CYBERSECURITY INNOVATION DAY 2020

30 JUL | 9AM (SGT) | LIVE WEBCAST

AWARDEES LOOKBOOK

AN INITIATIVE BY

CSA SINGAPORE

POWERED BY

TNB VENTURES

2019 CYBERSECURITY INDUSTRY
CALL FOR INNOVATION AWARDEES

Acronis

Advanced Malware Forensics

AMARIS•AI™
AGILE - INNOVATIVE - TRUSTED

Adversarial Attack on Artificial Intelligence

EMERSON™

Operational Technology (OT) Protection

EY Building a better working world

Cybersecurity Threat Intelligence

GROUP|IB

Cybersecurity Threat Intelligence

InsiderSecurity

Data Access Security

SCANTIST

Application Security Assessment

SecureAge

End Point Protection, Detection & Response

SECURE-iC
THE SECURITY SCIENCE COMPANY

Autonomous Vehicle Security

Acronis

Advanced Malware Forensics

Acronis is a global technology company with Corporate Headquarters in Schaffhausen, Switzerland and International Headquarters in Singapore. Acronis develops on-premises and cloud software for backup, disaster recovery, and secure file sync and share and data access.

Acronis's advanced malware analysis system uses Artificial Intelligence (AI) to study the behaviour of malware. This creates a solution for malware detection and forensic for both file-based as well as fileless malware, which is not a widely available solution to date. The solution will build a malware intelligence knowledge database that can help your organisation's Incident Response Team to better understand the emerging malwares, contain as well as remove these malwares from the system.

www.acronis.com

Customers (Enterprise, Government) and Partners (Managed Security Service Providers)

oi@acronis.com

National Cyber Security

Team

Presenter

Oleg Ishanov
Director of
Threat Research

Candid Wuest
Vice President
Cyber Protection Research

Alvin Kua
Product Manager

Adversarial Attack on Artificial Intelligence

Amaris.AI strives to advance the age of humanity with its trustworthy cutting-edge artificial intelligence and cybersecurity products.

Amaris.AI has developed an evaluation tool as well as technical guidelines to validate the robustness of Artificial Intelligence (AI) and Machine Learning (ML) models and systems against adversarial attacks. Its AI Robustness Framework (ARL) and evaluation tool will provide your organisation the robustness score of a proposed AI engine against adversarial attacks.

www.amaris.ai	Customers and Partners
enquiries@amaris.ai	General B2B/Enterprise, Finance, Telecommunications

Team

Presenter

Prof Yu Chien Siang
Chief Innovation and Trust Officer

Dr Patrick Chan
Chief Technology Officer

Operational Technology (OT) Protection

Emerson, a market leader in Engineering Automation Solution and IIoT provider, helps our customers to overcome production challenges and help them to prevent their facilities from cyber attacks. Our HQ in US and we have global offices and manufacturing plants world wide.

Emerson proposes an approach to delay attacks on Operational Technology systems by introducing a simulated environment ("honeypot") closely imitating a real control system environment of a power plant. This honeypot can be introduced to the network infrastructure via traffic routed from an additional DMZ network one layer closer to the office network. This gives your organisation an early warning of attack on your OT system, and provides a better understanding of what the attack is trying to achieve.

www.emerson.com

Customers

kenn.ong@emerson.com

Medical, Oil & Gas, Utilities

Team

Presenter

Roger Ng
Director

Kenn Ong
Manager

Cybersecurity Threat Intelligence

At EY Advisory, professionals work closely with clients to tackle today's complex issues and capitalise on opportunities that help them to grow, optimise and protect their businesses.

EY's Integrated Intelligence Engine (IIE) provides your organisation a platform to hypothesise as well as postulate possible threat actors' exploitation path based on the ingestion of both structured and unstructured cyber intelligence sources. The EY IIE reduces the time your organisation's cybersecurity analyst spends on research as well as analysis of threat intelligence reports. Through artificial intelligence and machine learning, EY IIE will correlate real-world events to possible cyber attacks to provide early warning before it happens to your organization.

www.ey.com

steve-yk.lam@sg.ey.com
nirmalya.ghosh@sg.ey.com
lawren.poh@sg.ey.com

Customers

Defense, Finance, Government, Health, Logistics, Media, Telecommunications, Transportation

Team

Presenter

Steve Lam
Partner

Nirmalya Ghosh
Senior Manager

Lawren Poh
Director

Cybersecurity Threat Intelligence

Group-IB is a Singapore-based provider of solutions aimed at detection and prevention of cyberattacks and online fraud. The company also specialises in high-profile cyber investigations and IP protection.

Group-IB is building an AI-driven cyber investigation ecosystem uncovering hidden connections to dismantle cybercriminal underworld. The solution addresses critical cybersecurity challenges in detecting and predicting cyber threats from public social discussions and DarkWeb.

The ecosystem, powered by Group-IB's proprietary cyber threat intelligence data collected throughout 17 years of incident response and investigations, will speed up cybercrime investigation process, shorten the time for assessing the severity of cyber threats, and will allow the prevention at early stages.

🌐 www.group-ib.com	🔍 Customers
✉ info@group-ib.com	💼 Cyber Security

Team

Presenter

Shafique Dawood
Head of Sales and
Business Development APAC

Vesta Matveeva
Head of Cyber Investigation
Department in APAC

Aleksandr Lazarenko
Head of R&D Department

InsiderSecurity

Data Access Security

InsiderSecurity is an award-winning, Singaporean cybersecurity product company, whose advanced behavior analytics is used by government and industry-leading enterprises today. InsiderSecurity detects malicious user activity that would be missed by firewalls and antivirus.

InsiderSecurity provides the solution to tackle the problem of unauthorised user access in Electronic Medical Record (EMR) systems by leveraging on its user and entity behaviour analytics (UEBA) technology. As it is done automatically and intelligently, InsiderSecurity solution helps your organisation to save time as well as effort in manual configuration and alert analysis. The solution analyses data from diverse data sources, provides greater visibility of user activity as well as detects more threats automatically with sophisticated user behaviour analytics.

insidersecurity.co

Customers and Partners

hello@insidersecurity.co

Cyber Security & Other Sectors

Presenter

Jonathan Phua
CEO

SCANTIST

Application Security Assessment

Scantist provides SaaS solutions that help software managers and developers identify and remediate vulnerabilities in application source-codes and binaries.

Scantist aims to minimise cyber-security risks associated with software applications that are built in-house or outsourced. Scantist's solution combines AI-based techniques with traditional programme analysis techniques to create a scalable and extensible malicious code/vulnerability identification framework. The solution helps your organisation to detect malicious code as well as vulnerabilities in software applications at the source code and binary level with actionable remediation and reports.

🌐 www.scantist.com

✉ contact@scantist.com

🔍 Customers & Series A Investment

💼 Automotive, Banking, Financial Services and Insurance (BFSI) and Infocomm

Presenter

Prof Liu Yang
CEO

SecureAge

End Point Protection, Detection & Response

SecureAge Technology provides data protection solutions that help prevent, protect, and shield governments and enterprises from possible data breaches.

SecureAge uses a collaboration of solutions from InsiderSecurity and ReaQta to provide visibility, detection, response, triaging and protection that covers the essential areas of security. This collaboration will use technology to detect anomalies and threats using known assets as a baseline. It provides your organisation with a single solution that covers Protection, Detection and Response to your endpoint system.

www.secureage.com

teowhin@secureage.com

Customers and Partners

Banking, Financial Services and Insurance (BFSI), Government and Manufacturing

Presenter

Ngair Teow Hin
CEO

SECURE-iC
THE SECURITY SCIENCE COMPANY

Autonomous Vehicle Security

Secure-IC's mission is to partner with clients to provide best-of-breed, end-to-end cybersecurity solutions for embedded systems and cloud connected objects. Secure-IC provides a unique approach by building a progressive path that brings its customers from security requirements to certified solutions.

Secure-IC provides a highly robust, architecture-agnostic as well as tamper-resistant security plug and play modules for post deployed Autonomous Vehicles. These are structured in two protection levels: firstly, through an intrusion detection system (IDS) using advanced machine-learning techniques enabling behavioural analysis based on information collected from different sub-domains, and secondly, through Defense-in-Depth mechanisms made of security bridges over the CAN bus as well as ethernet in order to enforce strictly isolated domains leveraging cryptographic-level security.

www.secure-ic.com

benjamin.lecocq@secure-ic.com

Customers and Investment

Defense, Semiconductor and Automotive

Team

Presenter

Benjamin Lecocq
SEA & Taiwan Business Manager

Charles Thooris
Director & Chief Sales Officer

Antoine Gouhier
APAC Project Manager

BOOK BUSINESS MEETINGS WITH THE AWARDEES TODAY

BIT.LY/CYBERINNODAY2020MEETINGS

Information is accurate as of 17 July 2020 .