THREAT

MONITORING, DETECTION & RESPONSE

2017 REPORT

Linked in Group Partner

Information Security

Crowd Research Partners

ALIEN VAULT

bitglass

BLUVECTOR

ControlScan

DELTA RISK
A CHERTOFF GROUP COMPANY

DOMAINTOOLS

Dtex systems

EventTracker
Actionable Security Intelligence

exabeam

observe it

SOFTACTIVITY

tenable

THREAT MONITORING DETECTION & RESPONSE 2017 REPORT

TABLE OF CONTENTS

INTRODUCTION

Information security teams worldwide are increasingly concerned about the rapid growth of cyber threats. To address this concern and provide peer insights, Crowd Research Partners, in partnership with the 370,000+ member Information Security Community on LinkedIn, has conducted an in-depth study on several important threat lifecycle topics.

This study is a summary of responses from over 400 cybersecurity professionals to provide a comprehensive snapshot on the evolving threat landscape, insider and external threats, preventative measures, threat monitoring and data collection, threat intelligence, threat detection, threat hunting, threat analytics, incident response, and incident recovery.

We believe that the insights from this report will provide valuable guidance on effectively identifying and addressing a range of cyber threats.

We would like to thank our study sponsors for supporting this research on a critical topic within the information security community: AlienVault® | Bitglass | BluVector | ControlScan | Delta Risk | DomainTools | Dtex | EventTracker | Exabeam | ObserveIT | SoftActivity | Tenable

In addition, we want to thank all survey participants who provided their time and input in completing the study.

We hope you will enjoy reading this report and gain insight from its major findings.

Thank you,

Holger Schulze

Holger Schulze
Founder
Linkedin Information
Security Community
✉ hhschulze@gmail.com

Linked in Group Partner
Information
Security

KEY FINDINGS

1 Dealing with advanced threats is the most significant concern for cybersecurity professionals: ransomware (48%), phishing attacks (48%) and attendant data loss (47%). The level of concern with these threat categories has grown significantly over the past 6 months.

2 Respondents noted significant challenges in responding to advanced threats - the most significant being the ability to detect threats (62%). Interestingly, survey participants also noted concerns with the lack of advanced security staff (41%) and slow speed of response (23%).

3 As with prior surveys, lack of budget (51%), lack of skilled personnel (49%), and lack of security awareness (49%) weighed in as the most significant obstacles facing security teams.

4 A large proportion of organizations use threat intelligence platforms – with 57% using one or more commercial threat intelligence providers followed by 47% using open source platforms.

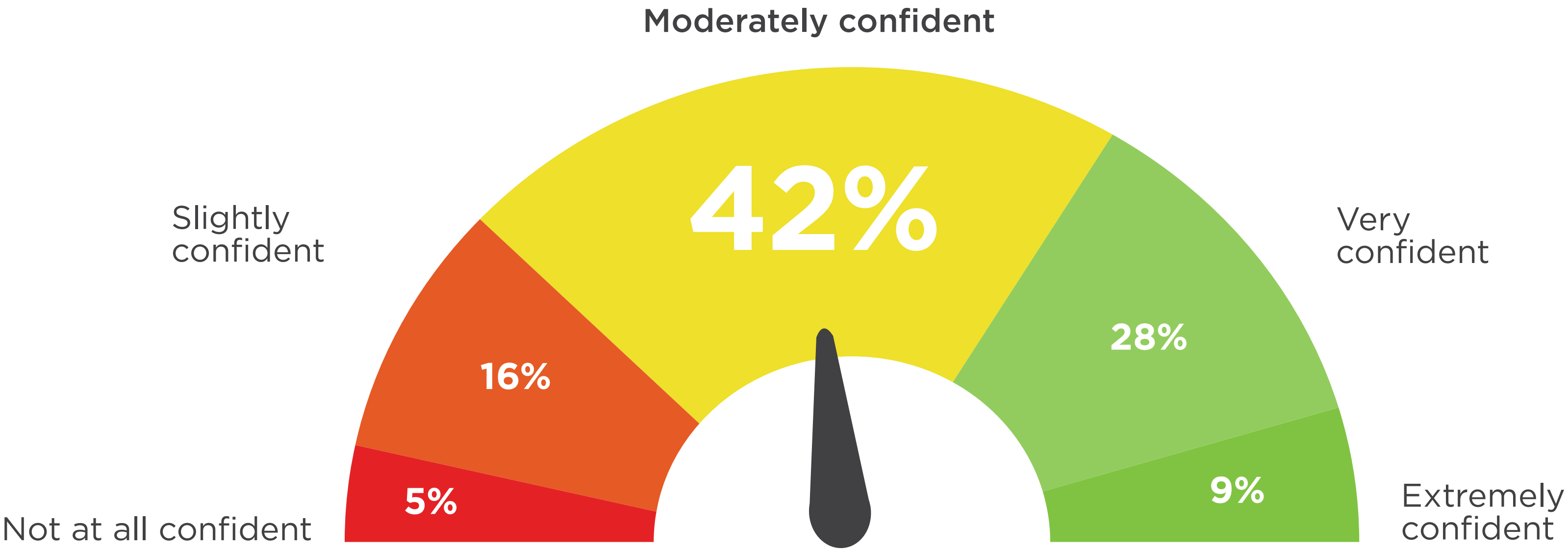
5 Insider threats continue to be a growing concern (51% perceived a growth in these threats over the past year) with inadvertent breaches (61%) identified as the leading cause. User training was identified by 57% of respondents as their leading method for combating such threats.

OVERVIEW

CONFIDENCE IN SECURITY POSTURE

For each of our surveys, we like to gain a perspective on organizations' overall confidence in their security posture. When comparing survey results to a prior survey conducted in January of 2017, we found that responses for the moderately to extremely confident categories declined by a collective 5 percentage points. This may be due to concerns following the recent spate of ransomware attacks.

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

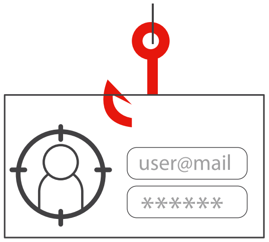


CYBER THREATS OF CONCERN

We asked respondents to identify the areas of cyberthreats most concerning to them. Not surprisingly, given the recent spate of ransomware attacks, this is a top area of concern (at 48%). Interestingly, phishing attacks and the attendant impact of data loss were also at about the same level of concern (48% and 47% respectively).

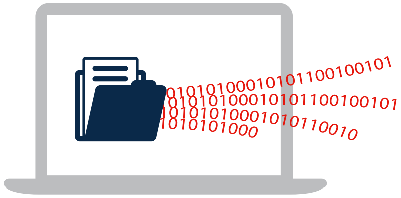
Security teams' concerns are evolving with the rapidly changing nature of cyberthreats. In comparing the results of this study to our Cybersecurity Trends report created earlier this year, we saw a marked growth in the level of concern with phishing attacks and malware – as well as significant new areas of concern with ransomware and attendant data loss. We also noted a similar growing concern with insider threats, even though the threat has a different underlying root cause.

Q: Which cyberthreats are you most concerned about?

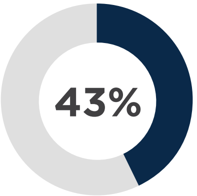


48%
Phishing attacks

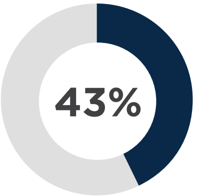
48%
Ransomware



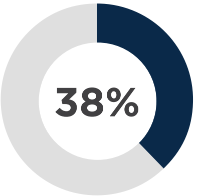
47%
Data exfiltration/data loss



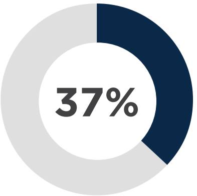
Insider attacks



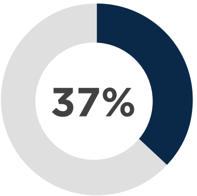
Malware



Unauthorized Access



Advanced persistent threats (APTs)/targeted attacks



Zero-day attacks

Hijacking of accounts, services or resources 36% | Web application attacks (buffer overflows, SQL injections, cross-site scripting) 28% | Denial of service attacks (DoS/DDoS) 26%

TOP SECURITY CHALLENGES

Given the cyberthreats of concern, we investigated how they related to the challenges faced by security teams. Here, we noted an interesting pattern of challenges related to the current generation of threats – their detection (62%), lack of advanced security staff (41%), and slow response times to remediate (23%). These challenges are consistent in the cybersecurity industry and were identified in other areas of this report.

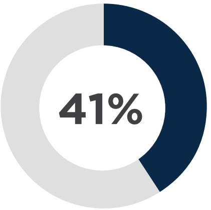
Q: Which of the following do you consider to be top challenges facing your security team?

62%

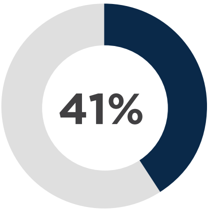
Detection of advanced threats (hidden, unknown, and emerging)

48%

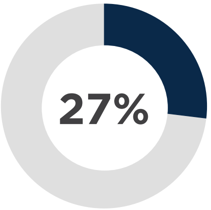
Detection and/or mitigation of insider threats (negligent, malicious, and compromised users)



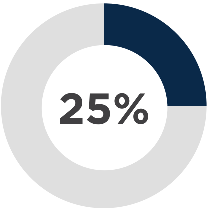
The lack of advanced security staff to oversee threat management



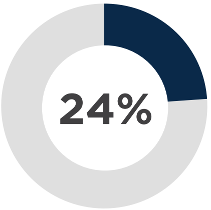
Getting full visibility to all assets and vulnerabilities across the entire environment



Lack of confidence in automation tools catching all threats



Lack of proper reporting tools



Monitoring security of cloud infrastructure

Slow response time to advanced threats 23% | Too much time wasted on false positive alerts 20% | Working with outdated SIEM tools and SOC infrastructure 19% |

ORGANIZATIONAL BARRIERS

Given the challenges faced by security teams, we wanted to understand the key organizational barriers preventing teams from effectively responding to cyberthreats. Consistent with our prior research, budget (51%), lack of skilled personnel (49%), and lack of security awareness (49%) were reported as the key inhibitors by half of the respondents.

Q: Which of the following barriers inhibit your organization from adequately defending against cyberthreats?

#1

Lack of budget

51%

#2

Lack of skilled/ trained personnel

49%

#3

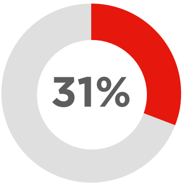
Lack of security awareness among employees

49%

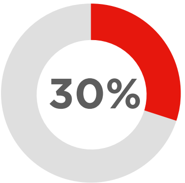
#4

Insufficient or inadequate tools available in house

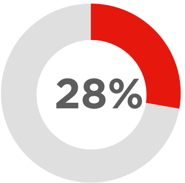
36%



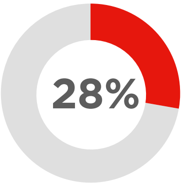
Poor integration/ interoperability between security solutions



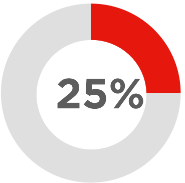
Too much data to analyze



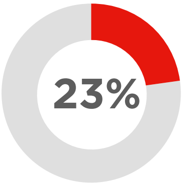
Lack of management support/awareness /buy-in



Lack of visibility into network traffic and other processes



Lack of collaboration between separate departments



Inability to justify additional investment

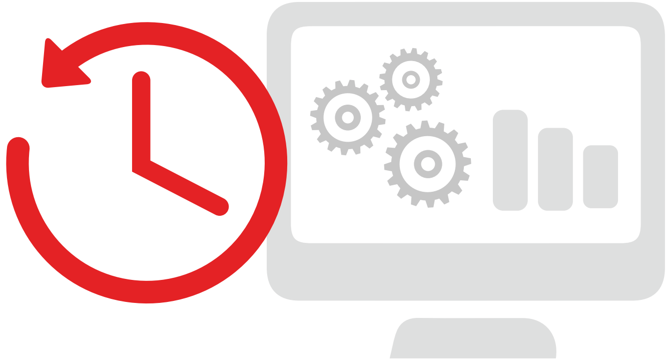
Lack of contextual information from security tools 23% | Difficulty in implementing new security systems/tools 21% | Too many false positives 20% | Lack of confidence in using the information to make decisions 15% | Lack of effective security solutions available in the market 14%

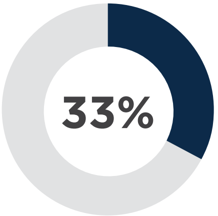
SECURITY BUSINESS IMPACT

When asked about the business impact of security incidents, system downtime was highlighted as having the biggest impact – as might be expected. Several significant consequences included disruption of business operations, reduced productivity, and the need to redeploy IT resources. Interestingly, revenue impact was only cited as a relatively minor factor – suggesting that either security teams have evolved their maturity to effectively manage risk or lack full visibility into the downstream business impact of security incidents.

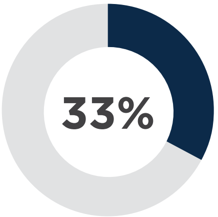
Q: What negative impact did your business experience from security incidents in the past 12 months?

38% System downtime

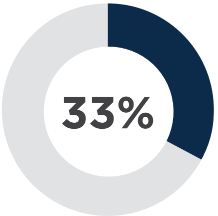




Disrupted business activities



Reduced employee productivity



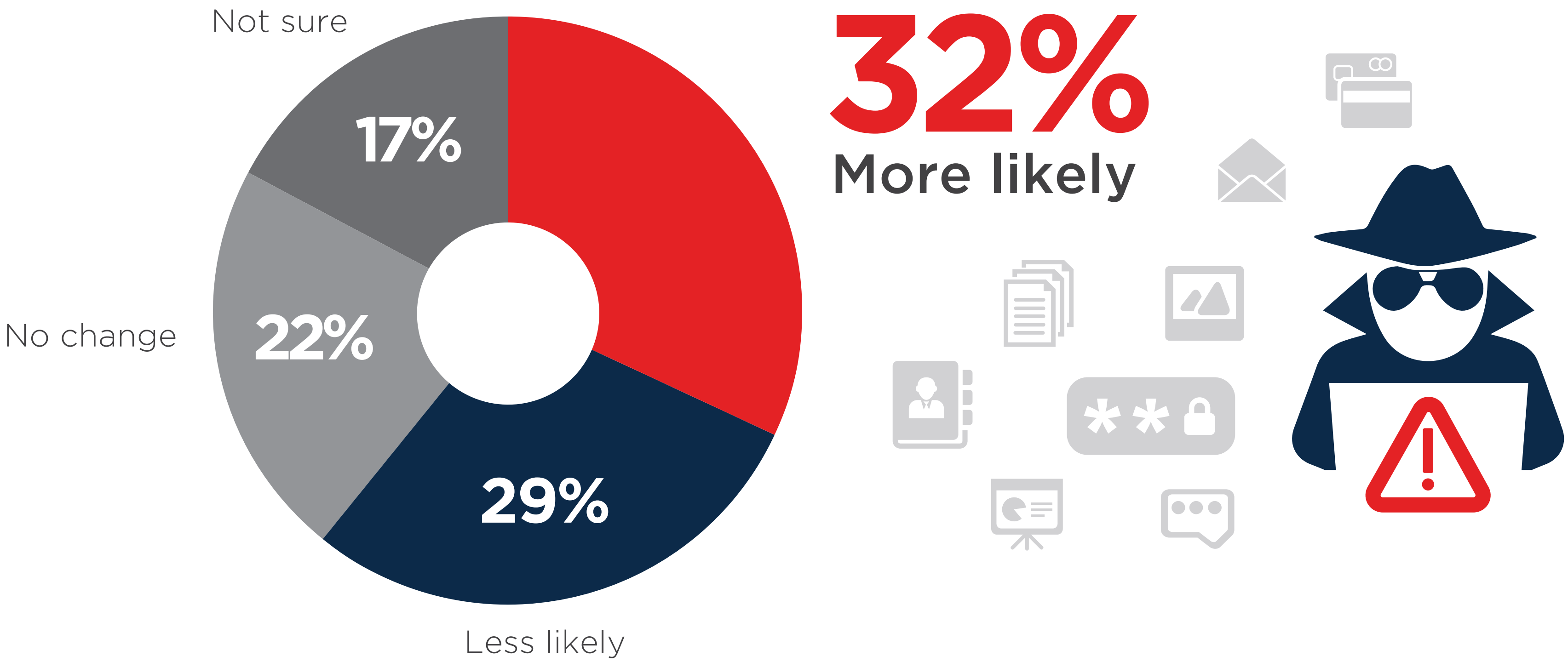
Deployment of IT resources to triage and remediate issue

No business impact 29% | Increased helpdesk time 26% | Data loss 24% | Reduced revenue/lost business 16% | Negative publicity/reputational damage 13% | Loss/compromise of intellectual property 11% | Customer loss 8% | Lawsuit/legal issues 6% | Regulatory fines 5%

CYBER ATTACK OUTLOOK

One of the points we investigated was to understand how sanguine security teams were in their assessment of exposure to future attacks. Here, we found a remarkably even distribution of expectations. Roughly a third (32%) expected that compromise was more likely, while a slightly smaller number (29%) felt that compromise was less likely. We suggest that this is a reflection of confidence in security posture – with the 51% of “Less Likely” and “No Change” respondents having varying degrees of confidence.

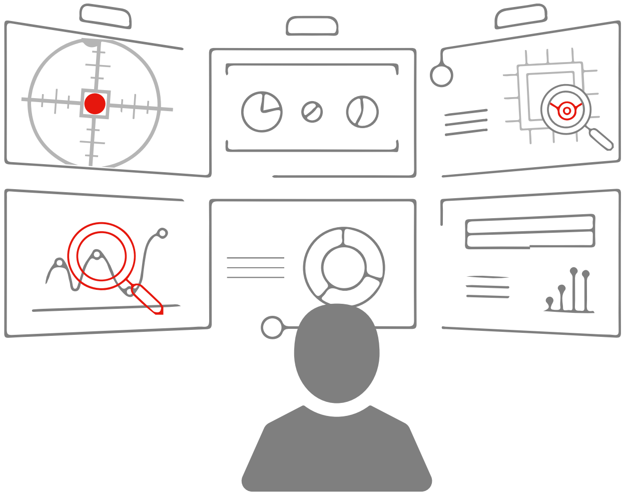
Q: What is the likelihood that your organization will become compromised by a successful cyber attack in the next 12 months, compared to last year?

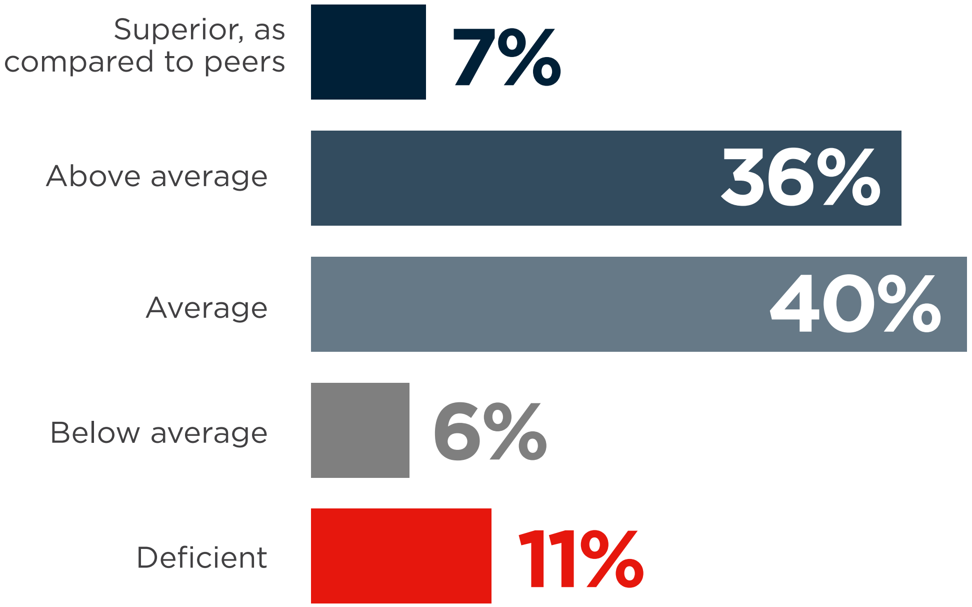


CAPACITY TO DETECT THREATS

Threat detection competence is a major factor in organizations' capacity to manage their cyber risk. Here, we saw an interesting pattern of over 83% indicating that they were average or above average. We're not sure of the reasons for this uneven distribution – particularly given a much more balanced response to expectations of compromise to cyber attack.

Q: How do you assess your organization's current ability to DETECT threats?





SOURCES OF MONITORING DATA

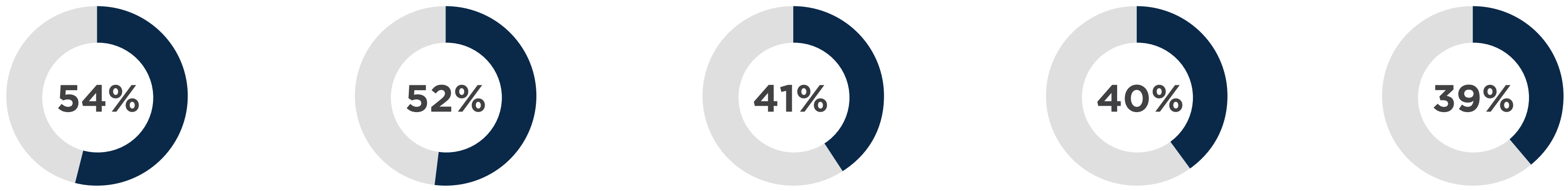
Not surprisingly, the most common sources of monitoring data are applications, firewalls, and endpoints. However, as evident from the survey results, there is a “long tail effect” with data collection from a broad range of sources.

Q: What systems, services and applications do you collect monitoring data from?

59%
Applications
(event logs, audit logs)

57%
Network-based firewalls
(IPS/IDS/UTM devices)

57%
Endpoint
(PC, laptop, mobile device, MDM, NAC, log collectors, anti-malware tools)



Vulnerability management tools

Host-based anti-malware

Network packet-based detection

Intelligence from your security vendors

Host-based IPS/IDS

Security intelligence feeds from third-party services 37% | User and Entity Behavior Analytics (UEBA) 35% | Whois/DNS/Dig and other Internet lookup tools 34% | SIEM technologies and systems 33% | Relational Databases (transactions, event logs, audit logs) 32% | Dedicated log management platform 31% | ID/IAM (identity and access management) systems 29% | Network-based malware sandbox platforms 29% | Cloud activity 24% | Netflow 22% | Social media applications (Facebook, Twitter) 19% | Terminal servers 19% | Management systems for unstructured data sources (NoSQL, Hadoop) 13%

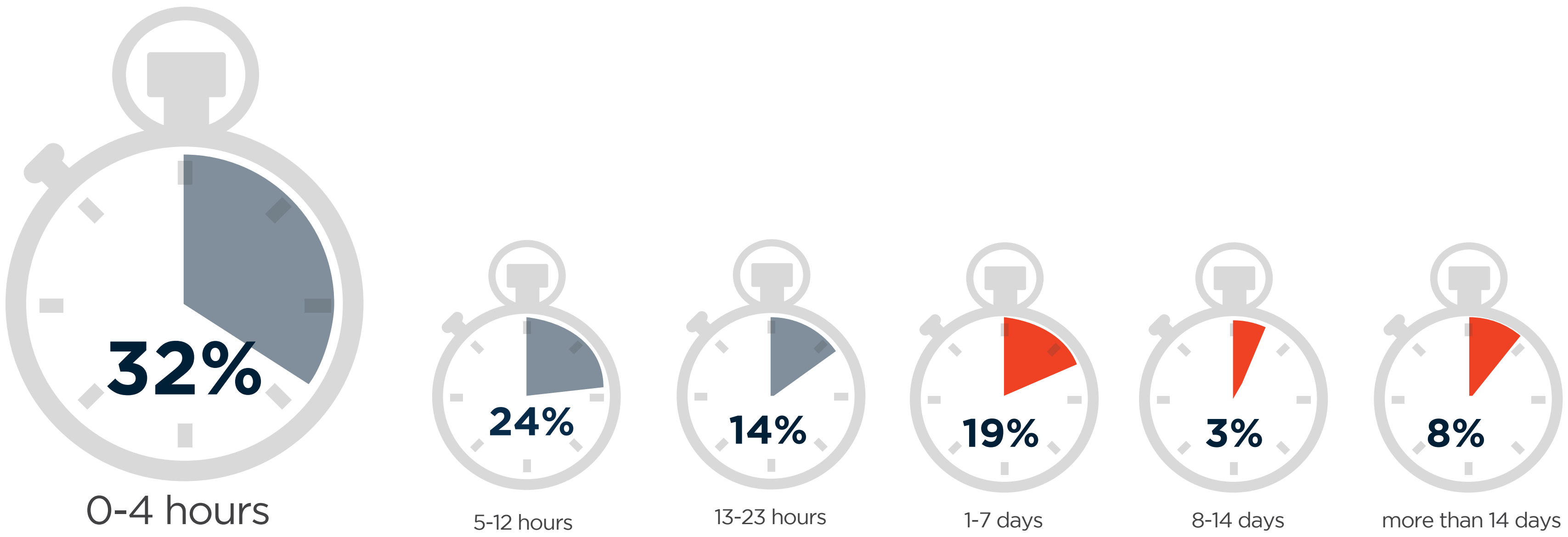
THREAT MANAGEMENT

THREAT MANAGEMENT RESPONSE

One of the interesting questions with security teams is their criteria for judging their competence. In looking at self-assessment of competence in ability to detect threats we found it was very strongly related to the time to detect and respond to incidents.

The data was striking in looking at the gap between <4 hour response and >1 day response. Close to 60% of companies considering themselves as superior had sub 4 hour response, whereas 75% of companies self-declaring as deficient had response time as greater than 1 day.

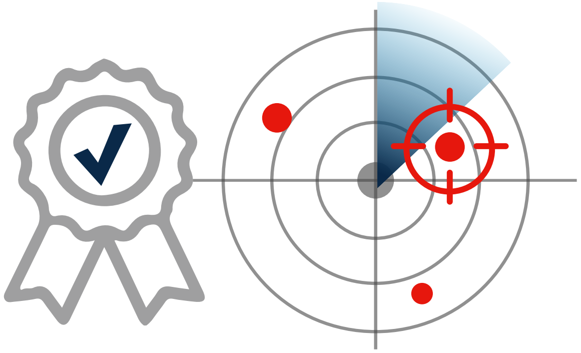
Q: On average how long does it take you to detect, validate and respond to suspected incidents in your organization?



THREAT MANAGEMENT PRIORITIES

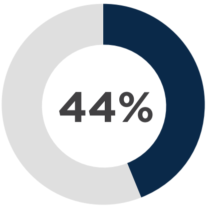
In the focus area of threat management, survey participants were asked about their top priorities. Not surprisingly, improved threat detection was the most significant priority – at 67% – by a large margin above improved investigation and analysis of threats at 44%.

Q: What are the most critical threat management priorities for your organization over the next 12 months?

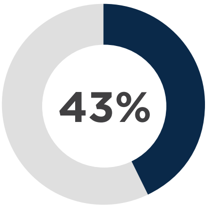


67%

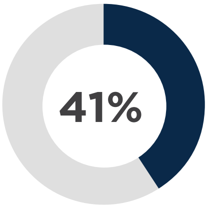
Improve threat detection



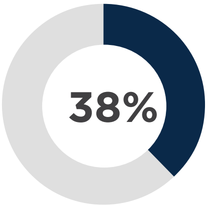
Improve investigating and analyzing threats



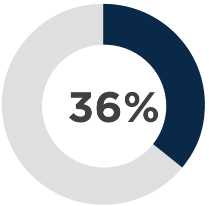
Proactive threat hunting



Improve blocking threats



Reduce unwanted / unauthorized traffic



Automate incident response

Improve lateral movement detection 32% | Aggregate security alerts 30% | Improve enforcement of usage policies 29% | Reduce false positive alerts 25% | Not sure 9%

RANSOMWARE

With the recent ransomware attacks making front-page headlines, we asked respondents about their preferred security solutions to combat this threat category. While organizations employed multiple methods of protection, anti-malware was the dominant preferred method (as expected) – at 76%. Interestingly, data backup and recovery was the second choice – at 65%.

Q: What security solutions do you currently employ to combat ransomware?

Anti Malware

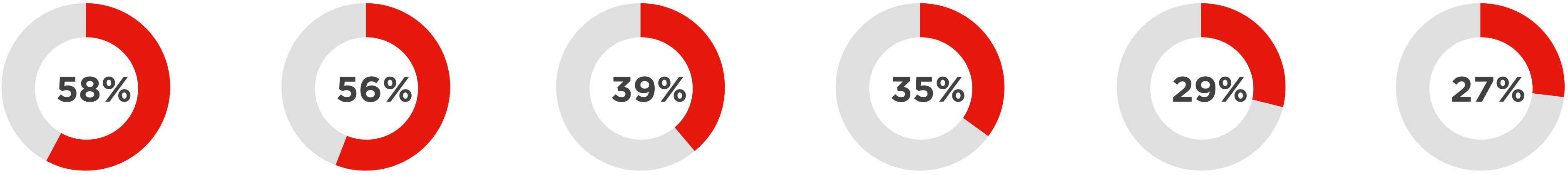
76%

Data backup and recovery

65%

Operating systems and software are current with latest patches

65%



58% Email and web gateways

56% User awareness

39% Advanced endpoint security

35% Application whitelisting

29% Security analytics

27% User and Entity Behavior Analytics (UEBA)

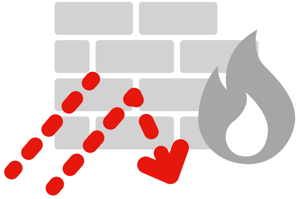
THREAT MANAGEMENT PLATFORMS

Security teams use a broad range of threat management platforms, products and services. Endpoint security is the most common (62%) with IDS/IPS/UTM/Firewalls a close second at 55%. Beyond this we see a “long tail” of platforms ranging from vulnerability management and log management to commercial threat intelligence.

Q: Please indicate which type of threat management platform(s) you use, if any.

62%

Endpoint security vendor

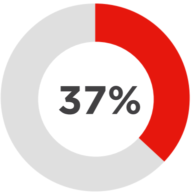


55%

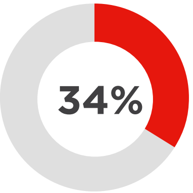
IDS/IPS/UTM/ Firewall vendor

39%

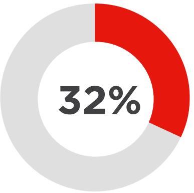
Vulnerability management vendor



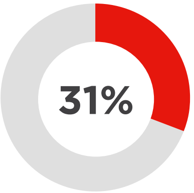
Log management vendor



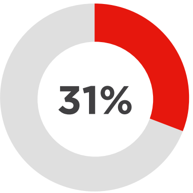
Identity and Access Management (IAM) vendor



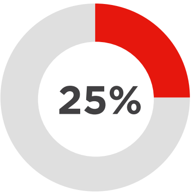
SIEM vendor



User and Entity Behavior Analytics (UEBA)



Application security vendor (including whitelisting/blacklisting)



Managed security services provider

Network packet broker/ Inline monitoring vendor 16% | Forensics vendor 16% | “Dark web” monitoring vendor 12% | CTI service provider 10% | Deception-based detection vendor 9% | CTI platform provider 8%

ASPECTS OF THREAT MANAGEMENT

Among our respondents, the primary pattern of threat management appeared to be one of “blocking” (deterrence at 67% and denial at 66%). Post event activities – detection (56%) and incident response (54%) – were not as commonly utilized. This reflects what we have seen as the most common security posture – defend first, but be prepared to respond to anything that gets through.

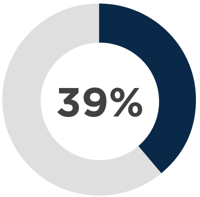
Q: What aspect(s) of threat management does your organization mostly focus on?

67%
Deterrence
(e.g., access controls, encryption, policies, etc.)

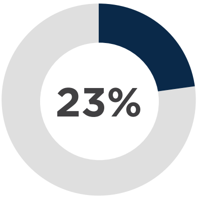
66%
Denial
(e.g., firewall)

56%
Detection
(e.g., user monitoring, IDS, UEBA, etc.)

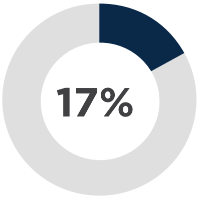
54%
Incident Response



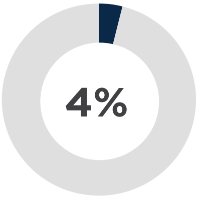
Analysis & Post Breach Forensics
(e.g., SIEM, log analysis, etc.)



Disruption
& Mitigation



Deception
(e.g., honeypots, etc.)



None

THREAT MANAGEMENT CAPABILITIES

What threat management capabilities do cybersecurity professionals prioritize? The capacity to rapidly identify and remediate attacks leads with 76 percent, followed by 24x7 threat intelligence, monitoring and analytics (72%), and threat reporting to identify vulnerabilities (68%).

Q: How valuable are the following features/capabilities?

76% Rapid identification and remediation of attacks

72% 24x7 threat intelligence, monitoring and analysis

68% Threat assessment reports to identify vulnerabilities and risks

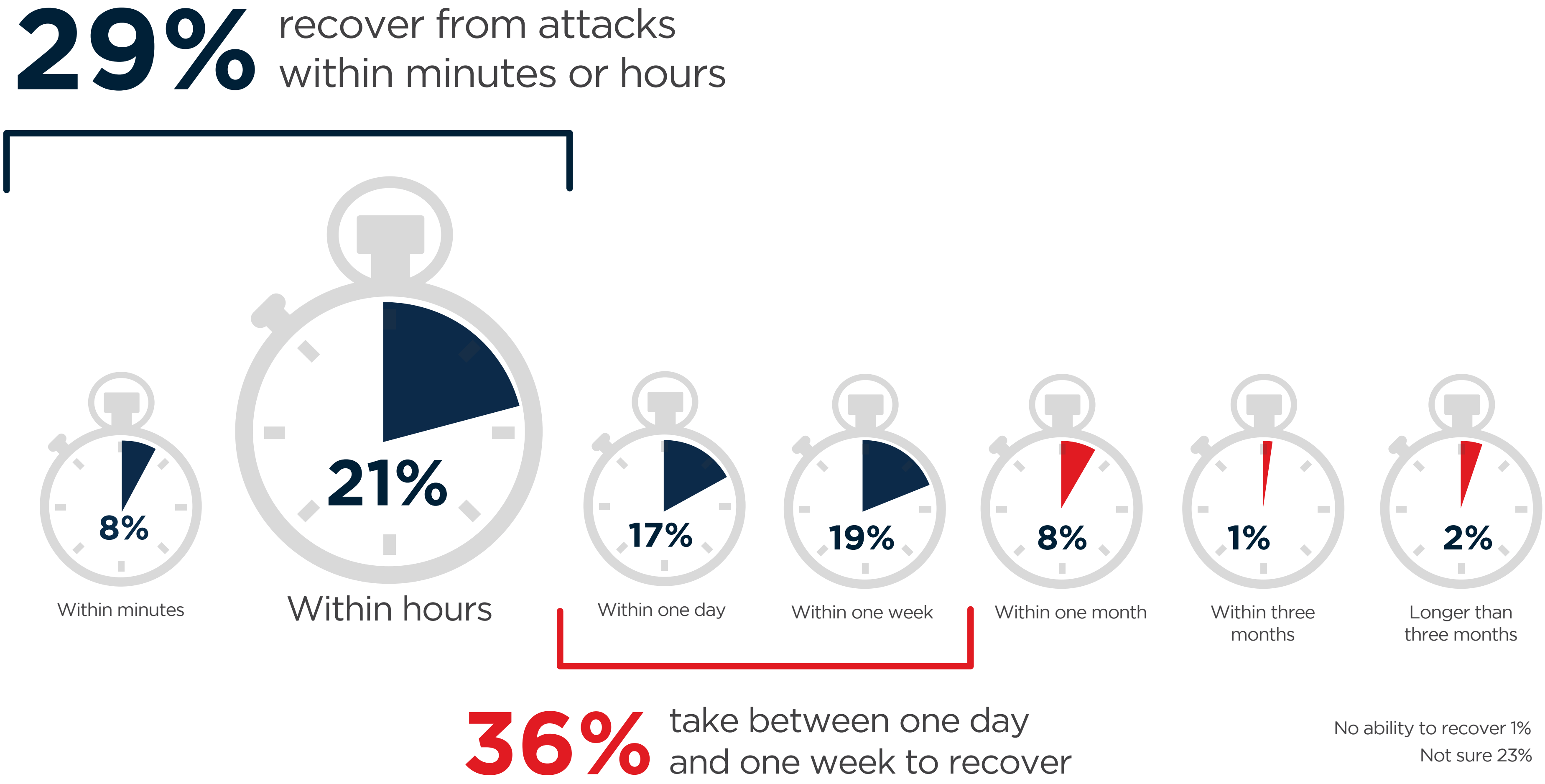
58% Security policy and controls management

Easy incident investigation 57% | Compliance oriented activities 34%

CYBER ATTACK RECOVERY

While 29 percent of organizations recover from cybersecurity attacks within minutes or hours, 36 percent take from a day up to a week to recover.

Q: How long does it take your organization to recover from a cyber attack (on average)?

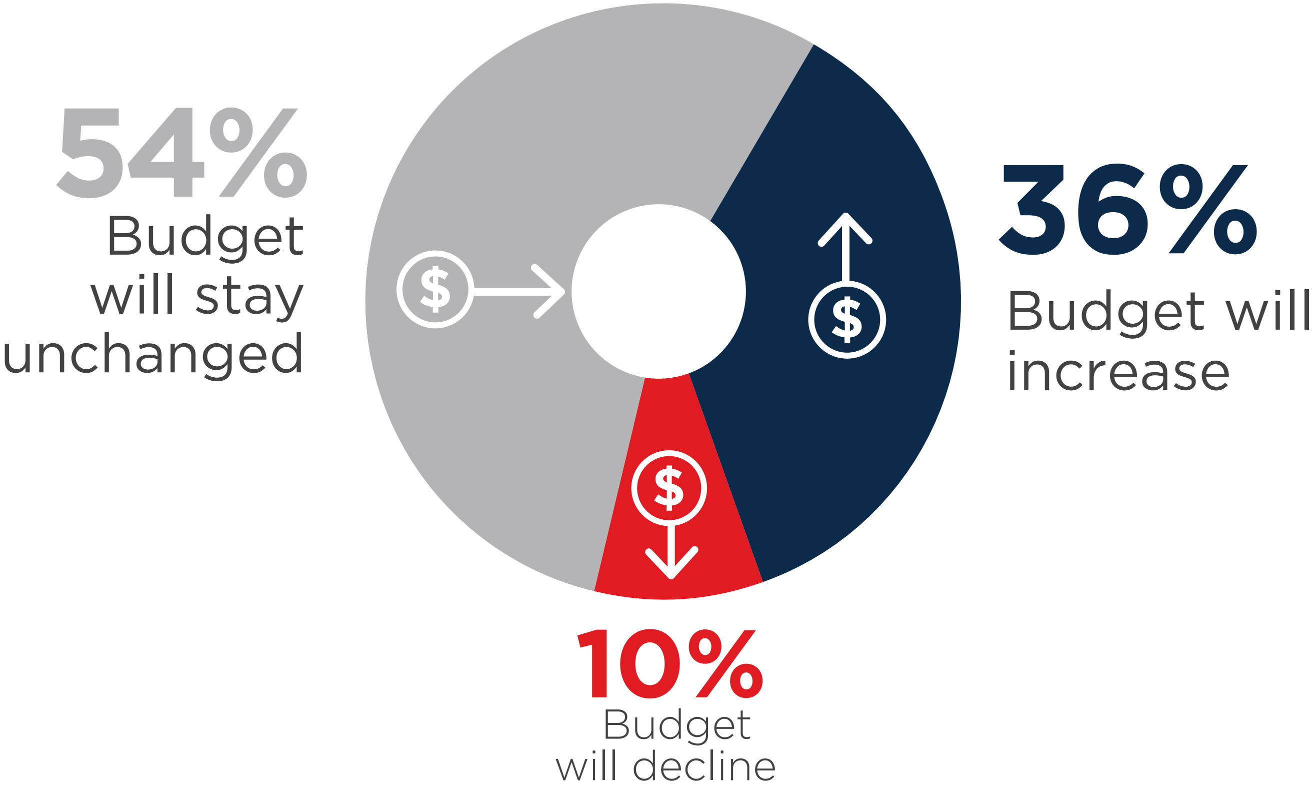


No ability to recover 1%
Not sure 23%

THREAT MANAGEMENT BUDGET

Budgets for threat management are expected to increase for over a third of organizations (36%) in the next 12 months.

Q: How is your threat management budget changing in the next 12 months?

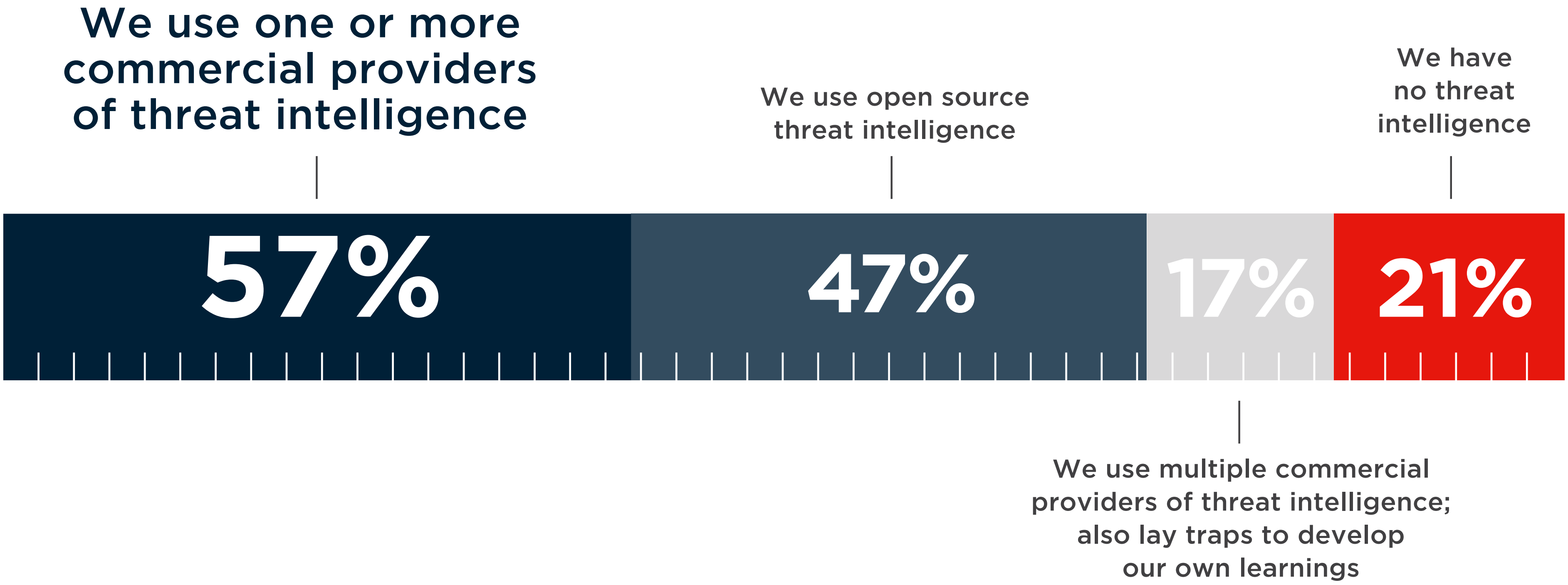


THREAT INTELLIGENCE

THREAT INTELLIGENCE MEASURES

As reported by survey participants, commercial threat intelligence is the most commonly used (57% use one or more commercial providers), with a second group using open source platforms (47%). Interestingly – and most surprising – roughly a fifth of respondents (21%) indicated that they did not use any threat intelligence.

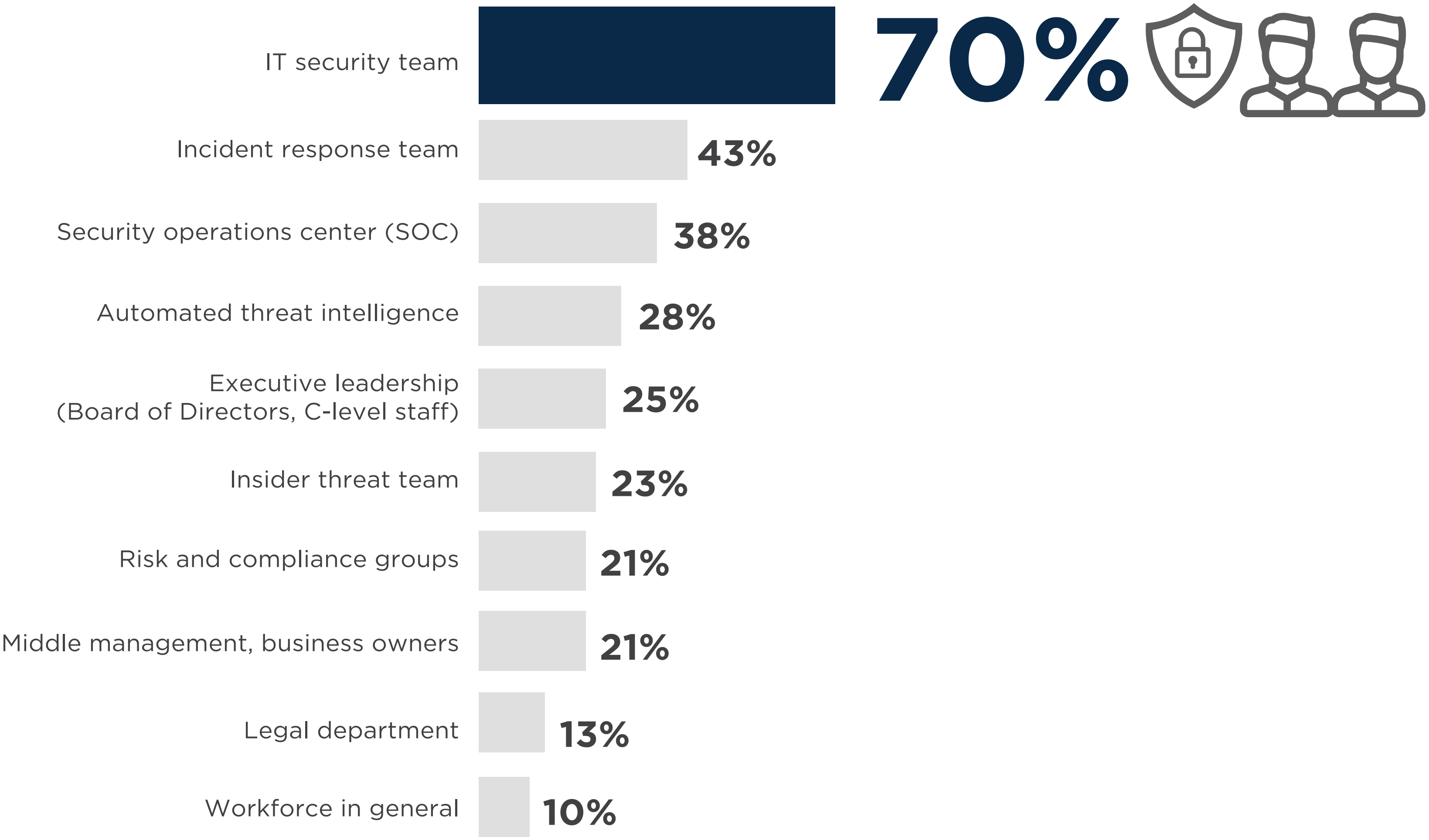
Q: What threat intelligence measures do you use?



USERS OF THREAT INTELLIGENCE

Our survey investigated the uses of threat intelligence. As would be expected, the IT security team is the primary consumer (70%), with the incident response and SOC teams being significant consumers of data (43% and 38% respectively). What is interesting is the breadth of usage – extending to executive management and legal.

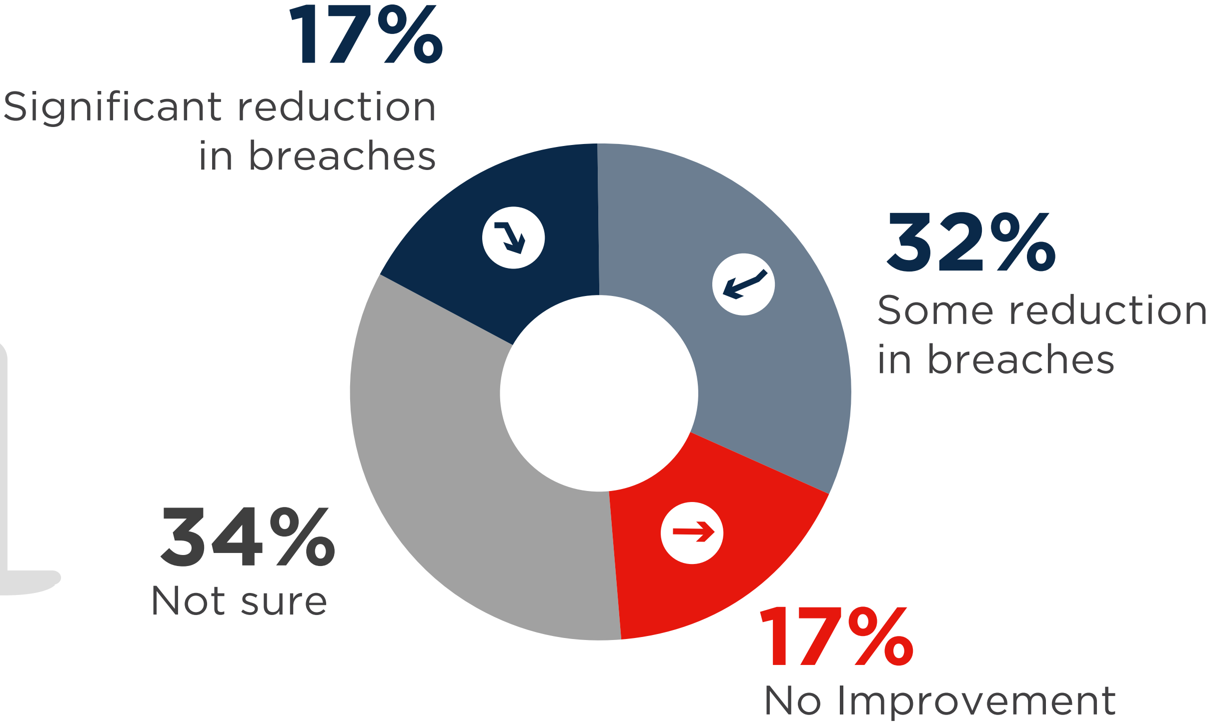
Q: Who are the primary consumers of threat intelligence in your organization?



THREAT INTELLIGENCE IMPACT

One of our most significant areas of investigation was to identify the benefits of the use of threat intelligence. As we found, about half (49%) of respondents reported a reduction in breaches – although to varying degrees.

Q: Has the occurrence of security breaches changed as a result of using threat intelligence solutions?



PRIORITIZATION OF SECURITY EVENTS

In threat management, an important question is how security events are brought to the attention of the IT/security team. Here we see a significant difference between all respondents, and those that declare themselves to be superior/above average in their ability to respond to detected threats. In particular, the latter group has more reliance on the use of intelligence services providers, conducting proprietary searches and UEBA (User and Entity Behavior Analytics).

For example, endpoint monitoring is used in 60% of all organizations as the leading mechanism of informing security teams, whereas threat intelligence services providers are used in a larger percentage (68%) for teams self-declaring as having superior or above-average practices.

Q: How are security events brought to the attention of the IT/security team?

Endpoint monitoring software alerts

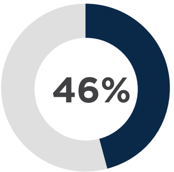
60%

User reports

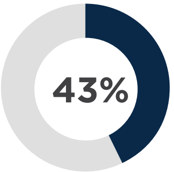
60%

Perimeter defenses (IPS/IDS/Firewall) alerts

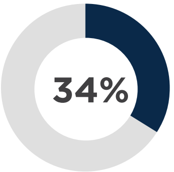
57%



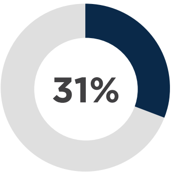
Error messages or application alerts



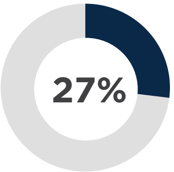
Alerts from other analytics platforms (besides SIEM)



Automated alert from our SIEM



Third party reporting on behavior coming from our network



Searching manually through our SIEM

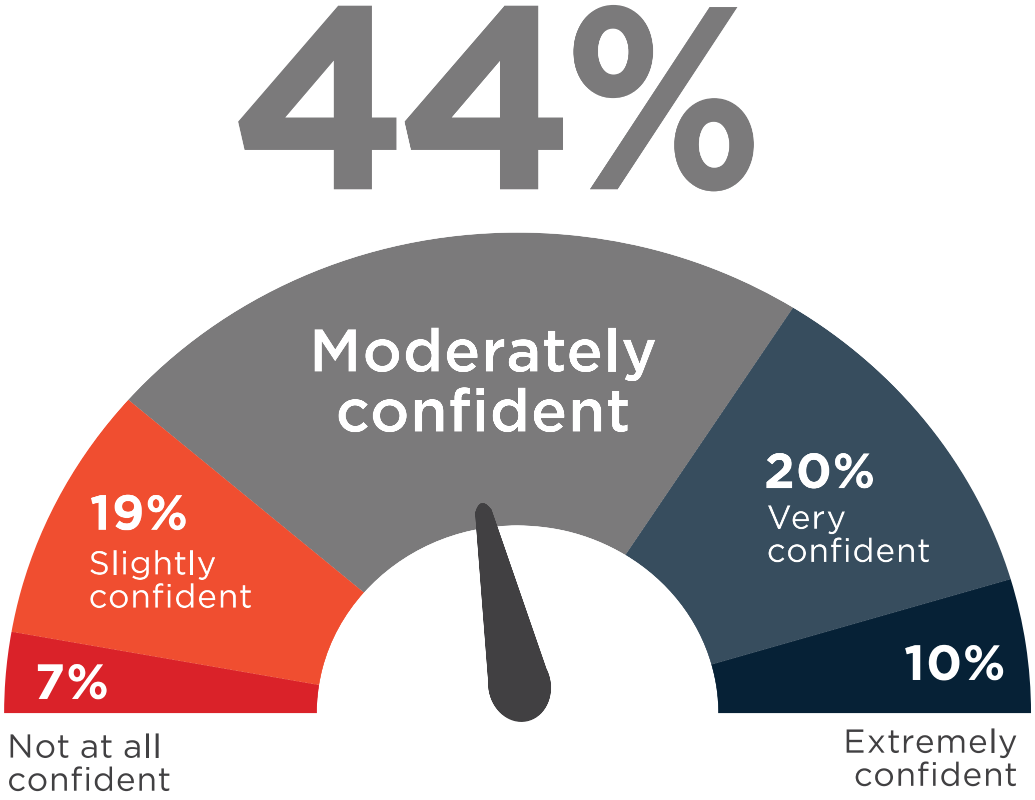
Detected through third-party vendor partner 26% | Retrospective review of logs or SIEM-related data (largely manual) 24% | Conducting searches with our security analytics platform (not SIEM) 21% | Intelligence services provider alerts 19% | UEBA 10%

INSIDER THREAT

INSIDER THREAT CONFIDENCE

Only 30% of organizations feel very to extremely confident about their insider threat security posture. This leaves a majority of organizations in a situation that requires improved insider threat policies, training and platforms to boost insider threat confidence.

Q: How confident are you in your organization's insider threat security posture?



NATURE OF INSIDER THREATS

As with our prior studies, we investigated the types of insider threats that our survey participants were concerned about. Several types of insider threats - inadvertent data breaches (64%), malicious data breaches (60%) and compromised credentials (60%) had a similar level of prominence.

Q: What type of insider threats are you most concerned about?

64%

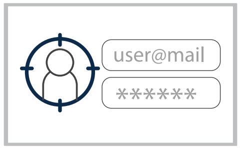
Inadvertent data breach or compromise

(e.g., careless user causing accidental breach)

60%

Malicious data breach or compromise

(e.g., user willfully causing harm)



60%

Compromised credentials

(e.g., outside infiltrators compromising an insider and using them or their credentials to cause harm)

57%

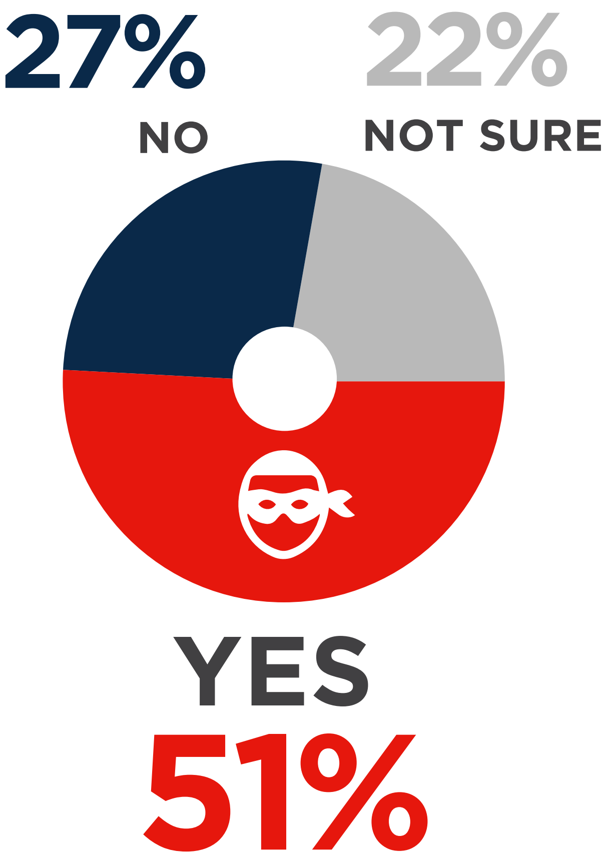
Negligent data breach or compromise

(e.g., user willfully ignoring policy, but not malicious)

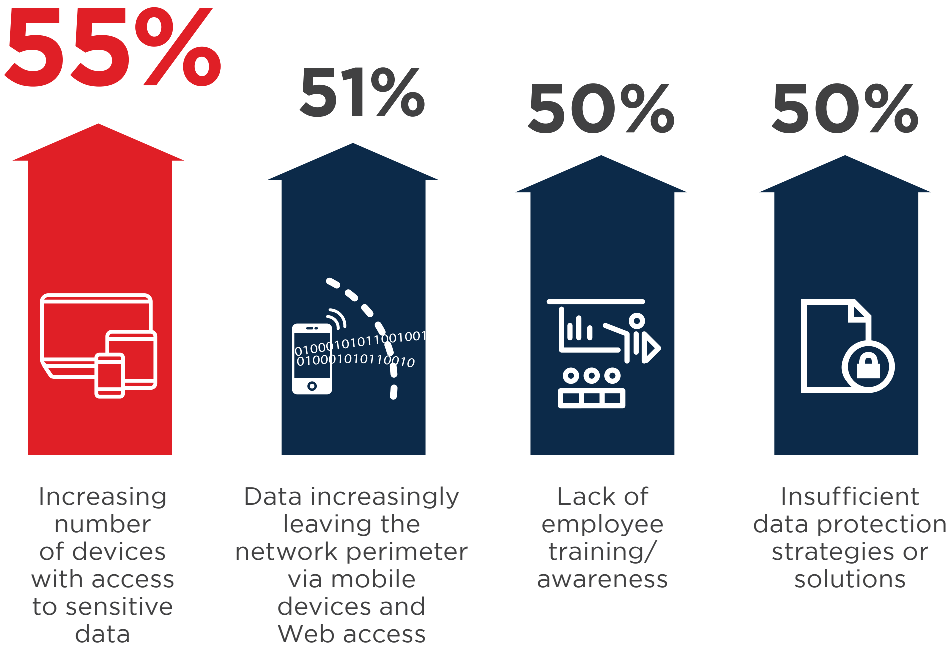
GROWTH OF INSIDER THREATS

We asked survey participants about the growth of insider threats. The majority of respondents indicated that such threats were on the rise (a majority of 51% agreeing with this). When asked about the reasons for this increase, the main reasons were related to a growth in the number of devices with access to sensitive data (55%), data leaving the traditional network perimeter on mobile devices (51%) and lack of employee training (50%).

Q: Do you think insider attacks have generally become more frequent over the last 12 months?



Q: What do you believe are the main reasons why insider attacks are on the rise?

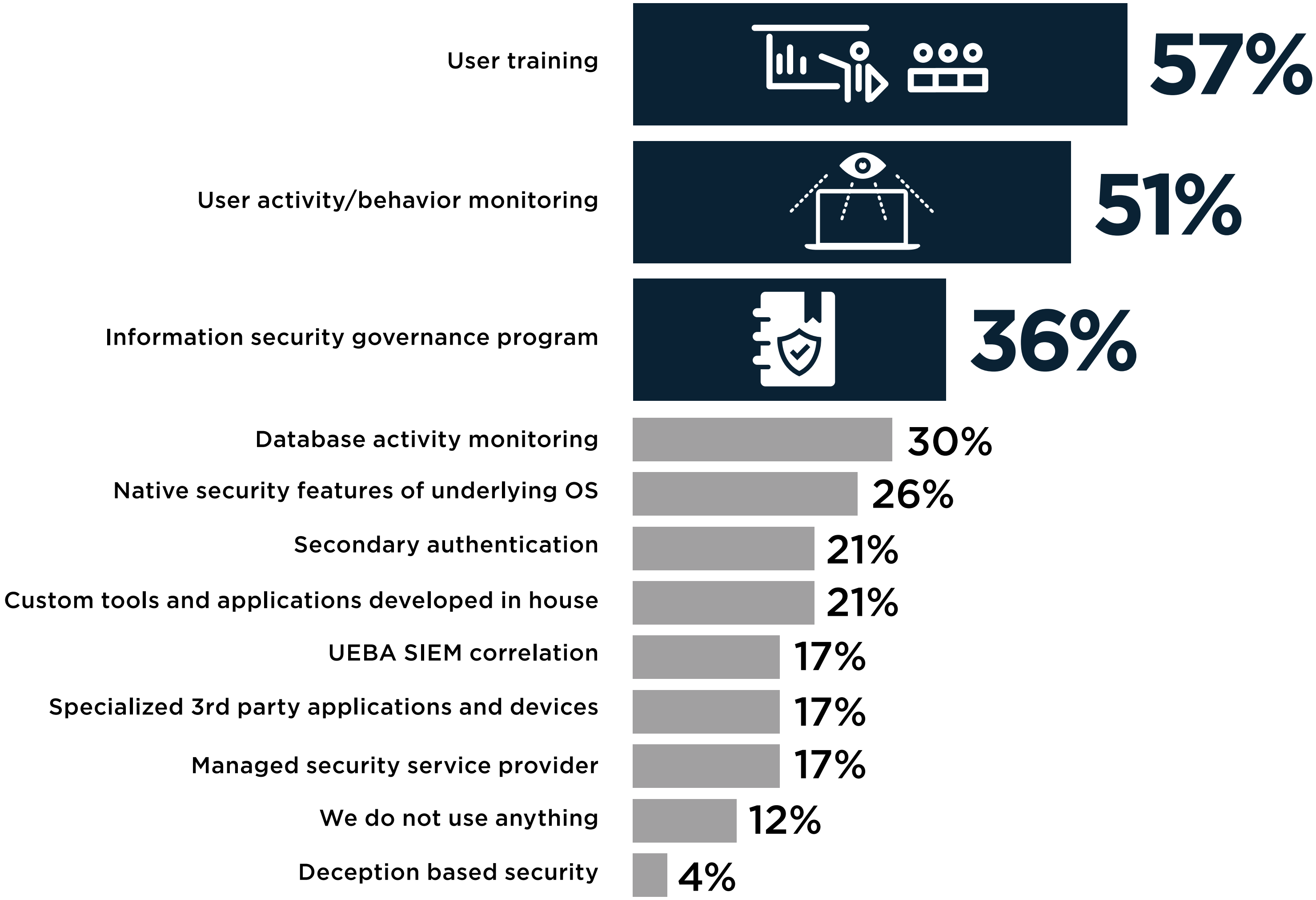


Technology is becoming more complex 43% | More employees, contractors, partners accessing the network 42% | Increasing use of cloud apps and infrastructure 31% | Increasing amount of sensitive data 27% | Increased public knowledge or visibility of insider threats that were previously undisclosed 24% | I don't think insider attacks are on the rise 8% | Not sure/other 8%

COMBATING INSIDER THREATS

When asked about the main practices and tools used by security teams to combat insider threats, user training was identified as the main tactic (57%) closely followed by user activity/behavior monitoring (51%). This is consistent with the assessment that careless insiders are one of the main causes of data loss.

Q: How does your organization combat insider threats today?



RISKY USERS

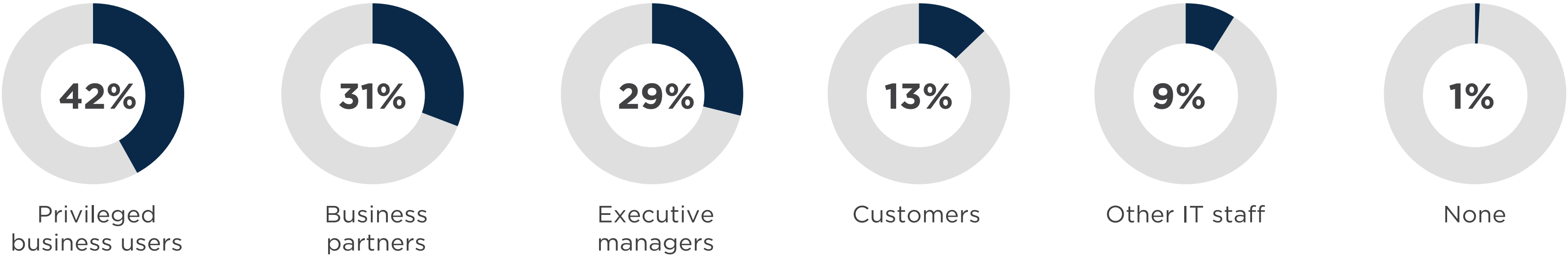
In this year’s survey, regular employees take the number one spot of users posing the biggest insider threat (50%). This is followed by privileged IT users, such as administrators with access to sensitive information (47%) and contractors, service providers and temporary users (also 47%).

Q: What user groups pose the largest security risk to your organization?

50%
Regular employees

47%
Privileged IT users/admins

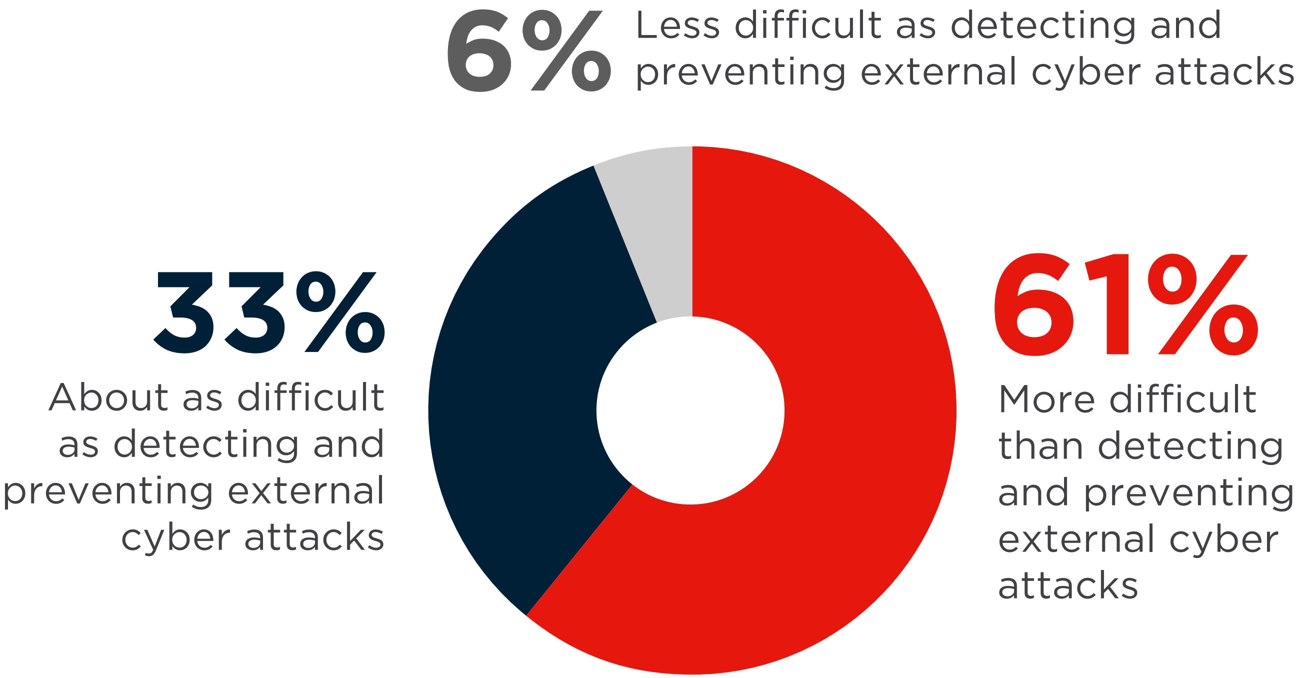
47%
Contractors, service providers, temporary workers



INTERNAL VS EXTERNAL ATTACKS

Similar to our previous surveys, the majority of respondents (61%) find it more difficult to detect and prevent an insider attack versus an external cyber attack.

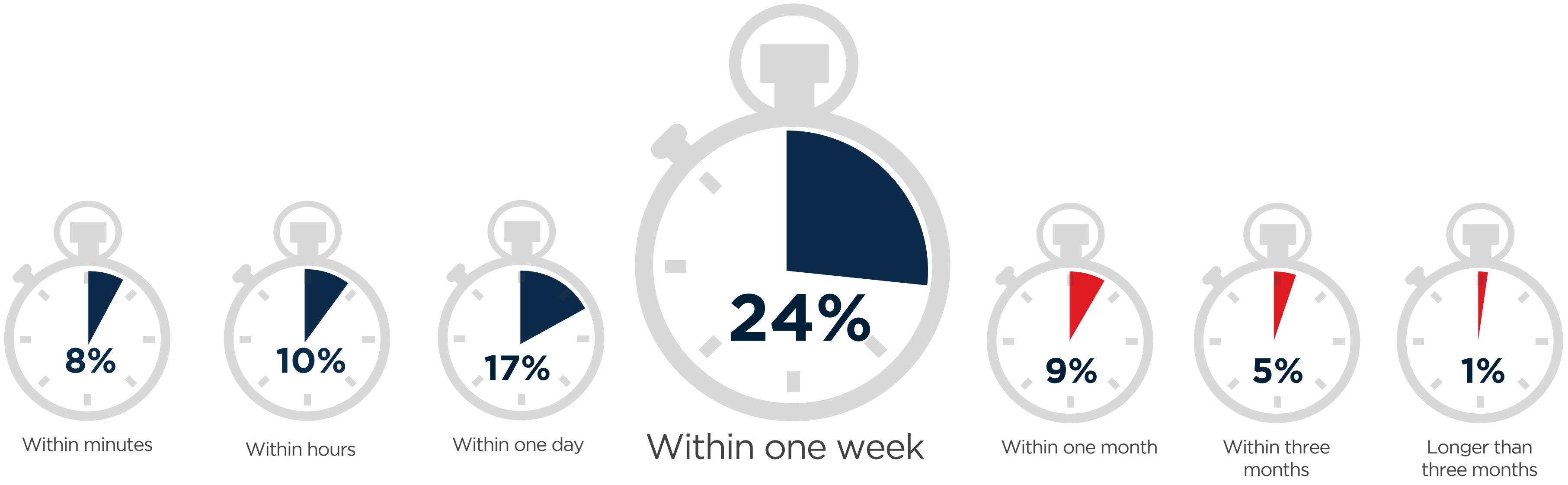
Q: How difficult is it to detect and prevent insider attacks compared to external cyber attacks?


6% Less difficult as detecting and preventing external cyber attacks
33% About as difficult as detecting and preventing external cyber attacks
61% More difficult than detecting and preventing external cyber attacks

SPEED OF RECOVERY

Expected recovery from insider attacks is taking longer than in previous years. Most frequently, 24% of organizations feel they could recover from an attack within one week. However, the share of organizations that can recover within a day or less has declined to 35% from 45% in previous surveys.

Q: How long would it take your organization to recover from an insider attack, on average?



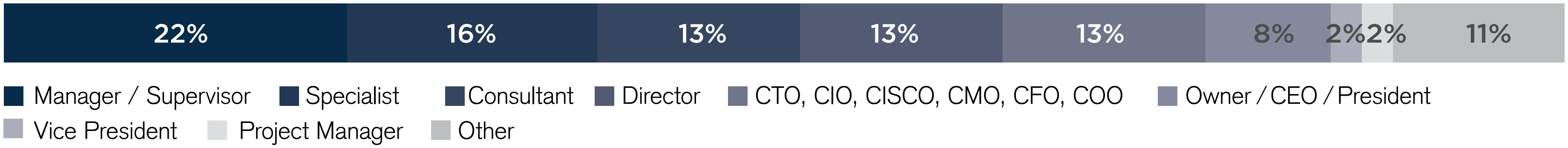
No ability to recover 2% | Not sure / Can't disclose 24%

METHODOLOGY & DEMOGRAPHICS

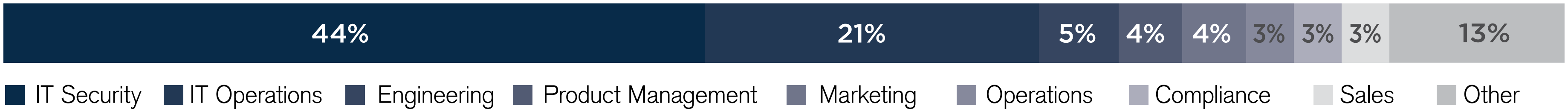
METHODOLOGY & DEMOGRAPHICS

The 2017 Threat Monitoring, Detection and Response Report is based on the results of a comprehensive online survey of over 400 cybersecurity professionals to gain more insight into the latest security threats faced by organizations and the solutions to detect, remediate, and prevent them. The respondents range from technical executives to managers and IT security practitioners. They represent organizations of varying sizes across many industries. Their answers provide a comprehensive perspective on the state of threat monitoring, detection and response today.

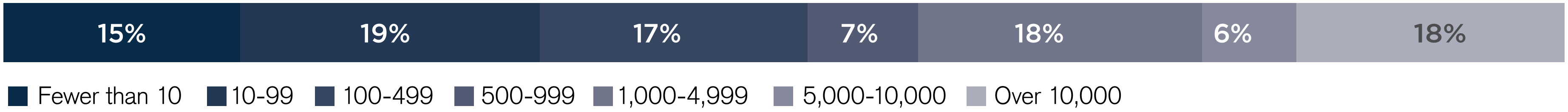
CAREER LEVEL



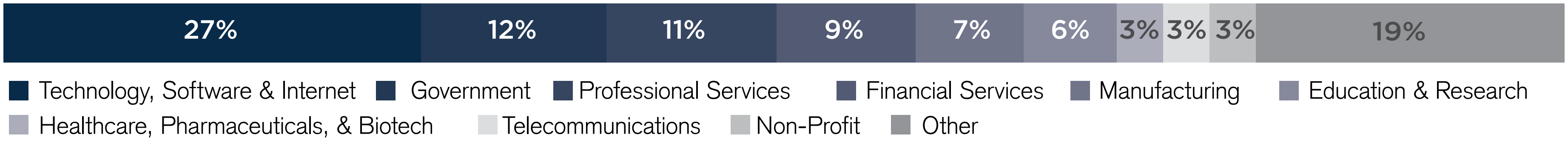
DEPARTMENT



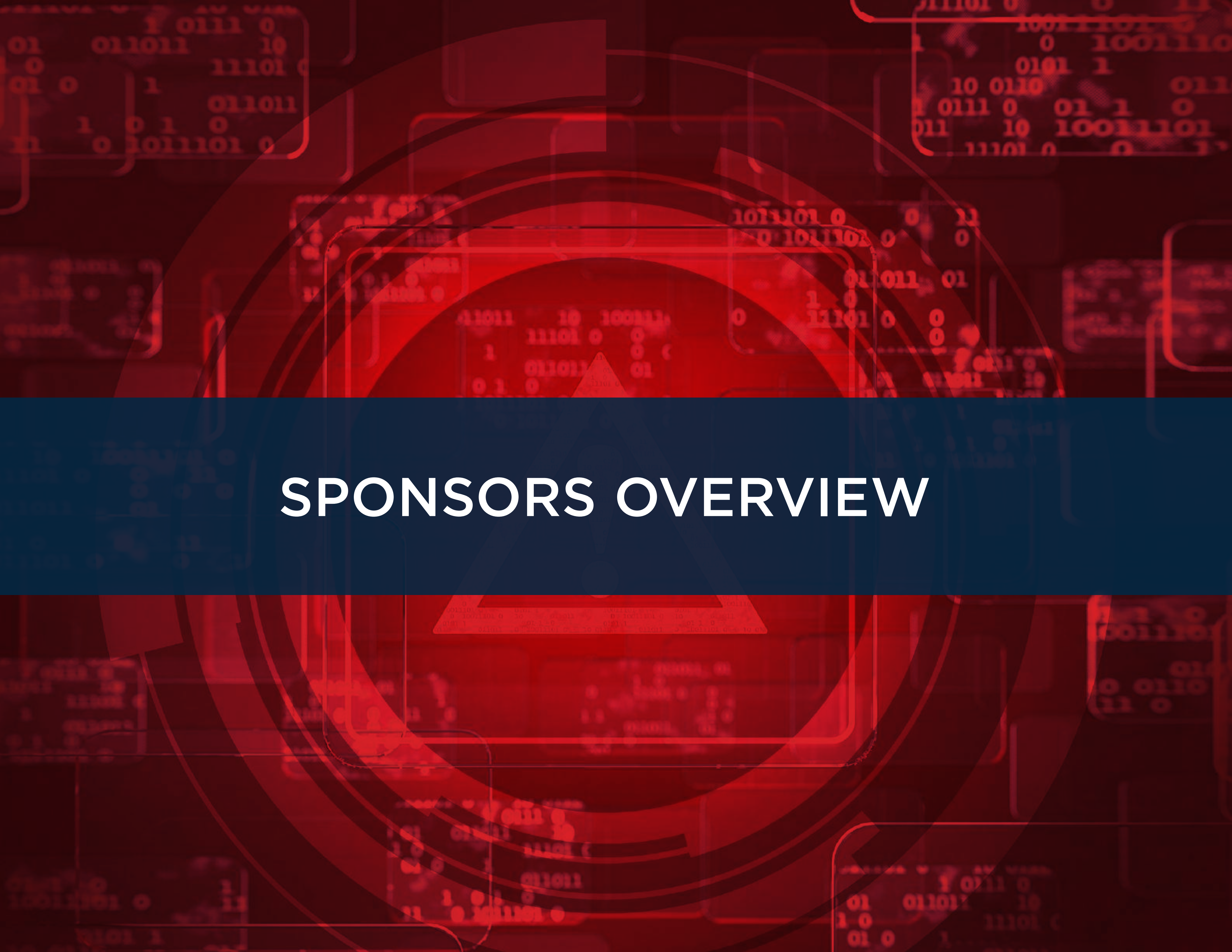
COMPANY SIZE



INDUSTRY



SPONSORS OVERVIEW



SPONSORS OVERVIEW

AlienVault® | www.alienvault.com

AlienVault® has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach combines our all-in-one platform, AlienVault Unified Security Management™, with the power of AlienVault's Open Threat Exchange®, making effective and affordable threat detection attainable for resource-constrained IT teams.

Bitglass | www.bitglass.com

Bitglass' Cloud Access Security Broker (CASB) solution provides enterprises with end-to-end data protection from the cloud to the device. It deploys in minutes and works across apps like Office 365, Salesforce, and AWS. Bitglass also protects data on mobile devices without the hassles of MDM.

BluVector | www.bluvector.io

BluVector helps security teams respond to malicious threats up to 80% faster than current approaches. As a leader in Network Security Monitoring & Analytics, BluVector applies supervised machine learning and automation so security teams can detect and respond to advanced security threats at digital speed.

ControlScan | www.controlscan.com

ControlScan managed security and compliance solutions help secure networks, protect payment card data and streamline the path to authentic PCI compliance. We deliver on our "We've Got Your Back" promise by combining deep-seated expertise with superior technologies for log monitoring and management, advanced endpoint security, unified threat management, file integrity monitoring and more.

SPONSORS OVERVIEW

Delta Risk | deltarisk.com

Delta Risk LLC provides cyber security and risk management services to government and commercial clients worldwide. Founded in 2007, Delta Risk offers managed security services, advisory and training, and incident response services to improve cyber security operational capability and protect business operations. Delta Risk is a Chertoff Group company.

DomainTools | www.domaintools.com

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network and connect them with nearly every active domain on the Internet. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work.

Dtex | www.dtexsystems.com

Dtex provides unique endpoint data and analytics to detect data breaches, insider threats, and outsider infiltration. It pinpoints threats by combining patterns of known bad behavior with advanced user behavior intelligence. Dtex provides visibility into everything users do on their work devices – on and off the corporate network – without compromising privacy.

EventTracker | www.eventtracker.com

EventTracker enables infosec teams to be more productive and effective by cutting through the big data noise of security monitoring and delivering actionable security intelligence. EventTracker combines an award-winning unified security management platform, threat intelligence, and a 24/7 SOC to catch more threats and accelerate appropriate responses and automate remediation.

SPONSORS OVERVIEW

Exabeam | www.exabeam.com

Exabeam is the leading provider of security intelligence solutions, trusted by the most demanding companies in the world to protect sensitive information against theft and breach. The Exabeam Security Intelligence Platform uniquely combines unlimited data collection, advanced analytics, and automated incident response into a modern platform for security management.

ObserveIT | www.observeit.com

ObserveIT helps 1,500+ customers identify and eliminate insider threat by combining the most comprehensive view of user activity on all endpoints, applications, and files with preconfigured insider threat indicators. The solution drastically decreases the risk of an insider threat incident, ensures organizations remain compliant, decreases time spent on investigating incidents, and prevents data loss.

SoftActivity | www.softactivity.com

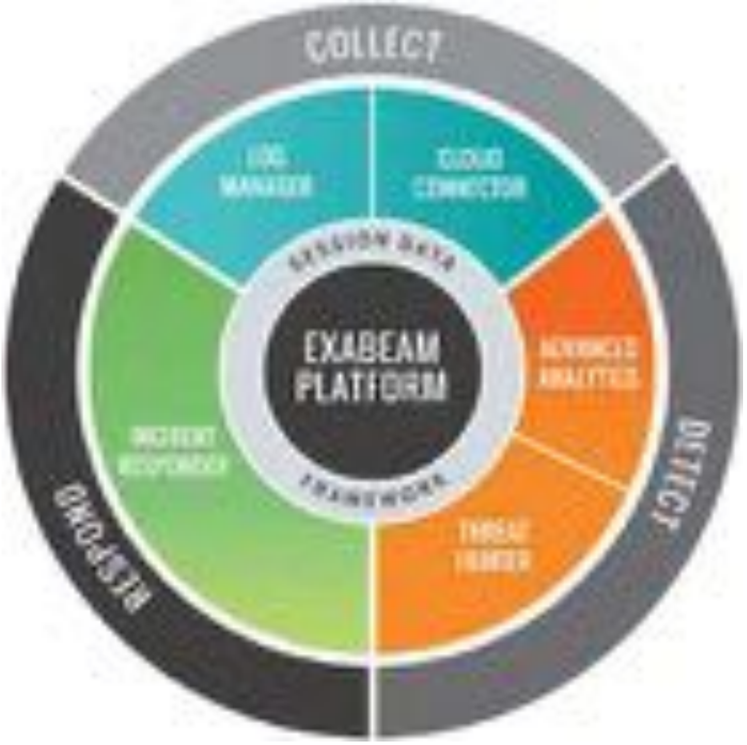
SoftActivity provides user monitoring software to thousands of organizations since 2003. View user activity and screens of remote computers in real time with our Activity Monitor. Record user sessions on terminal servers. Supervisors can view reports in the on-premise web console: used programs, websites, screen copies, attendance, files and communications history.

Tenable | www.tenable.com

Tenable transforms security technology through comprehensive solutions providing continuous visibility and critical context, enabling decisive actions to protect organizations of all sizes. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss.

exabeam

Today's Threats Keep Changing. Can Your SIEM Keep Up?



Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information.

The **Exabeam Security Intelligence Platform** uniquely combines unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products.

The result is the first modern security intelligence solution that delivers where legacy security information and event management (SIEM) vendors have failed.

LEARN MORE

Gartner 2015 CoolVendor

CYBERSECURITY CDM LEADER 2016

SC 2017 awards

INFORMATION MANAGEMENT 2017 AWARDS

CONTACT US

Interested in seeing your brand featured in the next report?

- Fact-based content
- Sales ready leads
- Brand awareness

Contact Crowd Research Partners for more information.

✉ info@crowdresearchpartners.com

Visit Crowd Research Partners for more details

Produced by:

Crowd Research Partners

LinkedIn Group Partner
Information Security