REAL TIME INFORMATION SYSTEM CONTINUOUS MONITORING: THE FOUNDATION OF COST-EFFECTIVE IT SECURITY

In the Matter of)
)
CAESARS Framework Extension:) NIST Interagency Report 7756
An Enterprise Continuous Monitoring)
Technical Reference Model)
(Second Draft))
)

Before
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce
fe-comments@nist.gov

February 2012

Comments of
The Center for Regulatory Effectiveness
1601 Connecticut Avenue, NW
Washington, DC 20009
202.265.2383
www.TheCRE.com/fisma

Center for Regulatory Effectiveness

REAL TIME INFORMATION SECURITY CONTINUOUS MONITORING: THE FOUNDATION OF COST-EFFECTIVE IT SECURITY

The Center for Regulatory (CRE) appreciates this opportunity to provide NIST with comments on the second draft of the CAESARS Framework Extension. The CAESARS FE is an important contribution to understanding how to effectively conduct continuous monitoring in enterprise-scale settings.

CRE has already made use of the initial public draft of the CAESARS FE in developing a Continuous Monitoring Best Practices study. The CRE study analyzed a NASA component's response to the RSA hack and cross-walked the security team's capabilities and actions against CAESARS FE to derive best practice principles. CRE's paper, *Federal Cybersecurity Best Practices Study: Information Security Continuous Monitoring* is available on CRE's FISMA Focus Interactive Public Docket here, http://www.thecre.com/fisma/?p=699 and is incorporated by reference as a part of these comments.

One reason why the CAESARS FE is an important IT security document is that it was written to be useful to industry as well as government. As the document's introduction explains, it was "designed to be applicable to industry, state governments, and tribal networks...."

The need for government and industry to share commonly applicable IT security models was recently highlighted in an audit report from the Department of Energy's Office of Inspector General which found, with respect to the Department's Smart Grid Investment Grant Program, that

> *Three of the five cyber security plans (required to be submitted by grantees) which we reviewed were incomplete, and did not always sufficiently describe security controls and how they were implemented.*[1]

The OIG Audit Report did note that the Department's

> *Management also commented that there are currently no Federal or state standards or regulations that mandate cyber security processesor practices for electric distribution systems.*[2]

CRE has previously explained that the IT security aspects of critical infrastructure protection will increasingly become the subject of significant federal regulatory activity.[3] CRE's comments on the CAESARS FE are focused on assisting NIST with the daunting but essential task of developing effective cybersecurity guidance applicable to diverse organizations.

[1] U.S. Department of Energy, Office of Inspector General, Audit Report, "*The Department's Management of the Smart Grid Investment Grant Program*," OAS-RA-12-04, January 2012, p. 2.

[2] Id., p. 7.

[3] http://www.circleid.com/posts/20111027_the_coming_cybersecurity_regulatory_revolution/

Concordance Between CAESARS FE and SP 800-137 Terminology

NIST should ensure that nomenclature is used in a consistent manner across the agency's computer security publications. An example of inconsistent terminology is the CAESARS FE document's use of the term "continuous monitoring (CM)" while cautioning readers in Footnote 4 that there is an acronym conflict with the term Configuration Management used in SP 800-series publications. The Second Draft is also in conflict with SP 800-137 which uses the term Information Security Continuous Monitoring (ISCM) in lieu of Continuous Monitoring, which had been used in the draft of SP 800-137.

Adding to the potential for confusion, the CAESARS FE document also uses the term "continuous security monitoring" in its discussion of the essential characteristics of a continuous monitoring implementation on p. 9. It is not clear whether the term is a substitute for CM/ISCM or whether it is a different concept.

Recommendation

CAESARS FE should be revised to change the term Continuous Monitoring to:

- Information Security Continuous Monitoring (ISCM) as used in SP 800-137; or to
- Real Time Continuous Monitoring (RTCM) or Real Time Information Security Continuous Monitoring (RTISCM) to emphasize that continuous monitoring data needs to be collected and analyzed while it is fresh and actionable.

Government/Industry Collaboration

The draft document correctly notes that developing "additional subsystem specifications, interface descriptions, and communication protocols" for the Framework Extension will "require the input and participation of security-tool vendors and their customers." It is not enough, however, for NIST to simply recognize the need and to welcome industry participation. The agency should take the additional step of establishing a collaborative computer security forum or other mechanism to provide a structure for voluntary government/industry discussions and information sharing on these issues.

Recommendation

NIST should establish a forum and/or process for working collaboratively with industry, on a voluntary basis, in developing broadly applicable cybersecurity technical specifications. The goals of the collaborative effort should include:

- Promoting participation by a diverse array of industry technical experts, including through outreach to smaller companies which may not be participating in existing NIST IT security activities but which are important sources of innovation and expertise;

- Coordinating the development of security guidance documents, models, and consensus and consortia standards[4] to ensure they are applicable to a wide range of governmental and non-government organizations; and

- Ensuring that all agency work products comply with the requirements of the Data Quality Act which sets standards for quality, integrity, objectivity and utility of virtually all federal agency information disseminations.

The Need for Applicability to Big Data

NIST recognizes the need to help federal agencies exploit and leverage the potential of Big Data. For example, *Information Week* recently published an article quoting Dr. Charles Romine, Director of NIST's Information Technology Laboratory, explaining that

> *"NIST can have a lot of impact on the big data question," Romine said, noting that the agency has been involved for years in analysis of how the federal government and private sector can better harness the power of large quantities of data. In 2009, for example, NIST helped publish a report called "Harnessing the Power of Digital Data."* [5]

Wikipedia states that Big Data "consists of datasets that grow so large that they become awkward to work with using on-hand database management tools."[6] The Wikipedia article notes the difficulties of capturing, storing and analyzing large data sets but explains such data capture and analysis is increasing because the "benefits of working with larger and larger datasets" include "allowing analysts to 'spot business trends, prevent diseases, combat crime.'"

There are also benefits to an organization being able to economically apply continuous monitoring to massive data sets which could provide analysts with an improved ability to spot systems use trends and to combat cybercrime.

The concluding sentence of the document, which discusses use of the CAESARS FE model for potential CM implementations across the entire federal government, is a clear statement that the document is intended to be applied to Big Data. The FE document, however, needs a discussion, prior to the final conclusion, discussing the applicability of the Framework to the massively-sized data sets referred to as Big Data.

[4] http://www.thecre.com/action/whitepaper.html.

[5] J. Nicholas Hoover, Information Week, *Federal Standards Body Focuses On Big Data, Cloud*, February 7, 2012.

[6] http://en.wikipedia.org/wiki/Big_data.

Recommendation

Prior to being finalized, a section should be added to the NIST Interagency Report discussing the applicability of the CAESARS FE technical reference model to Big Data.

Improving User Understanding of ISCM: Defining an Effective ISCM Implementation

The success of the CESAERS FE document will be directly tied to its usability. The draft document's usability should be improved by providing guidance to users in determining whether or not an ISCM instance is appropriately designed and implemented.

The definition section includes a Note on p. 9 that provides a broad and rather conceptual statement on the meaning of the terms "continuous" and "ongoing." The document then puts some meat on the bones of the Note and the SP 800-137 definition of CM with a "a more granular and process-focused description." While useful, this part of the document has a high potential for generating reader confusion.

The granular description in the italicized statement is immediately followed by a brief discussion and listing of the ISCM essential characteristics derived from the statement. This discussion, however, refers to the statement as a "definition" although it's not clear what the granular description of CM has defined.

CRE recommends, as discussed below, that the clarity of the section be enhanced by building on the existing text to make clear that what is being described/defined is an effective implementation of ISCM. Moreover, the definition of an effectively implemented ISCM should specifically state that the system is capable of supporting defensive actions selected and implemented by IT leadership and staff.

The concept of ISCM supporting defense of an organization in response to potentially hostile action is already in the document under essential characteristics. Specifically, the Framework's description of essential characteristics includes the phrase "informs automated or human-assisted implementation of remedies" which connotes the ability of ISCM to support established or novel defensive actions. Thus, CRE is recommending that the definition of an effectively implemented ISCM be expanded to include an already recognized essential characteristic.

The importance of ISCM defense support capabilities was discussed in CRE's Best Practices study which found that NASA's continuous monitoring system played a key role in analyzing and responding to an attack. The study explained that

> *If the NASA EOS Security Team was not able develop an effective response to the unexpected threat posed by the RSA hack or if their continuous monitoring tools could not be rapidly adapted to implement the new strategy, the agency's IT security was at an unacceptable risk of failure.* [Emphasis added][7]

[7] CRE, *Federal Cybersecurity Best Practices Study: Information Security Continuous Monitoring*, p. 15.

The definition of an effective ISCM implementation should indicate, as recommended below, the basis for describing the defense support characteristic as essential.

Recommendation

An effective implementation of Information Security Continuous Monitoring should be defined as:

> *A risk management approach to Cybersecurity that uses automated data feeds to maintain a current picture of an organization's security posture by making available for analysis all system interactions and non-actions which could compromise organizational effectiveness while providing visibility into assets, monitoring effectiveness of security controls, assisting in prioritizing remedies, and supporting protective actions.*

Emphasizing the Importance of Maintaining Current Situational Awareness

The first of the essential CM characteristics cited in the document is "[m]aintains a picture of an organization's security posture." On the positive side, the wording emphasizes that what is being maintained is not just a picture of the IT equipment's status but more importantly, the security posture of the organization itself. The temporal aspects of the characteristic, as indicated by the word "maintains," however, is vague.

Although the frequency of scans and measurements may vary based on risk management decisions, the characteristic should be worded to provide additional guidance while preserving flexibility. Specifically, the wording of the characteristic should indicate that it is essential that effectively implemented ISCM maintain an up-to-date picture of a organization's security posture.

The importance of maintaining a "real time" awareness was discussed throughout the CRE Best Practices study. The study's final Lesson Learned was: "Real Time Monitoring and Analysis: There is no substitute for IT security staff being able to monitor and analyze diverse security-related data on a continuous basis."[8]

Recommendation

The first essential characteristic on p. 9 should be modified to read: Maintains a current picture of an organization's security posture.

Ability to Manipulate/Extract Data from Diverse Sources

The Data Subsystem (Sec. 4.1.2) section of the document states the CAESARS database "also includes any tools that are required by the CAESARS Database/Repository to perform data-pull operations...." Sec.

[8] CRE, p. 20.

4.1.3, Analysis/Risk Scoring Subsystem discusses “multiple analytic tools” that allow evaluation of the data. What is missing from the architecture is any reference to the tools needed to extract, parse and/or otherwise manipulate the pulled data into a form/format so that it can be analyzed.

The CRE study found that NASA officials, in order to correlate unsuccessful login attempts with IP addresses, needed to compare time stamps from three different types of subsystems (firewalls, a VPN, and the RSA login log). Accomplishing this task required the security team to extract and parse the log data from diverse sources. Although the regexe process the security officials eventually decided on worked, it took significant effort. The Reference Architecture should include reference to the tools necessary to utilize the log data from multiple subsystems.

Recommendation

The discussion of the CAESARS Reference Architecture should be expanded, in either Sec 4.1.2 or 4.1.3, to include reference to tools that allow staff to extract, parse or otherwise manipulate subsystem sensor data in preparation for analysis.

Summary of Recommendations

The CAESARS FE Second Draft should be revised to:

1. Use the term Information Security Continuous Monitoring (ISCM), consistent with SP 800-137, in lieu of Continuous Monitoring.

2. Add a section discussing applicability of the CAESARS FE reference model to Big Data.

3. Define “Effectively Implemented ISCM” as:

   - *A risk management approach to Cybersecurity that uses automated data feeds to maintain a current picture of an organization’s security posture by making available for analysis all system interactions and non-actions which could compromise organizational effectiveness while providing visibility into assets, monitoring effectiveness of security controls, assisting in prioritizing remedies, and supporting protective actions.*

4. State that the first essential characteristic of an effectively implemented ISCM is,

   - *Maintains a current picture of an organization’s security posture.*

5. Expand the CAESARS Reference Architecture to include reference to tools for extracting, parsing and/or otherwise manipulating subsystem sensor data in preparation for analysis.