News release

EMBARGOED UNTIL

MONDAY 11 OCTOBER US 13.00 PM PACIFIC 16.00 PM EASTERN
EU 20.00 PM GMT 21.00 PM CENTRAL EUROPEAN TIME

TUESDAY 12 OCTOBER AUSTRALIA 09.00 AM AEDST and corresponding times elsewhere

GLOBAL COALITION BUILDS TO PROTECT CYBER RESEARCHERS

Cybersecurity Advisors Network (CyAN), a Paris-based global not-for-profit association representing cybersecurity professionals in 22 countries, today announced the formation of a global partnership to secure legal protections for good faith (*bona fide*) zero day researchers.

Said CyAN International Vice President and Zero Day Legislative Project leader, Peter Coroneos

“At a time of unprecedented scale and seriousness of cyber attacks threatening our personal information, the continuity of our businesses and the systems and infrastructure that support our societies, we find the very people we rely on to protect us remain under threat.”

Mr Coroneos explained, ’*w*hite hat’ zero day researchers form a critical piece in the remediation of exploitable connected systems. They uncover the existence of unpatched vulnerabilities and report them to vendors of the relevant products so they can be fixed. Regrettably, they face legal threats from some vendors sensitive to the discovery of flaws in their products.”

“The threats usually involve copyright and/or criminal laws that govern access or interference with computer systems. Outdated laws have not kept up with cyber challenges, stifling research efforts and reporting at a time when researchers should be supported.”

“That is why we are building an international coalition to advocate for changes to laws to ensure that zero day researchers will no longer fear heavy handed legal responses from companies whose products they are seeking to secure”.

The OECD* recognised the need for action in their 2021 guidance for policy makers observing:

> *In many countries, researchers face significant legal risk when reporting vulnerabilities to vulnerability owners. Vulnerability owners can threaten researchers with legal proceedings instead of welcoming their vulnerability reports. This legal risk, aggravated when stakeholders are located across borders, creates powerful disincentives* [for responsible disclosure]. * *Source: https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf*

A number of high profile cyber leaders have expressed support for the initiative…

“Security researchers are the public safety whistleblowers for technology that the world increasingly depends upon. It’s high time the world’s laws provided these good faith hackers safer ways to perform their vital research essential to securing the modern world,” said **Katie Moussouris**, Founder & CEO Luta Security; Founder, Microsoft Vulnerability Research (MSVR); Co-author & co-editor of International standards ISO 29147 Vulnerability disclosure and ISO 30111 Vulnerability handling processes

“Ethical cybersecurity research which help us clean up the digital environment deserves and needs proper legal protection” according to **Ciaran Martin, CB** former CEO, National Cyber Security Centre UK.

Chris Painter, former top US cyber diplomat added: “It’s important to separate malicious actors from responsible, ethical, researchers who conduct their research within settled best practices. Supporting the latter, while condemning the former, is a worthy cause.”

“If good-faith security research is the Internet's Immune System, then modernising legislation to recognise hacking as a dual-use and morally agnostic activity, as well as creating carve-outs for today's Internet's ‘digital locksmiths’, is the equivalent of resolving the Internet's auto-immune problem.” **Casey Ellis**, Founder/Chairman/CTO of Bugcrowd and Co-Founder of The disclose.io Project.

Stéphane Duguin, CEO on behalf of The CyberPeace Institute, agreed saying “Because of complexity and distributed nature of vulnerabilities, we need to empower and not penalize those who are working in good faith in the interest of public safety. Secure ICTs are key to creating a safe and stable cyberspace where we can unlock the potential of technology and empower individuals. Cybersecurity researchers are key to this mission.”

Also supporting the program is:

Vice-amiral d’escadre (Ret) Arnaud Coustilliere, former FR COMCYBER

Ends.

For further information please contact:

EU	Jean Christophe Le Toquin (France)	+33 607108714
US	Nick Kelly (+ Italy)	+39 339 2951303
APAC	Peter Coroneos (Australia)	+61 419 552 872