Issue 96 | November 2024

NTT DATA

# Radar

## The cybersecurity magazine

# Privacy: a right or a privilege?

By Francisco Javier García Lorente

**Privacy has emerged as one of the most contentious and fundamental issues of our society. As technology advances at a relentless pace, the line that separates privacy as an essential right from its consideration as an exclusive privilege becomes increasingly blurred. This debate carries legal, social, and technological implications that affect every individual. Therefore, we must reflect: is privacy an inherent right, or a privilege reserved for those with the necessary resources to protect it?**

## Privacy as a fundamental human right

In many countries, privacy is recognised as a fundamental right. Article 12 of the Universal Declaration of Human Rights states that "no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks." This principle has been extended through various constitutions and legislations across the world.

From this perspective, privacy is not only the right to be free from observation or interference without consent, but also the right to have control over personal information, how it is collected, used and shared. This notion has been reinforced by regulatory frameworks such as the current General Data Protection Regulation (GDPR) in the European Union, which provides a robust approach to ensuring that citizens have control over their data.

However, although the law recognises privacy as a right, the effective implementation and enforcement of this right varies considerably. Not all citizens, even in countries with strict regulations, enjoy the same level of protection for their privacy. This is where the question arises: is privacy an equal right, or does it, in practice, become a privilege accessible only to a few?

## The erosion of privacy in the digital age

The advancement of technology has brought with it an exponential number of new tools and platforms which, although they make life more efficient, have also significantly undermined privacy. Social networks, mobile applications, IoT (Internet of Things) devices, and artificial intelligence algorithms collect vast amounts of data about their users. This information is not only used to improve services but also for commercial purposes and surveillance.

The problem lies in the fact that people are often unaware of the extent of the data being collected or the implications this may have. Many times, they accept terms and conditions without reading them, thus relinquishing control over their personal information. Large technology corporations, such as Google, Facebook, or Amazon, use this information to create detailed user profiles, raising concerns about how this information is used, who has access to it, and for what purposes.

In this scenario, those with the financial and technological power to protect their privacy — through measures such as encrypted communications, VPNs, or even by paying for ad-free premium services — enjoy higher levels of privacy than those who lack access to these resources. This raises the troubling question of whether privacy is becoming a privilege reserved for the technological and economic elite.

## The inequality in digital privacy

The accessibility of advanced privacy tools creates a divide between ordinary citizens and those with more resources. People with high levels of technological knowledge can configure their devices and applications to minimise data collection, but for the average person, this capability is limited. Often, privacy is sacrificed for convenience or for access to "free" services that, in reality, trade personal data as currency.

A clear example of this is search engines and social networks. Companies like Google and Facebook offer free services to users but monetise these services by collecting vast amounts of data about their online behaviour to sell targeted advertising.

To avoid this, a user may choose paid services that promise greater privacy protection, such as non-tracking search engines or encrypted communication platforms. However, not everyone has the financial means or the knowledge to make this transition.

Furthermore, in many developing countries, access to technology is already limited, along with the options for protecting privacy. In these areas, the technological infrastructure is often not designed to safeguard users' rights, and governmental or corporate surveillance is more common, exacerbating the privacy gap.

### Privacy and state surveillance

Another aspect that complicates the debate is the increasing surveillance by governments. In the name of national security and combating terrorism, many states have implemented mass surveillance programmes that, although designed to protect citizens, also expose them to intrusions into their private lives. State surveillance is often justified by the need to protect society, but it can become a tool of control when used abusively.

The issue here is that the ability to resist state surveillance is also determined by resources. Those who can afford technologies that make tracking more difficult, such as end-to-end encryption or decentralised networks, may maintain a higher level of privacy than those who rely on services provided by governments or corporations that cooperate with surveillance programmes.

### Right or privilege?

In theory, privacy is and must be an inalienable human right. However, in practice, there are significant barriers that prevent everyone from enjoying this right on equal terms. Access to tools and resources that protect privacy is unevenly distributed, which turns privacy into a privilege for those who have the means to safeguard it.

This reality presents a critical challenge for modern societies: if privacy is indeed a right, then governments, businesses, and civil society actors must work together to ensure that everyone has access to the tools and knowledge necessary to protect their personal data. This includes not only strong legal frameworks but also education and accessible resources that empower individuals to take control of their digital privacy.

Ultimately, privacy should not be a privilege but a right accessible to all, regardless of their economic, geographical, or technological circumstances. Only then can we ensure that privacy remains a fundamental pillar of our individual freedoms in the digital world.

**Francisco Javier García Lorente**
Project Manager

# Two sides of the same coin: incidents and advances in digital security

Cyberchronicle by Leire Cubo Arce

**Recently, the world has witnessed several significant cyber incidents that have highlighted the fragility of digital infrastructures and the need for robust security measures. These events range from attacks on well-known companies to important advancements in cybersecurity.**

One of the most notable incidents was the cyberattack on **MoneyGram**, which took place at the end of September. This security breach compromised sensitive customer information, including names, Social Security numbers, and bank account details. The company decided to disable systems to contain the breach, resulting in service disruptions that lasted for up to a week.

Also, at the end of September, several Wi-Fi access points in train stations across the United Kingdom were targeted in a DDoS attack that redirected users to inappropriate content, highlighting vulnerabilities in public infrastructure.

One of the most significant incidents in October was the attack on the largest water supplier in the United States, **American Water**, which experienced a service disruption, although it has been confirmed that the water supply was not compromised. Nevertheless, investigations into potential data leaks are ongoing, and details about the nature of the attack that caused the incident remain unclear. This attack adds to a troubling trend of threats aimed at critical infrastructures.

Russian state media faced significant cyberattacks that disrupted their operations, exposing vulnerabilities within the infrastructure of state-controlled media. Meanwhile, in France, a hospital operator in Nantes suffered a cyberattack that caused operational disruptions. To date, details regarding potential data leaks have not been clarified.

Another notable attack targeted **Casio**, the famous Japanese electronics manufacturer. A ransomware attack impacted its operations in Tokyo, although specific details regarding possible data breaches were not disclosed.

In India, a malware attack affected governmental systems in Uttarakhand, raising concerns about cybersecurity measures within state institutions. Additionally, significant ports in Belgium faced disruptions due to a DDoS attack, highlighting the vulnerability of critical infrastructure to cybercriminals.

In a broader context, **T-Mobile** reached an agreement with the FCC to pay $15.75 million in response to several security breaches that exposed data of millions of customers, committing to invest in improving its cybersecurity systems.

**Kaspersky** became embroiled in controversy for automatically replacing its antivirus software with UltraAV, raising concerns among users, although this was part of an effort to protect Windows users following its exit from the market.

In another realm, **Cryptex**, a cryptocurrency exchange, was sanctioned for processing funds from criminal cyber activities, underscoring the growing focus of regulators on cybersecurity.

Moreover, the recent arrest of four individuals linked to the **LockBit** ransomware group demonstrates international cooperation in the fight against cybercrime, which could be a significant step towards dismantling these malicious organisations.

Recent advancements in 3D design tools, such as those presented by **Meta**, highlight the increasing need to address the cybersecurity challenges that accompany these innovations. With the democratisation of platforms that facilitate the creation of digital content, the risk of cyberattacks that can manipulate models or introduce malware into virtual environments rises.

As attacks become more sophisticated, it is crucial for organisations to strengthen their security measures and maintain constant vigilance against potential breaches. Investment in cybersecurity technology and ongoing education are essential steps to protect both businesses and their users.

Despite these incidents, not all news in the realm of cybersecurity is negative. In October 2024, several companies announced significant technological advancements. **CrowdStrike** launched Charlotte AI, an AI-powered assistant that promises to enhance the productivity of security analysts by automating threat detection and response.

Meanwhile, **Fortinet** introduced FortiAI, a tool designed to accelerate incident analysis, enabling organisations to interpret security events and generate useful insights more efficiently.

Additionally, **Palo Alto Networks** continues to innovate with its Cortex XSIAM platform, which utilises advanced AI technologies to create a fully autonomous security operations experience, improving the detection and remediation of complex threats.

**SentinelOne** also joined the forefront of cybersecurity with its Singularity Unity platform, which enhances threat-hunting capabilities, allowing security teams to manage larger volumes of attacks with greater accuracy.

These advancements in AI, encryption, and authentication underscore the ongoing efforts to strengthen digital defences against an increasingly sophisticated threat landscape. Cybersecurity is not merely a concern for the technology sector; it impacts all industries and services.

**Leire Cubo Arce**
Cybersecurity Consultant

# Privacy by design and cybersecurity

Article by Fernando del Valle Rodríguez

**In the era of digitalisation, privacy cannot be considered a separate element from cybersecurity. Users increasingly rely on digital services to manage their personal data, while cyber threats continue to evolve with the aim of exploiting this information. Therefore, integrating privacy from the design phase of any cybersecurity project is essential not only to protect users but also to comply with increasingly stringent regulations.**

## Differences and interdependence

Although privacy and cybersecurity are closely related, it is essential to understand that they are not the same. Cybersecurity focuses on protecting systems, networks, and data against cyberattacks or accidental damage, ensuring the confidentiality, integrity, availability, authenticity, and traceability of information. On the other hand, privacy centres on the proper management and protection of personal data, ensuring that it is handled in accordance with individuals' rights.

However, both disciplines are interdependent. Poor protection of privacy can lead to security breaches, and vice versa. For example, a cyberattack on a database containing unencrypted personal information could expose sensitive data that is subsequently used for fraud or sold in illegal markets. Similarly, mismanagement of privacy can facilitate attacks such as phishing. Therefore, it is crucial to design cybersecurity measures that also protect privacy.

## The concept of "Privacy by Design"

The Privacy by Design approach involves integrating data protection measures from the outset of developing a system or project, including those related to cybersecurity. This proactive approach seeks to ensure that privacy is not an added consideration at the end but an integral part of the project lifecycle, from conception to implementation.

In addition to facilitating compliance with regulations such as the General Data Protection Regulation (GDPR), Privacy by Design prevents unnecessary risks. Failing to implement this from the outset can lead to delays, costly changes, and penalties due to non-compliance, as well as loss of customer trust and reputational damage. Therefore, proactive design in data protection is not only a matter of legal compliance but also a key strategy for long-term success.

## Benefits of integrating privacy into cybersecurity projects

Incorporating privacy into cybersecurity projects yields significant benefits:

- **Regulatory compliance**: Data protection regulations, such as the General Data Protection Regulation (GDPR) or the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), require organisations to adequately protect personal data. Integrating privacy from the beginning facilitates compliance not only with these regulations but also with others such as NIS2, DORA, ENS, or international standards like ISO 27001 and ISO 29100.

- **Risk reduction**: Privacy violations not only entail economic losses but also severely damage companies' reputations, which can be difficult to repair. By integrating privacy from the outset, both technical and legal risks are minimised.

- **Customer trust**: Users are increasingly aware of the value of their personal information and prefer services that prioritise the protection of their privacy. Companies that do so will generate greater trust among their customers, which can in turn translate into a key competitive advantage.

## Strategies for incorporating privacy into cybersecurity projects

To ensure the effective implementation of privacy in cybersecurity projects, it is essential to adopt the following practices:

- **Client and project needs analysis**: The first step is to analyse the project's needs regarding privacy. If personal data is not being handled, it may not be necessary to implement specific measures, but if it is being managed, privacy must be prioritised from the outset.

- **Risk analysis and impact assessment**: Determining potential risks to privacy in the early phases allows for the establishment of timely corrective measures, minimising risks and ensuring that data processing is conducted securely.

- **Data minimisation**: Collecting only the strictly necessary data and setting clear limits on its retention is fundamental for reducing security risks and ensuring compliance with regulations.

- **Incorporation of users' data protection rights**: Including measures that guarantee users' rights, such as access, rectification, and deletion of their data, avoids costly modifications and ensures regulatory compliance.

The key to these strategies is the collaboration between the cybersecurity and privacy areas, ensuring smooth communication and a comprehensive approach to data protection.

## Challenges in Integrating Privacy into Cybersecurity

Despite the benefits, integrating privacy into cybersecurity projects presents certain challenges:

- **Initial costs**: Implementing advanced privacy measures from the early phases can increase costs in terms of time, resources, and technology. However, these costs are minor compared to the expenses arising from penalties or forced modifications in the later stages of the project.
- **Technical complexity**: Some measures, such as anonymisation or strong encryption, can be difficult to implement in complex systems, especially in legacy infrastructures. However, these measures are crucial to prevent breaches that may lead to financial and reputational damage.
- **Lack of training**: Many cybersecurity teams lack adequate training in personal data protection. Including privacy experts, such as those from the Legal & Compliance department, is essential to ensure that regulations and best practices are properly integrated.

## Future trends: Automation and new regulations

The future of privacy and cybersecurity lies in automation. Tools based on artificial intelligence will enable more proactive and efficient detection and mitigation of privacy threats. Furthermore, regulations such as the Artificial Intelligence Regulation will require organisations to adapt swiftly, particularly concerning their interconnection with personal data protection laws and standards.

The integration of privacy into cybersecurity projects is now more than just a good practice; it is a necessity. Adopting the Privacy by Design approach ensures the protection of both security and data privacy, facilitating regulatory compliance and gaining customer trust.

Companies that prioritise data protection will be better prepared to face the challenges of this digital era.

**Fernando del Valle Rodríguez**
Cybersecurity Consultant

# The rise of low-code/no-code platforms and security challenges: a new era of development

Trends by Damián Pardiñas Rodríguez

**In recent years, Low-Code/No-Code (LCNC) platforms have revolutionised the way companies develop applications. Tools like Retool, Microsoft's Power Platform, and other similar offerings enable individuals with little to no programming experience to create functional applications quickly and efficiently.**

This approach has democratised development, making it easier to create technological solutions within organisations and accelerating innovation. However, despite its many benefits, LCNC platforms present significant security challenges, a crucial aspect that cannot be overlooked.

## A surge driven by the need for agility

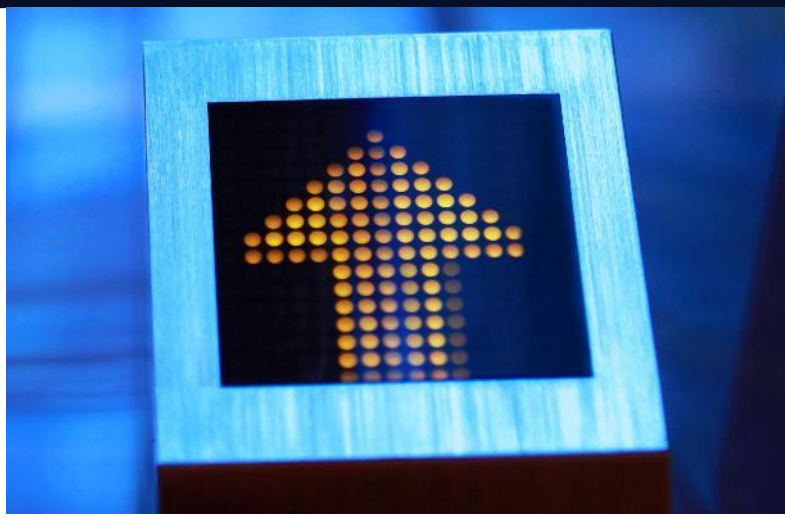
The increasing demand for customised applications in sectors such as commerce, education, and healthcare has driven the widespread adoption of LCNC platforms. These tools enable organisations to respond quickly to market needs without relying exclusively on specialised development teams. A good example is Retool, a low-code development platform that allows companies to create internal interfaces easily, leveraging existing data and systems. Similarly, Microsoft Power Platform provides organisations with the capability to build applications, automate workflows, and analyse data with minimal involvement from traditional developers.

The main appeal of LCNC platforms lies in their simplicity and ability to reduce time to market. However, this simplicity also brings new security risks. While the platforms facilitate development, much of the security of the code does not rest with the application developers but with the platforms themselves, presenting a series of important challenges.

## The impact of security on LCNC platforms: OWASP and the Top Ten

The rapid adoption of LCNC platforms has caught the attention of the Open Web Application Security Project (OWASP), an organisation known for its work in identifying security vulnerabilities in applications.

OWASP recently released a Top Ten specifically dedicated to the security risks of low-code/no-code platforms, highlighting the main challenges faced by organisations that rely on these technologies.



The top three vulnerabilities on this list are:

1. **Account impersonation**: The ease of delegating privileges within LCNC platforms often leads to scenarios where credentials and permissions are not managed properly, allowing attackers to impersonate identities and access critical resources.
2. **Authorisation misuse**: Incorrectly configured permissions and roles within LCNC applications are one of the most common risks, enabling unauthorised users to access data or functions that should be restricted.
3. **Data leakage and unexpected consequences**: Often, LCNC platforms allow data manipulation without adequate security controls, which can result in the unintentional exposure of sensitive information or the creation of unforeseen situations that compromise the integrity of the system.

This new OWASP list reflects how traditional security risks have evolved in the context of LCNC platforms, where authentication and authorisation issues, typically managed by experienced developers, now need to be controlled by the platform itself.

## Analysis tools for LCNC: new allies

In light of these risks, new tools are emerging that allow companies to monitor and analyse applications created on LCNC platforms. These tools are specifically designed to detect vulnerabilities, analyse configurations, and validate that applications meet the organisation's security standards. An example of such solutions includes LCNC security monitoring services that audit applications in real-time, detecting issues before they can be exploited by malicious actors.

Examples of these solutions include **Zenity** and **Valence Security**, which assist in auditing and managing the security of applications developed on LCNC platforms.

These tools are critical in an environment where the security of the code largely falls on the platform itself rather than on the developers. This represents a fundamental difference from traditional development, where developers had direct control over every line of code and could directly implement robust security practices.

In the case of LCNC platforms, most organisations rely almost entirely on the security mechanisms built into the platform, increasing the need to trust providers with a solid track record in security.

## New horizons and cyber responsibility

Low-code/no-code platforms have opened new opportunities to accelerate innovation and improve efficiency in application development. However, this approach has significant implications for security. The risks identified by OWASP highlight that, while LCNC platforms are powerful, they can also be vulnerable if not managed properly.

The responsibility for security, which traditionally rested with developers, is now largely transferred to the platform, underscoring the importance of selecting secure tools and continuously monitoring applications to mitigate potential risks.

Organisations must be aware of these challenges and adopt a proactive approach to protecting their applications, integrating specialised tools and ensuring that the LCNC platforms used meet the highest security standards.

**Damián Pardiñas Rodríguez**
Cybersecurity Expert Analyst

# Vulnerabilities

## Critical Vulnerability in Cisco Small Business

**Date:** October 2, 2024
**CVE:** CVE-2024-20518

**CVSS: 9.1**

**CRITICAL**

## Description

The critical vulnerability CVE-2024-20518, which affects various models of Cisco Small Business, could allow an attacker to execute arbitrary code and even cause a DoS attack.

These vulnerabilities are based on the administration interface of the Cisco Small Business routers, and through them, the attacker could even execute this code remotely.

Cisco has stated that there will be no updates for these models as they are beyond their maintenance and support period.

## Solution

Although the manufacturer will not release any security patches to address these vulnerabilities, they have provided the following recommendations to prevent exploitation.

- Disable remote management of the device; this would ensure that these devices can only be accessed via the LAN network and not externally.
- Block access to ports 443 and 60443; this would require the creation of network traffic rules for these blocks.

Further information on these mitigations can be found in the "References" section.

## Affected products

The vulnerability affects the following versions:

- RV042 Dual WAN VPN RoutersRV042G Dual Gigabit WAN VPN RoutersRV320 Dual Gigabit WAN VPN RoutersRV325 Dual Gigabit WAN VPN Routers

## References

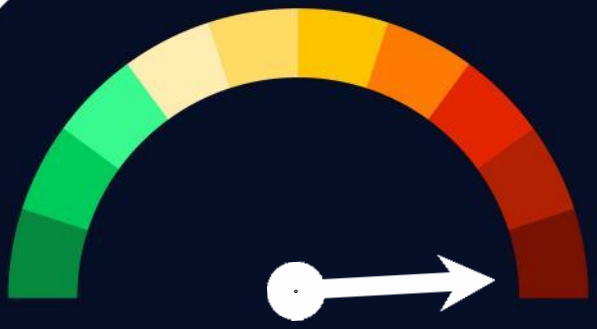
- incibe.com
- sec.cloudapps.cisco.com
- cvedetails.com

# Vulnerabilities

## Vulnerability in Siemens SINEC Security Monitor

**Date:** October 8, 2024
**CVE:** CVE-2024-47553 and 1 more



**CVSS: 9.9**

**CRITICAL**

## Description

The manufacturer Siemens has disclosed several vulnerabilities affecting its product, SINEC Security Monitor, with two of them being of critical severity:

- CVE-2024-47553: Due to a flaw in the "ssmtl-client" command input, an authenticated remote attacker with limited privileges could execute arbitrary code with root permissions.
- CVE-2024-47562: During the execution of the "sstml-client" command, there are management errors in special elements, which could allow commands to be executed with privileged users in the underlying operating system.

## Solution

To address these vulnerabilities, Siemens recommends that affected users update to version 4.9.0 or later.

Additionally, as an extra security measure, Siemens suggests that users ensure strong network access protection and advises them to rely on their own policies when configuring their environments.

## Affected products

The two aforementioned vulnerabilities affect the SINEC Security Monitor product, specifically in all versions prior to 4.9.0.

## References

- tenable.com
- siemens.com
- incibe.es



TLP:WHITE

# Microsoft October Security Patches

**Date:** October 8, 2024
**CVE:** CVE-2024-43468 and 116 more

**Critical**

## Description

Microsoft has released its monthly security update, addressing 117 vulnerabilities: 3 of them critical, 110 important, 3 moderate, and 1 low. The most critical vulnerabilities are:

- CVE-2024-43468: This is the most critical vulnerability. It has been detected in Microsoft Configuration Manager and would allow an unauthenticated attacker to execute commands remotely on the server.
- CVE-2024-38124: This is a privilege escalation vulnerability in Windows Netlogon that could allow an attacker to gain unauthorised access to system resources.

## Affected products

The October security update includes patches for the following resources, among others:

- Windows 10 - Versions 21H2, 22H2
- Windows Server 2022
- Windows 11 - Version 24H2
- Windows Server 2008
- Windows Server 2008

The complete list of affected products can be found at the following link: microsoft.com

## Solution

It is recommended to apply the October 2024 security patches from Microsoft as soon as possible.

## References

- microsoft.com
- news.sophos.com

# Security updates for vulnerabilities in GitLab

**Date:** October 9, 2024
**CVE:** CVE-2024-9164 y 7 más

**Critical**

## Description

Veeam has released a new bulletin with security updates addressing 8 vulnerabilities, including critical and high-severity issues, in its GitLab Community Edition (CE) and Enterprise Edition (EE) products.

Among the corrected vulnerabilities is the critical vulnerability CVE-2024-9164 (with a score of 9.6). This vulnerability affects GitLab EE and would allow an attacker to execute pipelines and impersonate a legitimate user to modify any branch of the repository.

These affected pipelines are automated processes that perform tasks such as compiling, testing, and deploying code, typically reserved for users with appropriate permissions.

## Affected products

The vulnerabilities published in the bulletin affect the following products (along with their corresponding versions):

- GitLab Community Edition (CE):
  - Versions prior to 17.4.2.
  - Versions prior to 17.3.5.
  - Versions prior to 17.2.9.
- Enterprise Edition (EE):
  - Versions prior to 17.4.2.
  - Versions prior to 17.3.5.
  - Versions prior to 17.2.9.

## Solution

It is strongly recommended that all installations running an affected version be updated as soon as possible in accordance with the GitLab security bulletin.

## References

- about.gitlab.com
- bleepingcomputer.com
- incibe.es

# Events

### Benelux Cyber Summit
*5 November*

The Benelux Cyber Summit is an annual event that brings together IT and cybersecurity leaders from across Europe to discuss the latest trends and technologies in cybersecurity. The event includes case studies, panel discussions, and networking sessions, focusing on topics such as the protection of critical infrastructures, security automation, and the use of artificial intelligence to detect threats. It also addresses regional regulations such as the GDPR and the NIS2 Directive, highlighting the importance of collaboration between the public and private sectors to combat cybercrime.

**Link**

### XXVI International Information Security Conference
*14 November*

ISMS Forum Spain organises the International Information Security Conferences annually, which serve as a meeting point for discussion and debate among representatives of all stakeholders in the sector. The International Conferences gather top national and international speakers to address the most current and relevant topics in Information Security. All of this takes place in an environment that fosters professional relationships and knowledge exchange.

**Link**

### Cybersecurity & Identification 2024 (CISO CTO WORLD)
*21 November*

The Cybersecurity & Identification event, which will take place on 21 November 2024 at the Ilunion Atrium Hotel in Madrid, focuses on the integration of cybersecurity and identity management. The day will address topics such as the impact of artificial intelligence on cybersecurity, challenges in identity management, and the protection of personal data. Global and local regulations will also be discussed, along with how new security solutions can be implemented in cloud systems.

**Link**

### XVII STIC CCN-CERT Conferences
*26-28 November*

Madrid will host the XVIII STIC CCN-CERT Conferences and the VI ESPDEF-CERT Cyber Defence Conferences, organised by the National Cryptological Centre (CNI) and the Joint Cyber Command (MCCE). This event, in collaboration with RootedCON, will bring together cybersecurity experts to discuss threats, new technologies, and active cyber defence. Practical workshops and conferences will be held in six thematic rooms, covering topics ranging from forensic analysis to blockchain, with participation from leading technology companies and international organisations.

**Link**

# Resources

### ➢ CylancePROTECT: Artificial Intelligence and Machine Learning

CylancePROTECT is a tool that aims to leverage machine learning techniques for real-time malware detection and prevention. Unlike traditional antivirus software or other known antivirus applications that rely on signatures, CylancePROTECT operates by identifying attacks based on the behaviour exhibited by unknown threats.

**Link**

### ➢ Zero Trust Security

The Zero Trust security approach posits that no access request is trusted by default, which translates to verifying every access attempt on the network. This concept is rapidly becoming the most sought-after enterprise network defence strategy, as it mitigates the risk of security breaches by ensuring that only authorised users and devices can access critical resources.

**Link**

### ➢ Apolo

Apolo is a SaaS tool that focuses on automating daily cybersecurity tasks and regulatory compliance. It promises to identify vulnerabilities and even has the capability to train employees who are new to cybersecurity. The comprehensive perspective of the solution ensures that the security of organisations and their stakeholders is maintained at a high level while meeting regulations in a cost-effective manner.

**Link**

### ➢ Proofpoint

The system has recently enhanced its phishing detection and blocking capabilities using cutting-edge technologies, enabling a quicker response to threats. The all-in-one platform prevents organisations from suffering numerous targeted attacks, ensuring secure and reliable communication within the corporate environment.

**Link**

### ➢ NIS2 Directive

The NIS2 Directive is a European regulation that establishes stricter cybersecurity requirements for organisations. This means that many companies are implementing new tools and measures to comply with the regulations, thereby strengthening their security posture and reducing the risk of cyber incidents.

**Link**

### ➢ Cyber Resilience Legislation

The proposed Cyber Resilience Act strengthens cybersecurity requirements for digital products, which has increased the development of tools that comply with the mentioned laws. This legislation aims to enhance the ability of organisations to withstand and recover from cyberattacks, in order to promote a secure and trustworthy digital environment.

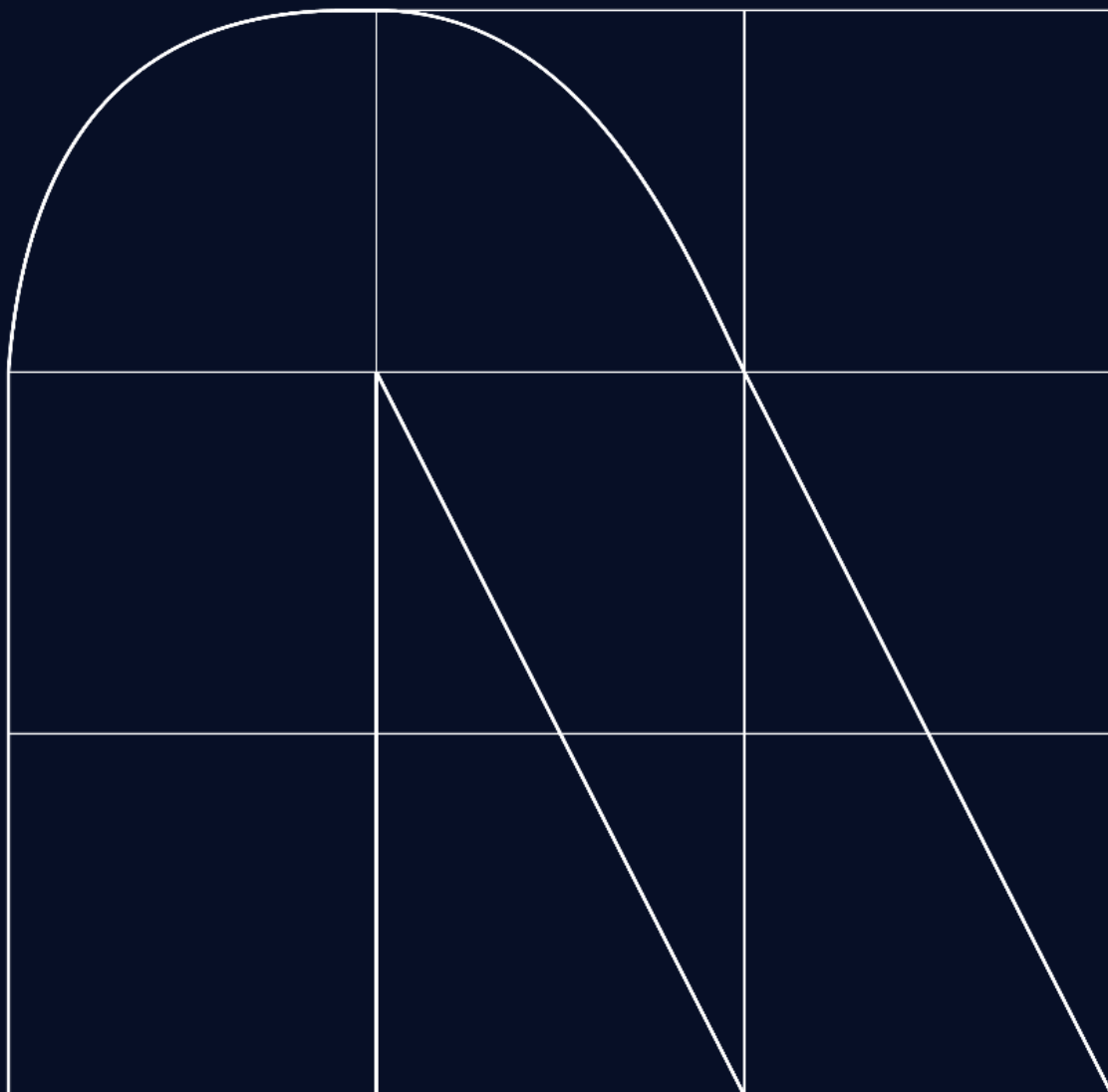
**Link**

### ➢ OSSEC

OSSEC focuses on the Host Intrusion Detection System (HIDS), which performs intrusion detection at the host level, log analysis, integrity checking, and rootkit detection. It is an open-source application that provides adequate software protection alongside all open-source vulnerabilities when configured properly. Specifically, they reported the log monitoring API and detected that the Offense API did not need to be included, leading to the disabling of the editing functionality for both APIs.

**Link**

**Subscribe to RADAR**



**Powered by the cybersecurity NTT DATA team**

es.nttdata.com