Ponemon INSTITUTE

The Value of Artificial Intelligence in Cybersecurity

Sponsored by IBM Security

Independently conducted by Ponemon Institute LLC

Publication Date: July 2018

The Value of Artificial Intelligence in Cybersecurity

Presented by Ponemon Institute, July 2018

Part 1. Introduction

Ponemon Institute is pleased to present *The Value of Artificial Intelligence in Cybersecurity* sponsored by IBM Security. The purpose of this research is to understand trends in the use of artificial intelligence and how to overcome barriers to full adoption.

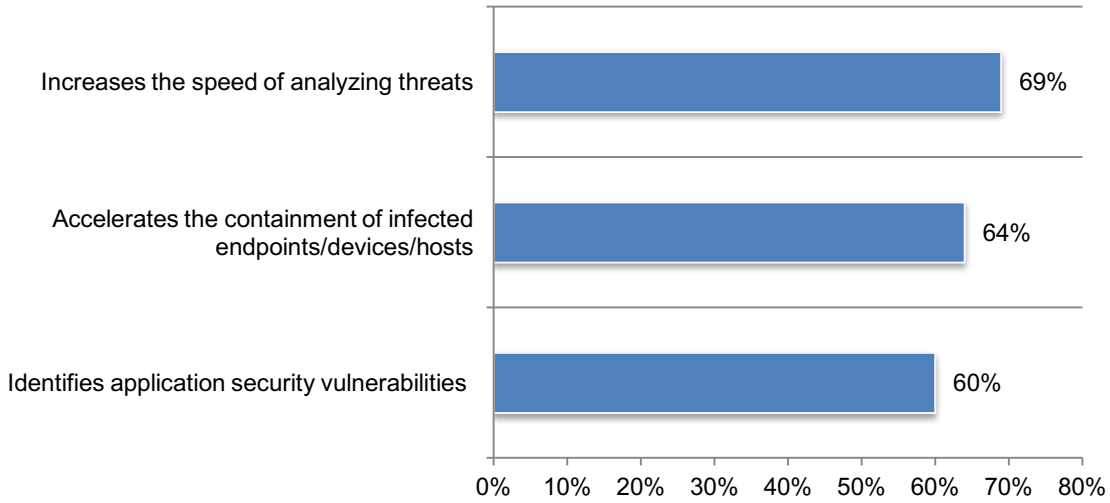
Ponemon Institute surveyed 603 IT and IT security practitioners in US organizations that have either deployed or plan to deploy AI as part of their cybersecurity program or infrastructure. According to the findings, these participants strongly believe in the importance and value of AI but admit that being able to get the maximum value from technologies is a challenge.

As shown in Figure 1, the adoption of AI can have a very positive impact on an organization's security posture and bottom line. The biggest benefit is the increase in speed of analyzing threats (69 percent of respondents) followed by an acceleration in the containment of infected endpoints/devices and hosts (64 percent of respondents). Because AI reduces the time to respond to cyber exploits organizations can potentially save an average of more than $2.5 million in operating costs.

In addition to greater efficiencies in analyzing and containing threats, 60 percent of respondents say AI identifies application security vulnerabilities. In fact, 59 percent of respondents say that AI increases the effectiveness of their organizations' application security activities.

Figure 1. How AI improves security posture

More than one response permitted



To improve the effectiveness of AI technologies, organizations should focus on the following three activities.

Attract and retain IT security practitioners with expertise in AI technologies. AI may improve productivity but it will increase the need for talented IT security personnel. Fifty-two percent of respondents say AI will increase the need for in-house expertise and dedicated headcount.

Simplify and streamline security architecture. While some complexity in an IT security architecture is expected in order to deal with the many threats facing organizations, too much complexity can impact the effectiveness of AI. Fifty-six percent of respondents say their

organizations need to simplify and streamline security architecture to obtain maximum value from AI-based security technologies. Sixty-one percent say it is difficult to integrate AI-based security technologies with legacy systems.

Supplement IT security personnel with outside expertise. Fifty percent of respondents say it requires too much staff to implement and maintain AI-based technologies and 57 percent of respondents say outside expertise is necessary to maximize the value of AI-based security technologies.

As the adoption of AI technologies matures, the more committed organizations become to investing in these technologies.

In this research, 139 respondents of the total sample of 603 respondents self-reported that their organizations have either fully deployed AI (55) or partially deployed AI (84). We refer to these respondents as AI users. We conducted a deeper analysis of how these respondents perceive the benefits and value of AI. Following are some of the most interesting differences between AI users and the overall sample of respondents who are in the planning stages of their deployment of AI.

- AI users are more likely to appreciate the benefits of AI technology. Seventy-one percent of AI users vs. 60 percent of the overall sample say an important benefit is the ability of AI to deliver deeper security than if organizations relied exclusively on their IT security staff.

- AI users are more likely to believe these technologies simplify the process of detecting and responding to application security threats. As a result, AI users are more committed to AI technologies.

- While AI users are more likely to believe AI will increase the need for in-house expertise and dedicated headcount (60 percent of AI users vs. 52 percent in the overall sample), these respondents are more aware than the overall sample that AI benefits their organization because it increases the productivity of security personnel.

- AI has reduced application security risk in organizations that have achieved greater deployment of these technologies. When asked about the effectiveness of AI in reducing application security risk, 69 percent of respondents say these technologies have significantly increased or increased the effectiveness of their application security activities vs. 59 percent of respondents in the overall sample who say their effectiveness increased in reducing application security risk.

- AI technologies tend to decrease the complexity of organizations' security architecture. Fifty-six percent of respondents in organizations that have more fully deployed AI report that instead of adding complexity AI actually decreases complexity. Only 24 percent of AI users say it increases complexity.

- As the use of AI increases, the more knowledgeable the IT security staff becomes in identifying areas where the use of advanced technologies would be most beneficial. Fifty-six percent of AI users rate their organizations' ability to accurately identify areas in their security infrastructure where AI and machine learning would create the most value as very high.

- AI improves the ability to detect previously "undetectable" zero-day exploits. On average, AI users are able to detect 63 percent of previously "undetectable" zero-day exploits. In contrast, respondents in the overall sample say AI can increase detection by an average of 41 percent.

Part 2. Key findings

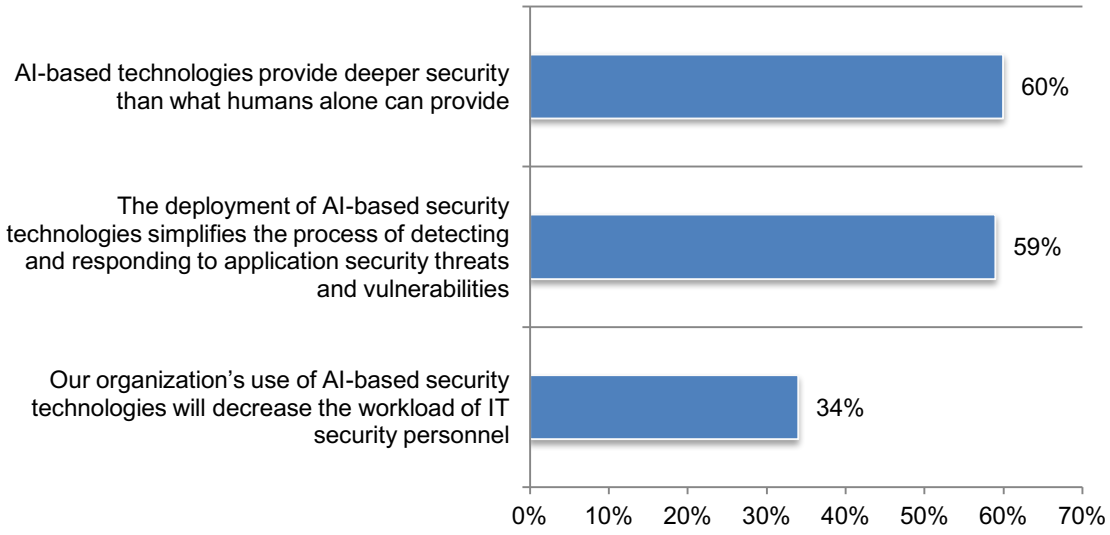
In this section of the report, we provide the detailed findings and trends of the research. The complete findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- Impact of AI on cybersecurity posture
- Current AI practices
- Challenges to AI deployment
- Best practices of organizations with more mature AI deployments

The impact of AI on cybersecurity posture

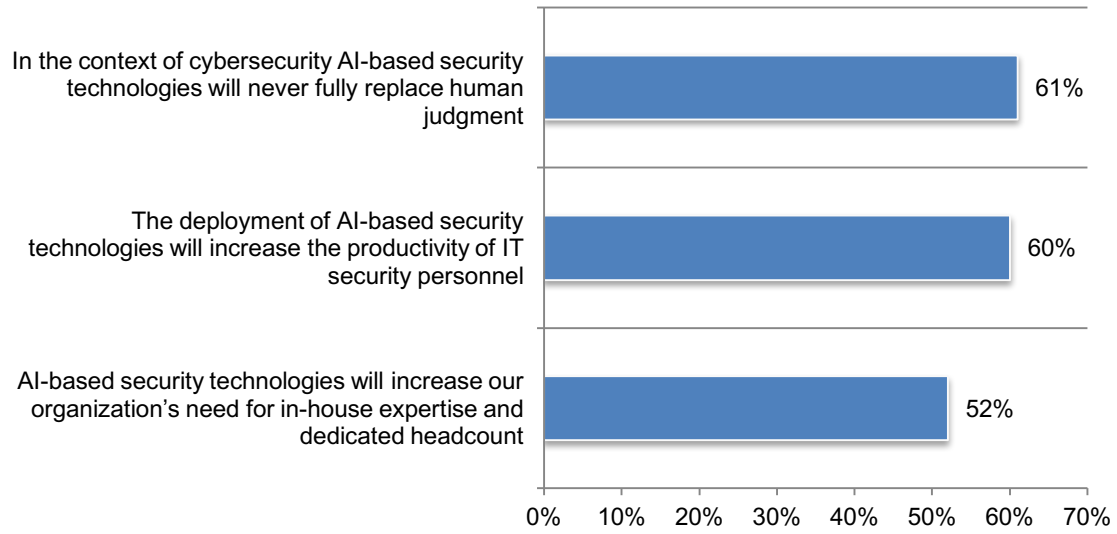
AI-based technologies improve security but will not reduce the need for staff. Working together, AI and IT security personnel can have a positive impact on organizations' cybersecurity posture. As shown in Figure 2, AI-based technologies provide deeper security than what humans alone can provide (60 percent of respondents). However, only 34 percent of respondents say the use of AI will decrease the workload of IT security personnel.

Figure 2. Benefits of AI
Strongly agree and agree responses combined



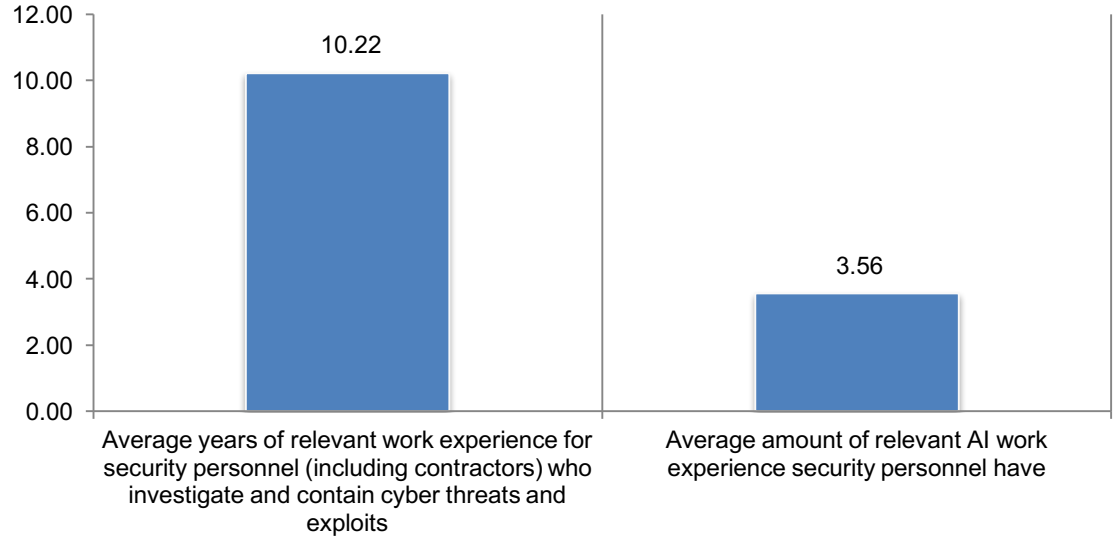
AI is expected to improve productivity and increase organizations' need for talented IT security personnel. As shown in Figure 3, 60 percent of respondents are positive about the ability of AI-based security technologies to improve the productivity of IT security personnel. Similarly, these technologies will never fully replace human judgment in organizations' efforts to improve their cybersecurity posture. More than half (52 percent of respondents) believe their organizations will need to hire more IT security staff to ensure they benefit from AI.

Figure 3. The impact of AI on staffing
Strongly agree and agree responses combined



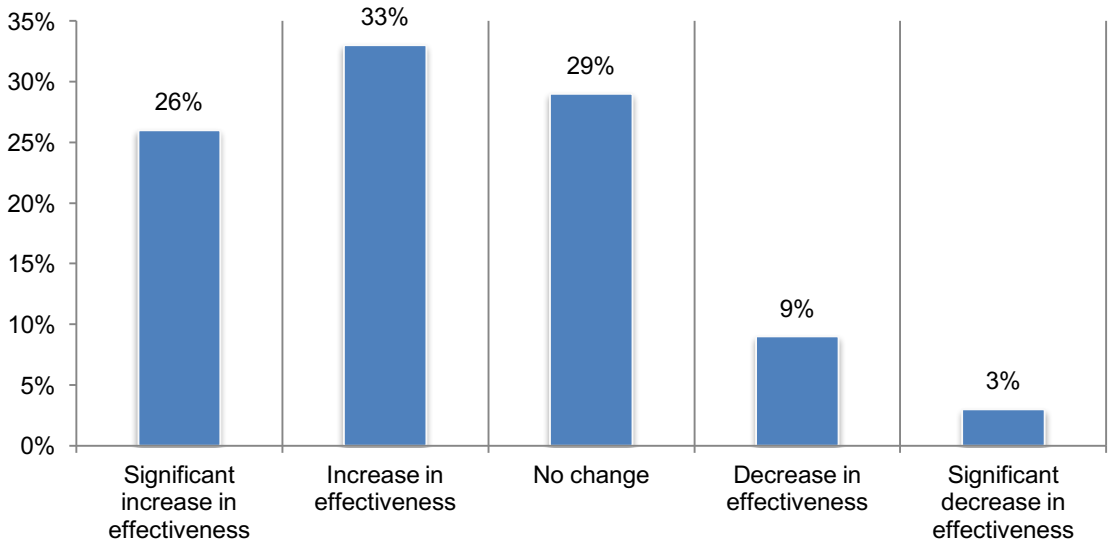
Expertise in AI will become more critical as organizations increase their use of these technologies. While the average years of relevant work experience for IT security personnel is more than 10 years, the average years of relevant AI work experience that security personnel have is about 4 years.

Figure 4. Years of relevant experience for security personnel
Extrapolated values



Application security improves with AI. Fifty-nine percent of respondents say that AI increases the effectiveness of organizations' application security activities within their organizations, according to Figure 5.

Figure 5. The impact of AI on reducing application security risk



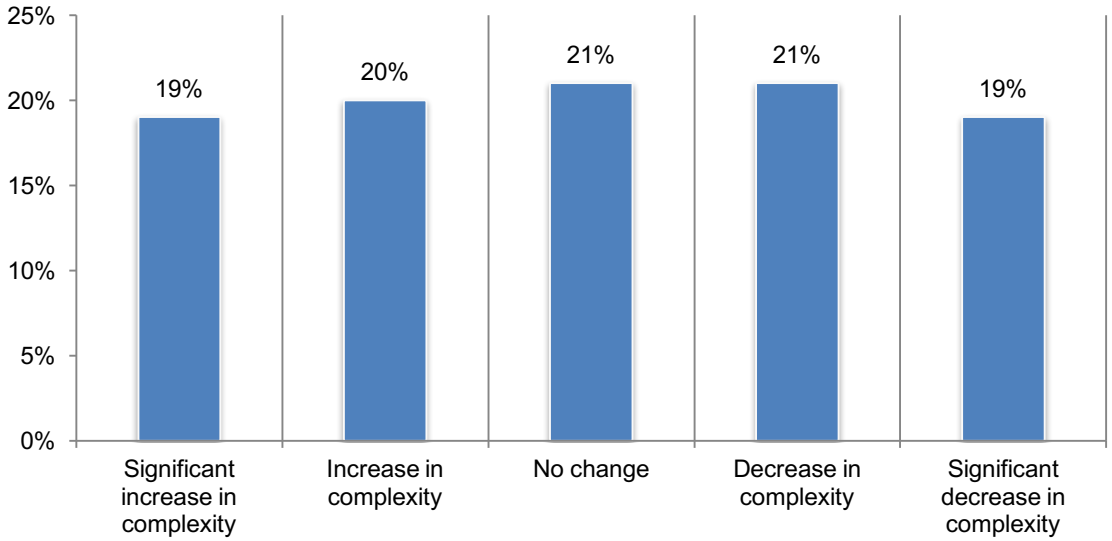
AI reduces the time to deal with cyber exploits. According to Table 1, when AI is used to contain cyber exploits, the time and cost are significantly reduced. The average cost of not using AI to address cyber exploits is more than $3 million versus $814,873 if AI is used. Thus, a company can potentially save an average of more than $2.5 million in operating costs.

Table 1. Labor hours spent containing cyber exploits each week	Not facilitated by AI	Facilitated by AI	Difference in hours and cost
Organizing and planning approaches to cyber defense	25.32	16.05	9.27
Capturing actionable intelligence about cyber exploits and malware infections	80.20	41.11	39.09
Investigating and detecting application vulnerabilities	195.88	70.48	125.40
Investigating actionable intelligence about cyber exploits or malware	66.28	24.23	42.05
Cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by cyber exploits or malware	212.89	39.63	173.26
Documenting and/or reporting upon the cyber event (in conformance with policies or compliance mandates)	25.07	15.91	9.16
Time wasted by security staff members chasing erroneous or false positives	400.83	41.42	359.41
Unplanned downtime due to cleaning, fixing or patching of malware-infected networks, applications and devices	3.95	1.90	2.05
Total hours per week	1,010.42	250.73	759.69
Total hours per year	52,541.84	13,037.96	39,503.88
Estimated total cost per year	$3,283,865.00*	$814,872.50*	$2,468,992.50*

*IT and IT security fully loaded pay rate is $62.50 (source: Ponemon Institute).

Organizations are divided as to whether AI will reduce or increase complexity. According to Figure 6, 39 percent of respondents say AI will increase complexity and 40 percent of respondents say complexity decreases.

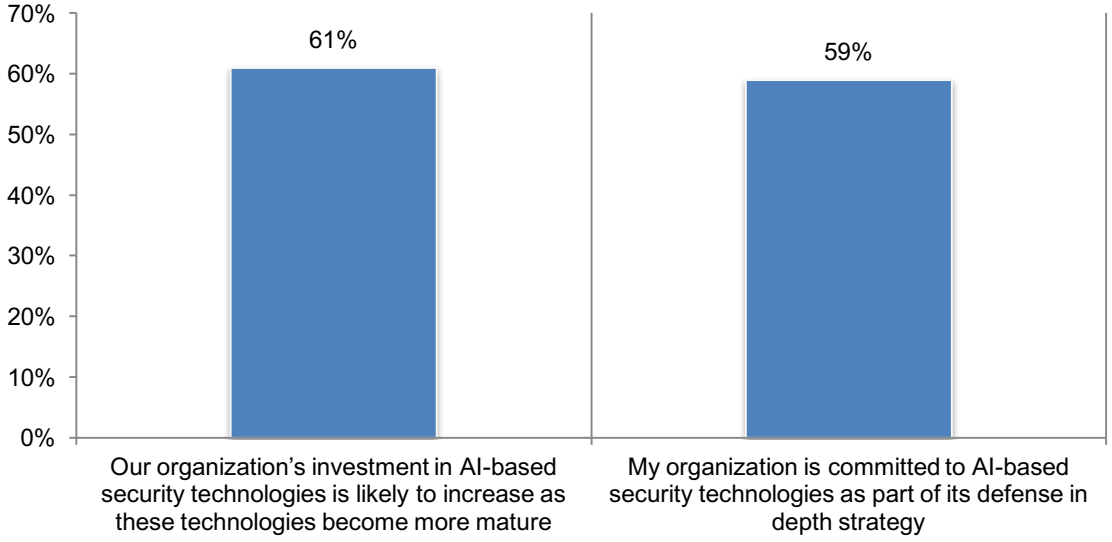
Figure 6. The impact of AI on reducing the complexity of IT security architecture



Current AI practices

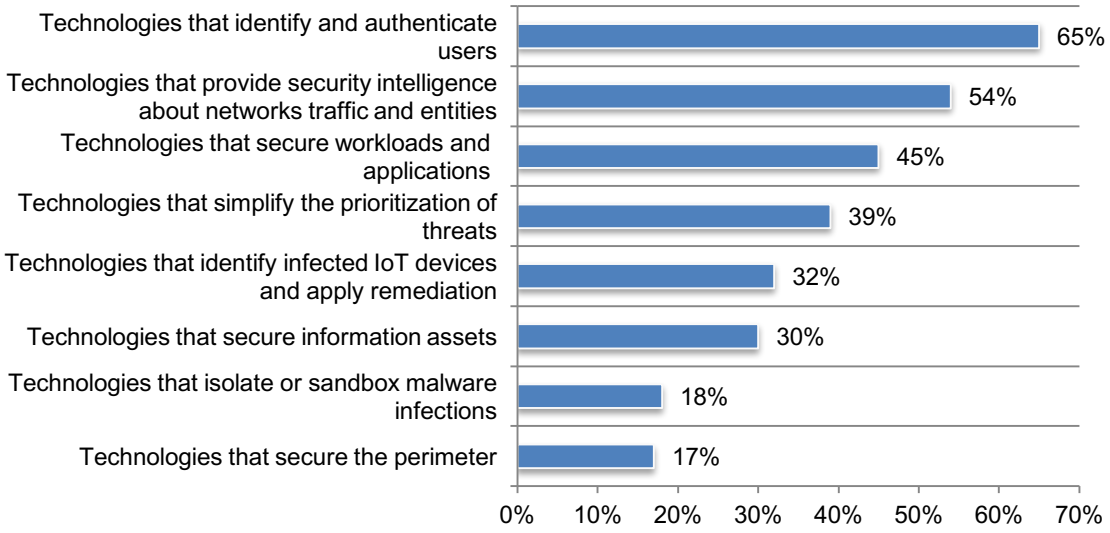
Organizations expect to increase their investment in AI. As the technology matures, investments will increase, according to 61 percent of respondents. Another reason for organizations to purchase AI is their commitment to these technologies as part of its defense in depth strategy, as shown in Figure 7.

Figure 7. Organizations are committed to investing in AI
Strongly agree and agree responses combined



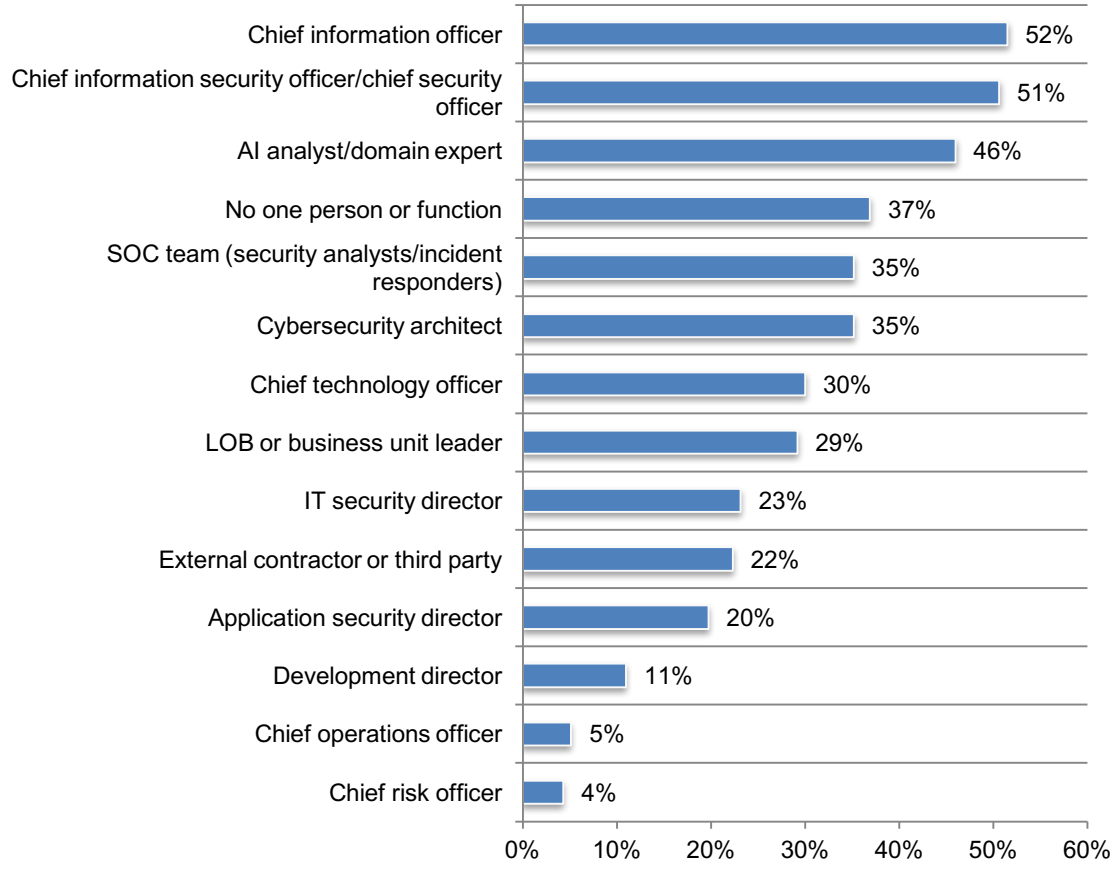
AI will most likely support technologies that identify and authenticate users. According to Figure 8, 65 percent of respondents say AI will support technologies that identify and authenticate users and 54 percent of respondents say it will be used with technologies that provide security intelligence about network traffic and entities.

Figure 8. Technologies most likely to be supported by AI
Three responses permitted



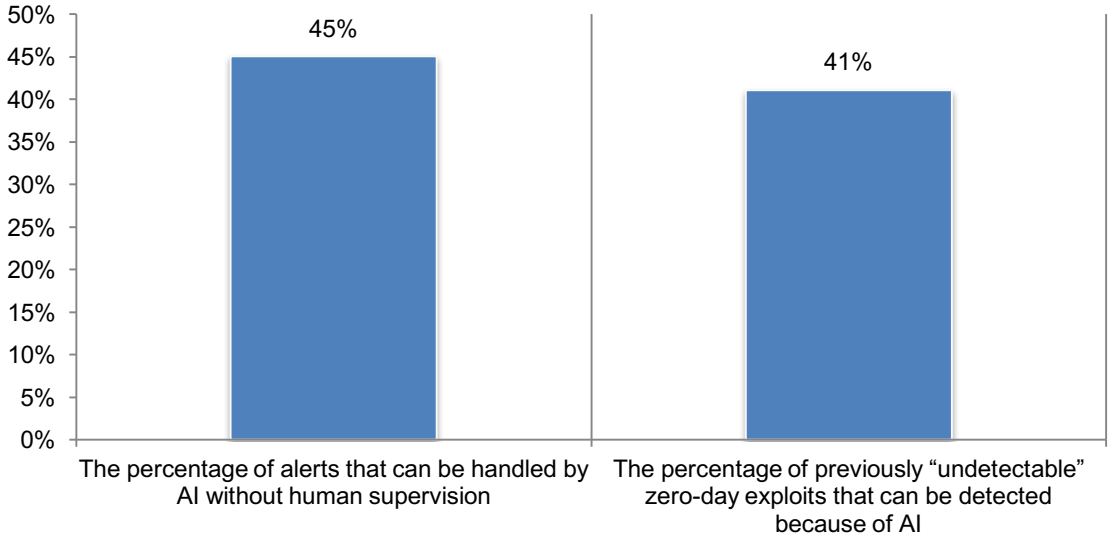
The CIO and CISO are determining their organizations' use of AI. While a variety of roles and function may influence how AI is used, the chief information officer and chief information security officer are most likely to influence how AI is applied in their organizations, as shown in Figure 9.

Figure 9. The key influencers in determining how AI is used
Four responses permitted



Human supervision is still required when dealing with alerts. As shown in Figure 10, an average of 45 percent of alerts can be handled by AI without human supervision. On average 41 percent of previously "undetectable" zero-day exploits that can be detected because of AI.

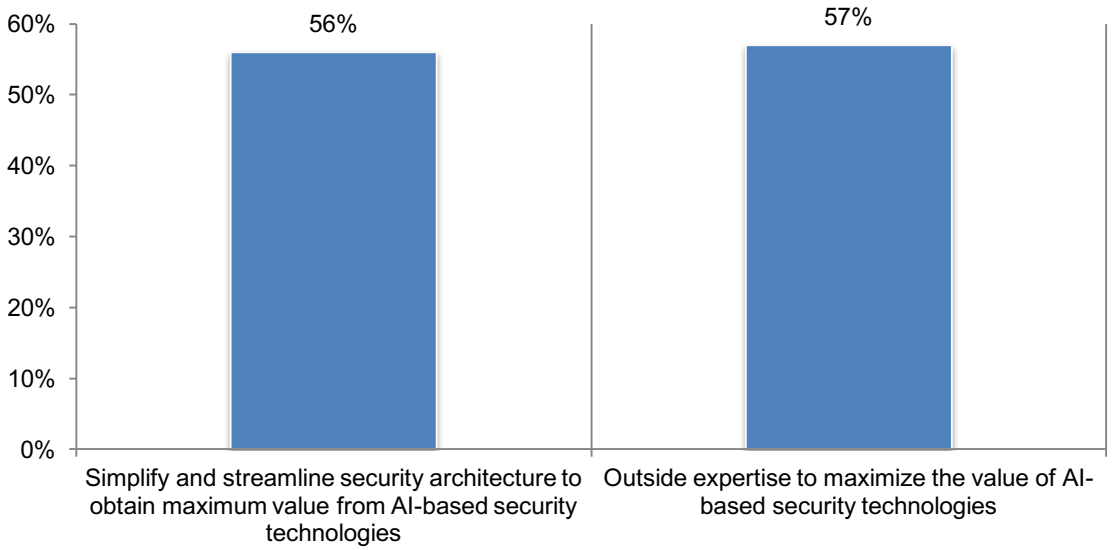
Figure 10. Percentage of alerts that can be handled by AI without human supervision and the percentage of zero-day exploits that can be detected by AI
Extrapolated values



Challenges to AI deployment

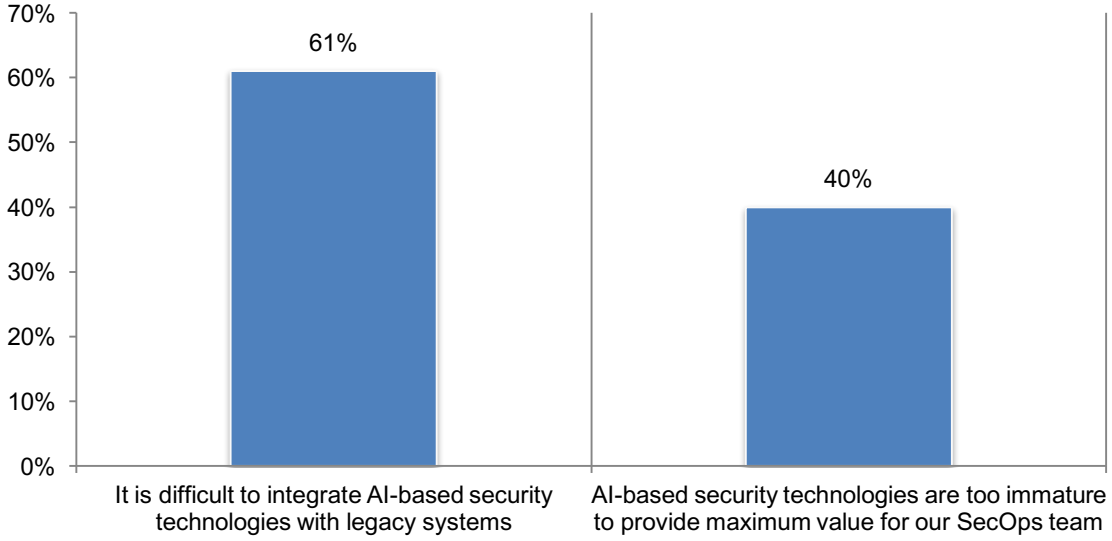
To have a successful deployment of AI, organizations need to avoid complexity of their IT security function and engage outside expertise. As shown in Figure 11, 56 percent of respondents say in order to maximize the value of AI their organizations' security architecture needs to be simplified and streamlined. Fifty-seven percent of respondents say it is important to turn to outsiders who have expertise in AI.

Figure 11. What organizations need to do to deploy AI
Strongly agree and agree responses combined



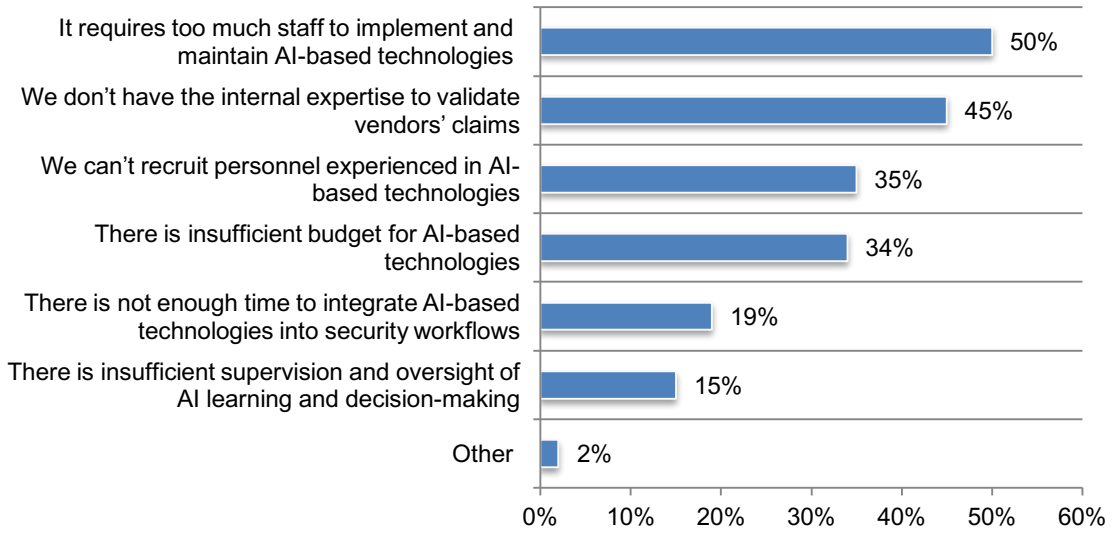
Today, integration with legacy systems and the immaturity of the technologies are challenges to deploying AI. According to Figure 12, 61 percent of respondents say their organizations find it difficult to integrate AI-based security technologies with legacy systems. Forty percent of respondents say the technologies are too immature to provide maximum value for their SecOps team.

Figure 12. Challenges to AI deployment
Strongly agree and agree responses combined



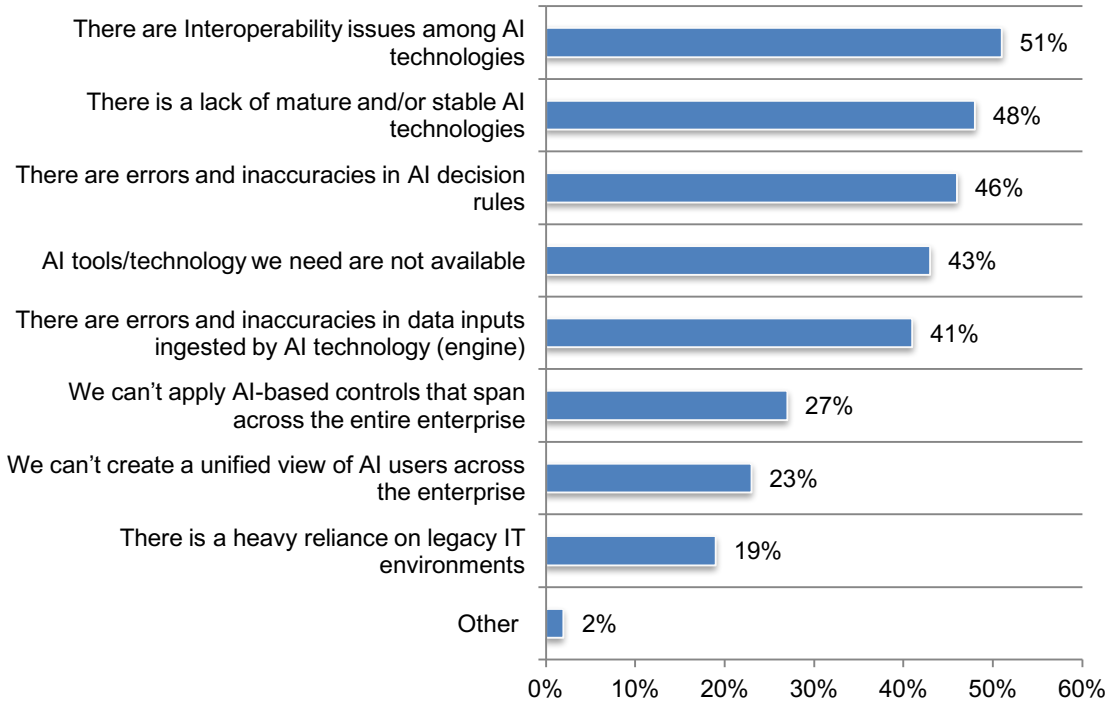
Staffing and internal expertise are the most significant governance challenges to AI deployment. As shown in Figure 13, 50 percent of respondents say it requires too much staff to implement and maintain AI-based technologies and 45 percent of respondents say the lack of internal expertise to validate vendors' claims are governance challenges.

Figure 13. Governance challenges to AI deployment
Two responses permitted



Interoperability issues and lack of mature AI technologies are current problems with AI technologies. According to Figure 14, more than half (51 percent of respondents) say there are interoperability issues among AI technologies and almost half (48 percent of respondents) say the lack of mature and/or stable AI technologies are barriers to effectiveness.

Figure 14. Barriers to the effectiveness of AI technologies
Three responses permitted

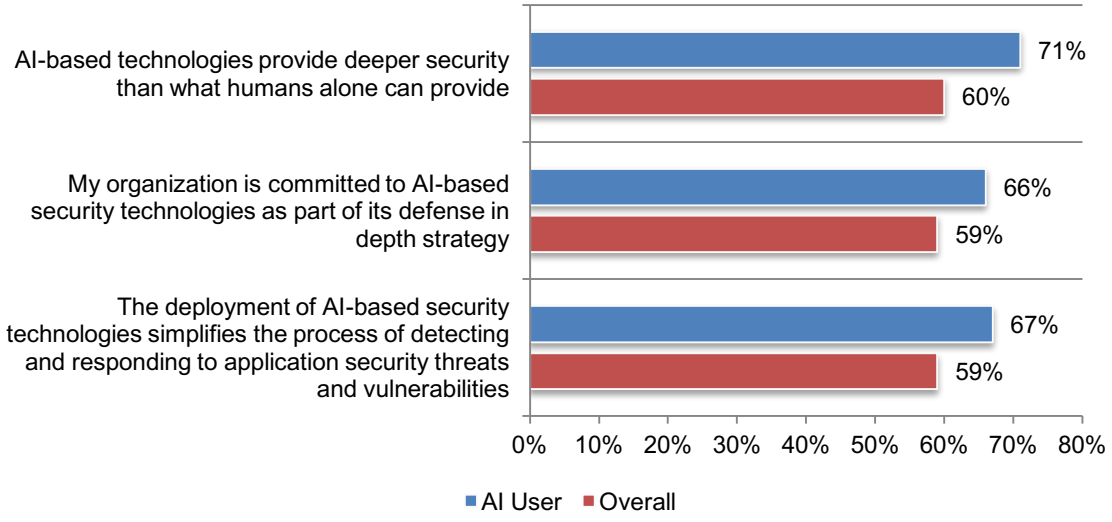


Best practices of organizations with more mature AI deployments

In this section, we provide an analysis of 139 respondents who say their organizations have either fully deployed AI (55) or partially deployed (84) AI. The findings from this sample of respondents provide insights into how these organizations have been able to address the challenges of deploying these technologies and are reaping the benefits. The following figures compare AI users to those who are in the early stages of planning and deploying AI.

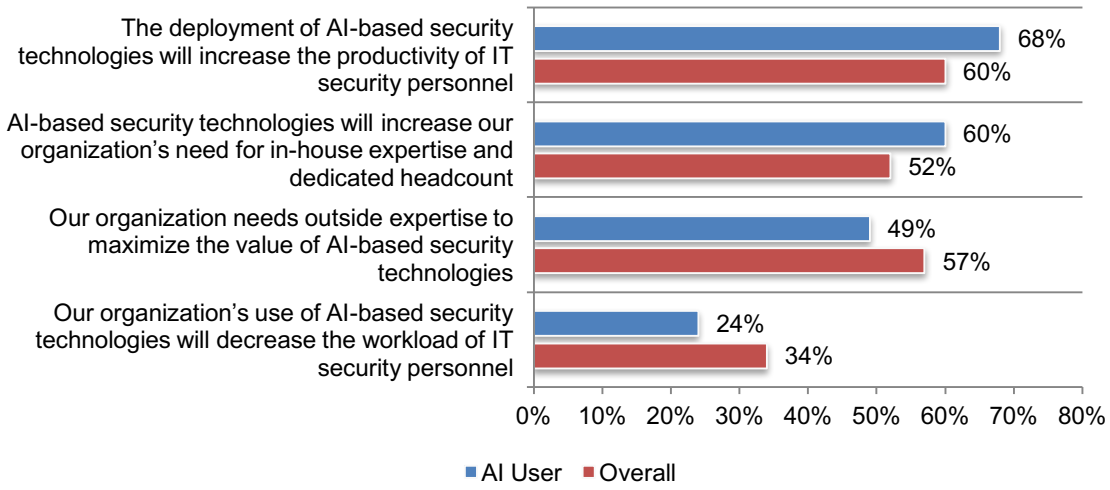
AI users are more likely to appreciate the benefits of AI technology. As shown in Figure 15, 71 percent of AI users vs. 60 percent of the overall sample say an important benefit is the ability of AI to deliver deeper security than if organizations relied exclusively on their IT security staff. AI users are more likely to believe these technologies simplify the process of detecting and responding to application security threats. As a result, AI users are more committed to AI technologies (66 percent of AI users vs. 59 percent of the overall sample).

Figure 15. Benefits of AI
Strongly agree and agree responses combined



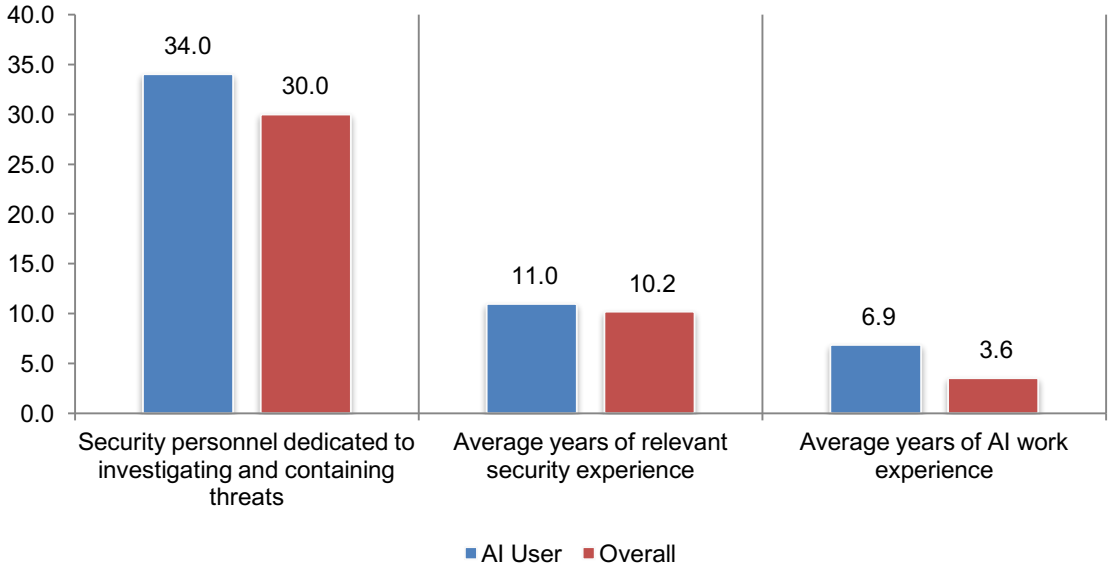
AI users are more likely to recognize that their IT security functions will need to hire more staff to support the use of AI technologies. As presented in Figure 16, only 24 percent of AI users say the workload of IT security personnel will decrease. While they are more likely to believe AI will increase the need for in-house expertise and dedicated headcount (60 percent vs. 52 percent), AI users are more aware than the overall sample that AI increases the productivity of security personnel.

Figure 16. The impact of AI on staffing
Strongly agree and agree responses combined



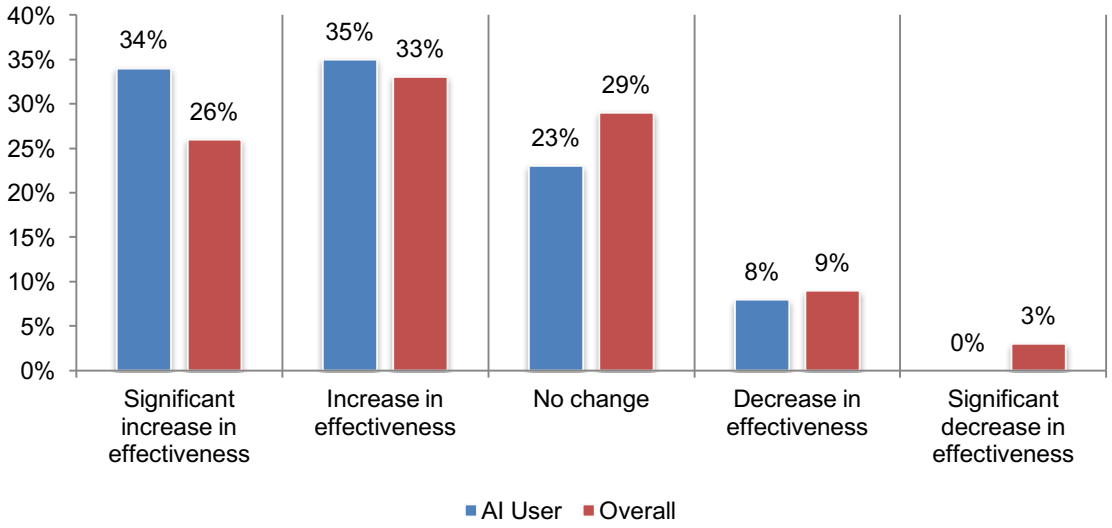
Organizations that have fully or partially deployed AI are increasing their in-house AI expertise. As shown in Figure 17, AI users have more IT security practitioners and more staff with relevant AI experience than the overall sample.

Figure 17. Relevant AI experience in the workplace
Extrapolated values



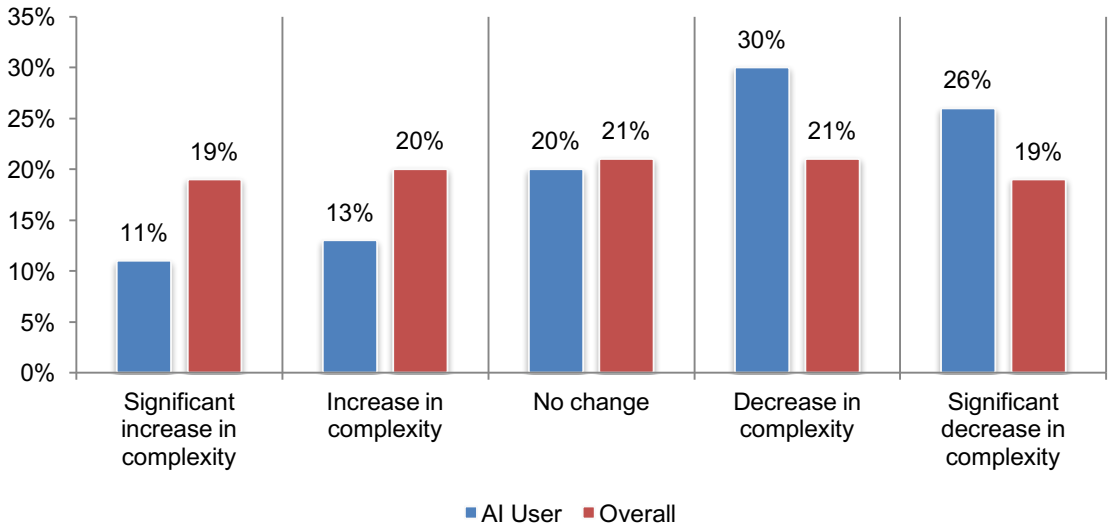
AI has reduced application security risk in organizations that have achieved greater deployment of these technologies. When asked about the effectiveness of AI in reducing application security risk, 69 percent of respondents say these technologies have significantly increased or increased the effectiveness of their application security activities vs. 59 percent of respondents in the overall sample, as presented in Figure 18.

Figure 18. Effectiveness in reducing application security risk
Very effective and effective responses combined



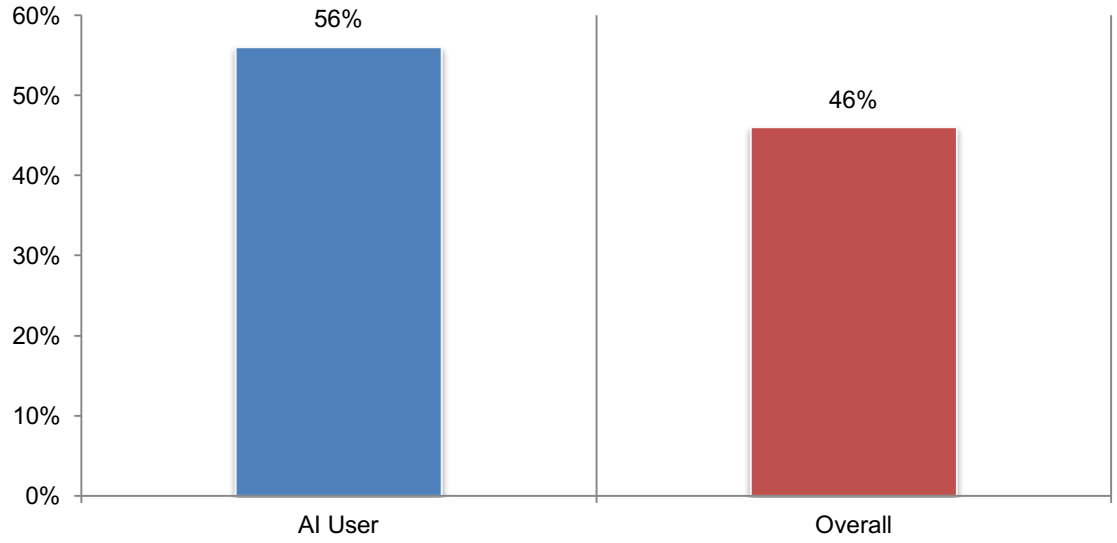
AI technologies tend to decrease the complexity of organizations' security architecture. Fifty-six percent of respondents in organizations that have more fully deployed AI report that instead of adding complexity it actually decreases complexity. Only 24 percent of these respondents say it increases complexity, as shown in Figure 19.

Figure 19. How will AI impact the overall complexity of an organization's security architecture



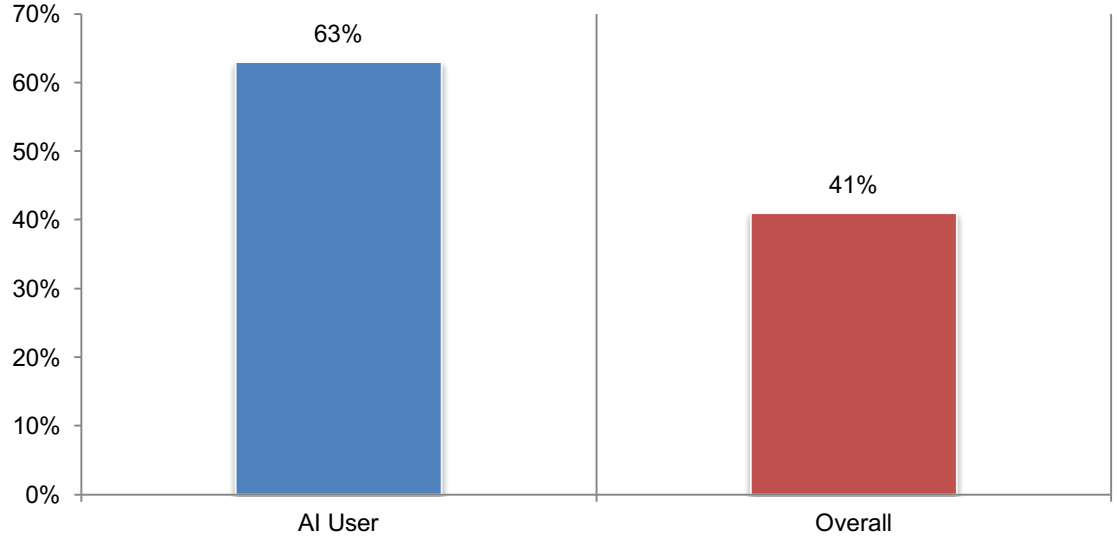
AI increases the ability to accurately identify areas where AI and machine learning creates the most value. As the use of AI increases, the more knowledgeable IT security staff becomes in identifying areas where the use of advanced technologies would be most beneficial. As shown in Figure 20, when asked to rate on a scale of 1= low ability to 10 = high ability, 56 percent of AI users rate their organizations' ability to accurately identify areas in their security infrastructure where AI and machine learning would create the most value as very high (7+ responses).

Figure 20. The ability to accurately identify areas where AI and machine learning would create the most value
7+ responses on a scale of 1 = low ability to 10 = high ability



AI improves the ability to detect previously "undetectable" zero-day exploits. On average, AI users are able to detect 63 percent of previously "undetectable" zero-day exploits. In contrast, respondents in the overall sample say AI improves the detection of these attack by an average of 41 percent, as shown in Figure 21.

Figure 21. The ability to detect previously "undetectable" zero-day exploits
Extrapolated values



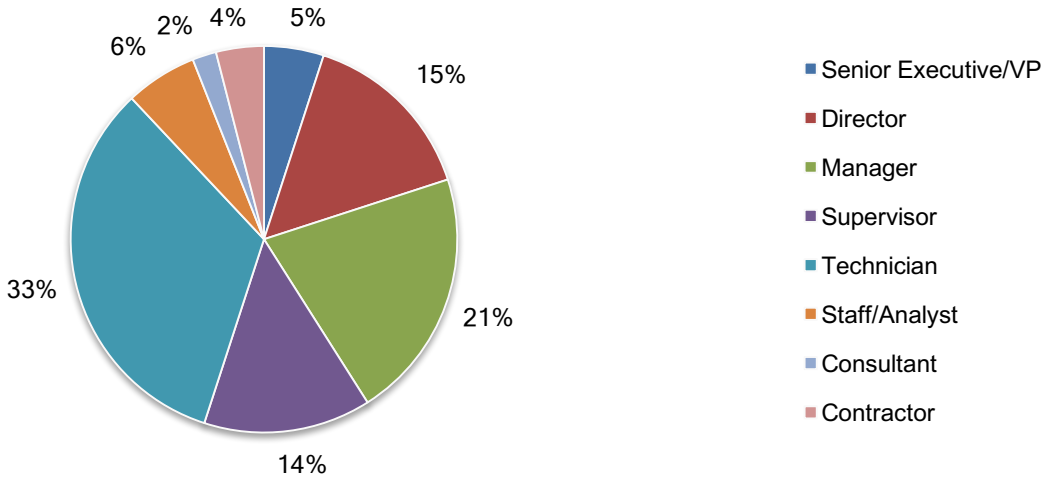
Part 3. Methods

The sampling frame was composed of 16,995 IT and IT security practitioners located in the United States that have either deployed or plan to deploy AI as part of their cybersecurity program or infrastructure. Table 2 reveals that 655 respondents completed the survey. Screening removed 52 surveys. The final sample was 603 surveys or a 3.5 percent response rate.

Table 2. Sample response	Freq	Pct%
Total sampling frame	16,995	100.0%
Total returns	655	3.9%
Rejected or screened surveys	52	0.3%
Final sample	603	3.5%

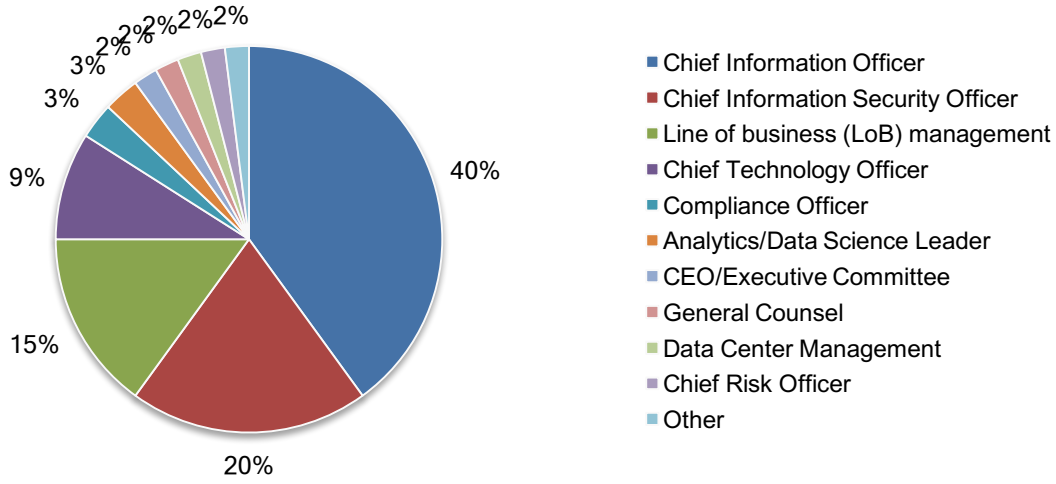
Pie Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (55 percent) reported their current position as supervisory or above.

Pie Chart 1. Distribution of respondents according to position level



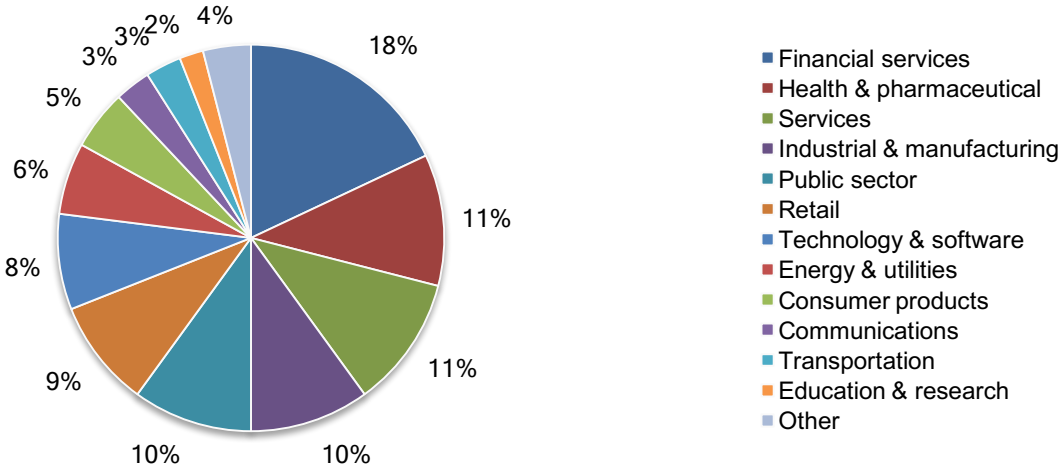
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Forty percent of respondents identified the chief information officer as the person to whom they report. Another 20 percent of respondents indicated they report directly to the chief information security officer, and 15 percent of respondents report to the line of business management.

Pie Chart 2. Distribution of respondents according to reporting channel



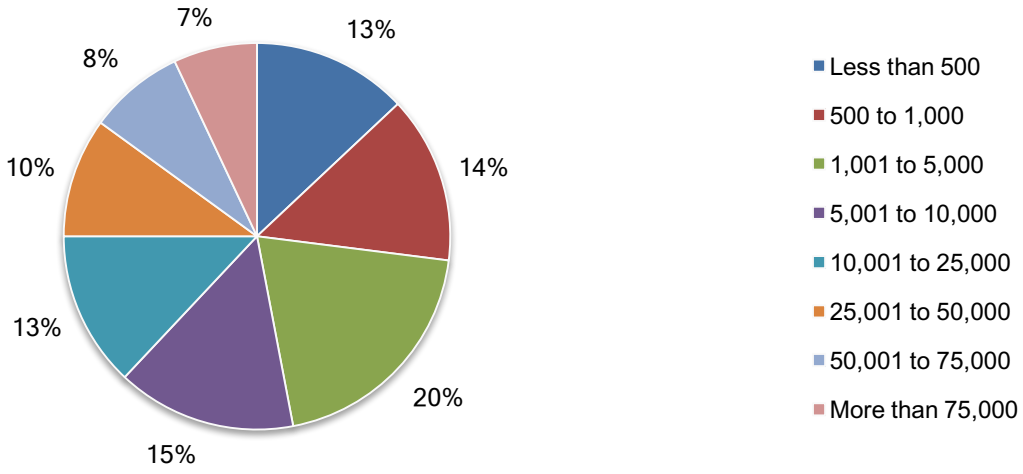
Pie Chart 3 displays the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by health and pharmaceuticals sector (11 percent of respondents), services sector (11 percent of respondents), industrial and manufacturing sector (10 percent of respondents) and public sector (10 percent of respondents).

Pie chart 3. Distribution of respondents according to primary industry classification



According to Pie Chart 4, more than half of the respondents (53 percent) are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 4. Distribution of respondents according to organizational headcount



Part 4. Caveats

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 in various organizations in the United States. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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 between May 14, 2018 and June 4, 2018.

Survey response	Freq	Pct%
Total sampling frame	16,995	100.0%
Total returns	655	3.9%
Rejected surveys	52	0.3%
Final sample	603	3.5%

Screening questions

S1. Does your organization presently deploy, or plan to deploy, AI-based security technologies?	Pct%
Yes, AI for cybersecurity is fully deployed within my company	9%
Yes, AI for cybersecurity is partially deployed (in-process) within my company	14%
Yes, we plan to deploy AI for cybersecurity within the next 12 months	36%
Yes, we plan to deploy AI for cybersecurity more than 12 months from now	41%
We do not have a plan to deploy AI for cybersecurity (stop)	0%
Total	100%

S2. Does your job involve detecting and responding to potentially malicious content or threats targeting your organization's information systems or IT security infrastructure?	Pct%
Yes	89%
No (stop)	11%
Total	100%

S3. [S1=Yes] How familiar are you with your organization's use or planned use of AI for cybersecurity?	Pct%
Very familiar	44%
Familiar	37%
Somewhat familiar	19%
No knowledge (stop)	0%
Total	100%

S4. Do you have any organizational responsibility for evaluating and/or selecting AI-based cybersecurity tools and vendors?	Pct%
Yes, full responsibility	41%
Yes, some responsibility	34%
Yes, minimal responsibility	25%
No responsibility (stop)	0%
Total	100%

Part 1. Background

Q1. What best describes your organization's current stage of maturity in its deployment of AI-based security technologies?	Pct%
Early stage – While AI-based security technologies are planned, they have not as yet been deployed	60%
Middle stage – While AI-based security technologies are planned, they are only partially implemented	26%
Late-middle stage – While AI-based security technologies are mostly implemented, they are subject to tweaks and refinements	9%
Mature stage – AI-based security technologies and decision rules are optimized and in maintenance mode across the enterprise	5%
Total	100%

Please rate each statement using the agreement scale provided below each item.	
Q2a. The deployment of AI-based security technologies simplifies the process of detecting and responding to application security threats and vulnerabilities.	Pct%
Strongly agree	23%
Agree	36%
Unsure	22%
Disagree	11%
Significantly disagree	8%
Total	100%

Q2b. Our organization's use of AI-based security technologies will decrease the workload of IT security personnel.	Pct%
Strongly agree	16%
Agree	18%
Unsure	21%
Disagree	30%
Significantly disagree	15%
Total	100%

Q2c. Our organization needs to simplify and streamline its security architecture to obtain maximum value from AI-based security technologies.	Pct%
Strongly agree	21%
Agree	35%
Unsure	23%
Disagree	13%
Significantly disagree	8%
Total	100%

Q2d. Our organization needs outside expertise to maximize the value of AI-based security technologies.	Pct%
Strongly agree	29%
Agree	28%
Unsure	16%
Disagree	15%
Significantly disagree	12%
Total	100%

Q2e. AI-based security technologies are too immature to provide maximum value for our SecOps team.	Pct%
Strongly agree	17%
Agree	23%
Unsure	22%
Disagree	25%
Significantly disagree	13%
Total	100%

Q2f. It is difficult to integrate AI-based security technologies with legacy systems.	Pct%
Strongly agree	29%
Agree	32%
Unsure	19%
Disagree	12%
Significantly disagree	8%
Total	100%

Q2g. AI-based security technologies will increase our organization's need for in-house expertise and dedicated headcount.	Pct%
Strongly agree	23%
Agree	29%
Unsure	17%
Disagree	17%
Significantly disagree	14%
Total	100%

Q2h. The deployment of AI-based security technologies will increase the productivity of IT security personnel.	Pct%
Strongly agree	27%
Agree	33%
Unsure	23%
Disagree	11%
Significantly disagree	6%
Total	100%

Q2i. Our organization's investment in AI-based security technologies is likely to increase as these technologies become more mature.	Pct%
Strongly agree	30%
Agree	31%
Unsure	19%
Disagree	13%
Significantly disagree	7%
Total	100%

Q2j. In the context of cybersecurity AI-based security technologies will never fully replace human judgment.	Pct%
Strongly agree	27%
Agree	34%
Unsure	15%
Disagree	18%
Significantly disagree	6%
Total	100%

Q2k. My organization is committed to AI-based security technologies as part of its defense in depth strategy.	Pct%
Strongly agree	25%
Agree	34%
Unsure	16%
Disagree	18%
Significantly disagree	7%
Total	100%

Q2l. AI-based technologies provide deeper security than what humans alone can provide.	Pct%
Strongly agree	29%
Agree	31%
Unsure	18%
Disagree	15%
Significantly disagree	7%
Total	100%

Q3a. Using the following 10-point scale, please rate the effectiveness of your organization's security technologies at reducing application security risk.	Pct%
1 or 2	12%
3 or 4	14%
5 or 6	23%
7 or 8	35%
9 or 10	16%
Total	100%
Extrapolated value	6.08

Q3b. How will the use of AI impact the effectiveness of application security activities within your organization?	Pct%
Significant increase in effectiveness	26%
Increase in effectiveness	33%
No change	29%
Decrease in effectiveness	9%
Significant decrease in effectiveness	3%
Total	100%

Q4a. Using the following 10-point scale, please rate the overall complexity of your organization's security architecture.	Pct%
1 or 2 (Low)	8%
3 or 4	10%
5 or 6	15%
7 or 8	33%
9 or 10 (High)	34%
Total	100%
Extrapolated value	7.00

Q4b. How will the use of AI impact the overall complexity of your organization's security architecture?	Pct%
Significant increase in complexity	19%
Increase in complexity	20%
No change	21%
Decrease in complexity	21%
Significant decrease in complexity	19%
Total	100%

Q5. Using the following 10-point scale, please rate your organization's ability to accurately identify areas in your security infrastructure where AI and machine learning would create the most value.	Pct%
1 or 2	13%
3 or 4	18%
5 or 6	23%
7 or 8	25%
9 or 10	21%
Total	100%
Extrapolated value	5.96

Q6. What are the security technologies most likely to be supported by AI? Please select your top 3 choices.	Pct%
Technologies that secure the perimeter	17%
Technologies that provide security intelligence about networks traffic and entities	54%
Technologies that secure workloads and applications	45%
Technologies that identify infected IoT devices and apply remediation	32%
Technologies that simplify the prioritization of threats	39%
Technologies that secure information assets	30%
Technologies that isolate or sandbox malware infections	18%
Technologies that identify and authenticate users	65%
Other (please specify)	0%
Total	300%

Q7. Who are key influencers/decision makers in setting your organization's use of AI-based technologies for cybersecurity? Please select your top 4 choices.	Pct%
AI analyst/domain expert	46%
Application security director	20%
Chief information officer	52%
Chief information security officer/chief security officer	51%
Chief operations officer	5%
Chief risk officer	4%
Chief technology officer	30%
Cybersecurity architect	35%
Development director	11%
External contractor or third party	22%
IT security director	23%
LOB or business unit leader	29%
SOC team (security analysts/incident responders)	35%
No one person or function	37%
Other (please specify)	0%
Total	400%

Q8. How does (or will) AI improve your organization's security posture? Please select all that apply.	Pct%
Accelerates the containment of infected endpoints/devices/hosts	64%
Creates the policies once and updates them everywhere	48%
Decreases the cost of cybersecurity operations	38%
Identifies application security vulnerabilities	60%
Improves the ability to prioritize threats and vulnerabilities	48%
Increases the productivity of current security personnel	53%
Increases the speed of analyzing threats	69%
Provides more in-depth knowledge about security threats	48%
Reduces application security risk	37%
Reduces the complexity of the cyber security architecture	29%
Reduces the false positive and/or false negative rates	45%
Reduces the headcount of IT security personnel	33%
Reduces the manual updating of firewall rules and security policies	29%
Reduces the number of insecure or non-compliant endpoints or things	47%
Reduces the number of security events that must be investigated	49%
Other (please specify)	0%
Total	697%

Q9. Please select the top 2 organizational or governance challenges to successfully deploying AI-based security technologies within your organization.	Pct%
It requires too much staff to implement and maintain AI-based technologies	50%
There is not enough time to integrate AI-based technologies into security workflows	19%
We can't recruit personnel experienced in AI-based technologies	35%
We don't have the internal expertise to validate vendors' claims	45%
There is insufficient budget for AI-based technologies	34%
There is insufficient supervision and oversight of AI learning and decision-making	15%
Other (please specify)	2%
Total	200%

Q10. Which of the following are barriers to the effectiveness of AI-based security technologies used by your organization today? Please select the top 3 factors.	Pct%
AI tools/technology we need are not available	43%
We can't apply AI-based controls that span across the entire enterprise	27%
We can't create a unified view of AI users across the enterprise	23%
There are errors and inaccuracies in AI decision rules	46%
There are errors and inaccuracies in data inputs ingested by AI technology (engine)	41%
There is a heavy reliance on legacy IT environments	19%
There are Interoperability issues among AI technologies	51%
There is a lack of mature and/or stable AI technologies	48%
Other (please specify)	2%
Total	300%

Q11. In the typical week, how many malware alerts does your organization receive?	Pct%
Less than 50	5%
50 to 100	19%
101 to 1,000	18%
1,001 to 5,000	25%
5,001 to 10,000	20%
10,001 to 50,000	6%
50,001 to 100,000	4%
More than 100,000	3%
Total	100%
Extrapolated value	10,765

Q12. In your experience, what percentage of these alerts can be handled by AI without human supervision?	Pct%
None	24%
Less than 10%	12%
10% to 25%	8%
26% to 50%	7%
51% to 75%	14%
76% to 99%	24%
100%	11%
Total	100%
Extrapolated value	45%

Q13. In the typical week, how many zero-day exploits go undetected (i.e., bypassing your organization's SIEM, IPS and AV systems)?	Pct%
Less than 50	12%
50 to 100	32%
101 to 1,000	33%
1,001 to 5,000	18%
5,001 to 10,000	3%
10,001 to 50,000	0%
50,001 to 100,000	2%
More than 100,000	0%
Total	100%
Extrapolated value	2,474

Q14. In your experience, what percentage of these previously "undetectable" zero-day exploits can be detected because of AI?	Pct%
None	10%
Less than 10%	14%
10% to 25%	11%
26% to 50%	26%
51% to 75%	18%
76% to 99%	18%
100%	3%
Total	100%
Extrapolated value	41%

Q15. How many security personnel (including contractors) are dedicated to the investigation and containment of cyber threats and exploits?	Pct%
1 to 5	6%
6 to 10	12%
11 to 20	13%
21 to 25	21%
26 to 50	30%
More than 50	18%
Total	100%
Extrapolated value	30.0

Q16. What percentage of dedicated security personnel (including contractors) have specialized skills relating to the supervision of AI tools and technologies?	Pct%
None	20%
Less than 10%	30%
10% to 25%	20%
26% to 50%	18%
51% to 75%	7%
76% to 99%	3%
100%	2%
Total	100%
Extrapolated value	20%

Q17. On average, how many years of relevant work experience do security personnel (including contractors) who investigate and contain cyber threats and exploits have?	Pct%
1 to 3 years	11%
4 to 6 years	13%
7 to 9 years	33%
10 to 15 years	27%
More than 15 years	16%
Total	100%
Extrapolated value	10.22

Q18. In your organization, what is the average amount of relevant AI work experience your security personnel have?	Pct%
1 to 3 years	55%
4 to 6 years	38%
7 to 9 years	7%
10 to 15 years	0%
More than 15 years	0%
Total	100%
Extrapolated value	3.56

Part 3. Estimating time containing cyber exploits

Q19. Approximately, how many hours each week are spent organizing and planning the organization's approaches to cyber defense? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q19a. Tasks/activities not facilitated by AI	Pct%
None	2%
Less than 5	20%
5 to 10	19%
11 to 25	21%
26 to 50	27%
51 to 100	10%
101 to 250	1%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	25.32

Q19b. Tasks/activities facilitated by AI	Pct%
None	9%
Less than 5	30%
5 to 10	21%
11 to 25	23%
26 to 50	14%
51 to 100	1%
101 to 250	2%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	16.05

Q20. Approximately, how many hours each week are spent capturing actionable intelligence about cyber exploits and malware infections? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q20a. Tasks/activities not facilitated by AI	Pct%
None	0%
Less than 5	5%
5 to 10	18%
11 to 25	21%
26 to 50	25%
51 to 100	14%
101 to 250	8%
251 to 500	5%
More than 500	4%
Total	100%
Extrapolated value	80.20

Q20b. Tasks/activities facilitated by AI	Pct%
None	0%
Less than 5	10%
5 to 10	15%
11 to 25	31%
26 to 50	29%
51 to 100	11%
101 to 250	1%
251 to 500	2%
More than 500	1%
Total	100%
Extrapolated value	41.11

Q21. Approximately, how many hours each week are spent by the cybersecurity or InfoSec team investigating and detecting application vulnerabilities? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q21a. Tasks/activities not facilitated by AI	Pct%
None	0%
Less than 5	3%
5 to 10	2%
11 to 25	7%
26 to 50	13%
51 to 100	22%
101 to 250	21%
251 to 500	23%
More than 500	9%
Total	100%
Extrapolated value	195.88

Q21b. Tasks/activities facilitated by AI	Pct%
None	0%
Less than 5	3%
5 to 10	6%
11 to 25	31%
26 to 50	20%
51 to 100	25%
101 to 250	11%
251 to 500	2%
More than 500	2%
Total	100%
Extrapolated value	70.48

Q22. Approximately, how many hours each week are spent evaluating actionable intelligence about cyber exploits or malware? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q22a. Tasks/activities not facilitated by AI	Pct%
None	0%
Less than 5	6%
5 to 10	11%
11 to 25	35%
26 to 50	20%
51 to 100	13%
101 to 250	10%
251 to 500	2%
More than 500	3%
Total	100%
Extrapolated value	66.28

Q22b. Tasks/activities facilitated by AI	Pct%
None	5%
Less than 5	16%
5 to 10	33%
11 to 25	27%
26 to 50	13%
51 to 100	3%
101 to 250	1%
251 to 500	2%
More than 500	0%
Total	100%
Extrapolated value	24.23

Q23. Approximately, how many hours each week are spent cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by cyber exploits or malware? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q23a. Tasks/activities not facilitated by AI	Pct%
None	0%
Less than 5	3%
5 to 10	7%
11 to 25	7%
26 to 50	11%
51 to 100	14%
101 to 250	23%
251 to 500	21%
More than 500	14%
Total	100%
Extrapolated value	212.89

Q23b. Tasks/activities facilitated by AI	Pct%
None	2%
Less than 5	23%
5 to 10	18%
11 to 25	15%
26 to 50	26%
51 to 100	9%
101 to 250	4%
251 to 500	3%
More than 500	0%
Total	100%
Extrapolated value	39.63

Q24. Approximately, how many hours each week are spent documenting and/or reporting upon the cyber event (in conformance with policies or compliance mandates)? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q24a. Tasks/activities not facilitated by AI	Pct%
None	8%
Less than 5	18%
5 to 10	13%
11 to 25	34%
26 to 50	21%
51 to 100	3%
101 to 250	2%
251 to 500	1%
More than 500	0%
Total	100%
Extrapolated value	25.07

Q24b. Tasks/activities facilitated by AI	Pct%
None	12%
Less than 5	27%
5 to 10	23%
11 to 25	21%
26 to 50	11%
51 to 100	5%
101 to 250	1%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	15.91

Q25. Approximately, **how much time is wasted** because alerts are erroneous (i.e., false positives)? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q25a. Tasks/activities not facilitated by AI	Pct%
None	0%
Less than 5	0%
5 to 10	0%
11 to 25	2%
26 to 50	7%
51 to 100	0%
101 to 250	13%
251 to 500	31%
More than 500	47%
Total	100%
Extrapolated value	400.83

Q25b. Tasks/activities facilitated by AI	Pct%
None	6%
Less than 5	14%
5 to 10	16%
11 to 25	30%
26 to 50	14%
51 to 100	12%
101 to 250	5%
251 to 500	3%
More than 500	0%
Total	100%
Extrapolated value	41.42

Q26. Approximately, how much downtime occurs each week because the cleaning, fixing or patching of malware-infected networks, applications and devices cause unplanned downtime? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q26a. Tasks/activities not facilitated by AI	Pct%
Less than 1	12%
1 to 2	26%
3 to 4	28%
5 to 6	19%
7 to 8	10%
9 to 10	2%
11 to 15	1%
More than 15	2%
Total	100%
Extrapolated value	3.95

Q26b. Tasks/activities facilitated by AI	Pct%
Less than 1	32%
1 to 2	38%
3 to 4	25%
5 to 6	4%
7 to 8	1%
9 to 10	0%
11 to 15	0%
More than 15	0%
Total	100%
Extrapolated value	1.90

Q27. What is the likelihood of a **data breach** involving 10,000 or more records containing sensitive or confidential personal information of customers or consumers (users) within the next 12 months? Your best guess is welcome.	
Q27a. Tasks/activities not facilitated by AI	Pct%
Less than 1%	0%
1 to 2%	0%
3 to 4%	3%
5 to 6%	7%
7 to 8%	11%
9 to 10%	11%
11 to 20%	28%
More than 20%	40%
Total	100%
Extrapolated value	16.6%

Q27b. Tasks/activities facilitated by AI	Pct%
Less than 1%	4%
1 to 2%	9%
3 to 4%	15%
5 to 6%	16%
7 to 8%	20%
9 to 10%	25%
11 to 20%	9%
More than 20%	2%
Total	100%
Extrapolated value	7.3%

Part 5. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive/VP	5%
Director	15%
Manager	21%
Supervisor	14%
Technician	33%
Staff/Analyst	6%
Consultant	2%
Contractor	4%
Other	0%
Total	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	Pct%
CEO/Executive Committee	2%
Chief Operating Officer	1%
Chief Financial Officer	0%
General Counsel	2%
Chief Information Officer	40%
Chief Information Security Officer	20%
Compliance Officer	3%
Chief Technology Officer	9%
Line of business (LoB) management	15%
Chief Security Officer	1%
Analytics/Data Science Leader	3%
Data Center Management	2%
Chief Risk Officer	2%
Other	0%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	1%
Financial services	18%
Health & pharmaceutical	11%
Industrial & manufacturing	10%
Public sector	10%
Retail	9%
Services	11%
Technology & software	8%
Transportation	3%
Other	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 500	13%
500 to 1,000	14%
1,001 to 5,000	20%
5,001 to 10,000	15%
10,001 to 25,000	13%
25,001 to 50,000	10%
50,001 to 75,000	8%
More than 75,000	7%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 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.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.