KDDI Europe

Global Threat Intelligence Report

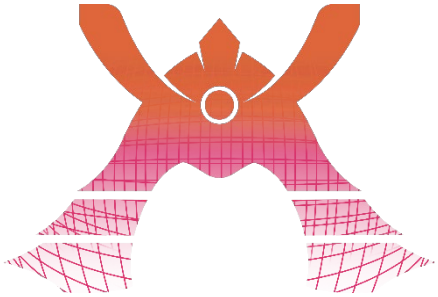
Featuring Regulatory Insights

Volume 8

December 2025

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

CrowdStrike fires “suspicious” employee [1]

CrowdStrike has announced that it fired a suspicious staff member who allegedly passed information about the company to a hacking group. The group published images showing dashboards containing links to the company’s dashboards, however CrowdStrike have maintained that their systems were never compromised and their customers can rest easy.

SitusAMC suffers data breach[2]

The financial technology company that provides services for real estate financing, including mortgage origination and servicing, with a client list including big names such as JP Morgan, Citi and Morgan Stanley, has reported that they have suffered a data breach. According to the company, on November 12th 2025, it became aware of the incident, notified law enforcement and begun investigations. It stated that both client and customer data may have been impacted but no encrypting malware was involved, more details are yet to be disclosed as this is still an ongoing investigation.

Threat Insights

What is Continuous Threat Exposure Management (CTEM)?

Continuous Threat Exposure Management (CTEM) is the continuous and repeated process of identifying, assessing, and addressing security risks associated with exposed digital assets; these assets make up an organisation's digital attack surface. Vulnerability management can be considered a subset of this process and should not be used interchangeably with CTEM.

Process

Service providers and vendors will usually have between 3 – 6 steps for the processes involved in Continuous Theat Exposure Management (CTEM) but they outline the same actions. Some providers may combine 2 or 3 actions into 1 while others will enumerate them individually. This part of the article will describe the process in much more general terms using simple language.

1. Firstly, you would want to identify which assets to require protection. Information will be collected from these assets and sent to the CTEM platform either by installing some specialised software on it or using other means.
2. Next, the Continuous Threat Exposure Management (CTEM) platform detects and assesses any risk and vulnerabilities found on the assets. Usually as part of the process, the CTEM system will assist in the prioritisation of which risks need to eliminate first by assigned scores or severity to the risks.
3. Then the process of response and recovery (remediation and mitigation) will occur. This is where the risk is eliminated, reduced or in some cases accepted by the organisation, it will depend on several factors including

the organisations appetite for risk or the nature of the asset and the service it provides.
4. Finally, the assets are continuously monitored to identify more risks and the cycle is repeated from step 1 indefinitely.

The process has been simplified but represents the procedures involved in Continuous Threat Exposure Management.

Challenges

We will look at some of the challenges involved in Continuous Threat Exposure Management.

1. Asset visibility: Asset visibility is often hindered by technical challenges such as virtual machines running on hypervisors like VMware ESXi or Microsoft Hyper-V. In these environments, host-level abstraction can make it difficult to obtain guest operating system logs and event data. Or by organisational issues like poor asset management. When monitoring tools cannot reach certain systems or when asset inventories are incomplete, critical resources may remain outside the security scope, increasing risk exposure.
2. Remediation ownership: In environments with multiple vendors managing interconnected assets, coordinating remediation can be complex. Actions by one provider may impact another system, requiring careful scheduling to avoid service disruptions. This can increase the time required for remediation and timing is crucial in cybersecurity.
3. Lack of manpower: Limited staff and competing priorities can delay remediation efforts. Manual patching processes may add further strain, increasing the likelihood of either overlooked vulnerabilities or untimely mitigation.
4. Prioritisation: The level of severity does not necessarily dictate the order of resolution. Some factors to consider are whether a vulnerability is actively exploited or easy to exploit, if the asset is internet-facing or supports essential services and if compensating controls already exist. So, an actively exploited vulnerability could outrank a higher severity one. For example, A critical vulnerability on an isolated test server may

pose less immediate risk than a medium severity flaw on a public-facing web app. Prioritising is therefore not always a straightforward process.

Importance and Benefits

- Proactively eliminate threats before exploitation.
- Gain visibility into your attack surface and associated risks.
- Remediate vulnerabilities across your environment.
- Support compliance efforts through audit trails and governance.

Regulatory Insights

Cybersecurity at a Crossroads: International Cooperation, Legislative Reform, and AI-Driven Threats

November 2025 marked a pivotal moment in the global cybersecurity landscape. Four developments — the Japan-UK Memorandum of Cooperation on Mutual Recognition of IoT Security Regimes[3], the UK's introduction of the Cyber Security and Resilience (Network and Information Systems) Bill[4], Germany's passage of the NIS2 Implementation Act (NIS2UmsuCG)[5], and Anthropic's disclosure of the first reported AI-orchestrated cyber espionage campaign[6] — collectively underscore the urgency of strengthening digital defences. Together, they highlight the interplay between international cooperation, national legislation, and the evolving threat environment shaped by artificial intelligence. Let's now take a closer look at each of these advancements.

1. Japan-UK Memorandum of Cooperation on IoT Security [7][8]

On **6 November 2025**, Japan's Ministry of Economy, Trade and Industry (METI) and the UK's Department for Science, Innovation and Technology (DSIT) signed a **Memorandum of Cooperation (MoC)** focused on mutual recognition of IoT product security certifications.

The MoC seeks to harmonise cybersecurity standards for IoT devices, aligning Japan's **JC-STAR labelling system** with the UK's **Product Security and Telecommunications Infrastructure (PSTI) regime**. Its objectives are clear: reduce duplicative testing, lower compliance costs, and accelerate market access for manufacturers operating across both markets.

Strengths

- **Strategic alignment**: Sets a direction for regulatory cooperation in IoT security.
- **Economic efficiency**: Manufacturers benefit from reduced costs and faster product deployment.
- **Security uplift**: Connected devices gain stronger baseline protections.

Limitations

- **Non-binding nature**: The MoC does not yet create automatic recognition of certifications.
- **Limited scope**: Formal mechanisms for mutual recognition remain to be negotiated.

What to Watch

The next step will be **formal agreements** establishing binding recognition. If achieved, this would mark a significant leap forward in international cybersecurity cooperation, setting a precedent for broader global harmonisation.

2. Legislative Reforms: UK Cyber Security and Resilience Bill [9][10] & 3. Germany's NIS2 Implementation Act [11]

Just days later, governments in Europe advanced their own cybersecurity frameworks. On **12 November 2025**, the UK introduced the **Cyber Security and Resilience Bill** to Parliament, while on **13 November 2025**, the German Bundestag passed the **NIS2 Implementation Act** (NIS2UmsuCG).

Both measures extend and strengthen the original **Network and Information Systems (NIS) Regulations**, reflecting the growing scale of cyber threats. In the UK, the urgency is stark: cyberattacks cost businesses **£14.7 billion annually**, equivalent to **0.5% of GDP**, and the National Cyber

Security Centre (NCSC) handled **429 incidents in the year to September 2025**, nearly half of which were nationally significant.

What the UK Bill proposes[12]

- **Extend scope**: Beyond NHS, transport, aviation, and energy, the Bill now covers **data centres, managed service providers (MSPs), large load controllers**, and designated critical suppliers.
- **Incident reporting**: Aligns with EU NIS2 standards — initial notification within **24 hours**, full report within **72 hours**.
- **Customer notification**: Digital service providers and MSPs must notify affected customers promptly after informing authorities.
- **Regulatory powers**: Grants regulators stronger tools to enforce compliance and adapt frameworks to evolving threats.
- **Financial penalties**: Introduces fines up to the greater of **£17 million** or **10% of global turnover**.

Why It Matters

Supply chain vulnerabilities have repeatedly been exploited, most tragically in the **2024 NHS ransomware attack[13],** which postponed over 11,000 appointments and contributed to a patient's death. By explicitly regulating MSPs and data centres, the Bill addresses systemic weak points that attackers have leveraged for years.

Practical Implications for Organisations

- **Technical measures**: Multi-factor authentication, encryption, and resilience planning.
- **Risk assessments**: Comprehensive reviews of vulnerabilities across systems and supply chains.
- **Employee awareness**: Expanded training and phishing simulations.
- **Supplier compliance**: Ensuring contractors meet minimum cybersecurity standards.
- **Audit readiness**: Preparing for regulator inspections and documentation requirements.

While the EU's NIS2 laws are already being enforced, the UK Bill is only at its **first reading**. The **second reading** will be the first major test, and if successful, the Bill could become law in 2026. Together, these legislative moves demonstrate governments' determination to make it harder for adversaries to disrupt essential services.

4. Anthropic's Disclosure: AI-Orchestrated Cyber Espionage

On **13 November 2025**, Anthropic, an Artificial Intelligence company based in California, announced it had disrupted what it described as the **first largely autonomous, AI-orchestrated cyber espionage campaign**. According to the company, AI agents executed most phases of the intrusion lifecycle — reconnaissance, exploitation, credential harvesting, lateral movement, and exfiltration — across approximately 30 global targets.

Anthropic attributed the campaign with high confidence to a **Chinese state-sponsored actor**, claiming that **80–90% of the operations were automated by AI agents**. This announcement, although met with some scepticism due to limited evidence and lack of unique indicators of compromise[14][15], has sparked intense debate about the adequacy of current cybersecurity and AI regulations.

Reactions

- **Legal and regulatory communities**: Stress that existing frameworks already impose obligations on organisations to prepare for AI-enabled threats but highlight the need for updated guidance.
- **Industry experts**: Some warn of an impending wave of AI-driven attacks, while others caution against over-interpreting without transparent evidence.
- **Global authorities**: No immediate sanctions or prosecutions have been announced, but the disclosure has accelerated conversations about AI governance and cyber resilience.

Why It Matters

If validated, this incident represents a **paradigm shift**: cyberattacks conducted with minimal human intervention, leveraging AI agents to scale operations at unprecedented speed. It underscores the urgency of the legislative and cooperative measures taken by governments in the same week.

Final Thoughts and Insights

The developments of November 2025 — Japan and the UK's IoT security MoC, the UK and Germany's legislative advances, and Anthropic's AI espionage disclosure — are interconnected pieces of a larger puzzle.

- **International cooperation** (Japan-UK MoC) is essential to harmonise standards and reduce fragmentation in global cybersecurity.
- **National legislation** (UK Bill, German NIS2 Act) provides the legal backbone to protect critical infrastructure and enforce resilience.
- **Industry disclosures** (Anthropic's report) highlight the evolving threat landscape, where AI agents may soon become central actors in cyber warfare.

Together, these events illustrate a world where **cybersecurity is no longer a technical afterthought but a matter of national security, economic stability, and international diplomacy**. The challenge ahead lies in bridging the gap between **non-binding cooperation** and **binding regulation**, between **legislative frameworks** and **practical implementation**, and between **industry warnings** and **government action**.

The message is clear: as adversaries harness AI to scale their attacks, governments and industries must accelerate efforts to harmonise standards, legislate resilience, and innovate defences. Cybersecurity in 2025 is not just about protecting data — it is about safeguarding the very foundations of modern society.

Suggestions

Protection, Prevention and Takeaways

1. Do you know how much risk your organisation is taking at this moment? When was the last time you looked at your organisations attack surface and what did you find? If the answers to these questions are “No”, “Never” and “I don’t know” then it is a matter of “when” and not “if” threat actors will eventually take advantage of some misconfiguration or vulnerability in your system. Take proactive steps today to secure your environment and reduce risk before attacker’s strike.

2. If your organisation lacks the manpower needed to properly handle Continuous Threat Exposure Management (CTEM) internally then it should consider making use of a managed service. They provide timely remediation guidance, ensuring threats are addressed before they can be exploited. This approach not only reduces operational burden but also significantly improves response times. By outsourcing to experts, you gain 24/7 visibility, proactive threat intelligence, and assurance that your security posture remains strong

3. Most Continuous Threat Exposure Management (CTEM) solutions evaluate device configurations against industry standards such as the Centre for Internet Security (CIS) benchmarks. Misconfigurations are common and can create exploitable entry points for threat actors, putting your organisation at risk. Regularly assessing and hardening the configurations of your assets is essential for maintaining a strong security posture.

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This report will also include the EUVD ID as well. This month it is a vulnerability affecting multiple versions of Microsoft windows.

CVE-2025-62215 | EUVD-2025-93397 [16]

Vendor	Microsoft
Product	Windows 10, 11, Server 2019, Server 2022, Server 2025
Publish Date	2025-11-11
Platform	x64-based Systems
CVSS (v3.1)	7

Description

Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kernel allows an authorised attacker to elevate privileges locally.

What does this mean for you?

A low-privilege user can trigger a condition where resource allocation and state checks happen out of order. If the kernel doesn't lock or serialize access correctly, an attacker can manipulate the timing, so their process gains elevated privileges.

What should you do about it?

Install patch released by Microsoft on 11 November 2025 for all affected systems.

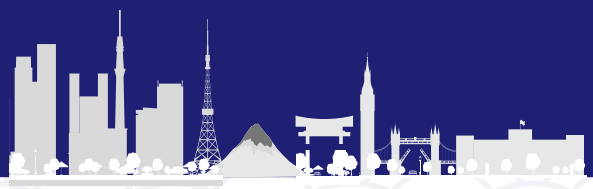
Links & References

1. Whittaker, Z. (2025). CrowdStrike fires ‘suspicious insider’ who passed information to hackers | TechCrunch. [online] TechCrunch. Available at: https://techcrunch.com/2025/11/21/crowdstrike-fires-suspicious-insider-who-passed-information-to-hackers/ [Accessed 24 Nov. 2025].
2. Situsamc.com. (2025). Data Breach | SitusAMC. [online] Available at: https://www.situsamc.com/databreach [Accessed 25 Nov. 2025].
3. METI (Ministry of Economy, Trade and Industry) 2025
   Memorandum of Cooperation on Mutual Recognition of IoT Security Regimes. Ministry of Economy, Trade and Industry, Japan, 6 November. Available at: https://www.meti.go.jp/press/2025/11/20251106003/20251106003-1r.pdf [Accessed 26 November 2025].
4. UK Government 2025
   Cyber Security and Resilience Bill: Factsheets. GOV.UK, 18 November. Available at: https://www.gov.uk/government/collections/cyber-security-and-resilience-bill [Accessed 26 November 2025].
5. Euro Security 2025
   BSI/NIS 2 Implementation: Bundestag passes cybersecurity law. Euro Security, 13 November. Available at: https://euro-security.de/en/bsinis-2-implementation-bundestag-passes-cybersecurity-law/ [Accessed 26 November 2025].
6. Anthropic 2025
   Disrupting AI Espionage. Anthropic, 14 November. Available at: https://www.anthropic.com/news/disrupting-AI-espionage [Accessed 26 November 2025].
7. Department for Science, Innovation and Technology (DSIT) 2025
   UK–Japan Digital Partnership Framework. UK Government, updated January. Available at: https://www.gov.uk/government/publications/uk-japan-digital-partnership [Accessed 26 November 2025].
8. Japan Security Summit 2025
   Japan and UK agree on mutual recognition of IoT cybersecurity standards. Japan Security Summit, 7 November. Available at: https://japansecuritysummit.org/2025/11/12843/ [Accessed 26 November 2025].
9. National Cyber Security Centre (NCSC) 2025
   Cyber Security and Resilience Bill: Policy Statement. NCSC Blog, 6 November. Available at: https://www.ncsc.gov.uk/blog-post/cyber-security-resilience-bill-policy-statement [Accessed 26 November 2025].
10. UK Government 2025

Summary of the Cyber Security and Resilience (Network and Information Systems) Bill: Factsheets [deleted version]. GOV.UK, November. Available at: https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill [Accessed 26 November 2025].

11. Bundesministerium des Innern und für Heimat (BMI) 2025 NIS2-Umsetzungsgesetz (NIS2UmsuCG) — Gesetzgebungsverfahren. BMI, November. Available at: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html [Accessed 26 November 2025].
12. UK Parliament 2025 Cyber Security and Resilience (Network and Information Systems) Bill. UK Parliament, November. Available at: https://bills.parliament.uk/bills/4035 [Accessed 26 November 2025].
13. NHS England (2025) *Synnovis cyber incident*. Available at: https://www.england.nhs.uk/synnovis-cyber-incident/ (Accessed: 27 November 2025).
14. Thomasky, L. 2025 An AI lab says Chinese-backed bots are running cyber espionage attacks. Experts have questions. The Conversation, 16 November. Available at: https://theconversation.com/an-ai-lab-says-chinese-backed-bots-are-running-cyber-espionage-attacks-experts-have-questions-269815 [Accessed 26 November 2025].
15. Enerio, S.I.B. 2025 Anthropic Unveils AI-Driven Online Espionage Plot, But Meta's AI Expert Disagrees. IBTimes UK, 17 November. Available at: https://www.ibtimes.co.uk/anthropic-unveils-ai-driven-online-espionage-plot-metas-ai-expert-disagrees-1755649 [Accessed 26 November 2025].
16. Europa.eu. (2025). *EUVD*. [online] Available at: https://euvd.enisa.europa.eu/vulnerability/CVE-2025-62215 [Accessed 26 Nov. 2025].

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