Bioengineer.org

Search…   🔍   🔒 Login   ☰

HOME   NEWS ⌄   EXPLORE ⌄   BLOG   COMMUNITY ⌄   CONTACT US

Home > NEWS > Science News > Chemistry

NTU Singapore and CSA Singapore launch joint centre for cybersecurity evaluation, research, and education

BY **BIOENGINEER** — May 18, 2022 in **Chemistry**   💬 0

f Share on Facebook   🐦 Share on Twitter   in Share on Linkedin   🤖 Share on Reddit

✈ Share on Telegram   VK   ↪

To meet the demands of Singapore's cybersecurity evaluation needs, **Nanyang Technological University, Singapore (NTU Singapore)** and the **Cyber Security Agency of Singapore (CSA)** officially launched the **National Integrated Centre for Evaluation (NiCE)** today.

Credit: Credit to: Nanyang Technological University, Singapore

To meet the demands of Singapore's cybersecurity evaluation needs, **Nanyang Technological University, Singapore (NTU Singapore)** and the **Cyber Security Agency of Singapore (CSA)** officially launched the **National Integrated Centre for Evaluation (NiCE)** today.

The first of its kind in South-East Asia, the joint centre serves as a one-stop facility for cyber security evaluation and certification. **NiCE** is a unique initiative that pools industrial and research expertise together to develop a sustainable academia-industry-government ecosystem for product evaluation and certification in Singapore.
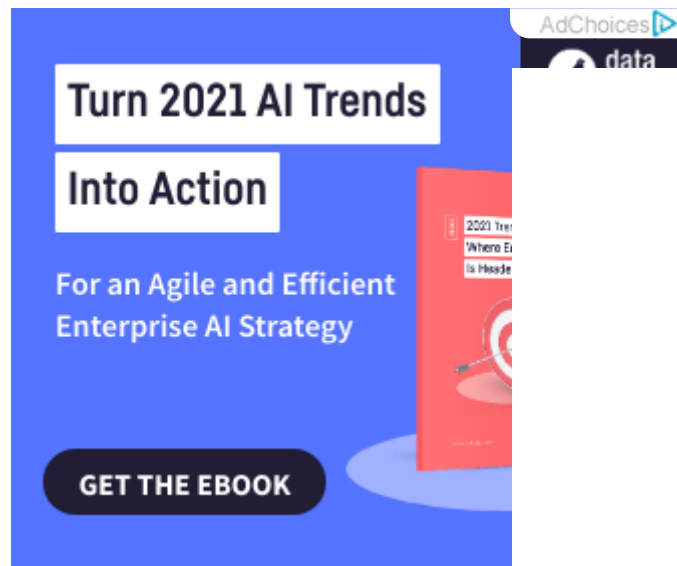
The centre also aims to help build a pipeline of local product evaluation talent, which will maximise economic opportunities and boost Singapore's branding as a cybersecurity hub.

The collaboration harnesses the strengths of NTU's research expertise in software and hardware security assurance and CSA's commitment to grow the nation's cybersecurity market by fostering innovations between cybersecurity industry and academia to build world-class products and services, and developing a robust talent pipeline.

Located on the NTU Smart Campus, NiCE was officially launched today by **Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity, Mrs Josephine Teo**.
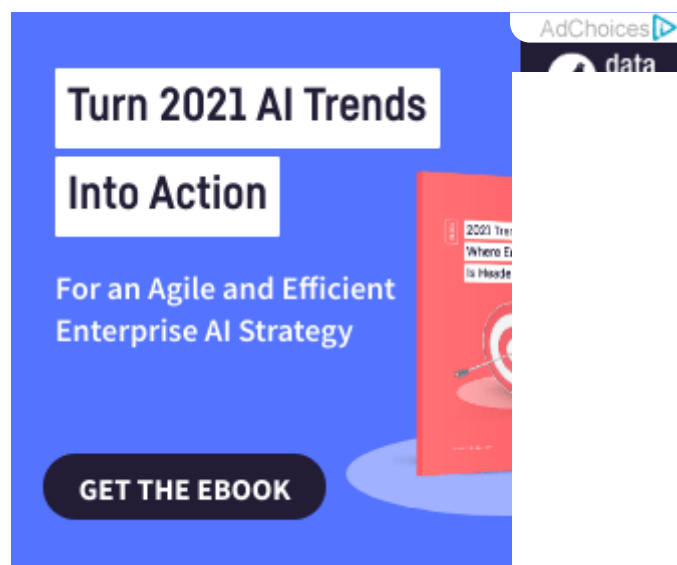
NTU Deputy President and Provost Professor Ling San said: "The rising threat of cyberattacks makes it vital that institutions, companies and agencies stay one step ahead of cyberthreats. Properly evaluating hardware to ensure that they are designed with security in mind, rather than added on as an afterthought, is the first step in keeping our cyber-physical systems safe. NTU's collaboration with CSA to set up NiCE leverages the University's strengths in areas such as computer science and engineering research and brings together industrial and research expertise in cybersecurity. The centre will also provide training and education to graduate students and industry professionals, allowing us to upskill and groom an important talent pool in this growing industry. This partnership underscores NTU's commitment as an academic anchor for industry partners."
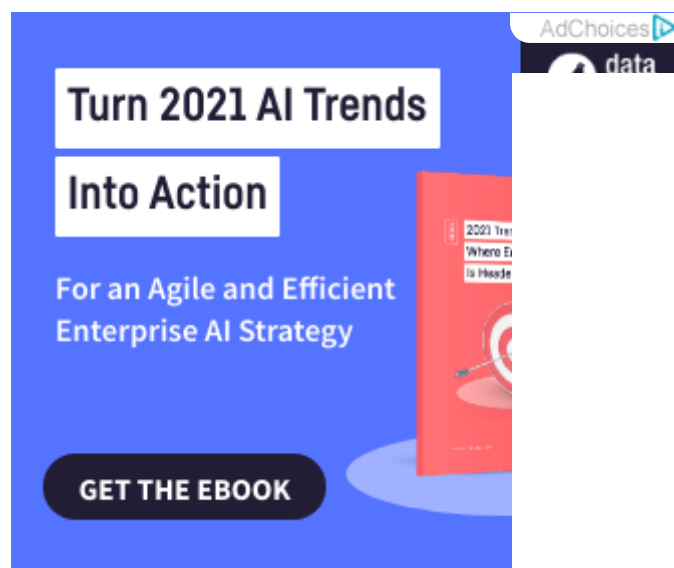
Mr. David Koh, Commissioner of Cybersecurity and Chief Executive of CSA, said: "As we move towards a digital future, it is important to ensure that new emerging technologies are designed securely. This collaboration between CSA and NTU underlines CSA's continual commitment in working with institutions 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."

The importance of cybersecurity evaluation and testing

The emergence of the Internet of Things (IoT) and increasing use of cyber-physical systems have led to a surge in devices and hardware components, such as communication points, storage, sensors, and actuators in such devices. According to a forecast by Business Insider Intelligence, it is estimated that there will be 64 billion IoT devices globally by 2025.

These components present themselves as potential entry points for hackers and malicious actors. End users have little means to assess if these components are secure and need to rely on independent experts to perform such security evaluation.
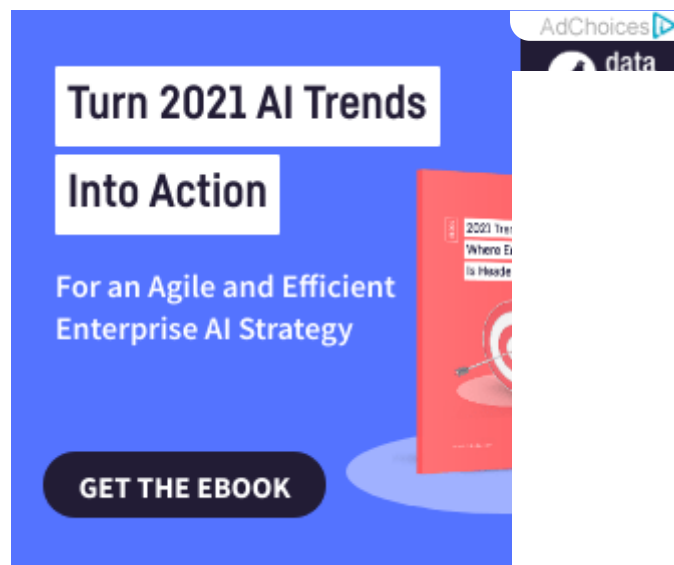
NiCE supports the national push towards greater security evaluation by providing an all-in-one platform for manufacturers and developers to test and certify their products.

The $19.5 million centre will provide support to the industry in three areas: creating a community of practice, developing a research eco-system, and furthering education and training.

Seeding a community of practice

The barriers to entry for the security evaluation industry is high due to high equipment cost and deep expertise needed to perform security evaluation at the highest assurance levels.

To seed a community of practice, NiCE will provide access to advanced equipment which evaluators and developers can use to perform evaluation at the highest assurance level. The centre will also maintain a pool of research and technical staff with the expertise to use the equipment and share their knowledge with other users.

This will contribute to a sustainable industry eco-system for product evaluation and certification in Singapore.

Growing the Testing, Inspection, and Certification industry for cybersecurity

NiCE will support the growth of the nascent Testing, Inspection, and Certification (TIC) industry through its facilities for the vulnerability assessment of software and hardware products, physical hardware attacks and their countermeasures.

To uplift the industry eco-system for cybersecurity testing and evaluation, NiCE will facilitate research and development in advanced security evaluation techniques, covering topics such as software and hardware security protections.

This will in turn support the capability building and knowledge transfer to the TIC industry, so that TIC companies specialising in cybersecurity testing and certification can support CSA and NiCE in providing quality services to end industry users.

The Singapore Accreditation Council (SAC) will work closely with CSA and NiCE to develop relevant accreditation programmes and facilitate the development of local TIC capabilities to support the cybersecurity eco-system. These include SAC's IT testing programmes which will enable accredited TIC companies to provide assurance on the accuracy and consistency of their test reports and certificates that support CSA's schemes such as the Cybersecurity Labelling Scheme (CLS).

NiCE Director **Professor Gan Chee Lip**, **Associate Provost (Undergraduate Education)** from **NTU's School of Materials Science & Engineering**, said: "At NiCE, the research in advanced techniques is co-located with the evaluation facilities and training programmes, allowing for tighter alignment and synergy between these activities. The setup at NiCE allows for greater access to cutting-edge academic research by the industry."

Building a pipeline of local product evaluation talent

As the demands for the nation's cybersecurity evaluation grow, so will the demand for competent security evaluators and a sustained talent pipeline of such professionals.

To meet this demand, NiCE will provide training, development, and certification for students and professionals to equip them with relevant security evaluation competencies, as well as knowledge about certification processes and evaluation methodologies necessary for them to transit seamlessly into the industry.

For example, NTU and CSA launched a **Graduate Certificate in Hardware Security Evaluation and Certification** last year which leverages the state-of-the-art facilities at NiCE to provide deep professional training on evaluation techniques. The certificate aims to train and upskill professionals in the industry as well as for professionals who are keen to join the industry.

NiCE will also enhance existing cybersecurity curriculum for students to include topics such as security evaluation. Students can also apply for internships at NiCE to gain exposure to the cybersecurity industry. Information on available courses, certification and internships are available on the NiCE website.

Ensuring safety through Security-by-Design

The work at NiCE is aligned with CSA's goal of promoting Security-by-Design through security evaluation. CSA kickstarted the process with the Singapore Common Criteria Scheme and Cybersecurity Labelling Scheme (CLS) to certify infocomm products in 2019 and 2020 respectively.

CSA and the Singapore Standards Council have also developed the national standard, Technical Reference 91, on Cybersecurity Labelling for Consumer IoT. This sets out the guiding principles to design and build safe and secure consumer IoT devices according to CLS security requirements.

As at end-April 2022, the two schemes have seen healthy take-up by manufacturers. More than 200 products have been submitted for labelling under the four levels of CLS and 20 products submitted for evaluation at higher assurance levels under the SCCS.

To make it easier for manufacturers to attain the highest CLS security rating, CSA has introduced an initiative known as **"CLS-Ready"**. This new initiative was announced by Minister Josephine Teo at the event. Security functionalities provided by CLS-Ready hardware will no longer be needed to be tested again at the end-device level, allowing developers and manufactures to save time and cost while not compromising on security. More details about CLS-Ready may be found in the factsheet in Annex A.

END

ANNEX A

MEDIA FACTSHEET

CLS-READY INITIATIVE

Launched in 2020, the Cybersecurity Labelling Scheme (CLS) rates consumer smart products on their level of cybersecurity based on four levels. CLS helps consumers make a more informed decision to purchase secure products, and also gives smart product manufacturers a competitive advantage when they roll out CLS-certified products. The CLS has seen good take-up by manufacturers with more than 140 products labelled under the four levels of the labelling scheme.

2   With the majority of products labelled under Levels 1 and 2, the Cyber Security Agency of Singapore (CSA) is making a push to encourage manufacturers to develop and label their smart products under Level 4, which has significantly higher cybersecurity assurance. One such requirement includes subjecting the products to a blackbox penetration testing by approved test laboratories.

CLS-Ready gives manufacturers a leg-up to meet CLS Level 4 requirements

3   CSA understands the challenges faced by manufacturers in implementing cybersecurity features from scratch into their products. The new **CLS-Ready** initiative will make it easier for smart product manufacturers to meet the requirements for the CLS Level 4 by streamlining the labelling process. Under CLS-Ready, smart product manufacturers can adopt hardware/security components (termed **CLS-Ready platforms**) – that have undergone the necessary testing required of CLS Level 4 – and integrate these into their commercial products. The CLS-Ready initiative will lower the barrier to entry for manufacturers of end devices in attaining CLS Level 4, especially SMEs and manufacturers of products that traditionally have no association with security. A CLS product built upon a CLS-Ready platform can rely on the existing certification of the platform to meet CLS Level 4 requirements.

4   For example, manufacturers can use a CLS-Ready certified chip in their end device, which will save them time and cost when testing their end device against CLS Level 4. For devices that have achieved CLS Level 4, manufacturers may often have to change the chips for their products down the road due to cost and supply reasons. By using a CLS-Ready chip, the end device would not need to go through another round of CLS Level 4 testing, as the core security mechanism in the chip would have already been assured as CLS-Ready.

5   Leveraging a CLS-Ready platform will benefit end-device manufacturers as they can focus on developing functionalities of the end-devices, without having to invest heavily on a team to develop the cybersecurity aspects of these devices. Chip manufacturers will also stand to benefit as a single CLS-Ready hardware will be able to support multiple end devices, thus expanding their market reach. The first company onboard the CLS-Ready initiative is **Infineon,** a semiconductor manufacturer which has its OPTIGA™ Trust M, a chip used in smart home and IoT consumer devices, certified with the CLS-Ready label.

6   Manufacturers applying for the CLS-Ready label will need to submit an application with supporting evidence and assessment report by an approved lab. The CLS-Ready label will be valid for the length of time for which the device will be supported with security updates, up to a maximum of five years. To encourage adoption, CSA will waive the application fees for CLS-Ready till October 2022.

7   For more details on the CLS and the CLS-Ready initiative, please visit www.go.gov.sg/csa-cls.

Media contact:

Mr Lester Hio
Manager, Media Relations
Corporate Communications Office
Nanyang Technological University, Singapore
Email: lester.hio@ntu.edu.sg

Ms Cheryl Lee

Senior Manager, Comms and Engagement Office

Cyber Security Agency of Singapore

Email: Cheryl_LEE@csa.gov.sg

About Nanyang Technological University, Singapore

A research-intensive public university, Nanyang Technological University, Singapore (NTU Singapore) has 33,000 undergraduate and postgraduate students in the Engineering, Business, Science, Humanities, Arts, & Social Sciences, and Graduate colleges. It also has a medical school, the Lee Kong Chian School of Medicine, set up jointly with Imperial College London.

NTU is also home to world-class autonomous institutes – the National Institute of Education, S Rajaratnam School of International Studies, Earth Observatory of Singapore, and Singapore Centre for Environmental Life Sciences Engineering – and various leading research centres such as the Nanyang Environment & Water Research Institute (NEWRI) and Energy Research Institute @ NTU (ERI@N).

Ranked amongst the world's top universities by QS, NTU has also been named the world's top young university for the past seven years. The University's main campus is frequently listed among the Top 15 most beautiful university campuses in the world and it has 57 Green Mark-certified (equivalent to LEED-certified) building projects, of which 95% are certified Green Mark Platinum. Apart from its main campus, NTU also has a campus in Singapore's healthcare district.

Under the NTU Smart Campus vision, the University harnesses the power of digital technology and tech-enabled solutions to support better learning and living experiences, the discovery of new knowledge, and the sustainability of resources.

For more information, visit www.ntu.edu.sg

About the Cyber Security Agency of Singapore

Established in 2015, the Cyber Security Agency of Singapore (CSA) seeks to keep Singapore's cyberspace safe and secure to underpin our Nation Security, power a Digital Economy and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions, and works with sector leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cyber security awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

CSA is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information. For more news and information, please visit www.csa.gov.sg.

 Share 12   Tweet 7   Share 2   Share   Share   Share 1

Related Posts

CMU and Columbia researchers magnify hidden biological structures with MAGNIFIERS
 May 18, 2022

Graphene-wrapped zeolite membranes for fast hydrogen separation
 May 18, 2022

NBA sees rise in acts of symbolic violence May 18, 2022

How on-screen representations of professions have changed over 70 years May 18, 2022