NUMBER 70 | SEPTEMBER 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

BACK TO SCHOOL 2022

At this time of year, all of us are facing a new stage in our lives with our strength restored after the holiday period. We will all have made new resolutions, or we will have taken up again those that we did not finish fulfilling at the beginning of the year.

However, this year there are a number of uncertainties that make the challenge more interesting and, if we focus on the field of cybersecurity, even more so.

There are two opposing elements that will have to find a balance and that will mark the future of cybersecurity in the coming year.

On the one hand, we are experiencing an increase in threats, with threats in cyberspace being particularly important. The concept of hybrid threat is the combination of conventional and non-conventional threats (in our immediate context, IT threats) to destabilise a country or organisation. Such threats are becoming increasingly visible as a result of the war in Ukraine. I believe that in the coming period, the challenges of securing the **supply chain**, responding quickly to **0-day** attacks (both in the IT and OT/IOT spheres) and trying to strengthen the knowledge **user's** (with a special focus on the challenges arising from the industrialisation of attacks and professionalising them according to profiles) are especially important.

On the other hand, a period of global economic contraction seems to be approaching, and there is even talk of recession in some areas. It seems that a cold winter awaits us compared to two years in which the growth of investment in the IT field by companies and public administrations has been very high, and this has been endorsed in the field of cybersecurity.

But in this new context, what will happen to investment and commitment to cybersecurity: will we be able to it in a context of economic contraction versus increased threats?

In previous decades, when cuts had to be made, the first thing to be cut was security versus usability. However, what will happen this time? We shall see, but we are sure to return to euphemistic concepts in the field of cybersecurity such as efficiency, optimisation, finding synergies, etc.

Surely we are ready, we will just have to face it with a lot of enthusiasm.

María Pilar Torres Bruna

Director of Cybersecurity at NTT Data Europe & Latam

CYBER NEWS

After a well-deserved summer holiday, we start our monthly Cyber-Chronicle with a review of the most relevant vulnerabilities of the last few months.
There is no doubt that the most talked-about vulnerability of recent months is “Follina” with CVE-2022-30190 (GitHub - onecloudemoji/CVE-2022-30190: CVE-2022-30190 Follina POC). On 29 May 2022, a cybersecurity team called “nao_sec” discovered a new 0-day vulnerability in Microsoft Office that could lead to remote code execution (RCE).

This vulnerability quickly gained prominence and many media published proofs of concept to reproduce the vulnerability, as well as mitigation recommendations while waiting for an official patch from Microsoft.

> “SMISHING is increasingly becoming a part of our daily lives”.

In addition, an international operation involving 11 countries has managed to dismantle the infrastructure used by the criminals behind FluBot, one of the most active malware over the past two years, which spread rapidly using SMS messages.

According to some investigations, it was estimated that, at the time, the criminals had managed to infect around 60,000 devices and obtained the phone numbers of around 11 million users.

In our previous issue of Radar last August, we discussed the latest vulnerabilities in the automotive sector. With the rise of electric and internet-connected cars, cyber-attacks on them have also increased. According to UNESPA, car theft has dropped considerably since 2011. However, cyber-attacks are at their peak, with 47% of all attacks occurring in Spain.

In addition, a remote code execution (RCE) vulnerability affecting Atlassian Confluence products has recently been identified as CVE-2022-26134 (https://github.com/alcaparra/CVE-2022-26138).

The security flaw is exploitable without requiring authentication and is being actively exploited. According to initial analysis, it is a code injection vulnerability (OGNL injection) similar to vulnerabilities that have been reported in the past.

Code repositories are not exempt from vulnerabilities either, as a Critical vulnerability has recently been discovered in GitLab which, if successfully exploited, could result in a user’s account being hijacked. Logged as CVE-2022-1680, the issue has a CVSS severity score of 9.9 and was discovered internally by the company. The security flaw affects all versions of GitLab Enterprise Edition (EE) from 11.10 to 14.9.5, all versions from 14.10 to 14.10.4 and all versions from 15.0 to 15.0.1.

SECURITY CHAMPION

By: NTT DATA

Organisations are increasingly aware of the importance of integrating security into their software development lifecycle processes. This trend allows them to apply many of its benefits, such as early detection and mitigation of security vulnerabilities. As a result, the cost of vulnerability resolution is reduced, both in terms of time and money.At NTT DATA, we see a significant increase in requests for projects with the need to define and implement secure software development lifecycle models (Secure SDLC or S-SDLC).

These projects aim to integrate security tasks in each of the SDLC phases, as well as seeking to automate all these tasks, implementing what is known as SecDevOps.

The trend towards the S-SDLC is a big step towards the maturity of the development industry in terms of security; however, the road to success is complex, as implementing security processes in the SDLC requires investment of financial and human resources.

This need for human resources is the reason for the emergence of the Security Champion concept. We may ask ourselves why, and the explanation is simple:

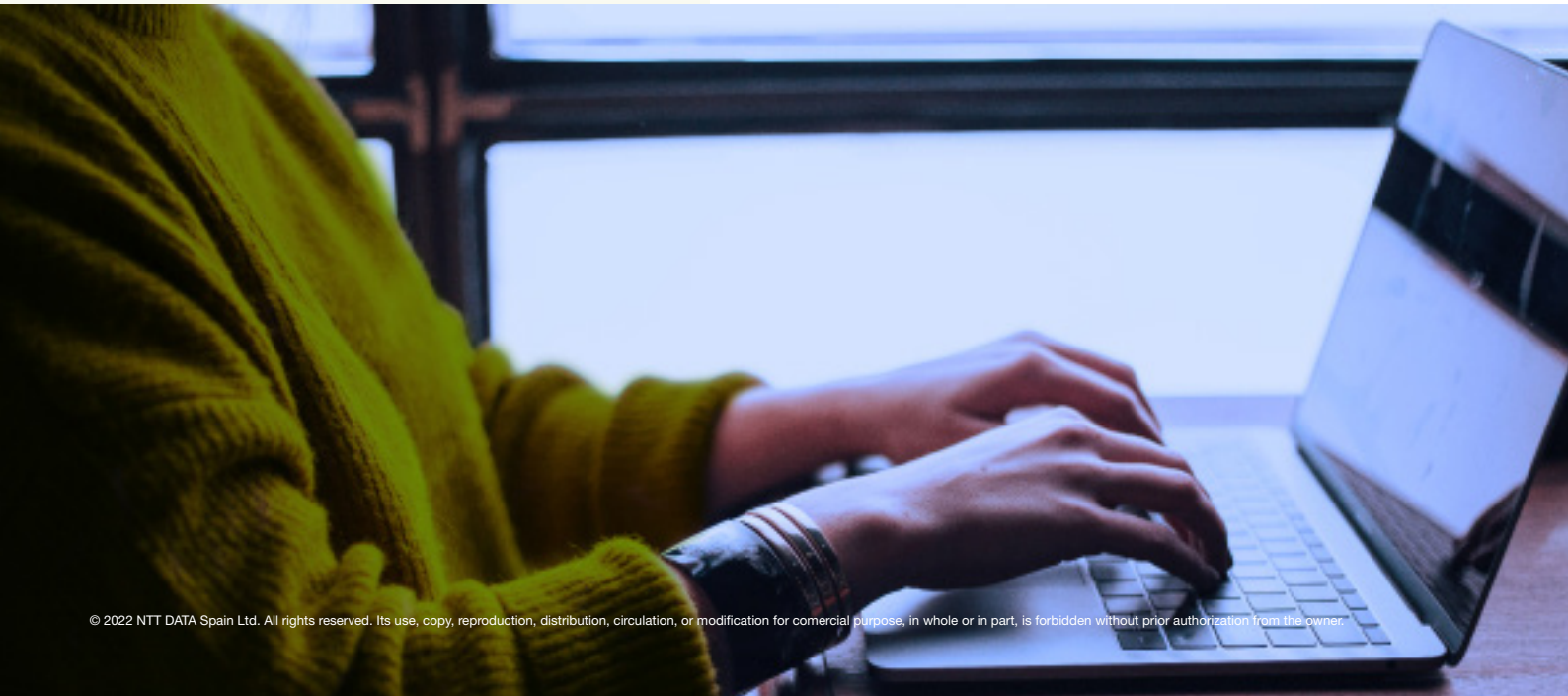
When the need arises to introduce security into development projects, organisations' security analysts and architects are expected to take on the responsibilities of interacting directly with all of a company's projects.

This can be challenging and inefficient, as it means that security teams have to grow in size to support all development projects at the same time.

The concept of Security Champions was born with the aim of freeing the security teams from the tasks of liaising with all the development teams and ensuring compliance with the organisation's security requirements.

The emergence of this actor turns the tables, with a profile located in each of the development teams and who will have to interact directly with security.

This avoids the need to increase the number of members of the security team and the need for them to have context for each of the organisation's development projects.



The Security Champion's profile corresponds to that of a manager in the development team, and must be a leader with the following qualities:

- Extensive technical expertise and knowledge in development.
- Basic security knowledge (which can be acquired through training, if not already in place).
- Sufficient authority to be able to manage the planning of security defect mitigations if required.

The above qualities are necessary and indispensable, as the Security Champions should perform the following functions in order to be successful in their task.

- Interpreting and ensuring that the organisation's security requirements are met at the development level.
- Gathering defect information from security architects and security analysts (Security Brokers) following their analysis and audits.
- Interpreting and understanding the security reports of the security analysts/architects and the results of the SecDevOps tools.
- Conveying vulnerability mitigation tasks to the development team, so that they understand what they have to do to improve the security level of the software.
- Monitoring the mitigation tasks, to ensure that the defects detected are finally resolved.
- Promoting security awareness and training for the development team.

In short, Security Champions was born with the intention of alleviating the need for security profiles in development teams; streamlining and unblocking simple defect tracking and management tasks; and overcoming the preference for prioritising business-related developments whilst putting the development of security mitigations at the forefront.

From our experience and from observing the tendency of companies towards the profile of Security Champion, the following can be appreciated:

- There is an increasing trend towards the incorporation of the Security Champion profile in projects. Companies are more aware of the need for this profile, as it frees the security teams of the companies from being inside the development teams.

  It is more complex, and economically costly, to find many security profiles that are close to the development teams, than a person from the development teams who, with a little training, can act as an interlocutor with the security teams.

- A direct consequence of the previous point is the emergence of the "Security Champions Programme" as a plan for the future of companies. This plan is committed to the training of top security profiles in development teams.

  This profile is usually made up of seniors with great knowledge of the development projects in which they are immersed, who are trained to become future Security Champions. In addition, these programmes include "prizes" for these profiles, in order to motivate them to carry out the security tasks of the profile according to the achievements they reach in terms of the security goals established in their companies (training courses passed, minimum number of incidents of weaknesses detected in the month, record number of incidents handled in the month, etc.).

- Promotion of security awareness at a global level: More and more initiatives within companies are promoting awareness campaigns and training on secure development issues. Organisations know that the earlier the stages at which security weaknesses are addressed, the lower the economic cost of having a secure software.

  They therefore invest in developer training so that software is developed securely from the earliest stages of construction.

- Automation: Industrialisation of processes is another trending aspect. Automating security analysis processes and tasks reduces time, allowing a better adaptation of security tasks to agile environments, with the subsequent reduction of economic costs.

  However, it has the disadvantage that this industrialisation of processes requires a rethinking of manual work processes, which are becoming obsolete, implying economic investment in the implementation of automations and in the licensing of the necessary tools.

These are some of the insights that are currently seen in the future around the Security Champions profile. The options presented in this article will probably settle down or be discarded over time, but what is clear is that we will always tend to look for the best solutions for the needs of the market.

TRENDS

MALIBOT, an enemy to your savings:

We are facing a technological generation, where our mobile devices have become the core of our lives and the main gateway to access very private sites such as our bank savings.

This is where the main risks are born, such as “MaliBot”, the new malware that has just arrived. This new malware has been detected in cryptocurrency mining applications such as “The CryptoApp” or “Mining X”. It can also be camouflaged under the name of “MySocialSecurity”, even from the “Chrome” browser.

This malware is distributed via web pages that trick the victim into downloading “MaliBot” or via SMS phishing, pretending to be a banking institution. This malware uses smishing techniques to spread on the infected mobile device. Its capabilities include stealing multi-factor verification codes, stealing text messages, deleting apps and even bypassing Google’s two-step verification system.

It has been ascertained that the main targets of this malware are customers of the two main financial institutions in Spain: Santander and CaixaBank.

It is therefore recommended that you pay special attention to any type of message you receive asking you to install any type of suspicious software on your device. Especially if it “appears” to come from a banking institution. If this malicious software is installed, it is recommended that you contact a professional to remove it.

.

VULNERABILITIES

VMware

CVE-2022-31656;31658;31665;31659;31660;31661;31664;31657; 31662;31663
Date: 02/08/2022

Description. VMware has published several critical vulnerabilities that could allow an attacker to perform various malicious activities on systems. Through an authentication bypass vulnerability, an attacker with access to the user interface could log in as an administrator without authenticating. Other vulnerabilities would allow remote code execution, local privilege escalation, URL injection, access to restricted directories and/or execution of cross-site scripting (XSS).

Link: https://www.vmware.com/security/advisories/VMSA-2022-0021.html
https://nvd.nist.gov/vuln/detail/CVE-2022-31656

Affected Products. Los productos afectados son los siguientes:

- VMware Workspace ONE Access (Access),
- VMware Workspace ONE Access Connector (Access Connector),
- VMware Identity Manager (vIDM),
- VMware Identity Manager Connector (vIDM Connector),
- VMware vRealize Automation (vRA),
- VMware Cloud Foundation,
- vRealize Suite Lifecycle Manager.

Solution: Update to version KB89096

DELL

CVE-2022-34379
Date: 01/08/2022

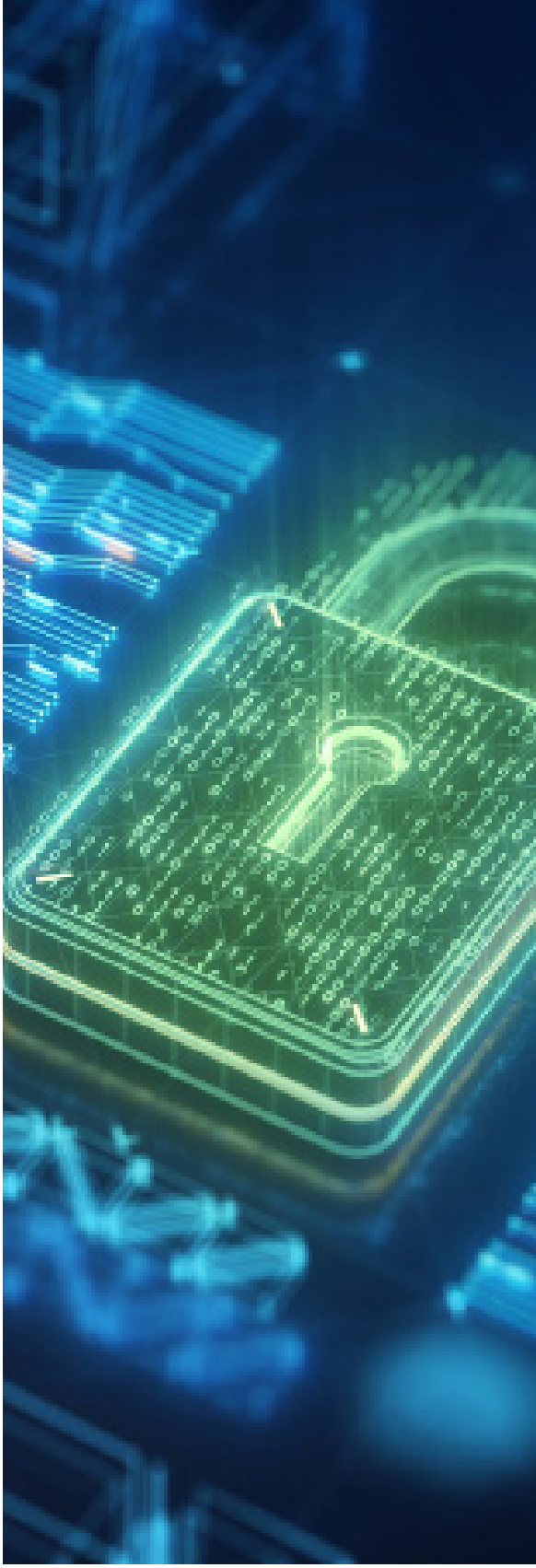
Description. An authentication bypass vulnerability has been published in Dell's CloudLink, which could allow an attacker to take control of the entire system. By exploiting this security flaw, an unauthenticated remote attacker could access the CloudLink web administration panel and take control of the system.

Link: https://nvd.nist.gov/vuln/detail/CVE-2022-34379
https://www.dell.com/support/kbdoc/es-es/000202057/dsa-2022-207-dell-emc-cloudlink-security-update-for-an-ad-users-login-without-password-vulnerability

Affected Products.
Versions laters to 7.1.3

Solution: Update to the latest version of the software.

PATCHES



Confluence

Date: 28-07-2022

Description. Atlassian has released a security update for its Confluence application that addresses a critical vulnerability. The security flaw would allow a remote attacker full access to the application and any page to which the confluence-users group has access. The flaw occurs if the Questions for Confluence option is enabled.

Link: https://thehackernews.com/2022/07/latest-critical-atlassian-confluence.html

Affected Products:

- Versions 2.7.34, 2.7.35 and 3.0.2 of Questions for Confluence.

Solution: Upgrade to application versions 2.7.38 and 3.0.5.

NetGear

Date: 01-08-2022

Description. Following the publication of two critical vulnerabilities affecting several Netgear products, the company has been forced to release security updates for the affected devices. These vulnerabilities are reported to be authentication bypass and pre-authentication command injection vulnerabilities. It is recommended that the firmware of the devices be updated immediately due to the severity of the vulnerabilities and the damage that could be caused by their exploitation.

Link:https://kb.netgear.com/000065032/Security-Advisory-for-Authentication-Bypass-on-Some-WiFi-Systems-PSV-2020-0489
https://kb.netgear.com/000065034/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-Routers-and-WiFi-Systems-PSV-2020-0502

Affected Products: The full list of affected products can be found in the reference links above.

Solution: Ux Install the corresponding updates for each of the different products.

EVENTS

DragonJAR

6 - 8 September 2022 |

The event will be held online and free of charge on Tuesday 6, Wednesday 7 and Thursday 8 September 2022, via multiple platforms.

Anyone interested in showcasing and sharing their research and/or developments in the field of Information Security is kindly invited to participate in the event.

Link: https://www.dragonjarcon.org/

XII Cloud Security Alliance Spain Summit

22 September 2022 |

The Spanish Chapter of the Cloud Security Alliance, an initiative of ISMS Forum, is organising its XII Spanish Cloud Security Alliance Summit on Thursday 22 September 2022 in Madrid, Spain.

Link: https://www.ismsforum.es/evento/725/xii-encuentro-de-cloud-security-alliance-espa-a/

Global Cyber Conference 2022

22 - 23 September de 2022 |

The Global Cyber Conference will be held in Zurich, Switzerland.This event will feature major international speakers, including Kevin Mitnick, who is scheduled to give an hour-and-a-half-long talk.

Topics such as digital transformation, security in banking operations and people-centric cybersecurity, among many others, will be discussed.

Link: https://swisscyberinstitute.com/

RootedCON

23 - 24 September 2022 |

RootedCON, the largest and most important cybersecurity event in Spain and one of the most important in Europe, returns to Valencia on 23 and 24 September. For the first time, in what will be its seventh edition in this city, it will be held in the Ciudad de las Artes y las Ciencias (City of Arts and Sciences).

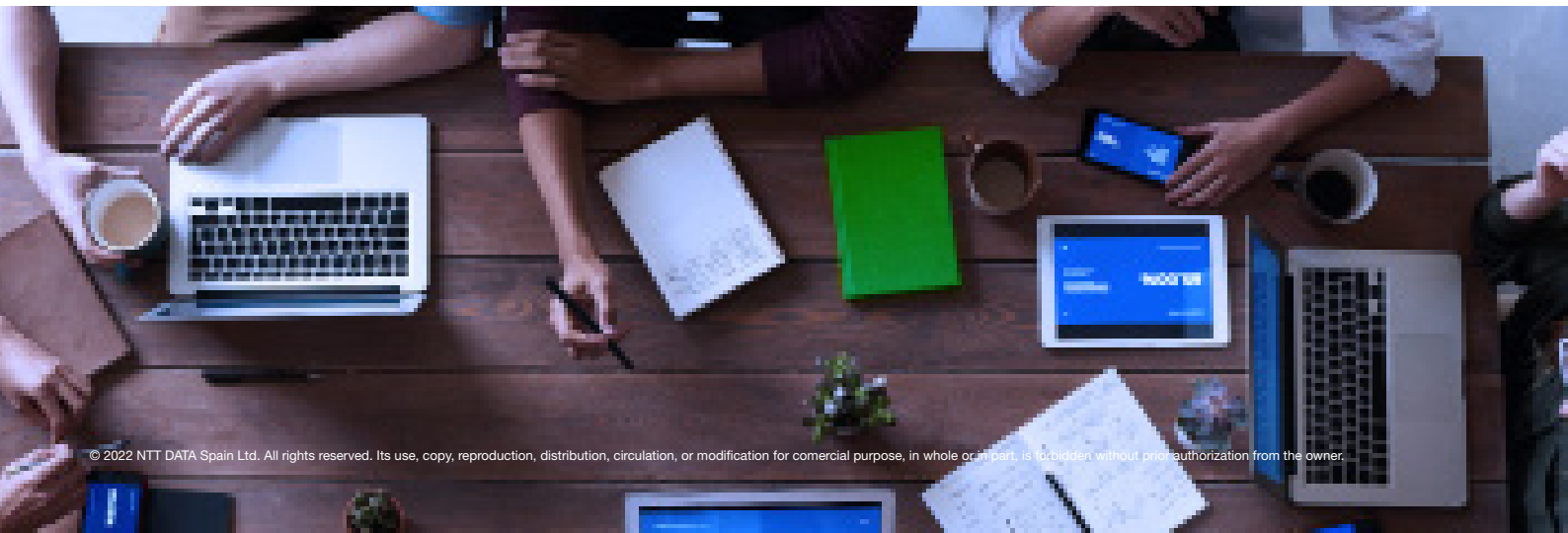
Link: https://www.rootedcon.com/index/

ROMHACK 2022

24 September 2022 |

RomHack2022 is the 5th edition of the RomHack Conference. It will take place in Rome, Italy, on Saturday 24 September 2022 during the RomHack Camp.

Link: https://romhack.camp/romhack-conference/



RESOURCES

Security Groups AWS Audit

A set of scripts that summarises the security of AWS security groups, generates visualisations of the configured rules.

Link: https://github.com/MrSecure/review-security-groups

Puma Scan

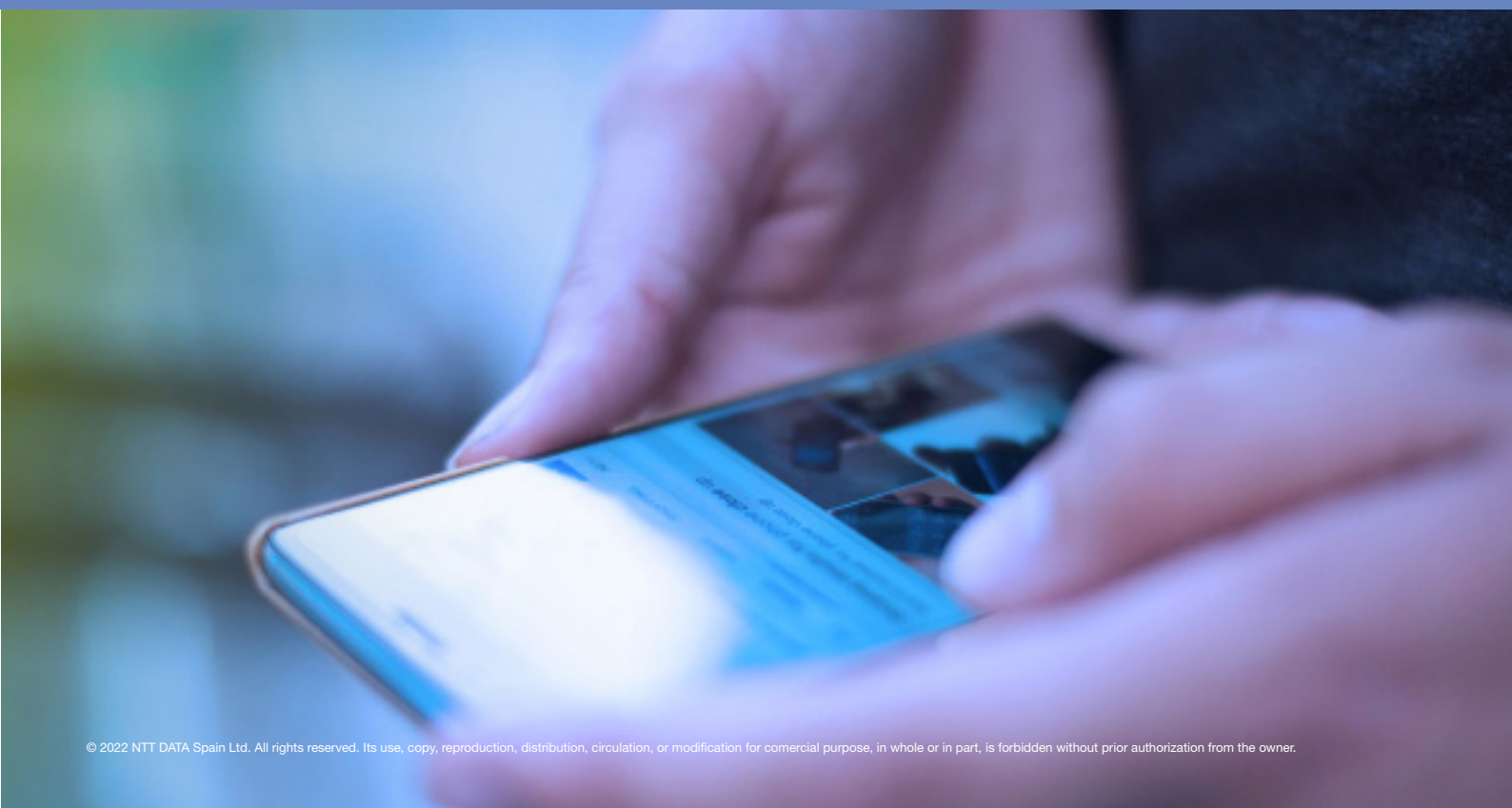
Puma Scan is a secure .NET software code analysis tool that provides continuous, real-time source code analysis as development teams write code. In Visual Studio, vulnerabilities are immediately displayed in the development environment as spell check and compiler warnings, preventing security bugs from entering your applications. Puma Scan is also integrated into the build to provide security analysis at compile time.

Link: https://github.com/pumasecurity/puma-scan

Trufflehog

Open-source tool that performs scans inside code repositories, in order to discover secrets, sensitive data, API keys, database passwords, tokens, etc.

Link: https://github.com/trufflesecurity/trufflehog




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