Cybersecurity Advisors Network

Cyber (In)Security

Issue #208 · 17 August 2026

The fortnightly newsletter of the Cybersecurity Advisors Network (CyAN)

From the CyAN Community

Stablecoin and Crypto Asset Wallet Types: Custody and Security Requirements

White paper by Kamran Israr Mirza (Kim) · 13 August 2026

Wallet architecture and key custody have become the highest-stakes control domain in digital assets, and Kamran Israr Mirza's new CyAN white paper sets out why. The paper maps five wallet classes and four custody models against PCI DSS v4.0, ISO/IEC 27001:2022, ISO/IEC 42001, NIST CSF 2.0 and the EU AI Act, works through the key management lifecycle alongside reserve security and governance, and closes with six board-level recommendations. Read on the CyAN site.

CyAN Announcements

CyAN Mentorship Programme, Autumn 2026: applications closed

Applications for the autumn 2026 mentorship cohort are now closed. We will be announcing the selected participants shortly.

White Hat CVE of the Week

Courtesy of White Hat IT Security, led by CyAN member Sándor Féher

Week 32 — CVE-2026-18577: "Take Control" taken over

N-able N-central · CVSS 3.1 base 8.1 (High) · CVSS 4.0 base 8.2

An incomplete patch for CVE-2026-18556 leaves N-able N-central open to authentication bypass and account takeover in all versions through 2026.3.1. N-central is a remote monitoring and management platform, so a compromised instance is a compromise of everything it manages, which puts this squarely in the managed-service-provider blast-radius category. Full summary on the CyAN site.

Week 33 — CVE-2026-63077: TeamCity under construction

JetBrains TeamCity · CVSS 3.1 base 9.8 (Critical)

Unauthenticated remote code execution is possible via the agent polling protocol in JetBrains TeamCity before 2026.1.3 and 2025.11.7. A CI/CD server is about the worst place to hand an unauthenticated attacker arbitrary code execution, given what build systems typically hold in the way of credentials and signing material, so this one deserves to jump the patch queue. Full summary on the CyAN site.

News from Around the World

- **US water utility attacks widen to at least 12 states.** CISA acting director Nick Andersen reported a significant increase in threat actors targeting programmable logic controllers at water utilities, with incidents now confirmed in Minnesota, Michigan, Georgia and South Dakota among others; Clayton County Water Authority in Georgia issued a precautionary boil-water advisory, since lifted. Authorities have linked the campaign to Iranian actors. (The Record, 5 August)
- **Cyberattack on CEVA Logistics ripples through European retail.** The French logistics group notified corporate clients of an intrusion affecting eight European warehouses, disrupting fulfilment for Bol, De Bijenkorf, Ace & Tate and Valve's Steam hardware distribution in Europe. Ceva confirmed that customer data including names, addresses, postcodes, telephone numbers and email addresses was potentially exposed; attribution and whether ransomware was involved remain undisclosed. (The Record, 11 August)
- **Ransomware crew hijacks a hospital's Facebook page.** Two weeks after a 26 July cyberattack on the AnMed health system, its Facebook page was used to post ransom demands by a group calling itself The Gentlemen, which *claims* to have taken six terabytes of sensitive health records. AnMed has confirmed the unauthorised posts and that several facilities remain closed, but states it has not confirmed the scope of any impact to patient information and that the claims are unverified. (The Record, 11 August)
- **Three intrusions at the UK criminal records office went undetected for two years.** The ICO found that ACRO Criminal Records Office suffered three separate intrusions between July 2021 and June 2023, with a Kentico CMS left unpatched for nearly four years and Trend Micro alerts, including Mimikatz detections, going unheeded; over 84,000 people were notified as a precaution in April 2023. Network segmentation stopped lateral movement into core systems. The Medusa group claimed responsibility, though no data ever appeared on leak sites. (The Record, 12 August)
- **Germany moves to give its intelligence agencies hacking and sabotage powers.** The German cabinet approved a 732-page bill allowing intelligence services to conduct cyber operations against foreign systems and sabotage adversary infrastructure, with explicit carve-outs against measures endangering human life. The bill has not yet cleared parliament, and civil liberties groups have said they will challenge it. (The Record, 13 August)

Are you a CyAN member? Tag **@Cybersecurity Advisors Network (CyAN)** in your LinkedIn posts to be featured here. Member tags land in *Tagged by Our Members*; everyone else in *Partners & Community*.

Tagged by Our Members

Kim Chandler McDonald — when digital harm comes out of the tap

Kim Chandler McDonald · CyAN Global VP

Prompted by Axios reporting on the attacks against US water systems, Kim argues that once the systems under attack control water, power, hospitals and transport, the boundaries between cybersecurity, public safety, national security and trust and safety stop being boundaries at all, and that the people working on either side of those lines need to be in the same room far more often. Read the article.

Also from Kim this fortnight: smart glasses and bystander consent after a Guardian report from Melbourne (post); who is actually liable when an autonomous AI agent does the hacking (post); why AI literacy has to mean more than spotting a deepfake (post); and a "Data Center Bill of Rights" for the communities living next to the AI build-out (post).

Bharat Raigangar — security questionnaires are dead, so what replaces them?

Bharat Raigangar · CyAN board member

Writing in TahawulTech, Bharat makes the case that annual CAIQs, SIGs and SOC 2 reports give boards a false sense of comfort now that attackers use AI to find and weaponise open-source flaws in hours rather than months. His replacement: continuous attack surface management, AI-driven intelligence on leaked credentials, and adaptive zero-trust controls that throttle vendor access as risk scores move. The question, as he puts it, is no longer whether a vendor is certified but how fast you can isolate them once they are breached. Read the piece.

Also from Bharat: a fireside chat with Mayowa Adegoke on communicating risk to the board, at the International TPRM Alliance executive briefing (post).

Partners & Community

CyAN backs the Trust & Safety Festival Sydney

6 August 2026

CyAN has formally stated its support for the first Australian edition of the Trust & Safety Festival, on the argument that trust and safety cannot sensibly be treated as separate from cybersecurity when the same systems, data and harms are involved but the practitioners are still working in parallel. The programme spans AI governance, online harms, platform responsibility, scams, privacy, child safety and technology-facilitated abuse.

MaTeCC returns to Rabat for a fourth edition

17 August 2026

MaTeCC, the cybersecurity, trust and digital resilience conference organised by Ecole High-Tech and a long-standing fixture of CyAN's work in Morocco and across Africa, will hold its fourth edition on 2 and 3 December 2026 in Rabat. Registration is open at matecc.org.

Member Spotlight

Sylvain Hajri

Founder & CEO, Epieos · Co-founder, OSINT-FR · Greater Paris, France

Sylvain is an OSINT specialist and former red-team consultant who has spent since 2020 building Epieos into a digital-investigation platform used by law enforcement, governments and a community of over six million users, with its results feeding criminal cases spanning cybercrime, disinformation, fraud, insider threat and child exploitation. He trains and speaks for INTERPOL, Europol and France's IHEDN, co-founded OSINT-FR, the largest French-speaking OSINT community at 18,000+ members, and runs the OSINT Village at LeHack. Epieos was recently recognised by the Spanish Royal Household for its support to Spanish law enforcement operations. Connect with Sylvain on LinkedIn.

Upcoming Events

GISEC GLOBAL 2026

16–18 September 2026 · Dubai Exhibition Centre, Expo City, Dubai · updated dates

The Middle East and Africa's largest cybersecurity event. Event details.

Ai Everything Abu Dhabi

6 October 2026 · Abu Dhabi · CyAN is Knowledge Partner

AI infrastructure and sovereign AI, with 150+ fast-growing AI companies and decision-makers across finance, government, energy, healthcare and manufacturing. Members interested in attending should contact Bharat Raigangar. Event details.

Trust & Safety Festival Sydney 2026

8–9 October 2026 · Pullman Sydney Hyde Park · CyAN is a supporting partner

Technology, policy, government, law, academia, civil society and frontline practice; attendance capped at 200, places by registration of interest. Event details.

MaTeCC 2026 — 4th edition

2–3 December 2026 · Rabat, Morocco

Cybersecurity, trust and digital resilience across Morocco and Africa, organised by Ecole High-Tech. Registration and programme.

> **About CyAN.** The Cybersecurity Advisors Network (CyAN) is a global, member-driven non-profit connecting cybersecurity professionals, advisors and organisations to raise the standard of digital trust and security worldwide. **Want to be featured?** Tag **@Cybersecurity Advisors Network (CyAN)** in your posts, and share your CyAN-published work with us.