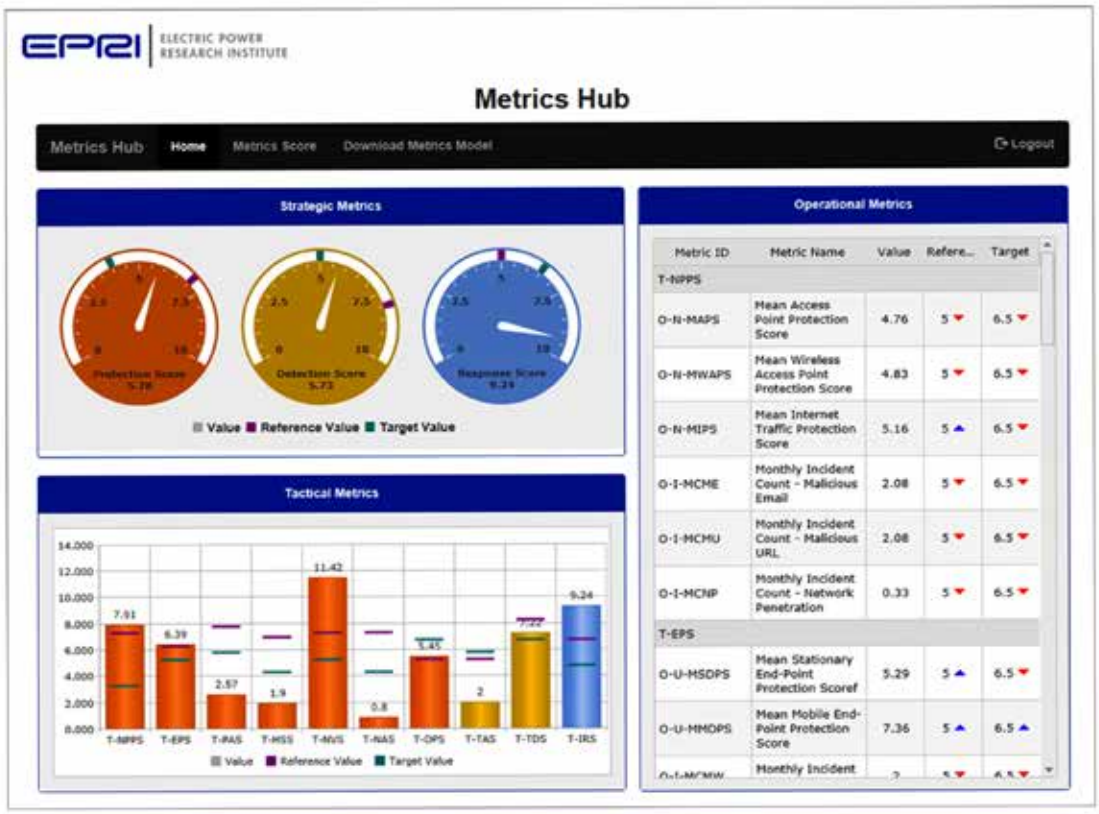

EPRI Cyber Security Metrics Operationalization Pilot with ConEd, AECC and TVA

Overview

EPRI has been building a security metrics framework to provide the electric sector with a data-driven continuous approach to evaluating the performance of its cyber security programs since 2015. EPRI identified 120 data points that can be used to calculate 60 metric scores that quantitatively reflect an organization's security posture in a consistent and repeatable way.

Eight utilities piloted EPRI security metrics between 2017 and 2018 and used them to quantitatively evaluate security programs. Key learnings from these pilots indicated a need for automated data collection, metrics visualization and root cause analysis capabilities for EPRI security metrics. EPRI's research team created a highly customizable platform called the EPRI Metrics Hub to operationalize cyber security metrics. The EPRI Metrics Hub is a web-based platform that supports automated cyber security data collection, security metrics calculation, visualization and analysis. It is a foundational tool to successfully implementing and leveraging EPRI security metrics in utility production environments.

EPRI created the EPRI Security Metrics Operationalization supplemental project to help utilities apply the EPRI Metrics Hub in their operations. Three utilities, Consolidated Edison (ConEd), Arkansas Electric Cooperative Corporation (AECC), and Tennessee Valley Authority (TVA) are currently participating in the project.

Participants identified cyber security data sources for security metrics calculations in their organizations and are currently working with EPRI to automate collection of this data for a seamless calculation process. EPRI's metrics visualization dashboard is an integral part of the EPRI Metrics Hub. The dashboard shows how utilities can

Project Lead:
Christine Hertzog
chertzog@epri.com

visualize security metrics using time series plots, histograms, tables, gauges and heat maps. Analysts can use Metrics Hub for root cause analyses and gain further insight into metrics trends through drill downs to source data. Changes in metric scores can be readily explained and correlated with network events since Metrics Hub will automatically collect data and dynamically compute and store metric scores for historical analyses.

Value Realized

Automating cyber security data collection and calculations unburdens utility resources from these routine tasks. The visualization dashboard unlocks new insights and actionable intelligence for cyber security teams that is quantifiable and consistently available. EPRI's Metrics Hub produces cyber security scores proven to be relevant to utility operations through their accurate depictions of security postures. The scores produced can be compared to reference values provided in Metrics Hub crucial for setting targets and establishing expected normal operations. Quantifiable metrics deliver a new level of confidence to utilities to support decisions that improve cyber security operations and mitigate cyber security risks. In addition, EPRI's Metrics Hub delivers intuitive visualizations of cybersecurity metrics to improve communication of results and management of cyber security risks.

Leadership/Innovation Demonstrated:

OT cyber security operations in the electric sector had no tools to quantitatively assess their own performance through an objective lens. Utilities relied upon disparate or qualitative information and anecdotal accounts to make decisions on security investments to mitigate risks. The participating utilities are helping to structure objective and quantitative evaluations of OT cyber security performance through a data-driven and consistent development of relevant metrics.

The lessons learned through this collaborative metrics operationalization effort will enable EPRI researchers to refine metrics formulae and underlying data points and more granularly describe utility security operations performance. As digitalization initiatives continue to impact utility cyber security operations, the Metrics Hub will enable more data collection and aggregation from new sources and deliver more actionable intelligence to inform risk mitigation decisions.

"The EPRI security metrics have the potential to provide detailed insight into the performance of ConEd's cyber security programs through the EPRI Metrics Hub. This tool will add tremendous value to our operations by allowing us to make data-driven decisions on what areas of our cyber operations can be improved and how. ConEd is looking forward to the completion of the metrics operationalization project and integrating metrics into our operations."

Mikhail Falkovich, Director-Information Security, ConEdison

TO JOIN OR FOR MORE INFORMATION, CONTACT THE FOLLOWING TECHNICAL ADVISORS:

West: *Brian Dupin*
650.906.2936
bdupin@epri.com

East: *Chris Kotting,*
980.219.0146;
ckotting@epri.com

Southeast: *Barry Batson*
704.595.2873
bbatson@epri.com

International: *Thomas TerBush,*
International Director,
+1 202.293.6344
TTerBush@epri.com

Product ID: 3002020729

March 2021

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