CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #132

NEWS:

Elon Musk’s Starlink could be used to transmit Australian election voting results

Original Source: The Guardian by Josh Taylor

Elon Musk's satellite internet service, Starlink, is being considered as a potential method to transmit voting results in Australian elections.

This proposal aims to leverage Starlink's extensive network to ensure reliable and secure communication of electoral data, especially in remote and rural areas where traditional internet services might not be as effective.

The initiative highlights the growing influence of private satellite networks in critical public sectors and raises questions about the security implications of depending on commercial space infrastructure for national electoral processes.

CyberSecurity Advisors Network

NEWS:

2. Worried about DeepSeek? Turns out, Gemini and other US AIs collect more user data

Original Source: ZDNet by Matene Toure

Recent analysis reveals that, contrary to popular concern, AI systems like Gemini are collecting more user data than DeepSeek.

This comparative insight into U.S. AI technologies underscores the extensive data collection practices prevalent in the industry, often surpassing those of widely debated systems.

The report highlights the need for greater transparency and regulatory scrutiny regarding how personal data is harvested and utilized by AI technologies. It calls for consumers and policymakers to reconsider the balance between technological advancement and privacy rights, emphasising the importance of establishing clear data governance frameworks.

CyberSecurity Advisors Network

NEWS:

3. Car Exploit Allows You to Spy on Drivers in Real Time

Original Source: Dark Reading by Nate Nelson

A newly discovered vulnerability in modern car technology allows for real-time spying on drivers, exposing a significant privacy risk.

This exploit targets the communication systems embedded within vehicles, enabling unauthorised access to live audio and location tracking without the driver's knowledge.

The exposure of such a flaw highlights the increasing security concerns as automobiles become more connected and technologically sophisticated.

Security experts are urging car manufacturers to enhance their cybersecurity measures and are advising drivers to be aware of the potential for such breaches and to seek updates and fixes that may mitigate these risks.

CyberSecurity Advisors Network

NEWS:

4. Inside Elon Musk’s ‘Digital Coup’

Original Source: Wired by Makena Kelly, David Gilbert, Vittoria Elliott, Kate Knibbs, Dhruv Mehrotra, Dell Cameron, Tim Marksman, Leah Geiger & Zoe Schiffer

An in-depth investigation reveals how Elon Musk’s inner circle has gained extraordinary, seemingly unfettered access to vast amounts of sensitive U.S. citizen data, including social media, biometric, financial, and government-related records.

Unlike officials who undergo stringent security vetting, these individuals—operating with no formal oversight—wield significant control over systems affecting national infrastructure, AI development, and online platforms.

The report raises critical questions: Why do private actors with no public accountability have access to such vast datasets? And without transparency or regulation, who ensures this data isn’t misused? The findings underscore the urgent need for scrutiny and safeguards to prevent a small, unelected group from exerting unchecked influence over critical digital ecosystems.

CyberSecurity Advisors Network

NEWS:

5. Dems ask federal agencies for reassurance DOGE isn't feeding data into AI willy-nilly

Original Source: The Register by Brandon Vigliarolo

US Democratic lawmakers are seeking reassurances from federal agencies regarding the use of DOGE, a data aggregation tool, amid concerns about its data handling practices and potential privacy implications.

This inquiry stems from worries that DOGE could be indiscriminately funnelling vast amounts of user data into AI systems without sufficient oversight or adherence to privacy standards.

The request highlights the broader issues of data protection and transparency in government technology deployments, pressing for clear policies that ensure data is managed responsibly and ethically in line with citizens' privacy rights.

CyberSecurity Advisors Network

NEWS:

6. ASIC sues FIIG Securities for cyber security failures

Original Source: itNews

The Australian Securities and Investments Commission (ASIC) has initiated legal action against FIIG Securities, accusing the firm of inadequate cybersecurity measures that failed to protect sensitive client data.

This lawsuit marks a significant move by the regulatory body to enforce stricter cybersecurity compliance among financial institutions.

ASIC's action underscores the growing importance of robust cyber defences in the financial sector, highlighting the legal and reputational risks companies face when they neglect cybersecurity.

The case serves as a stark reminder for businesses to prioritize the security of their digital infrastructures to safeguard against potential breaches and regulatory penalties.

CyberSecurity Advisors Network

NEWS:

7. GitHub Uncovers New ruby-saml Vulnerabilities Allowing Account Takeover Attacks

Original Source: The Hacker News by Ravie Lakshmanan

GitHub has identified critical vulnerabilities in the ruby-saml authentication library, which could allow attackers to carry out account takeover attacks.

These security flaws make it possible for cybercriminals to bypass authentication steps and gain unauthorised access to user accounts across various platforms that use this library.

The discovery has prompted urgent calls for developers to update their applications with the latest patched version of ruby-saml to prevent potential exploits.

This incident highlights the ongoing challenges in securing authentication mechanisms and the importance of maintaining up-to-date security practices in software development.

CyberSecurity Advisors Network

NEWS:

8. Microsoft Warns of Hospitality Sector Attacks Involving ClickFix

Original Source: SecurityWeek by Eduard Kovacs

Microsoft has issued a warning about a series of targeted cyberattacks against the hospitality sector, involving a malicious software called ClickFix.

The attacks are primarily focused on hotels, resorts, and other entities within the industry, exploiting vulnerabilities to steal sensitive information such as customer data and financial records.

ClickFix is deployed through seemingly benign email attachments that, when opened, initiate a chain of malicious activities.

Microsoft's alert emphasises the need for heightened cybersecurity measures in the hospitality industry, particularly in improving email security protocols and training staff to recognise potential cyber threats.

CyberSecurity Advisors Network

NEWS:

9. Apple to appeal against UK government data demand at secret high court hearing

Original Source: The Guardian by Rachel Hall

Apple is set to challenge a UK government request for data in a secret high court hearing, marking a significant clash over privacy and government surveillance powers.

The tech giant's appeal stems from concerns about the implications of such data access for user privacy and the potential setting of a precedent that could affect global operations.

This legal battle underscores the ongoing tension between technology companies and government agencies over access to digital information, highlighting the delicate balance between national security interests and individual privacy rights.

CyberSecurity Advisors Network

NEWS:

10. Legislative push for child online safety runs afoul of encryption advocates (again)

Original Source: Cyberscoop by Derek B. Johnson

A legislative effort aimed at enhancing online safety for children has once again clashed with encryption advocates.

The proposed measures seek to implement stricter controls on digital platforms to protect minors, but they have raised concerns about potentially undermining end-to-end encryption.

Encryption advocates argue that while protecting children is paramount, the security and privacy of all users must not be compromised.

This ongoing debate highlights the tension between safeguarding vulnerable internet users and maintaining robust privacy protections, emphasising the challenge of balancing these critical interests.

CyberSecurity Advisors Network

NEWS:

11. DeepSeek can be gently persuaded to spit out malware code

Original Source: The Register by Connor Jones

The AI tool DeepSeek, known for its data processing capabilities, has been found vulnerable to manipulation that can result in the generation of malware code.

Researchers demonstrated that with specific inputs, DeepSeek could be "gently persuaded" to produce harmful code, highlighting a significant security concern.

This revelation puts a spotlight on the potential dangers of AI systems when exploited by malicious actors.

It raises crucial questions about the ethical development and security hardening of AI technologies, urging developers to implement more robust safeguards against such vulnerabilities.

CyberSecurity Advisors Network

NEWS:

12. NIST Finalizes Differential Privacy Rules to Protect Data

Original Source: Dark Reading by Arielle Waldman

The US National Institute of Standards and Technology (NIST) has finalized its guidelines on differential privacy, establishing a framework designed to enhance data protection.

This move aims to provide organisations with a method to share useful information while ensuring that individual data remains private and secure.

The new rules advocate for incorporating differential privacy techniques into data analytics processes, effectively minimising the risk of personal data exposure.

These standards represent a significant step forward in the struggle to balance data utility and privacy, urging companies to adopt these practices to safeguard sensitive information.

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:

13. Meta Warns of FreeType Vulnerability (CVE-2025-27363) With Active Exploitation Risk

Original Source: The Hacker News by Ravie Lakshmanan

Meta has issued a warning about a critical vulnerability in the FreeType font rendering library, identified as CVE-2025-27363, which is currently at risk of active exploitation.

This vulnerability allows attackers to execute arbitrary code through specially crafted fonts. Given the widespread use of FreeType in various software applications, the potential impact is significant.

Meta urges developers and system administrators to apply the available patches immediately to mitigate the risk and prevent potential breaches that could lead to substantial data loss and system compromise.

CyberSecurity Advisors Network

NEWS:

14. CISA: Medusa ransomware hit over 300 critical infrastructure orgs

Original Source: BleepingComputer by Sergiu Gatlan

The US Cybersecurity and Infrastructure Security Agency (CISA) has reported that Medusa ransomware has compromised over 300 critical infrastructure organisations across various sectors.

This widespread attack underscores the growing threat of ransomware to essential services and national security.

CISA is urging affected organisations to take immediate action to mitigate the damage and prevent further breaches.

The advisory also calls for increased vigilance and enhanced security measures among all organisations to protect against this highly disruptive form of malware, which continues to evolve and find new targets.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

15. Cisco Patches 10 Vulnerabilities in IOS XR

Original Source: XXX

Cisco has released patches for ten vulnerabilities in its IOS XR software, which is widely used in carrier-grade routers and networking equipment.

These vulnerabilities range from high to critical severity and could allow attackers to cause denial of service, execute arbitrary commands, or escalate privileges.

The announcement stresses the importance for network administrators to apply these updates promptly to prevent potential cyber attacks that could disrupt network operations.

Cisco's proactive measures reflect its commitment to maintaining the security and integrity of its products amidst an increasingly complex threat landscape.

CyberSecurity Advisors Network

NEWS:

16. GITLAB Addressed Critical Auth Bypass Flaws in CE AND EE

Original Source: Security Affairs by Pierluigi Paganini

GitLab has successfully addressed critical authentication bypass flaws affecting both its Community Edition (CE) and Enterprise Edition (EE) platforms.

These vulnerabilities posed significant security risks, potentially allowing unauthorised users to gain access to private repositories and sensitive data without proper credentials.

The patches were issued swiftly following the discovery, underscoring GitLab's commitment to user security and the prompt response needed to avert potential data breaches.

Users of both editions are urged to update their systems immediately to ensure they are protected against these exploits.

CyberSecurity Advisors Network

NEWS:

17. Garantex crypto exchange admin arrested while on vacation

Original Source: BleepingComputer by Sergiu Gatlan

A recent legislative push aimed at enhancing online safety for children has once again sparked controversy among encryption advocates.

The proposed measures, which call for increased monitoring and restrictions on digital platforms, are meeting resistance from those who argue that they could undermine end-to-end encryption and infringe on privacy rights.

Advocates for digital privacy assert that while protecting children online is critical, it should not come at the expense of weakening encryption, which secures communications and protects users' data from unauthorised access.

This ongoing debate highlights the challenging balance between safeguarding vulnerable populations and preserving fundamental privacy protections.

CyberSecurity Advisors Network

NEWS:

18. That weird CAPTCHA could be a malware trap - here's how to protect yourself

Original Source: ZDNet by Lance Whitney

A recent report highlights a troubling trend where CAPTCHA tests, commonly used to verify user authenticity, are being manipulated to spread malware.

Cybercriminals are crafting fake CAPTCHA screens that mimic those of legitimate websites to deceive users into downloading malicious software.

This tactic not only compromises the security of the affected devices but also undermines trust in what has been a standard security measure on many online platforms.

The article provides essential tips on how to identify and avoid these fraudulent CAPTCHA tests, emphasising the importance of vigilance and updating security software regularly to protect against such sophisticated cyber threats.

CyberSecurity Advisors Network

NEWS:

19. Zoom Patches 4 High-Severity Vulnerabilities

Original Source: SecurityWeek by Eduard Kovacs

Zoom has addressed four high-severity vulnerabilities that could have allowed attackers to compromise users' devices and breach personal data.

These security flaws were found in various components of the video conferencing software, which if exploited, could enable unauthorised remote code execution and data theft.

The vulnerabilities highlight ongoing challenges in securing widely used communication tools. Zoom's prompt release of patches reflects its commitment to user safety amidst increasing reliance on digital communication platforms.

Users are strongly encouraged to update their software immediately to safeguard against potential cyber-attacks exploiting these issues.

CyberSecurity Advisors Network

NEWS:

20. Chinese cyberspies backdoor Juniper routers for stealthy access

Original Source: BleepingComputer by Bill Toulas

Chinese cyber espionage efforts have escalated with the discovery that state-sponsored hackers have installed backdoors in Juniper network routers.

This strategic move allows for stealthy, long-term access to network traffic, enabling the interception and manipulation of data.

The revelation underscores the sophistication and persistence of cyber threats posed by nation-state actors, particularly targeting critical infrastructure and corporate networks.

The incident has prompted urgent calls for network administrators to conduct thorough security audits and apply necessary patches or countermeasures to mitigate the risk of such covert surveillance activities.

CyberSecurity Advisors Network

NEWS:

21. This is the FBI, open up. China's Volt Typhoon is on your network

Original Source: The Register by Jessica Lyons

The FBI has issued a warning about 'Volt Typhoon,' a sophisticated cyberattack campaign originating from China, targeting U.S. networks.

This initiative involves a series of coordinated attacks designed to infiltrate critical infrastructure and exfiltrate sensitive information.

The urgency of the FBI's alert highlights the significant threat posed by these cyber incursions, which leverage advanced persistent threat (APT) tactics to gain long-term access to targeted systems.

The warning serves as a critical reminder for organisations to bolster their cybersecurity defences and remain vigilant against evolving threats from state-sponsored actors.

CyberSecurity Advisors Network

NEWS:

22. New North Korean Android spyware slips onto Google Play

Original Source: BleepingComputer by Bill Toulas

North Korean hackers have successfully infiltrated Google Play with sophisticated Android spyware, posing a significant threat to users' data privacy.

The spyware, disguised within seemingly legitimate applications, is capable of stealing a wide range of personal information, including contacts, messages, and device data.

This incident highlights the ongoing challenges faced by app stores in preventing the distribution of malicious software and underscores the need for users to be vigilant about the apps they download. It also calls for enhanced security measures by digital platforms to detect and block such threats more effectively.

CyberSecurity Advisors Network

NEWS:

23. Trump Administration Halts Funding for Two Cybersecurity Efforts, Including One for Elections

Original Source: SecurityWeek via Associated Press

The Trump administration has recently halted funding for two significant cybersecurity initiatives, including one specifically aimed at securing election systems.

This decision has sparked concerns among cybersecurity experts and advocates about the potential vulnerabilities in critical infrastructure and the integrity of upcoming elections.

The cessation of these funds raises questions about the commitment to combating cyber threats and maintaining robust security measures at a national level.

Critics argue that this move could leave the United States more exposed to cyberattacks, particularly during sensitive electoral processes.

CyberSecurity Advisors Network

NEWS:

24. Over 400 IPs Exploiting Multiple SSRF Vulnerabilities in Coordinated Cyber Attack

Original Source: The Hacker News by Ravie Lakshmanan

A coordinated cyber attack involving over 400 IP addresses has been exploiting multiple Server-Side Request Forgery (SSRF) vulnerabilities across various online platforms.

This widespread assault highlights a growing trend where attackers manipulate web servers to send requests to internal resources, leading to data breaches and unauthorised access to sensitive information.

The scale and sophistication of this attack underline the urgent need for organisations to enhance their web application security and closely monitor network activity. It also calls for the implementation of stricter security protocols to prevent such vulnerabilities from being exploited.

CyberSecurity Advisors Network

Prepare Your Business Now for NIS 2 Requirements

April 17th Webinar

CyAN partner SoSafe along with Retarus are hosting a webinar dedicated to the challenges of the NIS 2 directive, which imposes new cybersecurity obligations on European businesses and will include essential compliance information for entities.

📅 **March 25, 2025 | 🕒 9:30 AM – 10:30 CET | 💻 Online**

This webinar **(in French)** will cover:
✅ The concrete implications of NIS 2 and key actions to take
✅ Essential steps to secure systems and raise employee awareness
✅ Insights from a CISO on achieving compliance
✅ Practical solutions to meet the new regulatory requirements

Speakers include CyAN members:

- **Garance Mathias** – Partner Lawyer, Mathias Avocats
- **Pierre Noe**l – CISO, Bump
- **Jean-Baptiste Roux** – Awareness Expert, SoSafe

NEWS:

25. US Hasn’t Determined Who Was Behind Cyberattack That Caused Outage on Musk’s X

Original Source: SecurityWeek via Associated Press

Officials have yet to determine who was behind the cyberattack that caused a widespread outage on X (formerly Twitter), raising concerns over the platform’s security and resilience.

The disruption has fuelled speculation about whether state-sponsored hackers or cybercriminal groups were responsible, particularly given the platform's role in global communications.

Experts warn that major online platforms remain attractive targets for large-scale disruptions, highlighting the need for stronger cyber defences, rapid response mechanisms, and greater transparency when high-profile platforms face security incidents.

CyberSecurity Advisors Network

NEWS:

26. UK must pay cyber pros more than its Prime Minister, top civil servant says

Original Source: The Register by Connor Jones

A top UK civil servant has advocated for paying cybersecurity professionals more than the Prime Minister to attract top talent needed for national security.

This proposal highlights the critical demand for skilled cybersecurity personnel amid escalating global cyber threats.

The call for competitive salaries aims to address the growing difficulty in recruiting and retaining cyber experts essential for protecting national infrastructure.

The statement has sparked discussions about prioritising investment in cybersecurity talent to strengthen the nation's defences against increasingly sophisticated cyberattacks.

CyberSecurity Advisors Network

NEWS:

27. Microsoft patches 57 vulnerabilities, including 6 zero-days

Original Source: Cyberscoop by Matt Kapko

Microsoft has released updates to patch 57 vulnerabilities, including six classified as zero-days, which were actively being exploited.

This substantial update covers a broad range of issues across multiple Microsoft products, highlighting the company's ongoing efforts to tighten security defences against increasingly sophisticated cyber threats.

The patched vulnerabilities include those that could allow attackers to execute arbitrary code, gain elevated privileges, and bypass security features.

Users and organisations are urged to apply these updates immediately to protect their systems from potential exploits that could compromise data and operational security.

CyberSecurity Advisors Network

NEWS:

28. Apple discloses zero-day vulnerability, releases emergency patches

Original Source: Cyberscoop by Greg Otto

Apple has disclosed a critical zero-day vulnerability affecting several of its products and has swiftly released emergency patches to address the issue.

This vulnerability, which was being actively exploited, could allow attackers to execute arbitrary code with kernel privileges, posing a severe security risk to users.

The urgency of Apple's response emphasises the potential severity of the exploit and the necessity for users to update their devices immediately to protect against potential data breaches and system takeovers.

This incident highlights the ongoing battle against cyber threats and the importance of timely software updates in maintaining device security.

CyberSecurity Advisors Network

NEWS:

29. ‘Sloppy’ cops flout tech surveillance laws

Original Source: InnovationAus by Joseph Brookes

A recent report criticises law enforcement agencies for their 'sloppy' adherence to technology surveillance laws, accusing them of flouting regulations designed to protect citizens' privacy.

The investigation highlights instances where police have improperly accessed and used surveillance tools, leading to significant concerns about oversight and accountability.

This lax approach to legal compliance not only undermines public trust but also raises serious questions about the effectiveness of current regulatory frameworks in governing the use of advanced surveillance technologies by the police.

CyberSecurity Advisors Network

NEWS:

30. Allstate Insurance sued for delivering personal info on a platter, in plaintext, to anyone who went looking for it

Original Source: The Register by Jessica Lyons

Allstate Insurance is facing a lawsuit after allegedly exposing customers' personal information in plaintext, making it easily accessible to anyone who knew where to look.

The lawsuit claims that highly sensitive data—including names, addresses, and policy details—was left unprotected, violating industry security standards and consumer privacy laws.

Critics argue this represents a severe failure in basic cybersecurity hygiene, especially for an insurer handling vast amounts of private data.

The case underscores the risks of poor data protection practices and raises questions about corporate accountability when personal information is left vulnerable to exploitation.

CyberSecurity Advisors Network

CyAN Members Quick Reminder! #CyANQuiz?

Hey CyAN Cyber Champs,

Are you ready to put your cybersecurity skills to the test? The Quarterly #CyANQuiz Challenge is back on March 31st—and this time, the stakes are even higher!

🔹 30 questions. Timed. No second chances.
🔹 All based on recent cybersecurity news & events—so keep your knowledge sharp!

📅 **Check your inbox** on March 31st for the quiz link—**just click, answer, and climb the leaderboard!**
🏆 Why play? **Challenge yourself, have fun, and compete for awesome prizes** (while proving your cyber dominance).

This isn’t just a quiz—it’s a **year-long battle for bragging rights in the CyAN community!**

Think you’ve got what it takes? Step up and prove it!

ANALYSIS:

31. Strengthening the Human Firewall: Prioritising Mental Health in Cybersecurity Teams

Original Source: IT Security Guru by Jonathan Marnoch

Prioritising mental health is crucial for enhancing the effectiveness and resilience of cybersecurity teams.

Jonathan Marnoch emphasises the need for supportive work environments that recognise the high-stress nature of cyber roles. He suggests implementing mental health strategies like regular wellness checks, mental health days, and accessible support services.

These measures not only improve team well-being but also strengthen their ability to handle security threats.

A comprehensive approach to mental health ensures that professionals remain equipped to uphold strong cybersecurity defences.

For more on this subject check out article 40, "What Happens to Heroes?" – EPISODE #1: The Unsung Heroes of the Digital World from CyAN Member Annet!

ANALYSIS:

32. US must prioritize cybersecurity training for the military's engineers

Original Source: Cyberscoop by Alison King, Annie Fixler and Rear Adm. (Ret.) Mark Montgomery

Addressing the increasing cyber threats requires that the U.S. military prioritize cybersecurity training for its engineers.

This article discusses how bolstering the cyber training regimen for military personnel is essential to protect national security interests. It emphasises the need for a robust educational framework that can adapt to the evolving nature of cyber threats and equip engineers with the skills necessary to defend against sophisticated cyber attacks.

Enhancing this training is not just about technical skills but also about understanding the strategic implications of cyber warfare.

CyberSecurity Advisors Network

ANALYSIS:

33. The CISO as Business Resilience Architect

Original Source: Dark Reading by Randolph Barr

The evolving role of Chief Information Security Officers (CISOs) now encompasses being architects of business resilience, extending beyond traditional cybersecurity boundaries.

This shift reflects the increasing recognition of cyber risks as fundamental business risks. CISOs are tasked with designing and implementing strategies that not only protect information assets but also ensure business continuity in the face of cyber incidents.

The role demands a deep understanding of business processes, risk management, and strategic planning, making CISOs pivotal in aligning security initiatives with broader business objectives.

CyberSecurity Advisors Network

ANALYSIS:

34. Navigating AI-powered cyber threats in 2025: 4 expert security tips for businesses

Original Source: ZDNet by Dan Patterson

As businesses face an evolving landscape of AI-powered cyber threats in 2025, experts offer crucial security tips to stay protected.

The focus is on proactive defence strategies, including the integration of advanced AI tools for threat detection and response.

Experts emphasise the importance of continuous training for security teams to keep pace with AI developments.

They also recommend regular system audits and updates to safeguard against sophisticated AI exploits. Strengthening collaboration across industry sectors is advised to share insights and best practices in combating these next-generation threats.

CyberSecurity Advisors Network

ANALYSIS:

35. Pentesters: Is AI Coming for Your Role?

Original Source: The Hacker News

The rise of AI-driven security tools has sparked debate over the future of penetration testing and whether AI could replace human pentesters.

While AI excels at automating vulnerability scanning and identifying common exploits, experts argue that human intuition, creativity, and contextual understanding remain irreplaceable.

Pentesters bring critical thinking and adaptive problem-solving that AI lacks, making them essential in uncovering complex security flaws.

Instead of replacing pentesters, AI is expected to enhance their capabilities, allowing security professionals to focus on more advanced, high-impact testing scenarios.

CyberSecurity Advisors Network

ANALYSIS:

36. Cybersecurity Can’t Wait: Modern Enterprises Must Adapt

Original Source: TripWire

Modern enterprises must adopt a proactive cybersecurity strategy to stay ahead of evolving threats.

This article stresses that reactive approaches are no longer sufficient as cyberattacks grow more sophisticated and frequent.

Organisations are urged to implement continuous monitoring, real-time threat detection, and adaptive security frameworks to mitigate risks effectively. Investing in employee training, strong identity management, and AI-driven security tools is also highlighted as key to strengthening overall resilience.

Businesses that fail to adapt risk severe financial, operational, and reputational damage in an increasingly hostile digital landscape.

CyberSecurity Advisors Network

ANALYSIS:

37. 2025 Annual State of the Industry Report Summary

Original Source: Cyber Security Tribe

Traditional security measures often fall short in detecting and preventing insider threats, which pose significant risks to organizations.

This article explores how insiders—whether malicious or negligent—can bypass standard security controls, making detection more challenging than external attacks.

It emphasises the need for a more proactive approach, including behavioural analytics, real-time monitoring, and zero-trust frameworks to minimise insider risk.

Organisations are encouraged to foster a culture of security awareness, implement strict access controls, and continuously review security policies to adapt to evolving threats from within.

CyberSecurity Advisors Network

ANALYSIS:

38. Top Cybersecurity Concerns For 2025: Considerations For The C-Suite

Original Source: Forbes by Anurag Lal

The latest industry report provides a comprehensive overview of the cybersecurity landscape heading into 2025, highlighting key trends, emerging threats, and strategic priorities for businesses.

Findings indicate a surge in AI-driven attacks, increased regulatory scrutiny, and a growing emphasis on resilience over mere compliance.

The report stresses the need for organisations to invest in adaptive security strategies, workforce upskilling, and robust incident response frameworks.

As cyber risks become more complex, businesses must shift from reactive defence to proactive risk management to stay ahead of evolving threats.

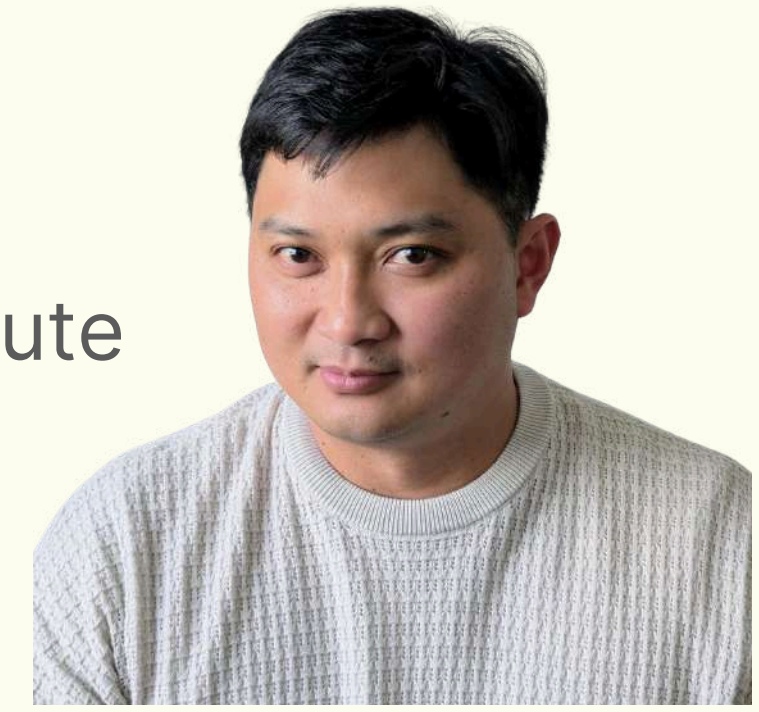
CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

39. Cyber Kill Chain: Breaking Down the Steps

By CyAN Member and General Secretary Fel Gayanilo



Fel Gayanilo provides a detailed breakdown of the Cyber Kill Chain, outlining the key stages attackers follow to infiltrate systems and execute cyber threats.

From reconnaissance and weaponisation to exploitation persistence, and data exfiltration, the piece explains how understanding these steps helps organisations move from reactive defenses to proactive security strategies and minimise risks before they escalate.

Fel emphasises that effective cybersecurity requires continuous threat intelligence, early detection, and rapid response strategies to stay ahead of attackers. He highlights the importance of monitoring attacker behaviours, identifying vulnerabilities early, and implementing adaptive security measures to disrupt threats before they cause significant damage.

By understanding attacker methodologies, cybersecurity teams can anticipate evolving threats, strengthen defenses, and enhance overall cyber resilience in an increasingly hostile digital environment.

CyAN CyAN Members
Op Eds, Articles, etc

40. “What Happens to Heroes?” – EPISODE #1: The Unsung Heroes of the Digital World

By CyAN member, Anidris IT Advisor/Data Protection Officer, and Author, Didier Annet

Didier Annet shines a light on the often-overlooked individuals who keep the digital world safe—cybersecurity professionals, analysts, and data protection officers working behind the scenes to protect sensitive systems and information.

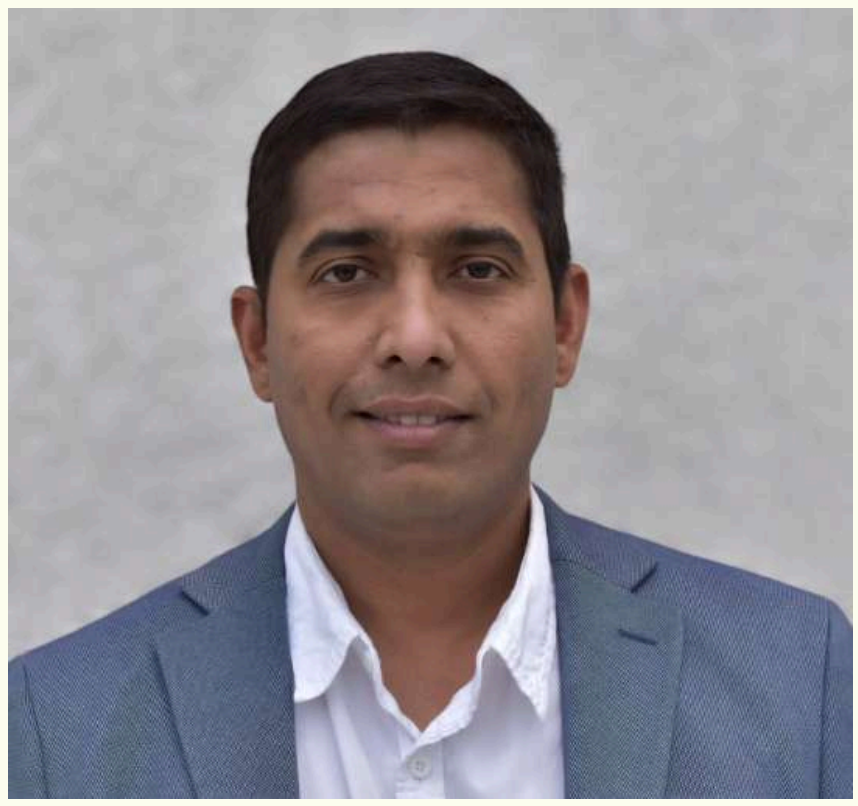
This first ‘episode’ in the series explores the challenges these experts face, from the relentless pace of cyber threats to the lack of recognition for their critical contributions.

Didier reflects on the emotional and ethical weight carried by those responsible for safeguarding digital infrastructure, highlighting the toll of staying ahead of attackers in an ever-evolving threat landscape.

He raises important questions about how these "unsung heroes" are supported, acknowledged, and motivated in an era of constant cyber conflict, emphasising the need for greater appreciation, resources, and mental health support to sustain their efforts.

CyAN Member's News:

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



Valued CyAN member Rupesh Shirke has been elevated to the grade of IEEE Senior Member, an honour bestowed only on those within the global engineering and technology community who have made significant contributions to their profession. This achievement reflects his dedication, expertise, and impact in advancing technology and cybersecurity.

Bharat Raigangar, a CyAN board member, has been recognised as a distinguished jury member for the CSG Awards 2025 at Enterprise IT World MEA! With his deep expertise in IT & Security, Bharat brings invaluable insights to honour excellence in cybersecurity. His leadership and commitment to elevating industry standards make him an outstanding choice for this role, and we look forward to seeing his contributions shape the awards.

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 Member's News:

What do reality TV, OSINT, and French celebrities on the run have in common? Meet CyAN member Sylvain Hajri!

Sylvain isn't just a rockstar within the OSINT community; he's also the founder of the search engine Epieos and the vibrant French community OSINT FR.

Beyond developing tools that empower analysts worldwide, Sylvain brings his expertise to reality TV, where he tracks celebrities on the run.

His recent podcast with OSINT producer Josh Axelrod delves into his early days in OSINT, the journey of building Epieos, the ethics of creating intelligence tools, and the hunter mindset essential for top-tier investigators.

This captivating conversation showcases one of CyAN's most innovative and intriguing members—don't miss it!

UPCOMING CyAN and CyAN Partner EVENTS:

- **Trust & Safety Forum at Forum INCYBER Europe (FIC), Lille, France: April 1-2**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April**
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April**
- **GISEC: Dubai Word Trade Center, Dubai, UAE: 6- 8 May**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK**
- **World AI Technology Expo UAE, Dubai, UAE: 14-15 May 2025 https://worldaiexpo.i**
- **MaTeCC, Rabat, Morocco: 7-9 June, 2025**

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