MAKING SECURITY MEASURABLE AND MANAGEABLE

Robert A. Martin
The MITRE Corporation
Bedford, MA

ABSTRACT

The security and integrity of information systems is a critical issue within most types of organizations. Finding better ways to address the topic is the objective of many in industry, academia, and government. One of the more effective approaches gaining popularity in addressing these issues is the use of standard knowledge representations, enumerations, exchange formats and languages, as well as sharing of standard approaches to key compliance and conformance mandates. These efforts fall into four basic building blocks of registries, languages/formats, standardized usage, and standardized processes. By establishing standardized and segregated interactions amongst their operational, development and sustainment tools and processes organizations gain great freedom in selecting technologies, solutions and vendors as well as easing the burden of work force training and sharing of information since the concepts and terminology becomes more ubiquitous versus vendor/implementation specific. The "Making Security Measurable" initiatives provide the foundation for answering today's increased demands for accountability, efficiency and interoperability without artificially constraining an organization's solution options.

INTRODUCTION

Over the past thirteen years, MITRE and others have developed a number of information security related standardizations that are increasingly being adopted by vendors and forming the basis for security operations management and measurement activities across wide groups of industry and government. This paper explores how these standardized registries, usage, languages and processes are facilitating the use of automation to assess, operate, and improve the security posture of enterprise security information infrastructures while also fostering resiliency and effective security coordination across the adopting organizations.

The basic premise of the "Making Security Measurable" effort is that for any enterprise to operate, measure, and manage the security of their cyber assets they are going to have to employ automation. For an enterprise of any reasonable size that automation will have to come from multiple sources. To make the finding, sharing, and reporting issues consistent and composable across different tools and partners there has to be a set of standardized definitions of the things that are being examined, reported, and managed by those different tools and described by different information sources. That standardization is what comprises the core of the "Making Security Measurable" efforts.

Information security operation, measurement and management, as originally practiced, is complex, expensive, and fraught with unique activities and tailored approaches. Solving the variety of challenges that were facing enterprises with regards to incident and threat analysis and management, patching, application security, and compliance management required fundamental changes in the way vendor technologies are adopted and integrated. These changes include the way enterprises organize and train to utilize these capabilities. Likewise, to support organizational discipline and accountability objectives while enabling innovation and flexibility, the security industry needed to move to a vendor neutral security operations, management and measurement strategy. The strategy had to be neutral to the specific solution providers while also being flexible enough to work with several different solutions simultaneously. Finally, the new approach had to enable the elimination of duplicative and manual activities, improve resiliency, and the ability of organizations to leverage outside resources and collaborate with other organizations facing the same threats and risks.

These objectives are being met by bringing architecturally driven standardization to the scoping and organization of the information security activities that our enterprises practice. By acknowledging the "natural" groupings of activities or domains that all information security organizations address—independent of the tools and techniques they use—a framework has been established within which organizations can organize their work independent of their current technology choices and flexible enough to adapt to tomorrows offerings. Likewise, by ex-

amining these domain groupings and the types of practices of coordination and cooperation that persist across and between them, it is possible to improve interoperability and independence of these groups by standardizing common concepts in the information that flows across and between them. These shared concepts are sometimes referred to as "boundary objects" and are a phenomenon known to those who study inter-community communications[1], but have not been leveraged explicitly for information security standardization.

RECASTING CYBER SECURITY PRACTICES USING ARCHITECTURE AND SYSTEMS ENGINEERING PRINCIPALS

In this paper we discuss how by leveraging the practices of systems engineering [1] we have recast our original cyber security solutions into a launching point for standardized functional decomposition-based security architectures. These architectures provide for a flexible, logical, and expandable approach to building and operating cyber security solutions for the enterprise, and one that improves resiliency and is more supportive of security operations, measurement, management, and sharing goals.

In this paper we look at the collection of cyber security related activities that most enterprises practice including inventorying assets; analysis of system configurations; analysis of systems for vulnerabilities; analysis of threats; studying intrusions; sharing indicators; reporting and responding to incidents; change management; assessing systems development, integration, and sustainment activities; and certification and accreditation of systems being deployed into the enterprise. (Note that this is an integrated list that includes activities tied to the operation of systems in the enterprise as well as those they create, deploy, and update systems.)

We also examine the different types of information that have been identified to support these activities. Finally, we identify the key activities and information that needs to be sharable and unambiguous in and amongst the different functions of today's cyber security environment. By identifying and collecting these functional components as standardized reusable concepts, we illustrate one of the major benefits that architecture brings to the study of security in the enterprise information technology landscape.

[1] Bowker and Star, *"Sorting Things Out"*, ISBN 0262522950, MIT Press, 1999.

ARCHITECTING SECURITY

We can lay the foundation for architecting measurable security by looking at security operations, measurement and management as an architecture issue and using a systems engineering approach to functionally decompose it, identifying the basic functions and activities that need to be done, and then getting appropriate technology to support the functions and activities.

Through the development and adoption of standardized enumerations, the establishment of languages and interface standards for conveying information amongst tools and organizations, and by sharing guidance and measurement goals with others by encoding them in these standard languages and concepts, organizations around the world can dramatically change the options available to address security of the enterprise's cyber environment. By then collecting the enumerations and shared repositories of standards-based guidance in publicly available registries and using them in standardized ways we can enable a vendor neutral ecosystem of information that multiple tools, practices, and organizations can interact with with no other a priori discussions or effort other than conforming to the usage requirements or the language and format specifications used to capture information in the registries.

The U.S. federal government and commercial enterprises have deployed new approaches to security measurement and management that leverage interoperability standards and enable enterprise-wide security operations measurement and policy compliance efforts. These security architecture driven operations measurement and management standardizations [2] are providing ways for these organizations to create test rules about their organization's minimum secure configurations, mandatory patches, and/or unacceptable coding practices that can be continuously assessed, reported, and any subsequent remediation steps planned, executed, and confirmed using commercial tools and standardized activities and practices. At the same time, these standardized items also provide a basis for repeatable, trainable processes and sharing along with enabling automation-based testing methods for deployment validation and regression testing throughout the operational lifetime of the systems.

Maybe more importantly, the establishment of architectural methods within the cyber security community is helping to open the doors to more resilient, faster, and better coordinated approaches to dealing with the next set of security problems. There is little doubt that each and every one of the current solutions being implemented to fight today's threats will be attacked in-turn by advances

in how systems and enterprises are attacked. But with a more consistent basis for understanding these new threats and methods, solutions can be leveraged faster and applied in more predictable time frames, shared more quickly, and with more understanding for the risks that remain.

BUILDING BLOCKS FOR ARCHITECTING MEASURABLE SECURITY

We believe there are four basic building blocks for architecting measurable security:

- Standardized enumerations of the common concepts that need to be shared.
- Languages for encoding high-fidelity[2] information about how to find the common concepts and communicating that information from one human to another human, from a human to a tool, from one tool to another tool, and from a tool to a human.
- Sharing the information through repositories of content[3] in languages for use in broad communities or individual organizations in a way that minimizes loss of meaning when content is being exchanged between tools, people, or both.
- Uniformity of adoption achieved through branding and vetting programs to encourage the tools, interactions, and content remain standardized and conformant.

The following sections discuss these building blocks in more detail.

ENUMERATIONS

Enumerations catalog the fundamental entities and concepts in information assurance, cyber security, and software assurance that need to be shared across the different disciplines and functions of these practices. The June 2007 National Academies report on the state of cyber security and cyber security research, "Towards a Safer and More Secure Cyberspace," [3] highlighted that metrics and measurements particularly rely on enumerations. As an example the report cited the Common Vulnerabilities and Exposures (CVE®) [4] list run by MITRE Corporation under funding from the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security (DHS), as an enumeration that enables all kinds of measurement by providing unique identifiers for publicly known vulnerabilities in software. There are a number of enumerations in the information assurance, cyber security, and software assurance space. Some examples are shown in Table 1.

Table 1. Enumerations

Name	Topic
Common Vulnerabilities and Exposures (CVE®)	Standard identifiers for publicly known vulnerabilities
Common Weakness Enumeration (CWE™)	Standard identifiers for the software weakness types in architecture, design or implementation that lead to vulnerabilities
Common Attack Pattern Enumeration and Classification (CAPEC™)	Standard identifiers for attacks
Common Configuration Enumeration (CCE™)	Standard identifiers for configuration issues
Common Platform Enumeration (CPE™)	Standard identifiers for platforms, operating systems, and application packages
SANS Top-20	Consensus list of the most critical vulnerabilities that require immediate remediation
Open Web Application Security Project's (OWASP) Top Ten	List of the ten most critical Web application security flaws
Web Application Security Consortium's (WASC) Threat Classification	List of Web security attack classes
CWE/SANS Top 25 Most Dangerous Programming Errors	Consensus list of the most dangerous types of programming errors that require immediate attention.

LANGUAGES

Standardized languages and formats allow uniform encoding of the enumerated concepts and other high-fidelity information for communication from human to human,

[2] High fidelity refers to the level of detail of the information encoded in a language that is sufficient to convey the understanding and knowledge of the one encoding the information to the one who decodes the information. If a person writes a test for how to check a configuration setting in a language then that language needs to be able to convey the specifics of the test so that another person or a tool reading the check as written in the language understands enough about the check to actually perform the test that was intended by the original author. If a language cannot retain the fidelity of the information to support this then it is not of sufficient fidelity.

[3] Content repositories are currently envisioned to be collections of tests to verify settings, patches, and installed software on systems to comply with organizational policies about their information technology systems and processes. Repositories are typically meant to be understandable by humans but used by tools to automate checking for compliance with the tests in the repository. Many different organizations are hosting public and private repositories already and we anticipate that to continue and expand as the need to share grows.

human to tool, tool to tool, and tool to human. For example, a configuration benchmark document written in the XCCDF and OVAL languages [5, 6] would be readable by a human and it would be consumable by an assessment tool, in that the tool would be able to directly import the tests and checks that are expressed in the document. As with the enumerations, there are a number of information assurance, cyber security, software assurance measurement and management oriented languages and formats. Some examples are shown in Table 2.

Table 2. Languages

Name	Topic
Extensible Configuration Checklist Description Format (XCCDF)	An XML specification language for writing security checklists, benchmarks, and related kinds of documents
Open Vulnerability and Assessment Language (OVAL®)	An XML language for writing assessment tests about the current state of an asset and expressing the results
Common Vulnerability Scoring System (CVSS)	A method for conveying vulnerability related risk and risk measurements
Assessment Result Format (ARF)	A standardized IT asset assessment result format that facilitates the exchange and aggregation of assessment results
Open Checklist Interactive Language (OCIL™)	An XML language for writing assessment tests about non-automated security checks about assets and expressing the results
Common Event Expression (CEE™)	A language and syntax for describing computer events, how the events are logged, and how they are exchanged
Malware Attribute Enumeration and Characterization (MAEC™)	A language for describing malware in terms of its attack patterns, detritus, and actions
Common Frameworks for Vulnerability Disclosure and Response (CVRF)	An XML-based format for reporting and sharing vulnerability information among multiple organizations
Common Weakness Scoring System (CWSS™)	A method for conveying weakness related risk and risk measurements
Cyber Observable Expression (CybOX™)	A language for describing cyber observables

REPOSITORIES

Repositories allow common, standardized content to be used and shared, whether across broad communities or within individual organizations. The sharing of content has been done for some time but doing so in standard machine-consumable languages and formats using standard enumerated concepts is fairly recent. Most of the listed repositories are in the midst of converting their content into machine-consumable form. Examples are shown in Table 3.

Table 3. Repositories

Name	Topic
Department of Defense Computer Emergency Response Team (DoD-CERT)	Information Assurance Vulnerability Alerts (IAVAs) and Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGS)
The Center for Internet Security (CIS)	CIS Security Configuration Benchmarks
National Security Agency (NSA)	NSA Security Guides
National Vulnerability Database (NVD)	U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references
National Checklist Program (NCP) Repository	U.S. government repository of publicly available security checklists/benchmarks
United States Government Configuration Baseline (USGCB)	U.S. government repository of security configuration baselines for IT products deployed across federal agencies that is expressed as SCAP XML documents
Red Hat Repository	OVAL Patch Definitions for Red Hat Errata security advisories
OVAL Repository	OVAL Vulnerability, Compliance, Inventory, and Patch Definitions

These are all examples of very public repositories with a variety of types of content that will be recast into standardized machine-consumable form using some of the Languages identified in Table 2 and the Enumerations in Table 1. However, there are also closed repositories where, for instance, a company may write a tailored set of policies about what they want to do to comply with Sarbenes-Oxley or something similar. They don't necessarily want

to share this with the world, but they do want to be standard across all of the different elements of their company and they want it available for their auditors and possibly their partners.

UNIFORMITY OF ADOPTION

Uniform adoption of standards by the community is best achieved through branding/vetting programs that can help the tools, interactions, and content remain conformant with the accepted usage of the standardized items.

MITRE's CVE project employs a highly successful CVE Compatibility Program that has vetted numerous information security products and services to ensure they are "CVE Compatible," that is, that they use CVE in a manner supports interoperation with other products that are also compatible and that they each have correctly mapped their capabilities concept of a particular vulnerability to the correct CVE Identifier for that vulnerability. Similarly, OVAL and CWE employ similar programs about promoting common usage of their respective items. The National Institute of Standards and Technology (NIST) also has a SCAP Validation Program for those vendors that currently provide, or intend to provide, SCAP-validated tools.

All of these programs, and others that may be developed in the future, will help ensure consistency within the security community regarding the use and implementation of the standardized items. They also assure users that the tools, services, and information from those organizations adopting the items are doing so correctly and there is a high confidence that they will work correctly when the tools and services are used together.

HOW THE ARCHITECTURAL BUILDING BLOCKS COME TOGETHER

The building blocks of architecting for measurable security are already in use in the enterprise security areas of configuration compliance assessment, vulnerability assessment, system assessment, indicator sharing, and threat assessment.

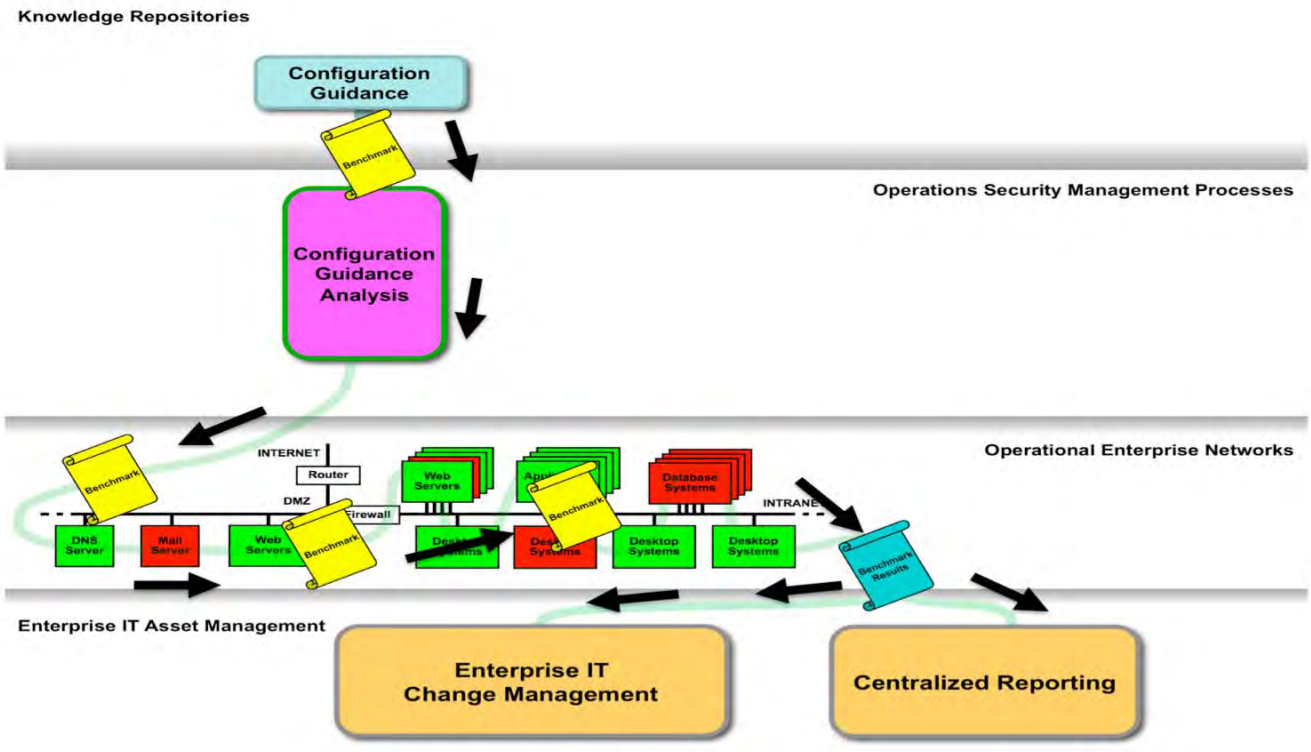

Figure 1: Assessment of Configuration Compliance Using Standards Vulnerability Assessment

Configuration Guidance, IT Change Management, and Centralized Reporting

An OMB memorandum from June 1, 2007 entitled "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" [7] references the content in NIST's National Vulnerability Database (NVD). This guidance is also referred to as part of the Federal Desktop Core Configuration (FDCC) [8] and is intended to bring consistency in the specific secure system software configuration of Microsoft XP and VISTA in use by the federal government. The part of the memo that is directed at VISTA directly points to a set of content that uses the XCCDF and OVAL languages along with the CPE and CCE enumerations [9, 10]. Subsequently, the United State Government Configuration Baseline (USGCB) has expanded the FDCC effort to other IT platforms in use throughout the federal government. These two efforts are fairly public example of a benchmark document in a repository using standard languages and enumerations.

Figure 1 above shows how an organization can utilize a tool-consumable benchmark document from a knowledge repository for configuration guidance. The benchmark provides the checking logic for a commercial tool that is used by the organization to conduct their configuration guidance analysis to assess the configuration compliance of the organization's computer systems. As shown in Figure 1, the results of the benchmark examination are also provided in standard language and enumeration terms as it is fed to the enterprise's IT change management and central reporting processes. Figure 1 also shows how security measurement and management activities can be abstracted through a systems engineering analysis view to establish the security activities of configuration guidance analysis, enterprise IT change management, and centralized reporting as functional areas to which you could manage.

Vulnerability alerts, for example those referenced in NVD, are another case in point. Sometimes these are standardized already, depending which source they come from. Figure 2 below shows how an organization can utilize a tool-consumable vulnerability assessment document from a knowledge repository, to provide the checking logic for a commercial tool that is used by the organization to conduct their vulnerability analysis to assess the vulnerability remediation compliance status of the organization's computer systems. For example, the errata from Red Hat, which are regularly posted with CVEs, OVAL Definitions, and CVSS scores. As shown in Figure 2, the results of the vulnerability assessments are fed to the enterprise's IT change management and central reporting processes.

Figure 2 also shows how vulnerability assessment and analysis can be abstracted through a systems engineering analysis view as a functional area to which you could manage.

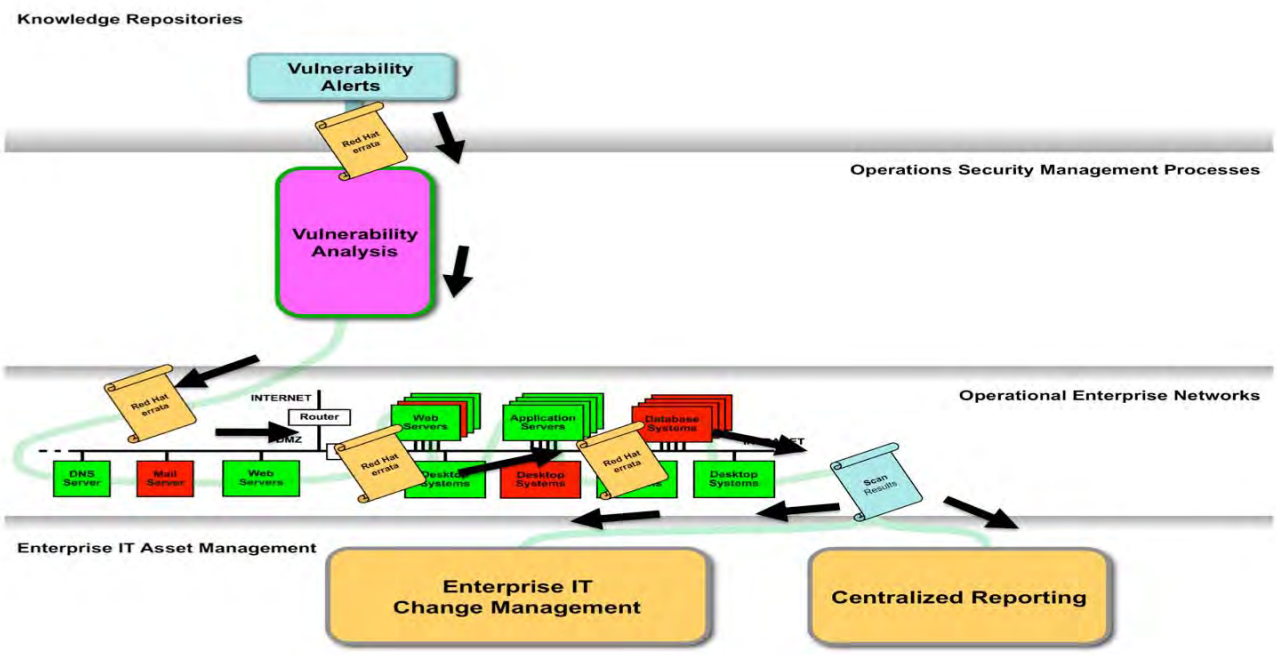

Figure 2: Assessment of Vulnerability Remediation Status Using Standards

System Assessment

System assessments and certifications are not yet as standardized. This is an area where standardization is being pursued through the development of efforts like CWE and CAPEC to address the developed components of a system along with the vulnerability and configuration assessment illustrated in Figures 1 and 2 above.

Figure 3 below shows how an organization could utilize a tool-consumable body of certification requirements from a knowledge repository for system certification guidance in order to capture the criteria for assessing the status of an organization's computer systems. For example, the Enterprise Mission Assurance Support Service (eMASS) effort being developed within the Department of Defense (DoD). As shown in Figure 3, the results of the certification and accreditation examination is fed to the enterprise's IT change management and central reporting processes.

Figure 3 also shows how certification activities can be abstracted through a systems engineering analysis view as a functional area to which you could manage.

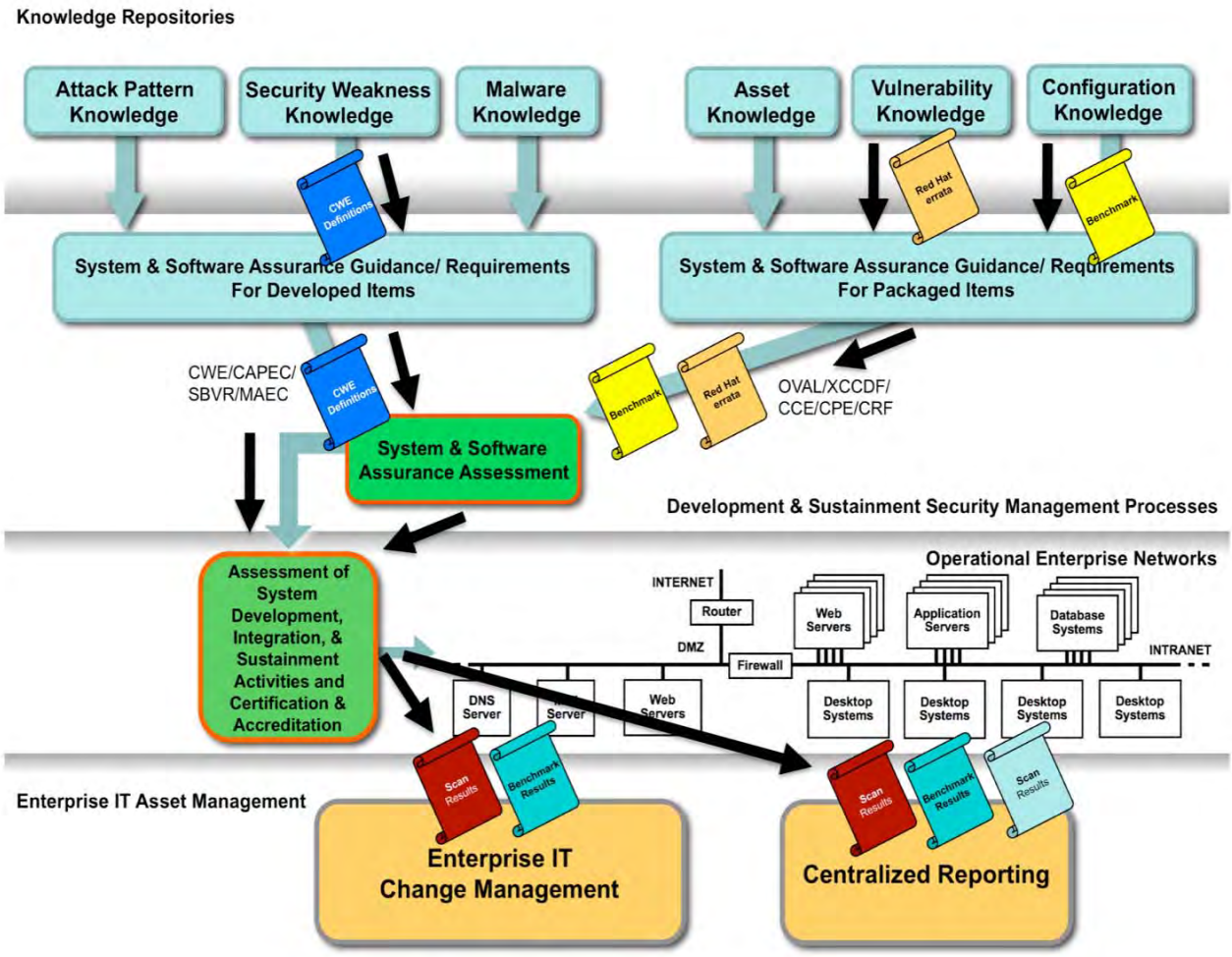

Figure 3: System Certification and Accreditation Using Standards

Threat Assessment: Threat alerts and assessment is another area that has not yet been fully standardized. Figure 4 below shows how an organization could utilize a tool-consumable information about threats from a knowledge source about new and existing threats, like the commercial threat reports that several security service providers offer, to provide an efficient way of comparing threat information such as targeted platforms, vulnerabilities, or weakness against the enterprises information about their assets and their status.

As shown in Figure 4, the results of analyzing new threat information can be fed to the enterprise's IT change management and central reporting processes. The threat analysis depicted in Figure 4 is the sixth of the security measurement and management activities we illustrated how to abstract to a vendor and tool neutral activity by taking a systems engineering analysis view of some of the different security activities of an organization.

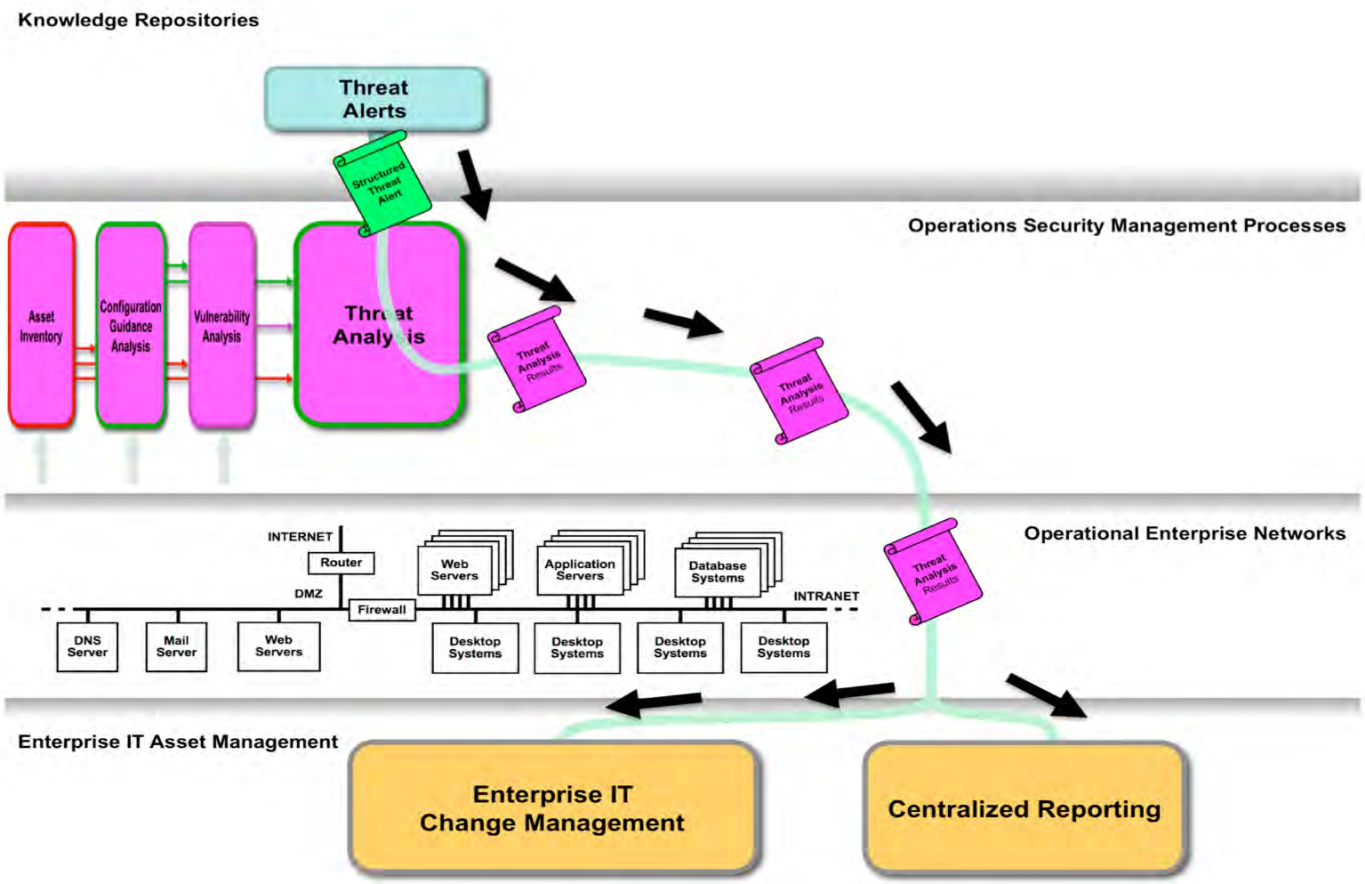

Figure 4: Threat Impact Assessment Using Standards

This same process of abstraction can be used to identify and define the other security measurement and management activities that an organization conducts. Figure 5 contains the current cut at the above and additional processes including an inventory asset activity, studying intrusion activities, notifications about incidents, assessment of systems development, integration, and sustainment activities. Those can all be functional pieces to which you could manage.

Furthermore, Figure 5 illustrates how the different security measurement and management activities are tied together through standards-based data interfaces that utilize the standard enumerations and standard languages discussed earlier. By utilizing these abstracted activities and enforcing the use of the standards-based interactions between them, an organization can bring commercially available technologies and tools to bear on their security problems but still keep control of the processes and activities rather than ending up with activities that are defined by the scope of the tools being used and that are coupled together by proprietary mechanisms.

Standard repositories of governance and guidance can help drive the business value of these standard measurement and management activities. The configuration guidance analysis, enterprise IT change management, and centralized reporting activities depicted in Figures 1 through 4 are several of the security measurement and management activities abstracted by taking a systems engineering analysis view of some of the different security activities of an organization.

This same process of abstraction can be used to identify and define the other security measurement and management activities that an organization conducts. Figure 5 contains our current abstraction of these additional enterprise security measurement and management processes

including process for: inventory asset activity; analysis of systems for vulnerabilities; analysis of threats; studying intrusion activities; notifications about incidents; assessment of systems development integration, and sustainment activities; as well as certification and accreditation of systems being deployed into the enterprise. These abstracted activities can all be utilized to describe and define the functional security capabilities that you could use to manage an enterprise's security in a vendor neutral manner.

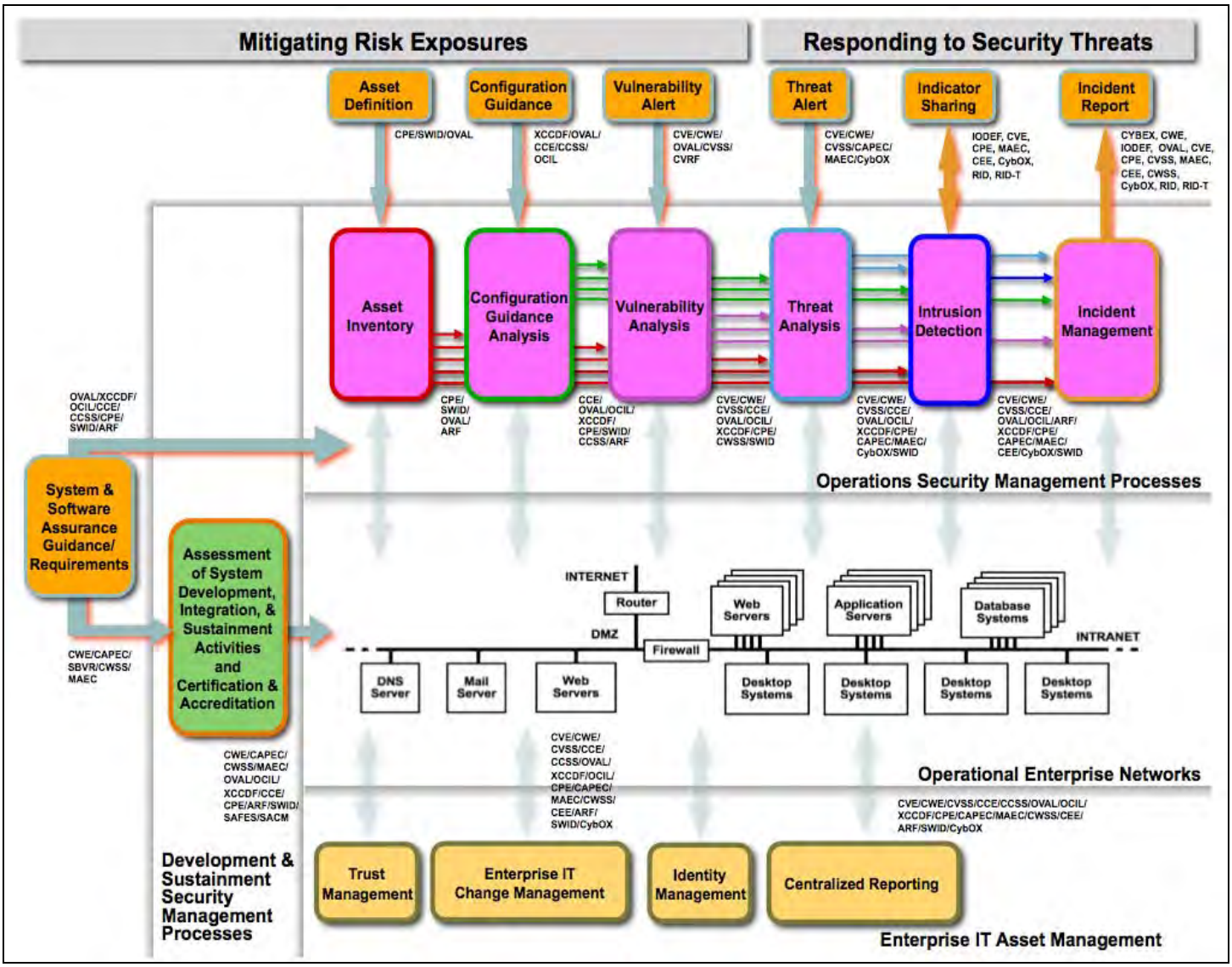

Figure 4: Decomposition and the Repositories Feeding Standard Measurement and Management Activities

Furthermore, Figure 5 illustrates how the different security measurement and management activities are tied together through standards-based data interfaces that utilize the standard enumerations and standard languages discussed earlier. By utilizing these abstracted activities and enforcing the use of the standards-based interactions between them, an organization can bring commercially available technologies and tools to bear on their security problems but still keep control of the processes and activities rather than ending up with activities that are defined by the scope of the tools being used and are coupled together by proprietary mechanisms.

Standard repositories of governance and guidance can help drive the business value of these standard measurement and management activities. As shown in the OMB guidance example, the information about how systems should be configured is captured by OVAL, XCCDF, CCE, and CPE.

REUSABLE AND SHARED REPOSITORIES

Similarly, as shown on the left side of Figure 5 above, these same standards can be used to capture how your

organization has configured and set up a new system when it has been approved for use in your enterprise. By using these standardized items, information can go right into your operational network management so that you can make sure the new system continues to be configured the way it was approved. You can also include standard guidance about which weaknesses from CWE [11] you want to be reviewed in your own development activity or in your supplier's development activity. In addition, the common attack patterns from CAPEC [12] can be used to define and document the types of penetration testing and attack scenarios your development team thought about defending against when they were doing their development and penetration testing.

For asset inventory, standardized information utilizing CPE and OVAL will let an organization know exactly what assets they have in a manner that is tool independent and usable in the other standard activities like configuration analysis. Similarly, if you know exactly how your assets are configured it's much easier to perform vulnerability analysis based on CVE, CWE, OVAL, and CVSS. Likewise, if you know what you have, how it's configured, and what it's vulnerable to, that will change the context and framework of how you do threat analysis.

Vulnerability alerts, for example those in NVD, are another case in point. Sometimes these are standardized already, depending which source they come from. Errata from Red Hat, Inc. for example are regularly posted with CVEs, OVAL Definitions, and CVSS scores. In this area particularly, the standards have already been adopted by industry.

Since threat alerts are not yet as standardized, this is an area where standardization could happen, and efforts like MAEC and CybOX are aimed at enabling that. Similarly, in incident reporting there are a lot of different ideas about what should be standardized and to what extent it should be standardized.

Finally, like any new area there are many aspects of usage that are still evolving. For example, the correct approach to managing changes, updates, or new content for shared repositories is evolving. The question of whether the repositories should be enabled as services, as static collections, or both is also open. Similarly, as new insights are made with respect to vulnerabilities, weaknesses, threats, and attacks there will surely be changes needed in how the different aspects of these types of information are knitted together and used. By bringing the various aspects of cyber security, information assurance, and software assurance into a consistent security architecture framework there will be many new opportunities and much faster responses to new threats and new information. A compelling use of the registries of enumerations and repositories, common usage, and standardized languages can be found in the Consensus Audit Guidelines [13] offered by the Center for Strategic and International Studies in Washington DC to advance key recommendations from the CSIS Commission report on Cybersecurity for the 44th Presidency [14]. The guidelines incorporate many of the items described in this paper as an approach to clearly and concisely communicate what needs to be done and what needs to be audited.

CONCLUSION

Measurable security and automation can be achieved by having government and public efforts:

- Address information security during the creation, adoption, operation, and sustainment in a holistic manner.
- Use common, standardized concepts.
- Communicate this information in standardized languages.
- Share the information in standardized ways.
- Adopt tools that adhere to the standards.

Much has already been done to transform the way security operations, measurement and management is conducted, but there is still plenty of work that needs to be addressed. The use of architecture and systems engineering principals has been shown to be effective and enabling. Ongoing efforts to address and evolve all of the activities in this arena will greatly benefit from the continued application of this methodology. Like most architecture efforts today, the true value of architecture is not apparent or appreciated until its enabling properties start to manifest themselves. With the changes in security practices and technologies outlined in this paper we have shown specific and measurable changes that are directly related to the use of architectural methods on security of information technologies in government and private industry. We have also shown the benefits in sharing that standardized information can bring.

By creating and evolving these types of standards and new approaches to security operations, measurement and management, each of us needs to step away from the traditional focus on local and enterprise issues. We must realize that much more powerful and productive solutions to these issues can be fostered through an emphasis on community-wide examinations of each of the technical areas where a multitude of concerns and needs are balanced and considered. The increased insights, resiliency and ability to leverage the collective knowledge

about what vulnerabilities and attacks affect us, what can be done to address them by leveraging everyone's insights and experience, and being able to find out about new attacks and issues from those who encounter them first are valuable benefits to trading off local concerns against community-wide concerns.

To further the goal of making security measurable and encourage participation and adoption of the different aspects of this work, MITRE established a public "Making Security Measurable" Web site [makingsecuritymeasurable.mitre.org] that informally collects all of the efforts listed in this paper, as well as others we know about, which together are helping or will help to make security more measurable.

REFERENCES

[1] Chestnut, H., "Systems Engineering Tools", Wiley, ISBN 0471154482, 1965.

[2] Martin, R. A., "Transformational Vulnerability Management Through Standards", CrossTalk: The Journal of Defense Software Engineering, May, 2005, (http://www.stsc.hill.af.mil/crosstalk/2005/05/0505Martin.html)

[3] Goodman, S. E., Lin, H. S., "Toward a Safer and More Secure Cyberspace", National Academy of Sciences, National Academies Press, 2007, ISBN-13: 978-0-309-10395-4

[4] "The Common Vulnerabilities and Exposures (CVE) Initiative", MITRE Corporation, (http://cve.mitre.org)

[5] Ziring, N., Quinn, S., "The Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4.", National Institute of Standards and Technology, January 2008, (http://csrc.nist.gov/publications/nistir/ir7275r3/NISTIR-7275r3.pdf)

[6] "The Open Vulnerability and Assessment Language (OVAL) Initiative", MITRE Corporation, (http://oval.mitre.org)

[7] Evans, K. S., "OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations", 1 June, 2007.

[8] "The Federal Desktop Core Configuration (FDCC) Effort", National Institute of Standards and Technology, (http://nvd.nist.gov/fdcc/index.cfm)

[9] "The Common Platform Enumeration (CPE) Initiative", MITRE Corporation, (http://cpe.mitre.org)

[10] "The Common Configuration Enumeration (CCE) Initiative", MITRE Corporation, (http://cce.mitre.org)

[11] "The Common Weakness Enumeration (CWE) Initiative", MITRE Corporation, (http://cwe.mitre.org)

[12] "The Common Attack Pattern Enumeration and Classification (CAPEC) Initiative", MITRE Corporation, (http://capec.mitre.org)

[13] "The Consensus Audit Guidelines (CAG)", SANS Institute, (http://www.sans.org/cag/print.php)

[14] "Commission on Cybersecurity for the 44th Presidency", Center for Strategic & International Studies Corporation, (http://www.csis.org/tech/cyber/)