



Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #135



NEWS:

1. US Weakens Disinformation Defenses, as Russia & China Ramp Up

Original Source: Dark Reading by Robert Lemos

As geopolitical tensions escalate, the US has notably reduced its efforts to combat disinformation, especially from key adversaries like Russia and China.

This rollback occurs despite increasing efforts by these nations to spread misinformation aimed at influencing global politics and US public opinion.

Security analysts express concerns that diminishing these critical defences could significantly heighten vulnerabilities to foreign interference, potentially impacting election security and undermining public trust in democratic processes.

The implications of these changes are profound, prompting debates on the balance between freedom and security in the digital age.



NEWS:

2. China-Nexus APT 'Weaver Ant' Caught in Yearslong Web Shell Attack

Original Source: Dark Reading by Alexander Culaf

Security researchers have uncovered a sophisticated cyber-espionage campaign by the China-nexus advanced persistent threat (APT) group known as 'Weaver Ant.'

The group has been deploying web shells across multiple victim networks globally for several years, exploiting vulnerabilities to gain persistent access and exfiltrate sensitive data.

This prolonged infiltration highlights significant weaknesses in current cybersecurity defences and underscores the challenges of detecting and mitigating APT activities.

The campaign's complexity and stealth demonstrate the evolving sophistication of state-sponsored cyber actors and the continuous arms race in global cybersecurity.



NEWS:

3. Police arrests 300 suspects linked to African cybercrime rings

Original Source: BleepingComputer by Sergiu Gatlan

In a significant crackdown on cybercrime, police forces across multiple countries have arrested over 300 individuals connected to extensive African cybercrime syndicates.

These groups have been involved in various fraudulent schemes, including phishing, romance scams, and advanced fee fraud, causing substantial financial losses worldwide.

This coordinated operation showcases the growing international collaboration in combating cyber threats and highlights the increasing sophistication of cybercriminal networks in Africa.

The arrests not only disrupt ongoing operations but also serve as a deterrent to the wider cybercriminal community, emphasising the global reach and consequences of law enforcement against online crime.



NEWS:

4. NIST Still Struggling to Clear Vulnerability Submissions Backlog in NVD

Original Source: SecurityWeek by Ryan Naraine

The National Institute of Standards and Technology (NIST) is facing ongoing challenges in managing a significant backlog of vulnerability submissions in its National Vulnerability Database (NVD).

This delay in processing and cataloguing vulnerabilities poses a risk to cybersecurity as unaddressed vulnerabilities remain exploitable for longer periods.

The backlog has been attributed to a surge in reported vulnerabilities and resource constraints.

This situation underscores the critical need for improved processes and additional resources to ensure timely updates to the NVD, which is essential for maintaining up-to-date security postures across industries.



NEWS:

5. Cloudflare now blocks all unencrypted traffic to its API endpoints

Original Source: BleepingComputer by Bill Toulas

In a significant security enhancement, Cloudflare has announced that it will now block all unencrypted traffic to its API endpoints, mandating HTTPS for all connections.

This move aims to bolster the security of data in transit, preventing interception and manipulation by malicious actors.

By enforcing encrypted communications, Cloudflare enhances the overall security framework for its users and sets a higher standard for API security practices across the tech industry.

This change reflects the growing emphasis on encryption as a fundamental aspect of cybersecurity in an increasingly interconnected digital landscape.

CyberSecurity Advisors Network



NEWS:

6. Trump's Aggression Sours Europe on US Cloud Giants

Original Source: Wired by Matt Burgess

Amidst escalating tensions over data sovereignty, European countries are increasingly wary of relying on U.S.-based cloud service providers.

This shift in sentiment is largely driven by recent aggressive stances taken by the Trump administration, which have intensified concerns about data privacy and cross-border data flows.

European regulators and businesses are now pushing for greater use of local cloud services to ensure data protection and compliance with stringent EU regulations.

This growing distrust could reshape the global cloud services market, driving innovation and investment in European cloud infrastructure as an alternative to U.S. giants.

CyberSecurity Advisors Network



NEWS:

7. Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks

Original Source: The Hacker News by Ravi Lakshmanan

Developers and security teams are on high alert following the discovery of a critical vulnerability in Next.js, a popular web development framework.

This security flaw allows attackers to bypass middleware authorisation checks, potentially enabling unauthorised access to sensitive data and functions.

The vulnerability, identified as highly severe, affects multiple versions of the framework and poses a significant risk to applications built on Next.js.

Immediate updates and patches have been released to address this issue, urging developers to upgrade their systems without delay to safeguard against potential exploits.

CyberSecurity Advisors Network



NEWS:

8. FBI Warns of Malicious Free Online Document Converters Spreading Malware

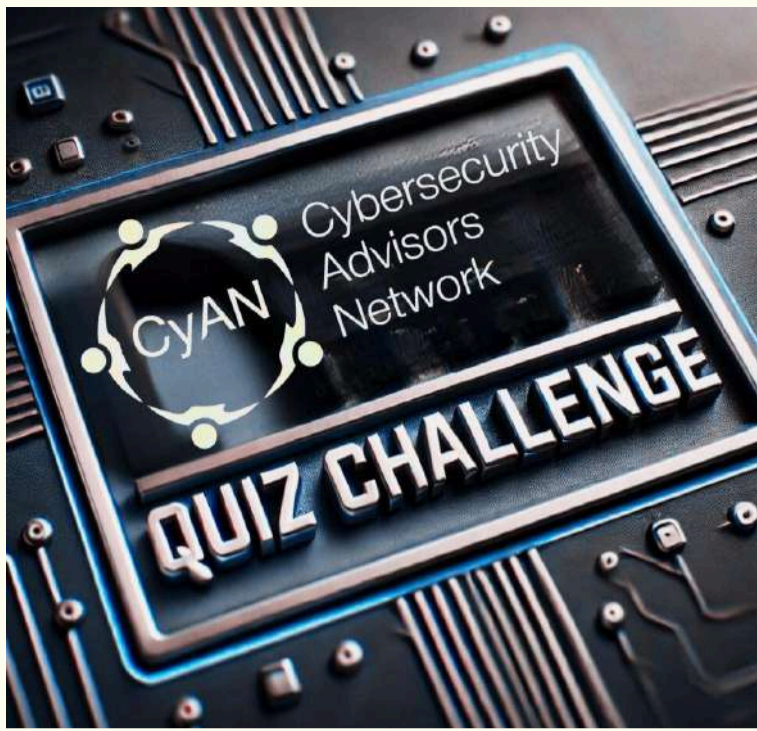
Original Source: Security Affairs by Pierluigi Paganini

The FBI has issued a warning about the risks associated with free online document converters, which have become a vector for distributing malware.

Cybercriminals are exploiting these platforms to embed malicious software into seemingly benign documents, leading to data theft, system compromise, and ransomware infections.

Users are advised to exercise caution and verify the security of any online converter used. This advisory underscores the importance of cybersecurity awareness and the need for robust protective measures when using online tools.

CyberSecurity Advisors Network



CyAN Members Only


Are You In the #CyANQuiz?

Hey CyAN Champions,

Have you got what it takes to outsmart your fellow cybersecurity pros? It's time to put your skills to the test in our Quarterly #CyANQuiz Challenge, kicking off on March 31st!

- ◆ 30 Questions. Timed. No second chances.
- ◆ Based on Recent Cybersecurity News & Events – Watch out for recent news and Cybersecurity events.

 **Check your email on March 31st for the quiz link;** just click, answer, and climb the leaderboard!

 Why Play? Compete, have fun, and win awesome prizes (while proving your cybersecurity dominance!)

Join the fun—this isn't just a quiz, it's a year-long challenge to **shine in the CyAN community!**

Think you can take the cyber crown? Prove it!



NEWS:

9. China says facial recognition should not be forced on individuals

Original Source: itNews

In a surprising move, the Chinese government has issued guidelines suggesting that facial recognition technology should not be imposed on individuals without consent.

This statement marks a significant shift in policy in a country known for its widespread use of surveillance technologies.

The new guidelines aim to address growing public concerns about privacy and personal freedoms, reflecting a broader debate on the ethical use of technology in society.

However, the implementation and enforcement of these guidelines remain to be seen, as they contrast with the extensive state surveillance practices currently in place.

CyberSecurity Advisors Network



NEWS:

10. AFP uses encryption powers to order technical assistance

Original Source: InnovationAus by Justin Hendry

The Australian Federal Police (AFP) is leveraging new encryption laws to compel tech companies to provide technical assistance in criminal investigations.

These powers enable the AFP to bypass encryption, facilitating access to data that could be crucial in solving cases.

While intended to enhance law enforcement capabilities, this use of power raises significant privacy and security concerns among civil liberties groups and the tech community, who argue it could undermine the security of digital communications and infringe on individual rights.

CyberSecurity Advisors Network



NEWS:

11. Service NSW to enforce multifactor authentication by 2026

Original Source: itNews by Eleanor Dickinson

In a proactive step towards enhancing digital security, Service NSW has announced that it will mandate multifactor authentication (MFA) for all its services by 2026.

This initiative aims to strengthen protection against cyber threats and identity theft, requiring users to verify their identity through multiple verification methods before accessing services.

The move reflects an increasing trend among government agencies to adopt stricter security measures to safeguard sensitive information and user data, aligning with global best practices in cybersecurity.

CyberSecurity Advisors Network



NEWS:

12. Prosecutors told to do more to strip 'revenge porn' abusers of victim images

Original Source: The Observer by Shanti Das

In response to the growing issue of 'revenge porn,' prosecutors are being urged to take stronger actions to remove illicit images from circulation and penalise perpetrators more severely.

This push for tougher enforcement comes amid reports of increasing incidents where private images are distributed without consent, causing significant distress to victims.

Legal experts and advocacy groups emphasise the need for robust legal frameworks that not only prevent the initial sharing of such images but also swiftly remove them from all digital platforms.

These efforts are part of a broader movement to protect individuals' privacy and dignity in the digital age, ensuring that abusers face significant legal consequences for their actions.

CyberSecurity Advisors Network



NEWS:

13. U.S. Treasury Removed Sanctions Against the Crypto Mixer Service Tornado Cash **Original Source: Security Affairs by Pierluigi Paganini**

The U.S. Treasury has lifted sanctions on Tornado Cash, a prominent cryptocurrency mixer, reversing a previous decision that had broadly impacted the crypto community.

This move comes after extensive discussions about the role of privacy in financial transactions and the legitimate uses of crypto mixing services.

Tornado Cash was initially sanctioned due to concerns over money laundering and other illicit activities.

The reversal highlights the complex balance regulators seek between preventing financial crimes and supporting technological and financial innovation.

The decision has been met with relief in the cryptocurrency sector, which advocates for stronger privacy protections for legitimate users while acknowledging the need for oversight to prevent abuses.



NEWS:

14. Microsoft Trusted Signing service abused to code-sign malware

Original Source: BleepingComputer by Lawrence Abram

Cybersecurity researchers have uncovered a troubling misuse of Microsoft's Trusted Signing service, where attackers have successfully code-signed malware, lending it an appearance of legitimacy.

This abuse poses significant risks, as signed software is generally trusted by operating systems and security software.

The incident reveals vulnerabilities in the digital signing process and raises questions about the reliability of security measures that depend heavily on certificates and signatures.

Microsoft is investigating the issue and working on strengthening its verification processes to prevent similar breaches in the future.



NEWS:

15. Zero-Day Broker Operation Zero Offers Up to \$4 Million for Telegram Exploits **Original Source: Security Affairs by Pierluigi Paganini**

Operation Zero, a prominent zero-day broker, has announced a bounty of up to \$4 million for new exploits targeting the popular messaging app Telegram.

This initiative reflects the high demand for vulnerabilities that can be used in cyber operations, emphasising the ongoing arms race in cybersecurity.

The lucrative offer aims to attract skilled hackers and researchers to uncover previously unknown security flaws.

Such bounties highlight the dual nature of the cybersecurity industry, where the discovery of vulnerabilities can either enhance security through patching or be exploited for malicious purposes, depending on who controls the information.



NEWS:

16. Coinbase was primary target of recent GitHub Actions breaches

Original Source: BleepingComputer by Lawrence Abrams

In a recent security incident, Coinbase, a leading cryptocurrency exchange, was identified as the primary target of breaches involving GitHub Actions.

Attackers exploited GitHub's continuous integration and delivery service to execute unauthorised actions and potentially access sensitive data.

The breach highlights the vulnerabilities associated with third-party platforms and the importance of securing software development pipelines.

Coinbase has responded by enhancing their security measures and collaborating with GitHub to address these vulnerabilities, aiming to prevent similar incidents in the future and protect user assets.

CyberSecurity Advisors Network



Webinaire : La relation de confiance entre le Data Protection Officer (DPO) et le Hacker Éthique


Nous avons le plaisir de vous inviter à un webinaire exclusif organisé dans le cadre de l'initiative Black Is Ethical, qui explorera une collaboration stratégique essentielle : la relation de confiance entre le Data Protection Officer (DPO) et le Hacker Éthique ou Construire une synergie efficace entre DPO et Hacker Éthique

 26 Mars, 2025 |  11:00 CET

 En ligne (lien transmis après confirmation)

Intervenants

- ◆ **Inssata RICOURT** – CISO & DPO, Fondateur de Black Is Ethical
- ◆ **Lara ALOUAN** – Chercheuse en sociologie, Orange
- ◆ **Yassir KAZAR** – CEO & Co-Founder, Yogosha
- ◆ **Étienne COUPRIE** – DPO de SogeCap
- ◆ **Léon MEIZOU** – Ingénieur, Spécialiste en répression de la cybercriminalité, Chercheur en Sécurité pour NASA en matière de Cybersécurité.

 **Jean-Christophe le Toquin**, Président de Cybersecurity Advisors Network (CyAN), Modérateur

 Pour plus d'informations et inscription, cliquez sur le code QR ci-dessus!



NEWS:

17. What CISA's Red Team Disarray Means for US Cyber Defense

Original Source: Dark Reading by Becky Bracken

The Cybersecurity and Infrastructure Security Agency (CISA) is currently grappling with internal challenges related to its red team operations, which are essential for testing and improving US cyber defences.

This disarray has raised concerns about the effectiveness of national cybersecurity strategies, especially at a time when threats are increasingly sophisticated.

The red team's role in simulating attacks to expose vulnerabilities is critical, and any disruption in their activities could significantly impact the nation's ability to detect and respond to real cyber threats.

The situation underscores the need for robust and well-coordinated cybersecurity practices to safeguard national interests.

CyberSecurity Advisors Network



NEWS:

18. Oracle denies breach after hacker claims theft of 6 million data records

Original Source: BleepingComputer by Sergiu Gatlan

Oracle has publicly refuted claims of a data breach after a hacker alleged the theft of 6 million records from their systems.

The hacker's claims, circulated widely online, suggested a significant security lapse. However, Oracle's investigation found no evidence supporting these claims, asserting that their security measures remained intact.

This incident highlights the challenges companies face in managing cybersecurity threats and the impact of false breach claims on reputation and trust.

It also underscores the importance of rigorous security protocols and timely, transparent communication in maintaining stakeholder confidence.

CyberSecurity Advisors Network



NEWS:

19. Nation-State 'Paragon' Spyware Infections Target Civil Society

Original Source: Dark Reading by Nate Nelson

The sophisticated 'Paragon' spyware, linked to a nation-state actor, has been discovered targeting civil society organizations worldwide.

This malware campaign is noted for its precision and stealth, designed to infiltrate systems and gather sensitive information without detection.

The impact on civil society is profound, threatening the privacy and security of activists and non-governmental organizations engaged in sensitive or controversial work.

The discovery of 'Paragon' underscores the growing trend of state-sponsored cyber espionage aimed at political manipulation and surveillance, raising serious concerns about digital security and human rights.

CyberSecurity Advisors Network



NEWS:

20. Medusa Ransomware Uses Malicious Driver to Disable Anti-Malware with Stolen Certificates **Original Source: The Hacker News by Ravi Lakshmanan**

The Medusa ransomware has evolved with a new tactic, using a malicious driver signed with stolen certificates to disable anti-malware software, enhancing its ability to infect systems undetected.

This development represents a significant escalation in ransomware sophistication, as attackers now manipulate legitimate software validation mechanisms to bypass security.

The use of stolen certificates complicates detection efforts, as it allows the malware to appear trustworthy to the system's security protocols.

This strategy underscores the necessity for enhanced vigilance and updated security measures to combat advanced ransomware threats.

CyberSecurity Advisors Network



NEWS:

21. Attack Update As FBI Warns Email And VPN Users—Activate 2FA Now **Original Source: Forbes by Davey Winder**

The FBI has issued a critical alert urging users of email services and VPNs to activate two-factor authentication (2FA) immediately.

This warning comes in response to a surge in cyber attacks targeting these services, exploiting weak or reused passwords.

By implementing 2FA, users can significantly enhance their security, creating an additional barrier against unauthorised access.

This precaution is particularly crucial as cybercriminals increasingly deploy sophisticated techniques to bypass traditional security measures.

The FBI's advisory highlights the ongoing need for robust cybersecurity practices to protect personal and organisational data.

CyberSecurity Advisors Network



NEWS:

22. Trump order put states at the forefront of cyber and natural disaster response

Original Source: Gov Exec by Chris Teale

A recent executive order by President Trump has shifted significant responsibility for responding to cyberattacks and natural disasters to state governments.

This directive aims to enhance local readiness and response capabilities by empowering states with more autonomy and resources. However, it also challenges states to rapidly upscale their infrastructure and training programs to effectively manage these critical situations.

The order reflects a strategic shift towards a more decentralised approach in managing emergencies, intending to foster quicker and more localised responses but also requiring significant coordination and support from federal agencies.

CyberSecurity Advisors Network



NEWS:

23. Groups Urge Congress to Extend Expiration Date for Cybersecurity Information Sharing Act **Original Source: American Public Power Association by Paul Ciampoli**

Advocacy groups are calling on Congress to extend the Cybersecurity Information Sharing Act's expiration date, emphasising the importance of continued and enhanced public-private collaboration in cybersecurity efforts.

The act facilitates the sharing of cybersecurity threat information between the government and private sector, playing a crucial role in preemptive threat detection and response.

Supporters argue that extending the act is vital for maintaining a robust defence against increasingly sophisticated cyber threats, ensuring that both sectors can rapidly exchange information and coordinate responses effectively.

CyberSecurity Advisors Network



NEWS:

24. The Trump Administration Wants USAID on the Blockchain

Original Source: Wired by Vittoria Elliott

The Middle East's rapid digitisation efforts are raising concerns about potential vulnerabilities in critical infrastructure.

This technological push aims to boost economic growth and modernise various sectors, but it also exposes these systems to cyber threats.

Experts warn that without robust cybersecurity measures, the region's infrastructure could be at risk of cyberattacks that disrupt essential services.

The article emphasises the need for comprehensive security strategies to safeguard these vital systems as they become increasingly interconnected and reliant on digital technologies.

CyberSecurity Advisors Network



CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Have you got what it takes to outsmart your fellow cybersecurity pros? It's time to put your skills to the test in our Quarterly #CyANQuiz Challenge, kicking off on March 31st!

- ◆ 30 Questions. Timed. No second chances.
- ◆ Based on Recent Cybersecurity News & Events – Watch out for recent news and Cybersecurity events.

 **Check your email on March 31st for the quiz link;** just click, answer, and climb the leaderboard!

💡 Why Play? Compete, have fun, and win awesome prizes (while proving your cybersecurity dominance!)

Join the fun—this isn't just a quiz, it's a year-long challenge to **shine in the CyAN community!**

Think you can take the cyber crown? Prove it!



ANALYSIS:

25. Is the Middle East's Race to Digitize a Threat to Infrastructure?

Original Source: Dark Reading by Apu Pavithran

The Middle East's rapid digitisation efforts are raising concerns about potential vulnerabilities in critical infrastructure.

This technological push aims to boost economic growth and modernise various sectors, but it also exposes these systems to cyber threats.

Experts warn that without robust cybersecurity measures, the region's infrastructure could be at risk of cyberattacks that disrupt essential services.

The article emphasises the need for comprehensive security strategies to safeguard these vital systems as they become increasingly interconnected and reliant on digital technologies.

CyberSecurity Advisors Network



ANALYSIS:

26. The Quantum Apocalypse Is Coming. Be Very Afraid

Original Source: Wired by Amit Catwalk

Imagine a world where today's encryption crumbles in seconds—this is the looming threat posed by quantum computing.

Often called the 'quantum apocalypse,' the scenario envisions a future where critical infrastructure, financial systems, and private communications are laid bare.

The article explores how quantum advancements could dismantle current cryptographic defences, sparking urgent investment in quantum-resistant technologies.

With adversaries already developing quantum capabilities, the race is on to secure digital systems before quantum breakthroughs force a global reckoning in cybersecurity.

CyberSecurity Advisors Network



ANALYSIS:

27. Why Canada and the EU Must Support Ukraine—And Each Other **Original Source: PrivID (Substack)**

This analysis explores the geopolitical and cybersecurity implications of the ongoing conflict in Ukraine, arguing for stronger support from Canada and the European Union.

The piece highlights how the conflict has not only regional but global cybersecurity ramifications, emphasising the need for collective action to counter threats and bolster security frameworks.

The author argues that supporting Ukraine is pivotal not just for regional stability but also as a stand against cyber aggression that could set precedents affecting global norms and cybersecurity policies.

The call for collaborative support from Canada and the EU reflects a broader strategy to enhance resilience against cyber threats and ensure a coordinated response to international security challenges.



ANALYSIS:

28. Nowhere to Run: The Online Footprint of an Alleged Kinahan Cartel Associate

Original Source: Bellingcat by Connor Plunkett, Peter Barth and Beau Donnelly

Digital footprints don't just expose everyday oversharers—they're now unravelling global crime networks.

This investigation tracks the online activity of an alleged Kinahan cartel associate, revealing how open-source intelligence (OSINT) tools can map relationships, locations, and movements with remarkable precision.

The piece highlights how social media and digital platforms, once seen as neutral ground, have become both tools of the trade for criminals and goldmines for law enforcement.

As the boundaries between digital life and real-world crime blur, the role of OSINT in modern policing is becoming impossible to ignore.



ANALYSIS:

29. The Human Factor: Redefining Cybersecurity In The Age Of AI **Original Source: Forbes by Tony Bradley**

As AI transforms cybersecurity, the human element is proving more essential—not less.

While machine learning brings speed, scale, and automation to threat detection, it lacks the nuance, ethics, and context-driven reasoning that human judgment provides.

This piece explores how people remain both a vulnerability and a vital line of defence, particularly in high-stakes decision-making.

It calls for sustained investment in human capability—through training, adaptability, and oversight—to ensure AI augments rather than replaces skilled professionals. In an age of automation, resilient cyber defence still begins with people.

CyberSecurity Advisors Network



ANALYSIS:

30. Strengthening Cybersecurity: Lessons from the Cybersecurity Survey

Original Source: International Monetary Fund by Rangachary Ravikumar

What's standing between nations and stronger cyber resilience?

A recent IMF survey offers clues, revealing persistent gaps in protecting critical infrastructure and inconsistencies in how countries approach cybersecurity.

The findings point to the urgent need for greater international cooperation, clearer standards, and the sharing of best practices.

With threats growing in speed and scale, the piece argues that no single country can go it alone—collective defence is now essential.

Investment in capacity-building, policy alignment, and cross-border collaboration will be key to staying ahead of an increasingly complex threat landscape



Has Trust in Democracy Survived the 2024 Election Year?

The Trust and Safety Forum is hosting a must-attend discussion on elections, disinformation, and democracy's resilience in the digital age as part of InCyber Forum Europe 2025.

 **April 1, 2025** |  **13:45 – 14:30 CET**

 **Lille, France** | **INCYBER FORUM EUROPE 2025**

The Panel:

 **Lorena Martinez** – Head of Editorial Operations, Europe & UK, Logically Facts


 **Laetitia Avia** – Digital Policy Expert, Lawyer & Former French MP

 **Stéphanie Ladel** – OSINT, IMINT & GEOINT Researcher & Trainer

 **Moderated by John Sullivan**, CyAN Board Member & Communications Chief

Discussion Topics:

 **Debunking disinformation** – What's working, and what needs to change?

 **The role of fact-checkers** – Minimising misinformation in real time

 **Building a balanced political environment** – The resources needed for election integrity

 **Scan the QR code above to get your free visitor's badge!**

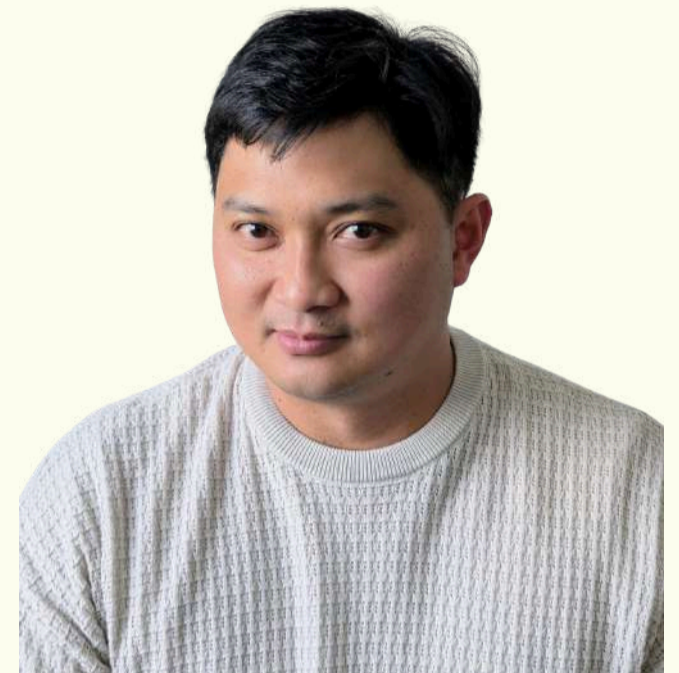


CyAN CyAN Members Op Eds, Articles, etc

31. CVE, CVSS, and EPSS: Which One Actually Matters for Security?

By CyAN General Secretary Fel Gayanilo

When it comes to measuring risk, not all cybersecurity metrics are created equal. Fel breaks down the roles of CVE, CVSS, and EPSS, examining how each contributes to a security team's understanding of vulnerabilities.



While CVE identifies flaws and CVSS scores their severity, EPSS stands out for its predictive power—estimating the likelihood a vulnerability will actually be exploited.

Fel's analysis calls for a shift toward more dynamic, intelligence-led security strategies that prioritise risk by likelihood, not just theoretical impact—enabling teams to stay ahead of the curve, not just react to it.

As threat actors move faster and exploit windows shrink, timing is everything. Metrics that help security teams prioritise what will be attacked—rather than what could be—are quickly becoming essential.



CyAN CyAN Members Op Eds, Articles, etc

32. Cybersecurity in Singapore - BlackHat Asia 2025 Here We Go!

By CyAN Member Nick Kelly

Few places are leaning into cybersecurity innovation quite like Singapore. With government support, a booming startup ecosystem, and growing international collaboration, the city-state is fast becoming a regional powerhouse.



As momentum builds ahead of Black Hat Asia 2025, Nick reflects on Singapore's strategic role in shaping cybersecurity conversations across the Asia-Pacific.

From policy to practice, the event promises to showcase both local leadership and global expertise—reinforcing CyAN's commitment to community, knowledge sharing, and advancing security on a global scale.

The energy is palpable, and the opportunities for cross-border learning and partnership are vast. If Singapore is any indication, the future of cybersecurity will be as collaborative as it is cutting-edge.

CyberSecurity Advisors Network



CyAN Member's News:

Breaking the Cycle: Combating Online IBSA for a Safer Digital Experience



Henry Adams



Kim Chandler



Caroline Humer



Robbert Hoving



Silvia Semenzin

Watch the enlightening recorded session of the webinar, "Breaking the Cycle – Combating Online Image-Based Sexual Abuse," a collaborative effort by the Cybersecurity Advisors Network (CyAN), Resolver Trust & Safety, and STISA.

This session brings together top experts Caroline Humer (STISA), Dr. Silvia Semenzin, and Robbert Hoving (OFFLIMITS) who delve into the profound impacts of IBSA and discuss actionable strategies to combat this form of digital violence.

Moderated by CyAN Global VP Kim Chandler McDonald, the webinar covers critical topics such as the role of technology in perpetuating IBSA, effective reporting mechanisms, and innovative approaches to creating a safer, more inclusive digital environment. It's not just a resource but a call to action, urging all stakeholders to unite and create safer digital spaces.





CyAN Member's News:

We at CyAN are ALWAYS overjoyed to celebrate our members successes and their contributions to the cybersecurity community!

Congratulations to CyAN member and CEO of White Hat IT Security, Sándor Fehér, for winning the Best CEO of the Year 2025 award from 'Behaviour - a HR-magazin' in the small business category! This prestigious recognition is a testament to Sándor's exceptional leadership and his commitment to excellence at White Hat IT Security. Sándor's leadership not only steers his company but also sets a high standard within the cybersecurity community!



Quite understandably, 'French Tech Amsterdam'—a gathering of the French and local tech community in Amsterdam, consisting of entrepreneurs, executives, and investors—celebrated CyAN member and winner of the 2024 European Cyber Women Trophy, Sarah Jane Mellor! (We think she's fabulous too!!!)





CyAN Member's News:

Congratulations to CyAN member and Founder of Vyanams Strategies (VYS), Vaishnavi J, and her team for their crucial support in developing the 5Rights Foundation's 'Children & AI Design Code'!



This landmark code, grounded in global regulatory frameworks, marks a significant step toward ensuring that AI systems prioritise the safety, privacy, and digital wellbeing of children.

Vaishnavi's collaborative efforts highlight the importance of intentional design in AI, paving the way for safer digital environments for our children.

It's a timely and necessary contribution as we navigate the intersection of emerging technologies and children's rights. The work done here not only shapes policy but sets a precedent for ethical innovation in the AI space.

Her dedication to such a transformative initiative is truly admirable—and worth celebrating across the entire CyAN community.

CyAN thrives because of the incredible talent, leadership, and dedication of our members, and we are proud to see them shaping the future of cybersecurity on a global stage! 🚀❤️



UPCOMING CyAN and CyAN Partner EVENTS:

- **Trust & Safety Forum at Forum INCYBER Europe (FIC), Lille, France: April 1-2 <https://tinyurl.com/mrruerfz>**
- **Supply Chain Cyber Security Summit (SCCS), Lisbon Portugal: 9-11 April 2025 <https://sccybersecurity.com/cyber-security-summit-europe/>**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April <https://tinyurl.com/2yhuztwk>**
- **GITEX ASIA, Singapore (Marina Bay Sands): 23-25 April <https://gitexasia.com/>**
- **GISEC Global, Dubai World Trade Centre: 6-8 May <https://gisec.ae/home>**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), London, UK: 8 May <https://www.thecyberospas.com/about/>**
- **CSG Awards 2025, Dubai: 7 May <https://csgawards.com/>**
- **World AI Technology Expo, Dubai: 14-15 May <https://worldaiexpo.i>**
- **CyAN 10th Anniversary Celebrations!**
- **GITEX Europe Messe, Berlin: 21-23 May <https://www.gitex-europe.com/>**
- **MaTeCC, Rabat, Morocco: 7-9 June <https://tinyurl.com/mtecz8vw>**
- **CyAN Q2 Community Call (APAC and the Gulf), June 11: 12:00 GST / 16:00 SGT / 18:00 AEST**
- **CyAN Q2 Community Call (EMEA and the Americas), June 11: 20:00 GST / 18:00 CET / 17:00 UTC / 12:00 EDT**





Bookings Open for the 2025 Cyber OSPAs

Tickets Available till March 26th!

 And the finalists are...

The entries are in, the judges have deliberated, and the finalists have been revealed. Now, it's time for the grand finale—the moment we celebrate the best and brightest in cybersecurity!

On 8th May 2025, under the dazzling lights of 133 Houndsditch, London, the Big SASIG Conference Dinner

will set the stage for an unforgettable evening of recognition, inspiration, and industry camaraderie.

Who will take home the top honours? Which names will be etched into cybersecurity history? Be there to witness the triumphs, toast to excellence, and celebrate the incredible individuals driving our industry forward!



2025 Cyber OSPAs



**Winners of the 2025 Cyber
OSPAs will be revealed on
Thursday 8th May**



Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!



CyberSecurity Advisors Network

**If you found
this
interesting,
please like and
share it with
your friends
and
colleagues!**

#ReallyInterestingCyberStuff!

#SharingIsCaring

