SANS

Analyst Program

Survey

SANS Vulnerability Management Survey 2022

Written by **David Hazar**

October 2022

VULCAN.

Executive Summary

The way companies build and deploy applications and services is evolving and the use of cloud, containers, and remote workers has continued to expand at a rapid pace. We are also increasingly relying on third-party software and libraries. Although these changes have resulted in increased options for identifying, tracking, and remediating vulnerabilities, security organizations must be actively involved in these changes in order to effectively evaluate and implement a vulnerability management (VM) program tailored to their organization's operations.

VM continues to be a struggle for many organizations. Although we are seeing improvements in maturity year over year, we see many companies struggling with backlogs of vulnerabilities they cannot fix—and a growing number of vulnerabilities they are not even responsible for fixing. These vulnerabilities may require their vendors or the open-source community to provide or implement the fix. VM programs spend a good deal of time identifying and communicating vulnerability details, yet sometimes the end goal of these activities—to help the technology organizations prioritize and treat or remediate the identified vulnerabilities—is overlooked.

Do we have a vulnerability management problem or a technology management problem? We should all be asking ourselves this question as we evaluate what we need to do to succeed in managing vulnerabilities and reducing risk for our respective organizations. Only by digging into the details to identify existing problems and starting to analyze how to solve them can we identify solutions.

Even though many organizations have well-defined VM programs, certain aspects of those programs continue to cause problems for survey respondents. Specifically, those aspects prevent them from maturing past Level 3 or Defined in many areas or functions of the program or for specific asset types.[1]

Some of the difficulties we might encounter are:

- Things change too quickly.
- We lack complete visibility (shadow IT).
- We don't budget for fixing vulnerabilities—and we don't have extra time or resources.
- Continued support for legacy assets and applications is required by the business.
- The work is not always recognized and rewarded.
- Security is accountable—but is not responsible—for much of the work.
- New vulnerabilities are continuously being discovered—so the work is never "done."
- We cannot fix what we don't manage.

[1] Refer to the SANS VM Maturity Model for definitions of Level 3 and Defined. For more information, visit www.sans.org/posters/key-metrics-cloud-enterprise-vmmm

How do we succeed? Most organizations already know how to patch and reconfigure assets and fix bugs in code, so some other obstacles must be at play. When reviewing a company's backlog, it is not uncommon for us to find that well over 50% of outstanding vulnerabilities cannot be remediated due to issues that are not receiving the proper attention or resources: "We can't patch these servers cause the applications running on them require the older vulnerable software and libraries to run," or "We can't patch or get rid of that browser because our internal apps require the older version." VM programs must get better at identifying these issues, so they can develop business cases for larger changes in our operating procedures or technology requirements. Only then will we be able to remove those obstacles.

Some of the key findings and takeaways from this year's survey include:

- More than 50% of respondents work for organizations that have adopted a cloud-first strategy.
- The percentage of companies with a formal VM program increased slightly from 75% in 2021 to 77% in 2022 with the remaining participants either having an informal program or planning on creating a formal program in the next 12 months.
- Around 4% more organizations are using a third party to manage their formal program.
- There was no significant change in the VM functions and asset types included in the programs for more traditional VM asset types or functions, but cloud infrastructure as a service and platform as a service, custom software or application development, and containers had far greater coverage over levels reported by respondents in 2019, 2020, and 2021.
- Security still plays the largest role in leading many VM functions, with the exception of remediation work such as patch and configuration management. Somewhat surprisingly, security's responsibility has increased in those areas by more than 10% since last year's survey.
- Automated discovery or scanning for vulnerabilities is included in almost 7% more organizations than last year.
- Maturity of change, patch, and configuration management capabilities are trending in the right direction.
- Cloud vulnerability management maturity is increasing.
- Less than half (43%) of our respondents are managing supply chain vulnerabilities proactively.

Figure 1 provides a snapshot of the 2022 survey respondents' demographics.

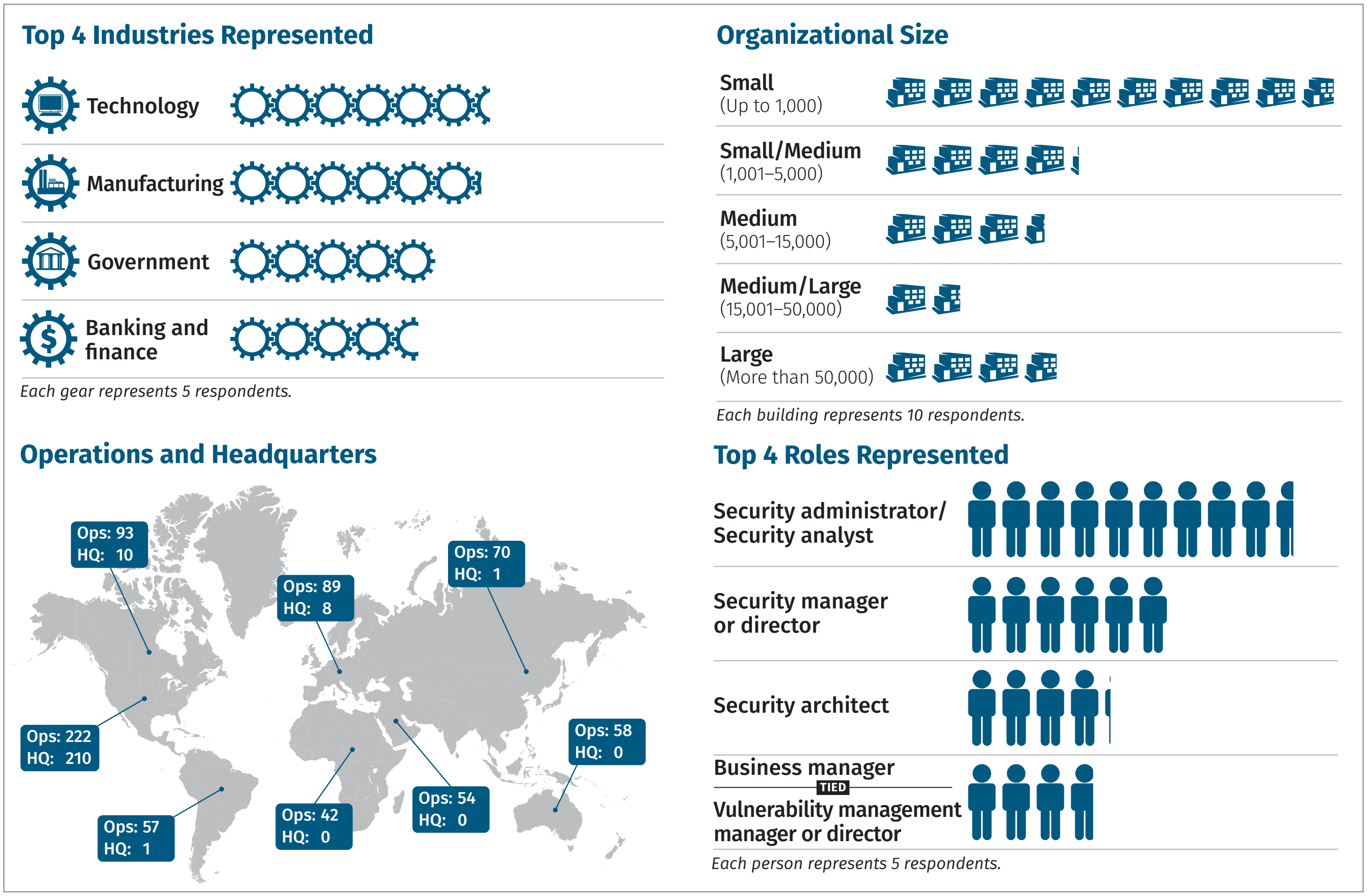


Figure 1. Key Demographic Information

Setting the Stage

The percentage of organizations with a formal program managed internally dropped a couple of percentage points to 61% which might be concerning if not for the fact that the use of third parties increased to 15% from 11% over the same period. Overall, there was a 2% increase in the number of respondents with formal programs. Those that do not have a formal program are still informally managing their vulnerabilities (17%) in some fashion or have plans to formalize a program in the next 12 months (6%). See Figure 2.

These results indicate that almost 94% of organizations at least have some processes in place to identify or manage their vulnerabilities with the remaining working on it.

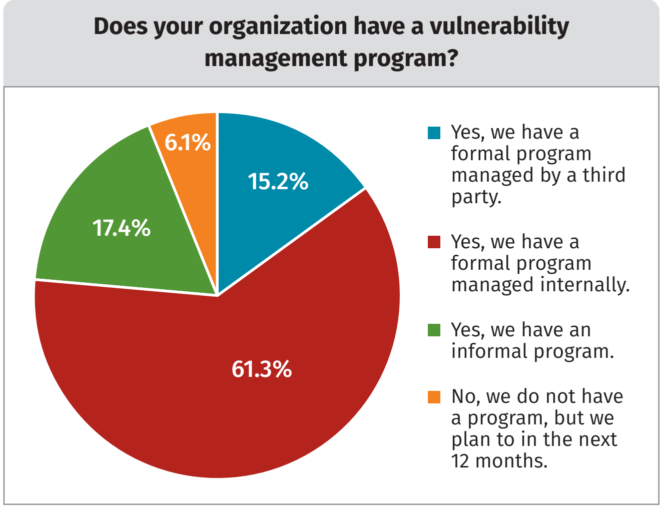


Figure 2. Formal vs. Informal Programs

This year, similar to previous years, we asked respondents to identify the specific types of assets and functions they included or planned to include in their vulnerability management program. While many of these measurements were similar to previous years, cloud infrastructure and platform as a service, custom software or application development (internal), and containers saw larger increases. See Figure 3. These increases are not surprising given how much more prevalent cloud and container usage has become over the last several years. Also, the technologies that help security teams identify vulnerabilities in cloud and containers have become much more prevalent and mature.

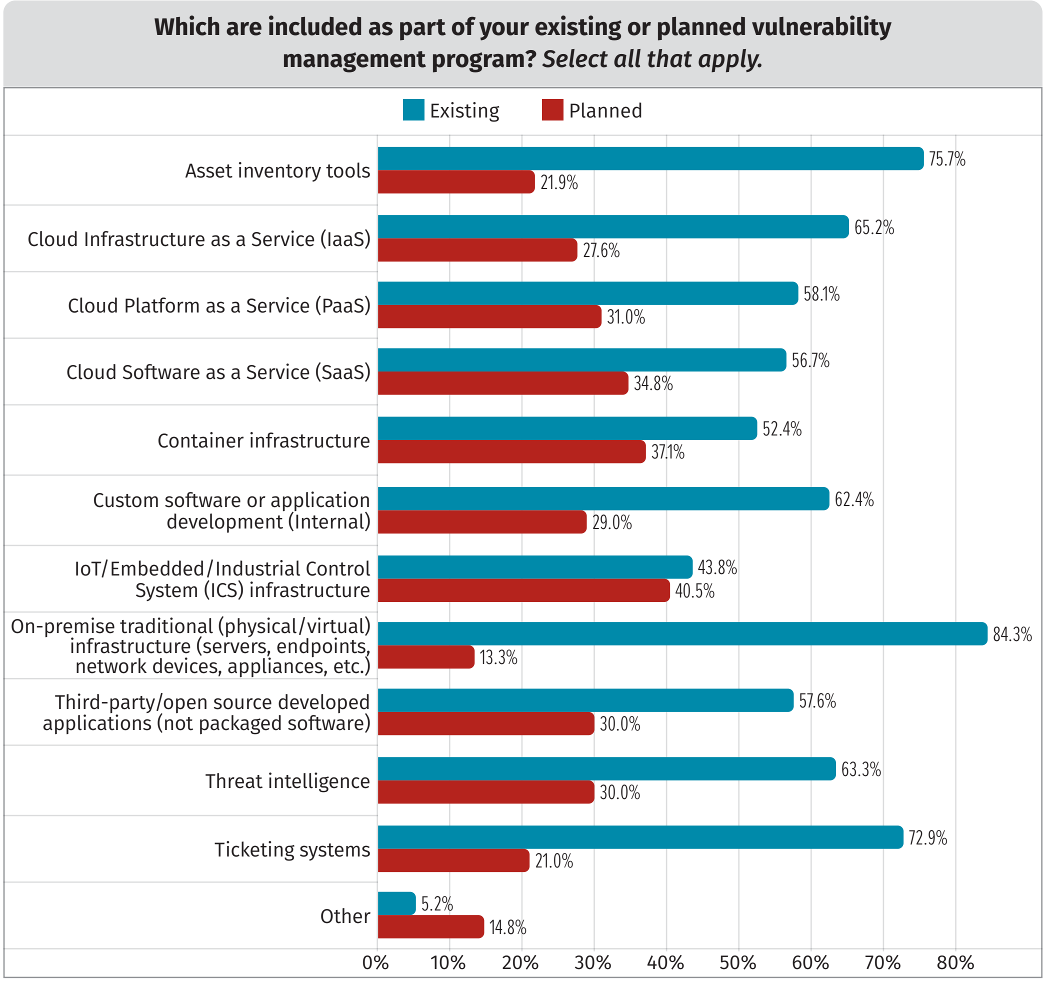
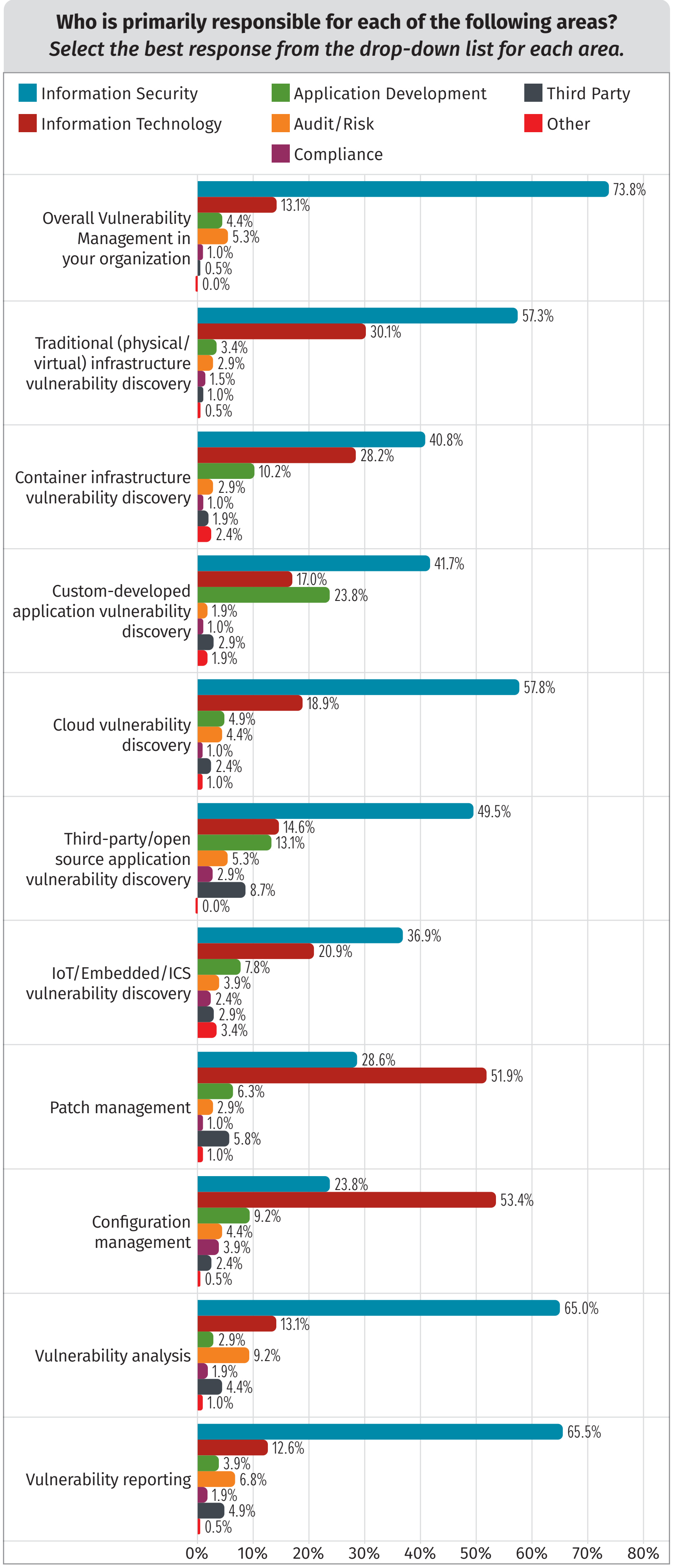

Which are included as part of your existing or planned vulnerability management program? ***Select all that apply.***

Figure 3. Vulnerability Management Program Assets

Responsibility for Vulnerability Management Programs

Information security continues to be the group within organizations most often assigned responsibility for overall vulnerability management, as shown by the increase to nearly 74% vs. 64% the previous year. IT organizations still take point for remediation activities such as patch (52%) and configuration management (53%) in most organizations (illustrated in Figure 4) yet these percentages are down 10% from last year, with information security apparently taking over those responsibilities for these organizations. Part of this could be due to the fact that there are more vulnerability management technologies that offer remediation capabilities. Another could just be a decision to gain efficiencies by having the teams that are finding the vulnerabilities also be more involved in fixing the vulnerabilities.



Who is primarily responsible for each of the following areas?
Select the best response from the drop-down list for each area.

Figure 4. Primary Responsibility

Year-Over-Year Comparison

Eighty-seven percent of respondent organizations perform automated vulnerability discovery, an increase this year of 7%, building on last year's 10% increase. Note that this survey question just measures whether any automated scanning is occurring and does not provide insight into whether all assets in a given category are subject to automated scanning.

Traditional, on-premises infrastructure continues to be the most common area of automated vulnerability discovery at 82%, which is almost 9% higher than last year. Automation increased in all other asset types, with cloud infrastructure as a service and custom software or application development (internal) seeing the largest gains. See Figure 5.

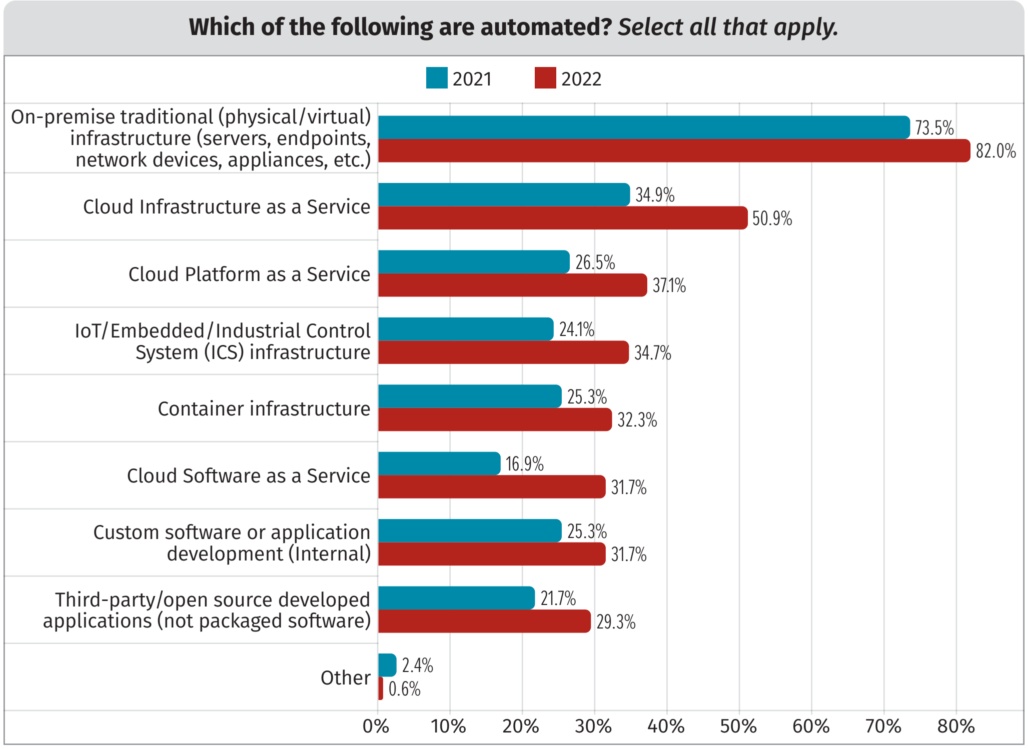


Figure 5. Automated Discovery by Asset Type

The increase in scanning for applications may be due to a rising general interest in application security, but the recent supply-chain vulnerabilities in third-party software libraries may play a role as well. The increase in cloud is not surprising given the increase in cloud adoption, cloud expertise, cloud maturity, and cloud-first strategies for many organizations during the past few years.

Fewer organizations are using manual patch and configuration management techniques (down more than 5% over last year) and 5% more respondents indicate they have moved to a continuous patch and configuration model vs. a defined cadence (weekly or monthly, for example). See Figures 6 and 7. Manufacturing, government, and technology organizations are the most likely to use the ASAP/continuous model for applying patches and configuration changes to their assets.

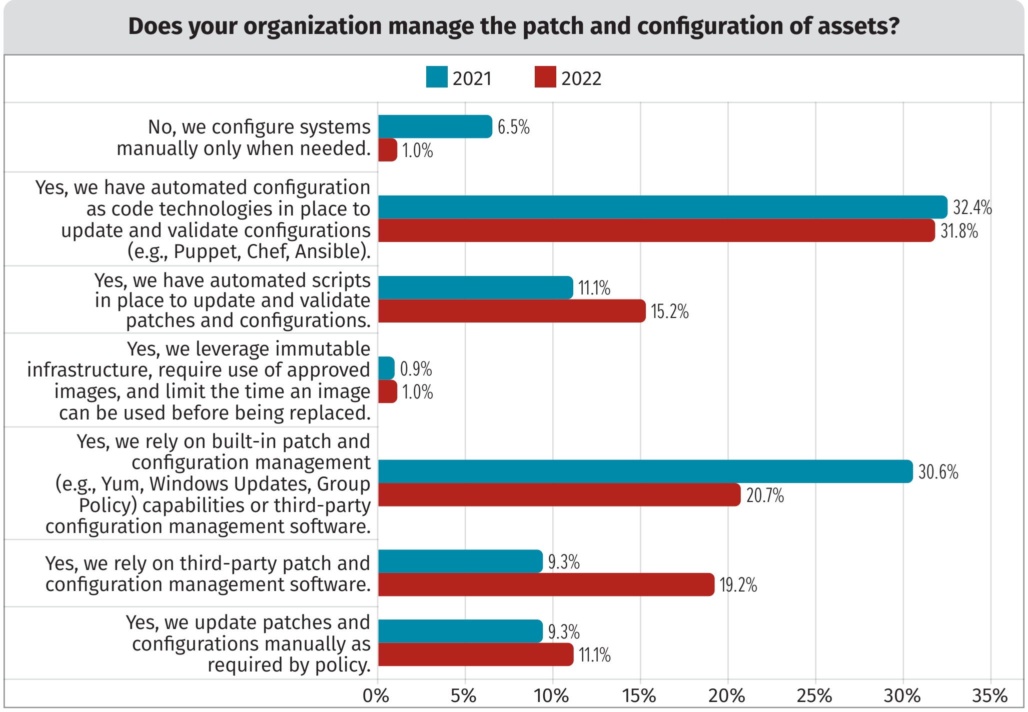


Figure 6. Patching and Configuration Management

Cloud and the Supply Chain

Nearly 55% of respondents' organizations have adopted a cloud-first strategy. (We did not ask this question in 2021.) It will be interesting to see how this percentage grows in coming years. Manufacturing, technology, cybersecurity, and banking and finance respondents were the most likely to indicate that their organizations had adopted a cloud-first policy or strategy. Manufacturing is probably the most surprising in that group.

We also added a couple of questions this year on supply chain vulnerabilities. Fewer than 50% of organizations (43%) are managing these proactively, and many organizations are relying primarily on existing asset inventories and traditional vulnerability management tools to identify and track these vulnerabilities. See Figures 8 and 9.

More so than the other industries, manufacturing, government, and technology organizations have moved to a more proactive approach to managing supply chain vulnerabilities. While asset inventories and traditional VM scanning technologies are still the most widely used technology for identifying supply chain vulnerabilities, it will be interesting to see how the use of software composition analysis changes over time along with image scanning and other less traditional forms of identification.

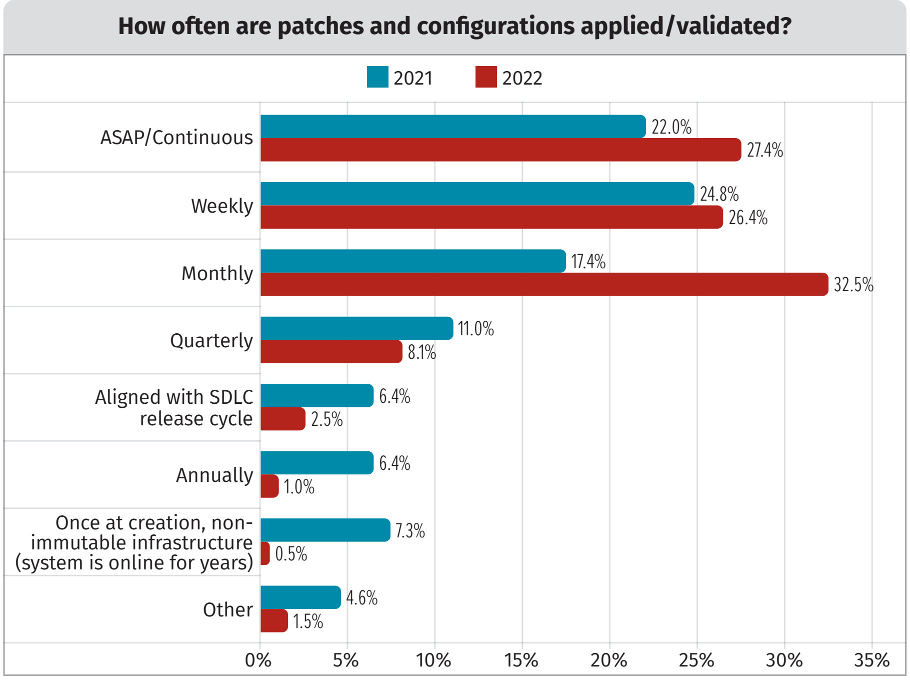


Figure 7. Treatment Frequency

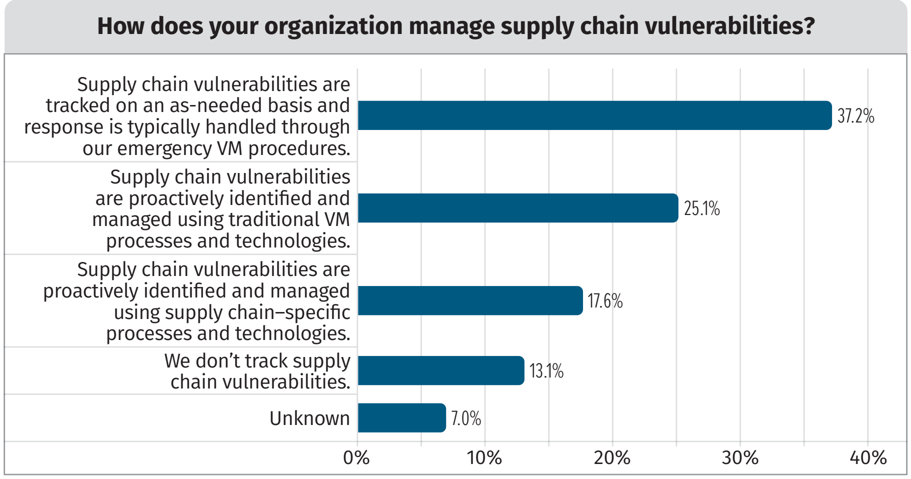


Figure 8. Managing Supply Chain Vulnerabilities

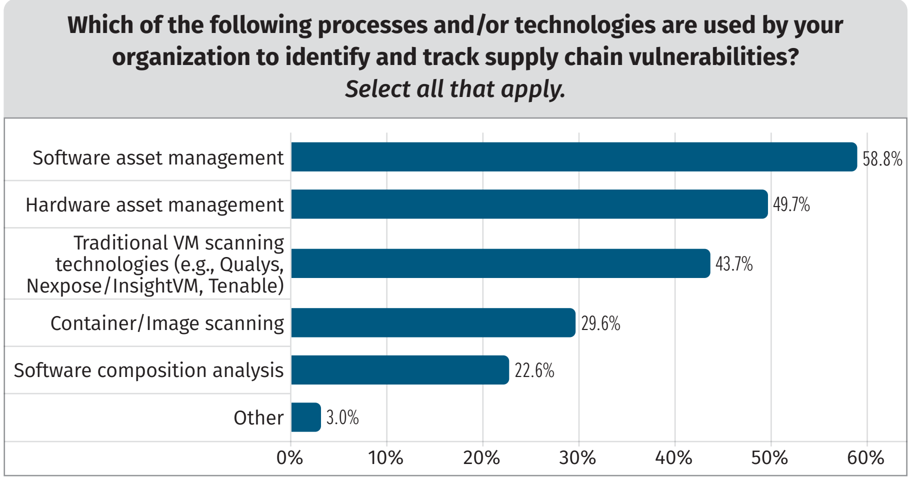


Figure 9. Supply Chain Vulnerability Identification and Tracking

VM Maturity

This is the second year we have asked respondents to rate their maturity based on the SANS Vulnerablity Management Maturity Model. As a result, we are now able to compare responses year over year in an attempt to spot any trends. This section looks at each of the phases of the vulnerability management lifecycle that are included in the maturity model and how the survey respondents graded themselves against that model.

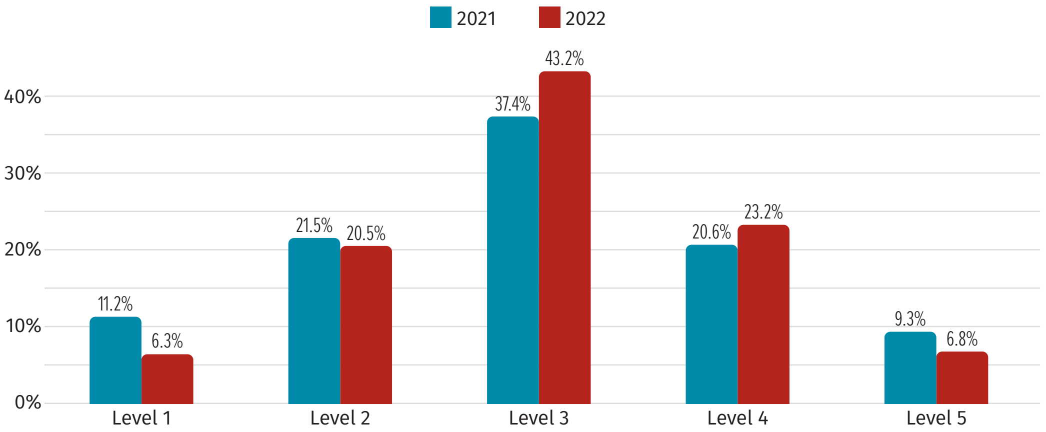
Prepare

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 may want to consider a similar approach to program development. Organizations cannot excel at everything right away—if they focus on more than a few capabilities each cycle, they will likely struggle to maintain focus and may not make significant gains on any one capability.

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. Maturity has shifted up a little more toward Level 3 (Defined) and Level 4 (Quantitatively Managed), but a smaller percentage of respondents indicated a Level 5 maturity in this category than last year. See Figure 10.

How would you rank the maturity of your VM policies and standards?



	% Change (FY2021–FY2022)		
	2021	2022	% Change
Level 1	11.2%	6.3%	-4.9% ▼
Level 2	21.5%	20.5%	-1.0% ■
Level 3	37.4%	43.2%	5.8% ▲
Level 4	20.6%	23.2%	2.6% ▲
Level 5	9.3%	6.8%	-2.5% ▼

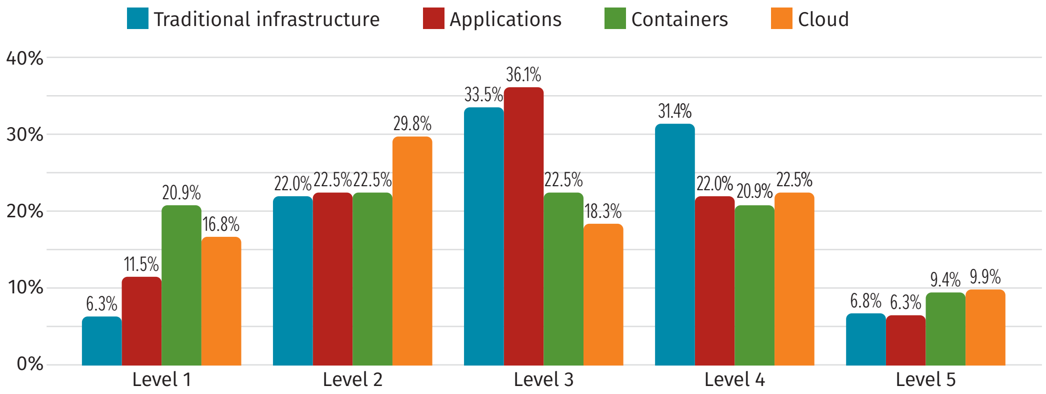
Figure 10. Maturity of Policies and Standards

This area is clearly trending in the right direction. We do hope to see more companies using automated controls to enforce their policies and standards in the future as emerging technologies make this easier. Cloud adoption and DevSecOps operating models definitely help provide options for defining and enforcing certain policies and standards in code. While there will always be some policies and standards that cannot be enforced with code, defining as many as possible can help compliance tremendously.

Context

With regard to asset inventories and the availability and quality of contextual information, the maturity is a bit lower (especially for non-traditional asset types) but is definitely trending in the right direction. We expect to see even more maturity in this area in the future as more companies implement passive asset-discovery technologies. These technologies leverage APIs to interrogate existing data sources along with network traffic to correlate information and get a better understanding about which assets exist in the organization and where there might be gaps. Many of our current technologies have accessible APIs, which makes this type of discovery and analysis possible and decreases our reliance on active and agent-based discovery. See Figure 11.

How would you rank the maturity of your asset inventory and the contextual information you need as input to various VM processes?
Select a scale for each category—traditional infrastructure, applications, containers, and cloud.



	% Change (FY2021–FY2022)		
	2021	2022	% Change
Level 1	17.8%	13.9%	-3.9% ▼
Level 2	30.8%	24.2%	-6.6% ▼
Level 3	26.2%	27.6%	1.4% ▲
Level 4	17.8%	24.2%	6.5% ▲
Level 5	7.5%	8.1%	0.6% ■

Figure 11. Maturity of Asset Inventory and Contextual Information[2]

Even without purchasing technologies, organizations can leverage APIs available in their cloud environments, virtualization hypervisors, and other types of programmable infrastructure. They can also leverage tagging and other capabilities that allow for the storage and retrieval of contextual information. If third-party technologies are not available, organizations can still build and maintain their own big data stores to collect and analyze the information. The main capabilities the newer passive asset management technologies provide are hundreds of pre-built integrations for different data sources and pre-built queries and correlation rules. Depending on how many data sources are needed to get an accurate representation of the environment, it may be possible to build and maintain something in-house.

[2] Note: We used the average for 2022, as we didn't break out categories in 2021.

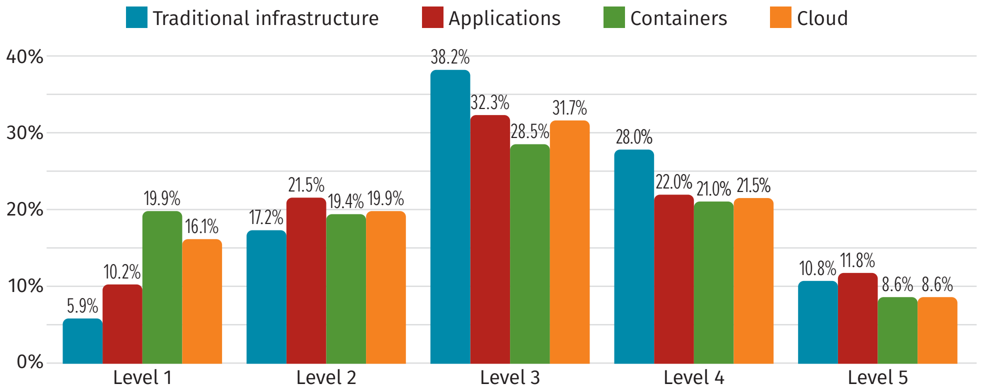
Identify

Many organizations mistakenly believe that if there are automated tools in place to identify vulnerabilities, then a vulnerability management program exists. Although identification is a key part of vulnerability management, it alone does not solve any problems. Identification can happen in many different ways, but the maturity model measures three of the most important methods: automated, manual, and external.

Automated Identification

The maturity of automated identification processes has improved for all asset types, but the more notable improvements have been for cloud (+14% Level 3+), applications (+13%), and containers (+12%). As organizations leverage automation and move to a more DevSecOps model for systems and software development, they have more visibility into the assets or images that need scanning. It is also possible that the shift to cloud and remote workforce has led to increased agent-based scanning, which tends to improve coverage, especially for more dynamic asset types. See Figure 12.

How would you rank the maturity of your automated vulnerability identification capabilities across traditional infrastructure, applications, containers, and cloud? *Select a scale for each category.*



	% Change (FY2021–FY2022)			
	Traditional infrastructure	Applications	Containers	Cloud
Level 1	-0.9% ■	-4.3% ▼	-11.2% ▼	-14.0% ▼
Level 2	-9.0% ▼	-7.6% ▼	1.9% ▲	4.4% ▲
Level 3	7.1% ▲	7.0% ▲	8.1% ▲	9.4% ▲
Level 4	6.6% ▲	0.7% ■	2.5% ▲	6.0% ▲
Level 5	-3.8% ▼	5.0% ▲	1.8% ▲	-1.1% ▼

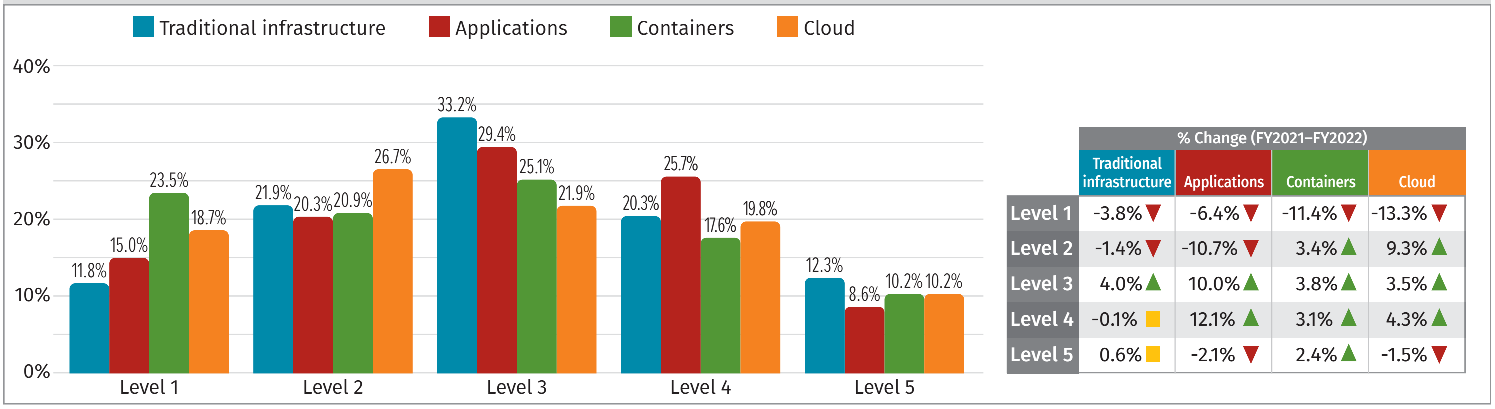
Figure 12. Maturity of Automated Vulnerability Capabilities by Category

The available options for scanning containers and containerized applications have grown over the past couple of years with a large increase in the number of registry scanning technologies (many of which are open source or free) and the number of Kubernetes integrations that provide container image scanning. The increased consolidation of version control technologies and use of automated pipelines by organizations has also made it easier for organizations to identify and track their applications. Also, software composition analysis tools are more readily available than they have been in the past. Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) options have become much more ubiquitous, and most organizations have multiple options for gaining visibility into the security of their cloud environments.

Manual Identification

Manual identification maturity has also improved over last year for most asset types, with applications seeing the largest increase in Level 3 or Defined and Above Maturity at 10% followed by containers (7%) and cloud at only 4%. Traditional infrastructure actually decreased slightly by 1% which could be due to demographics or a shift away from traditional operating models. See Figure 13.

How would you rank the maturity of your manual vulnerability identification capabilities across traditional infrastructure, applications, containers, and cloud? ***Select a scale for each category.***



	% Change (FY2021–FY2022)			
	Traditional infrastructure	Applications	Containers	Cloud
Level 1	-3.8% ▼	-6.4% ▼	-11.4% ▼	-13.3% ▼
Level 2	-1.4% ▼	-10.7% ▼	3.4% ▲	9.3% ▲
Level 3	4.0% ▲	10.0% ▲	3.8% ▲	3.5% ▲
Level 4	-0.1% 🟨	12.1% ▲	3.1% ▲	4.3% ▲
Level 5	0.6% 🟨	-2.1% ▼	2.4% ▲	-1.5% ▼

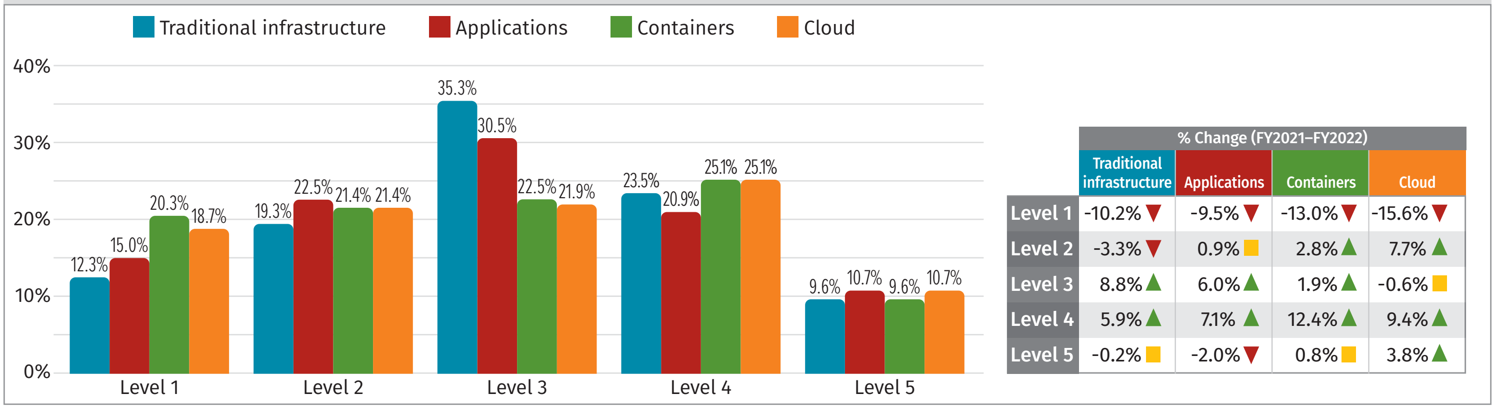
Figure 13. Maturity of Manual Vulnerability Capabilities by Category

Automated tools for identifying vulnerabilities continue to improve, but certain types of flaws are not easily found by these technologies. Manual assessment will always have a place in identifying those business and application-specific vulnerabilities. Organizations need to continue to mature these capabilities even as more automated scanning is introduced into environments.

External Identification

External identification may happen as part of a formal bug bounty program, but even without such a program, organizations need to have a defined way of handling external vulnerability reports. Many more respondents have set up and defined their processes for handling these types of vulnerabilities and engaging with external researchers. See Figure 14.

How would you rank the maturity of your external vulnerability identification capabilities across traditional infrastructure, applications, containers, and cloud? ***Select a scale for each category.***



	% Change (FY2021–FY2022)			
	Traditional infrastructure	Applications	Containers	Cloud
Level 1	-10.2% ▼	-9.5% ▼	-13.0% ▼	-15.6% ▼
Level 2	-3.3% ▼	0.9% 🟨	2.8% ▲	7.7% ▲
Level 3	8.8% ▲	6.0% ▲	1.9% ▲	-0.6% 🟨
Level 4	5.9% ▲	7.1% ▲	12.4% ▲	9.4% ▲
Level 5	-0.2% 🟨	-2.0% ▼	0.8% 🟨	3.8% ▲

Figure 14. Maturity of External Vulnerability Capabilities by Category

The reason for the increase could possibly be attributed to the binding directive from the US Cybersecurity and Infrastructure Security Agency (CISA), which was released in September 2020 and requires all US government agencies to have a published Vulnerability Disclosure Policy.[3] However, among respondents in government with US-based headquarters, the only asset type with a major increase was "Traditional Infrastructure," so there may be other reasons for this year-over-year increase.

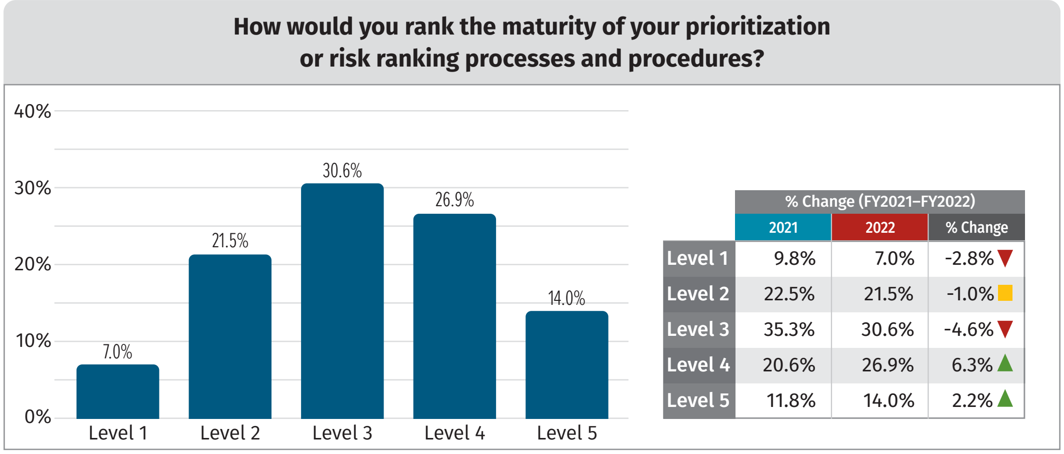
Although the most important aspect of this type of identification is to have and follow a defined vulnerability disclosure policy, many companies have found value in tapping into crowdsourced identification capabilities. The researchers involved in this kind of work tend to be much more specialized and can provide more rigorous testing within their area of focus.

Analyze

If organizations want to understand what is working and what is not in their respective programs, they must spend a good amount of time analyzing the data. Much of the focus in the industry is on prioritization—possibly because it is easier to market a product that can successfully help in this area—but it is also important to dig into the details and analyze why certain metrics fall short of expectations. (Why aren't teams patching patchable vulnerabilities? Why do certain technologies seem to consistently cause the most problems?)

Prioritization

Prioritization maturity has improved this year with more companies moving from Level 3 (defined) to Level 4 (quantitatively managed) and Level 5 (optimizing). See Figure 15. The marked increase in technologies available to consolidate and prioritize security vulnerabilities has likely made it easier for companies to prioritize more consistently and incorporate publicly available threat intelligence. This writer has definitely seen more adoption of these technologies over the past couple of years.



	% Change (FY2021–FY2022)		
	2021	2022	% Change
Level 1	9.8%	7.0%	-2.8% ▼
Level 2	22.5%	21.5%	-1.0% ■
Level 3	35.3%	30.6%	-4.6% ▼
Level 4	20.6%	26.9%	6.3% ▲
Level 5	11.8%	14.0%	2.2% ▲

Figure 15. Maturity of Prioritization or Risk Ranking Processes

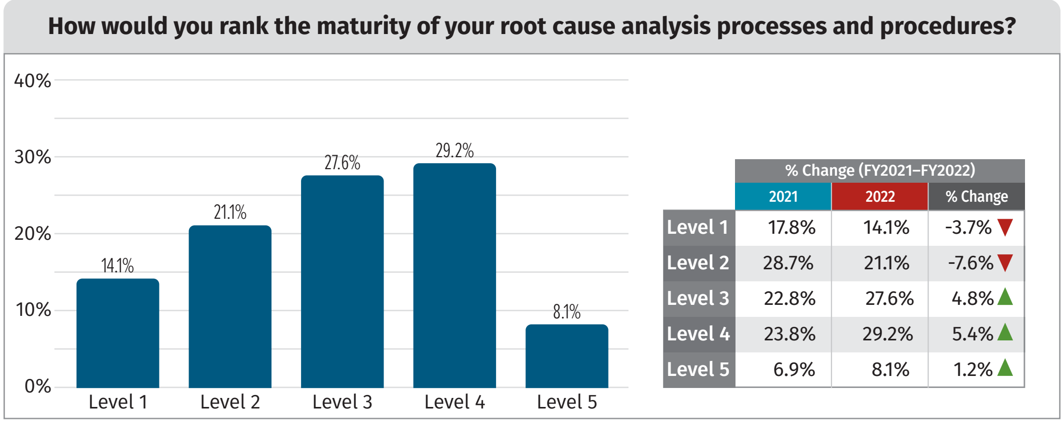
[3] "Binding Operational Directive 20-01—Develop and Publish a Vulnerability Disclosure Policy," Cybersecurity and Infrastructure Security Agency (CISA), www.cisa.gov/binding-operational-directive-20-01

As asset inventories, tags, or other mechanisms for storing context improve, organizations will be able to not only prioritize generally, but also prioritize within the reports and lists targeting specific stakeholder groups, program components, or program technologies. As internal threat intelligence capabilities increase, they may even be able to provide more company-specific customizations to the risk scores they use for prioritization. While this tactic can help focus on reducing the riskiest vulnerabilities, we have found it is not nearly as important as root-cause analysis.

Root-Cause Analysis

The maturity of organizations' root-cause analysis processes and procedures has flipped from leaning left or less mature to leaning right on the maturity model matrix. Even more organizations are exceeding the defined level for this capability than for prioritization, which was not the case last year. See Figure 16. We believe this is a positive sign because as we discussed in last year's survey results, many organizations struggle to adequately acknowledge and communicate problems within the program that may require support from outside the program and participating technology organizations.[4]

This year's survey showed that more organizations have started to generate owner and role level metrics and data to provide more focused visibility than in 2021. This visibility streamlines root-cause analysis.



	% Change (FY2021–FY2022)		
	2021	2022	% Change
Level 1	17.8%	14.1%	-3.7% ▼
Level 2	28.7%	21.1%	-7.6% ▼
Level 3	22.8%	27.6%	4.8% ▲
Level 4	23.8%	29.2%	5.4% ▲
Level 5	6.9%	8.1%	1.2% ▲

Figure 16. Maturity of Root Cause Analysis

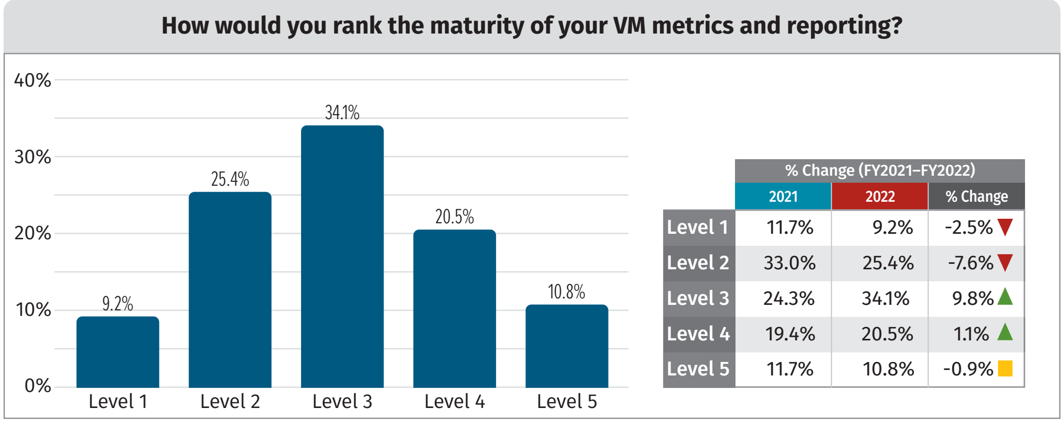
Communicate

Effective and efficient communication can help ensure the success of a vulnerability management program. Not only does it help establish buy-in, but it also helps influence behavior. In order to be effective, an organization needs to know what information is best suited for each stakeholder group. It can determine this by analyzing what changes need to happen within the different stakeholder groups and then determining which metrics are most likely to drive those changes or behaviors. It can't be all about the data—turn the data into a compelling story for more widespread understanding and adoption.

[4] "A SANS 2021 Survey: Vulnerability Management—Impacts on Cloud and the Remote Workforce," SANS, www.sans.org/white-papers/sans-2021-survey-vulnerability-management-impacts-cloud-remote-workforce/ (registration required to download paper).

Metrics and Reporting

Last year, the majority of organizations rated themselves at Level 2 (Managed), but this year most organizations have moved to at least a Defined or Level 3 maturity. See Figure 17. If organizations can get more accurate context to enable them to produce more targeted reports and establish treatment timelines and bug bars that correspond to their policies and standards, they can even more effectively measure compliance. This would help with root-cause analysis, getting buy-in from stakeholders, and possibly increasing top-down support from management.



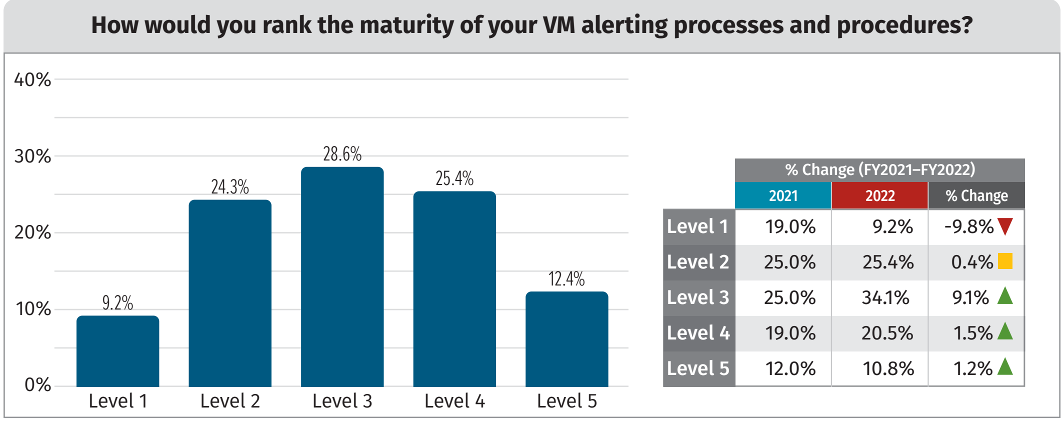
	% Change (FY2021–FY2022)		
	2021	2022	% Change
Level 1	11.7%	9.2%	-2.5% ▼
Level 2	33.0%	25.4%	-7.6% ▼
Level 3	24.3%	34.1%	9.8% ▲
Level 4	19.4%	20.5%	1.1% ▲
Level 5	11.7%	10.8%	-0.9% ■

Figure 17. Maturity of Metrics and Reporting

Alerting

Alerting can be highly effective if used judiciously. Organizations should carefully analyze where risk is too high to wait for reports and dashboards. They should also determine where alerts may be beneficial. It may be helpful to create alerts that nudge stakeholders to view their reports or action any tickets or backlog items. Be sure to work closely with those stakeholders to define requirements so they can help make them as effective as possible.

Last year, more organizations were confident in the maturity of their alerting capabilities than their metrics and reporting. The difference in maturity between these two capabilities is not as drastic this year, but this year there are more organizations at Level 4 (Quantitatively Managed) for alerting than last year. The year-over-year increase in alerting maturity is not quite as pronounced as the increase in reporting and metrics, but it was good to see a large drop in those at Level 1 (-10%). See Figure 18.



	% Change (FY2021–FY2022)		
	2021	2022	% Change
Level 1	19.0%	9.2%	-9.8% ▼
Level 2	25.0%	25.4%	0.4% ■
Level 3	25.0%	34.1%	9.1% ▲
Level 4	19.0%	20.5%	1.5% ▲
Level 5	12.0%	10.8%	1.2% ▲

Figure 18. Maturity of Alerting Processes and Procedures

Alerts are ideal for emergency vulnerabilities such as zero-day vulnerabilities or vulnerabilities actively being exploited. They may also help increase focus for monthly or quarterly goals set by the organization. Creating alerts for any vulnerabilities approaching defined due dates can also be helpful as long as those timeframes are achievable for each stakeholder group.

Treatment

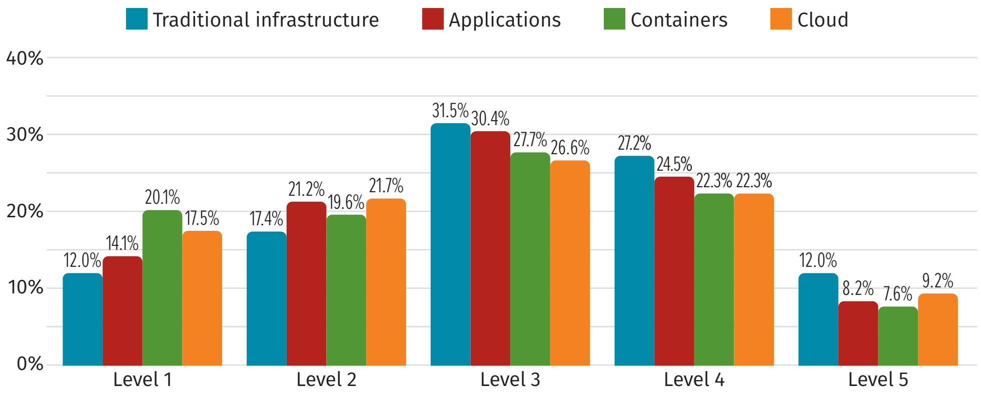
If an organization is doing everything else well, it would be natural to assume that treatment or remediation would follow. But alas, this is not always the case. Here is where root-cause analysis can help determine what may be preventing technology teams from moving forward. They may find that the solution to their problem lies not in how they identify and communicate vulnerabilities, but in how they build, deploy, and maintain their systems, software, and applications. While security teams are not typically directly responsible for these functions, effective preparation, identification, analysis, and communication will hopefully lead to crucial conversations about systems architecture and design. Maybe such involvement will allow them to participate in the next digital transformation project to more tightly integrate and automate change, patch, and configuration management processes.

At SANS, we have noticed that the organizations most effectively reducing their vulnerability backlogs have opted in to a continuous update approach to patch and configuration management. In this approach, teams continuously test against and apply the latest patches and versions of operating systems, software, libraries, and any required configuration changes. Build and deployment teams are required to have excellent test coverage, which is more easily accomplished through automation. While this might not describe your organization today, consider how to get the support to make these changes in your environment.

Change Management

As we look at organizations' maturity as it relates to change management, it has increased across the board, with the cloud asset type being the least mature and also increasing the least since last year (7%). See Figure 19 for this year's results. The dynamic nature of the cloud and the fact that cloud deployment teams may operate separately and distinctly from other infrastructure and application teams may contribute to the lower maturity. Traditional infrastructure and applications rate the highest, which makes sense because these areas were why organizations implemented change management in the first place.

How would you rank the maturity of your change management processes and procedures as they relate to VM across traditional infrastructure, applications, containers, and cloud? *Select a scale for each category.*



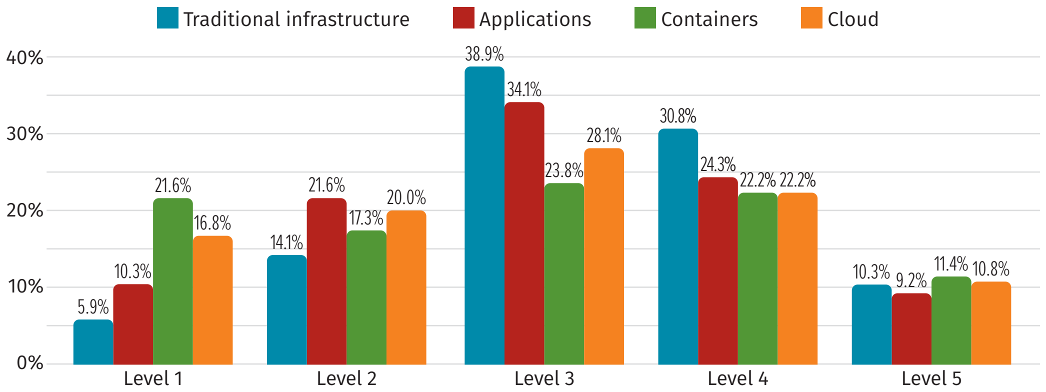
	% Change (FY2021–FY2022)			
	Traditional infrastructure	Applications	Containers	Cloud
Level 1	-3.7% ▼	-4.5% ▼	-8.3% ▼	-10.1% ▼
Level 2	-6.1% ▼	-1.4% ▼	-1.0% ■	9.0% ▲
Level 3	5.1% ▲	0.0% ■	5.2% ▲	0.2% ■
Level 4	5.6% ▲	10.7% ▲	12.5% ▲	9.5% ▲
Level 5	0.2% ■	-2.6% ▼	-1.2% ▼	-2.5% ▼

Figure 19. Maturity of Change Management by Category

Patch Management

Organizations are over 11% more mature in their patch management capability than configuration management for traditional infrastructure, but the difference is much less pronounced for other asset types. This difference could be because other asset types, especially containers, are not really patched as much as updated with a new image. Comparing results from this year with those from last year, the biggest increase in maturity occurred at Level 3 (defined). See Figure 20 for this year's survey results in this category.

How would you rank the maturity of your patch management processes and procedures as they relate to VM across traditional infrastructure, applications, containers, and cloud? ***Select a scale for each category.***



	% Change (FY2021–FY2022)		
	2021	2022	% Change
Level 1	4.2%	13.6%	9.4% ▲
Level 2	29.2%	18.2%	-11.0% ▼
Level 3	25.0%	31.2%	6.2% ▲
Level 4	33.3%	24.9%	-8.4% ▼
Level 5	8.3%	10.4%	2.1% ▲

Figure 20. Maturity of Overall Patch Management[5]

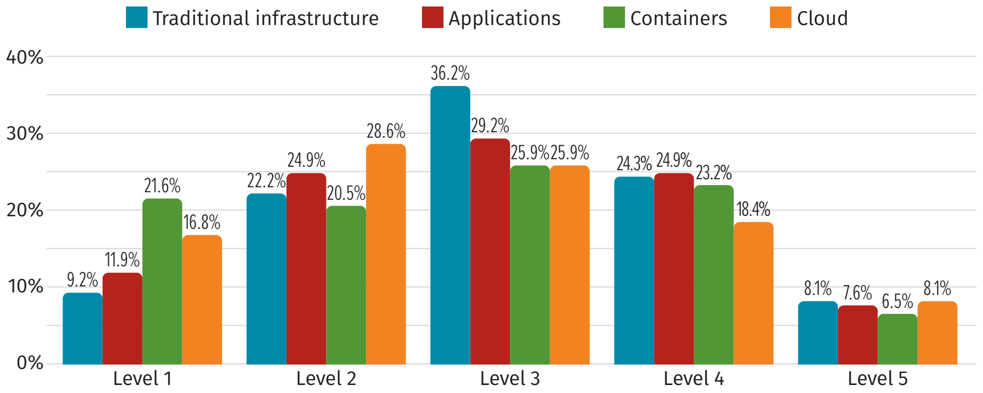
Keep in mind that this survey question measures the maturity of the organization's treatment processes, which doesn't always equate to 100% successful remediation of vulnerabilities. Organizations with mature processes can and do still encounter obstacles that cause patches and their associated vulnerabilities to be excluded from the regular process.

Configuration Management

For configuration management, organizations are generally less mature, but the increase between last year and this year is still very good with the maturity of containers increasing the most (14%) and cloud the least (1%). Last year we were surprised by the low maturity within the container space, so we are happy to see these improvements. See Figure 21 (on the next page) for this year's survey results in configuration management. We expect cloud capabilities to increase as more organizations leverage automation to build out and manage their cloud environments and as cloud-native options continue to mature.

[5] Note: We used the average for 2022, as we didn't break out categories in 2021.

How would you rank the maturity of your configuration management processes and procedures as they relate to VM across traditional infrastructure, applications, containers, and cloud? ***Select a scale for each category.***



	% Change (FY2021–FY2022)			
	Traditional infrastructure	Applications	Containers	Cloud
Level 1	-5.8% ▼	-8.5% ▼	-11.0% ▼	-11.4% ▼
Level 2	-6.8% ▼	0.4% ■	-5.8% ▼	-0.5% ■
Level 3	7.2% ▲	3.7% ▲	9.1% ▲	6.2% ▲
Level 4	9.3% ▲	3.4% ▲	8.5% ▲	3.8% ▲
Level 5	-3.9% ▼	-0.6% ■	-3.0% ▼	-0.2% ■

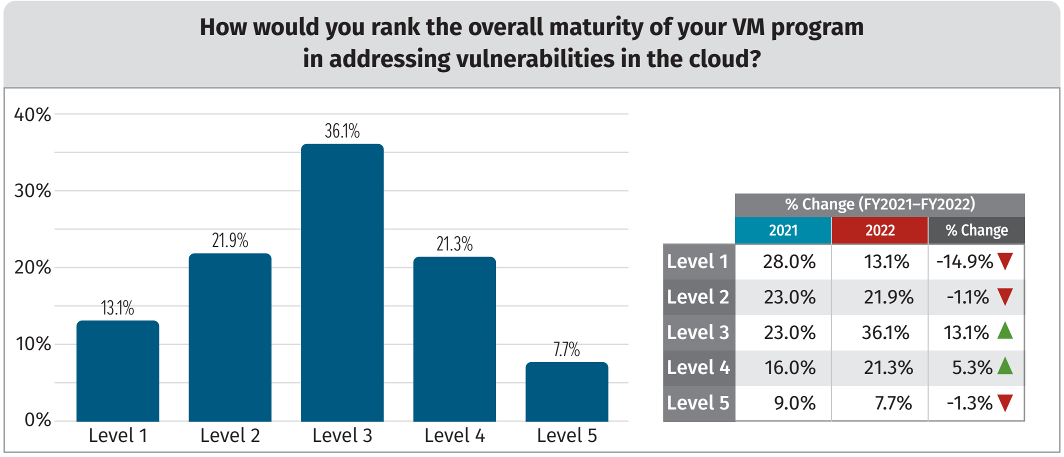
Figure 21. Maturity of Configuration Management by Category

Based on what the survey indicates about how organizations handle patch and configuration management, healthcare, education, and retail are the industries that rely the most on manual processes. This does not mean that no one in these industries is automating patch and configuration management, but there are more respondents indicating manual patching in these industries than in other industries. When we consider how those industries are operated and the design of their networks, this statistic makes more sense. The equipment used is usually more tightly controlled and may leverage technology to return the devices to the expected state when users log out (Kiosk Mode) or may require more firmware updates vs. traditional software-based patch and configuration changes. Combine this with a generally more distributed operating model, and it may explain why manual update processes are more common in these industries.

Manufacturing, technology, banking and finance, and government are the industries with the most automation, according to the survey results. Manufacturing was a surprising standout this year in terms of maturity in several categories. This industry has faced a rapidly evolving threat landscape over the past few years, which most likely inspired these gains.

Cloud Vulnerability Management

Cloud capabilities are definitely increasing. Last year, more than 50% of the organizations rated themselves at Level 1 or 2. This year, the number of respondents rating themselves a 1 dropped 15% from 28% down to 13%. Those ranking themselves at Level 3 (Defined) or higher increased 17% (to 65% this year from 48% last year). Cloud vulnerability management solutions have rapidly expanded in recent years. Many providers offer native solutions and many of the cloud security vendors have greatly improved their capabilities, which makes it easier for organizations to get better insight into the vulnerabilities in their cloud environments. See Figure 22 for this year's cloud vulnerability management rankings.



% Change (FY2021–FY2022)	2021	2022	% Change
Level 1	28.0%	13.1%	-14.9% ▼
Level 2	23.0%	21.9%	-1.1% ▼
Level 3	23.0%	36.1%	13.1% ▲
Level 4	16.0%	21.3%	5.3% ▲
Level 5	9.0%	7.7%	-1.3% ▼

Figure 22. Maturity of Cloud VM Overall

SANS sees a huge opportunity to mature even further in this area. Cloud operating environments are fully programmable so moving to Levels 4 and 5 should be even easier than in more traditional operating environments. For example, cloud-native alerting capabilities such as Amazon EventBridge and Azure Event Grid make it easy to create alerts that provide visibility into highly critical and time-sensitive issues. Also, big data capabilities make it faster and easier to generate valuable metrics and reports if those capabilities don't exist in the organization's traditional environments. Lastly, because IaaS assets and containerized applications are all created from images, organizations can move away from traditional scanning, patching, and configuration activities and focus on ensuring that teams are using current, approved images; continuously testing against these updated images; and automatically updating to approved images on a defined interval.

Summary and Final Recommendations

Based on the trends we see in this year's survey, things are looking up in the vulnerability management world. There's still work to be done, of course, but organizations have never had as much help as they do now. One way they can take advantage of this help is by strategically choosing to offload the responsibility for updating and configuring certain systems and applications to cloud providers by leveraging more platform and software as a service or serverless functions. On the application side, many organizations are already leveraging third-party libraries and frameworks to provide much of the needed functionality. This trend helps save time and effort by eliminating the need to scan, triage, and fix as much code. Security teams just need to make sure they proactively manage those supply chain vulnerabilities and are able to respond quickly when dangerous vulnerabilities are identified in the libraries they leverage. By shifting the responsibility for certain systems and software to others, organizations can focus more on the traditional asset types, where organizations need more visibility and control.

In addition to these third-party capabilities, the security industry has never had so many supporting technologies and services to help us succeed. No technology or service is perfect, but with the right support, many can provide substantial value to the organization. To really make a difference, however, an organization needs the right combination of people, process, and technology. The technologies might facilitate the gathering of data and can do some basic interpretation, but it is up to those of us on the front lines to really dig into the details to understand where the larger, more challenging problems exist. Then, we must work to find solutions. If the fix is manual and repetitive, we should look at improving our processes or automating the solution. If there is a gap in our technologies, we should work to close it either through customization or by working with the vendor to make improvements.

Through surveys like this one, SANS notes that organizations are incrementally improving year over year. Vulnerabilities will never cease to exist, but maybe in five to ten years, handling them will be business as usual. In order for that to happen, however, it will require not only maturing security capabilities, but also systems and software development and support capabilities. The advantage the industry has now is that there are organizations successfully managing vulnerabilities in systems and software at scale. Most of these companies are willing to share what they have learned, and some even provide software or services to help others manage their resources in a similar manner. Vulnerability management is hard but not impossible. Keep at it so we can see even more improvements in next year's survey.

Sponsor

SANS would like to thank this survey's sponsor:

VULCAN.