Disclosure And Amazon Disclaimer Privacy Policy Medical Disclaimer Terms Of Use

Bestgamingpro

Product reviews, deals and the latest tech news

☰ MENU

× Tech News Reviews Affiliate Disclosure Disclaimer Terms of Use Contact Us about Us

Home › Tech News › Singapore establishes a centre for the evaluation and certification of cybersecurity

SINGAPORE ESTABLISHES A CENTRE FOR THE EVALUATION AND CERTIFICATION OF CYBERSECURITY

Posted On: May 18, 2022

government would be able to spur the development of a robust testing, inspection, and certification (TIC) industry focused on cyber security.

The Cyber Security Agency of Singapore (CSA) and Nanyang Technological University (NTU), which jointly launched the facility on Wednesday, say the SG$19.5 million ($13.99 million) National Integrated Centre for Evaluation (NICE) will facilitate vulnerability assessments of software and hardware products, physical hardware attacks, and security measures.

They stated that access to security assessment facilities was problematic because of the high equipment costs and extensive knowledge normally needed to conduct cybersecurity evaluations at the highest assurance levels.

NICE, which would be housed on NTU Smart Campus, would make this technology available to researchers and developers, as well as housing a team of researchers and technicians who could make use of it.

Ling San, NTU's vice president and provost, said: "It is imperative that institutions, businesses, and government agencies keep on top of the ever-increasing danger of cyberattacks. In order to make our cyber-physical systems secure, the first step is to guarantee that hardware is built with security in mind, rather than as an afterthought."

David Koh, CEO of CSA and Commissioner of Cybersecurity, said that as Singapore moves towards a digital future, it is crucial to guarantee that new emerging technologies are securely constructed.

Hardware components like connection points and sensors, which are used in the Internet of Things (IoT) and cyber-physical systems (CPS), have grown in importance as a result. IoT devices will number 64 billion by 2025, according to CSA and Business Insider Intelligence estimates.

In its statement, the agency said that "these components constitute possible entry points for hackers and hostile actors". These components' security cannot be assessed by end-users, and they need to rely on independent specialists to do so."

A unified platform for testing and certifying goods would be provided by NICE to help Singapore's drive toward enhanced security assessment. The study and development of enhanced security assessment methodologies would also be supported by the centre.

Along with CSA and NiCE, the Singapore Accreditation Council (SAC) will create appropriate accreditation programmes. With the help of CSA's Cybersecurity Labelling Scheme, SAC's IT testing programmes allowed approved TIC businesses to guarantee that their test results and

CSA also introduced a new project named “CLS-Ready” on Wednesday to expedite the labelling procedure even more. This would eliminate the need to retest end-device security features provided by CLS-Ready hardware.

A CLS-Ready chip, for example, might save manufacturers time and money when putting their end-user device through the paces of CLS Level 4 testing. Because the chip’s main security mechanism has already been certified as CLS-Ready, these devices won’t need to go through another round of CLS Level 4 testing, according to CSA.

Applications for CLS-Ready labelling must include evidence and a lab evaluation report from a certified lab. For a maximum of five years, these labels would be valid as long as the devices were receiving security upgrades.

CSA said that payments for CLS-Ready labelling will be waived until October 2022 in an effort to boost adoption.

All consumer IoT gadgets including smart lights, smart door locks, smart printers, and IP cameras were included to the plan in January of this year. Wi-Fi routers and hubs for smart homes were the first equipment to be evaluated under the new system, which now applies to all connected devices.

With the goal of encouraging manufacturers to create more secure goods rather than only those with the best functionality and lowest cost, the CSA said the voluntary effort was also meant for customers to easily recognise items that had superior security measures.

Each extra asterisk in the CLS rating indicates an additional degree of testing and evaluation the product has undergone. According to level one, for example, products must meet basic security requirements such as ensuring unique default passwords and providing software updates, while level four products must have undergone structured penetration tests by approved third-party test labs and must have met level three requirements in order to earn this designation.

Catherine A. Leal

Subtly charming pop culture geek. Amateur analyst. Freelance tv buff. Coffee lover

Prev Post Next Post