March 2024

NTT DATA

# Radar

## Powered by women

# The adoption of AI in the field of cybersecurity

By Maria Pilar Torres

Surely all readers of this magazine have wondered several times in recent months how much AI and generative AI can contribute to our cybersecurity areas. We are witnessing how this technology advances steadily in other areas of organizations, as evidenced in the recent study conducted by NTT DATA and MIT on AI adoption with a focus on Latin America. In our field, there is a shortage of expert talent, and there are many repetitive tasks where this technology seems to be able to play a significant role.

To delve a little deeper into this point, we wanted to conduct an exercise to understand how AI is being used in cybersecurity areas, for which a simple survey has been launched. In addition to all the details that you can read in the report with the results, I would like to share several outputs:

**Realizing the value invested in AI in cybersecurity.**

*"More than 95% of organizations believe that AI will have a medium to high impact on cybersecurity areas"*

AI is generating high expectations in cybersecurity, translating into invested budget and organizational support. This implies that CISOs must materialize and quantify the value invested in AI in their area, demonstrating that some of the expected benefits have been achieved. This challenge is of particular importance in organizations that declare having been using AI in cybersecurity areas for more than 3 years.

**Defining specific use cases of AI in cybersecurity.**

*"The SOC is perceived as the area where AI can provide the most support, and if we look at the NIST domains, there is a widespread opinion that the identify, protect, detect, respond domains can greatly benefit from AI"*

Defining use cases will explain how AI is being adopted in cybersecurity while limiting the scope for assessment and quantification. Currently, one can start by defining use cases for SOC and then expanding into NIST domains and other areas such as governance or risk management.

**Talent management in AI & Cybersecurity**

*"Talent, or rather the lack thereof, is the main adoption barrier for AI"*

Organizations must consider the career path for AI and cybersecurity experts. These individuals seek new challenges, and if they cannot find them within an organization, they will move to another one. Seeking resilience in the turnover of this key personnel should also be part of the AI adoption strategy.

The report indicates that the presence of AI in cybersecurity areas is a fact, in some cases for several years. Therefore, it is necessary to mature the role of AI and maximize its value.

# The new cybersecurity regulations of 2024

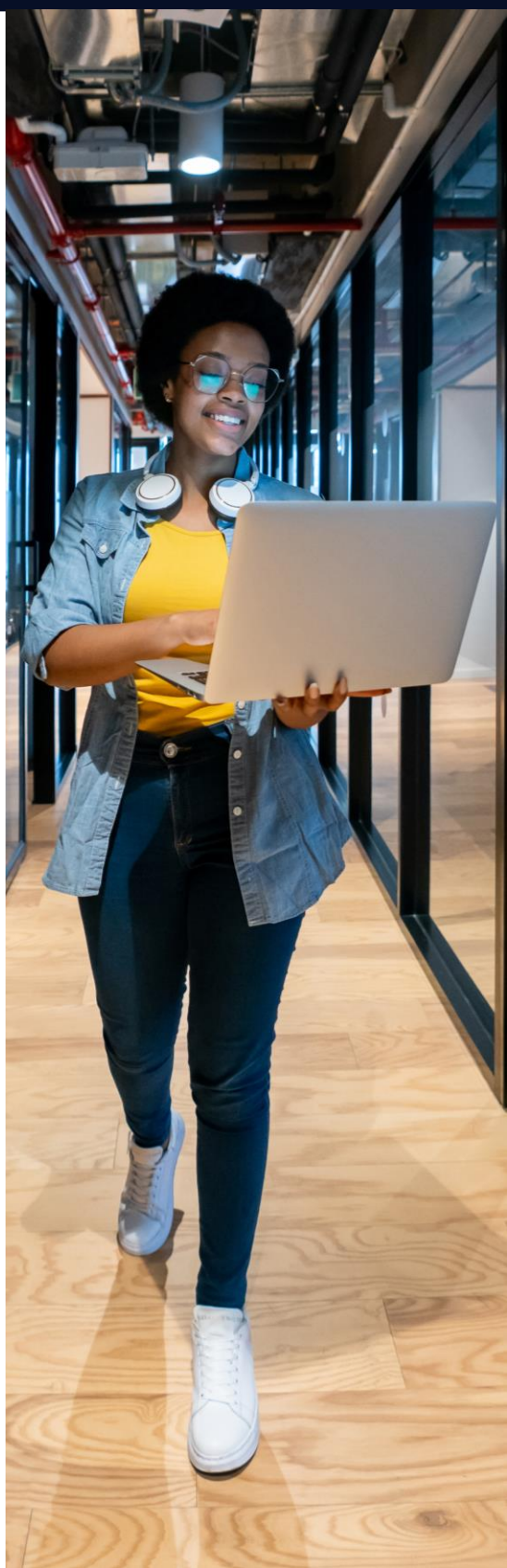
By Marta Fernández

Cybersecurity faces many challenges in 2024, from AI and cloud security to talent shortages, employee and societal awareness, and preparation for the quantum era. However, this year we must acknowledge that we are facing regulations that will come into effect, therefore compliance and proper risk management will be among the priorities on the agendas of many CISOs and cybersecurity professionals.

During the year 2024, several regulations will come into effect, be updated, or revised. For example, the GDPR may lead to stricter enforcement in 2024, the first package of technical standards on the Digital Operational Resilience Act (DORA) will be presented, which will come into force in financial entities across the EU in January 2025. Additionally, we will see updates with the new NIS2 regulation, the enforcement of WP.29, and the voting on the EU AI Act. Therefore, it is important to understand the scope and impact of each of these regulations in 2024 for each organization and to stay ahead, as non-compliance could have serious legal, financial, and reputational consequences. In this article, we will delve into the ever-changing world of new cybersecurity legislations and regulations that will come into play this year.

The European Union is taking some significant steps regarding security matters. This year, the NIS2 directive comes into force, adopted on December 14, with measures to be implemented by October 17. The new NIS2 breaks away from the limitations of its predecessor NIS1 (EU 2016/1148) by allowing the establishment of a high and common level across the Union. It focuses particularly on the resilience of third parties and providers of critical infrastructure services. It has a clear risk management approach, including specific provisions for reporting cybersecurity incidents. This encourages information sharing and public-private cooperation, crucial for managing cyber crises and disclosing vulnerabilities. In this risk-oriented approach, it also addresses supply chain security, and the regulation brings measures leading to monitoring and supervision of compliance to avoid penalties. Therefore, it is advisable for organizations subject to this regulation to start defining a cybersecurity plan to address the new requirements introduced by this regulation, starting from Threat Intelligence.

On the other hand, a regulation that will have more impact and significance is the legislation and regulation on artificial intelligence (AI). It is expected that the law will be ratified during the first quarter of 2024, with full implementation planned for 2026. Although AI technologies are not new, we are witnessing a growing adoption and usage accompanied by technical, commercial, and security challenges. These challenges have a global scope, affecting organizations, citizens, and society at large. Many debates have been opened to address how the use of AI will be monitored and how the data shared through AI will be regulated, ultimately how compliance with legal and even ethical requirements will be ensured.



The priority of the Parliament with the publication of this regulation is to ensure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory, and environmentally respectful. In essence, the Artificial Intelligence Act is the world's first regulation on AI, aiming to regulate artificial intelligence (AI) to ensure better conditions for the development and use of this innovative technology.

In April 2021, the Commission proposed the first regulatory framework for AI in the EU. The law also focuses on risk, categorizing it as Minimum, High, and Unacceptable. An evaluation is established by categorizing AI systems, which can be functional models, highly capable models, and general-purpose models. This regulation establishes prohibitions on the use of AI and ensures the rights of users, who must be informed when AI is involved in data processing. The aim is to reach an agreement by the end of this year. Depending on the level of risk, the new regulations establish obligations for providers and users. Let's analyze the different levels, starting with the highest exposure to risk:

- **AI systems of unacceptable risk** are those considered a threat to individuals and will be prohibited. This includes those that can lead to cognitive manipulation, classification of individuals, biometrics, and facial recognition.

- **AI systems of high risk** are those that negatively affect safety or rights. These include AI systems used in products subject to EU product safety legislation and specific areas such as biometric identification and categorization of individuals, management and operation of critical infrastructure, education and vocational training, employment, management of workers and access to self-employment, access to and enjoyment of essential private services and public services and benefits, law enforcement, migration management, asylum, border control, and assistance in legal interpretation and law enforcement.

- **AI systems of limited risk** must meet minimum transparency requirements.

AI is transforming cybersecurity with automated detection and response systems, but it also raises concerns about potential automated attacks and attackers using AI to develop more sophisticated and harder-to-detect attacks. Anticipating new attacks and gaining detection and response capabilities is another major challenge.

Cybersecurity also applies to products like cars, which increasingly include more software-based functionalities and connectivity. Therefore, since July 2022, all car manufacturers must comply with the new WP.29 UN R155/R156 regulation to obtain vehicle approval. WP.29 refers to the World Forum for Harmonization of Vehicle Regulations, which belongs to the United Nations Economic Commission for Europe (UNECE).

Starting in July 2024, homologation under this regulation will be required for all new vehicles sold in the European Union, regardless of when the manufacturer obtained vehicle type approval. In fact, to comply with the regulation, some older models that are still being produced may need to undergo changes to be re-homologated. The goal of this regulation is to ensure that there is a safety management framework for cars. From this year onward, cars must be certified under this regulation, guaranteeing that they are secure against the possibility of a cyber threat or potential attack through vehicle software vulnerabilities, sensors, or any other connected service.

In summary, regulations aim to provide the normative framework to standardize and establish minimum requirements that always ensure data and personal safety. We are experiencing a moment of transformation, with new technologies, products, and elements of the supply chain among others. Controlling and mitigating the security risk accompanying this transformation is crucial to avoid catastrophes and major losses, as well as resilience to potential threats. Regulations serve as an excellent framework and guide to accomplish this mission.

# Extreme hacking

By Mª Ángeles Gutiérrez

First, it was the IT world; by connecting it to the internet, we made it vulnerable and susceptible to hacking. Then, we connected the OT, the factories, the ATMs, and a few years ago, also the IoT. And now, ourselves. Just a few days ago, it was announced that a brain chip had been successfully implanted, allowing, among many other things, control of the phone or computer, and through them, almost any device, with just a thought...

It's true that we have been incorporating different devices into our bodies for years. We're talking about pacemakers, cochlear implants (direct stimulation of the auditory nerve), neurostimulators (for treating epilepsy or chronic pain through direct stimulation of brain areas or peripheral nerves), implantable glucose monitors, ocular retinal implants (partially restoring vision by stimulating the retina with electrical signals), subcutaneous RFID chips (radiofrequency identification devices), neuro-controlled prosthetics, pressure sensors (used to monitor intracranial pressure), implantable biomarkers (detect and monitor specific biomarkers in the body to provide information about overall health), but the latest announcements like Neuralink go a step further... we're connecting our own brains, becoming just another terminal. Connected to the network? Exposed like any device to being hacked?

The convergence between technology and the human body indeed poses new challenges. The growing integration of electronic devices into the human body, known as the connected body or cybernetic body, brings significant challenges.

The constant collection of biometric and health data allowed by these devices raises concerns about individual privacy and introduces new vulnerabilities. Implantable devices can be susceptible to cyberattacks, compromising the integrity and confidentiality of medical data, and even risking the individual's health with new infections and manipulations. Keeping these devices secure over time through updates is an unresolved technical challenge. The lack of common universal standards hampers interoperability and mass adoption, and they do not integrate securely and efficiently with the biological system without side effects.

Furthermore, the acceptance of these technologies by the population is still pending analysis, and how it affects the perception of identity and individual autonomy, as well as its impact on self-esteem. Pressure to conform to standards of beauty or performance may create a culture of insecurity and dissatisfaction with the natural body. Moreover, it may intensify inequalities by creating gaps between those who have access to these technologies and those who do not. How it will impact interpersonal relationships is another question. Excessive dependence on these devices could severely affect the body's ability to function naturally, and technological obsolescence could leave people at risk if the devices fail or become incompatible with new technologies.

In summary, anything connected to the network or with a wireless system is susceptible to hacking. To avoid giving up the benefits that the "connected body" will surely bring (a great opportunity for thousands of people with paralysis, ALS, vision loss, aphasia...), and to prevent and avoid the great temptation that will almost certainly arise to access information about our health and even directly manipulate our thoughts, let's make available for these new uses all that we have learned about security, both from a technical and regulatory standpoint. Let's not make the mistake again of deploying mass technologies that are immature from a cybersecurity standpoint. A lot is at stake here—our health and even our lives.

# Identity governance

By Andea Muñoz

Since the era of the industrial revolution, companies have evolved and adapted to the needs of a changing market, based on new discoveries and industry requirements. However, with the advent of the internet, this evolution has taken a much greater turn and begun an exponential acceleration, forcing companies to adapt more quickly to change. One of the cornerstones of this evolution is digital transformation, which could be summarized as the adoption of technology in all business processes.

In 2020, with the COVID-19 pandemic, this transformation was forced, and companies found themselves obliged to adapt. But what does it mean to have a company in the digital world? What are the implications for companies that do not control the data and information that moves through them? These challenges began to become urgent questions requiring immediate answers.

Before digital transformation, all data and information of companies were physically within their premises, so efforts were focused on protecting the perimeter and preventing data leakage. However, with digital transformation, the need for movement, remote work, and cloud adoption, the perimeter expands, becoming impossible to control, leaving companies without borders. The identity of individuals and authentication systems become relevant for the protection of data for these now decentralized companies.

Another point that has generated new security breaches and concerns among security areas but is nevertheless a global trend facilitating the work of companies is the movement to the cloud.

To the above, add the generational shift, where Millennials and Centennials become both the most important workforce and the strongest consumer base. These generations represent 59% of the workforce in companies, and they have a mindset to which companies must adapt. It is a mindset that requires agility and immediate attention to their needs, as they grew up with technology as a fundamental part of their lives.

For these generations, the need for more free time, work flexibility, and telecommuting possibilities are some of the key points to retain talent. These generations also lean towards processes being done quickly and generally through applications, without queues, contactless, and improving the user experience. All of this leads companies to the need to transform to remain relevant in the market. A clear example of this is seeing that the largest and fastest-growing companies are currently technology companies.

Given all of the above and with the increasing cyber threats, more and more companies prioritize identity security as a key point in their security strategies. This is reflected in the increased acquisition of technologies such as IAM (Identity and Access Management), PAM (Privileged Access Management), and MFA (Multifactor Authentication), as well as in recommendations from entities like Gartner, which place some of these technologies as key in the company's strategy and highlight their importance.

Privileged accounts bring other problems that must be taken into consideration, depending on the system being managed. Many passwords are written in the system's code, which is a bad practice, although more common than thought. However, it is done to protect the availability of the systems, which can result in keys not being changed for years. The security breach is further exacerbated when it comes to former employees.

In addition to the above, human errors must be considered. Humans are fundamental to organizations; however, several security breaches are generated in human resources. Among the most common errors, often due to lack of training in information technology, is saving passwords in inappropriate places like Excel, sharing passwords, leaving sessions open, all of which increase the likelihood of being attacked.

**What is identity governance and what does it encompass?**

Identity Governance (IDG) refers to the set of processes, technologies, and policies used to manage digital identity within an organization. This involves defining the roles of identities (which systems, how, and with what privileges and authorizations an identity can access) and ensuring proper management of these assignments. A digital identity can be a person who is part of the organization, a provider, or a system with a digital identity. Identity governance includes provisioning and de-provisioning identities, as well as access management.

**What to consider for effective identity governance?**

For a company to adopt identity governance effectively, the following recommendations should be considered:

Identify the identities, the scope of these identities both internally and with strategic allies and providers, and the risks associated with their management. Likewise, identify users with high privileges and the accounts they have access to. A consultation on identity governance is recommended for this.

Developing policies and procedures that clearly outline identity management within the company, including how users will be created, deactivated, with what authorizations, and under what scheme and procedure, must align with the best security and data privacy practices.

Analyzing and implementing appropriate IAM (Identity and Access Management) and PAM (Privileged Access Management) technologies is essential. For this, it is recommended to create a needs matrix, considering the number of users who will have access to the technology and the scope of business cases and technologies of the company that need to be integrated. This preliminary analysis is crucial for the successful adoption of technology, allowing the company to properly leverage what is acquired and avoid underutilized technologies.

For the above point, it is very important to have a strategic partner for consultancy, implementation, and deployment of technology. Having the right partner with experience and knowledge in identity governance, as well as other aspects of security, is key to success.

Involving and educating users within the organization on how to keep their passwords and access secure, as well as the importance of technological adoption, will make the process smoother and reduce resistance to change.

Continuously monitoring and reviewing compliance with identity management policies, the consistency of the data handled, and the effectiveness of the applied controls can be achieved through audits and constant analysis of identity management.

Another good practice is integrating IAM and PAM solutions with other security tools for timely detection and response to security incidents.

Lastly, compliance with regulatory requirements governing the industry and country, such as data protection laws and security standards like ISO 27001, must be taken into account.

# Maximizing Cyber Resilience

By Almudena Abolafia

In the ever-dynamic landscape of cybersecurity, proactive prevention and preparedness are essential.

In this article, we will explore how the strategic integration of Cyber Threat Intelligence (CTI) and Adversary Simulation can enhance organizations' cyber resilience. These two disciplines, when effectively combined, offer a holistic approach to identifying, assessing, and mitigating key cyber threats.

When we talk about CTI, we're not just talking about collecting data; it's much more than that. It's a dynamic and continuous process of data collection, thorough analysis, and application of specific threat information, malicious actors, or threat actors, as they are more commonly known, and their motivations. This intelligence can come from external sources such as threat feeds and publicly disclosed IOCs, as well as from internal sources such as security event logs identified by Blue Team teams or threat hunting activities on an organization's internal network to identify signs of malicious or unauthorized activity. By understanding the tactics, techniques, and procedures (TTPs) of adversaries, organizations can anticipate and prevent these attacks by generating detection rules based on these TTPs, and counter cyber threats more effectively.

On the other hand, Adversary Simulation, often confused with "Red Team exercise," goes beyond the classic pentesting or intrusion testing, where the focus is on identifying vulnerabilities. In this case, we're talking about emulating threat actors and replicating, as much as possible, the TTPs they use in their attacks, allowing for an assessment of the resilience of an organization's security posture and providing a realistic view of its detection and response capability to the possible vulnerabilities and weaknesses they would face in a real cyberattack. The main difference between an Adversary Simulation exercise and a Red Team exercise lies precisely in the need for collaboration between the CTI team and the Red Team during the exercise preparation phase.

**How does a CTI team enrich a Red Team?**

The synergy between the CTI team and the Red Team is crucial for an effective cybersecurity posture. Threat Intelligence (CTI) informs and customizes adversary simulation scenarios, significantly enhancing the Red Team's ability to design an attack scenario tailored to the organization's main threats. For example, the CTI team's identification of APT38 as a malicious actor focusing on financial institutions allows a Red Team serving a bank to model specific attacks based on the same TTPs and artifacts used by this threat actor, helping the organization identify its main points of failure and increase its cybersecurity maturity by improving its detection and response capabilities to cyberattacks.

For this synergy to be successful, the following activities must be carried out:

Identification of Key Threat Actors: Identify the main threat actors operating in the organization's sector and/or those who have recently affected its competitors, providing context on the TTPs used and attack objectives. This exercise is conducted by the Threat Intelligence (CTI) team during the "preparation phase" of a cyber exercise or cyberattack.

Attack Modeling Based on CTI Information: Model attacks based on the CTI information previously obtained, allowing for the design of realistic attack scenarios.

Customization of Attack Scenarios: Personalize attack scenarios, taking into account the specific tools (artifacts) and techniques used by the threat actor groups to be emulated against the target organization.

Vulnerability Analysis: Analyze the vulnerabilities that will be targeted for exploitation during the exercise. Understanding them will enable organizations to identify where to focus for proactive detection and rapid response to improve their security posture and minimize the impact of potential security breaches.

By aligning Red Team simulations with specific threats, organizations can maximize the efficiency of their security resources, focusing them on the most critical areas. Additionally, constant feedback between the CTI team and the Red Team ensures continuous improvement of the service, adapting the organization's security posture to emerging threats.

At NTT DATA, we believe that the deep integration of Threat Intelligence and Adversary Simulation services represents a crucial milestone in the evolution of cybersecurity strategies. Therefore, within our service catalog, we promote the execution of these exercises because, by combining these two disciplines, organizations will benefit from defending against current threats and strategically positioning themselves to address emerging challenges that may affect their sector. Cyber resilience and effective cybersecurity go beyond protection; they are the result of a proactive and evolutionary mindset.

The synergy between Threat Intelligence and Adversary Simulation is the path to a more robust and adaptive security posture, maximizing the cyber resilience of any organization.

# Artificial Intelligence: Navigating the Border Between Defense and Offense

By Mafalda Maciel Querido

We have found that Artificial Intelligence is not just a new buzzword or a "sexy" trend in the world of technology. In fact, Artificial Intelligence incorporates fields that we have known for a long time, such as Machine Learning and Deep Learning, with proven evidence, and now it has a new focus and its use has been democratized. However, its rapid evolution and use by society, as several studies have already shown, concern cybersecurity professionals. Furthermore, I would say that society will inevitably have to face it.

We can see the problem from two perspectives. On the one hand, we know that this technology will change the way we work, accelerate slow processes, allow for increased productivity, and address the shortage of professionals in this field. Organizations that do not jump on the innovation bandwagon will inevitably fall behind, as we have historically seen. On the other hand, we know that the line between the positive aspects and the imminent dangers brought by Artificial Intelligence is thin, and attackers typically strive to stay one step ahead. Like any hero, Artificial Intelligence will also have its villain.

The positive impacts that Artificial Intelligence brings to cybersecurity are undeniable: greater and better automation in threat detection and response, with the ability to analyze massive volumes of data at unprecedented speeds and thus identify anomalies more quickly, allowing security teams to anticipate risks and threats more effectively. It also helps in addressing the shortage of specialized human resources that we are experiencing; faster pattern and behavior analysis; adaptive systems that evolve to address new threats; increased predictability and the ability to make data-driven decisions more quickly. In summary, Artificial Intelligence can and should be used as an ally, helping us in terms of productivity, information analysis, and response speed in this rapidly transforming environment.

However, like any technology, it also brings new risks and, for cybersecurity, represents a new factor of speed, sophistication, and scope of attacks. As defense barriers evolve, so do the tactics used by malicious actors. Automation leads to the exploitation of vulnerabilities on a large scale. These actors, benefiting from the adaptability of systems, learn new ways to bypass security barriers as they encounter them. They employ tactics of deception and evasion that mimic legitimate human behavior, making them harder to detect. They utilize AI-driven reconnaissance for a comprehensive and faster analysis of potential targets, identifying vulnerabilities and entry points into an organization's infrastructure. They have the ability to create highly targeted and convincing phishing, smishing, and vishing messages, which, combined with the use of deepfake technology, elevate the entire field of social engineering to a more sophisticated, unpredictable, and difficult-to-detect level, bringing new disruptions to the precautions and defense mechanisms with which we must equip our employees.

In addition to the moral and ethical conflict arising from the use of Generative Artificial Intelligence —on which more and more institutions, both state and non-state, are conducting research—and the dangers related to the unintentional sharing of personal data and sensitive information, whether due to ignorance, lack of technological measures for prevention, or even negligence, there is an increased exposure of what many consider the weakest link, and for others, the first line of defense of organizations: the human element.

The massive use of this new technology has only just begun, and it already has a greater reach than any other technology or platform seen before, and the consequences are already being felt. Although there are not yet extensive studies on the impact that Artificial Intelligence will have on information security and cybersecurity from the perspective of human risk, or very specific statistical analyses, the first cases of attacks perpetrated based on Generative Artificial Intelligence technologies are already emerging.

Awareness among employees and society in general regarding Information Security remains one of the least evident and most difficult points to execute. We still face the challenge of preparing and alerting employees of organizations about the risks and importance of security, and doing so effectively to yield results. These results are difficult to measure because there are many variables that are hard to quantify and qualify.

So, how should we proceed in the face of these new and improved threats? How do we teach people to detect increasingly believable attacks at first glance? How do we detect anomalous behaviors when they increasingly resemble our own? Will we have to reinvent ourselves, and reinvent the way we raise awareness among our employees? At this moment, doubts arise for which, for now, we have few concrete answers.

Security teams must rethink their approach, adopting a proactive stance and adapting to the new reality generated by the implementation of advanced defensive technologies, with a central focus on maximizing automation, threat detection, operational agility, and improving decision-making. The urgent need to overcome resource limitations is undoubtedly an area where Artificial Intelligence emerges as an essential ally.

Relying on AI not only as a solution to resource shortages but as a strategic approach to facing constantly evolving risks and threats is imperative. In this sense, the reorganization of security teams should incorporate not only the implementation of advanced technologies but also the continuous exploration of new methodologies aligned with emerging challenges.

Building a strong security culture is crucial for long-term effectiveness, involving not only training employees with updated knowledge but also promoting a vigilant mindset in daily activities, both professional and personal. We must encourage critical analysis, constructive skepticism, and the application of best practices in all aspects of daily life, thus establishing a solid line of defense.

Ultimately, the convergence of technology and cybersecurity is a challenging area that requires the strategic union of Artificial Intelligence with human capabilities. Recognizing the inevitability of this technological battle of titans and embracing Artificial Intelligence as an indispensable ally is key to strengthening organizations against emerging threats.

# Threat Landscape in the Mining Sector

By Julissa Emily Calderon

The technological evolution in the mining sector, digitalization, and the adoption of advanced technologies to optimize their production processes, such as autonomous drills and trucks, digital twins, among others, are creating an increasingly connected operational environment. This has introduced new risks and expanded the surface of cyber threats that companies in this industry must face.

**Cyber Espionage**

Most mines worldwide are targeted to gather business intelligence information. Cybercriminals may be sponsored by interest groups that view mining companies as a "treasure" or even by national states launching espionage campaigns, as mining is an economically relevant sector for any country.

Information about geological exploration, the value of natural resources, corporate pricing strategies, and technological patents for exploration, extraction, and processing contain confidential and attractive intellectual property data for these attackers.

**Third-Party Access**

Mining companies often work with many external suppliers throughout the production chain, which often do not follow good security practices, compromising operations significantly.

Incidents related to supply chain attacks are a growing trend and pose a significant risk, as cybercriminals seek to reach their targets through trusted providers who are a key part of the value chain and critical processes of companies. The lack of establishing rules and permissions with minimal privilege in their network connections leaves access doors wide open and vulnerable to threats such as malware, which could infect the network and even reach industrial control systems, considering that many companies still do not have segmented their IT/OT networks with robust perimeter security controls. Recently, it has been known that APT attacks in industrial companies have used providers as a stealthy access window that has compromised operational continuity.

**Phishing Campaigns**

Phishing campaigns target mining personnel, not only high executives but also operations superintendents, control system supervisors, instrumentation technicians, and operators.

A notable attack was the one experienced by the Canadian mining company Goldcorp, which lost approximately 16GB of confidential information, including employee identifications, credentials, and budgetary documents, due to this threat.

Therefore, having an awareness program aimed at employees according to their role and functions in the company, who understand their participation and role in the company's cybersecurity, is important. Not all staff are exposed in the same way or will have a common attack vector, so specialized programs for each profile are important to ensure they are prepared for any dangerous situation.

Threats in the sector are evolving at an increasing rate for the mining industry, so it is important for operations managers to understand the current landscape of the risks they are continuously facing. There is a significant challenge in defining actions that allow companies to manage risks that may affect and compromise industrial operations, so they must be clear on how crucial it is to be prepared to protect their main assets to prevent real-time threats and block emerging attacks, applying "zero-trust" controls and policies to shield themselves against any attack.

# Navigating Privacy in an Interconnected World

By Emily Pereda

En la era de la hiperconectividad, nuestra vida cotidiana se ha visto profundamente transformada por la tecnología, ofreciendo comodidades y eficiencias que eran inimaginables hace apenas unas décadas. Dispositivos IoT, sistemas de domótica, y vehículos conectados han convertido lo que antes eran conceptos futuristas en componentes integrales de nuestra realidad diaria; sin embargo, esta transformación digital viene acompañada de crecientes preocupaciones sobre la privacidad y seguridad de los datos personales. Como profesional en ciberseguridad, y más recientemente, como madre, mi percepción sobre la tecnología ha evolucionado hacia una reflexión más crítica sobre cómo estas innovaciones afectan la privacidad y seguridad de nuestras familias.

**IoT and Home Automation: Convenience at the Cost of Privacy?**

The promise of a smart home has been realized through IoT devices and home automation systems, giving us remote control over lighting, climate control, and security. However, the convenience of these devices comes with inherent risks. Each connected device represents a potential attack vector for cybercriminals, who could access sensitive personal data or manipulate the functionality of home systems. For example, a targeted attack could compromise security cameras, revealing intimate details of our daily lives or allowing intruders to monitor our movements.

How many times have we come across stories or videos about children developing a fear of surveillance cameras? These tools, installed by us to provide peace of mind by being able to watch over our little ones while we attend to other tasks or even monitor them remotely while we're at work, are supposed to be a secure and reliable resource. However, reality can be different. Fear in children arises when their space, which should be one of safety and comfort, is violated. Documented incidents show how unauthorized individuals manage to access these cameras, interacting with children and transforming a protective environment into one of vulnerability and fear.

This intrusion not only breaches the physical security barrier we try to maintain around our children but also infringes upon the trust and sense of security that these devices are meant to provide. When a child feels threatened in their own home, the harm goes beyond a simple act of privacy invasion; it becomes a matter of emotional and psychological safety. The crucial question that arises then is: How can we ensure that technology designed to protect our loved ones does not become a source of anxiety and fear for them?

Addressing this concerning question involves tackling the problem from multiple angles, prioritizing both technological security and open communication and education. Firstly, it is essential to select surveillance devices from reputable brands that offer high levels of security, including advanced encryption and two-factor authentication, to make unauthorized access more difficult. Additionally, keeping the software of these devices constantly updated ensures that any known vulnerabilities are promptly addressed.

On the other hand, education and communication play a key role. It is essential to teach children about technology in an age-appropriate manner, explaining how these cameras work and the purpose they serve, reinforcing the idea that they are designed to keep them safe. Furthermore, it is important to listen to and validate their feelings if they express fear or concern, reassuring them that they are protected and that security measures are in place for their well-being. With robust technological security measures combined with effective and empathetic communication, we can use surveillance technology to maximize safety without compromising children's sense of security and comfort in their homes.

In the case of younger children who cannot yet speak or express themselves clearly, the situation is more challenging since they cannot directly communicate what is happening to them. Here, the setup we choose plays a fundamental role in addressing these difficulties.

# Continuous Evolution: Beyond Biometrics

Por Nelvys Pamela Porras

With the relentless advance of technology, artificial intelligence (AI) emerges as a key player in the transformation of access management. The ability of AI to analyze and adapt to user behavior patterns offers an additional layer of security. Machine learning-based systems can identify anomalous activities and detect potential threats before they materialize, providing a proactive response instead of a reactive one.

The search for new forms of authentication does not stop at biometrics and multifactor authentication. Behavior-based authentication emerges on the horizon as a possible futuristic frontier. This approach involves analyzing how a user interacts with devices and platforms, evaluating unique behavior patterns. As algorithms improve, this form of authentication promises to be more resilient to threats and less invasive for the user experience.

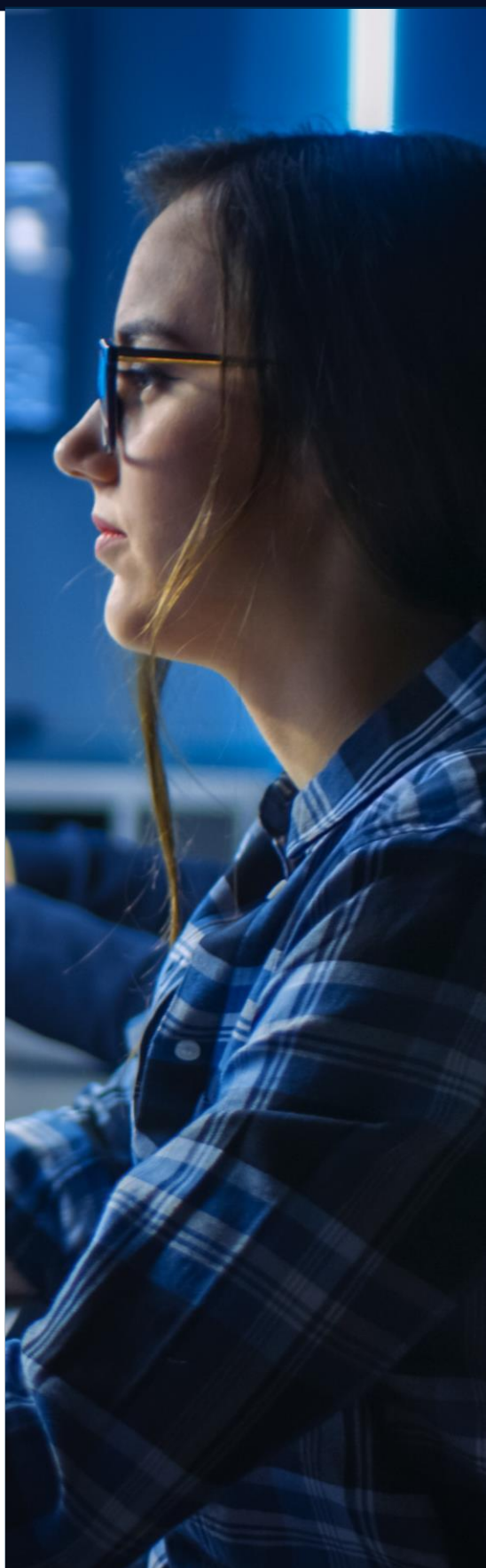
Traditional passwords remain a weak point in digital security. Threats of brute force attacks are constantly evolving, leveraging increasing computing power and the sophistication of techniques; nowadays, we observe how these emerging threats challenge the integrity of passwords and how the industry responds to these ever-evolving challenges.

Understanding user trends, factors contributing to the choice of weak passwords, and the tendency to reuse passwords should be considered. Understanding these aspects provides deeper insights into how security practices can adapt to address not only technological threats but also human behaviors that jeopardize security.

While fingerprints and facial recognition have been pioneers in biometrics adoption, recent improvements can be observed. Technologies such as retina scanning, voice, and handwriting dynamics are gaining ground, providing a wider range of biometric options. These advanced technologies address the security and privacy challenges associated with biometrics.

Biometrics are not limited to unlocking phones or managing photos; they are being integrated into sectors such as banking, healthcare, and transportation, transforming the way we interact with essential services and ensuring more secure authentication in multiple scenarios.

Concerns about the privacy and security of biometric data remain a central issue; to address these concerns, innovative solutions are being observed, such as data decentralization and the use of blockchain, which aim to address these concerns. Additionally, government regulations and industry standards are evolving to safeguard the integrity of biometric data.



Technological advances are evident in strengthening biometrics, from improvements in sensor accuracy to the integration of artificial intelligence for detecting impersonation attempts. These developments aim to address previous challenges and improve the overall acceptance of biometrics as a secure and reliable method.

The elimination of passwords and the adoption of biometrics aim to enhance the user experience; user-centered design shapes intuitive interfaces and secure authentication processes that are accessible and friendly to everyone, regardless of their level of technological expertise.

Analyzing resistance to change in the adoption of new authentication technologies, as well as understanding the psychology behind resistance to change, will allow for the development of effective strategies for transitioning to more secure and advanced authentication methods.

Beyond biometrics and multifactor authentication, examining new forms of authentication that may emerge in the future, from brainwave authentication to DNA-based authentication, becomes relevant in determining the boundaries of innovation and how they could further revolutionize digital security.

The constant transformation in the technological realm brings unexpected challenges; anticipating potential ethical, security, and privacy dilemmas that may arise with new authentication technologies will allow the industry to prepare and mitigate potential risks.

The elimination of passwords and the adoption of biometrics not only represent a shift in access management but also mark the beginning of a broader revolution in digital security; the milestones achieved so far highlight how the industry is leading the forefront of innovation and outlining perspectives for a secure, efficient, and user-centered digital future.



# Awareness in your daily life... Why not?

By Stephanie A. Ramos

When we think about awareness, it always comes to mind whether users in companies understand and have knowledge of what this word, activity, or action entails, and the reality is that if we look around in most companies, it remains a poorly managed topic. Now, if we think as individuals in daily life, who really carries out awareness topics regularly?... Very few.

If we shared this important topic with the importance it entails, we would surely avoid many security incidents, not only in our work life but also in our daily lives, giving fewer opportunities for extortion, exposing ourselves to the companies where we work, colleagues, and loved ones.

Have you ever wondered how you would start a strategy from your personal standpoint? What would you stop doing? How would you communicate this to your family and friends? We know that being in a cybersecurity world, the topic might be a bit simpler since we have the context at hand, and not only because of work, but we in cybersecurity understand and are aware of the global context. It's absurd that having this context and all that firsthand information, we are not doing anything. We continue to upload personal photos without due care about what we show in them, registering on sites whose security we are not sure about, accepting privacy notices that we never read completely, and responding to text messages and WhatsApp messages about things we can't explain how they reached us. And when we look back at the how and when, we fall into that small line that makes us so vulnerable.

What is awareness? If we google it, the literal translation is "conciencia" (awareness).

Awareness in cybersecurity refers to training on the importance of cybersecurity, empowering users through automated and personalized simulations of phishing attacks and malware, reducing the number of successful cyberattacks in companies.

Now, do we really have "Security Awareness"? How aware are we of what we do in our daily lives? If we always had that information present of what we should not expose and at the same time applied and shared it with our family nucleus, it would be much easier to create that network of good practices. Yes, it would be much easier because we would share these good practices in a natural way, with a simple "Don't upload photos of the house," or "Hey, remove your work location data from your social networks, there are specific platforms for that," or "Hey, daughter/son, be careful with the images you share from your school," or "Hey, be careful with your account passwords," among others.

Considering all the good practices shared with us in our jobs, all the actions we take in our daily work life, do we meet the deadlines for training? Do we really understand the guidelines? How can we stay updated if we are not paying attention to the firsthand information that has the best intention of creating awareness about security?

Many questions, few answers, well... let's make it worthwhile to have good awareness practices in our daily lives.

The recommendations are actually simple:

- Don't share your information on any platform.
- Make sure that QR codes, which seem so innocent and practical, are from the place you want to enter.
- Don't open unknown incoming emails out of curiosity! ... nothing is free, and the most logical thing can be the most illogical.
- Be suspicious when receiving messages or calls from strangers, and especially if they are from "acquaintances" but question topics or request something that isn't common. Why not? Ask or question. After all, if it's a friend or family member, of course, there's that trust and peace of mind. And if it's a colleague, even more so.
- If we know that in the company we use MFA or, colloquially, that double check of access to an app, system, account, etc., why not ask our close family members to apply it in their activities? With a casual 5-minute conversation, we can explain it at home.
- When it comes to passwords, many people tend to rely on their name, birthday, or pet's name. Let's be clever, show love for our security, and remember that if something has a password, it's because we surely store important information in it.
- What about the tickets we indiscriminately throw away? We don't have the caution to check if they contain any data that any curious or interested person could collect. You might think, "No, that only happens in movies." Well, have you considered that movies often become reality?

Why use personal devices for work matters when we can do it securely? As we're talking about awareness and being conscious of cybersecurity, why do we forget to be aware of the information we handle on our mobile devices? It's simple: don't download or share company-related content through unauthorized means.

I could go on with a few more points, however, it's important that, at the end of reading this, you take away how you live awareness topics day by day in the office, at home, with friends, and in society. Let's not make it easy for those who want our information or see us as access to data that doesn't even belong to us.

Let's make these practices our own, let's share them, let's create that network or strategy from our personal standpoint. And let's complicate accessibility to our privacy.

# Cyber Chronicle

We begin this month's cyber chronicle with news of a report by the cybersecurity company ESET, detailing the threat landscape in Spain and worldwide. According to the report, Spain stands out as one of the countries with the highest number of threat detections, trailing only behind Japan and the United States.

We continue this month's cyber chronicle with news of a report by the cybersecurity company ESET, detailing the threat landscape in Spain and worldwide. According to the report, Spain stands out as one of the countries with the highest number of threat detections, trailing only behind Japan and the United States.

The most popularly detected threat continues to be phishing, accounting for nearly one-third of all detected threats. The report warns of an increase in techniques used by cybercriminals, with the use of artificial intelligence becoming increasingly prominent. These techniques add sophistication to attacks by generating fake content, photomontages, deepfakes, or impersonations of relevant individuals. It is expected that the trend in these types of attack attempts will increase given the rapid growth of such tools and their increasingly easy accessibility, which is already happening and leads us to other terms, such as smishing and vishing.

Smishing, a type of phishing via SMS, follows a structure very similar to that of email phishing. It involves sending out hooks en masse, hoping that users will fall for the deception. The two most common operating methods are impersonating delivery service companies, telecommunications companies, or banks, and impersonating family members or acquaintances.

Regarding vishing, the Civil Guard has recently warned about the increase in this type of fraud and has advised the population to be cautious and careful, as advances in artificial intelligence technology make impersonating individuals through video calls increasingly realistic.

This leads us to discuss the professionalization of fraud, which has been increasing in recent years. There are reports of companies abroad dedicated expressly to setting up call centers pretending to be customer support teams for various services with the intention of defrauding potential users through the use of their information.
The YouTube user known as Savitar (who shares content related to ethical hacking and cybersecurity) recently recounted in one of his videos how a hacker dedicated to uncovering scams of this type operated. The methodology used was to gather information from these call centers after infecting all their equipment, and then contact the authorities to intervene and shut down the operation. The office from which they operated seemed quite professionalized, with it even being possible that some of the people working there were unaware of the illegality of their actions.

To emphasize this, an article from the ITUser portal describes how cybercrime now operates like any other business, with its objectives being equivalent to those of legitimate enterprises (cost reduction, efficiency improvement, and revenue generation), with these activities reaching a value close to 1.5% of global GDP. Paradoxically, the population's perception of their vulnerability to cyberattacks does not progress in line with their impact and popularity. As emphasized by the National Coordination Center of the INCIBE: "In general, year after year, users think they are less targeted. But, however, the real trend is increasing. In fact, the percentage of users reporting malware on their computers is very low, especially when compared to reality."

To conclude this month's cyber chronicle, it is important to note that, given the increase in cyber fraud amid the population's lack of perception, special attention should be paid to new technologies that are increasingly integrated into our lives. According to various sources, the most common attack vector so far remains email, through which computers or mobile devices can be infected. However, this situation may be very different in the not-too-distant future.

We have recently seen news in which companies like Apple released their new augmented reality glasses to the market, or even how the company Neuralink was conducting tests with a brain chip. We believe that the fraud industry is still far from approaching these devices, but as the supply and use of such technologies increase, the industry will see them as new attack vectors.

# Harvest Now, Decrypt Later

**Trends**

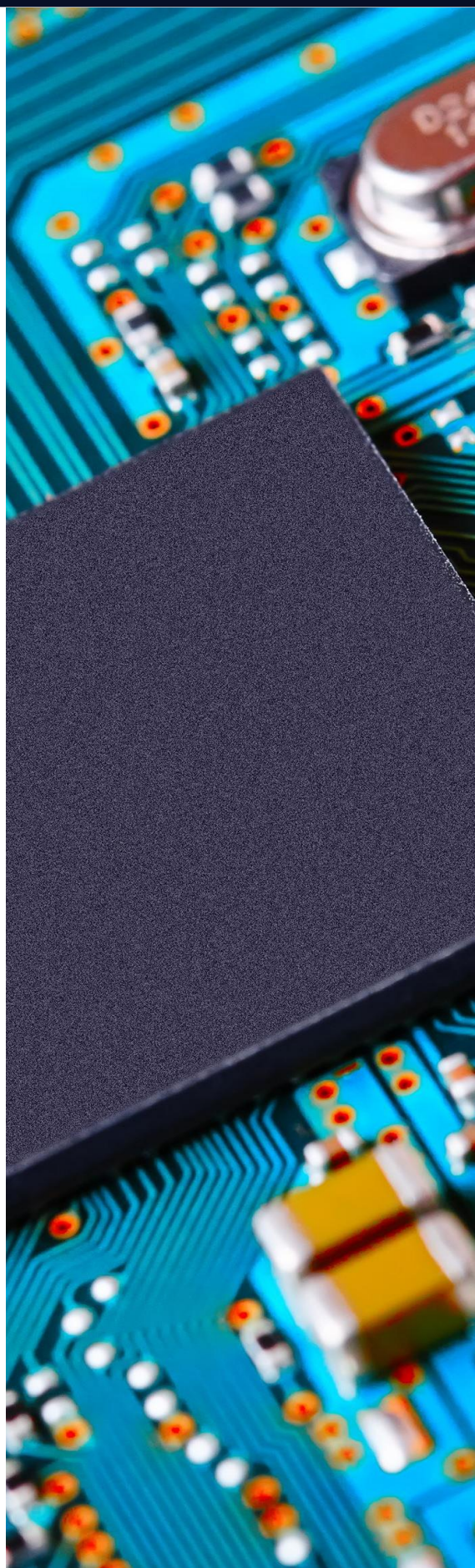
Over the past years, there has been extensive discussion about the potential global impact that widespread access to quantum technology could generate. As its operation and performance are becoming increasingly relevant, international cybersecurity institutes have initiated actions to try to establish preventive measures against the eventual revolution that this new technology could cause.

Unlike classical computers used today, where bits are used to represent information as 0 or 1, quantum computers use qubits, which not only represent classical bits but also incorporate an additional state where both are represented at the same time through a phenomenon called superposition. This provides a capacity to perform exponentially larger calculations than a conventional computer, posing a threat to current cryptographic systems that rely on computational difficulty to solve them. For this reason, there has been a growing interest in the development of quantum-resistant cryptographic algorithms.

To date, the security protocols used to protect the integrity and confidentiality of data are primarily based on RSA and ECC encryption. According to multiple studies conducted by the World Economic Forum, in addition to the timelines established by the CNSA, quantum computers pose a threat to these security encryptions as they would be considered vulnerable due to the computing power presented by this new technology. It is estimated that this global security gap could occur as early as the beginning of 2030. Therefore, classical systems are considered vulnerable to "Harvest now, decrypt later" (HNDL), where malicious actors steal and store data to decrypt it later if they obtain access to quantum computers.

Both IBM and Palo Alto have begun to express their action plans to prevent and counteract this future problem, especially after the message published by the National Institute of Standards and Technology (NIST), announcing that it will begin this year to develop and establish secure cryptographic standards against quantum computing. With the four "post-quantum" (PQC) ciphers chosen in 2022 after 6 years of international research and NIST's announcement in August 2023 about its plans to standardize 3 of the winning ciphers, their approval and implementation are expected to take place throughout 2024. These ciphers are: "Crystals Kyber," "Crystals-Dilithium," and "SPHINCS+."

With the continuous advancement of quantum computing development led by companies like IBM, Google, D-Wave, and IonQ, NIST's contribution provides immense support to mobilize all sectors dependent on the security of classical encryptions. The trend observed in recent months suggests that the year 2024 marks the beginning of significant changes in security protocols. This movement reflects the growing awareness of the need to adapt to the quantum era, highlighting the importance of developing and adopting quantum-resistant algorithms to continue securing the integrity and confidentiality of data.



# Vulnerabilities

## Remote code vulnerability in Cisco products

Date: 24th January 2024
CVE: CVE-2024-20253


### Description
Cisco has reported a critical vulnerability affecting a large number of its products.

This is a remote code execution vulnerability, caused by the inadequate processing of user-supplied input data. An attacker could exploit the vulnerability by sending a specially crafted message to a listening port on the affected device.

By exploiting this vulnerability, an attacker could execute arbitrary commands on the device's operating system with the user privileges of the web service. Additionally, with access to the operating system, the attacker could establish root access permissions on the system.

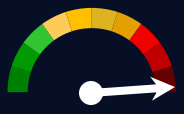
### Products affected
The vulnerability affects the following products:
- Unified Communications Manager (Unified CM)
- Unified Communications Manager IM & Presence Service (Unified CM IM&P)
- Unified Communications Manager Session Management Edition (Unified CM SME)
- Unified Contact Center Express (UCCX)
- Unity Connection
- Virtualized Voice Browser (VVB)

### Solution
The manufacturer has released updates for the affected products.

### References
- www.incibe.es
- sec.cloudapps.cisco.com

## Multiple Vulnerabilities in Fortinet Products

Date: 8th February 2024
CVEs: CVE-2024-23113 y 1 más




### Description
Fortinet reported last Friday two critical vulnerabilities in its FortiOS operating system.

The most critical vulnerability, CVE-2024-23113, is an externally controlled format string vulnerability (CWE-134), such as through user input, in the FortiOS fgfmd daemon.

The second vulnerability, CVE-2024-21762, is an out-of-bounds write vulnerability (CWE-787).

Exploiting either of these vulnerabilities could allow an unauthenticated remote attacker to execute arbitrary code or commands using specially crafted requests.

### Products affected
The mentioned vulnerabilities affect the following versions of the FortiOS operating system:
- FortiOS 7.4: Upgrade from version 7.4.0 to 7.4.2.
- FortiOS 7.2: Upgrade from version 7.2.0 to 7.2.6.
- FortiOS 7.0: Upgrade from version 7.0.0 to 7.0.13.
- FortiOS 6.4: Upgrade from version 6.4.0 to 6.4.14.
- FortiOS 6.2: Upgrade from version 6.2.0 to 6.2.15.
- FortiOS 6.0:

To view the rest of the affected products, you can refer to the provided links.

### Solution
Fortinet recommends disabling SSL VPN as a workaround and updating FortiOS to the following versions or higher: 7.4.3; 7.2.7; 7.0.14; 6.4.15; 6.2.16.

### References
- www.incibe.es
- www.fortiguard.com
- www.fortiguard.com

# Patches

CRITICAL **New Security Patches for GitLab CE/EE**

Date: 25th Januarye 2024
CVE: CVE-2024-0402 and 4 more

## Description

GitLab released a series of security patches on January 26th to address a set of 5 vulnerabilities, one of which is categorized as critical, while the others are rated as having medium severity.

The critical vulnerability, CVE-2024-0402, could allow an authenticated user to write files to arbitrary locations within the GitLab server when creating a workspace. This security loophole could lead to the distribution of malware.

The remaining vulnerabilities addressed in this security patch could allow for the following actions:

- Trigger a DoS attack (CVE-2023-6159).
- Access or exposure of confidential data (CVE-2023-5933 and CVE-2023-5612).
- Assign any user without restrictions to merge requests (MRs) created within a project in GitLab (CVE-2024-0456).

## Products affected

The affected GitLab versions are as follows:

- 12.7 prior to 16.6.6;
- 13.7 prior to 16.6.6;
- 14.0 prior to 16.6.6;
- 16.0 prior to 16.5.8;
- 16.6 prior to 16.6.6;
- All versions prior to 16.6.6;
- 16.7 prior to 16.7.4;
- 16.8 prior to 16.8.1.

## Solution

Update to GitLab CE/EE versions 16.5.8, 16.6.6, and 16.7.4. Version 16.8.1 only contains the patch for vulnerability CVE-2024-0402.

## References

- about.gitlab.com
- www.helpnetsecurity.com

CRITICAL **New Security Patches for Android Devices**

Date: 5th February 2024
CVE: CVE-2024-0031

## Descripción

Android ha publicado un nuevo boletín de seguridad que corrige una vulnerabilidad crítica y 45 vulnerabilidades de severidad alta.

La vulnerabilidad crítica consiste en un fallo de escritura fuera de límite presente en la función "attp_build_read_by_type_value_cmd", que de ser explotada permitiría al atacante ejecutar código de forma remota en el sistema operativo del dispositivo, sin necesidad de privilegios de ejecución *system*. Esta vulnerabilidad ha sido identificada como CVE-2024-0031.

Las vulnerabilidades corregidas en el parche afectan tanto al sistema operativo como a componentes del sistema como Arm, MediaTek, Qualcomm, o Unisoc.

## Products affected

Los productos afectados por dicha vulnerabilidad son los siguientes:

- Android Open Source Project (AOSP): versiones 11, 12, 12L, 13 y 14
- Componentes de Arm, MediaTek, Unisoc y Qualcomm

## Solution

Android recomienda comprobar que el fabricante del dispositivo haya publicado un parche de seguridad y aplicar la actualización correspondiente.

## References

- www.incibe.es
- source.android.com

# Events

### Innovate Cybersecurity Summit

This three-day event brings together cybersecurity executives and CISOs from across the USA to discuss and learn within an exclusive attendance framework. This year, it has been organized in Nashville, Tennessee, from February 25th to 27th.

Attendees of this experience have access to panels and training sessions led by CISOs addressing current best practices and challenges, while showcasing the latest cybersecurity technologies and opportunities.

It is a unique event from which valuable information can be learned to position your organization well in terms of protection and response to threats in this field.

**Link**

### Cyber Security World Madrid 2024

The event will take place in the Spanish capital on October 16th and 17th, at Pavilion 9 of Ifema Madrid. It will bring together cybersecurity professionals from corporate, business, and institutional sectors of leading cybersecurity companies worldwide to address the current increase in cyberattacks, their types, and investments in this field to protect organizations' data and activities.

This year, around 400 companies are expected to showcase their cloud solutions, with more than 350 speakers presenting the latest developments in the sector.

**Link**

### Infosecurity Europe 2024

This trade fair will take place from June 4th to 6th at ExCeL London, in the United Kingdom. It will bring together professionals and companies from the field of cybersecurity to discuss the latest developments in the field and share experiences through conferences and events within the fair, where knowledge can be expanded and networking opportunities can be explored.

It is considered one of the most important cybersecurity trade fairs in Europe, as it gathers a large number of solution providers.

**Link**

### Infosecurity México 2024

Event organized at the Centro Citibanamex in Mexico City to delve into cybersecurity, especially regarding the latest trends and methods of information security.

Attendees will have the opportunity to connect with key experts in the information security industry, which can help improve the protection of businesses by finding solutions that adapt to new challenges.

Therefore, the main themes that will be addressed during October 22nd and 23rd will include regulations, cybersecurity threats, and protection for both individuals and public institutions.

**Link**

# Resources

**Training and educational materials for cybersecurity specialists from ENISA (European Union Agency for Cybersecurity)**

Since 2008, ENISA has been providing cybersecurity material for anyone interested in expanding their knowledge. Their website includes information for both teachers and students to complement practical aspects.

The training is divided into four main areas: Technical (topics include forensic analysis, honeypots, and proactive detection), Operational (covering security advisory drafting and cloud incident management), Cooperation and Legal (identifying and managing cybercrime traces, cooperating with law enforcement), and CSIRT Configuration (training to effectively respond to cybersecurity incidents).
Link

**Revolutionizing Identity Management: How Web3 Decentralizes and Secures IAM Systems**

In the following link, DataVeritas explains the innovative field of Web3 and its relationship with the concept of decentralized identity. This revolutionary idea aims to give users full control over their digital identity, reducing the number of vulnerabilities caused by other types of management and the limitations faced by individuals when using them. All of this is fueled by fields such as blockchain and other types of current and innovative IAM technologies.

Web3 is therefore a great choice for decentralized identity management in a more secure manner, overcoming certain current challenges in IAM. It is a solution that has already been successfully tested in sectors such as banking or healthcare.
Link

**NIST Cybersecurity Framework (CSF) 2.0**
This is a Cybersecurity Framework published by the United States National Institute of Standards and Technology (NIST). Its origin dates back to 2014 when it was published with the aim of supporting the U.S. Cybersecurity Enhancement Act. The objective of this guide is to manage and reduce risks, as well as to strengthen cybersecurity measures.

Focusing on the tool itself, the NIST Cybersecurity Framework (CSF) 2.0 Reference Tool would allow studying the CSF 2.0 Core draft. This includes functions, categories, subcategories, and examples of implementation, offering versions readable by humans and machines in JSON and Excel formats, as well as allowing keyword search and terms. Within the tool, the following functions can be found:

- GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy.
- IDENTIFY (ID): Help determine the current cybersecurity risk for the organization.
- PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk.
- DETECT (DE): Find and analyze potential cybersecurity attacks and compromises.
- RESPOND (RS): Take action in response to a detected cybersecurity incident.
- RECOVER (RC): Restore assets and operations affected by a cybersecurity incident.

It is a tool in development and is expected to be completed in 2024, which will allow linking CSF with related cybersecurity frameworks, standards, guides, and resources. In future versions, users are expected to be able to generate their own version of CSF 2.0 Core by selecting other information and resources as a reference.
Link



# Radar
Powered by women

NTT DATA

**Mª Pilar Torres**
Cybersecurity Director

**Marta Fernández**
Cibersecurity Manager

**Mª Angeles Gutiérrez**
Cybersecurity Manager

**Andrea Muñoz**
Cibersecurity Manager

**Almudena Abolafia**
Cybersecurity Manager

**Julissa E. Calderón**
Cybersecurity Project Leader

**Emily J. Pereda**
Cybersecurity Lead Consultant

**Mafalda Maciel Querido**
Senior Lead Analyst Cybersecurity

**Nelvys P. Porras**
Cybersecurity Expert Analyst

**Stephanie A. Ramos**
Lead Analyst Cyber

# Radar

## Powered by women

**Powered by the cybersecurity NTT DATA team**

es.nttdata.com