SACM
Internet-Draft
Intended status: Informational
Expires: March 13, 2017

C. Coffin
B. Cheikes
C. Schmidt
D. Haynes
The MITRE Corporation
J. Fitzgerald-McKay
Department of Defense
D. Waltermire
National Institute of Standards and Technology

September 9, 2016

SACM Vulnerability Assessment Scenario
draft-ietf-sacm-vuln-scenario-02

Abstract

This document describes an automated enterprise vulnerability assessment scenario aligned with the SACM Use Cases. The scenario assumes the existence of endpoint management capabilities and begins with an enterprise ingesting vulnerability description information. Endpoints are assessed against the vulnerability description information based on a combination of examining known endpoint characterization information and collected endpoint information.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 13, 2017.

Table of Contents

1. Introduction

This document describes a detailed, enterprise-specific vulnerability assessment scenario from which information model elements can be discovered. This scenario also informs protocol and data model development in support of vulnerability assessment, as part of overall posture assessment (see Appendix B for examples of solutions that support this scenario).

Vulnerability discovery, disclosure, publication, and prioritization is out of scope. However, given the importance of prioritization in an enterprise's vulnerability assessment process, it is discussed in Appendix C.

Information on how the scenario aligns with SACM and other existing work is discussed in Appendix D through Appendix G.

2. Terminology

Vulnerability description information: Information pertaining to the existence of a flaw or flaws in software, hardware, and/or firmware, which could potentially have an adverse impact on enterprise IT functionality and/or security. Vulnerability description information should contain enough information to support vulnerability detection.

Vulnerability detection data: A type of guidance extracted or derived from vulnerability description information that describes the specific mechanisms of vulnerability detection that is used by an enterprise's vulnerability management capabilities to determine if a vulnerability is present on an endpoint.

Endpoint management capabilities: An enterprise IT department's ability to manage endpoint identity, endpoint information, and associated metadata on an ongoing basis.

Vulnerability management capabilities: An enterprise IT department's ability to manage endpoint vulnerabilities and associated metadata on an ongoing basis by ingesting vulnerability description information and vulnerability detection data, and performing vulnerability assessments.

Vulnerability assessment capabilities: An enterprise IT department's ability to determine whether a set of endpoints is vulnerable

according to the information contained in the vulnerability description information.

3. Assumptions

A number of assumptions must be stated in order to further clarify the position and scope of this document.

The document assumes that:

- The enterprise has received vulnerability description information, and that the information has already been processed into vulnerability detection data that the enterprise's security software tools can understand and use.
- The enterprise has a means of identifying enterprise endpoints through the execution of Target Endpoint Discovery Tasks although assertions about some details of this capability are made.
- The enterprise has a means of extracting relevant information about enterprise endpoints in a form that is compatible with the vulnerability description data.
- All information described in this scenario is available in the vulnerability description data and serves as the basis of assessments.
- The enterprise can provide all relevant information about any endpoint needed to perform the described assessment.
- The enterprise has a mechanism for long-term storage of vulnerability description information, vulnerability detection data, and vulnerability assessment results.
- The enterprise has a procedure for reassessment of endpoints at some point after initial assessment (see Appendix H for more information).

4. Vulnerability Assessment Pre-requisites

In order to successfully support the vulnerability assessment scenario, an enterprise needs to have the following capabilities deployed on their network and information readily available.

4.1. Endpoint Management Capabilities

Endpoint management capabilities are assumed to be in place within the enterprise, and are expected to collect a minimum set of attributes from the endpoints under management via Collection Tasks and to establish an endpoint's identity within the scope of that domain. Endpoint identity can be established by collecting certain identifying attributes, collectively known as the Target Endpoint Identifier, that allow for unique and persistent tracking of endpoints on the enterprise network. Examples include, but are not limited to, IP address, MAC address, Fully Qualified Domain Names (FQDNs), pre-provisioned identifiers such as Globally Unique Identifiers (GUIDs) or copies of serial numbers, certificates, hardware identity values, or similar attributes. To simplify the identification of an endpoint, a Target Endpoint Label may be created and assigned to refer to the Target Endpoint Identifier. All of the information collected by the endpoint management capabilities is stored, with appropriate metadata (i.e. timestamp), in a central location and used to build up a Target Endpoint Characterization Record and Target Endpoint Profile via a Target Endpoint Characterization Task. The endpoint management capabilities are expected to be performed on an ongoing basis, resulting in routine, or even event-driven, collection of basic endpoint information.

See Appendix I for information-specific details.

4.2. Vulnerability Description Information

Vulnerability description information is expected to be periodically received by the enterprise. Upon receipt, the vulnerability description information is expected to be assigned a unique tracking identifier, stored in a repository (with appropriate metadata) in raw form, and transformed into a machine-readable vulnerability detection data with unique tracking identifier understood by the components described by this scenario. This transformed form can be referred to as the vulnerability detection data. At some point, receipt and processing of vulnerability description data is expected to trigger the vulnerability assessment.

See Appendix I for information-specific details.

5. Endpoint Vulnerability Assessment Capabilities

When new vulnerability description information is received by the enterprise, affected endpoints are identified and assessed. The vulnerability is said to apply to an endpoint if the endpoint satisfies the conditions expressed in the vulnerability detection data.

A vulnerability assessment (i.e. vulnerability detection) is performed in two steps:

- Endpoint information collected by the endpoint management capabilities is examined by the vulnerability management capabilities through Evaluation Tasks.
- If the data possessed by the endpoint management capabilities is insufficient, a Collection Task is triggered and the necessary data is collected from the target endpoint.

Vulnerability detection relies on the examination of different endpoint information depending on the nature of a specific vulnerability. Common endpoint information used to detect a vulnerability includes:

- A specific software version is installed on the endpoint
- File system attributes
- Specific state attributes

In many cases, the endpoint information needed to determine an endpoint's vulnerability status will have been previously collected by the endpoint management capabilities and available in a Repository. However, in other cases, the necessary endpoint information will not be readily available in a Repository and a Collection Task will be triggered to collect it from the target endpoint. Of course, some implementations of endpoint management capabilities may prefer to enable operators to perform this collection under certain circumstances, even when sufficient information can be provided by the endpoint management capabilities (e.g. there may be freshness requirements for information).

The collection of additional endpoint information for the purpose of vulnerability assessment does not necessarily need to be a pull by the vulnerability assessment capabilities. Over time, some new pieces of information that are needed during common types of assessments might be identified. Endpoint management capabilities can be reconfigured to have this information delivered automatically. This avoids the need to trigger additional Collection Tasks to gather this information during assessments, streamlining the assessment process. Likewise, it might be observed that certain information delivered by endpoint management capabilities is rarely used. In this case, it might be useful to re-configure the endpoint management capabilities to no longer collect this information to reduce network and processing overhead. Instead, a new Collection Task can be

triggered to gather this data on the rare occasions when it is needed.

See Appendix I for information-specific details.

6. Vulnerability Assessment Results

Vulnerability assessment results present evaluation results along with sufficient context, so that appropriate action can be taken. Vulnerability assessment results are ideally stored for later use.

See Appendix I for information-specific details.

7. IANA Considerations

This memo includes no request to IANA.

8. Security Considerations

This document provides a core narrative that walks through an automated enterprise vulnerability assessment scenario and is aligned with SACM "Endpoint Security Posture Assessment: Enterprise Use Cases" [RFC7632]. As a result, the security considerations for [RFC7632] apply to this document. Furthermore, the data collected as part of the vulnerability assessment may provide attackers with useful information such as what software an enterprise is running on their endpoints. As a result, organizations should consider properly protecting this information.

9. Informative References

[charter-ietf-sacm-01]
Security Automation and Continuous Monitoring, "Charter, Version 1.0", October 2015, <https://datatracker.ietf.org/doc/charter-ietf-sacm/>.

[critical-controls]
Center for Internet Security, "Critical Security Controls, Version 6.0", <https://www.cisecurity.org/critical-controls.cfm>.

[cvrf] Industry Consortium for Advancement of Security on the Internet, "Common Vulnerability and Reporting Framework", May 2012, <http://www.icasi.org/cvrf/>.

[I-D.coffin-sacm-nea-swid-patnc]
Coffin, C., Haynes, D., Schmidt, C., and J. Fitzgerald-McKay, "SWID Message and Attributes for PA-TNC", draft-coffin-sacm-nea-swid-patnc-01 (work in progress), June 2016.

[I-D.cokus-sacm-oval-results-model]
Cokus, M., Haynes, D., Rothenberg, D., and J. Gonzalez, "OVAL(R) Results Model", draft-cokus-sacm-oval-results-model-01 (work in progress), September 2016.

[I-D.hansbury-sacm-oval-info-model-mapping]
mhansbury@mitre.org, m., Haynes, D., and J. Gonzalez, "OVAL and the SACM Information Model", draft-hansbury-sacm-oval-info-model-mapping-03 (work in progress), September 2016.

[I-D.haynes-sacm-oval-definitions-model]
Cokus, M., Haynes, D., Rothenberg, D., and J. Gonzalez, "OVAL(R) Definitions Model", draft-haynes-sacm-oval-definitions-model-01 (work in progress), September 2016.

[I-D.ietf-sacm-requirements]
Cam-Winget, N. and L. Lorenzin, "Security Automation and Continuous Monitoring (SACM) Requirements", draft-ietf-sacm-requirements-13 (work in progress), March 2016.

[I-D.rothenberg-sacm-oval-sys-char-model]
Cokus, M., Haynes, D., Rothenberg, D., and J. Gonzalez, "OVAL(R) System Characteristics Model", draft-rothenberg-sacm-oval-sys-char-model-01 (work in progress), September 2016.

[RFC7632] Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment: Enterprise Use Cases", RFC 7632, DOI 10.17487/RFC7632, September 2015, <http://www.rfc-editor.org/info/rfc7632>.

Appendix A. Change Log

A.1. Changes in Revision -02

Changed "capability" in the context of endpoint management, vulnerability management, and vulnerability assessments to "capabilities" to avoid confusion with the term "capability" in the terminology draft.

Made a few other minor editorial and clarification changes.

A.2. Changes in Revision -01

Clarified how the endpoint management capability can reconfigured over time to adapt to the needs of an enterprise. GitHub issue #12 (https://github.com/sacmwg/vulnerability-scenario/issues/12).

Included references to the various appendices in the document. GitHub issue #18 (https://github.com/sacmwg/vulnerability-scenario/issues/18).

Fixed typos and other minor editorial changes in the document. GitHub issue #19 (https://github.com/sacmwg/vulnerability-scenario/issues/18). GitHub issue #20 (https://github.com/sacmwg/vulnerability-scenario/issues/20). GitHub issue #22 (https://github.com/sacmwg/vulnerability-scenario/issues/22).

Updated references to the Critical Controls to Version 6.0. GitHub issue #23 (https://github.com/sacmwg/vulnerability-scenario/issues/23).

Aligned the scenario with SACM Tasks. GitHub issue #25 (https://github.com/sacmwg/vulnerability-scenario/issues/25).

A.3. Changes Since Adopted as a WG I-D -00

Made various organizational and editorial changes as proposed by Adam Montville. GitHub issue #4 (https://github.com/sacmwg/vulnerability-scenario/issues/4).

Removed the TODO from the Security Considerations section (https://github.com/sacmwg/vulnerability-scenario/issues/8).

Clarified the definition of "vulnerability detection data" to explain how it was guidance and provided instructions for security tools on how to carry out a vulnerability assessment. GitHub issue #13 (https://github.com/sacmwg/vulnerability-scenario/issues/13).

Changed "targeted collection" to "supplemental collection". GitHub issue #14 (https://github.com/sacmwg/vulnerability-scenario/issues/14).

Clarified that the ability for an enterprise to convert vulnerability description information and process it into a format usable by security tools is the same as the converting vulnerability description information into vulnerability detection data. GitHub issue #15 (https://github.com/sacmwg/vulnerability-scenario/issues/15).

Determine if we need to remove references to the long-term storage of data in repositories. GitHub issue #16 (https://github.com/sacmwg/vulnerability-scenario/issues/16).

Moved the information needs captured in Appendix D.2 into the Information Model. GitHub issue #17 (https://github.com/sacmwg/vulnerability-scenario/issues/17).

A.4. Changes in Revision draft-coffin-sacm-vuln-scenario-01

Clarification of the vulnerability description data IDs in sections 4 and 6.

Added "vulnerability remediation" to the Assessment Results and Data Attribute Table and Definitions sections.

Added Implementation Examples to Endpoint Identification and Initial (Pre-Assessment) Data Collection, Vulnerability Description Data, Endpoint Applicability and Assessment, and Assessment Results sections.

Added an example to vulnerability description data in the scope section.

Added a sentence to clarify vulnerability description data definition in the scope section.

Added data repository example for long-term storage scope item.

Added sentence to direct reader to examples of basic system information in endpoint identification section.

Split the examples of information to collect in the pre-assessment collection section into a basic and advanced list.

Added examples of data stored in the repository in the Assessment Results section.

Added sentence for human-assigned attributes in the Future Work section.

Replaced "vulnerability report" to "vulnerability description data" because the term report was causing confusion. Similarly, replaced "assessment report" with "assessment results".

Replaced "Configuration Management Database (CMDB)" with "Repository" which is SACM’s term for a data store.

Replaced endpoint "Role" with "Purpose" because "Role" is already defined in SACM. Also, removed "Function" because it too is already defined in SACM.

Clarified that the document does not try to define a normalized data format for vulnerability description data although it does not preclude the creation of such a format.

Included additional examples of software configuration information.

Clarified the section around endpoint identification to make it clear designation attributes used to correlate and identify endpoints are both persistent and unique. Furthermore, text was added to explain how the persistency of attributes may vary. This was based on knowledge gained from the Endpoint ID Design Team.

Updated the Security Considerations section to mention those described in [RFC7632].

Removed text around Bring Your Own Device (BYOD). While important, BYOD just adds complexity to this initial draft. BYOD should be addressed in a later revision.

Merged the list of "basic endpoint information" and the list of "human-assigned endpoint attributes" as both represent data we want to collect about an endpoint. Whether or not that data is natively available on the endpoint for collection or assigned by a human, computed, or derived from other data which may or may not be available on the endpoint for collection seems arbitrary. With this scenario, we primarily care about expressing information needs rather than how the information is collected or from where.

Appendix B. Implementation Examples

B.1. Endpoint Data Collection

Within the SACM Architecture, the Internal and External Collector components could be used to allow enterprises to collect posture attributes that demonstrate compliance with enterprise policy. Endpoints can be required to provide posture attributes, which may include identification attributes to enable persistent communications.

The SWID Message and Attributes for PA-TNC standard [I-D.coffin-sacm-nea-swid-patnc] defines collection and validation of software identities using the ISO Software Identification Tag Standard. Using this standard, the identity of all installed

software including the endpoint operating system, could be collected and used for later assessment.

The OVAL Definitions Model [I-D.haynes-sacm-oval-definitions-model] provides a data model that can be used to specify what posture attributes to collect as well as their expected values which can be used to drive an assessment.

The OVAL System Characteristics Model [I-D.rothenberg-sacm-oval-sys-char-model] can be used to capture information about an endpoint. The model is specifically suited to expressing OS information, endpoint identification information (such as IP and MAC addresses), and other endpoint metadata.

B.2. Vulnerability Description Information

The Common Vulnerability Reporting Framework (CVRF) [cvrf] is an XML-based language that attempts to standardize the creation of vulnerability description information. Using CVRF, the enterprise could create automated tools based on the standardized schema which would obtain the needed and relevant information useful for later assessments and assessment results.

B.3. Secondary Assessment

Within the SACM Architecture, the assessment task would be handled by the Evaluator component. If previously collected data is used, it would be obtained from a Data Store component.

Within the SACM Architecture, the Internal and External Collector components could be used to allow enterprises to collect posture attributes that demonstrate compliance with enterprise policy. Endpoints can be required to provide posture attributes, which may include identification attributes to enable persistent communications.

The SWID Message and Attributes for PA-TNC standard defines collection and validation of software identities using the ISO Software Identification Tag Standard. Using this standard, all installed software including the endpoint operating system could be collected and stored for later assessment.

The OVAL Definitions Model provides a data model that can be used to specify what posture attributes to collect as well as their expected values which can be used to drive an assessment.

The OVAL System Characteristics Model can be used to capture information about an endpoint. The model is specifically suited to

expressing OS information, endpoint identification information (such as IP and MAC addresses), and other endpoint metadata.

The SACM Internal and External Attribute Collector components can be used to allow enterprises to collect posture attributes that demonstrate compliance with enterprise policy. Endpoints can be required to provide posture attributes, which may include identification attributes to enable persistent communications.

B.4. Assessment Results

The OVAL Results Model [I-D.cokus-sacm-oval-results-model] provides a data model to encode the results of the assessment, which could then be stored in a Repository and later accessed. The assessment results described in this scenario could be stored and later accessed using the OVAL Results Model. Note that the use of the OVAL Results Model for sharing results is not recommended per section 7.3 of the OVAL and the SACM Information Model [I-D.hansbury-sacm-oval-info-model-mapping].

Within the SACM Architecture, the generation of the assessment results would occur in the Report Generator component. Those results might then be moved to a Data Store component for later sharing and retrieval as defined by SACM.

Appendix C. Priority

Priorities associated with the vulnerability description information, assessment results, and any remedy is important, but is treated as a separate challenge and, as such, has not been integrated into the description of this scenario. Nevertheless, it is important to point out and describe the use of priorities in the overall vulnerability assessment scenario as a separate issue with its own sets of requirements.

Priority in regard to vulnerability description information, can be viewed in a couple of different ways within an enterprise. The assessment prioritization involves prioritization of the vulnerability description information assessment process. This determines what vulnerability description information is assessed, and in what order it is assessed in. For instance, a vulnerability affecting an operating system or application used throughout the enterprise would likely be prioritized higher than a vulnerability in an application which is used only on a few, low-criticality endpoints.

The prioritization of remedies relates to the enterprise remediation and mitigation process based on the discovered vulnerabilities. Once

an assessment has been performed and applicable endpoints identified, enterprise vulnerability managers must determine where to focus their efforts to apply appropriate remedies. For example, a vulnerability that is easily exploitable and which can allow arbitrary code execution might be remedied before a vulnerability that is more difficult to exploit or which just degrades performance.

Some vulnerability description information include severities and/or other information that places the vulnerability in context. This information can be used in both of the priority types discussed above. In other cases, enterprise administrators may need to prioritize based only on what they know about their enterprise and the description provided in the vulnerability description information.

Examples of data attributes specific to priority of assessments and/or remedies include (but not limited to) the following:

- Enterprise - defined purpose of the device, criticality of the device, exposure of the device, etc.

- Severity attributes - A rating or score that attempts to provide the level of severity or criticality associated with a given vulnerability.

- Cyber threat intelligence - information such as tactics, techniques, and procedures of threat actors, indicators of compromise, incidents, courses of action, etc. that help the enterprise understand relevant threats and how to detect, mitigate, or respond to them.

Appendix D. SACM Usage Scenarios

The SACM "Endpoint Security Posture Assessment: Enterprise Use Cases" document ([RFC7632]) defines multiple usage scenarios that are meant to provide examples of implementing the use cases and building block capabilities. Below is a brief summary of some of these usage scenarios and how this document aligns and/or adds additional value to the identified usage scenarios.

- Automated Checklist Verification (2.2.2) - "An enterprise operates a heterogeneous IT environment. They utilize vendor-provided automatable security configuration checklists for each operating system and application used within their IT environment. Multiple checklists are used from different vendors to ensure adequate coverage of all IT assets." The usage scenario, as defined in the RFC, is targeted at the checklist level and can be interpreted as being specific to endpoint configuration. There is mention of

patch assessment and vulnerability mitigation, but the usage scenario could be expanded upon by including vulnerability verification. Replacing the idea of a checklist in the SACM usage scenario with vulnerability would allow the usage scenario to align almost exactly with the scenario described in this document. Instead of collecting automatable security configuration checklists, the enterprise would collect automatable vulnerability description information available from the vendor as described or possibly from other interested third-parties.

- Detection of Posture Deviations (2.2.3) - "An enterprise has established secure configuration baselines for each different type of endpoint within their IT environment. When an endpoint connects to the network, the appropriate baseline configuration is communicated to the endpoint. Once the baseline has been established, the endpoint is monitored for any change events pertaining to the baseline on an ongoing basis. When a change occurs to posture defined in the baseline, updated posture information is exchanged. When the endpoint detects a posture change, an alert is generated identifying the specific changes in posture." This usage scenario would support the concept of endpoints signaling or alerting the enterprise to changes in the posture relates to endpoint vulnerabilities in the same way that it would for configurations. Replacing the idea of a checklist with vulnerability description data allows the SACM usage scenario and the scenario described in this document to align in their objectives.

- Asynchronous Compliance/Vulnerability Assessment at Ice Station Zebra (2.2.5) - "An isolated arctic IT environment that is separated from the main university network. The only network communications are via an intermittent, low-speed, high-latency, high-cost satellite link. Remote network admins will need to show continued compliance with the security policies of the university, the government, and the provider of the satellite network, as well as keep current on vulnerability testing." This SACM usage scenario describes vulnerability assessment and aligns well with the vulnerability scenario described in this document. The endpoint assets are identified and associated data is published in a Repository. Vulnerability description information is collected and saved in a Repository as it is released. The vulnerability description information is queued for later assessment, then the assessment results and vulnerability description information are stored after assessment. The only real difference in this SACM usage scenario is the timing of the assessments. The scenario described within this document would have no problems adjusting to the timing of this SACM usage scenario or anything similar.

Appendix E. SACM Requirements and Charter - Future Work

In the course authoring this document, some additional considerations for possible future work were noted. The following points were taken from the SACM Requirements [I-D.ietf-sacm-requirements], SACM Charter [charter-ietf-sacm-01], and SACM Use Cases ([RFC7632]) documents and represent work that may be necessary to support the tasks or goals of SACM going forward.

- The SACM requirements mentions "Result Reporting" with applications but no detail around what the assessment results data set should include. In the case of vulnerability assessment results, context is important and details beyond just a Pass or Fail result are needed in order to take action. A good example of this might be the Priority of the vulnerability itself and how many systems it affects within the enterprise. With this in mind, it might be worthwhile to investigate a minimum data set or schema for assessment results. The concern here is with vulnerability description data, but this could apply to other enterprise processes as well.

- The "Human-assigned endpoint attributes" mentioned previously in this scenario are touched on in the SACM use cases, but the topic could probably be explored in much more depth. Enterprise policy and behaviors could be greatly influenced by endpoint attributes such as locations, how the endpoint is used, and criticality. When and how these data attributes are collected, as well as what the minimum or common set might look like, would be good topics for future related SACM work. In addition, the storage of these attributes could be central (stored in a data repository) or they could be assigned and stored on the endpoints themselves.

Appendix F. SACM Use Case Alignment

F.1. Endpoint Identification

This sub-step aligns with the Endpoint Discovery, Endpoint Characterization, and Endpoint Target Identification building block capabilities. The alignment is due to the fact that the purpose of this sub-step is to discover, identify, and characterize all endpoints on an enterprise network.

F.2. Endpoint Data Collection

This sub-step aligns with the Data Publication building block capability because this section involves storage of endpoint attributes within an enterprise Repository. This sub-step also aligns with the Endpoint Characterization and Endpoint Target

Identification building block capabilities because it further characterizes the endpoint through automated and possibly manual means. There is direct alignment with the Endpoint Component Inventory, Posture Attribute Identification, and Posture Attribute Value Collection building block capabilities since the purpose of this sub-step is to perform an initial inventory of the endpoint and collect basic attributes and their values. Last, there is alignment with the Collection Guidance Acquisition building block capabilities as the inventory and collection of endpoint attributes would be directed by some type of enterprise or third-party guidance.

F.3. Vulnerability Description Information

This step aligns with the Data Publication and Data Retrieval building block capabilities because this section details storage of vulnerability description information within an enterprise Repository and later retrieval of the same.

F.4. Applicability

This sub-step aligns with the Data Retrieval, Data Query, and Posture Attribute Value Query building block capabilities because, in this sub-step, the process is attempting to determine the vulnerability status of the endpoint using the data that has previously been collected.

F.5. Secondary Assessment

This sub-step aligns with the Data Publication building block capability because this section details storage of endpoint attributes within an enterprise Repository. The sub-step also aligns with the Collection Guidance Acquisition building block capability since the vulnerability description information (guidance) drives the collection of additional endpoint attributes.

This sub-step aligns with the Endpoint Characterization (both manual and automated) and Endpoint Target Identification building block capabilities because it could further characterize the endpoint through automated and possibly manual means. There is direct alignment with the Endpoint Component Inventory, Posture Attribute Identification, and Posture Attribute Value Collection building block capabilities since the purpose of this sub-step is to perform additional and more specific component inventories and collections of endpoint attributes and their values.

F.6. Assessment Results

This step aligns with the Data Publication and Data Retrieval building block capabilities because this section details storage of vulnerability assessment results within an enterprise Repository and later retrieval of the same.

Appendix G. Alignment with Other Existing Works

G.1. Critical Security Controls

The Center for Internet Security's Critical Security Controls [critical-controls] includes security controls for a number of usage scenarios, some of which are covered in this document. This section documents the alignment between the Center's controls and the relevant elements of the scenario.

G.1.1. Continuous Vulnerability Assessment

"CSC 4: Continuous Vulnerability Assessment and Remediation," which is described by the Center for Internet Security as "Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers." The scenario described in this document is aligned with CSC 4 in multiple ways:

CSC 4.1 applies to this scenario in that it calls for running regular, automated scanning to deliver prioritized lists of vulnerabilities with which to respond. The scenario described in this document is intended to be executed on a continuous basis, and the priorities of both vulnerability description information and the remedy of vulnerabilities are discussed in the Priority section earlier in this document.

This scenario assumes that the enterprise already has a source for vulnerability description information as described in CSC 4.4.

Both CSC 4.2 and 4.7 are made possible by writing information to a Repository since this makes previously collected data available for later analysis.

While this scenario does not go into the details of how prioritization would be calculated or applied, it does touch on some of the important ways in which prioritization would impact the endpoint assessment process in the Priority section. As such, the Priority section aligns with CSC 4.8, which deals with vulnerability priority. Vulnerability priority in this scenario is discussed in terms of the vulnerability description information priority during

receipt, as well as the vulnerability priority with regards to remedies.

The described scenario does not address the details of applying a remedy based on assessment results. As such, CSC 4.5 which deals with mitigations and patching, is out of scope for this work. Similarly, CSC 4.3 prescribes performing scans in authenticated mode and CSC 4.6 prescribes monitoring logs. This scenario does not get into the means by which data is collected, focusing on "what" to collect rather than "how", and as such does not have corresponding sections, although the procedures described are not incompatible with either of these controls.

The CSC 4 System Entity Relationship diagram directly aligns with the scenario described in this document with the exception of applying patches to endpoints.

G.1.2. Hardware and Software Inventories

This scenario is also aligned with, and describes a process for, collecting and maintaining hardware and software inventories, which are covered by the Center for Internet Security CSC 1 "Inventory of Authorized and Unauthorized Devices" and CSC 2 "Inventory of Authorized and Unauthorized Software." This scenario documents a process that is specific to collecting and maintaining hardware and software data attributes for vulnerability assessment purposes, but the collection of the hardware attributes and software inventory documented in the Endpoint Data Collection section that follows can also be used for the purpose of implementing authorized and unauthorized hardware and software management processes (e.g., scanning tools looking for unauthorized software). Moreover, the ability to accurately identify endpoints and, to a lesser degree, applications is integral to effective endpoint data collection and vulnerability management.

The Endpoint Data Collection section does not have coverage for the specific details described in CSC 1 and 2 as they are different processes and would be out-of-scope of this scenario, but the section does provide the data necessary to support the controls.

The Endpoint Identification and Endpoint Data Collection sections within this scenario align with CSC 1.1 and 1.4 by identifying enterprise endpoints and collecting their hardware and network attributes. The Endpoint Data Collection section aligns with and supports CSC 2.3 by defining a software inventory process and a method of obtaining operating system and file system attributes. The rest of the items from CSC 1 and 2 deal with implementation details and would be out-of-scope for this document.

Appendix H. Continuous Vulnerability Assessment

It is not sufficient to perform a single assessment when vulnerability description information is published without any further checking. Doing so does not address the possibility that the reported vulnerability might be introduced to the enterprise environment after the initial assessment completes. For example, new endpoints can be introduced to the environment which have old software or are not up-to-date with patches. Another example is where unauthorized or obsolete software is installed on an existing endpoint by enterprise users after vulnerability description information and initial assessment has taken place. Moreover, enterprises might not wish to, or be able to, assess all vulnerability description information immediately when they come in. Conflicts with other critical activities or limited resources might mean that some alerts, especially those that the enterprise deems as "low priority", are not used to guide enterprise assessments until sometime after the initial receipt.

The scenario above describes a single assessment of endpoints. However, it does not make any assumptions as to when this assessment occurs relative to the original receipt of the vulnerability description data that led to this assessment. The assessment could immediately follow the ingestion of the vulnerability description information, could be delayed, or the assessment might represent a reassessment of some vulnerability description information against which endpoints had previously been assessed. Moreover, the scenario incorporates long-term storage of collected data, vulnerability description information, and assessment results in order to facilitate meaningful and ongoing reassessment.

Appendix I. Data Attribute Table

The following table maps all major data attributes against each major process where they are used.

	vulnerability description data	Endpoint Identification and Initial Data Collection	Endpoint Applicability and Assessment	Assessment Results
Endpoint				
Collection date/time		X	X	

Endpoint type		X	X	
Hardware version/firmware	X	X	X	
Operating system	X	X	X	
Operating system attributes (e.g., version, service pack level, edition, etc.)	X	X	X	
Installed software name	X	X	X	X
Installed software attributes (e.g., version, patch level, install path, etc.)	X	X	X	X
Open ports/services	X	X	X	
Operating system optional component inventory	X	X	X	
Location		X		X
Purpose		X		X
Criticality		X		X

File system attributes (e.g., versions, size, write date, modified date, checksum, etc.)	X		X	
Shared libraries	X		X	
Other software configuration information	X		X	
External vulnerability description data				
Ingest Date	X		X	
Date of Release	X		X	
Version	X		X	
External vuln ID	X		X	X
Severity Score				X
Assessment Results				
Date of assessment			X	X
Date of data collection		X	X	X
Endpoint ide		X	X	X

ntification and/or locally assigned ID					
Vulnerable software product(s)	X	X	X	X	
Endpoint vulnerability status			X	X	
Vulnerability description	X			X	
Vulnerability remediation	X			X	

Table 1: Vulnerability Assessment Attributes

Authors' Addresses

Christopher Coffin
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: ccoffin@mitre.org

Brant Cheikes
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: bcheikes@mitre.org

Charles Schmidt
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: cmschmidt@mitre.org

Daniel Haynes
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: dhaynes@mitre.org

Jessica Fitzgerald-McKay
Department of Defense
9800 Savage Road
Ft. Meade, Maryland
USA

Email: jmfitz2@nsa.gov

David Waltermire
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20877
USA

Email: david.waltermire@nist.gov