



Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #140



NEWS:

1. Tariffs May Prompt Increase in Global Cyberattacks

Original Source: Dark Reading by Robert Lemos

As global tariffs rise, there's an escalating risk of increased cyberattacks, with nations potentially leveraging cyber tactics as part of economic warfare.

This poses a dual threat to international trade and cybersecurity stability, with adversaries likely targeting critical infrastructure and corporate networks. Such actions could magnify the potential for economic disruption and escalate international tensions.

The intertwining of economic strategies with cyber warfare underscores the crucial need for robust digital defences and proactive international cooperation to mitigate the risks associated with geopolitical conflicts.

Understanding these dynamics is essential for nations to prepare effective cybersecurity measures.



NEWS:

2. US Comptroller Cyber 'Incident' Compromises Org's Emails

Original Source: Dark Reading by Kristina Beek

In a significant cybersecurity breach, the US Comptroller's office has encountered an incident leading to the exposure of sensitive email communications.

This breach underscores vulnerabilities within governmental cybersecurity infrastructures and highlights the potential risks to critical governmental operations.

The incident reveals the importance of robust cybersecurity measures and continuous monitoring within government entities to protect sensitive information from such exposures.

It serves as a stark reminder of the challenges faced in securing government communications against sophisticated cyber threats.

CyberSecurity Advisors Network



NEWS:

3. Wyden blocks Trump's CISA boss nominee, blames cyber agency for 'actively hiding info' about telecom insecurity

Original Source: The Register by Jessica Lyons

Senator Ron Wyden has taken a firm stand against the nomination of the new CISA director, citing serious concerns over transparency and the agency's handling of telecom security.

The objection highlights ongoing issues within cybersecurity leadership and underscores the critical need for clear accountability in safeguarding national telecommunications infrastructure.

This controversy not only points to broader challenges in cybersecurity governance but also stresses the importance of maintaining high standards of transparency to foster trust and effectiveness in national security protocols.

CyberSecurity Advisors Network



NEWS:

4. Trump signs order stripping Chris Krebs of security clearance

Original Source: Cyberscoop by Greg Otto

In a controversial move, former President Trump has revoked the security clearance of Chris Krebs, the former director of CISA, sparking considerable debate within the cybersecurity community.

This action highlights the potential for politicisation of critical cybersecurity roles and raises significant concerns about the implications for national security.

The decision underscores the ongoing tensions and challenges in maintaining a non-partisan stance within security agencies, emphasising the necessity for stable and unbiased leadership in roles that are pivotal in safeguarding the nation's cyber and physical infrastructures.

It also prompts a broader discussion about the integrity and independence of national security positions.



NEWS:

5. Hackers target SSRF bugs in EC2-hosted sites to steal AWS credentials

Original Source: BleepingComputer by Bill Toulas

Hackers are exploiting Server-Side Request Forgery (SSRF) vulnerabilities in EC2-hosted sites to illicitly gain AWS credentials, exposing critical security flaws in cloud infrastructure.

This breach demonstrates the sophisticated methods used by cybercriminals to infiltrate cloud services, underscoring the urgency for enhanced security protocols and vigilant monitoring.

The exploitation of such vulnerabilities can lead to significant data breaches and operational disruptions, highlighting the need for continuous improvement in cloud security measures to protect against advanced threats.

CyberSecurity Advisors Network



NEWS:

6. Sensitive financial files feared stolen from US bank watchdog

Original Source: The Register by Iain Thomson

A recent cyberattack on a US bank regulatory body has sparked fears that sensitive financial files may have been stolen.

This incident highlights the vulnerabilities faced by financial institutions in safeguarding critical data.

The breach could potentially expose the financial sector to substantial risks, including fraudulent activities and financial instability.

This event underscores the importance of robust cybersecurity measures and the need for continuous monitoring and updating of security protocols to protect sensitive information from sophisticated cyber threats.

CyberSecurity Advisors Network



NEWS:

7. National Social Security Fund of Morocco Suffers Data Breach

Original Source: Security Affairs by Pierluigi Paganini

The National Social Security Fund of Morocco has recently experienced a significant data breach, compromising the personal and financial information of numerous citizens.

This breach underscores the persistent risks to sensitive data and highlights vulnerabilities within systems meant to protect such information.

The incident raises serious concerns about the safeguards in place and the potential consequences for affected individuals.

It calls for enhanced security protocols and vigilant monitoring to prevent future breaches, emphasising the importance of robust data protection strategies to mitigate risks and restore public trust.

CyberSecurity Advisors Network



NEWS:

8. BadBazaar and Moonshine malware targets Taiwanese, Tibetan and Uyghur groups, U.K. warns

Original Source: Cyberscoop by Tim Starks

The UK has issued a warning about BadBazaar and Moonshine malware campaigns targeting Taiwanese, Tibetan, and Uyghur political groups.

This cybersecurity alert underscores the increasing use of malware in geopolitical conflicts, with these specific threats designed to infiltrate and disrupt the activities of targeted groups.

The campaigns reflect broader trends in cyber espionage, where digital tools are used to influence and monitor political movements.

Such incidents highlight the need for heightened cybersecurity awareness and defences among politically active groups to prevent compromising sensitive information.

CyberSecurity Advisors Network



NEWS:

9. Critical FortiSwitch flaw lets hackers change admin passwords remotely

Original Source: BleepingComputer by Sergiu Gatlan

A newly discovered critical flaw in FortiSwitch devices permits hackers to remotely change admin passwords, putting network security at high risk.

This vulnerability exposes numerous networks to potential unauthorised access and control, highlighting the critical need for immediate patching and regular security assessments.

The flaw's discovery stresses the importance of maintaining up-to-date security practices and the continual evaluation of network hardware vulnerabilities to prevent exploitation by cybercriminals seeking to undermine organisational cybersecurity defences.

CyberSecurity Advisors Network



NEWS:

10. Fake Microsoft Office add-in tools push malware via SourceForge

Original Source: BleepingComputer by Bill Toulas

Cybercriminals are exploiting fake Microsoft Office add-in tools to distribute malware, targeting users on popular platforms like SourceForge.

This tactic highlights the ongoing issue of trust exploitation in software distribution.

Users downloading these add-ins face significant risks as the malware can compromise personal data and system integrity.

This situation underscores the necessity for heightened vigilance when downloading software from third-party sources and the importance of verifying the authenticity of add-ins to protect against sophisticated phishing and malware attacks.

CyberSecurity Advisors Network



NEWS:

11. Privacy fights over expiring surveillance law loom after House hearing

Original Source: Cyberscoop by Tim Starks

As the expiration of a key surveillance law approaches, heated debates emerge in the House over its renewal, raising significant privacy concerns.

This legislation's potential extension is contentious, with advocates arguing it is essential for national security while critics warn it could infringe on personal freedoms.

The discussions highlight the delicate balance between security needs and privacy rights, stressing the importance of crafting laws that both protect citizens from threats and respect their civil liberties.

This debate is crucial in shaping how surveillance tools are regulated and used in the future.

CyberSecurity Advisors Network



NEWS:

12. UK Orgs Pull Back Digital Projects With Looming Threat of Cyberwarfare

Original Source: Dark Reading by Kristina Beek

Fears of potential cyberwarfare have prompted UK organisations to pull back on digital initiatives, highlighting the growing concern over digital security in geopolitical tensions.

As the threat landscape evolves, businesses are increasingly prioritising robust cybersecurity measures over expansion and innovation.

This shift reflects a broader trend where organisations worldwide are reassessing their digital strategies to mitigate risks associated with cyber conflicts.

The situation underscores the need for continuous adaptation in cybersecurity practices to protect critical infrastructure and maintain business continuity in a volatile global environment.

CyberSecurity Advisors Network



NEWS:

13. Adobe Calls Urgent Attention to Critical ColdFusion Flaws

Original Source: SecurityWeek by Ryan Naraine

Adobe has issued an urgent alert to ColdFusion users about critical vulnerabilities that could allow attackers to execute arbitrary code remotely.

These flaws pose a significant risk to businesses and organisations using ColdFusion for web application development.

Immediate patching is advised to prevent potential exploits that could lead to data breaches and system compromises.

This situation highlights the continuous need for vigilant software maintenance and rapid response to security advisories in a landscape where even well-established platforms can become vectors for cyber attacks.

CyberSecurity Advisors Network



Holiday Schedule for (In)Securities!

Hop into the holiday spirit! Due to the upcoming Easter and ANZAC Day celebrations on the weeks of Monday, April 14th and 21st, we're taking a small breather just like our beach-loving bunny here.

We'll be publishing only one edition each week, on the Thursdays (April 17th and 24th).

So, while our newsletter takes a mini-holiday, we hope you enjoy your festivities too! Look out for the Easter edition dropping into your inboxes with just as much zest as a bunny on a beach vacation!

Thank you for being such fabulous readers. Stay safe, have fun, and let's keep cracking on those cyber eggs together!

 **Catch you on the sunny side of Cyberspace!**



NEWS:

14. 2 Android Zero-Day Bugs Under Active Exploit

Original Source: Dark Reading by Kristina Beek

WhatsApp has successfully patched a critical spoofing flaw that previously allowed hackers to potentially execute malicious code remotely.

This vulnerability highlighted significant security risks within the app, particularly in how messages and data are verified and handled.

The patch is a crucial update that strengthens the app's defences against sophisticated cyber attacks aiming to exploit communication platforms.

This update is vital for users to maintain secure communication and protect their personal information from being compromised by malicious entities.

CyberSecurity Advisors Network



NEWS:

15. Treasury Department bank regulator discloses major hack

Original Source: Cybersecurity Dive by Elizabeth Montalbano

The Treasury Department's bank regulator has recently disclosed a major cybersecurity incident, potentially compromising sensitive financial data.

This breach has raised significant concerns about the robustness of security measures in place to protect the critical financial infrastructure.

The incident not only underscores the importance of stringent cybersecurity protocols and constant vigilance but also highlights the broader implications for national economic security and the trust vested in institutions tasked with safeguarding financial data.

It prompts an urgent reassessment of security practices within financial regulatory bodies to prevent future vulnerabilities.

CyberSecurity Advisors Network



NEWS:

16. Inside a Powerful Database ICE Uses to Identify and Deport People

Original Source: 404 Media by Jason Koebler

The Treasury Department's bank regulator has recently disclosed a major cybersecurity incident, potentially compromising sensitive financial data.

This breach has raised significant concerns about the robustness of security measures in place to protect the critical financial infrastructure.

The incident not only underscores the importance of stringent cybersecurity protocols and constant vigilance but also highlights the broader implications for national economic security and the trust vested in institutions tasked with safeguarding financial data.

It prompts an urgent reassessment of security practices within financial regulatory bodies to prevent future vulnerabilities.

CyberSecurity Advisors Network



NEWS:

17. Dangerous, Windows-Hijacking Neptune RAT Scurries Into Telegram, YouTube

Original Source: Dark Reading Elizabeth Montalbano

The Neptune RAT, a Windows-hijacking malware, has found new propagation avenues through popular platforms like Telegram and YouTube.

This expansion into social and video platforms underscores the evolving nature of cyber threats and the innovative methods used by attackers to distribute malware.

The RAT's ability to control infected systems remotely poses significant risks to users, highlighting the importance of cybersecurity awareness and the need for robust protective measures against such sophisticated threats.

This development serves as a stark reminder of the need for continuous vigilance in the digital space.

CyberSecurity Advisors Network



NEWS:

18. SAP Patches Critical Code Injection Vulnerabilities

Original Source: Security Week by Ionut Arghire

SAP has recently patched several critical vulnerabilities that allowed for code injection in its software, highlighting the continuous threat to enterprise systems.

These vulnerabilities, if exploited, could allow attackers to take complete control over affected systems, demonstrating the critical nature of maintaining up-to-date security practices in enterprise software environments.

The patches address these severe risks and underscore the importance of prompt updates to safeguard business operations and sensitive data from sophisticated cyber-attacks.

CyberSecurity Advisors Network



NEWS:

19. WhatsApp Vulnerability Could Facilitate Remote Code Execution

Original Source: SecurityWeek by Eduard Kovacs

WhatsApp has addressed a critical vulnerability that previously could allow remote code execution, potentially exposing millions of users to cyber threats.

This flaw made it possible for attackers to send crafted messages that could execute malicious code on the recipient's device.

The patch significantly enhances the security of the messaging platform, reflecting WhatsApp's commitment to user safety in the face of evolving cyber threats.

This update is crucial for preventing attackers from exploiting the platform's widespread usage to spread malware or steal sensitive information.

CyberSecurity Advisors Network



NEWS:

20. ESET Vulnerability Exploited for Stealthy Malware Execution

Original Source: SecurityWeek by Ionut Arghire

Security researchers have disclosed a vulnerability in ESET's software that has been exploited to execute malware stealthily.

This flaw allows attackers to bypass traditional security measures, demonstrating the ongoing challenges faced by security technologies in detecting and preventing sophisticated cyber threats.

The vulnerability highlights the need for continuous updates and vigilance in security practices to protect against such elusive threats.

This incident underscores the importance of rapid response and adaptation by cybersecurity providers to safeguard users from emerging vulnerabilities.

CyberSecurity Advisors Network



NEWS:

21. UAC-0226 Deploys GIFTEDCROOK Stealer via Malicious Excel Files Targeting Ukraine

Original Source: The Hacker News by Ravie Lakshmanan

Threat group UAC-0226 has been observed distributing the GIFTEDCROOK stealer through weaponised Excel documents in a targeted campaign against Ukraine.

The malware is designed to exfiltrate sensitive data while evading detection, using familiar file formats to lower suspicion.

This tactic highlights the persistent risk posed by malicious document-based attacks, particularly in high-conflict regions.

It also reinforces the need for heightened vigilance, robust endpoint protection, and user training to detect and mitigate these deceptive and damaging threats.

CyberSecurity Advisors Network



NEWS:

22. Meta blocks livestreaming by teenagers on Instagram

Original Source: The Guardian by Dan Milmo

Instagram has introduced new restrictions preventing teenagers from livestreaming, part of a broader effort to improve online safety for younger users.

The platform's decision aims to limit exposure to harmful content and reduce the risk of exploitation, harassment, or manipulation during live broadcasts.

While the move may affect user engagement and content creation, it reflects growing global pressure on tech companies to prioritise child safety and wellbeing.

This policy shift underscores the difficult balance social platforms must strike between digital freedom and the responsibility to protect vulnerable users in real time.



NEWS:

23. EVEREST Ransomware Group's TOR Leak Site Offline After A Defacement

Original Source: Security Affairs by Pierluigi Paganini

The leak site used by the EVEREST ransomware group has been taken offline following a public defacement, disrupting one of its main channels for extortion and data exposure.

While it's unclear who was behind the attack, the incident raises questions about tensions within the cybercriminal ecosystem and the growing pushback against ransomware operators.

Though temporary, the takedown offers a brief reprieve for victims whose stolen data may have been published. It also illustrates how disruption tactics can challenge ransomware infrastructure, even as the broader threat landscape remains highly active.

CyberSecurity Advisors Network



NEWS:

24. Russian bots hard at work spreading political unrest on Romania's internet

Original Source: Bitdefender by Graham Cluley

A coordinated campaign of Russian-linked bots has been actively spreading disinformation and political division across Romanian social media platforms.

By amplifying polarising narratives and exploiting sensitive topics, these botnets aim to destabilise public discourse and erode trust in democratic institutions.

The operation is part of a broader pattern of influence campaigns seen across Eastern Europe, highlighting the persistent threat of state-backed information warfare.

This latest wave underscores the urgent need for stronger defences against digital propaganda and greater public resilience to manipulation.

CyberSecurity Advisors Network



NEWS:

25. Six arrested for AI-powered investment scams that stole \$20 million

Original Source: BleepingComputer by Bill Toulas

Authorities have arrested six individuals linked to a sprawling investment scam that used AI tools to deceive victims and steal over \$20 million.

The group allegedly used deepfakes, synthetic voice, and manipulated media to create convincing personas and fake endorsements, luring targets into fraudulent schemes.

This case highlights the growing role of generative AI in financial crimes and the difficulty of distinguishing between authentic and fabricated content.

It also raises urgent questions about the regulation and ethical use of emerging technologies in consumer-facing applications.

CyberSecurity Advisors Network



NEWS:

26. As CISA braces for more cuts, threat intel sharing takes a hit

Original Source: The Register by Jessica Lyons

As the Cybersecurity and Infrastructure Security Agency (CISA) faces looming budget cuts, experts warn of a potential decline in its ability to facilitate timely threat intelligence sharing.

With cyber threats growing in scale and complexity, the proposed funding reduction could hinder CISA's coordination with private and public sector partners.

This may leave critical infrastructure more vulnerable and weaken the collective cyber defence posture.

The situation raises serious concerns about the sustainability of national cybersecurity efforts in the face of shrinking resources and rising digital risks.

CyberSecurity Advisors Network



NEWS:

27. Counterfeit Android devices found preloaded with Triada malware

Original Source: BleepingComputer by Bill Toulas

Security researchers have uncovered counterfeit Android phones sold with Triada malware preinstalled, compromising users straight out of the box.

These low-cost devices, often marketed in emerging markets, give attackers immediate access to personal data, financial credentials, and app activity.

The discovery highlights the hidden risks in grey-market hardware supply chains and the exploitation of cost-sensitive consumers.

It also underscores the importance of device provenance and supply chain scrutiny as cybercriminals increasingly target users at the hardware level, bypassing traditional security measures entirely.



NEWS:

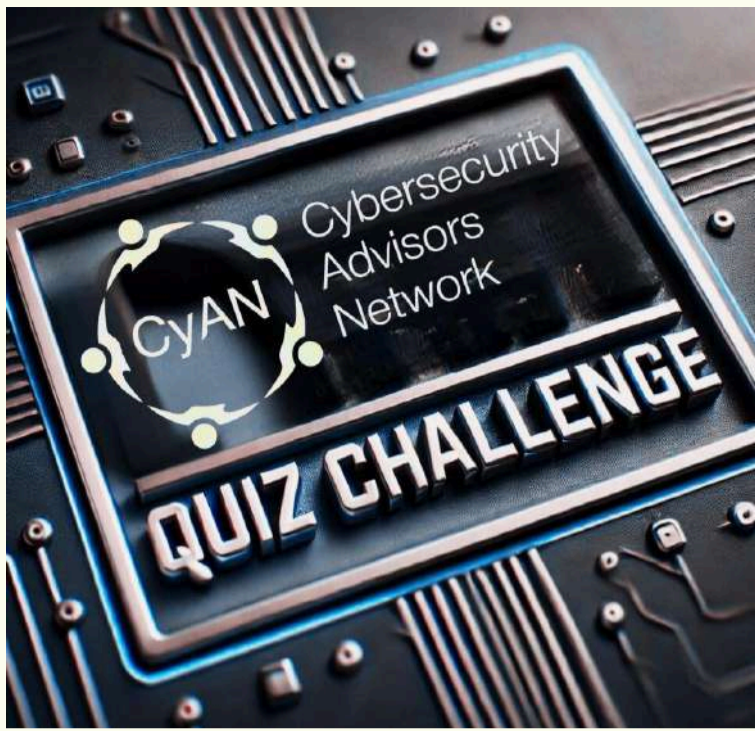
28. Joint Letter on Swedish Data Storage and Access to Electronic Information Legislation **Original Source: Global Encryption Coalition by Ryan Polk**

CyAN has joined over 20 civil society organisations, privacy advocates, and cybersecurity experts in signing an open letter urging Sweden to reconsider its proposed legislation on data storage and access to electronic information.

The signatories warn that the bill threatens to undermine end-to-end encryption, erode user privacy, and weaken trust in digital services—setting a troubling precedent across the EU.

The letter calls for transparent legislative processes, meaningful stakeholder consultation, and strong safeguards that uphold secure communications, democratic values, and international human rights obligations.

CyberSecurity Advisors Network



CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Round One of the Quarterly #CyANQuiz Challenge is officially in the books—congrats to those who took the plunge!

Missed it? Oof. You're going to have to wait for Round Two to redeem yourself... but don't worry, it's coming soon.

- ◆ **30 Questions. Timed. No second chances.**

- ◆ **Based on Recent Cybersecurity News & Events**

- 💡 **Why Play? Bragging rights. Community glory.**

Actual prizes. And the satisfaction of knowing you're sharper than your peers (well, most of them).

This isn't just a quiz—it's a year-long leaderboard battle to find CyAN's sharpest minds.

So keep reading (In)Securities, start prepping... and next time, don't miss your shot at the cyber crown!



ANALYSIS:

29. Groucho's Wit, Cloud Complexity, and the Case for Consistent Security Policy **Original Source: SecurityWeek by Joshua Goldfarb**

A witty comparison to Groucho Marx sets the stage for a deeper look at how inconsistent security policies in cloud environments create risk and confusion.

As hybrid and multi-cloud infrastructures expand, the need for unified governance across teams, tools, and service providers becomes critical. Without this alignment, organisations risk misconfigurations, regulatory breaches, and unclear accountability.

The analysis makes a strong case for moving away from patchwork approaches and toward cohesive security policies that reduce complexity, improve visibility, and support long-term resilience in increasingly dynamic environments.

CyberSecurity Advisors Network



ANALYSIS:

30. How Democratized Development Creates a Security Nightmare

Original Source: Dark Reading by Fernando José Karl

The rise of low-code, no-code, and citizen development has empowered teams across organisations to build and deploy software faster than ever—but it's also vastly expanded the attack surface.

Without strong oversight, these platforms can introduce insecure code, misconfigured APIs, and unmonitored applications that evade traditional security controls.

Shadow IT flourishes when innovation outpaces governance. To truly benefit from democratised development, organisations must pair creative freedom with proper access controls, visibility, and a shared responsibility model that supports security at every layer.

CyberSecurity Advisors Network



ANALYSIS:

31. Experts Optimistic About Secure by Design Progress

Original Source: Dark Reading by Arielle Waldman

Security leaders are cautiously optimistic that the Secure by Design movement is gaining traction, but meaningful change remains a work in progress.

While more vendors are integrating security earlier in the development lifecycle, inconsistencies in implementation and accountability still undermine progress.

Regulatory pressure and industry guidance are helping steer the shift, but true transformation requires a cultural pivot—one where usability, performance, and security aren't competing priorities.

Embedding security from the start isn't just good practice; it's becoming a baseline expectation.

CyberSecurity Advisors Network



ANALYSIS:

32. Machine identity a key priority for organisations' security strategies: CyberArk **Original Source: itNews**

With the explosion of connected devices, APIs, and automated workflows, managing machine identities has become a cornerstone of modern cybersecurity.

Organisations are shifting focus from just securing users to securing the non-human actors that now dominate network traffic.

Poorly managed machine credentials can lead to privilege escalation, data leaks, and blind spots across digital ecosystems.

The growing recognition of this risk is prompting more businesses to invest in machine identity management, integrating it into broader strategies for visibility, control, and trust in increasingly complex environments.


CyberSecurity Advisors Network



CyAN CyAN Members Op Eds, Articles, etc

At the recent CyAN APAC Sydney event, our VP Kim Chandler McDonald questioned the future of end-to-end encryption in light of increasing geopolitical and legislative pressures. Will global unity on encryption persist, or are we veering towards fragmentation?



 **Highlighting the panel was Peter Evans, CyAN member and CISO at the NSW Police Force, who stressed:**



- ✓ The reason the internet has been a success is because of End-to-End Encryption.**
- ✓ The foundational role of End-to-End Encryption in establishing trust.**
- ✓ The vulnerability of digital banking, e-commerce, and personal data security without robust encryption.**
- ✓ Despite regulatory challenges, the evolution and indispensability of encryption in safeguarding our digital world.**

CyAN Member Spotlight

Łukasz Gawron

Championing Cybersecurity in Poland

Just returned from the Forum INCYBER Europe (FIC) in France and the Secure International Summit in Bydgoszcz, Łukasz Gawron, CEO of #CyberMadeInPoland, offers a fresh perspective on Poland's increasing influence as a cybersecurity leader.



As Europe intensifies efforts in cybersecurity collaboration and ecosystem development, Poland is actively increasing its defence budget to over 4% of GDP and fostering growth in startups focused on dual-use and defence technologies.

Highlighting key points from the CEE Startups 2025 report, Łukasz advocates for Poland's potential to modernise its defence and strengthen digital security. He supports the creation of dedicated accelerators and investment funds to propel the sector forward.

For those keen on understanding the dynamics of European cybersecurity and Poland's strategic role, the upcoming **CYBERSEC EXPO & FORUM 2025** in Kraków is the place to be. This event will explore critical areas like startup funding, international cooperation, and regulatory frameworks that are pivotal in shaping the future of cybersecurity.

Join Łukasz in Kraków to engage, exchange ideas, and drive advancements in regional and global cybersecurity initiatives. Let's collaborate to forge a secure digital future.



CyAN Member's News:

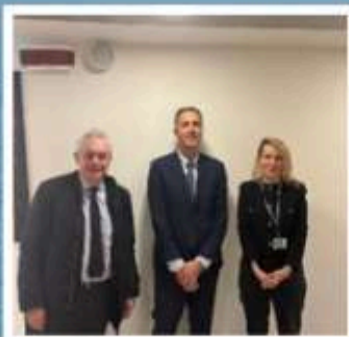
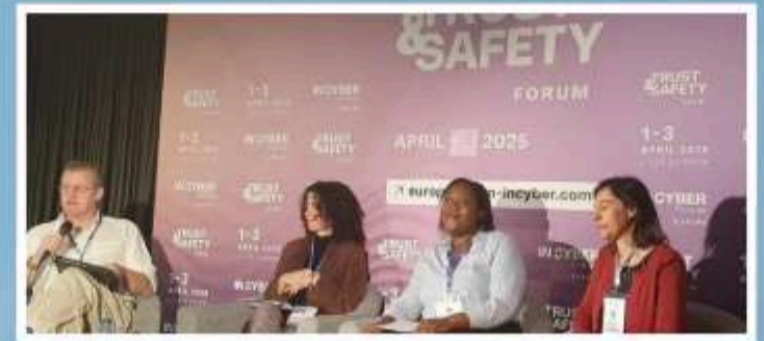
CyAN thrives because of the incredible talent, leadership, and dedication of our members, and we are proud to see them shaping the future of cybersecurity on a global stage! 🚀❤️



CyAN members from across Europe (and the US!) made a strong showing at the 2025 InCyber Forum and Trust & Safety events in Lille!

From panels to networking, our community brought energy, insight, and collaboration to the global stage.

Great days of connection and impact!





UPCOMING CyAN and CyAN Partner EVENTS:

- **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**





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

