EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Metrics Hub: A Data Aggregation Platform for Security Metrics

Technical Brief — *Technology Innovation*

BACKGROUND

OT security programs in utilities have been maturing over the last decade, protecting critical assets for the nation's power grid. Standards and frameworks such as NIST-CSF, NERC CIP, NIST SP 800-82 Rev. 1, and C2M2 have been instrumental in enabling the electric sector to identify cyber security needs and implement necessary controls to meet these needs. However, a gap not immediately addressed by common cyber security standards and frameworks remains with regards to quantitatively measuring how well cyber security programs perform.

Maturity models such as ES-C2M2 and similar frameworks fall short with reference to quantitively measuring the performance of cyber security and overall improvement that specific cyber security practices bring to an organization. Motivated by the need for a way to continuously, quantitively evaluate the performance of cyber security programs to drive improvement and inform cyber security investment, EPRI created security metrics for the electric sector.

EPRI security metrics for the electric sector leverage OT and IT data generated by cyber security infrastructure to produce a repeatable data-centric process for assessing the performance of cyber security programs. EPRI created 60 security metrics and identified 120 data points collected from inside an organization to calculate metrics that reflect the organization's security posture. To enable utilities to implement and use EPRI's security metrics, EPRI developed the EPRI Metrics Hub.

The EPRI Metrics Hub is a web-based commercial-grade data aggregation platform that supports automated cyber security data collection, security metrics calculation, visualization, and analysis. Metrics hub is a crucial tool for successfully implementing and leveraging EPRI security metrics. This executive brief introduces the EPRI metrics hub and highlights its key components, their functionality, and overall benefits to users.

EPRI METRICS HUB OVERVIEW

The EPRI metrics hub is a web-based commercial-grade data aggregation platform designed to support the EPRI security metrics framework by providing users a single point of agglomeration for security metrics and data used to compute these metrics. Metrics hub supports automated data collection, metrics calculation, visualization, analysis and reporting. Reports and analytics generated by metrics hub are crucial for facilitating strategic discussions among users across various business units and functional areas of an organization.

Metrics hub is a valuable resource for organizations seeking to implement EPRI's security metrics and use the metrics to evaluate their security programs. The hub is highly customizable allowing organizations to select metrics that are of interest to their operations along with custom dashboards for visualization, analysis, and reporting. EPRI security metrics are hierarchically divided into three broad categories strategic, tactical, and operational level metrics, a hierarchy that metrics hub fully supports and articulates through various graphs and visualization dashboards for each metric category.

Metrics hub's architecture incorporates a role-based design that not only enhances the security of the platform but allows users across functional areas to access custom metrics, dashboards, and reports that are relevant to their business units. Additionally, the platform is comprehensive. Designed to aggregate cyber security data that is measurable and repeatable including data generated from cyber security infrastructure as well as security metric scores collected over time. The platform is envisioned to support analytics and insights that will evaluate cyber security programs in a completely data-driven fashion independent of effort.

METRICS HUB ARCHITECTURE

The EPRI metrics hub contains several crucial components that support functionality such as automated data collection, metrics calculation, visualization, and report generation as shown in Figure 1.

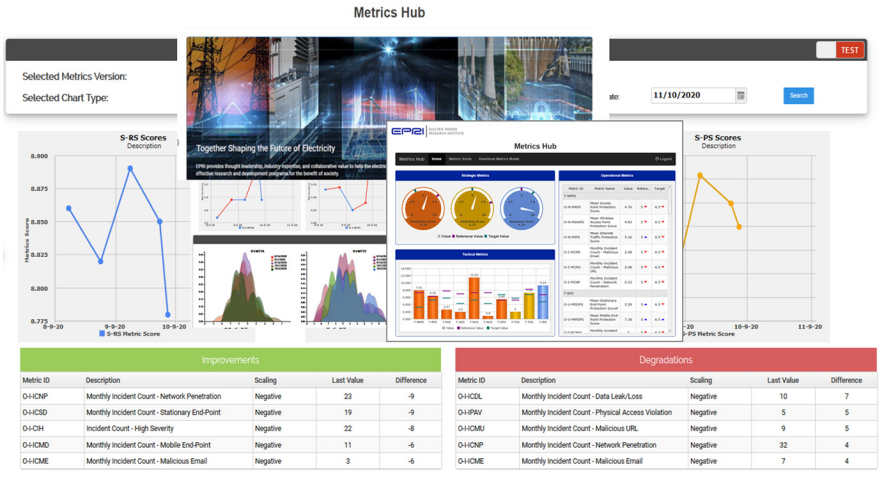

Figure 1 – EPRI Metrics Hub User Interfaces

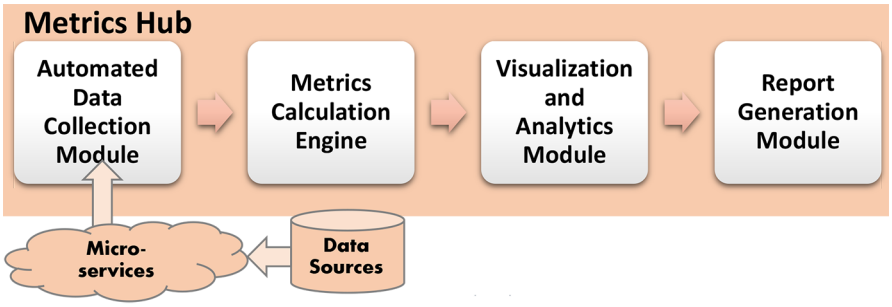

Figure 2 – EPRI Metrics Hub Architecture

Considering that EPRI security metrics are calculated from data sourced within organizations, the EPRI metrics hub utilizes an automated data collection module that interacts with local data sources within the organization, sends relevant data to the platform to calculate metrics. The visualization and analytics module display calculated metrics along with corresponding data which also provides input to the report generation module.

Organizations can deploy the EPRI metrics hub platform in two ways: Metrics Hub Enterprise and Metrics Hub Cloud respectively. With Metrics Hub Enterprise, an organization can deploy metrics hub into their operations and have full control over each component of the platform while with the Metrics Hub Cloud, some components of the metrics hub are deployed onto the cloud.

Metrics Hub Enterprise

EPRI Metrics Hub Enterprise is an on-premise deployment of metrics hub in which the utility has full control of the platform. A utility provides the infrastructures such as servers, databases, and end-user devices required to deploy and use the metrics hub. With this deployment, the utility manages every module of application including data and metrics with required support provided by EPRI whenever necessary. Figure 3 illustrates the EPRI metrics hub on-prem installation.

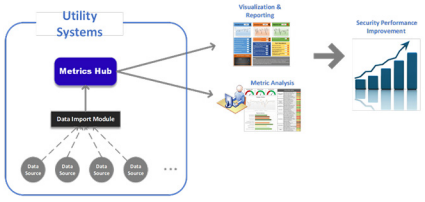

Figure 3 – EPRI Metrics Hub Enterprise On-Prem Installation

Metrics Hub Cloud

EPRI Metrics Hub Cloud is a cloud-based implementation of metrics hub also referred to as the partial off-prem deployment as shown in Figure 4.

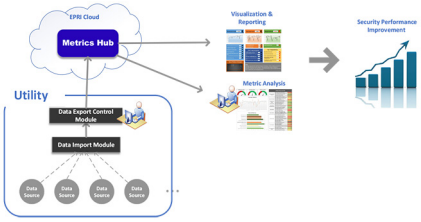

Figure 4 – EPRI Metrics Hub Cloud Partial On-Prem Installation

Metrics hub is deployed to a commercial cloud and is intended for utilities that do not have the infrastructure or simply prefer to use an external cloud. With this installation, the utility has full control of the data collection module. However, the metrics calculation engine along with the visualization and reporting module is deployed to the cloud. EPRI provides the infrastructure including servers and databases but the utility chooses how and when to interact with the metrics Hub server.

KEY FUNCTIONS

In 2017-2018, EPRI worked with 8 utilities to pilot EPRI's security metrics. The pilot enabled EPRI to identify several functions that could support organizations' efforts to operationalize EPRI's security metrics. Consequently, five crucial functions were incorporated into the EPRI Metrics Hub including 1) automated data collection, 2) metrics calculation, 3) metrics visualization, 4) insights and analytics along with 5) reporting. An overview of how metrics hub achieves each function is provided below.

Figure 5 – EPRI Metrics Hub Functions

Automated Data Collection

Data is the core of EPRI's security metrics. Each metric score is calculated from data collected inside the organization. Using measurable, repeatable, and relevant data sourced from inside the organization to calculate metric scores ensures the scores calculated are accurate. To cover all 60-security metrics, 120 data points are required. Collecting the data and updating manually is a complex and time-consuming process. EPRI metrics hub incorporates an automated data collection module that uses microservices to interact with local data sources and periodically send relevant data to the platform for additional processing. The data collected is synchronized and aggregated at the platform's processing engine before it is used to calculate security metrics.

Metrics Calculation

The data automatically collected is used to calculate security metrics. Metrics hub constitutes a metrics calculation engine that takes the data collected and applies a metrics formula to compute corresponding metrics. The metrics formulas aggregate data from various sources by taking their arithmetic, harmonic, and/or geometrics mean then calculating intermediate metrics which are further used to calculate the operational level metrics, in turn, used to calculate tactical level metrics and finally strategic level metrics. (For a detailed discussion of EPRI security metrics and formulas please see 3002010426). Each metric is assigned a weight based on its impact on the organization's security posture. In the EPRI metrics hub, each metric is assigned a default weight; however, organizations can customize metrics weights based on their needs and priorities.

Metrics Visualization

An important feature of the EPRI metrics hub is the dashboard. The dashboard displays calculated metrics along with the aggregated data used to calculate the metrics. Intuitive charts including time series plots, histograms, tables, gauges, and heat maps are used to visualize metrics. The dashboard is automatically populated using data and metrics dynamically calculated over a predefined period. The EPRI metrics hub visualization feature is customizable with each utility selecting the display that best meets their needs.

Insights and Analytics

The dashboard contains various charts that show metrics and data trends over a predefined period. Data analysts can use the EPRI metrics hub for root cause analyses and gain further insight into the trend of metrics calculated. Metrics data displayed can be drilled down examining each data point that contributed to the metric. Changes in metric scores can be readily explained and correlated with network events because the EPRI metrics hub will automatically collect data and dynamically compute and store metric scores overtime. The dashboard will display a summary of metrics that have significantly changed over time. Users can customize their dashboard to determine what insights they would like to visualize at a glance. Over time, the insights collected can inform decision-makers on risk management, resource allocations, and cyber security solutions and programs in which to invest.

Reporting

In addition to dynamically calculating metrics and displaying insights, the platform supports automated report generation. Based on metrics and data collected, a custom report can be generated. All metrics users within an organization will be able to generate a report that summarizes metric scores and data points for specific areas of interest to them. The report contains charts that highlight key changes in metric scores and insights into these changes. Reports will detail improvements and degradations along with correlation with the data collected. This correlation will allow program managers to review and evaluate cyber security practices, determine areas that need improvement, manage risk, and make informed investment decisions.

BENEFITS OF IMPLEMENTING METRICS HUB

There are several benefits to organizations that implement and use EPRI's metrics hub. In addition to allowing companies to calculate metrics that allow them to measure the performance of their cyber security programs, the EPRI metrics hub supports key functions in an organization like risk management and resource management. A few benefits to metrics hub are highlighted below.

Support for Risk Management

Risk management in cybersecurity identifies risks, vulnerabilities, and the necessary steps to ensure the organization is adequately protected. Metrics hub continuously computes metric scores that measure the performance of specific cyber security programs. Data such as asset vulnerabilities, mean time to respond or recover from incidents, number of incidents, etc. are used to calculate metrics. Over time, the scores inform risk management on what vulnerabilities and comprehensive solutions work best for these vulnerabilities.

Comprehensive Security Reporting

In addition to supporting risk management, the EPRI metrics hub also provides security reporting. The report generation module generates reports that are comprehensive and address a diverse audience which typically consists of executives, program managers, and technical staff. The metrics hub reports contain key performance indicators such as the number of incidents, mean time to response, and recovery which are of interest to technical staff directly handling incidents. Metric scores such as Detection of True Positive Rates and Network Perimeter Protection which are of interest to program managers who are directly responsible for evaluating programs and solutions in place are also reported. Executives can also benefit from the security metrics report generated by the metrics hub since it summarizes all metric scores into three strategic level scores while highlighting how the low-level scores contribute. Overall, the cyber security report metrics hub generates will facilitate discussions among practitioners or stakeholders across all tiers of cyber security operations.

Data-Driven Support for Cyber Security Investment Decisions

Information contained in reports and insights generated provide benefits beyond just keeping the organization informed. This information also helps organizations evaluate the programs, solutions, and practices that they employ for cyber security and make more effective investment decisions. Insights from the EPRI metrics hub can enable decision-makers to determine what programs are effective and need additional resources along with what pro-

grams are of no significant value and need to be retired. This is crucial for improving the organization's security posture by ensuring that effective cyber security solutions are deployed.

Overall Improvement in Cyber Security Operations

The EPRI metrics hub will contribute to an overall improvement of cyber security operations. Each metric score in EPRI's security metrics applies to a specific stakeholder. The stakeholders provide data for calculating the metrics and in turn have the benefit of metrics that continuously, quantitively evaluate their performance. Although a metrics-based approach typically exposes weaknesses in operations that were not obvious before, metric scores computed by metrics hub over time help technical staff and their management identify what operations are not performing satisfactorily and make relevant changes. The result of such a metrics-based approach to cyber security operations improves the organization's cyber security posture through meaningful incremental changes that are easy to track and can be repeated.

FURTHER INFORMATION AND WAYS TO BE INVOLVED

EPRI is currently helping utilities implement and customize security metrics in the Operationalization and Benchmarking Supplemental Project. The security metrics operationalization project is designed to support Metrics Hub implementation for companies who want to use EPRI metrics in their day-to-day operations. For more information on EPRI security metrics, please visit www.epri.com/security-metrics/ or email securitymetrics@epri.com.

FOR MORE INFORMATION

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Esther Amullen	*Engineer/Scientist II*
Program	Technology Innovation
Phone	704.595.2774
Email	eamullen@epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE NOT PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS NOT SUBJECT TO THE REQUIREMENTS OF 10 CFR PART 21.

Note

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together...Shaping the Future of Electricity

3002020222 December 2020

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

© 2020 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.