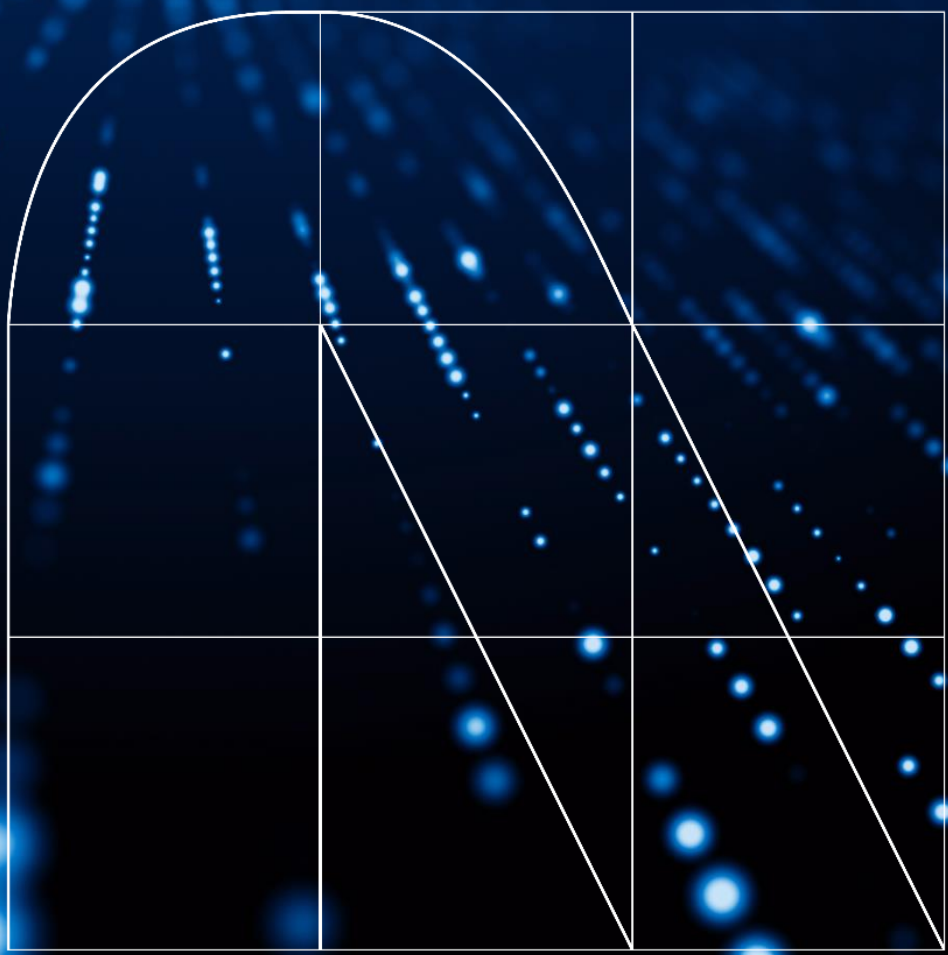
Issue 102 | May 2025

NTT DATA

Radar

The cybersecurity magazine



Navigating the Convergence of Cybersecurity in IT and OT

By Carlos Solano

In today's digital landscape, the convergence of Information Technology (IT) and Operational Technology (OT) has become a fundamental approach for organizations across various industries. As businesses increasingly rely on interconnected systems to drive efficiency and innovation, the need for a robust cybersecurity strategy that encompasses both IT and OT environments has never been more critical. This editorial explores the most relevant strategies for effectively managing cybersecurity in this converged landscape.

The integration of IT and OT brings numerous benefits, including enhanced data analytics, more informed decision-making, and more efficient operations. However, it also introduces significant cybersecurity challenges. OT systems, which control physical processes in industries such as manufacturing, energy, and transportation, were traditionally isolated from IT networks.

This separation provided a level of security, but as organizations embrace digital transformation, the lines between IT and OT are blurring, creating new vulnerabilities and opportunities for attackers.

By creating a cohesive approach between both worlds, organizations can ensure that all teams are aligned in their efforts to protect critical assets. Organizations must adopt a holistic view of their risks, considering the impact on operations.

This comprehensive assessment allows for the prioritization of security measures, ensuring that resources are effectively allocated to mitigate the most significant threats.

Implementing network segmentation is a crucial strategy for protecting OT systems from potential breaches originating in IT networks. By isolating OT environments through firewalls, virtual local area networks (VLANs), and demilitarized zones (DMZs), organizations can contain threats and limit attackers' ability to move laterally between networks.

Establishing strict access control measures is vital to safeguarding critical systems. Organizations should implement role-based access control (RBAC) and multi-factor authentication (MFA) to ensure that only authorized personnel can access sensitive data and systems.

This approach reduces the risk of insider threats and improves the overall security posture.

A unified incident response plan that addresses both IT and OT incidents is essential for effective threat management. This plan should outline roles, responsibilities, and procedures for detecting, responding to, and recovering from cybersecurity incidents. A coordinated response between both domains ensures that organizations can act quickly to minimize damage and restore operations.

Continuous monitoring solutions provide real-time visibility into IT and OT environments, enabling organizations to detect potential threats before they escalate. Using Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), and anomaly detection tools can significantly enhance an organization's ability to respond to emerging threats.

The convergence of IT and OT presents both opportunities and challenges for organizations. By adopting a comprehensive approach to cybersecurity that includes a unified security framework, risk assessments, network segmentation, and continuous monitoring, companies can effectively manage this complex landscape. As we move forward, it is imperative that organizations prioritize cybersecurity in their convergence strategies, ensuring the resilience and security of their operations in an increasingly interconnected world.

The future of industrial operations depends on our ability to protect these critical systems from evolving threats.

Carlos Solano
Cybersecurity Manager

Privacy in AI: A relevant enabler actor that sometimes operates without the necessary controls.

Cyberchronicle by Antonio Melo & Carlos Ortega

As the digital landscape becomes more complex, cybersecurity is emerging as one of the most pressing strategic challenges for businesses, governments, and citizens. Three recent news stories highlight the urgency of strengthening defenses: the alarming 137% increase in DDoS attacks in Europe, Spain's prominence as the primary target of cyberattacks, and Oracle's ongoing investigations into a possible breach in legacy environments related to the CVE-2021-35587 vulnerability.

Europe Under Attack: DDoS Attacks on the Rise

The latest European cybersecurity report reveals that distributed denial-of-service (DDoS) attacks have increased by 137% compared to the previous year.

These attacks, although brief (some peak in just 10 to 60 seconds), have become more sophisticated as they use combined techniques—known as multi-vector attacks—to bypass traditional defense measures.

The speed and precision of these attacks force organizations to adopt real-time mitigation solutions and artificial intelligence-based systems to detect and block malicious traffic flows before they can disrupt critical services.

Spain, the favorite target of cybercriminals

In the national context, recent statements by Indra's president, Ángel Escribano, have highlighted that Spain topped the list of countries attacked in February, surpassing powers such as the United States and Israel.

According to Escribano, Spain's growing technological and economic relevance, driven by an accelerated digitalization process and the expansion of digital infrastructure in strategic sectors, has made the country a prime target for targeted cyberattacks.

The exposure of a large base of small and medium-sized enterprises, combined with a relative lack of specialized cybersecurity professionals, worsens this situation and calls for a coordinated response between the public and private sectors.

Oracle in the Spotlight: Vulnerability in Legacy Environments

On the other hand, Oracle has initiated an investigation into a potential breach related to the CVE-2021-35587 vulnerability in legacy environments.

Although the vulnerability was identified and patched in 2021, it has been found that some older systems still using outdated versions of Oracle Access Manager remain exposed.

This vulnerability, with a CVSS score of 9.8, allows an attacker to gain unauthenticated access to systems via HTTP, compromising the integrity, confidentiality, and availability of the affected applications.

Cybersecurity experts urge organizations to immediately update their environments to prevent this breach from being exploited, which could lead to critical consequences and expand the scope of cyberattacks.

Reflections and Recommendations

El aumento vertiginoso de ataques DDoS en Europa, la consolidación de España como territorio vulnerable y la persistencia de brechas en sistemas legados como el de Oracle son una llamada de atención.

Estas amenazas subrayan la necesidad de que las organizaciones inviertan en tecnologías de detección y respuesta basadas en inteligencia artificial para anticipar y mitigar ataques en tiempo real.

Además, es necesario que se fortalezcan los protocolos de seguridad, actualizando de forma rigurosa y periódica sus sistemas, especialmente aquellos que operan en entornos *legacy*.

The rapid increase in DDoS attacks in Europe, the consolidation of Spain as a vulnerable territory, and the persistence of gaps in legacy systems like Oracle's are a wake-up call.

These threats highlight the need for organizations to invest in AI-based detection and response technologies to anticipate and mitigate attacks in real-time.

Furthermore, it is crucial to strengthen security protocols by rigorously and regularly updating systems, especially those operating in legacy environments.

Antonio Melo
Cybersecurity Analyst

Carlos Ortega
Cybersecurity Analyst

Availability vs Security in Industrial Environments

Article by Miren Ordoñez de Arce

"A hacker accessed the control system of a water treatment plant and caused the mass poisoning of the population of Oldsmar, Florida, in 2021," "Malware targeting a petrochemical plant disables protective mechanisms against catastrophic failures and causes an explosion that kills dozens of people in Saudi Arabia," or "Ransomware attack on a hydroelectric plant causes social chaos due to power outage in South America in 2022." Do these headlines sound familiar? No? Because they didn't happen. But they could have been a reality.

In 2021, in Oldsmar, Florida, a cybercriminal remotely accessed the control system of a plant via TeamViewer and increased the levels of sodium hydroxide (known as bleach) to dangerous levels, over 100 times its normal levels, potentially poisoning the town's water supply. However, an operator detected in real-time the changes made by the hacker and manually reversed them, preventing mass poisoning, hospital overcrowding, and the high costs of decontaminating and restoring the water system.

In 2017, a malware known as "Triton," also called "Trisis," was deployed at a petrochemical plant in Saudi Arabia, allowing cybercriminals to remotely control the factory's safety systems. These systems were the last line of defense against disasters that could threaten human life. They were designed to detect any hazardous situation and take action by shutting down systems completely, activating shutdown valves, and pressure release mechanisms.

If the malware had been successful, it could have disabled these safety systems, allowing undetected attacks or failures to result in explosions or toxic releases. However, the attack was detected when the malware caused a failure in the safety systems, triggering a safe shutdown of operations and preventing further movement or more significant damage.

Finally, in 2022, ransomware encrypted critical files in the control systems of a hydroelectric plant in South America, disrupting plant operations and demanding a ransom to release the data.

In the event of a ransomware success, prolonged disruptions in the power supply could have occurred, affecting millions of users and causing significant economic losses. However, the plant had properly established incident response protocols, allowing for early detection and containment of the attack. Additionally, the implementation of regular backups enabled the restoration of the affected systems without the need to pay the ransom, minimizing the impact of the attack.

These are just a few examples of the physical, human, economic, and reputational consequences that a cyberattack can cause in an industrial environment; and all of this stems from the exposure of industrial networks, which were previously completely isolated.

Although the first smart factories began to appear in 2014, it wasn't until 2016 that the term "Industry 4.0" started to be heard, referring to the integration of advanced production and operation technologies with intelligent technologies that communicate with each other throughout the supply chain, achieving process automation, personalized production, and increased efficiency, among others.

However, this has also made industries a lucrative target for cyberattacks, primarily due to:

- The increase in connectivity: the use of IoT devices in industrial environments has revolutionized the monitoring and control of assets, but it has also created multiple potential entry points for cyberattacks.
- The integration of new technologies with old ones: virtually most industries operate with legacy systems that were not designed with modern security in mind, leaving security gaps.

- The digitization of processes: the increase in automation and the ability to remotely control systems expand the attack surface.
- Human interaction: employees are the weakest link in the chain and, in many cases, are not adequately trained in cybersecurity practices, making them targets for social engineering attacks, carelessness, and mistakes.
- The increase of advanced threats: critical infrastructures are a highly lucrative target in terms of damage caused, as there is often interdependence between sectors, which can amplify and multiply the impact.

It is well known that in industrial environments, system availability is a priority over confidentiality or integrity, precisely due to the critical nature of industrial operations.

In many cases, industrial operations run continuously (such as in a power plant), so they cannot afford interruptions. Additionally, the consequences of downtime result in significant financial losses or even pose physical security risks.

On the other hand, many industrial systems require real-time responses for controlling critical processes, which is ensured through availability. It is also worth mentioning that these systems, in addition to being outdated, were designed with a focus on resilience, not security. Lastly, it is often observed that the risk of an interruption is greater than the risk of a security breach.

This is not new; nor is it a fact that was established a year ago, or five years ago. So, why isn't industrial cybersecurity given more importance? Is it only when a cyberattack occurs that real measures are taken? Is system availability really that prioritized?

This is not new; nor is it a fact that was established a year ago, or five years ago. So, why isn't industrial cybersecurity given more importance? Is it only when a cyberattack occurs that real measures are taken? Is system availability really that prioritized?

Let's imagine a car manufacturing plant, operating 24/7 to meet global demand, and one ordinary day, it suffers an attack that disrupts the production control software, shutting down the plant for days.

If the plant is forced to halt production, each hour of downtime could cost hundreds of thousands of euros, not to mention the reputational damage and potential additional penalties for contractual breaches. Had the plant considered security, although the initial cost of securing it would have been substantial, it could have prevented the attack or at least minimized the impact.

Although the systems themselves can fail and create a risk for operators, such as in the case where an assembly part could become suspended, causing a risk situation due to an interruption, the truth is that this can also be caused by a malicious actor, as we have seen with the mentioned cyberattacks. Therefore, by increasing security, malicious manipulations would be prevented.

Finally, there are increasingly more regulations and standards whose non-compliance results in significant financial penalties. Therefore, adhering to them not only helps secure the plant, assets, and information but also protects the reputation, maintains customer trust, and strengthens operational resilience.

Industrial cybersecurity, although it may initially seem costly, an obstacle to plant availability, or even an inconvenience, is like the silent hero that keeps the environment running, ensuring greater stability and business success. Therefore, perhaps it’s time to stop thinking about whether availability or security takes priority, and start taking actions that secure the environment while maintaining and ensuring operations.

Miren Ordoñez de Arce
Cybersecurity Lead Analyst

What profiles are sought for working in quantum technologies?

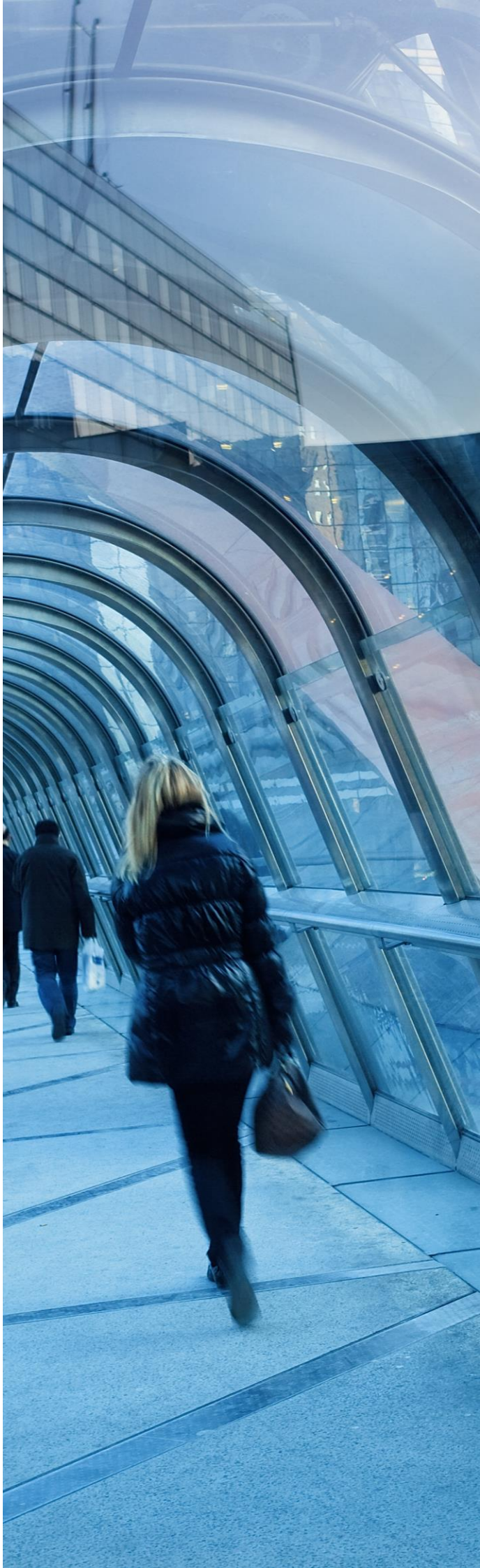
Quantum Space by María Gutiérrez

The field of quantum technologies is no longer a distant promise but is rapidly expanding and already demands qualified professionals. Quantum computing, quantum communications, quantum sensing, and metrology are the main areas shaping this new technological revolution, requiring close collaboration among physicists, mathematical engineers, computer scientists, philosophers, and cybersecurity experts, among others.

It is not only about understanding how quantum systems work from a theoretical perspective but also about building, operating, and protecting devices that behave differently from classical ones. At NTT DATA's quantum team, we have defined what we believe are the profiles required to form part of this new quantum workforce and the skills they must possess:

Quantum Business (QB) Specialist in identifying business opportunities in Quantum Technologies.

- A strategic mindset is required, as well as the ability to visualize how quantum technologies can transform business models. Additionally, expertise in business analysis and feasibility is necessary, along with the evaluation of the applicability and profitability of quantum solutions.
- Optimization of decision-making and the use of quantitative tools to prioritize investments in quantum technologies. Knowledge of emerging markets and an understanding of the impact of quantum computing on various industries (finance, healthcare, logistics, etc.). Additionally, it is important to have the ability to communicate quantum concepts to non-technical stakeholders.



Quantum Mathematics (QM) Specialist in mathematical modeling and quantum representation of problems.

- Modelado matemático avanzado. Diseño de representaciones QUBO, Ising y modelos gráficos. Optimización combinatoria, aplicación de métodos cuánticos y clásicos para problemas NP-hard. Algoritmos cuánticos para simulación. Desarrollo de enfoques híbridos y algoritmos heurísticos. Análisis de rendimiento, evaluación de métricas de eficiencia y precisión en soluciones cuánticas. Teoría de la información cuántica.

Quantum Researcher (QR) Researcher specialized in the study and validation of quantum algorithms for complex problems.

- Research and development. Exploration of new approaches in quantum algorithms. Comparative analysis, efficiency evaluation between classical and quantum algorithms, experimentation and validation, design of controlled experiments to test the performance of quantum algorithms. Scientific publication, writing, and dissemination of advancements in specialized journals and conferences. Transformation of data into appropriate representations for Quantum Computing.

Quantum HW Engineering (QHE) Engineer specialized in the design, implementation, and optimization of quantum hardware for the execution of algorithms and simulations.

- Quantum hardware architecture. Design and configuration of quantum processors and superconducting circuits, programming of quantum hardware using languages such as Qiskit, Cirq, and Ocean SDK. Optimization of execution on hardware, parameter tuning, and noise mitigation in qubits.
- Electronics and superconductivity, understanding the physical properties of quantum hardware, integration of hybrid systems, communication between quantum hardware and classical systems.

Quantum Deployment Team (QDT) Team responsible for the implementation, optimization, and deployment of quantum algorithms in IT production environments.

- Quantum code optimization. Refinement of quantum algorithms for efficient execution on hardware and simulators. Deployment in hybrid cloud, implementation of quantum solutions on platforms such as AWS Braket, IBM Quantum, and Azure Quantum. IT process automation, creation of CI/CD workflows for maintaining quantum code in production. Security and reliability in Quantum IT, implementation of security and stability standards in quantum environments.

Quantum Developer (QD) Developer specialized in programming, optimizing, and validating quantum algorithms to solve specific problems.

- Quantum programming. Use of languages such as Qiskit, Cirq, Ocean SDK, and Pennylane, development of quantum algorithms, implementation of algorithms such as QAOA, VQE, and Quantum Annealing. Optimization of quantum code, refinement of algorithms to improve efficiency and reduce errors. Analysis of quantum data, transformation, and preprocessing of data for use in quantum computing.

The profiles that start to be trained in this field today will be in a privileged position to lead the development of the next 5-10 years. Beyond academic training, it will be key to develop an interdisciplinary and flexible mindset, because working in quantum is not just about understanding a new way of computing—it's about learning to think in a radically different way!

Hyperconnectivity

Trends by Alejandro García Muñiz & Raquel Gálvez Huertas

It is hard to imagine a world without constant communication through technological devices and a continuous exchange of data. Hyperconnectivity has become an omnipresent concept that defines today's society. On one hand, organizations champion efficiency and productivity, while people seek greater well-being and more free time. In both cases, digital transformation seems to be the best ally in finding solutions, leading to an increasing number of interconnections across the network. On the other hand, this growing hyperconnectivity and technological dependence also bring a set of new challenges, such as mental health concerns or the wide variety of potentially exploitable vulnerabilities driven by digital risks and threats, which require innovative strategies to protect user privacy and security in a constantly evolving digital environment.

IoT Explosion: From Hundreds to Millions

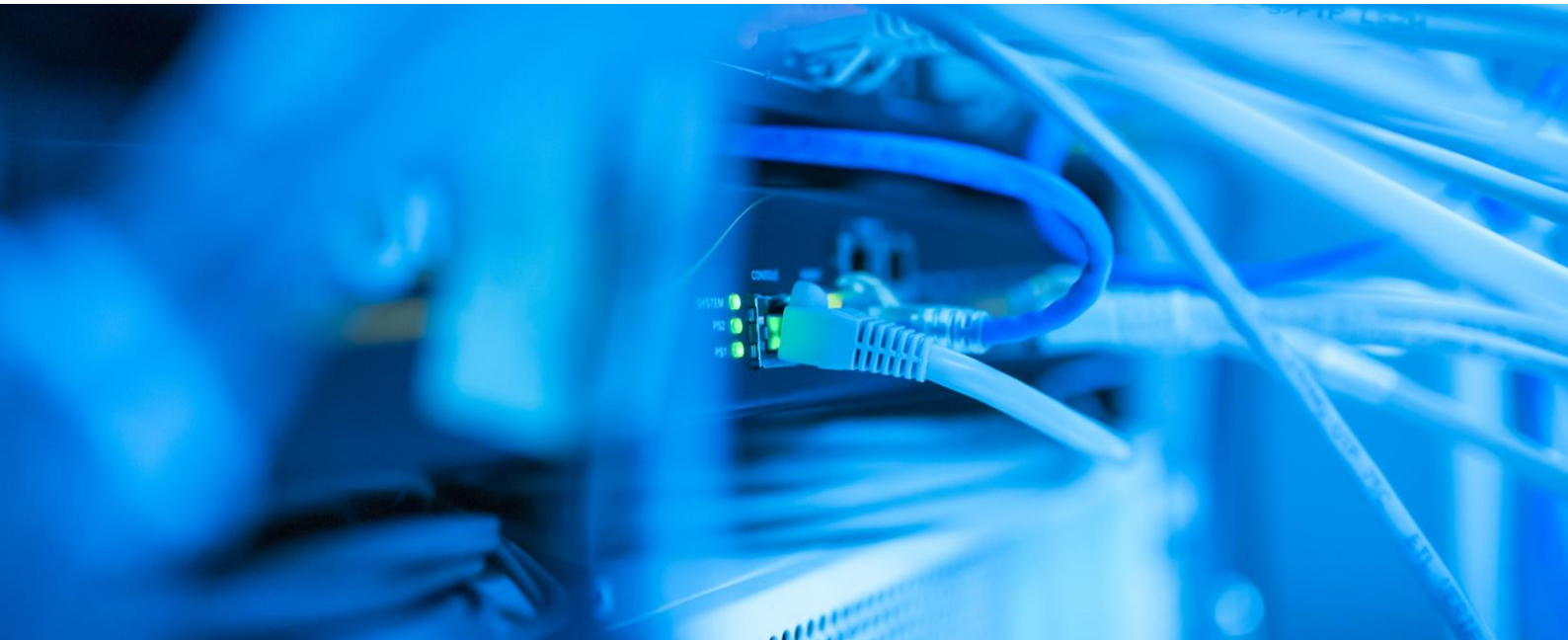
Since the emergence of the first IoT devices, there has been an exponential increase in the number of interconnected devices, surpassing the statistical expectations set by studies and surprising the industry with its rapid growth. In 2015, it was estimated that a total of 3.5 billion devices would be active and connected to the internet, but the actual figure hovered around 10 billion devices.

In those same studies, it was estimated that by 2020, there would be a total of 9.9 billion connected devices, reaching 21.5 billion by 2025. However, the actual figures showed that a total of 11.7 billion devices were connected in 2020, and by 2025, the number is expected to rise to around 75 billion devices, representing a percentage growth of more than 600%, driven primarily by advancements in AI and 5G.

Vulnerable and Dangerous

Currently, these devices are used in all social spheres and sectors, from home privacy to large organizations serving millions of users: education, healthcare, transportation, public administrations, etc. Security, from the design stage, becomes key in the development of these IoT devices to maintain the confidentiality, integrity, and availability of the information they handle, as more than 50% have critical vulnerabilities by default that are exploited by hackers before they can be patched.

Outdated firmware drives 60% of IoT attacks that could be prevented with automatic updates and security configurations that ensure devices are resilient from the start and prepared to face emerging threats. Furthermore, the integration of AI and LLMs in IoT devices increases the attack surface by amplifying the inherent vulnerabilities of each component, requiring more attention to security strategies.



More connections, more attacks

Building on the previous point, these security issues from the design stage, the number of vulnerabilities affecting devices, and the constant need to renew them, have created a significant opportunity for threat actors. In 2022, over 112 million attacks on IoT devices were recorded, nearly 200% more attacks compared to the 32 million in 2018. However, the real impact is seen in the statistics provided by major AV manufacturers in 2024, who stated that, during the first half of 2024, an average of more than 50 exploitation attempts were recorded weekly, with the total number of attacks increasing globally by 75%

New devices, new attackers

The era of hyperconnectivity has transformed the way we interact, but it has also opened the door to a range of complex threats. By 2025, threat actors are expected to exploit advanced technologies and tactics to take advantage of IoT vulnerabilities.

Among these dangers are groups such as Volt Typhoon, RansomHub, and Andariel, which systematically exploit vulnerabilities across various industrial and public sectors. Meanwhile, Sandworm, with ties to Russia's military intelligence agency, is focusing its efforts on critical technology systems.

On the other hand, CYBERAV3NGERS, affiliated with Iran, target critical infrastructures, including complex IoT systems. The Qilin Ransomware Group focuses on disrupting industrial processes, thereby shaking the trust and stability of integrated systems. In this context, the implementation of proactive security measures and the development of robust strategies to anticipate and mitigate these attacks become crucial to ensuring a secure and resilient IoT ecosystem

The who and the how?

The emergence of new actors is not the only factor to consider, as known actors remain an active threat. This is because their Tactics, Techniques, and Procedures (TTPs) are constantly evolving, allowing these actors to adapt to the changing IoT environment.

Among the most commonly used tactics since 2024, analyses reveal that deepfakes, advanced phishing, spoofing, and malicious applications are the most frequently employed to deceive users and infect devices. Through these devices, threat actors manage to execute attacks such as stealing stored credentials, inserting advanced persistent malware, and incorporating devices into botnet networks.

The future of interconnected threats

In addition to the above, by 2025, the repercussions of the interconnection of IoT devices with smart devices—some of which will begin to actively control the functioning of certain technologies at the public level due to the natural evolution toward smart cities—are expected to lead to an increase in data breaches, financial fraud, and identity theft fueled by deepfake technology.

These attacks will target the general public, but will also affect businesses, mainly due to policies allowing the use of personal devices at work and the use of professional data on external devices. On the other hand, they will also extend to industrial sectors, which are in the midst of digitalization, incorporating IoT technologies to automate tasks. This will inevitably lead to denial-of-service attacks that could halt production in entire factories.

Data breach or los of lives?

Considering all of the above, and adding the growth areas where IoT Devices (DIoT) have had the greatest impact, it can be seen that the sectors with the largest number of connected devices are some of the most critical, such as the healthcare sector, public administration, and the industrial sector, followed by the energy sector, which includes some critical infrastructures like nuclear, hydroelectric, or power plants.

This could represent a potential risk greater than it may appear at first glance, as these sectors are key to human well-being and the sustainability of welfare states in metropolitan areas. Potential disastrous scenarios could include the hijacking of operating rooms, denial of service attacks on critical energy infrastructures, or blocking signal reception at airports, leaving entire flight paths without ground visibility.

Conclusion

In light of this perspective, security professionals can only conclude that the interconnectivity of devices is a logical and inevitable step towards an increasingly globalized future.

However, when these devices are not properly protected, and users share data and grant permissions without prior training and awareness, the addition of connections between IoT devices and smart technology significantly amplifies the threat landscape, compromising both public security and individual privacy.

At this point, it is clear that what truly separates users and businesses from potential attacks is a widespread understanding of the security of devices, connections, and mobile applications. Therefore, education and training in cybersecurity are crucial.

Alejandro García Muñiz
Cybersecurity Analyst

Raquel Galvez Huertas
Cybersecurity Analyst

Vulnerabilities

Multiple vulnerabilities in MongoDB

Date: April 03, 2025
CVE: CVE-2025-3085 and 2 more

CVSS: 8.1

HIGH

Description

The Linux database system provider, MongoDB, published a notice on its website on April 3rd regarding various vulnerabilities. The security advisory includes vulnerabilities, two of which are recognized as high severity:

- CVE-2025-3085: With a CVSS of 8.1, this vulnerability affects Linux servers with TLS, where an error occurs in the verification of the intermediate certificate status, allowing for unauthorized authentication.
- CVE-2025-3083: With a CVSS of 7.5, this vulnerability would allow an unauthenticated attacker to cause a service crash through specific messages.

Solution

MongoDB has released a series of updates to address the mentioned vulnerabilities, as well as other lower-severity vulnerabilities, which are outlined in the following points:

- CVE-2025-3083: update to version 5.0.316.0.207.0.16.
- CVE-2025-3084: update to version 5.0.316.0.207.0.168.0.4.
- CVE-2025-3085: update to version 5.0.316.0.207.0.168.0.4.

Affected products

This vulnerability affects the following versions of MongoDB:

- 5.0X versions prior to 5.0.316.0.207.0.16.
- 5.0X versions prior to 5.0.316.0.207.0.168.0.4.

References

- csirt.telconet.net
- cert.gov.py

Vulnerabilidades

Critical vulnerability in Fortinet FortiSwitch GUI

Date: April 08, 2025
CVE: CVE-2024-48887

CVSS: 9.3

CRITICAL

Description

A critical vulnerability has been identified in Fortinet FortiSwitch GUI (CVE-2024-48887), which allows an unauthenticated remote attacker to change administrator passwords using a specially crafted request by exploiting an unverified password change in the FortiSwitch graphical user interface.

The discovery was internal, made by Daniel Rozenboom, who is part of the FortiSwitch interface development team. So far, there is no evidence that this vulnerability has been exploited, but it is recommended to apply the remediation patches as soon as possible

Solution

To mitigate the associated risks, it is recommended to take the following actions:

- FortiSwitch 7.6.0 update to 7.6.1 or higher).
- FortiSwitch 7.4.0 to 7.4.4 (update to 7.4.5 or higher).
- FortiSwitch 7.2.0 to 7.2.8 (update to 7.2.9 or higher).
- FortiSwitch 7.0.0 to 7.0.10 (update to 7.0.11 or higher).
- FortiSwitch 6.4.0 to 6.4.14 (update to 6.4.15 or higher).

Additionally, Fortinet recommends disabling HTTP/HTTPS access and restricting system access to trusted devices.

Affected Products

The affected versions are as follows:

- FortiSwitch 7.6.0.
- FortiSwitch 7.4.0 to 7.4.4.
- FortiSwitch 7.2.0 to 7.2.8.
- FortiSwitch 7.0.0 to 7.0.10.
- FortiSwitch 6.4.0 to 6.4.14.

References

- nvd.nist.gov
- fortiguard.fortinet.com
- thehackernews.com

April Android Security Bulletin Fixes Critical Vulnerabilities

Date: April 07, 2025
CVE: CVE-2024-45551 and 58 more

Critical

Description

The April 2025 Android Security Bulletin addresses a total of 59 vulnerabilities, including four critical ones. Three of them can be used for privilege escalation without user interaction (CVE-2025-22429, CVE-2025-26416, and CVE-2025-22423).

Also notable is the critical vulnerability CVE-2024-45551, where a Qualcomm subcomponent can incorrectly verify a PIN or password.

Additionally, there are two high-severity vulnerabilities that have been actively exploited, but in a targeted manner:CVE-2024-53150

- CVE-2024-53197

Affected products

The components affected by these vulnerabilities are::

- Framework
- System
- Kernel
- Third-party component:
  - Arm
  - Imagination Technologies
  - MediaTek
  - Qualcomm

In addition, it is stated that devices with Android 10 and later versions may also receive security updates.

Solution

Several security patches have been released in this bulletin, so it is recommended that all Android users update to the latest version to address the vulnerabilities.

References

- android.com
- nvd.nist.gov

Microsoft April 2025 Security Updates

Date: April 08, 2025
CVE: CVE-2025-29824 and 124 more.

Critical

Description

Microsoft has released its monthly security patch for April, addressing a total of 125 security vulnerabilities, of which 11 are critical.

Among these vulnerabilities, there is a zero-day vulnerability (CVE-2025-29824) with a score of 7.8. This vulnerability is focused on privilege escalation, where successful exploitation would allow a standard user to gain elevated privileges (administrator), affecting the common log file system (CLFS).

This vulnerability has been patched for Windows 11, while a fix for Windows 10 has not yet been provided.

Solution

Microsoft strongly recommends that its customers update their operating systems to the latest available version, which are currently:

- Cumulative update for Windows 11 Version 24H2 (version KB5055523).
- Cumulative update for Windows 11 Version 24H2 (version KB5055528).

Affected products

The products/versions affected by these vulnerabilities are::

- Versions prior to the April security update. The full list of affected products is available on the Microsoft portal.

References

- support.microsoft.com
- thehackernews.com
- incibe.es

TLP:WHITE

Events

RSA Conference
28 April – 1 May

The RSA Conference 2025 is one of the most prominent events in the field of cybersecurity. This gathering brings together experts, innovators, and industry leaders to explore the latest trends, technologies, and strategies in response to current security challenges. In addition to lectures and interactive workshops, attendees will have the opportunity to network, discover innovative solutions, and participate in activities such as the "Innovation Sandbox" competition.

Link

Cybersecurity & Data Innovation Summit
29 April

The 6th edition of the Cybersecurity & Data Innovation Summit 2025 will be held on April 29th in Madrid, positioning itself as a key event in the field of cybersecurity. This event offers exclusive networking opportunities with industry leaders and discussions on topics such as NIS2 directives, DORA strategies, innovations in AI applied to cybersecurity, combating ransomware, and more.

Link

Cloud Summit 2025
26 – 28 May

The European AI and Cloud Summit is a prominent event focused on artificial intelligence and cloud technologies, with 3,000 participants expected. It will bring together leaders, innovators, and experts to explore the latest advancements in areas such as generative AI, OpenAI, Microsoft Azure, and AI applications across various industries.

Key topics will include scaling AI startups and advanced data visualization tools, with companies like SquaredUp showcasing innovative solutions at the event, located at Booth 36.

Link

Recursos

➢ Burp AI

Burp AI is a tool integrated into Burp Suite Professional that uses artificial intelligence to enhance web security. It offers automated analysis to validate vulnerabilities, reduces false positives, and simplifies configurations such as login setups. It provides clear explanations of web technologies and allows the integration of advanced features through AI extensions, ensuring data privacy at all times.

Link

➢ OpenNHP

An open-source tool designed to implement zero-trust security in infrastructures, applications, and data. It uses advanced cryptographic protocols to hide network infrastructure details, such as ports and IP addresses, thus protecting resources from unauthorized access. Additionally, it ensures data privacy through encryption algorithms, reducing the attack surface and strengthening defenses against cyber threats.

Link

➢ Dalfox

An open-source tool designed to automatically detect XSS (Cross-Site Scripting) vulnerabilities. It offers an advanced testing engine that allows for parameter analysis, quick scans or detailed analysis, and vulnerability verification. It includes features such as flexible scanning modes, analysis of reflected, stored, and DOM-based parameters, and customization options with payloads and remote word lists.

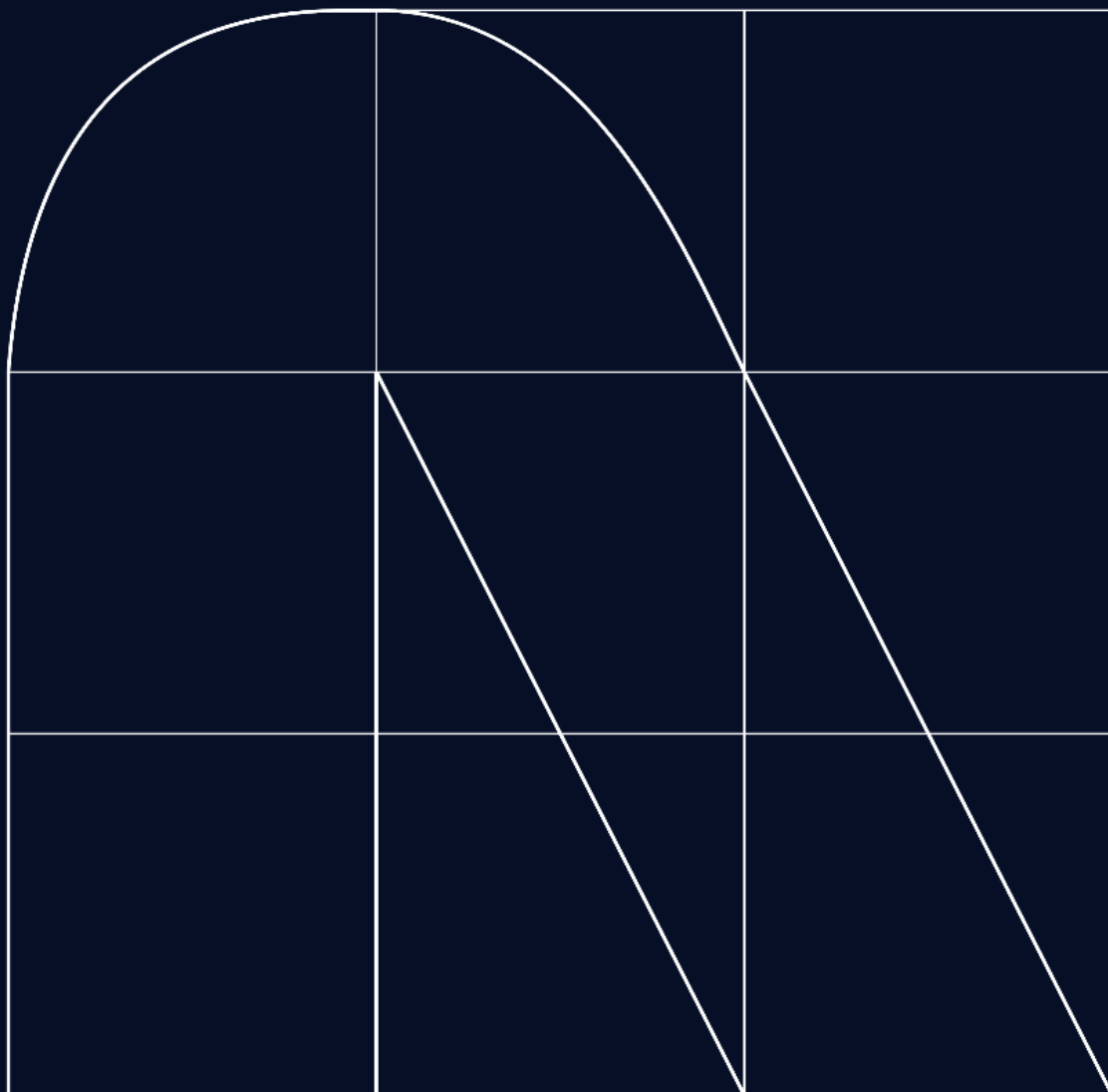
Link

➢ OpenCTI

An open-source platform designed to manage cyber threat intelligence. It allows for structuring, storing, organizing, and visualizing both technical and non-technical information about cyber threats using the STIX2 standard. It includes a modern interface based on GraphQL and can be integrated with tools such as MISP, TheHive, and MITRE ATT&CK. It facilitates data export and import in various formats, helping analysts extract meaningful insights from raw data.

Link

Subscribe to RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com