Security Automation and Continuous Monitoring WG

Use Cases Status Report
draft-ietf-sacm-use-cases-06

David Waltermire
IETF 89 – Mar 6 2014

Use Cases Document

- This document provides a sampling of use cases for aggregating data and assessing that data to determine an organization's security posture.
- From use cases, we can derive common functional networking capabilities and requirements for IETF-related standards.
- The scope of this document is limited to Enterprise Security Posture Assessment . Later documents can address other scopes.
- Existing IETF technologies might be suitable to address some of these functions and requirements.

Use Cases Status -06

- Updated the "Introduction" section to better reflect the use case, building block, and usage scenario structure changes from previous revisions.
- Updated most uses of the terms "content" and "content repository" to use "guidance" and "security automation data store" respectively.
- In section 2.1.1, added a discussion of different data types and renamed "content" to "data" in the building block names.
- In section 2.1.2, separated out the building block concepts of "Endpoint Discovery" and "Endpoint Characterization" based on mailing list discussions.
- Addressed some open questions throughout the draft based on consensus from mailing list discussions and the two virtual interim meetings.
- Changed many section/sub-section names to better reflect their content.

Open Questions - #1

Should section 2.1.2: Identify Endpoint Targets include authentication of the target?

Based on the current text, this building block appears to be using information that was previously defined/collected.

Proposal: Address authentication of endpoints as they are discovered in the previous "Endpoint Discovery" building block.

Old text:

Endpoint Discovery : To determine the current or historic presence of endpoints in the environment that are available for posture assessment.

New text:

Endpoint Discovery : To determine the current or historic presence of endpoints in the environment that are available for posture assessment. ***Endpoints are authenticated using appropriate mechanisms as they become part of the environment.***

Open Questions - #2

In section 2.1.2: Posture Attribute Identification, are we missing a building block that queries and analyzes any previously collected posture to determine if it is suitable for use in the evaluation?

Proposal: Add text to address analysis of previously collected data to determine what additional data to collect.

Old text:

Posture Attribute Identification: Once the endpoint targets and component inventory is known, it is then necessary to calculate what posture attributes are required to be collected to perform the evaluation. If this is driven by guidance, then the Data Query and/or Data Retrieval building blocks (see section 2.1.1) may be used to acquire this data.

New text:

Posture Attribute Identification: Once the endpoint targets and component inventory is known, it is then necessary to calculate what posture attributes are required to be collected to perform the evaluation. ***If existing stores of posture data are available, they are queried using the Data Query building block (see section 2.1.1) to determine what previously collected posture data, if any, is suitable for evaluation. Retrieved data is analyzed to determine if it is complete and current enough for use in the evaluation. Any unsuitable or missing posture data is identified for collection.***

Guidance may be used to describe what sources of data should be queried, the conditions under which data can be re-used, and what data must always be collected. The Data Query and/or Data Retrieval building blocks (see section 2.1.1) may be used to acquire this guidance.

Open Questions - #3-5

#3: In section 2.1.4: Posture Attribute Evaluation, what if data is unavailable or is not current enough to support the evaluation? This could be caused if collection did not occur (for some reason) and previous collection was too old.

Proposal: Add a statement about error handling in the "Posture Attribute Evaluation" building block.

#4: The end of section 2.1.4 states "Completion of this process represents a complete assessment cycle as defined in Section 2." Since this indicates completion of the section 2 process, it would be resonable for section 2.2 to follow. However, an additional use case section 2.1.5 follows.

Proposal: Integrate the 2.1.5 wording into section 2.1.4. Remove section 2.1.5

#5: Section 2.1.5 has been commented on as being duplicative of the previous use case in section 2.1.4 with the exception of the "Change Detection" building block.

Proposal: Integrate the 2.1.5 wording into section 2.1.4. Remove section 2.1.5.

Open Questions - #3-5 - Changes

2.1.4. Posture Evaluation

This use case describes the process of evaluating collected posture attribute values representing actual endpoint state against the expected state selected for the assessment. This use case can be initiated by a variety of triggers including:

1. A posture change or significant event on the endpoint.
2. A network event (e.g., endpoint connects to a network/VPN, specific netflow is detected).
3. Due to a scheduled or ad hoc evaluation task.

The building blocks of this use case are:

Collected Posture Change Detection: An operator or application should have a mechanism to detect the availability of new or changes to existing posture attribute values. The timeliness of detection may vary from immediate to on-demand. Having the ability to filter what changes are detected will allow the operator to focus on the changes that are relevant to their use and will enable evaluation to occur dynamically based on detected changes.

Posture Attribute Value Query: If previously collected posture attribute values are needed, the appropriate data stores are queried to retrieve them. If all posture attribute values are provided directly for evaluation, then this capability may not be needed.

Evaluation Guidance Acquisition: If guidance is required to drive the evaluation of posture attributes values, this capability is used to acquire this data from one or more security automation data stores. Depending on the trigger, the specific guidance to acquire might be known. If not, it may be necessary to determine the guidance to use based on the component inventory or other assessment criteria. The Data Query and/or Data Retrieval building blocks (see section 2.1.1) may be used to acquire this guidance.

Posture Attribute Evaluation: The comparison of posture attribute values against their expected values as expressed in the specified guidance. The result of this comparison is output as a set of posture evaluation results. ***If collected posture attribute values are unavailable or are out-of-date, error conditions will need to be expressed in place of specific posture evaluation results.***

Completion of this process represents a complete assessment cycle as defined in Section 2.

While the focus of this use cases is around enabling the comparison of expected vs. actual state, the same building blocks can support other analysis techniques that apply to collected posture attribute data.

Open Questions - #6

In section 2.2.4, should we include other building block references?

Proposal: Make no change. The current referenced building blocks provide adequate coverage of the usage scenario.

Next Steps

- Address remaining open questions based on consensus
- Review terminology use
  - Ensure that terminology is used consistently
  - Reduce use of terms - use plain language where possible vs. terms of art
- Prepare draft for WG last call before next IETF meeting

Questions?