Reducing Attack Surface: SANS' Second Survey on Continuous Monitoring Programs

A SANS Survey

Written by Barbara Filkins

Advisor: David Hoelzer

November 2016

Sponsored by
RiskIQ

Executive Summary

Continuous monitoring (CM) begets a process of continuous improvement that works to reduce attack surface and improve security posture, according to the 2016 SANS survey on CM conducted during the months of July to September. In it, 63% of respondents said CM was improving their security posture.

These improvements are occurring even though continuous monitoring capabilities are still maturing, and some capabilities seem to be moving backward. For example, results indicate that a segment of respondents is monitoring less frequently (when they should be monitoring more frequently), and some organizations have drastically reduced their ability to use vulnerability data to help respond to events since our 2015 survey. Table 1 provides a short comparison of key year-over-year results.

Continuous monitoring remains a complex set of processes and practices that involves presenting a true representation of an organization's exposure to cyber risk.

—2015 SANS CM Survey[1]

Table 1. Continuous Monitoring Report Card

CM Performance	2015[2]	2016	Grade
Have immature or nonexistent continuous scanning and remediation programs	37%	16%	A+ for a 200% increase in having a program
Conduct active vulnerability scans on a weekly (CSC-recommended minimum frequency) or better basis	38%	37%	D for basically no improvement
Practice continuous assessment	13%	11%	D- for a small decrease in practicing continuous assessment
Improved visibility into enterprise systems and infrastructures by initiating a CM program	44%	48%	B- for a slight improvement in visibility based on using CM
Improved ability to accurately detect and remediate malicious events	44%	28%	F for a substantial decrease in ability to accurately detect and remediate malicious events

Other improvements are evident in the results of this year's survey, revealing a shift in drivers from compliance to actual prevention and defense (through proactively patching, testing, and deploying patches and repairs), which 51% report having achieved successfully. Respondents also see the leading vulnerability (identified by 73% of respondents) as security misconfiguration! This is a big indicator of program maturity.

[1] "What Are Their Vulnerabilities? A SANS Survey on Continuous Monitoring," www.sans.org/reading-room/whitepapers/analyst/vulnerabilities-survey-continuous-monitoring-36377, p. 1.

[2] "What Are Their Vulnerabilities? A SANS Survey on Continuous Monitoring"

felt that the adoption of a continuous monitoring program has improved their organization's security posture

of respondents do not regularly assess key network devices such as firewalls and routers

report that they have no measures to protect connected assets during remediation

The road to improvement should start with asset and inventory management, and then move to assessing the organization's capabilities. Can processes be improved? Can present tools do the job? Organizations should measure effectiveness against metrics, such as those defined by the CIS publication, Measurement Companion to the CIS Critical Security Controls.[3] These and other CM program components are covered in the following pages.

[3] "A Measurement Companion to the CIS Critical Security Controls (Version 6)," www.cisecurity.org/critical-controls/documents/A Measurement Companion to the CIS Critical Security Controls VER 6.0 10.15.2015.pdf

About the Respondents

A total of 292 individuals who consider themselves to be actively involved in vulnerability assessment and remediation responded to this SANS survey conducted between July and September 2016.

Roles and Workforce

Respondents mainly represent the "doer" perspective, with 46% representing individuals involved in security and system administration and analysis, as well as network operations. An additional 28% represent management, and 26% represent various other roles, including auditor, developer and compliance officer/risk manager. The security community leads representation, with 52% from the security community (35% admin or analyst, 10% managers or directors, and 7% architects).

The majority of respondents' organizations (57%) had workforces of more than 2,000, with 16% representing organizations larger than 50,000. The single largest group (24%) worked at organizations of between 101 and 1,000 employees. Most are headquartered in the United States but have operations throughout the world. See Table 2.

Table 2. Geographic Location of Respondents' Organizations

Country/Region	Operations	Headquarters
United States	76.4%	66.8%
Asia	37.0%	9.6%
Europe	33.6%	10.6%
Canada	25.0%	3.4%
Australia/New Zealand	22.3%	2.7%
Middle East	20.5%	2.4%
South America	19.5%	3.8%
Africa	15.1%	0.7%

Government is the leading business sector in this survey, which makes sense, given the emphasis on continuous monitoring placed on federal systems by the Federal Information Security Management Act (FISMA).[4] Banking and finance, followed by technology and cyber security businesses, were also strongly represented. See Figure 1.

What is your organization's primary industry?

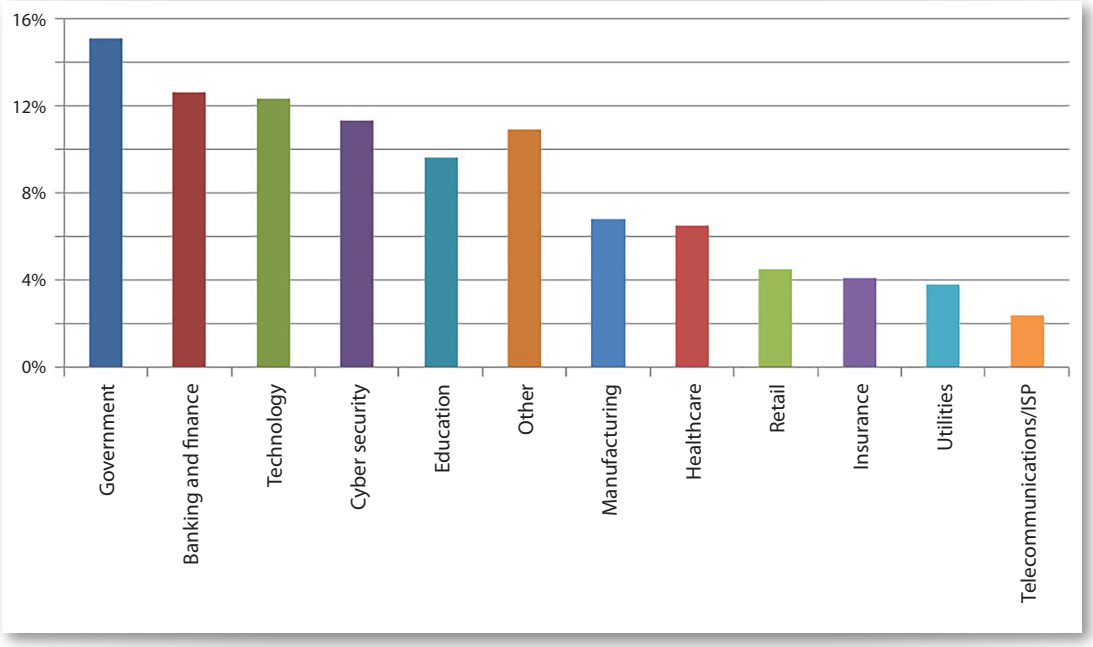

Figure 1. Many Industries Represented

[4] http://csrc.nist.gov/groups/SMA/fisma/faqs.html

Identifying critical assets and vulnerabilities has improved modestly, with a 6% increase over 2015 of those who think their programs are "mature," and a 14% increase in those who think their programs are "maturing." These gains, accompanied by a 23% decrease in those that feel their processes are "immature," indicate a positive change in perception. See Table 3.

Table 3. Maturity of Organizations for Identifying Critical Assets and Vulnerabilities

Process Maturity	Guidelines	2015	2016	% change
Mature	Formal identification and classification of critical assets; monitored at least weekly; integration of vulnerability status into SecOps and incident response (IR) programs	21.3%	27.1%	5.8%
Maturing	Informal identification of critical assets; monitored as needed; vulnerability data not automatically integrated into SecOps and IT programs	41.0%	54.8%	13.8%
Immature	No asset identification processes and a few processes for assessing systems, but the processes are not integrated, nor are they feeding other security and response programs	33.2%	10.3%	-22.9%
None	No process for identifying, classifying or assessing our systems	3.6%	5.9%	2.3%
Unknown/Unsure		0.8%	1.0%	0.2%

More Focus on Prevention

A sure sign of maturing programs is the shift in business drivers—moving from compliance in our 2015 survey, to prevention and detection (in 2016) in today's dynamic threat landscape. CM is actually becoming part of organizations' business survival strategies. Table 4 illustrates how the rank ordering of the drivers has changed.

Table 4. Primary Drivers for Continuous Monitoring Comparing Years 2015 and 2016[5]

What are the primary drivers behind your continuous monitoring program?

Answer Options	Rank in 2015	Rank in 2016
Defending assets through patch management, testing and deployment	5	1
Reducing attack surface (reducing risk)	2	2
Detecting incidents	4	3
Supporting incident response	9	4
Following and enforcing policies and procedures	6	5
Supporting operations	8	6
Identifying external threats that could be used to launch cyber attacks	N/A	7
Detecting unauthorized changes and misuse	7	8
Achieving compliance	1	9
Supporting remediation/workflow	10	10
Limiting legal liability	N/A	11
Asset identification and visibility	3	N/A

[5] The N/A notations in this table indicate that the related question was not asked in a particular year.

Drivers vs. Success

However, the success rate for satisfactorily achieving these goals needs to improve, despite the fact that 63% of respondents feel that the adoption of a CM program has improved their organization's overall security posture. With the exception of defending assets through patch management and supporting operations, fewer than half of the respondents for each driver feel that their organizations have been able to successfully achieve that driver. See Figure 2.

What are the primary drivers behind your continuous monitoring program?

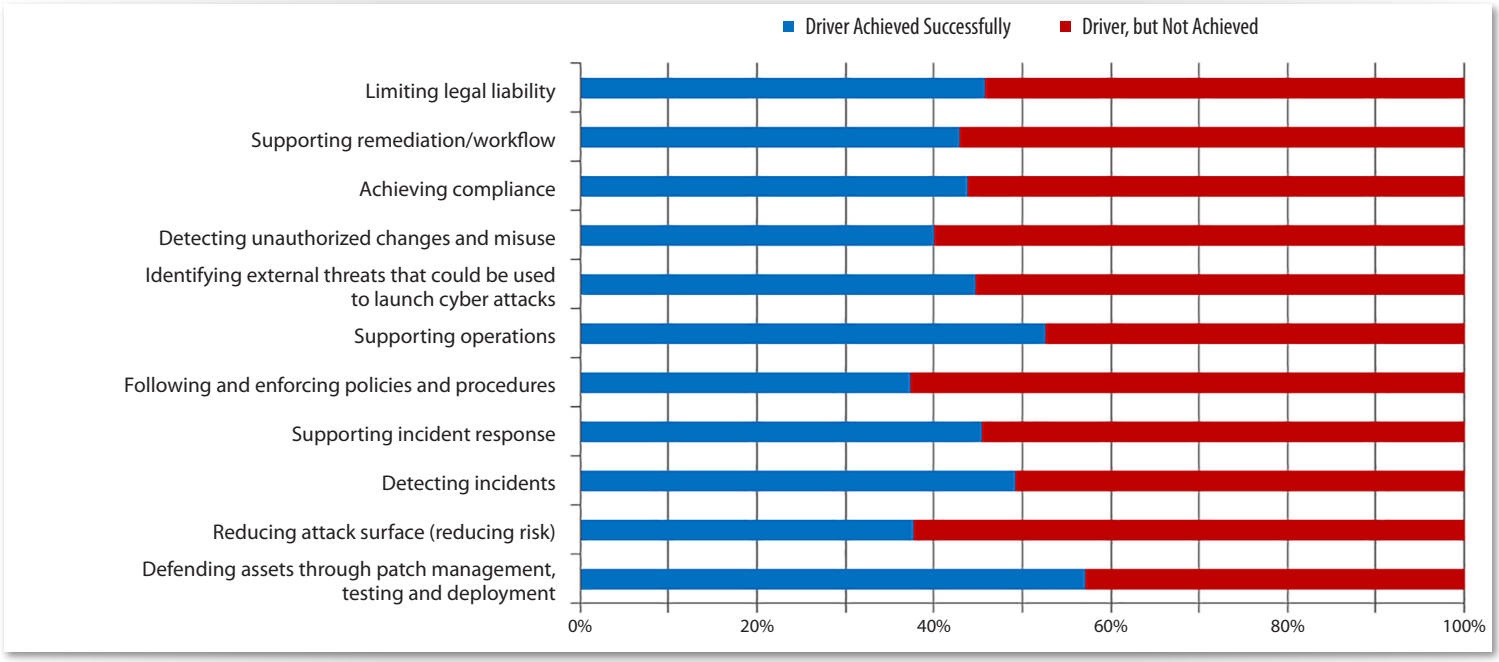

Figure 2. Achieved Versus Unachieved Drivers

This low rate of success is concerning because organizations may not be fully realizing the benefits or expectations of using CM. For example, only 38% of respondents have been successful in reducing attack surfaces with CM, which is key to reducing risk. This raises concern not just for federal systems, but for other organizations that rely on the National Institute of Standards and Technology (NIST) Risk Management Framework for their management of security risks.

> Continuous monitoring underlies the NIST Risk Management Framework (RMF), defined in NIST SP 800-30,[6] and required by the Federal Information Security Management Act (FISMA). U.S. government agencies must manage the portion of risk resulting from the incorporation of information systems into the mission and business processes of their organization using the RMF.[7]

[6] NIST SP 800-30 "Guide for Conducting Risk Assessments," http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Also, refer to NIST SP 800-37 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

[7] http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html

Vulnerabilities as Threats

A strong indicator that organizational awareness is maturing is that 73%, a clear majority, cite security misconfigurations, such as patches not being up to date or unauthorized ports open, as the leading threat to their organizations. See Figure 3.

What are the major categories of vulnerabilities you encounter during your scanning process? ***Select those you discover most frequently.***

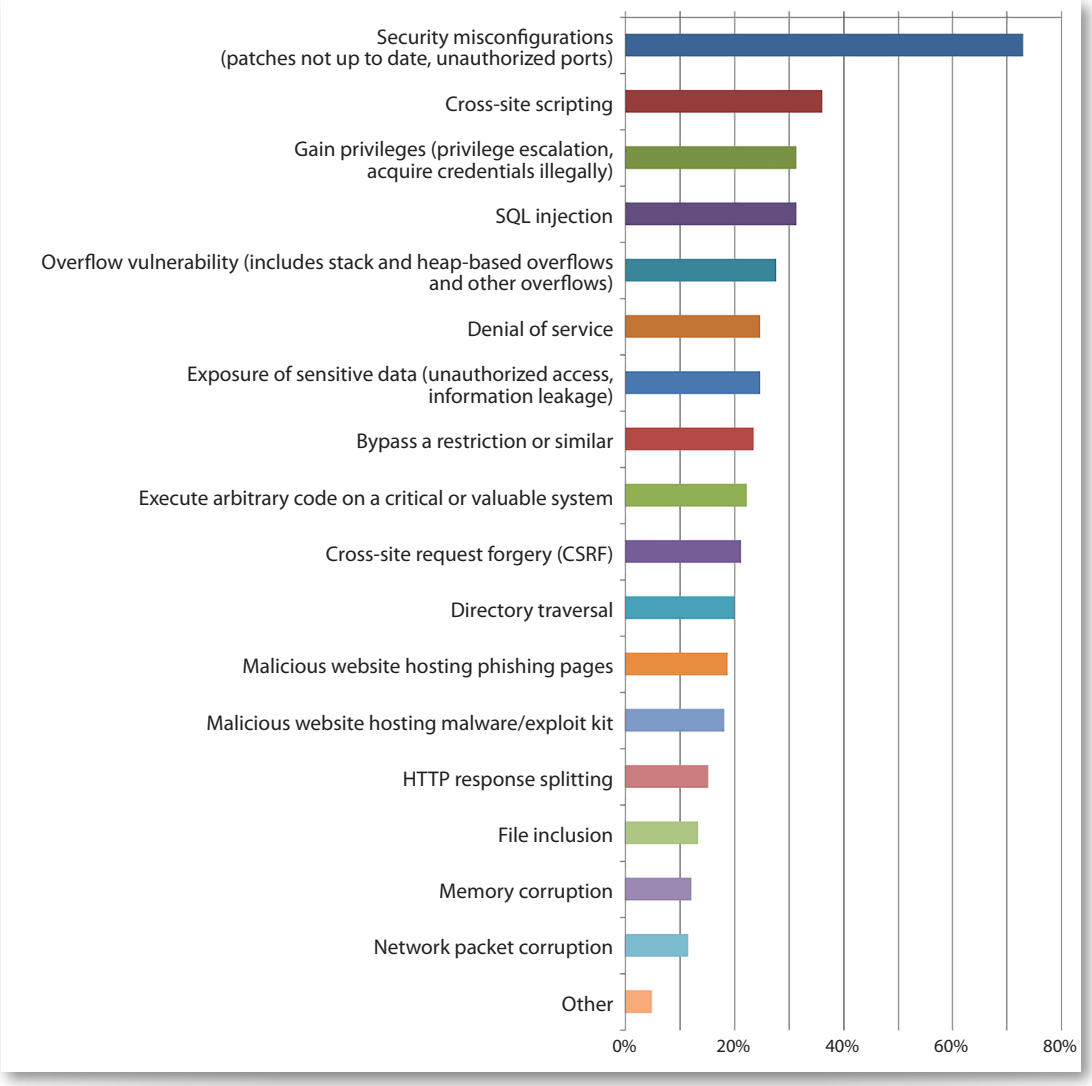

Figure 3. Major Categories of Vulnerabilities

TAKEAWAY:

Proper hygiene does not have to be expensive. An organization can establish a relatively low-cost program, such as the one developed by the Cyber Hygiene Campaign, which can achieve immediate and effective defenses against cyber attacks.[8] The Cyber Hygiene Toolkits provide key recommendations via easily understood instruction sheets and information for entities to improve their cybersecurity posture.[9]

This heightened awareness of security misconfigurations may be due to the increased emphasis on defending assets through patch management, testing and deployment, an area in which 51% of respondents' organizations have achieved success. Most security misconfigurations should be preventable through proper hygiene.

[8] www.cisecurity.org/cyber-pledge

[9] "Cyber Hygiene Toolkit," www.cisecurity.org/cyber-pledge/tools/index.cfm

Comprehensiveness of Programs

In 2015, 13% of respondents felt that they had wrapped 100% of their critical assets into their assessment programs. This number rises to 18% in 2016 (10% for devices and 8% for software). Clearly, organizations must continue to strive to include 100% of their critical assets, whether these are devices or software, in assessment and remediation programs. To do otherwise can lead to a false sense of confidence on the part of management and staff, who believe that the CM program is fully protecting their enterprise.

CIS Control 4: Continuous Vulnerability Assessment and Remediation[10]

CIS Control	Description
4.1	Run automated vulnerability scanning tools against all network systems at least weekly.
4.2	Correlate attack detection events with earlier vulnerability scan results.
4.3	Perform vulnerability scanning in authenticated mode; use a dedicated account.
4.4	Subscribe to a vulnerability intelligence service.
4.5	Deploy automated patch management and software update tools.
4.6	Monitor logs for scanning and administrator account activity.
4.7	Compare results of back-to-back vulnerability scans to check that remediation has been performed.
4.8	Establish a process to risk-rate vulnerabilities.

Asset Identification

A dependency exists between effective continuous monitoring and asset and configuration management. For example, if a rogue wireless access point appears and persists in a secure area, your asset management processes are not robust enough. If an unauthorized port is open and compromised, something fell short in your configuration management processes.

Critical asset identification and management is necessary for understanding the various security controls that need to be implemented for protection and how to maintain those controls. In a nutshell, you need to take the following steps:

1. Identify the critical assets. Determine what is essential for the business, who is accountable and what value the asset has. From an IT viewpoint, assets can include information (data elements, databases, procedures, archived information, continuity plans); software (application and system); devices (workstations, servers, and network devices); and services (email, DNS, managed storage, telecommunications).
2. Determine the secure baseline configuration for the asset, taking into consideration the production environment into which it will be placed.
3. Implement and test to understand the asset's behavior in that environment.
4. Document the resulting configuration baseline.
5. Monitor and remediate. That's where CM comes in.

[10] "CIS Critical Security Controls," www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf

Not All Inclusive

As in 2015, respondents considered servers (DNS, web, production) and network devices to be the most critical connected assets in need of monitoring. Supporting infrastructure (for example, underlying middleware or the network as a whole) has become increasingly critical to maintain the security of interconnected systems, especially in the modern era of mobile and cloud computing. In the 2016 SANS Healthcare Survey, for example, 75% considered high-integrity infrastructure free of malware to be an effective security control for reducing risk in cloud computing.[11]

Surprisingly, however, endpoints and workstations, ranked as third most-critical by 75% of respondents in 2015, are ranked only tenth in this year's results, despite multiple SANS surveys showing that endpoints—particularly user endpoints—are still very vulnerable to exploit.[12] See Figure 4.

What categories of information assets are connected to your network? Of those, which do you consider to be critical assets that should be monitored regularly, and which are included in your vulnerability assessment and remediation program?
Respond to only those that apply.

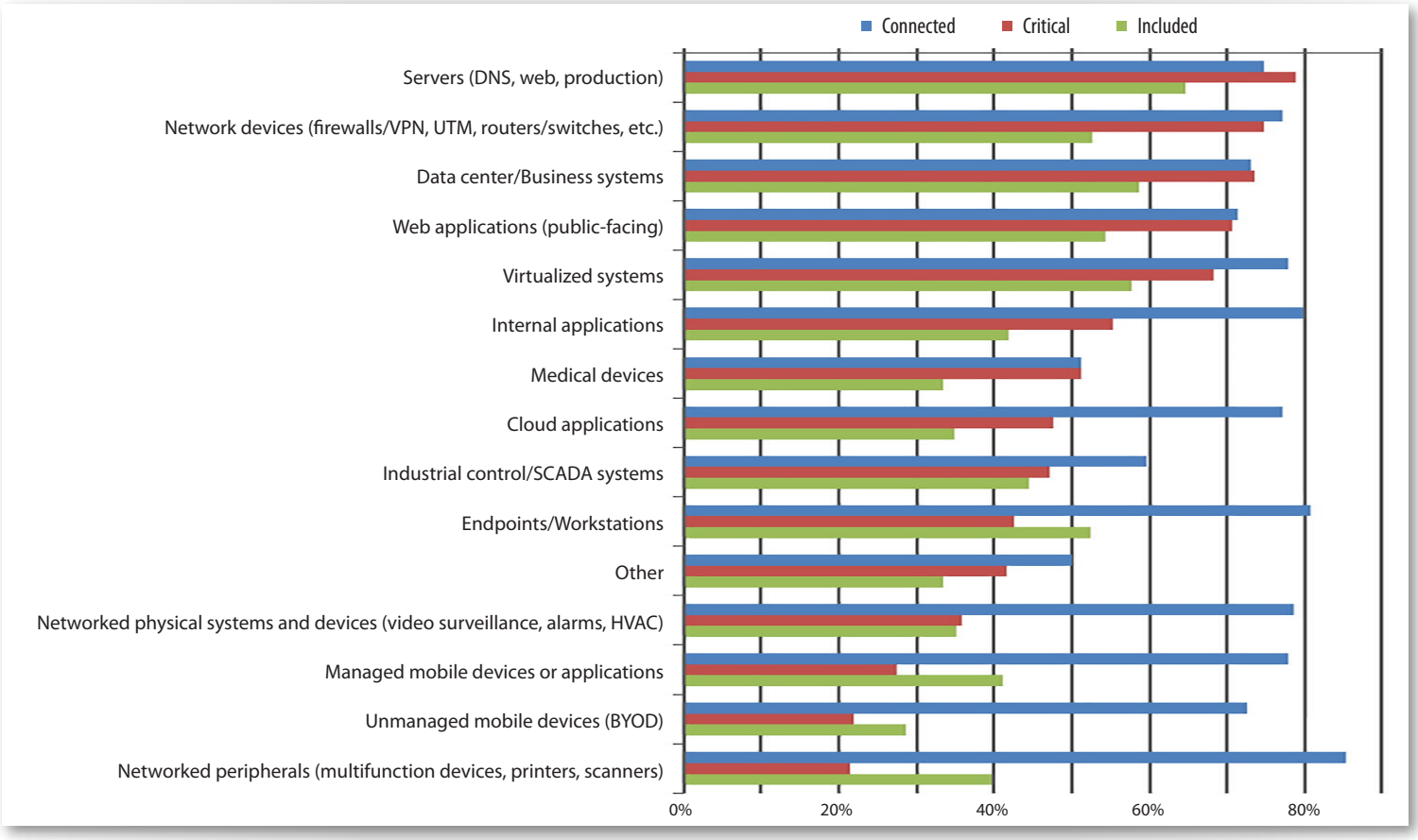

Figure 4. Connected, Critical, Included

[11] "Healthcare Provider Breaches and Risk Management Road Maps: Results of the SANS 2016 Information Security Practices in the Healthcare Industry," www.sans.org/reading-room/whitepapers/analyst/healthcare-provider-breaches-risk-management-road-maps-results-survey-informati-37105

[12] "Can We Say Next-Gen Yet? State of Endpoint Security," www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827

Overall, results show that although organizations consider most of their connected systems to be critical, they have yet to actually wrap these assets into their vulnerability assessment and remediation programs. This trend is greatest for key infrastructure components, as shown in Table 5.

Table 5. Comparison of Critical Assets Identified Versus Covered in Program

Asset	Critical	Included in Program	Difference
Servers (DNS, web, production)	78.8%	64.7%	14.1%
Network devices (firewalls/VPN, UTM, routers/switches, etc.)	74.9%	52.7%	22.2%
Data center/Business systems	73.7%	58.6%	15.1%
Web applications (public-facing)	70.7%	54.3%	16.4%
Virtualized systems	68.2%	57.8%	10.4%

This table indicates that many critical assets are not managed in a program that ensures an asset is configured to meet the organization's approved configuration standards. The differences seen in coverage actually fall above the "high risk threshold" (between 5% and 10%) for metrics related to CIS Control 3, as documented in the Measurement Companion to the CIS Critical Security Controls (Version 6).[13]

[13] "A Measurement Companion to the CIS Critical Security Controls (Version 6)," www.cisecurity.org/critical-controls/documents/A Measurement Companion to the CIS Critical Security Controls VER 6.0 10.15.2015.pdf, p. 6.

Still Not Continuous

Similar to our 2015 survey, this year's survey shows that the majority of organizations (92%) perform some level of active scanning, with 65% conducting such scans on a periodic basis (at least monthly). In 2015, 91% performed some level of active scanning and 56% did it on a periodic basis. Interestingly, there is a slight increase in the percentage of respondents who scan weekly as recommended in CSC 4, but this appears to be balanced by a decrease in daily scans and continuous assessment with periodic scans. See Table 6.

Continuous vulnerability scanning is a process wherein each new scan is initiated within 24 hours of the conclusion of the previous scan. This is more aggressive than the CSC 4 requirement of weekly scanning.

—2015 SANS CM Survey[14]

Table 6. Frequency of Active Scanning Between 2015 and 2016

Frequency of Active Scan	2015	2016	% change
We assess continuously AND conduct periodic point-in-time scans	8.3%	5.6%	-2.7%
Continuously (When one active scan completes, we start another.)	4.4%	5.1%	0.7%
Daily	6.3%	3.4%	-2.9%
Weekly (as recommended in CSC 4)	19.0%	22.5%	3.5%
Monthly or bimonthly	25.0%	28.7%	3.7%
Twice a year	7.3%	7.3%	0.0%
Annually	4.9%	4.5%	-0.4%
Only when needed (configuration changes, new threat information)	9.9%	10.7%	0.8%
Never	2.6%	0.6%	-2.0%
Unknown/Unsure	6.3%	7.3%	1.0%
Other	6.0%	4.5%	-1.5%

[14] "What Are Their Vulnerabilities? A SANS Survey on Continuous Monitoring," www.sans.org/reading-room/whitepapers/analyst/vulnerabilities-survey-continuous-monitoring-36377, p. 4.

Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets ([for] example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.

—The CIS Critical Security Controls for Effective Cyber Defense, Version 6.1[15]

Not all vulnerabilities discovered by respondents were in immediate need of patch and workaround, indicating that prioritizing is a critical aspect of remediating discovered vulnerabilities. Organizations are adhering to CIS Control 4.8 (see sidebar), which calls for risk rating vulnerabilities based on various factors to support more effective patch management within organizations.

Ranking Vulnerabilities

In this survey, 55% of respondents report that they are using some level of automation to address this process, with 12% reporting that this process is fully automated for them. See Figure 5.

Is your organization able to rank vulnerabilities based on exploitability and potential impact? If so, how automated is the process?

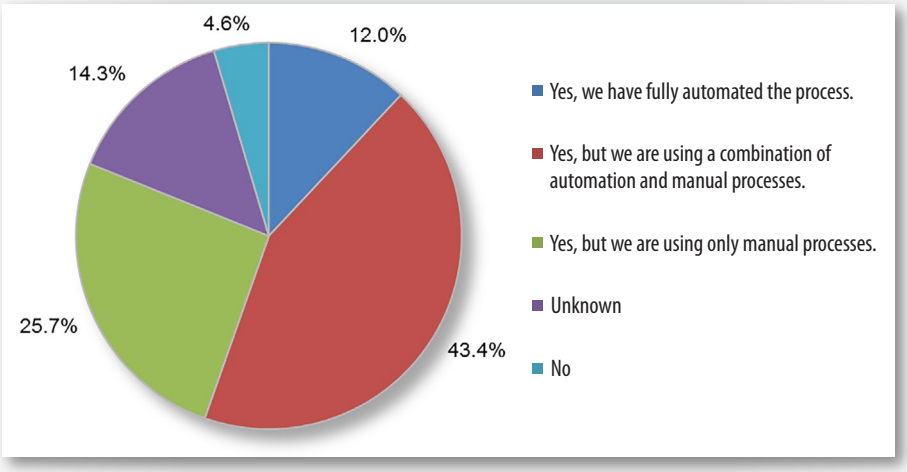

Figure 5. Vulnerability Prioritization

[15] "CSC 4: Continuous Vulnerability Assessment and Remediation: CSC 4.8," www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf, p. 18.

In this survey, 28% of respondents indicated that up to 9% of vulnerabilities detected required immediate attention, while the same number of respondents responded that 10–24% of their vulnerabilities needed immediate repair. See Figure 6.

Over the past 12 months, of the vulnerabilities discovered, what percentage were rated as "critical and in need of immediate patch, repair or workaround"?

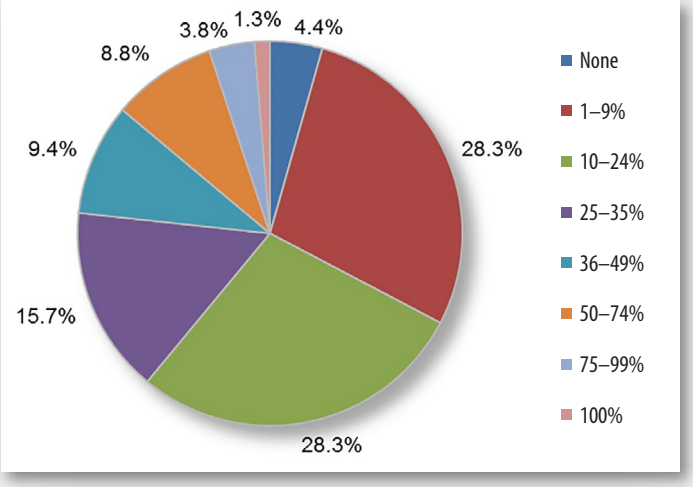

Figure 6. Criticality of Vulnerabilities

With only 4% of respondents saying that none of their vulnerabilities needed immediate repairs, that leaves 39% of respondents who are identifying vulnerabilities in immediate need of repair more than 25% of the time. In aggregate, there isn't much change in comparison to our 2015 survey. See Figure 7.

Over the past 12 months, of the vulnerabilities discovered, what percentage were rated as "critical and in need of immediate patch, repair or workaround"?

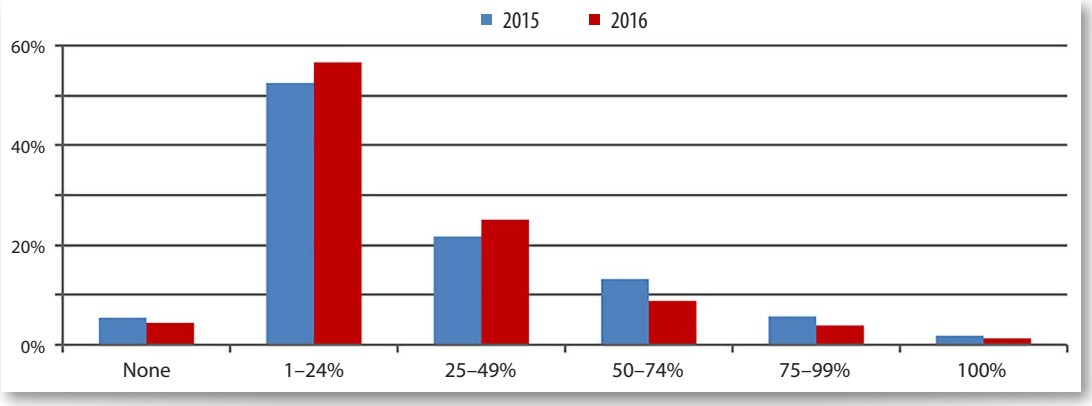

Figure 7. Percentage of Vulnerabilities Rated as Critical

Effective "Enough"

Overall, respondents appear satisfied with how effective their remediation processes are, with 54% selecting the option that their remediation processes are "effective enough," defined as keeping attackers out but needing more visibility into repair status and more workflow automation. See Figure 8.

How effective are your remediation processes?

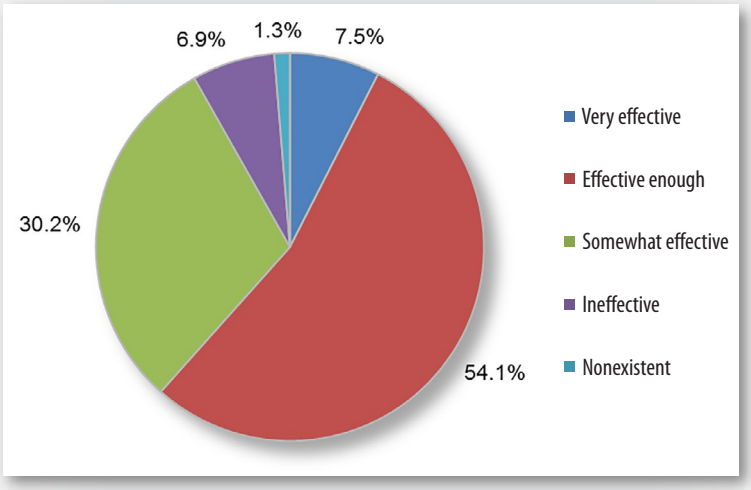

Figure 8. Effectiveness of Remediation Processes

Only 8% feel that their processes include automated prioritization and workflow to ensure vulnerabilities are repaired or shored up (with secure workarounds) across systems and attestation that repairs are maintained, warranting a "very effective" rating. The remaining 37% of those who have remediation processes (1% say they don't have processes) realize what they need to repair, but they are limited in follow-through, budgets, staff and tools, including automation.

Remediation Time Improving

Time to remediate is a measurement based on prioritization and criticality of vulnerabilities. Yet, the largest group of respondents, 21%, took, on average, two weeks to a month to remediate critical vulnerabilities, as shown in Figure 9.

"Remediation is difficult."

—2015 Survey Respondent re: impediments encountered in implementing CM

What is the average time it takes to repair, patch or implement a secure workaround for critical vulnerabilities, based on the past 12 months?

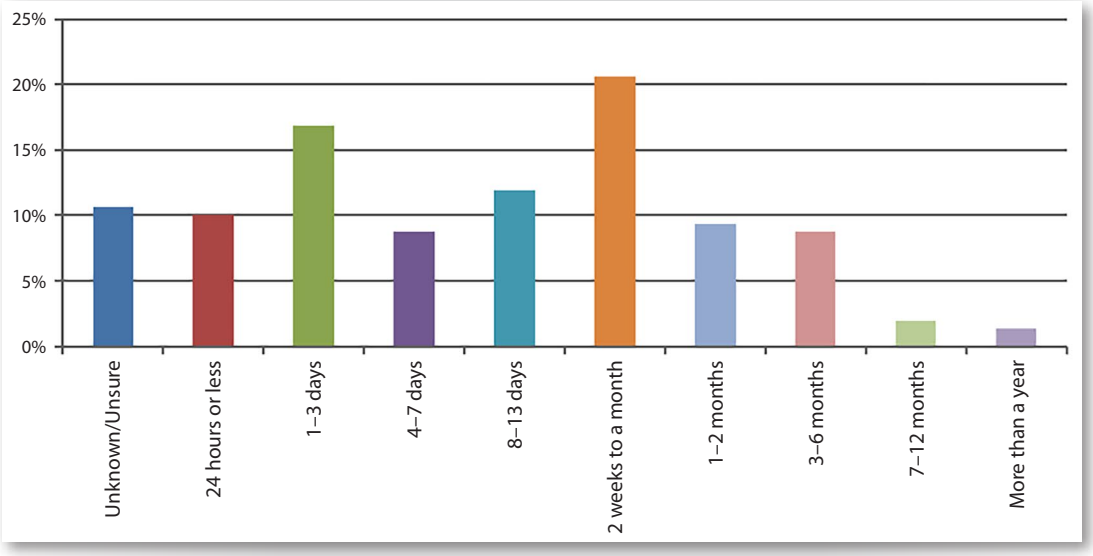

Figure 9. Time to Remediate

This is a substantial improvement from our 2015 survey results. In 2016, 68% of respondents were able to repair, patch or implement a secure workaround in less than one month as compared to 54% in 2015, dramatically shifting to shorter remediation times from 2015 in 2016. See Table 7.

Table 7.
Comparison of Time to Remediate 2015 vs. 2016

Time to Remediate	2015	2016
Under 1 month	53.6%	68.2%
1–2 months	16.7%	9.4%
3–6 months	10.8%	8.8%
7–12 months	5.6%	1.9%
More than a year	3.1%	1.3%

Remediation should consider more than returning vulnerable assets to service in a secure state. Organizations need measures to protect assets during the time it takes to repair them or when no repair is available. The majority of respondents (56%) report that they have no such measures!

Protecting assets during remediation can involve many approaches. Suggestions provided by respondents include the use of techniques such as network segmentation or isolation, web application firewalls (WAFs) and compensating controls.

Despite these improvements, the vast majority of critical vulnerabilities are not repaired within the risk thresholds established by the Measurement Companion to the CIS Critical Security Controls (Version 6), wherein a week of vulnerabilities in critical systems represent a moderate risk and those over a month represent high risk. See Table 8.

Table 8. Risk Thresholds Established by CSC 6.0[16]

ID	Measure	Risk Threshold
4.4	How long does it take, on average, to completely deploy operating system software updates to a business system (by business unit)?	• Lower – 1,440 Minutes (1 Day) • Moderate – 10,080 Minutes (1 Week) • High – 43,200 Minutes (1 Month)
4.5	How long does it take, on average, to completely deploy application software updates to a business system (by business unit)?	

Only a Fraction Remediated

Less than 6% achieved full remediation of all identified assets in 2016, which is slightly less than the 6% that did so in 2015. In 2016, 5% said they achieved 100% remediation for devices, and 4% did so for software. The largest group, 35%, reported 75% to 99% of their critical device assets being assessed; only 26% of respondents fall in this range for remediation. For software, there is also a significant difference: 28% have assessed 75% to 99% of their critical software, but only 19% have remediated in this range.

Recall the risk threshold previously discussed for critical asset identification and assessment, and it is easy to see that these remediation percentages still place the CM operations in the area of highest risk.

[16] "Measurement Companion to the CIS Critical Security Controls (Version 6)," www.cisecurity.org/critical-controls/documents/A Measurement Companion to the CIS Critical Security Controls VER 6.0 10.15.201, p. 7.

Continuous monitoring efforts, while not perfect, are already reaping benefits. Overall, 63% of respondents believe that the adoption of a continuous monitoring program has improved their organization's security posture, especially in the following areas. See Table 9.

Table 9. Top Areas of Improvement for CM

Area of Improvement	% Response
Visibility into enterprise systems and infrastructure	21.9%
Accurately detect and remediate malicious events	12.5%
Faster patch deployment	12.5%
Smaller attack surfaces = fewer incidents or breaches	10.4%
Visibility into unauthorized changes	9.4%
Faster remediation through asset identification	8.3%
Network reliability	8.3%
Visibility into external vulnerabilities	6.3%
Detect unauthorized changes to business applications	5.2%
Other	1.0%
System reliability	1.0%

But the challenge of how to improve always remains. Can the 2016 survey provide some insight in how to do things better?

Start In-House

Be aware that there may be much improvement that can be accomplished using resources and tools already in-house, provided that proper commitment, planning and prioritization can be achieved. As in 2015, the majority of 2016 respondents (54%) manage their vulnerability assessment and remediation activities or programs in-house. Another 42% use a combination of in-house management and outside managed services. Only 2% operate solely though managed services. See Figure 10.

How are your vulnerability assessment and remediation activities or programs managed? *Select the most appropriate.*

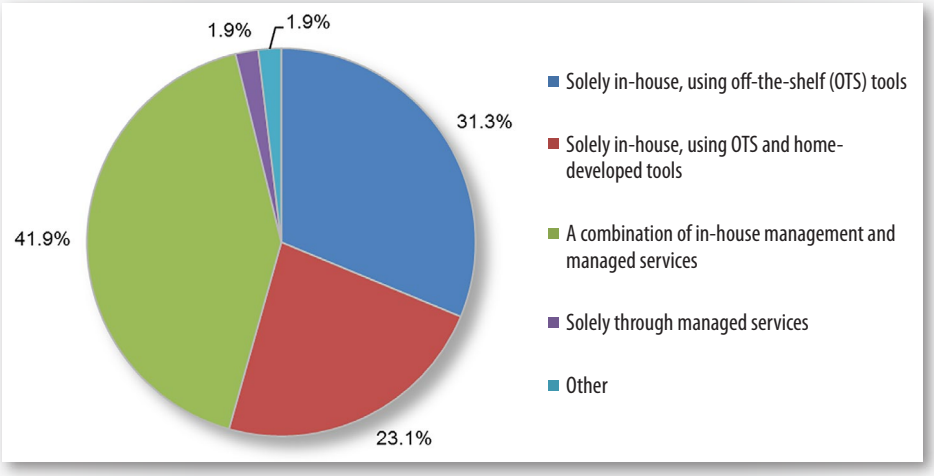

Figure 10. How Vulnerability and Remediation Activities and Programs Are Managed

Evaluate the Workflow

Reporting capabilities—the flow of information in support of CM activities—tie directly into the effectiveness of your procedures and your program. Staff members need key reports on operations and vulnerabilities, as well as a feedback loop for vulnerabilities discovered during events.

Again, as in 2015, 96% of this year's respondents depend on reports for patch status, and 90% utilize reports to determine vulnerability status. See Figure 11.

What are the key reports or information categories your security and operations staffs use to detect vulnerabilities? *Select only those that apply.*

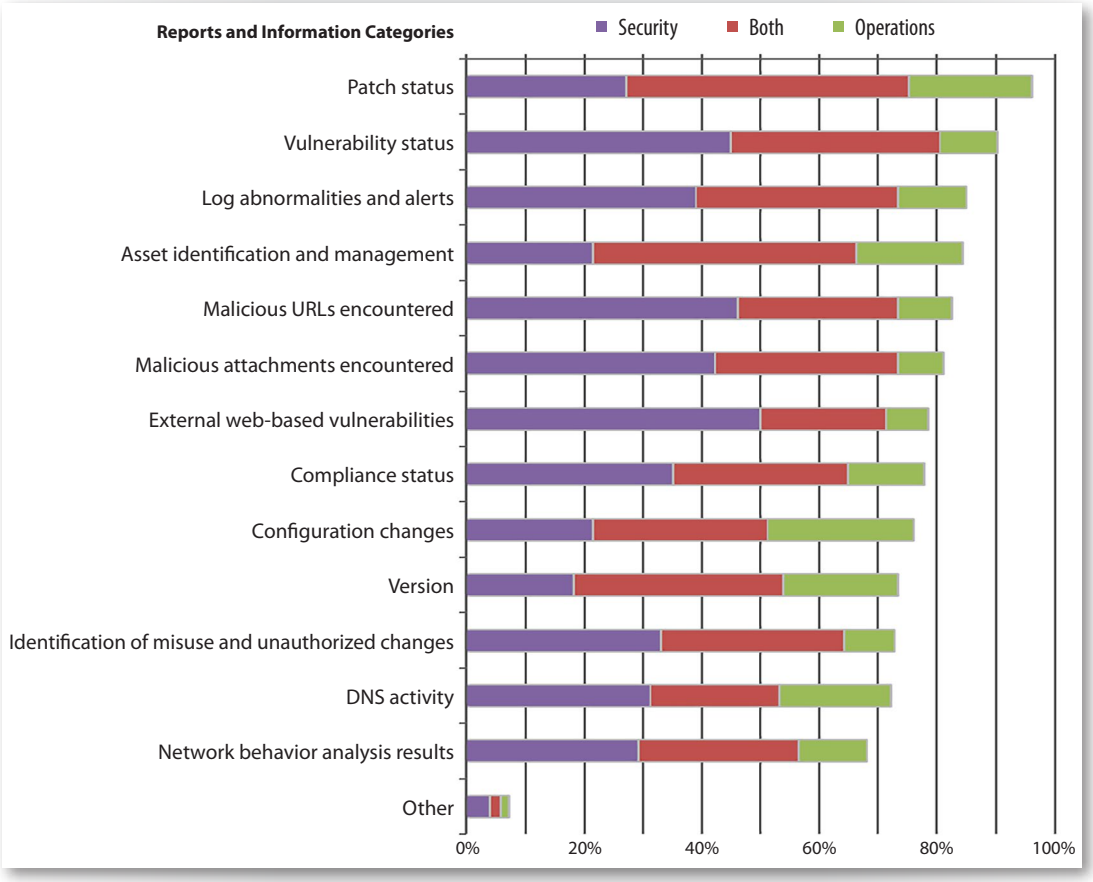

Figure 11. Key Reports or Information Categories Used to Detect Vulnerabilities

Take into account the different information needs of the various roles involved in CM. The 2016 survey revealed the following distinctions:

- Respondents in strictly security-related positions favor vulnerability status information and reports that can provide a view into external threats, including web-based vulnerabilities, malicious URLs and attachments.
- Respondents mainly from operations-related positions want information that concentrates on activity related to internal hygiene, such as configuration, patches and asset management.
- Respondents with a combined perspective across security and operations need information that reflects a more comprehensive view of CM processes, such as asset identification, configuration, reviewing logs and system activity, and tracking vulnerability status.

TAKEAWAY:
CM program managers should meet with the key players in the organization to work through process and information flow so they can understand limitations and bottlenecks in the program affecting cyber security and improve CM processes.

CIS Controls as Guide

The CIS Control 4, Continuous Vulnerability Assessment and Remediation, provides a ready guide for best practices related to CM programs. Most respondents either have already adopted many of its practices or plan to, as noted in Table 10.

Table 10. Adoption of CIS Control 4.0 Family

CIS Control	Description	Yes	No but have plans to	No and no plans
4.2	Correlate attack detection events with earlier vulnerability scan results	26.3%	53.1%	20.6%
4.4	Subscribe to vulnerability intelligence service	45.6%	36.9%	17.5%
4.6	Monitor logs for scanning and administrator account activity	55.0%	38.1%	6.9%
4.7	Compare results of back-to-back vulnerability scans to check that remediation was performed	47.5%	43.8%	8.8%

This table illustrates that utilizing vulnerability data with detection is of the lowest priority, while log monitoring, followed by vulnerability scanning, is already widely used or in the program plan.

Take Stock of What You Have

This year, respondents placed a greater emphasis on the lack of appropriate tools as an impediment to CM. This likely speaks to a renewed or heightened emphasis on automation, which was on the wish list of our 2015 survey respondents.

As shown in Figure 10, 54% of respondents use off-the-shelf tools, either solely or in conjunction with those developed in-house. However, before investing in new tools, take stock of what you have. You may find that training on and configuration of your current investment may address the current issues and gaps in utilization. Table 11 provides some high-level guidelines for the tools that would be involved in the management of your CM program.

Table 11. Checklist for CM Tools as Guided by CIS Controls

CSC	Title/Goal	Tool Category/Requirements
1	**Inventory of Authorized and Unauthorized Devices:** Understand what is on the network so it can be defended.	**System and Network Asset Management Tools** • Do your tools go beyond simple lists of assets? Can they discover devices on your network and poll the network at the intervals you need? Do they have a lightweight effect on network traffic? • Can these tools go beyond asset inventory and compare running configurations against a device configuration template in support of CIS Controls 3 and 4? • Do your tools support a centralized database repository and granular event data, and can this data be exported to a central monitoring environment?
2	**Inventory of Authorized and Unauthorized Software:** Allow only authorized software to execute on an organization's information systems and other assets.	**Anti-malware tools** • Do you have both network-based, malware-detection sandboxing tools and host-based antivirus and whitelisting tools? • Can your tools produce significant monitoring and event data both on a scheduled basis and on demand? • Do your tools support centralized management with data that can integrate and correlate with other data in a CM environment?
3	**Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** Use what you have!	**Enterprise Configuration Tools** • Does your organization already have the technology systems necessary to securely configure systems at scale, such as Microsoft® Active Directory Group Policy Objects, UNIX Puppet or Chef? • Do these systems utilize configuration standards or benchmarks, such as those defined by the Center for Internet Security or found in the NIST National Checklist Program Repository?
4	**Continuous Vulnerability Assessment and Remediation:** Implement patch management systems that cover both operating system and third-party application vulnerabilities.	**Configuration and Patch Management Systems** • Do you have a host-based agent that can update patch status and configuration items both on demand and scheduled? • Does it allow centralized collection of results? Does it tie into your asset inventory/management system? **Commercial Vulnerability Management Systems** • Can your enterprise tools perform both authenticated and unauthenticated scans? • How much data do they produce? Can you handle the output from continuous monitoring that involves scheduling daily or weekly scans of systems and subnets? • Do your tools allow you to compare a sound baseline of what is running at the endpoint/system/network level against newer scans to determine what has changed and what the risks are? • Do you need specialized Web application and database scanning tools or can your present scanners cover these technologies adequately as a starting point? • Does your platform support the use of cyber threat intelligence information?

TAKEAWAY:

Looking at procuring security products for continuous monitoring or negotiating the renewal of an existing license? Consider using Security Content Automation Protocol (SCAP)-validated tools.

SCAP, maintained by NIST and its industry partners, uses commonly accepted standards to enable automated vulnerability management and security policy compliance metrics.[18] Many security vendors support data import, export and analysis in standard SCAP-compatible formats that interoperate.

Evaluate your existing security information and event management (SIEM) and analytics platforms to see whether they are a reasonable starting point for aggregation and analysis, but keep in mind that governance, risk and compliance tools, and dashboards may offer more reporting and risk-scoring capabilities.

There are several starting points from which to develop a detailed set of requirements for a CM system, including the NIST Interagency Report 7756 (Second Draft).[17]

[17] "CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model (Second Draft)," http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf

[18] https://scap.nist.gov

Summary: Putting Improvement into Action

Continuous monitoring is not a single activity. Rather, it is a set of activities, tools and processes—asset and configuration management, host and network inventories, and continuous vulnerability scanning—that must be integrated and automated all the way down to the remediation workflow. This includes monitoring all systems and activities—at all times—for unauthorized changes, vulnerabilities, abnormal operation, needed patches and workarounds.

This survey points out that, although CM is shifting focus and slowly improving, it still has a way to go to attain the maturity needed to become a critical part of an organization's business strategy. It also hints at the steps an organization should take to improve its existing CM program or establish a new one.

Continuous monitoring programs do not necessarily call for a lot of new resources; they can be developed and/or applied using the skills and tools already in-house. Here are the key steps:

1. **Identify key workflows and any possible gaps.** You may find that your organization is already undertaking many of the activities associated with a CM program, but those activities lack a unified approach. Understand how the duties of security and IT operations overlap and complement each other, how communication and reporting occurs, and how action is taken on that communication.
2. **Undertake an asset identification project and use the results to identify your critical assets.** For a large enterprise, don't underestimate the time and effort this might take.
3. **Assess the currently available tools.** Do you have the proper tools in-house? Can they be configured to "do the job" before you invest in more advanced or complex tools? Are they interoperable? Can they share data to establish an asset and configuration baseline of enterprise assets? Can they transform this data into dynamic information for visualization and management of CM workflows?

Finally, and most important, the major challenge remains in capturing and holding management commitment—being able to address the basic impediments that this year remain much the same as last year's. See Table 12.

Table 12.
Impediments to Continuous Monitoring (2015 vs. 2016)

Impediment	2015 Rank	2016 Rank
Lack of budget	2	1
Lack of appropriate tools	4	2
Lack of trained staff	1	3
Lack of management support	3	4
Inability to integrate tools	5	5
Lack of awareness of how this can help us	6	6

To meet this last challenge, consider two additional activities:

4. **Commit resources to continuous monitoring.** Whether developing a new CM endeavor or improving the existing one, treat the effort as a serious project with established scope, schedule and resources under the direction of a dedicated program manager.

5. **Establish metrics.** Use metrics, such as those referenced in this paper for the CIS Controls, to allow management to assess the effectiveness of CM on the security posture of the organization, as well as to validate its return on the investment.

About the Authoring Team

Barbara Filkins, a senior SANS analyst who holds the CISSP and SANS GSEC (Gold), GCIH (Gold), GSLC (Gold), GCCC (Gold) and GCPM (Silver) certifications, has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. She is deeply involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, as well as the legal aspects of enforcing information security in today's mobile and cloud environments.

David Hoelzer is a SANS fellow instructor, courseware author and dean of faculty for the SANS Technology Institute. In addition to bringing the GIAC Security Expert certification to life, he has held practically every IT and security role during his career. David is a research fellow in the Center for Cybermedia Research, the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), and the Internet Forensics Lab. Currently, David serves as the principal examiner and director of research for a New York/Las Vegas-based incident response and forensics company and is the chief information security officer for an open source security software solution provider.

Sponsor

SANS would like to thank this survey's sponsor: