Big Data Cybersecurity Analytics Research Report

Sponsored by Cloudera

Independently conducted by Ponemon Institute LLC

Publication Date: August 2016

Big Data Cybersecurity Analytics Research Report

Ponemon Institute: August 2016

Part 1. Introduction

Ponemon Institute is pleased to present the findings of *Big Data Cybersecurity Analytics,* sponsored by Cloudera. The purpose of this study is to understand the current state of cybersecurity big data analytics and how Apache Hadoop[1] based cybersecurity applications intersect with cybersecurity big data analytics.

In this study, we surveyed 592 IT and IT security practitioners in the United States and 10 cybersecurity technology executives at 10 unique organizations that have built applications on Apache Hadoop. To ensure a knowledgeable respondent, we confirmed that all participants are in organizations using some form of big data analytics and they are knowledgeable about the technology. Some of these participants are users of the Apache Hadoop platform.

Following are key findings from the research.

- Organizations are 2.25X more likely to identify a security incident within hours or minutes when they are a heavy user of big data cybersecurity analytics.

- Sixty-five percent of respondents say the use of big data analytics is very important to ensuring a strong cybersecurity posture.

- Eighty-one percent of respondents say demand for big data for cybersecurity analytics has significantly increased over the past 12 months.

- Apache Hadoop significantly extends big data cybersecurity analytic applications capabilities:

  - ✓ 29 percent of these applications use Hadoop to increase data volumes by more than 100 percent
  - ✓ 72 percent of them use Hadoop to increase data processing by more than 76 percent
  - ✓ 43 percent of them use Hadoop to increase data access for analytics by more than 100 percent

- Heavy users of big data analytics have a higher level of confidence in their ability to detect cyber incidents than light users. With respect to 11 common cyber threats, the biggest gaps between heavy and light users concern the organization's ability to detect advanced malware/ransomware, compromised devices (e.g., credential theft), zero day attacks and malicious insiders. The smallest gaps in detection between heavy and light users concern denial of services, web-based attacks and spear phishing/social engineering.

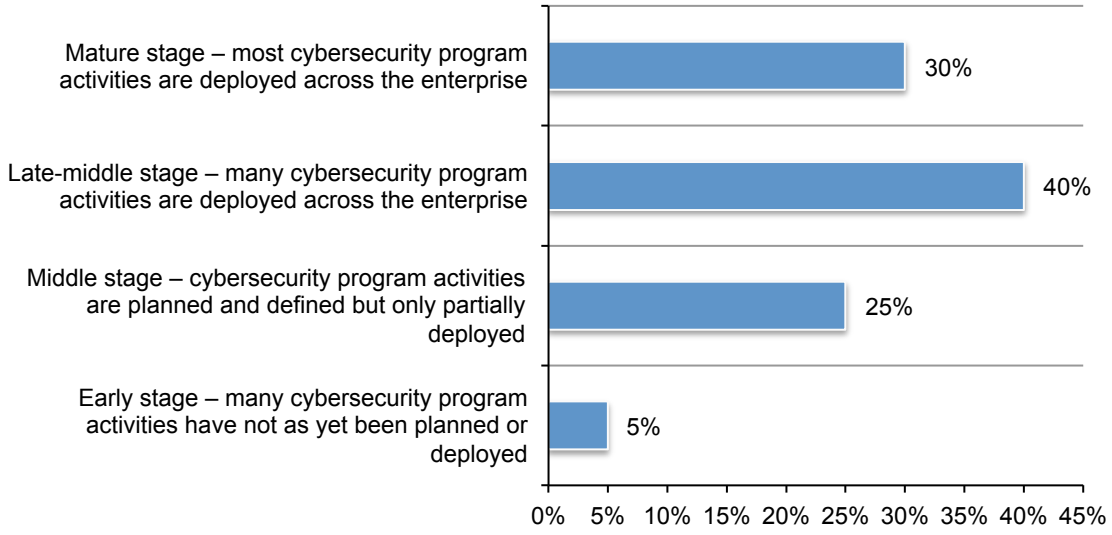
- Companies represented in this research are allocating an average of $14.50 million to IT security in fiscal year 2016 and an average of $2.32 million (16 percent) of this budget is allocated to analytics tools.

[1] Hadoop is an ecosystem of open source components that fundamentally changes the way enterprises store, process and analyze data. Unlike traditional systems, Hadoop enables multiple types of analytic workloads to run on the same data, at the same time, at massive scale on industry-standard hardware. CDH, Cloudera's open source platform, is the most popular distribution of Hadoop and related projects in the world (with support available via a Cloudera Enterprise subscription).

Part 2. Current state

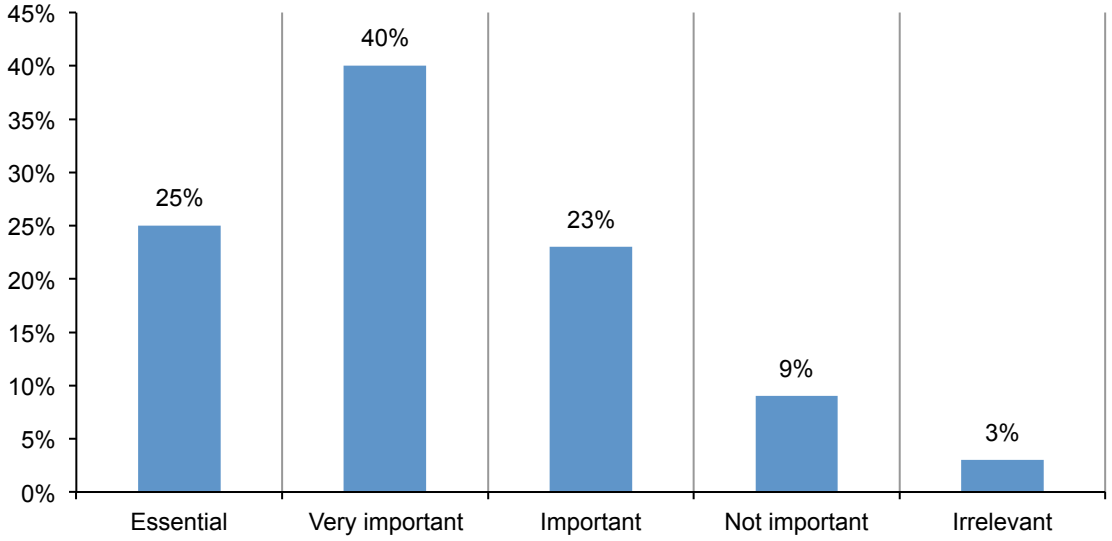
Most companies in this study have fairly mature cybersecurity programs. According to Figure 1, 70 percent of respondents say their organizations have many cyber security program activities deployed (late-middle stage) or most cybersecurity program activities are deployed (mature stage).

Figure 1. What best describes the maturity level of your cybersecurity program?



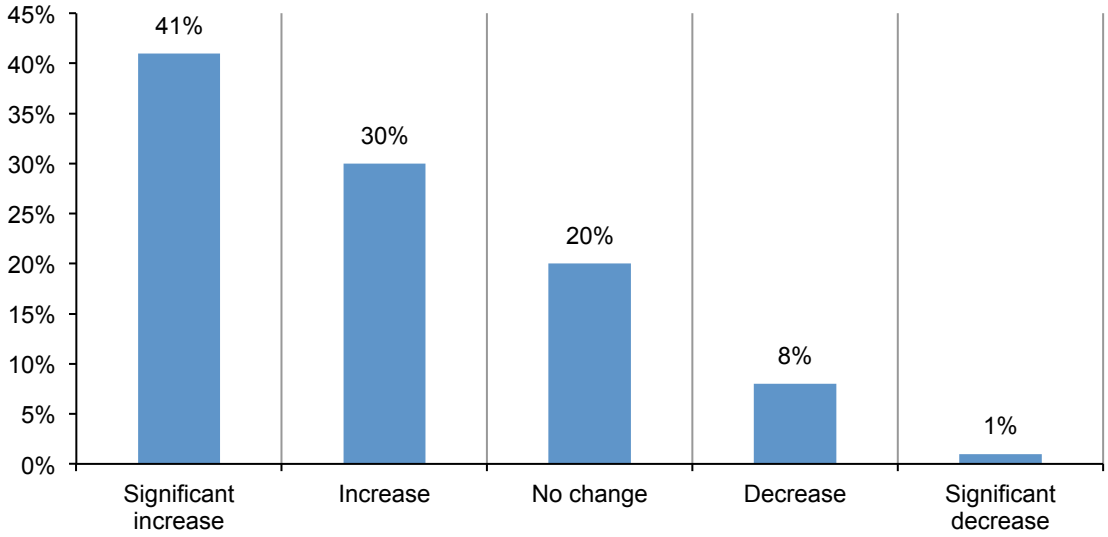
Big data analytics is key to a strong cybersecurity posture. Sixty-five percent of respondents say the use of big data analytics is essential (25 percent) or very important (40 percent) to ensuring a strong cybersecurity posture.

Figure 2. How important is the use of big data analytics for ensuring a strong cybersecurity posture?



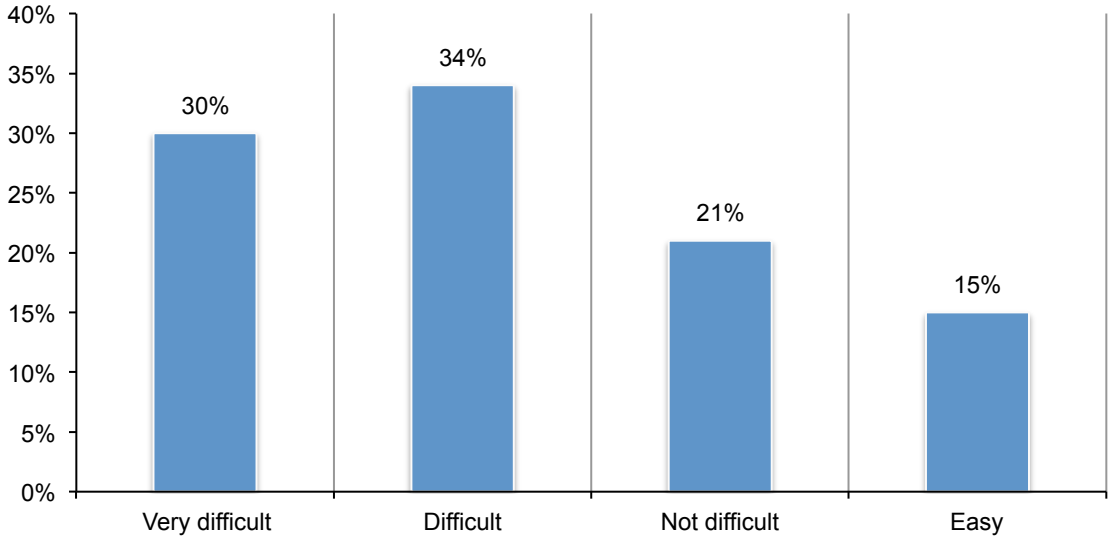
The more big data analytics is used, the greater the demand. According to Figure 3, 61 percent of light user respondents say user demand has increased significantly (38 percent) or increase (28 percent). In contrast, 75 percent of respondents of the heavy user group believe demand has increased significantly (43 percent) or increased (32 percent).

Figure 3. How has user demand for big data analytics for cybersecurity changed over the past 12 months?



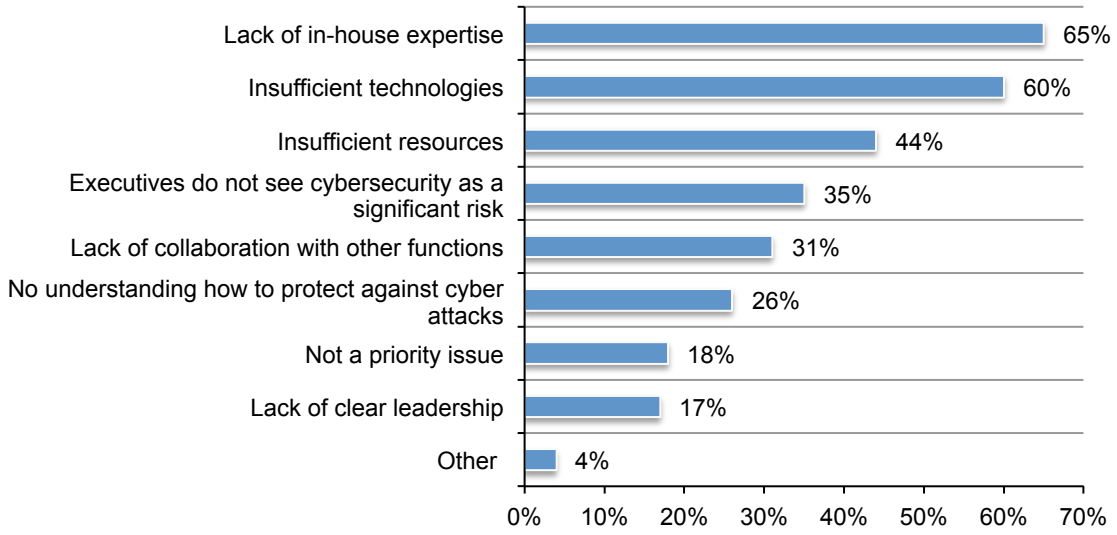
The typical deployment of cybersecurity analytics is a challenge for companies. As shown in Figure 4, deployment is considered very difficult (30 percent of respondents) and difficult (34 percent of respondents).

Figure 4. How difficult is the difficult deployment of cybersecurity analytics within your organization?



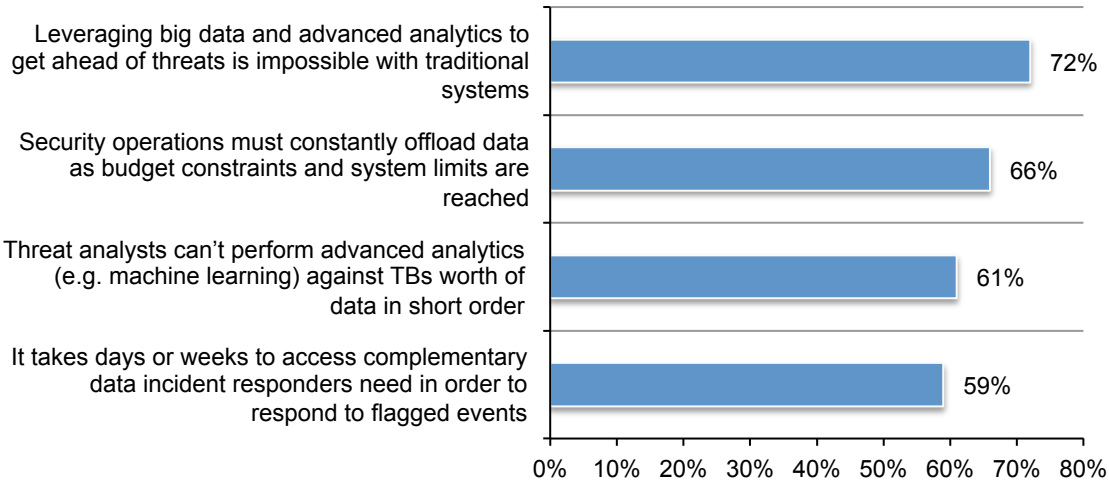
Expertise and technologies are needed for the successful adoption of big data analytics. Figure 5 presents the challenges companies face in the use of big data analytics. These are: lack of in-house expertise (65 percent of respondents), insufficient technologies (60 percent of respondents) and insufficient resources (44 percent of respondents).

Figure 5. What challenges prevent the effective use of big data analytics for cybersecurity?
Three choices permitted



Traditional systems are not helpful to a strong cybersecurity posture. According to Figure 6, 72 percent of respondents say leveraging big data and advanced analytics to get ahead of threats is impossible with traditional systems. Other issues with traditional systems include the need for security operations to constantly offload data as budget constraints and system limits are reached (66 percent of respondents), threat analysts can't perform advanced analytics against TBs worth of data in short order (61 percent of respondents) and it takes days or weeks to access complementary data incident responders need in order to respond to flagged events (59 percent of respondents).

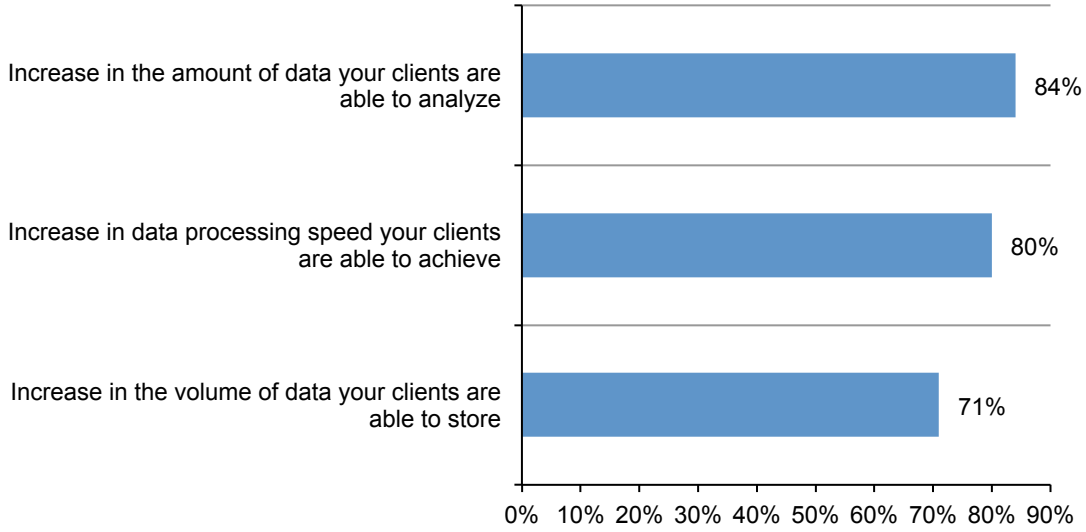
Figure 6. Problems with traditional systems
Strongly agree and Agree responses combined



Part 3. The world of big data cybersecurity analytics

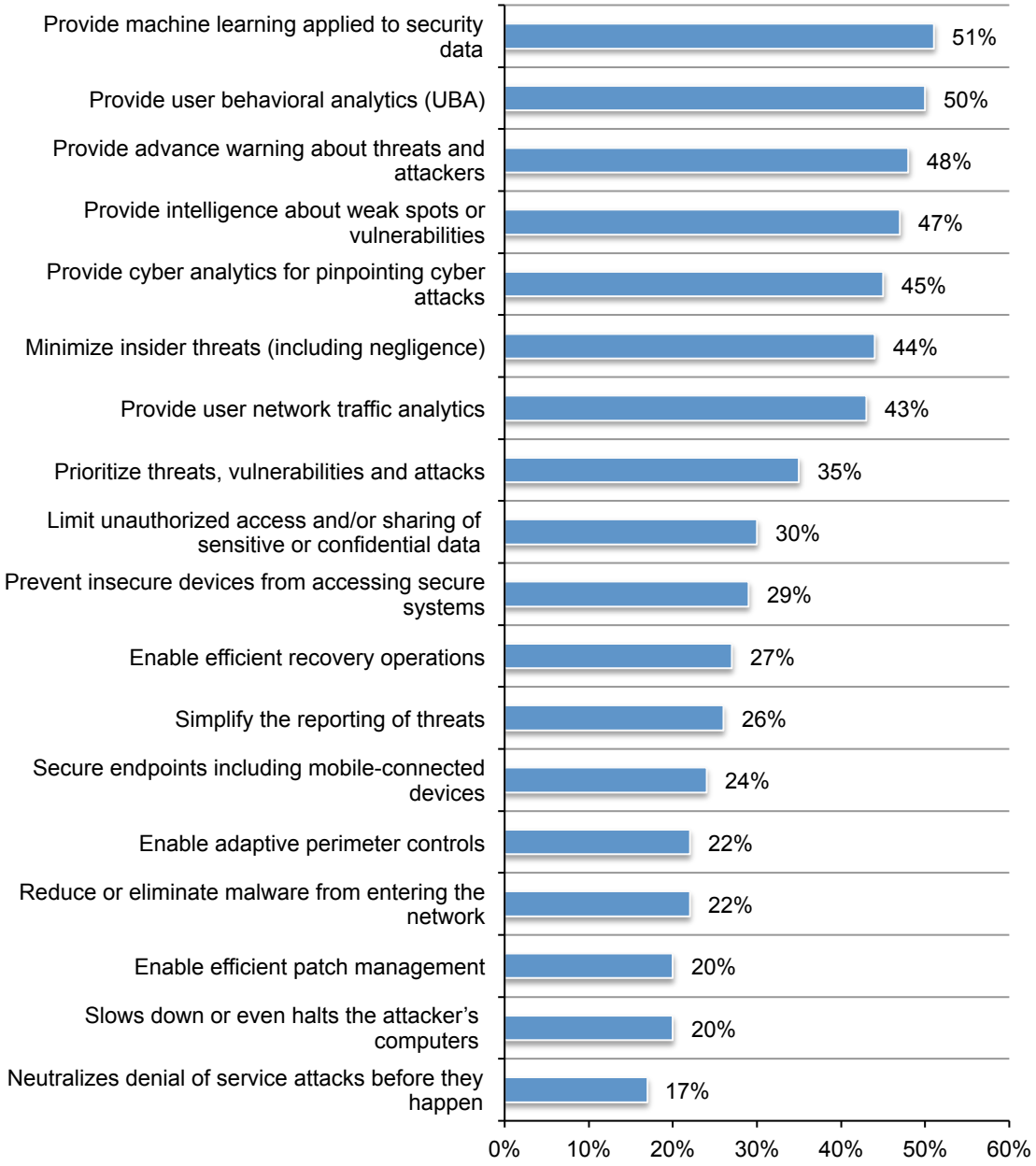
In addition to our study of users, we interviewed Cloudera's partners to learn their perceptions about building on Cloudera and Apache Hadoop. As noted in Figure 6, they saw an average increase of 71% in the volume of data their clients are able to store, an average of 80% increase in data processing speeds and an average of 84 percent increase in the amount of data clients are able to analyze.

Figure 6. Benefits of Apache Hadoop based applications
Extrapolated values on a percentage scale from 0% to more than 100%



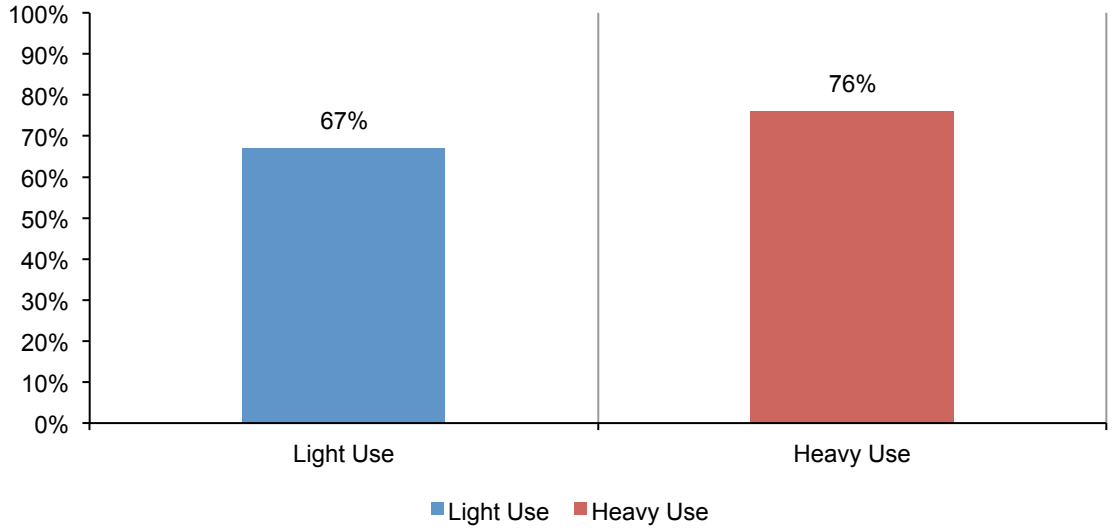
Machine learning applied to security data and UBA are the most promising features. Figure 7 presents what respondents believe are the top technology features for a strong cybersecurity posture are: machine learning applied to security data (51 percent of respondents), user behavior analytics (50 percent of respondents), advance warning about threats and attackers (48 percent of respondents), intelligence about weak spots or vulnerabilities (47 percent of respondents) and cyber analytics for pinpointing cyber attacks (45 percent of respondents).

Figure 7. What are the most promising enabling technology features?
Top six choices permitted



Big data analytics strengthens cybersecurity posture. Seventy-two percent of respondents say the use of big data analytics to detect advanced cyber threats is very important. In fact, 71 Heavy users are more likely to believe in the importance of big data analytics. As shown in Figure 8, 76 percent of high users believe big data analytics is very important as opposed to 67 percent of light user respondents.

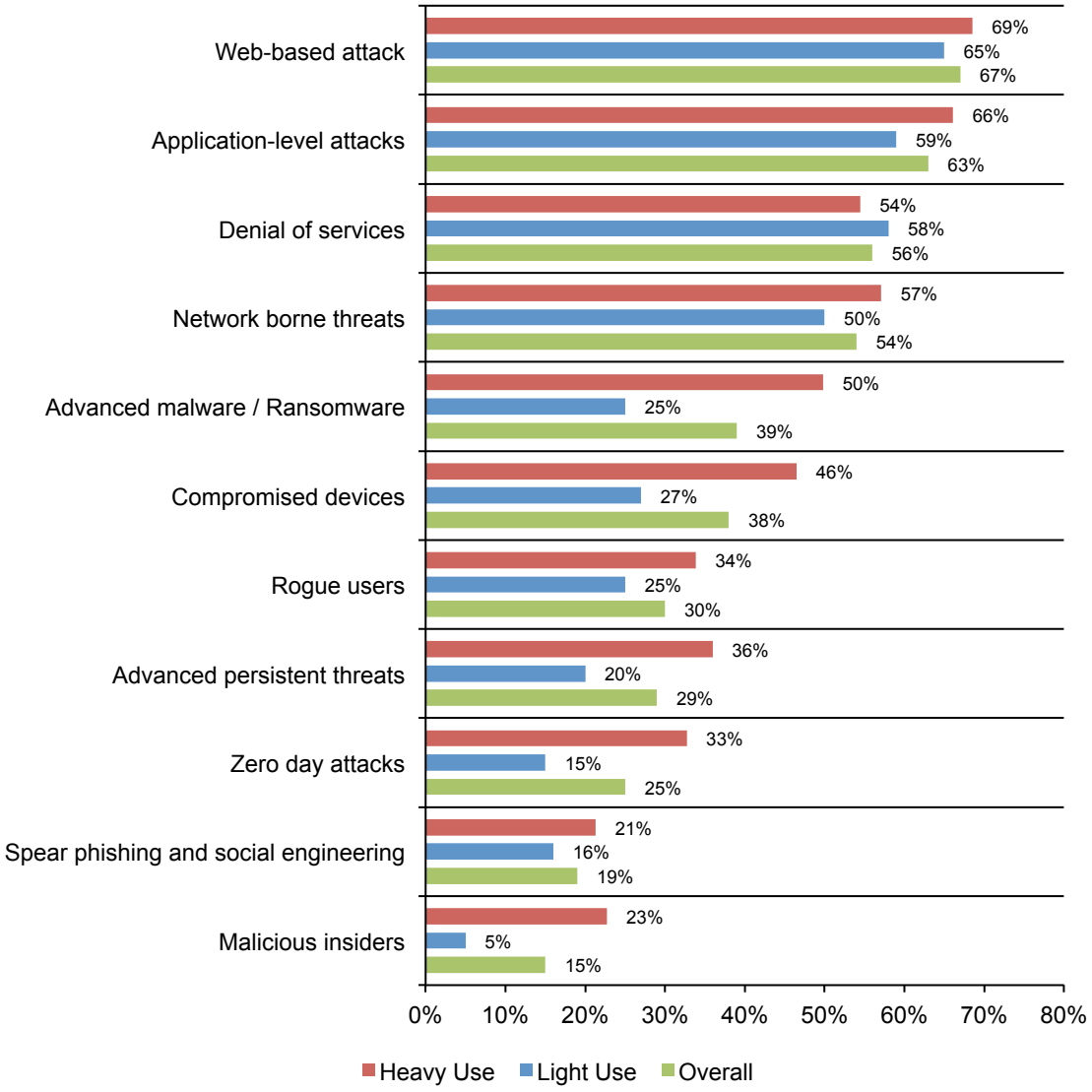
Figure 8. How important is the use of big data analytics to detect advanced cyber threats?
7+ percentage response on a 10-point scale



Companies are best at detecting web-based attacks. According to Figure 9, organizations represented in this study have the most confidence in detecting the following cyber incidents: web-based attacks (67 percent of respondents), application-level attacks such as SQL injection, cross site scripting or remote file inclusion (63 percent of respondents), denial of services (56 percent of respondents) and network borne threats (54 percent of respondents).

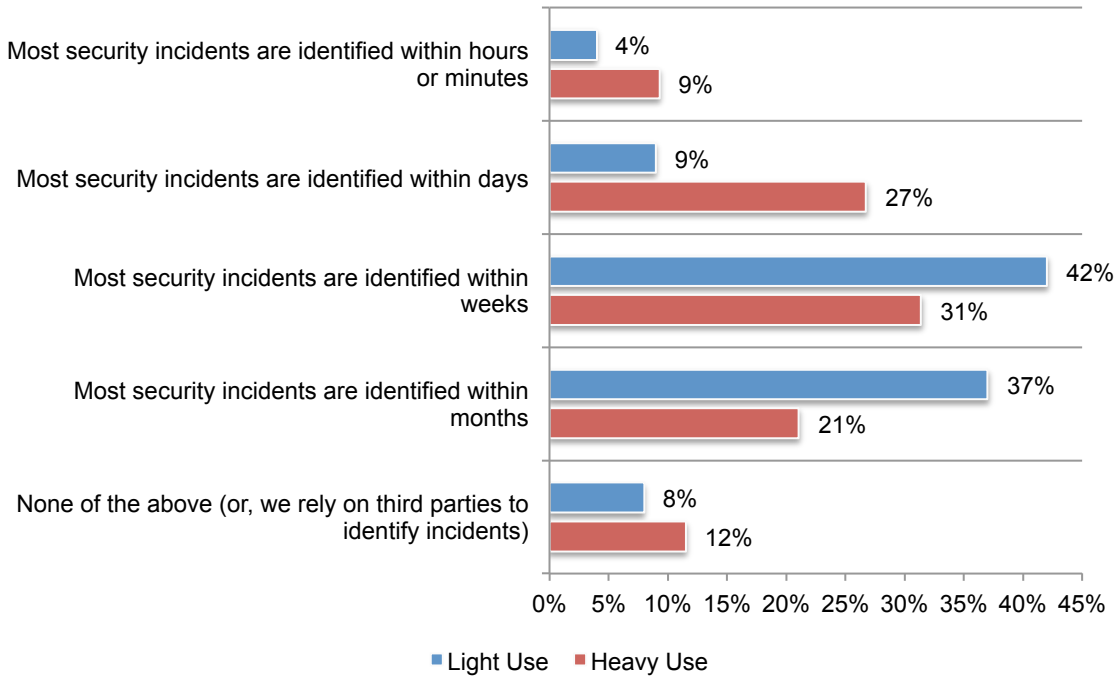
Heavy users are best at detecting cyber threats. As also shown in Figure 9, heavy users of big data analytics appear to have a much higher level of confidence in their ability to detect cyber incidents than light users. With respect to 11 common cyber threats, the biggest gaps between heavy and light users concern the organization's ability to detect advanced malware/ransomware (Diff=25 percent), compromised devices (Diff=19 percent), zero day attacks (Diff=18 percent) and malicious insiders (Diff=18 percent). The smallest gaps in detection between heavy and light users concern denial of services (Diff=-4 percent), web-based attacks (Diff=4 percent) and spear phishing/social engineering (Diff=5 percent).

Figure 9. Which cyber incidents are you best at detecting?
More than one choice permitted



As shown in Figure 9, 9 percent of heavy users of big data analytics can detect threats within hours or minutes, compared to 4 percent of light users.

Figure 10. How quickly can your organization identify a security incident?



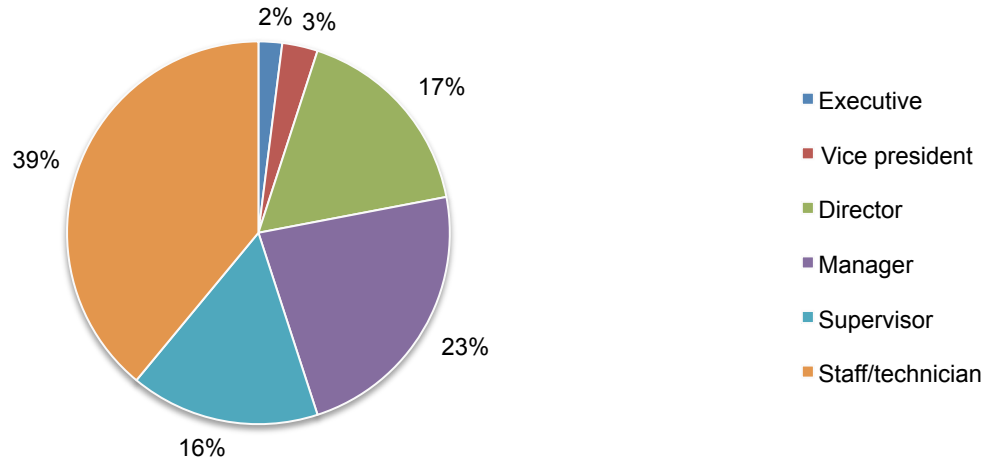
Part 3. Methods

A sampling frame of 18,280 IT and IT security practitioners in the United States were selected as participants in the research. Table 1 shows 656 total returns. Screening and reliability checks required the removal of 64 surveys. Our final sample consisted of 592 surveys or a 3.2 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	18,280	100.0%
Total returns	656	3.6%
Rejected surveys	64	0.4%
Final sample	592	3.2%

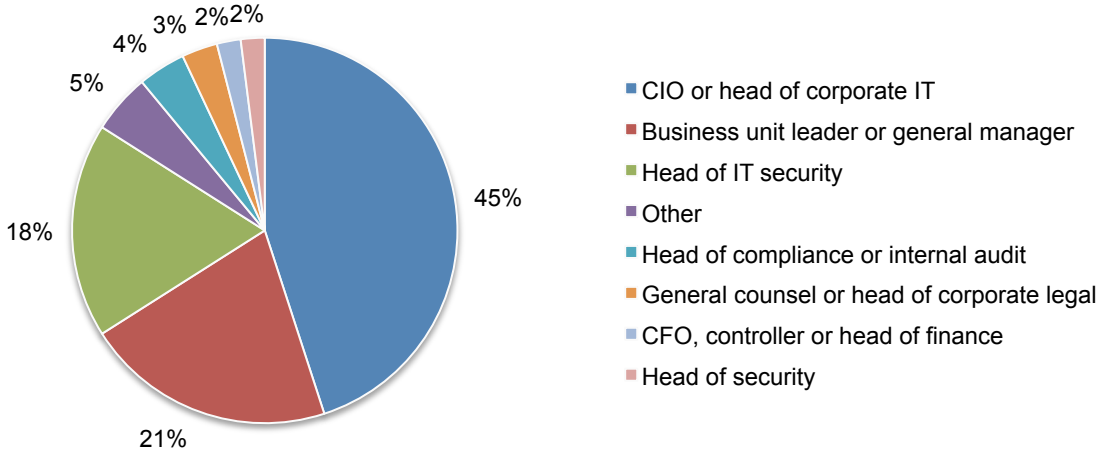
Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, 61 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



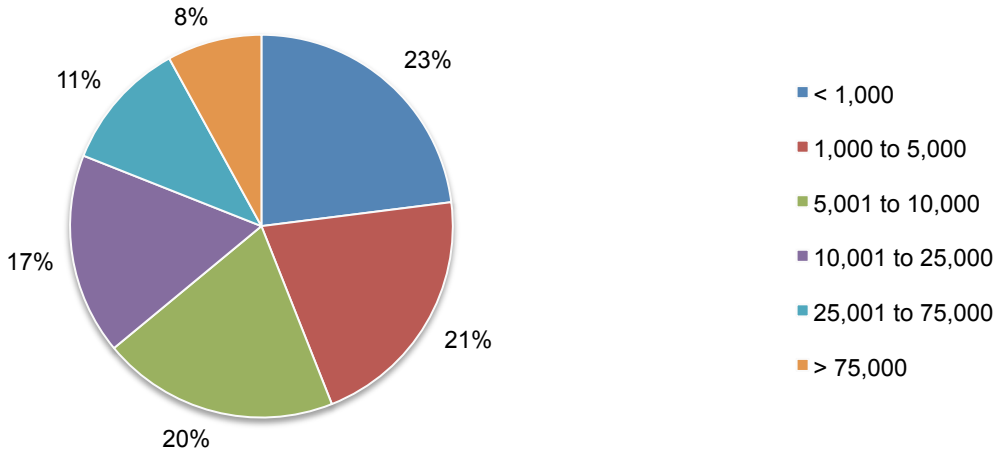
As shown in Pie Chart 2, 45 percent of respondents report directly to the CIO or head of corporate IT, 21 percent of respondents report to the business unit leader or general manager and 18 percent of respondents report to the head of IT security.

Pie Chart 2. Direct reporting channel



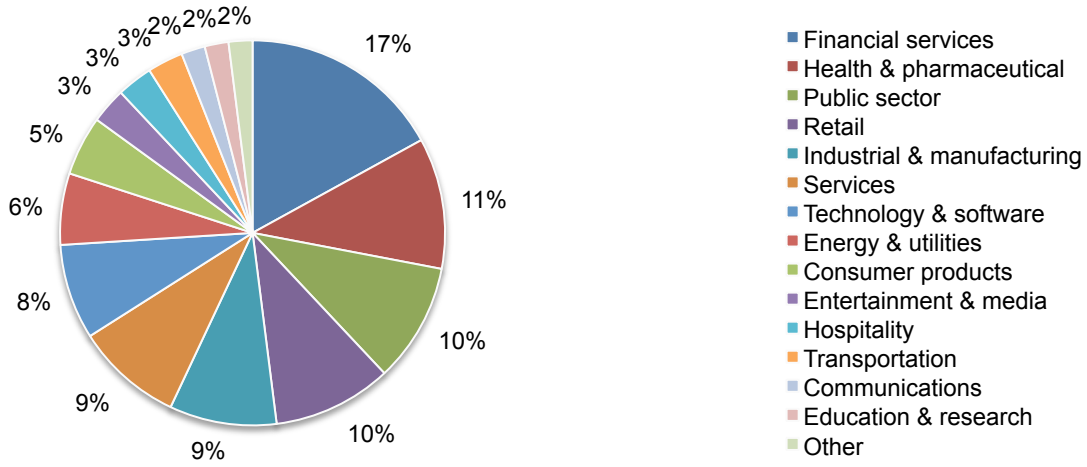
As shown in Pie Chart 3, 56 percent of respondents are from organizations with a global headcount of more than 5,000 employees

Pie Chart 3. Global employee headcount



Pie Chart 4 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by health and pharmaceutical (11 percent of respondents) and public sector (10 percent of respondents).

Pie Chart 4. Primary industry classification



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from lJune through July 2016.

Survey response	Freq	Pct%
Sampling frame	18,280	100.0%
Total returns	656	3.6%
Rejected surveys	64	0.4%
Final sample	592	3.2%

Part 1. Screening questions

S1. What best describes your organization's use of big data analytics for cybersecurity purposes	Pct%
None (stop)	0%
Light	20%
Moderate	24%
Heavy	27%
Very heavy	29%
Total	100%

S2. What best describes your level of involvement in using big data analytics for cybersecurity purposes?	Pct%
None (stop)	0%
Low	21%
Moderate	24%
Significant	33%
Very significant	22%
Total	100%

S3. What best describes your level of familiarity with Apache Hadoop or Cloudera?	Pct%
None (stop)	0%
Low	12%
Moderate	40%
Significant	24%
Very significant	24%
Total	100%

S4. What best describes your role as a user of big data analytics for cybersecurity?	Pct%
Business user of analytics	45%
Developer of applications	25%
Both user and developer	30%
None of the above (stop)	0%
Total	100%

Part 2: Security posture

Q1. How important is the use of big data analytics to detect advanced cyber threats?	Pct%
1 or 2	4%
3 or 4	10%
5 or 6	14%
7 or 8	19%
9 or 10	53%
Total	100%
Extrapolated value	7.64

Q2. What challenges prevent the effective use of big data analytics for cybersecurity? Please choose three top challenges.	Pct%
Insufficient resources	44%
Insufficient technologies	60%
Lack of in-house expertise	65%
Lack of clear leadership	17%
No understanding how to protect against cyber attacks	26%
Executives do not see cybersecurity as a significant risk	35%
Lack of collaboration with other functions	31%
Not a priority issue	18%
Other (please specify)	4%
Total	300%

Q3. Who determines the cybersecurity priorities or objectives within your organization? Please choose only one primary function.	Pct%
Board of directors	1%
CEO	3%
COO	0%
CFO	0%
CIO/CTO	25%
CISO/CSO	23%
Enterprise risk officer (CRO)	9%
Managed security service provider (MSSP)	13%
No one function determines cybersecurity priorities	26%
Other (please specify)	0%
Total	100%

Q4a. How has user demand for big data analytics for cybersecurity changed over the past 12 months?	Pct%
Significant increase	41%
Increase	30%
No change	20%
Decrease	8%
Significant decrease	1%
Total	100%

Q4b. If selected increase, what caused this change in demand? Please select all that apply.	Pct%
Response to cyber attacks	63%
Recruitment of expert staff	47%
Improvements in enabling technologies and/or the use of cyber analytics	55%
Changes in leadership, resource availability and organizational restructuring	30%
Changes in compliance requirements with laws and/or industry initiatives	27%
Total	222%

Q5. Which cyber incidents are you best at detecting? Please select all that apply.	Pct%
Rogue users	30%
Zero day attacks	25%
Network borne threats	54%
Advanced malware / Ransomware	39%
Spear phishing and social engineering	19%
Application-level attacks (SQL injection, cross site scripting or remote file inclusion)	63%
Advanced persistent threats	29%
Denial of services	56%
Compromised devices	38%
Malicious insiders	15%
Web-based attack	67%
Total	435%

Q6. Where are you seeing the greatest areas for cybersecurity risk? Please select five choices.	Pct%
Lack of system visibility	56%
Across 3rd party applications	55%
Negligent insiders	49%
Mobile devices such as smart phones	46%
External threats from social media	44%
Mobile/remote employees	43%
Malicious insiders	42%
Desktop or laptop computers	32%
Network infrastructure environment (gateway to endpoint)	31%
Cloud computing infrastructure and providers	27%
The server environment	24%
Virtual computing environments (servers, endpoints)	23%
Data centers	12%
Within operating systems	10%
Removable media (USB sticks) and/or media (CDs, DVDs)	6%
Total	500%

Q7. What are the most promising enabling security technologies? Please select six technologies in terms of importance to in meeting your organization's security objectives or mission. Technologies that . . .	Pct%
Provide machine learning applied to security data	51%
Provide user behavioral analytics (UBA)	50%
Provide advance warning about threats and attackers	48%
Provide intelligence about weak spots or vulnerabilities	47%
Provide cyber analytics for pinpointing cyber attacks	45%
Minimize insider threats (including negligence)	44%
Provide user network traffic analytics	43%
Prioritize threats, vulnerabilities and attacks	35%
Limit unauthorized access and/or sharing of sensitive or confidential data	30%
Prevent insecure devices from accessing secure systems	29%
Enable efficient recovery operations.	27%
Simplify the reporting of threats	26%
Secure endpoints including mobile-connected devices	24%
Reduce or eliminate malware from entering the network	22%
Enable adaptive perimeter controls	22%
Slows down or even halts the attacker's computers (use of honeypots)	20%
Enable efficient patch management	20%
Neutralizes denial of service attacks before they happen	17%
Total	600%

Q8. What best describes the maturity level of your organization's cybersecurity program or initiatives?	Pct%
Early stage – many cybersecurity program activities have not as yet been planned or deployed	5%
Middle stage – cybersecurity program activities are planned and defined but only partially deployed	25%
Late-middle stage – many cybersecurity program activities are deployed across the enterprise	40%
Mature stage – most cybersecurity program activities are deployed across the enterprise	30%
Total	100%

Q9. What best describes your organization's ability to identify security incidents?	Pct%
Most security incidents are identified within months	28%
Most security incidents are identified within weeks	36%
Most security incidents are identified within days	19%
Most security incidents are identified within hours or minutes	7%
None of the above (or, we rely on third parties to identify incidents)	10%
Total	100%

Q10. In your opinion, how important is the use of big data analytics for ensuring a strong cybersecurity posture within your organization?	Pct%
Essential	25%
Very important	40%
Important	23%
Not important	9%
Irrelevant	3%
Total	100%

Q11. Where is network visibility most important for the detection use cases you find most valuable? Please select one choice	Pct%
Connection data (netflow, flow)	26%
Packet data (IDS/IPS)	23%
Logs data (network device reporting)	20%
Forensic data (PCAP)	17%
Session context data (DPI session data, network meta information)	9%
Statistical data (counts)	5%
Total	100%

Q12. Did your organization's security posture improve as a result of greater network visibility?	Pct%
Yes	69%
No	21%
Unsure	10%
Total	100%

Q13a. Does your organization have a single cybersecurity platform that enables analysts to search, analyze and report on all network, user, endpoint, log, mobile, file/executable and threat intelligence data to support the incident analysis process?	Pct%
Yes	55%
No [go to Q.14]	45%
Total	100%

Q13b. If yes, does the cybersecurity platform support the collection and analysis of information for an unlimited timeframe?	Pct%
Yes	38%
No	62%
Total	100%

Q13c. If yes, does the cybersecurity platform support any data types (files, databases, binaries, video, images and documents)?	Pct%
Yes	40%
No	60%
Total	100%

Q13d. If yes, does the cybersecurity platform offer analytic flexibility to perform all the necessary analytics approaches your organization requires (statistical, correlation, behavioral and machine learning)?	Pct%
Yes	44%
No	56%
Total	100%

Q13e. If yes, does the cybersecurity platform offer integration with the datasets with other applications (commercial, open source or custom developed)?	Pct%
Yes	48%
No	52%
Total	100%

Part 3. Budget Questions

Q14. Who within your organization has funding authority for investment in cybersecurity solutions?	Pct%
CIO	27%
CTO	5%
CISO/CSO	21%
Data center management	3%
Compliance and legal	2%
LOB management	23%
Shared among various functions	19%
Total	100%

Q15a. What dollar range best describes your organization's IT security budget in the present fiscal year?	Pct%
Less than $2 million	2%
Between $2 to $4 million	1%
Between $4 to $6 million	3%
Between $6 to $8 million	5%
Between $8 to $10 million	9%
Between $10 to $12 million	20%
Between $12 to $14 million	13%
Between $14 to $16 million	10%
Between $16 to $18 million	12%
Between $18 to $20 million	12%
Between $20 to $25 million	7%
Over $25 million	6%
Total	100%
Extrapolated value	14.45

Q15b. What dollar range best describes your organization's IT security budget for analytic tools in the present fiscal year?	Pct%
Less than $2 million	77%
Between $2 to $4 million	6%
Between $4 to $6 million	6%
Between $6 to $8 million	4%
Between $8 to $10 million	3%
Between $10 to $12 million	1%
Between $12 to $14 million	2%
Between $14 to $16 million	1%
Between $16 to $18 million	0%
Between $18 to $20 million	0%
Between $20 to $25 million	0%
Over $25 million	0%
Total	100%
Extrapolated value	2.32

Q16a. In terms of a percentage of the current IT security budget, how much would your organization be willing to spend to reduce anomalous and potentially malicious traffic by 10 percent?	Pct%
Less than 5%	18%
Between 5% to 10%	36%
Between 10% to 20%	19%
Between 20% to 30%	12%
Between 30% to 40%	7%
Between 40% to 50%	3%
Between 50% to 60%	2%
Between 60% to 70%	2%
Between 70% to 80%	1%
Between 80% to 90%	0%
Between 90% to 100%	0%
Total	100%
Extrapolated value	16.0%

Q16b. In terms of a percentage of the current IT security budget, how much would your organization be willing to spend to reduce anomalous and potentially malicious traffic by 90 percent?	Pct%
Less than 5%	3%
Between 5% to 10%	5%
Between 10% to 20%	5%
Between 20% to 30%	12%
Between 30% to 40%	19%
Between 40% to 50%	18%
Between 50% to 60%	11%
Between 60% to 70%	12%
Between 70% to 80%	9%
Between 80% to 90%	6%
Between 90% to 100%	0%
Total	100%
Extrapolated value	45%

Q17. With respect to the typical IT security budget, please rank where your organization spends the most today and will spend 24 months in the future, 1 = spending the most and 7 = spending the least.	Spending today	Spending in the future
Governance, compliance and reporting	1.97	2.31
Data loss detection and prevention	3.89	4.03
Perimeter controls	1.56	2.54
Identity management	2.75	3.34
Correlation of security information from multiple sources	6.55	4.15
Anomaly detection	4.66	3.90
Advanced persistent threat (APT) detection/prevention	5.63	4.88

Part 4. Analytics for cybersecurity

Q19. How difficult is the typical deployment of cybersecurity analytics within your organization?	Pct%
Very difficult	30%
Difficult	34%
Not difficult	21%
Easy	15%
Total	100%

Q20. What best describes the level of involvement of third-party consultants (experts) in the deployment of cybersecurity analytics within your organization?	Pct%
None	10%
Low	13%
Moderate	19%
Significant	30%
Very significant	28%
Total	100%

Essential and very important responses.	Pct%
Q21a. How important is the ability to access and examine deep packet data in cybersecurity analytics?	56%
Q21b. How important is the ability to examine user behavior analytics (UBA) for cybersecurity?	54%

Following are key features of certain cybersecurity analytic tools in the market today. Please rate each feature using the importance scale. Then select the extent to which this feature is being deployed within your organization.	
Q22a. Provide unified data repository for "all" security data.	Pct%
Essential and very important responses	65%
Fully and partially deployed responses	44%

Q22b. Enable powerful analytic frameworks that enable insider and advanced persistent threat detection	Pct%
Essential and very important responses	69%
Fully and partially deployed responses	40%

Q22c. Give threat analysts powerful visual analysis toolsets that slice across multiple data sources at petabyte scale to identify outliers.	Pct%
Essential and very important responses	63%
Fully and partially deployed responses	39%

Q22d. Supply full entity-centered contextual information at security responders' fingertips—to speed investigation and support development of comprehensive mitigation strategies.	Pct%
Essential and very important responses	60%
Fully and partially deployed responses	41%

Attributions: Please rate each statement using the agreement scale provided below each item. Strongly agree and Agree responses.	Pct%
Q23a. Leveraging big data and advanced analytics to get ahead of threats is impossible with traditional systems.	72%
Q23b. Security operations must constantly offload data as budget constraints and system limits are reached.	66%
Q23c. It takes days or weeks to access complementary data incident responders need in order to respond to flagged events.	59%
Q23d. Threat analysts can't perform advanced analytics (e.g. machine learning) against TBs worth of data in short order.	61%

Q24. Would you be inclined to recommend your organization's analytic tools for cybersecurity to an acquaintance, colleague or friend?	Pct%
Strongly recommend	40%
Recommend	35%
Do not recommend	25%
Total	100%

Q25. How much does it cost to store one terabyte (TB) of your organization's security data?	Pct%
Less that $500 per TB	19%
$500 to $1,000 per TB	23%
$1,001 to $5,000 per TB	36%
More than $5,000 per TB	22%
Total	100%
Extrapolated value	2,510

Q26a. Which are the primary data sources used to identify incidents? Please select all that apply.	Pct%
SIEM alerts	33%
Third party notifications	15%
Network data analysis	30%
File/executable analysis	18%
User behavior anomalies	44%
Threat intelligence	42%
Forensic investigation	59%
IT operations alerts/outages	12%
Endpoint analytics	34%
Total	287%

Q26b. Which are the secondary data sources used to identify incidents? Please select all that apply.	Pct%
SIEM alerts	46%
Third party notifications	60%
Network data analysis	46%
File/executable analysis	21%
User behavior anomalies	34%
Threat intelligence	70%
Forensic investigation	23%
IT operations alerts/outages	34%
Endpoint analytics	39%
Total	373%

D1. What best describes your position level within the organization?	Pct%
Executive	2%
Vice president	3%
Director	17%
Manager	23%
Supervisor	16%
Staff/technician	39%
Other	0%
Total	100%

D2. What best describes your direct reporting channel?	Pct%
CEO/executive committee	0%
COO or head of operations	0%
CFO, controller or head of finance	2%
CIO or head of corporate IT	45%
General counsel or head of corporate legal	3%
Business unit leader or general manager	21%
Head of compliance or internal audit	4%
Head of IT security	18%
Head of security	2%
Other	5%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Pct%
< 1,000	23%
1,000 to 5,000	21%
5,001 to 10,000	20%
10,001 to 25,000	17%
25,001 to 75,000	11%
> 75,000	8%
Total	100%

D4. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	3%
Financial services	17%
Health & pharmaceutical	11%
Hospitality	3%
Industrial & manufacturing	9%
Public sector	10%
Retail	10%
Services	9%
Technology & software	8%
Transportation	3%
Other	0%
Total	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.