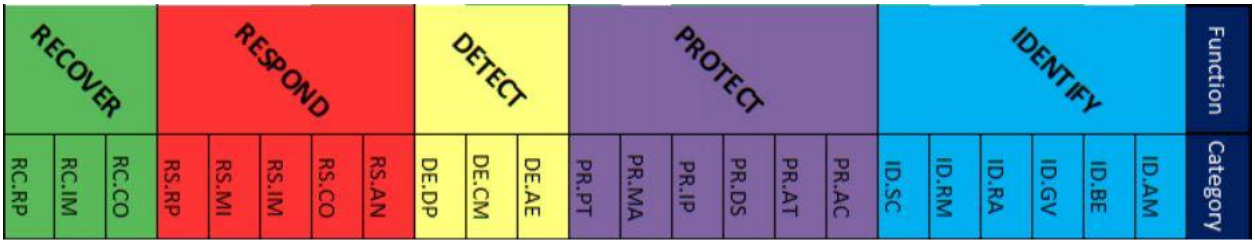

Overview of the Enterprise Security Profile Model

Summary

The Enterprise Security Profile Model (ESPM) is based upon the mapping of security controls, the measurement of those controls, and the metrics showing the security profile score. The ESPM provides a line-of- sight from the executive management perspective to the operational activities where the security controls are needed.

The ESPM aligns multiple security control sets to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). All of the security controls, regardless of the origin, are measured within a unique environment in order to provide a cumulative security profile for the entire enterprise.

Overview

The intent of this introductory document is to demonstrate that when security control sets align to the NIST CSF they can produce a quantitative security profile metric derived from operational measurements of organizational security controls. The ESPM provides a business perspective focused on the risk profile of an enterprise.

The CSF, with its informative reference, encompasses all controls throughout the entire organization and extends to the supply chain management. Many additional security control sets can align to the CSF to expand the reference of the high-level control descriptions. The HIPAA and PCI DSS control sets, focus on a specific category of data that needs protection while others, like the NIST SP 800-53, are designed to address security controls at the operational level. Organizations manage many control sets at the same time. Mapping, measuring and metrics contained in a single model will purposefully demonstrate the areas of strength and weakness as a part of a risk management strategy.

Mapping to the NIST CSF

Alignment

There are many control sets that must be managed in an enterprise. When each control set is aligned to a central framework such as the NIST CSF, the input of measurements and output of reports is simplified. An alignment of control sets forms an organizational security control catalog. When a security control is associated with an asset, such as a server, it can be associated with the single framework rather than multiple control sets. The single control referenced in the framework is the hub of the associated control sets.

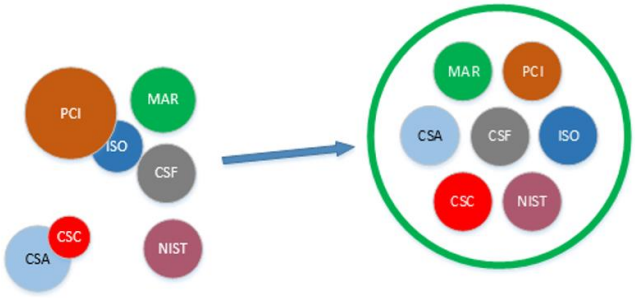

Figure 1: Mapping Control Sets in a Catalog

Vertical Comparison

It is common to see security controls mapped to other vendors controls in a horizontal comparison. For example, the Cloud Security Alliance control matrix has its proprietary controls listed in column A on a spreadsheet and the mapping to other controls are listed across many columns on the same row. The ESPM maintains each control on a single row (Control ID) and the mapping occurs vertically, found above or below each control row in Figure 2. (See Appendix A for the brief taxonomy of controls description).

STN	ON/OFF	CSF Function		CSF Category		CSF Subcategory	Priority	Control Set Source	Control ID	SRM Description
1.1-0.0	X	ID	1	AM	1	0	0	NIST CSF 1.1	ID.AM-0	Asset Management (ID.AM)
1.1-0.1	X	ID	1	AM	1	0	1	NIST CSF 1.1	ID.AM-0	The data, personnel, devices, systems, and fa
1.1-1.0		ID	1	AM	1	1	0	NIST CSF 1.1	ID.AM-1	Physical devices and systems within the orga
1.1-1.1		ID	1	AM	1	1	1	Critical Security Controls 6	1.1	Deploy an automated asset inventory discove
1.1-1.1	ON	ID	1	AM	1	1	1	NIST SP 800-53 Rev. 4	CM-8(1)	INFORMATION SYSTEM COMPONENT INVENT
1.1-1.1	ON	ID	1	AM	1	1	1	NIST SP 800-53 Rev. 4	CM-8(7)	INFORMATION SYSTEM COMPONENT INVENT
1.1-1.1	ON	ID	1	AM	1	1	1	NIST SP 800-53 Rev. 4	PM-5	INFORMATION SYSTEM INVENTORY
1.1-1.2		ID	1	AM	1	1	2	PCI DSS 3.2	2.4	Maintain an inventory of system components
1.1-1.2		ID	1	AM	1	1	2	PCI DSS 3.2	11.1.1	Maintain an inventory of authorized wireless a
1.1-1.2		ID	1	AM	1	1	2	PCI DSS 3.2	9.9.1	Maintain an up-to-date list of devices. The list
1.1-1.3		ID	1	AM	1	1	3	ISO/IEC 27001:2013	A.8.1.1	Inventory of assets - Assets associated with ir
1.1-1.4		ID	1	AM	1	1	4	Critical Security Controls 6	1.1	Deploy an automated asset inventory discove
1.1-1.4		ID	1	AM	1	1	4	Critical Security Controls 6	1.4	Maintain an asset inventory of all systems co
1.1-1.5		ID	1	AM	1	1	5	COBIT 5	BAI09.02	Manage critical assets. Identify assets that ar

Figure 2: Contol Comparison

Measurements

Together, the NIST CSF categories and the NIST SP 800-53 controls provide a spectrum of high-level views and the data centric, operational perspective. Providing accurate metrics requires specific measurements of the controls in the environments within which they are implemented. For example, if the security control of Asset Management was selected with the Critical Security Controls set, the control number of 1.1 (STN of 1.1-1.4) would be measured in two ways. One, it would receive a score signifying that it was installed and be turned "ON." Two, the performance of the control would be measured on a percentage scale between 1% and 100%. The result will be that the asset is identified for the Linux server in the cardholder data environment and can be reported as 75% effective control for this system.

STN	ON/OFF	CSF Function		CSF Category		CSF Subcategory	Priority	Control Set Source	Control ID	SRM Description	Rate	Weight	Assess	Analyze	N/A	Environments 1 2 3 4 5 6 7 8 9 10
1.1-0.0	X	ID	1	AM	1	0	0	NIST CSF 1.1	ID.AM-0	Asset Management (ID.AM)		100%	1			
1.1-1.0	ON	ID	1	AM	1	1	0	NIST CSF 1.1	ID.AM-1	Physical devices and systems within the organization are inventoried	99	100%	1	99		99
1.1-1.4	ON	ID	1	AM	1	1	4	Critical Security Controls 6	1.1	Deploy an automated asset inventory discovery tool and use it to build	75	100%	1	75		75

Figure 3: Measurements in the ESPM

Metrics

Cumulative Scoring

Opening the dashboard tab on the ESPN spreadsheet provides an enterprise perspective in which security controls are enabled (ON) to provide a cumulative control set score. The security

profile is derived from the layers of security control set evaluations and from different environments. This layering and cumulative scoring provides a quantitative result from the distinct control categories. Each value of the control set scoring is the aggregation of the scores for the security controls selected in each environment. If the control is determined to be active, it is turned ON and uniquely measured. The average score in the Description worksheet for each control selected in each environment is added to the sub-category cells on the dashboard. The sub-categories are averaged together to form the category score (the Control Catalog Score). From there values are averaged into the Functional Score and then into the final Security Profile Score.

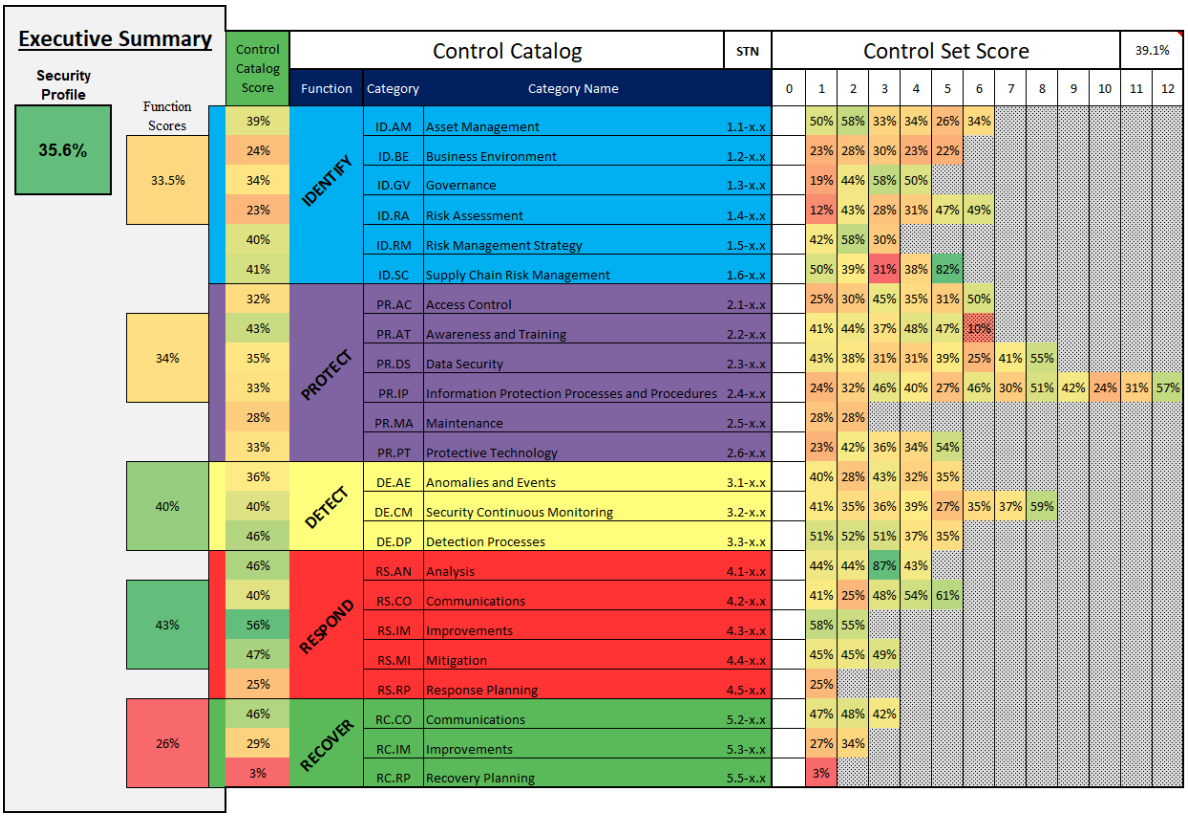

Figure 4: ESPM Dashboard

Conclusion

The ESPM aligns multiple security control sets to the NIST Cyber Security Framework. All of the security controls, regardless of the origin, are measured within a unique environment in order to provide a cumulative security profile for the entire enterprise.

The CSF provides an overall measurement for all security controls throughout the organization. When the CSF is coupled with the ESPM there is an overall qualitative risk management improvement in the score. The ESPM moves closer to a quantitative score as the control set is measured in at an operational level rather than a high-level maturity model evaluation.

Download the latest ESPM at http://www.veritysecurity.com/home/espm

Appendix A: Security Taxonomy Number

Operational Evaluation

The Security Taxonomy Number (STN) is the index number for the Enterprise Security Profile Model. The STN creates a hierarchy which associates the NIST Cyber Security Framework (CSF) with the distinct security control sets, such as PCI DSS, HIPAA, ISO 27001, COBIT and the NIST SP 800-53 document. It is used as a reference to multiple layers of management evaluation. The STN is a layer of abstraction that enables members of an organization to communicate and reference security controls without separating the alignment of controls during the discussion. In other words, an internal information security policy can name a single STN rather than list all of the security controls from each applicable control set.

At the highest level, the Protect function can be evaluated by the Executive management team. The Access Control (AC) category can be evaluated for improvement by the management team. Each unit can identify the related Separation of Duties (2.1-4.0) for their area of responsibility. An assessment of the control can be completed with the separate control sets mapped to a STN for the specific control instructions. For example, the ISO 27001 control A.6.1.2 is mapped to PR.AC-1 with an STN of 2.1-4.2, depicted as "Separation of Duties."

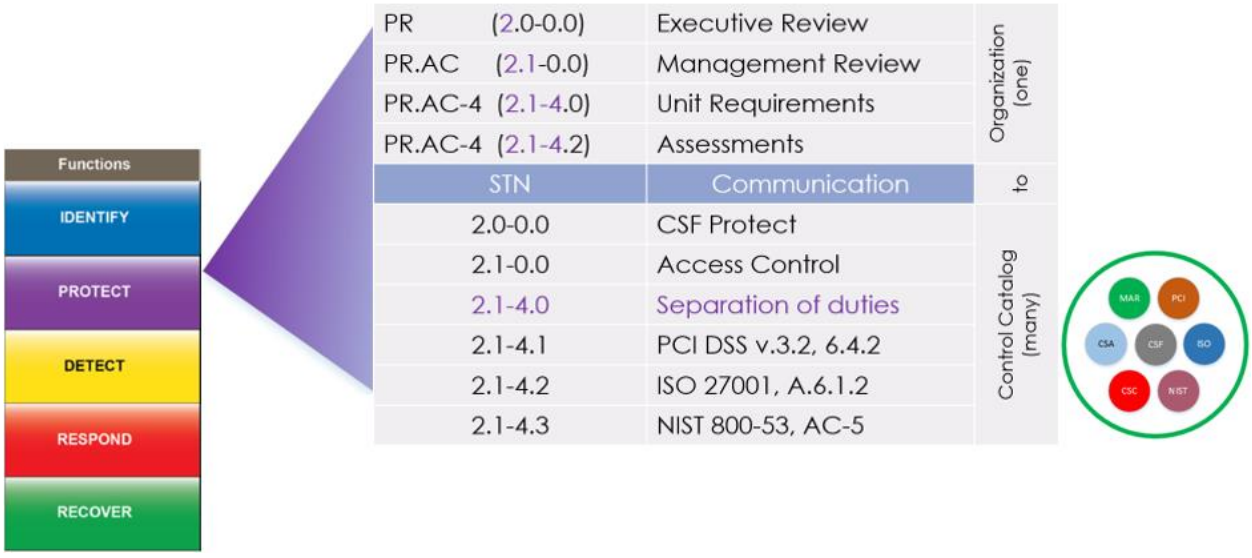

Figure 5: Taxonomy of Security Control Sets

A Chief Information Security Officer (CISO) or the Director of Security may ask, "What do we need to do to improve this score?" They will review the control catalog score column and describe the areas where there is a weakness or where they can achieve the greatest value with the available resources. The Director may focus on the lowest CSF Function Score to find a low control set score that is at the greatest risk. By looking at the layered security control sets within the Security Taxonomy (STN) the Director can identify where the specific security control needs to improve.

Appendix B: Evaluation Method

ESPM Evaluation Steps

1. Select the environment.
    a. Usually focus on the highest data classification.
    b. This data type may travers multiple environments throughout or external to the enterprise. Multiple environments may need to be evaluated in the assessment.
2. Apply a score to each security control for the environment column.
    a. Utilize the BRAAT method (http://www.veritysecurity.com/home/espm, derived from the NIST SP 800-37 document.
3. Review the Dashboard Control Set Scores.
4. Evaluate the CSF Category for each of the cumulative Control Set Scores.
5. Create a report or presentation based upon the Executive summary and the Security Profile for the data type or for the entire organization.
    a. Include the operational systems from where the security control ratings were derived.
    b. Include a business case or cost analysis for each system and a total recommended line item budget for each change.
    c. Demonstrate the Current Profile and the Target Profile based upon the recommended improvements.