PROTECT
OUR
POWER

Best Practices in Cybersecurity for Utilities

Educational Institutions (EIs) - Work Products

https://protectourpower.org/best-practices/pop-bp-ei-work-products.pdf

Introduction

Protect Our Power is comprised of experts from electric utility industry, the physical and cyber defense communities, finance and government. The group's bipartisan Advisory Panel has a singular focus to strengthen the nation's electrical power grid.

One of Protect Our Power's projects (Overview), has the objective of identifying Best Practices in cybersecurity for utility practitioners. This paper defines the work products expected from a selected Educational Institution for the Topic selected.

ProtectOurPower.org maintains a section of its website related to this project.

When considering the Work Products, it is helpful to continuously revert back to the 2 primary goals of the Project: 1 – to increase the speed at which the utilities are able to act, and 2 – expose and encourage the utilities to use Best Practices.

The Utilities are basically on a 3-5 year tech cycle on cyber - so when it comes time to reconsider a cyber-Topic (see the Taxonomy), the literature search comes into play because it is meant to organize into one place all the things a utility would have to look at to be smart about the subject. Basically, it is simply organizing and documenting what is available to help utilities within a given Topic area.

That contributes to goal #1 - because each of the 3000 electric utilities does not have to do that work, you will have already done it. So that's the best way I can describe the "Literature Search." Those words might conjure up something else, but what we are trying to do is described above.

Re goal #2 - the Competitor Analysis Matrix allows a utility to see who are the best vendors for the criteria they are interested in (the buying criteria are what you need to specify for the columns in the Matrix. Having the Matrix and being able to play with it a bit accomplishes goal #2 as best we can.

Expected work products include:

1. A Literature Review
2. A Vendor Discovery Search
3. Criteria Identification and Definition
4. A Comparative Analysis Matrix
5. A Best Practices conclusion paper

These work products are intended to provide a body of knowledge to a utility company seeking products or services from a vendor to address a specific cybersecurity need, issue or concern within a specific Best Practices topic area. This information should significantly jump-start and guide a utility's decision-making process within the subject matter studied.

A Literature Review

The Literature Review[1] is a Word document that delineates the pertinent references found (with links) that would be of interest to a utility involved in making buying decisions within the Topic Area. It may be different than what people conjure up by the words: "Literature Review."

The Utilities are basically on a 3-5 year tech cycle on cyber - so when it comes time to reconsider a cyber-Topic (see the Taxonomy), the literature search comes into play because it is meant to organize into one place all the things a utility would have to look at to be smart about the subject. Basically, it is simply organizing and documenting what is available to help utilities within a given Topic area.

That contributes to goal #1 - because each of the 3000 electric utilities does not have to do that work, the Literature Search addresses that need.

A Vendor Discovery Search

[1] The University of West Florida provides a webpage – and 3 examples that should guide the format of this deliverable.

Protect Our Power will supply an initial list of vendors within the topic area. Protect Our Power will also supply contact information for vendor personnel assigned to work with the educational institution. The initial list may not, however, be complete and the educational institution should identify additional vendors within the assigned topic area that have been overlooked. Information regarding each additional vendor identified should be provided to Protect Our Power so that appropriate contacts can be identified for use by the educational institution. Ultimately, the Taxonomy should sync with the list that the Educational Institution has selected.

What are we looking for in a final list? Theoretically, we are looking for the list of viable companies that sell the product/service related to the Topic (a sub-component of Cybersecurity). That could be a very long list, but in no case do we really need more than 30 companies (Educational Institutions may self-choose to do more). A target is to identify at least 80% of the viable companies in the vendor universe (under a specific Topic).

Criteria Identification and Definition

Criteria must be defined against which vendors within a topic are can be evaluated. Some of the criteria will be common to all topics (I.e., Common Criteria), which are not topic-specific but rather apply to all topics generally and are of importance in utility decision-making. These Common Criteria are included in the Comparative Analysis Matrix Template, and are given to the educational as standard columns in the matrix. A Topic Area may, however, have unique characteristics that require additional criteria (Unique Topic Criteria) to be defined. Protect Our Power will support efforts to obtain suggestions from vendors within a topic area to help define the Unique Topic Areas, but the educational institution will make the final decision on the criteria used to evaluate all vendors. Links to Criteria related information are as follows:

1. ***Criteria Advisory Board on POP website*** - https://protectourpower.org/bestpractices/criteria-advisory-board/
2. ***Criteria Advisory Board document*** - https://protectourpower.org/best-practices/pop-bp-ab-criteria.pdf
3. ***Criteria Discussion Document*** - https://protectourpower.org/best-practices/criteria-discussion.pdf
4. ***Spreadsheet related to Common Criteria*** - https://protectourpower.org/best-practices/criteria-common.xlsm
5. ***Spreadsheet related to Specific Criteria*** - https://protectourpower.org/best-practices/criteria-specific.xlsm

Analysis Matrix

The Comparative Analysis Matrix is an Excel Workbook with a spreadsheet that lists all the vendors in the topic area as rows, and all the criteria related to the topic as columns. The educational institution will enter an indicator in each row-column cell that indicates the strength of a vendor's capability within each criterion.

The Analysis Matrix also contains a Worksheet where each Vendor is mapped to MITRE's Attack Framework – see https://attack.mitre.org/. The Educational Institution should query the Vendors to obtain initial mappings, and then use that data set – altering where the Educational Institution has a different conclusion.

This generally addresses goal #2 mentioned above. The Competitor Analysis Matrix allows a utility to see who are the best vendors for the criteria they are interested in (the buying criteria are what you need to specify for the columns in the Matrix.) Having the Matrix and being able to play with it a bit accomplishes goal #2 as best we can.

Links to additional related documents are:

1. ***Vendor Comparison Matrix Documentation*** - https://protectourpower.org/best-practices/pop-bp-vendor-comparison-matrix-documentation.pdf
2. ***Vendor Comparison Matrix Master*** - https://protectourpower.org/best-practices/pop-bp-vendor-comparison-matrix.xlsm
3. ***Vendor Comparison Matrix (for data entry)*** - https://protectourpower.org/best-practices/pop-bp-vendor-comparison-matrix.csv

A very helpful approach is for the Educational Institution to provide a Matrix Fragment early in the process (after identifying the initial Vendor base within the Topic (see Work Product #2). A Matrix Fragment is just part of the Vendor Comparison Matrix – containing at least a subset of Vendors (rows) and a subset of Criteria (columns). The entries in the body of the Matrix can be real, temporary, or even made-up for now. A Matrix Fragment should be submitted using the .csv excel workbook (see #3 in the above list).

The Matrix Fragment helps to ensure POP and the Educational Institution are "on the same page" regarding what needs to be produced. The Fragment also allows POP to adjust its software (which returns to the Educational Institution a formatted Matrix [2]and Vendor Score calculations (i.e. a score for a Vendor using the Educational Institution's ratings in the body of the Matrix.)

Best Practice Conclusion Paper

The body of research generated should provide a sound basis for a short paper discussing the topic and ending with a Best Practice recommendation. The recommendation need not select a vendor, but might point to strengths of various vendors as examples that help put the recommendation(s) into context. The Best Practice recommendation may also point to sources of information (such as those discovered in the Literature Search) that are different than the vendor set for the Topic but support the final Best Practices recommendation.

Articles and information that are beneficial to connect with an Educational Institution's Conclusion Paper include:

1. **American Water Works Association Cybersecurity Report** - https://cultureofresilience.com/Articles/AWWA_Cybersecurity_Report.pdf
2. ***A Collection of Resources for Getting Started in ICS SCADA Cybersecurity*** – Robert M. Lee - https://github.com/ITI/ICS-Security-Tools/blob/master/guides/roblee.md
3. ***Cyberspace Solarium Commission*** - https://www.solarium.gov/ and their final report - https://www.solarium.gov/#h.p_rK7mL_1MeZw7
4. ***MITRE ATT&CK -*** is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. https://attack.mitre.org/
   a. Also see Threat Modeling of ICS Incidents/Failure Scenarios (Cyber) using ATT&CK for ICS by Harry Perper (Chief Engineer, National Cybersecurity FFRDC The MITRE Corporation) – at https://energycollection.us/Companies/MITRE/Threat-Modeling-ICS.pdf
5. ***Mapping to the NIST Cybersecurity Framework –*** example by Indegy - https://energycollection.us/Companies/Indegy/Adhering-NIST-Framework.pdf

[2] See this document for an example completed Matrix Fragment - https://protectourpower.org/best-practices/pop-bp-vendor-comparison-matrix-example.pdf

6. ***OT Security Best Practices (Gartner)*** - https://www.energycollection.us/Companies/Gartner/OT-Security-Best-Practices.pdf
7. ***Process Control System Security Guidance for the Water Sector*** - The cybersecurity practices are a set of recommendations for improving the security posture of the process control systems (PCS) used by water and wastewater utilities. They are actionable recommendations designed to produce maximum improvement in the short term, and lay the foundations for longer term implementation of complex security programs and controls. https://cultureofresilience.com/Articles/PCS_Security-Guidance.pdf and Cybersecurity Tool - https://EnergyCollection.us/Companies/American-Water-Works/Cybersecurity-Tool.pdf
8. A ***Survey of Security Tools for the Industrial Control System Environment*** - 2017-05-01 - by Idaho National Laboratory - This report details the results of a survey conducted by Idaho National Laboratory (INL) to identify existing tools which could be used to prevent, detect, mitigate, or investigate a cyber-attack in an industrial control system (ICS) environment. This report compiles a list of potentially applicable tools and shows the coverage of the tools in an ICS architecture. https://cultureofresilience.com/Articles/Survey-Security-Tools.pdf

Use by the Utilities

Protect Our Power maintains an extensive mailing list of utility cyber practitioners that have expressed interest in the work products associated with Best Practices in cybersecurity. Due to the vast set of capabilities needed to protect the grid from cyber-events, utilities may deploy new technology in several topic areas within each year, and may cover all the topic areas in a multi-year cycle. The topics selected by any utility for review depend on many factors, including: technology advances by vendors; a changing threat landscape; or, compatibility issues with other solutions. As an educational institution completes its work in a topic area and the work products are distributed to the utilities, they may reach out to the educational institution for further insight or work within the topic analyzed; these utility/educational institution relationships and the possibility for additional work can and should flourish independent from Protect Our Power.

Contact

Erick Ford | Project Manager
eford@protectourpower.org