panther

2022 STATE OF SIEM

Legacy SIEMs are holding back security teams, making their jobs much more complex

and far less enjoyable. They're also forcing organizations to waste millions of dollars during a time when they should be saving everywhere they can.

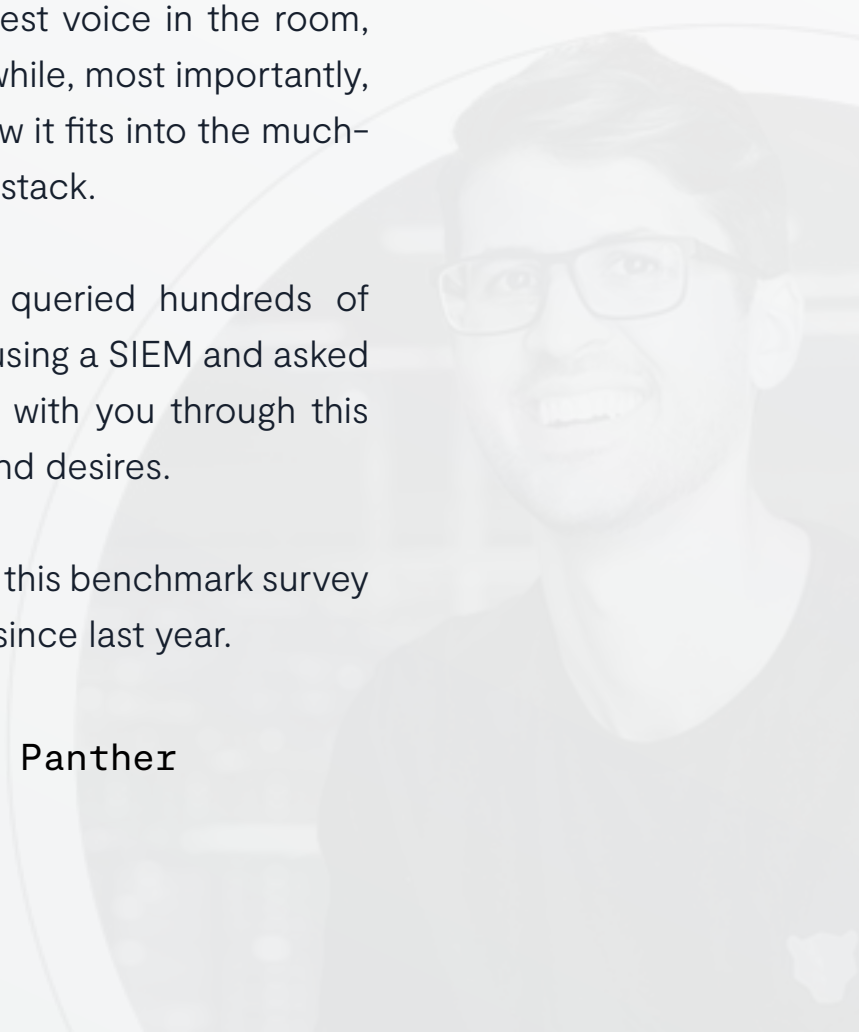
Everyone knows legacy SIEMs are outdated and expensive; even so, every new option introduced to the market represents only a slight incremental improvement. Panther is officially declaring war on legacy SIEM, war on incrementalism, and to battle for relief for security teams that are forced to settle for outdated, expensive, clunky tools.

At Panther, our goal is to be the loudest voice in the room, calling out the pitfalls of legacy SIEM while, most importantly, sharing what a modern SIEM is and how it fits into the much-needed next evolution of the security stack.

To help us fine-tune our plan, we queried hundreds of cybersecurity professionals currently using a SIEM and asked them to share with us, and ultimately with you through this report, their challenges, frustrations, and desires.

You can download the 2021 iteration of this benchmark survey here to see how things have changed since last year.

Jack Naglieri, CEO, Founder, Panther



panther

Key Findings

Most practitioners settle for patchy coverage.

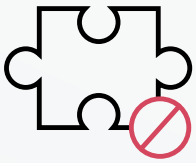
Nearly half of the security professionals believe their current SIEM solution covers only 50% of their critical security data. Only 15% estimate that more than three-quarters of their data is covered.

SIEM platforms can take a long time to deploy.

77% of respondents indicated that receiving high-value alerts takes longer than one month. 13% said it took longer than six months. It doesn't need to take that long.

False positives are a number one challenge.

When asked to identify their number one challenge when interacting with their current solution, the most common answer was false positives. This answer ranks above the next most common challenge (complex and hard to use) by a margin of 5%.



Cost, functionality, and innovation are the top reasons for seeking a new solution.

Whether happy or unhappy with their current solution, the most often cited reasons they would decide to switch are what they pay and what their platform won't do for them.

Challenges With Existing SIEM

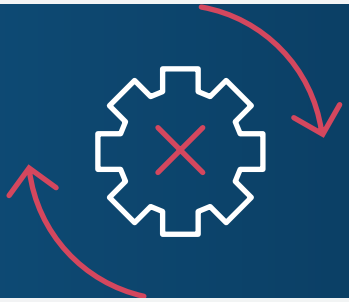
Implementing a SIEM requires some attention and, unsurprisingly, brings unforeseen problems. To learn what deficiencies were exposed as our respondents completed their current SIEM deployment, we asked them to indicate what roadblocks they encountered along the way. Some results reflect the same difficulties we found in last year's survey, but others indicate a shift in the struggles that plague security professionals today.

The most commonly selected option for this question, chosen by 22%, was three months for the deployment and implementation before their existing SIEM began receiving high-value alerts. An astonishing 13% took longer than six months.

This finding confirms what many practitioners know anecdotally – SIEM deployments take months to complete. This extended period is generally due to the need to choose an appropriate data source, integrate with that source, build schemas for the data format, craft detections, and so on

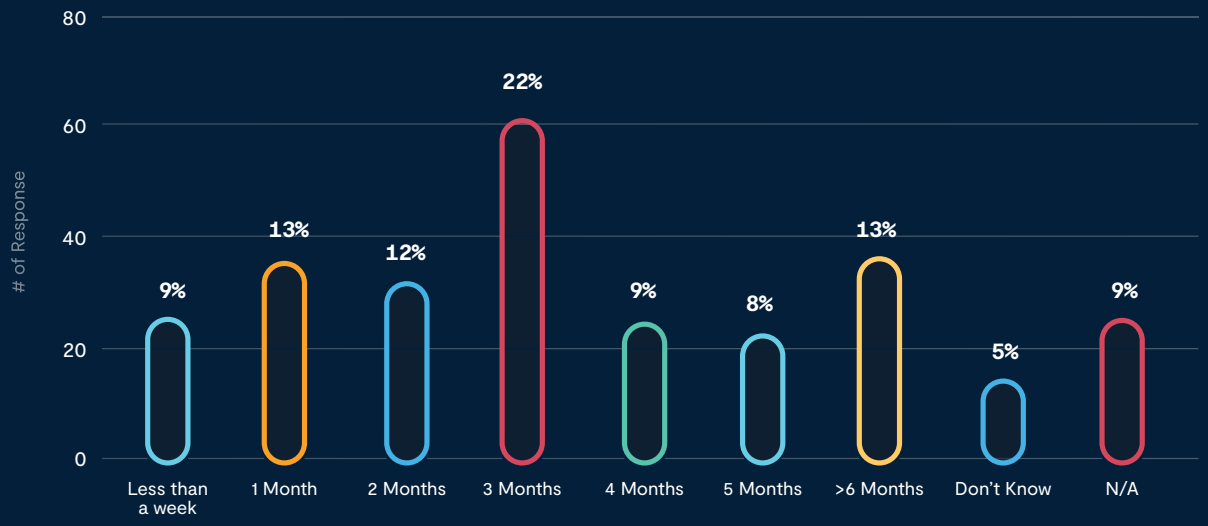
77%

of respondents indicated that receiving high-value alerts takes longer than one month.



Slow to implement, too complex, and too many false positives rank among the top challenges for 2022

How long would you estimate your SIEM deployment and implementation took to begin receiving high-value alerts?



One reason for this lengthy deployment time is the use of proprietary languages to write detections and run queries. If the team responsible for deploying and using the SIEM lacks appropriate skills, this can slow things down.

A modern SIEM tool should use an accessible language such as Python that is well-understood so that anyone with general programming skills can write detections and receive high-value alerts.

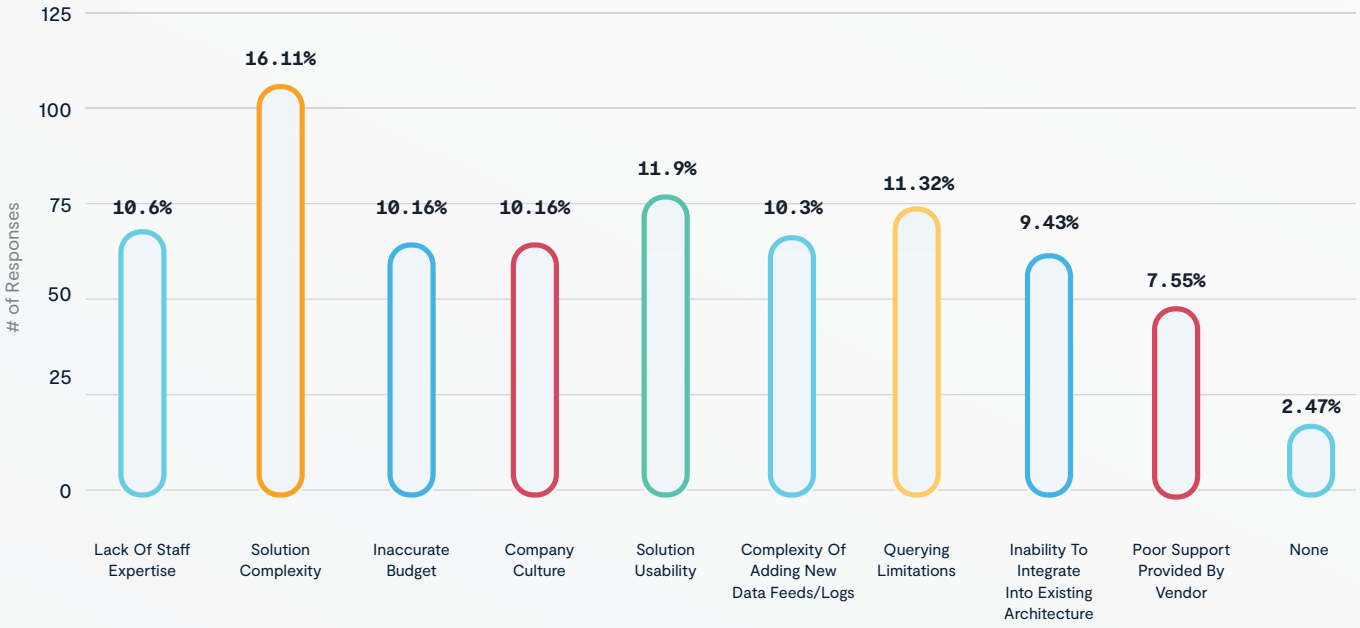
40%

say complexity is the top challenge their team encountered when implementing their SIEM.

SIEM platforms can be complex to implement and deploy for many reasons. The solution must be able to collect data from a variety of sources to detect threats and vulnerabilities. This process can be time-consuming, especially if the source systems are not already integrated with the SIEM.

Finally, security teams must configure the SIEM platform to meet the organization's specific needs. This setup can include configuring alerts, monitoring dashboards, and writing detection rules. Practitioners must complete all of this work before the SIEM begins providing valuable alerts.

What challenges did your SOC team encounter while implementing your current SIEM platform?



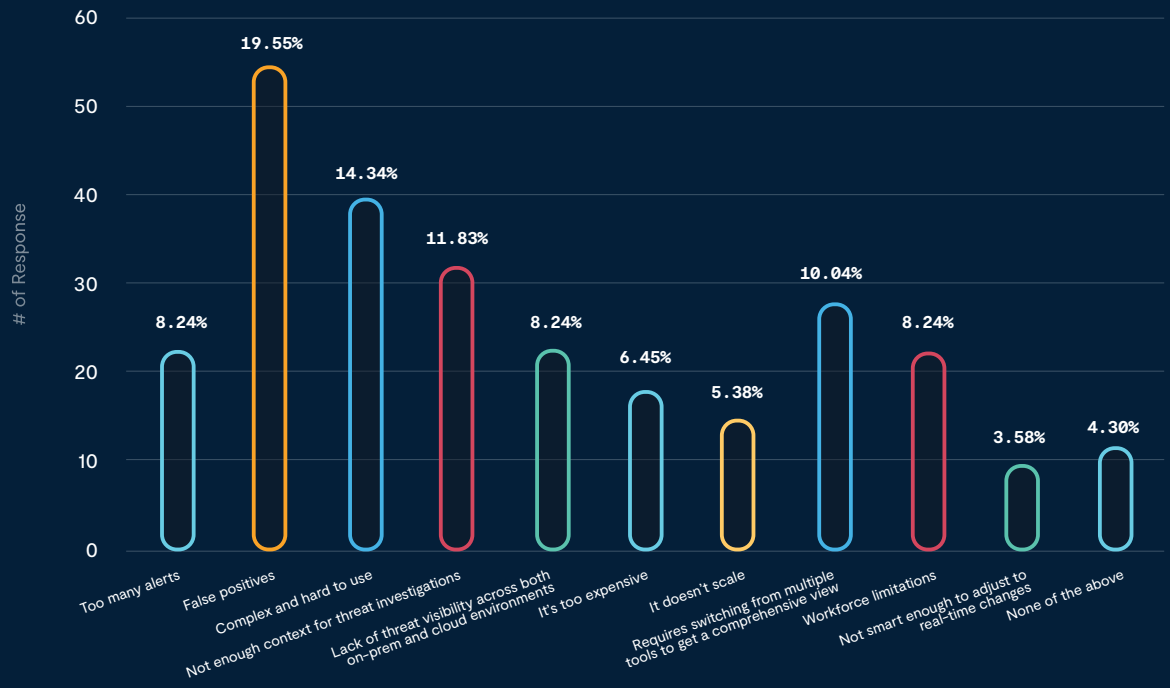
Today's IT environments are more complex than ever, with the cloud, Kubernetes, endpoints, networks, and applications all generating terabytes of security data.

SIEMs are supposed to solve the problem of ingesting all this security data and provide alerts on critical security issues that analysts can quickly investigate.

This data suggests that upwards of 40% of users suffer from poor alerts, which causes alert fatigue and burnout. This suggests the need for more fine-tuning of alerts in order to decrease the false positives that arrive.

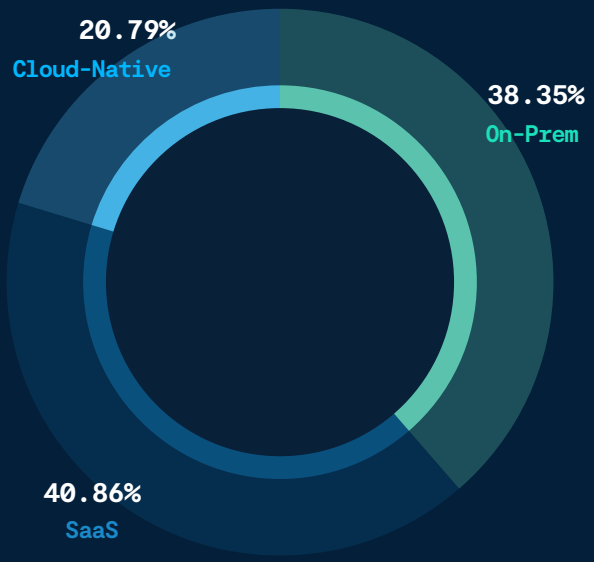
The majority say **false positives are the #1 daily challenge** they face when interacting with their current SIEM platform.

When it comes to interacting with your SIEM day-to-day, what is the #1 challenge you face with your current platform?



Cloud-native SIEMs are gaining on on-prem and SaaS solutions.

41% of the respondents to our survey indicated that their current SIEM is a SaaS solution. On-prem SIEM platforms came in a close second at 38%, followed by the relatively newer cloud-native category at 21%.



What best describes the type of SIEM platform your team uses?

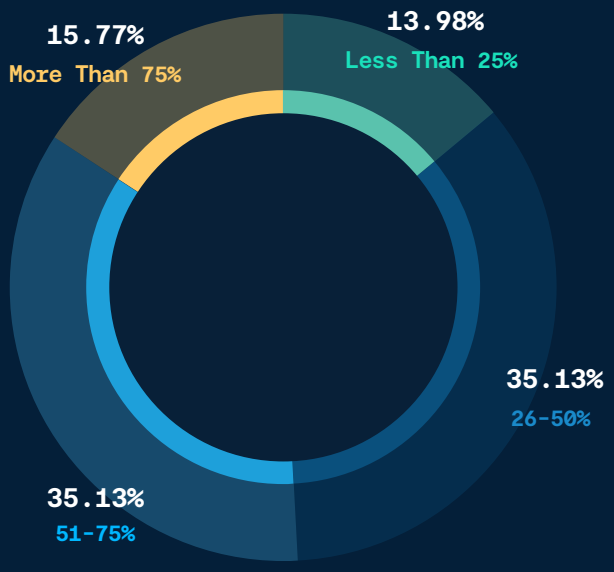
} part_two

Capabilities

A deep dive into the capabilities of our respondent's systems will add context to their previous answers about expectations and challenges. In this section, these security professionals answered questions about various aspects of the systems they work with, from log management to how much of their security data is covered.

49% believe their SIEM covers less than half of their security data.

A SIEM is a critical piece of an organization's security infrastructure and needs to cover all of its security data to be effective. If a SIEM only covers a fraction of an organization's security data, it will not be able to provide the comprehensive security coverage necessary for protecting an organization's networks and systems. Additionally, if a SIEM does not have complete visibility into an organization's security data, it will be unable to identify potential threats and vulnerabilities that could put an organization at risk.



What percentage of your security data is covered by your existing SIEM platform?

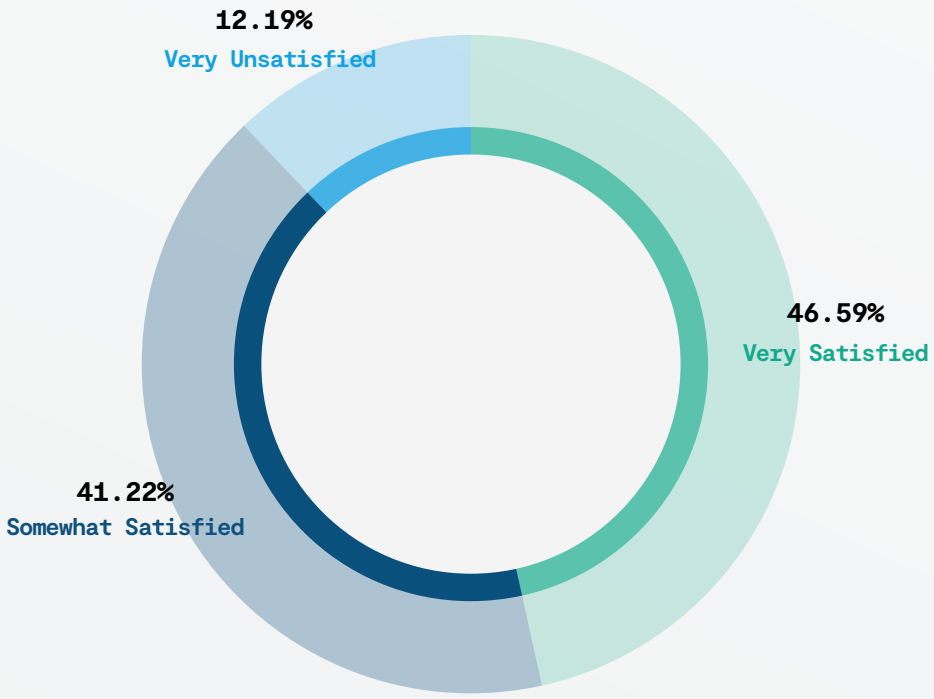
53%

of SIEM users are, at best, somewhat satisfied with log management.

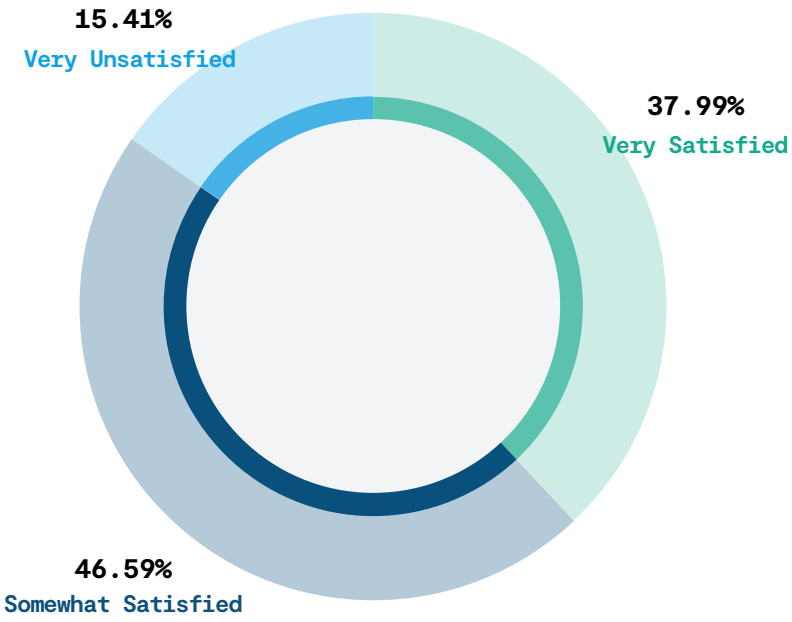
If you prefer a “glass half full” perspective, 47% of users are very satisfied with the log management capabilities of their current SIEM solution, but that number should be higher. Log management is essential to a successful cybersecurity strategy.

Organizations can collect and analyze logs to detect threats and vulnerabilities, understand how attackers operate, and investigate incidents.

How satisfied are you with your existing SIEM platform’s log management capabilities?



How satisfied are you with your existing SIEM platform's automated response capabilities?



SIEM has become a staple in modern-day SOCs for detecting security threats and managing compliance. A good SIEM is essential for helping organizations identify and remediate potential security threats and vulnerabilities before they disrupt business operations.

It should bring visibility to user behavior anomalies and automate many manual processes associated with threat detection and incident response. It isn't easy to overemphasize the importance of automated response, and SIEM users need a solution that excels in this area.

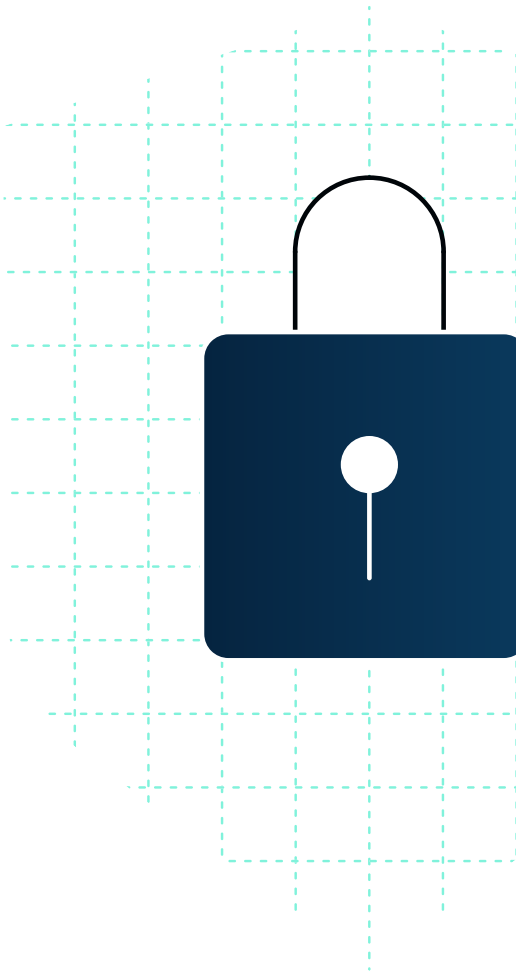
62%

of users are either very unsatisfied or only somewhat satisfied with their existing SIEM platform's automated response capabilities.

Adequate security today depends on having a solid data pipeline, structured data, and cloud-first workflows. Security professionals are aware of the static nature of traditional SIEM platforms, and many are concerned about the future. Many of today's SIEM providers designed their current solution more than ten years ago and haven't changed their approach much in the last decade.

Outlook for the Future

Cyber threats are constantly changing, and businesses must be prepared for the future. This means having a plan for how they will protect their data and ensure that their security solutions are up to date.



Traditional SIEM platforms are becoming increasingly obsolete, as they can't keep up with the changing landscape of cybersecurity. Over 40% are unhappy with their current solutions, and a quarter of them are looking for a replacement.

Businesses must be prepared to move to innovative cloud-based solutions that provide modern functionality more cost-effectively.

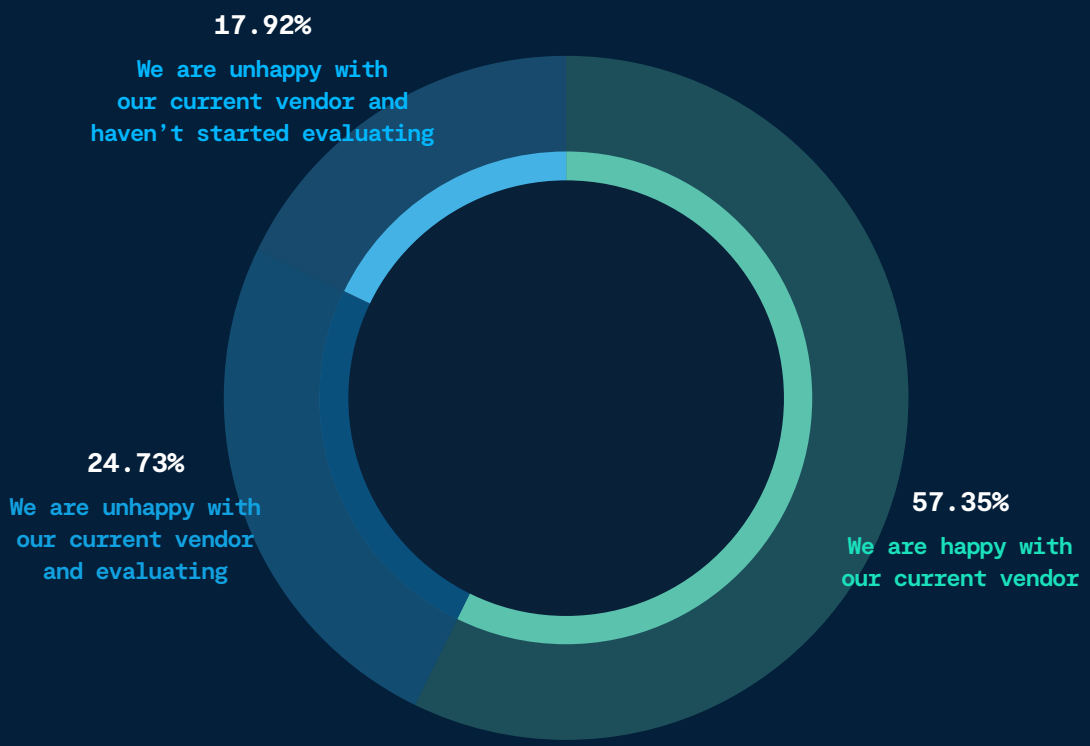
Let's turn our attention to how our respondents feel about the future of their security posture.

43%

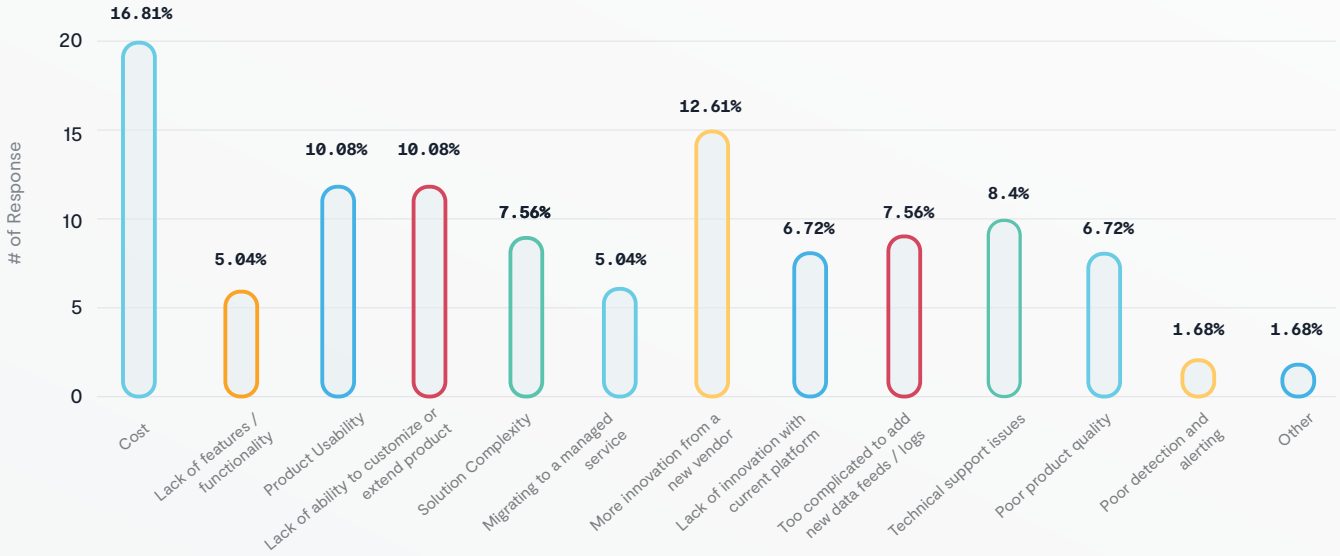
are unhappy with their current SIEM vendor, and 25% have started looking for a new one.

For the reasons this survey has revealed, the dissatisfaction felt by security leaders is reflected in a desire to find a better SIEM solution. Facing a tsunami of vulnerabilities and a cascade of threats motivates those charged with keeping their organization safe. It is only natural for these dedicated leaders to search for a more modern security information and event management solution.

When it comes to your SIEM plans for the upcoming 12 – 24 months, what is most accurate?



[If unhappy] What is your primary reason for considering a switch to a new vendor?

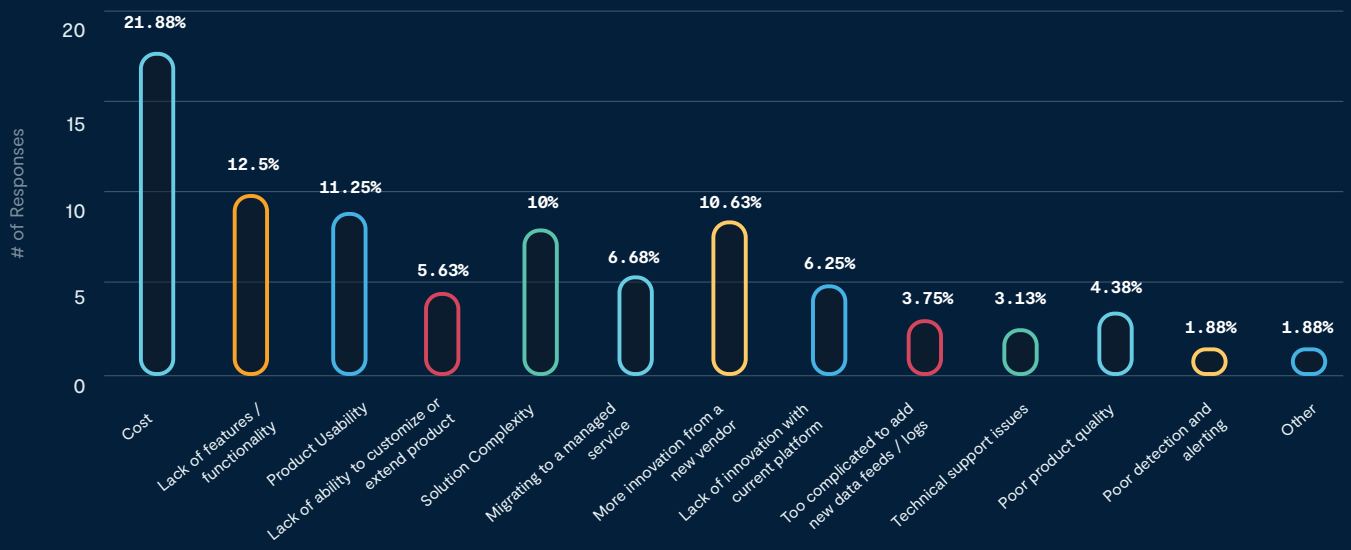


The primary causes of unhappiness are cost, more innovation in other vendors, and functionality.

Cost, complexity, and a desire for more innovative solutions are three primary drivers that organizations consider when making decisions about their IT tools.

As macroeconomic conditions change, IT teams will look to save where they can, including decommissioning tools that don't provide value or switching out tools to save cost. Reducing environmental complexity can also be a valuable way for security teams to continue to operate effectively or do more with the same resources.

[If happy] If you were to decide to switch to a new vendor, what would be the reasons?



Even for those who are happy with their current SIEM vendor, the top reason would be cost if they decide to switch.

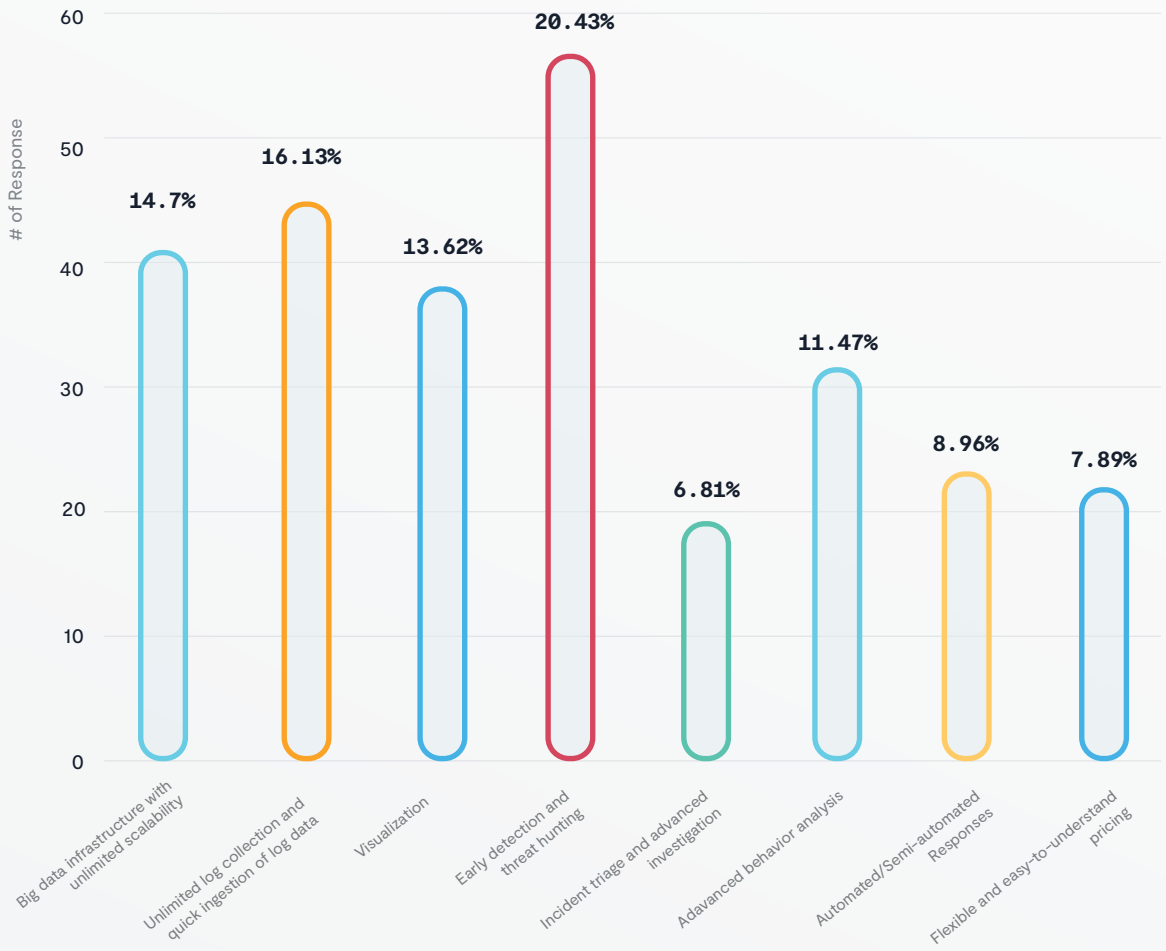
Making a strong statement about the exorbitant costs of traditional SIEM platforms, even of those that are happy with their current solutions, the cost is the thing that would drive them to look elsewhere.

Early detection and threat hunting is the top capability for security practitioners evaluating a new SIEM vendor.

When looking at what features and capabilities those in the market for a new SIEM want, it is noteworthy that threat hunting comes first, with over 20% of the picks. After all, to protect your business from potential cyber threats, you need to be able to identify and address any potential vulnerabilities before threat actors can exploit them. And that's where threat hunting comes in — it's a critical part of any organization's cybersecurity strategy and something that a good SIEM solution should provide.

It is also informative that in last year's survey, our respondents indicated that big data infrastructure with unlimited scalability was the most sought-after capability in a potential new system. Big data infrastructure comes in third this year, so it's still essential, but for many, it's been a brutal year of cyber attacks. Threat hunting as a means to compromise the adversary's ability to exploit new vulnerabilities seems more appealing this year.

If you were evaluating a new SIEM vendor, what features and capabilities would be most important to you?



Conclusion

This year's State of SIEM report illuminates some key takeaways. Like last year, the survey's responses indicate that traditional SIEM platforms are not adequate for detection at scale. Security teams are using these tools even though they can't get the scale and flexibility they need to do their jobs.

Additionally, these results clarify that an effective SIEM must use an accessible and well-understood language for detections and that teams should outsource complexity where they can. Leaders can reduce complexity by choosing cloud-native SIEM and relieving their team from managing and running an infrastructure and data pipeline.

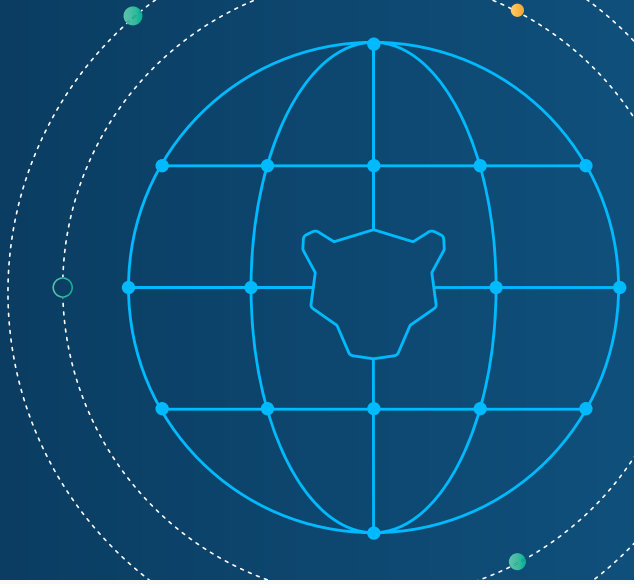
This year's revelations include the importance of starting with a high-value log source, then fine-tuning your system, and continuing to add more data by focusing on your threat models or critical infrastructures, such as business applications, customer data, and identities.

Lastly, don't overlook the total cost of ownership. Look beyond the licensing fee, and consider factors such as time to add a log source, writing new detections, editing and rolling back detections, and searching for IoCs.

Try Panther

panther.com

Who We Surveyed



On September 14, 2022, we interviewed 285 full-time cybersecurity professionals, each working as part of a team that currently uses a SIEM platform. The survey was conducted online via Pollfish using organic sampling. Learn more about the Pollfish methodology here.

We sought input from roles across the spectrum of security practitioners. The largest group, at 30%, are analysts, with 24% engineers and 17% from the C-suite.

Security teams use SIEMs in a variety of industries. We asked respondents to choose from 12 sectors that classify their organization. Tech was a clear standout, with 35 percent of respondents working for a technology company. Services and education evenly shared 18 percent, while finance and healthcare split 9 percent.

Overall, this year's breakdown mirrors last year's, with the largest segment of respondents being from the tech industry.

Team sizes range from 4-10 people for 22.22% of the respondents to 1-3 people for 9.68%. 11% work on teams of more than 50 people.

Copyright ©2022 Panther Labs Inc. All Rights Reserved.