Mapping Between
PP-Module for Endpoint Detection and Response (EDR), Version 1.0, 2020-10-23
and
NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.

- **SI-4.** The primary purpose of an EDR product is to monitor the activity of the system on which is installed, in support of SI-4, and to respond when anomalous, potentially malicious, or other significant activity is detected, in support of SI-4(5) and SI-4(7). Any other security controls an EDR product helps to satisfy is in support of that over-arching purpose (i.e. the security requirements are intended to ensure that enforcement of SI-4 and relevant sub-controls cannot be subverted).

- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.

- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

- **PP-Module.** A TOE that conforms to this PP-Module will also conform to the Protection Profile for Application Software (App PP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to that PP. This PP-Module refines some of the App PP requirements to ensure consistency between the PP and the PP-Module, but this does not affect the security controls that satisfying those requirements is intended to address.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
TOE Security Functional Requirements				
FAU_ALT_EXT.1	**Server Alerts**	SI-4(5)	**System Monitoring:** System-Generated Events	A conformant TOE has the ability to alert a user of the detection of potentially unauthorized activity on enrolled endpoints.
		SI-4(7)	**System Monitoring:** Automated Response to Suspicious Events	A conformant TOE supports part (a) of this control by automatically generating alerts when suspicious events are detected.
FAU_COL_EXT.1	**Collected Endpoint Data**	SI-4(23)	**System Monitoring:** Host-Based Devices	A conformant TOE may support this control by acting as a host-based device that monitors the behavior of the host and collects information about it. The extent to which this control is supported depends on the overlap between the data the TOE is capable of collecting and the specific host-based monitoring mechanisms the organization claims in the control assignment.
FAU_GEN.1/EDR	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to generate audit logs. The TOE supports the enforcement of parts (a) and (c) of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing. Part (b) is not satisfied by a conformant TOE because the PP does not define functionality to suppress or enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FIA_AUT_EXT.1	**Dashboard Authentication Mechanisms**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE supports this control by requiring user authentication to access its management interface. Note that the TOE may rely on platform-provided authentication rather than providing its own separate mechanism for this.
FIA_PWD_EXT.1	**Password Authentication**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to CNSS or DoD requirements or to those

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				specified in part (a) of this control.
FMT_SMF.1/ ENDPOINT	**Specification of Management Functions (EDR Management of EDR)**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMF.1/HOST	**Specification of Management Functions (EDR Management of Host Agent**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMR.1	**Security Management Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate users with roles, in support of part (a) of the control.
FMT_SRF_EXT.1	**Specification of Remediation Functions**	IR-4	**Incident Handling**	A conformant TOE may support part (a) of this control if the behavior reported by the TOE falls under 'incidents' and the actions taken in response to their detection is consistent with the organization's incident handling capability.
		SI-7	**Software, Firmware, and**	A conformant TOE may support part (b) of this control (depending on how

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
			Information Integrity	the assignment is completed) by implementing a mechanism to respond to potential malicious system activity (which would imply some unauthorized change to software, firmware, or information).
FPT_ITT.1	**Basic Internal TSF Data Transfer Protection**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between remote distributed TOE components.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of the TOE.
FTP_TRP.1	**Trusted Path**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of the TOE.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
Optional Requirements				
This PP-Module has no optional requirements.				
Selection-Based Requirements				
This PP-Module has no selection-based requirements.				
Objective Requirements				
FMT_TRM_EXT.1	**Trusted Remediation Functions**	AU-10	**Non-Repudiation**	A conformant TOE supports this control by having a means to assert itself as the originator of policy information. Note that the TOE itself may provide the digital signature function itself or it may rely on its platform to perform this.
		SC-13	**Cryptographic Protection**	A conformant TOE relies on digital signatures to assert the authenticity and integrity of commands and policies sent to the Host

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				Agent. Note that the TOE itself may provide the digital signature function itself or it may rely on its platform to perform this.
		SI-7	**Session Authenticity**	A conformant TOE supports this control through its use of a mechanism to assert the integrity of the policy data it sends. Note that the TOE itself may provide the digital signature function itself or it may rely on its platform to perform this.