2019

Cybersecurity
INSIDERS

SIEM REPORT

helpsystems

INTRODUCTION

Security Information and Event Management (SIEM) is a powerful technology that allows security operations teams to collect, correlate and analyze log data from a variety of systems across the entire IT infrastructure stack to identify and report security threats and suspicious activity.

The 2019 SIEM Report represents one of the most comprehensive surveys on SIEM to date, designed to explore the latest trends, key challenges, and solution preferences for SIEM.

The survey reveals that three-quarters of cybersecurity professionals confirm SIEM is very important to extremely important to their organization's security postures (76%). An impressive eight out of 10 SIEM users are satisfied with the effectiveness of their SIEM platform (86%). They say SIEM delivers on the promise of #1 faster detection and response, #2 more efficient security operations, and #3 better visibility into threats as the highest ranked benefits. For more than 7 out of 10 organizations, SIEM resulted in better detection of threats and a measurable reduction in security breaches. Survey participants consider SIEM most effective for #1 detecting unauthorized access, #2 advanced persistent threats, and 3# insider attacks. The single biggest hurdle to maximizing the value of SIEM continues to be the lack of skilled security staff, providing an opportunity for additional automation of threat management. When it comes to threat management priorities for the next 12 months, cybersecurity professionals focus on improving threat detection (55%), followed by proactive hunting for cyber threats (48%) and improved investigating and analyzing of threats (44%).

We would like to thank HelpSystems for supporting this unique research.

We hope you will enjoy the report.

Thank you,

Holger Schulze

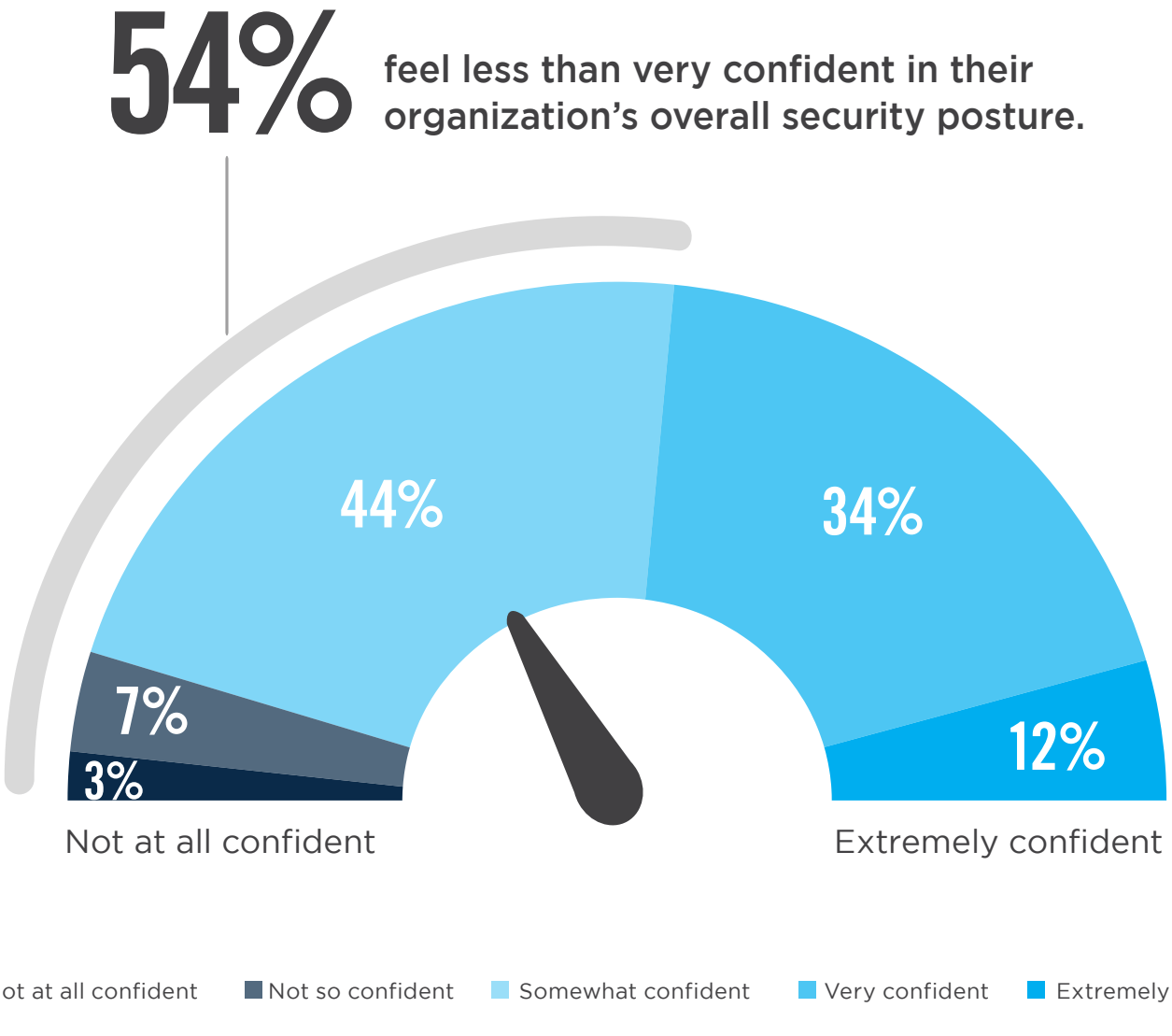
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

CONFIDENCE IN OVERALL SECURITY POSTURE

A majority of cybersecurity professionals (54%) feel less than very confident in their organization's overall security posture.

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

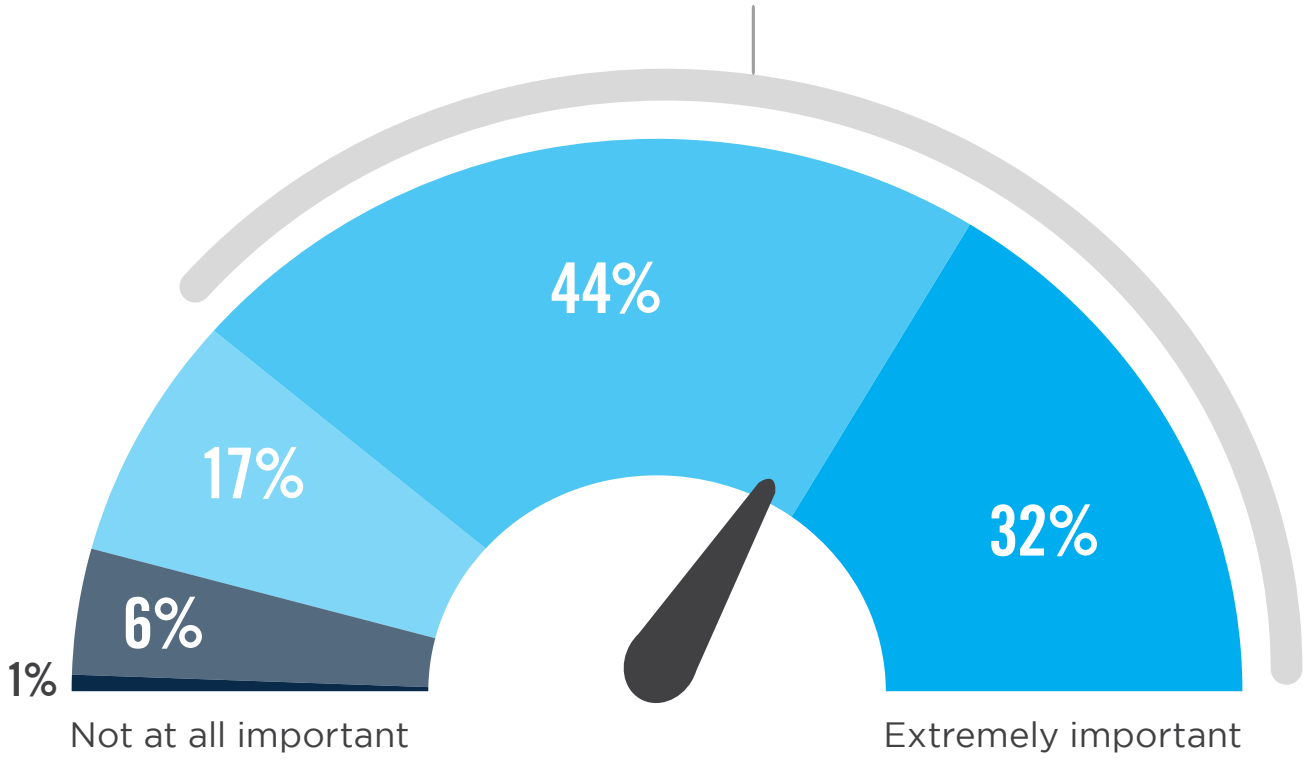


IMPORTANCE OF SIEM

Among the various security controls and technologies, SIEM plays a very to extremely important role in organizations' security postures, according to a large majority of IT security professionals (76%).

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

76% **Believe SIEM is very to extremely important to organizations' security postures.**



Not at all important | Not so important | Somewhat important | Very important | Extremely important

SIEM USE

Seven out of 10 organizations in our survey already use SIEM platforms for security information and event management. Twenty percent are planning to implement SIEM in the future. Of the SIEM adopters, almost eight of 10 organizations have been using SIEM for at least one year and 40% for more than three years.

Does your organization actively use a SIEM platform or service?

69%
YES, we use SIEM

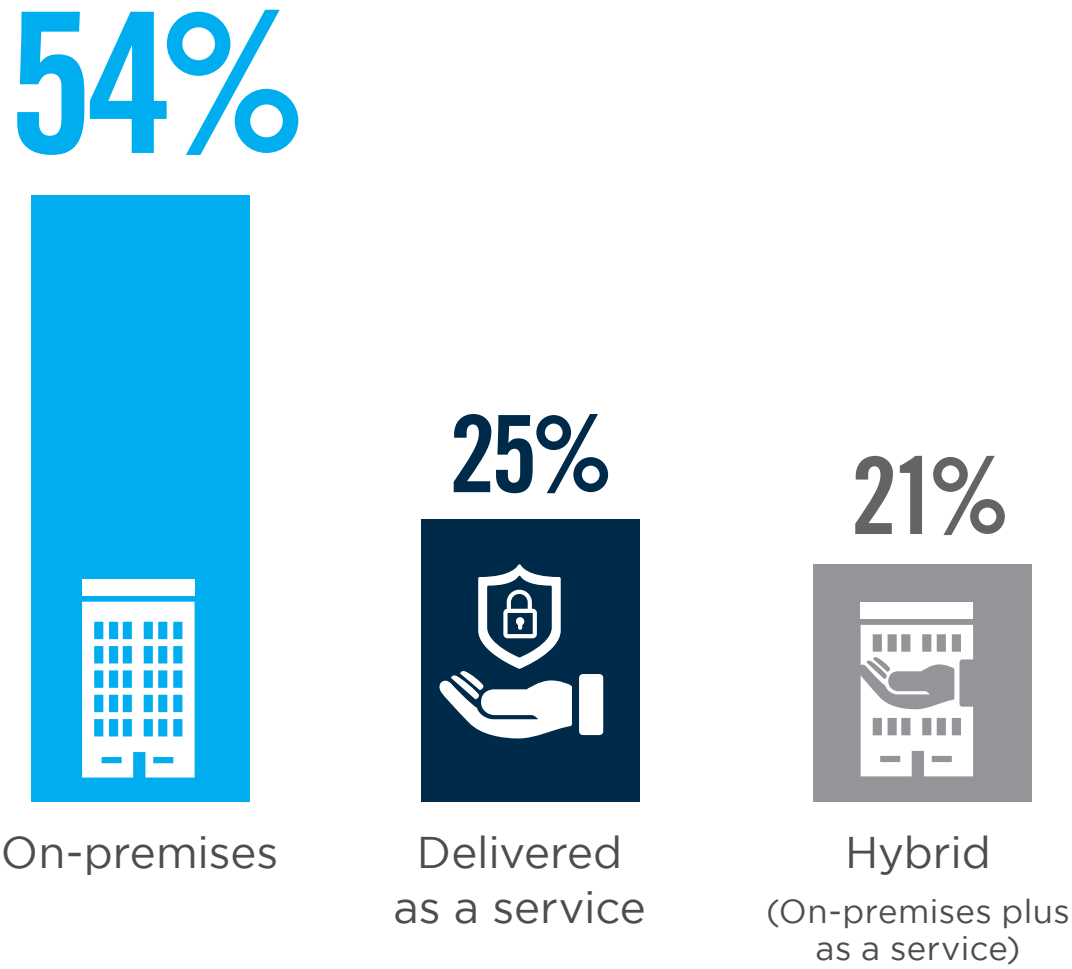
21%
NO, but SIEM is planned in the future

10%
No plans to use SIEM

SIEM DELIVERY

The majority of SIEM deployments are delivered on premises (54%). SIEM as a service is gaining momentum, either as a dedicated service (25%) or delivered in hybrid on-prem / service models (21%).

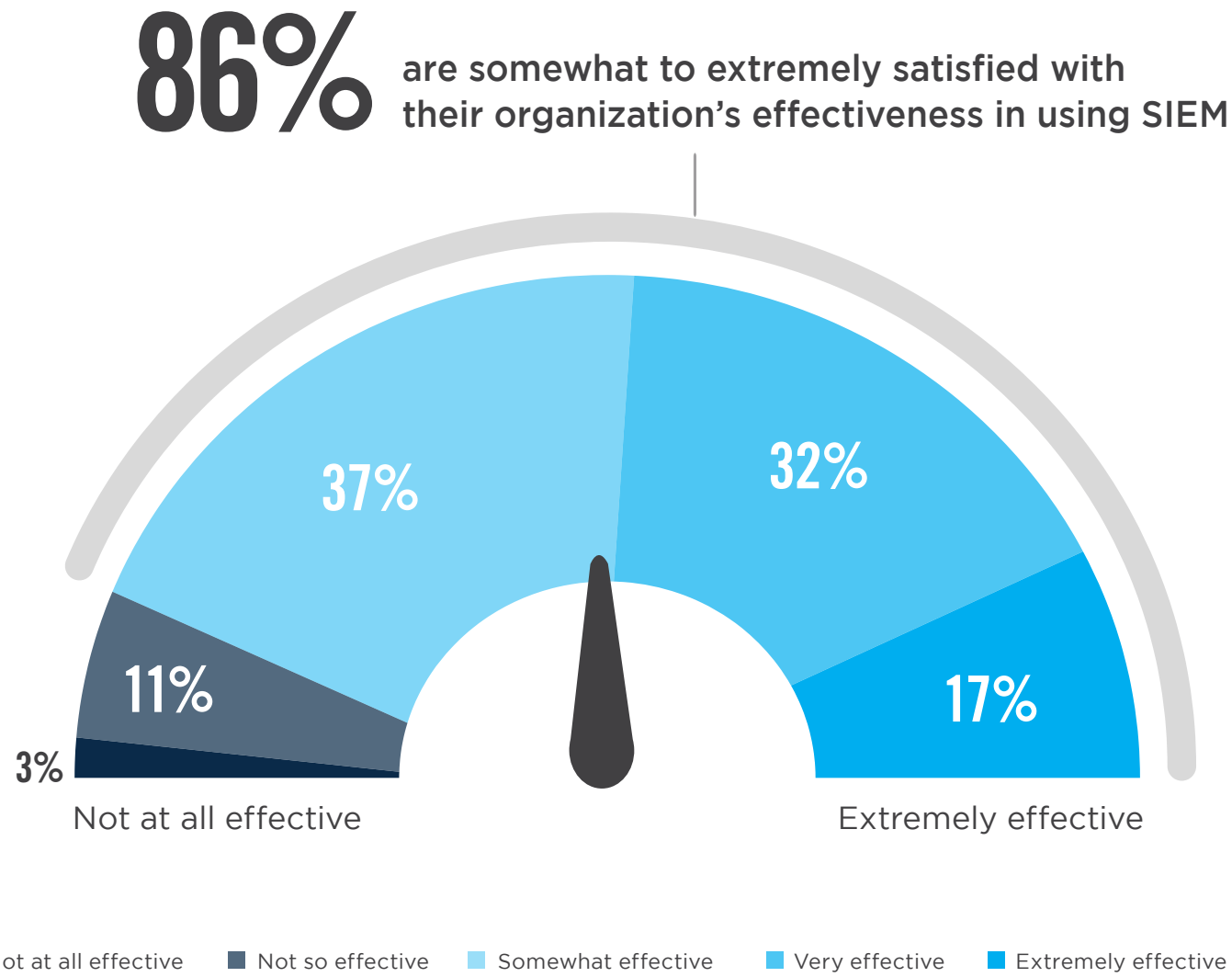
Is your SIEM delivered as a managed service or software installed on premises?



SIEM SATISFACTION

Companies are surprisingly satisfied with their SIEM investments. A large majority of 86% rate the effectiveness of their SIEM positively in its ability to identify and remediate cyber threats.

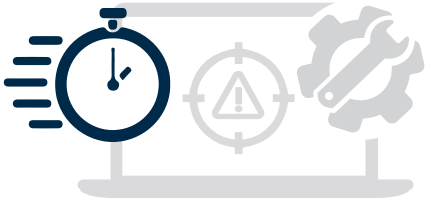
How would you rate your organization's effectiveness in using SIEM to identify and remediate cyber threats?



SIEM BENEFITS

When asked about the main benefits organizations derive from their SIEM platform, the ability to provide faster detection of and response to security events is most important (23%). This is followed by more efficient security operations (14%) and better visibility into threats (12%) – all key elements of the core value proposition of SIEM.

What main benefit is your SIEM platform providing?

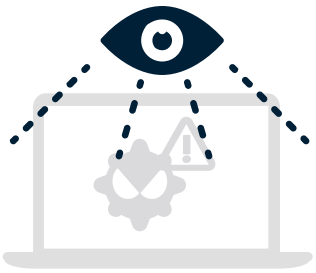


23%

Faster detection and response

14%

More efficient security operations



12%

Better visibility into threats

8%

Better prioritization of indicators of compromise (IOC)

8%

Better compliance posture

8%

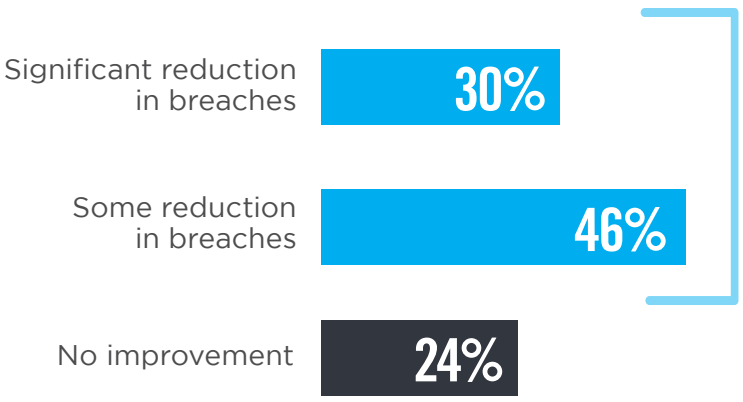
Better threat analysis

Better reporting of threat management 7% | Reduced staff workload through automation 6% | Better collection of threat data 6% | No benefits 3% | Better threat remediation 2% | Other 3%

SIEM REDUCES BREACHES

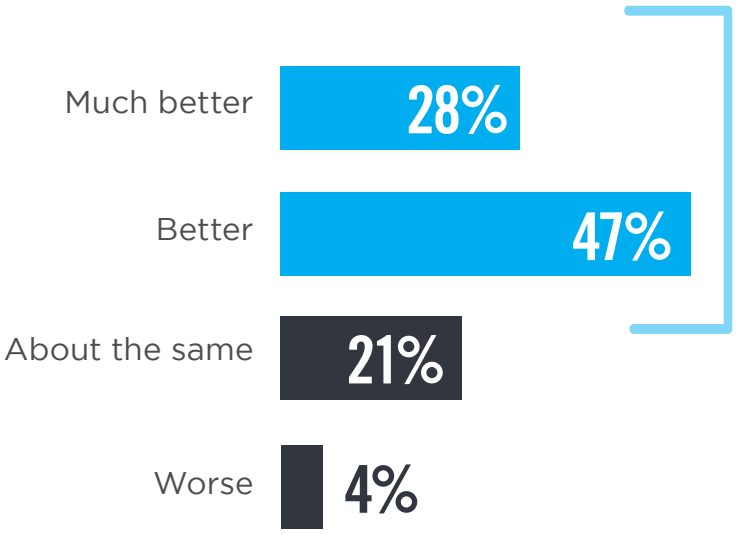
An overwhelming majority (three quarters) of respondents confirm that their deployment and use of SIEM resulted not only in improved ability to detect threats but also in a measurable reduction of security breaches for their organization. This is the ultimate confirmation of the technology's overall value and effectiveness.

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



76%
Report SIEM resulted in reduction of security breaches

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

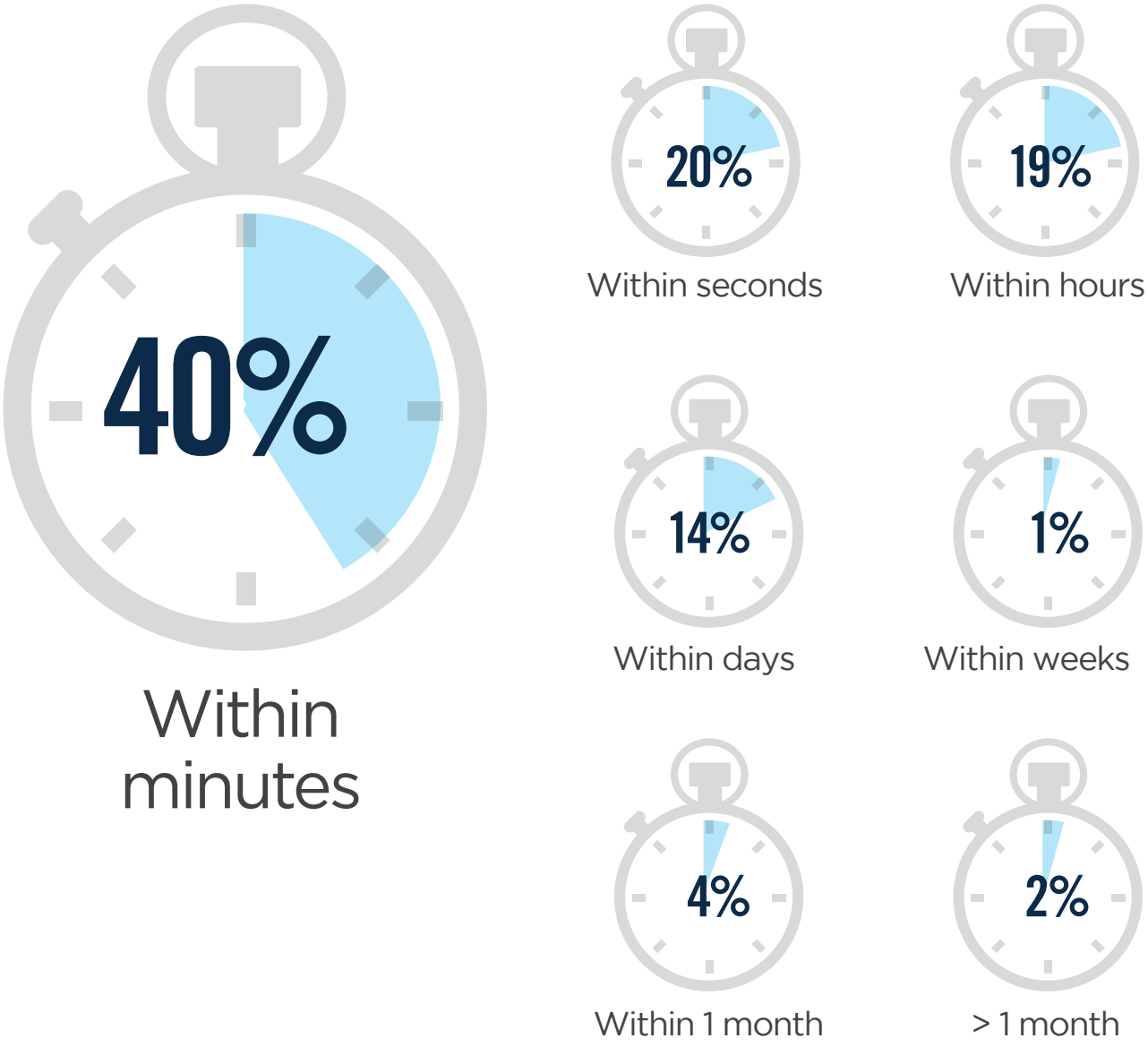


75%
confirm SIEM improved ability to detect threats

SPEED OF DETECTION

Eight out of 10 security events are detected within hours – half of them within minutes. It is reassuring that only a very small fraction of respondents report their SIEM detects security events only after weeks or months of dwell time.

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



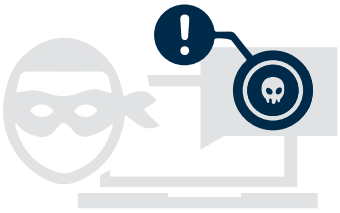
ATTACK DETECTION

Organizations report that their SIEM platform is most effective at detecting unauthorized access (46%), followed by advanced persistent threats (42%) and insider attacks (37%). However, the lower detection rates for prolific zero-day attacks (28%) or denial of service attacks (29%) are concerning.

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

46%

Unauthorized access



42%

Advanced persistent threats (APTs)/ targeted attacks

37%

Insider attacks (Malicious or careless insiders)

35%

Malware (viruses, worms, trojans)

34%

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

33%

Hijacking of accounts, services or resources

Ransomware 33% | Phishing attacks 33% | Denial of service attacks (DoS/DDoS) 29% | Zero-day attacks (against publicly unknown vulnerabilities) 28% | Cryptojacking 15% | Other 4%

BUSINESS IMPACT

Reduced employee productivity (35%) and negative impact on IT staff resources (28%) are the most significant areas of business impact security incidents have on organizations. Surprisingly, few respondents mentioned regulatory fines (7%) or reputational damage (10%) as a result of security breaches.

What negative impact did your business experience from security incidents in the past 12 months?

35%

Reduced employee productivity

28%

Deployment of IT resources to triage and remediate issue

27%

Increased helpdesk time

26%

Disrupted business activities

20%

System downtime

Data loss 19% | Reduced revenue/lost business 10% | Customer loss 10% | Negative publicity/reputational damage 10% | Loss/compromise of intellectual property 9% | Regulatory fines 7% | Lawsuit/legal issues 6% | Other 3%

SIEM KEY USE CASES

The survey confirms that the most important use case for SIEM is monitoring, correlation and analysis across multiple systems and applications (68%) to aid with the discovery of external and internal threats (62%).

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

68%

Monitor, correlate and analyze activity across multiple systems and applications

62%

Discover external and internal threats

51%

Monitor the activities of users

51%

Monitor server and database access

38%

Provide compliance reporting

Monitor a combination of cloud and on-premises infrastructure (as opposed to cloud-only or on-premises-only) 37% | Detect threats in cloud architecture including cloud access control (CASB) 36% | Detect industry/vertical specific attacks (e.g. healthcare break-the-glass, financial fraud) 36% | Provide analytics and workflow to support incident response 34%

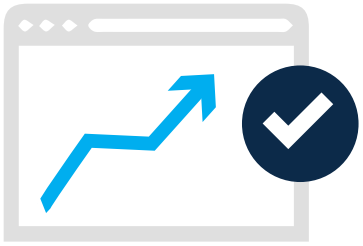
SIEM EVALUATION CRITERIA

As organizations evaluate new SIEM platforms, a number of decision criteria stand out. Cost considerations lead the list (66%), followed closely by product performance and effectiveness (65%) and product features (58%). Surprisingly, customer reviews (19%) play only a small role for organizations evaluating SIEM solutions in the market.

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

66%

Cost



65%

Product performance and effectiveness

58%

Product features/ functionality

52%

Support

43%

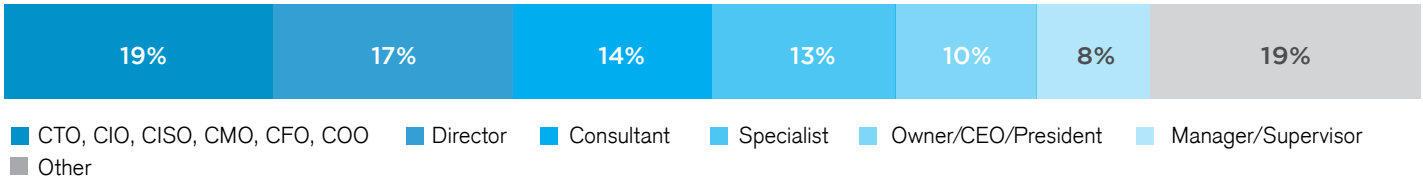
Product ease of use

Vendor experience and reputation 42% | Customer reviews 19% | Other 4%

METHODOLOGY & DEMOGRAPHICS

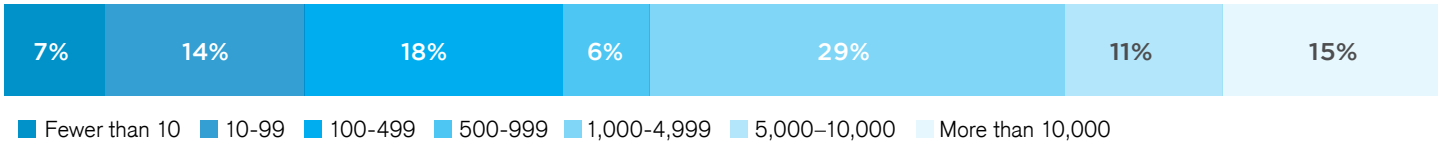
This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest trends, key challenges and solutions for SIEM. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section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

CAREER LEVEL

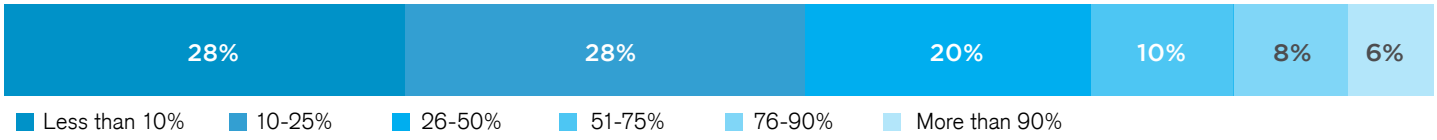


DEPARTMENT

COMPANY SIZE



SHARE OF IT INFRASTRUCTURE IN THE CLOUD



HelpSystems helps you protect business-critical data with a suite of integrated and automated security solutions for defense in depth, comprehensive visibility, and streamlined reporting across your on-prem and cloud environments.

www.helpsystems.com