



The Challenge of Building the Right Security Automation Architecture

Sponsored by Juniper

Independently conducted by Ponemon Institute LLC

Publication Date: June 2018

The Challenge of Building the Right Security Automation Architecture

Prepared by Ponemon Institute, June 2018

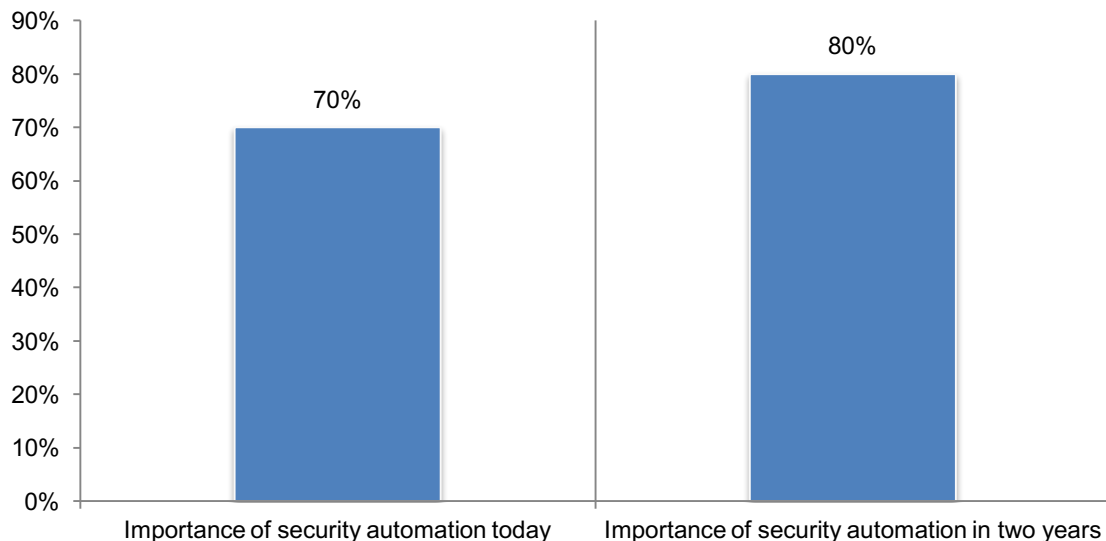
Part 1. Introduction

Security automation architecture can improve organizations' security posture by augmenting or replacing human intervention in the identification and containment of cyber exploits or breaches through the use of such technologies as artificial intelligence, machine learning, analytics and orchestration. Sponsored by Juniper, the purpose of this research is to understand the challenges companies face when deciding how, when and where to implement the right automation capabilities in order to improve productivity, reduce costs, scale to support cloud deployments and ultimately strengthen the security posture of the business.

Ponemon Institute surveyed 1,859 IT and IT security practitioners in Germany, France, the United Kingdom and the United States. All participants in this research are in organizations that presently deploy or plan to deploy security automation tools or applications and are familiar with their organizations use of security automation and have some responsibility for evaluating and/or selecting security automation technologies and vendors.

Security automation improves organizations' security posture. When asked to rate the importance of security automation on a scale of 1 = not important to 10 = very important, 70 percent of respondents say security automation is very important to their organizations' security posture and 80 percent of respondents rate the importance as very high in the next two years, as shown in Figure 1.

Figure 1. The importance of security automation to achieving a strong security posture
1 = not important to 10 = high importance, 7+ responses reported



Following are key takeaways from this research.

- **Security automation improves productivity and the ability to address the volume of threats.** The top two benefits of security automation are the increased productivity of IT security personnel and the automated correlation of threat behavior to address the volume of threats (64 percent and 60 percent of respondent, respectively). Fifty-four percent of respondents say these technologies simplify the process of detecting and responding to cyber threats and vulnerabilities.

- **Incident response, security analytics and malware investigation are the tasks most likely to be automated.** Fifty-nine percent of respondents say the tasks or processes that will be automated are incident response, security analytics and malware investigation. This is followed by threat intelligence (55 percent of respondents).
- **Automation improves organizations' ability to quickly analyze and prioritize threats and vulnerabilities.** The two primary improvements from automation is the ability to prioritize threats and vulnerabilities and an increase in the speed of analyzing threats, according to 64 percent of respondents. This is followed by the reduction in the false positive and/or false negative rate.
- **SIEM plus automation equals a stronger security posture.** Seventy-seven percent of respondents say they would like the ability to automate some of the daily manual tasks involved in using their SIEM, including the processing of alerts, events and logs. Sixty-six percent of respondents say this would result in a stronger security posture and 59 percent say it would improve productivity.
- **The integration of disparate security technologies is the biggest challenge to achieving an effective security automation architecture.** Seventy-one percent of respondents say the ability to integrate disparate security is the main challenge to achieving an effective security automation architecture. Ensuring the high availability of IT services and recruiting and retaining qualified personnel are also main challenges, according to 56 percent and 51 percent of respondents, respectively.
- **Complexity and knowing where to implement security automation are challenges to the use of security automation.** While security automation is considered important, 67 percent of respondents say the overall complexity of their organizations' security automation is very high. Furthermore, only 27 percent rate their ability to accurately identify areas in their security infrastructure where automation would create the most value, as high.
- **A lack of skilled personnel is the biggest barrier to successfully deploying security automation.** Fifty-seven percent of respondents say they are unable to recruit knowledgeable or skilled personnel to deploy their security automation tools. This barrier is followed by the inability to apply controls that span the entire enterprise, according to 55 percent of respondents.
- **Integration with legacy systems is difficult for many organizations.** Sixty-three percent of respondents say it is difficult to integrate security automation technologies and tools with legacy systems. Moreover, only 35 percent of respondents say their organizations have the in-house expertise to be effective in using security automation to respond to malicious threats. To be able to get the maximum value from security automation technologies, 59 percent of respondents say their organization needs to simplify and streamline the number of vendors in their architecture.
- **Lack of in-house experts diminishes the effectiveness of security within their organizations.** Sixty-two percent of respondents say the lack of in-house experts diminishes their organizations' security posture. Other negative effects on security posture are interoperability issues among security technologies and an increase in the severity and frequency of cyberattacks (57 percent, 55 percent and 54 percent, respectively).
- **Endpoint security and firewalls are mainly used to detect advanced threats targeting the network.** Sixty-three percent of respondents say their organizations have deployed or plan to deploy security technology specifically designed to detect advanced threats that have bypassed their perimeter defense and gained access to their network. Endpoint security and firewalls are primarily used to detect advanced threats (68 percent and 67 percent of respondents, respectively). Sixty-three percent of respondents say they detect advanced

threats by analyzing various logs, events and alerts. On average, organizations' security teams are spending almost two hours (115.5 minutes) each day processing alerts, events and logs to determine if any malicious activity is taking place inside their networks.

- **Companies will be migrating more data to the cloud in the next 12 months.** Sixty percent of respondents say their organization will be migrating more data to the cloud during the next year. Thirty-seven percent of respondents say their organization stores business-critical applications and data on-premises and 33 percent say they store such data both on-premises and in the cloud. Thirty-six percent of respondents say they manage all the security in the cloud and 30 percent say security is co-managed with a cloud service provider.
- **Deployment of SIEM helps in identifying advanced threats.** Forty-five percent of respondents say their organization uses SIEM and 78 percent of these respondents say it is extremely or somewhat helpful in identifying advanced threats within their organizations' network. Sixty-three percent of respondents say they use SIEM as a security platform that helps identify potentially malicious network activity and 45 percent of respondents say they use it to collect and store data required for compliance reporting.
- **What solutions are most effective in helping organizations identify advanced threats?** The top three security products deployed in organizations are: identity and access management (79 percent of respondents), endpoint solutions (69 percent of respondents) and IPS (57 percent of respondents). Forty-five percent of respondents say endpoint solutions are effective in identifying never-before-seen threats. Endpoint solutions are most often used to generate alerts, events or logs for their security team to analyze (44 percent of respondents).
- **Automation technologies that secure information assets and authenticate users are considered to be the most important.** Forty-nine percent of respondents say technologies that automate the security of information assets and the identification and authentication of users are most important. Forty-six percent of respondents say the automation of secure workloads and applications in the cloud is most important.
- **Business objectives are more likely than regulations to influence the design of security information architecture.** Seventy-one percent of respondents say business objectives have a very significant or significant influence in the design of their organizations' security automation architecture. Fifty-nine percent of respondents say compliance with policies, laws and regulations influence the design of the security automation architecture.
- **IT operations and IT security are the key influencers in the design of their organizations' security automation architecture.** The CIO, CISO and SOC team (53 percent, 51 percent and 41 percent of respondents, respectively) are the key influencers and decision makers of their organization's security automation architecture.
- **To determine effectiveness, organizations measure how much money security automation saves due to an increase in productivity.** Fifty-nine percent of respondents say a metric that shows how much money was saved due to productivity gains is most often used to show the effectiveness of security automation. This metric is followed by the ability to decrease security risk and reduction in the mean time to identify an attack (MTTI) according to 59 percent, 45 percent and 42 percent of respondents, respectively.

Part 2. Key findings

In this section, we provide a deeper analysis of the key findings. The full research results are presented in the appendix of this report. We have organized the findings according to the following themes:

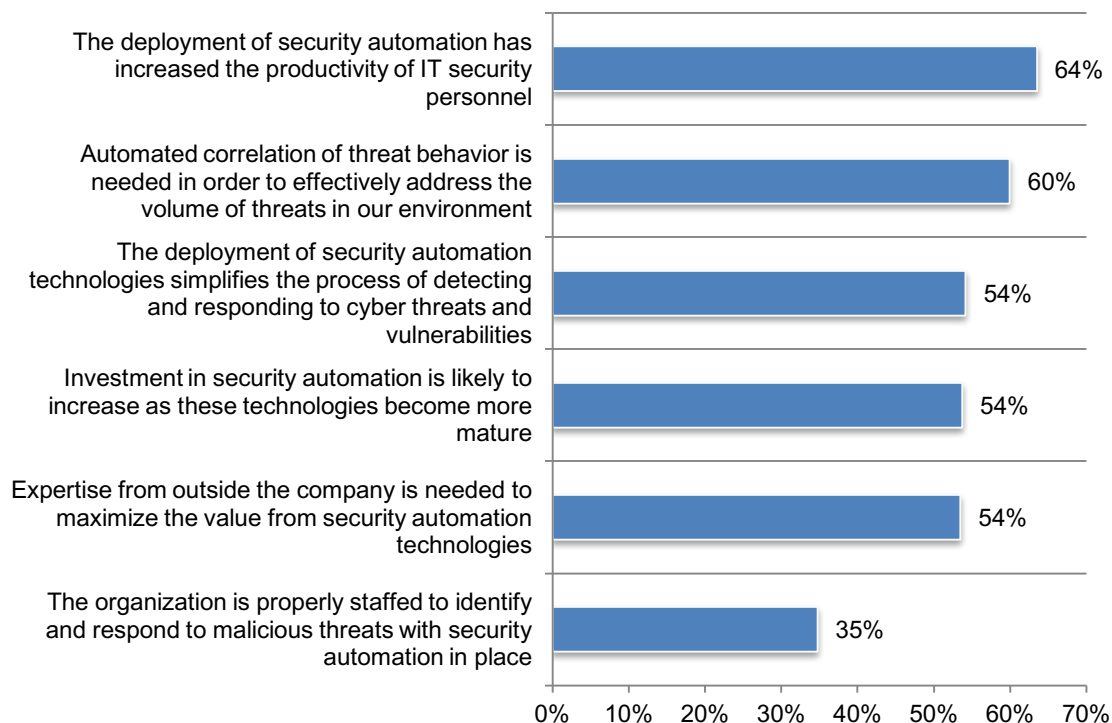
- The importance of security automation to cybersecurity
- Challenges and barriers to security automation adoption
- The effect of security practices on mitigating threats
- How companies are implementing security automation architecture

The importance of security automation to cybersecurity

Security automation improves productivity and the ability to address the volume of threats. Respondents recognize the growing importance of security automation and how it improves security posture. As shown in Figure 2, the top two benefits of security automation are the increased productivity of IT security personnel and the automated correlation of threat behavior to address the volume of threats (64 percent and 60 percent of respondent, respectively). Fifty-four percent of respondents say these technologies simplify the process of detecting and responding to cyber threats and vulnerabilities.

Figure 2. Reasons to deploy security automation technologies

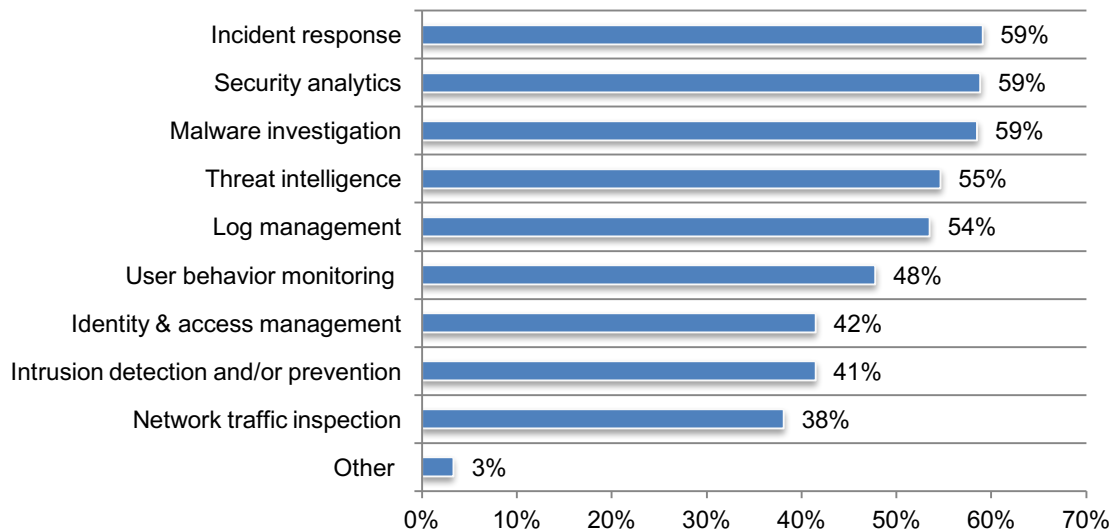
Strongly agree and Agree responses combined



Incident response, security analytics and malware investigation are the tasks most likely to be automated. As shown in Figure 3, 59 percent of respondents say the tasks or processes that will be automated are incident response, security analytics and malware investigation. This is followed by threat intelligence (55 percent of respondents). Sixty-nine percent of respondents say they specifically use or plan to use automation tools to analyze, correlate and consolidate various events, logs and alerts into actionable information on advanced threats.

Figure 3. What processes are, or will be, automated within their organization?

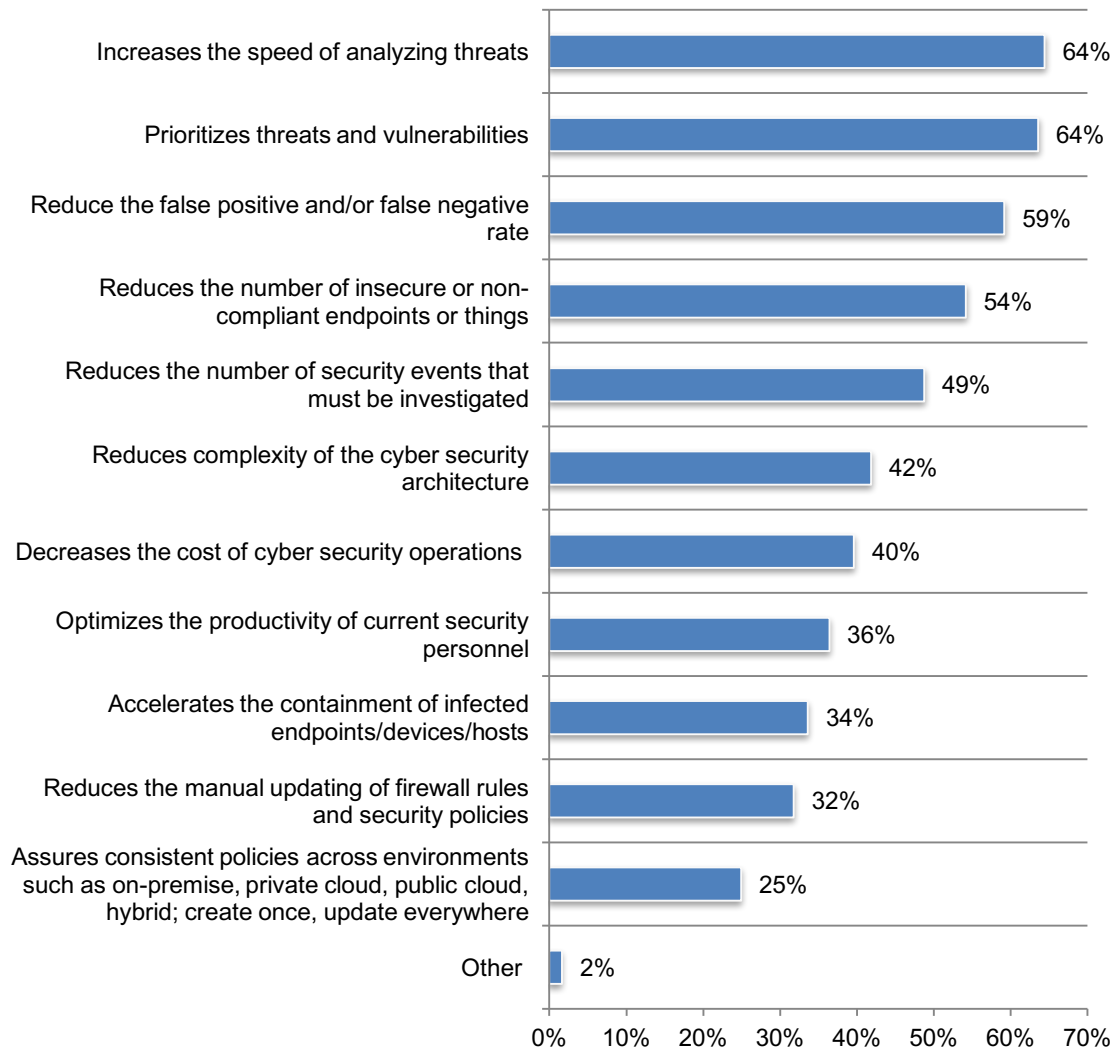
More than one response allowed



Automation improves organizations' ability to quickly analyze and prioritize threats and vulnerabilities. According to Figure 4, 64 percent of respondents note that the two primary improvements from automation is the ability to prioritize threats and vulnerabilities, and an increase in the speed of analyzing threats. This is followed by the reduction in the false positive and/or false negative rate.

Figure 4. How security automation improves security posture

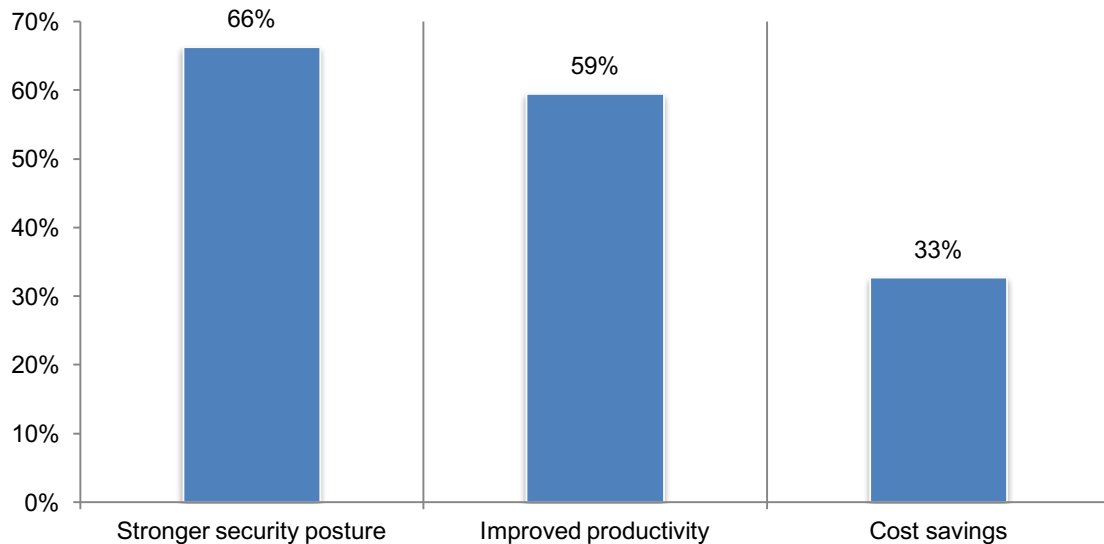
Five responses allowed



SIEM plus automation equal a stronger security posture. Seventy-seven percent of respondents say they would like the ability to automate some of the daily manual tasks involved in using their SIEM, including processing alerts, events and logs. According to Figure 5, 66 percent of respondents say this would result in a stronger security posture and 59 percent say it would improve productivity.

Figure 5. What benefits would you expect from automation of manual attacks involved in using SIEM?

More than one response allowed



The budget for security automation will increase significantly over the next two years.

Table 1 presents the average budget for security automation in the current year and the next two years. As discussed previously, 54 percent of respondents believe investment in security automation will increase as these technologies become more mature.

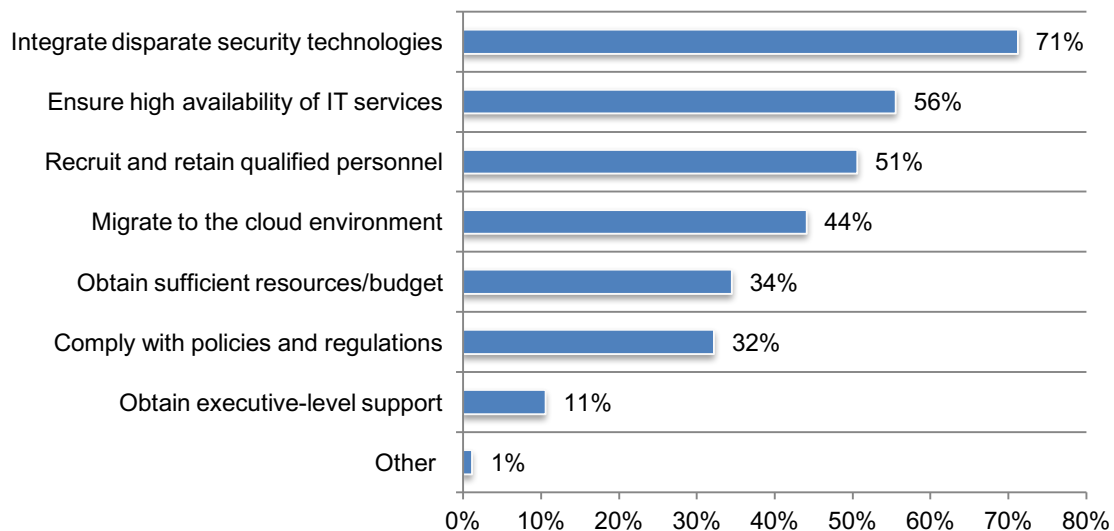
Table 1. Budget for security automation (\$millions)	Budget
Current annual budget for IT security activities	\$13.9
Current IT security budget allocated for security automation (an average of 28 percent)	\$3.9
IT security budget allocated for security automation in the next two years (an average of 38 percent)	\$5.3

Challenges and barriers to security automation adoption

The integration of disparate security technologies is the biggest challenge to achieving an effective security automation architecture. According to Figure 6, 71 percent of respondents say the ability to integrate disparate security is the main challenge to achieving an effective security automation architecture. Ensuring the high availability of IT services and recruiting and retaining qualified personnel are also main challenges, according to 56 percent and 51 percent of respondents, respectively.

Figure 6. What are the main challenges your organization faces to achieve an effective security automation architecture?

Three responses allowed

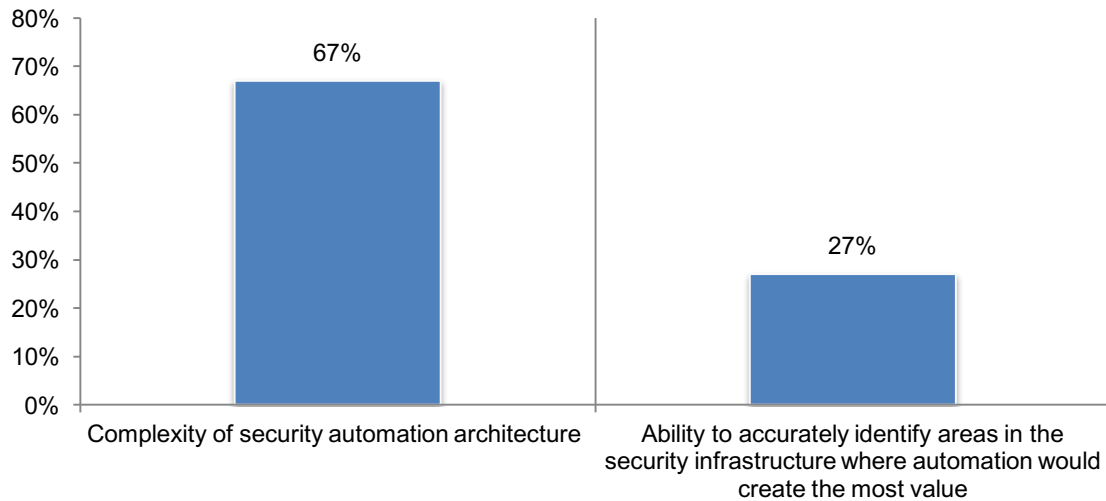


Complexity and knowing where to implement security automation are challenges to the use of security automation. Respondents were asked to rate the complexity of security automation architecture and the ability to identify areas in the security infrastructure where automation would create the most value from a scale of 1 = low complexity/ability to 10 = high complexity/ability.

While security automation is considered important, 67 percent of respondents say the overall complexity of their organizations' security automation is very high, as shown in Figure 7. Furthermore, only 27 percent rate their ability to accurately identify areas in their security infrastructure where automation would create the most value, as high.

Figure 7. Complexity of security automation architecture and the ability to identify areas where automation would create the most value

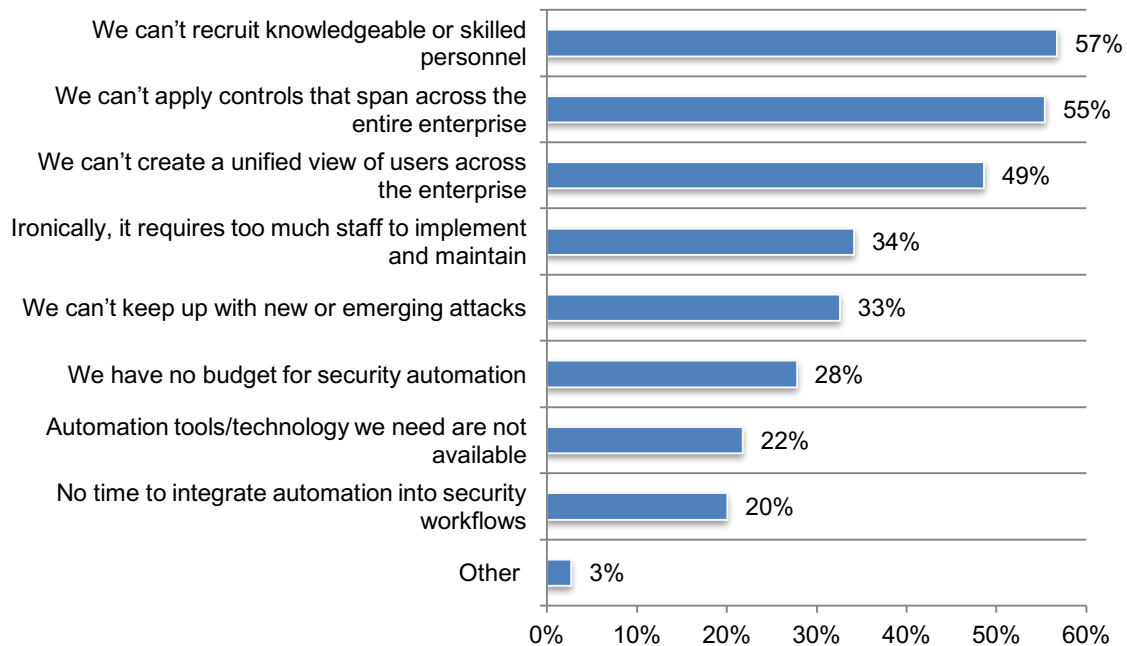
1 = low complexity/ability to 10 = highest complexity/ability, 7+ responses reported



A lack of skilled personnel is the biggest barrier to successfully deploying security automation. According to Figure 8, 57 percent of respondents say they are unable to recruit knowledgeable or skilled personnel to deploy their security automation tools. This barrier is followed by the inability to apply controls that span the entire enterprise, according to 55 percent of respondents.

Figure 8. Barriers to successfully deploying security automation

Three responses allowed

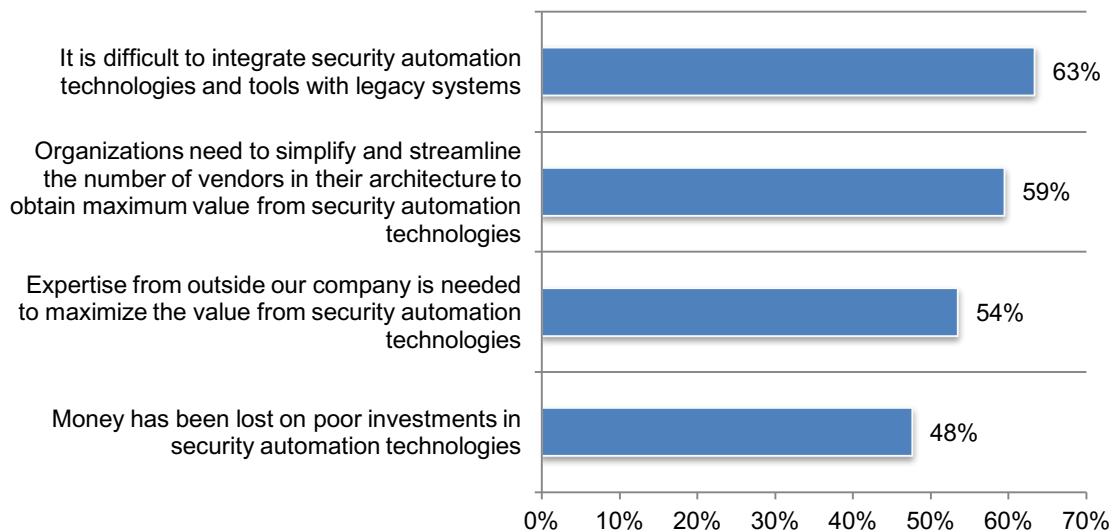


Integration with legacy systems is difficult for many organizations. As shown in Figure 9, 63 percent of respondents say it is difficult to integrate security automation technologies and tools with legacy systems. Moreover, only 35 percent of respondents say their organizations have the in-house expertise to be effective in using security automation to respond to malicious threats.

To be able to get the maximum value from security automation technologies, 59 percent of respondents say their organization needs to simplify and streamline the number of vendors in their architecture. Almost half of respondents (48 percent) say their organizations have lost money on poor investments in security automation technologies.

Figure 9. Difficulties in implementing security automation

Strongly agree and Agree responses combined

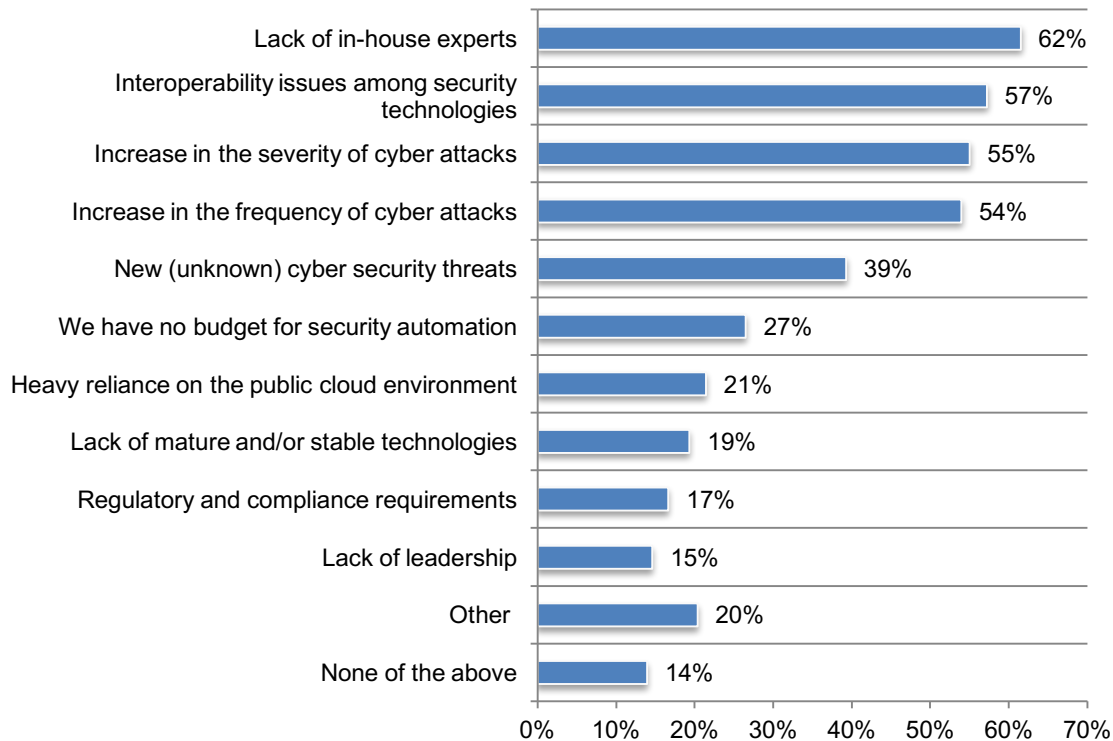


The effect of security practices on mitigating threats

Lack of in-house experts diminishes the effectiveness of security within their organizations. As shown in Figure 10, 62 percent of respondents say the lack of in-house experts diminishes their organizations' security posture. Other negative effects on security posture are interoperability issues among security technologies and an increase the severity and frequency of cyberattacks (57 percent, 55 percent and 54 percent, respectively).

Figure 10. Factors that diminish the effectiveness of security

Four responses allowed

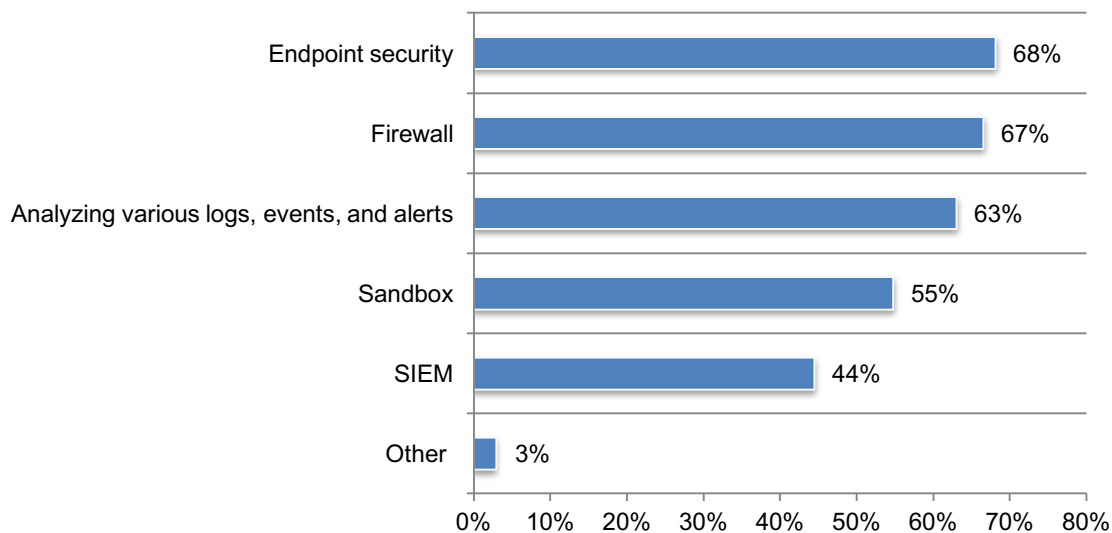


Endpoint security and firewalls are mainly used to detect advanced threats targeting the network. Sixty-three percent of respondents say their organizations have deployed or plan to deploy security technology specifically designed to detect advanced threats that have bypassed their perimeter defense and gained access to their network.

As shown in Figure 11, endpoint security and firewalls are primarily used to detect advanced threats (68 percent and 67 percent of respondents, respectively). Sixty-three percent of respondents say they detect advanced threats by analyzing various logs, events and alerts.

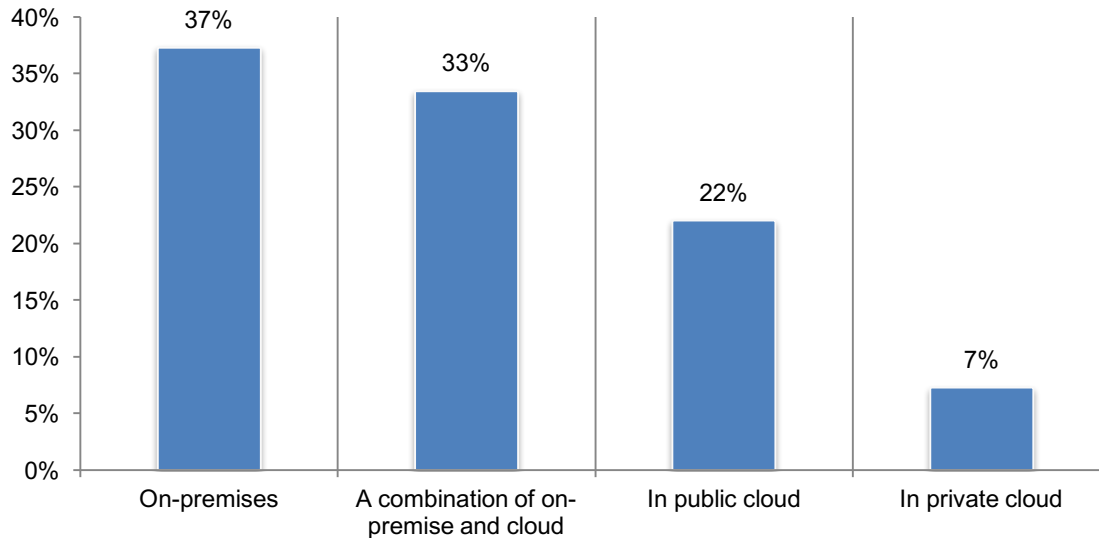
On average, organizations' security teams are spending almost two hours (115.5 minutes) each day processing alerts, events and logs to determine if there is any malicious activity is taking place inside their networks.

Figure 11. How do you detect advanced threats targeting your organization's network?



Companies will be migrating more data to the cloud in the next 12 months. Sixty percent of respondents say their organization will be migrating more data to the cloud in the next year. As shown in Figure 12, 37 percent of respondents say their organization stores business-critical applications and data on-premises and 33 percent say they store such data both on-premises and in the cloud. Thirty-six percent of respondents say they manage all the security in the cloud and 30 percent say security is co-managed with a cloud service provider.

Figure 12. Where do you store your business-critical applications and data?

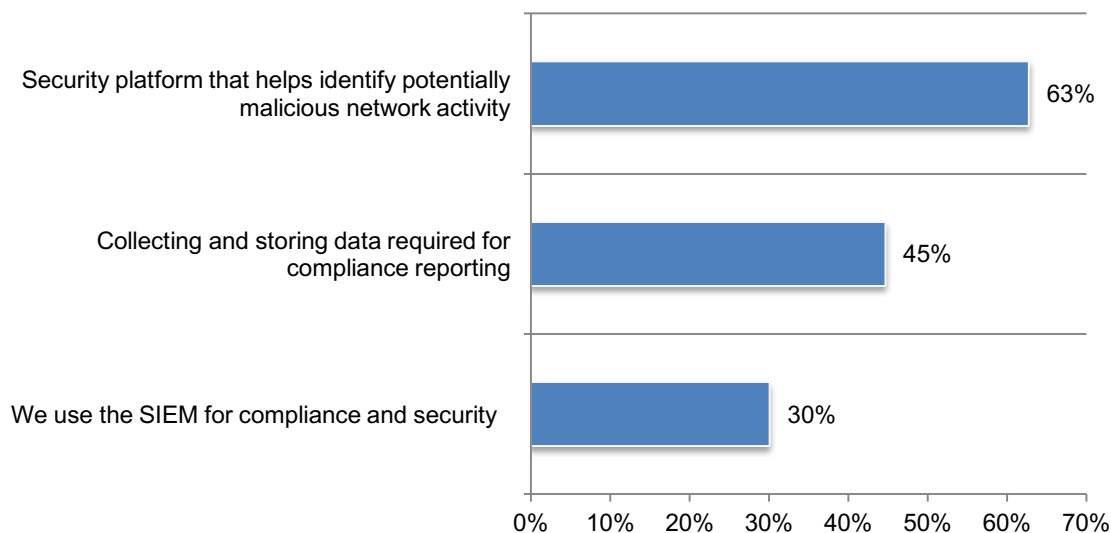


Deployment of SIEM helps in identifying advanced threats. Forty-five percent of respondents say their organization uses SIEM and 78 percent of these respondents say it is extremely or somewhat helpful in identifying advanced threats within their organizations' network.

As shown in Figure 13, 63 percent of respondents say they use SIEM as a security platform that helps identify potentially malicious network activity and 45 percent of respondents say they use it to collect and store data required for compliance reporting.

Figure 13. Which of the following best describes your organization's use of SIEM?

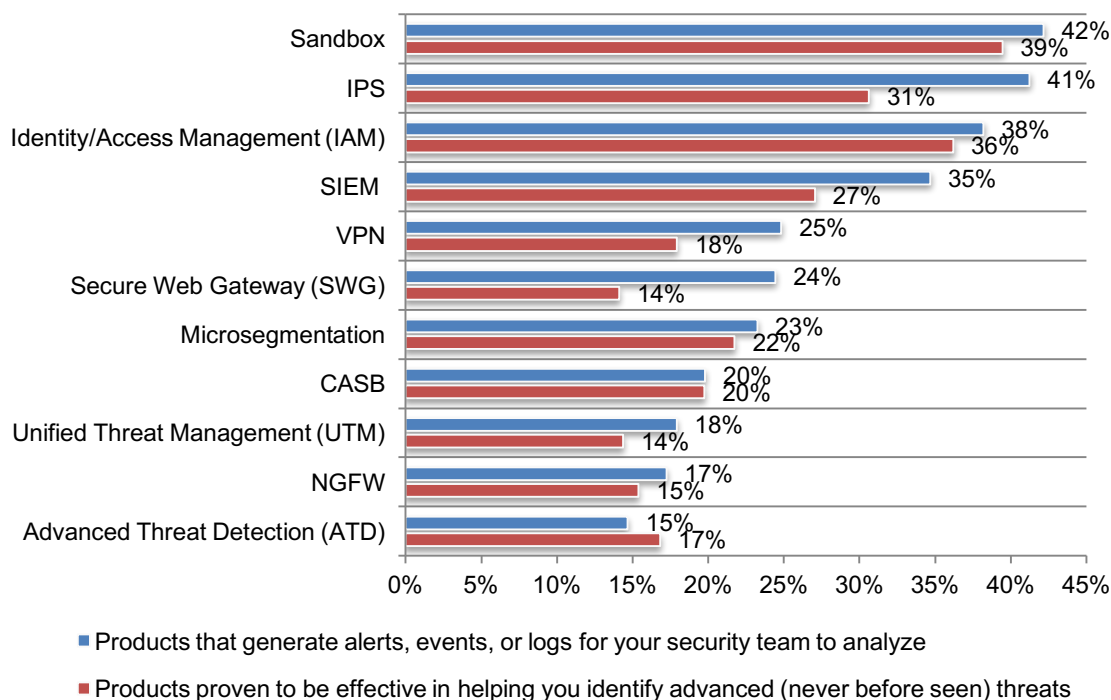
More than one response allowed



What solutions are most effective in helping organizations identify advanced threats? As shown in Figure 14, the top three security products deployed in organizations are: identity and access management (79 percent of respondents), endpoint solutions (69 percent of respondents) and IPS (57 percent of respondents). Forty-five percent of respondents say endpoint solutions are effective in identifying never-before-seen threats. Endpoint solutions are most often used to generate alerts, events or logs for their security team to analyze (44 percent of respondents).

Figure 14. Products used to generate alerts, events or logs and which ones are most effective

More than one response allowed

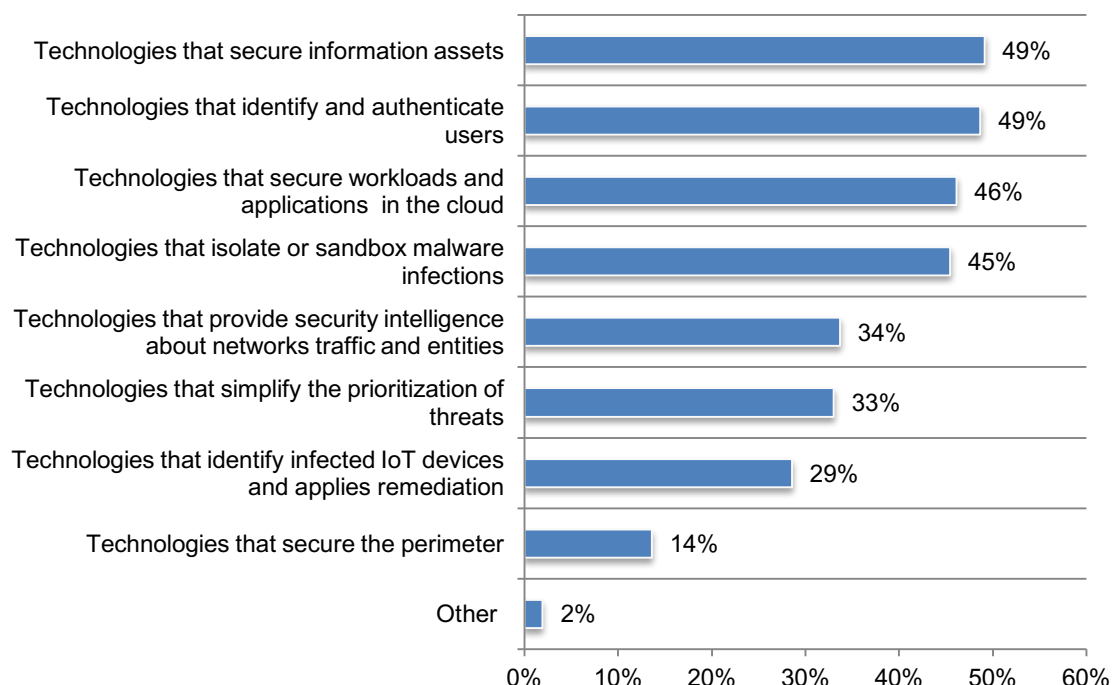


How companies are implementing security automation architecture

Automation technologies that secure information assets and authenticate users are considered the most important. As shown in Figure 15, 49 percent of respondents say technologies that automate the security of information assets and the identification and authentication of users are most important. Forty-six percent of respondents say the automation of secure workloads and applications in the cloud is most important.

Figure 15. What are the most important security automation technologies to minimize cyber threats?

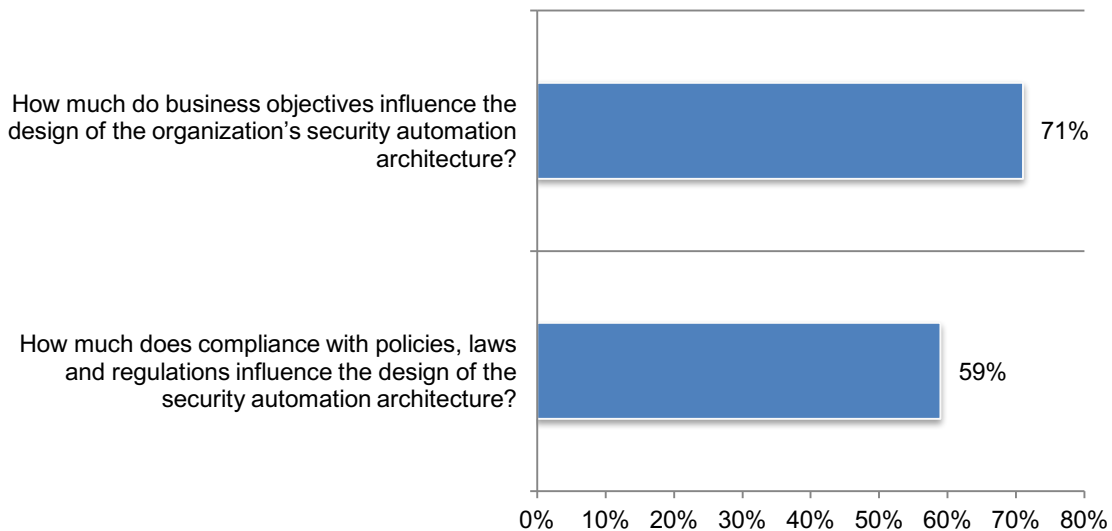
Three responses allowed



Business objectives are more likely than regulations to influence the design of security information architecture. According to Figure 16, 71 percent of respondents say business objectives have a very significant or significant influence in the design of their organizations' security automation architecture. Fifty-nine percent of respondents say compliance with policies, laws and regulations influence the design of the security automation architecture.

Figure 16. The influence of compliance and business objectives on security automation architecture

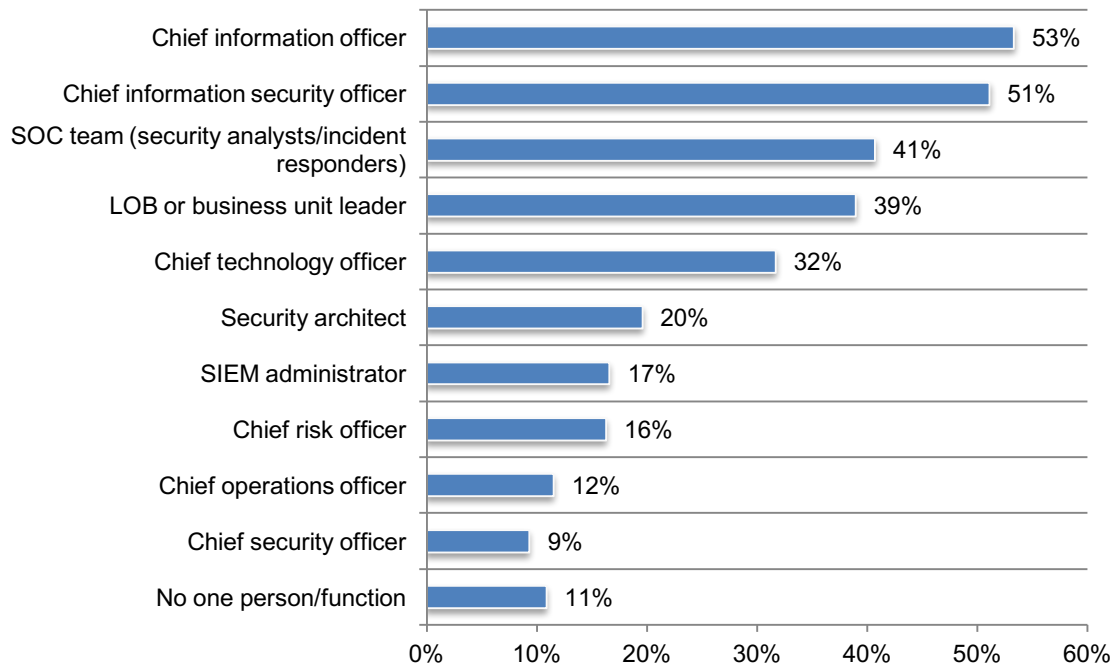
Very significant influence and Significant influence responses combined



IT operations and IT security are the key influencers in the design of their organizations' security automation architecture. As shown in Figure 17, the CIO, CISO and SOC team (53 percent, 51 percent and 41 percent of respondents, respectively) are the key influencers and decision makers of their organization's security automation architecture.

Figure 17. Who are the key influencers/decision makers in setting their organization's security automation architecture?

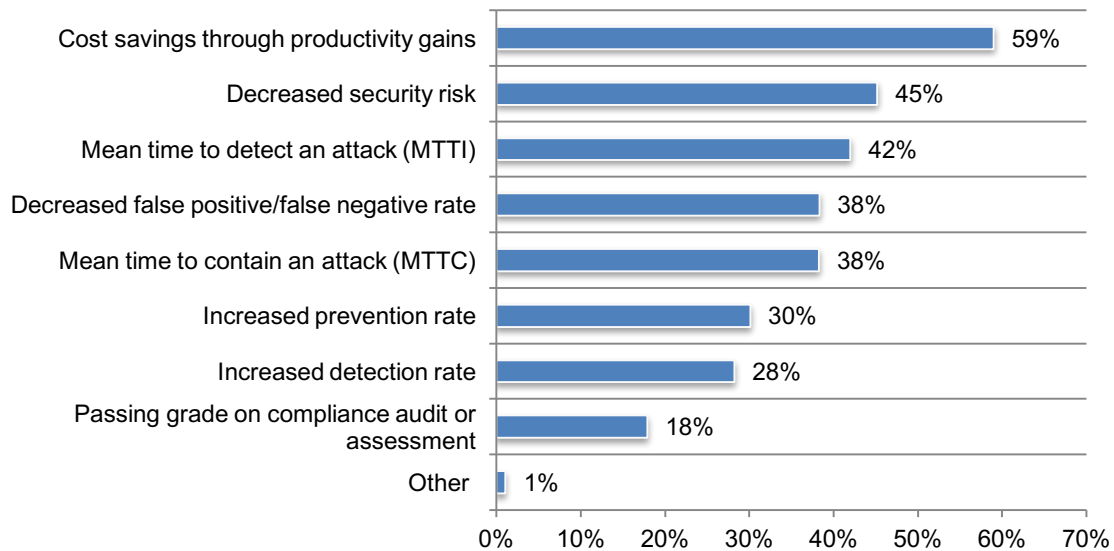
Three responses allowed



To determine effectiveness, organizations measure how much money security automation saves due to an increase in productivity. According to Figure 18, 59 percent of respondents say a metric that shows how much money was saved due to productivity gains is most often used to show the effectiveness of security automation. This metric is followed by the ability to decrease security risk and reduction in the mean time to identify an attack (MTTI) according to 59 percent, 45 percent and 42 percent of respondents, respectively.

Figure 18. What metrics are used to determine the effectiveness of your organization's security automation architecture?

Three responses allowed



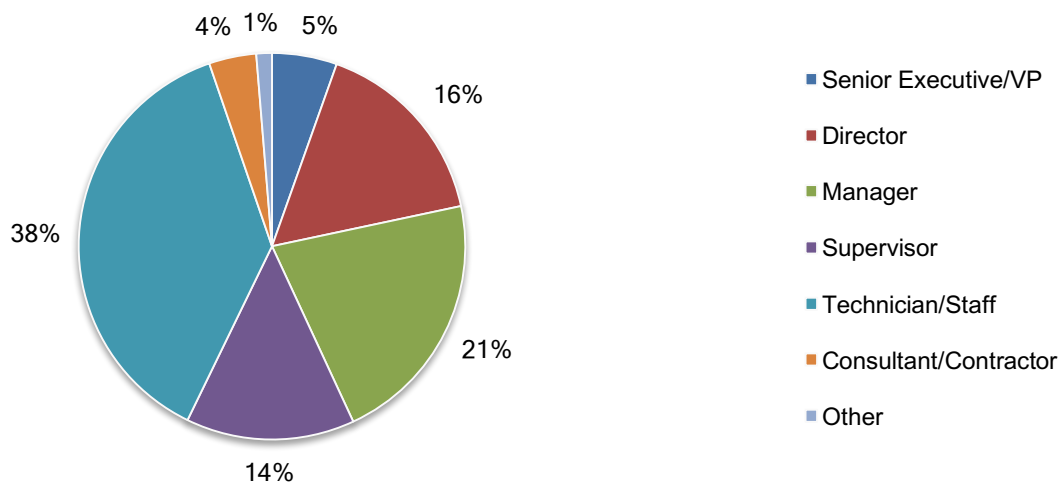
Part 3. Methods

The sampling frame is composed of 51,269 IT and IT security practitioners located in Germany, France, the United Kingdom and the United States, and who are familiar with their organizations use of security automation and have some responsibility for evaluating and/or selecting security automation technologies and vendors. Table 2 reveals that 2,055 respondents completed the survey. Screening removed 196 surveys. The final sample was 1,859 surveys or a 3.6 percent response rate.

Table 2. Sample response	US	UK	DE	FR	Global
Total sampling frame	17,633	11,090	11,557	10,989	51,269
Total returns	715	443	472	425	2,055
Rejected or screened surveys	57	46	38	55	196
Final sample	658	397	434	370	1,859
Response rate	3.7%	3.6%	3.8%	3.4%	3.6%

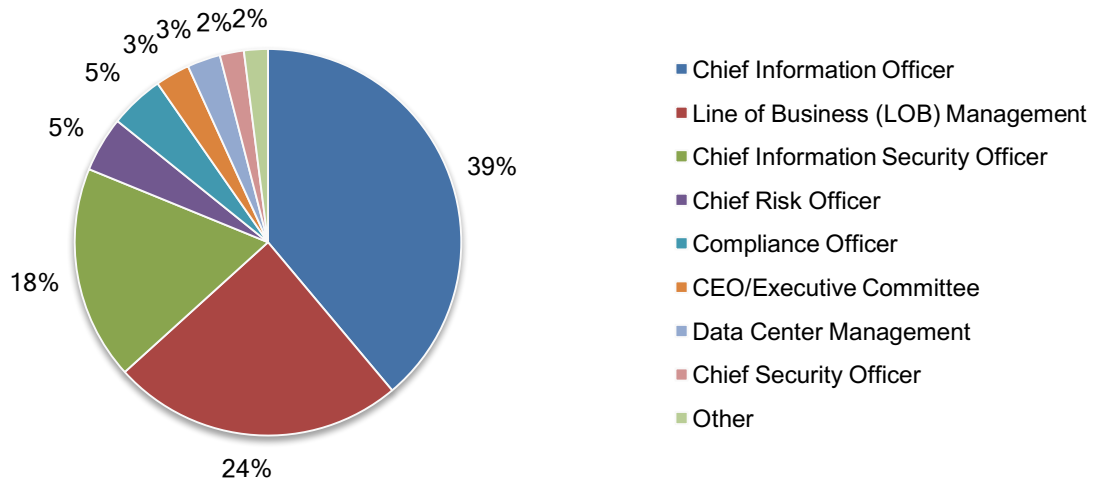
Pie Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (56 percent) reported their current position as supervisory or above.

Pie Chart 1. Distribution of respondents according to position level



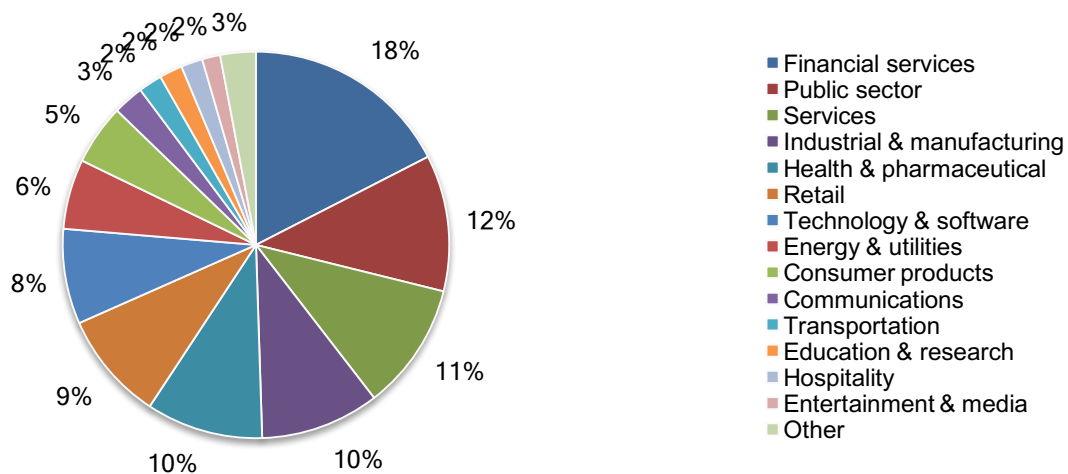
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Thirty-nine percent of respondents identified the chief information officer as the person to whom they report. Another 24 percent of respondents indicated they report directly to the line of business management, and 18 percent of respondents report to the chief information security officer.

Pie Chart 2. Distribution of respondents according to reporting channel



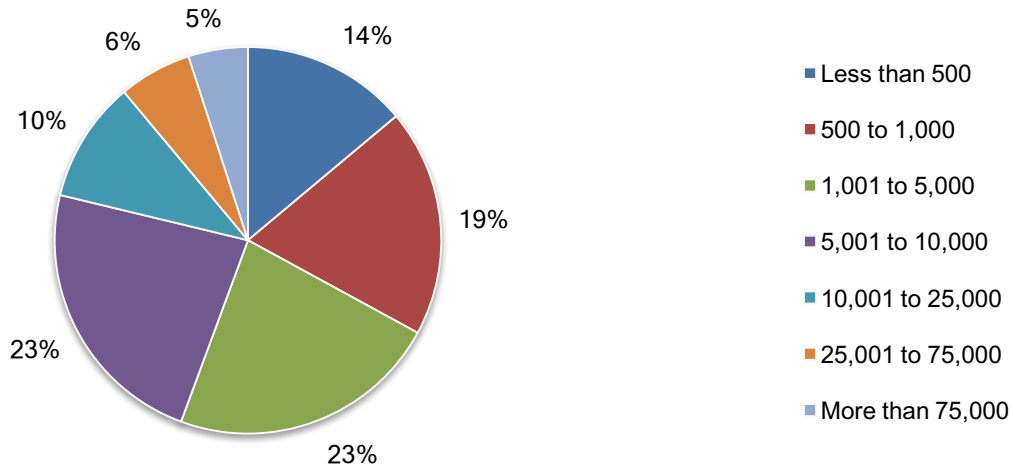
Pie Chart 3 displays the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by public sector (12 percent of respondents), services sector (11 percent of respondents), industrial and manufacturing sector (10 percent of respondents) and health and pharmaceuticals 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 (67 percent) are from organizations with a global headcount of more than 1,000 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, the United Kingdom, Germany and France. 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 March 29 and April 9, 2018.

Survey response	Consolidated
Total sampling frame	51,269
Total returns	2,055
Rejected surveys	196
Final sample	1,859
Response rate	3.6%
Sample weights	1.00

Part 1. Screening questions

S1. Does your organization presently deploy, or plan to deploy, security automation tools or applications?	Consolidated
Yes, security automation is currently deployed within my company	22%
Yes, we plan to deploy security automation within the next 12 months	41%
Yes, plan to deploy security automation more than 12 months from now	37%
No (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 infrastructure?	Consolidated
Yes	100%
No (stop)	0%
Total	100%

S3. How familiar are you with your organization's use of security automation?	Consolidated
Very familiar	31%
Familiar	37%
Somewhat familiar	32%
No knowledge (stop)	0%
Total	100%

S4. Do you have any responsibility for evaluating and/or selecting security automation technologies and vendors?	Consolidated
Yes, full responsibility	29%
Yes, some responsibility	55%
Yes, minimum responsibility	16%
No responsibility (stop)	0%
Total	100%

Part 2. Background questions on threat detection and automation

Q1. What tasks/processes are, or will be, automated within your organization? Please check all that apply.	Consolidated
Log management	54%
Network traffic inspection	38%
Incident response	59%
Intrusion detection and/or prevention	41%
Identity & access management	42%
Malware investigation	59%
Threat intelligence	55%
Security analytics	59%
User behavior monitoring	48%
Other (please specify)	3%
Total	457%

Q2a. Have you deployed security technology specifically designed to detect advanced threats that have bypassed your perimeter defense and gained access to your network?	Consolidated
Yes, already deployed	20%
No, but planning to in 2018	43%
No plans to do that	37%
Total	100%

Q2b. How do you detect advanced threats targeting your organization's network? Please select all that apply.	Consolidated
SIEM	44%
Sandbox	55%
Endpoint security	68%
Analyzing various logs, events, and alerts	63%
Firewall	67%
Other (please specify)	3%
Total	300%

Q3. Do you use any security oriented automation tools to analyze, correlate, and consolidate various events, logs, and alerts into actionable information on advanced threats?	Consolidated
Yes, already deployed	22%
No, but planning to in 2018	47%
No plans to do that	31%
Total	100%

Q4. Using a 10-point scale, how important is security automation to achieving a strong security posture within your company? (1 = not important to 10 = very important)	Consolidated
1 or 2	9%
3 or 4	9%
5 or 6	11%
7 or 8	30%
9 or 10	40%
Total	100%
Extrapolated value	7.14

Q5. Look ahead two years. Using a 10-point scale, how important will security automation be to achieving a strong security posture within your company? (1 = not important to 10 = very important)	Consolidated
1 or 2	3%
3 or 4	6%
5 or 6	10%
7 or 8	39%
9 or 10	41%
Total	100%
Extrapolated value	7.69

Q6. How does (or will) security automation improve your organization's security posture? Please select the top 5 responses.	Consolidated
Reduce the number of security events that must be investigated	49%
Reduce complexity of the cyber security architecture	42%
Optimize the productivity of current security personnel	36%
Reduce the number of insecure or non-compliant endpoints or things	54%
Accelerate the containment of an infected endpoints/devices/hosts	34%
Increase the speed of analyzing threats	64%
Reduce the false positive and/or false negative rate	59%
Prioritize threats and vulnerabilities	64%
Decrease the cost of cyber security operations	40%
Reduce the manual updating of firewall rules and security policies	32%
Assure consistent policies across environments such as on premise, private cloud, public cloud, hybrid; create once, update everywhere	25%
Other (please specify)	2%
Total	500%

Q7. Please select the top 3 barriers to successfully deploying security automation within your organization.	Consolidated
Automation tools/technology we need are not available	22%
No time to integrate automation into security workflows	20%
We can't create a unified view of users across the enterprise	49%
We can't apply controls that span across the entire enterprise	55%
We can't keep up with new or emerging attacks	33%
We can't recruit knowledgeable or skilled personnel	57%
Ironically, it requires too much staff to implement and maintain	34%
We have no budget for security automation	28%
Other (please specify)	3%
Total	300%

Q8. Which of the following factors diminish the effectiveness of security within your organization today? Please select the top 4 factors.	Consolidated
Heavy reliance on the public cloud environment	21%
Lack of mature and/or stable technologies	19%
Lack of leadership	15%
Regulatory and compliance requirements	17%
New (unknown) cyber security threats	39%
Interoperability issues among security technologies	57%
Increase in the severity of cyber attacks	55%
Increase in the frequency of cyber attacks	54%
Lack of in-house experts	62%
We have no budget for security automation	27%
Other (please specify)	20%
None of the above	14%
Total	400%

Q9. What best describes your organization's stage of maturity in its deployment of security automation?	Consolidated
Early stage – many security automation activities have not as yet been planned or deployed	46%
Middle stage – security automation activities are planned and defined but only partially deployed	27%
Late-middle stage – most security automation are deployed across the enterprise	17%
Mature stage – security automation has successfully been deployed across the enterprise	11%
Total	100%

Part 3. Attributions: The impact of security automation on cyber threats	
Please rate each statement using the agreement scale provided below each item. Strongly agree and Agree responses combined.	Consolidated
Q10a. The deployment of security automation technologies simplifies the process of detecting and responding to cyber threats and vulnerabilities.	54%
Q10b. Our organization's use of security automation technologies has decreased the workload of IT security personnel.	47%
Q10c. Our organization needs to simplify and streamline the number of vendors in our architecture to obtain maximum value from security automation technologies,	59%
Q10d. Our organization needs expertise from outside our company to maximize the value from security automation technologies.	54%
Q10e. Our organization has lost money on poor investments in security automation technologies.	48%
Q10f. It is difficult to integrate security automation technologies and tools with legacy systems.	63%
Q10g. We need automated correlation of threat behavior in order to effectively address the volume of threats in our environment	60%
Q10h. The deployment of security automation has increased the productivity of IT security personnel.	64%
Q10i. Our organization's investment in security automation is likely to increase as these technologies become more mature.	54%

Q10j. Our organization is properly staffed to identify and respond to malicious threats with security automation in place	35%
---	-----

Q11. Please rate the effectiveness of your organization's security automation technologies in minimizing cyber risk using the following 10-point scale. 1=not effective to 10=very effective.	Consolidated
1 or 2	12%
3 or 4	16%
5 or 6	32%
7 or 8	25%
9 or 10	15%
Total	100%
Extrapolated value	5.78

Q12. Please rate the overall complexity of your organization's security automation architecture using the following 10-point scale. 1=very low complexity to 10=very high complexity.	Consolidated
1 or 2	7%
3 or 4	10%
5 or 6	17%
7 or 8	27%
9 or 10	40%
Total	100%
Extrapolated value	7.17

Q13. Please rate your organization's ability to accurately identify areas in your security infrastructure where automation would create the most value, using the following 10-point scale. 1=not effective to 10=very effective.	Consolidated
1 or 2	20%
3 or 4	26%
5 or 6	27%
7 or 8	16%
9 or 10	11%
Total	100%
Extrapolated value	4.92

Part 4. Security automation architecture

Q14. What are the most important security automation technologies for minimize cyber threats in your organization? Please select your top 3 choices.	Consolidated
Technologies that secure the perimeter	14%
Technologies that provide security intelligence about networks traffic and entities	34%
Technologies that identify infected IoT devices and applies remediation	29%
Technologies that simplify the prioritization of threats	33%
Technologies that secure information assets	49%
Technologies that isolate or sandbox malware infections	45%
Technologies that secure workloads and applications in the cloud	46%
Technologies that identify and authenticate users	49%
Other (please specify)	2%
Total	300%

Q15. What are the main challenges your organization faces to achieve an effective security automation architecture? Please select your top 3 choices.	Consolidated
Ensure high availability of IT services	56%
Migrate to the cloud environment	44%
Integrate disparate security technologies	71%
Obtain sufficient resources/budget	34%
Comply with policies and regulations	32%
Recruit and retain qualified personnel	51%
Obtain executive-level support	11%
Other (please specify)	1%
Total	300%

Q16. What metrics are used to determine the effectiveness of your organization's security automation architecture? Please select your top 3 choices.	Consolidated
Cost savings through productivity gains	59%
Mean time to detect an attack (MTTI)	42%
Mean time to contain an attack (MTTC)	38%
Decreased security risk	45%
Increased prevention rate	30%
Increased detection rate	28%
Decreased false positive/false negative rate	38%
Passing grade on compliance audit or assessment	18%
Other (please specify)	1%
Total	300%

Q17. Who are key influencers/decision makers in setting your organization's security automation architecture? Please select your top 3 choices.	Consolidated
Chief information officer	53%
Chief operations officer	12%
Chief technology officer	32%
Chief information security officer	51%
Chief security officer	9%
Security architect	20%
SIEM administrator	17%
SOC team (security analysts/incident responders)	41%
Chief risk officer	16%
LOB or business unit leader	39%
No one person/function	11%
Total	300%

Q18. How much does compliance with policies, laws and regulations influence the design of your organization's security automation architecture?	Consolidated
Very significant influence	29%
Significant influence	30%
Some influence	26%
No influence	16%
Total	100%

Q19. How much do business objectives influence the design of your organization's security automation architecture?	Consolidated
Very significant influence	36%
Significant influence	35%
Some influence	19%
No influence	10%
Total	100%

Part 5. Deeper dive

Q20. Which of the following security products are deployed in your network? Please check all that apply.	Consolidated
NGFW	27%
Secure Web Gateway (SWG)	35%
IPS	57%
CASB	44%
VPN	43%
Identity/Access Management (IAM)	79%
Endpoint	69%
Sandbox	56%
Advanced Threat Detection (ATD)	22%
Unified Threat Management (UTM)	27%
Microsegmentation	32%
SIEM	45%
Total	536%

Q21. Which of these products generate alerts, events, or logs for your security team to analyze? Check all that apply.	Consolidated
NGFW	17%
Secure Web Gateway (SWG)	24%
IPS	41%
CASB	20%
VPN	25%
Identity/Access Management (IAM)	38%
Endpoint	44%
Sandbox	42%
Advanced Threat Detection (ATD)	15%
Unified Threat Management (UTM)	18%
Microsegmentation	23%
SIEM	35%
Total	343%

Q22. Which of these products have proven to be effective in helping you identify advanced (never before seen) threats? Please check any/all that apply.	Consolidated
NGFW	15%
Secure Web Gateway (SWG)	14%
IPS	31%
CASB	20%
VPN	18%
Identity/Access Management (IAM)	36%
Endpoint	45%
Sandbox	39%
Advanced Threat Detection (ATD)	17%
Unified Threat Management (UTM)	14%
Microsegmentation	22%
SIEM	27%
Total	298%

Q23a. Does your organization deploy SIEM?	Consolidated
Yes	45%
No	55%
Total	100%

Q23b. Which of the following best describes the use case for your SIEM?	Consolidated
Collecting and storing data required for compliance reporting	45%
Security platform that helps identify potentially malicious network activity	63%
We use the SIEM for compliance and security	30%
Total	137%

Q23c. If you're using the SIEM for security analysis, how helpful is it specifically in terms of identifying advanced threats inside your network?	Consolidated
Extremely helpful	37%
Somewhat helpful	41%
Not helpful	22%
Total	100%

Q24. In an ideal world, which of the following would you prefer?	Consolidated
All security products from a single vendor, seamlessly integrated with one pane of glass	37%
Best-of-breed products from multiple vendors, but all interoperable through APIs	37%
Most security products from a single vendor with integration options for a few specialized products	26%
Total	100%

Q25. How much total time does your team as a whole spend each day processing alerts, events, and logs to determine if there is any malicious activity inside your network?	Consolidated
30-60 minutes	12%
61-90 minutes	20%
91-120 minutes	29%
121-180 minutes	25%
More than 180 minutes collectively	13%
Total	100%
Extrapolated value (minutes)	115.5

Q26a. Would you like the ability to automate some of the manual tasks involved in using your SIEM – for example, in processing alerts, events, and logs each day?	Consolidated
Yes	77%
No	14%
Not sure	9%
Total	100%

Q26b. If yes, what benefits would you expect from this type of automation? Please select all that apply.	Consolidated
Improved productivity	59%
Stronger security posture	66%
Cost savings	33%
Total	158%

Q28. Where do you store your business-critical applications and data?	Consolidated
On-premise	37%
In public cloud	22%
In private cloud	7%
A combination of on-premise and cloud	33%
Total	100%

Q29. Will you be migrating more data to the cloud in the next 12 months?	Consolidated
Yes	60%
No	33%
Don't know	7%
Total	100%

Q30. If you leverage the cloud, do you manage security for that environment?	Consolidated
Yes, all of it	36%
No, none of it	21%
It is co-managed with a cloud service provider	30%
None of the above	12%
Total	100%

Part 6. Budget questions

Q31. Are you responsible for managing all or part of your organization's IT security budget this year?	Consolidated
Yes	64%
No (skip to D1)	36%
Total	100%

Q32. Approximately, what dollar range best describes the current annual budget for IT security activities across the enterprise?	Consolidated
Less than \$500,000	5%
\$500,000 to \$1,000,000	11%
\$1,000,001 to \$5,000,000	13%
\$5,000,001 to \$10,000,000	32%
\$10,000,001 to \$25,000,000	23%
\$25,000,001 to \$50,000,000	14%
\$50,000,001 to \$100,000,000	1%
More than \$100,000,000	1%
Total	100%
Extrapolated value	\$13,871,695

Q33. Today, what percentage of the current annual IT security budget will go to security automation?	Consolidated
Less than 10%	5%
10% to 15%	10%
16% to 20%	29%
21% to 30%	24%
31% to 40%	16%
41% to 50%	8%
55% to 75%	5%
76% to 100%	3%
Total	100%
Extrapolated value	28%

Q34. Looking ahead two years, what percentage of the current annual IT security budget will go to security automation technologies and platforms?	Consolidated
Less than 10%	0%
10% to 15%	5%
16% to 20%	16%
21% to 30%	22%
31% to 40%	23%
41% to 50%	16%
55% to 75%	12%
76% to 100%	7%
Total	100%
Extrapolated value	38%

Part 7. Your role and organization

D1. What organizational level best describes your current position?	Consolidated
Senior Executive/VP	5%
Director	16%
Manager	21%
Supervisor	14%
Technician/Staff	38%
Consultant/Contractor	4%
Other (please specify)	1%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Consolidated
CEO/Executive Committee	3%
Chief Financial Officer	1%
General Counsel	1%
Chief Information Officer	39%
Chief Information Security Officer	18%
Compliance Officer	5%
Line of Business (LOB) Management	24%
Chief Security Officer	2%
Data Center Management	3%
Chief Risk Officer	5%
Other (please specify)	0%
Total	100%

D3. What industry best describes your organization's industry focus?	Consolidated
Agriculture & food service	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	10%
Hospitality	2%
Industrial & manufacturing	10%
Public sector	12%
Retail	9%
Services	11%
Technology & software	8%
Transportation	2%
Other (please specify)	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Consolidated
Less than 500	14%
500 to 1,000	19%
1,001 to 5,000	23%
5,001 to 10,000	23%
10,001 to 25,000	10%
25,001 to 75,000	6%
More than 75,000	4%
Total	100%
Extrapolated value	11,053

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.