CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #143

Cybersecurity Advisors Network

CyAN

NEWS:

1.Cybersecurity CEO accused of running malware on hospital PC blabs about it on LinkedIn

Original Source: The Register by Brandon Vigliarolo

The CEO of cybersecurity firm Securolytics, already charged with planting malware on hospital systems, has drawn fresh attention by posting about the incident on LinkedIn. In his post, he appeared to downplay the seriousness of the allegations, framing the situation as a misunderstanding. Legal experts say public commentary could complicate his defence, particularly in a case involving critical infrastructure and patient safety. The LinkedIn post has also raised industry concerns about professionalism and trust, highlighting how public missteps during legal proceedings can worsen reputational fallout and damage the broader credibility of the cybersecurity sector.

CyAN Cybersecurity Advisors Network

NEWS:

2. Cybersecurity experts issue response to Trump order targeting Chris Krebs, SentinelOne

Original Source: Cyberscoop by Greg Otto

Cybersecurity experts have condemned a recent executive order from Donald Trump that threatens Chris Krebs, former director of CISA, and SentinelOne, a leading security vendor. The order accuses Krebs and the company of undermining election security, despite widespread consensus among security professionals that Krebs acted to protect electoral integrity. Industry leaders warn that politicising cybersecurity not only endangers public trust but also discourages critical private-sector collaboration. Experts stress that election security should remain a nonpartisan priority, insulated from political attacks that could weaken democratic resilience.

NEWS:

3. Marks & Spencer breach linked to Scattered Spider ransomware attack

Original Source: BleepingComputer by Lawrence Abrams

Marks & Spencer’s recent cyber disruption has now been linked to the notorious Scattered Spider ransomware group, according to new reports. The attack, which forced M&S to suspend online orders, is believed to have targeted a third-party supplier, enabling access to internal systems. Scattered Spider is known for sophisticated social engineering tactics that bypass traditional defences. Experts warn that supply chain vulnerabilities remain a major weak point for large organisations, urging companies to strengthen third-party risk management and incident response capabilities to limit collateral damage from indirect attacks.

CyAN Cybersecurity Advisors Network

NEWS:

4. House passes bill to study routers' national security risks

Original Source: Cyberscoop by Matt Braken

The US House of Representatives has passed a bipartisan bill directing federal agencies to study the national security risks posed by foreign-made routers and network equipment. Lawmakers cite growing concerns that compromised devices could be used for espionage, data theft, or critical infrastructure sabotage. The study aims to assess vulnerabilities in both consumer and enterprise networks and recommend mitigation strategies. Experts welcome the move, warning that as routers form the backbone of internet connectivity, backdoors or hidden exploits in these devices could have cascading consequences across industries and national defence.

Cybersecurity Advisors Network

NEWS:

5. Hitachi Vantara takes servers offline after Akira ransomware attack

Original Source: BleepingComputer by Sergiu Gatlan

Hitachi Vantara has confirmed it took several servers offline after falling victim to an Akira ransomware attack. Although the company says core business operations remain unaffected, investigations are ongoing to assess the extent of data exposure. Akira has been linked to a wave of attacks targeting major enterprises with double-extortion tactics — encrypting files while threatening to leak stolen data. Experts warn that even when operational disruptions appear limited, reputational damage, regulatory scrutiny, and long-term trust issues can follow. Organisations are urged to bolster ransomware defences and crisis response planning.

CyAN Cybersecurity Advisors Network

NEWS:

6. Over 1,200 SAP NetWeaver servers vulnerable to actively exploited flaw

Original Source: BleepingComputer by Bill Toulas

SAP has urgently patched a critical vulnerability in its NetWeaver platform after reports of active exploitation surfaced. The flaw allows unauthenticated attackers to execute arbitrary code, putting enterprise systems at significant risk. Although SAP moved quickly to issue fixes, experts warn that exploitation likely began weeks before detection, raising concerns about hidden breaches. Given NetWeaver's central role in powering financial, logistics, and manufacturing systems globally, organisations are urged to apply patches immediately, audit for signs of compromise, and strengthen monitoring around critical SAP environments.

Cybersecurity Advisors Network

NEWS:

7. Cybersecurity vendors are themselves under attack by hackers, SentinelOne says

Original Source: Cyberscoop by Tim Starks

SentinelOne has warned that cybersecurity vendors are increasingly becoming direct targets for hackers, who see them as high-value entry points into broader digital ecosystems. Attackers are exploiting trust relationships, software supply chains, and vendor access privileges to amplify the impact of breaches. Experts caution that security firms must not assume immunity from attack; instead, they should model themselves as prime targets and implement rigorous internal defences. The warning comes amid rising concerns that successful compromises of security providers could ripple across thousands of downstream clients and critical sectors.

Cybersecurity Advisors Network

NEWS:

8. VeriSource now says February data breach impacts 4 million people

Original Source: BleepingComputer by Bill Toulas

VeriSource has updated its disclosure regarding a February data breach, now confirming that personal information belonging to 4 million individuals was compromised. Exposed data includes names, Social Security numbers, and medical information, making victims vulnerable to identity theft and fraud. The breach highlights the ongoing risks associated with third-party data processors, especially those handling sensitive health and financial records. Experts stress that organisations must demand stronger security assurances from vendors, implement stricter data minimisation practices, and prepare robust breach response plans to protect affected individuals.

9. DragonForce expands ransomware model with white-label branding scheme

Original Source: BleepingComputer by Ionut Ilascu

DragonForce has launched a white-label ransomware offering, enabling affiliates to customise malware payloads with their own branding and messaging. This innovation lowers technical barriers for cybercriminals, allowing even inexperienced actors to carry out ransomware attacks at scale. Experts warn that the white-label model could dramatically expand the ransomware ecosystem, making attribution harder and encouraging a flood of smaller, harder-to-track campaigns. By fragmenting responsibility while multiplying attacks, DragonForce's model represents a dangerous evolution in ransomware-as-a-service operations.

CyAN Cybersecurity Advisors Network

NEWS:

10. WooCommerce admins targeted by fake security patches that hijack sites

Original Source: BleepingComputer by Bill Toulas

WooCommerce administrators are being targeted by a new phishing campaign that impersonates WordPress security advisories, urging urgent patching. Those who follow the fake instructions inadvertently install malware that grants attackers full control over their online stores, allowing theft of customer data, payment skimming, and malicious redirects. Given WooCommerce’s dominance in the e-commerce space, the scale of potential damage is significant. Experts stress the critical importance of verifying updates through official dashboards, avoiding emailed prompts, and enforcing strict access controls to reduce the risk of future compromise.

Cybersecurity Advisors Network

NEWS:

11. Amid CVE funding fumble, 'we were mushrooms, kept in the dark,' says board member

Original Source: The Register by Jessica Lyons

Following the near-collapse of CVE.org due to funding failures, board members have criticised the leadership for leaving them uninformed, likening themselves to "mushrooms, kept in the dark." The crisis exposed how vulnerable cybersecurity's core infrastructure can be when reliant on unstable funding and ad hoc governance. With CVE listings forming the backbone of vulnerability management worldwide, experts warn that future resilience demands formal oversight, diversified support, and a commitment to transparency. Without these, the fragility revealed in this incident could easily repeat — with far greater consequences.

Cybersecurity Advisors Network

NEWS:

12. More Ivanti attacks may be on horizon, say experts who are seeing 9x surge in endpoint scans

Original Source: The Register by Connor Jones

Security researchers are warning of a ninefold surge in scans targeting Ivanti Connect Secure and Policy Secure devices, raising fears of an imminent wave of new attacks. Despite patches issued earlier this year, many organisations remain vulnerable — and experts caution that even patched devices may harbour persistence mechanisms left by earlier compromises. Attackers are aggressively probing for weaknesses, suggesting that opportunistic exploitation is already underway. Organisations are urged to assume breach, conduct thorough forensic reviews, and monitor closely for signs of stealthy lateral movement within their networks.

13. Mobile provider MTN says cyberattack compromised customer data

Original Source: BleepingComputer by Bill Toulas

Africa's largest mobile provider, MTN, has confirmed a cyberattack compromised sensitive customer information, including phone numbers and SIM details. The breach affects its Namibian operations and may enable future attacks such as SIM swapping or identity fraud. MTN says it is working with regulators and has enhanced security measures, but the incident again exposes the vulnerability of telecoms — critical infrastructure that doubles as a treasure trove for cybercriminals. Regulatory scrutiny and customer backlash are now expected to intensify.

CyAN Cybersecurity Advisors Network

NEWS:

14. Vehicles Face 45% More Attacks, 4 Times More Hackers

Original Source: Dark Reading by Nate Nelson

Cyberattacks against connected vehicles have surged by 45% over the past year, with the number of attackers involved quadrupling. As cars increasingly function as mobile data hubs — integrating IoT devices, APIs, and over-the-air updates — their digital attack surface continues to expand. Researchers warn that vulnerabilities in vehicle software could lead not just to data theft, but to physical safety risks such as remote hijacking or disabling of critical systems. Without stronger cybersecurity standards and coordinated industry responses, connected vehicles could become a new frontline in cyber warfare and organised crime operations.

Cybersecurity Advisors Network CyAN

NEWS:

15. Gig-Work Platforms at Risk for Data Breaches, Fraud, Account Takeovers

Original Source: Dark Reading by Tatiana Walk-Morris

A new report warns that gig economy platforms are increasingly vulnerable to cyberattacks, with rising incidents of data breaches, account hijackings, and payment fraud. Freelancers often lack access to strong cybersecurity tools or training, making them easy targets for phishing and credential theft. Meanwhile, many platforms prioritise rapid growth over robust security measures, leaving critical vulnerabilities unaddressed. Experts caution that without stronger authentication, data protection, and user education, the gig economy could become a major hunting ground for cybercriminals — jeopardising trust and platform sustainability.

NEWS:

16. All Major Gen-AI Models Vulnerable to ‘Policy Puppetry’ Prompt Injection Attack

Original Source: SecurityWeek by Ionut Arghire

Researchers have discovered that all major generative AI models are vulnerable to a new attack method called "policy puppetry," where prompt injections trick systems into bypassing their safety controls. By subtly manipulating inputs, attackers can coerce models into producing prohibited content without triggering safeguards. The findings raise urgent concerns about the reliability of AI safety mechanisms, especially as companies race to integrate large language models into sensitive domains. Experts warn that unless defences are fundamentally rethought, AI systems could be weaponised against the very ethical frameworks designed to govern them.

CyAN Cybersecurity Advisors Network

NEWS:

17. Researchers Identify Rack::Static Vulnerability Enabling Data Breaches in Ruby Servers

Original Source: The Hacker News by Ravie Lakshmanan

Security researchers have identified a critical vulnerability in Rack::Static, a popular Ruby middleware, that could allow attackers to access and exfiltrate sensitive files stored on affected servers. The flaw stems from improper handling of URL-encoded paths, enabling directory traversal attacks that bypass normal access controls. With Rack used widely across Ruby applications, the risk of data breaches is significant, particularly for web apps handling personal or financial information. Experts urge developers to patch immediately, review server configurations, and audit logs for signs of unauthorised file access attempts.

18. Anthropic finds alarming 'emerging trends' in Claude misuse report

Original Source: ZDNet by Radhika Rajkumar

Anthropic’s latest report reveals troubling patterns of misuse in its Claude AI models, including rising attempts to bypass safeguards, generate harmful content, and assist in cybercriminal activities. The study highlights how threat actors are rapidly adapting their techniques to manipulate AI outputs, often using prompt chaining and obfuscation to evade detection. While Anthropic has tightened safety measures, the findings underscore the escalating arms race between AI developers and malicious users. Experts warn that as generative AI adoption grows, ongoing vigilance and dynamic defences will be essential to prevent widespread abuse.

Cybersecurity Advisors Network

NEWS:

19. Darcula adds AI to its DIY phishing kits to help would-be vampires bleed victims dry

Original Source: The Register by Jessica Lyons

The Darcula phishing-as-a-service operation has upgraded its DIY kits by integrating AI tools to generate more convincing phishing messages in multiple languages. By automating and localising scams, Darcula is making it easier for low-skilled cybercriminals to launch highly targeted attacks at scale. Researchers warn that AI-enhanced phishing campaigns lower the barrier to entry even further, increasing the volume, sophistication, and success rates of scams. As adversaries embrace generative AI, experts stress the need for better user education, advanced email security controls, and constant adaptation to evolving threat tactics.

Cybersecurity Advisors Network

NEWS:

20. ‘SessionShark' ToolKit Evades Microsoft Office 365 MFA | Dark Reading by Kristina Beek

Original Source: Dark Reading by Kristina Beek

Security researchers have uncovered SessionShark, a new phishing toolkit designed to bypass Microsoft Office 365 multi-factor authentication by stealing active session tokens. Instead of capturing passwords, SessionShark intercepts authenticated sessions, allowing attackers to impersonate users without triggering additional security checks. This tactic makes traditional MFA protections less effective against modern phishing attacks. Experts warn that session hijacking tools like SessionShark are part of a broader shift toward more sophisticated credential theft techniques, underscoring the urgent need for continuous monitoring, behavioural analytics, and stronger session management practices.

CyAN Cybersecurity Advisors Network

NEWS:

21. Assassin's Creed maker faces GDPR complaint for forcing single-player gamers online

Original Source: The Register by Brandon Vigliarolo

Ubisoft is facing a GDPR complaint after allegedly forcing players of single-player games like Assassin's Creed to remain constantly online, raising concerns over unnecessary data collection. Privacy advocates argue that mandating internet connections for solo gameplay violates European data protection laws by harvesting player data without sufficient justification. Ubisoft contends that online features enhance user experience, but critics say the move prioritises data monetisation over user rights. The case could set a major precedent for how gaming companies balance convenience, monetisation, and compliance in an increasingly connected market.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

22. Interlock ransomware claims DaVita attack, leaks stolen data

Original Source: BleepingComputer by Bill Toulas

The Interlock ransomware group has claimed responsibility for a cyberattack on healthcare giant DaVita, leaking stolen data after the company reportedly refused to meet ransom demands. While DaVita has yet to confirm the full extent of the breach, leaked materials appear to include sensitive patient information, intensifying concerns around the targeting of healthcare providers. Experts warn that ransomware attacks on critical sectors like healthcare carry devastating consequences — from operational shutdowns to life-threatening delays in care — and highlight the urgent need for stronger defences and sector-specific cybersecurity standards.

23. Verizon DBIR Flags Major Patch Delays on VPNs, Edge Appliances

Original Source: Security Week by Ryan Naraine

The 2025 Verizon Data Breach Investigations Report (DBIR) highlights a troubling trend: widespread delays in patching vulnerabilities in VPNs and edge devices. Attackers are increasingly exploiting these internet-facing systems, often months after patches become available. The report stresses that lagging updates, especially on critical infrastructure, are giving threat actors easy footholds for ransomware attacks, espionage, and supply chain compromises. Experts urge organisations to prioritise patch management for edge technologies, warning that failure to do so leaves businesses dangerously exposed to preventable breaches.

Cybersecurity Advisors Network

NEWS:

24. ‘Warning sign’: Espionage driving APAC cyber surge

Original Source: InnovationAus by Trish Everingham

A new report warns that cyberattacks across the Asia-Pacific region are increasingly being driven by state-linked espionage campaigns, not just financial crime. Researchers point to a sharp rise in cyber intrusions targeting government agencies, critical infrastructure, and defence contractors, with many attacks attributed to advanced persistent threat (APT) groups. The shift toward espionage-focused operations is seen as a warning sign of escalating geopolitical tensions being played out in cyberspace. Experts urge APAC nations to strengthen public-private partnerships and invest in threat intelligence to better defend against sophisticated nation-state threats.

CyAN Cybersecurity Advisors Network

ANALYSIS:

25. The Trouble with AI in Cybersecurity - Part 5: Ethics on Autopilot

Original Source: PrivID (Substack)

This instalment of The Trouble with AI in Cybersecurity warns that as AI becomes more embedded in cyber defences, ethical considerations are being dangerously sidelined. Developers and security teams often prioritise speed, automation, and competitive advantage over transparency, fairness, or accountability. The article argues that without deliberate ethical oversight, AI systems risk entrenching biases, escalating surveillance, and making critical decisions without human context. Experts stress that integrating ethical frameworks early — not retrofitting them later — is essential if AI is to enhance cybersecurity without undermining trust, privacy, and societal values.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

ANALYSIS:

26. Mobile Applications: A Cesspool of Security Issues

Original Source: Dark Reading by Robert Lemos

A new study highlights the persistent and worsening security problems plaguing mobile applications, particularly those handling sensitive user data. Researchers found that many apps suffer from insecure data storage, weak encryption practices, improper authentication, and excessive permissions — creating a massive, exploitable attack surface. Despite growing regulatory scrutiny, developers often prioritise speed and user experience over security, leaving critical vulnerabilities unaddressed. Experts warn that unless mobile app security becomes a design priority rather than an afterthought, breaches and privacy violations will continue to escalate across industries.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

27. M-Trends 2025: State-Sponsored IT Workers Emerge as Global Threat

Original Source: Dark Reading by Kevin Townsend

Mandiant’s M-Trends 2025 report highlights a growing threat: state-sponsored IT workers embedded in legitimate companies to quietly enable cyber espionage. Instead of relying solely on external attacks, nation-states are placing operatives inside technology firms, defence contractors, and critical infrastructure providers. These insiders can exfiltrate sensitive data, alter system configurations, and create long-term access points without triggering alarms. Experts warn that traditional cybersecurity defences focused on perimeter threats are insufficient against this tactic, urging organisations to enhance insider threat monitoring and zero-trust security models.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

28. Inside the Verizon 2025 DBIR: Five Trends That Signal a Shift in the Cyber Threat Economy

Original Source: SecurityWeek by Danelle Au

The 2025 Verizon DBIR outlines five major trends reshaping the cyber threat economy, including the rise of faster ransomware attacks, increased targeting of third parties, and the growing exploitation of human error. The report notes that attackers are focusing less on initial breaches and more on rapid monetisation, supply chain infiltration, and leveraging credential theft. Experts highlight that defensive strategies must evolve accordingly, emphasising speed, resilience, and deeper scrutiny of partner ecosystems. In a shifting landscape, success will depend on anticipating attacker priorities, not just reacting to breaches.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

29. Why NHIs Are Security's Most Dangerous Blind Spot

Original Source: The Hacker News

Non-human identities (NHIs) — such as API keys, service accounts, and machine credentials — have exploded in number but often lack proper oversight, making them one of cybersecurity’s most dangerous blind spots. Unlike human users, NHIs are rarely monitored closely, yet they frequently have broad access to critical systems and sensitive data. Attackers who compromise these identities can move laterally across networks with little resistance. Experts warn that without stronger governance, automated credential management, and real-time monitoring, organisations will remain dangerously exposed to breaches originating from overlooked machine identities.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

ANALYSIS:

30. Navigating Regulatory Shifts & AI Risks

Original Source: Dark Reading by Arnaud Treps

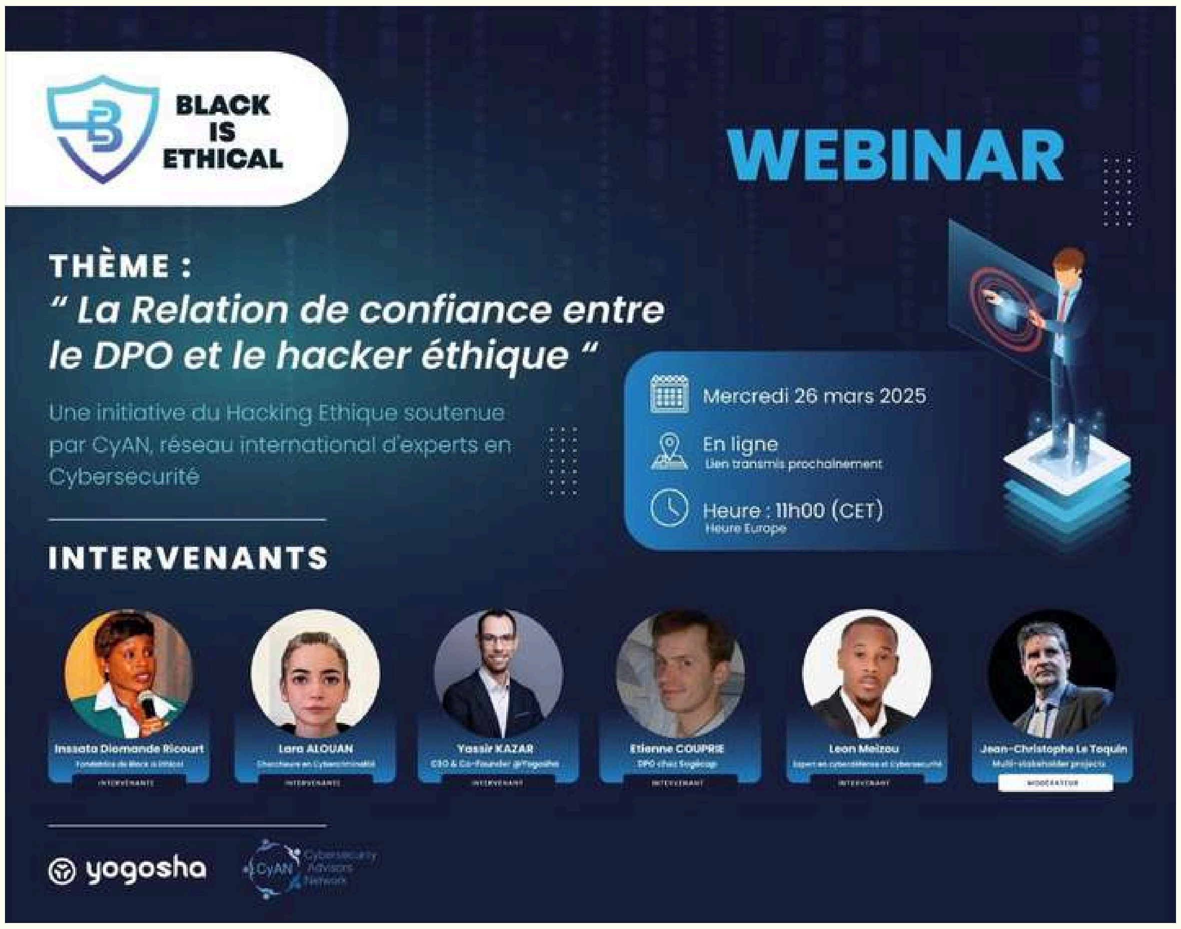
As AI adoption accelerates, organisations face mounting challenges from shifting regulatory landscapes and emerging cyber risks. Governments worldwide are introducing new laws targeting AI transparency, accountability, and data protection — while threat actors are increasingly weaponising AI tools to automate attacks. Experts caution that businesses must move beyond compliance checklists, embedding proactive governance frameworks that anticipate both regulatory expectations and evolving threat vectors. Those that treat cybersecurity and AI ethics as strategic imperatives, rather than reactive burdens, will be better positioned to adapt and thrive.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN Member's News:

Comment instaurer une relation de confiance entre le Data Protection Officer (DPO) et le Hacker Éthique ?



BLACK IS ETHICAL

WEBINAR

THÈME :
" La Relation de confiance entre le DPO et le hacker éthique "

Une initiative du Hacking Ethique soutenue par CyAN, réseau international d'experts en Cybersécurité

Mercredi 26 mars 2025

En ligne
Lien transmis prochainement

Heure : 11h00 (CET)
Heure Europe

INTERVENANTS

Inssata Diomande Ricourt	Lara ALOUAN	Yassir KAZAR	Etienne COUPRIE	Leon Meizou	Jean-Christophe Le Toquin
Fondatrice de Black is Ethical	Chercheure en Cybercriminalité	CEO & Co-founder @Yogosha	DPO chez Sogécap	Expert en cyberdéfense et cybersécurité	Multi-stakeholder projects
INTERVENANTE	INTERVENANTE	INTERVENANT	INTERVENANT	INTERVENANT	MODÉRATEUR

yogosha

CyAN Cybersecurity Advisors Network

Ce webinaire proposé par Black is Ethical le 26 mars dernier croise les regards de professionnels issus des domaines de la protection des données, de la sécurité offensive et de la gouvernance numérique. A été soulignée l'importance d'institutionnaliser les échanges entre fonctions conformité et cybersécurité offensive, notamment à travers des chartes d'engagement, des clauses contractuelles spécifiques et des procédures intégrées de gestion des incidents.

CyAN Cybersecurity Advisors Network

CyAN Member's News:

CyAN Global Vice President Kim Chandler McDonald has, for the fourth consecutive year, served as a judge for the Australian Space Awards, recognising outstanding leadership, innovation, and resilience across Australia's dynamic space sector.

Kim tells us that bringing a cybersecurity perspective to the judging is vital because, as she puts it, "Space may be the final frontier, but without securing the digital foundations that support it — from mission-critical systems to satellite communications — we risk undermining every breakthrough we achieve. Cybersecurity isn't optional; it's the bedrock of trust, innovation, and future exploration." Winners will be announced at a special celebration on May 29th at Ilumina, Sydney.

CyAN Cybersecurity Advisors Network

CyAN Member’s News:

Michael do Rozario Named Finalist for 2025 Lawyers Weekly Partner of the Year Awards

We are proud to share that Michael do Rozario, Partner at Corrs Chambers Westgarth, has been named a finalist in the prestigious Lawyers Weekly Partner of the Year Awards 2025.

Michael is recognized in two categories that reflect his deep commitment and passion: Cyber Partner of the Year and Pro Bono Partner of the Year. His achievements highlight outstanding contributions to both cybersecurity law and community service through pro bono work.

Congratulations, Michael, on this well-deserved recognition!

CyAN Cybersecurity Advisors Network

UPCOMING CyAN and CyAN Partner EVENTS:

- 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.io
- 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

MaTeCC
3rd edition
Morocco: A Trusted Ground for Cybersecurity and Personal Data Protection
Tuesday 24 & Wednesday 25 June, 2025
Dawliz Hotel, Rabat - Morocco

CyAN Cybersecurity Advisors Network

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