NTT DATA

Adoption of Artificial Intelligence in Cybersecurity in America

2024

Index

Introduction

Like other countries in the world, America is in a constantly developing digital era, introducing revolutionary technological advances that drive people and companies to renew their knowledge to excel in today's competitive and demanding markets. However, there are specific questions about the use of artificial intelligence (AI). This technology is emerging as a driver of change, evolution, and efficiency in large organizations.

According to the study published by NTT DATA in collaboration with MIT, AI adoption has grown significantly, from 58% in 2020 to 71% in 2023.

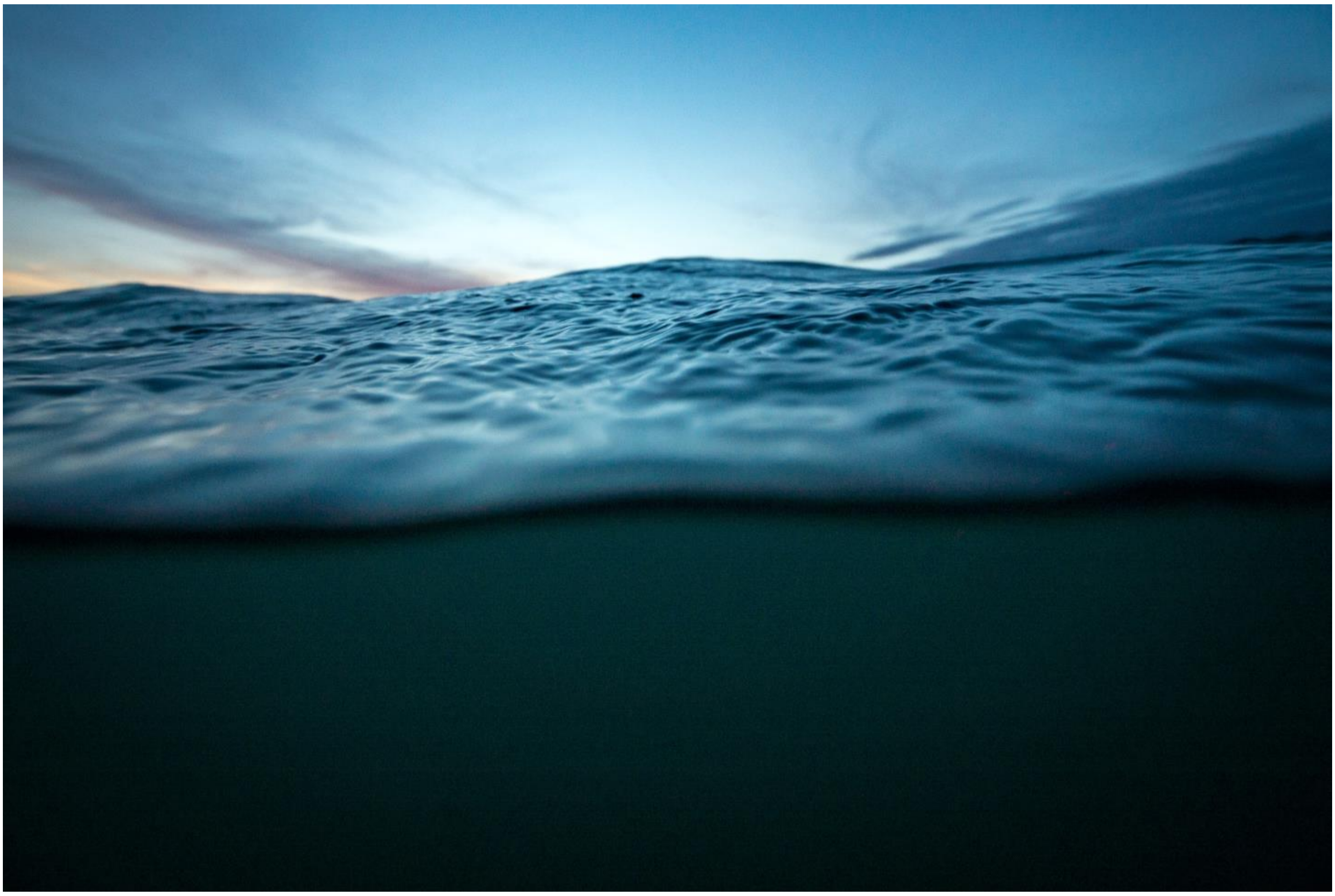
In the process, there are areas in an organization where it is valuable insight into how AI can help transform these areas. In this report in particular we will look at how AI can transform areas of cybersecurity.

Cybersecurity teams are subjected to an ever-increasing flow of data from internal (security monitoring) and external (threat intelligence) sources, which in many cases must be processed in real-time to ensure the protection of assets.

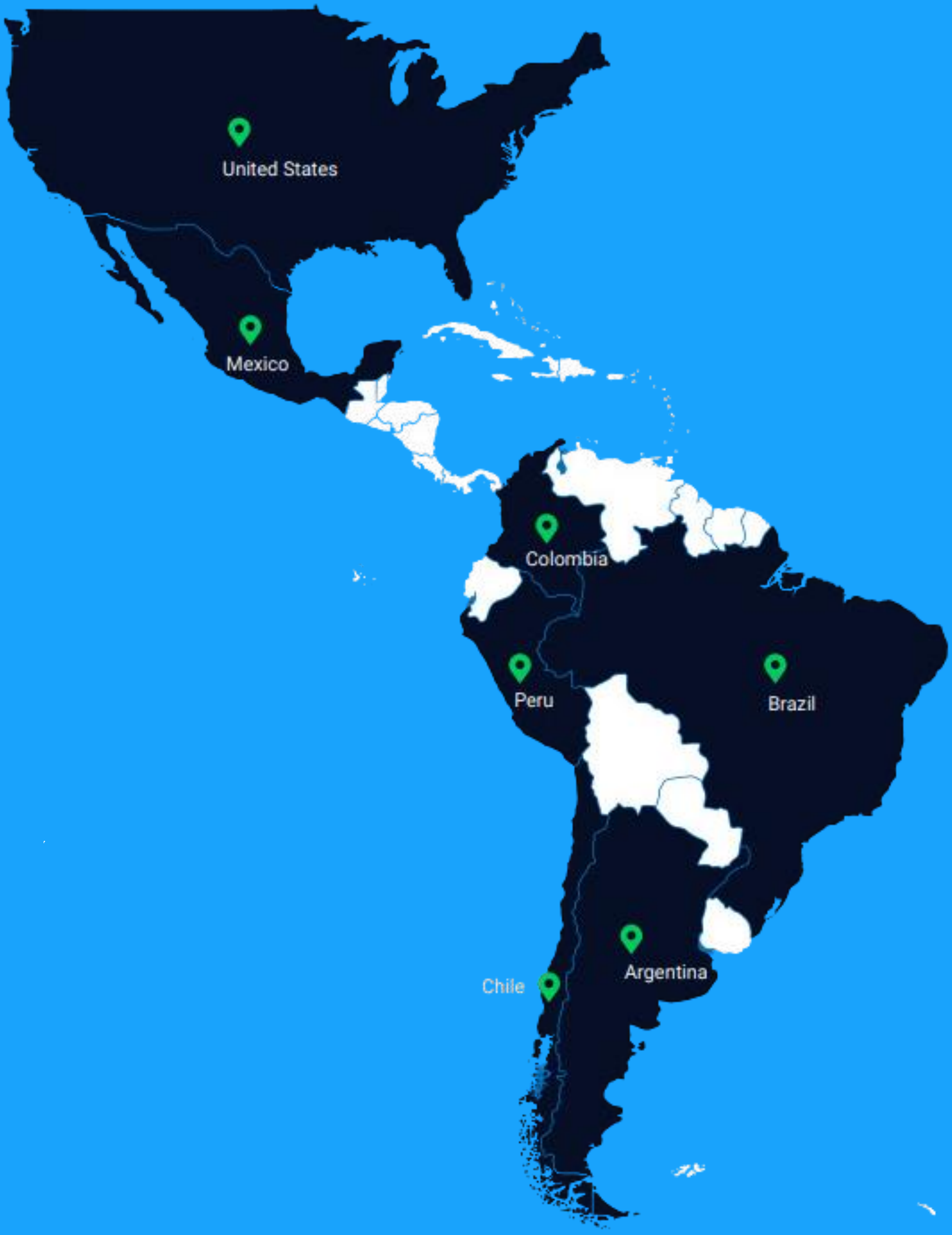
This report aims to explore how organizations in Americaare approaching the adoption of AI in the areas of cybersecurity.

In addition to the feedback from the primary survey (120 surveys and ten interviews), a specific survey on AI adoption in cybersecurity has been applied to CISOs and cybersecurity professionals from 32 organizations in the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Peru, and The United States. Responses have also been gathered from organizations at the regional level.

All of the data included in this report is consolidated information from the responses collected based on the perspective we have on AI and cybersecurity at NTT DATA.



Countries participating in the study

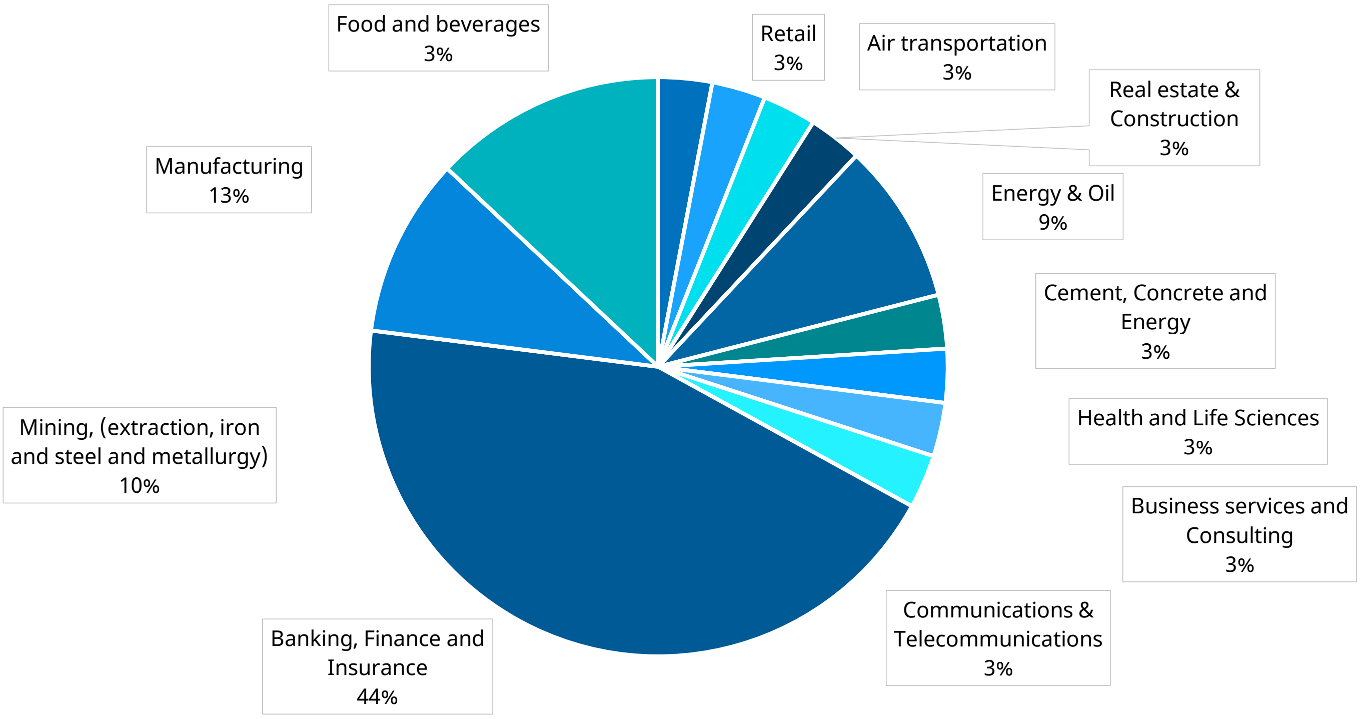


Study Methodology

To understand how the maturity of Artificial Intelligence is experienced in the cybersecurity areas of American companies, in addition to the feedback from the primary survey (120 surveys and 10 interviews), a specific survey on AI adoption in cybersecurity has been applied to CISOs and cybersecurity professionals from 32 organizations in the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Peru, and the United States. Responses have also been gathered from organizations at the regional level.

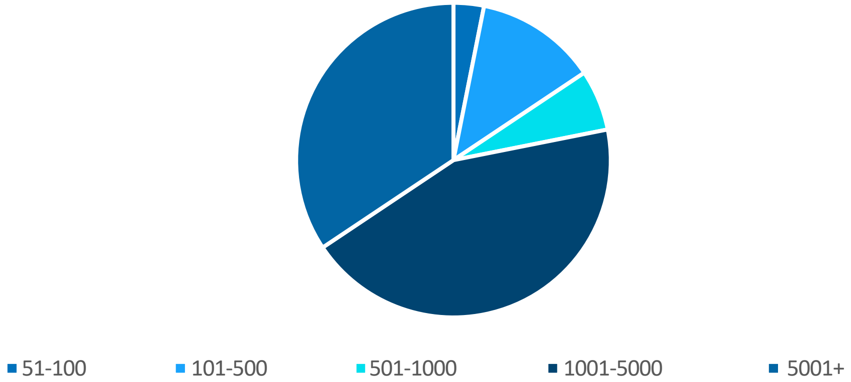
It is essential to mention that these insights have been gathered from CISOs or people who play a leading role in the areas of cybersecurity. The survey sample covers different sectors, with the finance, insurance, and industry sectors (mining, manufacturing) showing greater interest in the report and the process findings.

Participating companies by industry



Lastly, in this second survey focused on the adoption of AI in cybersecurity, the participating organizations are large and relevant companies in the American region.

Employees of participating companies

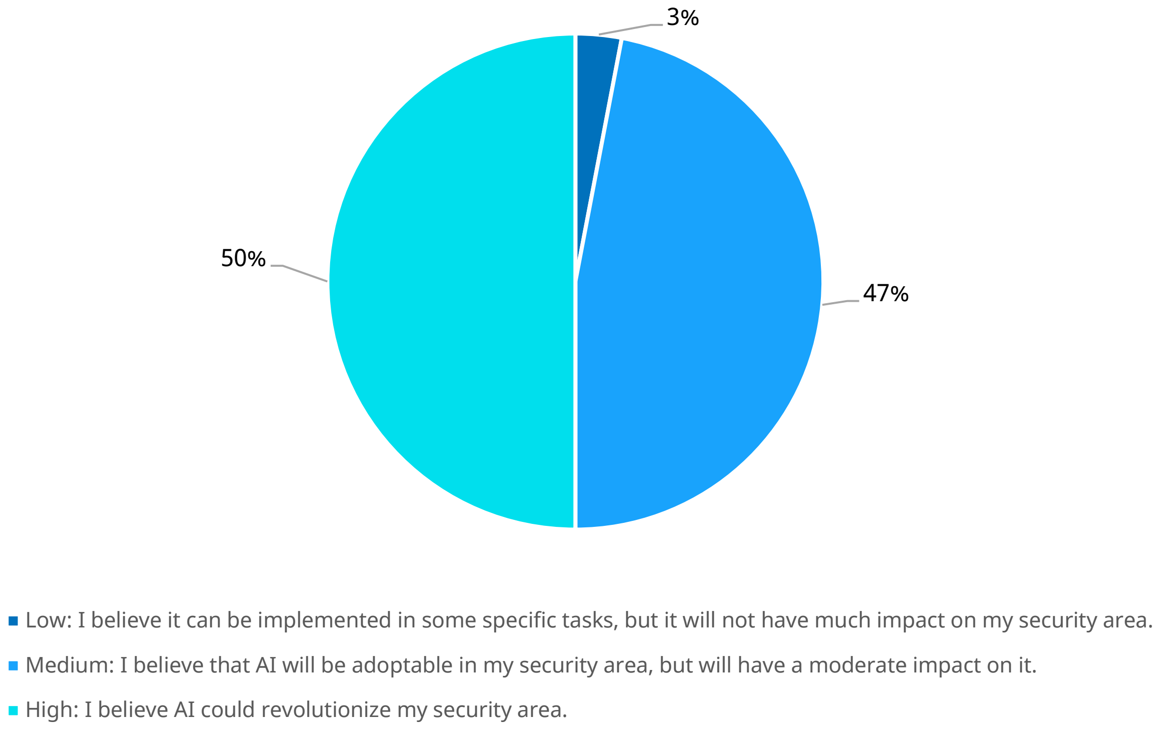


Perception of the Adoption of AI in Cybersecurity in America

> AI is a co-pilot and can help us save time in the detection and analysis of events, but it always must be supervised.
>
> *CISO, Industrial Company, Chile*

The 2023 study seeks to provide a comprehensive analysis of the consolidation and advancement of AI in the region. As a result, a notable growth in its adoption is evident, with a significant leap from 58% in 2020 to 71% in 2023. It also delves into the significant challenges that companies face in the region, such as the lack of specialized technical knowledge and adequate financial resources for the effective implementation of AI-based solutions. Some 20% of companies have not yet incorporated AI into their operations, marking a wide margin for expansion and future growth in the adoption of this emerging technology.

Perceived AI potential for security areas

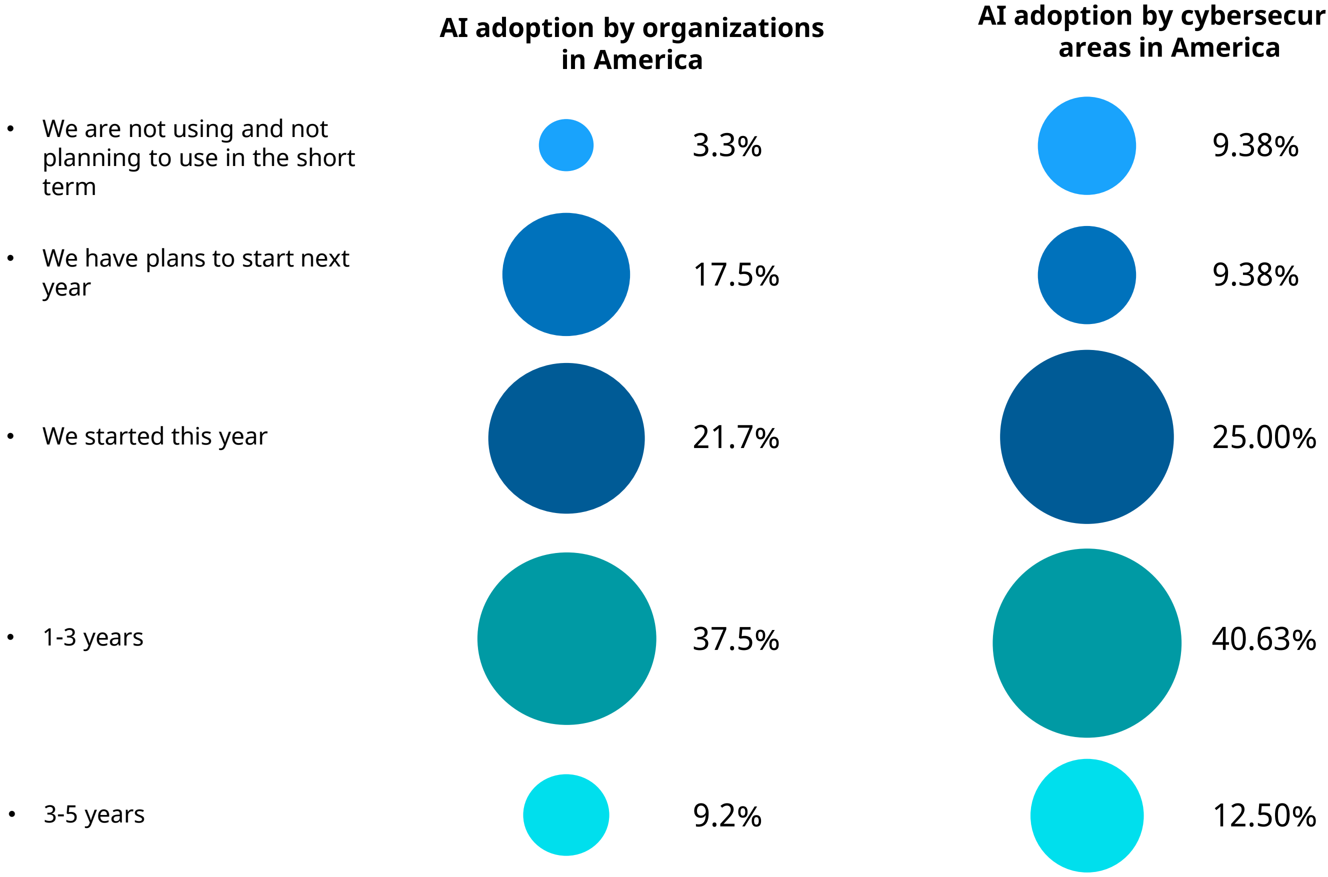


The first step to adopting a technology is to recognize its impact and potential. In the case of AI, companies recognize a medium to high impact on the improvement and efficiency of cybersecurity activities.

> “The use of AI as part of the security solutions we have been using will increase over time, so its adoption in companies will be incremental. Brands whose products do not start using AI run the risk of being replaced by those that do.
>
> *Industry company, Peru*

Perception of the Adoption of AI in Cybersecurity in America

The following diagram compares the period during which American companies have been working with AI (left) and the period during which American organizations' cybersecurity areas have been working with AI (right).
It can be observed that, in cybersecurity, on the one hand, there is a higher percentage of companies that do not want to start with the adoption of AI compared to the 3.3% that do not want to start with the adoption in the rest of the areas. However, in the categories of "we started this year," "we have been working for between one and three years," and "more than three years and less than five," there is a higher percentage of companies that say they are already working with AI in cyber compared to organizations that acknowledge that they are adopting AI. Is this a contradiction?

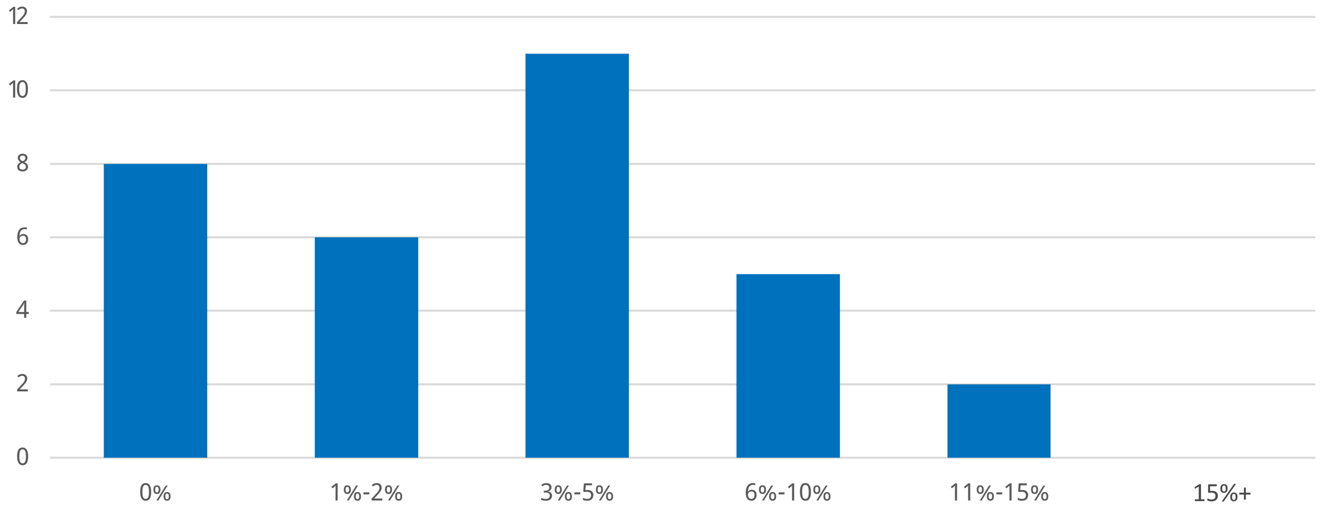


Two reflections emerge from these data.

Cybersecurity tool manufacturers have been working with AI for years to improve defensive controls such as DLP, firewalls, anti-spam protection, and role assignment in IAM, among others. Some CISOs are very aware of the power of these functionalities, and although they have not developed ad-hoc AI systems for the area, they do acknowledge that they have been working with AI for years.

And, since the survey of AI adoption in American organizations was not sent to CISOs, and it seems cybersecurity teams have been working with AI for longer than non-CISOs, it is worth reflecting on how CISOs are pitching their work within their company. There may be a lack of socialization of how the tools they invest in using AI to improve the cybersecurity of the organization. This socialization is vital when it comes to getting a larger budget. Currently, cybersecurity areas declare that they invest the following percentage of their budget in the adoption of AI:

Annual cybersecurity budget invested in AI projects (%)



> We have established an AI working group. Use cases for the application of AI have been identified, and some of these are related to information cybersecurity.
>
> *CISO, Regional organization*

Perception of the Adoption of AI in Cybersecurity in America

Maturity stages of companies regarding the use of AI

The following illustration details the adoption journey of companies.

1. No experience

No AI solution has yet been implemented and no investment has been made in this area.

2. Exploration

The company has started to explore AI solutions and has some preliminary research, but has not yet implemented any AI solutions in production.

3. Production

The company has already been adopted, but has not yet reached a significant scale in its use.

4. Advanced implementation

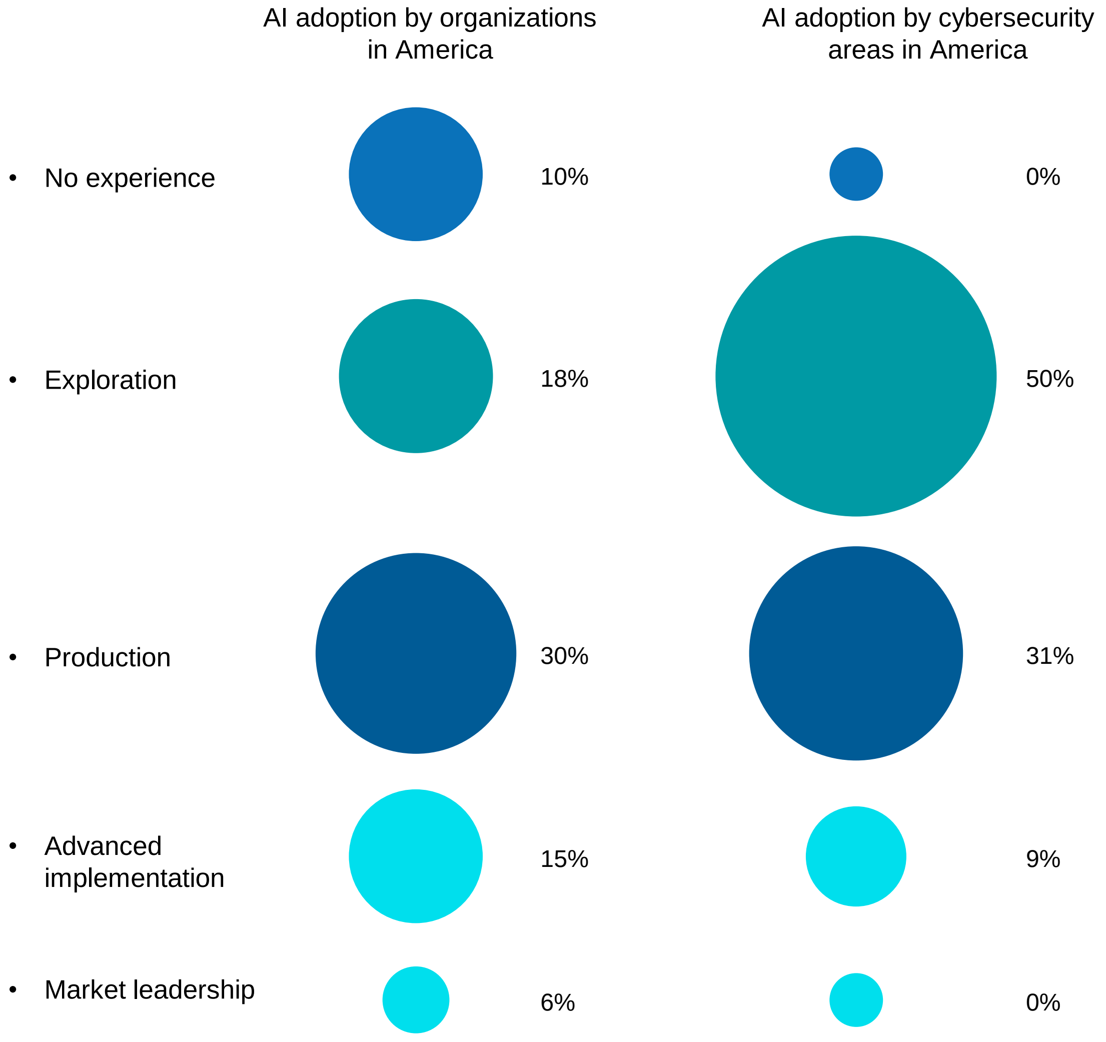
The company has implemented large-scale AI solutions with tangible and successful outcomes from their use across the organization.

5. Market leadership

The company is a market leader in the use and adoption of AI and has achieved a significant competitive advantage in its industry through the application of AI solutions, with capabilities to create AI-based products and services.

While in the maturity stages, it seems that all companies have had contact with AI in cybersecurity activities, a lower level of maturity can be seen in the AI areas compared to other areas of the organization. Although 53.13% of companies say they have been working with AI for more than a year, however, these companies do not consider themselves to be market leaders.

This raises the question of whether adoption has been conscious or through cyber security tools including AI and what is causing this stagnation.

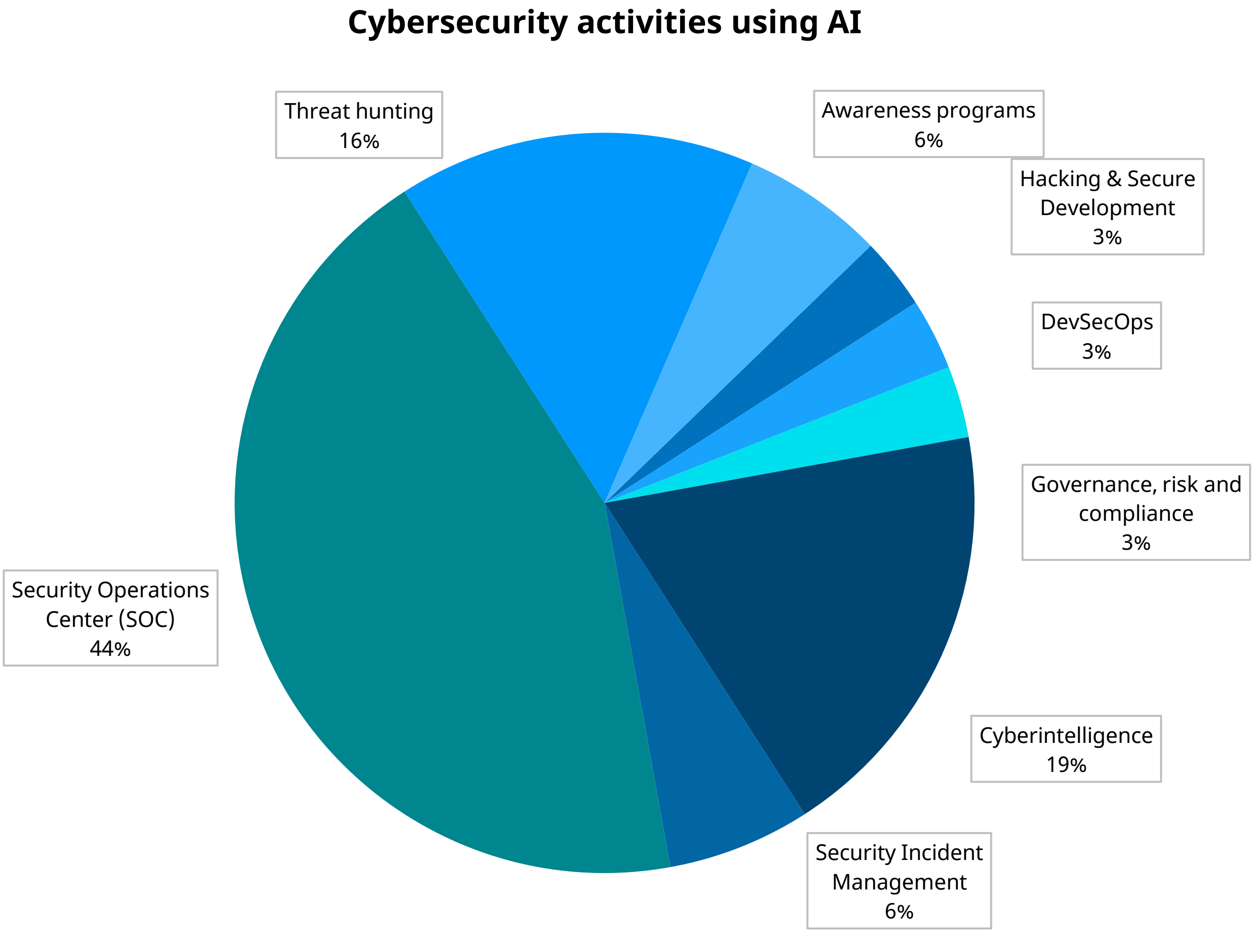


> “AI has enormous potential in information cybersecurity; however, it is important to be conservative about the speed of adoption, which should be gradual, starting with one-off, repetitive activities, and then expanding its use to more complex tasks.
>
> *CISO, Industry Company, Peru*

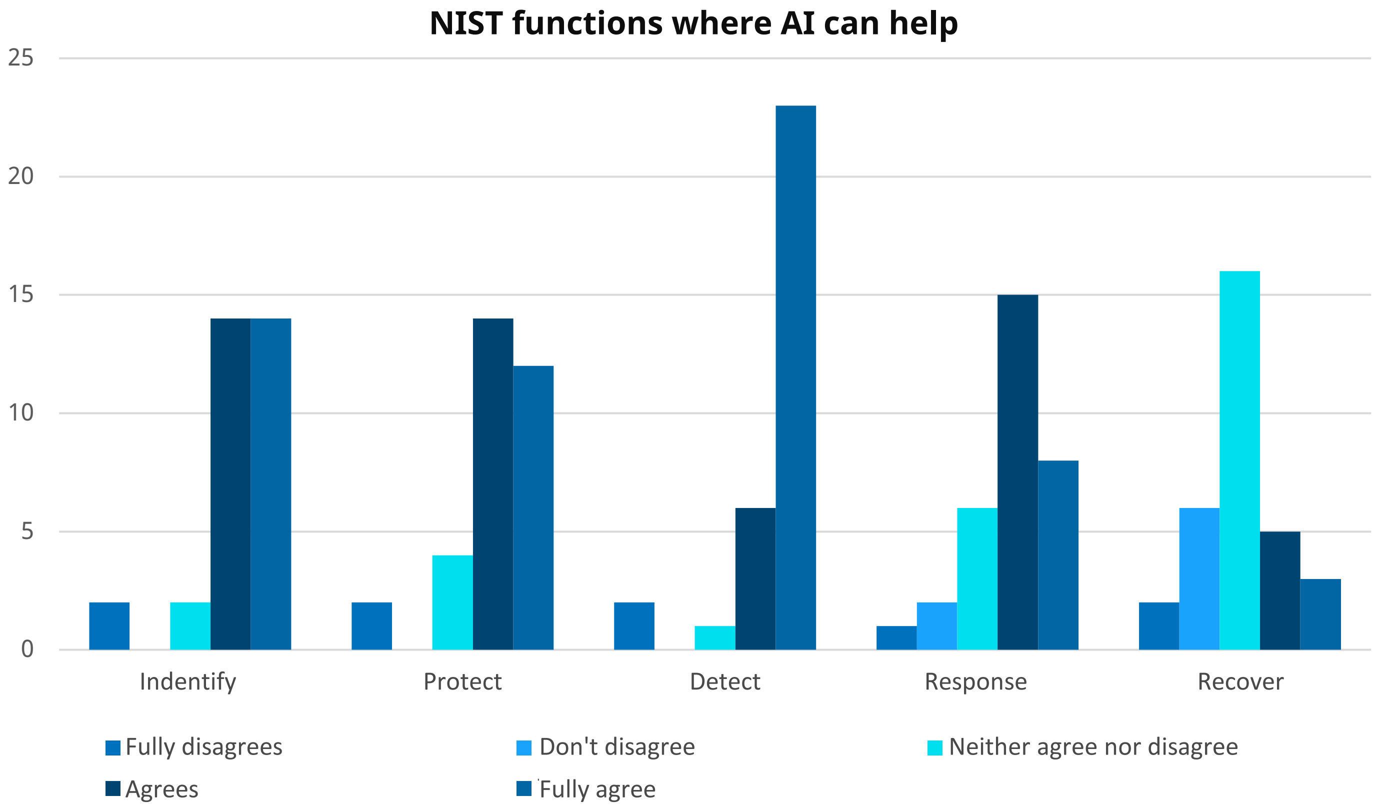
Maturity and expectations of Artificial Intelligence in Cybersecurity

> “AI is becoming an asset in the cybersecurity of companies; however, it faces a tough challenge in response and recovery. It is emerging through the protection tools that are starting to be implemented.
>
> *CISO, Mining Industry, Peru*

After understanding how organizations are self-perceived in adopting AI in cybersecurity, it has been analyzed in which cybersecurity activities AI has been applied. SOC is the area where AI has been used the most; however, no organization claims to have used this technology in Red team and identity incident management activities.

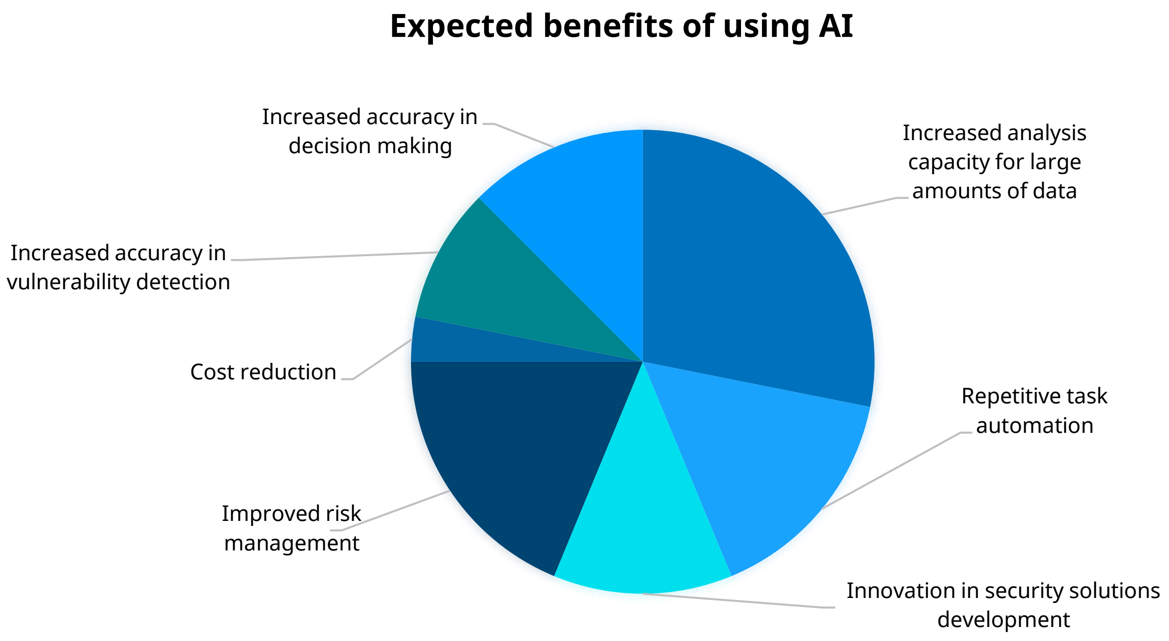


Also, organizations agree that AI can support in identifying, protecting, detecting and responding domains. The recovery phase is the most uncertain, perhaps because nowadays it is perceived as an activity that is rarely performed and it is not worth training a system to support this phase.

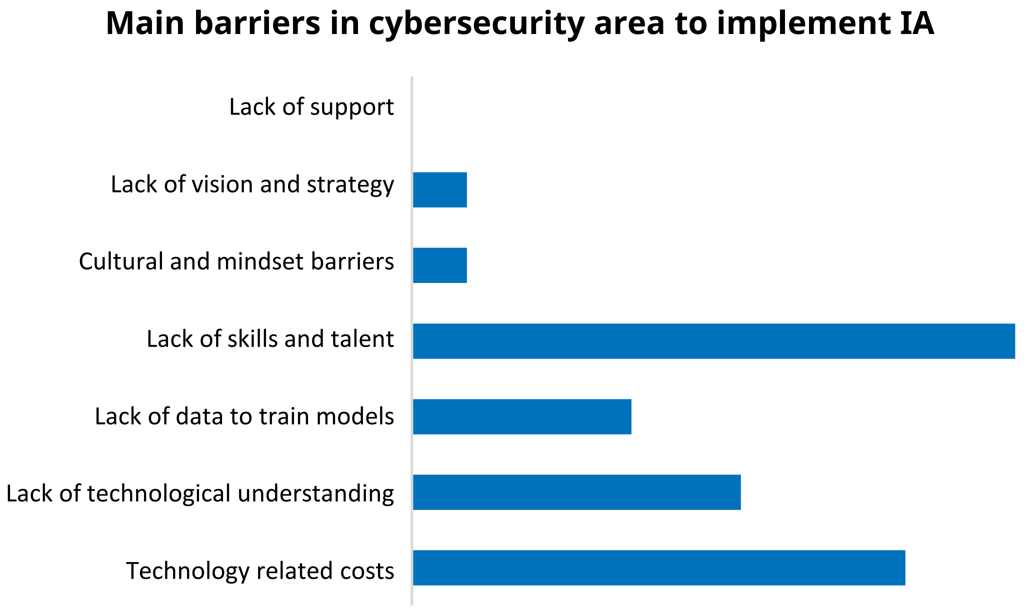


Benefits and barriers to implementing Artificial Intelligence in Cybersecurity

One of the questions was related to the benefits expected from the use and adoption of AI. There has not been a unanimous response, with several benefits seen with equal importance.



These benefits lead to other benefits. For example, if a greater automation for repetitive tasks can be achieved, this will reduce the talent gap of cyber-savvy people needed as the current ones receive higher-value tasks to perform. This is seen as a major barrier to the implementation of AI in cybersecurity today.

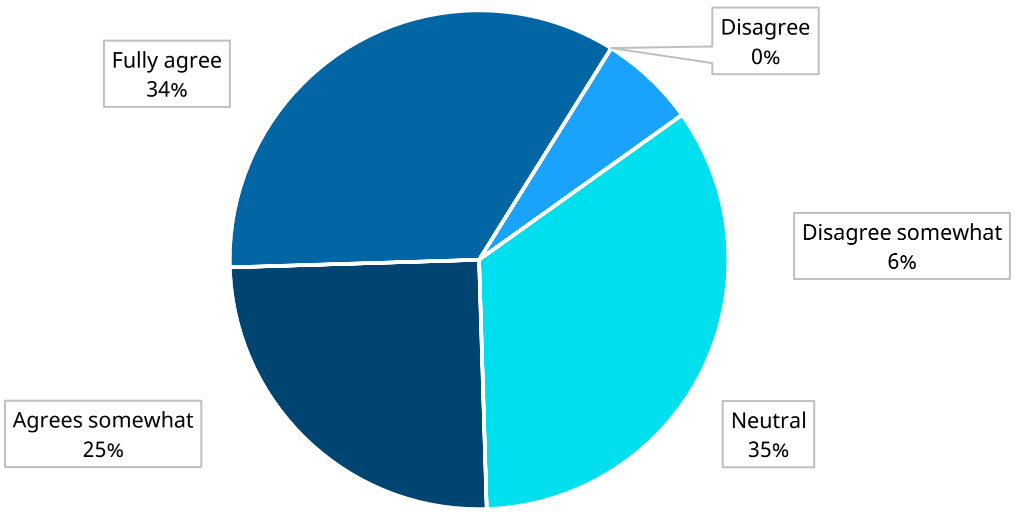


Costs and lack of understanding of AI are the following perceived barriers after the lack of talent.

Benefits and barriers to implementing Artificial Intelligence in Cybersecurity

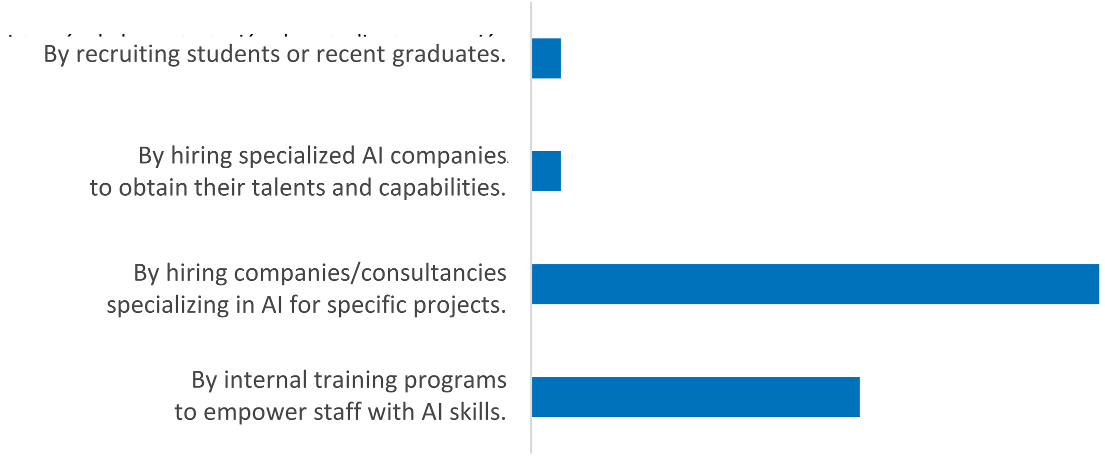
A key issue in adopting AI, including in cybersecurity, relates to support from the organization. A large group agrees or somewhat agrees with the statement, "I have support from the organization to apply AI in the cybersecurity areas." There is another group that is neutral to that statement. A positive aspect to highlight is that the opinion of not agreeing or somewhat disagreeing is a minority.

I have support from the organization to use AI in cybersecurity areas



Organizations are mostly relying on hiring specialized consulting firms or building in-house capabilities to obtain the skills and talent needed for AI-related work.

Acquiring skills and talent needed for AI-related work



Conclusions and Challenges

In this last section of the report, we highlight the main "take-aways" from this analysis and the challenges ahead in the coming months.

Defining AI Use Cases in Cybersecurity

More than 95% of organizations believe that AI will have a medium or high impact on cybersecurity areas. AI is generating high expectations in cybersecurity, which translates into budget investment and organizational support. This means that CISOs must materialize and monetize the value invested in AI in their area, proving that benefits have been successfully achieved. This challenge is critical for organizations that claim to have been using AI in cybersecurity areas for more than three years.

Defining AI Use Cases in Cybersecurity

The SOC is considered the area where AI is most supported, and based on the NIST domains, the general opinion is that the domains that identify, protect, detect, and respond can greatly benefit from AI. The definition of use cases will explain how AI is being adopted in Cybersecurity, while narrowing the scope to value and assess. Today, it is possible to define SOC use cases and then extend them to NIST domains and other domains such as governance or risk.

There are some AI insights or applications where it will have a high impact in the short or medium term:

1. Threat and anomaly detection: Using machine learning and data analytics, AI can identify unusual patterns or suspicious behavior on a network, which could indicate an intrusion, malware, or any other type of cyber threat. This early and accurate detection capability is critical to preventing attacks or limiting the potential damage.

2. Cybersecurity incident response: Once a threat is identified, having a rapid response capability is crucial. AI can automate responses to cybersecurity incidents, such as isolating compromised systems or patching vulnerabilities. This not only improves the speed of response but also reduces the burden on cybersecurity teams, allowing them to focus on more complex challenges.

CISO, Banking, LATAM

AI and Cybersecurity for Talent Development

Talent - or, rather, the lack of it - is the main barrier to AI adoption. Organizations must rethink the career path they will give to AI and cybersecurity professionals.

These professionals are seeking new challenges, and if they can't find them in one organization, they will switch to another.

Finding resilience in the turnover of these key personnel should also be part of the AI adoption strategy.

María Pilar Torres Bruna
Head of Cybersecurity in Iberia and LATAM
maria.pilar.torres.bruna@nttdata.com

Carla Passos Schwarzer
Head of Cybersecurity in Brazil
carla.passosschwarzer@emeal.nttdata.com

Jose Uzcategui
Head of Cybersecurity in Chile
jose.uzcategui@emeal.nttdata.com

Miguel Angel Garzón Ramirez
Head of Cybersecurity in Colombia
miguel.angel.garzon.ramirez@emeal.nttdata.com

Andrea Isabel Muñoz Parreño
Head of cybersecurity in Ecuador
andreaisabel.munozparreno@emeal.nttdata.com

Cristhian Israel Atristain Garcia
Head of Cybersecurity in Mexico
cristhianisrael.atristaingarcia@emeal.nttdata.com

Néstor Gerardo Ordoñez
Head of Cybersecurity in the USA
nestorgerardo.ordonez@emeal.nttdata.com

Andrea Araujo Braga
Manager of Marketing and Communication of the Americas
andrea.araujo.braga@nttdata.com

Gabriela Gutiérrez Sánchez
Head of Marketing and Communications of the Americas
dulcegabriela.gutierrezsanchez@nttdata.con

About NTT DATA

NTT DATA - a part of NTT Group - is a trusted global innovator of IT and business services headquartered in Tokyo. We help clients transform through consulting, industry solutions, business process services, IT modernization and managed services. NTT DATA enables clients, as well as society, to move confidently into the digital future. We are committed to our clients' long-term success and combine global reach with local client attention to serve them in over 50 countries. Visit us at nttdata.com.

NTT DATA