STATE OF THREAT DETECTION & RESPONSE

www.panther.com

panther

Introduction

With data breaches at an all-time high and the ways in which malicious actors go after organizations getting increasingly sophisticated, security teams are facing unprecedented challenges in securing their organizations.

Adding to the challenges for security teams, threat detection and response can be hampered by tools that haven't evolved to handle the massive amount of data generated by today's cloud infrastructure and applications. Teams may also be hindered by server-based architectures that require significant operational overhead in order to handle large volumes of data (if they can at all), or by a lack of automation that makes processes too manual and inefficient. Teams may also be falling behind due to high volumes of alerts and false positives, leading to alert fatigue and burnout.

We wanted to gain insights into the experience of security teams who are at the helm of their organization's detection and response operations and uncover more about what they experience each day. Do they feel their current processes and tools are effective? What are their biggest challenges? What improvements do they want to make going forward? We surveyed over 400 security engineers and analysts to understand the current state of detection and response.

Key Findings

Here are some of the insights we gained into the state of threat detection:

- **The biggest challenge is efficiency.** Most respondents say efficiency issues, like time wasted on false positives and a lack of efficient processes, are their biggest challenges today.
- **Automation would make them more effective.** They believe that automating manual tasks would have the greatest impact on making security operations more efficient.
- **Over the last 12 months, 48% have seen a 3x increase in the number of alerts per day.** This is an alarming growth rate, and for teams already stretched thin, this rate of increase exacerbates an already problematic situation.
- **Over 50% find that at least half of alerts are false positives.** Managing a high volume of false positives is contributing to alert fatigue, and impacting security teams' ability to focus on more high-value tasks.
- **55% have built their own detection and response tool, but less than half found it to be highly effective.** The need to build their own tools likely stems from dissatisfaction with the tools available, so they're taking on the momentous task of building their own when no commercial offerings can do the job.

Table of Contents

Profile of Who We Surveyed

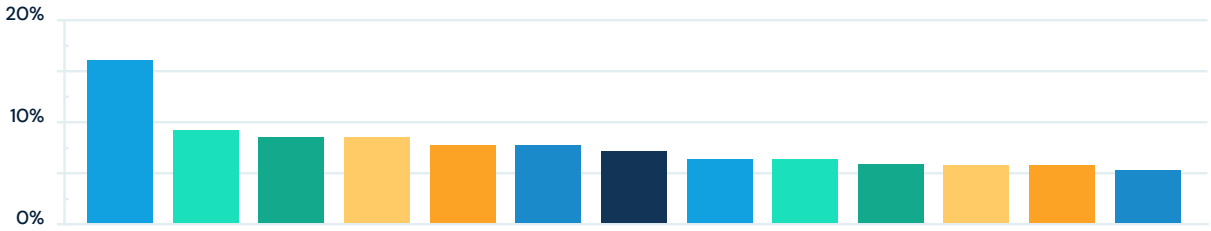
PART 1

We designed this survey to reflect the “boots on the ground” perspective for security organizations. To achieve this purpose, we limited the pool of respondents to active security practitioners, primarily security analysts, and security engineers.

What best describes your job title?

Security engineer	54.8%
Security analyst	45.2%

What industry does your company primarily operate in?

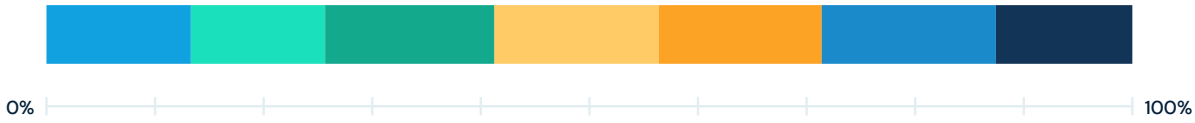


Technology	15.2%
Retail	9.3%
Finance	8.1%
State/Local Gov	8.1%
Utilities/Energy	7.6%
Education	7.6%
Healthcare	7.3%
Services	6.6%
Hospitality	6.6%
Manufacturing	6.3%
Insurance	5.9%
Federal	5.6%
Other	5.4%

What best describes the size of the company you work for?

Small business	Medium business	Large business	Major Corporation
1-100 Employees	100-999 Employees	1,000-10,000 Emp.	10,000+ Employees
24.3%	**30.9%**	**21.6%**	**23.1%**

How many people are on your security team?



1 - 3	12.5%
4 - 10	12.5%
11 - 20	15.7%
21 - 30	15.0%
31 - 40	14.3%
41 - 50	15.7%
51+	14.3%

Would you describe the company you work for as a cloud-first organization? *[Cloud-first definition: the company has only ever existed within the cloud from its inception - not a company with a cloud-first strategy.]*

Yes	41.0%
No	32.6%
I don't know	26.2%

Current State of Threat Detection & Response Programs

PART 2

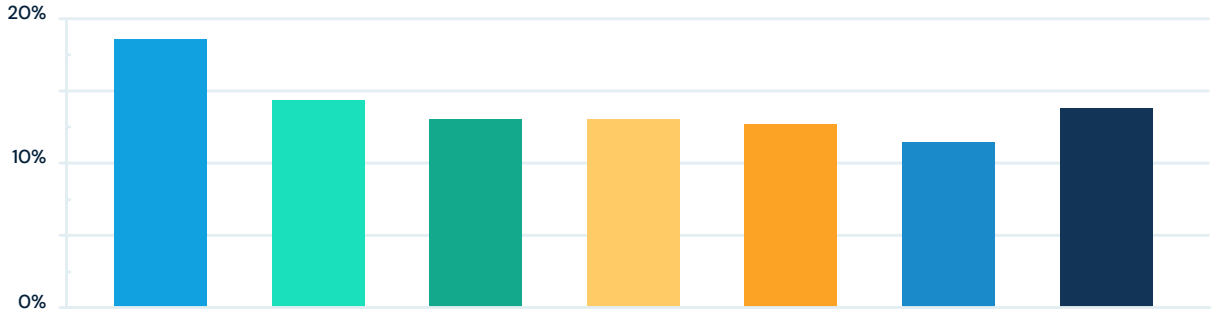
We wanted to capture and understand the means and methods of current threat detection and response programs. We were interested in finding out what practitioners believe would help them be more effective, what changes they have made, and what they would still like to change.

Reducing mean time to response is the #1 priority for detection and response programs

When asked what they feel is the top priority of their current threat detection and response program, the number one answer, at 17.9%, was to reduce mean time to response (MTTR). MTTR, or the average time needed to return a system to operational condition after receiving notification of a failure or attack, is a metric that many organizations use to assess the efficiency of their program.

14.7% replied that their next priority is to decrease the cost of incidents, followed by threat hunting at nearly 13.8%.

What would you say is the top priority of your current threat detection and response program?



Reduce mean time-to-response	17.9%
Decrease cost of incidents	14.7%
Threat hunting	13.7%
Optimize SOC operations	13.7%
Work unrelated to threat detection and response	13.2%
Shift to proactive detection	12.2%
Other	14.2%

Efficiency-related challenges are a top concern

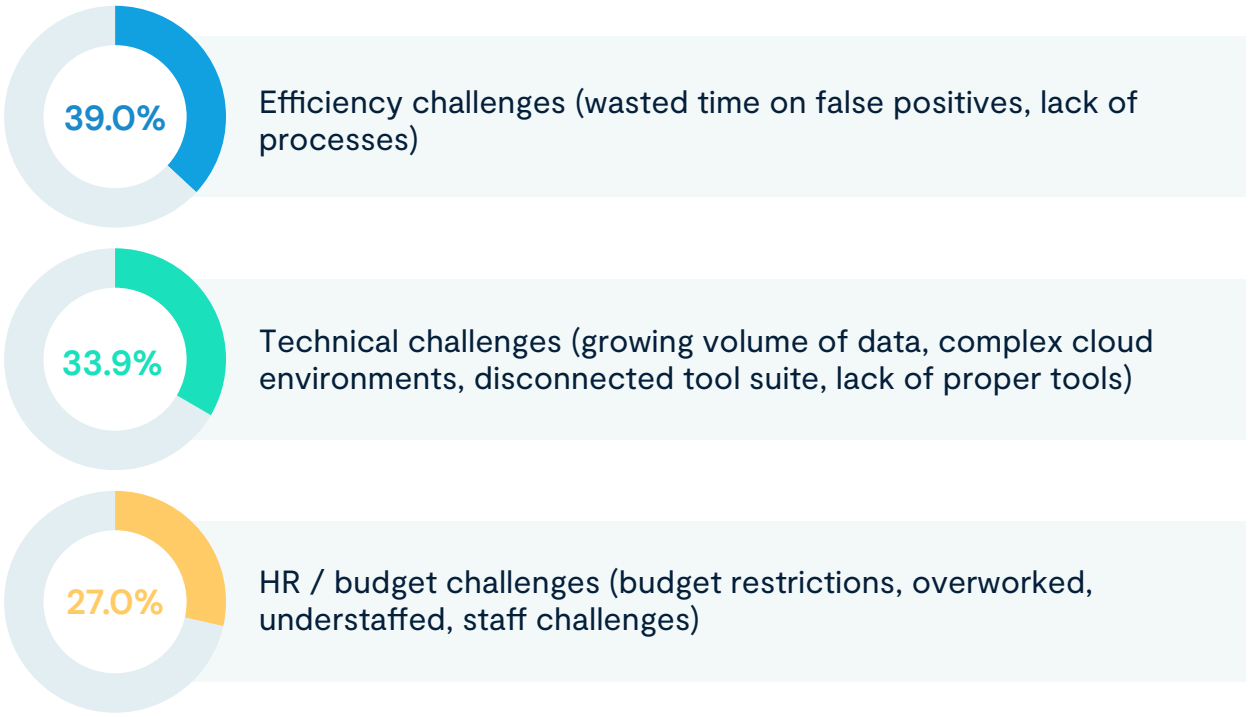
After exploring top priorities, we also asked respondents about the top challenges facing their threat detection and response programs.

The largest segment of our respondents (39.1%) feel that their top challenges are efficiency issues, such as time wasted on false positives and a lack of efficient processes.

However, the second largest segment at 33.9% see their top challenges as being technical: the growing volume of data, complex cloud environments, lack of proper tools, and more.

Finally, the remaining segment (27%) sees their challenges as related to staffing and budget, as they contend with budget restrictions, overworked employees, and understaffed teams.

Which of the following do you consider to be the top challenges of your threat detection and response program?



Only 41% of respondents categorized their detection and response program as “very effective”

Significantly less than half of respondents expressed a high degree of confidence in their detection and response program, with 26.8% of security professionals stating that they do not feel their security program is very effective. This is a significant concern given the critical role of information security in ensuring business continuity.

The number of cyberattacks against companies in all sectors is growing rapidly. If security practitioners are worried about their ability to keep their company safe in the current environment, it’s imperative for leadership to take notice, understand the challenges, and work to provide greater resourcing and support.

Overall, how effective would you say your current detection and response program is?

Very effective	41.3%
Somewhat effective	31.9%
Not very effective	26.8%

28% of respondents would not be surprised if they saw their company in the news for a breach

When asked if they would be surprised if they saw their company in the news for a breach, a concerning 28% said they would not be surprised. This aligns closely to the 27% from the previous question who stated that they did not feel their detection and response program was effective. Similarly, the percentage who would be very surprised or somewhat surprised also aligned closely with the percentages who felt their security programs were very or somewhat effective.

In 2020, ***TechRepublic*** reported that as many as 65% of companies worldwide experienced an operational technology system intrusion within the previous year.

Additionally, the *ITRC* found that in 2021, there were 1,862 compromises consisting of data breaches, exposures, and leaks — which is 68% higher than 2020, and the highest number of compromises since 2015.

The growing number of cyber attacks against businesses today should give organizations reason to take these risks seriously and evaluate the resources they are devoting to effectively enable their security teams.

How surprised would you be if you saw your company in the news for a security breach?

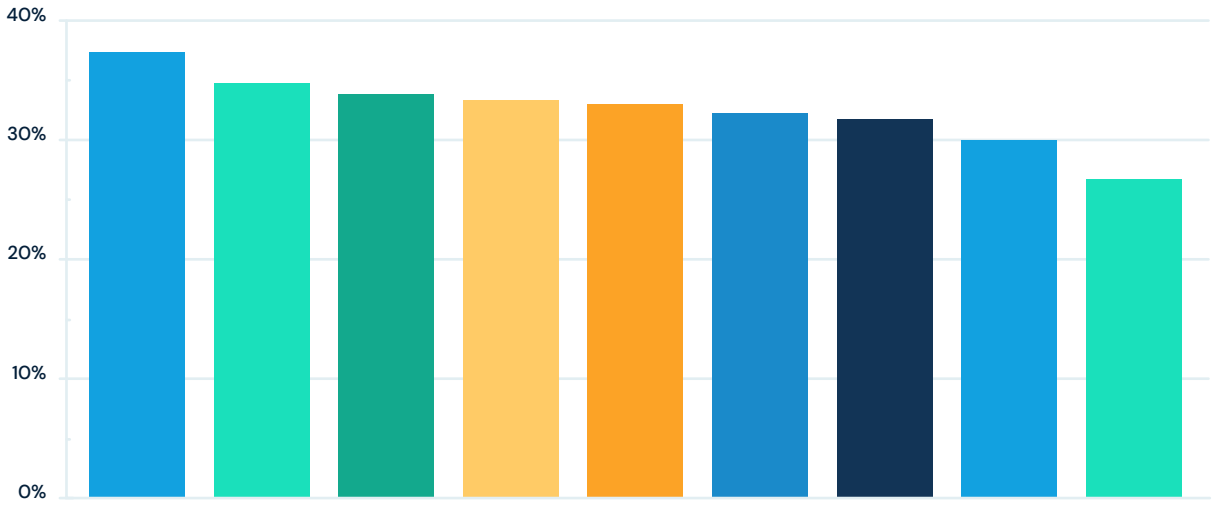
Standardizing SOPs has had a positive impact on detection and response programs

The survey asked each respondent to indicate what changes they have made to their detection and response program that have had a positive impact in the past 12 months. Each respondent was allowed to choose all that applied from a list of nine possibilities.

Creating Standard Operating Procedures (SOPs) was noted as a positive change by more respondents than any other answer, with 37.6% stating that this has had a positive impact on their program. However, several other answers were also chosen by significant portions of respondents, including reducing visibility gaps (34.6%), improving team communication (34%) and limiting the scope of daily duties (33.4%).

Additionally, adopting machine learning and hiring more specialists were each selected by nearly a third of the respondents.

What changes, if any, have you made to your detection and response program over the past 12 months that had a positive impact?



Creating Standard Operating Procedures	37.5%
Reducing visibility gaps	34.6%
Improving overall team communication	34.4%
Limiting scope of daily duties	33.4%
Adopting machine learning	32.9%
Hiring more security specialists	32.9%
Increasing automation	32.6%
On-boarding a new product or replacing an existing product	30.2%
We made no changes	27.0%

Automation is seen as the most impactful way to improve effectiveness of detection and response programs

When we asked our respondents what would have the greatest impact toward making their threat detection and response program more effective, the number one answer was automation, with 23.6% of the respondents indicating that automation would be the most impactful. Next, “finding solutions to manage a high volume of data” came in at 20.2%, and “better collaboration with internal teams” came in at 19.7%.

The amount of security data that teams need to ingest, analyze, and retain is growing exponentially, which explains why many teams are looking to automation and big data solutions to help them improve detection and response. Additionally, more collaboration with internal teams could be viewed as a way to ensure that security considerations are taken into account earlier in projects or software deployments so the security team can be more proactive with respect to planned changes.

To make your threat detection and response program more effective, what would have the greatest impact?

Automating the response of manual tasks	24.5%
Better collaboration with internal teams	20.0%
Hiring full-time team members or contractors	20.0%
Investing in machine learning technologies	19.0%
Finding solutions to manage high volume of data	16.3%

Section Summary

As we see from the above, the number one priority of security teams is reducing mean time to response. Yet one of their biggest challenges is efficiency, which directly impacts that mean time to response. This lack of efficiency is likely why 26.8% view their current detection and response system as “not very effective.”

Becoming more efficient through the use of automation and better handling of big data is the key to improving not only the efficacy of the security team, but the posture of an organization overall.

Let’s now turn our attention to the types, frequency, and volume of alerts that security teams deal with on a daily basis.

Growing Volumes of Alerts

PART 3

To quantify what security teams are up against, we wanted to understand the volume and type of alerts they face. We also wanted to know what effect the current volume and growth of alerts has on their ability to manage their response activities effectively.

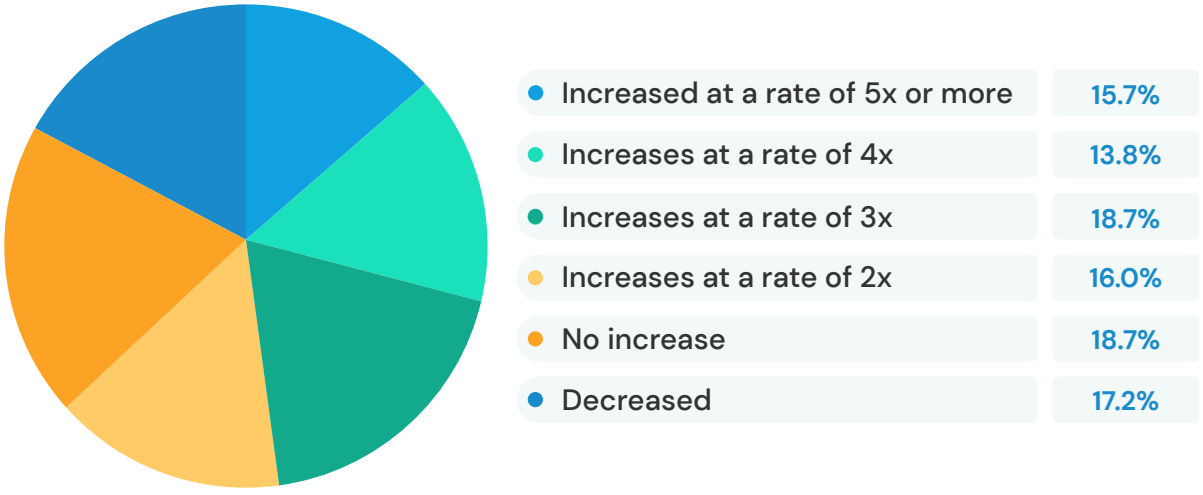
Almost half of respondents have seen the volume of alerts more than triple in the last year

Anecdotally, any security professional can tell you that the volume of security alerts is increasing and has been for several years. This survey puts some hard numbers around what many security teams are experiencing.

The largest group of respondents (18.7%) said they have seen a three-fold increase in alerts in the past 12 months, and roughly half (48.2%) have seen three, four, or five times the number of alerts in that same period.

Given the backdrop of a shortage in qualified security professionals, it is easy to imagine how managing the escalation in alert volumes puts an incredible strain on security teams.

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



Over 50% of respondents find that at least half of alerts are false positives

False positives cause alert fatigue which can reduce effectiveness and efficiency

of security teams. To understand the magnitude of this problem, we asked our respondents what percentage of their alerts were determined to be false positives.

The results indicate that the respondents are split into four groups: 25.3% say that less than 25% are false positives, 24.3% say between 25% and 50% of their alerts are false positives, 25.1% say between 50% and 75% are false positives, and 25.3% say 75% or more of their alerts are false positives. Even with only a quarter of alerts proving to be false positives, a security team can get bogged down with triage and investigations. At over 75%, dealing with false positives would take a significant toll on efficiency.

What percentage of these alerts were false positives?

Less than 25%	25.5%
25 – 50%	24.3%
>50 – 75%	25.1%
75% or more	25.3%

37% are getting more false positives than ever before

When asked to state whether the number of false positive alerts was on the rise, consistent, or decreasing, the survey respondents were split roughly into thirds. The largest group at 37.1% said they see more false positives than ever before, with “staying consistent” and “decreasing” virtually the same at 31.2% and 31.7% respectively. It is encouraging that a third have found ways to reduce their false positives, but still, two-thirds are sinking or only treading water.

How is the number of false positives changing?

We’re getting more false positives than ever	39.6%
We’re getting about the same false positives as usual	32.2%
We’re getting less false positives than usual	28.3%

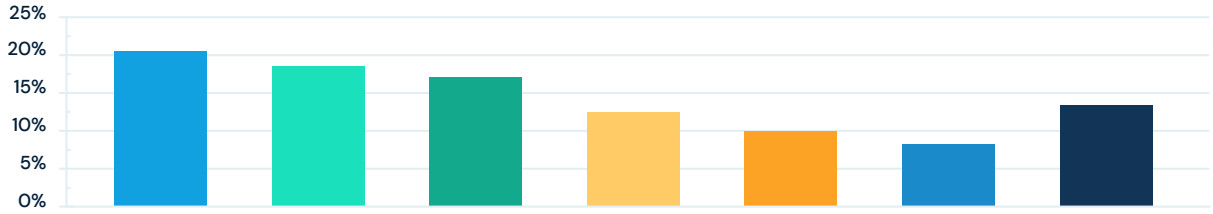
Increasing automation reduces false positives

To dig deeper into what those teams that reported a reduction in false positive alerts are doing to achieve these results, we asked that group of participants to select what changes they've made that have reduced their false positives.

Increased automation, at 20.2%, was the most common attributor to fewer false positives. This number is consistent with other responses in the report that signify the importance of automation in threat detection and response.

Modified detection logic (18.6%) and refined tool configuration (17.1%) round out the top three spots which indicate that detection and response teams are utilizing a feedback loop to understand where "noisy" alerts are coming from and tune detection rules and tools accordingly.

If less than usual, what changes have you made to reduce the number of false positives?



Increased automation	20.2%
Modified detection logic	18.6%
Refined tool configuration	17.0%
Integrated threat intelligence	12.4%
Integrated User and Entity Behavioral Analysis (UEBA)	10.0%
Improved contextualization	7.8%
Other	13.9%

56% of teams are experiencing alert fatigue

Given the explosion in the volume of alerts security teams are facing, coupled with the growing portion of these alerts that are false positives, it makes sense that 55.5% of teams are experiencing alert fatigue. Being crushed under a tsunami

of alerts is an industry-wide problem, and security solution providers must be able to deliver tools that produce higher-quality signals that reduce noise while still flagging suspicious activity.

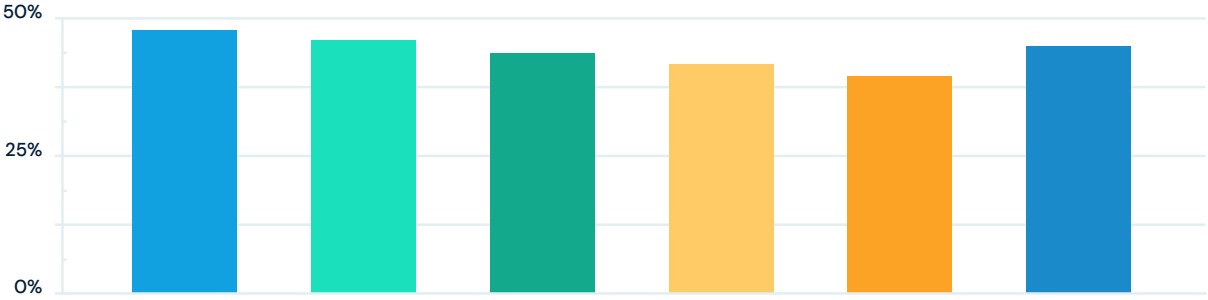
Would you say the number of alerts is causing alert fatigue amongst your team?

Using AI/ML to review alerts before they reach a human is the number one action to reduce alert fatigue

Of those who have been able to reduce alert fatigue, nearly half (46.5%) said they use machine learning and artificial intelligence to review and vet alerts before passing them on for human review as one means of providing relief.

42% said that one way they reduce alert fatigue is to rotate who triages the incoming alerts, and 37.6% stated that automating responses to common alerts has helped reduce fatigue.

If yes, what are you doing to reduce alert fatigue?



Using machine learning/AI to review alerts before triggering human review	46.5%
Rotating who triages alerts	42.0%
Automating the response of common alerts	37.6%
Leveraging threat intel and other enrichment sources for added context	32.7%
Ignoring alerts	32.3%
Skip – We aren't currently doing anything to address alert fatigue	39.4%

Section Summary

The numbers presented in this section yield evidence of what many security professionals know intuitively: There are too many alerts for teams to handle effectively, and the number is growing exponentially.

Given this taxing situation, it is critical for security solution providers to deliver the tools that modern security teams need to effectively test and tune detections, automate routine tasks, and utilize enrichment from threat intelligence providers and other sources to limit false positives and minimize alert fatigue.

Current Threat Detection Tool Stack

PART 4

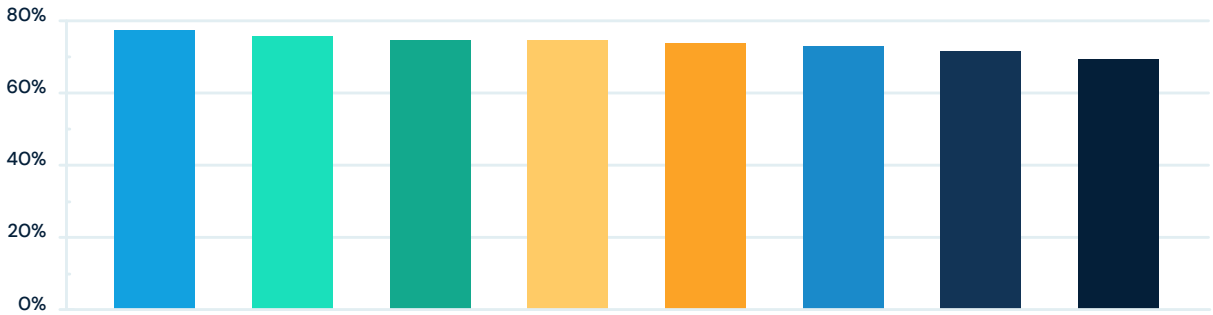
We wanted to gather information in order to examine what tools security teams use, along with what they like and don't like about these tools. We also wanted to know how many security organizations built their own solutions, and if they did, how well that worked for them.

Three-quarters of respondents report consistent use of common categories of tools

Security teams have a myriad of tools at their disposal, and some of these tools work better than others, depending on the specific needs of the business and the organization's attack surface. To gather insight into which tools work well and which tools practitioners struggle with, we first asked what kinds of tools do they use?

Responses were quite consistent, with roughly 75% of security practitioners responding that they use each of the tools we asked about.

Which tools do you use?



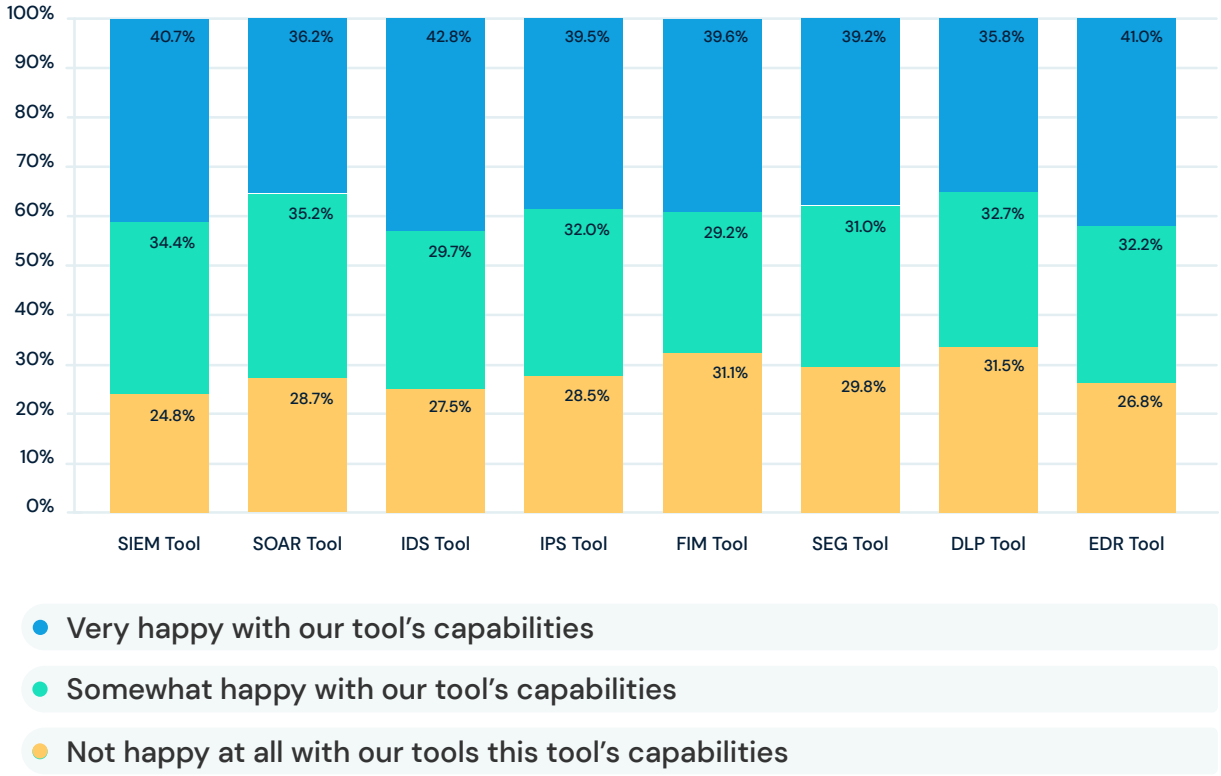
Data Loss Prevention (DLP) tool	78.9%
IDS (Intrusion Detection System) tool	78.6%
IPS (Intrusion Prevention System) tool	78.4%
Security Email Gateway (SEG) tool	78.4%
FIM (File Integrity Monitoring) tool	78.1%
End Point Detection & Response (EDR) tool	77.9%
SOAR (Security Orchestration, Automation and Response) tool	75.4%
SIEM (Security Information and Event Management) tool	74.2%

Over one-quarter aren't happy with the capabilities of any of their tools

Our respondents may be using all of these tools, but are they happy with the capabilities? Satisfaction levels across tools remained fairly consistent, yet they were not very high, ranging from 35.8-42.8%.

Dissatisfaction ratings were also fairly consistent, with roughly 25% of respondants "not happy at all" with each category of tool.

If you use the tool, are you happy with it?



55% have built their own detection and response tool

Over half of respondents stated that they have built an in-house solution to support their detection and response efforts. Given the relatively low satisfaction scores with every tool category noted above, it is not surprising that security teams have sometimes found it necessary to create their own custom-built solution rather than relying on a commercial tool.

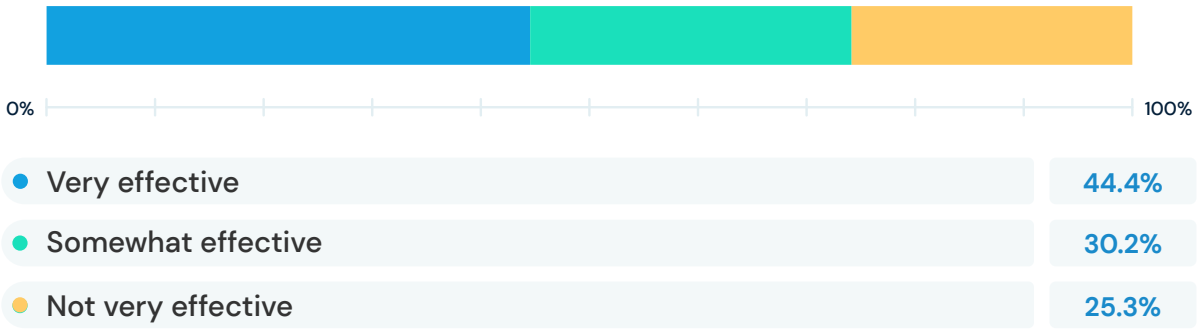
However, security vendors should take note of this and better understand where their tools are not adequately meeting the needs of detection and response teams so they can make improvements. At the end of the day, security teams need easy-to-use and effective tools so they can spend their time focused on the security of their organization, not building and maintaining custom tools.

Has your team built an in-house solution to support your threat detection and response efforts?

25% said the tool they built was highly ineffective

Further supporting the need for easy-to-use and effective commercial security tools, 25.3% of respondents said their home-grown tool was highly ineffective, and an additional 30% said it was only somewhat effective. This is not surprising since it takes significant time and effort to build and maintain a custom tool, and if the team members responsible for building it leave the company, that can make it even more difficult to support.

How effective was that tool at supporting your threat detection and response efforts?



Section Summary

The answers in this section highlight two critical factors that warrant further consideration. The first is that while detection and response teams use a variety of tools, less then 50% of respondants are fully satisfied with the capabilities provided. This low satisfaction is likely what drove over half of these teams to try to create their own. And, unfortunately, building their own tools also didn't result in the effectiveness they had hoped for.

This is important feedback for security vendors to pay attention to and ensure they are being responsive to the needs of security practitioners. There are plenty of tools out there to help with detection and response, but many lack the capabilities that security teams really need to do their jobs effectively.

Plans For The Future

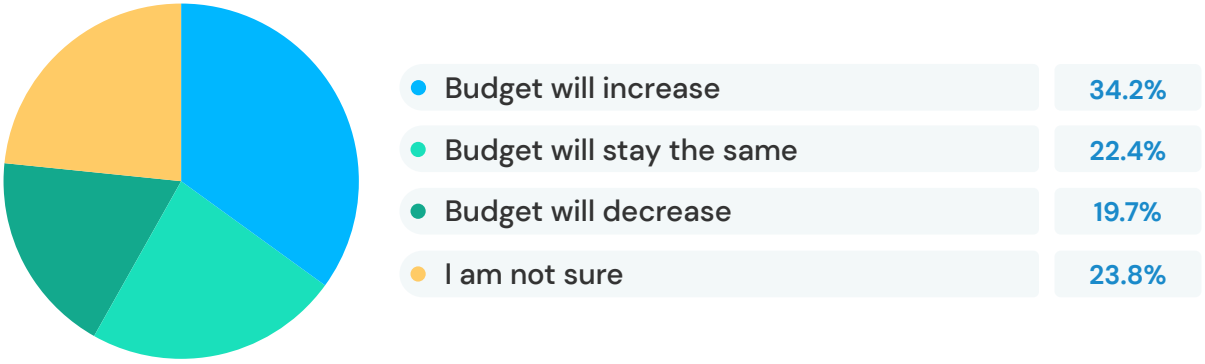
PART 5

In this last section, we take a look at how our respondents see the future by exploring their budget expectations and priorities for the coming year.

Over a third anticipate an increase in their security budget

As what the entire industry may see as a positive signal, 34.2% of our respondents who have visibility into their organization's financial projections expect their threat detection and response software budget to increase in the next 12 months. Only 19.7% expect to see a decrease in available funds.

How is your budget for threat detection and response software going to change over the next 12 months?

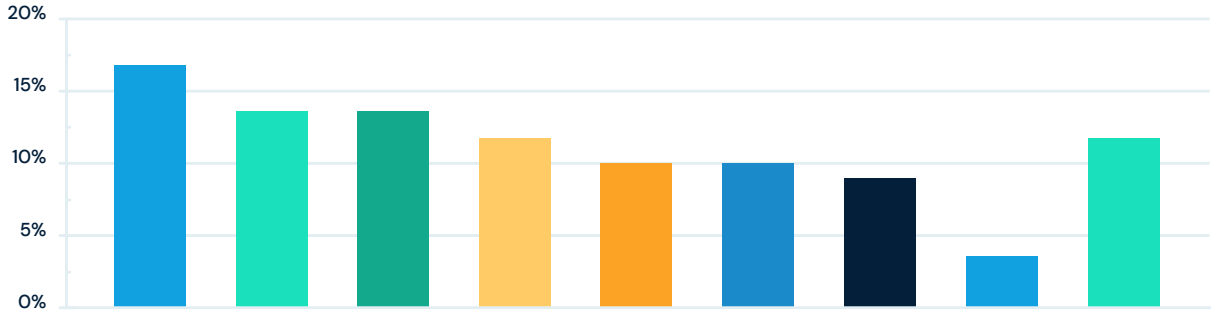


Improving the speed of response rate is the top priority for the next 12 months

At 17%, improving the speed of their response capability is the top priority next year for security teams. Speed, flexibility, and scale are critical to successful detection and response programs.

The next highest priority chosen was advancing the organization's cloud security posture (12.3%), and, for the third spot, a two-way tie at 11.8% between adding more sensors and ensuring complete coverage — two closely related needs — both of which speak to the need for full visibility into across company infrastructure and systems.

When it comes to your threat detection and response program, what would you say is your top priority for the next 12 months?



Ensuring complete coverage of organizational resources	16.9%
Advancing our cloud security posture	13.5%
Adding more security sensors	13.5%
Improving the speed of our response rate	11.8%
Aggregating security logs into a single place	10.1%
Reducing false positives	10.1%
Getting management buy-in to expand funding	8.4%
Generating better reporting metrics	3.3%
Other	11.8%

Actionable Tips to Prepare for the Future of Detection and Response:

Detection-as-code

The “Everything-as-Code” evolution is changing how security teams write, test, and harden detections. By adopting universal coding languages like Python, and applying software development principles to the process for writing, testing, tuning, and releasing detections, security teams can more effectively craft high-fidelity alerts tuned to their specific environment.

This brings significant benefits in terms of reliability, accuracy, and quality, which all contribute to reducing noise and lessening alert fatigue.

Scalability

Security teams need complete visibility into their environment in order to protect it. This means collecting complete data up and down the stack to get as much context as possible to understand what normal operations look like, and to effectively flag suspicious activity. But in order to adequately collect and synthesize the massive amount of data flowing today, security teams need scalable architecture for their detection and response tools in order to keep up with cloud-scale data volumes. Security is increasingly becoming a big data problem, so security teams need solutions that treat it as such.

Take advantage of automation

As we saw above, the biggest challenge to security teams today is efficiency. One of the best ways to increase efficiency is through automation. However, good automation requires context, not only to route alerts to the right teams, but to ensure alerts can be triaged, prioritized, and actioned appropriately.

Threat detection and response platforms that can enrich log data and programmatically add context to alerts can make automation much easier and more effective.

Conclusion

Threat detection and response at modern scale is challenging, no matter how large or experienced your team is.

The answers provided by our respondents confirm what many security practitioners experience firsthand every day. Teams need more effective automation and scalability as they endeavor to analyze large volumes of security data. Commercial tools are often not living up to their expectations, but security teams also struggle to build their own internal tooling that can perform as needed.

However, it is encouraging to see that many respondants expect their budget for security to increase in the coming year, which is an important step towards helping security teams implement the tools, processes and staffing they neeed to operate effectively.

About Panther

Panther Labs was founded by a team of veteran security practitioners who faced the challenges of security operations at scale and set out to build a platform to solve them. The result was Panther, a refreshingly practical platform for threat detection and response powered by a highly scalable security data lake and detection-as-code. Panther gives security teams the power to detect any breach, anywhere and is trusted by customers like Snowflake, Dropbox, Zapier, and more.

www.panther.com