NUMBER 77 | ARPIL 2023

NTT DATA
Trusted Global Innovator

# Radar

## Cybersecurity magazine

# INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION:RELEVANT ASPECTS FOR THE BOARD OF DIRECTORS.

Human errors, lack of control, internal fraud or criminal actions in the processing of information are issues that are beginning to be on the agenda of the Boards of Directors of companies, as they can cause business paralysis, direct economic losses (millions of US$), non-compliance with legislation and a negative impact on the image, reputation and credibility of the company. All of this prevents the organisation from adequately achieving its corporate objectives.

Information is the resource that enables the organisation to plan and operate its business. Without information available and protected, the organisation can suffer an incident that, depending on its size and type of business, can put it out of business for a period of time or forever, directly and negatively affecting shareholders.

One of the principles of Corporate Governance is the “Sustainability of the Organisation”. This means the continuity of information to carry out the services and/or produce the products it makes available to the market. It is therefore the responsibility of the Board of Directors to ensure that an adequate information protection process is in place.

Shareholders, through the Board of Directors, need to be aware of the organisation’s cyber risks and information protection maturity. This maturity level is the result of a detailed assessment of various information security, cybersecurity and privacy protection controls. The Board needs to know the existence (or not) of controls that prevent or minimise the loss, theft or unavailability of information. They need to know the resilience of information protection.

The World Economic Forum’s Centre for Security, the Internet Security Alliance and the National Association of Corporate Directors, in their document “Principles for Board Governance of Cyber Risk (2021)”, recommend that the Board of Directors and Senior Management consider a “cyber-resilient organisation”:

- Cybersecurity at the service of business strategy.
- Economic drivers and impact of cyber risk.
- Alignment of cyber risk management with business needs.
- Ensuring that the organisational structure supports cyber security.
- Integration of cyber security expertise into board governance.
- Fostering systemic resilience and collaboration.

This month’s Radar Magazine features controls and new technologies to facilitate the protection of information and the generation of better information for the Board of Directors. FAIR (Factor Analysis Information Risk), a quantitative risk management methodology; Artificial Intelligence and ChatGPT considerations; and Operational Technology (OT) which, according to Gartner estimates, has a market 10 (ten) times larger than Information Technology (IT).

**Enrique Bernao Rosado**

Cybersecurity Manager at NTT DATA Europe & Latam

# CYBER NEWS

We begin our Cyber Chronicles with a concern that is troubling many organisations worldwide. GoDaddy, one of the world's leading web hosting companies, has reported a security breach that has compromised its cPanel shared hosting environment.

According to the company, unknown attackers managed to break into its servers and steal source code, as well as install malware on the systems.

Although customer reports alerted GoDaddy to the security breach in early December 2022, the attackers managed to gain access to the company's network several years earlier.

> "BlackLotus, a stealthy and unified extensible firmware interface (UEFI) bootkit, has emerged as the first publicly known malware capable of evading Secure Boot defences".

During this time, the attackers were able to use compromised sites to redirect traffic to several unknown domains. Since GoDaddy is one of the largest domain registrars in the world, this is a cause for concern for the more than 20 million customers worldwide who use its hosting services.

On the other hand, BlackLotus, a stealthy and unified extensible firmware interface (UEFI) bootkit, has emerged as the first publicly known malware capable of evading Secure Boot defences, making it a potent threat in the cyber landscape.

"This bootkit can run even on fully upgraded Windows 11 systems with UEFI Secure Boot enabled". As we can recall, UEFI bootkits are deployed in the system firmware and allow full control of the operating system (OS) boot process, making it possible to disable OS-level security mechanisms and deploy arbitrary payloads during boot with high privileges.

This powerful and persistent toolkit is offered for sale for USD$5,000 (and USD$200 for each subsequent new version), is programmed in assembler and C and has a size of 80 kilobytes. It also has geofencing capabilities to prevent infecting computers in Armenia, Belarus, Kazakhstan, Moldova, Romania, Russia and Ukraine.

From the other side of the world, Chinese cyber-espionage group Mustang Panda, aligned with China, has been spotted using a new custom backdoor called MQsTTang as part of an ongoing social engineering campaign that began in January 2023. MQsTTang uses the IoT messaging protocol MQTT for command and control communications.

The group's attacks have targeted European entities in the context of Russia's invasion of Ukraine last year, although attacks against unknown entities have also been observed in Bulgaria and Australia, as well as against a government institution in Taiwan.

The MQsTTang backdoor allows the execution of arbitrary commands received from a remote server and is distributed through RAR files that contain an executable that presents file names with diplomatic themes. The findings come days after Symantec revealed a cyber espionage operation carried out by the Chinese state-owned APT41 group, which targeted two subsidiaries of an Asian conglomerate in the materials and composites sector.

On the other hand, we move to Mexico, where a new strain of ATM malware called FiXS has been detected and has been targeting banks since early February 2023. FiXS hides inside another non-malicious program and is compatible with any ATM machine that supports CEN/XFS. It is believed that the attackers found a way to interact with the ATM through the touchscreen. One of the notable features of FiXS is its ability to dispense money 30 minutes after the last ATM reset. FiXS is similar to another strain of ATM malware called Ploutus.

The latter has allowed cybercriminals to withdraw cash from ATMs using an external keyboard or by sending a text message. FiXS is the latest in a long line of malware that has targeted ATMs to steal money. It should be noted that this type of malware could spread across the region and affect ATMs in the US, Central and South America.

This brings our Cyber Chronicles to a close, we will continue to report on current news from the world of cyber security.

# THE IMPORTANCE OF EFFECTIVE CYBERSECURITY RISK MANAGEMENT IN ORGANISATIONS

By: NTT DATA

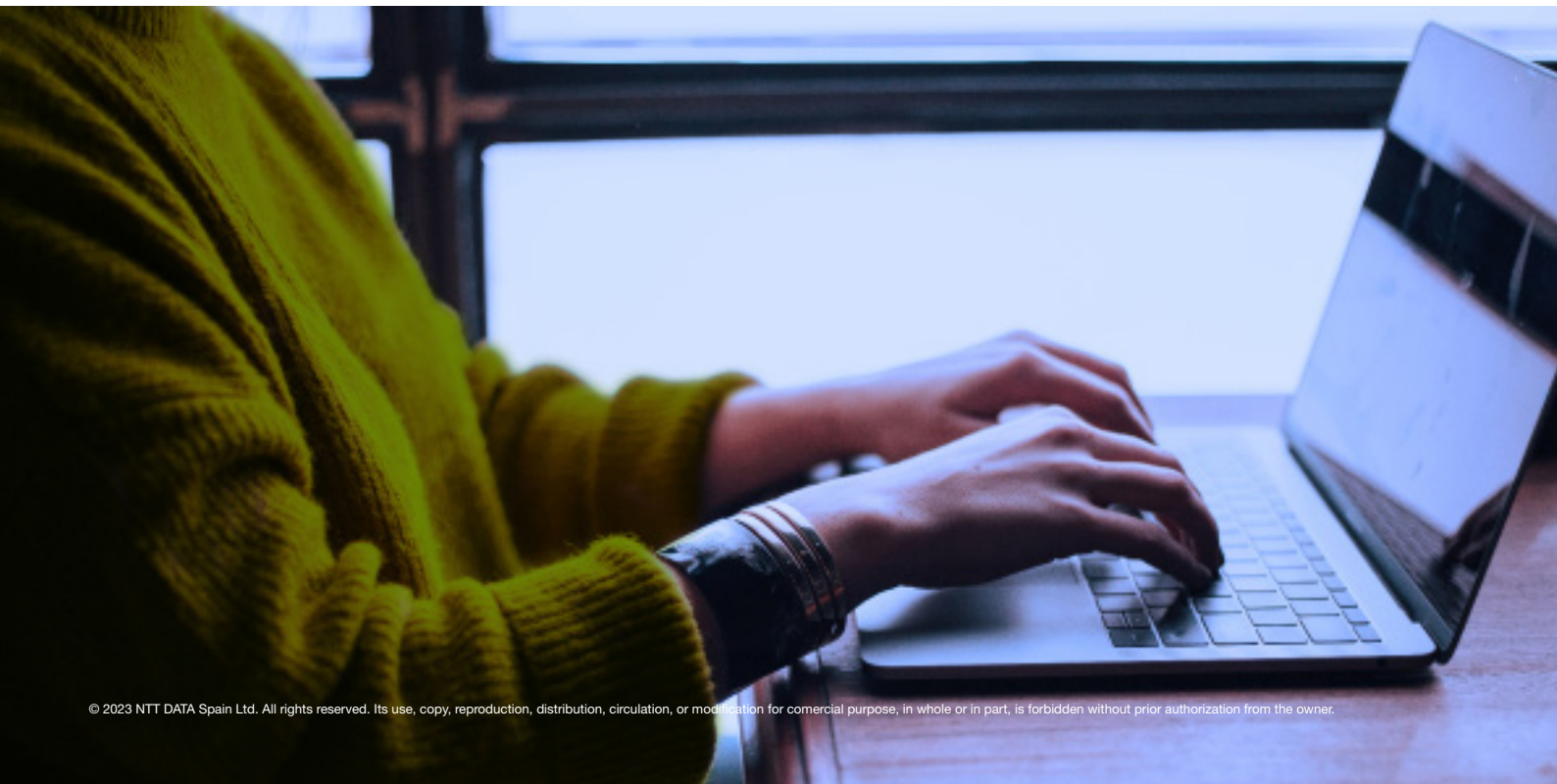
Information security and cybersecurity risk management seeks to guarantee the actions that support the integrity, confidentiality and availability of information assets within organisations. Many companies already have a defined and mature information security risk management methodology, in addition to being committed to taking actions to treat and mitigate their risks by going through different stages of identification, analysis and evaluation, as well as risk treatment.

There are currently many published and applied methodologies and frameworks for risk management. Most organisations have chosen to align themselves with qualitative assessment methods, which have helped them to determine the value of risks in terms of impact and likelihood.

Although in certain cases, the defined methodology assigns quantitative ranges of risk exposure, this assignment is a “possibility” but not a “probability” as such, supported by supporting information.

In relation to IS risks, key stakeholders such as CISOs, security risk managers, IT managers, executives and partners, among others, are questioning the following:

- Is our risk management sufficient to respond to and support the security investments we need to make?
- Are the results of the risk management we apply sufficient to support the valuation of critical risks for the company?
- Does the final impact on the organisation assess values based on statements of likelihood that are close to reality?
- Does the risk methodology support the planning of actions to be carried out as part of the information security programme in the short, medium and long term, considering the urgency and the main ailments we have?



The alternative of using quantitative methods to help define more accurately the decisions to be taken is generating more interest due to the importance of supporting the costs that could be incurred in the event of a security breach and the need to support security investments.

In addition, making the right decisions based on relevant information represents a major challenge in any company process. Information security and cyber security risk management is no exception: analysing information to gain a close understanding of the likelihood of a risk event occurring will help to act proactively by applying necessary controls. Conversely, acting reactively when the "fire" has already broken out could have a major impact.

This is why decision-makers are looking to improve their risk analysis and focus it on tangible values in monetary terms of loss, which gives them the ability to take risk management to the next level by being able to sustain the required investments. In addition, they will be able to define with this value the allocation of a short, medium and long term implementation horizon.

To apply it, a good alternative is to use the FAIR framework initially defined for cybersecurity risks (it can be used to analyse other types of risks). This framework analyses risk on the basis of a hierarchical taxonomy, on which a first level is composed of "frequency of loss event" and "magnitude of loss". These terms in subsequent levels are composed of other values which in sum will help to arrive at the value of the risk independently considering the scenario it faces.

However, companies that wish to start using a quantitative risk analysis methodology must go through a transformation and transition process, especially to be able to measure losses, resilience of their controls and success rate of attackers.

As part of the process of adopting the new methodology will be the measurement of these variables or the implementation of new controls that will allow the organisation to have valid information in the following months.

To begin the journey, organisations can use sector-based information, for example, as long as it represents a good source of data. This will serve to challenge assumptions and make the analysis with more accurate estimates, which will be of greater value to companies.

Lastly, in this adoption process, companies can look at quantitative and qualitative risk analysis methodologies as complementary, and qualitative does not need to disappear. They can decide to run the quantitative analysis on the scenarios with the greatest impact for the organisation and focus on obtaining information from those cases only.

Peter Drucker famously said that "What cannot be measured cannot be controlled; what cannot be controlled cannot be managed; what cannot be managed cannot be improved".

Well, the positive thing about this new approach is that it allows us to measure and quantify the economic impact of an attack on an organisation and this will allow us to control, manage and improve the risk management process.

# IMPACT OF CYBER INCIDENTS ON CRITICAL INFRASTRUCTURE IN OUR DAILY LIFE

By: NTT DATA

The latest edition of the IT security magazine "Cybersecurity Today" reported on recent cyber-attacks in industrial environments and the need to improve security in these areas. In recent months, there have been several cyber-attacks in the industry that have caused production disruptions and considerable financial losses. One of the most notable attacks affected a major oil and gas production plant in the Middle East, which was forced to temporarily shut down due to an intrusion into its industrial control system.

**Industrial cybersecurity, risk of human lives.**

Industrial cybersecurity is of vital importance to safeguard people's lives. Critical infrastructures such as power plants, water treatment plants and transport facilities are highly automated and depend on industrial control systems for their proper functioning.

A cyber-attack on these systems can cause serious damage to public health, the environment, and the economy.

It is therefore crucial that these facilities have robust security measures in place to protect their industrial control systems against potential cyber threats. Industrial cybersecurity not only protects critical infrastructures, but also helps to ensure the continuity of production and supply of essential goods and services for society.

In summary, industrial cybersecurity is fundamental to safeguard people's lives and protect the economy from the possible harmful effects of a cyber-attack.

**Cyber-attack on water plant.**

In February 2021, a cyber-attack was reported on a water treatment plant in the city of Oldsmar, Florida, in the United States. According to local authorities, an unknown hacker managed to gain access to the plant's systems and increased the level of sodium hydroxide (NaOH) in the treated water.

The attack was quickly detected by a plant operator, who noticed an increase in the level of NaOH in the treated water and corrected it before any damage occurred. The plant was temporarily disconnected from the Internet and an investigation was carried out to determine the nature of the attack and its origin.

Local and federal authorities confirmed that the attack was perpetrated by an external hacker and that it was carried out through unauthorised remote access software.

The water treatment plant improved its security measures and implemented new measures to protect its industrial control systems.

This incident highlights the need to improve cybersecurity in critical infrastructures, such as water treatment plants, to avoid possible damage to public health and the environment.

Local and federal authorities have urged all critical facilities to review their security systems and update their protection measures against possible cyber attacks

What measures should the industry take to protect itself with cybersecurity tools in industrial environments?

**Here we present some of these measures:**

1. Implementation of a security policy: The industry should establish a clear and detailed security policy, which describes the security procedures that must be followed to ensure the protection of industrial control systems. This may include access rules, password policies and physical security measures.
2. Security tools: The industry should implement security tools, such as firewalls, intrusion detection systems and antivirus software, to protect industrial control systems against potential threats. These tools can help detect and prevent cyber-attacks before they cause any damage.
3. Regular update of software: The industry should regularly update the software of industrial control systems to ensure that they are protected against the latest security threats. This may include applying security patches and software updates to close known vulnerabilities.

4. Limitation of access: Industry should limit access to industrial control systems to only those employees who need access to perform their duties. Physical and logical access controls can be implemented to ensure that only authorised people are allowed access to the systems.
5. Penetration tests: The industry should conduct regular penetration tests to evaluate the effectiveness of its security measures. This can help identify potential vulnerabilities and areas that need improvements in security protection.

**Why is the development of a Contingency Plan important?**

A contingency plan for cyber-attacks on the OT industry must be comprehensive and encompass all phases of the process, from prevention to recovery.

Organisations, given the current threat surface and due to the proliferation of new cybercriminals, must not only be aware of industry-targeted campaigns, but also systemically consider defensive pillars to minimise the impact of an attack on their organisation.

The following are the key actions that should be included in an effective emergency plan:

- Preparation: identification of critical assets and vulnerabilities of the OT infrastructure, assessment of risks and establishment of appropriate security measures to prevent attacks.
- Detection: establishment of intrusion detection systems and tools to detect attacks in real time.
- Containment: isolating the affected systems and stopping the spread of the attack.
- Research: determination of the cause and scope of the attack, information gathering and documentation of the facts.
- Mitigation: implementation of measures to minimise the damage caused by the attack.
- Recovery: restoration of OT infrastructure systems and functionality to their pre-attack state.
- Evaluation: review of the emergency plan and the actions taken, identification of possible improvements and adjustment of the plan accordingly.

It is important to stress that an effective contingency plan must be practical, accessible and regularly updated. In addition, it is essential that all employees are familiar with the plan and know their role in the event of a cyber-attack.

Collaboration and teamwork are essential for an effective response to a cyber-attack in the OT industry.

OT incident prevention is an ongoing process and requires constant organisational commitment. By adopting effective security measures and working in partnership with security experts, organisations can protect their industrial assets and ensure business continuity.

# TRENDS

## GPT: A door that opens the way

While in our last edition we explained some generalities of ChatGPT (chatbot developed by OpenAI) in terms of its definition, objective, pros and cons for the common user, it is also necessary to talk about the impact that is beginning to be forged at the corporate level for its adoption and thanks to the evolution of the GPT model.

Since it was released in November 2022, ChatGPT has been the focus of a constant debate on security. However, it is important to take a look back to realise its progress and the role of having it as an ally to give it that tinge of trustworthiness in the enterprise environment..

As everyone knows, OpenAI is a company governed by the non-profit organisation OpenAI Incorporated, but also comprised of another for-profit subsidiary - OpenAI Limited Partnership, Since they started developing their idea in 2015, it was only in 2019 that they started their relationship with one of the tech giants - Microsoft - to train their models with Azure technology, thus enabling OpenAI to not give up their research purpose and on the other hand, Microsoft to continue maturing their products as their exclusive cloud provider to the point of implementing an application interface (API) that would allow them to reach both the enterprise world and developers to build solutions in a more secure way on top of their GPT, CODEX and DALL-E models.

In simple terms it would be defined as follows:

- GPT, executes a variety of natural language tasks, used to execute question-answering, text summarisation, machine translation and AI conversation.
- CODEX, based on GPT-3, converts natural language into code. It is not designed to replace the work of programmers, but rather to assist them in coding certain routine fragments or optimising existing code.
- DALL.E, creates images from a natural language description.

With all the boom and the benefits of ChatGPT, some of these models may go unnoticed, although they are beginning to gain relevance in the environment of large companies to provide improvements in response times, effectiveness and user experience, factors that have been decisive in recent years in user interaction with respect to a product or service.

Finally, it is extremely important to clarify that the simple fact of having one of these modules does not imply that everything will work as if by magic for the organisation, we must be aware that they only form a part of the solution and around them there will be an important piece to work on the controls to be implemented in the communication of the services to be defined in the backend and ensure that both internal and external users who have access are validated and receive what their functions allow them to.

For this, it is necessary not to lose sight of two concepts that will always go hand in hand and are complementary in the success of a solution today, SECURITY and PRIVACY. SECURITY is aimed at protecting against malicious threats while PRIVACY guarantees that only those users who are authorised to access the data can do so.

# VULNERABILITIES



## Fortinet

CVE-2023-25610
Date: 08/03/2023

**Description**. On 8 March, a critical vulnerability affecting the administrative interface of FortiOS and FortiProxy was published that could allow an attacker to execute arbitrary code on the device or perform a DOS attack on the graphical user interface by sending specially crafted requests. Vulnerability CVE-2023-25610 would be caused by a buffer underflow. In this type of vulnerability, the application's buffer would load the information provided to it at a rate slower than the buffer's processing time, resulting in a request for adjacent memory.

**Link:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-fortinet-0
https://www.fortiguard.com/psirt/FG-IR-23-001

**Affected products.** This vulnerability affects the following versions of FortiOS and FortiProxy:

- FortiOS: 7.2.0 to 7.2.3.; 7.0.0 to 7.0.9.; 6.4.0 to 6.4.11.; 6.2.0 to 6.2.12.; 6.0 all versions.
- FortiProxy: 7.2.0 to 7.2.2.; 7.0.0 to 7.0.8.; 2.0.0 to 2.0.11.; 1.2 all versions.; 1.1 all versions.

**Solución**: The main solution to solve this vulnerability is to update FortiOS or FortiProxy to the following versions:

- FortiOS: 7.4.0 or higher; 7.2.4 or higher.;7.0.10 or higher.; 6.4.12 or higher.; 6.2.13 or higher.
- FortiProxy: 7.2.3 or higher.;7.0.9 or higher.;2.0.12 or higher.
- FortiOS-6K7K: 7.0.10 or higher.;6.4.12 or higher.;6.2.13 or higher.

The manufacturer has also provided a number of alternative solutions for those who are unable to update their products to these versions:

- Disable the HTTP/HTTPS administrative interface.
- Limit the range of IPs that can communicate with the administrative interface of the applications.

## Aruba

CVE-2023-22747; 22748;22749;22750;22751;22752.
Date: 01/03/2023

**Description.** On 01 March, a report was published by several researchers detailing numerous vulnerabilities that could affect Aruba products. This report notifies the existence of 33 vulnerabilities classified as: 6 critical, 19 important and 8 moderate. In the following, we will detail the critical vulnerabilities: A number of vulnerabilities have been reported that could lead an attacker to execute arbitrary code by sending specifically crafted packets to UDP port (8211) using the Aruba Networks Access point management protocol (PAPI). The CVEs for this vulnerability are as follows: CVE-2023-22747, CVE-2023-22748, CVE-2023-22749 and CVE-2023-22750. The other two critical vulnerabilities affecting Aruba products would allow through a buffer overflow the execution of arbitrary code on the system by sending specially crafted packets to UDP port (8211) using the PAPI protocol. This is a remote code execution vulnerability. The CVEs for this vulnerability are as follows: CVE-2023-22751 and CVE-2023-22752.

**Link**: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04454en_us
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt

### Affected products

The vulnerabilities affect the following Aruba products: ArubaOS: 8.6.0.19 and prior versions; ArubaOS: 8.10.0.4 and prior versions; ArubaOS: 10.3.1.0 and prior versions; SD-WAN: 8.7.0-2.3.0.8 and prior versions. This vulnerability also affects several Aruba products that will no longer be supported.

**Solution:** The main solution is to update to the following versions of the affected Aruba products: ArubaOS: 8.10.0.5 and following versions; ArubaOS: 8.11.0.0 and following versions; ArubaOS: 10.3.1.1 and following versions; SD-WAN: 8.7.0.0-2.3.0.9 and following versions. Additionally, Aruba has also published a series of recommendations to minimise the chances of being affected by one of these vulnerabilities: To minimise the chances of an exploitation, the communication between the controller/access gates and the access point should be restricted by a single layer 2 segment or a Vlan. Additionally, if the controller/gateways and gateways cross to layer 3 it is advisable to have firewall rules that restrict device communications. Finally, by activating the extra security for the PAPI protocol that is provided from the manufacturer, it will prevent vulnerabilities.

# PATCHES

## Cisco

Date: 02-03-2023

**Description.** Cisco has released a firmware update for the web management interface of its 6800, 7800 and 8800 series IP phones, which fixes the following critical vulnerability:

- CVE-2023-20078: This vulnerability could allow an unauthorised remote user to execute arbitrary code or cause a denial of service attack on the Cisco IP Phone 6800, 7800 and 8800 series management web interface. This vulnerability was caused by a flaw in the validation of the entered information allowing an attacker to exploit this vulnerability by sending specially crafted requests.

**Link:**
https://cve .report/CVE-2023-20078
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP#details

**Affected products:**

- Cisco IP phones version 6800, 7800 and 8800.

**Update**: Update the security patches published by the manufacturer of the corresponding device.

## Apple

Date: 02-02-2023

**Description.** Apple has published a security report indicating multiple updates for its iPadOS, iOS and macOS devices. These patches fix the following vulnerabilities: CVE-2023-23531, of critical severity, CVE-2023-23530, of high severity.

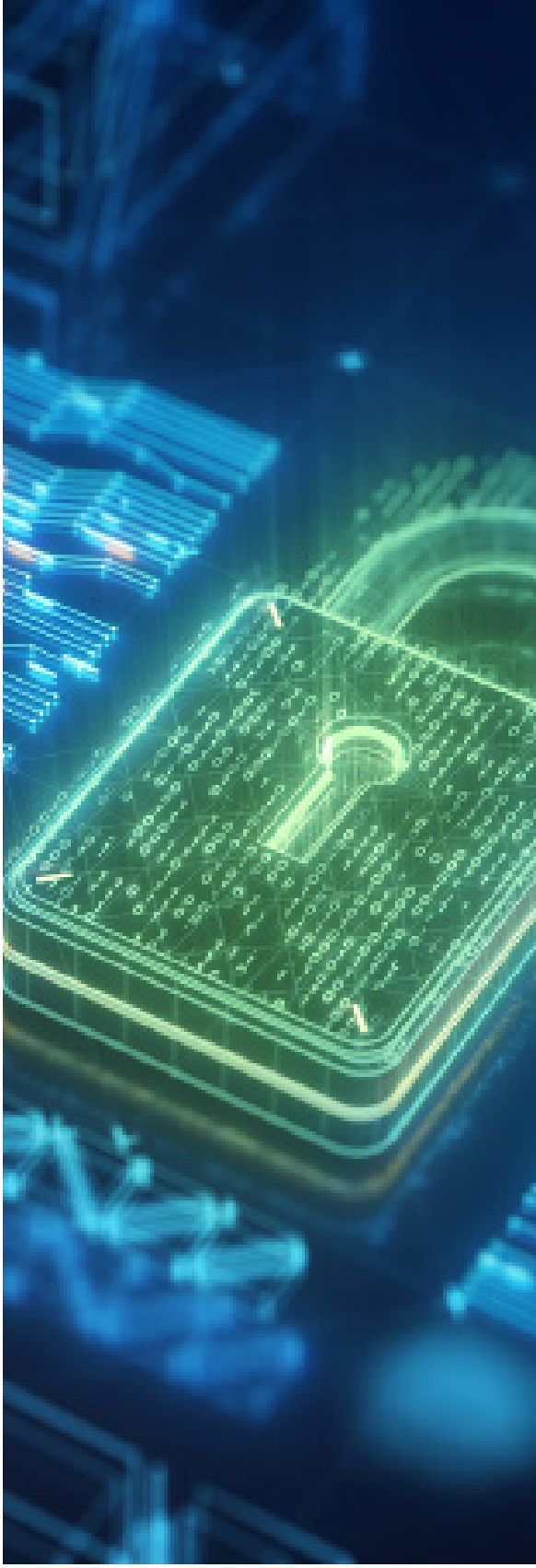
- CVE-2023-23531: this vulnerability would allow an attacker to execute arbitrary code on the computer by exploiting NSPredicate expressions that could bypass the validation performed by the NSPredicateVisitor component, which allows the attacker to bypass any type of validation.
- CVE-2023-23530: In the case of this vulnerability, an attacker could exploit the blacklists used by NSPredicate, which prevented the use of certain classes or methods that could compromise the security of the device. Clearing these lists could allow an attacker to execute arbitrary code on the device.

**Link:** https://techmonitor.ai/technology/cybersecurity/apple-security-vulnerabilities-ios-macos-ipados
https://www.trellix.com/en-us/about/newsroom/stories/research/trellix-advanced-research-center-discovers-a-new-privilege-escalation-bug-class-on-macos-and-ios.html

**Affected products:** The fixed vulnerabilities affected the following versions:

- macOS 13.2 and prior.
- iOS 16.3 and prior.
- iPadOS 16.3 and prior.

**Update:** Update the security patches published by the manufacturer of the corresponding device.



# EVENTS

## Cisco Develop 2023

**5 - 6 April 2023 |**

An event to explore the ideas and perspectives of enterprise and cloud-native software with a vision of the future. Attendees will connect in person or virtually to discuss contemporary perspectives and learnings relevant to working with cloud technologies.

**Link**: https://developer.cisco.com/develop/2023

## TecnoSec

**26 - 27 April 2023 |**

The High Security and Intelligence Technologies event, TecnoSec 2023, is a meeting point for Critical Infrastructure security institutions and bodies. TecnoSec is the ideal venue to foster national and international meetings and cultivate valuable contacts for the security industry.

**Link:** https://www.tecnosec.es/

## RSA Conference 2023

**24 - 27 April 2023 |**

The RSA Conference is one of the largest and best-known cybersecurity conferences in the world. It is held every year in San Francisco and attracts more than 40,000 attendees from around the world. Topics covered at RSA include everything from risk management and compliance to cloud security and mobile security.

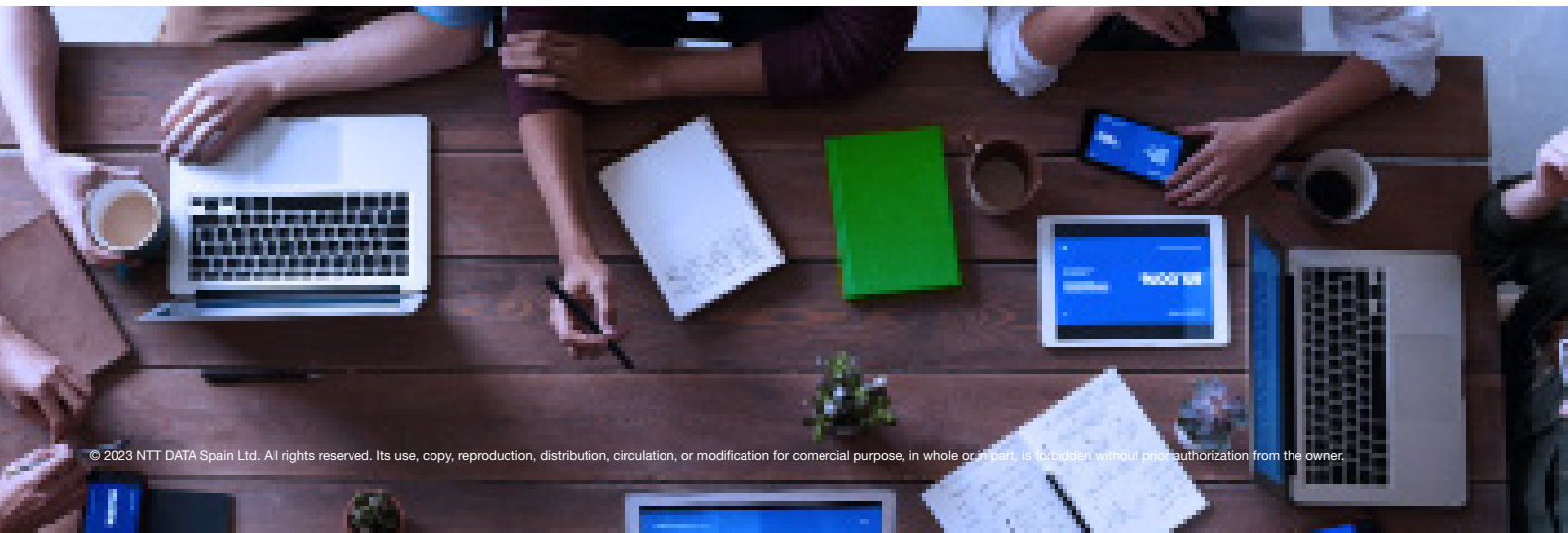
**Link:** https://www.rsaconference.com/usa

## SANS Pen Test Austin 2023

**17 - 22 April 2023 |**

SANS Pen Test Austin 2023 is six days of in-depth, hands-on training in penetration testing, network teaming, purple teaming and exploit development for professionals who need to know how to find vulnerabilities within their organisations, understand risk and prioritise resources based on potential real-world attacks.

**Link:** https://www.sans.org/cyber-security-training-events/pen-test-austin-2023/



# RESOURCES

## Do you know your risks? INCIBE

To help companies assess their cybersecurity status and move towards higher levels of protection, INCIBE offers a self-diagnosis tool specially designed for this purpose. Through a series of questions, the user will be guided to determine their information security status, which risks threaten the company's operation and which aspects need to be improved. All this, to start measuring. To start improving.

**Link: https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos**

## CSA CCM v4.0 Addendum - IBM Cloud Framework for Financial Services

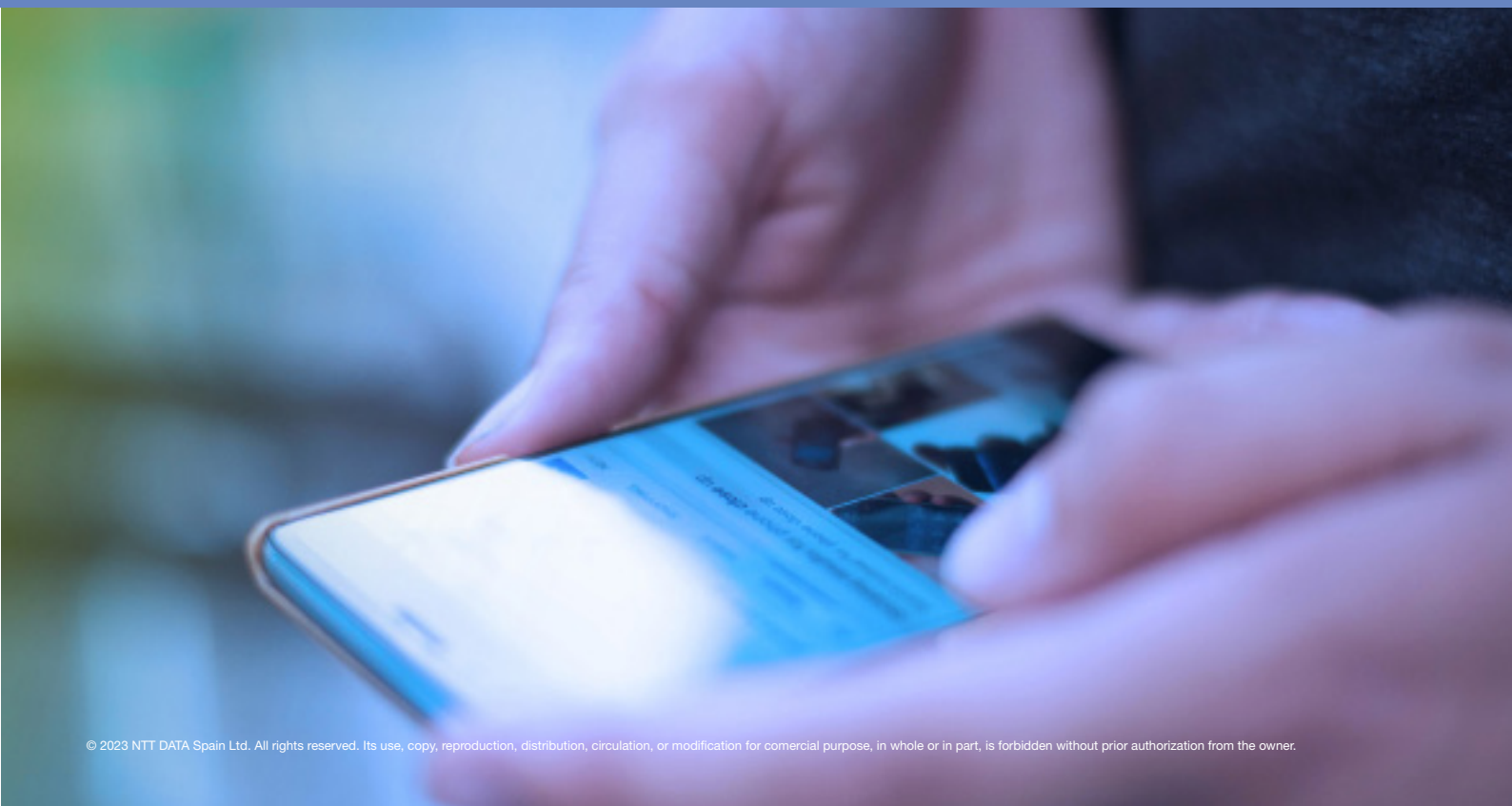
This document is an appendix to CSA CCM v4.0 for IBM Cloud Framework for Financial Services v1.1.0 that contains the mapping of controls between CCM and IBM Cloud Framework for Financial Services. The document is intended to help IBM Cloud Framework for Financial Services compliant organisations meet CCM requirements.

**Link: https://cloudsecurityalliance.org/artifacts/csa-ccm-v4-0-addendum-ibm-cld-framework/**

## STAR Enabled Solutions FAQ

A STAR Enabled Solution is a product or service that uses the CCM framework or the Consensus Assessment Initiative Questionnaire (CAIQ). Its technologies and tools have been evaluated and meet the security requirements set by the CSA. This verification process allows companies to more easily deploy tools that align or comply with STAR, the CCM framework, and best practices.

**Link: https://cloudsecurityalliance.org/artifacts/star-enabled-solutions-faq/**




NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com