2019

Cybersecurity INSIDERS

SIEM REPORT

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 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.

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 8 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 hope you will enjoy the report.

Thank you,

Holger Schulze

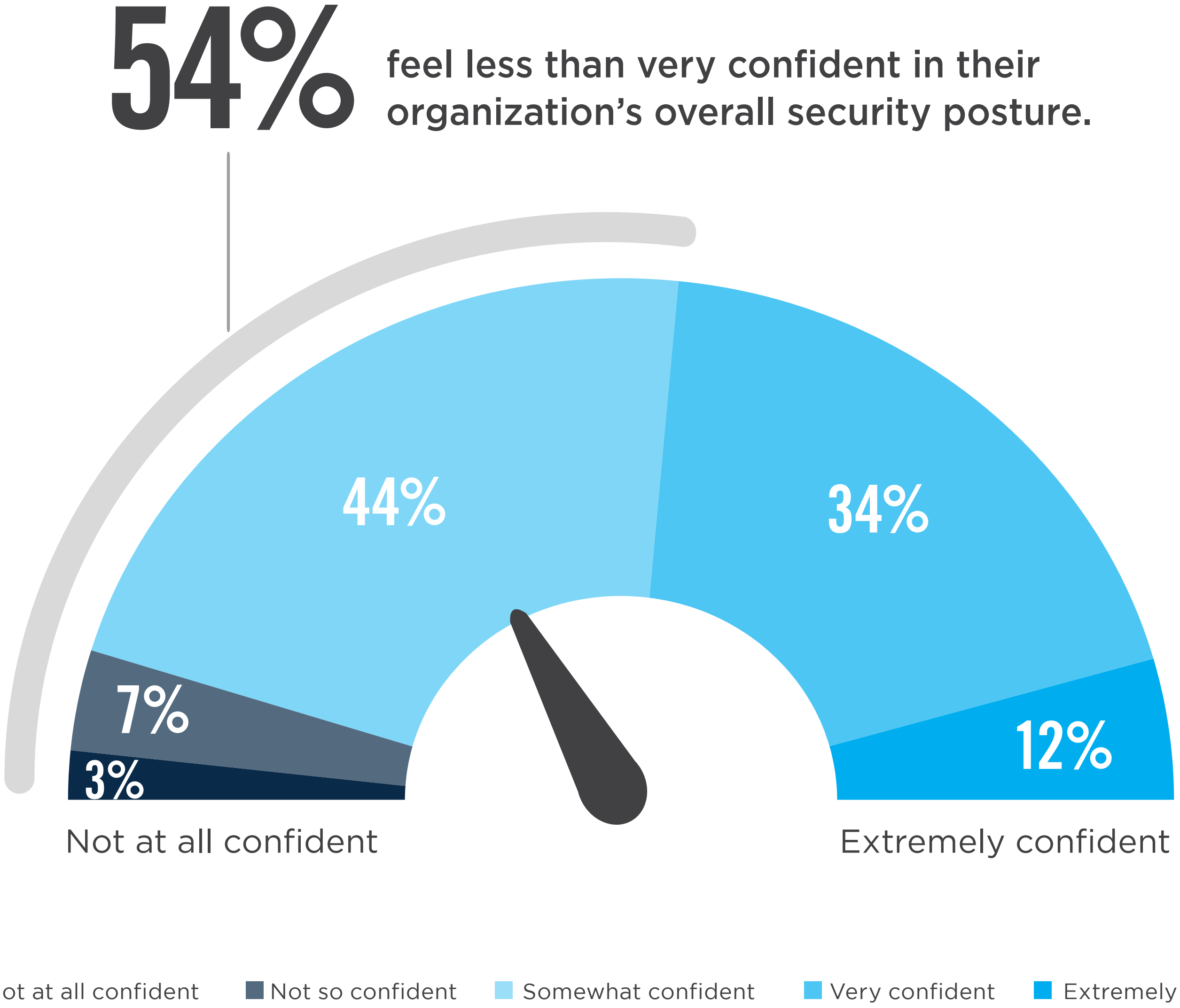
Holger Schulze
CEO and Founder
Cybersecurity Insiders

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?

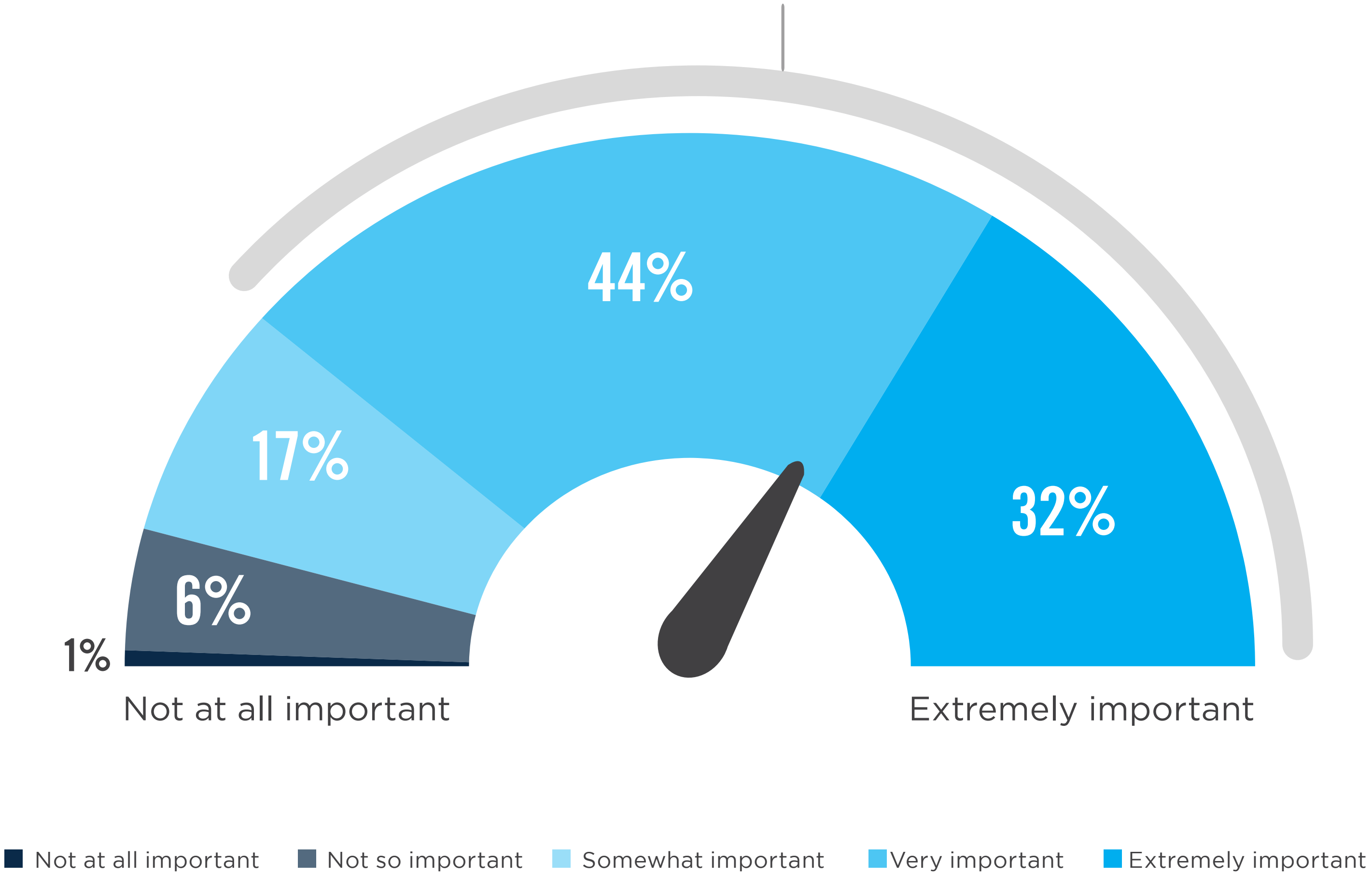


IMPORTANCE OF SIEM

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?

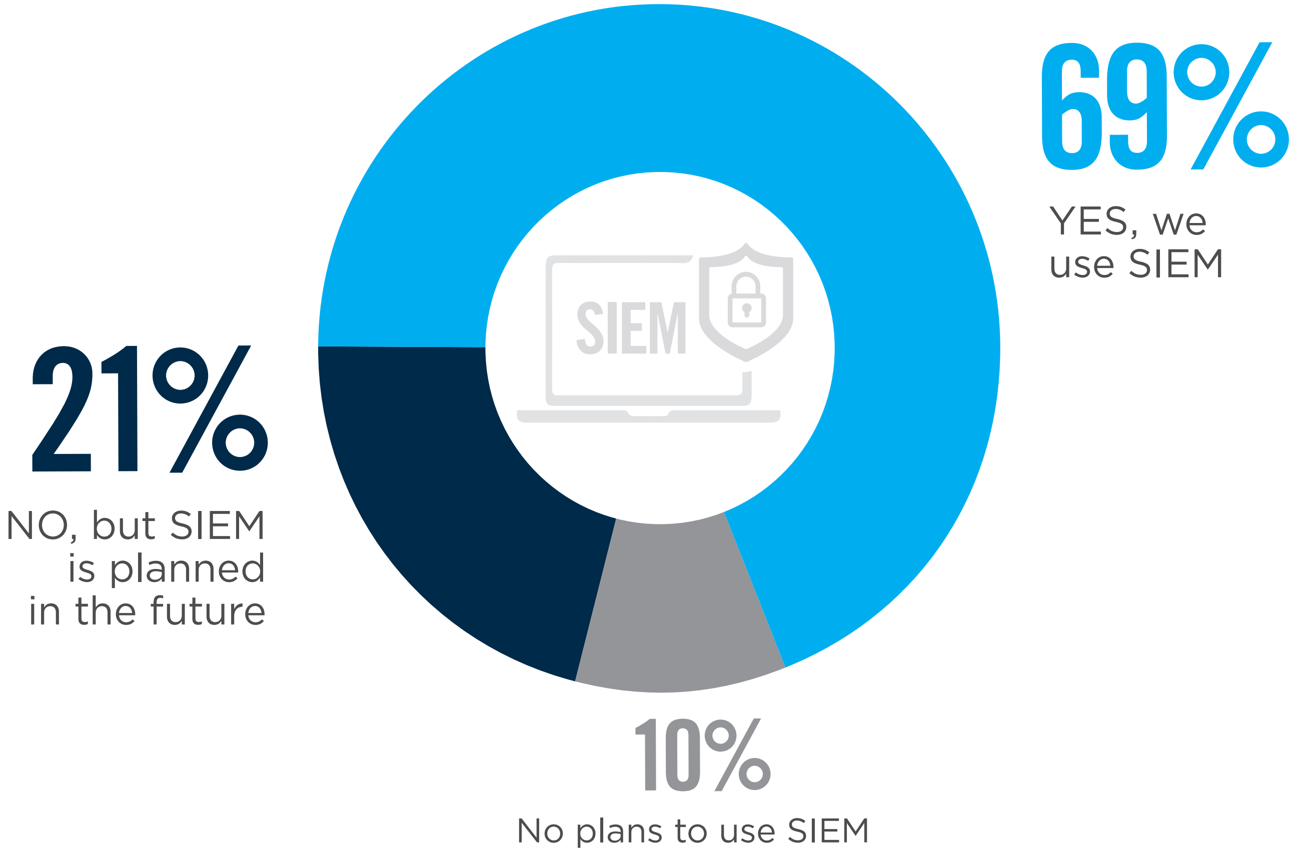
76% Believe SIEM is very to extremely important to organizations' security postures.



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.

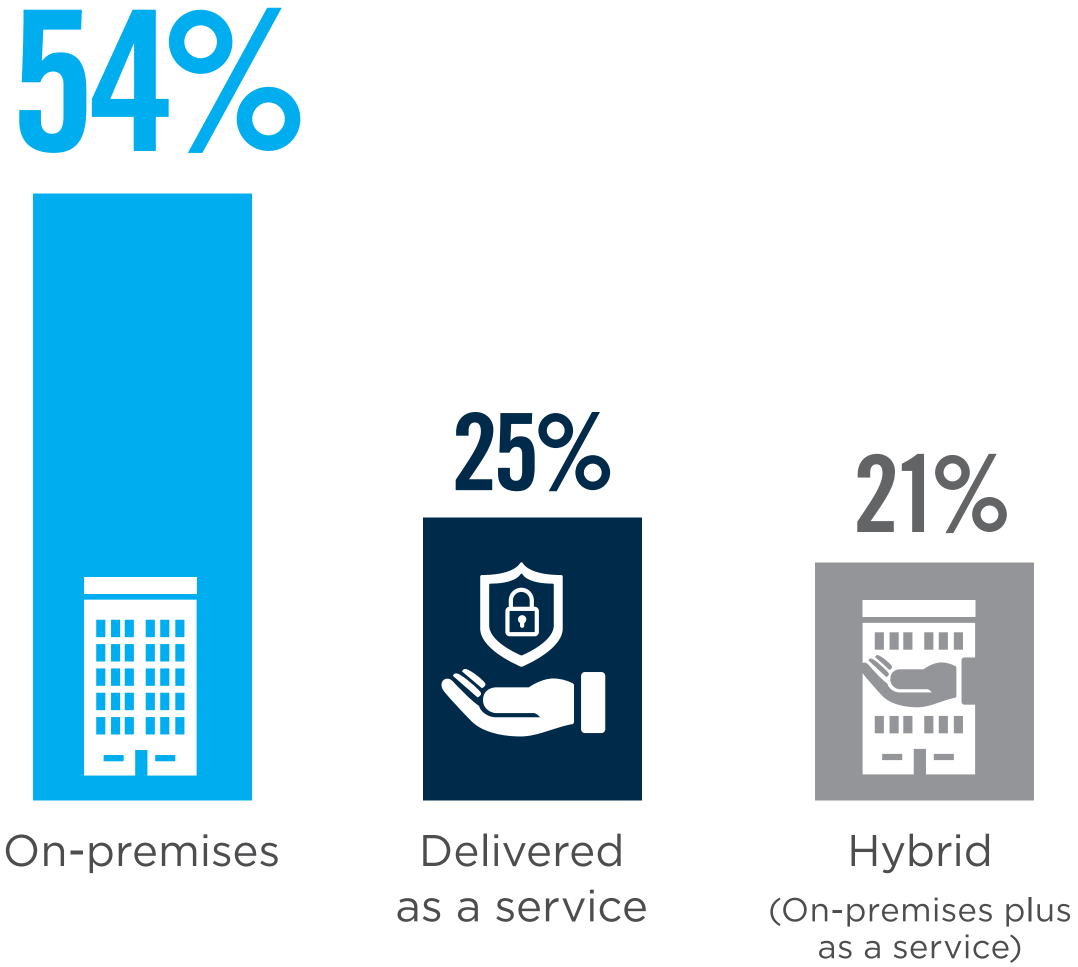
Does your organization actively use a SIEM platform or service?



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?

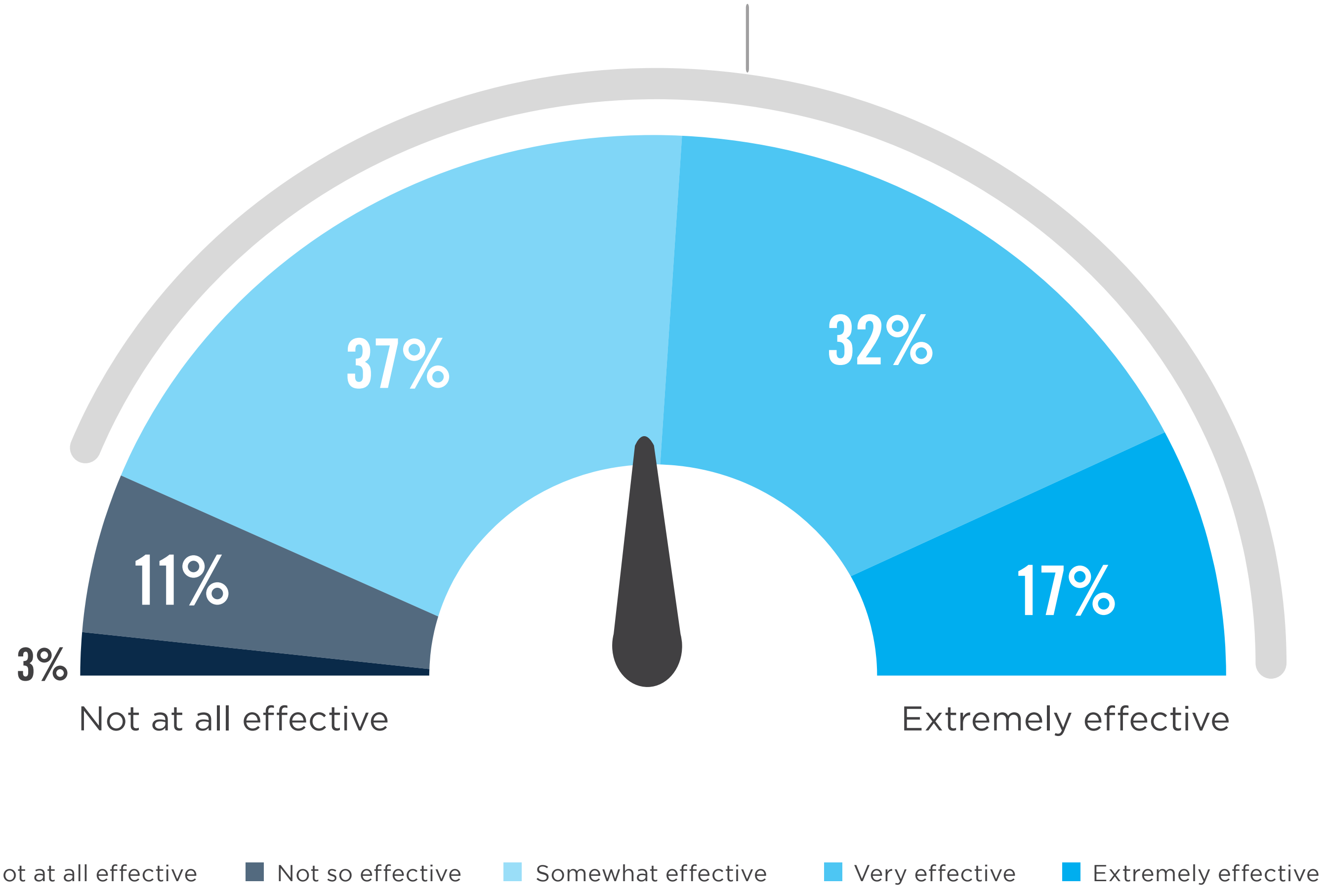


SIEM SATISFACTION

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?

86% are somewhat to extremely satisfied with their organization's effectiveness in using SIEM



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

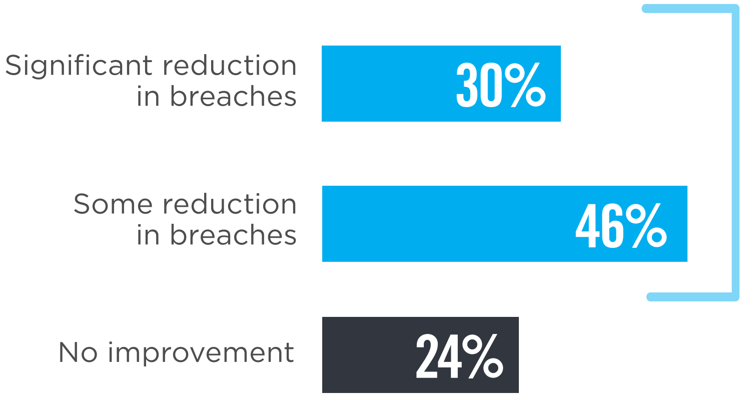
8%
Better threat analysis

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 of 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.

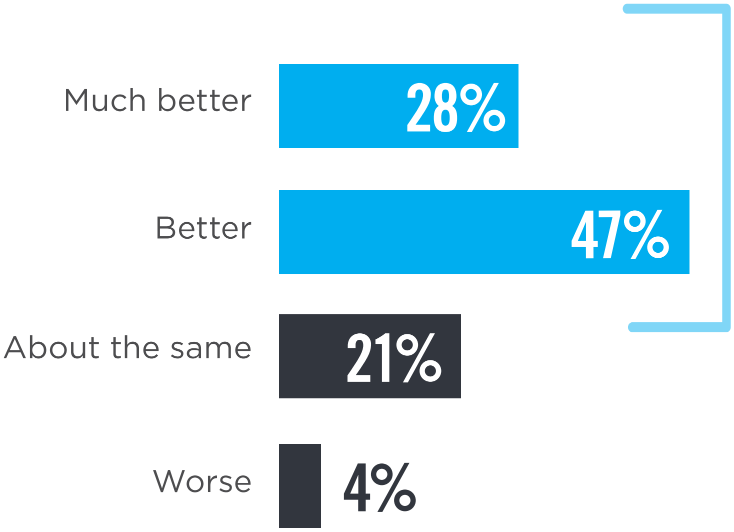
Has the occurrence of security breaches in your organization changed as a result of using SIEM?



76%

Report SIEM resulted in reduction of security breaches

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



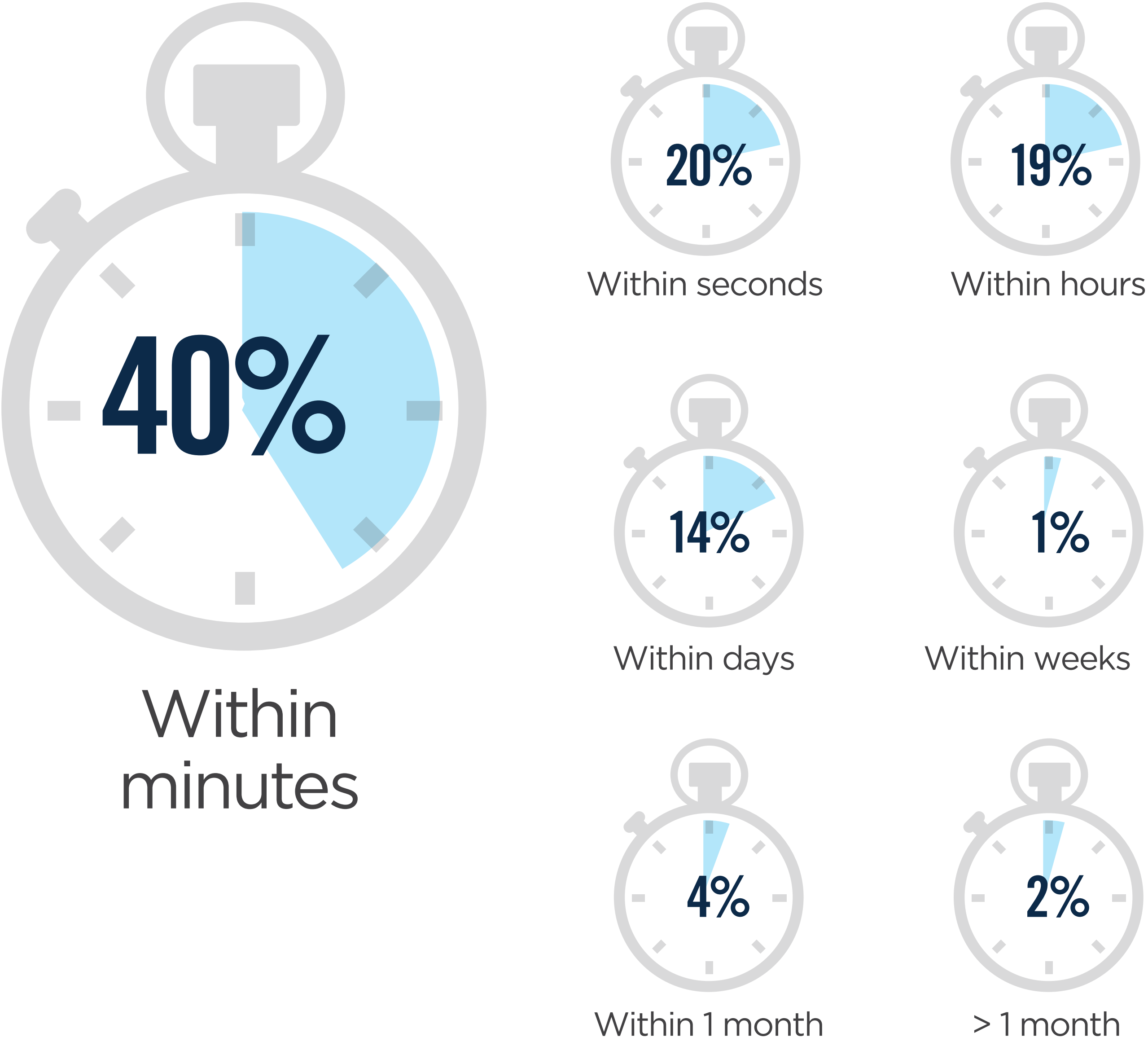
75%

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.

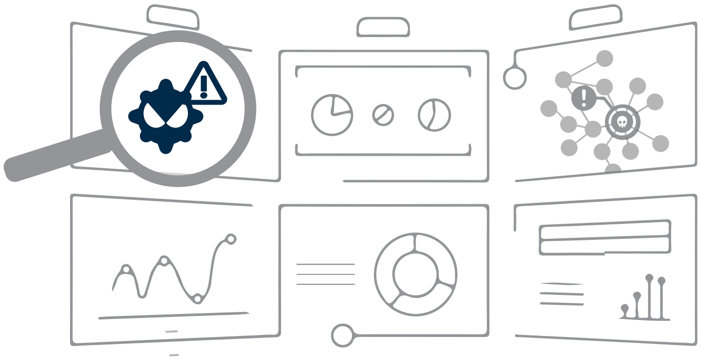
How quickly can your SIEM platform typically detect possible security events or compromise?



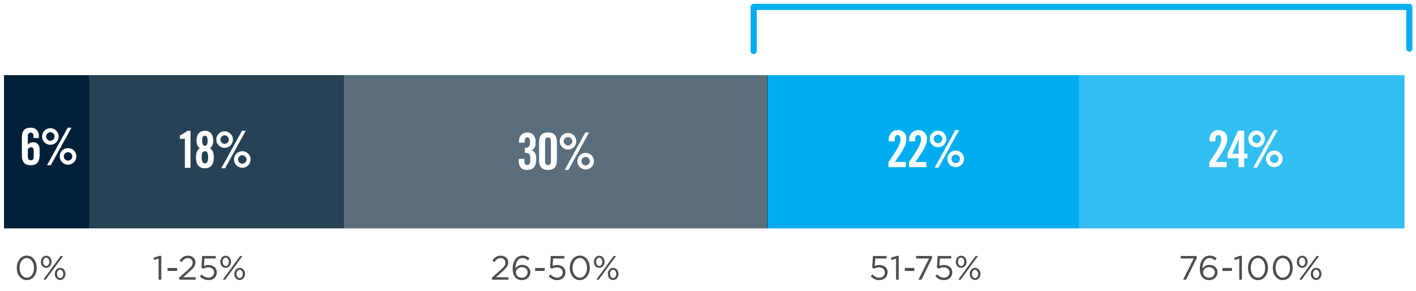
DETECTION RATE

Forty-six percent of cybersecurity professionals say that their SIEM detects at least half of all security incidents.

What percentage of security events or compromises are detected by your SIEM platform?



46% organizations say SIEM detects at least half of security events.



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

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 HURDLES

The lack of skilled security staff to operate SIEM is the single biggest bottleneck to more effective use of the platform (40%). This is followed by the need to manually create or refine rules and lack of budget (tied at 34%), and being overwhelmed by too many false positive alerts (31%).

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

40%

Lack of skilled/trained staff to operate effectively

34%

Having to manually create/refine rules

34%

Lack of budget

31%

Too many false positives

Too many false positives 31% | System complexity 30% | Lack of contextual information from security tools 27% | Company culture 26% | Lack of security awareness among employees 23% | Difficulty implementing and deploying the solution 21% | Lack of management support/awareness/buy-in 21% | Lack of visibility into network traffic and other processes 20% | Poor integration/interoperability between security solutions 19% | Insufficient or inadequate tools available in-house 18% | Poor vendor support 14% | Lack of effective security solutions available in the market 12% | Other 4%

SECURITY CHALLENGES

The biggest challenges faced by organizations' security teams include monitoring of cloud infrastructures (37%), lack of visibility across IT environment (33%), and the lack of skilled security staff (32%) – one of our perennial cybersecurity challenges.

Which of the following do you consider to be top challenges facing your security team?

37%

Monitoring security of cloud infrastructure

33%

Getting full visibility to all assets and vulnerabilities across the entire environment

32%

The lack of advanced security staff to oversee threat management

32%

Too much time wasted on false positive alerts

Detection of advanced threats (hidden, unknown, and emerging) 31% | Lack of visibility into context around threats 28% | Monitoring threats from mobile devices 27% | Lack of proper reporting tools 27% | Slow response time to advanced threats 25% | Detection and/or mitigation of insider threats (negligent, malicious, and compromised users) 24% | Working with outdated SIEM tools and SOC infrastructure 20% | Lack of confidence in automation tools catching all threats 18% | Other 4%

CRITICAL SIEM CAPABILITIES

The most critical SIEM capabilities prioritized by cybersecurity professionals are real-time analysis and alerting of security threats (61%), and the detection of threats and integration of threat intelligence (51%).

What SIEM capabilities are most important to you?

61%

Real-time analysis and alerting of security threats

51%

Threat intelligence integration

50%

Advanced threat detection

50%

Incident response and forensics

Threat prioritization 47% | Data, system & application monitoring 45% | Dashboards 44% | Correlation and linking of individual events into useful information 41% | Advanced analytics (such as artificial intelligence (AI) or machine learning (ML) 41% | Retention of historical data and forensic analysis 41% | Reporting 41% | User monitoring 39% | Collection of security event information in a central repository 33% | Ability to customize platform to organization-specific requirements 25% | Workflow and case management 24% | Support of compliance requirements 21% | Other 4%

SIEM INTEGRATION

SIEM platforms are highly integrated with other systems and applications to increase the breadth of data analyzed to alert and report on security events. The most common integrations are with intrusion detection and prevention systems (58%), followed by firewalls (53%) and event application logs (50%).

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

58%

Intrusion detection/ prevention (IDS/IPS)

53%

Next generation firewall (NGFW)

52%

Web application firewall (WAF)

50%

Applications (event logs, audit logs)

43%

Anti-malware/ ransomware

43%

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

40%

Data loss prevention (DLP)

Identity and Access Management (IAM) 38% | User behavior monitoring 37% | Network access control (NAC) 36% | Vulnerability management tools (scanners, configuration and patch management, etc.) 33% | Security intelligence feeds from third-party services 33% | Cloud activity 33% | Static Endpoints (PC, endpoint protection, log collectors) 33% | Vulnerability management (VM) 32% | Threat intelligence from security vendors 31% | Dedicated log management platform 30% | Netflow 30% | Relational Databases (transactions, event logs, audit logs) 30% | Network packet-based detection 30% | Unified threat management (UTM) 29% | Anti Denial of Service solution (Anti DDoS) 27% | Whois/DNS/Dig and other Internet lookup tools 27% | Mobile Endpoints (mobile devices, MDMs, mobile apps) 27% | SIEM technologies and systems 27% | Network-based malware sandbox platforms 25% | Management systems for unstructured data sources (NoSQL, Hadoop) 19% | Endpoint detection and response 14% | Asset discovery 12% | Social media applications (Facebook, Twitter) 11% | Other 4%

THREAT MANAGEMENT FOCUS

Cybersecurity professionals prioritize investment in threat detection (62%) over incident response (53%) and deterrence (49%). Only very few organizations place high value on deception technologies (16%).

What aspect(s) of threat management does your organization mostly focus on and invest in?

62%

Detection
(e.g. user monitoring, IDS, UEBA)

53%

Incident response & mitigation

49%

Deterrence
(e.g. access controls,

48%

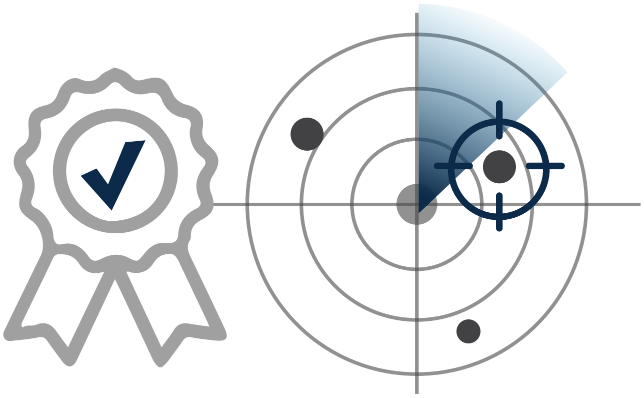
Denial
(e.g. firewall, threat

Compliance 45% | Analysis & Post Breach Forensics (e.g., SIEM, log analysis, etc.) 45% | Deception (e.g., honeypots, etc.) 16% | None 2% | Other 3%

THREAT MANAGEMENT PRIORITIES

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%). Improved automation of threat response only reaches the number four spot with 40%.

▶ **What aspect(s) of threat management does your organization mostly focus on and invest in?**



55%

Improve threat detection

48%

Proactive threat hunting

44%

Improve investigating and analyzing threats

40%

Automate incident response

39%

Improve lateral movement detection

Improve alerting 37% | Reduce false positive alerts 35% | Improve blocking threats 31% | Improve compliance posture 30% | Reduce unwanted/unauthorized traffic 27% | Improve enforcement of usage policies 24% | Aggregate security alerts 8% Not sure/other 4%

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%

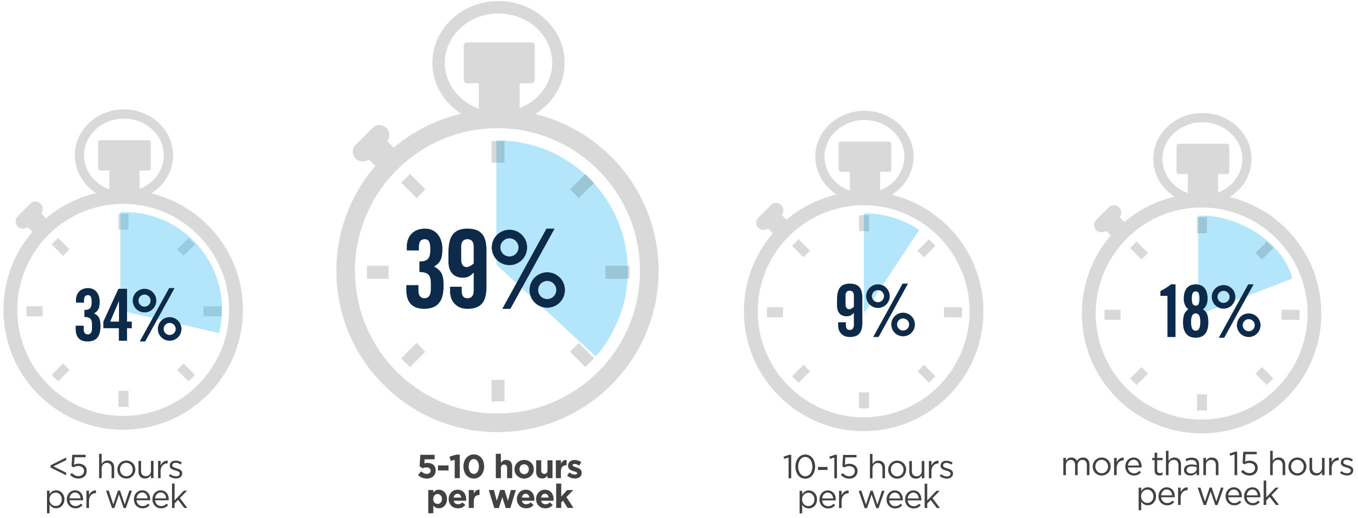
Provide compliance reporting

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%

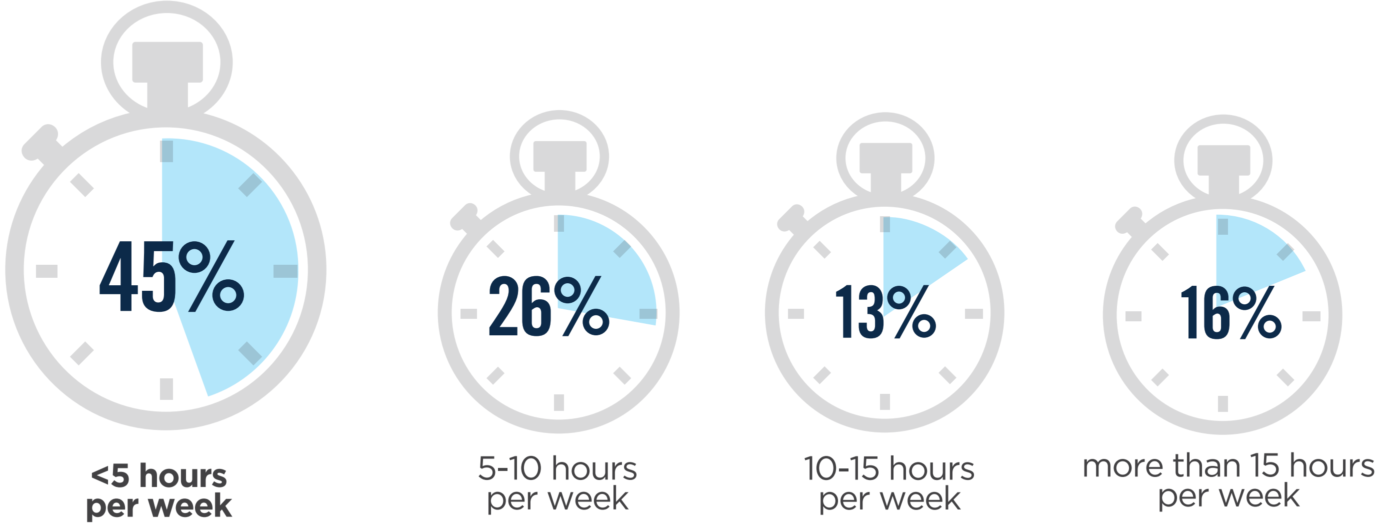
TIME SPENT WITH SIEM

Most commonly, users spend five to 10 hours a week researching SIEM alarms (39%). This is followed by a third of users who spend less than five hours a week (34%). Over a quarter of respondents spends more than 10 hours a week researching SIEM alarms (27%). Typically, about half of users spend less than five hours per week creating rules for their SIEM platform (45%). This is followed by a quarter of users who spend five to 10 hours a week (26%). Almost a third respondents spend more than 10 hours a week creating SIEM rules (29%).

How much time per week is spent researching alarms from the SIEM platform?



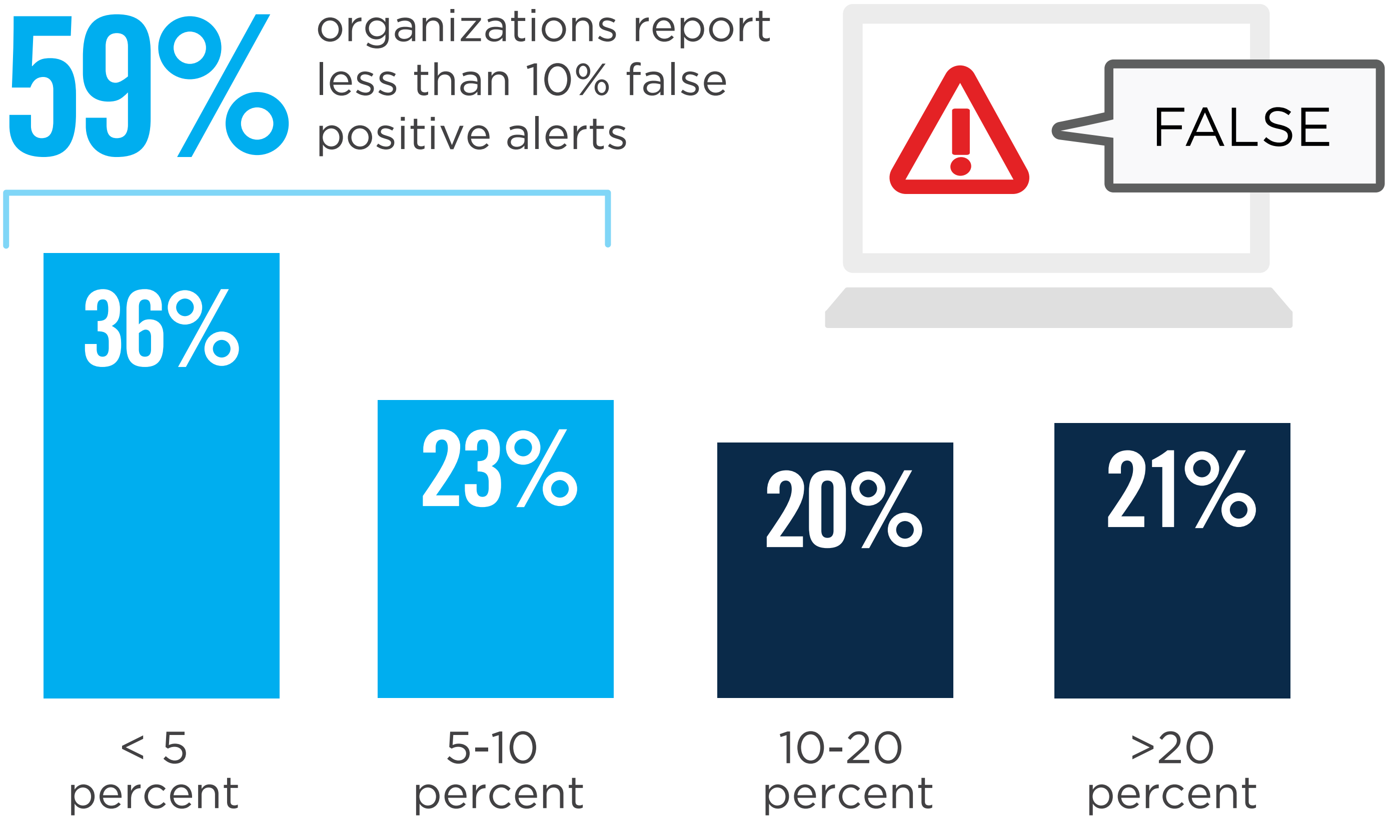
How much time per week is typically spent creating correlation rules for your SIEM platform?



FALSE POSITIVES

While a majority of 59% of organizations report less than 10% of false positive alerts, the remaining 41% experience over 10% false positives each week with the attending consequences for security productivity and accuracy.

What percentage of threat alarms on a weekly basis are false positive?



SWITCHING SIEM VENDORS

For companies considering switching to a new SIEM vendor, cost factors play the biggest role (56%), followed by a perceived lack of features (43%) and ease of use (29%).

▶ **What are the main reasons why you would consider switching to a new SIEM vendor?**

56% License/ subscription cost

43% Lack of features/ functionality

29% Lack of ease of use

25% Lack of ability to customize

Solution complexity 24% | Too many false positives 23% | Support issues 21% | Poor product performance 18% | Migrating to a Managed Service 18% | Too complicated to add new data feeds 18% | Lack of out-of-the-box integration with other security controls 7% | Other 15%

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%

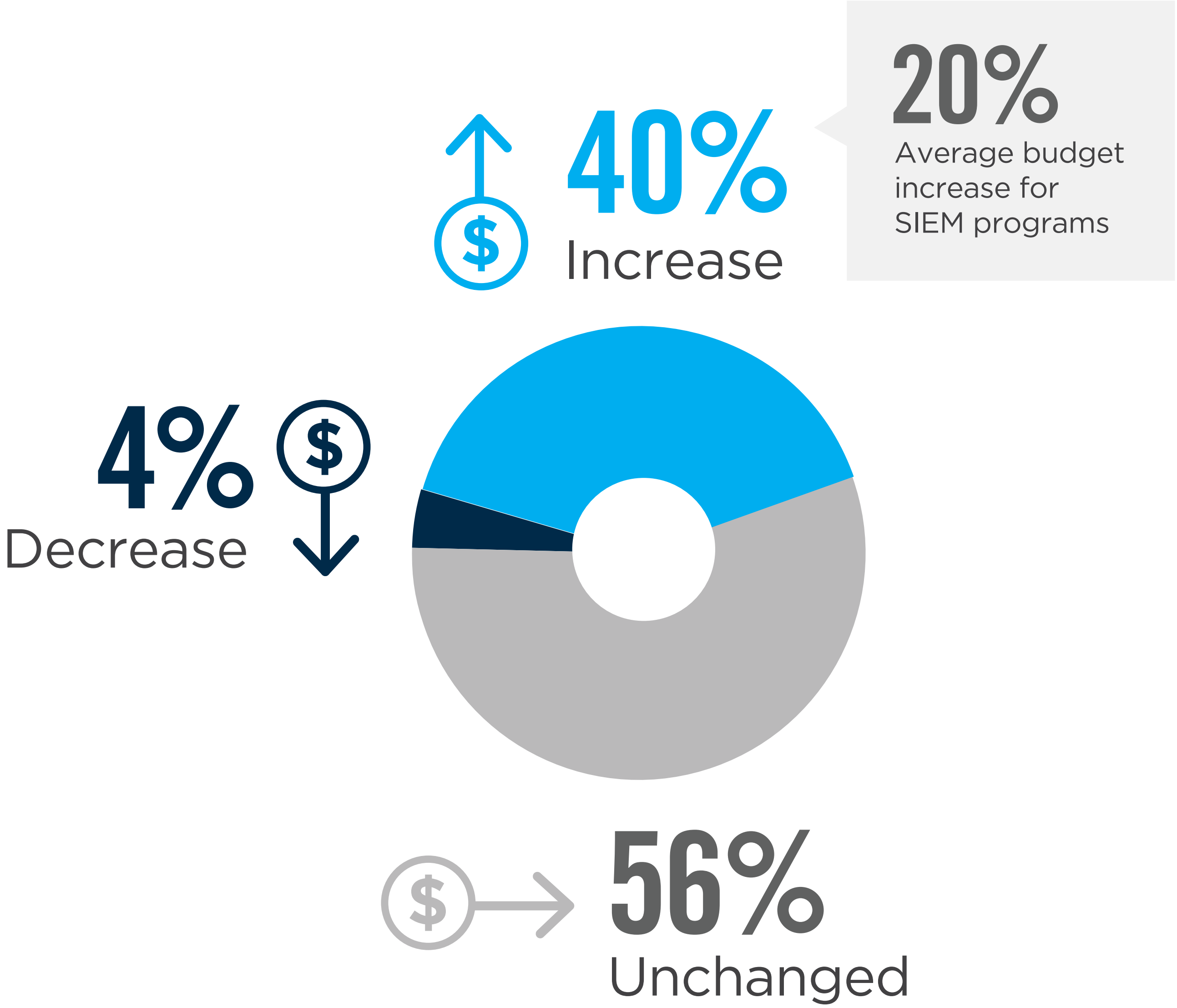
Product ease of use

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

SIEM BUDGET TRENDS

A solid 40% of organizations expect budgets for SIEM technology to increase over the next 12 months by an average of 20%. A majority of 56% anticipates no budget changes.

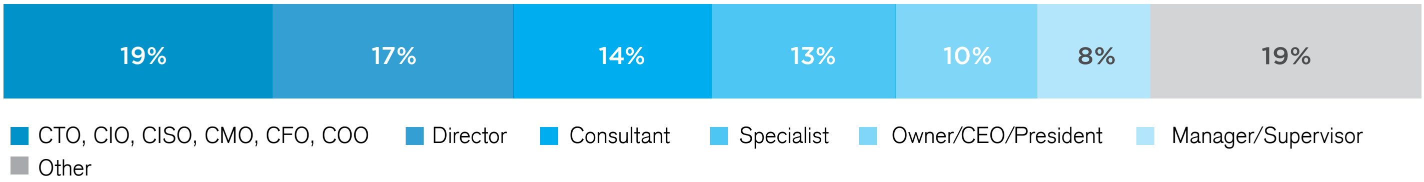
How do you expect your organization's SIEM related budget to change over the next 12 months?



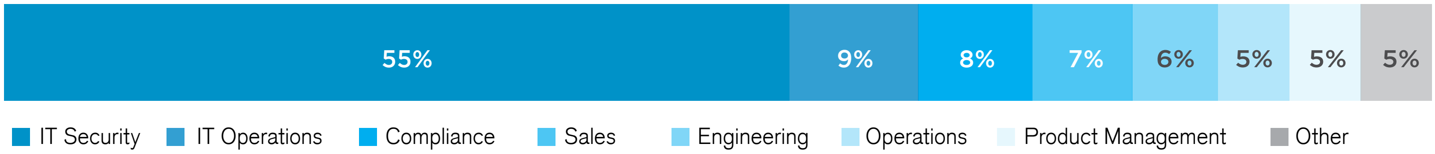
METHODOLOGY & DEMOGRAPHICS

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.

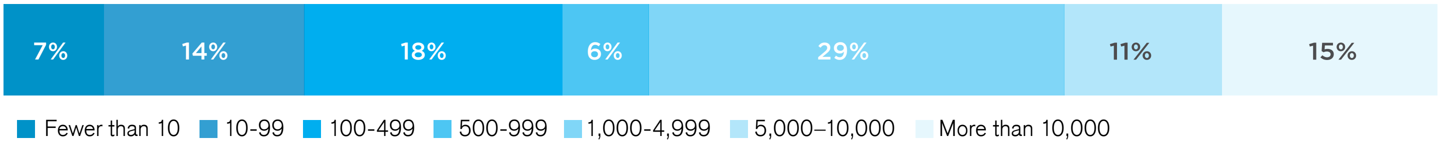
CAREER LEVEL



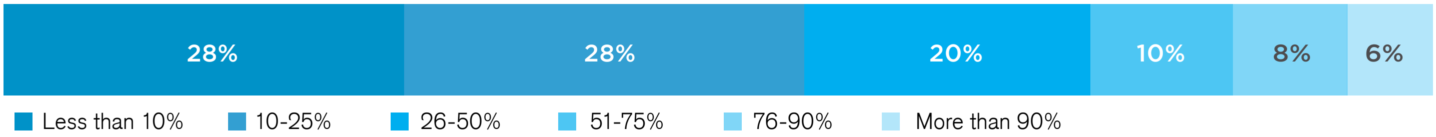
DEPARTMENT



COMPANY SIZE



SHARE OF IT INFRASTRUCTURE IN THE CLOUD


Less than 10%
More than 90%