NUMBER 83 | OCTOBER 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

HOW TO MANAGE RISKS IN NEW ARTIFICIAL INTELLIGENCE MODELS?

In the interconnected fabric of our age, cybersecurity transcends its technical role to become the fortress that protects our digital infrastructure. It is the safeguard of trust in our daily operations. Artificial intelligence (AI) is used in many business and production applications, including automation, language processing and productive data analysis. This allows companies across the board to optimise their manufacturing processes, operations, and improve internal efficiency. Through various computer programming rules, AI allows a machine to behave like a human and solve problems.

It is worth mentioning that no AI module comes ready from the start to operate and function as a real support for business work and decision making. It is important to decide on a strategy and data boundary for training and subsequent implementation. Large companies currently pushing AI have the resources to set up the necessary infrastructure for training (GPUs/TPUs, huge databases, etc.). Models can be retrained with specific data from smaller companies (a technique called Transfer Learning). In this pre-processing stage the role of experts related to the system being trained is key, otherwise the model will make predictions that are not aligned to reality.

The incorporation of AI is not exempt from the emergence of new potential security and data protection breaches that companies must consider and to which they must dedicate resources and time. Best practices recommend anonymising the data used for training, but in some instances, it is possible to re-identify the source of the data. Machine learning and deep learning models look for patterns in the data, so it is important that the data delivered is verified/prepared by an expert (e.g., a data governance expert), as the model will only be as good as the data used for training.

A new and vitally important aspect to consider arises here. An AI system, while it can become a great ally for a company's decision-making, also introduces a new set of vulnerabilities, which can be exploited maliciously to extract sensitive information or take control of the system.

Therefore, complying with a minimum framework of security measures and controls by the IA system becomes a baseline requirement when implementing the system and moving to a production environment. The right choice of security controls and minimum development will help to strengthen the security and privacy of information and increase confidence in the use of AI systems. This framework will help to recognise, measure, and mitigate the cybersecurity risks that an AI system can create in an organisation, minimising the number of potential security breaches that the system may have at the time.

Enrique Berano Rosado
Cybersecurity Managerr at NTT DATA Europe & Latam

CYBER NEWS

In this edition of RADAR, we will talk about supply chain attacks in the software development process, a technique known as Supply Chain Compromise according to the Mitre. The use of modern web development frameworks has made it possible to prevent common web attack techniques; one only has to look at the OWASP TOP 10 2021 to realise that exploit injections have moved into third place. However, cybercriminals also update their attacks, which is why, in recent years, supply chain attacks have been on the rise - one need only recall the disaster caused by Log4j in 2021. A supply chain attack is a breach of a widely used software component or library to impact end applications.

> "a bug in the library that interacts with the database engines, making it possible to execute query, modify or delete SQL statements with poisoned parameters.."

Since then, supply chain attacks have become an effective modality for cybercriminals, who implement different tactics and techniques to affect software components or their developers. For example, we can look at the recent attack in June on the MOVEit solution (CVE-2023-34362), the market-leading software for secure file transfer. Interestingly, the attackers exploited a SQL injection in production and used this breach to gain access to databases of companies such as BBC, British Airways, Aer Lingus, Boots, among others.

The cybercriminals apparently found a bug in the library that interacts with the database engines, making it possible to execute query, modify or delete SQL statements with poisoned parameters. On the other hand, the connection user between MOVEit and the database runs with administrator privileges, making it possible for the attackers to gain remote access to the application server. The Cl0p group is apparently involved in the attack, as they used a backdoor known as LEMURLOOT to exfiltrate the data. The companies affected by the attack were notified and the MOVEit team activated its incident response plan, generating the respective indicators of compromise and associated patches to mitigate the breach.

Another supply chain attack that is affecting the Python community is the recent campaign launched in August, apparently North Korean, on Open Source libraries. The cybercriminals are allegedly including malicious code in widely known dependencies that are managed by the famous PyPI package manager (pip). The technique used consists of creating libraries with names and descriptions very similar to the official ones, but with small variations, in such a way that unwitting developers import these malicious libraries such as Vmconnector, Tableediter and pyVmomi, are some of the affected libraries. Cybercriminals clone the official project and then include malicious code snippets and finally upload them to the Python package manager.

This slightly changes the name of the library using special characters. According to ReversingLabs' analysis generated from its Titanium platform, which is a tool used to monitor Open Source libraries and analyse their source code (SAST), cybercriminals reportedly included malicious code in the spoofed Vmconnect library where code snippets were identified with the ability to create operating system processes; enumerate system information and obfuscate data using base64 and connections to remote websites.

By analysing the domains found in the URLs in the source code, Reversing Labs was able to determine that they were possibly related to the Lazarus group (widely known to be funded by the North Korean government), which has claimed responsibility for recent ransomware attacks. The vector appears to be shifting, as developers' reliance on package managers and lack of awareness may be playing into the hands of the cybercriminal group. ReversingLabs has also detected these same supply chain attack techniques in package managers for languages such as NodeJS (npm), Ruby (gem) and C# (nuget).

We can also recall the attack on 3CX in March this year, according to Mandiant, the 3CX desktop application was infected with malicious code after North Korean cybercriminals compromised the 3CX company's development environment through sophisticated internal network attacks. The attackers' goal was to modify this legitimate software to include RAT-like code snippets to gain unauthorised access to 3CX end-user computers. The impact of the attack is being studied months later because such sophisticated and creative techniques were unknown.

The attack apparently started with a 3CX developer installing trading software with malicious code, and the cybercriminals quickly infected the machine and used it as an entry vector into the internal network. It is also known that credentials and secrets were compromised by scanning code repositories from the developer's account. With these accesses, the attackers made lateral moves until they reached the CI/CD environments of the 3CX desktop application. According to Mandiant, DLL injection and service-level persistence techniques were executed to include malicious libraries in the application's official source code. Mandiant attributes the attack to the North Korean cybercriminal group Nexus.

Finally, these supply chain attacks are already being addressed by application security tool vendors. The team at Snyk, a third-party component vulnerability scanning tool, maintains an up-to-date list of malicious libraries being uploaded to traditional package managers. During August, the Snyk team reported more than 500 malicious libraries, almost 20% of which were written in the C and C++ languages, which may indicate that even IoT devices are being targeted by cybercriminals.

Supply chain attacks will continue to be an effective attack vector for cybercriminals when organisations fail to implement adequate security measures. The development and procurement processes for third-party software, components and libraries should be pillars of assurance. Investment in robust application security programmes is essential to ensure that the software lifecycle is secured, and that in case of cyber-attacks on third-party components and libraries, a timely reaction is possible. In the short term, the implementation of Software Bill of Materials (SBOM) is essential to determine the attack surface of organisations against threats to the software supply chain.

USE OF FAIR AS A KEY METHODOLOGY IN FAIR QUANTITATIVE RISK ANALYSIS

By: NTT DATA

The FAIR quantitative risk methodology has been discussed for many months now. A previous edition of RADAR introduced the methodology and its benefits. However, there are many doubts about its use, the effort needed to adopt it in an organisation and what kind of information is necessary to implement this methodology. In this article we want to take a closer look at how we should approach the analysis of a scenario and what kind of questions we will have to ask ourselves.

Let's consider some scenarios:

- Unavailability of transactional web banking in the banking sector
- Unavailability of a web shopping channel in the retail sector
- Unavailability of an insurance registration website of an insurance company

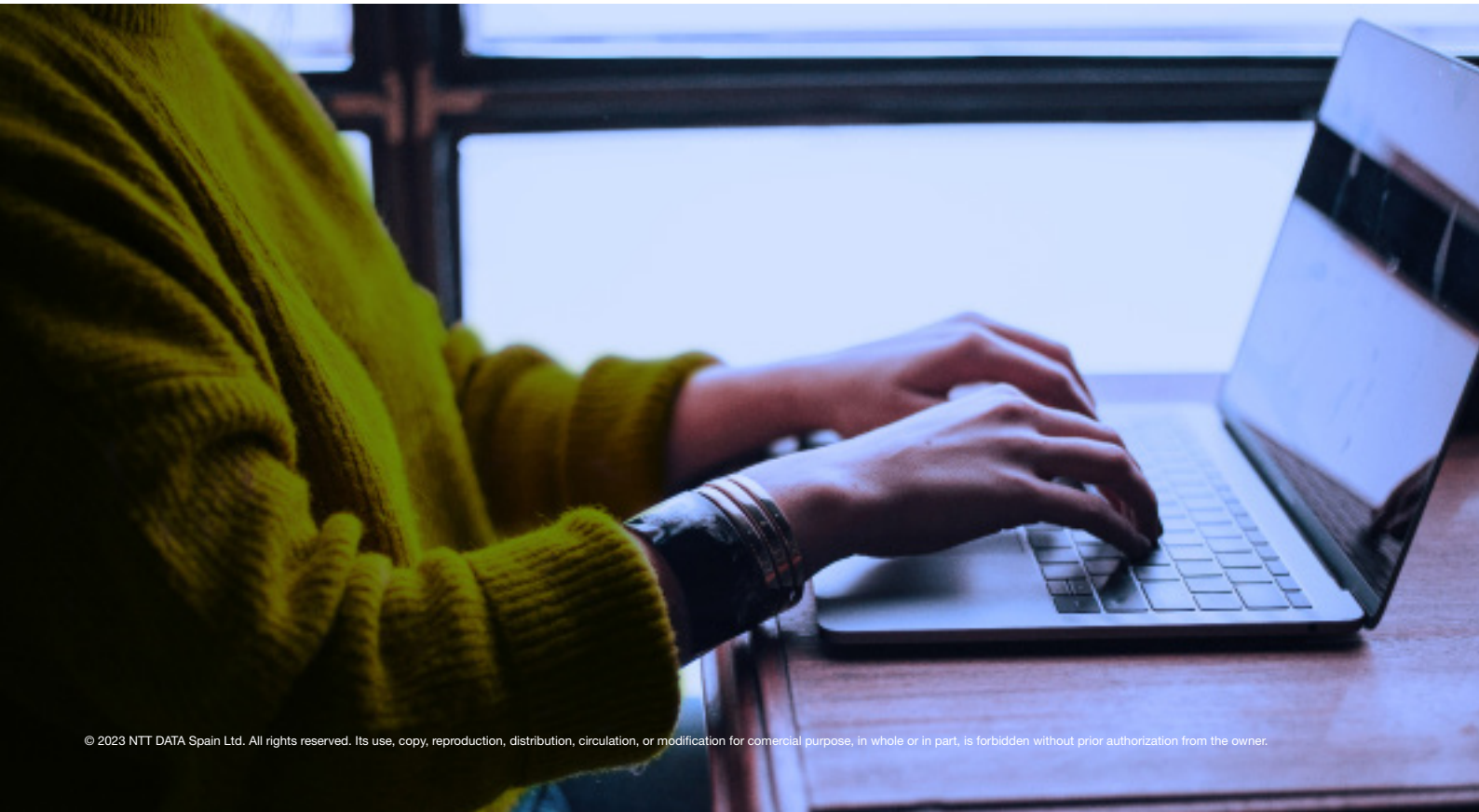
In these scenarios, FAIR helps us to answer the following questions:

- How much money will I lose next year in the most likely scenario due to unavailability of that system?
- How much will I lose as a minimum?
- What is the maximum?

Concrete data presented at the C-level can help to leverage investments needed to mitigate existing risks. The first step: contextualise in terms of the organisation, determining the sector to which it belongs, its processes and critical assets. This will serve to define the scope of the scenario to be assessed. The scenario must contemplate an asset and a threat agent, for example: transactional banking website with loss of availability due to ransomware. It is important to emphasise that each scenario (asset + threat agent) that we find must be analysed separately in FAIR, although as scenarios are analysed and information is gathered, it will be applicable to subsequent scenarios.

Once the scenario has been defined, we can begin to make assessments of loss magnitude and frequency of loss events. We will start with the magnitude of loss, which is divided into two main categories: primary loss (direct loss to the organisation and/or key stakeholders) and secondary loss (loss to the organisation and/or key stakeholders as a result of a negative reaction from second or third parties).

For primary loss magnitude assessments, think of 6 sub-categories: reputation, productivity, replacement, productivity, competitive advantage, and penalties.



To start with this assessment, we need to ask the following questions:

- Productivity loss: after the attack and the loss of availability of the transactional website, how many workers are affected in the best-case scenario, and how many in the worst-case scenario? What is their salary, and therefore, what is the economic loss in the best- and worst-case scenarios? As the model also asks for a "most likely" value, we can ask the question in the most likely scenario or simply average the minimum and maximum value.
- Recovery costs: the analysed organisation should have a recovery plan. How many people will execute this recovery plan as a minimum and as a maximum? How many hours are they expected to work as a minimum and as a maximum? What is their rate? With this information we can calculate how much the recovery will cost in a minimum, maximum value and we can use the average for the most likely scenario.
- Loss due to fines and judgements: the asset under analysis will have several clients who may be affected. how many will be affected as a minimum, and as a maximum, and what fine could we pay if there is a complaint? With this information it is now possible to calculate how much the organisation would pay in fines and judgements. The most likely value can be calculated based on the number of people likely to be affected and the likely cost of the fine, or simply as an average of the minimum and maximum values.
- The reputational damage caused in the scenario also needs to be quantified. What is the minimum and maximum reputational damage loss, and how much would it be in the most likely scenario?
- Likewise, there will be losses due to competitive advantage over other organisations providing the same service. Perhaps the information on this loss can be obtained from historical data on incidents where there have been movements of customers to another organisation. What was the minimum loss recorded? and the maximum? and the most common?
- Finally, replacement losses must be considered if applicable. That is, if the asset(s) involved in the scenario should be replaced when the assessed scenario occurs. Likewise, the minimum, maximum and most likely replacement value shall be considered.

Let us recall that the magnitude of loss is divided into two parts (primary and secondary), so we now need to analyse losses caused by second or third parties. For the secondary loss, we analyse the following information:

- Secondary loss per response: the impact on customers will generate that part of the organisation's work team will focus on the notification of these customers. How many customers will require attention as a minimum, and as a maximum, and how much will the most likely value be? What will the cost of notification be? With this, the minimum, maximum and most likely secondary productivity loss can be calculated.
- Secondary loss due to fines and judgements: there could be claims and complaints from our clients or due to them being fined by their own clients because our incident affected a service that they were unable to provide in a timely manner. In this case, an analysis should be made of what would be the minimum expected for these fines, sentences, or sanctions. What value would be the most likely and what could we expect in the worst case?
- Secondary productivity loss: for this value we need to think about what additional team we need to hire to deal with the complaints and claims we are going to receive. For example, the organisation may need to reinforce the legal department or have external legal advisors. At this point we will think about how many additional people we will need at a minimum, at a maximum and most likely, for how long and at what rate. With these values, we can calculate minimum, average, and maximum values.
- Secondary reputational loss: This value refers to loss of share value and failure to meet customer acquisition projections. Think about how much we stand to lose from these events as a minimum, how much as a maximum and how much would be most likely.

Once all these questions have been answered, the monetary loss analysis of the scenario is concluded. The last step is to determine the frequency of loss events and vulnerability of the asset in scope of the scenario.

For the frequency of loss events, an analysis of past incidents can be performed, and it should be determined how many events will occur next year at a minimum, at a maximum and on average. For example, in an asset unavailability scenario, you can review how many times that asset has been unavailable in the last 5 years, and take the minimum, maximum and average value as the most likely.

And finally, and perhaps the most complex question in the analysis: measuring the resilience of the asset. This asset will have different security measures already in place in the organisation, this will greatly reduce the vulnerability to attackers - in what % of attacks, at best, are the security controls expected to prevent the attack? and in the worst case? and in the most likely case?

Now, with all the information collected, it is possible to enter all the information into the analysis tool, which allows us to have an estimate of the loss. The interesting thing about FAIR is that it will return 3 values:

- Value 1: minimum loss value.
- Value 2: most probable loss value.
- Value 3: maximum loss value.

In addition to this, the tool provides a visualisation of how many events per year are possible (based on the event and vulnerability information provided). In other words, we will be able to say how many events there will be as a minimum, as a maximum and in the most likely scenario.

Once this point has been reached, the strategy begins: what projects can we implement to increase resilience, how much will this resilience improve, and how much does the model tell us that we will lose with this new security measure? The important thing will be to define what measures, initiatives, investments, and implementations to carry out and to ensure that these projects have a greater economic impact than their cost in losses. From that moment on, companies will be able to use the full potential of FAIR.

TRENDS

Trends: security and privacy in Artificial Intelligence

According to the Artificial Intelligence Index Report (2023), around 31 countries have issued and/or approved some regulatory framework related to AI during the period 2016 to 2022. The aim of such regulation is to provide privacy and security guidelines to be considered for projects involving the design, development, and deployment of an AI system.

So, what should be done to ensure the security and privacy of an AI system?

For an AI system to be secure and guarantee the right to personal data protection, it must be verified whether it complies with legal, organisational, and technical controls. To this end, it is essential that, based on a framework focused on current regulations, an assessment can be made to determine the level of maturity of the AI system and, if necessary, to adopt the necessary corrective measures.

But what domains should be analysed in an artificial intelligence framework?

a) First, proper **identification and transparency of the AI system** must be ensured. Aspects such as purpose, identification of responsibilities, transparency, and identification of context of use should be analysed and ensure that such information exists.

b) **AI system fundamentals:** Ensuring that the fundamentals of the AI system are correctly defined. Aspects to be analysed include identification of the development policy, adequacy of the basic theoretical models, as well as the methodological framework and identification of the basic architecture.

c) **Data management:** Ensuring that the processes for collecting, storing, processing, and protecting the data used by an AI system are properly defined. Aspects such as: determination of the origin of data sources, control of bias, data preparation and data quality should be analysed.

d) **Risk management:** Ensuring the identification, assessment, control and monitoring of risks associated with the implementation and operation of an AI system. Aspects such as mapping, measurement and management should be analysed.

e) **Incident and malfunction information exchange:** Ensuring effective communication between organisations and stakeholders regarding security incidents, vulnerabilities, and malfunctions in an AI system. Issues such as serious incident reporting, access to data and AI system source code should be addressed.

f) **Verification and validation:** Ensuring that the AI system works in accordance with the established requirements and produces accurate and reliable results. Aspects such as: consistency, performance, safety, and traceability should be analysed.

A thorough review of these domains and adaptation of artificial intelligence systems to meet them will enable organisations to get the most out of this technology, without compromising their business or the trust of their customers.

VULNERABILITIES

HP

CVE-2023-30908;-2650;-4304
Date: 07-09-2023

Description. On 7 September, a critical vulnerability (CVE-2023-30908) affecting the OneView product, dedicated to infrastructure management developed by Hewlett Packard Enterprise, was published. At the same time, two vulnerabilities (CVE-2023-2650 (High) and CVE-2022-4304 (Medium) have also been published on the same product.

These vulnerabilities allow a remote attacker to bypass authentication and gain unauthorised access to HPE OneView, because of how the tool handles user credentials, a request explicitly designed for HPE OneView can be manipulated.

By exploiting these vulnerabilities an attacker can obtain sensitive information such as encryption keys and passwords or perform a denial of service (DoS) attack against HPE OneView.

Link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04530en_us
https://nvd.nist.gov/vuln/detail/CVE-2023-30908

Affected Products: All versions prior to v8.5 or v6.60.05 LTS.

Solution: The recommended solution to address this vulnerability is to apply the latest security patches v8.5 or v6.60.05 LTS.

Linux

CVE-2023-4206
Date: 06-09-2023

Description. This overflow vulnerability is associated with the route4_change function in the net/sched/cls_route.c file. Through the manipulation of an unknown input, a buffer overflow class vulnerability is caused.

The exact effects of a successful attack are not known, although it could lead to denials of service and possible privilege escalation. There is currently no known exploit for this vulnerability.

Link: https://www.debian.org/security/2023/dsa-5492
https://www.suse.com/security/cve/CVE-2023-4206.html
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b80b829e9e2c1b3f7aae34855e04d8f6ecaf13c8

Affected Products: The resources affected by this vulnerability are as follows:

- Red Hat Enterprise Linux 8 or later
- SUSE Linux Enterprise Desktop/Server 15 or earlier
- Debian 6.1.38-1 or earlier and 4.19.249-2 (version 6.1.52-1 fixed)

Solutions: The resolution will consist of upgrading to the latest versions released by each manufacturer.

PATCHES

Apple

Date: 07-09-2023

Description. Apple has released a security update for iOS and iPadOS that fixes two zero-day exploits (CVE-2023-41064 and CVE-2023-41061). The security flaw affects the latest version (16.6) of the iOS operating system, was discovered by researchers at Citizen Lab, which belongs to the zero-click family, and manages to infect the device with the Pegasus malware without the need for user intervention.

The exploit involves PassKit attachments that contained malicious images sent from an attacker's iMessage account to the victim for NSO Group's Pegasus software.

This vulnerability is associated with a buffer overflow over the ImageI/O component, which allows applications to read and write most image file formats.

Link:
https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/
https://support.apple.com/en-us/HT213905

Affected products: The vulnerability affects all supported versions (16.6 and earlier).

Update: The patches are applied by installing iOS 16.6.1 and iPadOS 16.6.1.

Google Chrome

Date: 11-09-2023

Description. Google has released a security update for a critical zero-day vulnerability in Chrome (CVE-2023-4863). This vulnerability is exploited via a buffer overflow in the component that handles WebP, a raster graphics file format that replaces JPEG, PNG, and GIF file formats. Execution of this vulnerability can cause denial-of-service failures or allow malicious code to be executed on systems.

This vulnerability may be being exploited as Google is aware that an exploit for this vulnerability exists, as reported by Apple Security Engineering and Architecture (SEAR) and The Citizen Lab at the University of Toronto's Munk School.

Link: https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
https://nvd.nist.gov/vuln/detail/CVE-2023-4863

Affected products: The vulnerability affects all versions prior to 116.0.5845.187 for Mac and Linux, and 116.0.5845.187/.188 for Windows.

Update: Google has released an automatic update to the new versions 116.0.5845.187 for Mac and Linux, and 116.0.5845.187/.188 for Windows.

EVENTS

FS-ISAC FinCyber Today Summit

1- 4 October 2023 |

This summit is a multi-day, face-to-face event for IT security professionals working in financial institutions. It shows attendees how they can apply new IT security trends and practices in real life to better protect their organisation. The event covers several topics. For example, “Fraud, Identity and Money”, “GRC and Resilience” and “Intel and Global Attacks”. Attendees can choose the topic that best suits their business needs.

Link: https://www.fsisac.com/events/2023-fincyber-today-summit

CSA Virtual Research Summit

17 October 2023 |

CSA is hosting a special event showcasing the research projects that will define cloud security in the coming year. With an eye on important cloud and cybersecurity trends, the CSA Research Summit will offer the latest updates on new and existing research projects and provide critical tools and guidance for the cloud-adopting community. With the cloud finally entrenched as the primary IT system worldwide, cloud security is now the foundation of cybersecurity programs.

LInk: https://www.csaresearchsummit.com/event/17e14892-a68e-4db9-82a9-528bf4bdbb4e/summary

Capacitaciones Blackhat

23 - 26 October 2023 |

SecTor has built a reputation for bringing together experts from around the world to share their latest research and techniques on clandestine threats and corporate defences. The conference provides an unrivalled opportunity for IT security professionals, managers and executives to network with their peers and learn from their mentors. This year SecTor is launching the “Certified Pentester” programme, a one-day, hands-on exam.

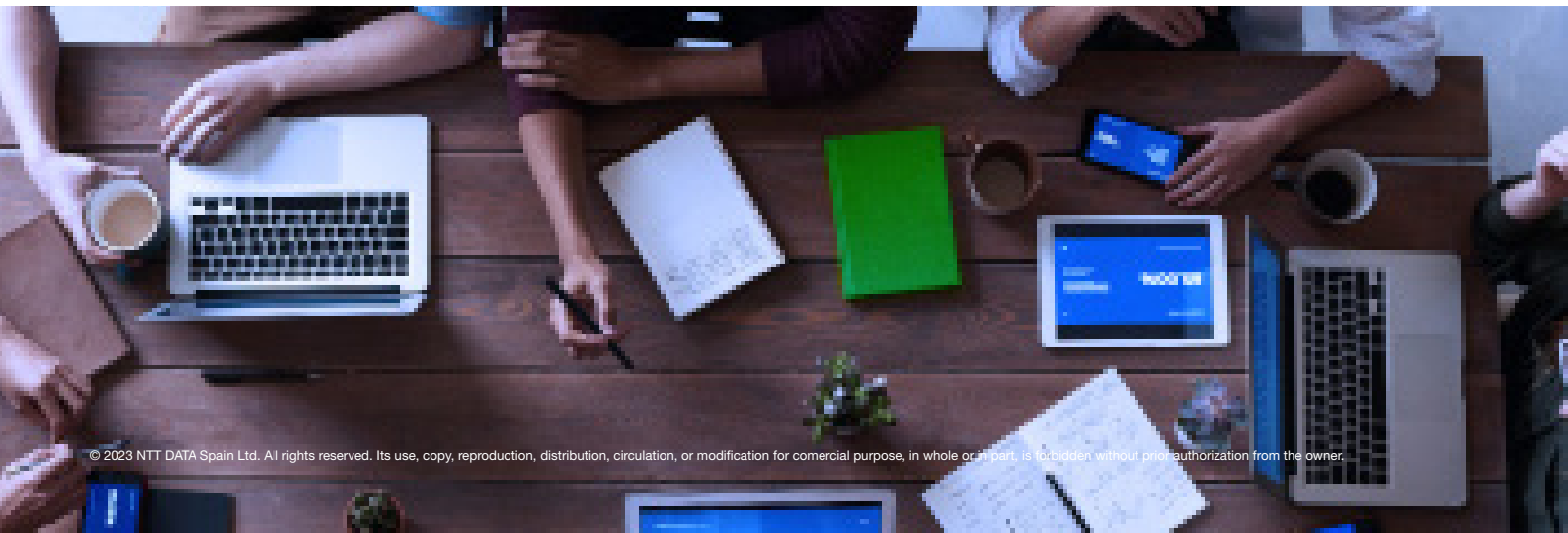
Link: https://www.blackhat.com/sector/2023/

SANS Ciber Solutions Fest

27 - 28 October 2023 |

This conference helps organisations plan their security investments. It aims to connect industry thought leaders and suppliers with security decision-makers and practitioners. It is free and held entirely online.

Link: https://www.sans.org/blog/coming-soon-sans-cyber-solutions-fest-2021/



RESOURCES

Cloud Native application protection platform survey report

Microsoft commissioned CSA to produce a survey and report to better understand the industry's knowledge, attitudes and opinions regarding CNAPP security. The survey was conducted online in April 2023 and received 1201 responses from IT and security professionals. The report aims to provide insight into organisations' cloud security priorities and challenges, reveal the current state of CNAPP implementation, and identify current methods and challenges in security posture management, cloud workload protection and DevSecOps.

Link: https://cloudsecurityalliance.org/artifacts/state-of-cnapp-survey-report/

CSA Assurance Education FAQ

The Certificate of Cloud Audit Knowledge (CCAK) and STAR Lead Auditor Training are two assurance training offerings that are part of CSA's Security, Trust, Assurance and Risk (STAR) programme, the world's largest cloud assurance programme.

Link: https://cloudsecurityalliance.org/artifacts/csa-assurance-education-faq/

Secure configurations in industrial devices

The hardware and software bases that are configured and installed in the system are just as important as the bases of social engineering that have been taught to employees, since the chain is broken by the weakest link, and that is human beings. In this article INCIBE provides, among other things, a list of good practices for the bastioning of OT devices.

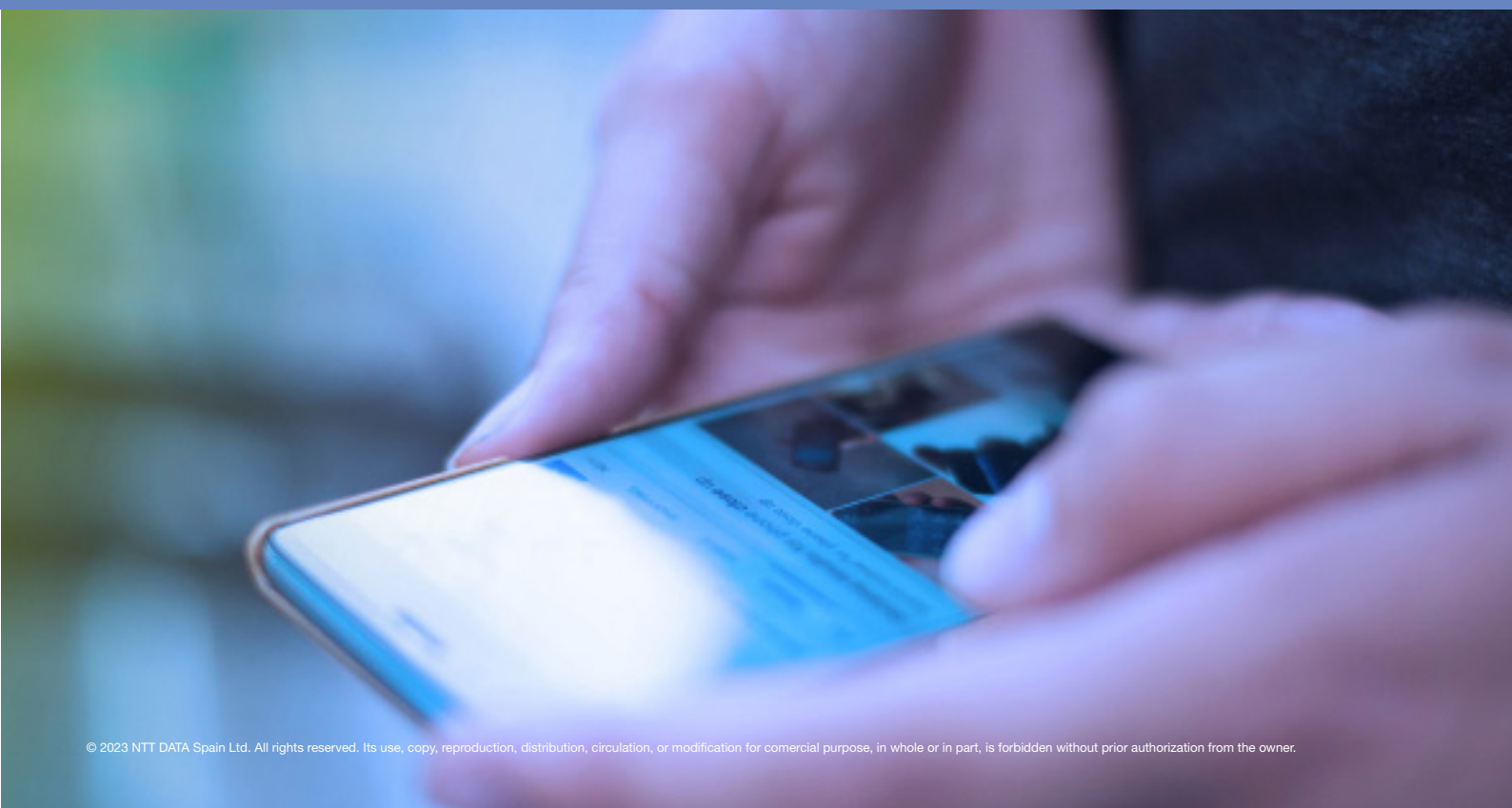
Link: https://www.incibe.es/incibe-cert/blog/configuraciones-seguras-en-dispositivos-industriales

External access in ICS

External access is a technology that will be increasingly implemented in companies due to the benefits it produces, such as the convenience it offers to employees and the reduction of costs.

Even so, it should be noted that with this technology we must be very careful, as it can also cause different cybersecurity problems for the company, such as access by unwanted users or the theft of sensitive information, which is why the use of tools such as VPN connections or the implementation of dedicated monitoring equipment, such as SOC OT, are very important to ensure the security of remote access.

Link: https://www.incibe.es/incibe-cert/blog/accesos-externos-en-sci-arma-de-doble-filo



RESPONSIBLE CYBER

María Pilar Torres Bruna

Cybersecurity Director at NTT DATA Latam and Peru

maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schwarzer

Cybersecurity Director at NTT DATA Brasil

carla.passosschwarzer@emeal.nttdata.com

Miguel Angel Garzón Ramírez

Cybersecurity Manager at NTT DATA Colombia

miguel.angel.garzon.ramirez@emeal.nttdata.com

Fernando Vilchis

Cybersecurity Director at NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Cybersecurity Manager at NTT DATA USA

nestor.ordonez.ramirez@emeal.nttdata.com

Jose Uzcategui

Cybersecurity Manager at NTT DATA Chile

jose.uzcategui@emeal.nttdata.com


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