THE STATE OF VULNERABILITY MANAGEMENT

NOPSEC | www.nopsec.com

Introduction

Unremediated vulnerabilities are open doors that let malicious actors walk right through. Today, security teams are challenged enough by finding and shutting those open doors to keep their organization safe. Keeping track of those vulnerabilities and responding quickly and efficiently is one challenge—finding openings they might not even know about is another.

The future of vulnerability management is risk-based. Yet I often see that without a risk-based approach to prioritizing the ever-growing list of vulnerabilities, organizations leave themselves exposed. But how at risk are organizations really? Are security teams finding successful approaches to their vulnerability management, or are open doors around their attack surface inviting disaster into their organization?

In order to better understand organizational vulnerability management and gain some insights into the questions above, we surveyed 426 security professionals to discover and quantify their day-to-day challenges, frustrations, and priorities. What we found is that some organizations have effective ways to detect, respond to, and remediate their vulnerabilities, while other organizations have more blind spots than they think.

Let these insights be helpful to you as you evaluate and strengthen your vulnerability management program.

Lisa Xu
Nopsec, CEO

Key Findings

- **Prioritizing risk around exploitability and criticality is a top objective.** Other top objectives include identifying known vulnerabilities and gaining a clear picture of insider threats to their attack surface.

- **70% say their vulnerability management program (VMP) is only somewhat effective or worse.** Only 30% of respondents have a very effective VMP. 36%, said their program is at least somewhat effective, and 34% responded that their VMP was not very effective at all.

- **The top challenge is shadow IT.** Blind spots in the attack surface limiting visibility into total risk exposure is the top challenge for security teams. A lack of trained staff to remediate vulnerabilities is another top challenge.

- **Teams have insufficient threat intelligence.** 53% of respondents said their organization does not consume third-party threat intel, like penetration tests, vulnerability disclosures, and IP or domain reputation scores. 58% also do not use a risk-based rating system to prioritize vulnerabilities.

- **Vulnerabilities take too long to patch.** Only 18% said vulnerabilities require remediation within 24 hours of becoming known, and 62% of companies take 48 hours or longer—some more than two weeks—to patch known critical vulnerabilities.

- **There's a rise in vulnerabilities.** 58% of companies that track the volume of vulnerabilities have seen them double, triple, or quadruple over the past 12 months. Additionally, 22% reported the same level of vulnerabilities.

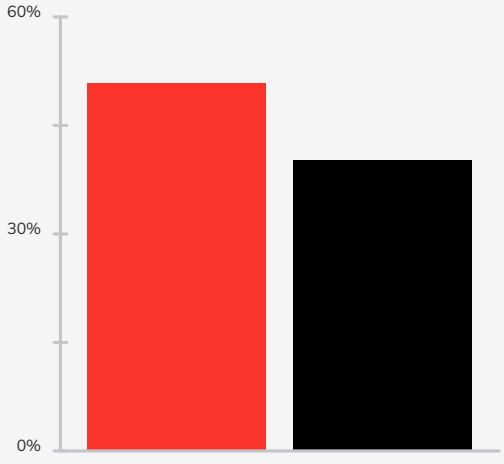
- **Attacks are more sophisticated than ever.** More than any other characterization, companies say they are seeing an increase in the sophistication of attacks. Additionally, security teams are seeing more DDoS attacks as well.

Table of Contents

Methodology and Participant Demographics

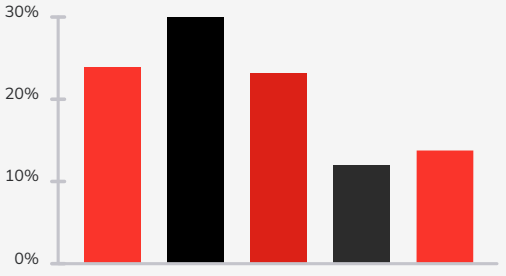
Starting on April 10, 2022, we surveyed 426 security professionals directly responsible for managing cyber vulnerabilities in their day-to-day work. The survey was conducted online via Pollfish using organic sampling. To provide greater context around the findings presented in this report, we offer more details about who we surveyed and the methodology used. Learn more about the Pollfish methodology *here*.

Gender



Male	55.8%
Female	44.1%

Age

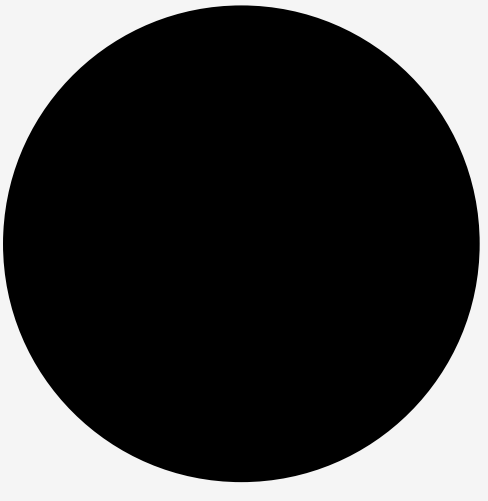


18 - 24	23.0%
25 - 34	30.0%
35 - 44	22.5%
45 - 54	11.2%
> 54	13.1%

Country

United States	100.0%

Employment Status

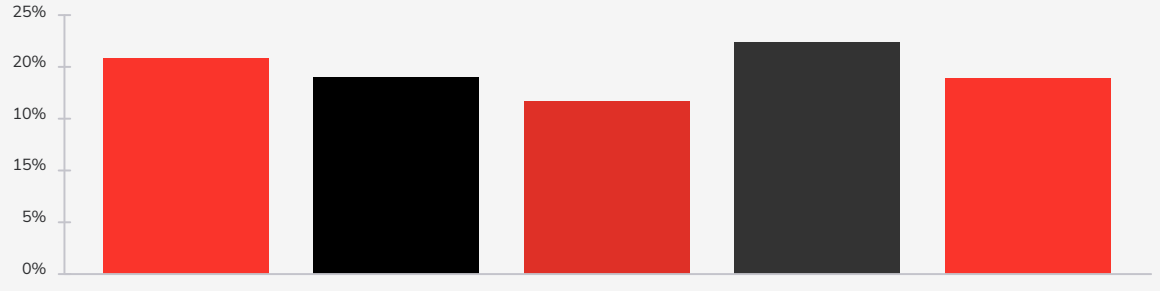


Employed for wages	100.0%

What industry does your company primarily operate in?

Financial services, insurance, real estate	10.0%
Higher education, K-12 education	10.5%
Non-profit	8.9%
Healthcare, biotech, pharma, medical	9.1%
Marketing, advertising, media	10.0%
IT, technology, software	9.6%
Manufacturing, warehouse, logistics	10.3%
State, local, federal government	10.3%
Military/Defense	10.8%
Other	10.0%

What best describes your job title/role?



Information Security Manager	20.6%
Chief Information Security Officer	19.4%
Cybersecurity Analyst	18.0%
Penetration Tester	22.5%
Other	19.2%

Have you had a vulnerability that led to a breach in the past 12 months?

The respondents to this survey are representative of a large cross-section of security professionals. Women's voices are well represented, representing 44.1% of the respondents. Typical of the security industry, 53.1% of our respondents are younger than 35, with the largest group being between 25 and 34.

Respondents are evenly represented from across nine major industries. From these industries, we received responses from CISOs, Information Security Managers, and Cybersecurity Analysts, with the plurality of 22.5% being Penetration Testers.

Now, with context around who our respondents were, let's take a closer look at what we uncovered.

PART#1

State of Vulnerability Management

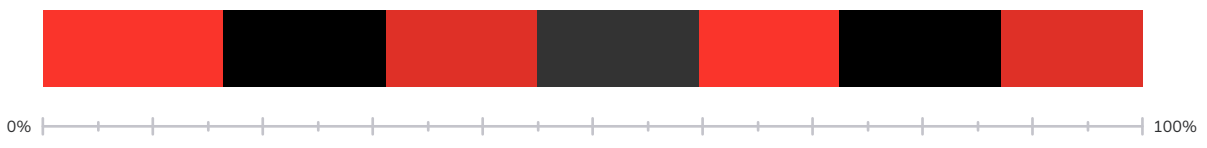
Identifying and remediating vulnerabilities across an organization is a security team's top priority, of course. But what approaches are they using to do so? This section seeks to shine a light on vulnerability management programs (VMPs) as they exist today, including the processes and tools the respondents currently use. We discover the objectives these security professionals have for their VMPs and highlight some of their challenges and frustrations.

The top objective for security practitioners is prioritizing risk.

At 35%, the number one objective for security professionals is to prioritize their vulnerability remediation and mitigation efforts based on the risk posed to the organization. How exploitable the vulnerability is and the criticality of the exposed assets would be the criteria used to establish their priorities.

As you would reasonably expect, vulnerabilities must be identified before teams can prioritize them, which is why the second largest segment (32.9%) of respondents listed vulnerability identification as their top objective. An equal number of respondents (32.9%) are also focused on understanding their attack surface for an insider threat.

- What would you say are the top objectives you are aiming to achieve with your Vulnerability Management Program?

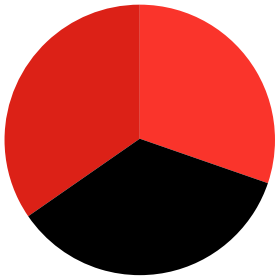


Prioritize risk based on those vulnerabilities that are exploitable and criticality of the assets	34.9%
Identify known vulnerabilities across the enterprise	32.8%
Understand the attack surface for an outside adversary	29.8%
Understand the attack surface for an insider threat	32.8%
Optimize the remediation workflow to minimize the chance of a breach	28.4%
Maintain metrics regarding the effectiveness of patch management	30.9%
Other	27.9%

70% of respondents say their VMP is only somewhat or not very effective.

When asked their impression of the overall effectiveness of their current vulnerability management program, 34% responded that it was not very effective. Slightly more, 35.9%, said their program was at least somewhat effective. Ultimately, less than a third (30.1%) of respondents have a very effective VMP.

- Overall, how effective would you say your current Vulnerability Management Program is?



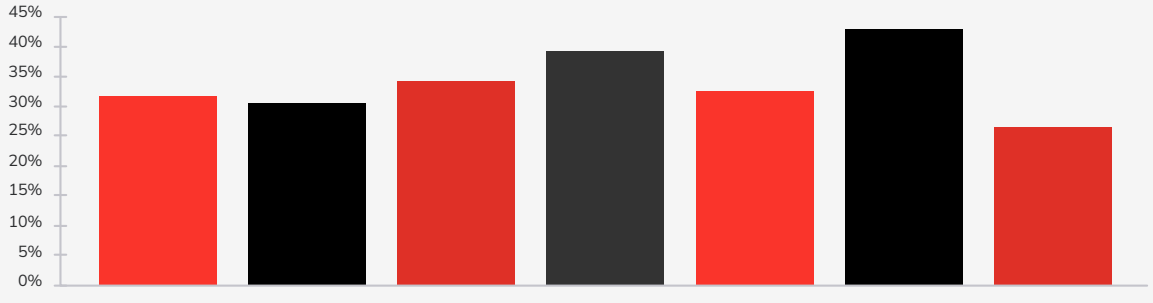
Very effective	30.0%
Somewhat effective	35.9%
Not very effective	34.0%

The top factor for VMP effectiveness is in-house talent.

For those above who replied that their VMP is “very effective,” could they give us insights on why they answered that way? When asked to choose all that applied, the top factor contributing (for 43%) to their effectiveness is their organization's in-house talent that understands vulnerability management. We applaud them for attracting and retaining top cybersecurity talent, but given the skills gap the security industry is experiencing, this response indicates a need for more automated vulnerability management solutions.

Other top factors include attributing their effectiveness to their tech stack (38.3%), and to the strength of their written organizational policies about vulnerability management (34.4%).

• What would you say are the top factors that make your Vulnerability Management Program so effective?



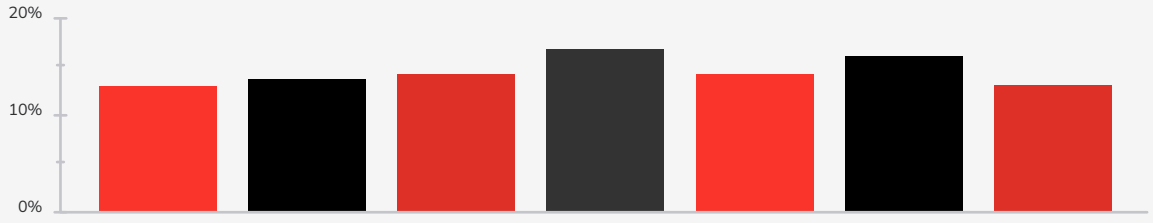
Taking a risk-based approach to prioritization	31.2%
Executive support and buy-in	30.4%
Written organizational policies about vulnerability management	34.3%
Our vulnerability management tech stack	38.2%
Visibility into assets and the ability to scan the entire attack surface	32.0%
In house talent that understands vulnerability management	42.9%
External consultant support for vulnerability management	25.7%

The number one challenge with vulnerability management is shadow IT assets.

More than any other challenge, shadow IT limiting the visibility of risk exposure was cited by the largest segment of respondents (16.9%) as their most vexing problem. Additionally, 16.2% mentioned a lack of trained staff to remediate vulnerabilities as another top challenge. 13.9% cited having no executive support or requirements for

assets to be scanned for vulnerabilities and an additional 13.9% cited IT not taking action on vulnerabilities discovered or poor patch management practices as other challenges.

- When it comes to vulnerability management what would you say is your #1 challenge?



Inability to prioritize / triage vulnerabilities based on asset criticality, number of exposures, and level of risk to the environment	12.9%
Limitations of the vulnerability management tool(s)	13.3%
No executive support or requirements for assets to be scanned for vulnerabilities	13.8%
Shadow IT assets/blind spots in our attack surface that limit visibility of our total risk exposure	16.9%
IT not taking action on vulnerabilities discovered / poor patch management practices	13.8%
Lack of trained staff to effectively make progress in remediating our overload of vulnerabilities	16.2%
Scanning activity taking systems offline or creating other accessibility issues	12.9%

Top three types of vulnerability scanning are servers, applications and code, and IoT/OT devices.

What type of vulnerability scanning are security teams currently performing? The results were almost evenly split, with respondents replying with servers and applications and code as what they're scanning the most (with 34% each). An additional 33.8% are also primarily scanning for IoT and OT devices.

- What type of vulnerability scanning are you currently performing?

Desktops/laptops	32.1%
Network infrastructure devices (routers, switches, etc.)	33.3%
Servers	34.0%
Applications and code	34.0%
IoT / OT devices	33.8%
Cloud assets	33.5%

Half of organizations use crowdsourcing or bug bounties.

When asked if they do any crowdsourcing or offer a bug bounty program to identify vulnerabilities in their environment, slightly over half (50.9%) said they do. Interestingly enough, for those who have a crowdsourcing or bug bounty program, only half (51.6%) replied above that they have a formal vulnerability disclosure program.

- Does your organization do any type of crowdsourcing or bug bounty programs to identify vulnerabilities in your environment?

Summary

The state of vulnerability management in organizations today is lacking in several significant areas. Besides a general sense that their VMP is ineffective, respondents report that they struggle to combat shadow IT and gain a clear picture of the organization's attack surface. The top objective is to devise a method to prioritize vulnerabilities based on the risk they present to the organization.

Our respondents indicate they would like to see improvement in two areas: finding a better way to associate vulnerabilities with risk and an effective method for accurately identifying the attack surface. Now, let's turn our attention to the state of the threat landscape as perceived by security professionals.

PART#2

State of the Threat Landscape

With the insights into the state of vulnerability management at the organizations of our respondents, it’s time to understand our respondents' threat landscape a bit more. What types of threats are they facing, how have those threats changed, and how are they currently managing vulnerabilities with the tools and approaches they have? Some interesting insights around how these companies make security decisions emerge as well.

Most organizations do not use third-party threat intelligence sources.

We asked our respondents if they leverage any third-party vendors to provide threat intelligence data through, for example, penetration tests, vulnerability disclosures, proprietary data on the dark web, and IP or domain reputation scores. A surprising 52.8% said they do not look to outside sources for information about threats.

- Do you leverage any third party vendors to provide threat intelligence data for your organization (e.g., pentests, vulnerability disclosures, proprietary data on the dark web, IP or domain reputation score, etc.)?

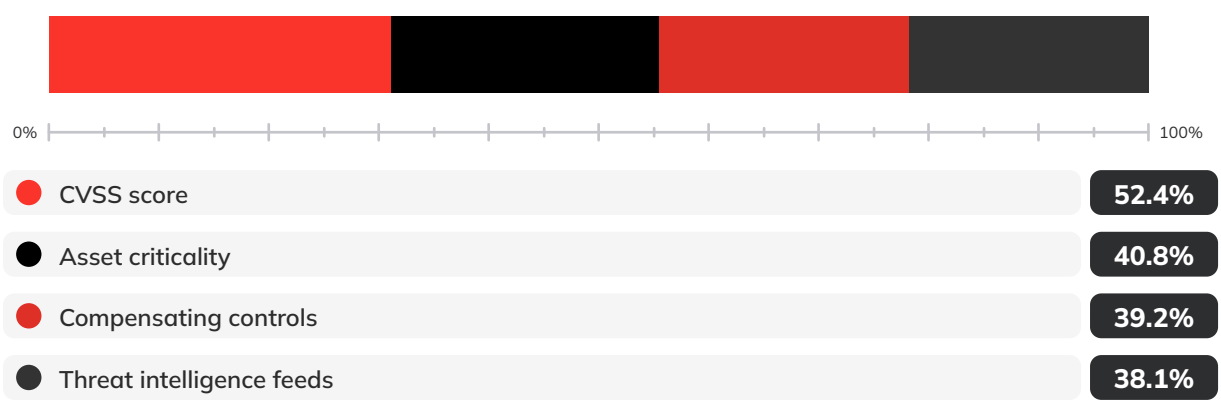
Most organizations don't risk-rate vulnerabilities.

57.5% of respondents also indicate that their company does not use a risk-based rating system to prioritize vulnerabilities. A reasonable conclusion is that these firms simply remediate all vulnerabilities in a first-identified-first-remediated fashion. Given today's overload of vulnerabilities, it is doubtful that this method is effective for all but the smallest organizations.

- Does your organization rate the risk of vulnerabilities?

Of those who rate the risk of vulnerabilities, here are the tools they use.

- What factors does your organization use to rate risk?



Few organizations prescribe how quickly vulnerabilities are to be patched.

The amount of time that an individual vulnerability can exist within a network or application until it must be remediated is generally a function of the risk posed by the vulnerability. Only 28.2% of respondents indicate that their organizations have documented service level agreements (SLAs) to designate how quickly vulnerabilities are to be remediated. Understandably, organizations that do not use a risk-based prioritization scheme would struggle to construct meaningful SLAs.

- Does your organization have documented service level agreements (SLAs) to designate how quickly vulnerabilities should be patched?

62% of companies take 48 hours or longer—some more than two weeks—to patch known critical vulnerabilities.

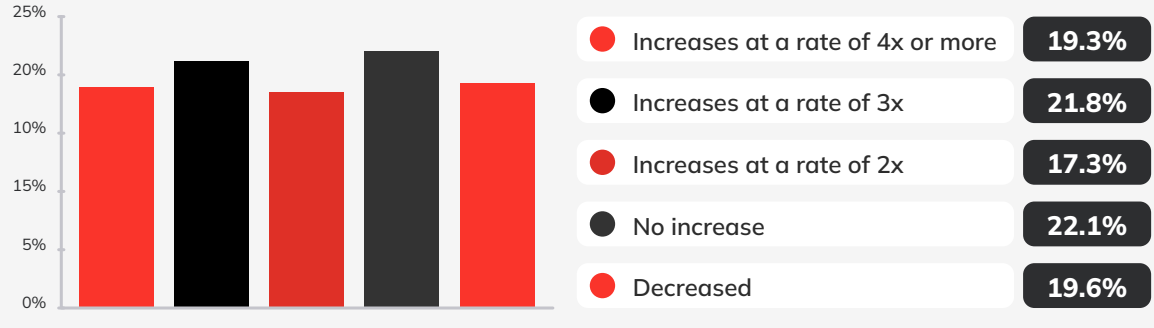
The plurality of respondents (20.4%) say they require critical vulnerabilities to be patched within 48 hours of when they are identified. Only 17.8% said these CVSS 9.0 and above vulnerabilities require remediation within 24 hours of becoming known, and 13.62% let them languish for up to two weeks.

- How quickly does your organization require critical vulnerabilities (CVSS of 9.0 and above) to be patched after they have been identified?

58% of companies that track the volume of vulnerabilities have seen them double, triple, or quadruple over the past 12 months.

When asked if the volume of vulnerabilities has increased in the past 12 months, only 22.2% of those that track volume changes reported no increase, with 19.6% saying they saw a decrease. The remaining 58.2% experienced a rise in this period—some as much as fourfold.

- How has the volume of security vulnerabilities changed over the past 12 months?



The sophistication of attacks is increasing more than any other type or attribute.

When asked how they would describe the type of threats they see in their organization, all the likely suspects—zero-day, malware, phishing, and DDoS—all received significant nods. But the largest group of respondents (38%) said that they noticed an increase in the level of sophistication of attacks more than any other characteristic. The number of DDoS attacks was mentioned as a close second, with 34.7% making that observation.

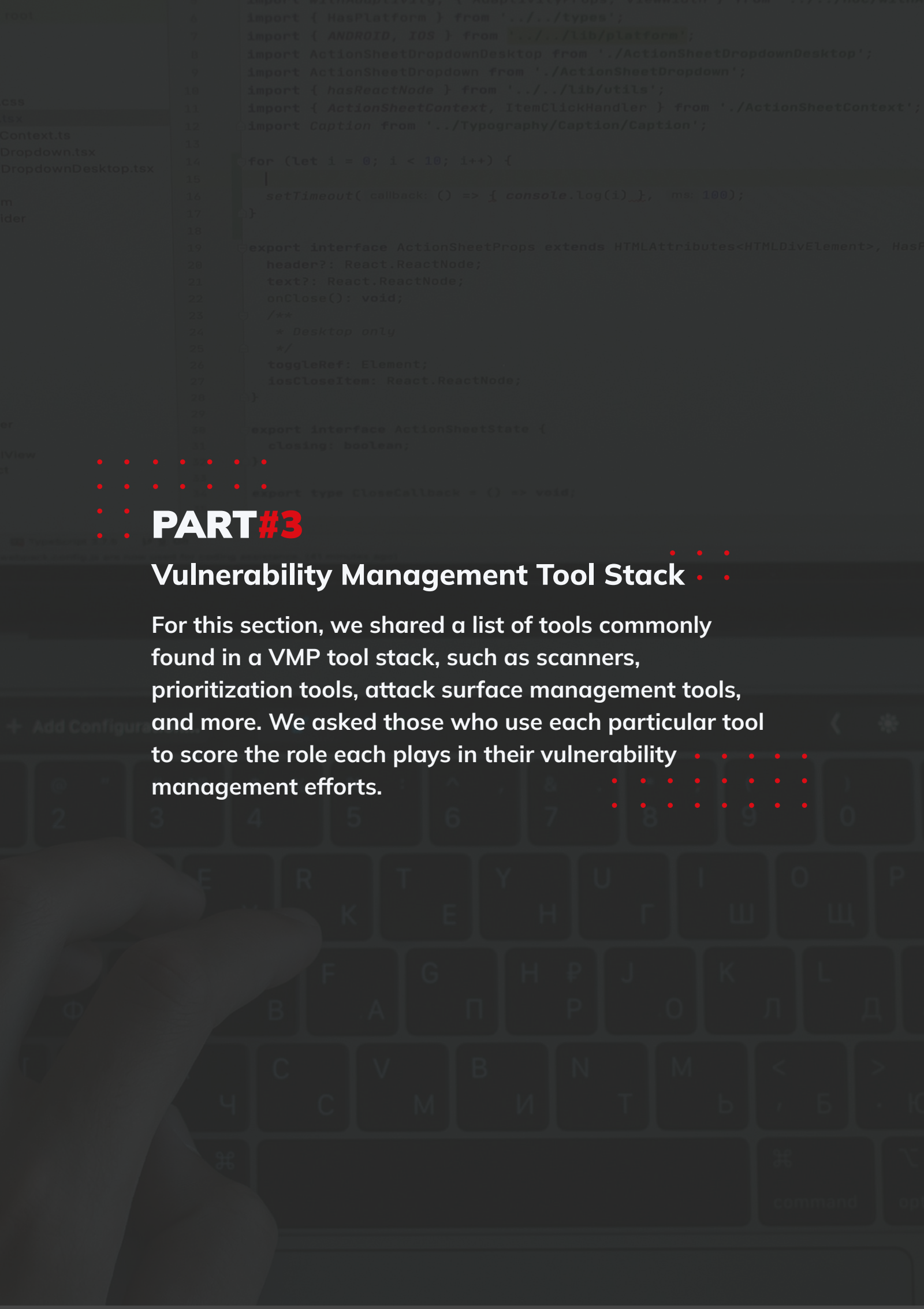
- How would you describe the type of threats you are seeing in your organization?

There has not been a noticeable change in the type of threats we are seeing	33.5%
The sophistication of attacks is increasing	38.0%
We are seeing an increased number of zero day attacks	32.1%
We are seeing an increased number of malware attacks	29.5%
We are seeing an increased number of phishing attacks	33.1%
We are seeing an increased number of DDoS attacks	34.7%

Summary

Even though vulnerabilities are on the rise and the sophistication of attacks is increasing, most organizations still don't risk-rate vulnerabilities, rely on outside threat intelligence, or dictate how quickly vulnerabilities must be patched. These are not sustainable omissions for modern organizations facing an increasingly severe threat landscape.

In our next section, we'll take a closer look at the tools organizations use to manage vulnerabilities.



PART#3

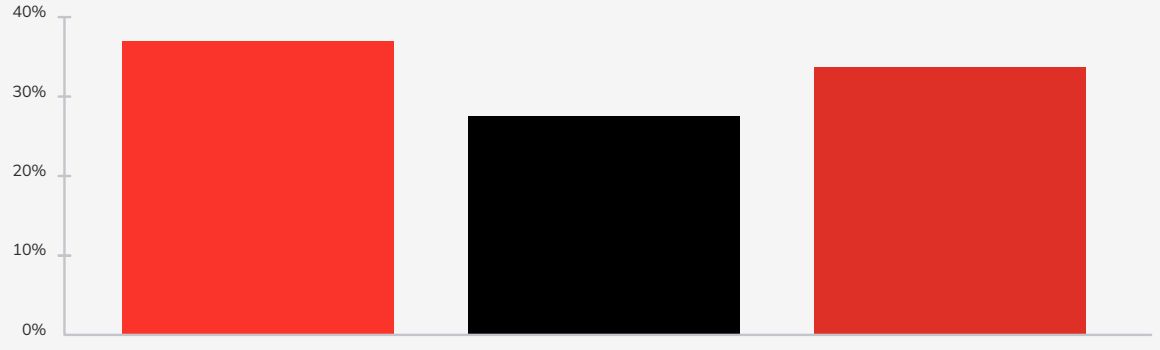
Vulnerability Management Tool Stack

For this section, we shared a list of tools commonly found in a VMP tool stack, such as scanners, prioritization tools, attack surface management tools, and more. We asked those who use each particular tool to score the role each plays in their vulnerability management efforts.

38.2% consider vulnerability scanning tools a major component of their vulnerability management program and rely on it daily.

Conversely, 34.6% say the tool is a minor component of their program and depend on it ad hoc.

• Please score the role the following tools play in your work to manage vulnerabilities: your vulnerability scanner tool



This tool is a major component of our VM program and we rely on it regularly (daily/weekly)	38.2%
This tool is a moderate component of our VM program and we rely on it infrequently (monthly/quarterly)	27.2%
This tool is a minor component of our VM program and we rely on this tool in an ad hoc fashion	34.6%

36.9% view their vulnerability prioritization technology as a major component of their vulnerability management program and rely on it at least weekly.

30.1% see their vulnerability prioritization technology as a minor component of their overall program.

• Please score the role the following tools play in your work to manage vulnerabilities: your vulnerability prioritization technology tool

This tool is a major component of our VM program and we rely on it regularly (daily/weekly)	36.9%
This tool is a moderate component of our VM program and we rely on it infrequently (monthly/quarterly)	32.9%
This tool is a minor component of our VM program and we rely on this tool in an ad hoc fashion	30.1%

36.4% use their attack surface management (ASM) tool regularly and consider it a major component of their vulnerability management program.

29.9% are using their ASM on an ad hoc basis and consider the tool a minor component of their program.

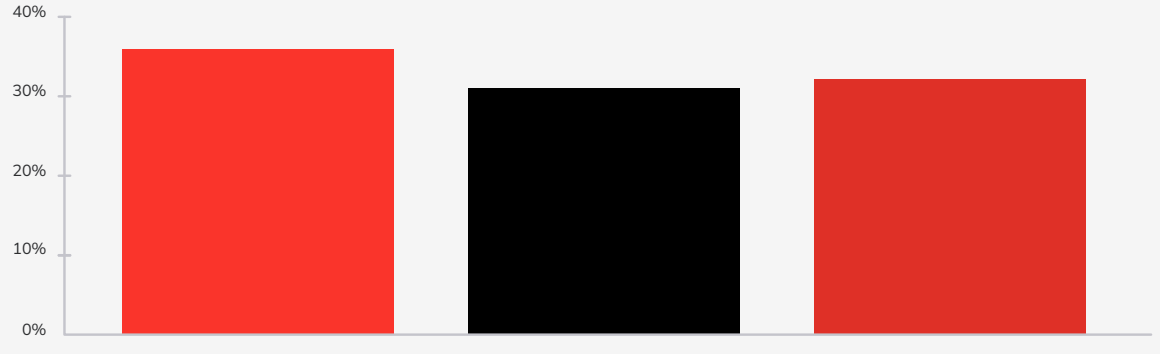
- Please score the role the following tools play in your work to manage vulnerabilities: your attack surface management Tool

This tool is a major component of our VM program and we rely on it regularly (daily/weekly)	36.4%
This tool is a moderate component of our VM program and we rely on it infrequently (monthly/quarterly)	34.5%
This tool is a minor component of our VM program and we rely on this tool in an ad hoc fashion	29.9%

36.7% consider their breach and attack simulation tool a major component of their vulnerability management program.

31.9% don't view their breach and attack simulation tool as a critical component and only use it on an adhoc basis.

- Please score the role the following tools play in your work to manage vulnerabilities: your breach and attack simulation (BAS) tool

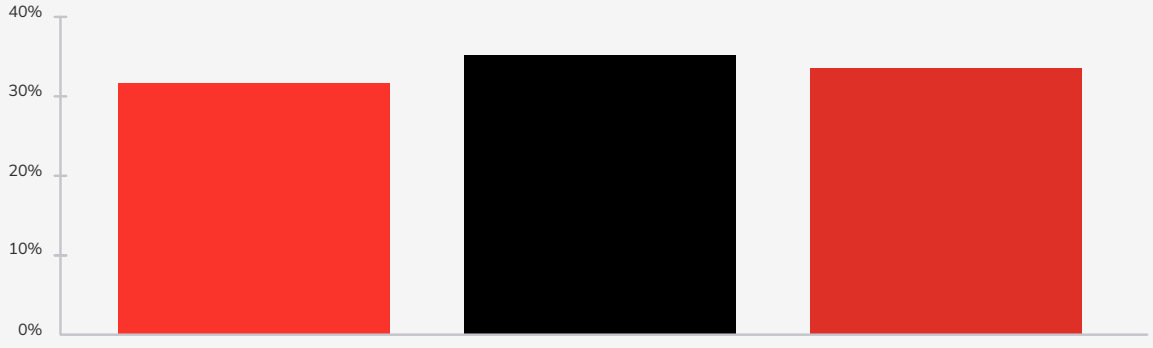


This tool is a major component of our VM program and we rely on it regularly (daily/weekly)	36.7%
This tool is a moderate component of our VM program and we rely on it infrequently (monthly/quarterly)	31.3%
This tool is a minor component of our VM program and we rely on this tool in an ad hoc fashion	31.9%

31.5% say their security orchestration and automated response (SOAR) tool is a major component of their vulnerability management program.

33.3% say the tool is a minor component of their overall program.

- Please score the role the following tools play in your work to manage vulnerabilities: your security orchestration and automated response (SOAR) tool



This tool is a major component of our VM program and we rely on it regularly (daily/weekly)	31.5%
This tool is a moderate component of our VM program and we rely on it infrequently (monthly/quarterly)	35.2%
This tool is a minor component of our VM program and we rely on this tool in an ad hoc fashion	33.3%

36.9% use their threat intelligence (TI) tool regularly and consider it a major component of their vulnerability management program.

33.5% use their TI sporadically and consider the tool a minor component of their program.

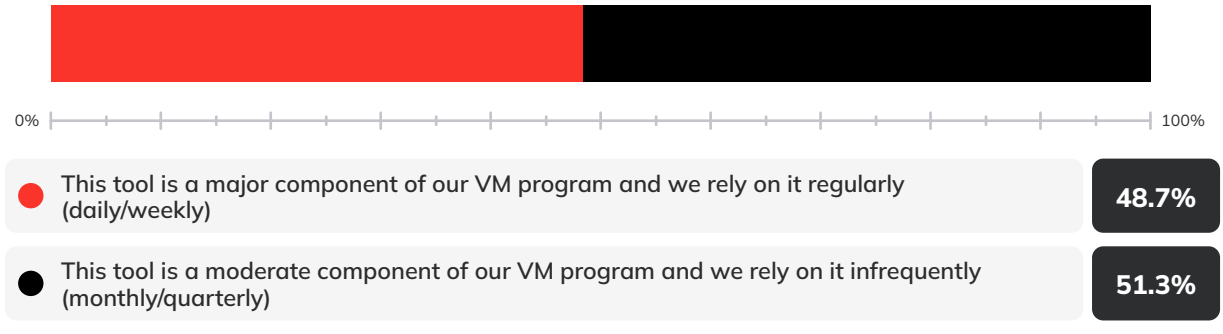
- Please score the role the following tools play in your work to manage vulnerabilities: your threat intelligence tool

This tool is a major component of our VM program and we rely on it regularly (daily/weekly)	36.9%
This tool is a moderate component of our VM program and we rely on it infrequently (monthly/quarterly)	29.5%
This tool is a minor component of our VM program and we rely on this tool in an ad hoc fashion	33.5%

48.7% score their extended detection & response (XDR) and endpoint detection and response (EDR) and network detection and response (NDR) tools as major components of their vulnerability management program.

51.3% score their XDR, EDR, and NDR tools as moderate components and rely on it infrequently.

- Please score the role the following tools play in your work to manage vulnerabilities: your extended detection & response (XDR) or endpoint detection & response (EDR) and network detection & response (NDR) tool



Summary

The choice that earned the description "a major component of the VM program..." more than any other is extended detection & response (XDR), endpoint detection & response (EDR), and network detection & response, with 48.7% of respondents giving this the best possible mark.

This response is notable because it indicates that respondents are taking a more reactive approach to vulnerability management than proactive. The technologies selected focus on the response to a security event. Instead, the focus should be placed on proactive remediation, helping prevent events before they happen. VPT tools are best leveraged for this more modern approach

Contrarily, SOAR received the fewest "major component" nods.

PART#4

Plans and Priorities For the Future

An organization needs to not only have the tools and approaches to stay safe today, but also needs to build scalable and efficient strategies for the future. From new tools to additional staff to how they expect their budgets to change, let's look at future plans, priorities, goals, and expectations of our respondents.

The priority for the next year is to purchase a new tool or upgrade their current tool.

The largest group (16.9%) said the number one priority for their VMP over the next 12 months is purchasing a new tool or upgrading their existing vulnerability assessment tool they already have. Because they too will need new tools, two of the other choices—increasing enterprise visibility for 100% scanning (14.8%) and adding breach attack simulation (BAS) capabilities (12.4%)—will likely put these respondents in the "purchasing new tools" category as well.

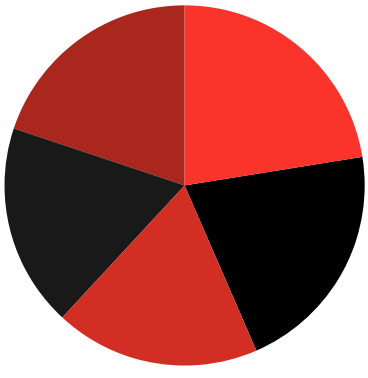
- What would you say is your #1 priority of your vulnerability management program over the next 12 months?

Purchasing a new tool or upgrading the existing vulnerability assessment tool	16.9%
Hiring additional staff trained in vulnerability management	13.6%
Increasing enterprise visibility for 100% scanning coverage of on-premise and cloud assets	14.7%
Adding breach attack simulation capabilities	12.4%
Implementing baseline security configurations and scanning for compliance	13.3%
Improving executive-level communications and reporting for vulnerability and risks	14.5%
Other	14.3%

43% feel that hiring more people will make their program more effective.

A plurality of 21.8% said that adding staff to the VMP would have the most impact on the program's effectiveness going forward. An additional 20.9% feel the same way, but will be looking for consultants or contractors rather than FTEs to fill those roles.

- To make your vulnerability management program more effective, what would have the most impact?

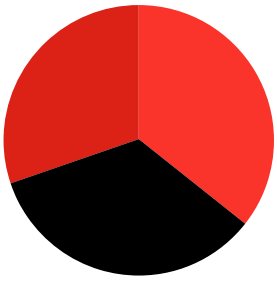


Adding staff to the vulnerability management program	21.8%
Hiring consultants or contractors to improve the program	20.8%
Maturing our program by implementing SLAs, written policies, and metrics	18.5%
Faster patching and mitigations implemented by IT operations	18.3%
Bringing in new technology capabilities (e.g., new vulnerability assessment tools, penetration testing tools, automation)	20.4%

Budgets are expected to increase.

When asked how their budget for vulnerability management will change over the next 12 months, 36.6% of those involved in budget-related decisions foresee an increase. Surprisingly, 29.3% of that group expect their budget to shrink.

- How is your budget for vulnerability management going to change over the next 12 months?

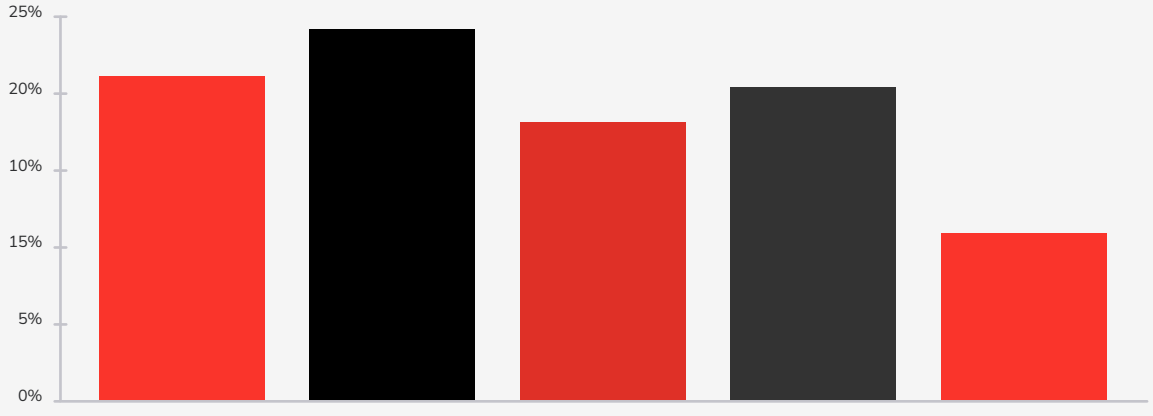


Budget will increase	36.6%
Budget will stay the same	34.0%
Budget will decrease	29.3%

Over three-quarters expect a budget increase of at least 26%.

The results were optimistic when we asked those who expect a budget increase in the next 12 months to speculate how much that increase might be. The largest group of 24.4% expects modest growth of 26% to 50%, but only 21.7% expect anything less than that. 15.7% are looking forward to a 100% increase or more.

- By what percentage will it increase?

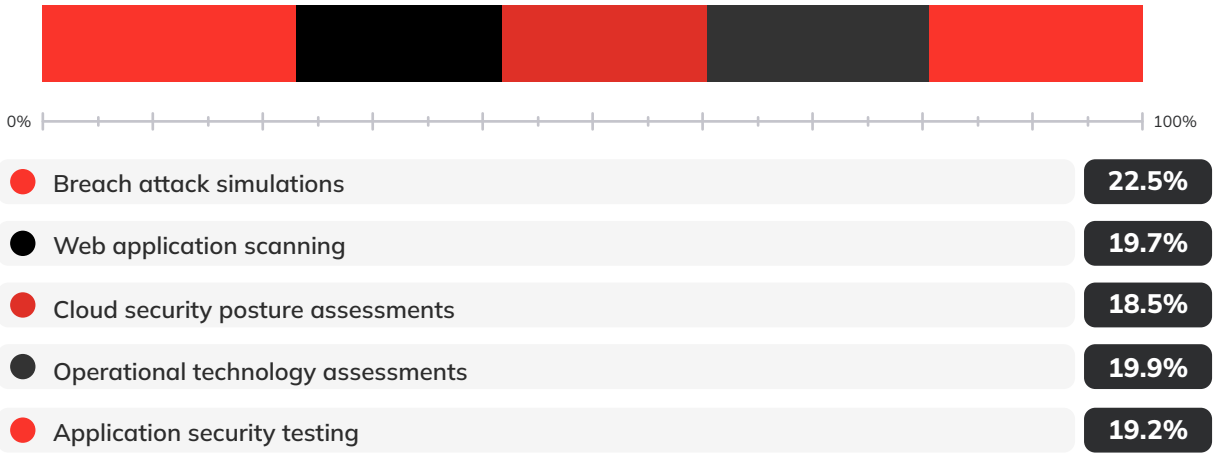


25% or less	21.7%
26% - 50%	24.3%
51%- 75%	17.3%
76% - 100%	20.8%
100% or more	15.6%

Many are intrigued with breach attack simulation.

For 22.5% of respondents, breach attack simulations were the most interesting or promising vulnerability management technology. Operational technology assessments were the number two choice (20%), followed by web application scanning (19.7%).

- What vulnerability management technologies are most interesting to you/most promising?



Summary

Overall, it is fair to say that organizations are optimistic in their plans and expectations for their VMP going forward. They expect to purchase new or upgrade their existing tools, are looking to hire more people, and expect budgets to increase as well. The largest groups answered each question in this section from a positive perspective.

PART#5

Takeaways

The security professionals surveyed here have certainly provided a number of insights into how prepared—or unprepared—organizations are when it comes to detecting and addressing their vulnerabilities. Below are some takeaways that will be vital to organizations in their journey to increase the effectiveness of their VMP.

Risk-based prioritization is vital.

The simple reality is that not all exposures are created equal. The same vulnerability can represent a greater or lesser risk even from one organization to another. Risk scores will vary depending on the criticality of the assets exposed and a host of other variables as well.

The only way cybersecurity defenders can ever hope to transition from a reactive approach to vulnerability management to a proactive one is to adopt a risk-based vulnerability management (RBVM) program.

The status quo is not cutting it.

This survey makes it clear that enterprises don't move as fast as the available technology. How things are done today will not be sufficient to defend against tomorrow's challenges, and preparing for an uncertain future requires leadership with foresight today.

By their answers, many of our respondents signaled that they are drowning in vulnerabilities without an effective, structured way to manage them. Yet those respondents experiencing success are doing so because they have learned to prioritize vulnerabilities according to the risk they pose to their organization.

Attack surfaces are more complex than ever before.

Organizations need a tool that takes inventory of all the various kinds of assets in their environment and routinely seeks to discover new ones. Growing and decentralized harder-to-account-for attack surfaces prove the validity of the adage, "You cannot protect what you don't know about." Your risk profile will be more comprehensive and accurate when you know where attackers are more likely to find success.

Today's varying combinations of IT infrastructures—On-Prem, Cloud, and Hybrid—bring their own unique vulnerabilities to be stack racked and remediated. Only an RBVM approach can make sense of these various environments and provide a clear remediation path forward.

Teams are experiencing a tsunami of vulnerabilities, and the increase in volume will continue.

Many of our respondents are experiencing a vulnerability overload where CVEs alone don't provide all of the necessary prioritization context to take actual meaningful remediation actions. For many companies, promptly addressing all known vulnerabilities is not an option. Only a risk-based prioritization scheme will enable them to maximize the effectiveness of the vulnerability management resources available to them.

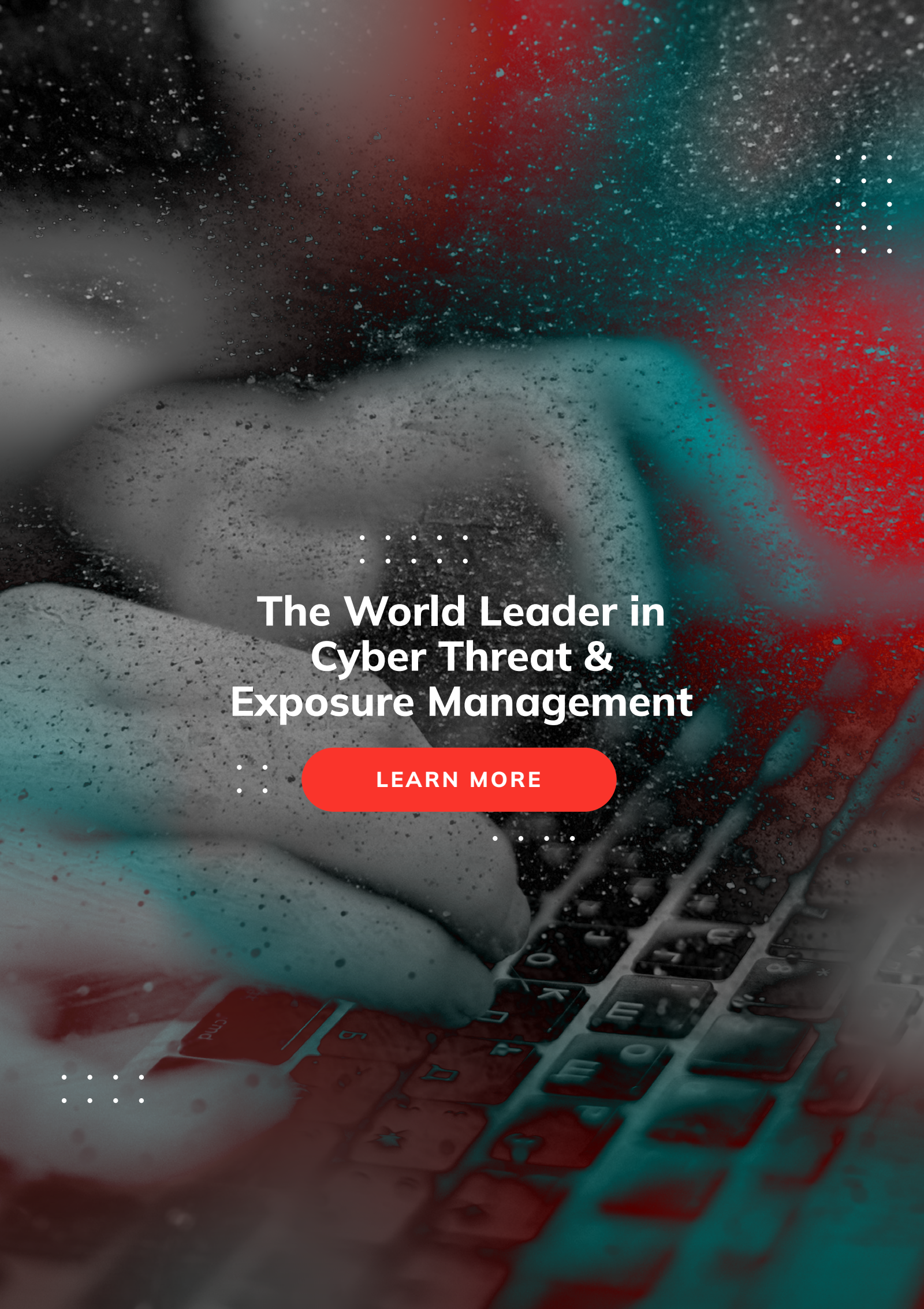
Sophisticated attacks require sophisticated solutions.

Vulnerability management is not a job performed effectively by just one piece of technology. Sophisticated protection that meets modern security challenges will include inputs from a scanner tool, threat intelligence feeds, an EDR solution, ASM, and BAS technology, all aggregated together.

A successful RBVM program leverages technologies that play well together. The more you can feed into one centralized platform, the better. When you avoid working in separate systems, it simplifies the workflow of security teams, saving time and energy.

Conclusion

The job doesn't end at just prioritizing vulnerabilities, because a vulnerability is still a vulnerability until it is remediated and mitigated. True RBVM bridges the gap between Security Teams and IT Ops to do just this. The best way to facilitate this bridge is to ensure that your RBVM platform integrates with your IT Ops team's information technology service management (ITSM) solution to create and send tickets. Go a step beyond by building mutually accountable SLAs for both the security team and the IT Ops team to ensure everyone knows what is expected and what success or failure looks like. This is the only way to prepare for the future of cybersecurity.


The World Leader in
Cyber Threat &
Exposure Management
LEARN MORE