State of SIEM 2021

Insights From 400 Security Professionals

runpanther.io

Introduction

The threat detection market is undergoing a radical transformation fueled by continuously evolving changes to infrastructure, remote workforce, budget restructuring, and other business, compliance, and security drivers.

Traditional SIEM platforms no longer meet the growing needs of security practitioners who face new and emerging threats. In its early days, SIEM was shaped by compliance drivers that dominated the era, like PCI or HIPAA. In recent years, however, SIEM has struggled to keep-up with the challenges of cloud adoption and other digitization initiatives. Traditional SIEM has fallen behind in three critical areas: speed, flexibility, and scale.

We wanted more insight into current SIEM challenges, frustrations, and desires when it comes to capabilities. To answer these questions, we sought out IT security professionals who use a SIEM platform to better understand what they're seeing, what they're concerned about, and what they want to improve.

Methodology

On June 9th, 2021, we surveyed 400 IT security professionals who actively use a SIEM platform as part of their job. Respondents to our survey (in order of prevalence) were CISOs/CIOs/CTOs, Security Engineers, Security Analysts, and Security Architects.

Key Findings

Up to 12 months for deployment and implementation. Over 18 percent of respondents indicated that the time it took to receive high-value alerts — from deployment to implementation — was 12 months or longer.

Biggest Challenge: Too many alerts. Nearly a quarter of the respondents said that the biggest challenge they face with their current SIEM platform is receiving too many alerts.

Cost versus capabilities don't align. Over 40 percent of the IT security professionals surveyed said their organization was overpaying for their SIEM relative to the system's capabilities.

Poor network visibility. With eight possible capabilities to choose from, the most significant percentage of respondents indicated they were unsatisfied with their current SIEM platform's network visibility capabilities.

Big data and scalability are most important. Nearly 30 percent — the largest group — said that big data infrastructure and scalability would be the two most important capabilities if they were evaluating a new SIEM vendor.

_01 Profile of Who We Surveyed

Our survey interviewed 400 full-time employees, all of whom work in IT security. Additionally, each of the respondents is part of a security team that currently uses a SIEM platform, which is defined by our survey as “a set of tools and services offering a holistic view of an organization’s information security.”

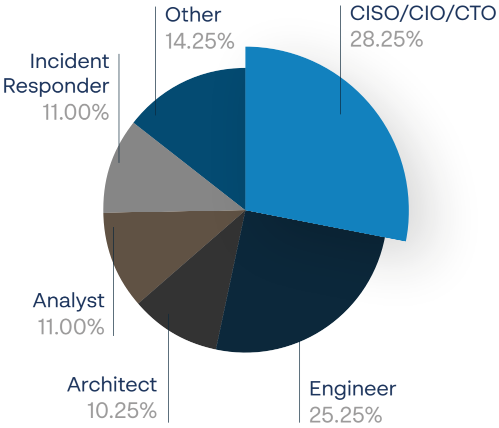
Survey respondents work for companies based in the United States, United Kingdom, Canada, and Australia. They are 58 percent male, and 48 percent are younger than 35 years old.

Role

Knowing they were involved in an IT security team that utilizes a SIEM, we wanted to learn more about the respondent’s role within their organization. The largest group holds positions in the C suite. While we didn’t differentiate between CISO, CIO, and CTO, 28.2 percent have one of these positions.

Security engineers were the next largest group, with 25.3 percent of the respondents. Architects, analysts, incident responders, and others are pretty evenly spread across the remaining 46.5 percent.

What best describes your role?

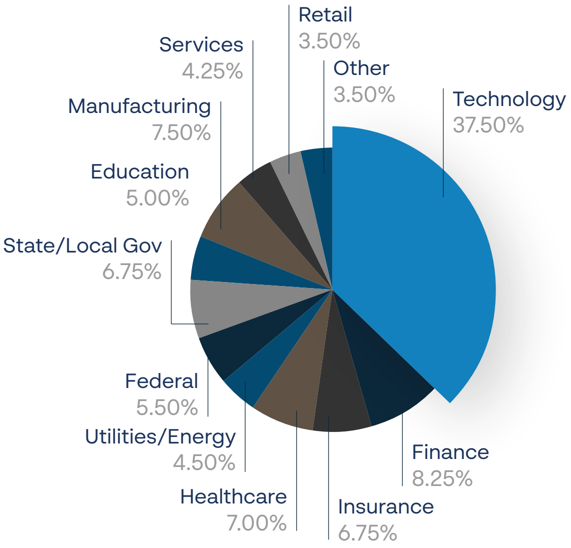


Industry

SIEMs are used across all sectors. We asked respondents to choose from a selection of 12 industries that classify their organization. Only technology was a clear standout. As you might expect, 38 percent of the respondents in our survey worked for a technology company.

Finance, insurance, healthcare, state/local government, and manufacturing split 36 percent nearly evenly. Utilities, Federal government, education, services, retail, and others fill out the remaining 26 percent.

What best describes the industry your organization operated in?

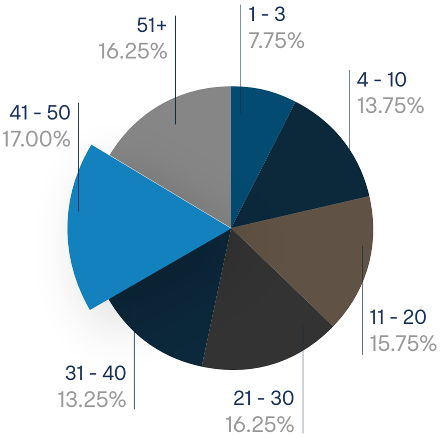


_01 Profile of Who We Surveyed

Team size

With the notable exception of the very smallest group, our respondents were evenly distributed by team size. 41 to 50 security team members are the largest group with 17 percent. The other six categories were within 3 percent of each other, except the one to three-member teams, which are only 8 percent.

How many people are on your security team?



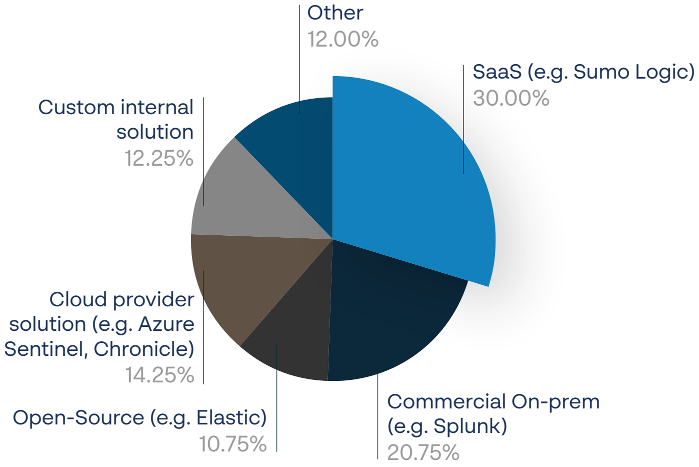
Type of SIEM

When asked how they would describe the type of SIEM platform their team uses, the largest group answered, “SaaS.” Those SaaS users came in at 30 percent, nearly 10 percent more than the next group of commercial on-prem.

These responses indicate that security teams are, indeed, leaning into SaaS solutions. This trend is important because SaaS solutions significantly reduce overhead and keep teams focused on data gathering and building detection capabilities. SaaS frees them from unproductive upgrading, patching, and software maintenance tasks.

Following the 20 percent that uses commercial on-prem, cloud provider solutions came in at slightly over 14 percent. Then custom internal systems and others, both at around 12 percent. The smallest group at nearly 11 percent is open-source.

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



To achieve our goal of providing insights into the unique challenges faced by SIEM users, we directed our survey exclusively toward practitioners currently working in the field. We felt that this group of professionals could present the most accurate and relevant feedback.

Our survey encompassed a demographic representative of the entire security industry. Large companies, as well as small shops, are included. This representation is important because, for protection against many types of attacks, the only difference between a Fortune 500 company and a fresh startup is the resources available for threat detection and remediation.

Security issues look different from the C suite than from the perspective of an analyst in a SOC defending an active attack. We tried to present a view that includes every perspective in the organization, every market sector, and every type of SIEM.

_02 Expectations and Challenges

Since each respondent is actively involved with their organization's current SIEM deployment, we wanted to learn about their experiences: What challenges they face, the difficulties they encounter, and what is working well.

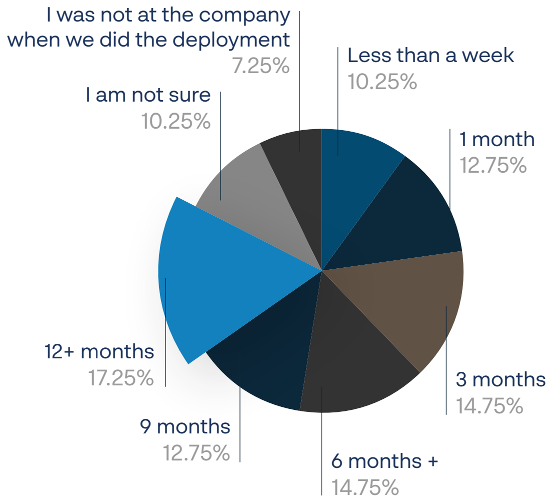
Questions in this section cover time to implement, ease of deployment, and ongoing challenges. The answers provide valuable insights about areas where traditional SIEM platforms fail to measure up to expectations adequately.

It takes over six months on average to deploy and implement a SIEM.

It was less than encouraging to learn that over half of the respondents who knew, said it took over six months to begin receiving high-value alerts after deploying a SIEM. This extended period is likely attributable to the many forces outside the security organization's control. Coordinating with operations departments to get security tools deployed on IT and production infrastructure often has inherent delays. There is also a learning curve related to cross-training teams that negatively impacts the time-to-value equation.

Solutions that include investigation workflows and built-in detections designed with an eye toward ease of onboarding can significantly decrease the time-to-value of a SIEM deployment.

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



_02 Expectations and Challenges

Query speed, complexity, and culture are the top challenges encountered while implementing a SIEM

The implementation of a new security tool predictably brings with it a set of challenges. To learn what deficiencies were exposed as our respondents completed their current SIEM deployment, we asked them to choose from a set of common challenges. Some of the results were predictable in that they reflect the difficulties of many traditional SIEM deployments, but some uncovered interesting struggles inherent to the company's culture.

Query speed: Nearly 50 percent of respondents included slow queries in their list of top challenges while implementing their current solution. Almost every security team running a SIEM has felt the pain of slow queries. Considering these architectures are over ten years old and were never intended for cloud-based workloads, this is no surprise.

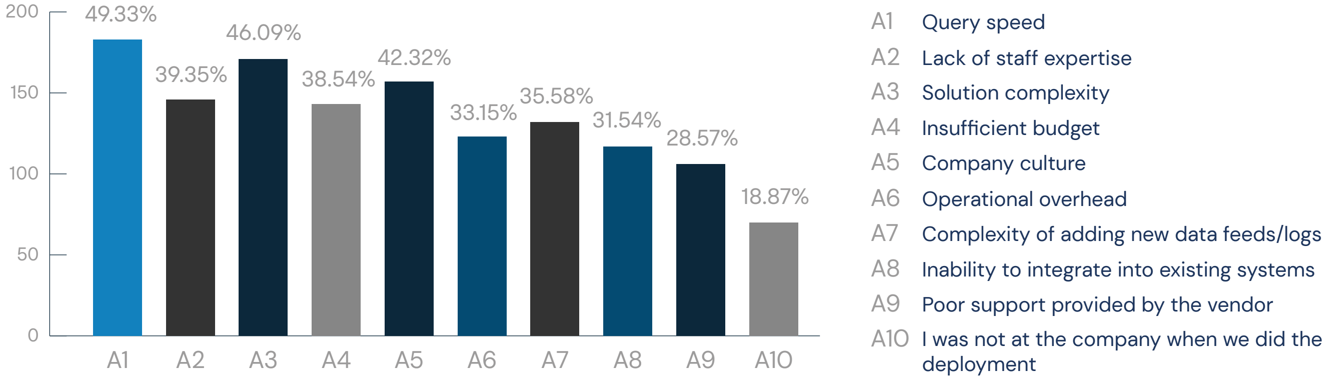
Complaints about speed and cost are all too familiar. Teams are paying a considerable amount of money for systems that can't meet their scale requirements and are too cumbersome and slow to run. SaaS and cloud data warehouse tech will pave the way for the next ten years of solutions.

Complexity: Over 46 percent agree that in legacy SIEM platforms, there is low confidence that searches that span several months back will ever complete, providing the answer to practitioners' questions. The answers provided by this survey's respondents offer a good case for cloud platforms and detection as code.

Cloud platforms continually move up the infrastructure stack to simplify and abstract extraordinarily complex concepts like pub-sub, container orchestration, queueing, and more. When writing detections in a universally recognized, flexible, and expressive language like Python, you can write more custom and complex detections to fit the precise needs of your enterprise.

Culture: Over 42 percent of the respondents indicate that they work in an organization whose culture is, in some way, creating additional hurdles for the security team. In an environment where on-prem software, servers, and networks still rule the day, SIEM implementation requires a high degree of coordination and cooperation with IT and operations teams. This type of situation has a long history of fostering a company culture in which security is seen as a necessary evil and not given a seat at the table where decisions affecting the company's direction are made.

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



_02 Expectations and Challenges

Top day-to-day challenges interacting with a SIEM are alerts, visibility, and writing rules

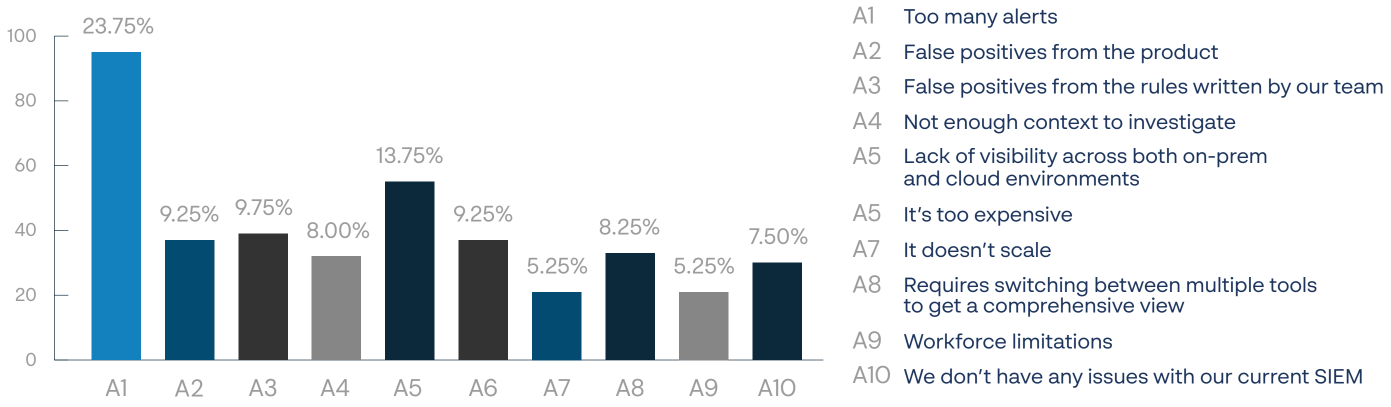
We wanted to know how the respondents interact with their current SIEM on a daily basis and what difficulties are presented. It is instructive for the entire community to understand where traditional SIEMs fall short routinely.

Too many alerts: Almost 24 percent of respondents indicated that the top challenge with their current SIEM is that it often generates too many alerts. Whether spurious or accurate, this result can cause alert fatigue or apathy, which leads to high-priority threats being ignored. This critical condition can cause data breaches to go unnoticed much longer than ever intended.

Lack of visibility across both on-prem and cloud environments: Many legacy approaches with on-prem infrastructure have strict limits on ingestion and retention. Nearly 14 percent of the respondents feel their biggest day-to-day challenge is related to a lack of visibility. To provide practitioners the information they need, purpose-built platforms with visibility across the entire enterprise are required. Designed to collect, assemble, parse, transmit, store, archive, and distribute this massive amount of security data, next-gen solutions can solve the lack of visibility challenge.

False positives from the rules written by our team: Nearly 10 percent of these SIEM users believe that their inability to write effective and efficient detection rules ends up hurting them in the long run. Often lacking in traditional SIEM is the ability to create custom-tailored rules, then programmatically test, version, and manage version control.

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



A SIEM's value and effectiveness depends on the sources of data and how well it has been architected, tuned, and maintained. Over the years, the industry's approach has been to keep extracting more and more security data — but with systems incapable of providing adequate visibility or effectively processing that much data. Most security professionals agree that automation is required to address the growing number of alerts and the high volume of false positives.

The Cyberwire Daily Briefing indicates that security personnel in U.S. enterprises waste approximately 25 percent of their time chasing false positives because security alerts or compromise indicators were erroneous. Security professionals feel angry and annoyed that they are still required to use SIEM technology that limits their ability to do their job.

_03 Capabilities

High-scale threat detection and response solutions are only now entering into a state of maturity — that is, if maturity is defined as having the capability to meet the demands of today's data-intensive and threat-ladened business environment.

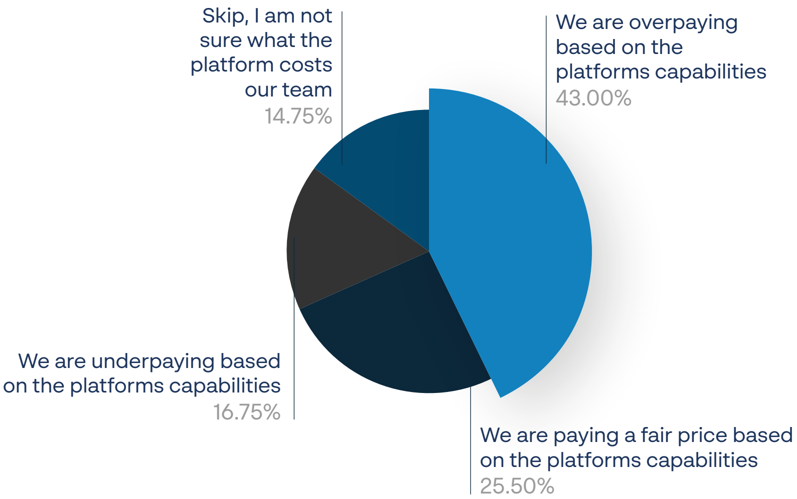
The questions in this section are designed to uncover how the respondents feel about their current solution and to discover, as accurately as possible, their perception of their SIEM's value as it relates to capabilities and cost.

43 percent believe they are overpaying

Over the years, data volumes have gone from GB/day to TB/day, yet the SIEMs never adjusted their model. As a result, teams are forced to pay millions of dollars for licensing not designed for cloud-scale volumes. Even worse, teams have to pick and choose log data to send to stay below platform limits.

Of those respondents who felt qualified to comment on the value of capabilities related to what they pay for their SIEM, over 50 percent believe they are overpaying. Only about 20 percent believe the value of their SIEM's capabilities exceeds the cost.

When thinking about the cost of your current SIEM platform, which of the following is most accurate?



Most and least satisfying capabilities

When faced with the primary capabilities of a traditional SIEM and asked to rate them according to how satisfied they are with their existing platform, an interesting picture emerged. It was not a picture of extreme satisfaction versus utter disappointment. Instead, the results of this exercise produced an image of consistency across the board.

The winners in the "Very Satisfied" category are:

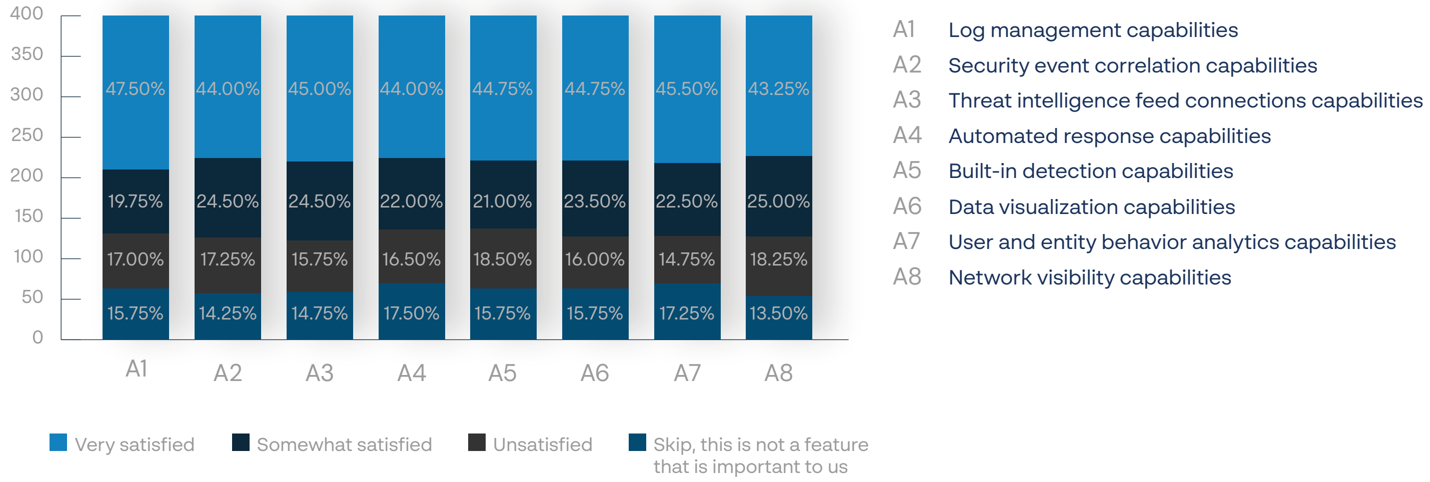
- Log management: 190 very satisfied and 63 unsatisfied responses.
- User and entity behavior analytics: 182 very satisfied and 69 unsatisfied responses.
- Threat intelligence feed connections: 180 very satisfied and 59 unsatisfied responses.

The "Unsatisfied" category yields:

- Built-in detection: 74 unsatisfied and 179 very satisfied responses.
- Network visibility: 73 unsatisfied and 173 very satisfied responses.
- Security event correlation: 69 unsatisfied and 176 very satisfied responses.

Note that no capability received a very satisfied vote from even half of the respondents. And, across all the capabilities, there was barely more than a 4 percent spread in either very satisfied or unsatisfied ratings.

How satisfied are you with your existing SIEM platforms capabilities listed below?

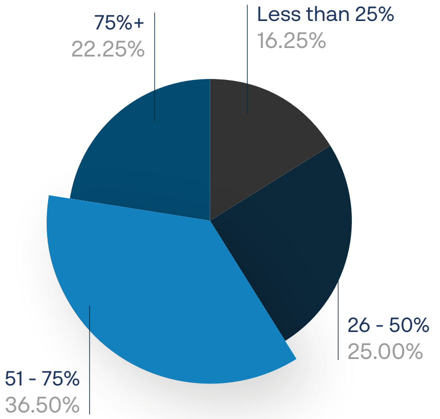


How much data is covered

The results of this topic underscore the need for high-scale monitoring and reliable, fault-tolerant, and elastic data processing pipelines to handle security data. SIEM tools do the bare minimum to help teams get their data in and do not provide repeatability, best practices, or structured data.

Less than 77 percent of the respondents believe that their SIEM covers even 75 percent of their data. Nearly 17 percent understand that their existing platform covers less than a quarter of their data.

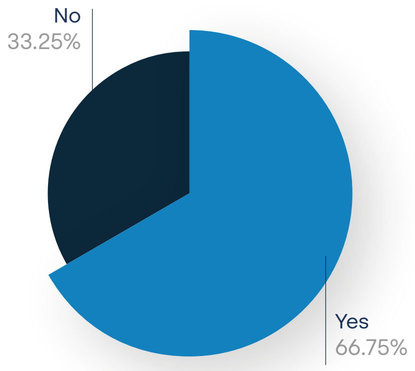
What percentage of your security data is covered by your existing SIEM platform?



One third believe their SIEM will not be able to keep up

When asked if they believe their current SIEM platform will be capable of handling the volume of security data their organization generates in the future, a third of the respondents expect their existing platform to keep falling behind.

Do you believe your current SIEM platform will be capable of handling the volume of security data your organization generates in the future?



SIEMs were designed over ten years ago when the world was a very different place. Essentially they haven't changed their approach in the last decade. Effective security today depends on solid data pipelines, structured data, and cloud-first workflows.

Security professionals are aware of the static nature of traditional SIEM platforms. Many feel they pay too much for the capabilities provided and are concerned about what the future holds.

_04 Outlook For the Future

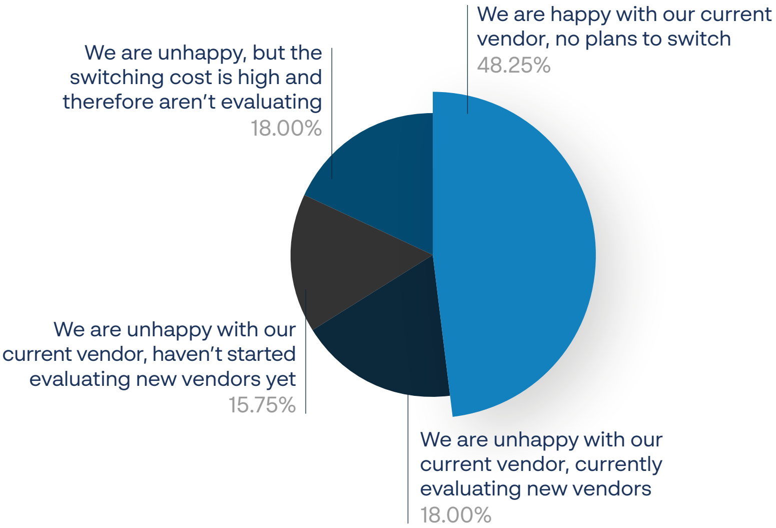
This section presents answers to critical questions about our respondents' intentions to stick with their current platform or find something more suitable for their needs. We extend those questions to discover the “why” behind their intentions and the “what” that motivates them.

Are you happy with your current SIEM vendor?

Over 50 percent of our respondents are not happy with their current SIEM vendor. This is a large number by any standard.

Our survey participants have problems and infrastructure similar to many companies using SaaS services to do their jobs. They can not, and should not, spend time and energy building, tuning, maintaining, and scaling software they can easily purchase. Instead, they should work with vendors who work to solve the challenges uncovered in this survey full-time and have entire teams dedicated to the success of their platform.

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



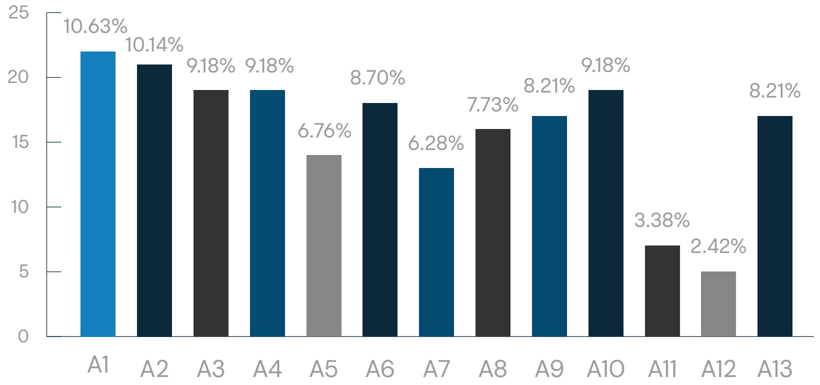
Why are you unhappy with your current platform?

For those respondents that indicated they are unhappy with their current platform, their top three “why” answers are:

- Cost - 10.6 percent
- Lack of features and functionality - 10.1 percent
- At 9.2 percent we have a three-way tie for product usability, lack of ability to customize, and technical support.

The inadequacies of traditional SIEM technology can very quickly become overwhelming, baffling, and frustrating. No longer can security teams be forced into high-scale operational roles. This outdated paradigm takes too much valuable time away from detecting, responding, and automating the analysis of potentially nefarious activity. Additionally, teams need to write code and produce more elegant solutions for analysis, moving away from strictly defined and specialized languages.

If unhappy, what is your primary reason you are unhappy with your current platform?



A1	Cost
A2	Lack of features/functionality
A3	Product usability
A4	Lack of ability to customize or extend product
A5	Solution complexity
A6	Difficult to run at scale
A7	Migrating to a managed service
A8	More innovation from a new vendor
A9	Too complicated to add new data feeds/logs
A10	Technical support issues
A11	Poor product quality
A12	Poor detection and alerting
A13	Other

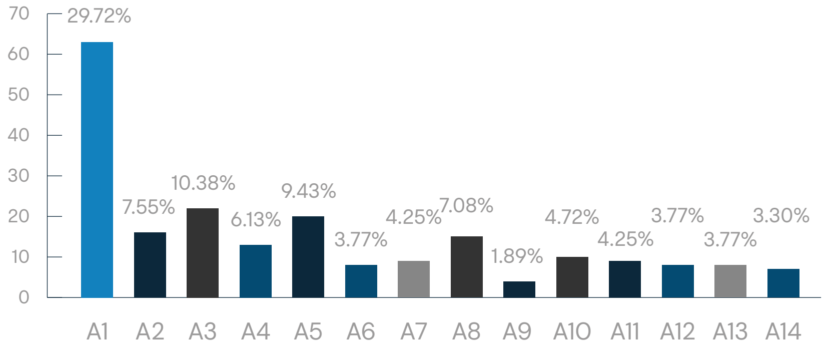
If happy, why would you switch to a new vendor?

Even those respondents who indicated they were happy with their current vendor would be willing to change vendors for a better price, more usability, or less complexity.

- Nearly 35 percent said cost is the factor that would cause them to switch vendors.
- Product usability came in second with over 11 percent, citing this as a good reason to change.
- For less complexity, almost 9 percent are willing to throw out their current vendor.

Using tools that are cloud-services or cloud-centric likely come with an ideal pricing model and less operational burden.

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



A1	Cost
A2	Lack of features/functionality
A3	Product usability
A4	Lack of ability to customize or extend product
A5	Solution complexity
A6	Difficult to run at scale
A7	Migrating to a managed service
A8	More innovation from a new vendor
A9	Lack of inovation with current platform
A10	Too complicated to add new data feeds/logs
A11	Technical support issues
A12	Poor product quality
A13	Poor detection and alerting
A14	Other

What features and capabilities are most important to you?

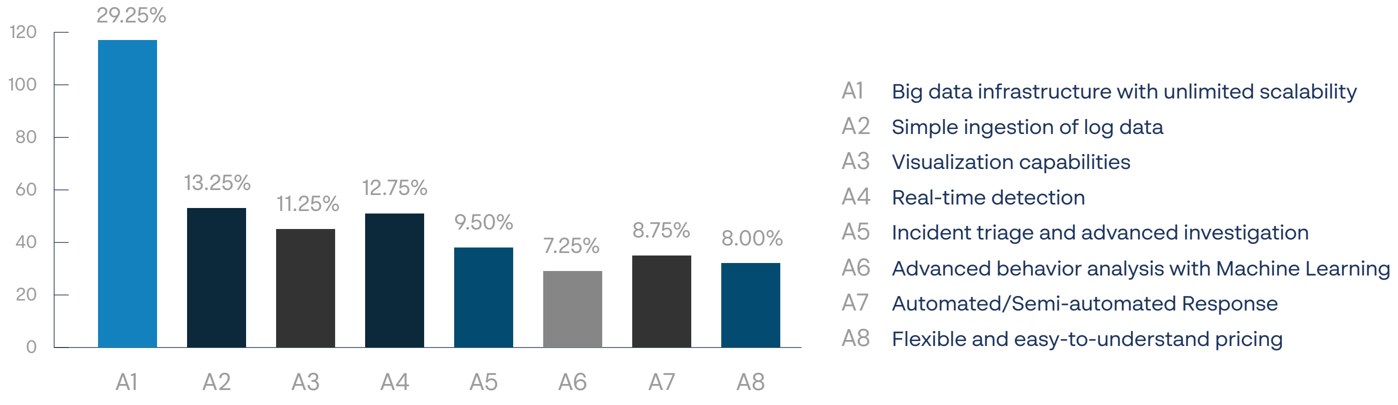
With a statement that speaks loud and clear about where the respondents see the future, the vast majority of those that intend to change vendors are most attracted to features and capabilities related to big data and scalability.

When asked what features and capabilities are most important to them:

- Over 29 percent answered that big data infrastructure with unlimited scalability is the most important.
- Over 13 percent are attracted by simple ingestion of log data.
- Nearly 13 percent most want real-time detection capability.

Data volumes are not stopping; practitioners should embrace cloud services like data lakes and SaaS services to make their life easier. Relying on services provides less control but with the advantage of very minimal overhead, which is very much worth it in a small team.

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



Conclusion

This survey's responses clearly indicate that traditional SIEM platforms fail to provide a robust enough solution for detection at scale. Security teams are, in large part, stuck using these tools even though they can't get anywhere close to the scale and flexibility they need to do their jobs.

After long delays in deployment and implementation, practitioners are met with unsatisfactory results in query speed and system complexity. Too many alerts, lack of visibility, and difficulty creating effective rules add to the mounting frustration of those charged with protecting sensitive data and critical infrastructure.

Outdated pricing models prevent many organizations from implementing solutions that can meet their current needs, not to mention scale to include the avalanche of security data the future will surely bring.

Detection-as-code, automation, and big data infrastructure and scalability must be an integral part of tomorrow's detection and response platforms.

panther

Thank you

runpanther.io