Issue 93 | August 2024

NTT DATA

Radar

Cybersecurity magazine

The Future of SOCs: Revolution and Resilience in Cybersecurity

By Javier Portabales Campos

In the current context, Security Operations Centers (SOCs) have established themselves as fundamental elements in the defense strategy in terms of cybersecurity, providing continuous surveillance and an agile response to threats. As we move into the future, the opportunities and benefits of having one multiply and become more relevant.

On the one hand, there is the evolution of artificial intelligence and machine learning, which allows SOCs to be more efficient in threat detection, continuously improving incident detection and response. Through advanced algorithms, they can identify anomalous patterns and resolve potential incidents before they occur. This might remind us of the film Minority Report, but it not only enhances incident response capabilities but also reduces the time and costs associated with cyberattacks since attackers are integrating artificial intelligence into their attacks.

In addition to this, learning will improve closer integration with various real-time data sources, ranging from network and system monitoring to the collection of global threat intelligence. With a holistic and real-time view of threats, these centers can make more informed and proactive decisions, enhancing the overall security of the organisation.

Another improvement will be automation, which will play a crucial role in the SOCs of the future. Repetitive and tedious tasks, such as initial alert analysis and data collection, can be managed by automated systems. This allows human analysts to focus on solving more complex problems and long-term strategy, increasing the operational efficiency and effectiveness of security operations. The democratisation of AI and its integration into market products means that they are being integrated into XDR solutions and correlation systems. This enables security centers to scale up with smarter technology rather than with people.

As cyber threats become more sophisticated and global, collaboration between different centers will become essential. The future will see greater sharing of intelligence and best practices between organisations and countries, something we already do at NTT DATA with our global network of SOCs. This global collaboration will enable a more robust and coordinated defence against malicious actors, benefiting the global community as a whole.

Another fundamental pillar will be skills development. Cybersecurity is an ever-evolving field, and keeping teams updated with the latest trends, techniques, and tools is crucial. SOCs will offer continuous training programmes, using simulations and practical exercises to prepare analysts for any eventuality.

The rise of emerging technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence presents new opportunities and challenges for cybersecurity. SOCs will need to be equipped to adapt quickly to these changes, implementing specific security measures to protect these environments and ensure the integrity of data and systems.

As we can see, SOCs are not only a necessity in the present but also represent an opportunity to build a safer and more resilient future. With the integration of advanced technologies, process automation, and increased global collaboration, security operations centers are in a privileged position to face the cybersecurity challenges of tomorrow. Organisations that invest in the development and continuous improvement of their SOCs will be better prepared to protect their assets and data, ensuring continuity and success in an increasingly digital world.

Javier Portabales Campos
Cybersecurity Director

The Cybersecurity Challenge

Cyberchronicle byJuan Fernandez Martinez & Diego Alonso Fernandez

In recent weeks, there has been a worrying wave of cyberattacks that have jeopardised the security of multiple companies and government organisations. The months of May and June 2024 were no exception, with attacks affecting major Spanish entities such as Telefónica, Iberdrola, and Banco Santander. These attacks have exposed the data of millions of users, increasing the risk of fraud and identity theft.

Telefónica suffered an attack that compromised the information of 120,000 customers and employees, although they assure that no critical data was exposed. On the other hand, the intrusion into Iberdrola affected 850,000 customers, extracting data such as names, surnames, and DNI numbers. These events highlight an alarming trend in the country's cybersecurity, with increasingly severe consequences for the privacy and security of citizens.

Among the multiple incidents in June, the cyberattack on the Directorate-General for Traffic (DGT) stood out for its magnitude and potential impact on the Spanish population. The Research and Analysis Group of the Traffic Division of the Civil Guard (GIAT) announced that several users had attempted to access driver data and their access was cut off. These users have been identified and are under investigation.

It all started with a post on criminal forums specialising in the buying and selling of sensitive data, where a user claimed to have information on up to 34 million drivers.

According to the published photo, the cybercriminals had obtained the following records: licence plate, type, make and model of the vehicle, name, address and town of the owner, and current insurance details. This allowed buyers to access specific data about individuals without needing to purchase the entire database.

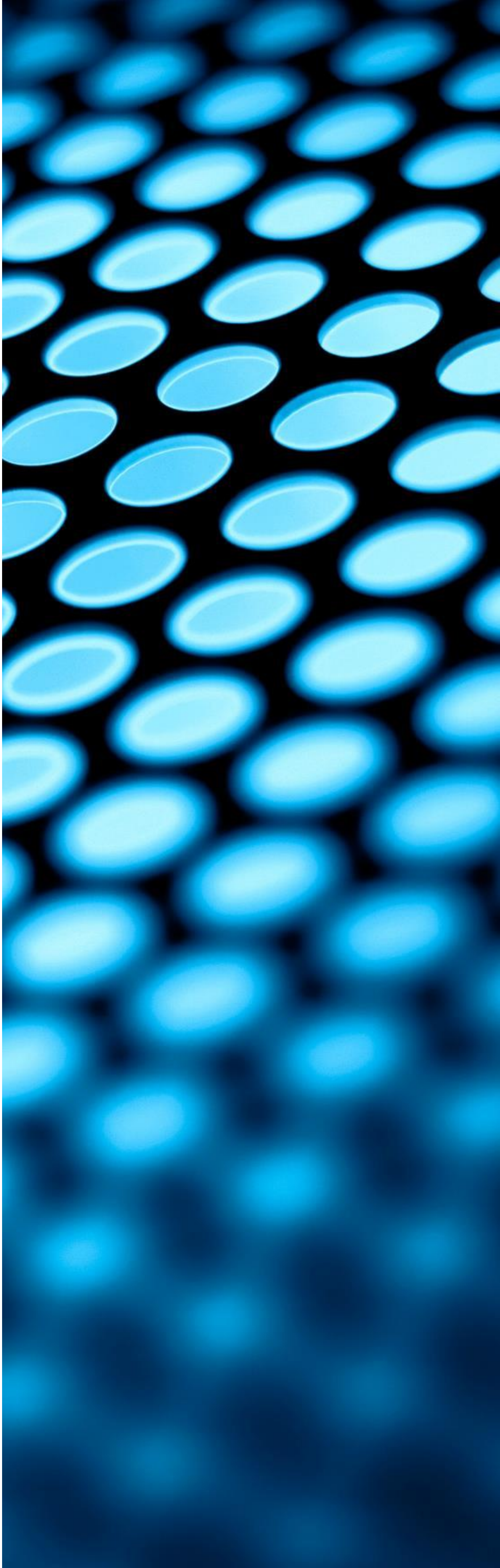
Another incident adds to the growing list of Spanish entities that have fallen victim to data breaches. The DGT is a repeat target, as in March of this year, a young man from Murcia was arrested for obtaining compromised data on 40 million drivers and vehicles, which he intended to sell.

On that occasion, the attacker had acquired all the technical characteristics of millions of vehicles associated with the personal data of each owner, aiming to create a searchable database to later profit from it.

These recent cyberattacks are a stark reminder of the growing cyber threats facing Spain. The scale of the compromised data and its potential malicious use underscore the urgent need to strengthen cyber defences across all sectors, both governmental and corporate. The personal data of millions of drivers is now at risk of being used for fraud, phishing, and other malicious activities.

The sale of this information further exacerbates the situation, facilitating access to personal data by cybercriminals worldwide.

It is crucial for users to be aware of these risks and take preventive measures, such as avoiding unnecessary sharing of personal information, using strong and unique passwords, and being cautious of suspicious emails and messages. Security in the digital world not only relies on infrastructures but also on the prudence and awareness of each user.



Juan Fernandez Martínez
Cybersecurity Analyst

Diego Alonso Martínez
Cybersecurity Analyst

SOC 3.0: The Evolution of the Blue Team

Article by Jose Julio Ruiz de Loizaga Ruiz

Historically, the threats faced by cybersecurity have increased exponentially year after year. This is expected, as vulnerabilities are discovered, new malware families, APTs, and new techniques and tactics emerge. However, in recent years, a new characteristic has come into play. The number of threats is no longer the main problem; the real issue is their sophistication. There has been an increase in complexity based on the use of the latest technologies, such as AI and machine learning.

SOCs are facing a new challenge; traditional techniques are no longer sufficient to counter new threats. The solution lies in using the same technologies to meet these new challenges.

Integration of AI in SOCs

"*Artificial intelligence could be the best or the worst thing to happen to humanity.*" - Stephen Hawking.

The ability of attackers to develop more sophisticated and harder-to-detect cyberattacks creates a complex scenario to tackle. The image of a teenager in their room attempting to access systems has long disappeared. Now, multidisciplinary teams, including experts in new technologies, particularly AI, are involved.

The algorithms on which AI is based can analyse large volumes of data to identify vulnerabilities in security systems, allowing attackers to create highly personalised malware and exploits. They can also generate phishing attacks that perfectly mimic human communication and can be surgically targeted, automatically gathering information from the intended victim.

Given this scenario, the only solution is to combat AI with AI.

The premise is clear, new technologies are emerging as crucial tools to enhance the efficiency and effectiveness of SOCs in the face of new attacks and threats..

SOCs must evolve; AI is necessary to analyse large volumes of data in real-time to detect possible attacks and help mitigate them almost immediately through its integration into advanced orchestration systems (SOAR).

AI will also support technicians in investigating difficult-to-resolve cases by providing information that allows experts to more efficiently focus on the data to be analysed. If all countermeasures are compromised, AI also facilitates post-incident analysis, extracting valuable information that can be used to strengthen defences and prevent future breaches.

However, it is not just about implementing artificial intelligence within SOCs; machine learning will support in carrying out repetitive and routine tasks such as event correlation and alert classification, freeing up analysts to focus on more complex and strategic issues. Deep learning will help enhance implemented use cases and analyse them throughout their lifecycle. Natural language processing (NLP) or image recognition will aid in detecting phishing or data exfiltration, for example.

User and Entity Behaviour Analytics (UEBA), while a specific application of artificial intelligence, can be considered a technology in itself, assisting in detecting insiders within organisations.

The incorporation of these technologies is not trivial; each Security Operations Centre needs to be independently analysed to determine the best way to adapt these new tools within it. The tools used, the managed information, its quality, and its volumes will be crucial in designing an optimal transition.

However, the ultimate goal is not merely the integration of new tools.

The real change.

It might seem that the goal is to fully automate SOCs, diminishing the importance of the human factor, but that is not the case. Up until now, technicians have been at the heart of SOCs, handling tasks ranging from alert analysis to forensic analysis, as well as trivial, repetitive tasks that add little new value.

The true evolution lies in establishing two axes within the SOC. In one axis, technicians will remain central, leveraging their knowledge, experience, and interpretive skills to address new cases, new techniques, and innovative ways to attack and defend systems.

In another axis, new technologies are industrializing every task and enabling autonomous management by a system, such as tasks that provide support and assistance to technicians.

The third component of the new SOCs will be the interplay between both "worlds": tasks executed by technicians will help new technologies develop their capabilities, teaching automated systems to make more informed and effective decisions.

New profiles.

To unlock the full potential of new technologies and their integration into a SOC, one fundamental variable is the capabilities of technicians.

In the relatively near future, we will need technicians who not only understand security threats but also have sufficient knowledge to leverage new technologies effectively..

We will have experts in malware with advanced knowledge in machine learning capable of developing engines to detect new ransomware or trojans, or fraud technicians who can leverage graph analysis of financial institution operations. Terms like "K-means," "Random Forest," or Generative Adversarial Networks (GANs) will be as familiar as API, Framework, or WAF, and we all will need to assimilate these new technologies. Within SOCs, this will be fundamental, dare I say, vital.

Perhaps the greatest challenge we face is not only a shortage of cybersecurity professionals but also the need for profiles that combine multiple technological disciplines to drive the evolution of SOCs.

In a few words...

The new threats compel us to implement these changes and integrate new technologies. It will require evolving the structure and way of working within SOCs. Technicians will not only need to be cybersecurity professionals but also experts in training and enhancing new technologies. These are changes we must undertake, much like installing antivirus software years ago due to the rise in malware.

José Julio Ruiz de Loizaga Ruiz
Cybersecurity Technical Manager

Cybersecurity Challenges in the Age of Artificial Intelligence: A Path to Responsible Democratisation

Tendencias por Gerard Marin Raventós

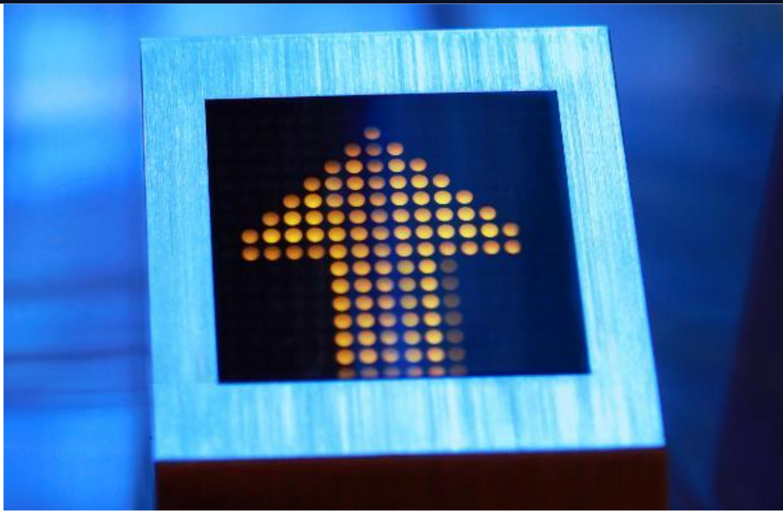
One day it could be an unauthorized intrusion, the next a ransomware attack, and the day after, a phishing campaign affecting half the organization. Following a period of "relative calm," there is a data breach, and to cap it off, a DDoS attack originating from 28 different countries. Although somewhat exaggerated, the truth is that working in a SOC is complex and subject to constant changes.

In addition to all this, there is another dimension to consider: managing incidents in emergency situations where speed and efficiency must be the foundations of such management. Beyond the technical elements present in a SOC (such as SIEM, EDR, XDR, AI, etc.), is not the people who are there making the final decisions. Individuals in these roles should have the appropriate skills and attitudes for their positions.

Starting with the most active role, those responding to an incident in a SOC should always be aware that they can go from a relaxed calm to high-stress tension in seconds. Not only should they be aware, but they should also be prepared to act accordingly. They should feel comfortable working under pressure, be diligent in executing procedures (when they exist), and able to make quick decisions. Since incident detection is primarily handled by technical systems, the ability to respond to an incident is highly valued: the response should be correct, appropriate, and relevant.

However, it is also possible that during incident management, procedures may not be in place or actions taken may not yield the expected results. In such cases, SOC operators should also have a problem-solving mindset, often linked to imaginative and creative thinking, to find a way around obstacles encountered.

Lastly, but equally important, knowing how to work as part of a team is vital when tasks involve coordination and cooperation with colleagues. Therefore, the ability to work collaboratively and the humility to recognize one's limits and seek help from others are the final attitudes and skills one should possess when working in a SOC.



But working in a SOC is not just about being stressed throughout the shift, managing incidents, and making decisions. There are moments of calm where operators can continue to perform other types of tasks and functions such as analysis, report writing, or procedure development.

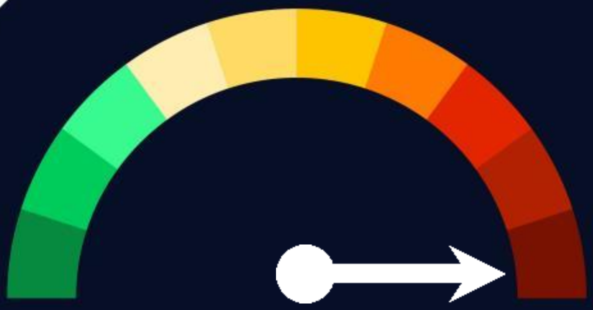
In this second aspect, two important characteristics emerge for someone working in a SOC. The first is having a proactive attitude. Working in a SOC is not only reactive to incidents; it also requires workers to have a disposition towards improvement, research, and vulnerability detection. It involves reviewing current protocols and procedures to see if they can be enhanced. In essence, when not responding to a materialized threat, the work involves facilitating, improving, and making future responses more efficient.

Gerard Marin Raventós
Cybersecurity Consultant

Vulnerabilities

Critical vulnerability in the MongoDB Compass tool

Date: July 1, 2024
CVE: CVE-2024-6370



CVSS: 9,8

Critical

Description

A critical vulnerability has been discovered in the interactive tool MongoDB Compass, used for querying, optimizing, and analyzing data in MongoDB.

This vulnerability, identified as CVE-2024-6376, allows for code injection due to incomplete sandbox protection configuration in the handling of Compass connections using the ejson shell analyzer.

This flaw is categorised under CWE-20, as it allows for data input but incorrectly validates that the input meets the necessary properties for securely processing the data.

Solution

Affected users are advised to update to version 1.42.2, which has been released by the developers of MongoDB Compass. This update includes necessary fixes to address the vulnerability, enhancing the overall security of the application.

- MongoDB Compass: Update to version 1.42.2 or later.

Affected Products

This vulnerability affects the following versions of the product:

- MongoDB Compass: versions prior to 1.42.2.

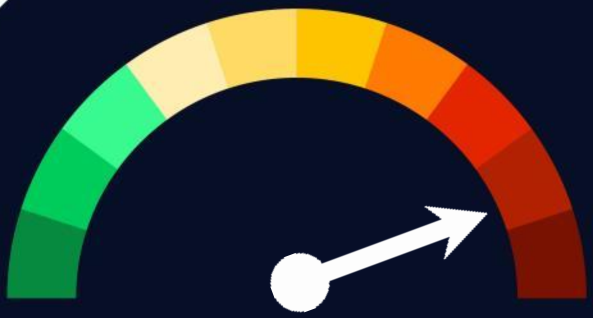
References

- nvd.nist.gov
- jira.mongodb.org

Vulnerabilities

High severity vulnerability in GitLab CE/EE

Date: June 27, 2024
CVE: CVE-2024-5655



CVSS: 8,8

Critical

Description

A security vulnerability has been detected in GitLab CE/EE, classified as highly critical. This vulnerability allows attackers to trigger pipelines (execution lines) as if they were another user under specific circumstances. This can result in unauthorised code execution and potential alterations to projects and data within GitLab.

The vulnerability originates in the workflow of re-targeting Merge Requests (MR). When a target branch is merged, pipelines could be automatically triggered without user intervention. An attacker could manipulate this functionality to execute pipelines under another user's identity, representing a serious security risk.

Solution

Users of GitLab are strongly advised to update their products to the following versions:

- GitLab CE/EE: update to version 17.1.1, 17.0.3, or 16.11.5.

GitLab has not found evidence that these vulnerabilities are being exploited, but due to their high criticality, it is crucial to apply the updates as soon as possible.

Affected Products

The versions of the affected products are as follows:

- Versions between 15.8 and 16.11.5 of GitLab CE/EE.
- Versions between 17.0 and 17.0.3 of GitLab CE/EE.
- Versions between 17.1 and 17.1.1 of GitLab CE/EE.

References

- nvd.nist.gov
- www.incibe.es

Google's July security update

Date: July 1, 2024
CVE: CVE-2024-31320 and 24 more

Critical

Description

Google's July 2024 security patches include updates affecting Google's Pixel (Android) devices.

Among the patches addressing 25 security vulnerabilities, one (CVE-2024-31320) has been classified as critical in the Framework component, which could lead to local privilege escalation without the need for additional execution privileges. This corrects a security issue that allowed third-party applications to bypass the prompt message using setSkipPrompt.

This patch also addresses seven other high-severity issues, including three privilege escalation bugs in the Framework component, three privilege escalation vulnerabilities in the System component, and one information disclosure flaw in the System component.

Additionally, new patches were released on 5 July 2024, resolving a total of 17 vulnerabilities found in the Kernel, Arm, Imagination Technologies, MediaTek, and Qualcomm components.

Affected Products

The products affected by this vulnerability as follows:

- SolarWinds Serv-U 15.4.2 HF 1 and earlier versions (CVE-2024-28995).
- SolarWinds Platform 2024.1 SR 1 and earlier versions (CVE-2024-28996, CVE-2024-28999, and CVE-2024-29004).

Solution

Google recommends updating to the released security patches to address the vulnerabilities present in Pixel devices.

References

- source.android.com
- www.securityweek.com

Patches

Splunk releases several patches to fix vulnerabilities

Date: July 1, 2024
CVE: CVE-2024-36985

Critical

Description

Splunk has released patches to fix a high-severity vulnerability (CVE-2024-36985). This vulnerability allows a non-admin user to execute remote code via an external search referencing the "splunk_archiver" application. The specific issue lies in the "copybuckets.py" script within this application

Solution

Splunk recommends all users update the affected products to the patched versions (9.2.2, 9.1.5, and 9.0.10) as soon as possible.

These updates eliminate the possibility of exploiting the vulnerability by securing the external search process and implementing stricter access controls.

Additionally, users are advised to review and strengthen permissions for low-privilege users and monitor any unusual activity associated with the "splunk_archiver" application.

Affected Products

The vulnerability affects the following products:

- Splunk Enterprise: versions prior to 9.2.2.
- Splunk Enterprise: versions prior to 9.1.5.
- Splunk Enterprise: versions prior to 9.0.10.

References

- cve.mitre.org
- www.incibe.es
- www.securityweek.com

Events

Manchester Cybersecurity EXPO (24 July)

Cyber Security EXPO is the only exclusive recruitment event designed for clients and recruitment agencies operating within the cybersecurity industry. The EXPOs are an excellent way to interact and network with various employers looking to hire workers for both temporary and permanent cyber roles. The event is free for all attendees.
Link

Gartner Security & Risk Management Summit Tokyo (24 – 26 July)

The Gartner Security & Risk Management Summit Tokyo 2024 is an event that will take place in Tokyo, Japan, from 24 to 26 July. This event will cover various key topics, such as generative AI, risk management, cloud security, and more. Additionally, attendees will have the opportunity to participate in expert-led sessions on threat intelligence, incident response, and the critical role of human factors in building resilient security systems.
Link

The V Women in Security Forum (1-2 August)

The V Women in Security LATAM & Caribbean Forum 2024 is a flagship event organized by the Women in Security Community of ASIS International with the support of the ASIS Panama Chapter. This forum aims to highlight the most relevant challenges and opportunities in security, sustainability, digital transformation, cybersecurity, leadership, and resilience in the region.
Link

Black Hat USA (3 - 8 August)

One of the most significant events in the field of cybersecurity, Black Hat USA offers conferences, workshops, and training sessions showcasing the latest advancements and trends in computer security.
Link

DEFCON 32 (8 - 11 August)

DEFCON is one of the largest and oldest hacker conferences in the world, where talks, competitions, and workshops on various aspects of cybersecurity and hacker culture take place.
Link

Resources

Spain To Implement Free Parental Controls On Electronic Devices

The Spanish government will implement a law requiring free parental controls on all electronic devices sold in the country to protect minors from inappropriate content and cyberbullying. Manufacturers will be mandated to include these tools at no additional cost.
Link

NASA Plans to Build Nuclear Plants on the Moon

NASA has announced plans to build nuclear power plants on the Moon by 2030, aiming to provide a reliable energy source for future missions and lunar bases. This project seeks to develop technologies capable of withstanding the extreme conditions of space and ensuring a continuous supply of power for lunar exploration.
Link

Solana Labs Launches Saga: A Blockchain Smartphone for Web3

Solana Labs has launched Saga, its new smartphone designed with blockchain technology to support Web3 applications. This device aims to facilitate the adoption of cryptocurrencies and decentralized applications, providing a secure and optimized platform for users and developers within the blockchain ecosystem.
Link

New Amazon Alexa Feature Will Mimic the Voice of a Deceased Family Member

Amazon has announced a new feature for Alexa that will allow the voice assistant to mimic the voice of a deceased loved one using artificial intelligence. This technology aims to create more personalized and comforting experiences for users, although it has raised concerns about the ethics and privacy implications of its use.
Link

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com