria Recognition Arrangement (CCRA) từ năm 2008. Ở Nhật, Cục thúc đẩy CNTT (IPA) là tổ chức có trách nhiệm xây dựng các tài liệu, tổ chức đánh giá và đưa ra khuyến nghị áp dụng ISO/IEC 15408 cho cơ quan nhà nước.

Dựa vào tiêu chuẩn ISO/IEC 15408 Nhật Bản đã đưa ra tiêu chuẩn cho mình là bộ tiêu chuẩn JIS X 5070 đưa vào áp dụng lần đầu vào năm 2001. Viện Công nghệ và đánh giá ITE (National Institute of Technology and Evaluation) đã cho phép hai tổ chức được cấp chứng nhận dựa trên tiêu chuẩn ISO/IEC 15408.



Hình 1: Mô hình của tổ chức áp dụng ISO/IEC 15408 ở Nhật Bản

Chương trình Đánh giá và chứng nhận an toàn CNTT (JISEC) được hình thành từ tháng 4 năm 2001, với mục đích để đánh giá các chức năng bảo mật và chất lượng trong sản phẩm và hệ thống CNTT. Cho đến nay nhiều thiết bị đã được đánh giá và cấp chứng nhận bởi chương trình này gồm các hệ quản trị cơ sở dữ liệu, tường lửa, cơ sở hạ tầng khóa công khai (PKI), hệ thống CNTT, thẻ thông minh, nhiều thiết bị điện tử khác (như máy ảnh, máy quay, máy photocopy..).

Trong tháng 10 năm 2003, Nhật Bản tham gia vào CCRA với tư cách là thành viên tham gia theo hình thức công nhận Tiêu chuẩn chung (CCRA) và trong năm 2011, Nhật Bản đã chính thức tham gia CCRA với tư cách là thành viên đầy đủ của tổ chức này với 2 phòng thí nghiệm chuẩn được công nhận bởi các nước thành viên của CCRA. Việc tham gia đầy đủ vào CCRA nhằm mục tiêu nâng cao hơn nữa khả năng cạnh tranh quốc tế của các sản phẩm CNTT Nhật Bản.

c) Mô hình triển khai áp dụng ISO/IEC 15408 của Singapore

Chương trình đánh giá và cấp chứng nhận của Singapore (Singapore Common Criteria evaluation and certification Scheme - SCCS) được thành lập vào năm 2005, và nằm dưới sự điều hành của Cục phát triển thông tin và truyền thông Singapore - IDA. chương trình này được thành lập để tổ chức thực hiện đánh giá đánh giá sản phẩm an toàn thông tin dựa theo tiêu chuẩn ISO/IEC 15408. Đây là một nội dung trong Quy hoạch an toàn thông tin và truyền thông Singapore và kế hoạch tổng thể để tăng cường an toàn mạng, góp phần nâng cao độ tin cậy của các sản phẩm CNTT Singapore để nâng cao tính cạnh tranh của các sản phẩm này và củng cố danh tiếng của Singapore như là một đất nước đáng tin cậy.

SCCS sẽ cung cấp các hỗ trợ cho các nhà sản xuất và các tổ chức muốn đánh giá các sản phẩm và hệ thống CNTT của mình, nhằm giảm chi phí và tăng tính hiệu quả của các hoạt động đánh giá cũng như cấp chứng nhận ATTT dựa trên các tiêu chí chung (CC) và bộ tiêu chuẩn (ISO/IEC 15408). Với tư cách thành viên trong CCRA thành viên Công nhận, nghĩa là Singapore sẽ chấp nhận tất cả các đánh giá và chứng nhận cho sản phẩm và hệ thống CNTT đã được các phòng thí nghiệm chuẩn của CCRA thực hiện.

Mục tiêu của SCCS bao gồm:

* Đảm bảo việc đánh giá các sản phẩm CNTT được thực hiện tiêu chuẩn quốc tế và được công nhận bởi cộng đồng quốc tế, nhằm giúp tạo lập niềm tin vào sự an toàn của các sản phẩm này;
* Cải thiện các tài liệu PP sẵn có nhờ bổ sung thêm các chức năng và yêu cầu an toàn nhằm tăng cường mức độ đảm bảo an toàn cho các sản phẩm;
* Loại bỏ sự lãng phí khi phải đánh giá nhiều lần với các sản phẩm đã được thực hiện bởi các phòng thí nghiệm chuẩn của CCRA;
* Tiếp tục nâng cao tính hiệu quả và tiết kiệm chi phí trong quá trình đánh giá và chứng nhận cho các sản phẩm và PP.

d) Một số tiêu chuẩn về đánh giá an toàn thông tin đã ban hành

* ISO/IEC 15408-1:2009 Information Technology - Security Techniques - Part 1: Evaluation Criteria for IT Security.
* ISO/IEC 15408-2:2009 Information Technology - Security Techniques - Evaluation Criteria for IT - Part 2: Security functional components.
* ISO/IEC 15408-3:2008 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3: Security assurance requirements.
* ISO/IEC 27006:2011 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.
* ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing.
* ISO/IEC TR 27008:2011 Information technology - Security techniques - Guidelines for auditors on information security controls.
* ISO 19011:2011 Guidelines for auditing management systems.
* ISO/IEC 18045:2008 Information technology - Security Techniques - Methodology for IT Security Evaluation.
* ISO/IEC TR 19791:2010 Information technology - Security Techniques - Security assessment of operational systems.
  1. Trong nước

Trong những năm gần đây, CNTT được áp dụng rộng rãi tại các doanh nghiệp, các cơ quan và tổ chức tại Việt nam. Hiện nay CNTT được ứng dụng rộng khắp trong nhiều công việc hàng ngày từ công tác quản lý, chỉ đạo, chuyên môn đến các hoạt động kinh doanh, giải trí. Song song với sự phát triển đáng mừng đó là thách thức cần đảm bảo an toàn thông tin cho các hệ thống, ứng dụng CNTT, việc đảm bảo an toàn cho các hệ thống đó không chỉ là trách nhiệm của chính các tổ chức đó mà nó còn cần vai trò trách nhiệm của các cơ quan chính phủ để có thể bảo vệ người dùng cũng như các lợi ích của quốc gia.

Nhiều cơ quan, tổ chức đã bắt đầu quan tâm đến đánh giá và cấp chứng nhận an toàn cho các hệ thống CNTT của mình. Nhu cầu này dẫn đến có khá nhiều các công ty, tổ chức và cá nhân tham gia vào lĩnh vực đánh giá an toàn thông tin. Tuy vậy việc đánh giá an toàn thông tin hiện nay chưa hề được cơ quan tổ chức nào giám sát cũng như không tuân thủ theo một tiêu chuẩn nào, do đó kết quả của đánh giá không thực sự tin cậy, nó chỉ là thỏa thuận song phương giữa đơn vị yêu cầu đánh giá và tổ chức thực hiện đánh giá, do đó các kết quả này không hề được công nhận bởi bất kỳ tổ chức thứ ba nào thế nên lợi ích đem lại từ việc đánh giá này không tương xứng với chi phí mà tổ chức cần đánh giá phải bỏ ra. Thậm chí trong một vài trường hợp, do khách hàng không có kiến thức về đánh giá an toàn thông tin nên nhiều tổ chức, cá nhân đánh giá thực hiện các công việc đánh giá tùy tiện hoặc tổ chức đánh giá không có kinh nghiệm và năng lực nên kết quả không đem lại một lợi ích nào cho tổ chức.

Tuy các cơ quan nhà nước đã có ý thức về đảm bảo an toàn thông tin, tuy nhiên việc thuê đánh giá an toàn thông tin cho hệ thống hiện tại chỉ là một khía cạnh trong bức tranh đảm bảo an toàn thông tin. Để có thể xây dựng một giải pháp tổng thể cho đảm bảo an toàn thông tin, việc quan tâm đến đảm bảo an toàn thông tin từ khâu đầu tư xây dựng hệ thống ban đầu là vô cùng quan trọng. Do hiện tại các cơ quan chức năng chưa đưa ra được các hướng dẫn cho lựa chọn các sản phẩm CNTT nào phù hợp với yêu cầu của tổ chức, nên các đơn vị hiện tại vẫn mua sắm theo tư vấn cũng như theo kinh nghiệm mà không theo một tiêu chí rõ ràng nào, điều này dẫn đến việc đảm bảo an toàn thông tin cho hệ thống theo yêu cầu là rất khó khăn.

Nhận thức được vấn đề này, Bộ Thông tin và Truyền thông đã xây dựng Bộ tiêu chuẩn về đánh giá an toàn thông tin cho các sản phẩm và hệ thống công nghệ thông tin và đã được ban hành thành bộ Tiêu chuẩn Việt Nam TCVN 8709:2011 trên cơ sở chấp nhận toàn bộ bộ tiêu chuẩn ISO/IEC 15408 phiên bản mới nhất. Bộ tiêu chuẩn này được xây dựng nhằm hướng đến mục tiêu trợ giúp cho các tổ chức khi đầu tư các sản phẩm CNTT của mình có sở cứ để xây dựng các tiêu chí để lựa chọn sản phẩm, giúp các nhà phát triển sản phẩm CNTT xây dựng các tài liệu ST cho sản phẩm của mình để sau khi được đánh giá bởi cơ quan chức năng (Các phòng thí nghiệm chuẩn) sẽ được công nhận bởi tất cả các tổ chức tại Việt Nam.

Trước tình hình an toàn thông tin phải đối mặt với nhiều thách thức, rủi ro, Việt Nam đã chú trọng xây dựng và ban hành hệ thống tiêu chuẩn liên quan đến an toàn thông tin. Các tiêu chuẩn đã và đang xây dựng tập trung vào 2 khía cạnh đó là quản lý và đánh giá an toàn thông tin.

Một số tiêu chuẩn đã được ban hành:

* TCVN 8709-1:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát.
* TCVN 8709-2:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn.
* TCVN 8709-3:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn.
* TCVN 11386:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống phương pháp đánh giá an toàn thông tin.
* TCVN 12820:2020 Công nghệ thông tin – Các kỹ thuật an toàn – Hồ sơ bảo vệ cho chức năng phòng chống xâm nhập trên thiết bị tường lửa/thiết bị mạng
* TCVN 12819:2020 Công nghệ thông tin – Các kỹ thuật an toàn – Hồ sơ bảo vệ cho thiết bị tường lửa lọc lưu lượng có trạng thái
* TCVN 12637:2019 Công nghệ thông tin - Các kỹ thuật an toàn - Hồ sơ bảo vệ cho trình duyệt Web
* TCVN 12821:2020 Công nghệ thông tin – Các kỹ thuật an toàn – Hồ sơ bảo vệ cho thiết bị lưu trữ di động
* TCVN 12822:2020 Công nghệ thông tin - Các kỹ thuật an toàn - Hồ sơ bảo vệ cho hệ quản trị cơ sở dữ liệu
* TCVN 13468:2022 Công nghệ thông tin - Các kỹ thuật an toàn - Hồ sơ bảo vệ cho phần mềm ứng dụng
  1. Hiện trạng sản phẩm phòng, chống mã độc trên thiết bị đầu cuối (AV)

Tại Việt Nam, Chính phủ cũng ngày càng quan tâm tới các thiết bị phần cứng, phần mềm an toàn thông tin nội địa nhằm tăng cường bảo đảm an toàn, an ninh mạng phục vụ chính phủ điện tử, đô thị thông minh và hệ thống thông tin quan trọng quốc gia.

Kể từ thời điểm Luật An toàn thông tin mạng với các quy định về quản lý, thúc đẩy doanh nghiệp, hoạt động kinh doanh trong lĩnh vực an toàn, an ninh mạng có hiệu lực tháng 7/2015 đã bước đầu định hình nên thị trường, doanh nghiệp an toàn thông tin mạng Việt Nam với sự tham gia của 89 doanh nghiệp đến thời điểm hiện tại. Hoạt động của doanh nghiệp đã chuyển dịch từ hướng tự phát, nhỏ lẻ sang chuyên nghiệp, phát triển đa dạng sản phẩm, dịch vụ, chất lượng về đội ngũ nhân sự và hệ thống trang thiết bị kỹ thuật.

Năm 2019, Bộ Thông tin và Truyền thông đã tham mưu Thủ tướng Chính phủ ban hành Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường đảm bảo an toàn, an ninh mạng, chỉ đạo, định hướng đối với việc thúc đẩy phát triển thị trường an toàn, an ninh mạng nội địa thông qua các cơ chế khuyến khích sản phẩm, dịch vụ nội địa, tăng tỷ lệ đầu tư cho an toàn, an ninh mạng. Chỉ thị 14/CT-TTg năm 2019 là yếu tố trực tiếp tác động và tạo sự chuyển mình mạnh mẽ của thị trường, doanh nghiệp an toàn, an ninh mạng, đặc biệt là Hệ sinh thái sản phẩm an toàn, an ninh mạng Việt Nam.

Tính đến tháng 11 năm 2020, Hệ sinh thái sản phẩm an toàn thông tin mạng Việt Nam hiện có 109 sản phẩm do các doanh nghiệp Việt Nam sản xuất và cung ứng ra thị trường, trong đó:

Sản phẩm nội địa đã có mặt tại **21/22** nhóm chủng loại (chiếm tỷ lệ **95,45%**), tăng **35,57%** so với năm 2019.

Sản phẩm an toàn cho thiết bị đầu cuối có 18 sản phẩm.

Sản phẩm an toàn lớp mạng có 34 sản phẩm.

Sản phẩm an toàn lớp ứng dụng có 15 sản phẩm.

Sản phẩm bảo vệ dữ liệu có 08 sản phẩm.

Nhóm giải pháp định hướng phát triển theo hình thức cung cấp dịch vụ có 34 sản phẩm.

Danh sách các sản phẩm Bảo vệ máy tính cá nhân/máy chủ (PC/Laptop/Server Security) do công ty Việt Nam phát triển hiện nay bao gồm:

|  |
| --- |
| 1. Viettel Endpoint Detection & Response (VCS-aJiant) 2. [CMC](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\2%20CMC\0%20CMC%20CompanyProfile_2019.pdf) - [Internet Security](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\2%20CMC\1%20CMC%20Internet%20Security.pdf) 3. CMC [Antivirus](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\2%20CMC\12%20CMC%20Antivirus.pdf) 4. CMC [CryptoShield](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\2%20CMC\5%20CryptoShield_DS.pdf) 5. CMC SOC [Endpoint Detection Response](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\2%20CMC\3%20EDR%20ENG.pdf) 6. CMC Malware Detection and Defence 7. [BKAV](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\1%20BKAV\Brochure%20Bkav.pdf) [Pro](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\1%20BKAV\4%20Bkav%20EDR.pdf) 8. BKAV [Endpoint SMB](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\1%20BKAV\4%20Bkav%20EDR.pdf) 9. [BKAV](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\1%20BKAV\Brochure%20Bkav.pdf) Endpoint AI 10. [CyRadar](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\4%20CyRadar\0%20Proposal_CyRadar%20Security.pdf) [Endpoint Detection & Response](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\4%20CyRadar\1%20Introduce_CyRadar%20EDR.pdf) 11. [Cty 129](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\16%20Công%20ty%20129\Giới%20thiệu%20Công%20ty%20TNHH%20một%20thành%20viên%20129%20-%20Ban%20Cơ%20yếu%20Chính%20phủ.pdf) - [BCY Endpoint Security](file:///C:\Users\DT_HOA\AppData\Roaming\OneDrive%20-%20Hanoi%20Thang%20Long%20Primary%20and%20Secondary%20School\WORK%20-%202021\PHAT%20TRIEN%20THI%20TRUONG\Documents\AIS@\1%20HĐ_SPATTT\HST%202020\16%20Công%20ty%20129\1%20BCY%20EDR.doc) 12. HSOC Agent 13. HPT GoldenBow (HSOC EDR) 14. Veramine Detection & Response Platform |

* Theo đó, hiện nay tại Việt Nam với sự góp mặt của 14 dòng sản phẩm bảo vệ thiết bị đầu cuối tiêu biểu từ các doanh nghiệp trong nước cho thấy sản phẩm phòng chống mã độc trên thiết bị đầu cuối được các doanh nghiệp trong nước ưu tiên phát triển.

1. Giới thiệu bộ tiêu chuẩn ISO/IEC 15408 và hồ sơ bảo vệ (PP)
   1. Bộ tiêu chuẩn ISO/IEC 15408

ISO/IEC 15408 được trình bày dưới dạng một tập hợp của ba phần riêng biệt song có liên quan mật thiết nhau, nhằm đưa ra bộ khung đánh giá chung và các tiêu chí đánh giá chung nhất cho đánh giá an toàn thông tin.

Phần 1 (ISO/IEC 15408–1) là phần giới thiệu và trình bày về mô hình tổng quát. Trong phần này có định nghĩa các khái niệm và nguyên tắc chung cho đánh giá an toàn CNTT, trình bày một mô hình tổng quát cho đánh giá, các cấu trúc biểu thị các mục tiêu an toàn CNTT, các cấu trúc lựa chọn và xác định các yêu cầu an toàn CNTT. Nội dung phần 1 đưa ra các thông tin cơ sở và mô hình tham chiếu khi đánh giá; hướng dẫn lập các đặc tả mức cao cho các sản phẩm và hệ thống; cấu trúc các hồ sơ bảo vệ và các tập đích an toàn, xây dựng các yêu cầu và các đặc tính an toàn cho các sản phẩm và hệ thống CNTT.

Phần 2 (ISO/IEC 15408-2) hướng dẫn lập báo cáo các yêu cầu chức năng an toàn cho các sản phẩm và hệ thống CNTT. Các yêu cầu chức năng an toàn được chuẩn hóa chung cho các sản phẩm và hệ thống CNTT và được biểu diễn trong một tập hợp các thành phần chức năng, các họ và các lớp. Phần 2 được dùng làm tham chiếu cho các tiêu chí đánh giá bắt buộc trong báo cáo về yêu cầu chức năng an toàn, để xác định xem một sản phẩm hay hệ thống CNTT có thỏa mãn các tiêu chí đánh giá đã nêu, các chức năng an toàn đã yêu cầu hay không.

Phần 3 (ISO/IEC 15408-3 hướng dẫn lập báo cáo cấp độ các yêu cầu đảm bảo an toàn cho các sản phẩm và hệ thống CNTT. Các tiêu chí đảm bảo an toàn được chuẩn hóa chung cho các sản phẩm và hệ thống CNTT và được biểu diễn dưới dạng một tập hợp các thành phần, các họ và các lớp trong một hồ sơ bảo vệ hoặc một tập đích an toàn. Phần 3 được dùng làm tham chiếu cho các tiêu chí đánh giá bắt buộc trong báo cáo về yêu cầu đảm bảo an toàn, để đánh giá cho các hồ sơ bảo vệ và các tập đích an toàn, xác định cấp độ đảm bảo an toàn cho một sản phẩm hay hệ thống CNTT trên cơ sở mức độ thỏa mãn các tiêu chí đánh giá đã nêu.

Như vậy, trong 3 phần của bộ tiêu chuẩn, phần 1 là phần tổng quan, trình bày mô hình tổng quát cho đánh giá an toàn thông tin; phần 2 và phần 3 là chi tiết các tiêu chí chung về chức năng an toàn và yêu cầu đảm bảo chung cho các sản phẩm và hệ thống CNTT. Để đạt được sự so sánh hiệu quả giữa các kết quả đánh giá, các đánh giá cần được thực hiện theo một khung của mô hình chính thức trong đó có các tiêu chí đánh giá chung. Điều này làm tăng thêm tính chính xác, nhất quán và khách quan của kết quả đánh giá.

* 1. Hồ sơ bảo vệ (PP)

a) Giới thiệu

Hồ sơ bảo vệ (PP) là tài liệu mẫu để xây dựng đích an toàn ST. Nó giúp nhà phát triển xây dựng hồ sơ cụ thể cho đối tượng cần được đánh giá, giúp người tiêu dùng định hướng vào một nhóm các yêu cầu an toàn và giúp nhà kiểm định dựa vào đó để đánh giá sản phẩm. Nếu đích an toàn ST được xây dựng cho một đối tượng cụ thể thì PP lại được xây dựng chung cho một loại đối tượng nào đó. PP mô tả các yêu cầu chung cho các TOE, bởi vậy nó thường do một nhóm người tiêu dùng hoặc một nhóm nhà phát triển sản phẩm viết. PP chứa một tập các yêu cầu an toàn hoặc từ bộ tiêu chuẩn, hoặc được xác định rõ, trong đó có chứa một cấp đảm bảo đánh giá (EAL).

**Sử dụng PP/ST**

PP là một phát biểu về một tập hợp chung các nhu cầu an toàn. Vì thế PP thường được sử dụng như là:

- yêu cầu của người tiêu dùng hoặc nhóm nguời tiêu dùng (chỉ mua một loại sản phẩm CNTT nào đó nếu nó đáp ứng PP);

- yêu cầu của cơ quan quản lý (chỉ cho phép sử dụng một loại sản phẩm CNTT nếu nó đáp ứng PP);

- yêu cầu của nhà phát triển sản phẩm CNTT (chỉ phát triển loại sản phẩm CNTT đáp ứng các yêu cầu PP).

Ghi chú:

- PP chỉ đặc tả về an toàn và không phải là một đặc tả an toàn chi tiết (những mô tả chi tiết về thuật toán, các cơ chế, các hoạt động chi tiết...)

- PP là một đặc tả của một kiểu sản phẩm CNTT, không phải là đặc tả của một sản phẩm đơn lẻ. Sử dụng ST sẽ tốt hơn trong trường hợp muốn đặc tả một sản phẩm đơn lẻ.

- PP được sử dụng như là "mẫu" của một ST. PP mô tả một tập hợp các nhu cầu của người sử dụng, trong khi một ST tuân thủ với PP đó mô tả một TOE thỏa mãn những nhu cầu đó.

- Một PP cũng có thể được sử dụng như là một mẫu cho một PP khác. Có nghĩa là một PP có thể tuyên bố tuân thủ các PP khác. Trường hợp này là hoàn toàn tương tự như trường hợp một ST so với một PP.

ISO 15408 không cho phép bất kỳ hình thức tuân thủ từng phần nào, vì vậy PP hoặc ST phải tuân thủ đầy đủ với các PP tham chiếu. Tuy nhiên, có hai kiểu tuân thủ ("chặt chẽ" và "có thể diễn giải") và kiểu tuân thủ nào sẽ được xác định bởi PP. Để thực hiện việc này, PP tuyên bố (trong phần Phát biểu tuân thủ PP) về những kiểu tuân thủ được phép cho ST. Tuân thủ chặt chẽ và tuân thủ có thể diễn giải được áp dụng riêng biệt cho mỗi PP, có nghĩa là một ST có thể tuân thủ chặt chẽ với một số PP và tuân thủ có thể diễn giải với một số PP khác. Một ST chỉ được phép tuân thủ với một PP theo phương thức diễn giải nếu PP này cho phép một cách rõ ràng điều này, trong khi một ST luôn có thể tuân thủ chặt chẽ với mọi PP.

Các PP được công bố sẽ thường yêu cầu tuân thủ có thể diễn giải. Điều này có nghĩa là các ST tuyên bố với PP này sẽ phải đưa ra một giải pháp cho các vấn đề an toàn chung đã nêu trong PP, song có thể thực hiện điều này theo cách tương đương hoặc chặt chẽ hơn cách đã mô tả trong PP. “Tương đương nhưng chặt chẽ hơn” về nguyên tắc có nghĩa là PP và ST có thể chứa các phát biểu khác hoàn toàn về các thực thể khác, sử dụng các khái niệm khác,... miễn là về tổng thể phải đạt được mức độ như nhau hoặc hạn chế hơn về TOE và mức độ như nhau hoặc ít hạn chế hơn về môi trường hoạt động của TOE.

b) Khung nội dung PP

Hồ sơ bảo vệ (PP) chứa một tập các yêu cầu an toàn hoặc từ bộ tiêu chuẩn, hoặc được xác định rõ ràng, trong đó có chứa một EAL (có thể được tăng thêm các thành phần đảm bảo bổ sung khác). PP cho phép biểu thị độc lập với thực thi các yêu cầu an toàn cho một tập các TOE thỏa mãn hoàn toàn một tập các mục tiêu an toàn. Mỗi PP cần có khả năng tái sử dụng và xác định rõ các yêu cầu TOE biết trước đó thỏa mãn các đối tượng đã xác định cả về mặt chức năng và về mặt bảo an. Mỗi PP cũng chứa các sở cứ thực tế cho các mục tiêu an toàn và các yêu cầu an toàn. Nội dung của PP được gồm các nội dung chính sau:

|  |  |
| --- | --- |
| 1 | Giới thiệu PP   * 1. Tham chiếu PP   2. Tổng quan TOE |
| 2 | Các tuyên bố tuân thủ   * 1. Tuyên bố tuân thủ CC   2. Tuyên bố PP   3. Sở cứ tuân thủ   4. Tường trình tuân thủ |
| 3 | Định nghĩa các vấn đề an toàn   * 1. Các đe dọa   2. Các chính sách an toàn về tổ chức   3. Các giả thiết |
| 4 | Các mục tiêu an toàn   * 1. Các mục tiêu an toàn cho TOE   2. Các mục tiêu an toàn cho môi trường hoạt động   3. Sở cứ các mục tiêu an toàn |
| 5 | Định nghĩa các thành phần mở rộng   * 1. Định nghĩa các thành phần mở rộng |
| 6 | Các yêu cầu an toàn   * 1. Các yêu cầu chức năng an toàn   2. Các yêu cầu đảm bảo an toàn TOE   3. Sở cứ các yêu cầu an toàn |

Mỗi PP có thể được phát triển bởi cộng đồng người dùng, các nhà phát triển sản phẩm CNTT hoặc các đối tác khác quan tâm đến việc xác định ra một tập các yêu cầu chung. Mỗi PP đem đến cho người dùng một phương tiện để tham chiếu đến một tập xác định cho các nhu cầu an toàn và các điều kiện đánh giá theo các yêu cầu này.

1. Phương pháp xây dựng tiêu chuẩn

Để đánh giá an toàn cho các sản phẩm phát hiện và phản hồi điểm cuối (EDR), các quốc gia, tổ chức (trong đó có tổ chức Common Criteria) đã xây dựng các bộ hồ sơ bảo vệ khác nhau. Các hồ sơ bảo vệ do các quốc gia, tổ chức tự phát triển sẽ có nhưng ưu điểm và hạn chế, đặc biệt, trong một số trường hợp, kết quả đánh gia, sự công nhận lẫn nhau hồ sơ bảo vệ là hữu hạn.

Qua tham khảo các hồ sơ bảo vệ, đối với sản phẩm phát hiện và phản hồi điểm cuối (EDR), hồ sơ bảo vệ “Protection Profile module for Endpoint Detection and Response (EDR)” của Hiệp hội đảm bảo thông tin quốc gia của Hoa Kỳ (NIAP), phiên bản 1.0, ngày 23/10/2020 là được chính thức công nhận bởi Common Criteria và cũng được nhiều nước trên thế giới sử dụng làm hồ sơ bảo vệ này phục vụ hoạt động đánh giá của mình, bao gồm: Mỹ, Anh, Úc, Canada, Thụy Điển,...

Trên cơ sở đó, để xây dựng hồ sơ bảo vệ cho sản phẩm phát hiện và phản hồi điểm cuối (EDR) và áp dụng tại Việt Nam, nhóm nghiên cứu lựa chọn “Protection Profile module for Endpoint Detection and Response (EDR)” của NIAP, phiên bản 1.0, ngày 23/10/2020 là tài liệu tham chiếu để xây dựng qua hình thức chấp nhận nguyên vẹn, chỉnh sửa một số nội dung cho phù hợp với Việt Nam.

1. Giới thiệu tiêu chuẩn tham chiếu (tiêu chuẩn gốc)

Hồ sơ bảo vệ hợp tác cho sản phẩm phát hiện và phản hồi điểm cuối (EDR) (Protection Profile module for Endpoint Detection and Response (EDR) phiên bản 1.0. được phát triển công khai bởi cộng đồng kỹ thuật quốc tế bao gồm: các nhà cung cấp sản phẩm, các phòng đo kiểm và được NIAP và CC chính thức sử dụng.

Link tài liệu: [PP-Module for Endpoint Detection and Response (EDR) (niap-ccevs.org)](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm)

Theo chính sách của CCRA, kết quả đánh giá theo các PP được xem xét, phê duyệt sẽ được công nhận lẫn nhau giữa các quốc gia tham gia CCRA.

Khung nội dung chính của hồ sơ bảo vệ này như sau:

|  |
| --- |
| 1 Introduction  1.1 Overview  1.2 Terms  1.2.1 Common Criteria Terms  1.2.2 Technical Terms  1.3 Compliant Targets of Evaluation  1.3.1 TOE Boundary  1.3.2 TOE Platform  1.4 Use Cases  2 Conformance Claims  3 Security Problem Description  3.1 Threats  3.2 Assumptions  3.3 Organizational Security Policies  4 Security Objectives  4.1 Security Objectives for the TOE  4.2 Security Objectives for the Operational Environment  4.3 Security Objectives Rationale  5 Security Requirements  5.1 App PP Security Functional Requirements Direction  5.1.1 Modified SFRs  5.2 TOE Security Functional Requirements  5.2.1 Security Audit (FAU)  5.2.2 Identification and Authentication (FIA)  5.2.3 Security Management (FMT)  5.2.4 Protection of the TSF (FPT)  5.2.5 Trusted Path/Channels (FTP)  5.3 TOE Security Functional Requirements Rationale  6 Consistency Rationale  6.1 Protection Profile for Application Software  6.1.1 Consistency of TOE Type  6.1.2 Consistency of Security Problem Definition  6.1.3 Consistency of Objectives  6.1.4 Consistency of Requirements  Appendix A - Optional SFRs  Appendix B - Selection-based SFRs  Appendix C - Objective SFRs  Appendix D - Extended Component Definitions  D.1 Background and Scope  D.2 Extended Component Definitions  Appendix E - Implicitly Satisfied Requirements  Appendix F - Bibliography  Appendix G - Acronyms |

1. Giới thiệu dự thảo tiêu chuẩn hồ sơ bảo vệ cho sản phẩm phát hiện và phản hồi điểm cuối (EDR)

Dự thảo tiêu chuẩn “Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin – Hồ sơ bảo vệ cho sản phẩm phát hiện và phản hồi điểm cuối (EDR)” gồm có 10 phần chính và 05 phụ lục, cấu trúc cụ thể như sau:

|  |
| --- |
| Lời nói đầu  1 Phạm vi áp dụng  2 Tài liệu viện dẫn  3 Thuật ngữ và định nghĩa  4 Ký hiệu và chữ viết tắt  5 Giới thiệu Hồ sơ bảo vệ  6 Các yêu cầu áp dụng  7 Mô tả các vấn đề an toàn  8 Các mục tiêu an toàn  9 Các yêu cầu bảo mật  10 Đặc điểm về tính nhất quán  Phụ lục A Các SFR tùy chọn  Phụ lục B SFR cơ sở được lựa chọn  Phụ lục C SFR mục tiêu  Phụ lục D Định nghĩa thành phần mở rộng  Phụ lục E Các yêu cầu đáp ứng hoàn toàn  Thư mục tài liệu tham khảo |

1. Kết luận

Nhu cầu đánh giá, kiểm định an toàn thông tin tại Việt Nam là rất lớn, xuất phát từ nhu cầu thực tế của các tổ chức mong muốn có cơ sở để lựa chọn các sản phẩm và hệ thống CNTT phù hợp với các yêu cầu chức năng và đảm bảo an toàn thông tin của tổ chức.

Đối với sản phẩm phát hiện và phản hồi điểm cuối (EDR), đây là thiết bị thuộc nhóm sản phẩm chống tấn công xâm nhập đã được quy định tại Luật an toàn thông tin mạng, việc thực hiện kiểm định đánh giá hợp chuẩn, hợp quy đối với các sản phẩm an toàn thông tin mạng là yêu cầu bắt buộc theo quy định tại Luật an toàn thông tin mạng.

Mặc dù các tiêu chuẩn quốc tế về đánh giá sản phẩm CNTT theo tiêu chí chung ISO/IEC 15408 đã được công bố, song việc xác định các yêu cầu cụ thể cho từng loại sản phẩm CNTT còn gặp nhiều khó khăn. Một số nước như Mỹ, Trung Quốc,… đang xây dựng hoặc áp dụng các tiêu chuẩn đánh giá cho sản phẩm phát hiện và phản hồi điểm cuối (EDR). Do vậy, việc xây dựng và áp dụng TCVN về “Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin – Hồ sơ bảo vệ cho sản phẩm phát hiện và phản hồi điểm cuối (EDR)” là hướng đi phù hợp xu thế quản lý của thế giới và các quy định pháp luật của Việt Nam.

1. Tài liệu tham khảo
2. Protection Profile module for Endpoint Detection and Response (EDR) v1.0
3. TCVN 8709-1:2011 (ISO/IEC 15408-1:2009) Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 1: Giới thiệu và mô hình tổng quát [CC1].
4. TCVN 8709-2:2011 (ISO/IEC 15408-2:2009) Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 2: Các thành phần chức năng an toàn [CC2].
5. TCVN 8709-3:2011 (ISO/IEC 15408-:2009) Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 3: Các thành phần đảm bảo an toàn [CC3].
6. Tiêu chí chung để đánh giá an toàn CNTT, Phương pháp đánh giá, CCMB-2012-09-004, Phiên bản 3.1, Sửa đổi 4, 9/ 2012 [CEM].
7. Các hoạt động đánh giá đối với tường lửa STF cPP, Phiên bản 1.0, 27/2/2015 [SD-FW].
8. Các hoạt động đánh giá đối với thiết bị mạng cPP, Phiên bản 1.0, 27/2/2015 [SD-ND].
9. CCMB-2012-09-001 *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model (Tiêu chí chung dùng đánh giá an toàn về công nghệ thông tin – Phần 1: Giới thiệu và các Mô hình chung)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.
10. CCMB-2012-09-002 *Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Components (Tiêu chí chung dùng đánh giá an toàn về công nghệ thông tin – Phần 2: Các thành phần chức năng an toàn)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.
11. CCMB-2012-09-003 *Common Criteria for Information Technology Security Evaluation - Part 3: Security Assuarance Components (Tiêu chí chung dùng đánh giá an toàn về công nghệ thông tin – Phần 3: Các thành phần đảm bảo an toàn)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.
12. CCMB-2012-09-004 *Common Evaluation Methodology for Information Technology Security - Evaluation Methodology (Phương pháp Đánh giá Chung dùng cho an toàn công nghệ thông tin – Phương pháp đánh giá)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.
13. Arranement on the Recognition of Common Criteria Certificates
14. <https://www.commoncriteriaportal.org>
15. <http://www.cse-cst.gc.ca/>
16. <http://www.ipa.go.jp/security/jisec/jisec_e/>
17. <http://www.niap-ccevs.org/>