

## Metrics Center™: Technical Note #1 for Review and Comment

Metrics Center is the name of the new metrics catalog project at SecurityMetrics.org. Metrics Center is, like SecurityMetrics.org, available to an invitation-only community of security practitioners and researchers that are interested in measuring, analyzing and improving security. Metrics Center will offer several services, the first of which is a catalog for sharing definitions of security metrics. In addition to providing a collection of attributes that define a metric, the Metrics Center will also provide mappings that associate a metric with topics of interest, called “contexts”. A “context” can be:

- A regulation, e.g. SOX or HIPAA
- An industry requirement, e.g. PCI
- A standard, e.g. ISO 27002-5
- A best practice, e.g. ITIL or COBIT or CISWG
- A functional de-composition of a process
- Or almost anything else that is of general utility

The purpose of this email is to provide a very brief introduction to the features of the catalog service and to solicit comments and feedback. Specifically, we are interested in thoughts that you have on:

- Feature set
- The set of attributes that we plan to store as part of a complete and unambiguous definition of a metric.
- The set of “contexts” that should be part of the initial release of the Metrics Center catalog

Here is the feature set of the catalog service that is planned for the first release:

- Catalog Explorer: A web UI that allows one to navigate the set of stored metric definitions
- Metric Editor: A web UI that allows one submit a new metric definition or propose a change to an existing one. It also allows one to
- Metric Versioning: A function that tracks changes to metric definitions and supports a workflow that takes a metric from initial proposed inclusion in the catalog, through reviews, revisions, approval, and publication—followed by periodic updates.
- Catalog Search: Structured search via contexts and unstructured Google-like search based upon the words used to describe the metric. In addition on can edit associations between metrics and “nodes” within context hierarchies.
- Metric Rating: Users can assign a rating to a metric and the catalog will compute an overall score that is displayed as zero to five stars (like NetFlix movie ratings)
- Metric Ranking: Like Google page-ranks, a value will be assigned to a metric based upon the number of “hits” and “links” associated with it.
- Metric Licensing: In the event that a contributor wishes to treat the metric definition as intellectual property whose usage is governed by one of the widely-used open source licenses, this can be specified as part of the metric definition.

The following screenshot shows a view of the Metrics Center catalog service browser-based user interface. Contexts are displayed as hierarchical trees of tags on the left hand side; and the right hand side is reserved for displaying either lists of metrics or forms for editing their definition. This first screenshot shows a list of metrics associated with PCI Control Objective 6, Requirement 11. Mousing-over the context tag on the left provides a text definition. Selecting a tag produces a list of associated metrics, displayed in the right pane. Selecting a metric in the right pane produces a display of the metric definition, presented as a collection of attributes. A second screenshot shows the display when a metric is selected. Some attributes are meaningful to end-users; while others are primarily used by the system.

User Attributes are:

- **Name:** The name of the metric
- **Version:** A sequentially assigned version number for the metric definition
- **Rating:** A score that is derived from user ratings of the metric. Displayed as 0-5 stars
- **Views:** The number of page views that have been served as a measure of a metric's popularity
- **Description of Results:** A description of results produced by the metric in terms, including unit(s) of measure
- **Target:** A description of desired result--can be as simple as "Low is good"
- **High Water Mark:** All time record high value or a value that is considered to be in the highest 10%.
- **Low Water Mark:** All time record low value or value that is considered to be in the lowest 10%.
- **Objective:** A description of what the metric is designed to measure and why it is important
- **Abstract:** A discussion of key characteristics, how to interpret, background, etc.
- **How to Calculate:** A detailed description of how to calculate the metric from raw data sources
- **Sources:** Description of sources that could provide needed data to compute the metric
- **Measurement Frequency:** Suggested measurement rate, e.g. real-time, hourly, daily, weekly, etc
- **Default Visualization:** An image that represents an effective way to visualize computed results
- **License:** A reference to a license such as GPL, LGPL, Mozilla, etc that defines terms of use
- **Created/Updated:** Dates
- **State:** Possible states: Draft, Reviewed, Published
- **Tags:** A list of tags from one or more context hierarchies to indicate the metric's relevance to a topic
- **Owner:** The name of the metric's owner who has the authority to transition the metric state--Note that Metrics Center implements a workflow in which a metric's definition can transition from a draft state to a reviewed state and published state. The "owner" is responsible for overseeing this process in a timely fashion. The set of owners will be selected from volunteers within the Metrics Center community.
- **Contributors:** A list of individuals that have contributed to the definition of the metric
- **Use Cases:** A description of practical experiences in using the metric from registered Metrics Center members, can include identification of unintended consequences
- **Cost to Measure:** Discussion of implementation costs

- **Scale:** Discussion of issues related to scalability—For example, a metric about detailed configuration compliance might discuss issues of coverage associated with intermittently connected devices
- **Scope:** Discussion of issues related to scope—For example, this section can identify meaningful “sub-aggregations” such as by business unit, location, or operating system

System Attributes are:

- **Id:** Unique identifier assigned when created
- **Change Log:** A chronological log of changes or suggestions for change for each attribute.

The following screenshot shows what happens when one double clicks on the (pink) highlighted metric:



Authorized users will be able to edit the values for each attribute. A change log is maintained that can be reviewed. A designated metric owner can “promote” changes to create a new numbered metric version.

With respect to contexts (left pane), the current plan for the initial release of the catalog is to provide tag hierarchies and metrics mappings for the following contexts:

- PCI DSS 1.1
- ISO 27002
- NIST SP 800-53 Controls
- CISWG (Computer Information Security Working Group) Metrics
- Sarbanes-Oxley

We are soliciting feedback on the following:

- The above list of features. Any suggestions?
- The above list of metric attributes. What have we forgotten?
- The above list of supported contexts. What additional contexts are important?

The initial Metrics Center catalog will be available to a limited audience of contributors in May with public launch scheduled for June 2008. Please submit your comments as soon as possible to [betsy.nichols@plexlogic.com](mailto:betsy.nichols@plexlogic.com)