Global Threat Intelligence Report

Featuring Regulatory Insights

Volume 14 - June 2026

KDDI Europe

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

News

The Latest Cybersecurity news

Henry Finnah
Security Service Engineer

7-Eleven data breach [1]

On 9 March 2026, the world's largest convenience store chain, 7-Eleven has suffered a data breach. According to a filing made at the Attorney General office in the state of Maine, US, 2 individuals from the state were affected and undisclosed information was stolen.

However according to information on HaveIBeenPwned the infamous ShinyHunters extortion group listed 7-Eleven on its leak website. This allegedly stolen data which has since been published online and analysed by HaveIBeenPwned appears to be inconsistent with 7-Elevens statement on the incident. Roughly 185,300 individuals are estimated to have been affected by the leak.

FBI warns of data-theft attacks [2]

The FBI warns of Kali365, a phishing-as-a-service platform targeting Microsoft 365 users that steals authentication tokens and session credentials rather than passwords, letting attackers access Outlook, Teams, OneDrive and other services without triggering password checks.

Kali365 automates attacks and lowers technical barriers, enabling inexperienced criminals to capture session tokens during login flows.

Because token-based compromises can go undetected by traditional defences, the FBI urges caution when approving authentication requests, and recommends monitoring active sessions, revoking compromised tokens, enforcing conditional access and token expiration, and deploying real-time detection and response measures.

Threat Insights

Anthropic's Mythos Model

On 28 May 2026, Anthropic, the company behind the Claude AI assistant, announced the release of Claude Opus 4.8, an incremental but meaningful upgrade to its flagship model. [3]

However, while Opus 4.8 represents steady progress, the most significant aspect of the announcement appears in a short section outlining what comes next: the upcoming release of Mythos-class models. Anthropic revealed that these models, currently restricted to a small number of organisations, are expected to be made available to customers "in the coming weeks."

Unlike Opus, Mythos is not just an improved conversational or coding assistant; it is a frontier AI system with advanced cybersecurity capabilities. Early testing suggests it can autonomously analyse software, identify vulnerabilities, and uncover thousands of previously unknown flaws across major systems.

Reports suggest that Mythos-based systems have already identified large volumes of high-severity vulnerabilities, significantly increasing the speed of discovery compared to human researchers.

This represents a fundamental shift. Traditional vulnerability discovery relies on expert researchers and time-consuming manual analysis. Mythos compresses this process by combining reasoning, automation, and large-scale code analysis, enabling weaknesses to be identified far more quickly than before.

However, some industry experts have raised concerns. Current AI-generated bug and vulnerability reports are often duplicated, low-value, or not immediately actionable, creating noise rather than meaningful outcomes. Code maintainers report seeing an increase in low-impact or unvalidated AI submissions lacking proof of concept. Their concern is that the release of such models could significantly increase this "noise."

Potential industry impacts include:

- Much faster vulnerability discovery, which may lead to alert overload and prioritisation challenges for security teams
- Increased pressure to shorten patch cycles and move towards near real-time remediation
- A continued shift towards detection and response, rather than prevention alone

Mythos signals a step change in the speed and scale of vulnerability discovery, altering how organisations prioritise, patch, and defend. However, it is important to recognise that this

does not automatically translate into usable exploits; prioritisation and response will remain the core challenges.

A CISO provided their perspective, noting that, as with previous disruptive technologies, attackers are likely to adopt these capabilities first, forcing defenders into a reactive position. However, over time, defenders typically adapt and close the gap.

While such tools can rapidly expose weaknesses, they can just as effectively be used to identify and remediate them. The expectation is not necessarily a surge in zero-day vulnerabilities followed by a sudden decline; rather, it is more likely that a small number of notable incidents will emerge, followed by rapid response and mitigation by security practitioners.

There is also a strong possibility that defenders will proactively leverage these tools to identify and patch vulnerabilities before attackers can exploit them, partially shifting the advantage back to defenders.

Regulatory Insights

Monica Galiano
Information Security Officer

UK Government approved Cyber Essentials scheme: Why MFA for all Cloud Services and Faster Patching Have Become Non-Negotiable

In April 2026, the IASME[4] consortium and the UK National Cyber Security Centre (NCSC) introduced **Cyber Essentials Requirements for IT Infrastructure v3.3,** bringing some of the most consequential updates to the scheme since its inception. These are not incremental refinements — they are direct responses to recurring failure patterns identified through breach investigations, audit findings and a threat landscape in which identities and cloud infrastructure have become primary attack surfaces. In this article we summarise the key changes introduced in v3.3, examine what prompted them, and consider a high-profile incident that illustrates precisely why rigorous enforcement of these controls matters — and how the outcome might have been very different had Cyber Essentials v3.3 been applied with full diligence. We also explore an area where the standard still leaves difficult judgement calls for auditors: the treatment of SSO and reauthentication for access to critical systems.

Version 3.3 of the Cyber Essentials Requirements for IT infrastructure had already been announced on 13 February 2026, giving organisations, time to prepare ahead of the 26 April 2026 go live date. The update applies to assessment accounts created after the implementation date, with an allowed transition of six months for active accounts created before that date. Its message is simple: the baseline for cyber hygiene has been raised, particularly for organisations that depend on cloud services, outsourced platforms and remote administration.[5]

Cyber Essentials has always been intended as a practical, accessible standard rather than a comprehensive security framework. It focuses on five technical controls: firewalls, secure configuration, security update management, user access control and malware protection. Version 3.3 does not change that foundation. Instead, it removes ambiguity in areas where ambiguity had become a security risk.

The most important changes are threefold. First, cloud services cannot be excluded from scope where they host organisational data or services. The requirements now define a cloud service as an on-demand, scalable service, hosted on shared infrastructure and accessible via the internet. That includes familiar business platforms such as Microsoft 365, Google Workspace, SaaS applications, MDM services and virtual desktop platforms. [6]

Second, MFA is now mandatory for cloud services where it is available. Organisations that fail to enable MFA for a cloud service where available - whether MFA is free, bundled, or a paid option - will automatically fail the assessment. This is a significant shift from a “strongly expected” control to a hard compliance requirement. IASME’s update explicitly states that non-implementation of MFA where available is now an auto-fail condition. [IASME]

Third, high-risk and critical security updates must be installed within 14 days of release. This applies to operating systems, router and firewall firmware, and applications, including associated files and extensions. Questions A6.4 and A6.5 are now auto-fail questions: if an organisation cannot demonstrate that these updates are installed within 14 days, it fails regardless of its performance elsewhere. [IASME]

These changes reflect how attackers actually operate. Identity is now one of the most heavily targeted parts of enterprise infrastructure. Cloud accounts often provide direct access to email, files, financial workflows, administrative consoles and customer data. A single compromised account may be more damaging than a compromised laptop. MFA is not a perfect control, particularly against session theft, adversary-in-the-middle phishing and poorly governed push approvals, but it remains one of the most effective basic defences against credential stuffing, password reuse and simple account takeover.

The 14-day patching requirement is equally pragmatic. Modern exploitation windows are short. Public proof-of-concept code, automated scanning and opportunistic exploitation often follow disclosure within days. Allowing high or critical vulnerabilities to remain open for weeks or months undermines the

value of any baseline assurance scheme. IASME notes that the updates were informed by scheme feedback, breach investigations, audits and ongoing assessment findings, which suggests the changes are not theoretical; they are responses to recurring failure patterns. [IASME]

The DigiCert incident reported in May 2026 provides a useful case study.

Public reporting says attackers breached DigiCert's internal support portal in April 2026 using a malicious screensaver file, ultimately obtaining code-signing certificates that were later linked to malware activity. Reporting also states that DigiCert revoked 60 certificates and introduced additional controls including stricter MFA, suspension of affected support accounts and disabling Okta FastPass access for the support portal. [CyberPress] [Ebuilder Security]

If Cyber Essentials v3.3 had been applied rigorously to the relevant environment, several barriers should have reduced the likelihood or impact of such an attack. A malicious screensaver is an executable file type that should fall within malware protection and secure configuration controls. Proper application control, restricted user privileges and prevention of unnecessary executable file types can limit whether a user can launch such a file. Strong update management reduces the chance that malware can exploit known vulnerabilities after execution. Separate administrative accounts reduce the risk that a compromised standard user session immediately becomes an administrative incident.

Most importantly, if the support portal was a cloud service, it would need to be in scope and protected by MFA where available. Under v3.3, it could not be treated as peripheral or excluded because it was "just" a support platform. That matters because support systems often expose sensitive workflows: customer records, certificate lifecycle functions, privileged resets, identity recovery processes and internal case notes. In many organisations, support tooling is effectively part of the control plane.

However, the DigiCert example also shows the limits of a baseline standard. Cyber Essentials can require MFA, but it does not fully solve the question of which MFA model is appropriate for a critical system. Some forms of SSO and passwordless access can be highly secure when implemented with phishing-resistant methods, device compliance checks and conditional access. Others can introduce risk if one successful authentication grants broad access to

sensitive portals without fresh verification.

This creates difficult edge cases for auditors. Suppose a critical certificate management system is accessed through corporate SSO. The identity provider enforces MFA at login, and the user's session persists for several hours. Is that enough? Cyber Essentials v3.3 requires MFA for cloud services where available and expects users to authenticate with unique credentials before access. It also recognises passwordless authentication, including FIDO2, within its definitions. But it does not provide a detailed, risk-tiered requirement for step-up authentication, transaction-level reauthentication, or disabling SSO for especially sensitive administrative actions. [NCSC]

For low-risk SaaS applications, centralised SSO with MFA may be entirely appropriate. For critical systems - certificate authorities, privileged access management platforms, financial approval systems, domain administration consoles, CI/CD signing systems and cloud root accounts - the better approach may be stricter. That could include phishing-resistant MFA, short session lifetimes, device binding, just-in-time privilege elevation and reauthentication before sensitive actions such as issuing certificates, exporting keys, changing MFA methods or approving support access.

The legal and assurance implication is important. Cyber Essentials certification should not be mistaken for proof that every high-risk workflow has been secured to a level proportionate to its impact. It is a baseline. Auditors must assess whether the stated scope is complete, whether MFA is truly enabled for all relevant cloud services, and whether patching evidence supports the 14-day requirement. But they may not always be able to determine, within the scheme's boundaries, whether an SSO configuration creates unacceptable residual risk for a crown-jewel system.

The conclusion is that Cyber Essentials v3.3 is a necessary tightening of the UK's baseline security standard.

It closes obvious loopholes: excluding cloud services, delaying critical patches and treating MFA as optional. Those loopholes no longer reflect the threat landscape. Incidents such as the DigiCert compromise show that attackers target identity, support systems, trusted software channels and small configuration weaknesses that can have outsized downstream consequences.

But v3.3 should be treated as the floor, not the ceiling. Organisations handling sensitive trust services, privileged administration or high-impact customer data should go beyond certification. They should map critical workflows, require phishing-resistant MFA where possible, apply step-up authentication for sensitive actions and continuously review whether SSO is reducing risk or merely centralising it. Cyber Essentials v3.3 makes basic failure harder to excuse. Mature security still requires judgement beyond the questionnaire.

Suggestions

Protection, Prevention and Takeaways

1

Organisations should deploy UEBA/real-time session monitoring and integrate auth logs into SIEM/XDR to detect anomalous token use. Traditional logs (login success/failure) are no longer sufficient. Modern attacks increasingly steal session tokens rather than passwords, abuse valid sessions to avoid detection and move laterally using legitimate identities.
UEBA helps by building baselines of normal behaviour (login times, locations, device types, access patterns), detecting anomalies such as Impossible travel, sudden access to high-privilege apps and unusual API/token usage

2

Try to enforce phishing-resistant MFA (FIDO2/hardware keys), block legacy authentication, and train users to deny unexpected approval prompts. Common MFA methods (SMS, push notifications) are vulnerable to: MFA fatigue attacks (spamming approvals), SIM swapping and Phishing proxies (e.g., Evilginx, Kali365)
Use authentication methods that cannot be intercepted such as FIDO2 / WebAuthn (hardware keys like YubiKey), Device-bound credentials (TPM-backed) and Passkeys where supported

3

AI tools like Mythos will increase discovery speed but also create a lot of noise. Not all findings will be useful and validation is necessary to avoid overwhelming security teams. Effective prioritisation will be absolutely necessary after the release of this model and security teams will need to be ready when it the time comes.

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-2026-45659 | EUVD-2026-31518[10]

Vendor	Microsoft
Product	SharePoint Server (2016, 2019, Subscription Edition)
Publish Date	22 May 2026
Platform	On-prem SharePoint (collaboration / document management servers)
CVSS (v3.1)	8.8

Description

This vulnerability is caused by deserialization of untrusted data in SharePoint. It allows a low-privileged authenticated attacker to execute arbitrary code remotely on the SharePoint server

What does this mean for you?

This can lead to a full compromise of a SharePoint server, access to sensitive data and credential harvesting.

What should you do about it?

Apply the latest patch from Microsoft for SharePoint 2016 / 2019 / Subscription.

Links & References

1. hIonut Arghire (2026). *185,000 Likely Impacted by 7-Eleven Data Breach*. [online] SecurityWeek. Available at: https://www.securityweek.com/185000-likely-impacted-by-7-eleven-data-breach/ (Accessed 28 May 2026)
2. Cybersecurity Insiders (2026) 'FBI warns about new Kali365 phishing platform targeting Microsoft 365 accounts', Cybersecurity Insiders, (accessed 29 May 2026).
3. Anthropic (2026) "Claude Opus 4.8", Anthropic, 28 May 2026. Available at: https://www.anthropic.com/news/claude-opus-4-8 (Accessed 29 May 2026).
4. IASME (n.d.) *IASME Home*. Available at: https://iasme.co.uk/ (Accessed: 8 June 2026).
5. IASME (2026) Important update: Changes to Cyber Essentials for April 2026. 12 February. Available at: https://iasme.co.uk/articles/important-update-changes-to-cyber-essentials-for-april-2026/ (Accessed: 8 June 2026).
6. National Cyber Security Centre (2026) *Cyber Essentials: Requirements for IT Infrastructure v3.3*. April. Available at: https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-3.pdf (Accessed: 8 June 2026).
7. AnuPriya (2026) *Hackers use malicious screensaver file to breach DigiCert and steal EV code-signing certificates*. CyberPress, 5 May. Available at: https://cyberpress.org/hackers-use-malicious-screensaver-file/ (Accessed: 8 June 2026).
8. eBuilder Security (2026) *DigiCert breach via screensaver enables malware signing, Microsoft Defender chaos*. 11 May. Available at: https://ebuildersecurity.com/cyber-news/digicert-breach-screensaver-malware-signing-microsoft-defender-false-positives/ (Accessed: 8 June 2026).
9. 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).

10. Europa.eu. (2026). *EUVD*. [online] Available at: https://euvd.enisa.europa.eu/vulnerability/CVE-2026-45659 (Accessed 29 May 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