Singapore's CSA, NTU Unveils NiCE for Cybersecurity Measures

- Yen Ocampo
- May 20, 2022

Image Credits: ntu.edu.sg

-
-
-
-

The Cyber Security Agency of Singapore (CSA) together with the Nanyang Technological University, Singapore (NTU Singapore) inaugurated the National Integrated Centre for Evaluation also tagged as NiCE -a partnership that intends to modernise the country's national hardware security evaluation and certification ecosystem.

This collaboration between CSA and NTU underlines CSA's continual commitment to working with institutions of higher learning and industry to build up the cybersecurity manpower pipeline and facilitate a national cybersecurity ecosystem that will provide good business opportunities and jobs.

– David Koh, Commissioner of Cybersecurity and Chief Executive, Cyber Security Agency of Singapore

Koh noted that as the nation progresses toward a digital future, it is crucial that new developing technologies be created securely. The cutting-edge facilities will serve as a "one-stop-shop" for hardware device product research, testing, and security review. It will support a Community of Practice for Testing, Inspection, and Certification. NiCE provides a one-stop shop for manufacturers and developers to test and certify their devices. The SGD 19.5 million centres will help the sector in three ways: by establishing a community of practice, generating a research eco-system, and expanding education and training.

The start of the Internet of Things (IoT) and the rising use of cyber-physical systems have resulted in an increase in the number of devices and hardware components in such devices, such as communication points, storage, sensors, and actuators.

Meanwhile, to create a community of practice, NiCE will provide access to advanced technology that can be used by evaluators and developers to conduct evaluations at the highest assurance level, 3. The centre will retain a pool of research and technical staff with equipment-operating expertise. This will add to Singapore's product review and certification ecosystem, and it will help develop the Testing, Inspection, and Certification (TIC) business by

assessing software and hardware vulnerabilities, physical hardware attacks, and their countermeasures.

In addition, NiCE will encourage research and development in advanced security evaluation methodologies, including software and hardware security protections, to strengthen the industry ecosystem for cybersecurity testing and evaluation.

In turn, this will help the development of capabilities and the transfer of knowledge to the TIC industry, allowing TIC companies specialising in cybersecurity testing and certification to assist CSA and NiCE in providing quality services to end-users.

The Singapore Accreditation Council (SAC) will collaborate closely with NiCE and CSA to develop relevant accreditation programmes and facilitate the development of local TIC capabilities to support the cybersecurity ecosystem.

These include SAC's IT testing programmes, which will enable accredited TIC businesses to provide assurances on the integrity and consistency of their test reports and certificates in support of CSA's programmes such as the Cybersecurity Labelling Scheme (CLS).

NiCE will provide training, development, and certification for students and professionals so they can transfer into the industry effortlessly and will integrate security evaluation into the cybersecurity curriculum for students. NiCE also offers cybersecurity internships.

CSA also introduces 'CLS-Ready' initiative

NiCE's work is consistent with the CSA's goal of fostering Security-by-Design through security evaluation. CSA began certifying Infocomm devices in 2019 and 2020 with Singapore's Common Criteria Scheme and CLS.

CSA and the Singapore Standards Council issued Technical Reference 91 on Consumer IoT Cybersecurity Labelling. This outlines how to design and construct secure consumer IoT devices according to CLS criteria.

At the end of April 2022, the two schemes were acknowledged by the manufacturers and more than two hundred products have been submitted for labelling under the four levels of CLS while twenty more products were submitted for evaluation at higher assurance levels under the SCCS.

CSA's initiative through the "CLS-Ready" project helps manufacturers achieve the highest CLS security grade. This new programme was announced by Josephine Teo, Minister for Communications and Information and Minister-in-Charge of Smart Nation and Cybersecurity adding that the security functionalities provided by CLSReady hardware will no longer be needed to be tested again at the end-device level, allowing developers and manufacturers to save time and cost while not compromising on security.