2022

Cybersecurity
INSIDERS

SIEM REPORT

coresecurity
by HelpSystems

INTRODUCTION

The dramatic rise and evolution of cyber threats make rapid and effective management of security incidents essential in protecting organizations' data, identities, and IT assets.

This survey shows the important role security Information and Event Management (SIEM) platforms play in helping organizations better identify and act on security threats and suspicious activities before they cause significant damage.

The 2022 SIEM Report is based on a survey of 348 cybersecurity professionals and represents one of the industry's most comprehensive annual studies on SIEM, exploring the latest trends, key challenges, and solution preferences in this market.

Key findings include:

- 80% of cybersecurity professionals consider SIEM very to extremely important to their organization's security posture – up six percentage points from last year.
- 85% rate their SIEM as effective in identifying and remediating threats – up five percentage points from last year.
- Organizations report that the main benefits they are realizing with SIEM include more efficient security operations (21%), faster detection and response (14%), and better visibility into threats (13%).
- 81% confirm SIEM has improved their ability to detect and respond to threats – up five percentage points from last year.

We would like to thank Core Security, by HelpSystems, for supporting this unique research.

We hope you enjoy this report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

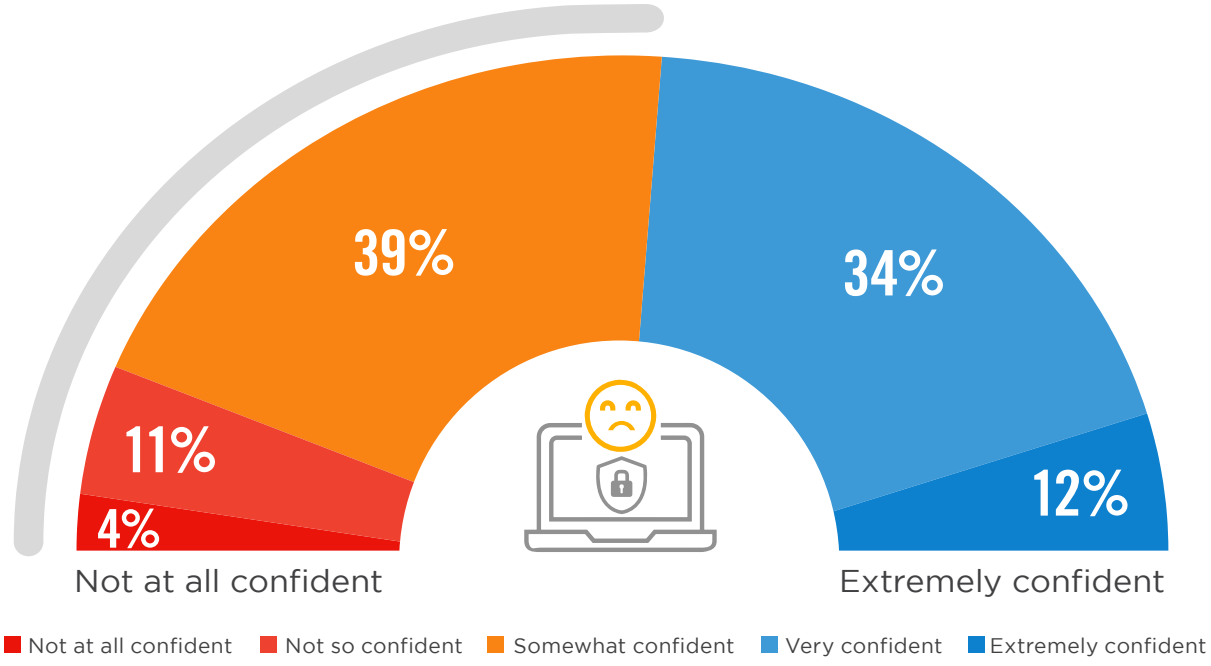
CONFIDENCE IN SECURITY POSTURE

Over half of cybersecurity professionals (54%) feel, at best, only somewhat confident in their security posture. This shows a deterioration in confidence (by three percentage points) over last year and suggests that breaches and a worsening threat environment are having a negative impact on security confidence within many organizations.

How confident are you in your organization's overall security posture?

An increase of three percentage points from last year

54% feel, at best, only somewhat confident in their organization's overall security posture

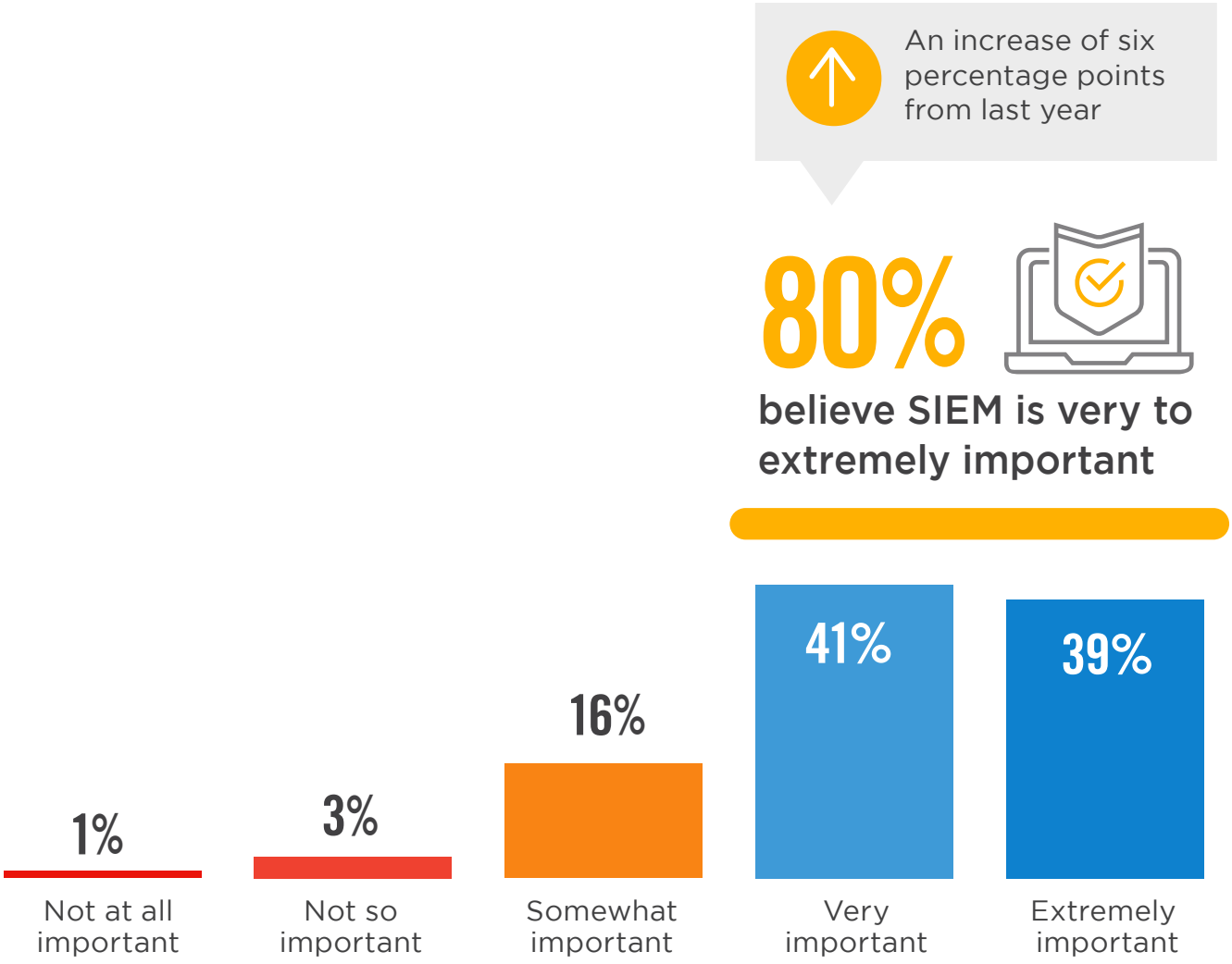


Organizations that actively use SIEM solutions report higher levels of confidence, with a majority (60%) being very or extremely confident in their security posture, whereas only 46% of those without SIEM report being very or extremely confident.

IMPORTANCE OF SIEM

So how important is SIEM to organizations' security postures? Eighty percent of cybersecurity professionals rate their SIEM solutions, which perform real-time analysis of security alerts and prioritize threats from many different types of data sources, extremely important to their security posture (up six percentage points from last year).

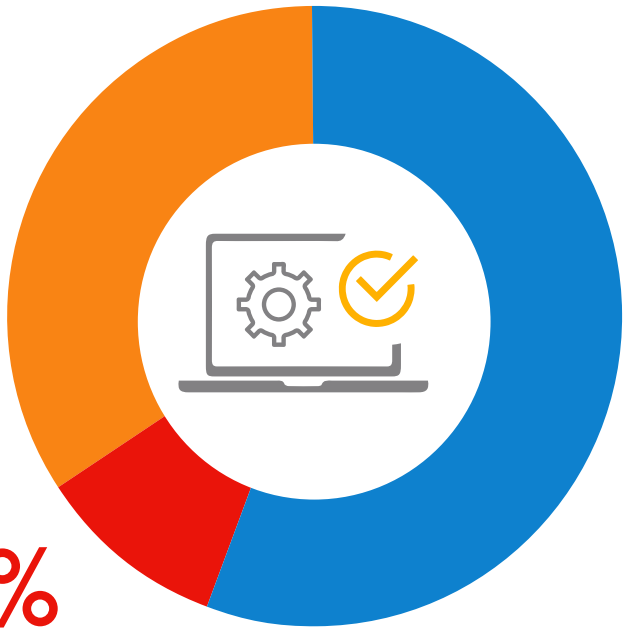
How important is SIEM to your organization's security posture?



SIEM ADOPTION ON THE RISE

When asked if organizations are actively using SIEM, more than half (56%) of those surveyed confirmed they already use SIEM platforms for security information and event management. Thirty-four percent are planning to implement SIEM in the near future, showing that SIEM is being prioritized by organizations as they are maturing their security programs.

Does your organization actively use a SIEM platform or service?



34%
NO, but SIEM is planned in the future

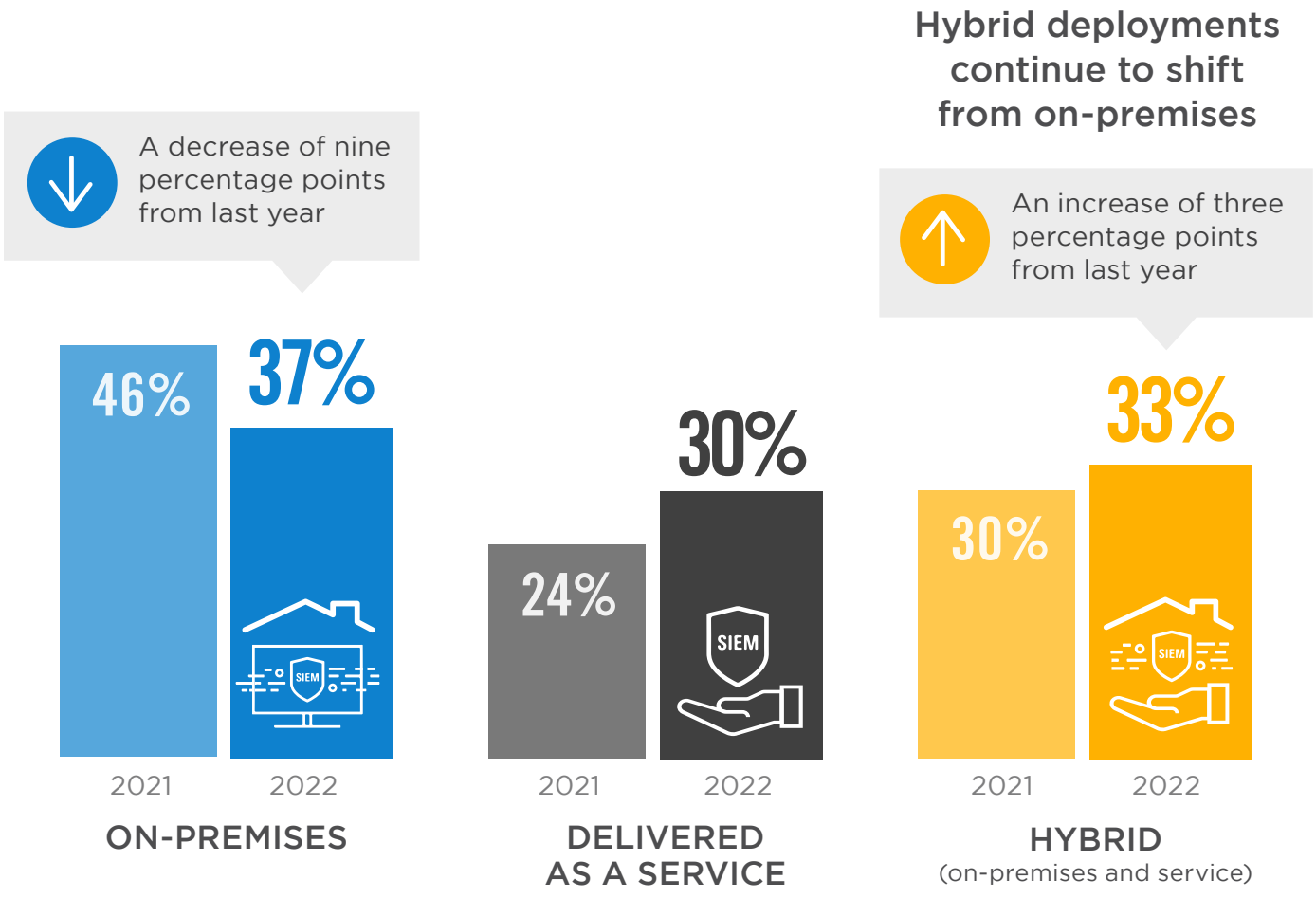
56%
YES, we use SIEM

10%
No plans to use SIEM

SIEM DELIVERY

Since last year, a continued shift is visible from traditional, on-premises SIEM deployment to hybrid (33% – up three percentage points from last year) and service-based components (30% – up six percentage points from last year). While over one-third of SIEM deployments are still delivered on-premises (37%), this represents a significant drop of nine percentage points since last year.

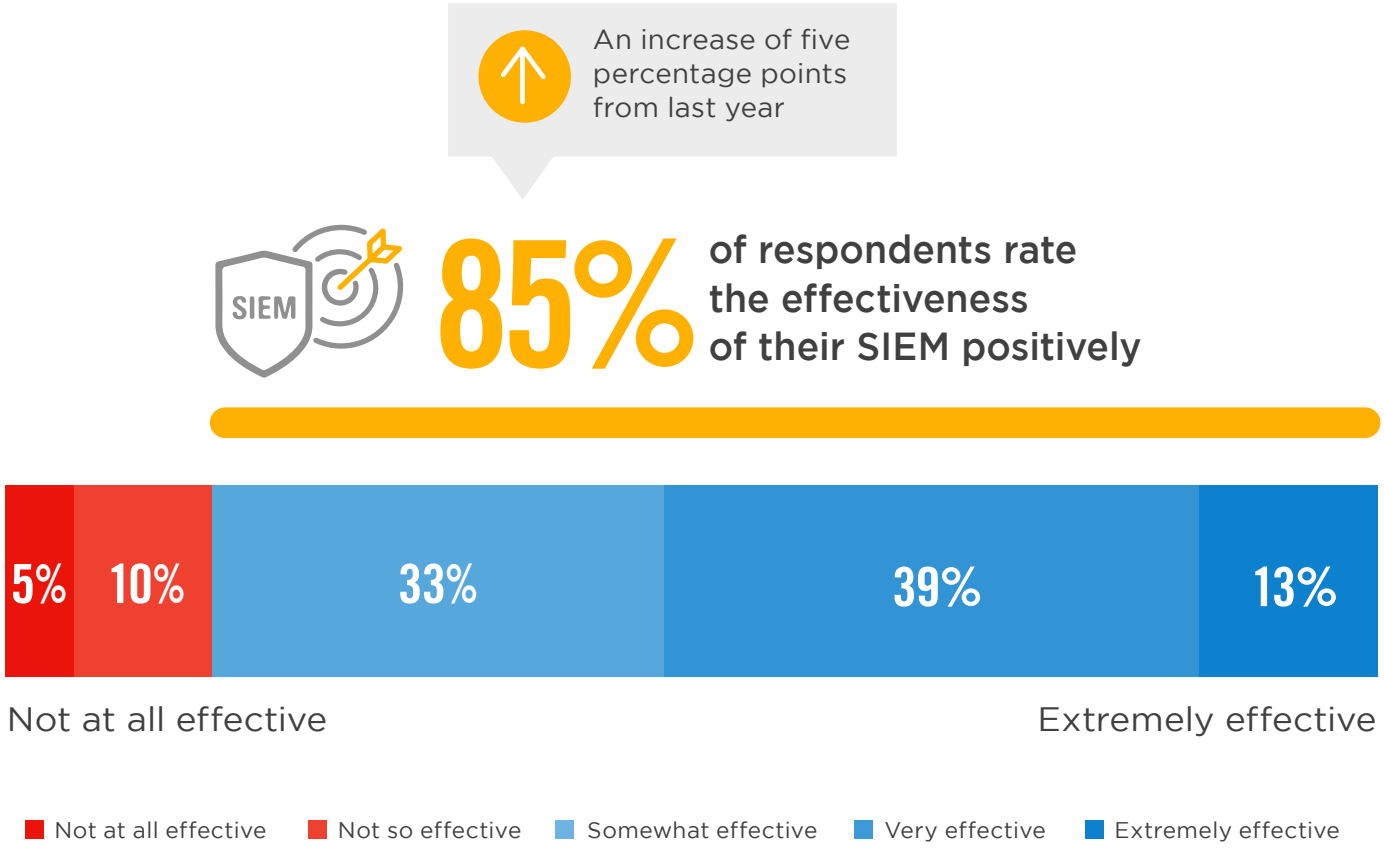
Is your SIEM planned/delivered as a managed service (SaaS) or as software installed on premises?



SIEM EFFECTIVENESS

Most organizations (85%) in our survey rate the effectiveness of their SIEM platform positively in its ability to identify and remediate cyber threats. This is an increase of five percentage points since last year. Among active SIEM users, the effectiveness ratings increase to 89% of organizations.

How would you rate your organization's effectiveness in using SIEM to identify and remediate cyber threats?



SIEM BENEFITS

We asked survey participants about the key benefits they are realizing from SIEM. More efficient security operations jumped to the top of the benefit list (21% – up eight percentage points from last year). This is followed by faster detection of and response to security events (14%) and better visibility into threats (13%) – all key elements of the core value proposition of SIEM.

What main benefit is your SIEM platform providing?

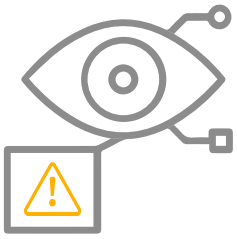
An increase of eight percentage points from last year

21%

More efficient security operations

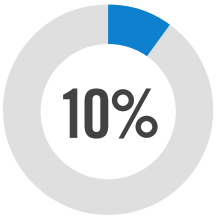
14%

Faster detection and response

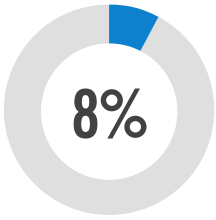


13%

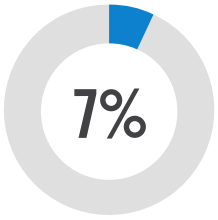
Better visibility into threats



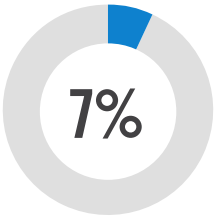
Better compliance posture



Better collection of threat data



Better threat analysis



Better reporting of threat management

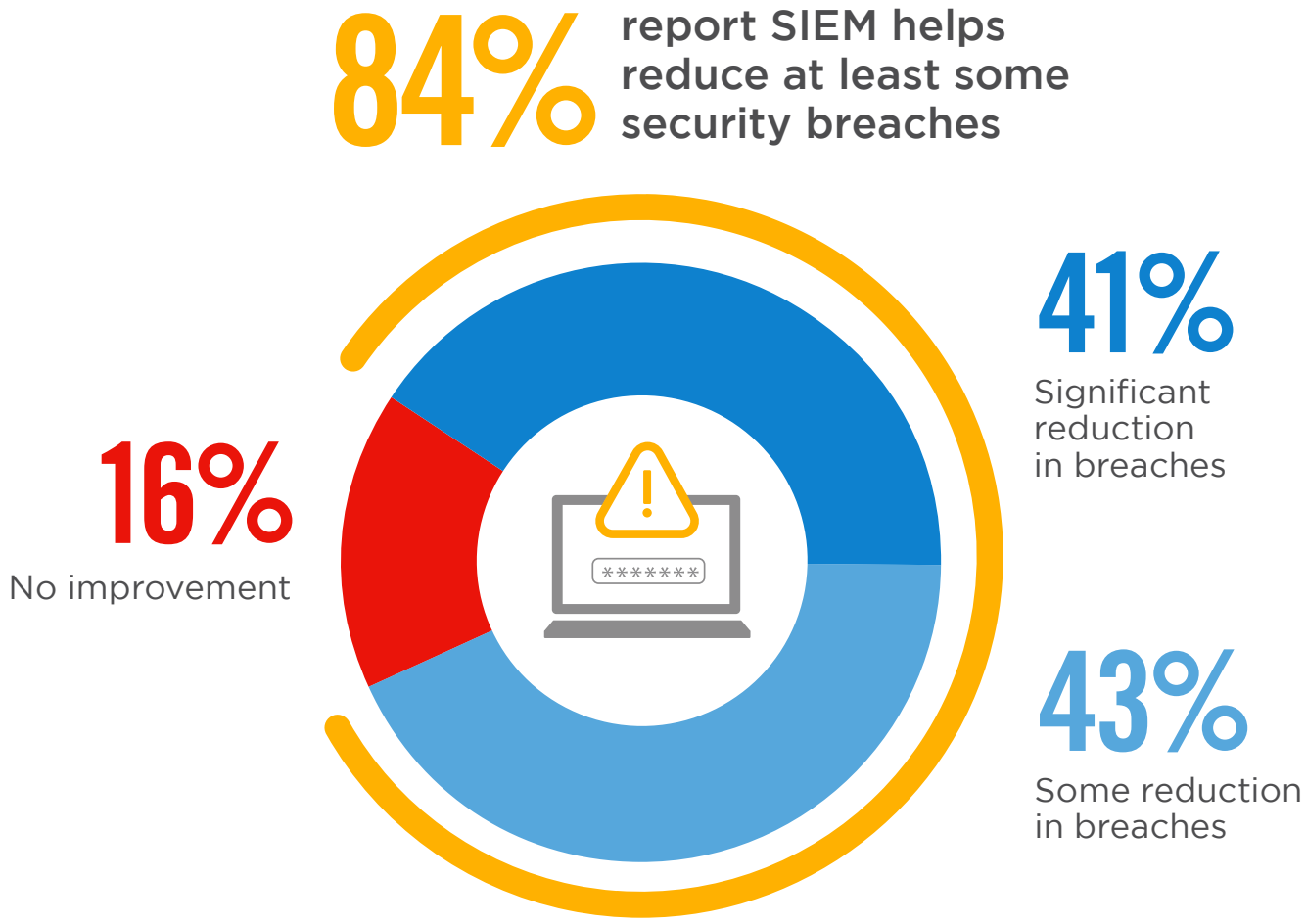
An increase of five percentage points from last year

Better prioritization of indicators of compromise (IOC) 6% | Reduced staff workload through automation 6% | Better threat remediation 3% | No benefits 2% | Other 3%

FEWER BREACHES WITH SIEM

How well can SIEM reduce the occurrence of security breaches? A significant majority (84%) of organizations in our survey have experienced a measurable reduction of security breaches as a result of using SIEM, confirming the technology's overall value and effectiveness.

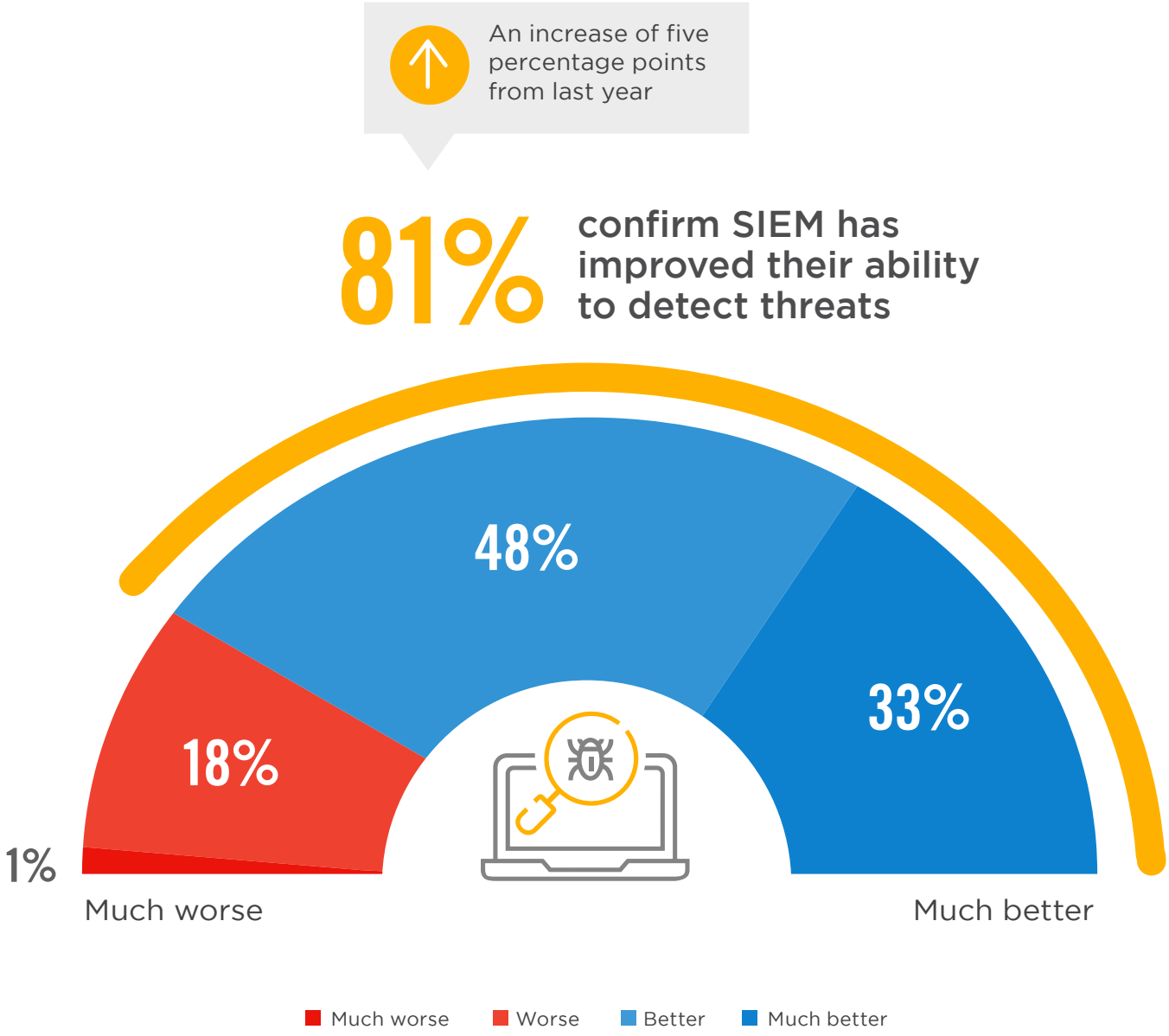
Has the occurrence of security breaches in your organization changed as a result of using SIEM?



SIEM THREAT DETECTION

How does SIEM improve an organization's ability to better detect threats? More than eight out of 10 of survey respondents confirmed their SIEM resulted in an improved ability to detect threats (81% – up five percentage points from last year).

How has your ability to detect threats changed after implementing SIEM?



FASTER DETECTION WITH SIEM

Speed of detection is crucial, as damage can increase significantly with the amount of time infections can dwell in a system. More than three quarters of survey participants (78%) indicate their SIEM can detect possible security events within hours. Half of the organizations can even detect the events within minutes (50%).

How quickly can your SIEM platform typically detect possible security events or compromise?

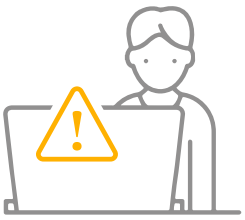
78% can detect security events within hours, and half of them within minutes

ATTACK DETECTION

Survey respondents report that SIEM technology is still the most effective solution at detecting unauthorized access (66% – up three percentage points from last year). This is followed by detection of malware (61%) and web application attacks (52% – up eleven percentage points from last year). When compared to last year's results, we observe an increase in SIEM technology effectively detecting virtually every type of attack.

Which types of attacks is SIEM technology most effective in detecting?

An increase of three percentage points from last year



66%

Unauthorized access

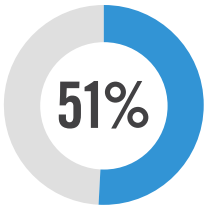
61%

Malware (viruses, worms, trojans)

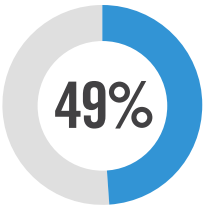
An increase of eleven percentage points from last year

52%

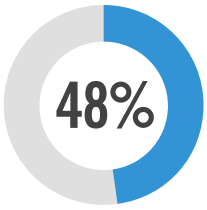
Web application attacks (buffer overflows, SQL injections, cross-site scripting)



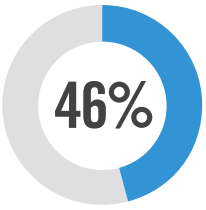
Hijacking of accounts, services, or resources



Advanced Persistent Threats (APTs)/ targeted attacks



Denial of service attacks (DoS/DDoS)



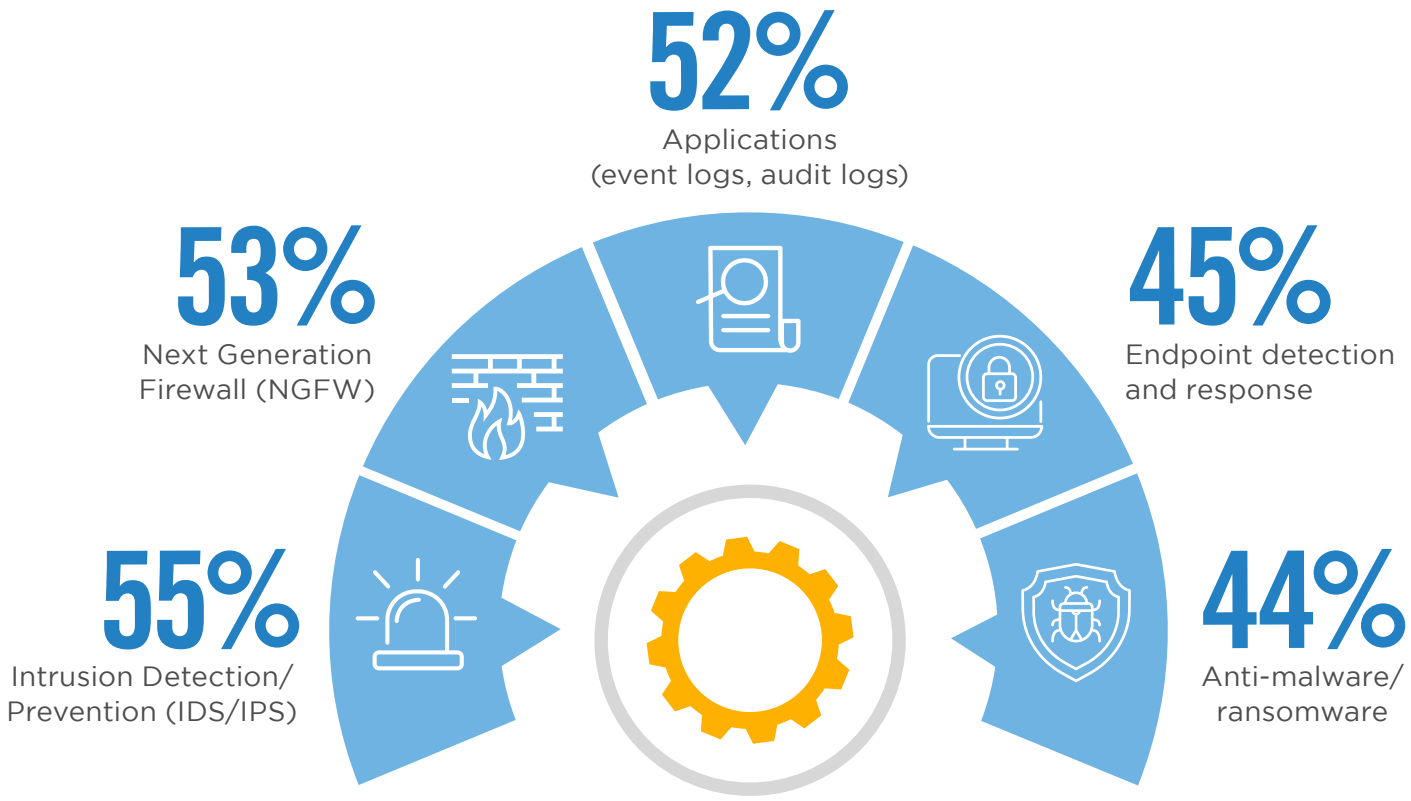
Insider attacks (malicious or careless insiders)

Ransomware 38% | Phishing attacks 36% | Zero-day attacks (against publicly unknown vulnerabilities) 28% | Cryptojacking 21% | Other 8%

SIEM INTEGRATION

What systems and applications do organizations typically integrate with their SIEM platforms to increase the scope of data that is analyzed to alert and report on security events? According to our survey respondents, organizations most commonly integrate intrusion detection and prevention systems (IDS/IPS) (55%), followed by Next Generation Firewalls (NGFW) (53%) and applications to analyze event and audit logs (52%).

What systems, services, and applications are integrated with your SIEM platform?



Identity and Access Management (IAM) 43% | Server data (IBM i/AS400, Linux, UNIX, Windows) 40% | Network access control (NAC) 40% | Threat intelligence from security vendors 39% | Data loss prevention (DLP) 39% | Web application firewall (WAF) 35% | Static endpoints (PC, endpoint protection, log collectors) 33% | Vulnerability management tools (scanners, configuration and patch management, etc.) 31% | Cloud activity 31% | Security intelligence feeds from third-party services 29% | Whois/DNS/Dig and other Internet lookup tools 28% | Vulnerability management (VM) 28% | Anti Denial of Service solution (Anti DDoS) 28% | Dedicated log management platform 27% | User behavior monitoring 27% | Unified threat management (UTM) 26% | Network packet-based detection 25% | Netflow 24% | Other 6%

SIEM USE CASES

What are the most important use cases for SIEM? Organizations report that monitoring, correlation, and analysis of event data across multiple systems and applications (71%) is the most common use case for their SIEM platform. This is followed by discovery of external and internal threats (51%) and user activity monitoring (44%).

What are the most important use cases you utilize your SIEM platform for?

71%

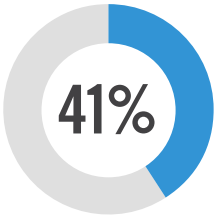
Monitor, correlate, and analyze activity across multiple systems and applications

51%

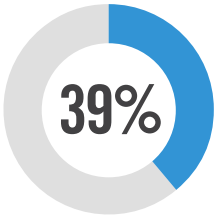
Discover external and internal threats

44%

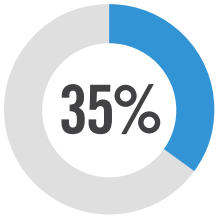
Monitor the activities of users



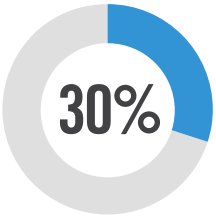
Monitor server and database access



Detect threats in cloud architecture including cloud access control (CASB)



Provide compliance reporting



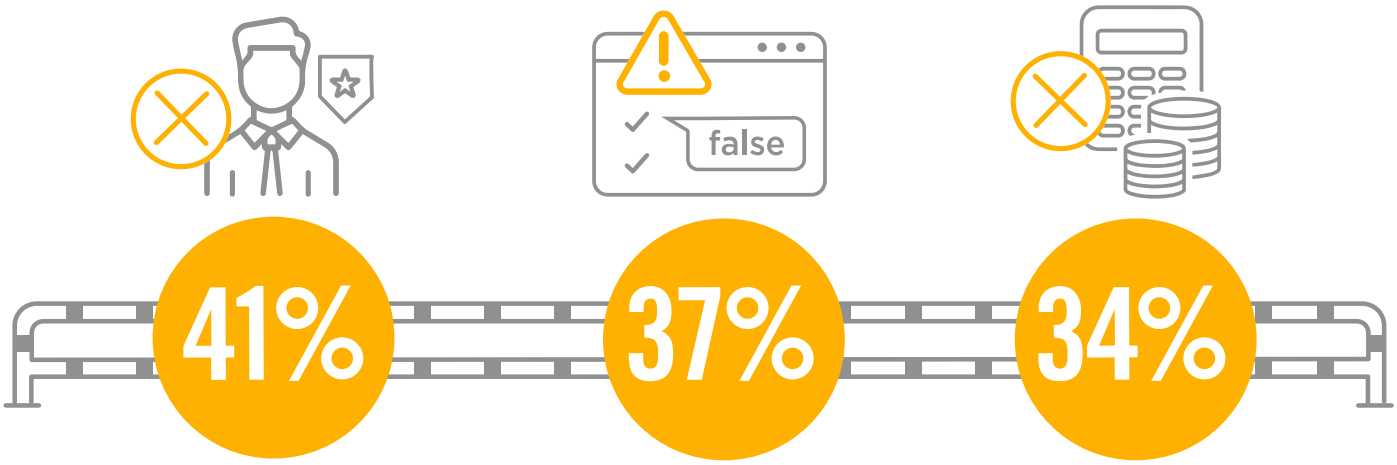
Monitor a combination of cloud and on-premises infrastructure

Provide analytics and workflow to support incident response 29% | Detect industry/vertical specific attacks (e.g. healthcare break-the-glass, financial fraud) 24% | Other 5%

HURDLES TO SIEM SUCCESS

When asked what hurdles organizations are experiencing in maximizing the value of their SIEM platforms, lack of skilled staff to effectively operate SIEM remained the biggest challenge (41%). This is followed by handling too many false positives (37%) and lack of budget (34%). The numbers are lower than in previous surveys, suggesting that organizations are improving on their use of SIEM platforms.

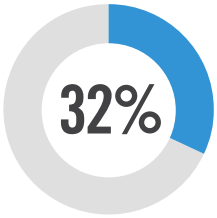
What are your biggest hurdles in maximizing the value of your SIEM platform?



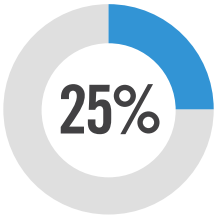
Lack of skilled/trained staff to operate effectively

Too many false positives

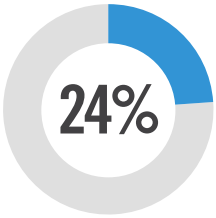
Lack of budget



System complexity



Poor integration/ interoperability between security solutions



Lack of contextual information from security tools

Having to manually create/refine rules 23% | Company culture 22% | Lack of security awareness among employees 19% | Lack of visibility into network traffic and other processes 19% | Lack of management support/awareness/buy-in 17% | Difficulty implementing and deploying the solution 16% | Insufficient or inadequate tools available in-house 15% | Poor vendor support 14% | Lack of effective security solutions available in the market 10% | Other 10%

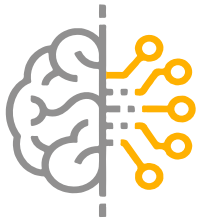
SIEM CAPABILITIES

The most important SIEM capabilities to organizations include real-time analysis and alerting of potential threats (58%), threat intelligence integration (51%), and correlating and linking individual events into useful information (49%).

What SIEM capabilities are most important to you?

58%

Real-time analysis and alerting of potential threats

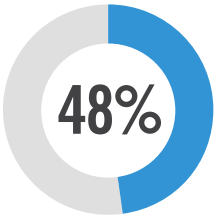


51%

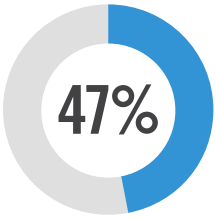
Threat intelligence integration

49%

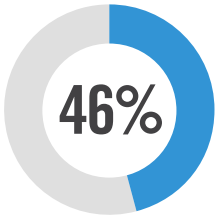
Correlation and linking of individual events into useful information



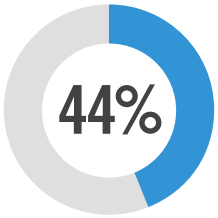
Collection of security event information in a central repository



Incident response and forensics



Advanced analytics (such as artificial intelligence (AI) or machine learning (ML))



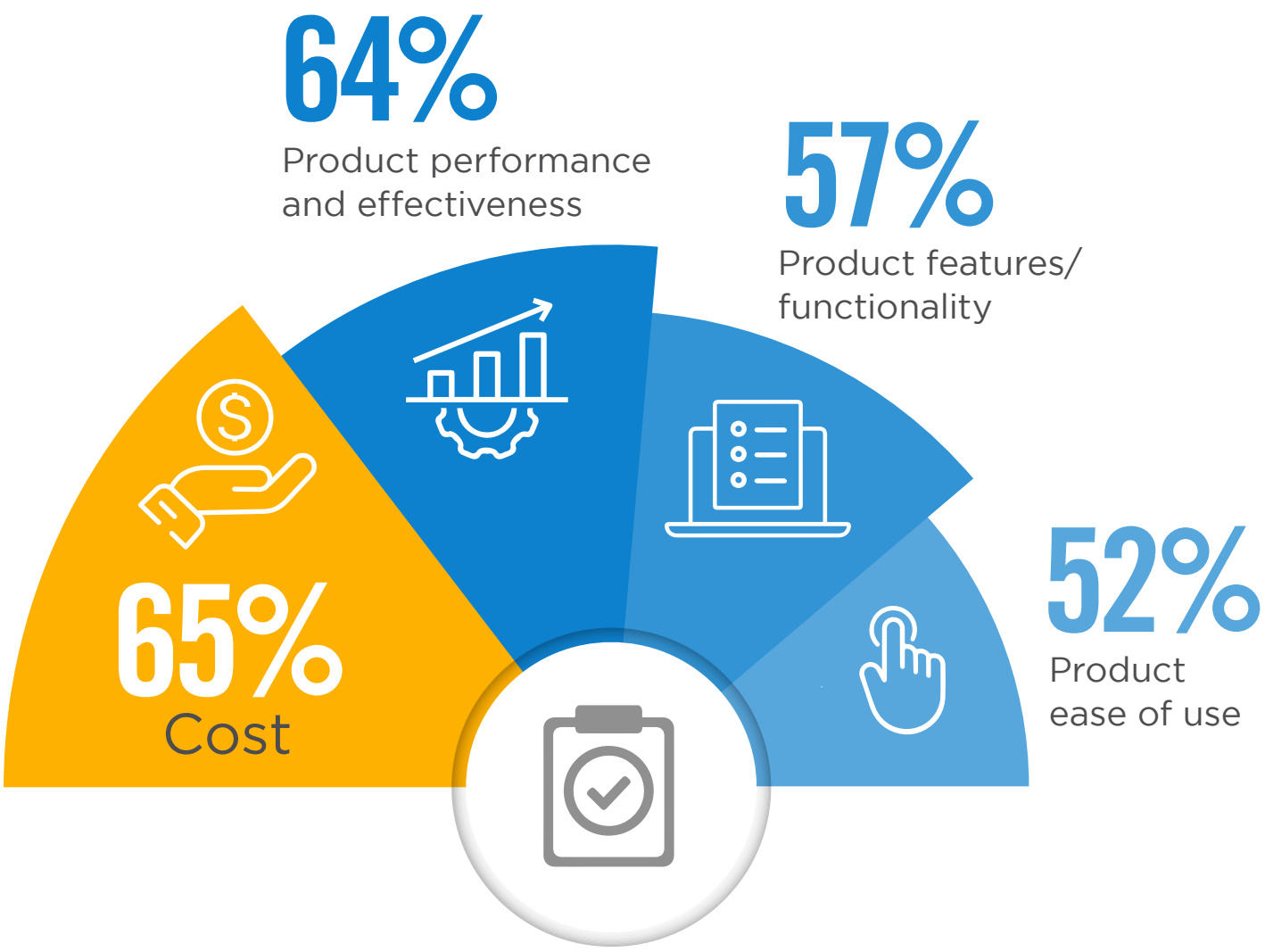
Threat prioritization

Dashboards 41% | Advanced threat detection 41% | Reporting 39% | Data, system & application monitoring 39% | User monitoring 37% | Support of compliance requirements 34% | Workflow and case management 30% | Retention of historical data and forensic analysis 30% | Ability to customize platform to organization-specific requirements 24% | Multi-Tenancy 18% | Other 3%

SIEM EVALUATION CRITERIA

How do organizations decide which SIEM solution to select? Among the key evaluation criteria, cost rose to the top of the list (65% – up five percentage points from last year). This is followed by product performance and effectiveness (64% – up five percentage points from last year), pushing product features and functionality to third place (57% – down nine percentage points from last year).

What criteria do you consider most important when evaluating a SIEM solution?

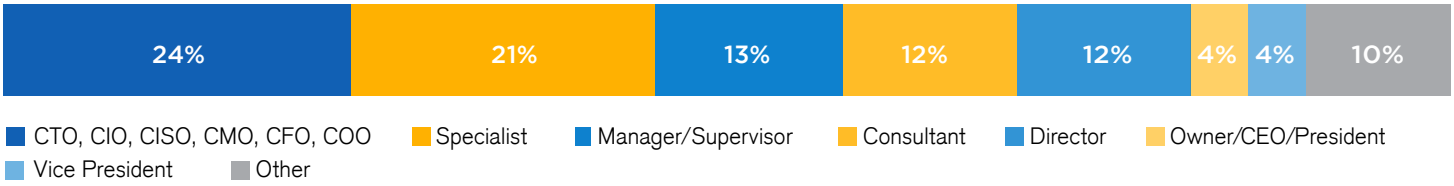


Support 51% | Vendor experience and reputation 43% | Customer reviews 23% | Other 3%

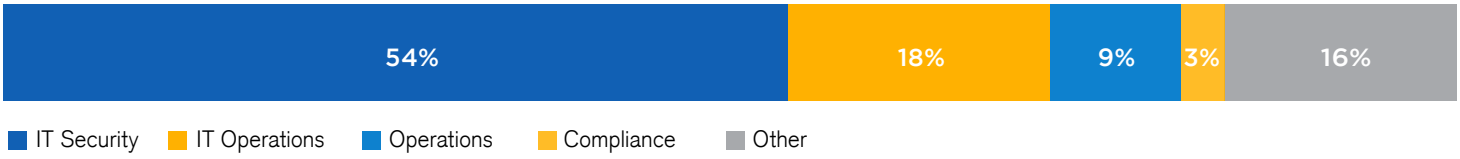
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 348 IT and cybersecurity professionals in the US, conducted in March 2022, to gain more insight into the latest trends, key challenges, and solutions for SIEM. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

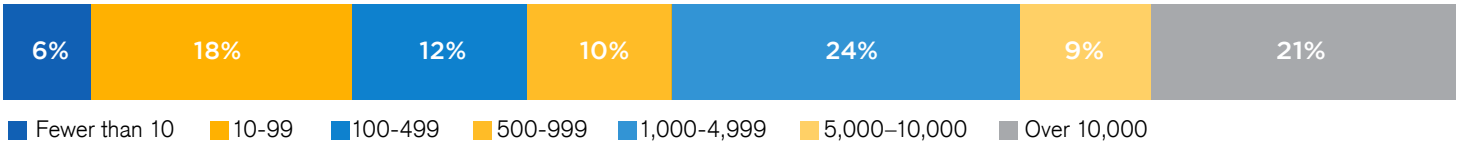
CAREER LEVEL



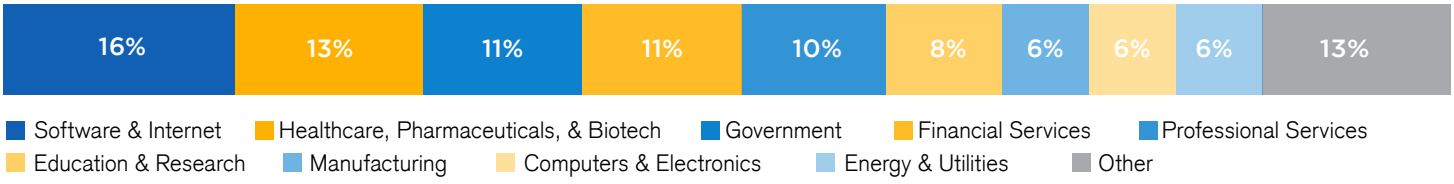
DEPARTMENT



COMPANY SIZE



INDUSTRY



Core Security provides leading-edge cyber threat prevention and identity governance solutions to help you prevent, detect, test, and monitor risk in your business.

www.coresecurity.com

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com