Interested in learning more about security?

SANS Institute InfoSec Reading Room

Beyond Continuous Monitoring: Threat Modeling for Real-time Response

Sponsored by
Symantec Corporation

Beyond Continuous Monitoring: Threat Modeling for Real-time Response

October 2012
A SANS Whitepaper

Written by: G. Mark Hardy

Introduction

Malware. Hackers. Espionage. Advanced Persistent Threat. Cyberwar. Dangers to the enterprise abound and are getting worse. Arrays of attackers seek to exploit vulnerabilities in military, government and civilian systems. Every element of our IT enterprise is a target, from laptops to network infrastructure. Defenders must block all attacks; to win, attackers need to succeed at only one. Factor in increasing complexity, tightening budgets and a limited pool of security experts, and the prospect for maintaining effective security appears bleak.

Yet there is hope. The majority of successful attacks are not a result of exploiting unknown vulnerabilities (often known as *0-days*), but are perpetrated by taking advantage of known problems that remain unpatched. The State Department reported that "80% of attacks leverage known vulnerabilities and configuration management setting weaknesses,"[1] so the best opportunities in security remediation are to identify and correct, in real time, any misconfiguration or known vulnerable systems. By maintaining effective awareness of the current state of enterprise IT assets and taking prompt action to patch, update or even disconnect vulnerable systems, the vast majority of attacks can be stopped before they even start.

Knowing what systems are present and their state of security is much of the battle. This knowledge provides defenders with a baseline understanding of configurations and potential vulnerabilities. This first line of defense is known as *continuous monitoring*.

In its purest sense, continuous monitoring is inwardly focused on activities such as vulnerability assessment and patch management. The goal is to provide situational awareness of systems and their potential vulnerabilities. Yet simply knowing a problem exists doesn't offer protection. One has to be able to act correctly and in time to keep up with the evolving threat and minimize risk.

Risk, or exposure to adversity, is a combination of vulnerability (exposure), threat (adversary), impact (cost) and probability (likelihood). If any of these factors are zero, the risk (exposure to danger) is zero. A simple equation for risk is:

Risk = Vulnerability x Threat x Impact x Probability

Effective security lies in managing risk. A structured process for managing risk is often referred to as a *Risk Management Framework (RMF)*.

Continuous monitoring is an essential component of a successful RMF. It's also required by law. Federal CIOs and security staff must meet multiple legal and administrative requirements to protect their enterprises under the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) publications and other guidance. Although a lot of synergy exists among these references, they have been developed intermittently over the course of the last decade, and not all guidance objectives agree.

---

1 www.state.gov/documents/organization/156896.pdf, page 7.

By understanding and using federal standards and guidelines, agencies and services can make enterprise reporting to the Department of Homeland Security (DHS), OMB or Department of Defense (DOD) a byproduct of good local enterprise management. What is needed is a way to make such reporting universal in expression, easy-to-integrate, cheap and fluid from one level to the next. For example, if we go beyond measuring configuration and reviewing firewall and IDS logs, we can analyze the types of attacks and intrusions attempted against our systems to prevent the same or similar incidents in the future. Taking such measurements allows us to piece together an overall model of the threat, determine patterns and gain insight into the opponent's goals, strategies and tools.

The threat model we develop from this approach can then be used to orchestrate responses in real time. Rather than rely on alerts and notifications from event monitoring agents, enterprises can use threat modeling, through timely and accurate inputs, to mitigate and defeat attack scenarios before they fully unfold.

Before Continuous Monitoring

Continuous monitoring has evolved as a best practice for managing risk on an ongoing basis. In 2002, NIST issued Special Publication 800-30, the Risk Management Guide for Information Technology Systems.[2] This work focused on integrating risk management into the Software Development Life Cycle (SDLC) and remains a great tutorial on the subject of risk management for those new to the discipline.

The compliance mentality of 2002 was far from continuous. Rather, OMB Circular A-130 specified a three-year accreditation period.[3] Not only were these reviews too far apart to impact security programs favorably, but also the certification and accreditation (C&A) tended to become an expensive and time-consuming risk management checklist inspection item rather than a defense strategy. Annual reporting sufficed, and the word *continuous* did not appear even once in this particular OMB document!

Also in 2002, baseline legislation for security reporting became law for federal agencies under the Federal Information Security Management Act (FISMA), Title III of the Electronic Government Act, enacted as Public Law (P.L.) 107-347 on December 17, 2002. FISMA lays out a framework for federal agencies to annually review, report and remediate IT security. At its inception, this law represented a tremendously important step in codifying and formalizing security reporting.

That reporting, however, was mostly manual, and the process of reviewing networks and systems was cumbersome and expensive. Senator Tom Carper estimated that by 2009, the government had spent $40 billion related to FISMA,[4] and yet breaches of federal systems seemed to be a regular occurrence. FISMA compliance represented a great start, but it didn't solve federal security issues—it merely reported them.

Congress has attempted to update FISMA several times. The 2010 Federal Information Security Amendments Act[5] specified "continuous automated monitoring of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency to assure conformance with regulations."[6]

This legislation did not pass: It died after being reported out of committee. Rather than wait for Congress to provide leadership, in March 2010, the Executive Office of the President took the initiative to mandate continuous monitoring in federal systems.

To improve and centralize reporting for federal agencies, the OMB, in its management role under FISMA, issued a directive in the form of Memorandum M-10-15, "FY2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."[7] This document, sometimes referred to as *FISMA 2.0*, states that "agencies need to be able to *continuously monitor* security-related information from across the enterprise in a manageable and actionable way."

Instead of annual paper or e-mail reports, the directive mandated the use of the CyberScope[8] reporting tool and directed the implementation of continuous monitoring described in NIST Special Publication 800-53.[9] By FY 2011, 19 of 24 agencies were submitting automated data feeds to CyberScope.[10]

---

2 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

3 www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

4 www.govinfosecurity.com/articles.php?art_id=1893

5 www.govtrack.us/congress/bills/111/hr4900

6 www.govtrack.us/congress/bills/111/hr4900/text, Section 3556, paragraph (b)(1)

7 Executive Office of the President, Office of Management and Budget, Memorandum M-10-15, April 21, 2010, accessed at www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

8 http://scap.nist.gov/use-case/cyberscope

9 http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

10 Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002, page 19

Continuous Monitoring Today

Consider how often changes occur on an organization's servers, desktops and applications (Microsoft Super Patch Tuesday, Adobe updates and so on). Now multiply this by the number of systems in the enterprise. Then consider how often adversaries discover new exploits and flaws in the types of enterprise systems in use. What results is a risk environment in a state of constant flux. Periodic updates are insufficient; the goal is to strive for continuous monitoring.

In continuous monitoring, first focus on what is important, then select and implement controls, and then define the information that lets IT staff know whether there have been any changes. There is a critical need to recognize how quickly things can change, get the information needed to respond to those changes and create the ability to respond correctly and promptly.

Frequency of scanning is unique to each organization and depends on a number of factors, including system and data sensitivity, available tools and resources, types of systems covered under the plan, regulations applying to those systems, storage capacity and how often those systems are expected to change. NIST SP 800-137 devotes five pages to determining frequency of scans (pages 25–29).[11] NIST SP 800-92 offers recommendations on logging configuration settings based upon system impact (low, moderate, high), log retention and rotation, frequency of transfer to log management infrastructure, and periodicity of log analysis.[12]

If monitoring is considered "continuous," it doesn't have to be "real time." For example, a pilot flying in formation at an air show needs positional information far more frequently than a captain piloting a ship in the open ocean. Both consider themselves to be maintaining a continuous picture, but changes usually occur much faster in the air. The IT environment must strike a balance. If we saturate our networks with real-time reporting data, we would never get any real work done. If we don't monitor enough, however, we could leave open a window of vulnerability for attackers to strike.

There are tools and frameworks for controls that, in aggregate, are comprehensive enough to mitigate most threats. One such guideline, first released in 2009, is the 20 Critical Security Controls (20CSC).[13] Also known as the *Consensus Audit Guidelines (CAG)*, these controls provide a roadmap to FISMA compliance. They are designed to counter an adversary's actions (conducting reconnaissance, gaining access, keeping access and exploiting target systems) by stopping attacks early and mitigating the impact of any attacks that make it through.

The controls are prioritized by their capability to provide a direct defense against attacks. In July 2012, Gen. Keith Alexander, Director of the National Security Agency (DIRNSA), specifically cited the 20CSC as a model standard for organizations to use to protect their systems.[14] John Streufert, who led significant improvements in cybersecurity at the Department of State as Chief Information Security Officer, now serves as the Director of the National Cybersecurity Division for the DHS and is working to bring the 20CSC to all federal systems.

---

11 NIST Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", accessed at http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

12 NIST Special Publication 800-92, "Guide to Computer Security Log Management", accessed at http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf, pages 4–6

13 www.sans.org/critical-security-controls

14 www.c-spanvideo.org/program/ThreatstotheU, media clip time offset 37:20

The recommendations in this paper are fully consistent with the 20CSC—in particular, three controls are applicable to this discussion: Critical Security Controls 1 and 2 address inventory of hardware and software. Critical Security Control 4, Continuous Vulnerability Assessment and Remediation, correlates to the top two Australian government strategies to mitigate targeted cyber intrusions: promptly patch applications and operating system vulnerabilities.

To monitor security controls, you must first know what systems are present. The process of discovery must be continuous: As a new system comes online, tools detect its presence and begin to check it. What is its configuration? Has it been patched and kept up to date? If not, what vulnerabilities does it pose? Even if patched, are the capabilities of the new system sufficient to protect the level and quantity of information it contains? Finally, how do the tools report this information? Does the information simply go into a log? Is it presented to an operator? Or does it get rolled up into a Security Information and Event Management (SIEM) product?

As part of the NIST RMF cycle, the security life cycle consists of six steps (see Figure 1).

By conducting an ongoing appraisal of security in the enterprise, management gains insight into the current state of affairs. This understanding is often called *situational awareness*.

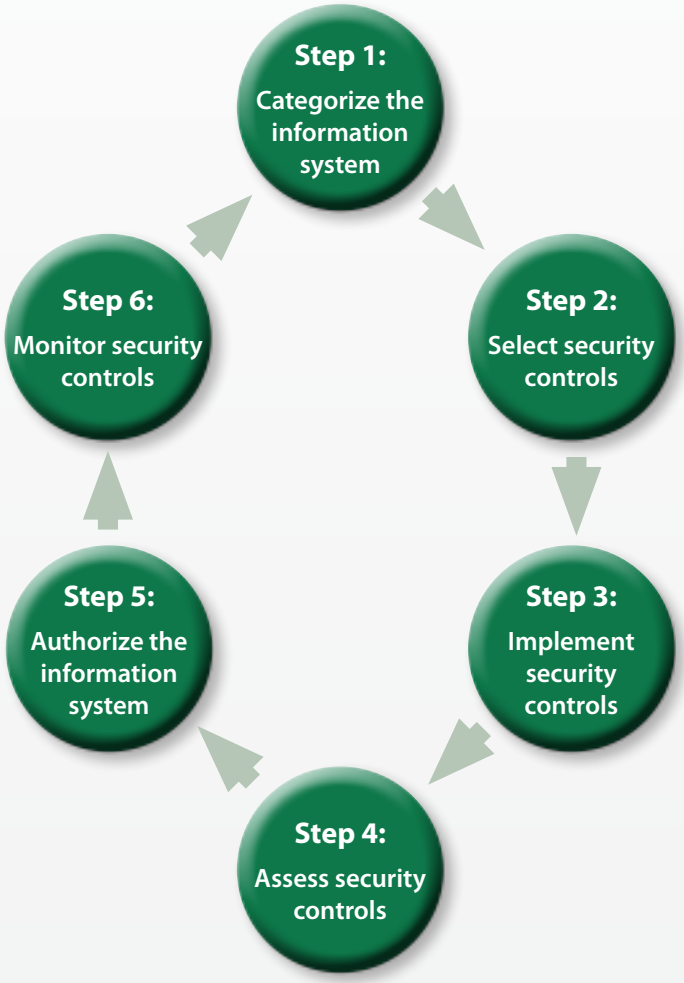

Figure 1. The NIST Risk Management Framework [15]

15 Adapted from NIST Special Publication 800-53, accessed at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf, page 17.

Situational Awareness

The most valuable intelligence continuous monitoring can provide is situational awareness. Situational awareness is a term that refers to knowing what is around you, where it's going, what it's doing and how it might affect you. Situational awareness is important in work that involves significant consequences, such as military operations, piloting aircraft or managing a large enterprise. In cyberdefense, situational awareness is a prerequisite for meaningful action. After all, if you don't understand something, how can you make the right decision?

Figure 2 depicts a decision-making model that originated with the military: the OODA loop (Observe, Orient, Decide, and Act).

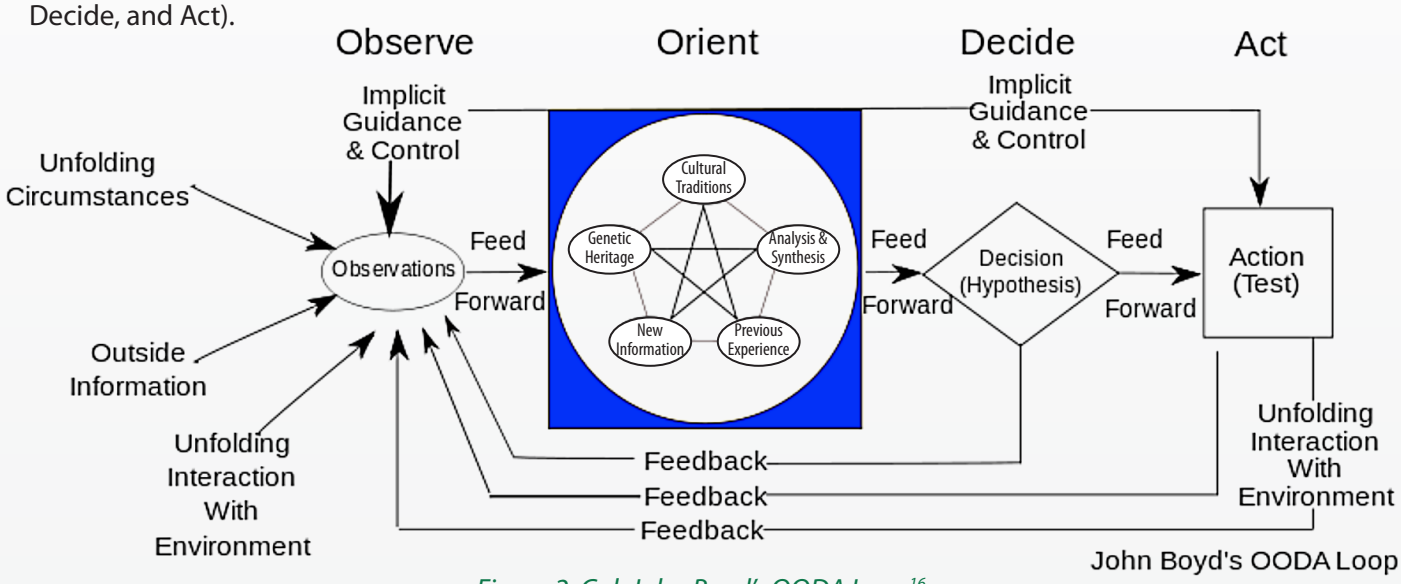

Figure 2. Col. John Boyd's OODA Loop[16]

Developed by Col. John Boyd,[17] the concept was to rapidly assimilate observations and information, synthesize those ideas through a process refined over time, select a course of action from among available options and then implement it. By observing the results of this action, new information presents itself, and the loop begins again. Combat pilots were trained to create situations that evolved faster than an opponent could respond. By getting ahead of an opponent, the pilot could get inside the opponent's OODA loop and win the dogfight.

In cyberdefense, situational awareness is a prerequisite for informed action. Failure to understand what's occurring around you means failure to make the correct decisions—ones that protect systems appropriately. Situational awareness and OODA loops also apply because a key component of situational awareness is observation. Knowing what is in our environment is foundational and is represented by the first two controls of the 20 Critical Security Controls:[18] inventory of authorized and unauthorized devices and inventory of software.

Thus, to be tactically successful (and thereby have a chance to achieve strategic success), rapid comprehension of the environment and understanding the implication of changes or events is critical. The best approach is to predict the future by thoroughly understanding the present and make rapid, intelligent decisions to counter attacks before they achieve success.

16 This representation of John Boyd's OODA loop, accessed at http://en.wikipedia.org/wiki/File:OODA.Boyd.svg was created by Patrick Edwin Moran and is used here with permission under the Creative Commons License

17 Osinga, Frans. (2007). Science, Strategy and War: The Strategic Theory of John Boyd. Abingdon, UK: Routledge.

18 www.sans.org/critical-security-controls

From Monitoring to Modeling

Continuous monitoring provides a steady stream of data that can be used to identify and correct security deficiencies. To get ahead of the problem (or to get inside the attacker's OODA loop), we can model the attacker's behavior so we can anticipate what comes next. This systematic process of identifying and rating threats is called threat modeling.

There are three types of threat modeling: asset-based, software-based and attacker-based.

An example of an asset-based approach developed by the Carnegie Mellon Software Engineering Institute is CERT's Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®).[19] This approach addresses the following questions:[20]

- What assets require protection?
- What level of protection is needed?
- How might an asset be compromised?
- What is the impact if protection fails?

Note that asset-based threat modeling is still predominately internally focused; only the third question is outward-looking—and even then, the methodology focuses primarily on the impact of a compromise rather than its source. Nonetheless, the desired output is a prioritized list of threats, which can then be further examined to assess impact.

Software-based threat modeling is an essential component of The Open Web Application Security Project (OWASP). OWASP's threat modeling process, described as "a structured approach that enables you to identify, quantify, and address the security risks associated with an application,"[21] can also be applied to other information systems.

Another resource called *STRIDE*, published by Microsoft, contains a threat categorization model, along with a goal-oriented approach that considers the motivations of an attacker.[22] STRIDE stands for Spoofing, Tampering, Reputation, Information disclosure, Denial of service and Elevation of privilege. Note that these terms correlate with the security properties of authentication, integrity, nonrepudiation, confidentiality, availability and authorization respectively.[23] Currently, Microsoft advocates its Security Development Lifecycle Threat Modeling Tool.[24] Again, these threat categorization strategies are focused primarily on software and applications.

---

19 www.cert.org/octave

20 Carol Woody, Applying OCTAVE: Practitioners Report, 3, accessed at www.cert.org/archive/pdf/06tn010.pdf

21 www.owasp.org/index.php/Application_Threat_Modeling

22 http://msdn.microsoft.com/en-us/library/ff648641

23 http://blogs.msdn.com/b/sdl/archive/2007/09/11/stride-chart.aspx

24 www.microsoft.com/security/sdl/adopt/threatmodeling.aspx

The concept of attacker-based threat modeling is to try to understand the mind and motivation of attackers and figure out how they might attack. Some consider this to be the opposite of asset-based threat modeling.[25] In the military, the following strategic framework is often used: Identify the goals of an opponent (*ends*), the methods he can employ against friendly forces (*ways*) and the resources available to accomplish this (*means*). Chapter 5 of The National Military Strategy for Cyberspace Operations is dedicated to a discussion of this framework at a high level.[26] The concept of an OODA loop is present in this military document—the first strategic priority listed is to "gain and maintain the initiative to operate within adversary decision cycle."[27]

Attacker-based threat modeling focuses not only on preparing friendly forces for defense (and offense), but also examines adversary capabilities and intent. If we know what an opponent wants, the tools available, and the ways they can affect our systems and networks, we can better model the threat. Rather than basing our strategy on what an opponent has already done, we can expand the strategy to include what an opponent may want and try to do. This leads to the concept of *predictive analysis*.

25 www.rdacorp.com/2008/11/elementary-application-security-part-1-look-both-ways-before-crossing-the-street

26 www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf, pages 13–18. Original document is classified SECRET, but this version is redacted to become UNCLASSIFIED.

27 www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf, page F-1

From Threat Modeling to Predictive Analysis

The concept of predictive analysis involves using statistical models and decision tools that analyze current and historical data to make predictions about future events. A well-known example of this is credit scoring. Based on a person's past behavior, banks can make risk-based decisions on how much credit to extend and on what terms. Universities even offer graduate degree programs in predictive analytics.[28] [29]

To effectively conduct predictive analysis in the cybersecurity space, you need sensors, data and trends. Although federal systems face some specific threats that may not target civilian systems (e.g., enemy attempts to access tactical military data), many threats target contractors, vendors, consultants and even employees to attempt to reach targeted information or systems. So this type of analysis must be included in your predictions of where threats may originate within the organization.

Predictive analysis originated in malware identification—when a worm or virus was released, copycat authors often tried to modify the successful ones and re-release the malware for their own reasons. By identifying those worms or viruses that had the greatest potential for modification, vendors could develop signatures or heuristics that would likely stop copycats, even if the copycat malware had not yet been seen and analyzed.

In the enterprise environment, predictive analysis involves assimilating data from a number of sources, weighing them against historical patterns, and building a set of scenarios that can be used to identify and predict hostile actors and actions. The more information available, the more likely it is that the threat models will mirror reality and, therefore, the more accurate the predictions. This is true in the case of most exploits, except for new, disruptive or deliberately unpredictable actors.

According to an article in *Government Computer News (GCN)* magazine, predictive analysis involves a number of steps:[30]

- Understanding the problem
- Tying prediction variables to the problem
- Selecting appropriate statistical models relevant to the problem
- Preparing the input data for application of the models
- Validating the models with test data
- Applying the models to production data, observing the accuracy over time and making adjustments as necessary

28 www.scs.northwestern.edu/program-areas/graduate/predictive-analytics

29 www.cdm.depaul.edu/academics/Pages/MSinPredictiveAnalytics.aspx

30 Raj Nathan, Joydeep Das, Predictive Analysis Has a Growing Role in Government, accessed at http://gcn.com/Articles/2010/04/01/Commentary-Nathan-Das-predictive-analysis.aspx?Page=3

For example, each year the Internal Revenue Service (IRS) receives millions of fraudulent income tax refund claims and returns that underreport income. They developed the Taxpayer Compliance Measurement Program that used detailed audits to create a scoring system that identified similarities in these types of returns. By applying this scoring algorithm to tax returns, the IRS can better flag for audit questionable returns, resulting in higher tax capture. As new tax-related legislation was passed, the IRS adjusted its model to look at returns for errors or potential fraud associated with specific items (e.g., the First-Time Homebuyer Credit).[31]

For a more detailed discussion, there is an excellent paper written by Dr. Thomas Davenport and Dr. Sirkka Jarvenpaa titled "Strategic Use of Analytics in Government." This paper makes the case for adapting private-sector analytics approaches ("business intelligence") for public-sector use.[32]

There is an opportunity here for federal CIOs and the vendor community to develop forward-looking practices and tool sets that can help enterprises extend their continuous monitoring into threat modeling and beyond to predictive response. This capability would be a valuable addition that would move IT security well beyond mere compliance toward a sustainable system that can adapt dynamically to evolving threats.

31 IRS Form 5405, First-Time Homebuyer Credit and Repayment of the Credit, accessed at www.irs.gov/pub/irs-pdf/f5405.pdf

32 http://hou23bogs01.clearlake.ibm.com/sites/default/files/Strategic%20Analytics.pdf

From Theory to Practice

NIST Special Publication 800-53 specifies guidance on actions to be taken in the event of certain event triggers, such as a breach that results in a loss of confidence in system confidentiality or integrity, or a newly identified and credible threat to information systems. Significant changes to configuration or risk management strategy also would trigger actions such as reassessing the security state of the system, initiating corrective actions or even repeating the formal process of reauthorizing the information system.[33]

Another document, known as the CAESARS Reference Architecture Report,[34] combines the work of the Department of State (DOS), the IRS and the Department of Justice (DOJ). Developed by DHS, CAESARS represents the essential functional components of a security risk scoring system. Written specifically to support managers and security administrators of federal IT systems, it provides an integrated end-to-end process for the following:

- Assessing the actual state of each IT asset under management
- Determining the gaps between the current state and accepted security baselines
- Expressing in clear, quantitative measures the relative risk of each gap or deviation
- Providing simple letter grades that reflect the aggregate risk of every site and system
- Ensuring that the responsibility for every system and site is correctly assigned
- Providing targeted information for security and system managers to use in taking the actions to make the most critical changes needed to reduce risk and improve their grades[35]

CAESARS uses an asset status database that can readily indicate deviations of systems from baseline configurations. By defining a decision support system that uses a continuous monitoring approach instead of isolated assessments, CAESARS provides a strategy to comply with NIST and OMB guidance and mandates.

Although NIST and OMB have taken the lead in providing frameworks and concepts for continuous monitoring, there is still a need for standards to support reporting and consolidating threat information that could be useful to multiple government organizations. OMB's established mechanism for reporting is CyberScope.[36] However, the federal government has not developed any plug-and-play tool sets to connect monitoring systems to reporting tools, nor are they expected to do so.

OMB states, "Agencies should not build separate systems for reporting. Any reporting should be a by-product of agencies' continuous monitoring programs and security management tools."[37] OMB also encourages "agencies to seek out and utilize private sector, market-driven solutions resulting in cost savings and performance improvements—provided agency information is protected."[38]

Security vendors have developed tools to automate the process of network discovery, configuration management, vulnerability reporting and other security monitoring and reporting functionality. Some require software agents that run on hosts and report to a central server; others are agentless, gathering data by polling systems but not actually running on the target system. Tools that conduct monitoring and reporting, along with collected logs and security information, can be input into a SIEM or other management system. Together, these provide the continuous monitoring ecosystem from which situational awareness, threat modeling and predictive analysis are achieved.

---

33 NIST Special Publication 800-53 Revision 3, pages 28–29

34 www.dhs.gov/xlibrary/assets/fns-caesars.pdf

35 www.dhs.gov/xlibrary/assets/fns-caesars.pdf, page xi

36 http://scap.nist.gov/use-case/cyberscope

37 OMB Memorandum M10-15, accessed at www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf, page 2

38 OMB Memorandum M10-15, accessed at www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf, page 8

Conclusion

Continuous monitoring is an effective best practice for maintaining security awareness in today's threat environment. For federal systems, continuous monitoring is the legal standard. Non-federal CIOs should also examine the benefits of this capability.

By building an automated monitoring system that is linked to an automated set of actions and responses, we gain situational awareness, change the dynamics of a cyber attack and place ourselves within the OODA loop of many opponents.

Organizations also need to consider what's on the frontier for continuous monitoring. Today, cloud providers may offer snapshot security assessments to customers, but rarely do they offer ongoing visibility into their inner workings. Mobile services, in particular the trend of more enterprises approving bring-your-own-device (BYOD) policies, represent another area for continuous monitoring solutions. As these trends increase in the federal IT ecosystem, CIOs will look to security vendors for increasingly comprehensive tools and resources to maintain situational awareness for the entire enterprise.

With proper intelligence gathered through continuous monitoring, we can gain visibility into threats that are materializing and make better decisions on what defenses to employ. Through predictive analysis, we can anticipate what problems might occur and take actions to defend our systems before the attack. All of this yields improved situational awareness, the understanding of what is in our environment and how it can affect us.

Federal agencies are making efforts to move from periodic to continuous monitoring, but much work remains to be done. According to the Administration's FY 2011 FISMA report, only the VA reported 100% continuous monitoring capabilities across asset, configuration and vulnerabilities.[39]

That means there is a significant opportunity for improvement of the national cybersecurity posture by effectively implementing continuous monitoring. The goal should be to reach 100% on the next FISMA report—and stay there. Our opponents are not letting down their guard—neither should we!

39 www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf, page 21

About the Author

G. Mark Hardy is managing editor of the SANS Analyst Program and a leadership instructor with the SANS Institute. As founder and president of National Security Corporation, he has been providing cybersecurity expertise to government, military and commercial clients for more than 25 years.

G. Mark serves on the National Science Foundation's CyberWATCH Advisory Board and is a retired U.S. Navy Captain. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics, an MBA and a master's degree in strategic studies. He also holds the GSLC, CISSP, CISM and CISA certifications.

SANS would like to thank its sponsor:

Last Updated: June 29th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Cyber Defence Japan 2017	**Tokyo, JP**	**Jul 05, 2017 - Jul 15, 2017**	**Live Event**
SANS Cyber Defence Singapore 2017	**Singapore, SG**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS ICS & Energy-Houston 2017	**Houston, TXUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Los Angeles - Long Beach 2017	**Long Beach, CAUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Munich Summer 2017	**Munich, DE**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DCUS**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
Security Awareness Summit & Training 2017	**Nashville, TNUS**	**Jul 31, 2017 - Aug 09, 2017**	**Live Event**
SANS San Antonio 2017	**San Antonio, TXUS**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS Boston 2017	**Boston, MAUS**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Prague 2017	**Prague, CZ**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Hyderabad 2017	**Hyderabad, IN**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Salt Lake City 2017	**Salt Lake City, UTUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS New York City 2017	**New York City, NYUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS Adelaide 2017	**Adelaide, AU**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Chicago 2017	**Chicago, ILUS**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VAUS**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS San Francisco Fall 2017	**San Francisco, CAUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Tampa - Clearwater 2017	**Clearwater, FLUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NVUS**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS Dublin 2017	**Dublin, IE**	**Sep 11, 2017 - Sep 16, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, ILUS**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
Rocky Mountain Fall 2017	**Denver, COUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MDUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, GB**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, DK**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS SEC504 at Cyber Security Week 2017	**The Hague, NL**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London July 2017	**OnlineGB**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**