2020

Cybersecurity INSIDERS

SIEM REPORT

CORE SECURITY

A HelpSystems Company

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 2020 SIEM Survey 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.

Key findings include:

- 75% believe SIEM is very important to extremely important to their organization's security posture.
- 82% rate the effectiveness of their SIEM positively.
- Top three benefits to SIEM are faster detection and response, better visibility, and more efficient security operations.
- 74% have seen a reduction in security breaches as a result of using SIEM.

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

We hope you enjoy this report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

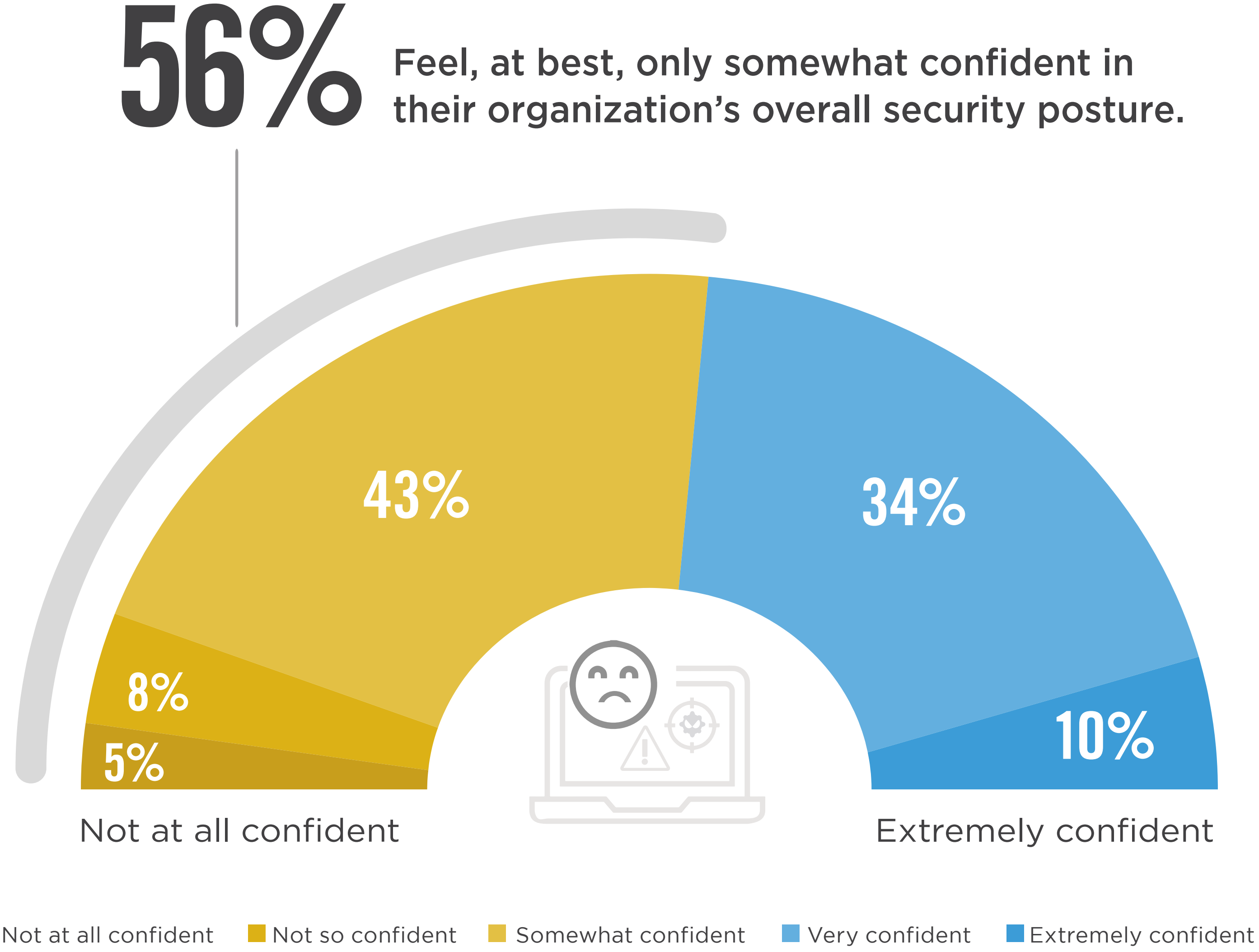
Cybersecurity
INSIDERS

All Rights Reserved. ©2020 Cybersecurity Insiders

CONFIDENCE IN OVERALL SECURITY POSTURE

A majority of cybersecurity professionals (56%) feel, at best, only somewhat confident in their organization's overall security posture.

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



Organizations that actively use SIEM technology report higher confidence in their overall security posture (53%) than organizations that do not use SIEM (44%).

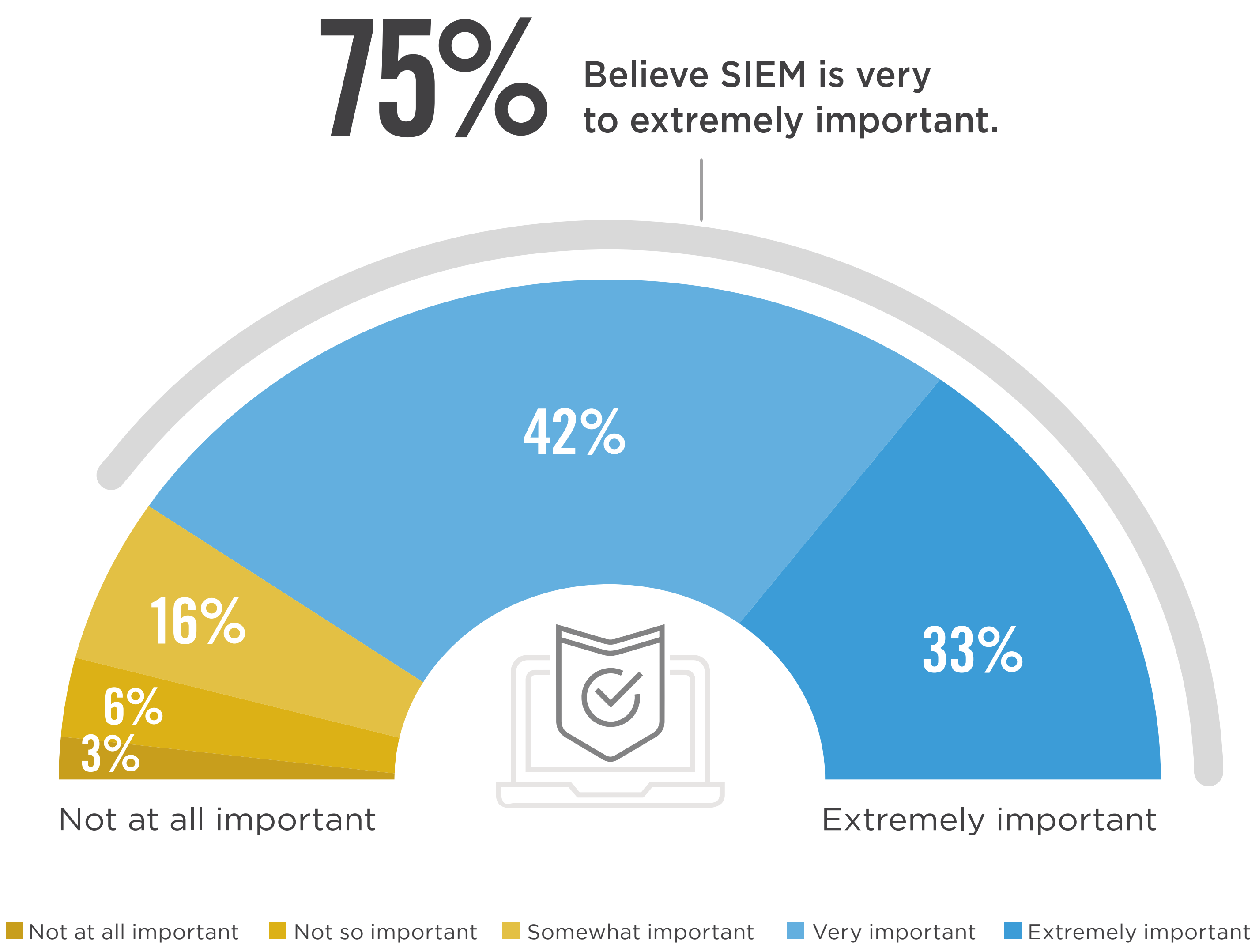
All Rights Reserved. ©2020 Cybersecurity Insiders

IMPORTANCE OF SIEM

Among the various security controls and technologies, SIEM plays a critical role in organizations' security postures. For 75% of IT security professionals, SIEM is very to extremely important.

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

75% Believe SIEM is very to extremely important.

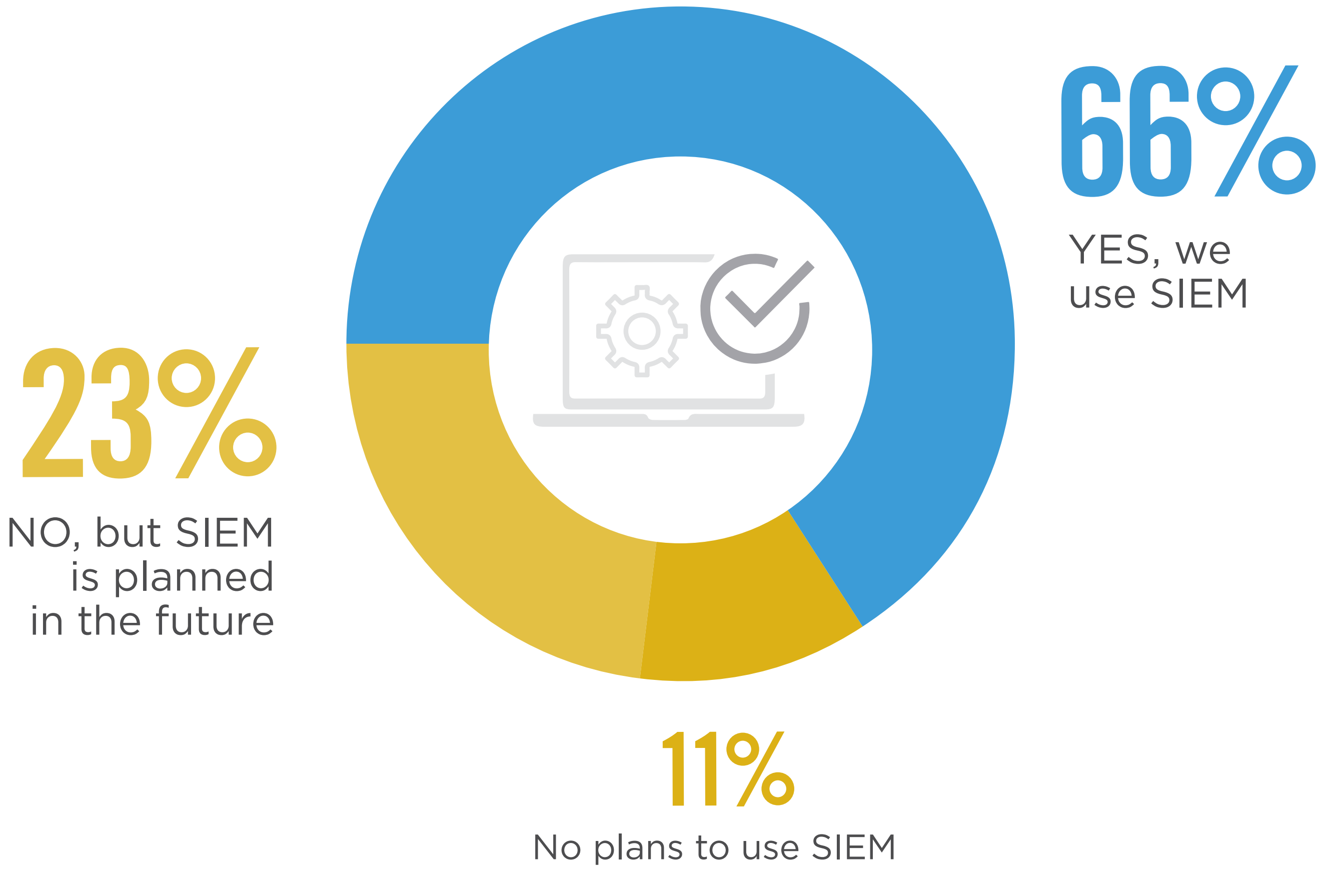


All Rights Reserved. ©2020 Cybersecurity Insiders

SIEM USE

Nearly seven out of 10 organizations in our survey already use SIEM platforms for security information and event management. Twenty-three percent are planning to implement SIEM in the future. Organizations that actively use SIEM technology report higher confidence in their overall security posture (53%) than organizations that do not use SIEM (44%).

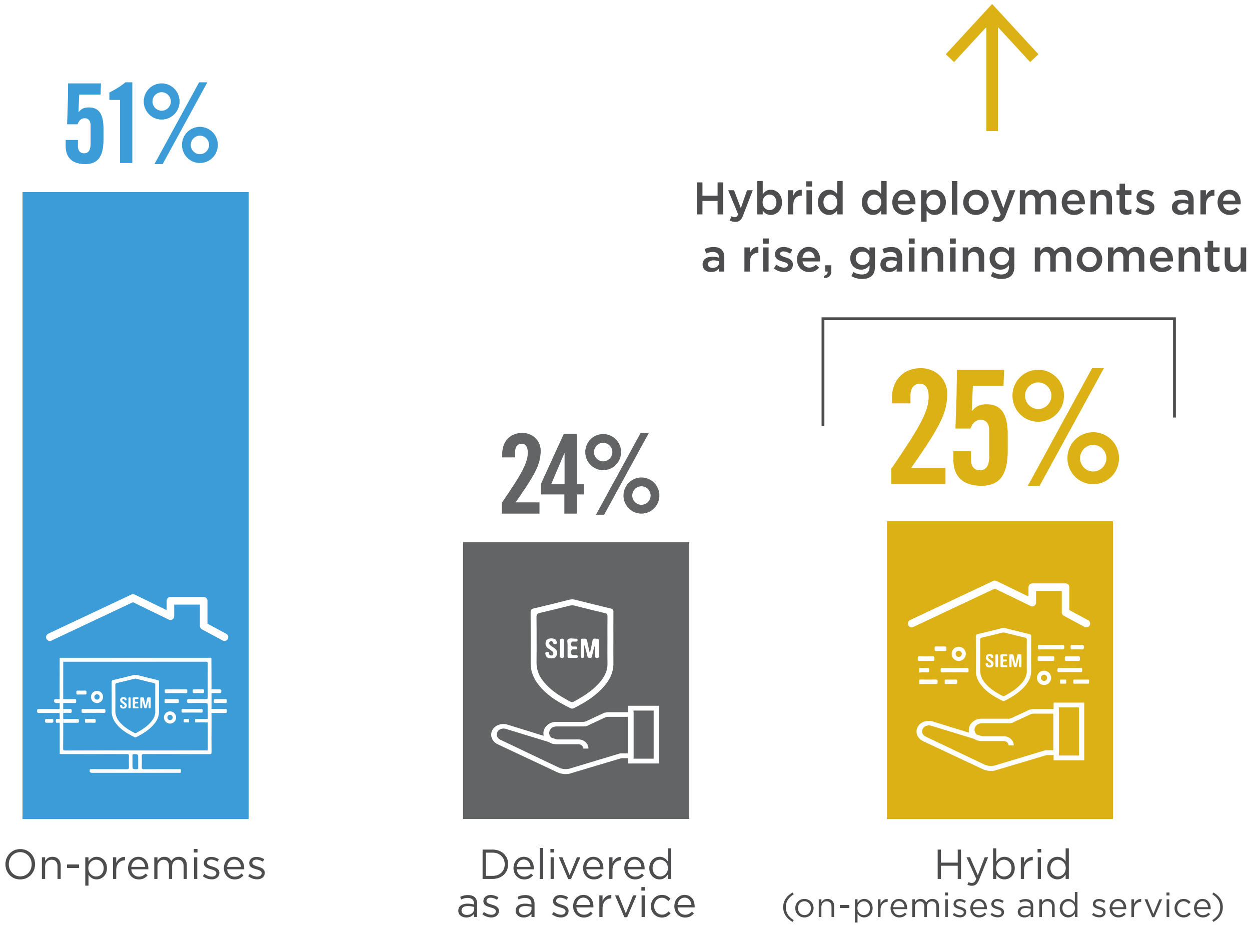
Does your organization actively use a SIEM platform or service?



SIEM DELIVERY

The majority of SIEM deployments are still delivered on-premises (51%). However, hybrid deployments of SIEM with on-premises and service-based components are gaining momentum (25%). A four percent increase from last year's report (21%).

▶ **Is your SIEM planned/delivered as a managed service or software installed on premises?**

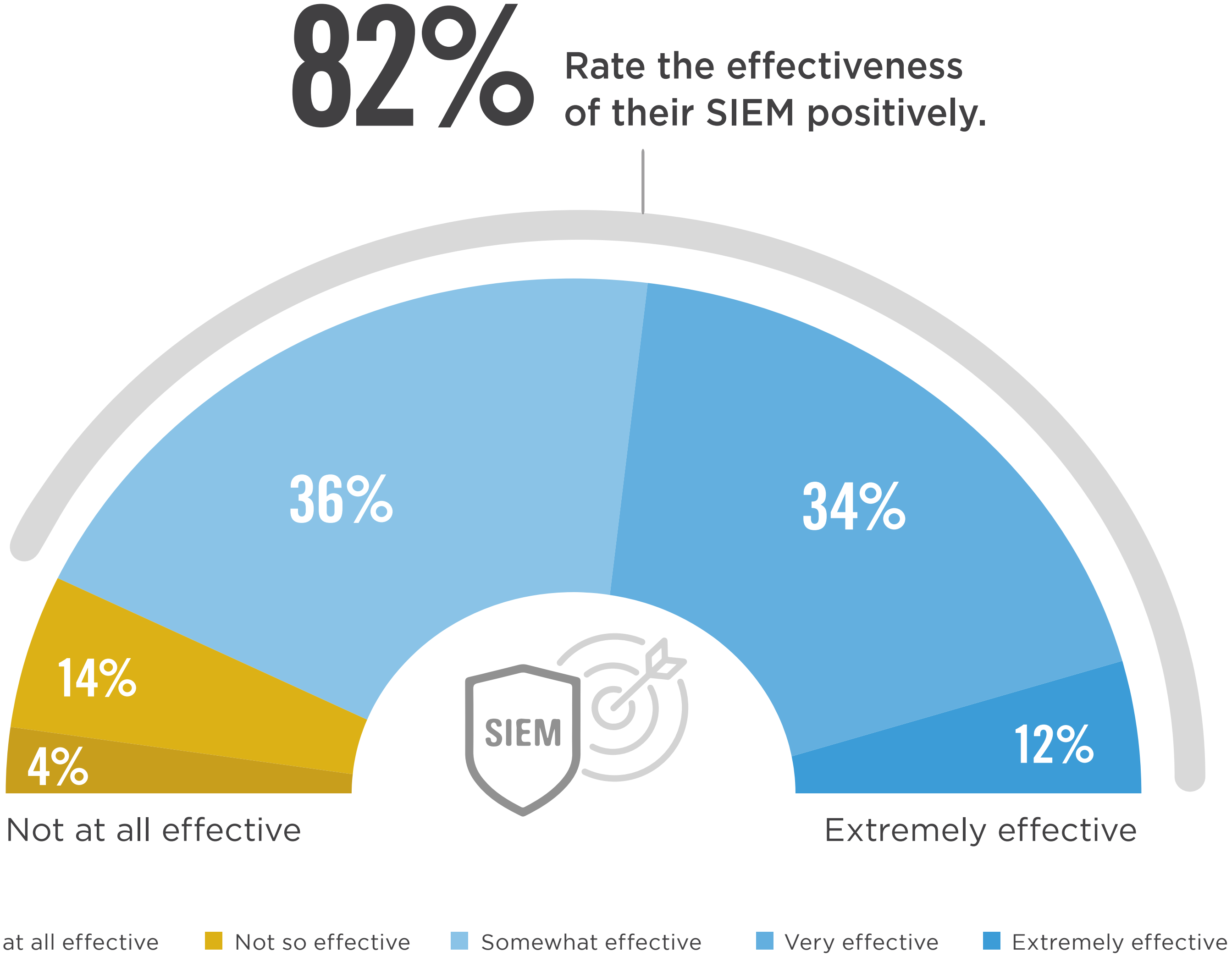


All Rights Reserved. ©2020 Cybersecurity Insiders

SIEM EFFECTIVENESS

A large majority (82%) 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?



All Rights Reserved. ©2020 Cybersecurity Insiders

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 (17%). Better visibility into threats jumped to the second place this year (15%), followed by more efficient security operations (13%) – all key elements of the core value proposition of SIEM.

What main benefit is your SIEM platform providing?

17%

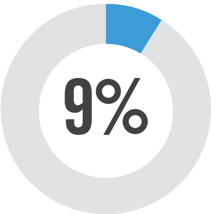
Faster detection and response

15%

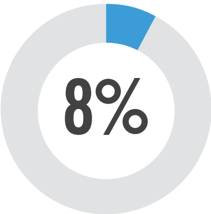
Better visibility into threats

13%

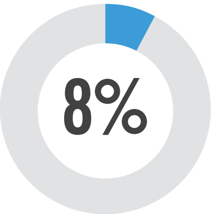
More efficient security operations



Better compliance posture



Better prioritization of Indicators Of Compromise (IOC)



Better threat analysis

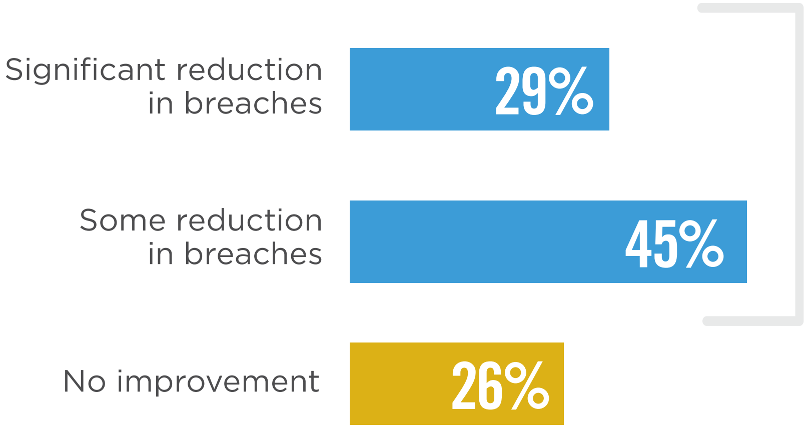
Reduced staff workload through automation 6% | Better collection of threat data 6% | Better reporting of threat management 6% | No benefits 5% | Better threat remediation 2% | Other 5%

All Rights Reserved. ©2020 Cybersecurity Insiders

SIEM REDUCES BREACHES

Nearly three quarters of respondents confirmed 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 (74%). This is the ultimate confirmation of the technology's overall value and effectiveness.

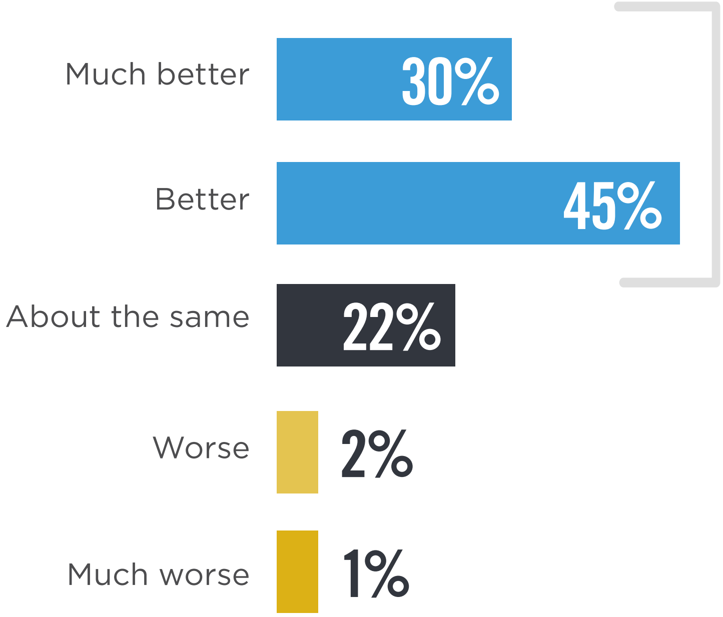
Has the occurrence of security breaches in your organization changed as a result of using SIEM?



74%

Report SIEM resulted in reduction of security breaches

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



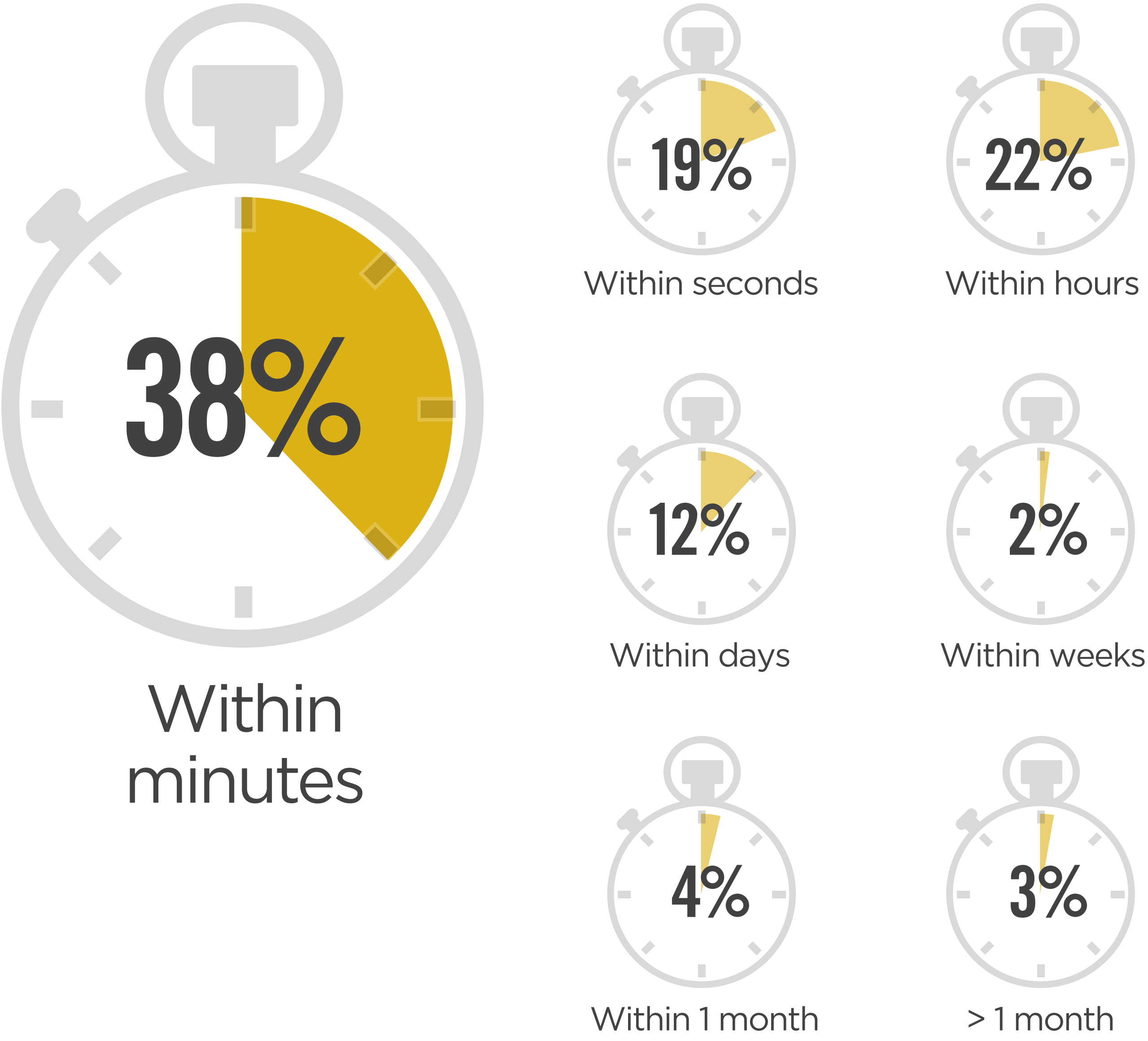
75%

confirm SIEM improved ability to detect threats

SPEED OF DETECTION

SIEM users confirm that eight out of 10 security events are detected within hours – more than half of them within minutes (57%). It is reassuring to see 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?



BUSINESS IMPACT

When asked about the negative impact security incidents had on an organization's business, reduced employee productivity (32%) and negative impact on IT staff resources (30%) are the most frequently highlighted areas. Surprisingly, few respondents mentioned regulatory fines (5%), customer loss (8%) or negative publicity (10%) as a result of security breaches.

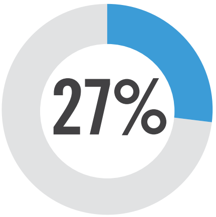
What negative impact did your business experience from security incidents in the past 12 months?

32%

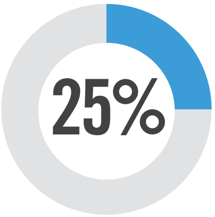
Reduced employee productivity

30%

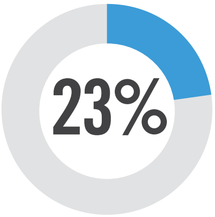
Deployment of IT resources to triage and remediate issue



Disrupted business activities



Increased helpdesk time



System downtime

Data loss 18% | Reduced revenue/lost business 11% | Negative publicity/reputational damage 10% | Customer loss 8%
Loss/compromise of intellectual property 7% | Lawsuit/legal issues 5% | Regulatory fines 5% | Other 3%

All Rights Reserved. ©2020 Cybersecurity Insiders

ATTACK DETECTION

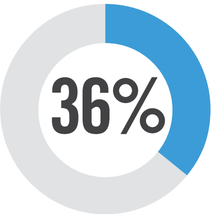
Organizations report that their SIEM platform is most effective at detecting unauthorized access (50%), followed by advanced persistent threats (40%) and malware (38%).

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

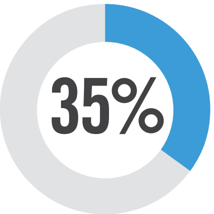
50%
Unauthorized access

40%
Advanced Persistent Threats (APTs)/ targeted attacks

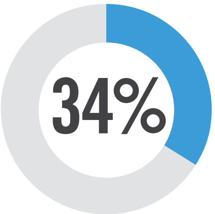
38%
Malware (viruses, worms, trojans)



Insider attacks (malicious or careless insiders)



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



Denial of service attacks (DoS/DDoS)

Hijacking of accounts, services or resources 33% | Phishing attacks 31% | Ransomware 31% | Zero-day attacks (against publicly unknown vulnerabilities) 25% | Cryptojacking 15% | Other 5%

SIEM INTEGRATION

SIEM platforms are typically highly integrated with other systems and applications to increase the breadth of data that is analyzed to alert and report on security events. The most common integrations are with intrusion detection and prevention systems (59%), followed by next-generation firewalls (54%) and application logs (49%).

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

59%

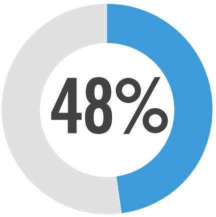
Intrusion Detection/ Prevention (IDS/IPS)

54%

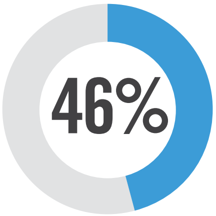
Next Generation Firewall (NGFW)

49%

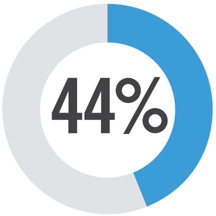
Applications (event logs, audit logs)



Web Application Firewall (WAF)



Anti-malware/ ransomware



Server data (IBM i/AS400, Linux, UNIX, Windows)

Data Loss Prevention (DLP) 40% | Vulnerability management tools (scanners, configuration and patch management, etc.) 39% | Vulnerability Management (VM) 39% | Identity and Access Management (IAM) 36% | User behavior monitoring 36% | Threat intelligence from security vendors 35% | Network Access Control (NAC) 34% | Static endpoints (PC, endpoint protection, log collectors) 33% | Security intelligence feeds from third-party services 33% | Network packet-based detection 30% | Relational databases (transactions, event logs, audit logs) 30% | Unified Threat Management (UTM) 29% | Dedicated log management platform 29% | Cloud activity 29% | Netflow 29% | Endpoint detection and response 28% | Mobile endpoints (mobile devices, MDMs, mobile apps) 28% | Whois/DNS/Dig and other Internet lookup tools 26% | Network-based malware sandbox platforms 24% | Anti Denial of Service solution (Anti DDoS) 24% | Asset discovery 18% | SIEM technologies 17% | Management systems for unstructured data sources (NoSQL, Hadoop) 16% | Social media applications (Facebook, Twitter) 13% | Other 5%

All Rights Reserved. ©2020 Cybersecurity Insiders

SIEM USE CASES

The survey reveals that the most important use case for SIEM is monitoring, correlation and analysis of event data across multiple systems and applications (72%), followed by aiding with the discovery of external and internal threats (59%) and user monitoring (49%).

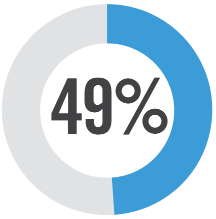
What are the most important use cases you utilize your SIEM platform for?

72%

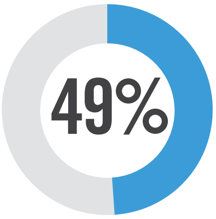
Monitor, correlate and analyze activity across multiple systems and applications

59%

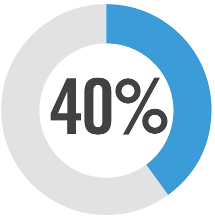
Discover external and internal threats



Monitor the activities of users



Monitor server and database access



Provide compliance reporting

Provide analytics and workflow to support incident response 39% | Monitor a combination of cloud and on-premises infrastructure (as opposed to cloud-only or on-premises-only) 35% | Detect industry/vertical specific attacks (e.g. healthcare break-the-glass, financial fraud) 34% | Detect threats in cloud architecture including cloud access control (CASB) 31% | Other 1%

SIEM EVALUATION CRITERIA

As organizations evaluate new SIEM platforms, some decision criteria are more important than others. Cost considerations lead the list (65%), followed closely by product performance and effectiveness (64%) and product features (59%). Surprisingly, customer reviews (20%) are less important for organizations evaluating SIEM solutions in the market.

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

65%

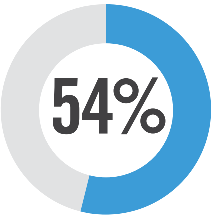
Cost

64%

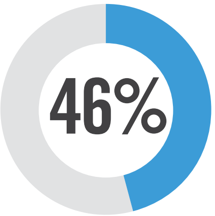
Product performance and effectiveness

59%

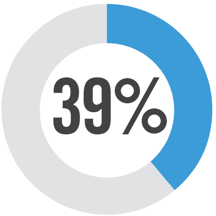
Product features/functionality



Support



Product ease of use



Vendor experience and reputation

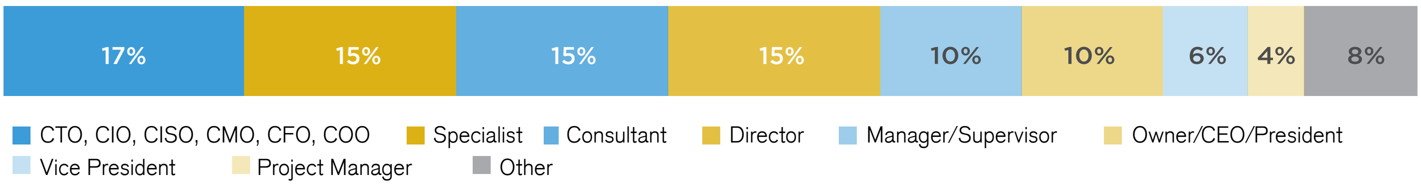
Customer reviews 20% | Other 5%

All Rights Reserved. ©2020 Cybersecurity Insiders

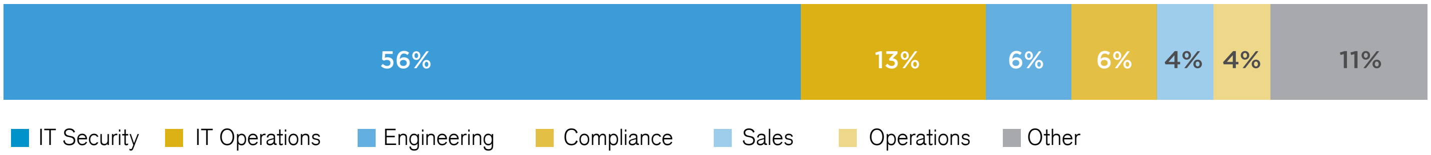
METHODOLOGY & DEMOGRAPHICS

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.

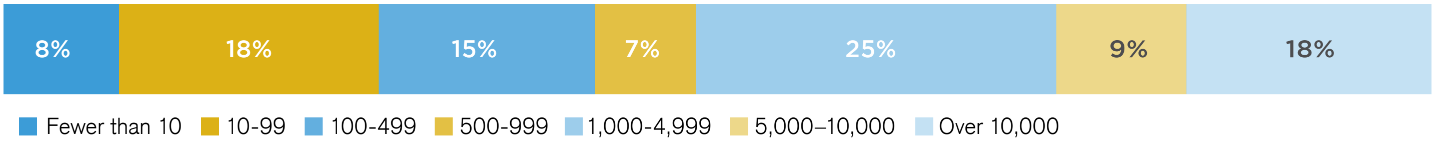
CAREER LEVEL



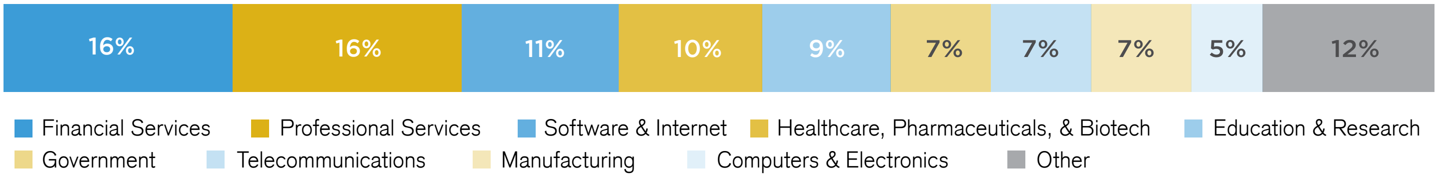
DEPARTMENT



COMPANY SIZE



INDUSTRY



All Rights Reserved. ©2020 Cybersecurity Insiders

CORE SECURITY
A HelpSystems Company

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