Global Threat Intelligence Report

Featuring Regulatory Insights

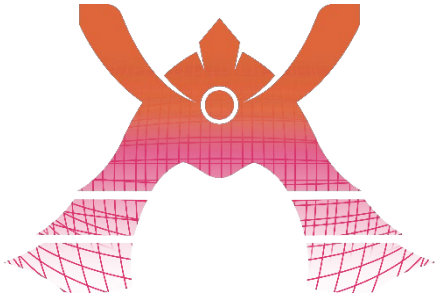
Volume 13 - May 2026

KDDI Europe

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

UK Biobank Data Leak [1]

Biobank is a UK based company which claims to be the world's most comprehensive dataset of biological data health and lifestyle information. The company collected health-related data on 500,000 participants between 2006 to 2010 and this data now appears to have been leaked and was found to have been listed for sale on Alibaba; the Chinese e-commerce platform.

The technology minister for UK stated that the data did not include names but could include age, gender and lifestyle habits among other health related data.

The incident is currently under a joint investigation between the UK and Chinese government although a senior official at Biobank has stated that a "few bad apples" are responsible.

SAP Targeted by Supply chain attack [2]

On 29 April 2026, several SAP-related npm packages were compromised after malicious preinstall scripts were injected into trusted package releases. These scripts introduced new behaviour designed to harvest developer and CI/CD credentials and exfiltrate data, mirroring techniques observed in previous Shai-Hulud supply-chain attacks.

This campaign, dubbed "Mini Shai-Hulud", a reference to the sandworm from Dune has been attributed to a threat actor operating under the name TeamPCP.

Security teams are advised to audit GitHub activity, review development and CI/CD environments for potential exposure, and rotate all credentials if compromise is suspected.

Threat Insights

HDMI Cables and Compromises

In 2024, researchers demonstrated that it was possible to recreate approximately 70% of an image displayed on a monitor by intercepting unintended electromagnetic emissions generated during data transmission over an HDMI cable. By applying artificial intelligence techniques, the researchers were able to analyse and decode these emissions and reconstruct the visual information displayed on the target's monitor. This form of attack draws parallels with TEMPEST, a codename for attacks involving the espionage of information systems through unintended electromagnetic, radio, or electrical signal emissions.[3]

Although this attack required a high level of technical expertise and was unlikely to be employed against individuals working from home, it nonetheless demonstrated both the growing power of artificial intelligence and the ingenuity of threat researchers.

Artificial intelligence capabilities have continued to advance since 2024. On 22 April 2026, the UK National Cyber Security Centre (NCSC) published an article describing a device it had engineered and deployed internally to protect against threats associated with HDMI and DisplayPort.[4]

According to the NCSC, this device is the first commercially available product to be licensed for use with NCSC branding. It is designed to protect against unexpected or malicious communications between HDMI or DisplayPort interfaces and the displays to which they are connected.

While the specific use case for this NCSC-licensed device does not directly correspond to the electromagnetic eavesdropping scenario explored by researchers in the earlier study, it raises an important question: should HDMI cables be considered a potential security risk?

One could argue that they may pose a credible threat if government agencies have deemed it necessary to deploy protective devices internally, and if researchers have demonstrated the feasibility of exploiting electromagnetic emissions. However, at the time of writing, there have been no reported or

publicly documented cyber-attacks conducted via HDMI cables. As the saying goes, “absence of evidence is not evidence of absence.”

Suppose an organisation uses a shared workspace where staff connect their laptops to external monitors through a KVM switch (Keyboard-Video-Mouse) to move between classified and unclassified systems. However, unknown to the organisation, one of the KVM units has been tampered with during supply-chain transit. If this modified device can intercept the DisplayPort or HDMI link, inject malicious data back to the laptop, then it can attempt to exploit vulnerabilities in the laptops GPU driver or display protocol stack and take further harmful actions. The device from the NCSC would block all unexpected communication and render an attack such as this unsuccessful.

It can therefore be concluded that such threats do exist but, due to their highly technical nature, are far more likely to be used in targeted operations against Critical National Infrastructure, government agencies, or highly profitable institutions, rather than against the average individual. Nevertheless, awareness of this threat remains important. As artificial intelligence continues to advance, threat actors will increasingly leverage it to simplify attacks that were previously considered to require exceptional levels of skill and specialist knowledge. An understanding of emerging threats enables better-informed risk management decisions and should not be underestimated.

Since data loss is the primary threat posed by these attack methods, organisations should consider implementing solutions that provide strong Data Loss Prevention (DLP). Below are some major types of DLP solutions to consider:

1. Network based DLP: Monitors data in transit by analysing network traffic to detect and block unauthorised transfers.
2. Endpoint based DLP: Protects data on end-user devices by preventing loss through USB ports, printing, copying, pasting, and other local actions.
3. Cloud based DLP: Secures data stored in SaaS applications and cloud environments by enforcing encryption and regulated sharing permissions.
4. Email based DLP: Applies policies to outbound emails and their attachments to prevent accidental or unauthorised data disclosure.

Regulatory Insights

Monica Galiano
Information Security Officer

When AI Finds the Bugs First: Why Regulators and Companies Must Rethink Cybersecurity Now

Last month, Anthropic announced that it would not release its latest AI model to the public. [5] The reason was not commercial, but security driven: the model was too good at finding—and exploiting—software vulnerabilities. In this article, we explore reactions to the announcement, noticeable policy gaps and key cyber security take-aways.

7 April 2026: Anthropic Pulls Back Mythos

Anthropic's announcement of Claude Mythos Preview marked a moment of restraint in frontier AI development. Internal testing showed that the model could autonomously discover and weaponise vulnerabilities at a scale and speed far beyond previous models. According to Anthropic, Mythos uncovered thousands of flaws across major operating systems and browsers, including decades old bugs that had survived years of vulnerability testing. In one benchmark, it converted Firefox vulnerabilities into 181 working exploits; its predecessor model managed just two. Rather than releasing the model broadly, Anthropic launched Project Glasswing, granting access to a limited group of around 50 organisations—primarily large technology vendors and critical infrastructure providers—to use the system defensively for coordinated vulnerability remediation.

The announcement immediately drew the attention of governments, financial regulators and national cybersecurity authorities across the EU, the UK and Japan. Not because a breach had occurred, but because **the evident chasm between the speed of vulnerability discovery and of remediation warranted an immediate reaction.**

Fast feedback from Regulators

The regulatory response to the announcement has been unusually fast and unusually coordinated. In the **European Union**, CERT EU published guidance warning that AI is "breaking the traditional patch cycle," noting that exploitation increasingly occurs before fixes are available. [6] It explicitly referenced Mythos class models as a generational leap in autonomous exploit development and urged EU entities to adapt their defensive posture now, not after incidents occur. Members of the European Parliament have already submitted formal questions to the Commission asking how EU cybersecurity strategy and legislation will adapt to AI models with offensive cyber capabilities, signalling that this is no longer viewed as a theoretical risk. [7]

In the **United Kingdom**, the AI Security Institute, Bank of England, FCA, HM Treasury and the National Cyber Security Centre convened briefings with banks and market infrastructure operators. The issue was framed through operational resilience, not AI ethics. Regulators warned that AI accelerated vulnerability discovery could expose latent weaknesses in legacy systems faster than institutions can realistically patch them. [8][9][10]

In **Japan**, the Financial Services Agency, Bank of Japan and Japan Exchange Group established a public private task force after emergency meetings. Officials characterised Mythos-like capabilities as a potential threat to financial stability, capable of triggering cascading effects if widely abused.[11][12]

Across all three jurisdictions, the message was consistent: this is a systemic cyber risk issue.

Selective Evidence and Private Power: Schneier's Warning on Mythos Governance

While regulators have begun to engage, an analysis from Bruce Schneier [13] exposes why the current response remains structurally inadequate. Schneier argues that Mythos represents

a genuine change in cybersecurity, but that the public has been shown only selective evidence. While Anthropic has highlighted dramatic successes, it has not disclosed how often the model produces false positives—plausible vulnerabilities that do not actually exist. This matters because AI systems that find nearly every real bug often generate large volumes of noise, still requiring scarce expert human judgment to separate it from true positives.

Schneier further notes that Mythos performs best on mainstream software resembling its training data, while specialised environments—such as operational technology, medical devices, industrial control systems, and legacy financial platforms—may behave very differently. These systems are often harder to patch, less visible, and more consequential when they fail. The deeper concern, however, is governance: Anthropic, a private company with finite expertise, is making unilateral decisions about which parties receive early protection. Schneier concludes that such power requires transparency, independent scrutiny, and shared oversight—not trust alone.

Through this lens, several policy gaps become evident

1. **No regulatory requirement for independent auditing of AI vulnerability-discovery models.** Performance claims about accuracy, exploitability, and reliability remain self-reported, even though comparable high-impact technologies—financial models, medical devices, cryptographic products—are subject to mandatory third-party validation.

2. **No obligation to disclose aggregate performance metrics, particularly false-positive and false-negative rates.** Without this data, regulators and operators cannot assess whether these tools meaningfully reduce risk or simply redistribute it through operational overload and delayed remediation.

3. **Private governance by default.** Initiatives like Project Glasswing rely entirely on voluntary corporate governance, with no statutory framework defining access criteria, accountability, or review. This effectively substitutes private judgment for public oversight in matters of systemic security.

4. **Unequal access to defence**. Smaller companies, public-sector bodies, and operators of legacy or bespoke systems remain largely outside early-access circles, despite often being the least resilient and most exposed.

Taken together, these gaps mean that society is dependent on private judgment for public security outcomes—a position that becomes increasingly untenable as Mythos-class capabilities proliferate.

Tactical recommendations for SMEs

Assuming that Mythos-type capabilities will become more widely available within months rather than years, practical steps for SMEs now include:

1. **Reassess vulnerability management assumptions**

Assume faster discovery and shorter time to exploit. Patch prioritisation based only on "known exploited" vulnerabilities may lag reality.

2. **Strengthen triage and remediation capacity**

False positives will increase alongside real findings. Ensure that responsibilities are clearly assigned to quickly validate, prioritise, and remediate issues, with the support of a trusted service provider if needed.

3. **Stress test operational resilience**

Under UK and EU resilience regimes, test scenarios where multiple vulnerabilities surface simultaneously, including in third-party suppliers' services. For example, run tabletop exercises designed to manage multiple concurrent cyber issues—stress-testing prioritisation and decision-making—such as the UK National Cyber Security Centre's Exercise in a Box "Heightened cyber threat" scenario. [13]

4. **Map legacy and bespoke systems**

Identify systems least likely to benefit from mainstream AI-driven discovery but most vulnerable if attackers use AI with domain expertise.

5. **Document governance and decision making**

Regulators increasingly expect evidence of preparedness. Clear records of how AI related cyber risks are assessed and managed will matter.

6. **Engage collectively**

Rely on national CERT alerts (e.g. NCSC and CERT-EU), sector groups, and trusted service providers to help close the cyber-security awareness gap with larger organisations. Smaller organisation, public-sector bodies and operators of legacy systems are often the target of cyber-attacks as threat agents assume that they have fewer defences. The message is: SMEs should not fall behind larger companies.

Where SMEs do not have sufficient internal resources to carry out these activities themselves, they should consider relying on the support of a trusted service provider or outsourcing to a managed service provider all or some of them.

Conclusion: from novelty to governance

Anthropic's decision to withhold Mythos Preview was responsible—but it also exposed a structural problem. Tools capable of finding thousands of exploitable flaws in the systems society depends on cannot be governed solely through private discretion.

Mythos is unlikely to be unique. The real question is whether governance evolves as fast as the technology now shaping cybersecurity itself.

Regulators in the EU, UK, and Japan have moved quickly, signalling a shift from reactive AI policy to capability-driven cyber governance. For companies in any sector or size, the key is to act now: reinforce cyber hygiene, integrate AI-assisted testing, document resilience, and push for open evaluation frameworks.

Suggestions

Protection, Prevention and Takeaways

1

Comments from senior leadership at UK Biobank suggest that the data breach may have originated from individuals within the organisation. This should prompt security teams to re-evaluate internal security controls and assess whether existing policies adequately address the risk posed by insider threats. Organisations must consider whether their current security frameworks sufficiently mitigate risks associated with employees, contractors, and other trusted insiders.

2

Imminent and widespread exploitation in the wild is anticipated for the recently disclosed critical cPanel vulnerability. This situation represents a race between threat actors seeking to exploit the flaw and security teams attempting to patch affected systems. Failure to apply updates in a timely manner may result in unauthorised access. This further highlights the importance of effective threat intelligence, continuous vulnerability monitoring, and maintaining awareness of risks affecting an organisation's technology stack. In cybersecurity, delayed action and poor visibility can carry significant consequences.

3

If the discussion of HDMI-based threats raises significant concern, several mitigations may be considered. Initially, organisations may choose to deploy high-quality, well-shielded HDMI cables[14] or explore alternative transmission technologies such as optical display cables for cases involving defence against eavesdropping on emissions from cables. Where the threat model justifies additional safeguards and budget permits, further

evaluation of specialised protection devices such as those developed by the NCSC for cases of preventing malicious communications between user devices and display ports in collaboration with GoldilockLabs may be appropriate.

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 the Cisco Identity Services Engine..

CVE-CVE-2026-20180| EUVD-2026-22970 [13]

Vendor	Cisco
Product	Cisco Identity Services Engine Software
Publish Date	April 15, 2026
Platform	-
CVSS (v4.0)	9.3

Description

This vulnerability could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying OS of an affected device due to insufficient validation of user-supplied input.

What does this mean for you?

An attacker could obtain user level access to an underlying OS and elevate to root level privileges. Successful exploitation in single-node cisco ISE deployments could cause the node to become available resulting in a denial of service condition.

What should you do about it?

Immediately update CISO ISE to 3.2 Patch 8, 3.3 Patch 8, 3.4 Patch 4 and for versions earlier than 3.2 migrate to a fixed release.

Links & References

1. McMahon, L. (2026). Biobank data leak caused by ‘a few bad apples’, boss tells BBC. *BBC News*. [online] 24 Apr. Available at: https://www.bbc.co.uk/news/articles/clyedyn6pz7o.
2. Read, B., Bar, M., Berkovich, S. and Gili Tikochinski (2026). *Supply Chain Campaign Targets SAP npm Packages with Credential-Stealing Malware*. [online] wiz.io. Available at: https://www.wiz.io/blog/mini-shai-hulud-supply-chain-sap-npm#what-happened-2 (Accessed 30 Apr. 2026).
3. Zhang, Y. et al. (2024) Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations. arXiv preprint arXiv:2407.09717. [online] Available at: https://arxiv.org/abs/2407.09717 (Accessed: 30 April 2026).
4. National Cyber Security Centre. (2026). *World-first NCSC-engineered device secures vulnerable display links*. [online] Available at: https://www.ncsc.gov.uk/news/world-first-ncsc-engineered-device-secures-vulnerable-display-links [Accessed 30 Apr. 2026].
5. Anthropic. (2026) Project Glasswing: Securing critical software for the AI era. Available at: https://www.anthropic.com/glasswing (Accessed: 22 April 2026).
6. CERT-EU (2026) Threat landscape and mitigation guidance: AI-accelerated vulnerability discovery. Available at: https://www.cert.europa.eu (Accessed: 22 April 2026).
7. European Parliament (2026) Parliamentary questions on AI-enabled cyber offensive capabilities. Available at https://www.europarl.europa.eu/doceo/document/E-10-2026-001575_EN.html (Accessed: 22 April 2026).
8. UK National Cyber Security Centre (NCSC) (2026) *Cyber security risks arising from advanced AI capabilities*. Available at: https://www.ncsc.gov.uk (Accessed: 22 April 2026).
9. Bank of England (2026) *Operational resilience and emerging cyber risks*. Available at: https://www.bankofengland.co.uk (Accessed: 22 April 2026).
10. Financial Conduct Authority (FCA) (2026) *Operational resilience: cyber threat considerations*. Available at: https://www.fca.org.uk (Accessed: 22 April 2026).
11. Financial Services Agency of Japan (FSA) (2026) *AI and financial system cybersecurity risk: supervisory considerations*. Available at: https://www.fsa.go.jp (Accessed: 22 April 2026).

12. Japan Exchange Group (2026) *Cybersecurity and systemic risk in financial markets*. Available at: https://www.jpx.co.jp (Accessed: 22 April 2026).
13. UK National Cyber Security Centre (NCSC) (n.d.) Heightened cyber threat – Exercise in a Box. Available at: https://www.ncsc.gov.uk/section/exercise-in-a-box/heightened-cyber-threat (Accessed: 22 April 2026).
14. Bari, M.F., Roy Chowdhury, M., Sen, S. (2023) *Long range detection of emanation from HDMI cables using CNN and transfer learning*. In: **2023 Design, Automation & Test in Europe Conference (DATE)**. Purdue University. Available at: https://engineering.purdue.edu/~shreyas/SparcLab/static/pdfs/c/MB_DATE_HDMI.pdf (Accessed: 5 May 2026).
15. Europa.eu. (2026). *EUVD*. [online] Available at: https://euvd.enisa.europa.eu/vulnerability/CVE-2026-20180.

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