About the CIS Controls Assessment Specification

Purpose

The CIS Controls provide essential best practices that organizations can implement to improve their cybersecurity posture. In addition to implementing the CIS Controls, it is also important that organizations measure their implementations to ensure that Safeguards are in place and working properly. The purpose of the CIS Controls Assessment Specification (CAS) is to provide a common understanding of what should be measured in order to verify that CIS Safeguards are properly implemented. The hope is that those developing related tools will then build these measures into their tools so that the CIS Controls are measured in a uniform way.

Note that the focus of CAS is on **what to measure** rather than **how to measure**. With the goal of being platform agnostic, a conscious effort was made to avoid addressing the how to measure in writing CAS, leaving those platform specific details to specific implementations of these measures. Tool developers will determine the "hows" that are appropriate for their tools and use cases.

Methodology

The CIS Controls provide cybersecurity best practices designed to help organizations of all types secure a wide variety of systems. Because the CIS Controls cover so many security topics, and apply to such a wide variety of hardware and software that can be used in many different ways, measuring the CIS Controls is a complex challenge. Different approaches to measuring the Controls can result in multiple ways of measuring the same Safeguard.

One useful distinction is measuring whether a Safeguard has been implemented vs. measuring how well the Safeguard was implemented. Measuring whether a Safeguard is implemented need not be a binary yes or no; for instance, it could be a numerical score indicating how many endpoints in an environment have implemented that Safeguard. Measuring how well a Safegaurd is implemented looks more to the intended effect of the Safeguard examining whether the desired security gains are being realized. Measuring whether a Safeguard is implemented often involves checking whether something is configured in a certain way, while measuring how well often requires more involved checks including more active testing.

While both of these measurement approaches are useful and have their place, for this first version of CAS, we have focused on measuring whether a Safeguard has been implemented (which we have termed Level 1 checks). It is our hope that future versions of CAS will expand to include measurements of how well a Safeguard is implemented as well (which we have termed Level 2 checks).

Specific configuration details are not specified in CAS, as these would vary from platform to platform, and would encroach on how to measure. When there are multiple ways to implement a Safeguard, CAS attempts to be generic enough to cover these varying methods in its measures. Where assumptions are made, CAS attempts to explicitly state them.

Structure of a Safeguard Measurement

This section describes the standard structure of a Safeguard Measurement in CAS.

Basic CIS Safeguard Information

This section includes the Safeguard number, title, description, asset type, security function, and implementation group. This information matches the information in the CIS Controls v8.1 document.

Assumptions

Assumptions are provided inside of the section to which they are most applicable, or not in any specific section if they are general to the entire Safeguard measurement.

Safeguard Dependencies

This is an optional section that may not appear for all Safeguard measurements. When present, this section lists any other Safeguard that are prerequisites for measuring this Safeguard. Completion of the Safeguard specified in this section will typically generate data necessary as an Input for measuring this Safeguard.

Inputs

This section includes the data that is expected as an input in order to measure this Safeguard.

Operations

This section specifies actions to be performed on the inputs in order to generate the measures. The operations provide a linkage between the inputs and measures.

Measures

This section describes the information that should be measured, generally as a result of performing operations on the inputs. Measures are combined to form metrics.

Metrics

This section describes standard metrics that can be calculated from the measures, providing a description of the metric along with the formula for calculating the metric. In general, CAS attempts to frame metrics in a positive light - e.g., the ratio of items that are compliant with the Safeguard (as opposed to the ratio of items that are not compliant). The provided metrics are not meant to be an exhausive list of metrics, rather it is just meant to list some examples of common metrics that are likely to be useful. The hope is that if appropriate measures have been defined, other metrics can be built from those measures to suit different use cases.

Procedure Review

This is an optional section that may not appear for all Safeguard measurements. When present, this section describes a manual review of a procedure that helps fulfill the Safeguard.

Versioning

CAS follows a semantic versioning approach based on semver.org and having the following format:

- Major: Significant and material changes to
    - The organization of the document
    - Structure of Safeguard measures
    - Inputs, measures, metrics on the whole
- Minor: Material changes to parts of Safeguard measures or metrics
- Point: Immaterial changes, such as prose typos, document look and feel