KDDI Europe

A Year on the Frontline

GLOBAL THREAT INTELLIGENCE REPORT

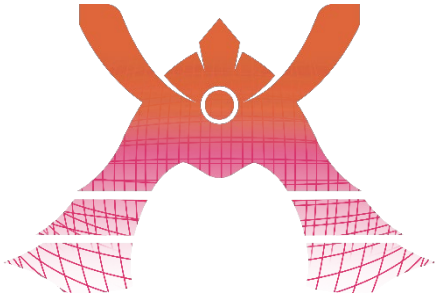
1st Anniversary Special Edition

Volume 12 - April 2026

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

Table Of Contents

Introduction



Welcome to the Threat Report. The purpose of this document is to provide an overview of the latest cybersecurity threats, trends and regulations that could impact organisations worldwide. By analysing recent incidents and emerging threats, we aim to equip our team and customers with the knowledge and insights necessary to proactively defend against potential attacks.

At KDDI Europe, our dedication to protecting our clients and their systems is unwavering. We are continuously investing in security technologies and training our staff to enhance defences and respond swiftly to any threats. We are deeply committed to ensuring that our customers are protected in accordance with the highest standards of cybersecurity.

It is our belief that our success is linked to the success of our customers' businesses. By safeguarding your operations, we aim to provide a secure environment where your business can thrive and grow. Thank you for taking the time to review this report.

News

The Latest Cybersecurity news

Henry Finnah
Security Service Engineer

OpenAI to acquire Promptfoo [1]

On 9 March 2026, OpenAI posted a press release on their website stating their acquisition of Promptfoo, a company that builds open-source tools for evaluating, securing and testing AI applications.

Promptfoo is a company founded in 2024 and is responsible for providing a service that allows developers to identify and remediates vulnerabilities in AI systems, and it is this technology that OpenAI intends to integrate into their own platform for building and operating AI coworkers.

There has been no disclosure on how much was spent on this acquisition but some unverified sources state that Promptfoo was valued at around $86 million.

Starbucks suffers data breach [2]

On 10 March 2026, Starbucks sent out a notice to customers informing them of an incident which may have impacted some of their personal information.

The notice goes on to state that Starbucks became aware of the potential unauthorised access to certain accounts on 6 February 2026 and an investigation was commenced in addition to taking containment measures. It was determined that personal information including names, social security numbers, dates of birth, financial account numbers and routing numbers may have been accessed by the unauthorised third party.

The unauthorised third-party gained access by obtaining login credentials through phishing websites impersonating the Starbucks Partner Central platform.

Threat Insights

AI Chatbots: The New Attack Vector

AI needs little introduction; it would be rare to find someone today who has no idea what it is or has never heard the term. It has been integrated into almost every major business application and social media platform. Modern AI systems, particularly Large Language Models (LLM) based inferences are embedded into major business applications and productivity suites.

Businesses are increasingly deploying this technology in the chatbots on their websites to handle customer queries in a more natural, human-like tone. Unfortunately, threat actors have also realised that, given the right set of prompts, it is possible to manipulate AI chatbots into revealing sensitive information or performing unintended, potentially harmful actions. This article will focus on organisations that are using LLMs

Despite being relatively new in mainstream deployment, AI systems have already demonstrated multiple exploitable attack surfaces. Threat actors have shown the ability to:

- **Inject hidden or adversarial prompts** to subvert model behaviour.
- **Exploit backend APIs** that the chatbot may implicitly call.
- **Trigger unintended model behaviours** by leveraging edge-case inputs, jailbreaks, or context-poisoning.
- **Pivot to backend systems and data stores** through insecure integrations or excessive permissions.

AI chatbots typically serve as a thin front-end layer for complex backend pipelines involving data ingestion, orchestration logic, third-party APIs, and privileged system components. This architecture significantly increases their attractiveness as a target. Key risk factors include:

1. They may have high privilege access.
2. They ingest data from third-party sources that could be poisoned by attackers.
3. AI security practices are not yet mature; rapid adoption has outpaced safeguards.
4. Users misplace their trust in these bots, often enough to reveal sensitive information.

In conclusion, AI is here to stay, and strong efforts need to be made to secure its use and development.

Regulatory Insights

Monica Galiano
Information Security Officer

New Frontiers for Vulnerability Scanning: How Requirements Are Evolving in the EU and the UK

Over the past month, policymakers in both the European Union and the United Kingdom have taken decisive steps to close longstanding regulatory gaps in vulnerability management — particularly around how vulnerabilities must be identified, monitored, and reported. With the EU's publication of a draft guidance for the Cyber Resilience Act (CRA) and the UK's legislative push to expand the NIS Regulations to cover critical digital supply chain enablers, vulnerability scanning has shifted from a best practice recommendation to a legal obligation.

This article explains who is now in scope, what regulators expect, and the timelines that CISOs, cloud providers, and manufacturers must prepare for.

The EU CRA and the "Remote Processing" Clarification

On 3 March 2026, the European Commission published its long-awaited draft guidance for the EU Cyber Resilience Act (CRA) [3]. This document marks a turning point for product-integrated cloud service providers (CSPs) and for companies whose products rely on "remote data processing".

The guidance confirms that the CRA applies to Products with Digital Elements (PDEs) placed on the EU market. Crucially, it clarifies that remote data processing solutions — including cloud-based components — fall within scope when they are integral to the product's functionality.

In practice, this means that if you supply a PDE for distribution or use in the EU as part of a commercial activity,

and the product relies on a cloud backend to function, then that backend is subject to the same CRA vulnerability handling obligations as the product itself.

The New Incident Reporting timeline

The CRA [4] introduces a strict reporting regime under Article 14 §§1 and 2. From the **11 September 2026**, manufacturers and in-scope cloud providers must comply with a "24h / 72h / 14-day" notification rule:

- **24 hours**: An "early warning" to the national Computer Security Incident Response Team (CSIRT) and to ENISA after becoming aware of an actively exploited vulnerability.
- **72 hours**: A detailed notification of the vulnerability.
- **14 days**: A final report once a corrective measure (patch or mitigation) is available.
- **For severe incidents**: a final report within one month from the 72 hours submission is required under NIS 2 laws.

Be aware of your business size: notably, manufacturers that qualify as microenterprises or small enterprises may not be fined for failures to meet the 24h deadline for reporting vulnerabilities and severe incidents.

A key clarification: a cloud service provider is only subject to the CRA's 24h/72h/14-day rule when its cloud service is an essential, integrated, manufacturer-controlled component of a PDE. Otherwise, the provider may fall under NIS2, but not the CRA.

Vulnerability Handling and ENISA's "Single Entry Point"

Alongside the CRA guidance, the Digital Omnibus package (updated in **mid-March 2026**) [5] has formally advanced the creation of a Single-Entry Point (SEP) managed by ENISA. This platform serves as a unified interface for reporting vulnerabilities and incidents under NIS2, the CRA, GDPR, and DORA. Adopting a "report once, share many" architecture, the SEP automatically distributes notifications to ENISA, national CSIRTs, and, where applicable, sectoral regulators and data protection authorities. De facto, this establishes a consolidated, EU-wide ecosystem for identifying, cataloguing, coordinating, and disclosing vulnerabilities, with ENISA acting as the central clearinghouse for European digital resilience.

The UK Cyber Security & Resilience (CSR) Bill

The UK is moving in parallel: as of the **5 March 2026**, following the Public Bill

Committee's latest report, the CSR Bill entered its final legislative stages [6]. This Bill significantly expands the 2018 NIS Regulations to bridge the gap between traditional infrastructure and modern digital enablers. It specifically targets:

- **Cloud Computing Services**: The Bill provides a modernised, "scalable and elastic" definition of cloud services, imposing stricter security duties on providers to prevent cascading impacts on the UK economy.
- **Managed Service Providers (MSPs)**: Often the "hidden" back door into sensitive networks, medium and large MSPs are now formally brought into the regulatory perimeter under the Information Commissioner's Office (ICO).
- **Data Centres**: Now officially classified as Critical National Infrastructure (CNI), putting them on the same legal footing as the energy and water sectors.

UK: Retirement of free Web Check service, and announcement of new Vulnerability Management Service

The NCSC announced the retirement of the free Web and Mail Check Services [7] effective **31 March 2026** citing major advances in the external attack surface management (EASM) market.

The message is clear: **Government-provided basic scans are no longer adequate.** Organisations must now procure professional-grade, continuous scanning solutions to meet their duties under the CSR Bill.

Just weeks earlier, the UK Government launched a centralised **Vulnerability Monitoring Service (VMS)** for the public sector, reporting an 84% reduction in cyber-attack fix times [8].

The VMS is powered by Detectify, an EASM solution also available through the UK Government's G-Cloud procurement framework.

Through G-Cloud, public bodies may purchase dedicated, high-frequency scanning instances beyond the standard VMS offering.

Comparing EU and UK vulnerability management requirements

Continuous perimeter monitoring is now a foundational compliance expectation across cybersecurity regulatory frameworks. Although EU and UK regulations are broadly aligned in respect to robust vulnerability and incident management practices, we highlight some differences in the approach:

Metric	EU (CRA/NIS2)	UK (CSR Bill/NCSC)
Target Entities	Manufacturers, CSPs, Software Devs	MSPs, Data Centres, Critical Suppliers
Primary Scanning Focus	Lifecycle vulnerability handling (CVD)	External Attack Surface Management (EASM)
Reporting deadline	NIS2: 24h (Early Warning) / 72h (Details) / one month after full notification CRA: 24h (Early Warning) / 72h (Details) / 14 days after corrective measure has been made available	24h (Significant) / 72h (Details)
Major Milestone	Sept 11, 2026 (CRA Reporting)	March 31, 2026 (NCSC Tool Retirement)
Regulatory Lead	ENISA / National CSIRTs	Ofcom / Information Commissioner / NCSC

Noticeably, only NIS 2 requires a full report one-month after the submission of the 72h incident notification. CRA requires notifying ENISA and relevant CSIRT also after the vulnerability has been remediated. As opposite, the UK has adopted a flexible approach where a third report is only required on a case-by-case basis.

“ You cannot secure (and report on) what you cannot see”

Conclusion: the attack surface visibility mandate

Whether you are a CSP, a data-centre operator under the UK’s CSR Bill, or a manufacturer integrating remote processing under the EU’s CRA, the legal message is clear: you cannot secure what you cannot see.

With the NCSC retiring its legacy tools on 31 March 2026 and the EU’s 24h/72h/14-day reporting regime approaching, the burden of discovery has shifted. Relying solely on a cloud provider’s “shared responsibility” statement is no longer sufficient. Regulators now expect organisations to maintain an independent, real-time audit of their exposed perimeter, including cloud-facing assets.

In this environment, a vulnerability left unmonitored for more than 24 hours is no longer just a technical oversight — it is a regulatory failure.

Column: Security Forefront

What Threats Await Us In 2026?

In this column, we share our perspective on the latest cybersecurity trends, drawing on a wide range of sources. For this edition, while referring to the report 'LAC Security Insight'[9] written by LAC[10], the one of the top cybersecurity company in Japan, we would like to forecast incident trends in 2026 and gain insights.

Hiroki Morishita
IT Security Specialist

The Shockwave of Threats Has Already Begun

The year 2026 opened with an unmistakable signal: the global cyber threat landscape is accelerating faster than at any point in the last decade.

In February 2026, the Alphav/BlackCat ransomware attack occurred, causing Change Healthcare to malfunction, disrupting healthcare payment processing across the United States, and resulting in the leakage of personal information of over 100 million people. [11]

Simultaneously, Europe experienced a broader rise in cyber-attack volume as part of a global upward trend. The region saw an 18% year-over-year increase in weekly attacks, fuelled by ransomware escalation and GenAI-driven intrusion campaigns.[12]

Threats Taking Shape in 2026 – Three Core Trends

LAC's 2025 findings in Japan identified structural weaknesses, including identity gaps, user-driven execution and exposed infrastructure. These same weaknesses were exploited globally in early 2026 as ransomware and GenAI-enabled intrusions surged across the US and Europe.

1. **Human-Layer Exploitation Accelerated by AI:** Social-engineering attacks such as ClickFix variants, Browser-in-the-Browser, and AI-generated phishing will intensify. Attackers will increasingly bypass traditional awareness-driven defences by exploiting psychological triggers and producing highly convincing, localised content.
2. **Identity & Access as Primary Attack Surfaces:** Stolen credentials will continue driving intrusions across VPNs, cloud services, and hybrid identity platforms (e.g., Entra ID). Misconfigured conditional access, weak MFA, and identity sprawl will make identity systems the most consistently targeted control layer.
3. **Infrastructure Compromise via Virtualisation & Modern Web Stacks:** Attackers will increasingly pivot through hypervisors (ESXi/vCenter) to move laterally into AD and servers. At the same time, vulnerabilities in modern web frameworks (e.g., React Server Components) will expand opportunities for direct server-segment infiltration.

Strategies That Can't Wait – Three Keys

Organisations must now reinforce identity, infrastructure, and governance frameworks to counter threats that have clearly become global in scale.

1. **Prepare for AI-Driven Threat:** Update user education for AI-powered deception, enhance detection models against AI-generated threats, and ensure global governance to mitigate regional gaps in patching discipline, SOC maturity, and cross-border data transfer limitations.
2. **Strengthen Identity & Access Governance**: Adopt phishing-resistant MFA, continuously audit conditional access policies, minimise privileged accounts, and tighten lifecycle management. Identity must be treated as the primary security perimeter.
3. **Harden Foundational Virtualisation & Supply Chains:** Monitor hypervisors with endpoint-level rigor, detect web shells and lateral-movement tools early, and reinforce supply-chain resilience—especially around SDKs, plugins, and third-party dependencies that can silently introduce compromise.

Suggestions

Protection, Prevention and Takeaways

1

Organisations need to educate their staff on the safe use of AI chatbots. It is not uncommon for employees to enter sensitive information or upload documents to publicly accessible AI services, often without even creating an account. Users must understand how to interact with AI systems safely. Each chatbot operates differently, and varying data-retention policies mean that information submitted to these platforms may be stored for long periods and potentially used to train models, improving their performance at the risk of a potential data breach.

2

For organisations that deploy their own AI chatbots, security should be considered at the very beginning of the planning process. Threat modelling should be done for the AI system, risks need to be assessed early, the architecture must be secured to implement segmentation between models, APIs and data stores and lastly by performing supply chain due diligence. These are first steps towards ensuring the eventual deployment will be secure.

3

If vulnerability management was a legal requirement tomorrow, where would your organisation stand? Is your business prepared should legislation suddenly require mechanisms for vulnerability scanning be in place. It is essential for a business to be aware of any and all vulnerabilities which may exist in its environment, not just for itself but also for the sake of its customers.

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 multiple versions of Microsoft SharePoint.

CVE-2026-20963 | EUVD-2026-2114 [13]

Vendor	Microsoft
Product	SharePoint Server 2019, Subscription Edition and Enterprise Server 2016
Publish Date	Jan 13, 2026
Platform	-
CVSS (v3.1)	8.8

Description

Deserialisation of untrusted data in Microsoft Office SharePoint allows an authorised attacker to execute code over a network.

What does this mean for you?

An attacker could compromise a server, including data theft, malware deployment, and lateral movement without user warning or interaction.

What should you do about it?

Install the 13 January 2026 security updates from Microsoft to remediate.

Thank you for reading

Thank you for reading. We hope this report has been helpful and insightful for you.

This report was created by our experts - not AI. Our team continuously studies, researches, and learns to provide our customers with the best security guidance and to deliver the latest, most meaningful insights for our audience.

At KDDI, we remain committed to delivering clear insights, reliable expertise, and meaningful value for our partners.

< Our Other Team Members>

Shintaro Takeda
Editorial Supervisor & EMEA CISO

Stuart Robertson
Photographer & Senior Applications / Infrastructure Engineer

Konoka Kawakami
Editorial Design Supervisor & Business & Marketing Manager

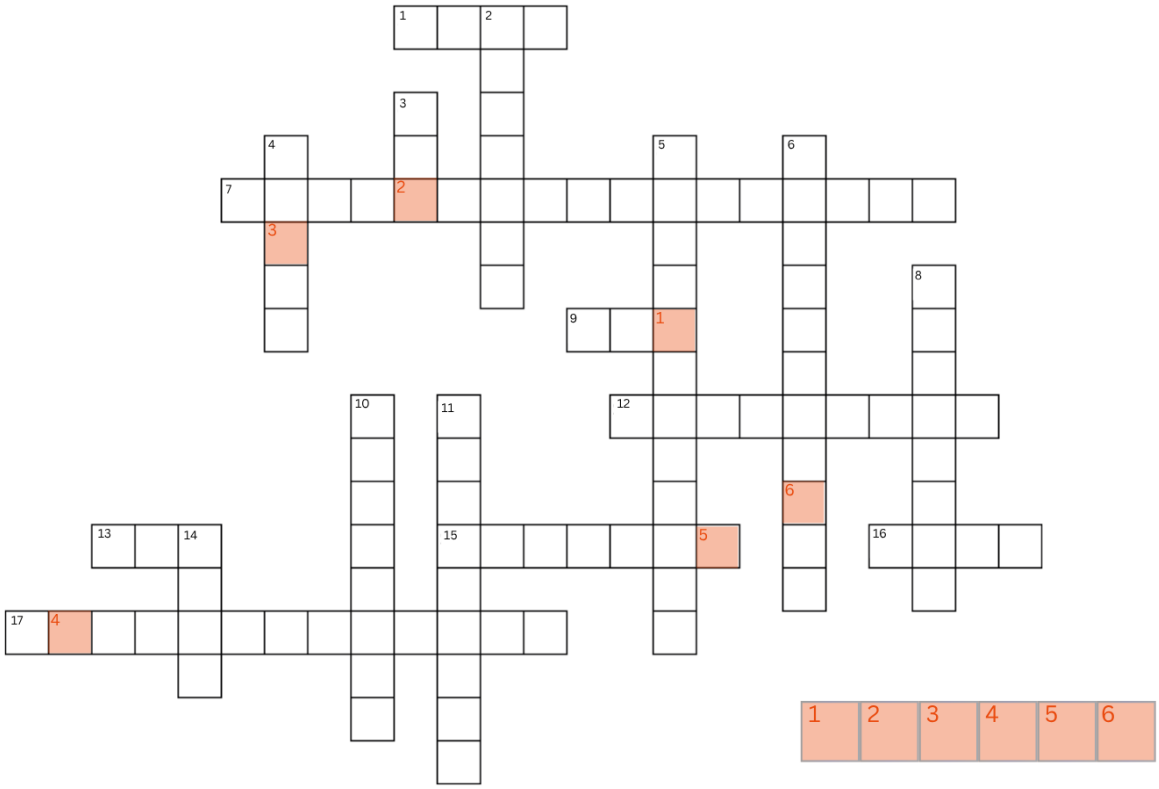
Crossword Challenge

Enjoy a moment of fun with our interactive crossword puzzle featured on next page! Within the crossword, several boxes are highlighted in Orange. The letters in those red boxes form a special keyword.

How to Participate:

1. Complete the crossword puzzle.
2. Identify the keyword formed by the orange-marked boxes.
3. Submit your answer via LinkedIn DM or email it to us with the keyword.
   Email: marketing_email@uk.kddi.eu
   LinkedIn: https://www.linkedin.com/company/kddi-europe-limited/

Prize:
The first **5 people** to submit the correct keyword will receive a **KDDI tumbler**.
Deadline: 5 May 2026 (5/5). Prizes can be sent **within the UK.**
We hope this small activity adds an enjoyable break as you explore our report!



Across

1. What EU regulation defines strict rules for collecting, storing, and processing personal data to protect individuals' privacy?
7. What technique attackers use to manipulate people into giving access?
9. What cryptographic protocol protects web traffic and forms the basis of secure HTTPS?
12. What security model uses "never trust, always verify"?
13. What type of cryptography protects against quantum computers?
15. Threat What term describes security risks coming from within an organisation?
16. What acronym refers to "Harvest Now, Decrypt Later" attacks?
17. What term describes a weakness in software or systems that attackers can exploit to gain unauthorised access?

Down

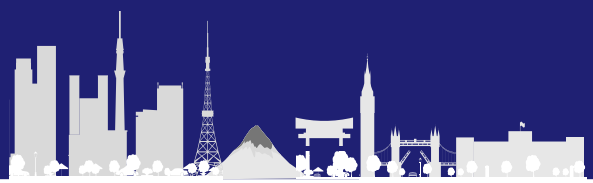
2. What authorised simulation of a real cyberattack is performed to test how well an organisation's systems can withstand intrusions?
3. What security method adds a second authentication factor?
4. Which city is KDDI group's headquarter located?
5. What malware type steals sensitive information like login data?
6. What do attackers often steal or purchase to gain direct system access?
8. What common attack tricks users into revealing credentials?
10. What essential activity prevents exploitation of vulnerabilities?
11. What tool scans systems for malicious software and helps prevent infections?
14. What continuous cybersecurity process monitors, prioritises, and manages exposure across an organisation on an ongoing basis?

Links & References

1. Openai.com. (2026). *OpenAI to acquire Promptfoo*. [online] Available at: https://openai.com/index/openai-to-acquire-promptfoo/ [Accessed 31 Mar. 2026].
2. Maine.gov. (2026). *Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches*. [online] Available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/585e41ad-c38b-407c-8ce8-1f281d570d97.html.
3. European Commission (2026) *Commission publishes for feedback draft guidance to assist companies in applying the Cyber Resilience Act | Shaping Europe's digital future*. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-publishes-feedback-draft-guidance-assist-companies-applying-cyber-resilience-act (Accessed: 31 March 2026).
4. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)* (2024) *Official Journal L, 2024/2847, 20.11.2024*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847 (Accessed: 31 March 2026).
5. European Commission (2025) *Proposal for a Regulation of the European Parliament and of the Council on the simplification of the implementation of harmonised rules on artificial intelligence, cybersecurity, and data (Digital Omnibus)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0836 (Accessed: 31 March 2026).
6. UK Parliament (2026) *Cyber Security and Resilience (Network and Information Systems) Bill*. Bill 385 2024-26 (as amended in committee). Available at: https://bills.parliament.uk/bills/4035 (Accessed: 31 March 2026).
7. National Cyber Security Centre (NCSC) (2025) *NCSC ending Web Check and Mail Check in March 2026*. Available at: https://www.ncsc.gov.uk/news/ncsc-ending-web-check-and-mail-check-march-2026 (Accessed: 31 March 2026).
8. Department for Science, Innovation and Technology (2026) *Government cuts cyber-attack fix times by 84% and launches new profession to protect*

public services. Available at: https://www.gov.uk/government/news/government-cuts-cyber-attack-fix-times-by-84-and-launches-new-profession-to-protect-public-services (Accessed: 31 March 2026).
9. LAC Co., Ltd. (2026) LAC Security Insight Vol.16 (Winter 2026), referred and translated by Hiroki Morishita, KDDI Europe Limited, Available at: https://www.lac.co.jp/lacwatch/pdf/20260226_lsi_vol15.pdf (Accessed: 30 March 2026).
10. LAC Co., Ltd. (2026) Available at: https://www.lac.co.jp/ (Accessed: 30 March 2026).
11. Cyber Security News (2026) *Top 10 Cyber Attacks of 2026.* Available at: https://cybersecuritynews.com/top-10-cyber-attacks-of-2026/ (Accessed: 30 March 2026).
12. Check Point (2026) *Global Cyber Attacks Rise in January 2026 Amid Increasing Ransomware Activity and Expanding GenAI Risks.* Available at: https://blog.checkpoint.com/research/global-cyber-attacks-rise-in-january-2026-amid-increasing-ransomware-activity-and-expanding-genai-risks/ (Accessed: 30 March 2026).
13. Europa.eu. (2026). *EUVD.* Available at: https://euvd.enisa.europa.eu/vulnerability/CVE-2026-20963 [Accessed 2 Apr. 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