2021

Cybersecurity
INSIDERS

SIEM REPORT

CORE SECURITY
A HelpSystems Company

INTRODUCTION

Security Information and Event Management (SIEM) is an evolving category of tools that collect, aggregate, analyze, and log event data from systems across the IT stack to monitor, identify, and report security threats and suspicious activity.

The 2021 SIEM Survey Report represents one of the most comprehensive annual surveys on SIEM to date as it explores the latest trends, key challenges, and solution preferences. 2021 marks the third edition of the SIEM Report, providing the ability to analyze the trends year over year.

Key findings include:

- 74% of IT security professionals consider SIEM very to extremely important to their organization's security posture
- 80% rate their SIEM as effective in identifying and remediating cybersecurity threats
- The key benefits of SIEM include better visibility, followed by faster detection of and response to security events, and more efficient security operations
- Over three quarters of respondents confirmed that their use of SIEM improved their ability to detect and respond to threats (76%)

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

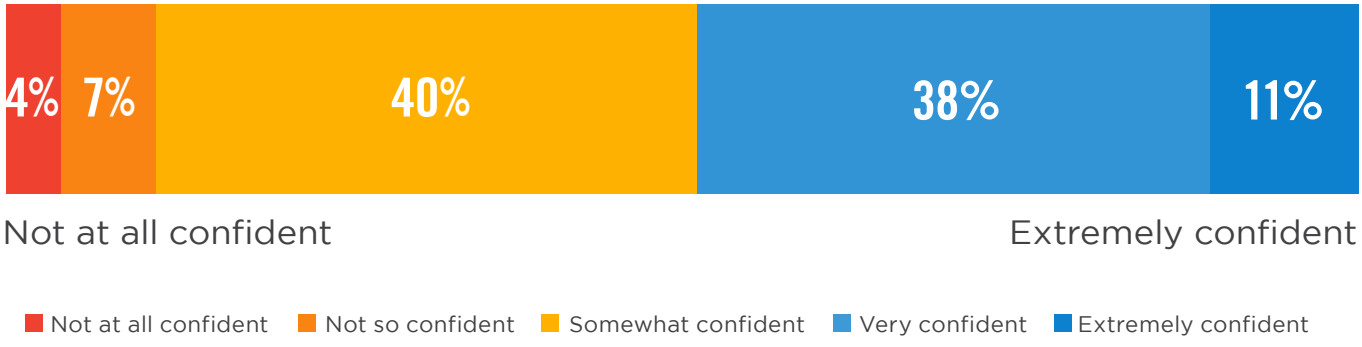
Cybersecurity
INSIDERS

CONFIDENCE IN SECURITY POSTURE

Just over half of cybersecurity professionals (51%) feel only somewhat confident or worse in their organization's overall security posture.

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

51% Feel, at best, only somewhat confident in their organization's overall security posture.



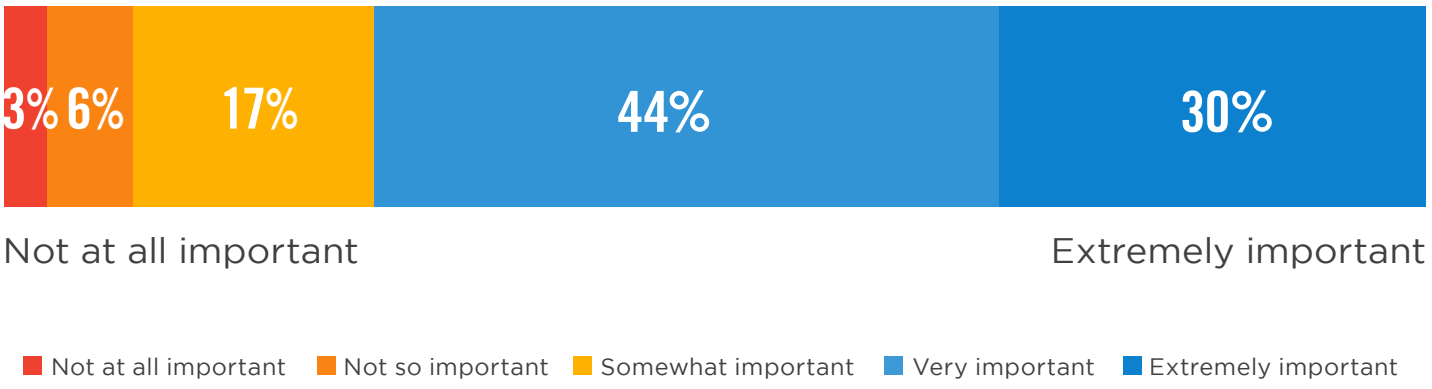
Organizations that actively use SIEM solutions report higher levels of confidence, with 57% being very or extremely confident in their security posture, whereas only 49% of those without a SIEM report being very or extremely confident.

IMPORTANCE OF SIEM

SIEM solutions, known for performing real-time analysis of security alerts, play a critical role in organizations' security postures. These tools can prioritize threats from many different types of assets, including networks, applications, devices, user activity logs, different operating systems, databases, firewalls, or network appliances. For 74% of IT security professionals, SIEM is very to extremely important.

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

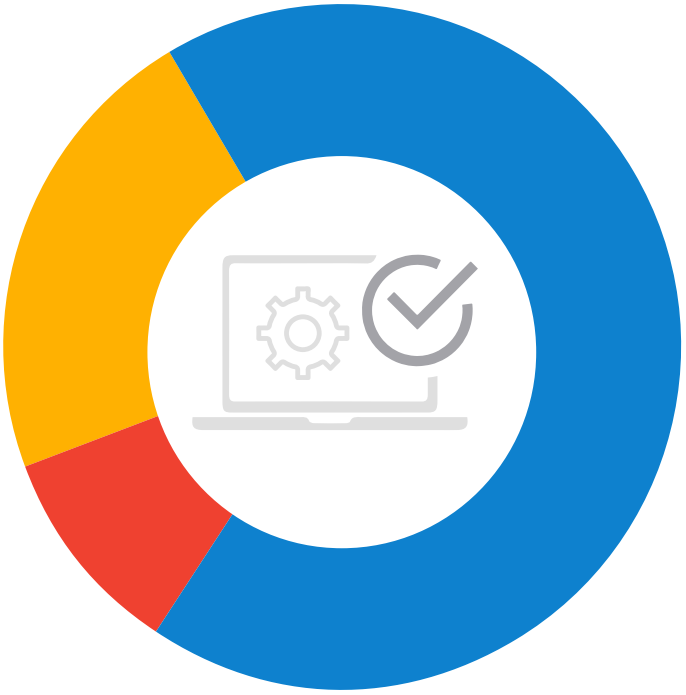
74% Believe SIEM is very to extremely important.



SIEM ADOPTION ON THE RISE

Nearly seven out of 10 of those surveyed already use SIEM platforms for security information and event management. This shows a steady increase of two percent over last year's survey. Twenty-two percent are planning to implement SIEM in the future.

Does your organization actively use a SIEM platform or service?



22%
NO, but SIEM is planned in the future

10%
No plans to use SIEM

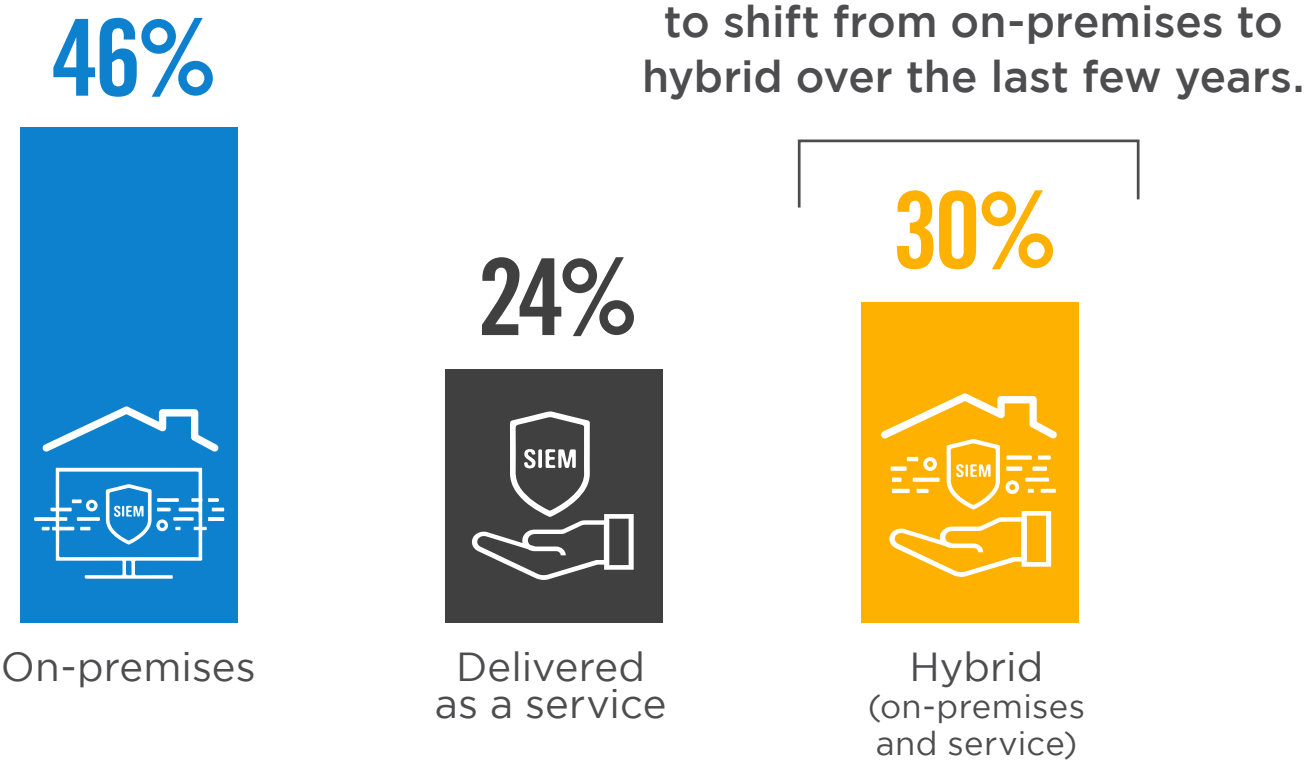
68%
YES, we use SIEM

SIEM DELIVERY

The shift from on-premise SIEM deployments to hybrid on-premises and service-based components is gaining momentum (30%, up by five percentage points since last year). While most SIEM deployments are still delivered on-premises (46%), this represents a drop of five percentage points since last year.

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

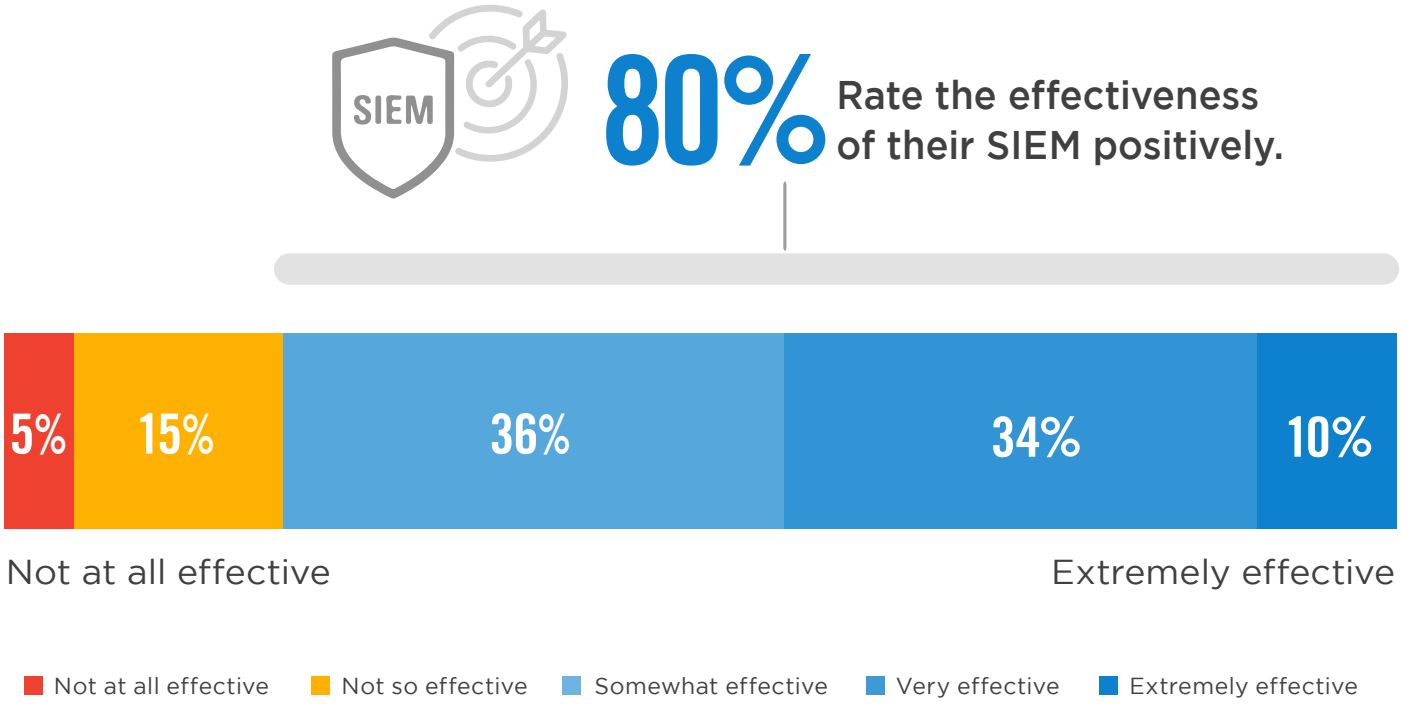
Hybrid deployments continue to shift from on-premises to hybrid over the last few years.



SIEM EFFECTIVENESS

Eight out of ten organizations in our survey positively rate the effectiveness of their SIEM in its ability to identify and remediate cyber threats.

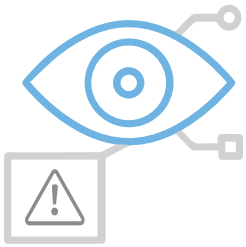
How would you rate your organization's effectiveness in using SIEM to identify and remediate cyber threats?



SIEM BENEFITS

Better visibility into threats jumped to the top benefit of SIEM platforms, according to respondents using the technology (16%). This is followed by faster detection of and response to security events (14%) and more efficient security operations (13%) – all key elements of the core value proposition of SIEM.

What main benefit is your SIEM platform providing?



16%

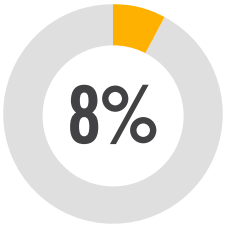
Better visibility into threats

14%

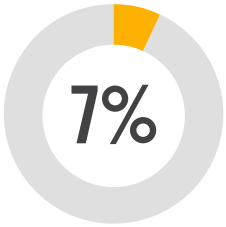
Faster detection and response

13%

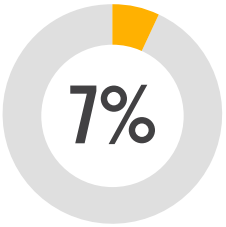
More efficient security operations



Better threat analysis



Reduced staff workload through automation



Better reporting of threat management

No benefits 6% | Better prioritization of Indicators Of Compromise (IOC) 6% | Better collection of threat data 6% | Better compliance posture 5% | Better threat remediation 2% | Other 6%

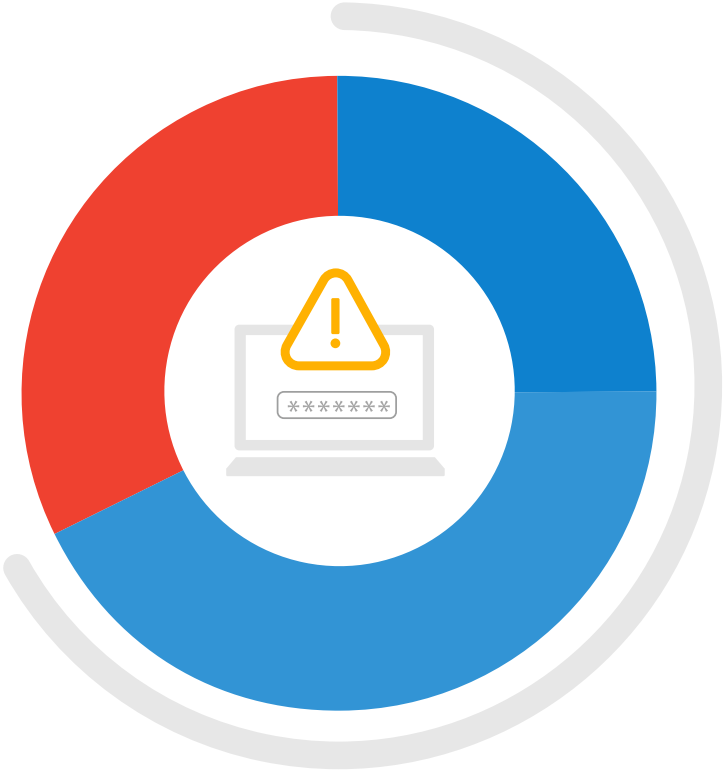
FEWER BREACHES WITH SIEM

Organizations have seen a measurable reduction in the number of security breaches as a result of using SIEM (68%), confirming the technology's overall value and effectiveness.

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

68%

Report SIEM resulted in a reduction of security breaches



25%

Significant reduction in breaches

43%

Some reduction in breaches

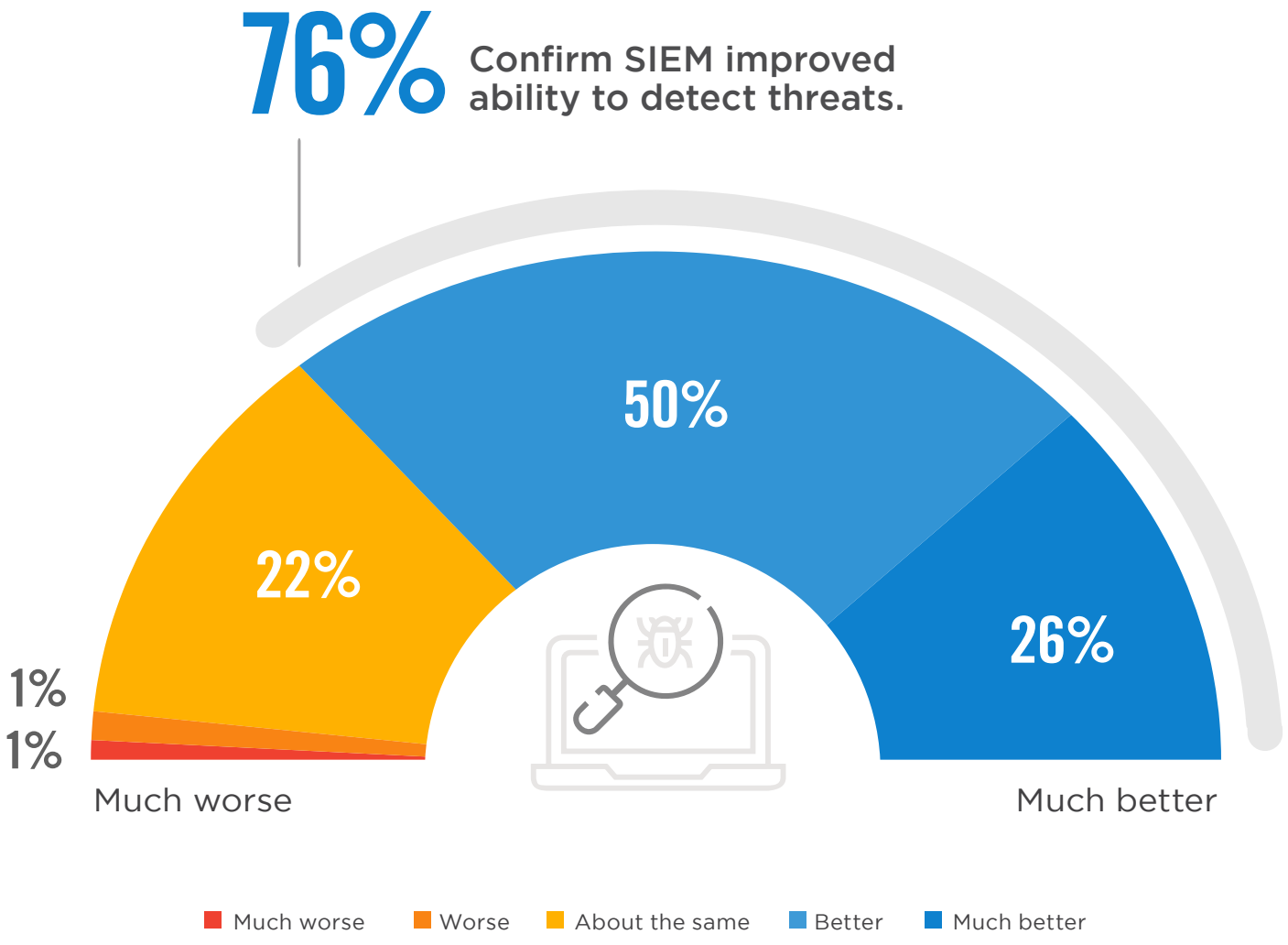
32%

No improvement

SIEM THREAT DETECTION

Over three quarters of respondents confirmed their deployment and use of SIEM resulted in an improved ability to detect threats (76%).

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

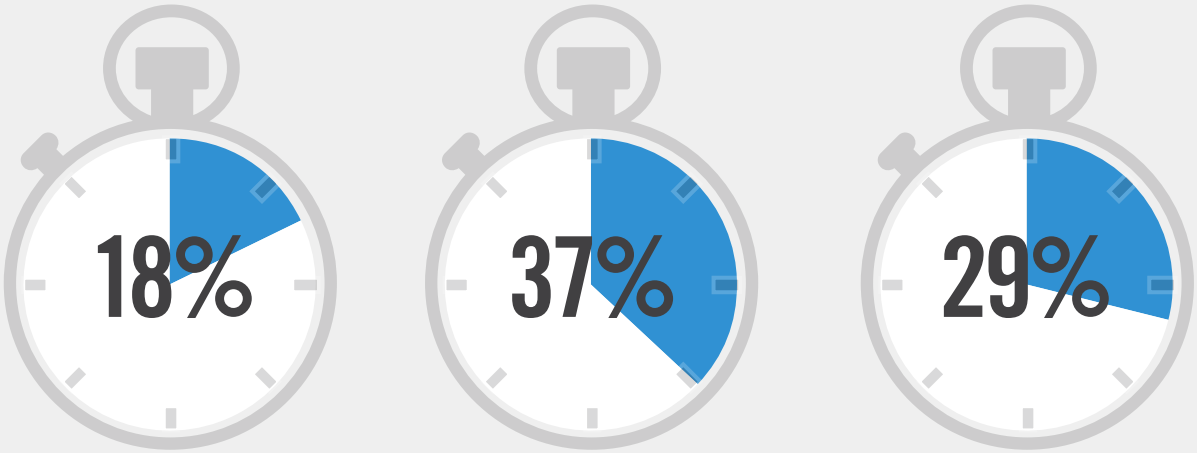


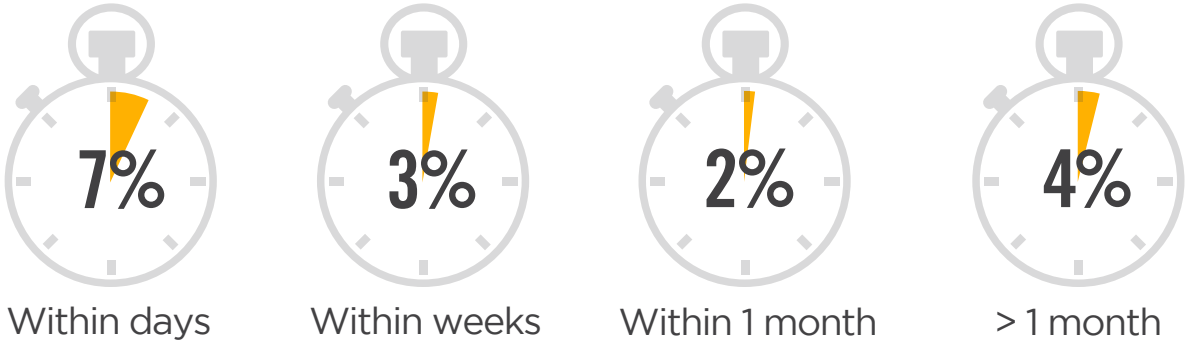
FASTER DETECTION WITH SIEM

The longer an infection dwells in a system, the more damage it can do. Eighty-four percent of security events are detected within hours. Impressively, more than half of these events are detected within minutes (55%). 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?

84% **Of security events are detected within hours, more than half of them within minutes.**





ATTACK DETECTION

When asked about what types of attacks SIEM technology is most effective at detecting, organizations reported that their SIEM platform is most effective at detecting unauthorized access (63%), followed by detection of malware (50%) and Denial of Service (DoS) attacks (47%). When compared to last years results, we saw an increase of SIEM technology effectively detecting almost every attack type.

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

63%

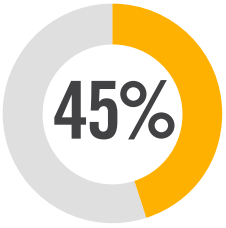
Unauthorized access

50%

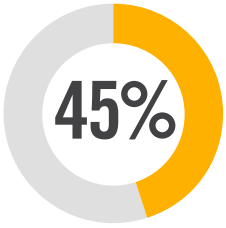
Malware (viruses, worms, trojans)

47%

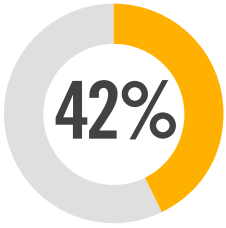
Denial of Service attacks (DoS/DDoS)



Insider attacks (malicious or careless insiders)



Hijacking of accounts, services, or resources



Advanced Persistent Threats (APTs)/ targeted attacks

Web application attacks (buffer overflows, SQL injections, cross-site scripting) 41%| Phishing attacks 37% | Ransomware 30% | Zero-day attacks (against publicly unknown vulnerabilities) 27% | Cryptojacking 20% | Other 7%

SIEM INTEGRATION

To increase the scope of data that is analyzed to alert and report on security events, SIEM platforms need to closely integrate with other systems and applications. According to the organizations asked in our survey, the most common integrations are with intrusion detection and prevention systems (56%), followed by endpoint detection and response (52%) and next-generation firewalls (51%).

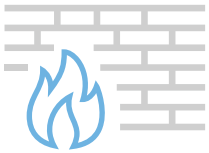
What systems, services, and applications are integrated with your SIEM platform?

56%

Intrusion Detection/ Prevention (IDS/IPS)

52%

Endpoint detection and response

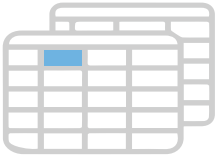


51%

Next Generation Firewall (NGFW)

50%

Anti-malware/ ransomware



47%

Applications (event logs, audit logs)

46%

Vulnerability Management (VM)

Vulnerability management tools 45% | Web Application Firewall (WAF) 45% | Server data 44% | Asset discovery 32% | Static endpoints 32% | Relational databases 32% | Netflow 32% | Unified Threat Management (UTM) 31% | Security intelligence feeds from third-party services 31% | Network packet-based detection 31% | Identity and Access Management (IAM) 30% | User behavior monitoring 30% | Cloud activity 30% | Dedicated log management platform 29% | Network Access Control (NAC) 28% | Mobile endpoints 26% | Whois/DNS/Dig and other internet lookup tools 25% | Anti Denial of Service solution (Anti DDoS) 24% | Network-based malware sandbox platforms 23% | Management systems for unstructured data sources 18% | Social media applications 18% | Other 8%

SIEM USE CASES

When asked about the most important use cases for SIEM, organizations report that monitoring, correlation, and analysis of event data across multiple systems and applications (74%) is the most critical use case. This is followed by discovery of external and internal threats (55%) and user activity monitoring (49%).

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

74%

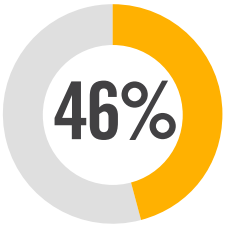
Monitor, correlate, and analyze activity across multiple systems and applications

55%

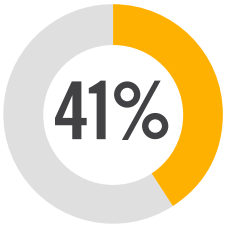
Discover external and internal threats

49%

Monitor the activities of users



Provide analytics and workflow to support incident response



Monitor server and database access

Monitor a combination of cloud and on-premises infrastructure

Provide compliance reporting 36% | Detect industry/vertical specific attacks (e.g., healthcare break-the-glass, financial fraud) 29% | Detect threats in cloud architecture including cloud access control (CASB) 25% | Other 3%

HURDLES TO SIEM SUCCESS

Like with any cybersecurity technology, there can be hurdles to maximizing the value of SIEM platforms. Our survey panel reports that lack of skilled staff to operate SIEM effectively (44%) is typically the biggest hurdle, followed by system complexity (37%) and having to manually create or refine rules (35%).

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

44%

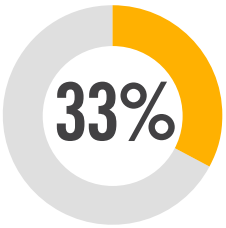
Lack of skilled/trained staff to operate effectively

37%

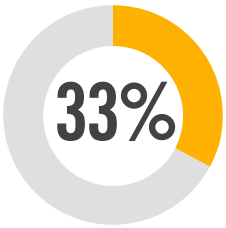
System complexity

35%

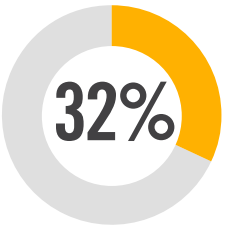
Having to manually create/refine rules



Lack of budget



Too many false positives



Poor integration/ interoperability between security solutions

Lack of security awareness among employees 25% | Company culture 25% | Lack of contextual information from security tools 21% | Lack of management support/awareness/buy-in 19% | Lack of visibility into network traffic and other processes 18% | Difficulty implementing and deploying the solution 14% | Poor vendor support 13% | Insufficient or inadequate tools available in-house 13% | Lack of effective security solutions available in the market 8% | Other 4%

SIEM EVALUATION CRITERIA

We asked organizations what decision criteria they consider most important when evaluating SIEM platforms. Interestingly, product features and functionality rose to the top of the list (66%), from the third spot last year, pushing cost considerations to the second spot (60%). This is followed closely by product performance and effectiveness (59%).

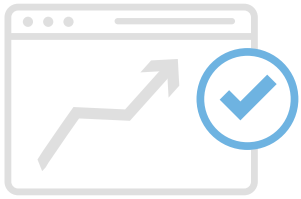
What criteria do you consider most important when evaluating a SIEM solution?

66%

Product features/functionality

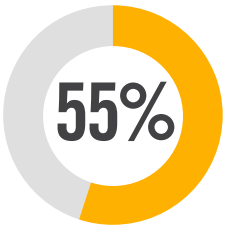
60%

Cost

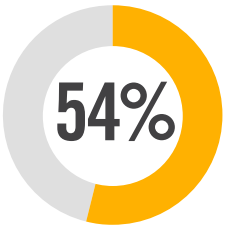


59%

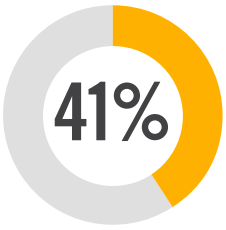
Product performance and effectiveness



Product ease of use



Support



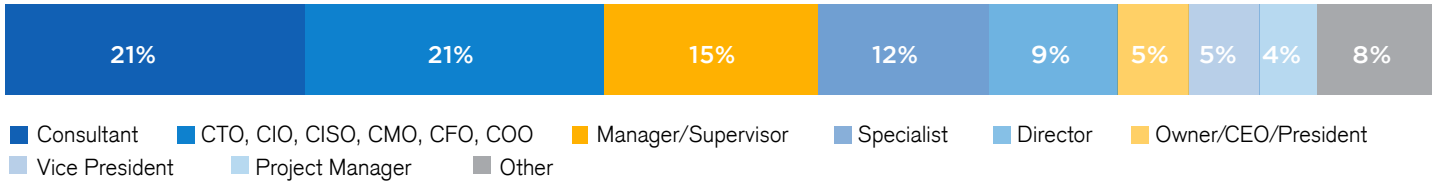
Vendor experience and reputation

Customer reviews 20% | Other 6%

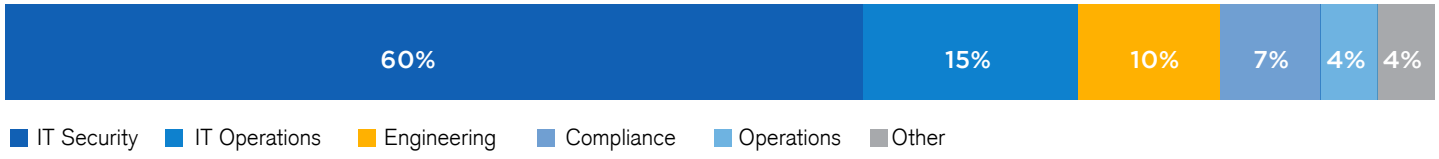
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 267 IT and cybersecurity professionals in the US, conducted in January 2021, 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.

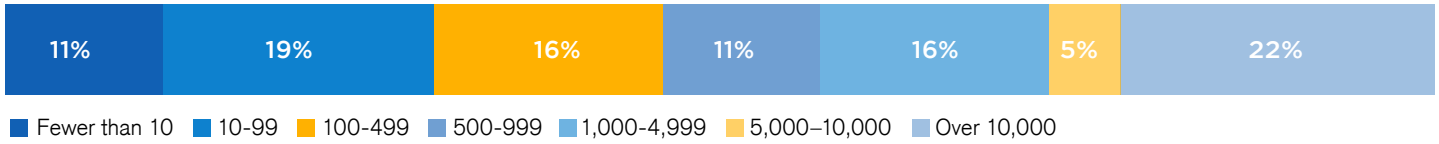
CAREER LEVEL



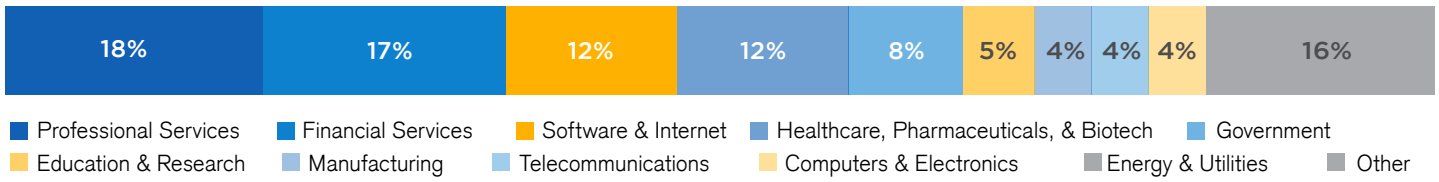
DEPARTMENT



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