SANS

Analyst Program

Survey

A SANS 2021 Survey: Vulnerability Management—Impacts on Cloud and the Remote Workforce

Written by **David Hazar**

November 2021

ARCTIC WOLF AUTOMOX BlackBerry Intelligent Security. Everywhere. cisco Cisco Umbrella
ExtraHop Gigamon® RAPID7 VULCAN.

©2021 SANS™ Institute

https://t.me/learningnets

Executive Summary

Vulnerability management (VM) continues to be a struggle for many organizations. As we observed last year, companies have been tracking vulnerabilities in their systems and third-party software since the late 1990s and shortly after had the ability to automatically identify vulnerabilities in their systems, software, and even custom-developed applications.[1]

However, even though many organizations have well-defined vulnerability management programs, there are certain aspects of these programs that continue to vex survey respondents and prevent their organizations from maturing.

Identifying most vulnerabilities is typically not very hard, but fixing vulnerabilities is difficult for a variety of reasons. Respondents listed these, among others:

- We don't budget for it—and we don't have extra time or resources.
- Operational teams are already overworked.
- It never ends. Even if we remediate everything, new vulnerabilities are constantly being discovered, and reports come in at different times and in different formats, depending on the tools or teams being leveraged for identification.
- It's a business expectation, but not always a business requirement; therefore, the effort is not always recognized and rewarded.
- Security is accountable—but not responsible—for much of the work.

To succeed with vulnerability management, it takes a coordinated effort among security, IT (both systems and software development), and the business operations groups. Organizations must also identify, acknowledge, and track the roadblocks and technical debt within the organization. Many times there are significant barriers that prevent timely remediation of vulnerabilities. It is not uncommon to analyze vulnerability backlogs and determine that well over 50% of the outstanding vulnerabilities cannot be remediated following normal treatment processes or with the operational budgets and resources currently allocated.

In this year's survey, we looked at some of the same measures we looked at in the previous two surveys. However, we also wanted to get more information on the responding organizations' maturity across the different phases of the VM life-cycle. To accomplish this, we asked respondents to rate themselves against the SANS Vulnerability Management Maturity Model, which addresses the following life-cycle phases and functions:

- Prepare
  - Policy and standards
  - Context
- Identify
  - Automated identification
  - Manual identification
  - External identification (security researchers and crowdsourced identification)

[1] "SANS Vulnerability Management Survey 2020," www.sans.org/white-papers/39930/ [Registration required.]

https://t.me/learningnets

- Analyze
  - Prioritization
  - Root cause analysis
- Communicate
  - Metrics and reporting
  - Alerting
- Treat
  - Change management
  - Patch management
  - Configuration management

We developed and released the SANS Vulnerability Management Maturity Model in late 2019 after many students of the class that SANS Certified Instructor Jonathan Risto and the writer of this paper co-authored asked what framework or standard they could use to measure their own maturity. Since then, we have also had many students of MGT516: Managing Security Vulnerabilities: Enterprise & Cloud ask for information about how they are doing compared with the industry or compared to their peers. So, we added the maturity model to the survey this year. We wanted to begin tracking this data so that it is available for organizations to provide that point of comparison.

Some of the key findings and takeaways from the survey include:

- The percentage of companies with a formal program continues to increase from 63% in 2020 to 75% in 2021 with the remaining participants either having an informal program or planning on creating a formal program in the next 12 months.
- An increase in cloud, container, and custom software development or application VM requirements and capabilities over levels reported in 2019[2] and 2020,[3] accompanied by maturity across almost all life-cycle phases being comparatively lower for these asset types.
- In terms of roles and responsibilities, the data shows that IT is taking a larger role in running the overall VM program than in the past, but this difference could also be due to the demographics of this year's survey.
- More than half the respondents (68%) are at least at a defined level of maturity for their prioritization or risk ranking processes and procedures.
- Many organizations have a continued lack of confidence in the maturity of their configuration management capabilities, especially for container and cloud assets.

Because we conducted similar vulnerability management surveys in 2019 and 2020,[4] we also analyzed some of the changes to determine what progress has been made and identify some of the year-over-year differences.

---

[2] "SANS Vulnerability Management Survey," April 2019, www.sans.org/white-papers/38900

[3] "SANS Vulnerability Management Survey," November 2020, www.sans.org/white-papers/39930

[4] "SANS Vulnerability Management Survey," April 2019, www.sans.org/white-papers/38900 and "SANS Vulnerability Management Survey," November 2020, www.sans.org/white-papers/39930

https://t.me/learningnets

Survey Demographics

As with the past couple of years, the majority of respondents came from organizations headquartered in North America, followed by Europe and Asia. Although 81% of respondents have operations in the United States, survey results still show a global presence—almost one-third of the respondents' organizations have operations in Canada, Europe, and Asia, and close to a quarter maintain operations in Australia/New Zealand and Latin/South America. The industries shifted a little bit from previous years, with government and technology organizations edging out respondents from financial services for the top spots followed by cybersecurity, education, healthcare, manufacturing, and retail. Small and midsize businesses had greater participation than in previous years, but companies with more than 10,000 employees accounted for 31% of the participants. Despite more participation from companies with a smaller size in terms of people, 53% of companies had a revenue of over $250 million.

Figure 1 provides a snapshot of the demographics for the respondents to the 2021 survey.

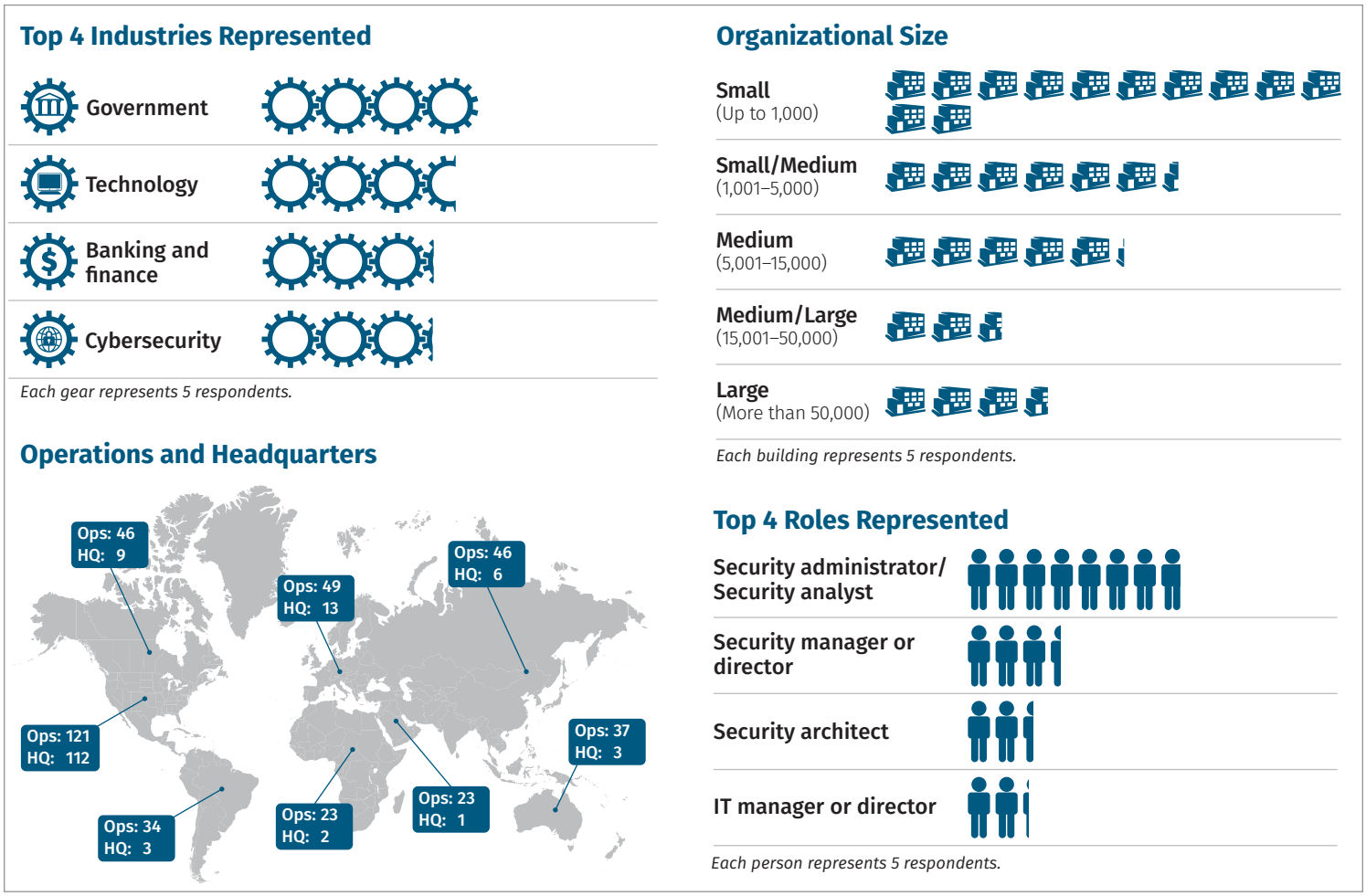

Figure 1. Key Demographic Information

https://t.me/learningnets

Setting the Stage

It was great to learn that the percentage of organizations with formal programs managed either internally (63%) or through a third party (11%) is up more than 11 percentage points from last year and almost 20 points from 2019. The majority of those that do not have a formal program are still informally managing their vulnerabilities (18%) in some fashion, while the remainder have plans to formalize a program in the next 12 months (7%). This is the first year that no respondents indicated they did not have any program and did not plan to have one. See Figure 2.

These results indicate that more than 92% of organizations have at least some processes in place to identify or manage their vulnerabilities. As expected, the larger the organization, the more likely it is to have a formal program (see Table 1). The industries most likely to have a formal program are financial services and government.

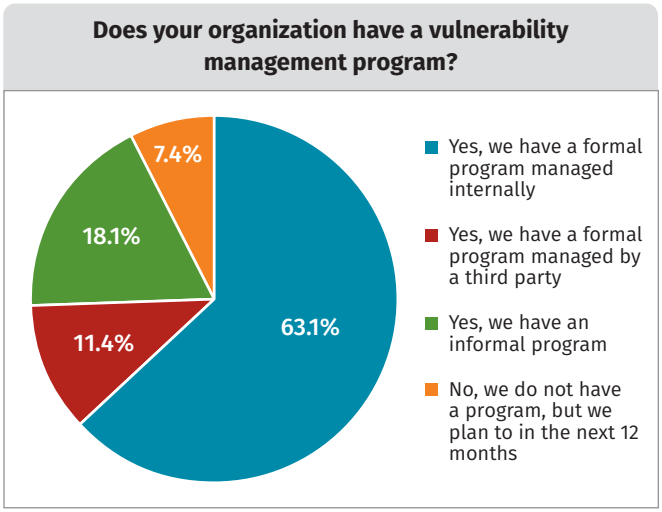

Figure 2. Formal vs. Informal Programs

Table 1. Formal Versus Informal Programs by Organization Size

Does your organization have a vulnerability management program?	Organization Size										
	Total	Fewer than 100	101–500	501–1,000	1,001–2,000	2,001–5,000	5,001–10,000	10,001–15,000	15,001–50,000	50,001–100,000	More than 100,000
Total Count	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Yes, we have a formal program managed internally.	62.3%	69.2%	52.0%	60.9%	57.9%	46.2%	72.7%	60.0%	78.6%	60.0%	76.9%
Yes, we have a formal program managed by a third party.	11.3%	0.0%	32.0%	8.7%	10.5%	0.0%	9.1%	13.3%	14.3%	0.0%	0.0%
Yes, we have an informal program.	17.9%	7.7%	12.0%	21.7%	21.1%	38.5%	18.2%	20.0%	0.0%	20.0%	23.1%
No, we do not have a program, but we plan to in the next 12 months.	7.3%	23.1%	4.0%	4.3%	10.5%	15.4%	0.0%	6.7%	0.0%	20.0%	0.0%
No, we do not have a program and don't plan to.	1.3%	0.0%	0.0%	4.3%	0.0%	0.0%	0.0%	0.0%	7.1%	0.0%	0.0%

Respondents also indicated the specific types of assets and functions that they included or planned to include in their vulnerability management program. Not surprisingly, infrastructure is still the main focus, with on-premises infrastructure being included by the most organizations (95%) and various cloud services making a strong showing. See Figure 3 on the next page.

https://t.me/learningnets

Reviewing the 2021 results against those from 2020, we saw big increases to the assets that were existing or planned to be part of the VM program in almost every category, with the exception of traditional on-premises infrastructure, which had only a small increase. This could be attributed to the fact that the participation was already high, but it also may align with a shift away from traditional operating models.

Responsibility for Vulnerability Management Programs

Information security is still the most common group assigned responsibility for overall organizational vulnerability management (63%), but IT was responsible for VM in a greater number of organizations this year. Respondents continue to indicate that a lot of responsibility is placed on IT organizations for remediation activities such as patch (63%) and configuration management (65%), as illustrated in Table 2. Manufacturing and retail were the industries most likely to respond that overall vulnerability management was an IT responsibility. Audit, risk, and compliance are still more heavily involved in application vulnerability management than other asset types. They are most involved in vulnerability analysis and reporting, which may be due to their primary focus being on the business and its associated risks.

Which are included as part of your existing or planned vulnerability management program? *Select all that apply.*

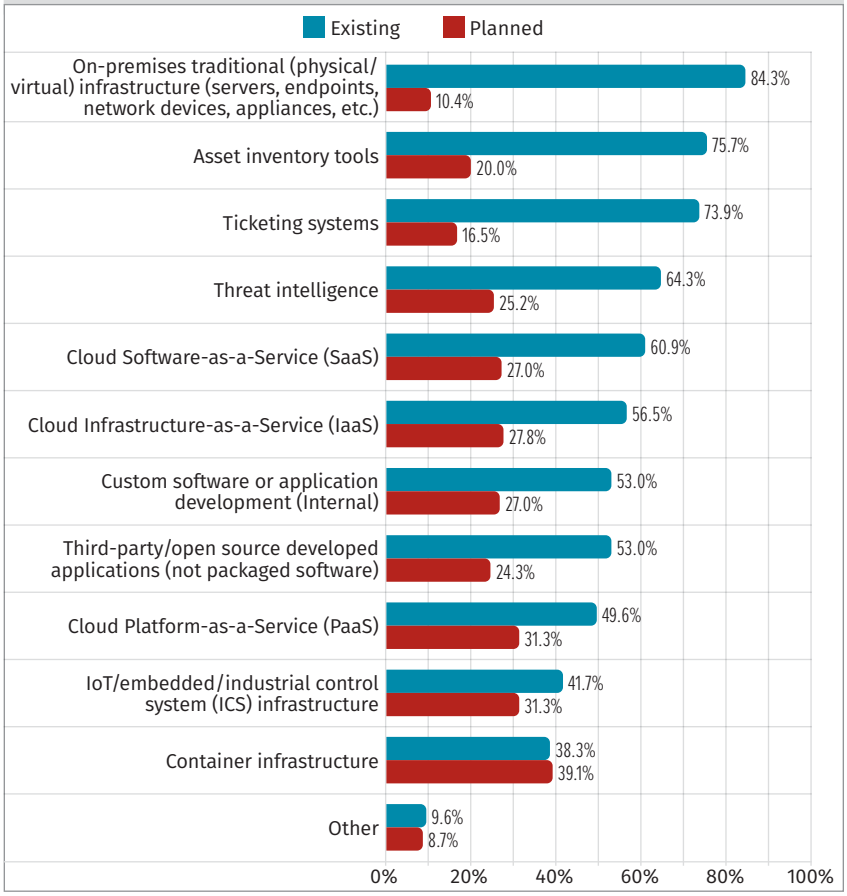

Figure 3. Vulnerability Management Program Assets

Table 2. Primary Responsibility

	Information Security	Information Technology	Application Development	Audit/Risk	Compliance	Third Party	Other
Overall vulnerability management in your organization	63.4%	23.2%	2.7%	4.5%	1.8%	0.9%	2.7%
Vulnerability reporting	60.7%	11.6%	4.5%	8.0%	2.7%	1.8%	4.5%
Vulnerability analysis	59.8%	13.4%	7.1%	4.5%	3.6%	3.6%	2.7%
Traditional (physical/virtual) infrastructure vulnerability discovery	50.0%	31.3%	3.6%	3.6%	2.7%	0.9%	4.5%
Cloud vulnerability discovery	47.3%	13.4%	6.3%	3.6%	3.6%	4.5%	3.6%
Third-party/open source application vulnerability discovery	47.3%	11.6%	8.9%	7.1%	2.7%	5.4%	2.7%
Custom-developed application vulnerability discovery	43.8%	18.8%	14.3%	5.4%	0.9%	0.9%	0.9%
Container infrastructure vulnerability discovery	40.2%	17.0%	6.3%	6.3%	3.6%	0.9%	1.8%
IoT/embedded/ICS vulnerability discovery	34.8%	13.4%	8.0%	5.4%	0.9%	4.5%	2.7%
Patch management	16.1%	63.4%	6.3%	1.8%	3.6%	3.6%	1.8%
Configuration management	12.5%	65.2%	5.4%	5.4%	3.6%	2.7%	1.8%

https://t.me/learningnets

Automated vulnerability discovery increased by 10 percentage points to 81% of respondents, but that does not ensure that all assets in a given category are subject to automated scanning. Traditional, on-premises infrastructure continues to lead other asset types in being automatically assessed for vulnerabilities at 74%, with all others selected by fewer than 35% of respondents. We continue to see the least amount of automated discovery happening for applications and IoT/embedded systems. See Figure 4.

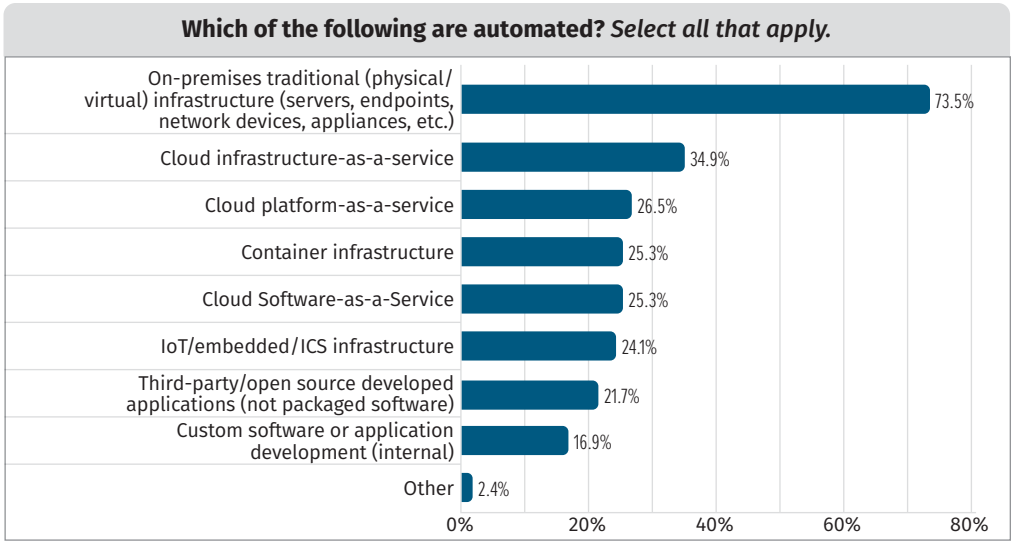

Figure 4. Automated Discovery by Asset Type

The numbers for IoT/embedded/ICS systems might be due to the fact that many organizations are using their traditional infrastructure scanning technologies in this space. Although the lower percentages for some of these asset types are somewhat surprising, it is important to recognize that organizations could still be using manual forms of identification and relying on patch and configuration management tools to notify them of outdated software or insecure configurations.

Although a smaller number of respondents are managing business partner vulnerabilities compared with the 2019 survey, how these business partners are assessed has not changed drastically. It does, however, seem that more businesses are comfortable asking for access to scan for vulnerabilities in their partners' environments. See Figure 5.

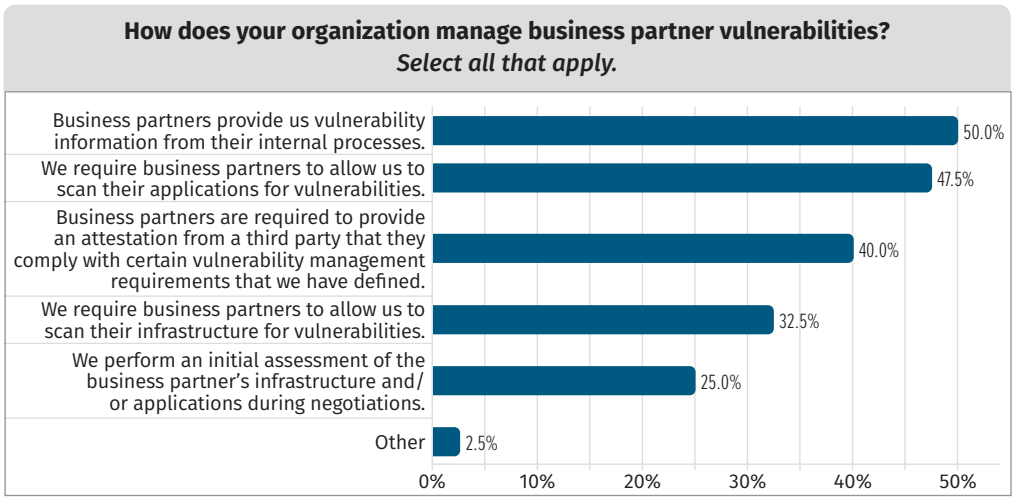

Figure 5. Partner Management

https://t.me/learningnets

VM Maturity

This is the first year we have asked respondents to rate their maturity based on the SANS VM Maturity Model. It will be interesting to see how maturity changes and the different trends in future surveys.

Prepare

Preparation is an important part of any program and it is not a one-time activity. Many organizations have moved to more iterative styles of systems and software development, and it is helpful to follow a similar iterative approach to program development. Organizations cannot excel at everything right away. If they are focusing on more than a few items in each cycle, they will almost certainly struggle to maintain focus and make significant gains.

Policies and Standards

The maturity of respondents' policies and standards is almost a perfect bell curve with most organizations at a defined level of maturity. See Figure 6.

This means that a good number of organizations have started to mature past defined policies and standards to measuring compliance and, in some cases, leveraging automation to make compliance with policies and standards easier for the business. Having defined policies and standards is essential to measuring our progress and effectiveness, and setting clear expectations for auditors and other interested third parties. If an organization can improve reporting and automate compliance for some or many of the standards it has defined, it will reduce the burden for program participants and allow them to focus on aspects of the program that are more difficult to automate.

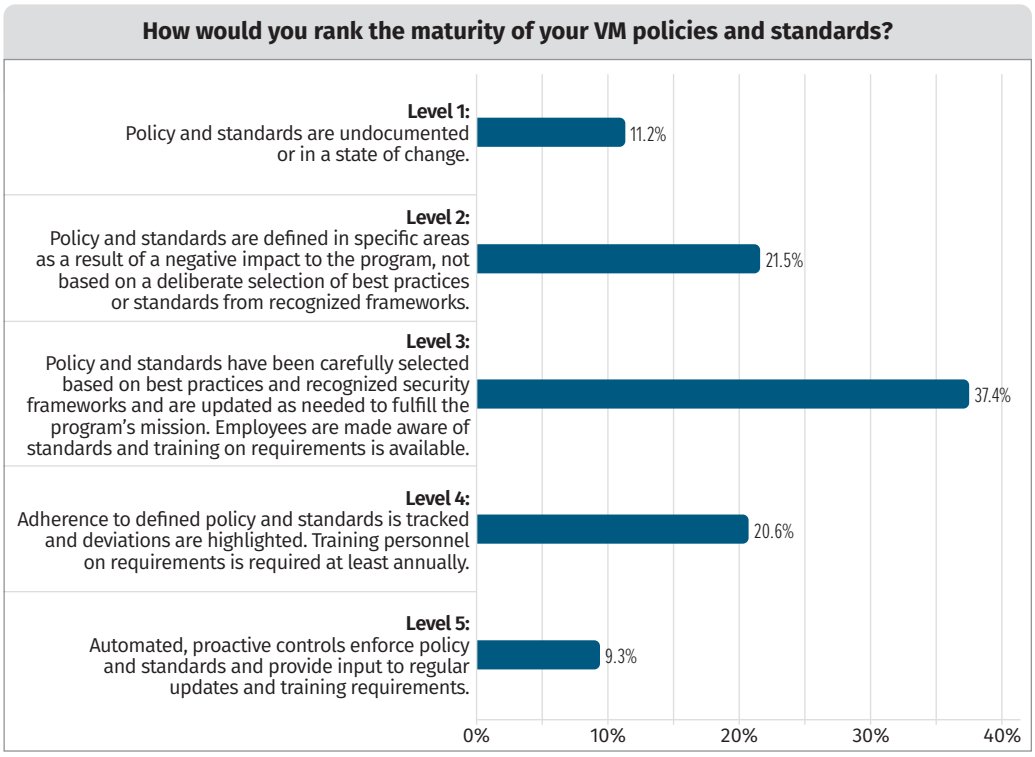

Figure 6: Maturity of Policies and Standards

https://t.me/learningnets

Context

When looking at the next category in the prepare phase of the VM life-cycle, it is not surprising that the maturity shifts lower. Many organizations continue to struggle to keep track of and manage their assets. See Figure 7.

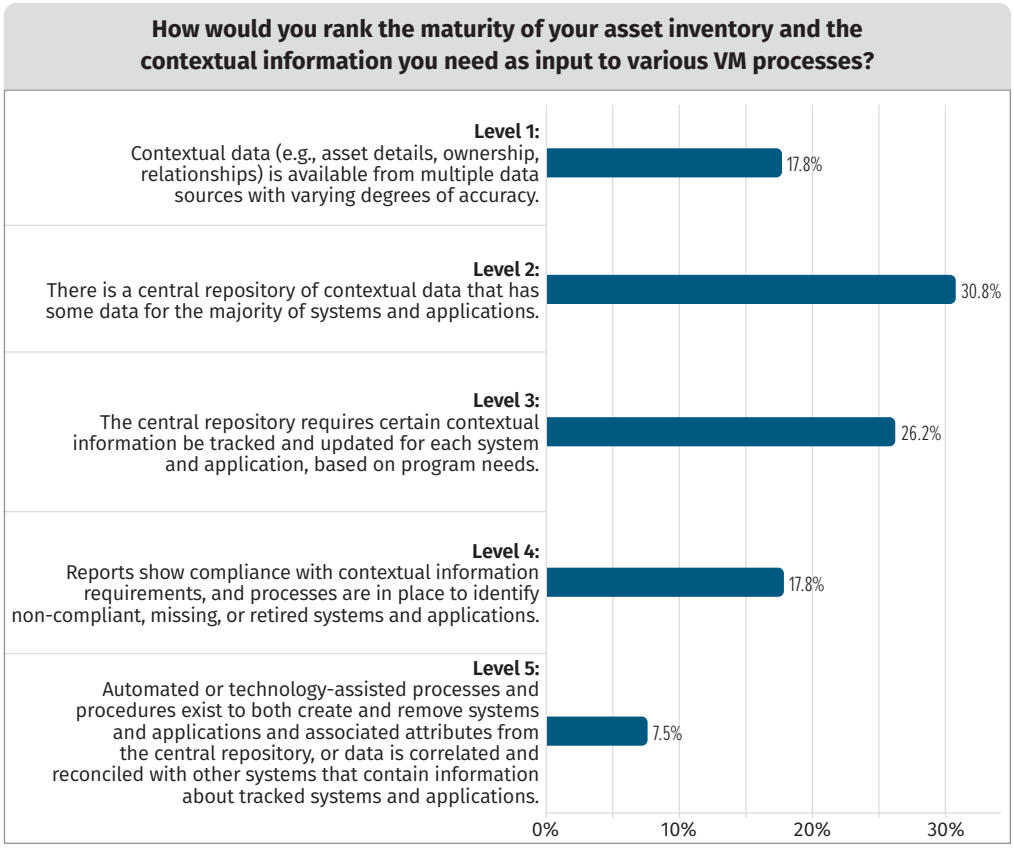

Figure 7. Maturity of Asset Inventory and Contextual Information

Although cloud and other types of programmable infrastructure may make querying our assets easier, the assets are now much more dynamic and may lack context if we are not appropriately leveraging tagging and other capabilities to store and leverage that context. Even if we are properly tagging our assets, our VM tools may struggle to leverage these tags and may not easily handle aging out assets that are more dynamic in nature. This is where tighter integration between our different tools can help—whether it be integration between our asset management and VM tooling or our programmable infrastructure and our asset management or VM tooling.

Identify

Identification is often how we define our vulnerability management programs. If there are automated tools in place to identify vulnerabilities, then we have a vulnerability management program. Although identification is a key part of vulnerability management, it does not solve the problem in a vacuum, which is why we cover so many different topics in the maturity model. Identification can happen in many different ways, but to simplify the model, there are three different functions we measure for maturity: automated identification, manual identification, and external identification.

https://t.me/learningnets

Automated Identification

Automated identification of traditional infrastructure is by far the most mature area in this survey. See Figure 8.

This makes a lot of sense, because we have had tools available to help us with this for decades and there are many vendors in this space. Where companies seem to be struggling the most is in implementing similar capabilities for containers and the cloud. Some of the reasons for the lack of maturity in these areas may be a combination of these being newer deployment and operational models for a lot of organizations and possibly a need for vendors to improve their capabilities to assess and report on these types of resources. Although many of the traditional vulnerability management vendors are capable of scanning in the cloud and include container scanning capabilities, these capabilities are not always as mature or well-understood by consumers.

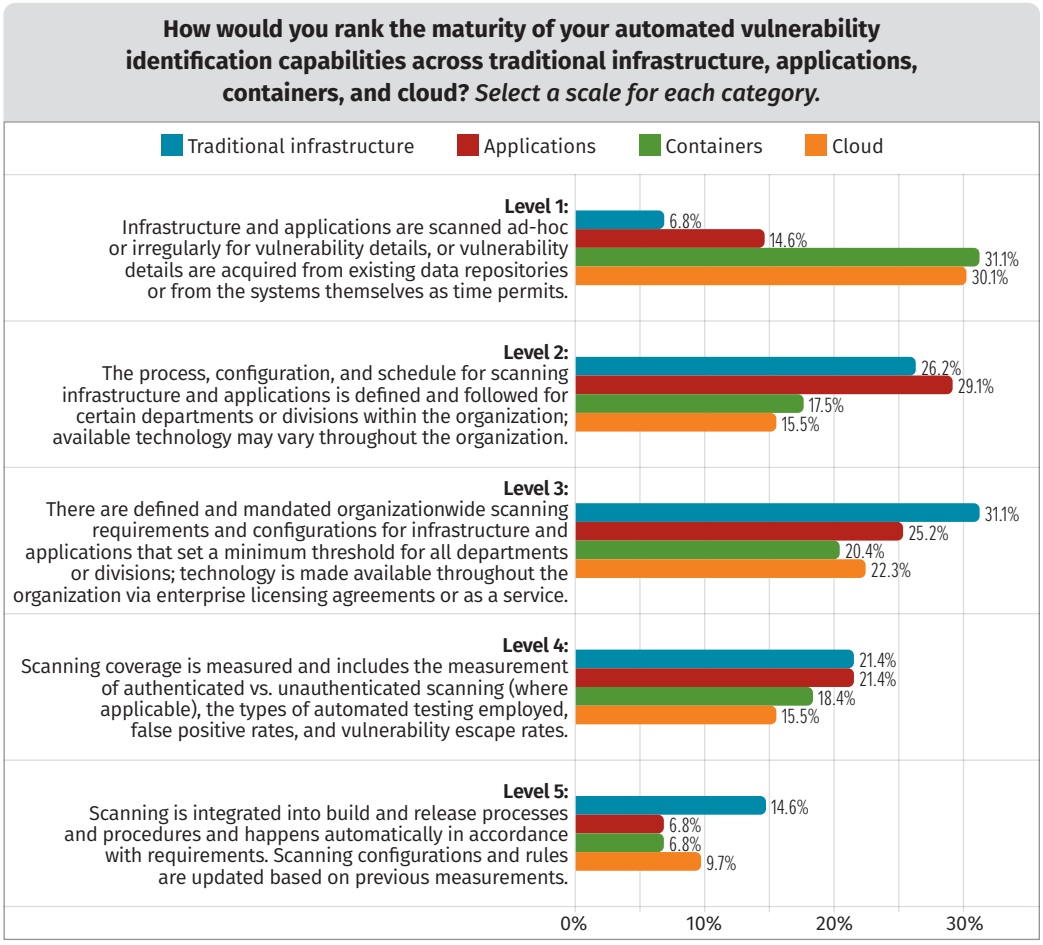

Figure 8. Maturity of Automated Vulnerability Capabilities by Category

Surprisingly, automated vulnerability identification for applications is somewhere in the middle. The reason this is surprising is that we find that many companies struggle with application security or application vulnerability management much more than with their infrastructure due to either a lack of dedicated resources or an inadequate understanding of how to engage with development teams to drive remediation. We guess that many of the struggles in this area come after identification, which may be why maturity here is higher than expected.

https://t.me/learningnets

Manual Identification

Manual identification maturity closely follows the trends we see in automated identification, but it is slightly less mature than automated identification across the board. See Figure 9.

Organizations have so much to monitor and assess these days that the trend is toward automation and away from manual processes. Nevertheless, it is important that organizations not ignore this function as certain application-layer vulnerabilities are not easily identified through automated identification technologies. Also, manual identification can provide much-needed data to justify time spent remediating identified vulnerabilities and can help organizations focus on the highest risk vulnerabilities in their backlogs.

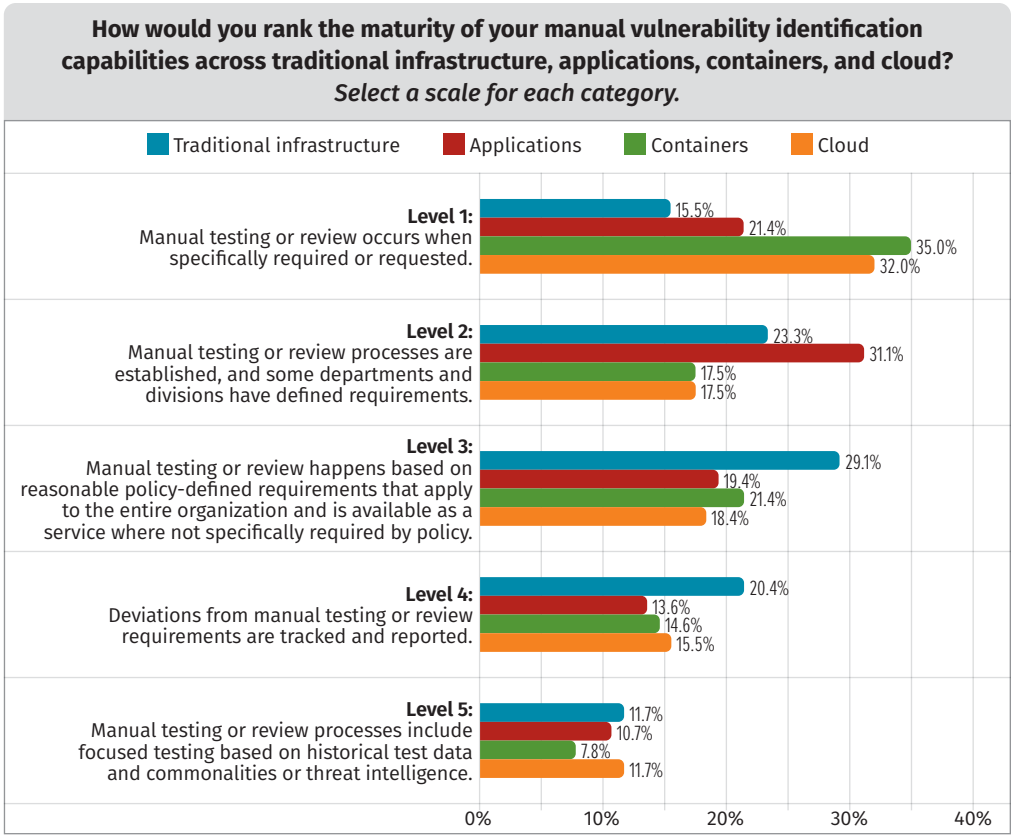

Figure 9. Maturity of Manual Vulnerability Capabilities by Category

External Identification

External identification may happen as part of a formal bug bounty program, but even if an organization does not have a bug bounty program, it needs to have a defined way of handling external vulnerability reports. Many of the respondents' organizations have definite room for growth in this area. See Figure 10.

The most important aspect of this function is to have and follow a defined vulnerability disclosure policy (VDP), but many companies have found that tapping into crowd-sourced identification capabilities can be valuable. The researchers that are involved in this kind of work tend to be much more specialized and can provide significantly more rigorous testing within their area of focus.

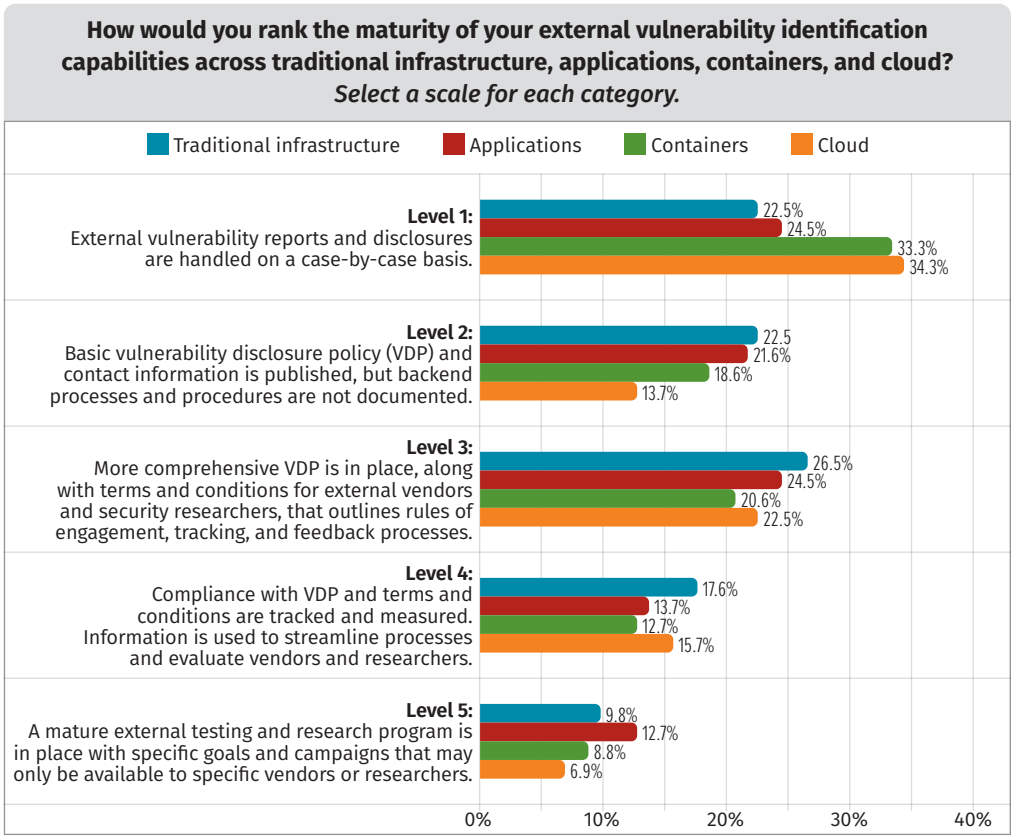

Figure 10. Maturity of External Vulnerability Capabilities by Category

https://t.me/learningnets

Analyze

If organizations want to understand what is working or not working in their programs, they will spend a good amount of time analyzing the data. While much of the focus in the industry is on prioritization—possibly due to the fact that it is easier to market a product that can successfully help you in this area—it is also important to dig into the details and analyze why certain metrics are not what we would hope for or expect. Why aren't teams patching patchable vulnerabilities? Why do certain technologies seem to consistently cause the most problems?

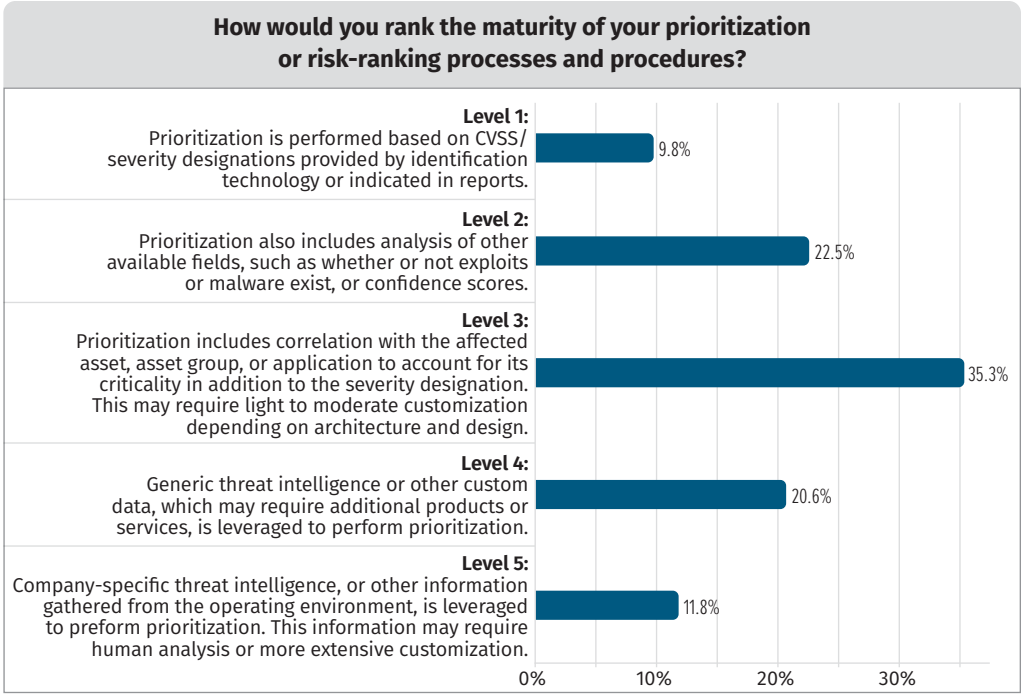

Figure 11. Maturity of Prioritization or Risk Ranking Processes

Prioritization

With all the industry talk and tooling around prioritization and risk scoring, it is not surprising that around 68% of respondents are defined Level 3 or better for maturity of their risk-ranking or prioritization procedures. See Figure 11.

Even though an organization's asset inventories may not be perfect, there is still value to be gained from joining this data set with its vulnerabilities to allow for better prioritization of the vulnerabilities. Layering threat intelligence on top of the other attributes the organization uses helps make the prioritization more relevant temporally.

Root Cause Analysis

What is a bit more surprising is that 54% self-select at Level 3 or better for root cause analysis. So, while there is a bit more focus on prioritization, over half the respondents have a defined process for looking into root cause issues as well. See Figure 12.

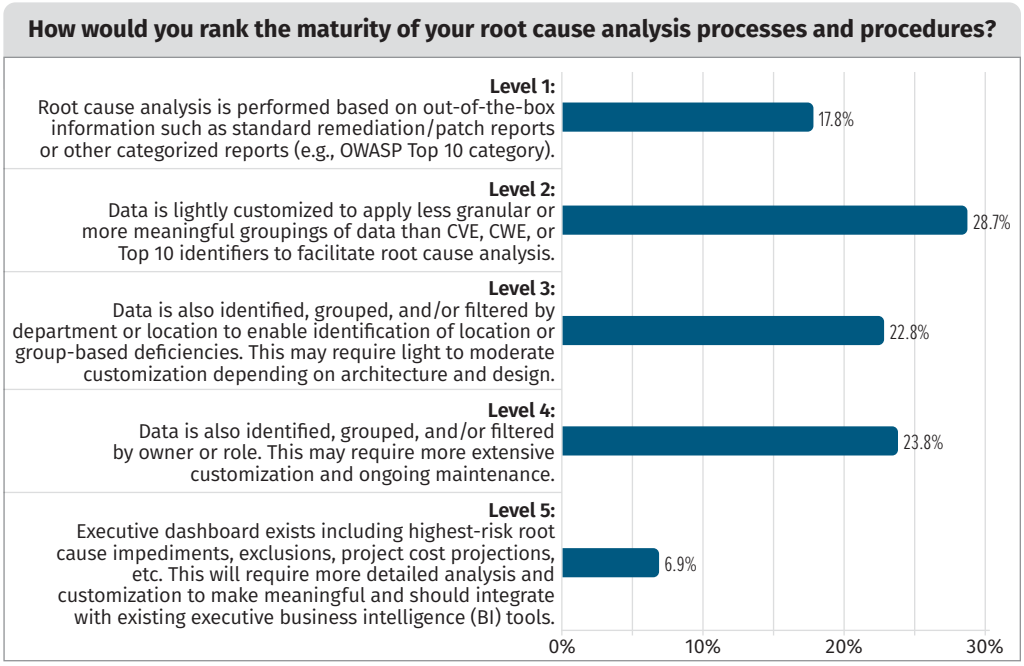

Figure 12. Maturity of Root Cause Analysis

https://t.me/learningnets

This is surprising because we find that many organizations struggle to adequately acknowledge and communicate problems that may require support from outside the program and participating technology organizations. This may show that the problem is not identifying the problems, but instead communicating them adequately or broadly enough to get support for change.

Communicate

Communication plays a key role in establishing buy-in from the community of VM stakeholders. Use cases can range from getting executives and board members to fund special projects that deal with technical debt to influencing IT and development stakeholders to engage more meaningfully in treating or remediating vulnerabilities. Making sure we are building and refining the right stories—backed by data—is a key component of this phase of the life cycle.

Metrics and Reporting

We need to understand what reports and metrics resonate with our audience, but reports and metrics alone do not always leave a lasting impression. See Figure 13.

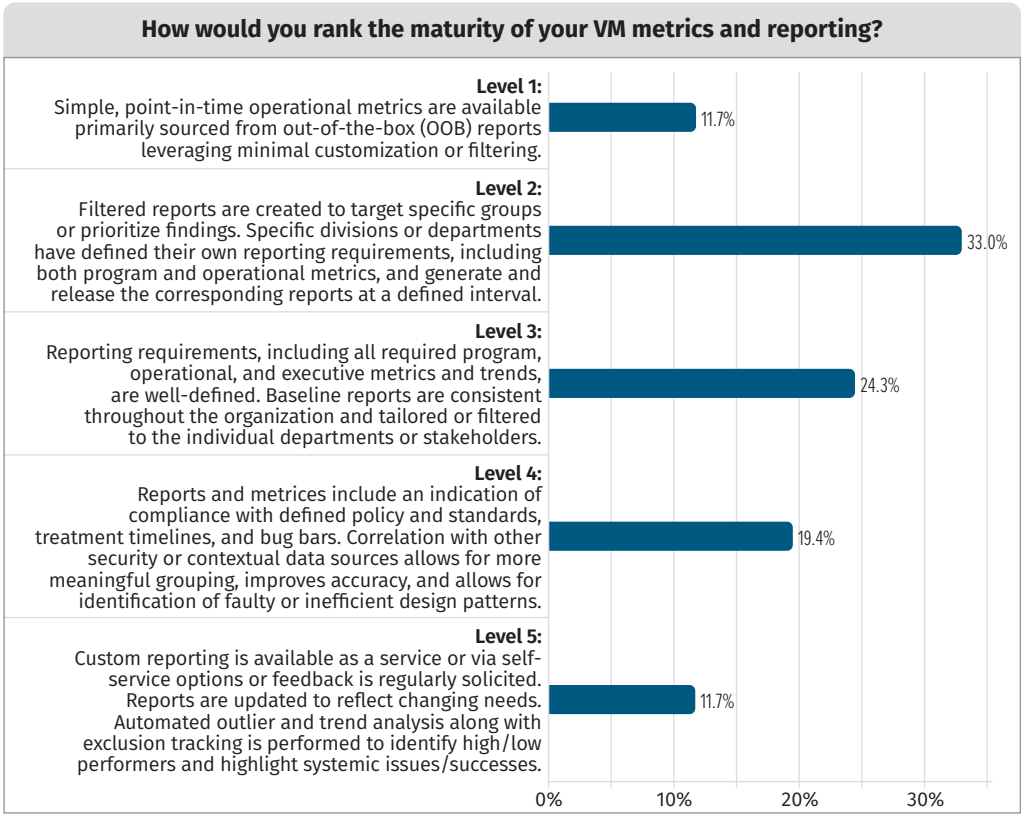

Figure 13. Maturity of Metrics and Reporting

Alerting

We also need to make sure we are properly defining both the quantity and quality of the alerts we are sending out to our different stakeholders. Not everything is a fire and analysts will ignore alerts if the system generates too many. Still, the strategic use of alerts can nudge people in the right direction and help us respond to critical or emergency issues.

https://t.me/learningnets

When looking at reporting, metrics, and alerting in terms of organizational maturity, it appears that organizations are a little more confident in their alerting capabilities than in the reports and metrics they have available to present to stakeholders. This is most likely due to the relatively poor selection of out-of-the-box reports and metrics and the difficulty of creating custom reports and metrics in many of the identification technologies. See Figure 14.

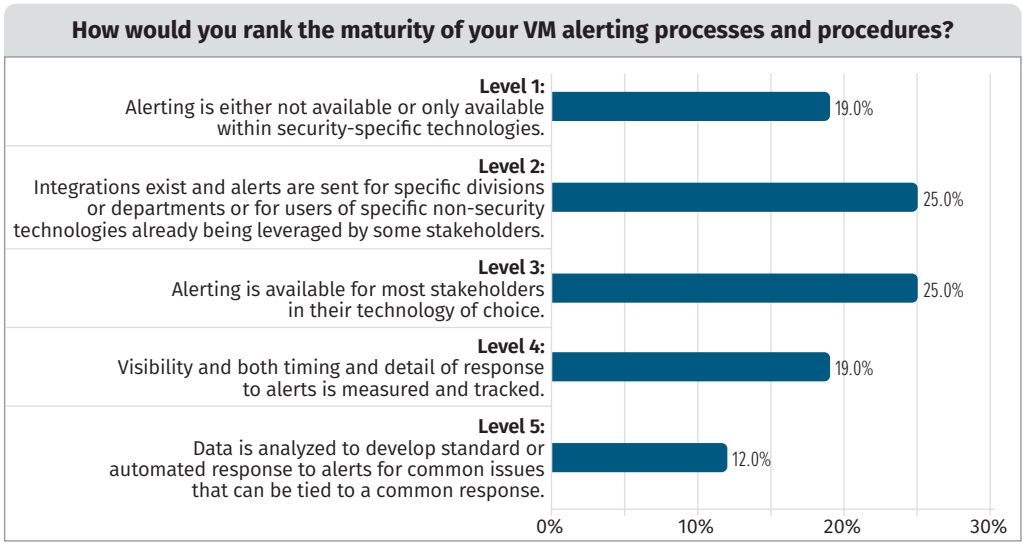

Figure 14. Maturity of Alerting Processes and Procedures

With alerts, we can focus on certain critical issues, and it is easier to tailor the messaging and drive specific behaviors. With reports and metrics, if we have not put in the effort to target specific groups with specific vulnerabilities on which they have both the responsibility and capability to act, then chances they will not have the desired effect. The vulnerabilities that the responsible stakeholder can act on will get lost in a sea of vulnerabilities that they are either not responsible for or that cannot be solved with a simple patch, configuration change, or small update to the code.

Treat

Treatment or remediation is the end goal of any vulnerability management program. The problem is that it is rarely the responsibility of a single team. Moreover, the responsible parties are typically not directly responsible for vulnerability management. These teams were likely not hired to remediate vulnerabilities. Instead, they were hired to build product or engineer systems and supporting infrastructure. This is one of the reasons why robust analysis and consistent, clear, and simple communication are key to overall success.

> **If these stakeholders feel as if the organization is wasting their time or that the data being presented is suspect, it is easy for them to disengage and focus on what they were hired to do—which, again, is not vulnerability management.**

While there is an expectation that we all care about security and that it is important, there will always be competing priorities. Vulnerability management program leaders need to find a way to balance the needs of the program with those of the overall business. They also need to recognize when groups of vulnerabilities are too difficult to resolve within the organization's existing architecture or within the responsible group's existing budget or resources. Once these groups are identified, the conversations need to be directed away from the engineering and operations teams and toward the executives and board members who can approve special projects or budget allocations to resolve the underlying roadblocks.

https://t.me/learningnets

Change Management

As we looked at organizations' maturity as it relates to change management, containers and cloud seem to be the most immature, which mirrors most of the other phases and functions assessed. Traditional infrastructure and applications rate on the higher end, which makes sense as these areas were why we implemented change management in the first place. See Figure 15.

The struggle with containers and cloud is not only that they are newer technologies, but also that they do not integrate as easily into traditional change management practices because of the dynamic nature of these resources. Organizations need to spend time adapting their change processes and procedures or determine how to qualify many of the container and cloud changes as standard changes to reduce the number of rigorous reviews.

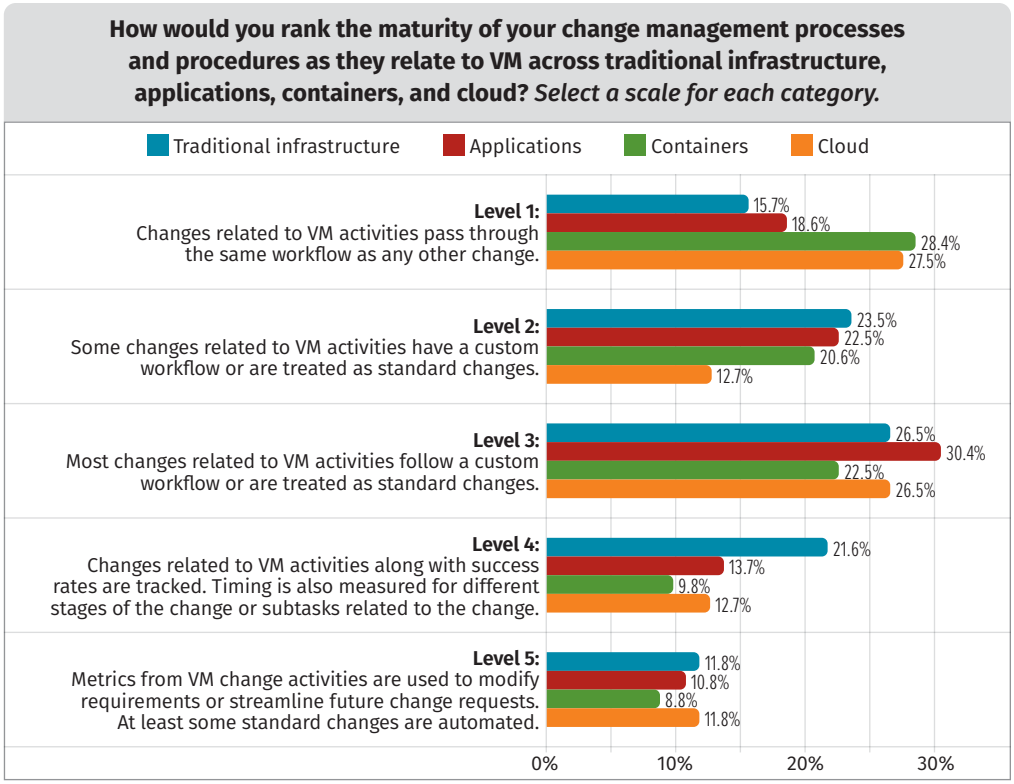

Figure 15. Maturity of Change Management by Category

Patch Management

Although we didn't measure the maturity of patch management across all categories, we would assume that the process would rank more mature than configuration management for most organizations across most asset types based on the reduced complexity associated with setting up and managing patches in comparison to configurations. See Figure 16.

Keep in mind, however, that we are measuring the maturity of the organizations' treatment processes. This does not account for the possibility there are obstacles that cause patches and their associated vulnerabilities from being excluded from the regular process. Our processes may still be mature even if our ability to execute those processes may be less mature for specific types of vulnerabilities.

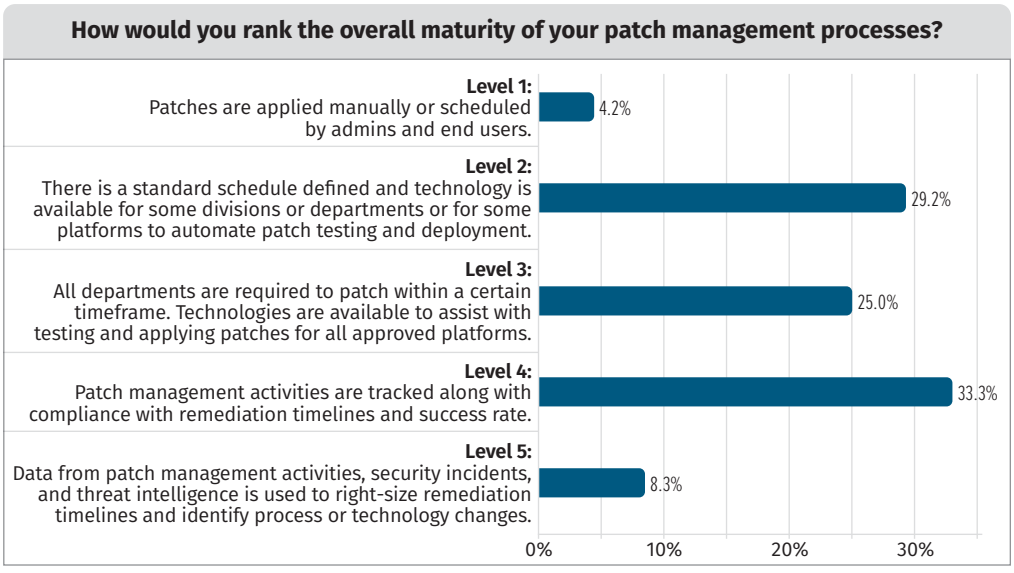

Figure 16. Maturity of Overall Patch Management

https://t.me/learningnets

Configuration Management

For configuration management, we see a similar picture. See Figure 17. It is surprising that containers do not rank as more mature in this category. Container architecture lends itself to more fixed, immutable configurations given that most containers are not designed to support change once they are running. This would seem to simplify configuration management and virtually eliminate drift.

However, it is possible respondents are struggling to manage and assess their container images and therefore do not have confidence in the configuration of these assets.

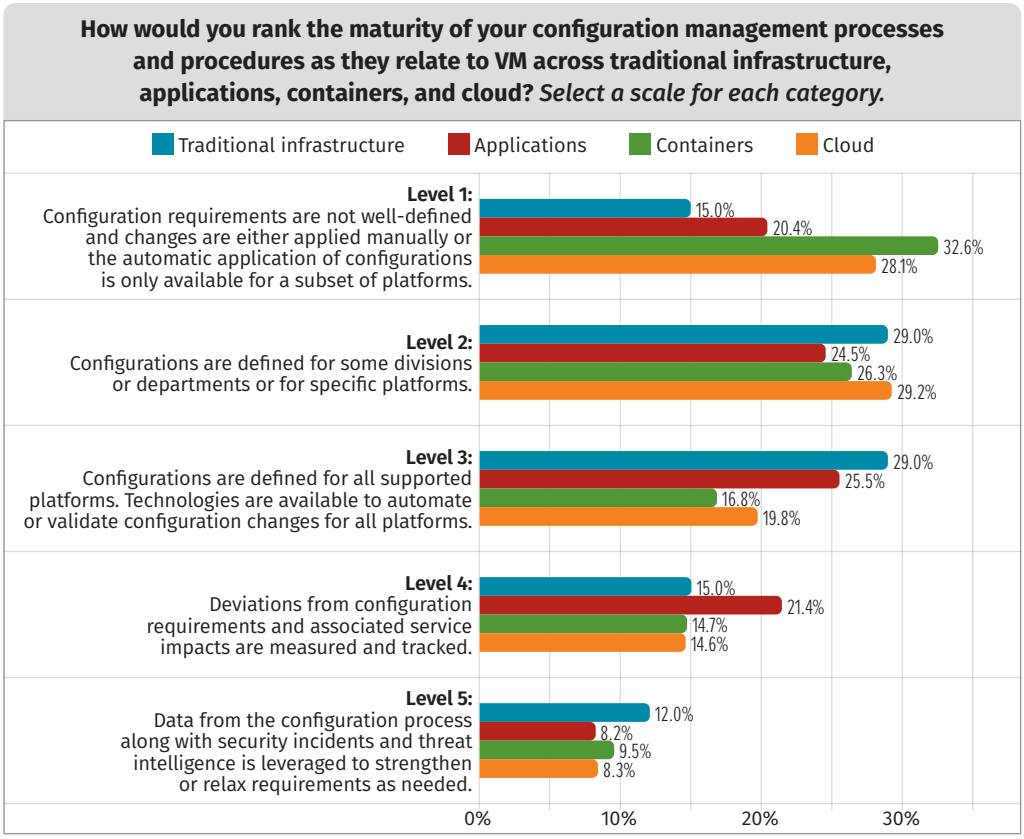

Figure 17. Maturity of Configuration Management by Category

Cloud Vulnerability Management

The last area of maturity we covered was how well respondents felt their organization was doing at managing vulnerabilities in the cloud. Just over 50% of the organizations rated themselves as falling within Levels 1 or 2. This is not surprising, given the fact that we are still struggling with traditional infrastructure even years after implementation—and the cloud adds layers of complexity, scale, and change on top of everything else. See Figure 18.

SANS thinks that there is a huge opportunity to do better VM in the cloud, but it will take careful planning and design to ensure the scale and rate of change do not wipe away these benefits. To be successful, organizations need to have a strong understanding of the shared responsibility model, where the responsibility of the cloud provider ends and the organizations begins, as well as what cloud-native or other technologies are available to help them succeed.

Cloud and container architectures can help organizations reduce the workload associated with managing configurations, especially for platform- and software-as-a-service or serverless infrastructure.

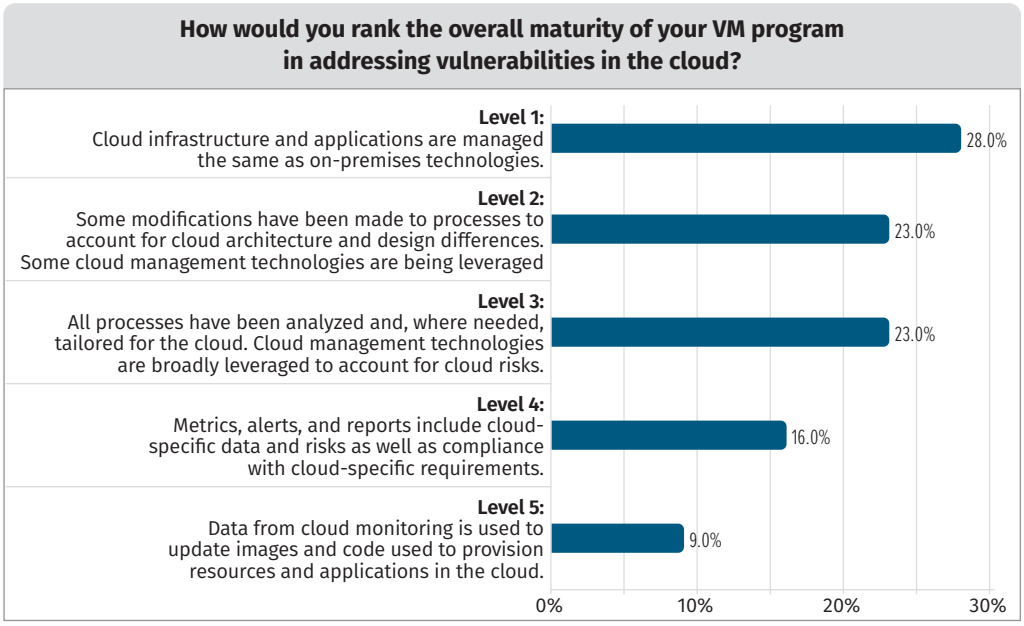

Figure 18. Maturity of Cloud VM Overall

https://t.me/learningnets

Summary and Final Recommendations

Most organizations are trying their best to manage vulnerabilities. Typically, however, organizations face challenging and expensive problems that are preventing certain types of vulnerabilities from being addressed. Organizations need to highlight these obstacles, communicate them effectively, and justify the funding and support required to remove these obstacles if they wish to succeed. As we continue to move away from traditional on-premises infrastructure toward containerized or cloud operating models, we need to take advantage of any opportunities that help us avoid similar obstacles in the future. Almost any move from one environment to another will, at least temporarily, reduce the number of vulnerabilities. If organizations are not thoughtful in building in solutions to the common issues we are experiencing today, it won't be long before it ends up right back where it started or in even worse shape due to the ease with which its footprint can grow and expand.

By reviewing the maturity information provided in this survey, organizations can quickly see how their current programs compare with others and where they might want to focus. It can also help organizations understand where it might take more time or effort to mature. Chances are, if most organizations are struggling with maturity for a certain function, it is probably because those functions take quite a bit more time and effort. That doesn't necessarily mean it is an area that we should avoid, but it can help us make more informed decisions about short-, medium-, and long-term road maps for maturing our programs. There is no quick fix to vulnerability management. Organizations need to incrementally and thoughtfully mature over time to succeed.

https://t.me/learningnets

About the Author

David Hazar is a SANS analyst, instructor, and co-author of SANS MGT516: Managing Security Vulnerabilities: Enterprise and Cloud. He is also an instructor and contributor for SANS SEC540: Cloud Security and DevOps Automation. A security consultant based in Salt Lake City, Utah, David focuses on vulnerability management, application security, cloud security, and DevOps. David has 20+ years of broad, deep technical experience gained from a wide variety of IT functions held throughout his career, including: developer, server admin, network admin, domain admin, telephony admin, database admin/developer, security engineer, risk manager, and AppSec engineer. He holds the CISSP, GWAPT, GWEB, GMOB, GCIA, GCIH, GCUX, GCWN, GSSP-.NET, and GSTRT certifications.

Sponsors

SANS would like to thank this survey's sponsors:

ARCTIC WOLF

AUTOMOX

BlackBerry
Intelligent Security. Everywhere.

cisco Cisco Umbrella

ExtraHop

Gigamon®

RAPID7

VULCAN.

https://t.me/learningnets