WHITE PAPER

Continuous Monitoring

Introduction & Considerations – Part 1 of 3

Abstract

This white paper is Part 1 in a three-part series of white papers on the sometimes daunting subject of continuous monitoring (CM) and how to successfully manage your own CM program. Intended for security professionals who are new to CM, this first document discusses common misconceptions and provides definitions, an introduction and brief history of CM.

Part 2 in this series will address monitoring strategy including the frequency and method of assessments, and Part 3 will cover strategies for managing assessment costs.

Contents

Introduction

What is continuous monitoring?

Continuous monitoring (CM) is referenced by several names with nuances in definition. CM is also known as continuous controls monitoring (CCM) for compliance activities such as the Certification and Accreditation (C&A) / Assessment and Authorization (A&A) process. In this context, CCM is referenced interchangeably with the term Continuous reauthorization which utilizes CM to maintain Authorization/Authority to Operate (ATO) as part of the A&A/C&A process.

In addition to using the term "continuous monitoring," the Department of Homeland Security (DHS) coined the term Continuous Diagnostics and Mitigation (CDM), which it is more likely to use. The National Institute of Standards and Technology (NIST) uses indirect terms like "ongoing assessment/ongoing remediation" and Information Security Continuous Monitoring (ISCM).

The term "continuous monitoring" will be referenced throughout this three-part series of papers as the de facto term.

DHS and NIST are thought leaders in the field of CM, defining what CM should be, what it should do and how it should look. These two agencies have slightly different takes on what CM is, but provide a vast majority of the guidance, direction, momentum and thought leadership on this topic. DHS tends to place greater emphasis on operational security in regard to CM philosophy, while NIST focuses slightly more on tying CM to compliance C&A/A&A activities.

CM provides a way to bridge the gap between operational security and compliance. As a mechanism to provide assurance in an information system's current level of risk, CM is intended to enhance or replace the C&A process of the past, using a more frequent and iterative approach to assessing security compliance.

NIST provides the following definition for CM: "…maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

Is continuous monitoring mandatory?

To date, legislative attempts to make CM mandatory for federal information systems have failed. However, this is primarily due to the inclusion of unrelated items in the legislation, rather than the government's inability to recognize that CM is important. The mandate will come, but the timing is unknown.

Most federal departments and agencies recognize the importance of implementing a CM program and are taking preparatory steps, while others are waiting for final federal criteria and guidance. Only a handful of the most forward-thinking agencies have tried to implement CM in earnest. These agencies are often more focused on a narrow band of controls, like vulnerability and configuration scanning, which are easily automated and / or seemingly more critical than other controls. Process-oriented controls like policy-writing and personnel security have not received as much attention in the CM world. Some controls are less important, but none are unimportant. There is no consensus on the frequency and methodology that should be used for an effective and comprehensive continuous control monitoring strategy.

The current body of CM guidance & literature

iPost

The U.S. State Department created its own model for CM called iPost. iPost is primarily based on monitoring the security status of Microsoft Windows machines using very select automated processes. This model was documented in iPost: Implementing Continuous Risk Monitoring at the Department of State, which provides tangible ways and formulas to monitor devices and score them according to basic variables like how many vulnerabilities or misconfigurations are present, how many patches are missing and how old the antivirus definitions are.

While it was written specifically for State Department infrastructure and policies, this model was admired by other federal agencies. iPost was then altered to be more generally applied, and then rebranded as Portable Risk Score Manager (PRSM) and made available to the public.

CAESARS / CAESARS (FE)

Following the creation of iPost, the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) model was developed and documented by DHS with input from the State Department, the IRS and the Department of Justice. The defining document, which was last updated in 2010, incorporates many of the same concepts as State's iPost model, as well as input from other agencies. It is more mature and extensible than iPost, but DHS recognized that it fell short in the following regard, as noted in original CAESARS document dated September 2010:

"CAESARS is not, in itself, a full risk management system. CAESARS cannot, for instance, evaluate security controls in the NIST SP 800-53 Planning or Management families, such as those for capital planning or risk assessment. It cannot create, evaluate, or manage security policies."

The original CAESARS was effective at monitoring automatable controls and using automated scoring, yet less so for policy or process-oriented controls which required manual review. It was well received in the federal community and embraced as the basis for a set of new interagency reports written by NIST, with input from National Security Administration (NSA) and DHS. The goal was to make the CAESARS model viable for all federal agencies.

This NIST-adapted version of CAESARS is called CAESARS Framework Extension (FE). It is designed to make the initial DHS CAESARS model even more extensible and scalable to the very largest organizations, with greater emphasis on the many non- automatable controls. Because the model was developed entirely by federal civilian agencies, it took some adaption to make it suitable for military and intelligence agencies as well as state and local governments. CAESARS FE is defined by several NIST interagency reports (NISTIR), including NISTIRs 7756, 7799 and 7800. These reports are significant and relevant; however, they are still in draft.

The NISTIRs

As the introductory document for CAESARS FE, NISTIR 7756 defines the components of a mature CM implementation and the roles of those components. The six components or subsystems are: Presentation/Reporting, Content, Collection, Data Aggregation, Analysis/Scoring and Task Manager. While most of the data collection discussed in NISTR 7756 supports automated monitoring, the report indicates that a CM model should also allow for non-automated controls which "require some human data collection effort."

Building upon NISTR 7756, NISTR 7799 describes ways the six subsystems can act in very complex use cases. The report is devoted to describing possible work flows between the six subsystems. It defines all possible inputs and outputs from one subsystem to another, as well as describes how the subsystems feed each other, and how data integrity and synchronization is maintained.

NISTIR 7800 defines how to implement this model for three specific CM domains: vulnerability, configuration and asset management. Given that NISTR 7800 covers just three CM domains while NISTIR 7756 indicates there are "at least 11," one can infer future draft NISTIRs will cover remaining domains such as event, incident and malware.

NIST SP 800-37 and 137

The NISTIRs 7756, 7799 and 7800 are NIST's way of moderating DHS CAESARS model to make it accessible for everyone. However, in addition to iPost and CAESARS, NIST has also written its own documents on the subject of CM.

The first, NIST SP 800-37, describes NIST's Risk Management Framework (RMF), which is the current way to reference C&A/A&A. There are some points of divergence between NIST and iPost and CAESARS. NIST defined how to implement RMF and made an effort to integrate CM with FISMA compliance and RMF. NIST also described details of the model and how it integrates with NIST RMF, FISMA compliance and risk management overall. Alternatively, iPost and CAESARS focused less on compliance and more on results in providing the greatest reduction of host risk in the least amount of time.

Dedicated to CM, NIST SP 800-137 describes steps to develop and implement a CM program. SP 800-137 spends the most time on the subject of manual control assessment as part of the CM scheme and includes factors influencing the frequency of assessments in CM, which will be covered in Part 2 of this series.

Misconceptions & clarifications

Continuous vs. Constant

One large obstacle in the discussion of CM is the semantic differences and confusion with the terms continuous, constant and automated. Continuous is in many ways a relative term, in that OMB (Office of Management & Budget) A-130 defined a three- year cycle for assessing controls; therefore, any increment less than that may seem “continuous” by comparison. However, “continuous” does not mean “constant.” NIST 800-137 states that controls should be “assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. Data collection, no matter how frequent, is performed at discrete intervals.”

Continuous ≠ Automated

Another layer of confusion ensues when equating “continuous” with “automated.” If control monitoring is supposed to happen constantly/ continuously, how could a person do it? It would have to be automated, right? While all Information System controls should be continuously monitored whether or not there are automated means, some controls simply must be assessed manually and these manual assessments will not happen as frequently. This dispels a common misconception that continuous monitoring means all controls must be automated and must be assessed constantly, which is neither true nor possible.

Continuous monitoring ≠ Network security monitoring

Some people understandably equate the term continuous monitoring with tools like IDS, IPS and SIEM because they are security tools that monitor the network continuously. Security vendors tend to exacerbate this problem by skewing the definition of CM to rebrand their offerings as CM tools. Network security monitoring (NSM) is a reactive process, while CM is a proactive process. NSM monitors traffic, while CM monitors controls and security posture.

Automating the protection ≠ Automating the assessment of protection

Another pitfall occurs with phrases like “automate the control.” It is one thing to say that a control can be automated, which means that a control can be provided by an automated means. However, this is not the same as saying a control can be assessed or tested by automated means. For example, an Active Directory or LDAP server can authenticate a user automatically if the correct username and password are provided; a person is not required to review and confirm the correct password was provided. If we want to assess the corresponding access controls, not all of them can be assessed automatically. This difference is more evident in Part 2 of this series which will discuss automation domains and “automatable” controls.

Summary

CM is a way of assessing the implementation and effectiveness of controls in a way that is more frequent than previous methods. The goal of CM is to provide a higher level of assurance to the relevant stakeholders that their information systems are 1) as secure as the day they were authorized to be put into production, 2) adhering to the protection plans designed for them, 3) operating at an acceptable level of risk, and 4) stay current with the latest threats, patches, etc. It is important to remember that "continuous" in the context of CM does not mean constant or automated and that different controls can be assessed at different frequencies. How to determine the frequency of these assessments is the primary topic of Part 2 in this series.

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.
For more information, go to **rsa.com**.