Devo AI Survey: Quick Read Report

Conducted by Wakefield Research on behalf of Devo

SURVEY

The Devo Survey was conducted by Wakefield Research among 200 IT security professionals from larger organizations, defined as companies with $500 million+ in revenue, between January 30th and February 9th, 2023, using an email invitation and an online survey.

1. Which of the following ways, if any, has your organization adopted automation in its Security Operations Center (SOC)?

	TOTAL
SOAR (Security Orchestration, Automation and Response) Solutions	53%
Cloud SIEM (Security Information and Event Management) Solutions	52%
AIOps (Artificial Intelligence for IT Operations)	51%
Machine learning-based analytics	48%
Automated threat detection and alerts	45%
Automated threat response	42%
Other	-
None of these	-
QuickFacts±	
Any (Net)	**100%**

± Data under "QuickFacts" were derived from the responses, not included as response options that were read during fielding. We include QuickFacts in instances where we feel they will be helpful.

2. Compared to last year, by how much will your organization change its investments in cybersecurity automation in the coming year?

	TOTAL
Over 20% increase	-
11% - 20% increase	14%
6% - 10% increase	41%
1% - 5% increase	25%
No change	6%
1% - 5% decrease	4%
6% - 10% decrease	8%
11% - 20% decrease	2%
Over 20% decrease	1%
I don't know	1%
QuickFacts±	
Increase (Net)	80%
Decrease (Net)	14%
More than 10% increase (Net)	14%

3. In which of the following scenarios, if any, would increased automation in the SOC be most helpful to fill staffing gaps in your team?

	TOTAL
Incident analysis	54%
Landscape analysis of applications and data sources	54%
Threat detection and response	53%
New threat mitigation and prediction	49%
Training	44%
Other	-
None of these, automation would not help fill our team gaps	-
There are no gaps in my team	1%
QuickFacts±	
There are gaps on my team (Net)	100%
Automation would help fill our team gaps (Net)	100%

± Data under "QuickFacts" were derived from the responses, not included as response options that were read during fielding. We include QuickFacts in instances where we feel they will be helpful.

4. Which of the following, if any, are reasons why you are not satisfied with your organization's adoption of automation in the SOC?

	TOTAL
Limited scalability and flexibility of available solutions	42%
High costs associated with implementation and maintenance	39%
Difficulty integrating with existing systems and infrastructure	37%
Lack of internal expertise and resources to manage the solution	34%
Concerns about data security and privacy	34%
Slow to adopt the latest technology	33%
Concerns about the reliability and accuracy of the technology	31%
Lack of flexibility in tools we can use	28%
Other	-
None of these – I'm satisfied with my organization's adoption of automation in the SOC	4%
QuickFacts±	
Any (Net)	96%
Flexibility/Integration (Net)	78%

5. In which of the following ways, if any, is your organization using AI in cybersecurity?

	2023	2022
IT asset inventory management	58%	79%
Understanding strengths and gaps in cybersecurity	49%	41%
Threat detection	46%	59%
Explaining relevant information to stakeholders	43%	42%
Breach risk prediction	38%	42%
Incident response	37%	28%
Other	1%	-
My organization is not using AI in cybersecurity	-	-
QuickFacts±		
Using AI in cybersecurity (Net)	100%	100%

± Data under "QuickFacts" were derived from the responses, not included as response options that were read during fielding. We include QuickFacts in instances where we feel they will be helpful.

6. For which of the following reasons, if any, do you believe malicious actors are better at using AI than your organization?

	Total
Better knowledge of the latest AI advancements	50%
Less constrained by ethical considerations when using AI	49%
More flexible and agile approaches to using AI	48%
More experience using AI	47%
More willing to take risks with cutting edge AI techniques	47%
Other	-
I don't believe malicious actors are better at using AI than my organization for any reason	1%
QuickFacts±	
Believe malicious actors are better at using AI than my organization, for any reason (Net)	100%

7. Which of the following positive business effects, if any, have you seen as a result of your company's use of AI in cybersecurity?

	Total
Increased efficiency of security processes	47%
Improved response time to security threats	45%
More efficient processes	41%
Increased revenue	39%
Greater ability to meet compliance obligations	38%
Reduced costs associated with hiring and training new employees	37%
Reduced downtime	34%
Other	-
None of these	-
QuickFacts±	
Any (Net)	100%
Financial benefits (Net)	65%
Efficiency benefits (Net)	70%

± Data under "QuickFacts" were derived from the responses, not included as response options that were read during fielding. We include QuickFacts in instances where we feel they will be helpful.

8. Have you or someone you know in your organization ever used an AI tool that was not provided by your company to help with work?

	Total
Yes, me	80%
Yes, someone I know	23%
No	4%
QuickFacts±	
Yes (Net)	96%

9. Which of the following scenarios, if any, would motivate you to use AI tools that are not provided by your company?

	Total
The tools are easier to use or have a better user interface than tools at my company	47%
The tools have more advanced or specialized capabilities than tools at my company	46%
The tools allow me to do my work more efficiently	44%
The tools help to fill gaps in my team	42%
The tools are recommended by a colleague or peer	42%
My company is too slow to adopt the latest tools	41%
Other	-
Nothing would motivate me to use AI tools that are not provided by my company	-
QuickFacts±	
There are scenarios that would motivate me to use AI tools that are not provided by my company (Net)	100%

± Data under "QuickFacts" were derived from the responses, not included as response options that were read during fielding. We include QuickFacts in instances where we feel they will be helpful.

10. Which of the following best describes what your organization would do if an employee were using an unauthorized AI tool?

	Total
Request the employee to stop use, but allow use later after a risk assessment	41%
Request the employee to stop use and not assess the tool for possible future use to mitigate risk	37%
My organization would not take any action on this – employees can use any AI tools	19%
My organization has no way of tracking this	4%
QuickFacts±	
My organization has a way of tracking AI use (Net)	97%
My organization would request an employee stop using an unauthorized AI tool (Net)	78%

± Data under "QuickFacts" were derived from the responses, not included as response options that were read during fielding. We include QuickFacts in instances where we feel they will be helpful.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.