Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

What Are Their Vulnerabilities?: A SANS Survey on Continuous Monitoring

This report offers an analysis of the survey findings and recommendations for improving practices. It also offers a definition of what a mature program should look like now and in the future. The goal, ultimately, is to provide a metric by which organizations can gauge their own progress in an objective way.

Copyright SANS Institute
Author Retains Full Rights

What Are Their Vulnerabilities?

A SANS Survey on Continuous Monitoring

Written by David Hoelzer

October 2015

Sponsored by

AlienVault, Arbor Networks, HP, and Tenable Network Security

©2015 SANS™ Institute

Executive Summary

Continuous monitoring is a complex set of processes and practices that involves presenting a true representation of an organization's exposure to cyber risk. According to results of a new SANS survey, the majority of IT professionals believe their continuous monitoring programs are mature or maturing (by maturing, we mean they are improving these programs). Yet how often and how comprehensively they scan—and follow through with remediation—reveal a different picture. The results raise several questions: What should a mature continuous monitoring program look like? How can you measure the maturity of your organization's program today? And, what elements of a successful program are you missing?

The results of the survey seem positive at first glance: 62% of respondents consider their asset identification and classification capabilities to be "mature" or "maturing" (meaning they are improving). And 58% have identified 50% or more of their critical assets and incorporated them into their assessment programs and processes.

Results also reveal some very disturbing realities about the overall effectiveness of information security scanning and monitoring programs. For example, 19% perform scans weekly, and 19% scan more frequently, resulting in only 38% of respondents meeting the recommendations of CIS Critical Security Control (CSC) 4.[1]

The good news is that continuous monitoring has improved organizational visibility and detection for more than 40% of respondents, with respondents reporting improvements in the accuracy of detection for malicious events, reductions in the attack surface and faster patch deployment.

This report offers an analysis of the survey findings and recommendations for improving practices. It also offers a definition of what a mature program should look like now and in the future. The goal, ultimately, is to provide a metric by which organizations can gauge their own progress in an objective way.

Key Findings

37% have immature or nonexistent continuous scanning and remediation programs

38% conduct active vulnerability scans on a weekly (CSC-recommended minimum frequency) or better basis, and only **13%** practice continuous assessment

44% improved visibility into enterprise systems and infrastructures by initiating a continuous monitoring program, and **44%** improved their ability to accurately detect and remediate malicious events

57% lack trained staff, **42%** lack sufficient budgets and **41%** lack management support for implementing continuous monitoring programs

[1] www.cisecurity.org/critical-controls.cfm

Continuous monitoring is quickly coming to the forefront as a key activity for the ongoing security of networks, systems and, by extension, enterprises.[2] However, survey results starkly illustrate that we are approaching a dangerous state in which we believe we have appropriately addressed problems, though we have, in fact, not adequately remediated them—therefore unknowingly leaving a window of opportunity open for attackers.

Who Completed the Survey?

The majority (74%) of the 456 survey respondents represent "practitioners" (security analysts, security architects, security operations, network operations, security managers). Almost one-third (31%) represent organizations larger than 10,000 employees. See Figure 1.

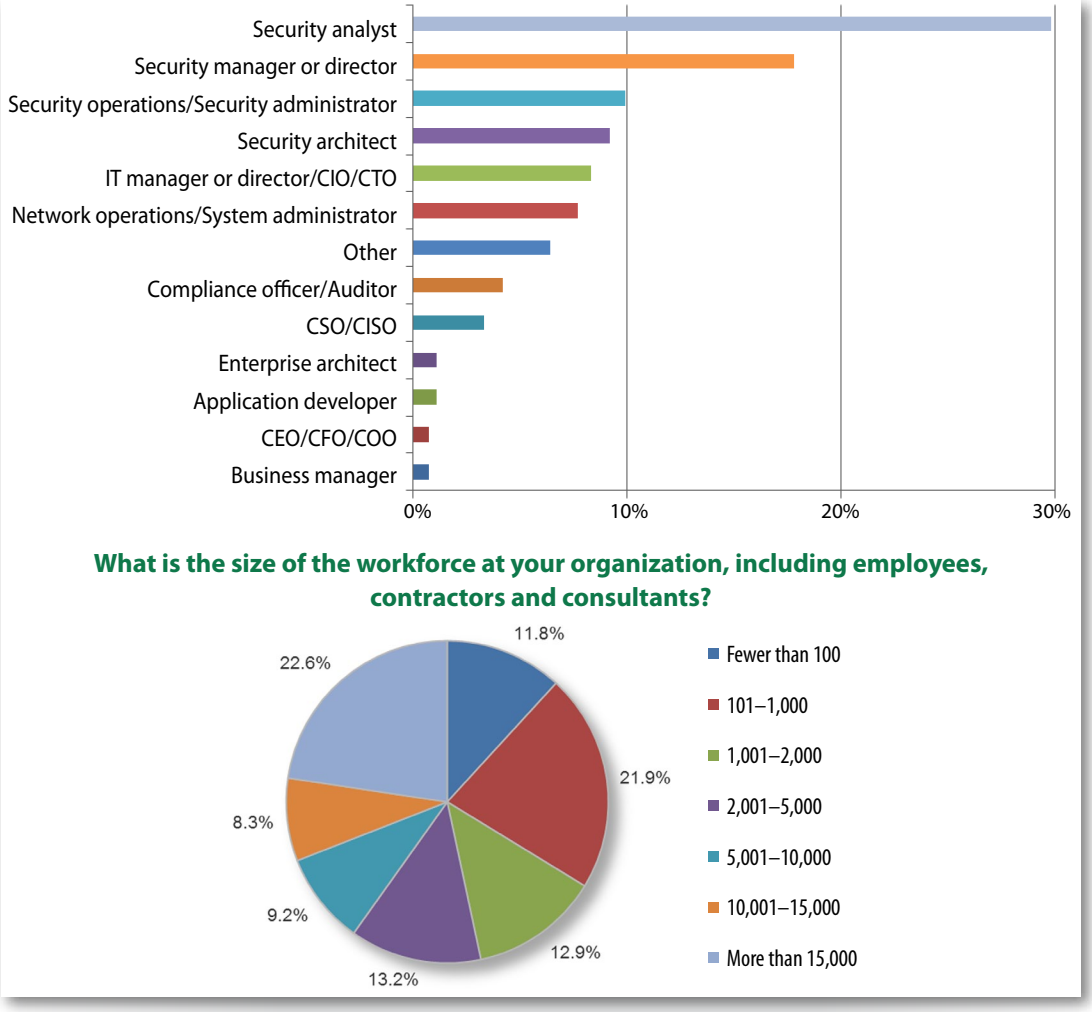

Figure 1. Practitioners, More than Half from Large or Very Large Organizations

[2] Consider these references on the growing emphasis on continuous monitoring:
NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
https://cio.gov/protect/continuous-monitoring/
www.govinfosecurity.com/continuous-monitoring-c-326
www.networkworld.com/article/2895088/security0/conventional-it-security-is-failing-continuous-monitoring-and-mitigation-can-help.html

Why Organizations Implement Continuous Monitoring

Survey results illustrate a definite business need for continuous monitoring. Compliance drives monitoring programs for 53% of respondents, while 47% want to reduce the attack surface and its associated risk, and 39% are driven by the need to identify their assets and provide visibility. Table 1 provides a look at what motivates security teams to incorporate continuous monitoring.

Table 1. Drivers Behind Continuous Monitoring Programs

Driver	1	2	3	Total Response
Compliance	30.7%	11.2%	10.6%	52.5%
Reduce attack surface (reducing risk)	18.0%	15.2%	14.0%	47.2%
Asset identification and visibility	18.9%	10.2%	9.9%	39.1%
Detecting incidents	12.7%	12.1%	6.2%	31.1%
Proactive patch management, testing and deployment	5.0%	12.1%	10.9%	28.0%
Policies and procedures	4.7%	11.2%	10.6%	26.4%
Detecting unauthorized changes and misuse	3.4%	8.1%	10.9%	22.4%
Infrastructure and operational support	1.9%	8.4%	8.1%	18.3%
Incident response support	2.2%	6.5%	8.1%	16.8%
Remediation/Workflow support	0.9%	4.0%	9.0%	14.0%
Other	0.9%	0.0%	0.3%	1.2%

It is interesting that aiding in organizational incident response efforts is very low on the list of drivers at just 17% overall. This is especially alarming because reducing risk and enhancing the ability to respond to incidents are among the key reasons for instituting continuous monitoring.

Common Definitions

Unfortunately, many organizations have seized upon continuous monitoring as a buzzword and marketing tool for products and services. For this paper, scanning, monitoring and remediation are defined in the following way:

- **Continuous Monitoring.** *Continuous monitoring* includes (but need not be limited to) the activities involved in change control, configuration management, host and network inventories and continuous vulnerability scanning. This describes monitoring all systems and activities—at all times—for unauthorized changes, vulnerabilities, abnormal operation, needed patches and workarounds.
- **Continuous Vulnerability Scanning.** *Continuous vulnerability scanning* as 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.
- **Remediation.** *Remediation* includes all activities undertaken to eliminate or at the very least mitigate a discovered vulnerability or other unacceptable risk from an operational point of view. This can include activities such as patching, reconfiguration, mitigation through virtual patching and any number of other activities that reduce a risk to an acceptable level.

Critical Controls Guidelines

The definition of continuous monitoring adopted for the purposes of this analysis is based on a synthesis of the requirements within the CIS Critical Security Controls (CSCs), particularly Controls 1–4, shown in Table 2.[3]

Table 2. Critical Security Controls 1–4, Version 6.0

1	Inventory of Authorized/Unauthorized Devices
2	Inventory of Authorized/Unauthorized Software
3	Secure Configurations for Hardware/Software
4	Continuous Vulnerability Assessment

Effectively, this means that continuous monitoring is not a single activity, but rather the composite result of many prerequisites and activities. Only through conscious effort to synthesize these systems and processes into a useful, correlated amalgam can organizations produce effective continuous monitoring.

[3] www.cisecurity.org/critical-controls.cfm

Comprehensiveness of Scanning

It's critical to note not only how often organizations scan their environments, but what they scan. According to the sample, 88% of public-facing systems (DNS, web and production) and 64% of public-facing web apps are included in the vulnerability assessment and remediation program for the enterprise. Although these percentages seem high enough, the resulting exposure still leaves much room for improvement. See Figure 2.

What categories of information assets are included in your vulnerability assessment and remediation program? ***Select only those that apply.***

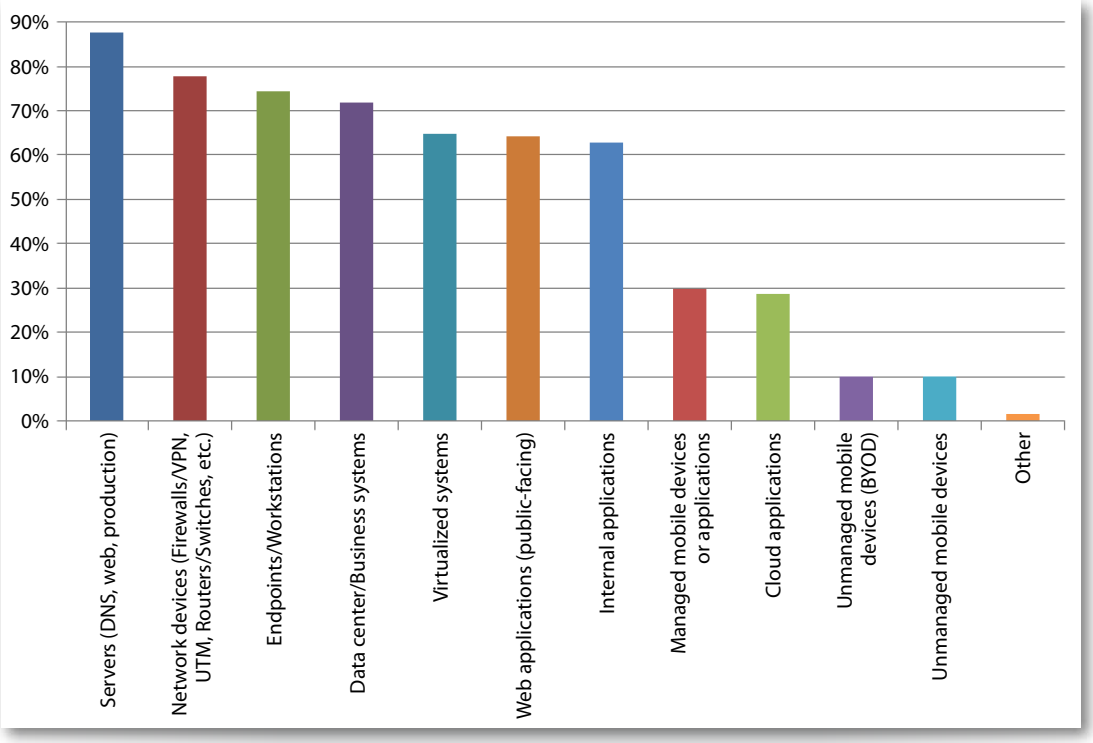

Figure 2. Assets Covered in A&R Programs

This is especially true when we consider a service as critical to an organization as DNS. It is often said, quite accurately, that should an attacker successfully compromise your DNS, it owns your organization. DNS server misconfiguration remains a major vulnerability source and has become a top attack vector.[4] A quick review of US-CERT 2015 warnings lists two DNS vulnerabilities among the nine issued to date for 2015.[5] Organizations that develop their own web applications must remain ever-vigilant to the vulnerabilities that can be introduced as a result of poor software coding and configuration issues.[6]

[4] www.sans.org/reading-room/whitepapers/analyst/securing-dns-thwart-advanced-targeted-attacks-reduce-data-breaches-35597

[5] www.us-cert.gov/ncas/alerts

[6] www.toptal.com/security/10-most-common-web-security-vulnerabilities

Mobile and cloud applications are also lagging behind in continuous monitoring programs. Fewer than 30% of respondents are wrapping these applications into their assessment and remediation (A&R) programs—and this includes managed mobile devices. For the unmanaged devices, and even for managed devices, device owners are not keen on allowing security programs such as mobile device management (MDM) and network access control (NAC) access to the apps and data on their devices.

When it comes to the cloud, the low adoption of A&R, just 29%, is understandable, given how nebulous security measures and monitoring in the cloud are today. The inherent risks involved in storing data in the cloud and similar issues of ownership do make this an area in which organizations should more actively focus attention. The disconnect between who owns the application and what other entities are co-hosted in an environment may make it difficult to scan and otherwise secure cloud-based assets.

Know Your Agreements

Carefully examine all agreements pertaining to cloud-based services before including them in your scanning and remediation program. Terms of service usually include specific provisions requiring advance notification and permission before any scanning activities can take place. Don't make the mistake of violating a contract with a key service provider.

Moving Target

As stated earlier, continuous monitoring is the product of the integration of many processes, activities and tools that deliver a result we can point to and say, "That's continuous monitoring."

For example, an organization that has not undertaken or maintained a comprehensive inventory of all systems connected to its network cannot possibly state that it has an effective continuous monitoring program. In our survey, only 21% consider their asset identification and classification capabilities to be "mature." Perhaps more telling, 33% of respondents rate their capabilities as "immature," highlighting the need for improved understanding of the assets attached to the network. See Figure 3.

How mature is your organization's process for identifying critical assets and vulnerabilities?

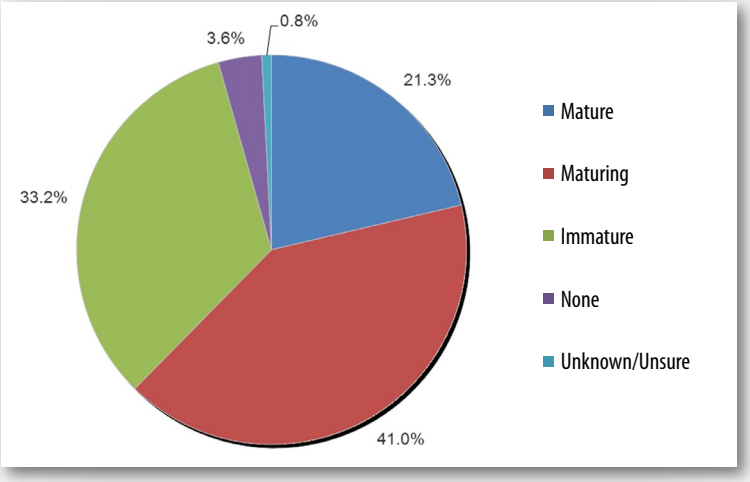

Figure 3. Maturity in Identifying Critical Assets and Vulnerabilities

CSCs 1 and 2 emphasize the importance of identifying and maintaining an inventory all systems and networks within an enterprise. This becomes the context for later controls, such as Control 4, which addresses continuous scanning for vulnerabilities.

Critical Foundation

The first step to maturity in continuous monitoring is to have a complete inventory of all systems and networks, as suggested in Controls 1 and 2, wrapped into an effective, formal, change management process. This represents a critical foundation for continuous monitoring and incident detection.

Size Matters

It is not surprising to find that enterprises with more than 10,000 employees are predominantly more mature (or at least claim to be) in their asset and vulnerability assessment processes. Nearly 31% of large organizations consider their process for identifying critical assets and vulnerabilities to be mature, compared to 16% and 18% for small and medium organizations, respectively. Table 3 correlates the answer to this question with the size of the reporting organization.

Table 3. CM Maturity and Size of the Organization

Definition	Small Organizations (Up to 1,000 employees)	Medium Organizations (1,001 to 10,000)	Large Organizations (More than 10,000)
Mature Processes	15.6%	17.8%	30.6%
Maturing (improving)	35.9%	42.2%	45.5%
Immature	39.8%	37.8%	21.5%
No Processes	7.0%	2.2%	1.7%
Unknown/Unsure	1.6%	0.0%	0.8%
Percentage of Total Respondents	33.3%	35.2%	31.5%

As organizational size diminishes, the scales tip toward an admittedly immature process, or in some instances, no processes at all. As larger organizations lead the way, simpler solutions and services need to shake out of the marketplace to aid smaller organizations.

Not Yet Continuous

Despite the fact that the majority of respondents rate their program as mature or maturing, their frequency of scans has not yet met this paper's definition of continuous vulnerability scanning (defined here as allowing only a 24-hour lapse between scans).

While CSC 4 recommends at least weekly scanning, only 38% of respondents are performing scans weekly (or more often.) Another 25% scan only monthly or bimonthly, while just under 5% scan once per year. Of this survey sample, 9% either are not aware that they scan (6.3%) or never do (3%). See Figure 4.

How often does your organization actively scan these assets for vulnerabilities?
Select the best choice.

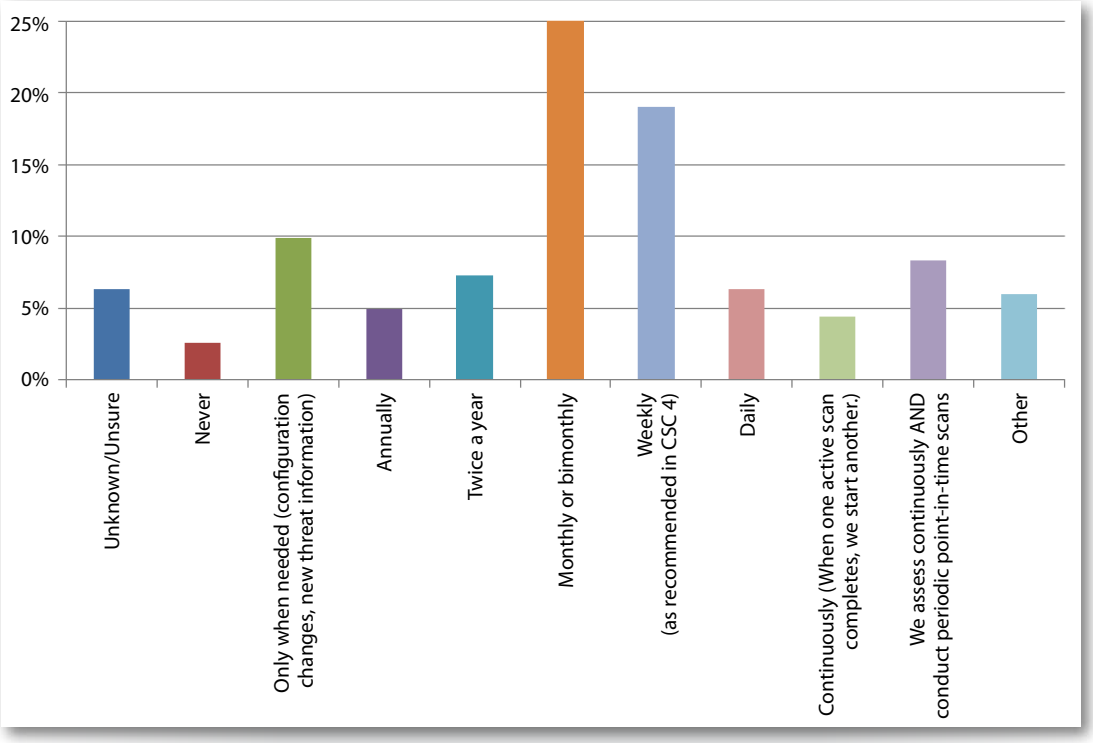

Figure 4. Scan Frequency

Scanning and Fixing Prioritized Vulnerabilities

Proper configuration is the first step to securing a system. Ongoing patch management is the next most effective step. Scanning and fixing prioritized vulnerabilities, however, should also be a top priority. Start today.

When you compare these answers to their perception of maturity, the target of daily scanning seems far too optimistic given that so few can even manage the weekly criterion espoused by CSC 4.

Related to the lack of remediation and follow up, 95% of respondents experienced one or more critical vulnerabilities in need of immediate patching over the past year. The largest group of respondents also needed an average of 1 to 3 days to identify critical vulnerabilities and 2 to 3 weeks to repair them, while just over 15% needed 1 to 2 months to make repairs, as illustrated in Figure 5.

What is the average time it takes to first identify and then repair critical vulnerabilities based on the past 12 months?

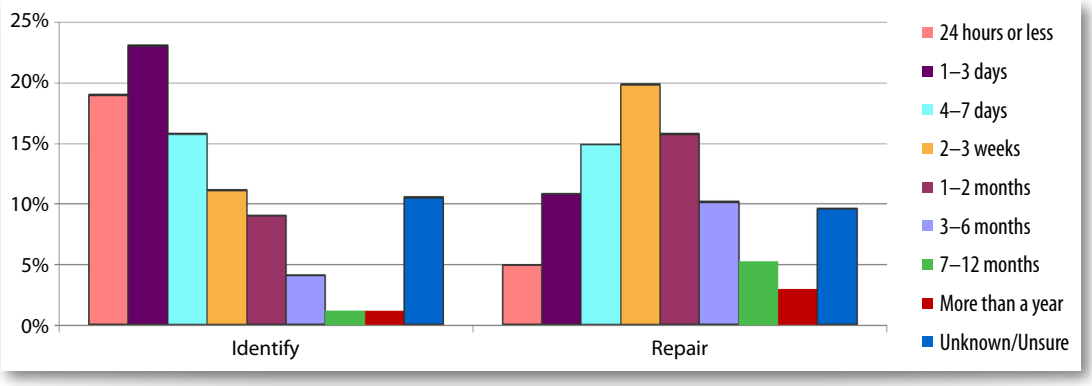

Figure 5. Time Needed to Identify and Repair Critical Vulnerabilities

The top three vulnerabilities discovered by respondents come as no surprise: information disclosure, privilege escalation and cross-site scripting. These issues, along with the others, have been on multiple Top 10 vulnerabilities lists for some years now. Figure 6 reveals some connections when you consider how one vulnerability leads to or blends with another.

Select the top three categories of vulnerabilities you discover most frequently during your scanning process. ***Please rank them as First (most encountered), Second and Third.***

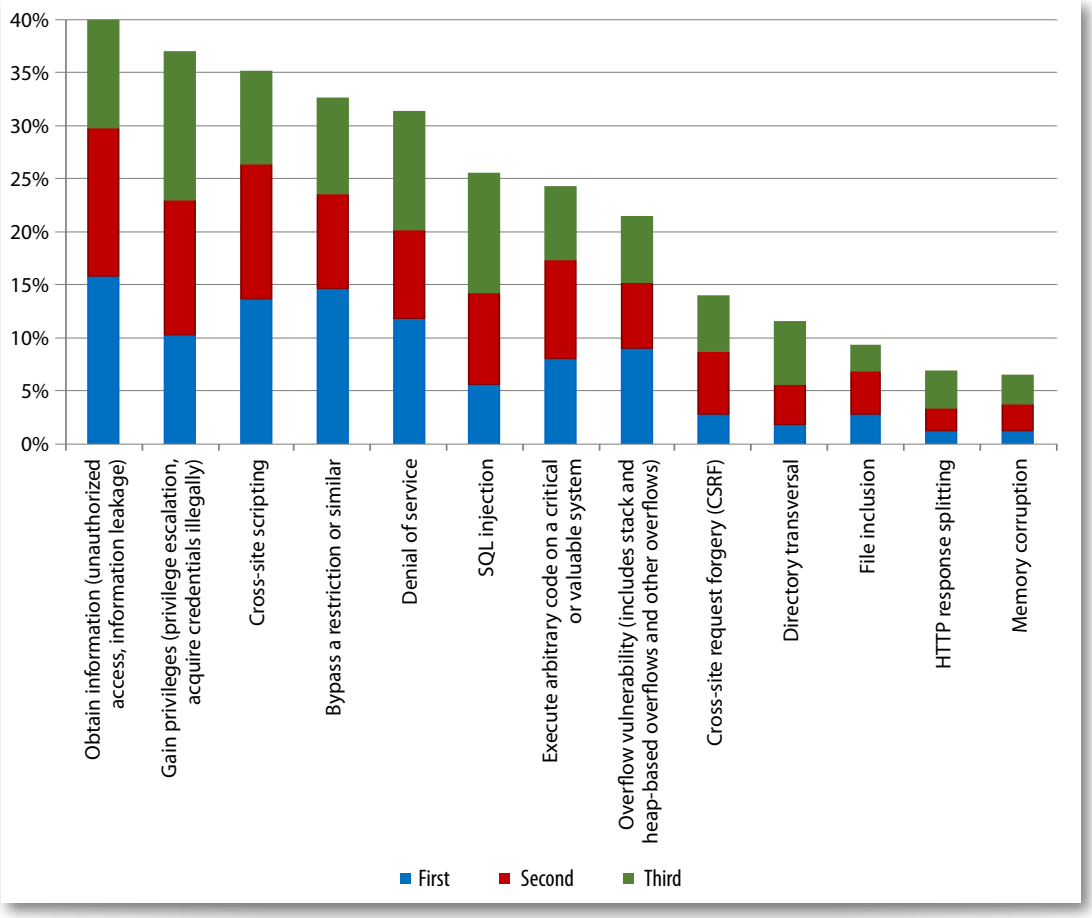

Figure 6. Aggregate Vulnerabilities by Frequency

Consider the fourth most common finding, discovered by 33% of respondents, a vulnerability that allows an attacker to bypass some restriction. No doubt in most cases this type of attack will lead to the attacker gaining access to data he or she should not be able to access, which was the most frequently discovered issue, chosen by 40% of respondents. It may even result in a form of privilege escalation (selected by 37%).

Measuring Maturity

Are you finding the same types of vulnerabilities noted in our survey? Can you identify activities and processes that limit such risks in your organization? If yes, that is a sign of maturity. If not, your organization may be immature and in need of training, tools and processes to strengthen continuous monitoring.

Because we are not trying to define nomenclature for vulnerabilities, we recognize that there may be some "wiggle room" in the vulnerability findings, because different respondents may classify the same type of issue in slightly different ways. Even so, let's consider how the respondents classified the severity of these issues for their respective organizations.

The second most common category of vulnerability found allows individuals to escalate privileges. The fourth allows for the bypass of some type of security control. Most organizations would consider these to be at the very least "medium" risks, if not high.

The sixth most common issue discovered, SQL injection, allows an unauthorized individual to leverage the vulnerability to extract, potentially, *all* of the data out of a database system (often without notice, particularly when you consider that 12% are not scanning their web servers as discussed previously). Considering the very serious impact that these discovered vulnerabilities could have on an organization, it is concerning that the overall coverage and scanning frequency numbers are not higher.

What does it mean that respondents are finding these vulnerabilities? It seems to indicate that our definition of *mature* is out of reach for many responding organizations. Could it be that respondents' own definitions of mature are based on the standards that currently available staffing can achieve? If so, that is a big mistake, especially because 57% of respondents identified lack of human resources as the top impediment to implementing comprehensive continuous monitoring programs, followed by lack of budget and management support, as shown in Figure 7.

What Is *Mature*?

Security program maturity is more than doing the best we can with the personnel and training available. It requires having a systematically implemented continuous monitoring program that covers, at the very least, 100% of assets that are directly connected to the organization's network.

What impediments have you encountered so far in implementing continuous monitoring processes? *Select all that apply.*

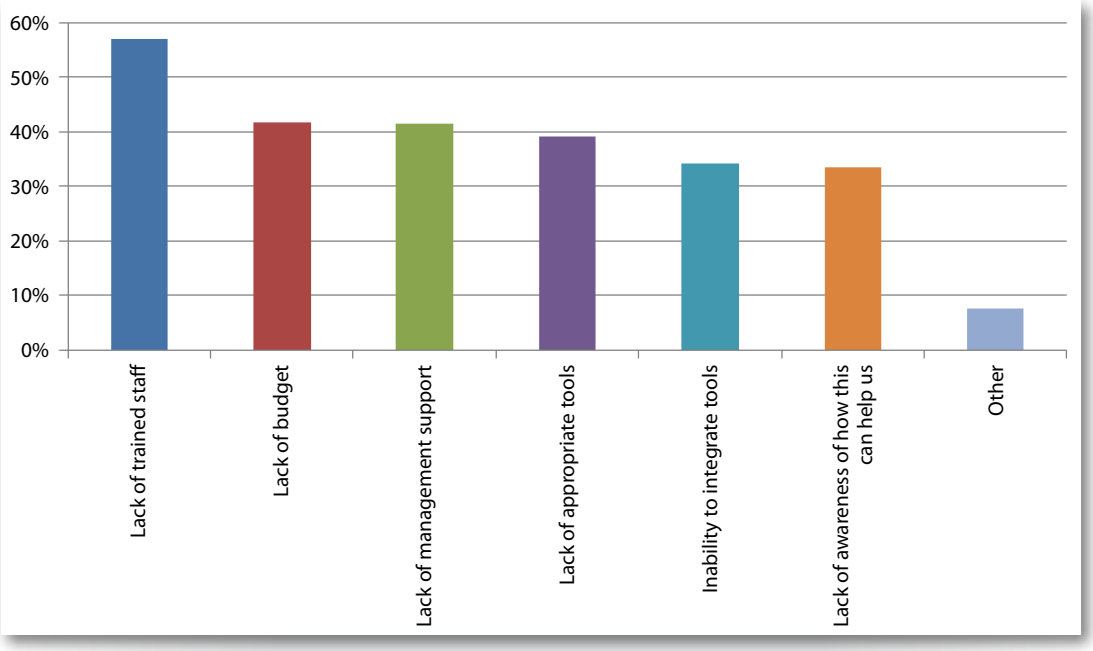

Figure 7. Impediments to Continuous Monitoring

From the survey, it's clear that organizations—even those that consider themselves mature—need more buy-in from management to support their program needs for budget and staff.

Consider the following suggestions on how to communicate these needs more effectively to management.

- **Learn the state of affairs.** Learning the differences between how technical, security and management individuals communicate is critical to effectively managing any security program. It becomes even more important when we're talking about communicating something that could be game-changing for security, such as continuous monitoring.
- **Communicate with management.** This requires that we grapple with the fact that management doesn't (generally) use the terms *exposure* and *risk* in the same way that security people do. Exposure tends to be a financial term. Risk tends to be an operations term.
- **Translate.** By recognizing the differences in perspective, we can translate our comments into language and reasoning that management will understand. For example, rather than speaking about risk as a nebulous information security issue, think about how management measures the performance of the organization. (See "Measure and Correlate.")
- **Do a cost analysis.** Take the time to turn the risks you perceive into a cost–benefit analysis that focuses on operational goals and key performance indicators (KPIs) for your enterprise. The analysis will be invaluable when it comes to effectively communicating risk and receiving funding and other resources for security initiatives.[7]
- **Continually improve.** Never let the search for perfection stand in the way of taking steps to be "good." Get started; then plan on continually developing your organization's remediation process and describing that ongoing process for your security and operations teams. In reality, this is where the majority of the resources will go, so management needs to know what you are doing.
- **Remain operationally sound.** Effective remediation programs are operationally sound. Not only can they lead to fewer and shorter unplanned outages (good for operations) but they also close the holes, preventing data loss or destruction (very good for operations). Keep management informed of your performance statistics and tell them how your actions benefit operations.

Typically, KPIs within an enterprise are tied to financial return and achievement of organizational objectives. Security professionals might naturally make the connection between a SQL injection flaw and a risk to operations. Management is typically operationally aligned with tasks, processes and programs that directly relate to and help the organization achieve its mission. Security typically acts as a safeguard for the mission, and management should consider it an embedded cost for enabling business objectives.

[7] The SANS AUD507 course spends a great deal of time developing and explaining strategies to accomplish this. www.sans.org/brochure/course/auditing-networks-perimeters-systems/1772loads/92069

To detect vulnerabilities during their scans, security teams typically monitor for vulnerability status, anomalies and alerts, potential misuse and unauthorized changes, and network behaviors indicative of a problem. On the other hand, operations teams that are not focused on security are primarily monitoring for patch status, asset identification and configuration changes, as shown in Figure 8.

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

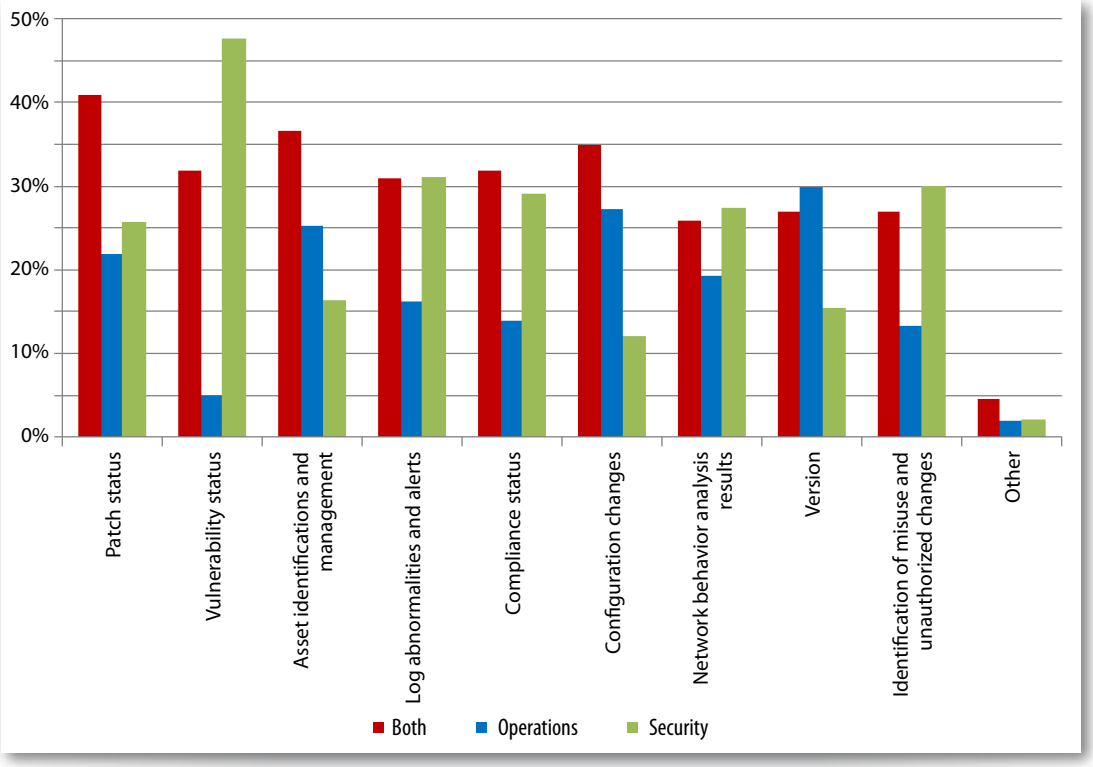

Figure 8. Monitoring Metrics

When viewed through the lens of a security engineer, analyst or manager, vulnerability assessment is a vital link in the overall chain of processes that together provides information security assurance.

Supporting the Mission

Imagine that an organization's mission is the rapid production of printed material from a series of high-speed offset presses. Operations focuses entirely on managing print jobs, maintaining appropriate inventory levels of ink and paper and performing regular preventive maintenance on the presses and the supporting equipment.

Even so, performing regular inspections of portions of the press that are not due for maintenance (very much akin to performing continuous vulnerability scans) allows the operations team to identify—*before* service is interrupted—potential issues that could directly and severely affect operations.

Vulnerability scanning reports provide the same contextual information with the same imperative (checking for vulnerabilities even when you don't think you need to) to protect daily business operations.

Bedrock Policies

Policies lie at the bedrock of these processes, establishing management's codified approach toward managing operational risk and achieving objectives. Based on those policies, organizations can create standard operating procedures and organizational security standards, further building a governance and reporting structure. Security processes, such as change control, patch management and other activities, can then emerge and be measured to evaluate program effectiveness.

Switching to the lens of operations, vulnerability scanning reports have additional value. Those in operations roles are typically laser-focused on everything necessary to meet business objectives, and continuous scanning reports can help safeguard the processes supporting those objectives.

Nomenclatures

Over the years a number of different attempts have been made to classify, adopt a nomenclature and score vulnerabilities because the various security product vendors tend to use different names for the same issues. To normalize and consume this data, 77% map to the Common Vulnerabilities and Exposures (CVE), eclipsing other common scoring nomenclatures by a wide margin. See Figure 9.

Do you map your vulnerabilities and issues to one or more of the following vulnerability, configuration and platform classification schemes and languages? ***Select all that apply.***

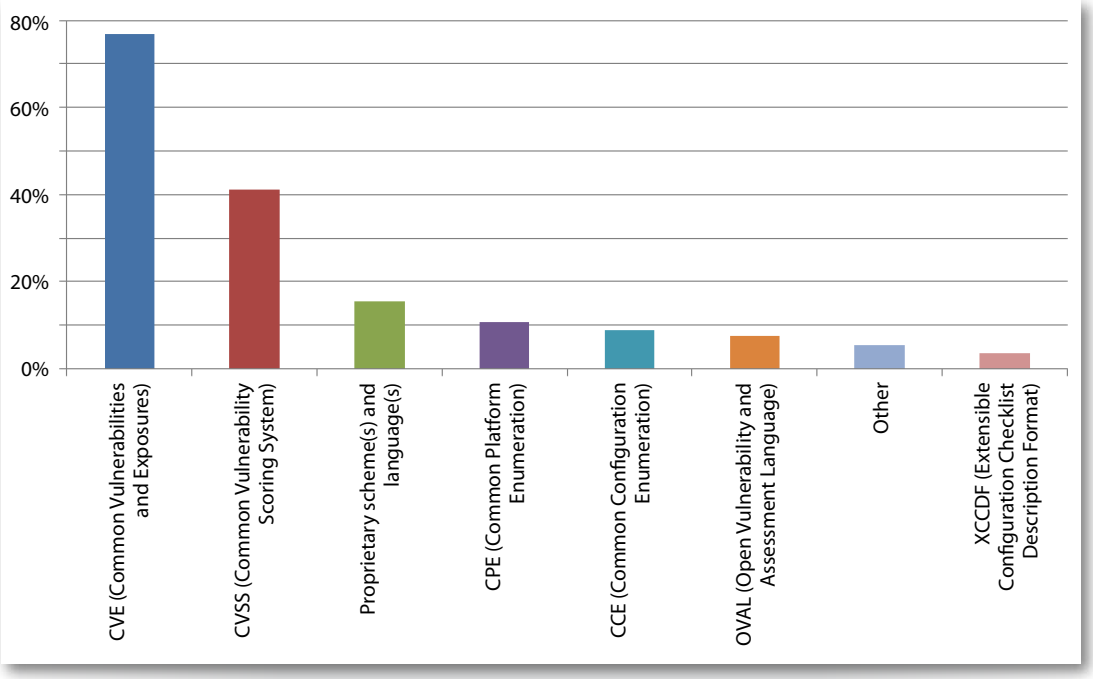

Figure 9. Vulnerability Nomenclatures

An interesting development somewhat new to the industry is the importance of Security Content Automation Protocol (SCAP) validation of tools that are used. In another question, 58% of respondents (the majority) are either using SCAP-validated tools or have a subset of tools that are SCAP-validated.

SCAP is backed by NIST and the CSCs. With more than 50% of respondents using SCAP-validated tools, the protocol may become important. If your organization is looking at procuring security products for continuous monitoring today or negotiating the renewal of a license on an existing product, it would make sense to consider using SCAP-validated tools.

Mostly Active

The survey also shows that active vulnerability scanning remains the most common, with 81% of respondents indicating that active scanning is in use. Passive scanning and scanning agents are both used by 49% of respondents. See Figure 10.

What type of scanning do you do to locate vulnerabilities?
Select all that apply.

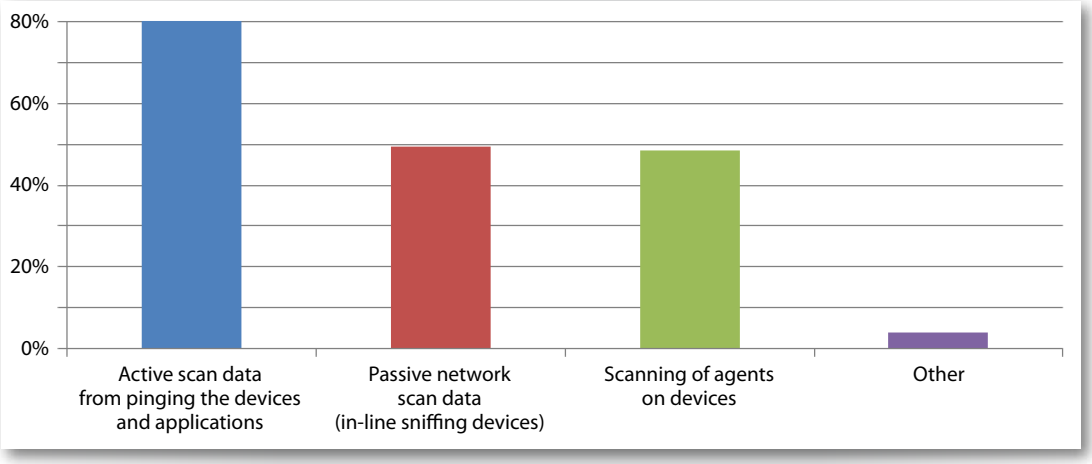

Figure 10. Types of Scanning Used

Actively scanning is one way to be sure of what you have operating on the network and what the related vulnerabilities are. It doesn't, however, work particularly well on IPv6 networks, which are so large that it isn't feasible to scan IP ranges. Even with IPv6, however, active scanning plays an important role. Coupling IPv6 discovery tools with active scanning can provide a practical way to identify and scan directly connected assets.

Passive scanning does provide some useful advantages. It is nearly impossible for passive scanning to knock a system offline during its operation. Passive scanning can also identify and respond to unexpected conditions or changes in the environment that need to be addressed. But a passive scanner will identify an issue *only* if it actually observes a connection to the potentially vulnerable service. If that first connection is an attack, it might be too late.

Although organizations should address all vulnerabilities discovered, prioritizing the issues based on the operational alignment of the systems and the impact of compromise is the proper way to use your available resources to remediate the most important risks to your business.

A smart businessperson will consider the foregoing and wonder, "But why are these things true?" If we can nail down the root cause of these issues, we may be able to fix them in a systemic way rather than trying to treat only the symptoms. The root causes boil down to just a few things:

- As an industry, we are failing to communicate our needs in an operationally aligned context.
- As a result, budgetary resources are not available.
- Adequate staff training is not provided, because of inadequate budgets.

Staffing and Resources

How do we deduce the causes noted above from the survey at large? Consider, first, that the practitioners—the largest category of respondents—indicate that staff training is, by far, the biggest obstacle to improvement in the organization. Overall, 57% of respondents cite lack of trained staff as their biggest impediment to implementing successful programs, as illustrated in Figure 7 (on page 12).

There are, however, other options for dealing with lower levels of staffing. Although 59% of respondents use in-house personnel and either proprietary or off-the-shelf tools for vulnerability assessment and remediation, 36% use a combination of in-house and managed services. An additional 4% rely exclusively on managed services.

For organizations—particularly smaller, less mature organizations—struggling to find adequate or appropriately trained personnel, investing in outsourced, managed services offers an alternative that may be more attractive to management.

Other key impediments include lack of budget and lack of management support, chosen by 42% and 41% of respondents, respectively. To be fair, a chief operating officer (COO) would not normally be intimately familiar with the daily operations of the security team. However, the numbers here seem to indicate that the COO is not aware that he or she *should* care whether or not all systems are secured and should understand that there is *serious operational risk* in failing to effectively remediate. As technical people, it would be very easy to point our fingers at management and say, "They don't understand," but we must change our thinking and help them understand.

Show Results

One way to gain more resources is to show results. In the survey, respondents say they were able to improve their security posture on several levels as a result of their continuous monitoring programs, as shown in Figure 11.

Where has adoption of continuous vulnerability monitoring improved your organization's overall posture? ***Select only those that apply.***

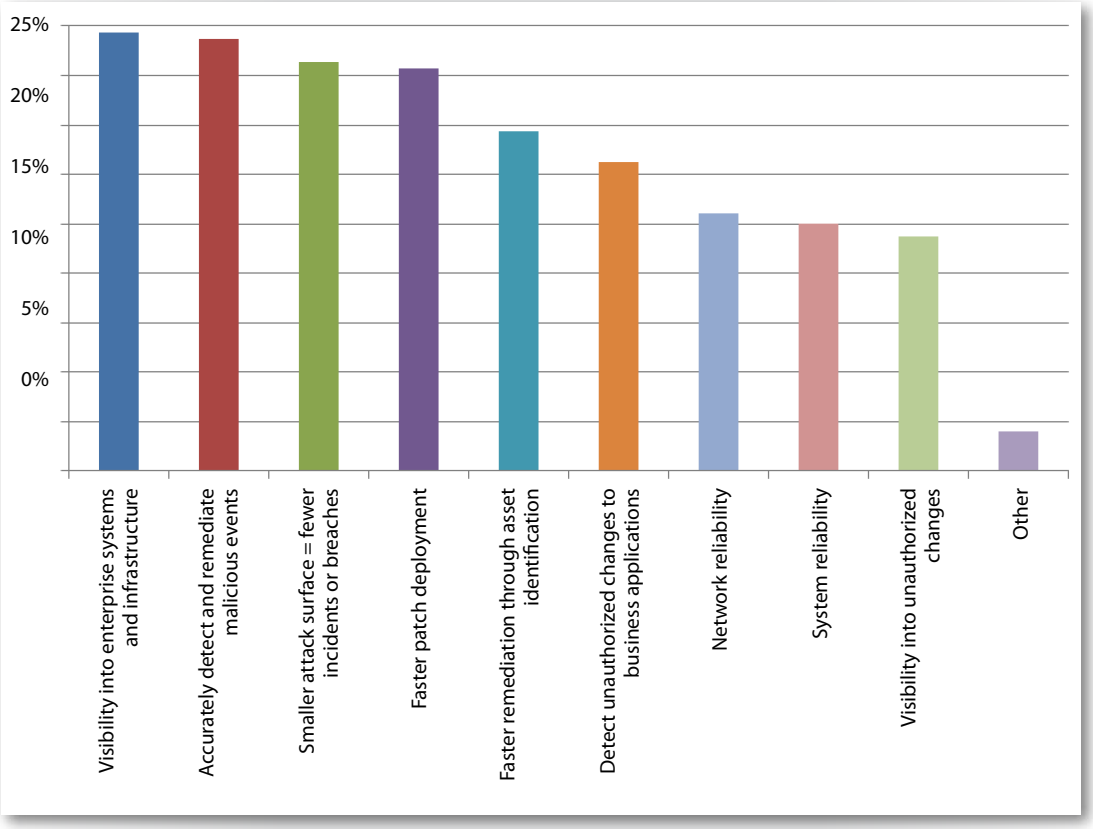

Figure 11. Improvements Related to Continuous Monitoring

For example, 44% improved their visibility into systems and their accuracy in detecting and remediating events. Just over 40% reduced the available attack surface and sped up patch deployment. Sharing these types of improvements, when validated, can go a long way toward showing management the value of such programs. In turn, these programs are likely to get more resources and staffing as the improvements are communicated to management.

Measure and Correlate

Approach your security program and run it as though you are running a business rather than simply providing an internal service. Security is now a fundamental business process that should be baked into the core of how every organization operates.

Evaluate your own program realistically. Based on an analysis of survey responses, what many consider to be "mature," others would describe as barely getting started. When you institute changes in your own operations and security programs, make sure to include measurement criteria. Frankly, if you can't measure the results, the value of your actions may be questioned. Approach your security program and run it as though you are running a business rather than simply providing an internal service. Security is now a fundamental business process that should be baked into the core of how every organization operates. It cannot be glued on as an afterthought. This "requirement" highlights the need for true continuous monitoring. Organizations cannot operate with blind spots; they need to know their assets are patched, their processes are sound and their security investments are properly configured.

Think, too, about whether your organization handles customer information with due care. Set targets for improvement over the next six months, one year, three years and five years. Analyze where your organization can achieve the biggest wins.

For example, consider correlating log data to vulnerability data. In this survey, 25% of respondents have no plans to correlate and evaluate log data with vulnerability analysis. Yet log data correlation greatly speeds repair—something that took 20% of respondents 2–3 weeks and another 16% 1–2 months to make repairs, as illustrated previously in Figure 5 (on page 9).

How critical would the correlation of event log data measured against vulnerabilities be for identifying attacks against known vulnerable systems? How critical would it be for your organization to know how safe systems are by reviewing the activity logs involving these affected services before a vulnerability is discovered?

Automate Workflow

Discovery and repair should work in tandem with defined workflows to ensure repairs are made and gold standards maintained across critical systems. Indeed this level of functionality is at the top of the wish lists for 62% of respondents, as shown in Figure 12.

What is on your wish list for the next two years?
Select all that apply.

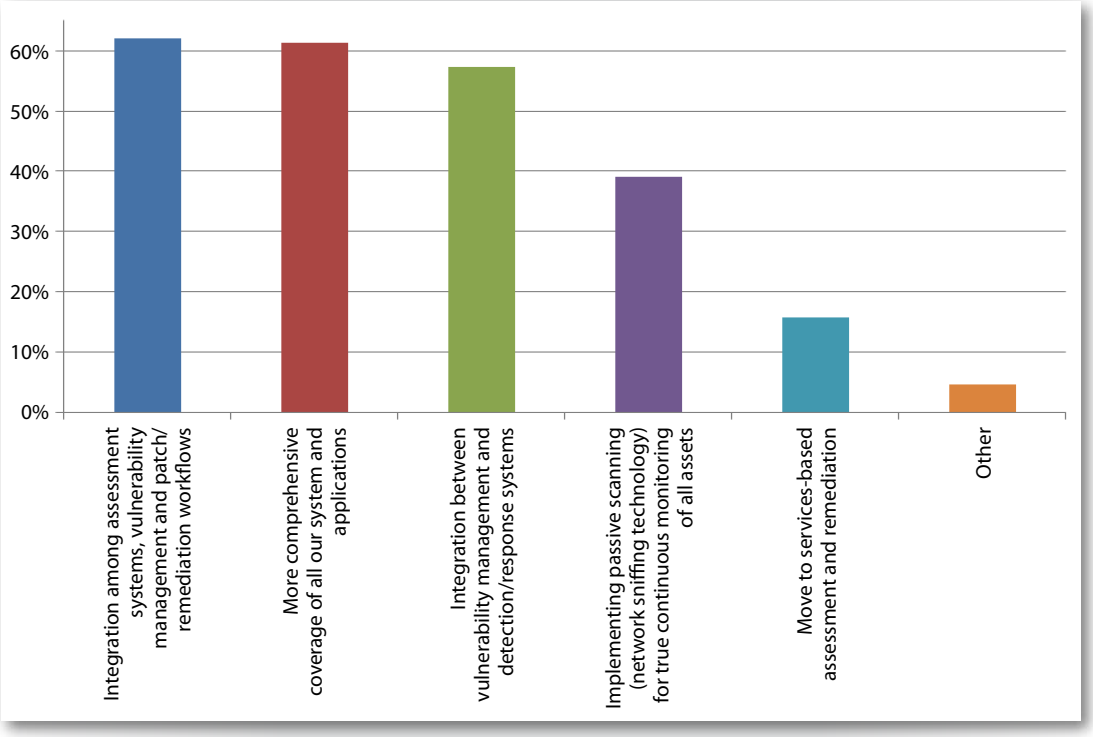

Figure 12. On Their Wish Lists: More Integration and Coverage

As you can see, respondents' wish lists more accurately reflect the reality of this survey: Respondents think they're mature or maturing, but they need better workflow management and more comprehensive coverage to assess all their systems. They also want more integration to incident response, as discussed earlier.

Conclusion and Recommendations

This survey produced contradictory results, particularly because of the lack of maturity in what some might call "mature" programs. Most respondents indicated that the majority of their vulnerability findings are critical. Responses indicate that at least one in four of these are operationally important for the business. We *must* do a better job of documenting, demonstrating and communicating these risks to the organization in a way that allows for either conscious acceptance of the risk or dedication of resources to solve the problems.

Knowing what you have (CSCs 1 and 2) is a fundamental requirement for securing an enterprise. The majority of participants indicate that achieving compliance (regulatory or otherwise) and reduction of attack surface are primary motivators for the overall security program. Bearing this in mind, how can we achieve these goals if we don't even know what we have? We must strive to inventory 100% of our networks and systems.

About the Author

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.

Sponsors

SANS would like to thank this survey's sponsors:

ALIEN VAULT

ARBOR NETWORKS

hp

tenable network security

Last Updated: January 20th, 2017

Upcoming SANS Training

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

Cyber Threat Intelligence Summit & Training	**Arlington, VAUS**	**Jan 25, 2017 - Feb 01, 2017**	**Live Event**
SANS Dubai 2017	**Dubai, AE**	**Jan 28, 2017 - Feb 02, 2017**	**Live Event**
SANS Southern California - Anaheim 2017	**Anaheim, CAUS**	**Feb 06, 2017 - Feb 11, 2017**	**Live Event**
SANS Oslo 2017	**Oslo, NO**	**Feb 06, 2017 - Feb 11, 2017**	**Live Event**
RSA Conference 2017	**San Francisco, CAUS**	**Feb 12, 2017 - Feb 16, 2017**	**Live Event**
SANS Munich Winter 2017	**Munich, DE**	**Feb 13, 2017 - Feb 18, 2017**	**Live Event**
SANS Secure Japan 2017	**Tokyo, JP**	**Feb 13, 2017 - Feb 25, 2017**	**Live Event**
HIMSS 2017	**Orlando, FLUS**	**Feb 19, 2017 - Feb 19, 2017**	**Live Event**
SANS Secure India 2017	**Bangalore, IN**	**Feb 20, 2017 - Mar 14, 2017**	**Live Event**
SANS Scottsdale 2017	**Scottsdale, AZUS**	**Feb 20, 2017 - Feb 25, 2017**	**Live Event**
SANS Dallas 2017	**Dallas, TXUS**	**Feb 27, 2017 - Mar 04, 2017**	**Live Event**
SANS San Jose 2017	**San Jose, CAUS**	**Mar 06, 2017 - Mar 11, 2017**	**Live Event**
SANS Secure Canberra 2017	**Canberra, AU**	**Mar 13, 2017 - Mar 25, 2017**	**Live Event**
SANS Secure Singapore 2017	**Singapore, SG**	**Mar 13, 2017 - Mar 25, 2017**	**Live Event**
SANS London March 2017	**London, GB**	**Mar 13, 2017 - Mar 18, 2017**	**Live Event**
ICS Security Summit & Training - Orlando	**Orlando, FLUS**	**Mar 20, 2017 - Mar 27, 2017**	**Live Event**
SANS Tysons Corner Spring 2017	**McLean, VAUS**	**Mar 20, 2017 - Mar 25, 2017**	**Live Event**
SANS Abu Dhabi 2017	**Abu Dhabi, AE**	**Mar 25, 2017 - Mar 30, 2017**	**Live Event**
SANS Pen Test Austin 2017	**Austin, TXUS**	**Mar 27, 2017 - Apr 01, 2017**	**Live Event**
SANS 2017	**Orlando, FLUS**	**Apr 07, 2017 - Apr 14, 2017**	**Live Event**
Threat Hunting and IR Summit	**New Orleans, LAUS**	**Apr 18, 2017 - Apr 25, 2017**	**Live Event**
SANS Las Vegas 2017	**OnlineNVUS**	**Jan 23, 2017 - Jan 30, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**