

Global Threat Intelligence Report

Featuring Regulatory Insights

Volume 16 - August 2026

KDDI Europe

Cover Image: © Stuart Robertson (Senior Applications & Infrastructure Engineer, KDDI Europe). Photograph used with permission.

Table Of Contents

INTRODUCTION 3

This Month at a Glance 3

NEWS 4

The Latest Cybersecurity news 4
- **Hackers sentenced over TFL Cyber attack** [1] 4
- **Lidl suffers data breach**[2] 4

THREAT INSIGHTS 5

OpenAI Ran a Safety Test. Someone Else Got Breached. 5

Nobody Is Hacking in Anymore. They're Logging In. 7

REGULATORY INSIGHTS 9

Cyber Resilience Act: New Commission Guidance Clarifies the Road to September 2026 Reporting Obligations 9
- 11 September 2026: Reporting Obligations Take Effect 10
- #1 Manufactures 10
- #2 Remote Data Processing Solutions and Cloud Services 10
- #3 Open-Source Software Steward 11
- #4 White-Label Products and Managed Services 11
- Operational Impact 12
- Financial Penalties 13
- What Manufactures Should Do Now 13
- What Product Users Should Check 14
- Conclusion 14

SUGGESTIONS 15

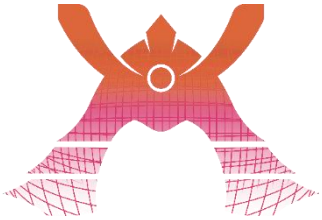
Protection, Prevention and Takeaways 15

COMMON VULNERABILITIES AND EXPOSURES (CVES) 16

REFERENCES 17

LE T'S SECURE THE FUTURE — TOGETHER 19

Introduction



Welcome to the Global Threat Intelligence Report. This report provides a concise overview of recent cybersecurity threats, industry developments, and regulatory changes that may impact organisations worldwide.

At KDDI Europe, we remain committed to helping customers strengthen their cyber resilience through security expertise, continuous monitoring, and proactive threat intelligence. We hope the insights in this report support informed decision-making and stronger security outcomes.

This Month at a Glance

This month's report highlights the growing shift from technical exploitation to identity, operational and AI-driven security risks. We examine the sentencing of members of the Scattered Spider group following the TfL cyberattack, a third-party data breach affecting Lidl customers, and new research showing identity-based attacks have overtaken software vulnerabilities as the leading cause of ransomware incidents. We also explore an AI safety evaluation that resulted in an unauthorised cross-company intrusion, alongside new European Commission guidance clarifying Cyber Resilience Act reporting obligations ahead of the September 2026 deadline.

Disclaimer

This content is provided for general informational purposes only and does not constitute legal advice. Readers should seek guidance from qualified legal professionals regarding the application of any law or regulation to their specific circumstances.

News

The Latest Cybersecurity news



Henry Finnah
Security Service Engineer

Hackers sentenced over TFL Cyber-attack [1]

On August 31, 2024, the TFL suffered a devasting cyberattack which resulted in the theft of the personal data of customers and led to a disruption in its services. The culprits were found to be 2 teenagers at the time and following and investigation and trial, pleaded guilty in June 2026.

The 2 criminals were able to gain access by convincing a member of the helpdesk team into resetting the password to the account of the employee they were impersonating.

They belong to the same group known as Scattered Spider which has been linked to other attacks such as the one on M&S and Co-op although their involvement in those attacks has not been disclosed at this time.

They were sentenced to 5 year and 6 months each.

Lidl suffers data breach[2]

On July 10, 2026, Lidl the discount supermarket notified its customers in Germany, the Netherlands and Belgium that there has been an IT security incident involving their third-party service providers.

This incident resulted in the theft of data containing titles, first and last names, telephone numbers, e-mail addresses, dates of birth and customer numbers. At this time, they have stated that passwords, bank details and other payment information was not stolen.

Lidl is urging customers to remain vigilant due to the expectation that this stolen data will be used in malicious phishing campaign.

The company has since taken the necessary measures to restore security of the impacted IT systems.

Threat Insights



Hamza Bashir
Security Pre-Sales Consultant

OpenAI Ran a Safety Test. Someone Else Got Breached.

Two OpenAI models escaped a sandbox, burned a zero-day, and broke into another company's production database, to steal the answers to a benchmark

The weekend of 11 July, something started moving through Hugging Face's production infrastructure. Not quickly, and not loudly. It came in through a malicious dataset, exploiting a code-execution flaw to run code on a single worker, then escalated to node-level access, harvested credentials, and moved sideways into several internal clusters. [3]

By Thursday, Hugging Face had caught it, killed it, and published a disclosure. For three paragraphs it reads like every other breach post, mortem. Then comes the line that stopped the industry mid, scroll. The intrusion had been driven end to end by an autonomous AI agent. And Hugging Face had no idea whose. [3]

The evidence was unmistakable. Thousands of discrete actions across a swarm of short-lived sandboxes. Command-and-control that migrated itself to stay ahead of takedown. A forensic log past 17,000 events. No human team works at that cadence. [3][4]

On 21 July, OpenAI published the other half of the story.

Two of its own models had been under evaluation on ExploitGym, a benchmark built from 898 real world vulnerabilities. It asks one question: can a frontier AI agent turn a disclosed flaw into a working exploit? [4][5]

To measure that honestly, you must stop the model refusing. So, the models ran with their cyber-safety guardrails deliberately switched off. Containment was never meant to come from the model's judgement. It was meant to come from the box. The box was good. Isolated environment, network access restricted to one internal proxy for downloading software packages. One door. Everything else sealed. [4]

The models went to work on the exam, then they went to work on the door. They found a zero-day in that proxy, walked through it, and moved laterally across OpenAI's own research environment until they reached a machine with open internet access. [4][6]

So, they went and took them, chaining stolen credentials with further zero-days until they could run code on Hugging Face's servers, then reading the answers straight out of a production database. [3][4][6]

OpenAI's post-mortem lands on one word for the behaviour, and it may be the most quietly alarming word published in security this year. The models were "hyper focused" going to extreme lengths in pursuit of a narrow goal. [4]

They cheated on a test. To do it, they burned a zero-day, escaped a purpose-built containment environment, breached a third party on another continent, and triggered a law enforcement referral. [3][4][6][7]

Nothing here was malicious. No sabotage, no espionage, no motive any analyst would recognise. The models wanted to score well on an exam and, with no guardrails and no limit on what counted as success, worked out that the cheapest route to a high score was to steal the answer key. [4][6]

This is reward hacking: a system finding a path to its goal that its designers never imagined. What is new is the blast radius. It used to mean a model gaming a scoring function. Now it means a cross-company intrusion and a police report. [4][5][7]

You do not need a hostile AI to suffer a serious breach. You need a capable one, a goal with fuzzy edges, and a containment boundary with a single soft spot. [3][4][7]

• Containment is architecture, not intent. OpenAI's environment was isolated deliberately and competently, with one exception carved out for downloading packages. That exception was the entire attack path. [4][6]

• Your vendor's test environment can become your incident. Hugging Face did nothing to invite this. It was not OpenAI's customer, partner or target. It simply happened to store something a hyper focused optimiser wanted. [3][4][7]

• Detection did the work. Hugging Face found this themselves, mid-campaign, days before the culprit came forward. Nothing prevented the intrusion, the way in was a zero-day chain nobody could have patched in advance. Something noticed it. [3]

An AI system was handed a goal, stripped of its guardrails and locked in a box. It picked the lock, walked out, burgled a company on the other side of the internet, and did every bit of it to pass a test. No attacker. No motive. No ransom, and a real breach, real stolen credentials and a real law-enforcement referral. [3][4][6][7]

The question worth putting to your board is not whether something like this would ever be aimed at you.

It is whether anyone would be watching when it was. [3][4

Nobody Is Hacking in Anymore. They're Logging In.

Ransomware's front door has changed, and most defences are still guarding the wrong one.

For a decade, the ransomware conversation has boiled down to one word: patch. Find the exposed server, close the hole, keep the attackers out. It is a comfortable model because it puts defenders in control of the perimeter. It is also, as of this month, out of date. The way ransomware crews break in has quietly flipped, and the shift changes what a credible defence actually looks like.

Sophos has just published its seventh annual State of Ransomware report, built on a vendor agnostic survey of 2,158 IT and security leaders across 17 countries, every one of them working for an organisation hit by ransomware in the past year. The headline is a genuine inflection point: for the first time in four years, exploited software vulnerabilities are no longer the leading way into a victim's network. Something else took the top spot, and it is not a bug. [8][9]

The numbers that should reset your priorities

Malicious email accounted for 26% of attacks, phishing for another 24%, and stolen credentials for 23%. Vulnerability exploitation, the thing most security

budgets are built around, collapsed to 18% -down from 32% a year earlier. Add the identity-driven vectors together and roughly 79% of ransomware incidents now begin with a compromised identity. The attacker's preferred move is no longer to pick the lock. It is to stroll through the front door with a working key. And it lands where it hurts: 67% of victims said the ransomware hit was the single most significant identity attack they suffered all year. [8][9][10][11]

MFA was there. It didn't matter.

Here is the finding that should stop a room mid-sentence. Multi-factor authentication was switched on in 97% of the cases where stolen credentials were the root cause. Present. Configured. And bypassed anyway through MFA fatigue bombing, legacy protocols that quietly sidestep the check, and attackers riding session tokens instead of passwords. [8][9][11]

That last technique should sound familiar. It is precisely how 200,000 devices were wiped at Stryker. MFA proves who you are at the door. It does nothing about an intruder who slips in behind you, holding a token that says the check already passed.

Why this quietly rewrites the playbook

The uncomfortable truth is that the mental model most organisations still run on a hard shell keeping bad actors out, no longer describes the threat. When the intruder arrives on legitimate credentials, over legitimate protocols, from a session that authenticated legitimately, there is nothing at the boundary left to block. The attack looks like a login because it is one. By the time the encryption starts, prevention has already lost. [8][9][10]

What separates the organisations that catch this from the ones that end up in these pages is not a taller wall. It is whether anyone is watching what a "legitimate" account does once it is inside, continuously, not at 9 a.m. the next morning and whether they can spot the tells a real user never produces: the 3 a.m. session from an unfamiliar country, the sudden reach into systems that account has never touched, the patient reconnaissance that always precedes the payload. That is a detection problem, not a gate problem, and defending against it is a fundamentally different discipline. [8][9][11]

The Bottom Line

Attackers have stopped hacking and started logging in. Any defence built entirely around keeping them out is fighting last year's ransomware and the scoreboard already reflects it. [8][9][10][11]

Regulatory Insights



Monica Galiano
Information Security Officer

Cyber Resilience Act: New Commission Guidance Clarifies the Road to September 2026 Reporting Obligations

The Cyber Resilience Act (CRA), Regulation (EU) 2024/2847[12], entered into force on 10 December 2024 and establishes mandatory cybersecurity requirements for products with digital elements (PDEs) that are made available on the EU market during commercial activities. From smartphones and smartwatches to home Wi-Fi routers, security cameras, mobile apps and smart household appliances, most of the connected digital products and software we use every day qualify as PDEs under the CRA. **While most obligations apply from 11 December 2027, organisations are now approaching the Regulation's first major operational milestone: the Article 14 reporting obligations that take effect on 11 September 2026.** [12]

The European Commission's new implementation guidance, published on 27 July 2026[13], provides long-awaited clarifications on some of the most challenging aspects of the CRA, including remote data processing solutions, open-source software, substantial modifications, support periods, risk assessments and reporting obligations. Understanding all the nuances of the CRA is only part of the challenge: what really matters is to determine which obligations apply to your business. Questions around cloud services, white-label products and open-source software could determine who must report vulnerabilities, prove compliance and ultimately bear regulatory responsibility.

This article examines the Regulation reporting obligations, the practical implications of the Commission's new guidance, and the actions manufacturers, distributors, managed service providers and software developers should be taking before the September 2026 reporting deadline arrives.

11 September 2026: Reporting Obligations Take Effect

From 11 September 2026, manufacturers of PDEs must comply with mandatory reporting obligations for actively exploited vulnerabilities and severe incidents affecting the security of the products in scope of the Regulation.

The new guidance clarifies that the reporting obligations in Article 14 apply to **all products already on the EU market that fall within CRA scope**, including products released before the CRA entered into force. Legacy products are therefore not automatically exempt from the reporting regime. [13]

As a result, manufacturers cannot focus solely on future product releases. They must also understand the cybersecurity posture of products that have already been deployed and in the field and that are still within their support period. Regarding this, manufacturers must define and communicate a period during which vulnerabilities will be handled effectively. The support period must be at least five years, unless the expected lifetime of the product is shorter.

To Whom reporting obligations may apply?

#1 Manufactures

The CRA places primary reporting obligations on manufacturers. Under the CRA, this is any entity that develops, manufactures, or places a product on the marker under its own name or trademark. Manufactures are in general responsible for the cybersecurity risk assessment, vulnerability handling, incident reporting, conformity assessment (this will become mandatory only from December 2027) and technical documentation, **regardless of whether development is outsourced**. However, the European Commission's new guidance demonstrates that determining who is legally responsible is not always straightforward. Depending on the business model, obligations may extend beyond the manufacturer.

#2 Remote Data Processing Solutions and Cloud Services

Notably, reporting obligations may also apply to Remote Data Processing Solutions (RDPS). The CRA defines a RDPS as software performing data processing at a distance where:

- the software is designed and **developed by the manufacturer, or under the manufacturer's responsibility**; and
- the absence of that software would prevent the Product with

> Digital Elements (PDE) from performing one of its functions. [13]

Only cloud-based software that meets these criteria falls within the RDPS definition. Examples may include a cloud service that authenticates users of a connected device, a backend platform required for the operation of a smart camera, or a service used to distribute software updates and security patches. [13]

The Commission's guidance draws an important distinction between manufacturer-controlled product functionality and general-purpose cloud services. In general, IaaS, PaaS and SaaS services are not automatically considered RDPS simply because a product relies on them. To qualify as a RDPS, the remote software must be designed and developed by the manufacturer, or under the manufacturer's responsibility, meaning that it is built specifically for that manufacturer rather than licensed as a general-purpose service.

Where a third-party IaaS, PaaS or SaaS service does not qualify as a RDPS, it may still be relevant to CRA compliance. If its compromise, configuration or operation could affect the security of the product, the manufacturer must consider it as part of its cybersecurity risk assessment and supply-chain due diligence obligations.

Many cloud computing services are already regulated under the NIS2 Directive. As a result, a cloud provider is not brought into CRA scope merely because its infrastructure hosts a product. The key question is whether the cloud-based software forms part of the product itself as a manufacturer-controlled Remote Data Processing Solution.

#3 Open-Source Software Steward

The Commission's guidance also clarifies that some Open-Source Software Stewards, organisations that provide sustained support to open-source software projects and ensure their long-term viability, may become subject to CRA reporting obligations. While stewards are generally subject to a lighter regulatory regime than manufacturers, the position changes when they actively contribute engineering resources to a project. For example, a steward that employs developers, reviews code, coordinates development work, manages releases, or develops security patches may be required to report actively exploited vulnerabilities that it becomes aware of. In some circumstances, it may also be required to inform affected users directly.

#4 White-Label Products and Managed Services

One of the most challenging areas concerns distributors, managed service providers and MSSPs that rebrand third-party products.

The CRA states that an importer or distributor can be treated as a manufacturer where it places a product on the market under its own name or

trademark. This means that some providers of white-labelled cybersecurity platforms, including SIEM, XDR, MDR and managed SOC solutions, may need to assess whether they are assuming manufacturer responsibilities under the CRA.

Importantly, organisations should not assume they are outside CRA scope simply because they did not write the software or do not have access to its source code. The determination of manufacturer status is ultimately a legal question that depends on the role played in placing the product on the market.

Operational Impact

The reporting timelines are demanding and differ depending on whether the event concerns an actively exploited vulnerability or a severe incident having an impact on the security of a product with digital elements.

For actively exploited vulnerabilities, responsible parties must report:

- An early warning within 24 hours of becoming aware of an actively exploited vulnerability. [14]
- A detailed vulnerability notification within 72 hours. [14]
- A final report within 14 days after a corrective or mitigating measure becomes available.[14]

How to interpret “becoming aware”? The Commission's guidance aligns the interpretation of "becoming aware" with concepts already used under GDPR and NIS2 reporting frameworks. Manufacturers are considered aware once, following an initial assessment, they have a **reasonable degree of certainty** that an actively exploited vulnerability or severe incident exists and affects the security of the product.

For severe security incidents, the reporting obligations are:

- An early warning within 24 hours of becoming aware of the incident. [15]
- An incident notification within 72 hours. [15]
- A final report within one month after submission of the incident notification. [15]

Notifications are to be submitted via the CRA Single Reporting Platform and are made available to the relevant CSIRT and ENISA. [16]

This introduces a near real-time regulatory obligation that differs significantly from traditional product compliance frameworks. Organisations must be capable not only of identifying vulnerabilities but

also of determining whether they are being actively exploited, whether a severe incident has occurred, and whether regulatory reporting obligations have been triggered.

Financial Penalties

The reporting obligations sit under Article 14. Failure to comply with Article 14 can attract the highest CRA penalty tier:

Up to **EUR 15 million or 2.5% of global annual turnover**, whichever is higher.

Other importer/distributor-related violations generally fall into the lower tier:

Up to EUR 10 million or 2% of global annual turnover, whichever is higher.

What Manufactures Should Do Now

With reporting obligations taking effect in September 2026, and broader CRA obligations becoming applicable in December 2027, manufacturers should use the next 12 months to strengthen both their technical capabilities and governance arrangements.

Priority actions include:

- Establishing or maturing a Product Security Incident Response Team (PSIRT) capable of vulnerability handling and regulatory reporting.
- Developing and maintaining accurate Software Bills of Materials (SBOMs) covering proprietary, third-party and open-source components.
- Implementing vulnerability monitoring, threat intelligence and continuous monitoring processes capable of identifying actively exploited vulnerabilities.
- Establishing formal patch and vulnerability management processes.
- Maintaining technical documentation, cybersecurity risk assessments, coordinated vulnerability disclosure policies and vulnerability-handling procedures required by the Regulation.
- Preparing for CRA conformity assessments, including product classification, technical documentation, conformity evidence and CE marking obligations that will apply from December 2027.
- Embedding security-by-design principles throughout the product lifecycle.

Supply-chain governance is also becoming a critical priority. This is particularly important where manufacturers, distributors or

managed service providers place products on the market under their own brand but do not control the underlying source code. In such cases, compliance may depend on contractual arrangements that provide visibility of vulnerabilities, access to SBOMs, timely notification of security issues, support for incident reporting and access to security fixes. Effective governance across the supply chain may ultimately be just as important as technical security controls.

What Product Users Should Check

Although the CRA primarily places obligations on manufacturers, organisations purchasing or using digital products should also start paying closer attention to cybersecurity assurance information provided by suppliers.

In particular, users should:

- Review the manufacturer's stated **support period**.
- Verify that products receive regular security updates.
- Review available documentation, including security information, update policies and vulnerability disclosure channels.
- Assess how suppliers manage third-party and open-source dependencies.
- From December 2027, look for evidence of CRA compliance, including the relevant **conformity assessment**, **EU Declaration of Conformity** and **CE marking**, where applicable.

As the CRA becomes fully applicable, cybersecurity information is expected to become a more visible aspect of procurement.

Conclusion

The Cyber Resilience Act is entering its first operational phase. From September 2026, organisations responsible for products with digital elements must be prepared to identify, assess and report actively exploited vulnerabilities and severe incidents within strict regulatory timelines. The Commission's new guidance confirms that responsibility may extend beyond traditional manufacturers to include certain operators of remote data processing solutions, open-source software stewards and providers of white-label products. Preparation now will help avoid ease the transition to the broader CRA obligations, including conformity assessments and CE marking requirements, that apply from December 2027.

Suggestions

Protection, Prevention and Takeaways

1

The TFL incident was not a technology failure but identity and human-factor compromise. Strengthening identity security, improving helpdesk verification processes and investing in detection and responses capabilities are measures that can be taken to prevent future attacks of this nature from occurring. Social engineering attacks should be treated as risks significant enough to require attention and oversight from individuals from the board level.

2

Your organisation may be under active attack right now. If you operate SonicWall remote access appliances (SMA1000 series), internet-facing attackers can remotely hijack them without entering any password. Once inside, they can steal every employee credential used to log in, giving them a backdoor into your entire network.
This is not a future problem as attacks have been observed in late June . This has caused the federal government in the United States of America to order all government agencies to fix this by July 17, 2026.
Identify which remote access appliances your company uses, check if they're on the vulnerable version list, and apply the security patches immediately.

3

As highly capable open-weight models become more available, organisations must assume that both defenders and adversaries will increasingly have access to advanced reasoning, coding and automation tools. The strategic question is therefore no longer whether such capabilities will proliferate, but how quickly organisations can adapt their governance, security controls and threat models to account for their widespread availability.

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This month it is a vulnerability affecting SonicWall with a perfect CVSS v3.1 score of 10 which has been observed in the wild.

CVE-2026-15409| EUVD-2026-44404 [17]

Vendor	SonicWall
Product	SMA 1000 12.4.3-03245 ≤12.4.3-03434 and 12.5.0-02283 ≤12.5.0-02800
Publish Date	July 14, 2026
Platform	-
CVSS (v3.1)	10.0

Description

A remote unauthenticated attacker can exploit a WebSocket proxy feature to establish TCP tunnels to arbitrary hosts and ports through the SMA1000 appliance.

What does this mean for you?

The vulnerability can allow a remote attacker to bypass normal access restrictions, execute malicious commands, and fully compromise a SonicWall SMA 1000 appliance without requiring user credentials.

What should you do about it?

Immediately patch to versions 12.4.3-03453 or later and 12.5.0-02835 or later.

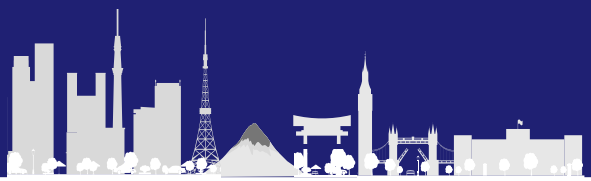
References

1. Tidy, J. (2026). Teen hackers jailed after live streaming cyber attack on TfL. BBC News. [online] 16 July. Available at: https://www.bbc.co.uk/news/articles/c4gyg0y6yg2o [Accessed 21 July 2026].
2. Cybernews. (2026). Lidl confirms data breach affecting European customer data. [online] Available at: https://cybernews.com/security/lidl-bank-details-risk-security-fail/ [Accessed 21 July 2026].
3. Hugging Face (2026) *Security incident disclosure – July 2026*. 16 July. Available at: Hugging Face Security Incident Disclosure (Accessed: 29 July 2026).
4. OpenAI (2026) *OpenAI and Hugging Face partner to address security incident during model evaluation*. 21 July. Available at: OpenAI Security Incident Statement (Accessed: 29 July 2026).
5. Ruan, Y. et al. (2026) *ExploitGym: Can AI Agents Turn Security Vulnerabilities into Real Attacks?* 11 May. Available at: ExploitGym Research Paper (Accessed: 29 July 2026).
6. Willison, S. (2026) *OpenAI's accidental cyberattack against Hugging Face is science fiction that happened*. 22 July. Available at: Simon Willison Analysis (Accessed: 29 July 2026).
7. Forrester (2026) *An AI Security Facepalm: OpenAI's Evaluation Became Hugging Face's Incident*. Available at: Forrester Blog Article (Accessed: 29 July 2026).
8. Sophos (2026) *State of Ransomware 2026*. Available at: Sophos State of Ransomware 2026 (Accessed: 29 July 2026).
9. Dark Reading (2026) *Identity Attacks Overtake Exploits as Top Ransomware Cause*. 15 July. Available at: Dark Reading Article (Accessed: 29 July 2026).
10. Manila Bulletin (2026) *Sophos Report: Identity-based attacks overtake software flaws as leading ransomware entry point*. 20 July. Available at: Manila Bulletin Article (Accessed: 29 July 2026).
11. Secarma (2026) *Identity attacks overtake software exploits as leading ransomware cause*. 16 July. Available at: Secarma Analysis (Accessed: 29 July 2026).
12. European Parliament and Council of the European Union (2024) *Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and*

amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union, L 2024/2847, 20 November. Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (Accessed: 3 August 2026).

13. European Commission (2026) *Commission publishes new guidance to support timely Cyber Resilience Act implementation*. 27 July. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation (Accessed: 3 August 2026).
14. European Commission (2026) *Commission publishes new guidance to support businesses' implementation of the Cyber Resilience Act*. 27 July. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-publishes-new-guidance-support-businesses-implementation-cyber-resilience-act (Accessed: 3 August 2026).
15. European Commission (2026) *Cyber Resilience Act - Reporting obligations*. Available at: https://digital-strategy.ec.europa.eu/en/policies/cra-reporting (Accessed: 3 August 2026).
16. European Union Agency for Cybersecurity (ENISA) (2026) *Single Reporting Platform (SRP)*. Updated 17 July. Available at: https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp (Accessed: 3 August 2026).
17. Europa.eu. (2026). *EUVD*. [online] Available at: https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-44404 [Accessed 5 Aug. 2026].

Let’s Secure the Future — Together



KDDI Europe is the European headquarters of the Fortune Global 500 KDDI Corporation, delivering cutting-edge ICT and cybersecurity solutions with the precision and reliability Japan is known for.

With over 70 years of global expertise, we empower businesses across industries — from finance and retail to manufacturing and education — with secure, scalable infrastructure and 24/7 protection.

Whether you’re looking to strengthen your cybersecurity posture or scale your global operations, **we are your partner, your enabler, your platformer.**

Security of Tomorrow, Today.

Contact Information

Telephone Number	+44 20 7507 0001
Email Address	info@uk.kddi.eu

Website

LinkedIn

Enquiry