PP-Module for Endpoint Detection and Response (EDR)

Version: 1.0

2020-02-02

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-02-02	Draft - first version released

Contents

1 Introduction

1.1 Overview

This Protection Profile (PP) Module describes the security functionality of Endpoint Detection and Response (EDR) systems in terms of CC, and defines functional and assurance requirements for such products. EDR is enterprise management software that collects endpoint host data to detect potentially unauthorized activity on endpoints and to enable threat hunting and other incident response actions to remediate malicious behaviors. These requirements cover basic security characteristics and behaviors for EDR products; the platform on which the EDR runs may be a physical or virtual Operating System (OS), and on-premises or in a cloud environment.

EDR products rely on additional software running on the endpoint, called the Host Agent, to communicate commands or policy changes and to receive endpoint host data. Security requirements for the Host Agent are addressed in the separate [Host Agent] Module. Evaluation of an EDR system will require evaluations of different system components consisting of EDR and [Host Agent]. Each evaluation must satisfy the requirements in both the [MOD_EDR_V1.0] or [MOD_HA_V1.0] in addition its Base-PP [PP APP V1.3]. Evaluation of an EDR system will require multiple evaluations of different system components: one against this ESM EDR Module for the EDR and at least one other against the [Host Agent] Module with its base [AppPP].

There are two primary architectural categories addressed by requirements in this PP-Module, as seen in Figure 1.

- Endpoints communicate over the Internet to an EDR hosted by a cloud service provider (Software as a Service).
- Endpoints communicate with an on-premises EDR in a hub and spoke network model.

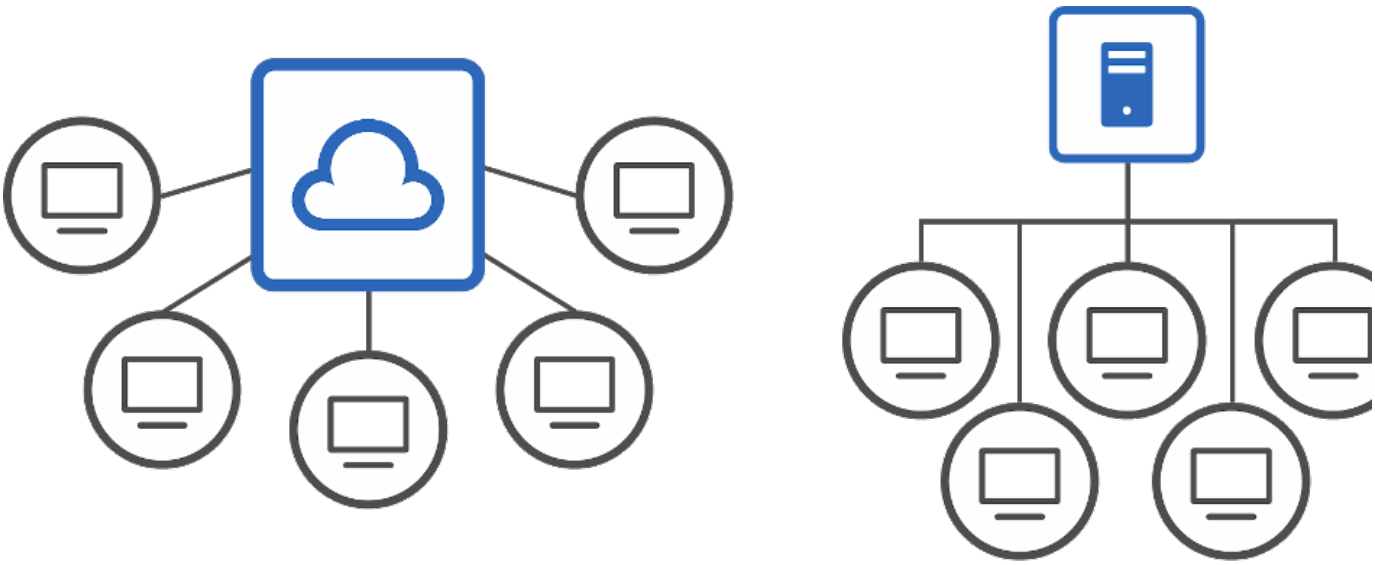

Figure 1: Primary EDR Architectures

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.

Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in a ST.
Target of Evaluation (TOE)	The product under evaluation.

1.2.2 Technical Terms

Alert	An event or notification on the management dashboard that highlights potentially unauthorized activity.
Endpoint	A computing device that runs a general purpose OS, a mobile device OS, or network device OS. Endpoints can include desktops, servers, and mobile devices.
Endpoint Detection and Response (EDR)	Server software that analyzes collected EDR Host Agent data for detecting, investigating, and remediating unauthorized activities on endpoints. The terms *TOE* and *EDR* are interchangeable in this document.
Endpoint Detection and Response System (EDR)	The EDR server and the Host Agents they operate with.
Enroll	The act of registering a HA endpoint with the EDR.
Host Agent	Complementary software that executes on endpoints to collect data about the endpoint and executes commands sent to the endpoint from an Enterprise Security Management (ESM) server or service. An example command sent to an endpoint could be to enforce a policy from an ESM, to collect some files, or to run an OS command.
Management Dashboard	A management interface for the configuration of EDR policy, visualization of collected endpoint alert data, and issuing of remediation commands.
Potentially Unauthorized Activity	This refers to the set of activities detected by the TOE, specific items detected may be unique to the TOE
SOC Analyst	Security Operations Center (SOC) Analyst is typically the person responsible for reviewing potentially unauthorized activities via alerts and performing remediation and clean up.

1.3 Compliant Targets of Evaluation

1.3.1 TOE Boundary

The TOE boundary for the EDR encompasses all the software from the TOE vendor that represents the server or enterprise management side of the EDR System. This will typically, but not always, be software running behind a web application or dashboard, and possibly with other software services running to send and receive data with a Host Agent. The EDR may also make use of a database to store collected and analyzed data. Any database software itself is outside the scope of the TOE, as is any web server software used to serve a web application or dashboard, and the underlying operating system or cloud platform. The figure below shows EDR (right) communicating with its Host Agent (left) over an untrusted network.
The requirements for the Host Agent are not covered in this Module, however it is expected that an ESM System will evaluate against this ESM EDR Module for the EDR and the [Host Agent] Module with its base [AppPP].

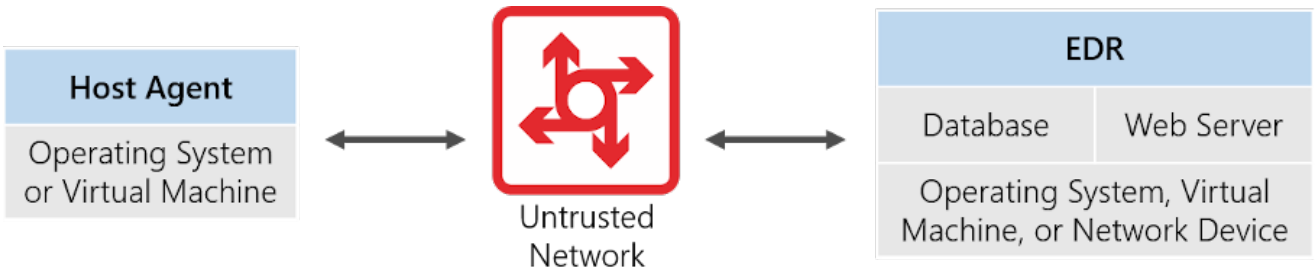

Figure 2: EDR and Host Agent Communications

1.3.2 TOE Platform

The TOE platform, which consists of the OS or Cloud platform on which the EDR software executes and is outside the scope of evaluation. However, the security of the EDR relies upon it.
Any communications with trusted remote file reputation or threat intelligence services is relevant to overall EDR System security but is also outside the scope of evaluation.

1.4 Use Cases

Requirements in this PP-Module are designed to address the security problems in at least the following use cases. An EDR's functionality may be extended by addons, plugins, threat feeds, or other reputation services. These are out of scope of this Module.

[USE CASE 1] Detection of Potential Unauthorized Activity

The detection of potentially unauthorized activity, software, or users is enabled by the collection of host-based endpoint data to a central EDR where the data is analyzed.

[USE CASE 2] Remediation of Malicious Activity

The ability to initiate remediation commands to attempt a clean up of detected malicious activity is a key use case of EDR.

[USE CASE 3] Discovery

The capability to effectively browse, query, and export aggregated host-based endpoint data enables a SOC analyst to discover adversaries in post-compromise scenarios.

2 Conformance Claims

Conformance Statement

This inherits exact conformance as required from the specified and as defined in the and addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

CC Conformance Claims

This is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [].

Package Claims

This is TLS Package Version 1.1 Conformant.

3 Security Problem Description

The security problem is described in terms of the threats that the EDR is expected to address, assumptions about the operational environment, and any organizational security policies that the EDR is expected to enforce.

3.1 Threats

T.MISCONFIGURATION

An attacker is a legitimate privileged user with access to change the configuration of the EDR's security capabilities. Attackers may attempt to hide malicious activities from other privileged users.

T.CREDENTIAL_REUSE

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may guess or harvest legitimate credentials from the EDR, endpoints, or insecure network activity.

3.2 Assumptions

These assumptions are made on the Operational Environment in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an Operational Environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

A.CONNECTIVITY

The EDR relies on network connectivity to carry out its management activities. The OE will provide reliable network connectivity for the EDR to operate. The EDR will robustly handle occasional instances when connectivity is unavailable or unreliable.

3.3 Organizational Security Policies

This PP-Module defines no additional organizational security policies beyond those defined in the Base-PP.

4 Security Objectives

4.1 Security Objectives for the TOE

O.MANAGEMENT

The TOE must facilitate management by the enterprise, providing consistent and supported interfaces for their security-relevant configuration, maintenance, and operation.

Addressed by: FAU_ALT_EXT.1, FAU_COL_EXT.1, FMT_SMF.1(1), FMT_SMF.1(2), FMT_SMR.1, FMT_SRF_EXT.1, FMT_TRM_EXT.1 (objective)

O.ACCOUNTABILITY

The TOE must provide logging facilities which record management actions undertaken by identified and authenticated management users.

Addressed by: FAU_GEN.1, FIA_PWD_EXT.1, FIA_AUT_EXT.1

O.PROTECTED_TRANSIT

To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOE s will use a trusted channel to protect all communications. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application or to unauthenticated users.

Addressed by: FCS_DTLSS_EXT.1 (from TLS Package), FCS_DTLSC_EXT.1 (from TLS Package), FCS_HTTPS_EXT.1 (from Base-PP), FCS_TLSC_EXT.1 (from TLS Package), FCS_TLSC_EXT.2 (from TLS Package), FCS_TLSS_EXT.1 (from TLS Package), FCS_TLSS_EXT.2 (from TLS Package), FTP_ITC.1, FTP_TRP.1

4.2 Security Objectives for the Operational Environment

The Operational Environment of the TOE implements technical and procedural measures to assist theTOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the Operational Environment consist of a set of statements describing the goals that the Operational Environment should achieve. This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3 are incorporated as security objectives for the environment. The following security objectives for the operational environment assist the EDR in correctly providing its security functionality. These track with the assumptions about the environment.

OE.RELIABLE_TRANSIT

Wired or wireless network traffic between theEDR and host agents will be consistently and always available unless specific in evaluation activity tests.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives.

Threat, Assumption, or OSP	Security Objectives	Rationale
T.MISCONFIGURATION	O.MANAGEMENT	The threat T.MISCONFIGURATION is countered by O.MANAGEMENT as this provides for management and audit of administrative activities.
T.CREDENTIAL_REUSE	O.PROTECTED_TRANSIT, O.PROTECTED_STORAGE	The threat T.CREDENTIAL_REUSE is countered by O.PROTECTED_TRANSIT as this provides for confidentiality of transmitted data. The threat T.CREDENTIAL_REUSE is countered by O.PROTECTED_STORAGE (from [AppPP]) as this provides for confidentiality of locally stored credentials.
A.CONNECTIVITY	OE.RELIABLE_TRANSIT	The Operational Environment objective OE.RELIABLE_TRANSIT is realized through A.CONNECTIVITY.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following notations are used:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1".

5.1 App PP Security Functional Requirements Direction

In a PP-Configuration that includes App PP, the TOE is expected to rely on some of the security functions implemented by the application as a whole and evaluated against the Base-PP. The SFRs listed in this section are defined in the Base-PP and relevant to the secure operation of the EDR. This section describes any modifications that the ST author must make to the Base-PP SFRs to satisfy the required EDR functionality.

5.1.1 Modified SFRs

This PP-Module does not modify any SFRs defined by the App PP.

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 Security Audit (FAU)

FAU_ALT_EXT.1 Server Alerts

FAU_ALT_EXT.1.1 The EDR shall alert authorized users on a management dashboard in the event of any of the following:

a. Change in Host Agent enrollment status
b. Detection of potentially unauthorized activity on enrolled endpoints

Application Note: The intent of this requirement is to specify the minimum set of management dashboard alert capabilities the EDR must be capable of displaying to an authorized user.

Examples of Detection of potentially unauthorized activity on enrolled endpoints include; anomalous activity, escalation of privileges, and lateral movement.

FAU_ALT_EXT.1.2 The EDR shall provide a visualization of detected alerts of potentially unauthorized incidents, and shall include:

a. An initial incident severity and [**selection**: *assessment*, *categorization*, *score*, *ranking*]
b. An incident timeline

Application Note: The intent of this requirement is to specify the minimum set of incident visualizations the EDR must be capable of displaying to an authorized user. Visualization is broadly defined as the display of incident data to an authorized user on the management dashboard. The visualization is not required to be interactive.

FAU_ALT_EXT.1.3 The EDR shall provide a data export capability for selected alerts with a specified standards-based format of [**selection**:

- *Structured Threat Information eXpression (STIX)*,
- *Cyber Observable eXpression (CybOX)*,
- *Incident Object Description Exchange Format (IODEF)*,
- *Common Event Format (CEF)*,
- *Log Event Extended Format (LEEF)*

].

Application Note: The intent of this requirement is to specify a selection of standards-based formats the EDR must provide for the export of selected alerts, at least one must be selected.

FAU_COL_EXT.1 Collected Endpoint Data

FAU_COL_EXT.1.1 The EDR shall collect the following minimum set of endpoint data from a Host Agent:

a. Operating System (OS) version, architecture, and IP Address
b. Privileged and unprivileged endpoint account login activity
c. Process creation
d. Libraries and modules loaded by processes
e. Filenames and [**assignment**: *other metadata*] of files created and [**assignment**: *other activities performed to files*]on persistent storage
f. [**assignment**: *Other host data*]

Application Note: The intent of this requirement is to specify the minimum set of endpoint data that the EDR must be capable of collecting. The assignments may be empty, a single item, or multiple items.

FAU_GEN.1 EDR Audit Generation

FAU_GEN.1.1 The EDR shall generate an audit record of the following auditable events:
- EDR management dashboard login activity
- Remediation commands sent to a Host Agent, affected endpoint, or network devices
- EDR configuration changes
- [**assignment**: *Other auditable events*]

Application Note: The intent of this requirement is to specify the minimum set of audit records generated about actions on the EDR.

FAU_GEN.1.2 The EDR shall record within each audit record at least the following information:
- date and time of the event
- type of event
- subject identity
- (if relevant) the outcome (success or failure) of the event
- [**assignment**: *other audit relevant information*].

Application Note: This requirement outlines the information to be included in audit records. All audits must contain at least the information mentioned in FAU_GEN.1.2, but may contain more information which can be assigned.

5.2.2 Identification and Authentication (FIA)

FIA_PWD_EXT.1 Password Authentication

FIA_PWD_EXT.1.1 The EDR shall support the following for the Password Authentication Factor:

1. Passwords shall be able to be composed of any combination of [**selection**: *upper and lower case letters*, *[**assignment**: a character set of at least 52 characters]*], numbers, and special characters: [**selection**: *"!"*, *"@"*, *"#"*, *"$"*, *"%"*, *"^"*, *"&"*, *"*"*, *"("*, *")"*, *[**assignment**: other characters]*]
2. Password length up to [**assignment**: *an integer greater than or equal to 64*] characters shall be supported.

Application Note: The ST author selects the character set: either the upper and lower case Basic Latin letters or another assigned character set containing at least 52 characters. The assigned character set must be well defined: either according to an international encoding standard (such as Unicode) or defined in the assignment by the ST author. The ST author also selects the special characters that are supported by TOE they may optionally list additional special characters supported using the assignment.

FIA_AUT_EXT.1 Dashboard Authentication Mechanisms

FIA_AUT_EXT.1.1 The EDR shall [**selection**:
- *leverage the platform for authentication*,
- *provide the following authentication mechanisms, authentication based on username and password and [**selection**:*
  - *authentication with external Smartcard and PIN,*
  - *invocation of platform-provided functionality,*
  - *no other factors*

  ]

] to support logins to any management dashboard orAPI.

Application Note: The selection specifies if Smartcards are also supported, one selection must be made.

5.2.3 Security Management (FMT)

FMT_SMF.1/HOST Specification of Management Functions (EDR Management of Host Agent)

FMT_SMF.1.1/HOST The EDR shall be capable of performing the following functions that control behavior of the Host Agent:

Management Function	Administrator	SOC Analyst	Read-Only User

Configure the time frame for sending Host Agent data to the EDR [**assignment**: *list of configurable time frames*]	X	O	-
Assign a label or tag to categorize or group individual endpoint systems	X	O	-

Application Note: This requirement captures all the configuration functionality the EDR provides the administrator to configure the EDR Host Agents.

Chart legend: X = Mandatory, O = Optional, - = N/A

FMT_SMF.1/ENDPOINT Specification of Management Functions (EDR Management of EDR)

FMT_SMF.1.1/ENDPOINT The EDR shall be capable of performing the following management functions:

Management Function	Administrator	SOC Analyst	Read-Only User
Configure the amount of time to retain data collected by the EDR [**assignment**: *time frame to retain data*]	X	O	-
Obtain or display the connectivity status of a Host Agent	X	O	O
Define a configurable blacklist of [**selection**: *filenames*, *folders*, *file hashes*, [***assignment**: other factors*]]	O	X	-
Configure visual suppression of incident alerts based on a configurable blacklist of [**selection**: *filenames*, *folders*, *file hashes*, [***assignment**: other factors*]]	O	X	-

Application Note: This requirement captures all the configuration functionality the TSF provides the administrator to configure the EDR.

Chart legend: X = Mandatory, O = Optional, - = N/A

FMT_SMR.1 Security Management Roles

FMT_SMR.1.1 The EDR shall maintain the roles of administrator, SOC analyst, read-only user.

Application Note: The EDR will be configured, maintained, and used by different user roles. At a minimum, one administrative role shall be supported, one SOC analyst who can issue remediation commands to host agents, and one read-only user who can only view data. The user accounts need not be named literally, but they must have the implication of such roles.

FMT_SRF_EXT.1 Specification of Remediation Functions

FMT_SRF_EXT.1.1 The EDR shall be capable of performing the following remediation functions:

Management Function	Administrator	SOC Analyst	User
Quarantine an endpoint by [**selection**: *logically quarantining the endpoint from the network unless whitelisted*, *quarantining the malicious file on the endpoint*]	O	X	-
Terminate a running process on an endpoint	O	X	-
Retrieve potentially unauthorized or affected files from an endpoint	O	O	-

Application Note: This requirement captures all the remediation functionality the EDR provides the SOC Analyst and optionally the Administrator.

Logically quarantine from the network refers to restricting communications from the endpoint to the rest of the network, it may include a restricted whitelist.

Chart legend: X = Mandatory, O = Optional, - = N/A

5.2.4 Trusted Path/Channels (FTP)

FTP_ITC.1 Trusted Channel (Host Agent)

FTP_ITC.1.1 The [**selection**:

- *EDR shall use [**selection**: TLS as defined in the TLS Package, HTTPS as defined in the*

Base-PP] ,
- *EDR shall leverage the platform for [**selection**: TLS, HTTPS]*

] to provide a trusted communication channel between itself and another trusted IT product that is logically distinct from other communication channels, provides assured identification of its endpoints, protects channel data from disclosure, and detects modification of the channel data.

Application Note: The intent of the above requirement is to use the cryptographic protocols identified in the requirement to establish and maintain a trusted channel between the EDR and the Host Agent. Only TLS or HTTPS can be used in this trusted channel.

This requirement is to ensure that the transmission of any logs, process lists, system information, etc, when commanded, or at configurable intervals, is properly protected. This trusted channel also protects any commands and policies sent by the EDR to the Host Agent. Either the Host Agent or the EDR System is able to initiate the connection.

This trusted channel protects both the connection between an enrolled Host Agent and the EDR and the connection between an unenrolled Host Agent and the EDR during the enrollment operation. Different protocols can be used for these two connections, and the description in the TSS should make this difference clear.

The trusted channel uses TLS, or HTTPS as the protocol that preserves the confidentiality and integrity of EDR communications. The ST author chooses the mechanism or mechanisms supported by the EDR, and then ensures the correct requirements are included the ST if not already present. Protocol, RBG, Certificate validation, algorithm, and similar services may be met with platform provided services.

FTP_ITC.1.2 The [**selection**: *EDR shall*, *EDR shall leverage the platform to*] provide functionality to permit the EDR and Host Agent to initiate communication via the trusted channel.

FTP_ITC.1.3 The [**selection**: *EDR shall*, *EDR shall leverage the platform to*] provide functionality to initiate communication via the trusted channel for [**assignment**: *list of service for which the EDR is able to initiate communications*]

FTP_TRP.1 Trusted Path (for Remote Administration)

FTP_TRP.1.1 **Refinement:**The [**selection**:
- *EDR shall use [**selection**: TLS as defined in the TLS Package, HTTPS as defined in the Base-PP]* ,
- *EDR shall leverage the platform for [**selection**: TLS, HTTPS]*

] to provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths, provides assured identification of its endpoints, and protects the communicated data from modification and disclosure.

FTP_TRP.1.2 **Refinement:** The [**selection**: *EDR shall*, *EDR shall leverage the platform to*] permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3 **Refinement:** The [**selection**: *EDR shall*, *EDR shall leverage the platform to*] require the use of the trusted path for all remote administration actions.

Application Note: This requirement ensures that authorized remote administrators initiate all communication with the EDR via a trusted path, and that all communications with the EDR by remote administrators is performed over this path. The data passed in this trusted communication channel are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the EDR.

6 Consistency Rationale

6.1 Application Software Protection Profile

6.1.1 Consistency of TOE Type

If this PP-Module is used to extend the Application SoftwarePP, the TOE type for the overall TOE is still a software-based application. The TOE boundary is simply extended to include the EDR functionality that is built into the application so that additional security functionality is claimed within the scope of the TOE.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the App PP as follows:

PP-Module Threat	Consistency Rationale
T.MISCONFIGURATION	This threat applies to management functionality that is introduced in thisPP-Module and does not affect the functionality described by the Base-PP.
T.CREDENTIAL_REUSE	This threat applies to authentication functionality that is introduced in thisPP-Module and does not affect the functionality described by the Base-PP.

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the App PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.MANAGEMENT	This objective extends the Base-PP's O.MANAGEMENT objective by supporting the management functions that are specific to the EDR TOE type.
O.ACCOUNTABILITY	This objective relates to the ability of theTOE to identify and authenticate users, and to record the behavior of these users. The Base-PP does not define an authentication mechanism so this objective does not affect the enforcement of the Base-PP's SFRs.
O.PROTECTED_TRANSIT	This objective extends the Base-PP's O.COMMS objective by ensuring that the communications related to the EDR and enrolled Host Agents are secured in the same manner as other sensitive data.

This PP-Module does not define any objectives for theTOE's operational environment. The objectives for the TOE's Operational Environment are consistent with the App PP based on the following rationale:

PP-Module Operational Environment Objective	Consistency Rationale
OE.RELIABLE_TRANSIT	This objective relates to an external interface that does not exist in the Base-PP and does not affect Base-PP functionality.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the App PP that are needed to support Endpoint Detection and Response (EDR) functionality. This is considered to be consistent because the functionality provided by the App is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the App PP as well as new SFRs that are used entirely to provide functionality for Endpoint Detection and Response (EDR). The rationale for why this does not conflict with the claims defined by the App PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
This PP-Module does not modify any requirements when the App PP is the base.	
Mandatory SFRs	
FAU_ALT_EXT.1	This SFR defines auditable alerts for the EDR. It does not impact the [AppPP] functionality.
FAU_COL_EXT.1	This SFR defines the minimum event data that theEDR collects from a Host Agent. It does not impact the [AppPP] functionality.
FAU_GEN.1	This SFR defines the minimum event data that theEDR server must record about authorized management dashboard activity. It does not impact the [AppPP] functionality.
FIA_PWD_EXT.1	This SFR defines specific authentication criteria for passwords. It does not impact the [AppPP] functionality.
FIA_AUT_EXT.1	This SFR defines authentication mechanisms for the EDR. It does not impact the [AppPP] functionality.

FMT_SMF.1/HOST	This SFR defines a specific set of management functions for an Host Agent by an EDR. It does not impact the [AppPP] functionality.
FMT_SMF.1/ENDPOINT	This SFR defines a specific set of management functions for an EDR by an EDR. It does not impact the [AppPP] functionality.
FMT_SMR.1	This SFR defines a specific set of management roles for anEDR. It does not impact the [AppPP] functionality.
FMT_SRF_EXT.1	This SFR defines a specific set of remediation functions for an EDR. It does not impact the [AppPP] functionality.
FTP_ITC.1	This SFR defines a specific set of functions for logically distinct secure communication with a Host Agent. It does not impact the [AppPP] functionality.
FTP_TRP.1	This SFR defines a specific set of functions for secure remote administration of the EDR. It does not impact [AppPP] functionality.
Optional SFRs	
This PP-Module does not define any optional requirements.	
Selection-based SFRs	
This PP-Module does not define any selection-based requirements.	
Objective SFRs	
FMT_TRM_EXT.1	This SFR defines protections for the integrity of commands sent to the Host Agent. It does not impact the [AppPP] functionality.

Appendix A - Optional SFRs

This PP-Module does not define any optional SFRs.

Appendix B - Selection-based SFRs

This PP-Module does not define any selection-based SFRs.

Appendix C - Objective SFRs

This section is reserved for requirements that are not currently prescribed by this PP-Module but are expected to be included in future versions of the PP-Module. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met.

FMT_TRM_EXT.1 Trusted Remediation Functions

FMT_TRM_EXT.1.1	The EDR shall digitally sign commands and policies sent to the Host Agent in accordance with FCS_COP.1.1(3).
	Application Note: The intent of this requirement is to cryptographically tie any policy updates or commends sent to the Host Agent as being from the EDR. This is not to protect the policies in transit as they are already protected by FTP_DIT_EXT.1.1. The digital signature used to sign policies or commands must be selected in FCS_COP.1.1(3). The use of this requirement makes FCS_COP.1.1(3) from the Base-PP a mandatory requirement.

Appendix D - Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

D.1 Background and Scope

This appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

Functional Class	Functional Components
Security Audit (FAU)	FAU_ALT_EXT Server Alerts FAU_COL_EXT Collected Endpoint Data
Identification and Authentication (FIA)	FIA_PWD_EXT Password Authentication FIA_AUT_EXT Dashboard Authentication Mechanisms
Security Management (FMT)	FMT_SRF_EXT Specification of Remediation Functions
Security Management (FMT)	FMT_TRM_EXT Trusted Remediation Functions

D.2 Extended Component Definitions

FAU_ALT_EXT Server Alerts

Components in this family define requirements for system activity that causes theTSF to generate an alert of the activity and for the contents of these alerts.

Component Leveling

FAU_ALT_EXT.1, Server Alerts, describes alert triggers and the information contained in alerts.

Management: FAU_ALT_EXT.1

The following actions could be considered for the management functions in FMT:

- Configure visual suppression of alerts.

Audit: FAU_ALT_EXT.1

There are no auditable events foreseen.

FAU_ALT_EXT.1 Server Alerts

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_ALT_EXT.1.1

The EDR shall alert authorized users on a management dashboard in the event of any of the following:

a. Change in Host Agent enrollment status
b. Detection of potentially unauthorized activity on enrolled endpoints

FAU_ALT_EXT.1.2

The EDR shall provide a visualization of detected alerts of potentially unauthorized incidents, and shall include:

a. An initial incident severity and [**selection**: *assessment*, *categorization*, *score*, *ranking*]
b. An incident timeline

FAU_ALT_EXT.1.3

The EDR shall provide a data export capability for selected alerts with a specified standards-based format of [**selection**:

- *Structured Threat Information eXpression (STIX)*,
- *Cyber Observable eXpression (CybOX)*,
- *Incident Object Description Exchange Format (IODEF)*,
- *Common Event Format (CEF)*,
- *Log Event Extended Format (LEEF)*

].

FAU_COL_EXT Collected Endpoint Data

Components in this family define requirements for the data that is collected from a Host Agent.

Component Leveling

FAU_COL_EXT.1, Collected Endpoint Data, identifies the specific data collected from a Host Agent.

Management: FAU_COL_EXT.1

The following actions could be considered for the management functions in FMT:

- Configuration of the time period for transmission of collected data.
- Configuration of label or tag information to associate collected data with individual endpoint systems or groups of systems.

Audit: FAU_COL_EXT.1

There are no auditable events foreseen.

FAU_COL_EXT.1 Collected Endpoint Data

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_COL_EXT.1.1

The EDR shall collect the following minimum set of endpoint data from a Host Agent:

a. Operating System (OS) version, architecture, and IP Address
b. Privileged and unprivileged endpoint account login activity
c. Process creation
d. Libraries and modules loaded by processes
e. Filenames and [**assignment**: *other metadata*] of files created and [**assignment**: *other activities performed to files*] on persistent storage
f. [**assignment**: *Other host data*]

FIA_PWD_EXT Password Authentication

Components in this family define requirements for password authentication criteria.

Component Leveling

FIA_PWD_EXT.1, Password Authentication, defines the length and character set requirements for password authentication factors.

Management: FIA_PWD_EXT.1

No specific management functions are identified.

Audit: FIA_PWD_EXT.1

There are no auditable events foreseen.

FIA_PWD_EXT.1 Password Authentication

Hierarchical to: No other components.

Dependencies to: FIA_AUT_EXT.1 Dashboard Authentication Mechanisms

FIA_PWD_EXT.1.1

The EDR shall support the following for the Password Authentication Factor:

1. Passwords shall be able to be composed of any combination of [**selection**: *upper and lower case letters*, *[**assignment**: a character set of at least 52 characters]*], numbers, and special characters: [**selection**: *"!"*, *"@"*, *"#"*, *"$"*, *"%"*, *"^"*, *"&"*, *"*"*, *"(", ")"*, *[**assignment**: other characters]*]
2. Password length up to [**assignment**: *an integer greater than or equal to 64*] characters shall be supported.

FIA_AUT_EXT Dashboard Authentication Mechanisms

Components in this family define requirements for authentication behavior that is unique to anEDR TOE.

Component Leveling

FIA_AUT_EXT.1, Dashboard Authentication Mechanisms, identifies the only authentication factors that may be used for authentication to a management interface of an EDR.

Management: FIA_AUT_EXT.1

No specific management functions are identified.

Audit: FIA_AUT_EXT.1

There are no auditable events foreseen.

FIA_AUT_EXT.1 Dashboard Authentication Mechanisms

Hierarchical to: No other components.

Dependencies to: No dependencies.

FIA_AUT_EXT.1.1

The EDR shall [**selection**:

- *leverage the platform for authentication*,
- *provide the following authentication mechanisms, authentication based on username and password and [**selection**:*
  - *authentication with external Smartcard and PIN,*
  - *invocation of platform-provided functionality,*
  - *no other factors*

  ]

] to support logins to any management dashboard orAPI.

FMT_SRF_EXT Specification of Remediation Functions

Components in this family define requirements for remediation functions that anEDR can perform to affect the behavior of an endpoint system.

Component Leveling

FMT_SRF_EXT.1, Specification of Remediation Functions, lists the supported remediation functions and identifies the management roles that may perform these functions.

Management: FMT_SRF_EXT.1

No specific management functions are identified.

Audit: FMT_SRF_EXT.1

There are no auditable events foreseen.

FMT_SRF_EXT.1 Specification of Remediation Functions

Hierarchical to: No other components.

Dependencies to: FMT_SMR.1 Security Management Roles

FMT_SRF_EXT.1.1

The EDR shall be capable of performing the following remediation functions:

Management Function	Administrator	SOC Analyst	User
Quarantine an endpoint by [**selection**: *logically quarantining the endpoint from the network unless whitelisted*, *quarantining the malicious file on the endpoint*]	O	X	-
Terminate a running process on an endpoint	O	X	-
Retrieve potentially unauthorized or affected files from an endpoint	O	O	-

FMT_TRM_EXT Trusted Remediation Functions

Components in this family define how theTOE can assert the authenticity of the remediation actions it requests from Host Agents.

Component Leveling

FMT_TRM_EXT.1, Trusted Remediation Functions, requires all management activities bound for a Host Agent to be digitally signed.

Management: FMT_TRM_EXT.1

No specific management functions are identified.

Audit: FMT_TRM_EXT.1

There are no auditable events foreseen.

FMT_TRM_EXT.1 Trusted Remediation Functions

Hierarchical to: No other components.

Dependencies to: No dependencies.

FMT_TRM_EXT.1.1

The EDR shall digitally sign commands and policies sent to the Host Agent in accordance with FCS_COP.1.1(3).

Appendix E - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.
[AppPP]	Protection Profile for Application Software
[Host Agent]	Module for ESM Host Agent, Version 1.0, July 2019

Appendix F - Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ASLR	Address Space Layout Randomization
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CMC	Certificate Management over CMS
CMS	Cryptographic Message Syntax
CN	Common Names
CRL	Certificate Revocation List
CSA	Computer Security Act
DEP	Data Execution Prevention
DES	Data Encryption Standard
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
DSS	Digital Signature Standard
DSS	Digital Signature Standard
DT	Date/Time Vector
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EDR	Endpoint Detection and Response
EDR	Endpoint Detection and Response System
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NFC	Near Field Communication

NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMB	Office of Management and Budget
OS	Operating System
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PP	Protection Profile
PP	Protection Profile
PP-Module	Protection Profile Module
RBG	Random Bit Generator
RFC	Request for Comment
RNG	Random Number Generator
RNGVS	Random Number Generator Validation System
S/MIME	Secure/Multi-purpose Internet Mail Extensions
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
ST	Security Target
SWID	Software Identification
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
XCCDF	eXtensible Configuration Checklist Description Format
XOR	Exclusive Or