CYBERSECURITY INNOVATION DAY 2023

PROGRAMME GUIDE

29 September 2023

4-6 PM

Sands Expo & Convention Centre
Begonia Ballroom, Level 3

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

PROGRAMME

Opening Address

Mrs Josephine Teo
Minister for Communications and Information,
Minister-in-charge of Smart Nation and Cybersecurity

CyberSG Partnerships

CyberCall 2022 Award and Appreciation

Launch of CyberCall 2023

Reception, Networking and Booth Visits

For a list of exhibitors, refer to booth layout at the end of this guide.

End of Event

CYBERCALL 2022

EXPERT PANEL

Ashish Thapar
Vice President & Head Security Consulting (Asia Pacific)
Nippon Telegraph and Telephone (NTT)

Dr. Chen Binbin
Associate Professor, Information Systems Technology and Design (ISTD)
Singapore University of Technology and Design (SUTD)

Eddie Toh
Partner, Cyber Advisory and Head of Forensic Technology
KPMG

Dr. Goh Weihan
Associate Professor
Singapore Institute of Technology (SIT)

Jackson Tan
Chief Executive Officer
SYNthesize Pte Ltd

John Lee
Managing Director, Asia Pacific
Global Resilience Federation (GRF)
Asia Pacific

Matthias Yeo
Chief Executive Officer
CyberXCenter

Paul Choo
Managing Director
Tangram Asia Capital

Sugar Chan
Manager
Boston Consulting Group (BCG)

Dr. Tan Teik Guan
Chief Executive Officer
pQCee

Dr. Vivy Suhendra
Associate Professor (Practice Track)
School of Computing
National University of Singapore

CyberSG R&D Programme Office

The CyberSG R&D Programme Office is an initiative led by the Cyber Security Agency of Singapore (CSA), Nanyang Technological University (NTU) and its partners to propel Singapore to the forefront of cybersecurity development and implementation.

Our grant and challenge initiatives provide funding to encourage Research Institutes (RIs), Institutions of Higher Learning (IHLs), and businesses to propose projects that will enhance capabilities throughout the whole Technology Readiness Level (TRL) spectrum.

TRANSLATIONAL/ INNOVATION GRANTS

~S$ 400K

WHAT ARE WE LOOKING FOR?

Projects that show the use of cybersecurity technologies for commercial application(s), or solve specific use cases and challenges.

38 teams

12-18 months

THEMATIC CHALLENGE

~S$ 750K

WHAT ARE WE LOOKING FOR?

Projects that contribute to establishing Singapore as a trustworthy smart nation.

9 teams

18-30 months

GRAND CHALLENGE

~S$ 6M

WHAT ARE WE LOOKING FOR?

Projects that align with the government's strategic direction and address short- and long-term challenges.

2 teams

30-36 months

Timeline

- **Sep-Dec 2023: Application**
- 2024: Research and Technology Innovation
- 2025: R&D Commercialisation
- 2025: Customer Evaluation

For more information, contact vinay.ms@ntu.edu.sg

AN INITIATIVE BY: CSA SINGAPORE

POWERED BY: NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

CYBERCALL 2022
INNOVATORS

AWARDED COMPANY	AWARDED PROJECT	COMPANY REPRESENTATIVE
CUSTODIO TECHNOLOGIES	**OT Threat Vector Path Discovery on Digital Asset Map**	**Mr Martin Lui** General Manager Custodio Technologies https://custodiotech.com.sg/
FIRST WATCH® INDUSTRIAL CYBER SECURITY	**OT Kernel Prevention of Cyber Attacks**	**Mr Bob Stokes** Managing Director First Watch https://firstwatchprotect.com/
SCANTIST	**Secure Open-Source Supply Chain via AI-enabled Patching and Delivery**	**Dr. Liu Yang** Co-Founder and Director Scantist https://scantist.com/
S2T Unlocking Cyberspace	**Privadence**	**Dr. Ori Sasson** Director Stimulation Software & Technology (S2T) https://www.s2t.ai

CyberSG Talent, Innovation and Growth Collaboration Centre

Powered by NUS Enterprise

The CyberSG Talent, Innovation and Growth Collaboration Centre is co-driven by the Cyber Security Agency of Singapore (CSA) and National University of Singapore (NUS) to accelerate talent development, innovation, and growth in the cybersecurity industry.

The Centre brings together academia, industry, government, and international partners to harness synergies across new and existing cybersecurity programmes, thereby fostering collaboration across the cybersecurity landscape, locally and internationally.

It is structured around **three key pillars**:

TALENT

Increase the pipeline and number of cyber professionals, and build interest and cyber capabilities in our broader talent pool.

Key Programmes:

- SG Cyber Talent
- SG Cyber Associates
- Accelerated Conversion Programme

INNOVATION

Catalyse co-innovation with industry, bridge the path from innovation to commercialisation, and nurture promising cybersecurity companies for Singapore.

Key Programmes:

- SG CyberCall
- SG CyberBoost

GROWTH

Enable cybersecurity companies anchored in Singapore to scale regionally and globally, growing their businesses and impact as enterprises of tomorrow.

Key Programme:

- CyberGrowth

We're looking for local and international ecosystem collaborators!

The Centre is inviting Institutes of Higher Learning (IHLs), industry partners, government agencies and international cybersecurity hubs to co-deliver our Talent, Innovation and Growth programmes.

Reach out to us at https://go.gov.sg/tig-mailing-list

AN INITIATIVE BY: CSA SINGAPORE

POWERED BY: NUS National University of Singapore | Enterprise

Cybersecurity Industry Call for Innovation 2023

The Cybersecurity Industry Call for Innovation (CyberCall) aims to catalyse the development of innovative cybersecurity solutions to meet national cybersecurity and strategic needs, with the potential for commercial application.

Benefits

FOR INNOVATORS

- Up to S$1M funding to develop new solutions
- New business opportunities with large end-users
- Gain exposure to a network of investors

FOR END-USERS

- Test new products with mitigated end-user risk
- Co-innovate to secure organisation beyond market offerings
- Platform to discuss pressing challenges among end-users

Innovation Opportunities

We welcome proposals in the following focus areas including, but not limited to:

OPEN CATEGORY (CSOC)

- Cybersecurity for Artificial Intelligence (AI)
- AI for Cybersecurity
- OT/IoT Security
- Cloud Security
- Privacy-Enhancing Technologies

END-USER DRIVEN CHALLENGES

CSA has put together a list of end-users who are looking for solutions in areas mentioned above.

Open to local and overseas* companies

**Overseas companies will need to have the intention to register a company in Singapore or partner with a Singapore registered company. Please refer to the submission template for details.*

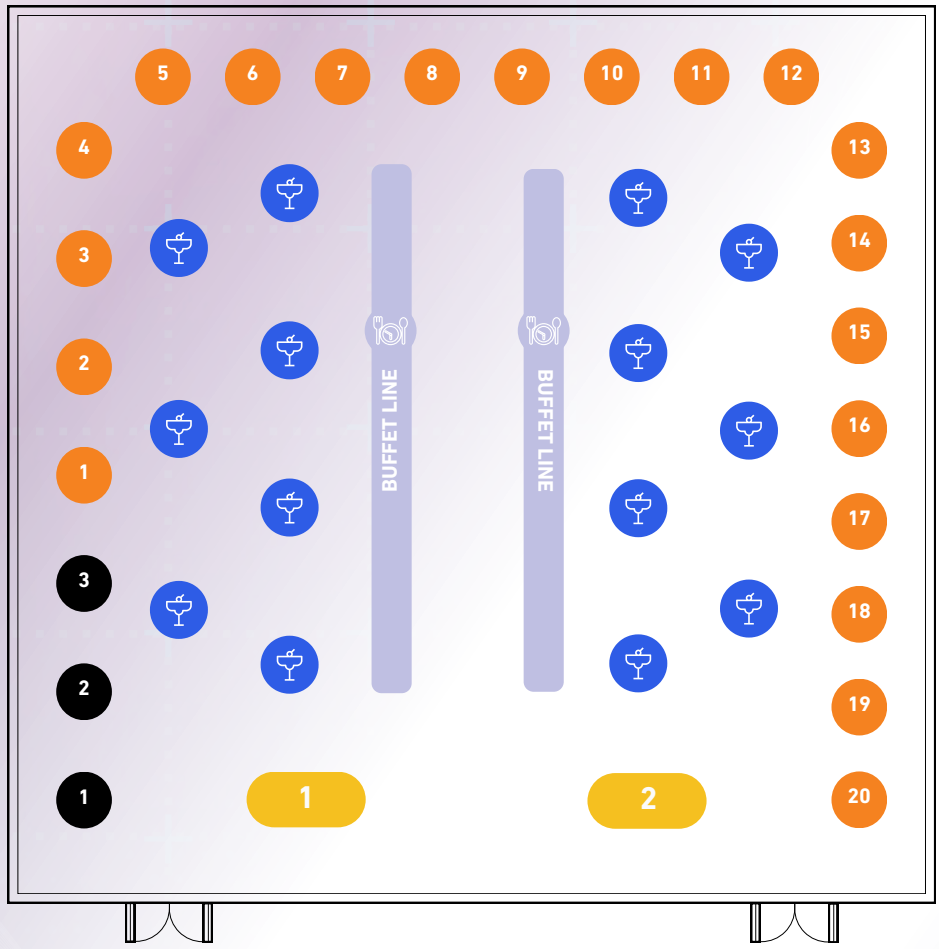
Submit proposals by 30 November 2023, 2359hrs (SGT)

AN INITIATIVE BY: CSA SINGAPORE

POWERED BY: NUS National University of Singapore | Enterprise

BOOTH LAYOUT

BEGONIA JUNIOR BALLROOM



CYBERCALL INNOVATORS

1 Custodio Technologies
2 First Watch
3 Scantist
4 S2T
5 Acronis
6 Amaris AI
7 Attila Cybertech
8 CyberOwl
9 Flexxon
10 Group-IB
11 InsiderSecurity
12 MicroSec
13 Protos Labs
14 Seagate
15 SecureAge Technology
16 Secure-IC
17 SkillSpar
18 ST Engineering
19 TAU Express
20 Thales

CSA PROGRAMMES

1 CyberSG Research & Development Programme Office
2 CyberSG Talent, Innovation and Growth Collaboration Centre / CyberCall

INSTITUTES OF HIGHER LEARNING (IHL)

1 iTrust Centre for Research in Cyber Security
2 National Cybersecurity R&D Laboratory (NCL)
3 National Integrated Centre for Evaluation (NiCE) @ NTU

Cocktail Table

Refreshments

EXHIBITORS

PAST AND PRESENT CYBERCALL INNOVATORS

Acronis

AMARIS·AI™ AGILE · INNOVATIVE · TRUSTED

ATTILA CYBERTECH

CYBEROWL

CUSTODIO TECHNOLOGIES

FIRST WATCH INDUSTRIAL CYBER SECURITY

FLEXON™

GROUP-IB

InsiderSecurity

MICROSEC

PROTOS LABS

S2T Unlocking Cyberspace

SCANTIST

SEAGATE

SecureAge

SECURE-IC THE SECURITY SCIENCE COMPANY

skillspar

ST Engineering

TAU EXPRESS

THALES

INSTITUTES OF HIGHER LEARNING

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

NUS National University of Singapore

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Tap exhibitor to see full poster

CYBERSECURITY INNOVATION DAY 2023

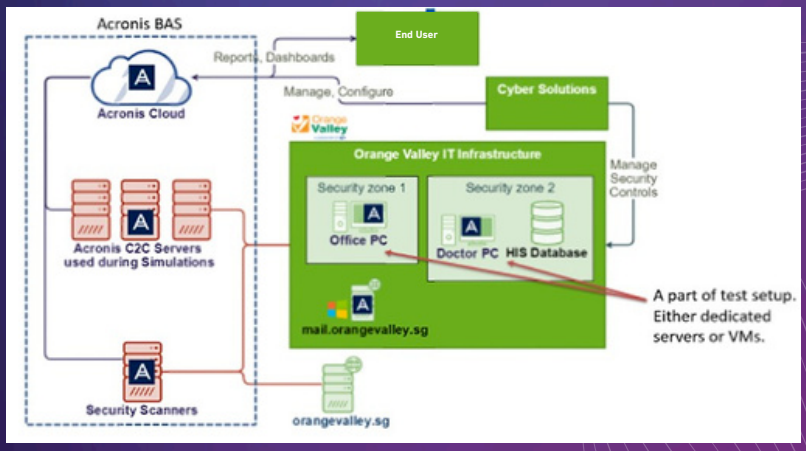
CYBERCALL INNOVATOR

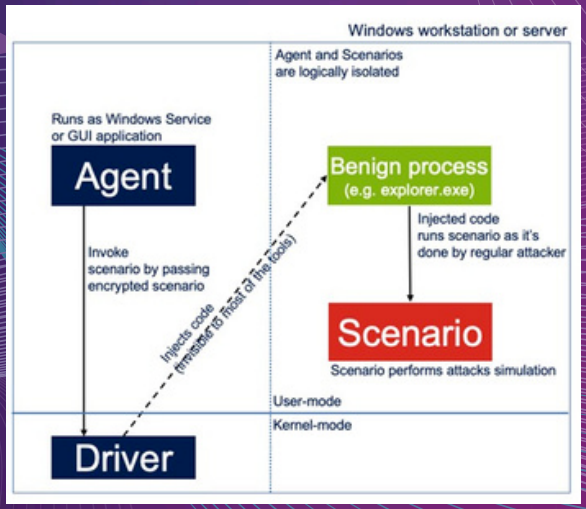
Challenge Statement:

Develop an effective evaluation system for the security posture of outsourced partner's systems, including gaining insights into the internal security controls of third-party partners, improving assurance mechanism, and granting access rights to vendors on a need-to-know basis.

Solution: Effective Evaluation of the Security Posture of Outsourced Partner's Systems

Acronis is proposing to introduce a system for real-time risk assessment to evaluate the actual security posture of third-party employees, who are involved in the provision of outsourced services. Assessment is performed as a continuous simulation of different re-constructed attack methods and tactics that are usually used by different adversaries. If the attack scenario was successful, specific improvements to the security controls will be recommended.





Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges.

Acronis offers antivirus, backup, disaster recovery, endpoint protection management solutions, and award-winning AI-based anti-malware and blockchain-based data authentication technologies through service provider and IT professional deployment models.

https://www.acronis.com/

oi@acronis.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

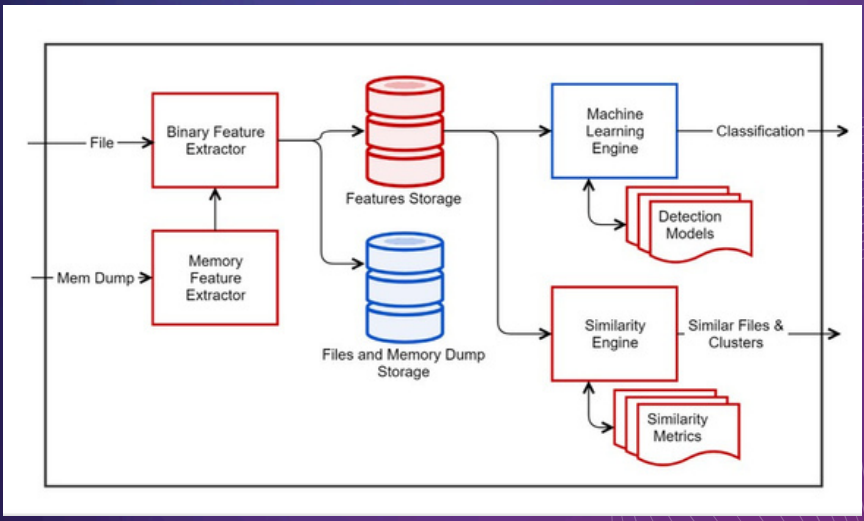
CYBERCALL INNOVATOR

Challenge Statement:

Build an advanced malware detection solution that can detect, dissect and analyse malware (including new versions and fileless varieties).

Solution: Advanced Malware Forensic using AI

Acronis developed the Advanced Malware Forensics platform for automated malware detection and analysis using machine learning (ML) algorithms. The AI platform classifies and attributes malicious files, performs searches for similarities in malware, and extracts indicators of compromise from files and memory dumps. It also studies and analyses the behavior of malware, and helps to automate incident response and threat detection operations.



Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges.

Acronis offers antivirus, backup, disaster recovery, endpoint protection management solutions, and award-winning AI-based anti-malware and blockchain-based data authentication technologies through service provider and IT professional deployment models.

https://www.acronis.com/

oi@acronis.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

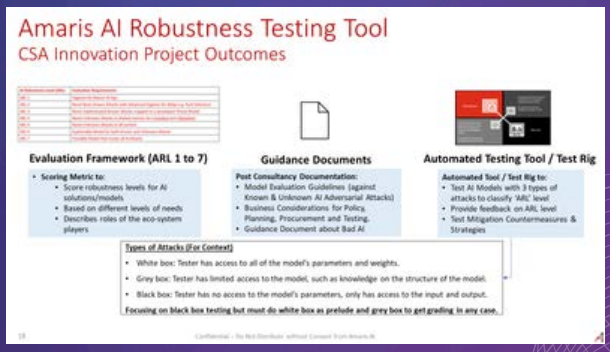
CYBERCALL INNOVATOR

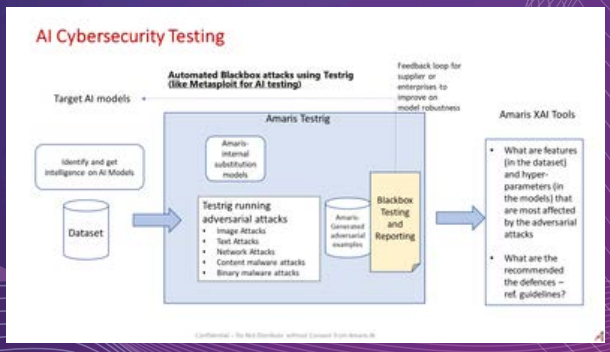
Challenge Statement:

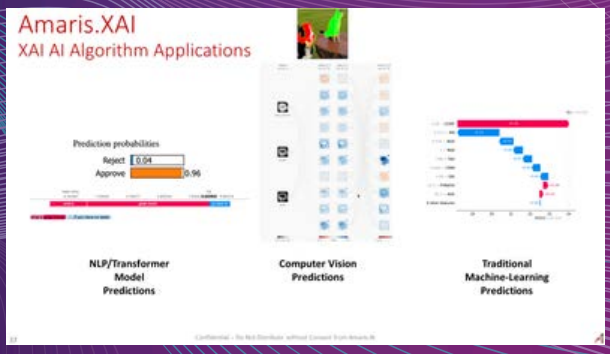
Develop a tool and propose technical guidelines to validate the robustness of artificial intelligence (AI) and machine learning (ML) models and systems against adversarial attacks.

Solution: Enhancing AI Robustness: Developing Tools and Guidelines for Adversarial Attack Validation

Amaris.AI worked with a CyberCall end-user on this project to develop a tool and technical guidelines to validate AI Robustness against adversarial attacks. Three subsequent outcomes were made: (1) general guidance documents and the release of a standard on AI security, TR99 (2) AI robustness evaluation framework, and (3) a tool to validate AI robustness against adversarial attacks.







AMARIS•AI™
AGILE · INNOVATIVE · TRUSTED

Amaris.AI is an artificial intelligence cybersecurity company based in Singapore that provides artificial intelligence assurance, intelligent automation, and edge artificial intelligence solutions.

https://www.amaris.ai/

hayley.tan@amaris.ai
benjamin.kang@amaris.ai

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

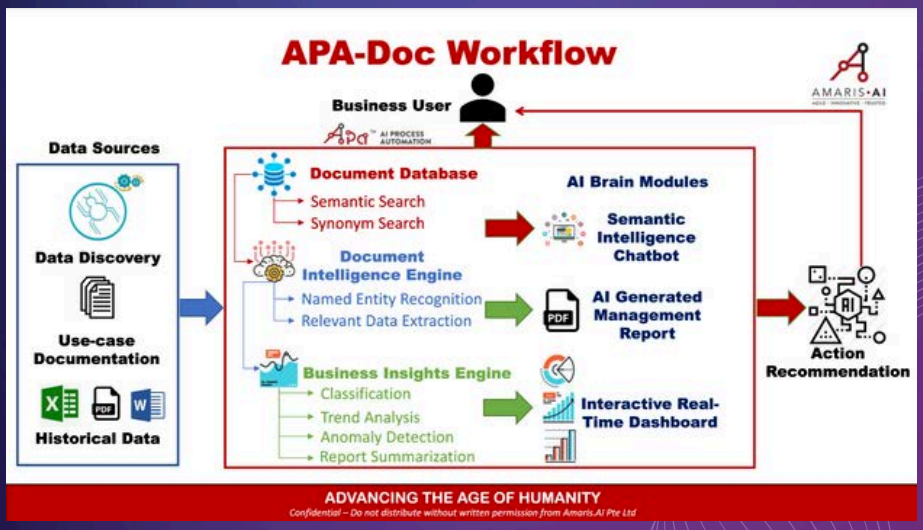
CYBERCALL INNOVATOR

Challenge Statement:

Build an application to take in data files, perform queries and data extraction, and have analytics, dashboarding and reporting capabilities.

Solution: Cybersecurity Risk Assessment and Audit Data Analytics

Amaris.AI is currently embarking on a project to provide risk assessment and audit data analytics for reporting purposes. This project utilises natural language processing to process risk assessment and audit reports for artificial intelligence sense-making and reporting.



AMARIS•AI™
AGILE · INNOVATIVE · TRUSTED

Amaris.AI is an artificial intelligence cybersecurity company based in Singapore that provides artificial intelligence assurance, intelligent automation, and edge artificial intelligence solutions.

https://www.amaris.ai/

hayley.tan@amaris.ai
benjamin.kang@amaris.ai

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

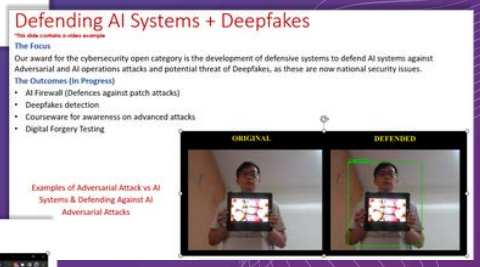
CYBERCALL INNOVATOR

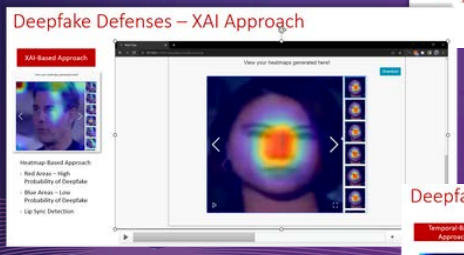
Challenge Statement (Open Category):

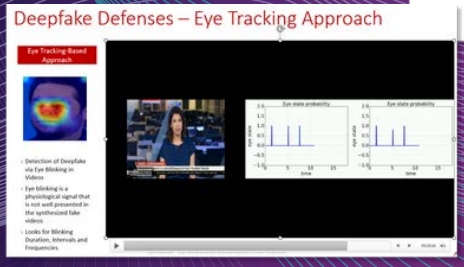
Develop defensive systems to defend artificial intelligence (AI) systems against adversarial and AI operations attacks and to fight the threat of deepfakes, as these are now national security issues.

Solution: Defending AI Systems and Fighting Deepfakes

Amaris.AI is working on this project to defend organisations against deepfakes and other sophisticated adversarial attacks. This project will provide defense counter-measures against adversarial attacks (vision, large language models), deepfakes and fake news.







AMARIS•AI™
AGILE · INNOVATIVE · TRUSTED

Amaris.AI is an artificial intelligence cybersecurity company based in Singapore that provides artificial intelligence assurance, intelligent automation, and edge artificial intelligence solutions.

https://www.amaris.ai/

hayley.tan@amaris.ai
benjamin.kang@amaris.ai

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

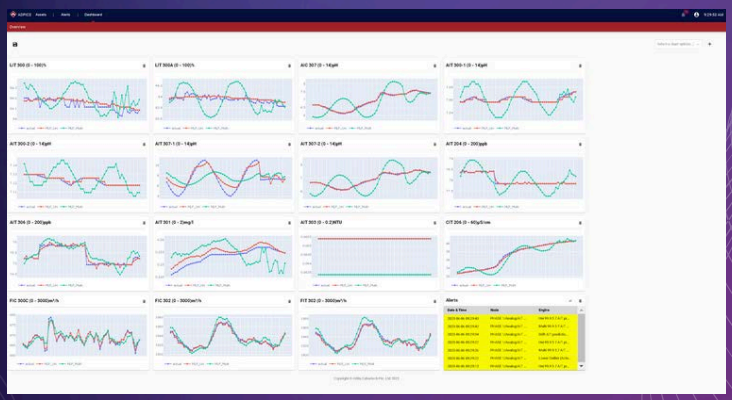
CYBERCALL INNOVATOR

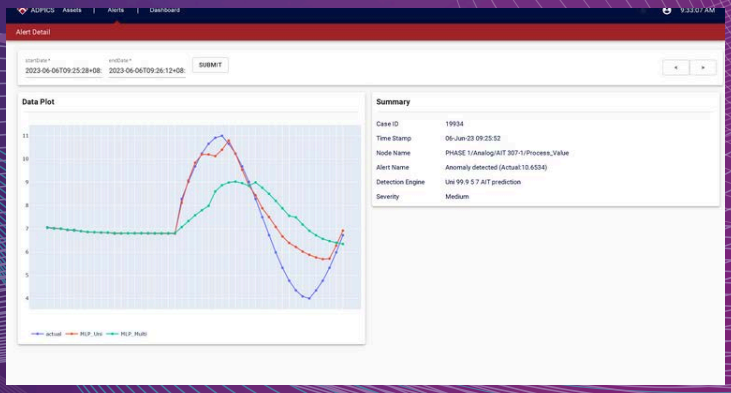
Challenge Statement:

Develop an innovative Operational Technology Intrusion Detection solution based on the normalcy of known process models, abnormality of networks and system traffic between field devices and Human Machine Interface (HMI).

Solution: Anomaly Detector and Protector of ICS (ADPICS)

Attila's Anomaly Detector & Protector of ICS (ADPICS) leverages Artificial Intelligence and domain expertise to analyse the behaviour of processes within SCADA and Programmable Logic Controllers (PLC). By conducting this analysis, ADPICS can identify anomalies and forecast potential failures of instruments and equipment in Industrial Control Systems (ICS).





ATTILA CYBERTECH

Attila Cybertech Pte. Ltd. is a consultancy and solutions provider in Operational Technology (OT) Cybersecurity. With a team possessing extensive knowledge and experience in the OT domain, Attila Cybertech excels in evaluating, advising, and safeguarding industrial automation and control systems, including SCADA, DCS, RTUs, PLCs, and HMIs in the Critical Information Infrastructure sectors such as Energy, Water, Maritime, Transportation, and Finance.

https://www.attilatech.com/

sales@attilatech.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

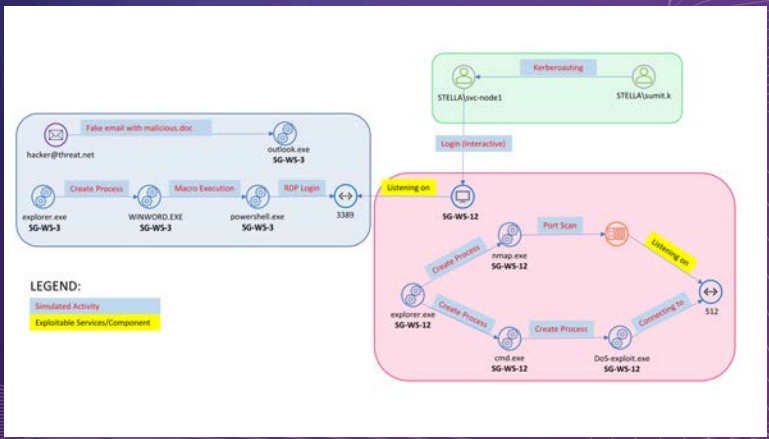
CYBERCALL INNOVATOR

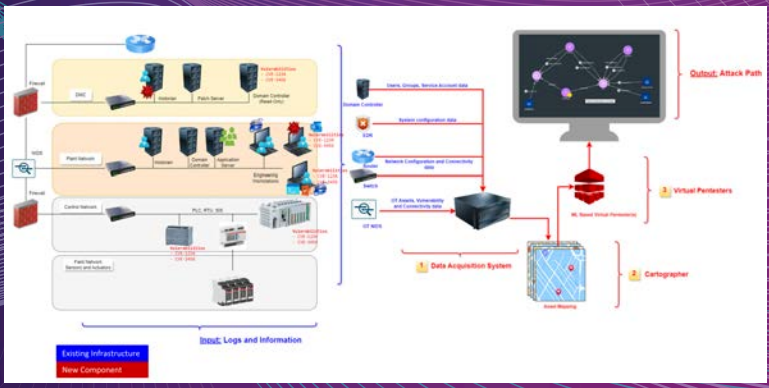
Challenge Statement:

Develop an automated solution that extracts the current network asset map and vulnerabilities, conducts penetration tests (PT) on digital assets, discovers paths of intrusion of the assets without operating on the actual Operational Technology (OT) system based on the MITRE attack framework and suggests remediation.

Solution: CyOTValidate

CyOTValidate is an innovative solution that performs non-intrusive threat discovery on OT networks. Our cutting-edge solution will create a comprehensive digital map of the intended network based on logs and data collected from multiple sources. Coupled with advanced machine learning (ML) models, the solution will perform virtual pen-testing on this map. Results of the pen-testing will include actionable recommendations in a report that is automatically generated. Instead of expensive physical pen-testing or creating a digital twin, companies can now leverage on this cost-effective solution for continuing scanning for irregularities and design modelling.





CUSTODIO TECHNOLOGIES

Established in 2014, Custodio started as a CyberSecurity R&D Centre of Israel Aerospace Industries (IAI) Ltd for Asia. In 2016, Custodio Technologies turned into a fully-fledged cybersecurity company providing proactive defence solutions that was successfully translated from R&D programmes. Custodio continues to actively participate in R&D innovation projects in view of the ever-evolving cyber threats. With a team of Cybersecurity R&D talent pool, Custodio Technologies also develops customised solutions for customers with specific needs.

https://www.custodiotech.com.sg/

sales@custodiotech.com.sg

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

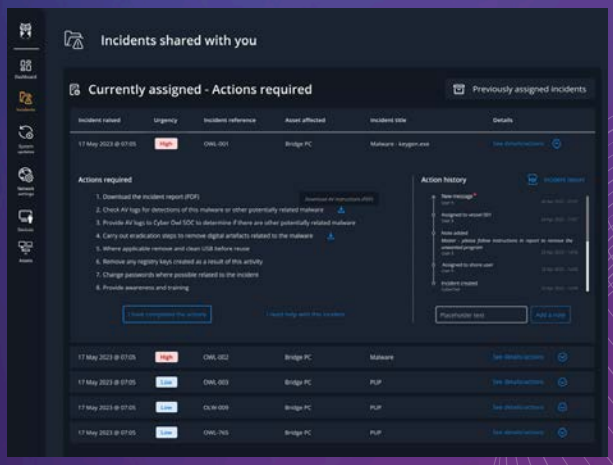
CYBERCALL INNOVATOR

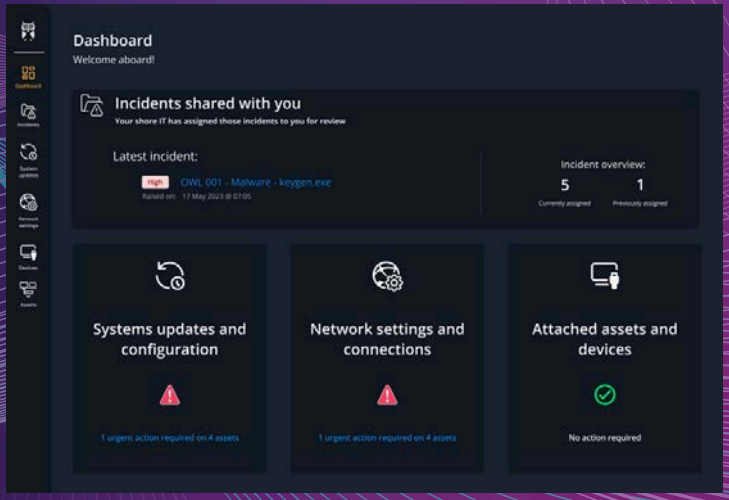
Challenge Statement:

Build a threat detection and risk profiling system catered for maritime vessel systems that can analyse, correlate and provide a coherent overview of threats spanning across the Information Technology (IT), Operational Technology (OT) and Internet of Things (IoT) system networks in real time.

Solution: Decentralised Security for Shipping

Cybersecurity technology is generally designed to centralise control. CyberOwl is turning this approach on it's head by developing technologies to decentralise cyber risk management. This distributes ownership to crew and engineers at the "point of use", while seamlessly coordinating security automation and response workflows across the centre and the edge. This innovation empowers crew to be responsible for cyber hygiene and compliant behaviour.





CYBEROWL

CyberOwl helps asset operators in the maritime and critical national infrastructure sectors gain visibility of systems on their remote assets, actively manage the cyber risks and gain assurance of cyber compliance.

https://www.cyberowl.io/

richard.wagner@cyberowl.io

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

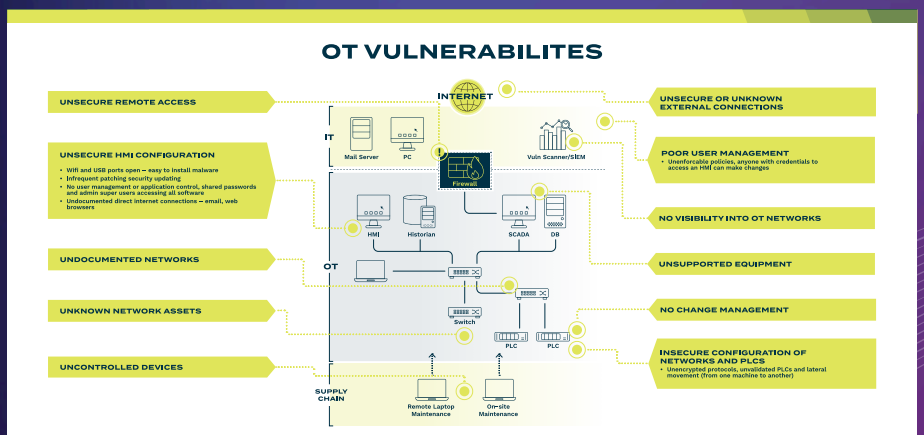
CYBERCALL INNOVATOR

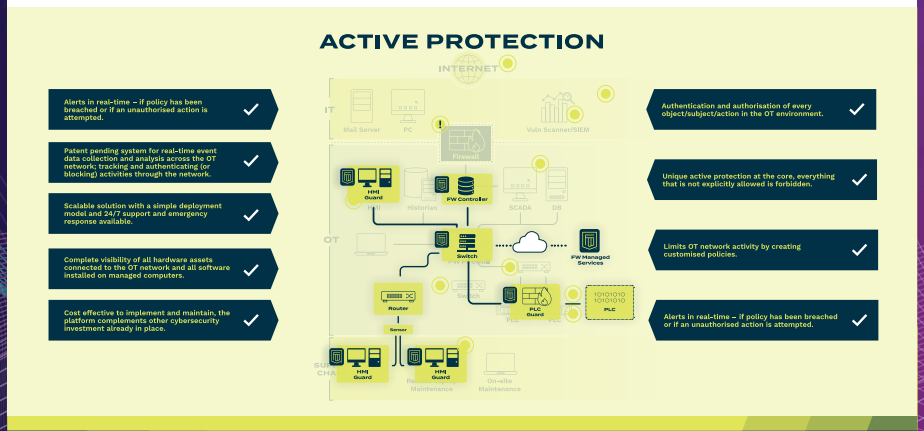
Challenge Statement:

Develop an artificial intelligence (AI)-driven data provenance engine to identify, respond to, and mitigate cyber intrusions by analysing behaviour patterns and event signatures.

Solution: OT Kernel Prevention of Cyber Attacks

The First Watch AI engine will convert hacker techniques into event sequences, employing machine learning in near-real time. This will provide early and accurate warnings of ongoing attacks, enabling proactive manual intervention to prevent damage and swiftly block intruders' further access.





FIRST WATCH®
INDUSTRIAL CYBER SECURITY

First Watch, a New Zealand-based cybersecurity company, specialises in software development protecting critical infrastructure assets like SCADA computers and PLCs. The patented approach - Active Protection - ensures that unauthorised activities within industrial networks are promptly detected and stopped. This cutting-edge platform prioritises the authorisation of actions by automation engineers, guaranteeing robust security.

https://www.firstwatchprotect.com/

info@first-watch.co.nz

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

CYBERCALL INNOVATOR

Challenge Statement (Open Category):

Address the ever-evolving cyber threat landscape with an innovative solution that plugs the existing gaps and proactively counters increasingly sophisticated cyber attacks, to protect our most sensitive and vulnerable data.

Solution: X-PHY® AI Embedded Hardware-Based Cybersecurity Solution

Flexxon's flagship cybersecurity solution, the X-PHY®, is the world's first AI-embedded hardware-based cybersecurity solution. It proactively detects anomalies in behavioral data access patterns to effectively shut down potential incursions in real-time to prevent critical data loss and exposure.

Founded in 2007 and headquartered in Singapore, Flexxon is a global company that specialises in next generation hardware cybersecurity solutions and industrial NAND storage devices. Rooted in its strong pedigree as a leading industrial NAND flash storage solutions provider, Flexxon is committed to protecting the basic rights of all citizens of the digital economy through constant innovation to address the evolving cybersecurity needs of today.

https://www.flexxon.com/

camelliachan@flexxon.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

POWERED BY:

CYBERSECURITY INNOVATION DAY 2023

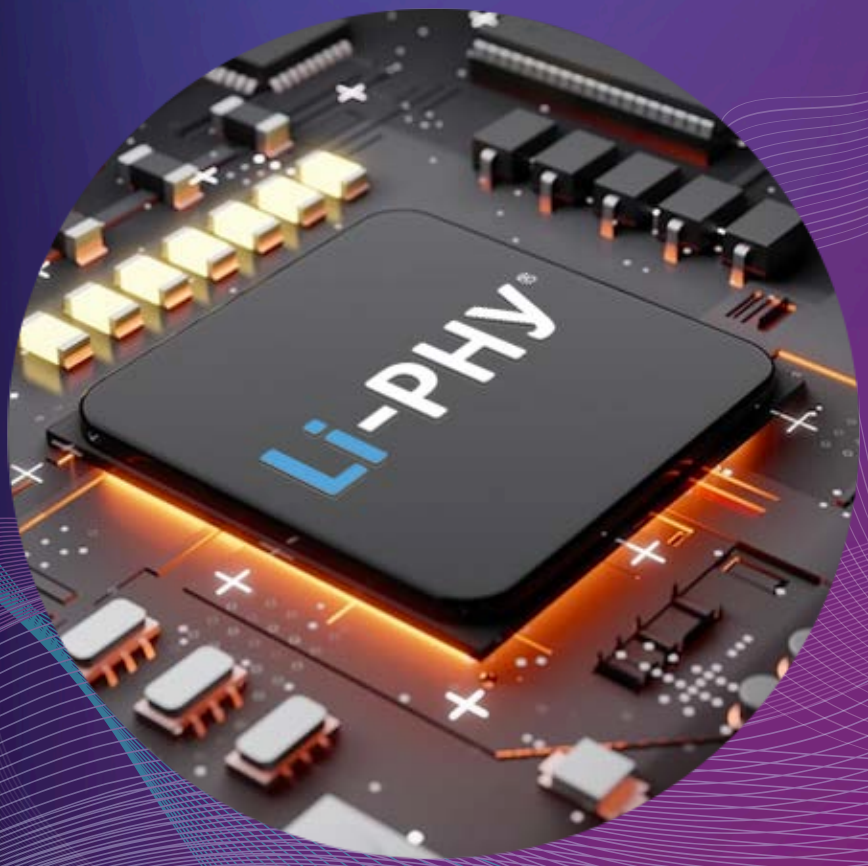
CYBERCALL INNOVATOR

Challenge Statement (Open Category):

Design a solution that would address the gap between traditional software-centric security approaches and intricate hardware interactions to fortify data centers against emerging and evolving threats, while preserving the robustness and integrity of critical digital infrastructures where massive volumes of data reside.

Solution: Li-PHY® System Defender

Li-PHY System Defender is a unidirectional intelligent system that is powered by embedded artificial intelligence (AI). The solution can analyse memory dumps by utilising advanced differential and integration algorithms to provide a reliable, end-to-end, holistic system protection.



FLEXXON™

Founded in 2007 and headquartered in Singapore, Flexxon is a global company that specialises in next generation hardware cybersecurity solutions and industrial NAND storage devices. Rooted in its strong pedigree as a leading industrial NAND flash storage solutions provider, Flexxon is committed to protecting the basic rights of all citizens of the digital economy through constant innovation to address the evolving cybersecurity needs of today.

https://www.flexxon.com/

camelliachan@flexxon.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

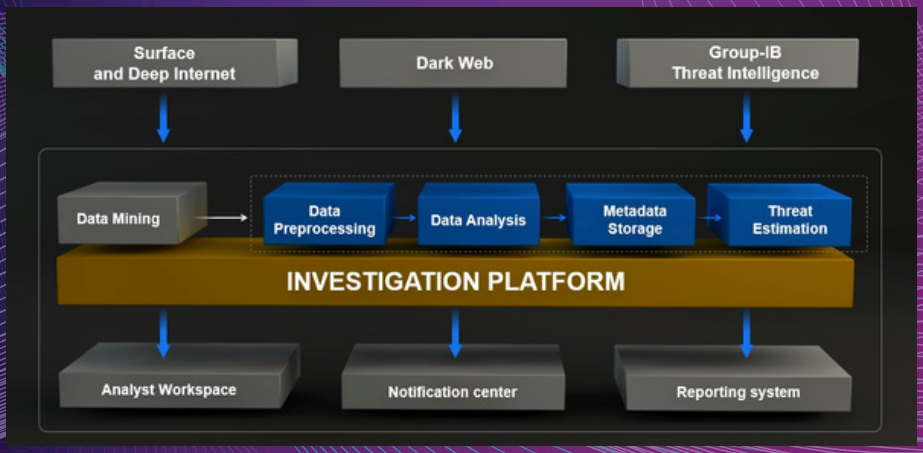
CYBERCALL INNOVATOR

Challenge Statement:

Build a system which is able to detect new or imminent cyber threats from public conversations on blogs, Twitter and Dark Web forums.

Solution: Begemotik

Begemotik is an innovative solution to efficiently investigate cyber threats and threat actors in Dark Web and social networks. It uses big data, threat intelligence and machine learning (ML) & Natural Language Processing (NLP) to create digital profiles of hackers, uncover cyber communities, and correlate discussions to automate and facilitate the work of investigators. Its flexibility, visualisation and interactive assistance make it viable for tech, finance, government and law enforcement.



GROUP-IB

Group-IB, with its headquarters in Singapore, is one of the leading solutions providers dedicated to detecting and preventing cyberattacks, investigating high-tech crimes, identifying online fraud, and protecting intellectual property. Group-IB's technological leadership and R&D capabilities are built on the company's 20 years of hands-on experience in cybercrime investigations worldwide and over 70,000 hours of cybersecurity incident response.

https://www.group-ib.com/

info@group-ib.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

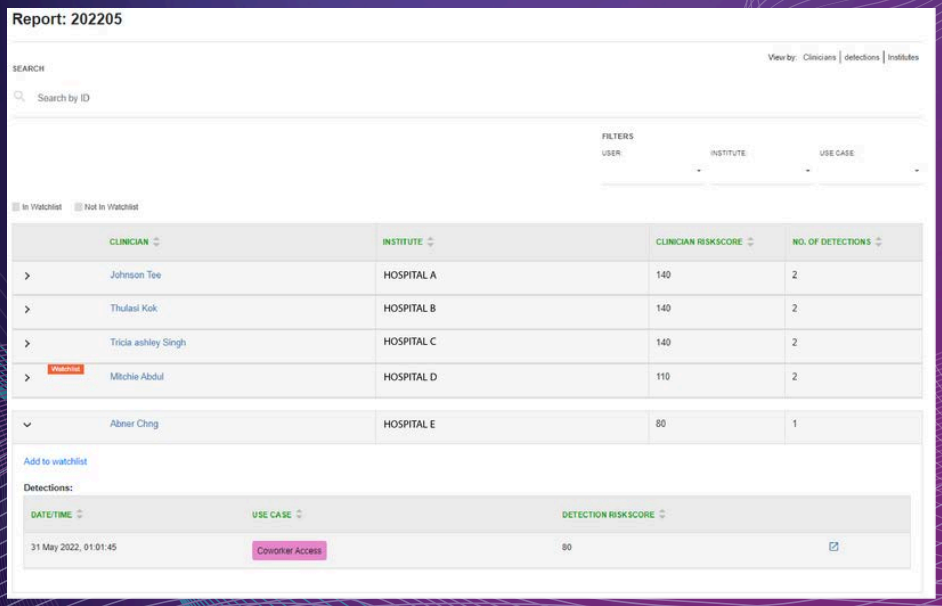
CYBERCALL INNOVATOR

Challenge Statement:

Electronic healthcare record systems have to be safeguarded from unauthorised access and data abuse. There is a need to quickly and effectively detect any user activity that is unauthorised, or not in line with clinician-patient relationships. Traditionally, effective monitoring of access logs is challenging. Pre-defined rules are manually defined and are often difficult to calibrate. Alerts have to be manually reviewed, which are tedious, time-consuming, and not responsive enough.

Solution: Electronic Medical Record (EMR) Monitor

InsiderSecurity worked with healthcare end-users to develop a product named EMR Monitor to address this problem, leveraging on InsiderSecurity's expertise and technology in user behaviour analytics. The product learns the user activity and automatically detects unauthorised activity, without the need for manually defined rules. It detects suspicious activity that is difficult, if not impossible, to catch previously and it enables a faster response.



InsiderSecurity

Founded by Singaporean cybersecurity experts in 2015, InsiderSecurity has a track record of developing advanced, homegrown cybersecurity products that are used by listed companies, government agencies and many small and medium-sized enterprises (SMEs) today. InsiderSecurity is able to detect internal cyber threats early before there are any serious data losses. Its technology is useful for early detection of supply chain attacks such as the SolarWinds and Kaseya cyber attacks.

https://www.insidersecurity.co/

sales@insidersecurity.co

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

CYBERCALL INNOVATOR

Challenge Statement:

Design and build an integrated solution using automation, analytics and artificial intelligence (AI) to enhance threat detection capabilities, improve asset protection using automated response and increase visibility of the cloud environment for a holistic defence of the Cloud.

Solution: Cloud Security X (CSX)

Cloud Security X (CSX) is an innovative cloud security solution that uses advanced analytics and AI to secure all cloud layers, i.e. Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service. CSX simplifies cloud security. In particular, CSX will be a game changer for small and medium-sized enterprises (SMEs) by providing access to affordable and good cloud security services.

InsiderSecurity

Founded by Singaporean cybersecurity experts in 2015, InsiderSecurity has a track record of developing advanced, homegrown cybersecurity products that are used by listed companies, government agencies and many small and medium-sized enterprises (SMEs) today. InsiderSecurity is able to detect internal cyber threats early before there are any serious data losses. Its technology is useful for early detection of supply chain attacks such as the SolarWinds and Kaseya cyber attacks.

https://www.insidersecurity.co/

sales@insidersecurity.co

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

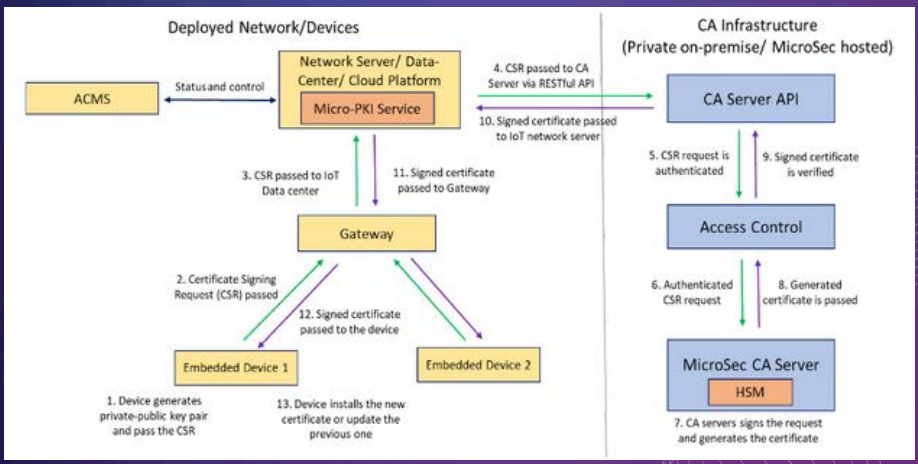
CYBERCALL INNOVATOR

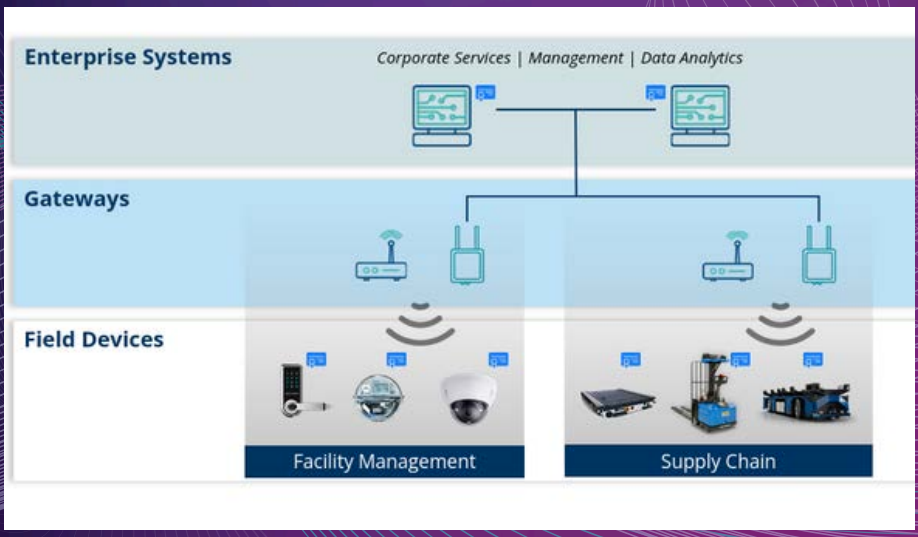
Challenge Statement (Open Category):

Design an end-to-end cybersecurity solution for constrained Internet of Things (IoT) sensor devices.

Solution: MicroPKI - An optimised Public Key Infrastructure (PKI) for IoT and Connected Devices

We have developed a Micro-PKI technology to enable PKI on resource and bandwidth-constrained IoT devices. It is an end-to-end security solution which includes two-way authentication, signature generation/verification, key exchange, data encryption and certificate management. A 150-byte micro-certificate is utilised to allow public key infrastructure to be deployed on a sensor network platform.





MICROSEC

A deep tech, cybersecurity company, MicroSec is a global market leader in IoT security for OT environments, and is the world's first company to achieve Security-by-Design for constrained IoT devices, enabling end-to-end security from the Edge (level 0/1) to the cloud and on-premise. MicroSec's industry expertise includes critical infrastructure for utilities, energy, 4G/5G, mining, as well as manufacturing, supply chain/logistics, and automotive.

http://www.usec.io/

rodney@usec.io

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

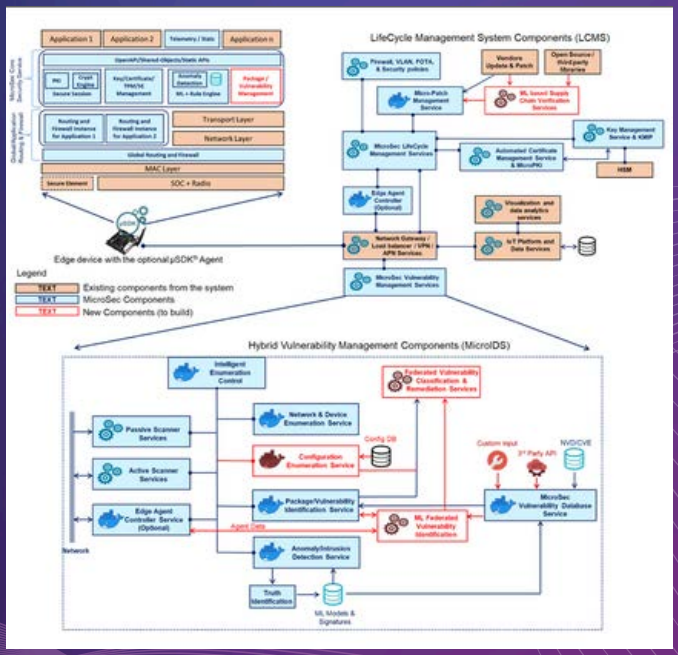
CYBERCALL INNOVATOR

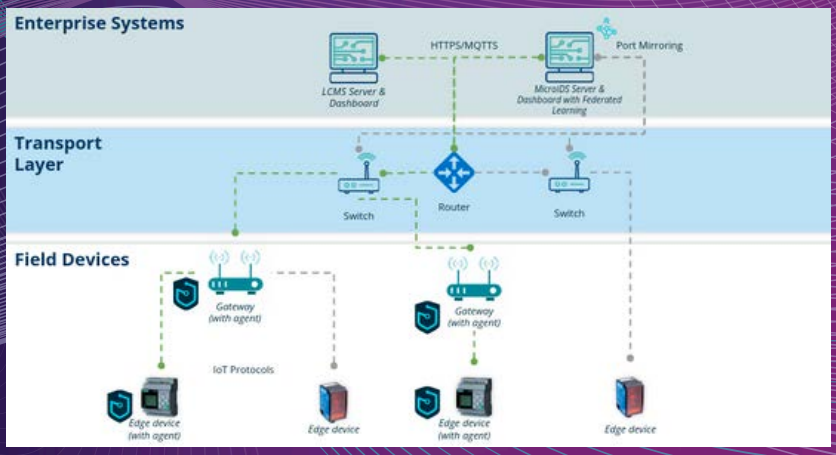
Challenge Statement (Open Category):

Design a unified Internet of Things (IoT) or Industrial Internet of Things (IIoT) security solution for connected products utilising edge computing.

Solution: MicroFL - An Optimised Federated Learning Framework for True Edge Devices

An intrusion detection solution that can achieve machine learning (ML)-based anomaly detection on (constrained) edge devices including Micro controllers, providing protections from zero-day attacks. The machine learning will improve its detection accuracy by including federated learning capabilities, which allows multiple edge agents to train models without sharing their raw data, helping to protect sensitive information from being shared.





MICROSEC

A deep tech, cybersecurity company, MicroSec is a global market leader in IoT security for OT environments, and is the world's first company to achieve Security-by-Design for constrained IoT devices, enabling end-to-end security from the Edge (level 0/1) to the cloud and on-premise. MicroSec's industry expertise includes critical infrastructure for utilities, energy, 4G/5G, mining, as well as manufacturing, supply chain/logistics, and automotive.

http://www.usec.io/

rodney@usec.io

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

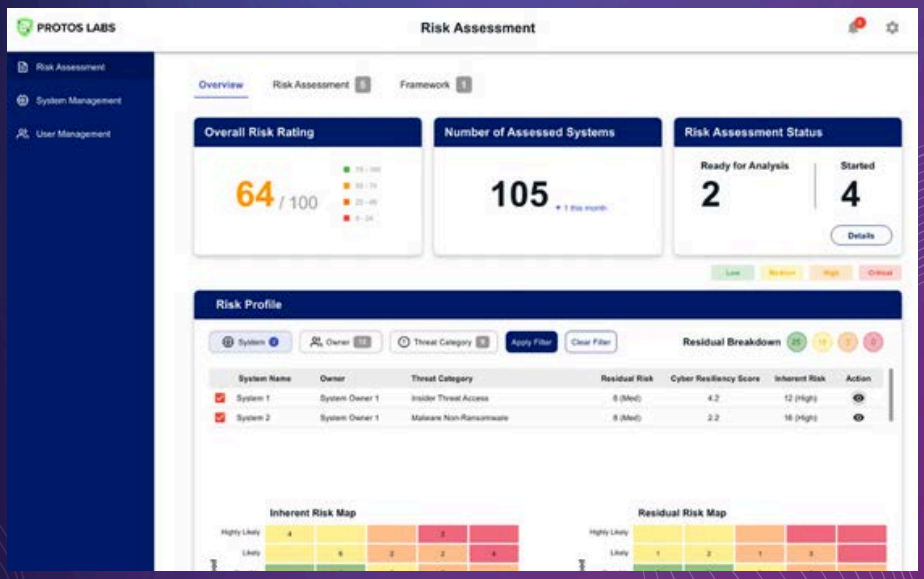
CYBERCALL INNOVATOR

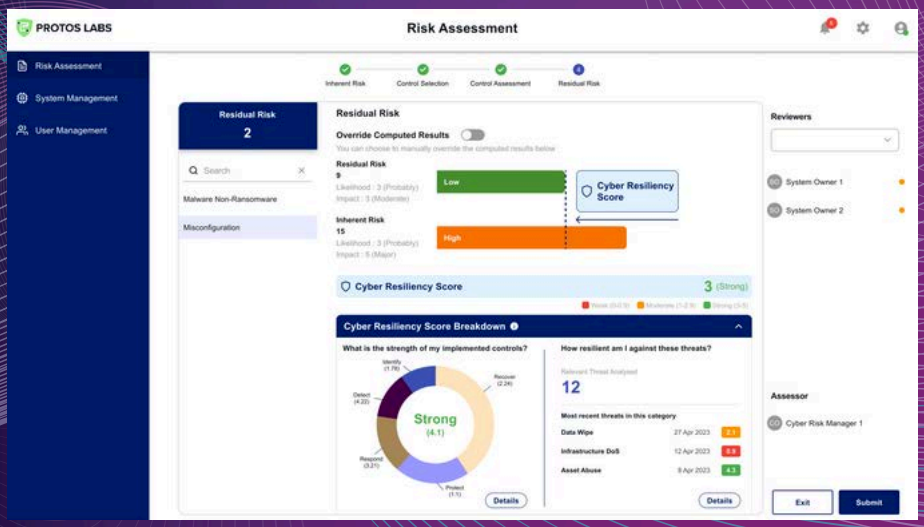
Challenge Statement:

Develop a solution to conduct cybersecurity risk and compliance assessments (from identification to remediation) and leverage the same data set to calculate the return on investment (ROI) on security investments.

Solution: NEXUS

We developed NEXUS, a cyber risk intelligence platform for a leading university in Singapore. It prioritises real-world cyber attacks and vulnerabilities using a threat-based approach, enabling continuous assessment and rapid remediation. Using insurance-grade risk models, it quantifies return on security investment (ROSI). It leverages threat intelligence, advanced machine learning, statistical models, combining diverse datasets to provide real-time cyber risk insights for the end-user.





PROTOS LABS

Protos Labs, founded in 2021, is a Singapore-based cybersecurity company led by ex-Booz Allen cybersecurity leaders Joel Lee and Simeon Tan. Our cyber risk analytics solution enables organisations to achieve an end-to-end view of their cyber programme across real-world threats, attack surface, risk and controls and financial loss quantification. This solution is used by enterprises and insurers alike, where we support cyber underwriting for the latter.

https://www.protoslabs.sg/

enquiry@protoslabs.sg

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

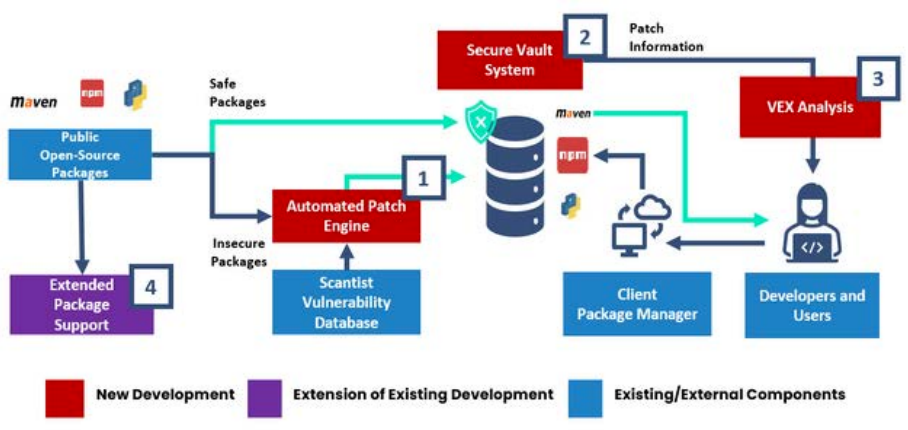
CYBERCALL INNOVATOR

Challenge Statement (Open Category):

Enhance the security of open source components used in the software development process.

Solution: Secure Open-Source Supply Chain via AI-enabled Patching and Delivery

Scantist's Secure Open-Source Supply Chain automates the supply of risk-managed open-source packages that can be used without maintenance, security, or compatibility concerns. The solution leverages AI and code-generating Large Language Models (LLMs) to create security-hardened versions of open-source packages at scale, ensuring fast and effortless mitigation of open-source risks for software development teams.



SCANTIST

Scantist, a Singaporean company specialising in application security tools and services, was a spin-off of Nanyang Technology University (NTU). Scantist's main focus is on providing comprehensive software application protection against both known and unknown vulnerabilities and code across applications, ensuring enhanced security for their clients' software solutions.

https://www.scantist.com/

jeremy@scantist.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

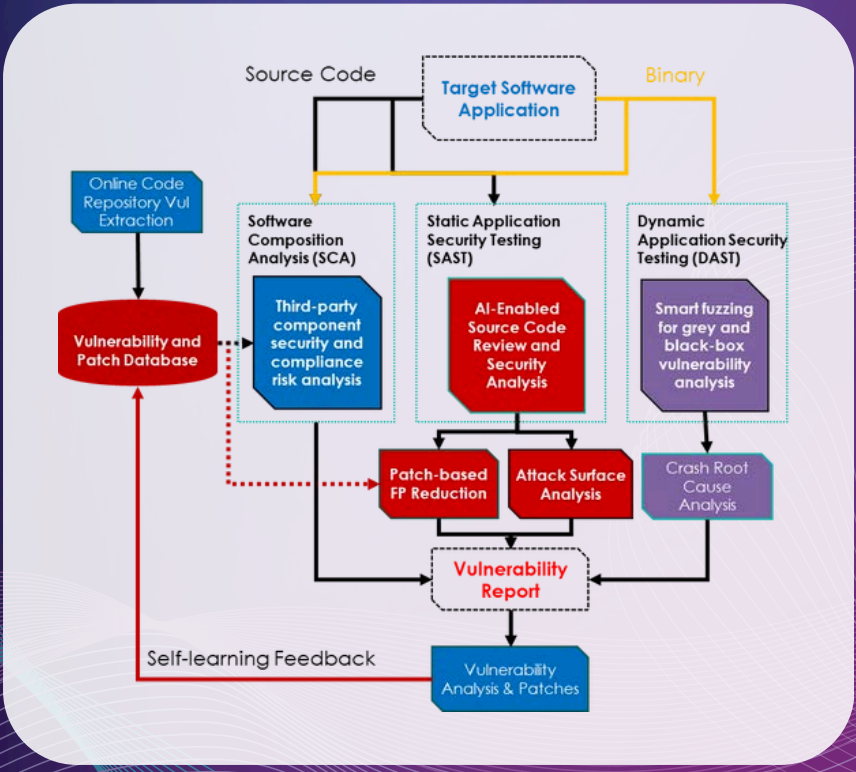
CYBERCALL INNOVATOR

Challenge Statement:

Scan and review software and applications (developed in-house and commercial products) to identify malicious code and vulnerabilities, as well as provide recommendations on remediation actions.

Solution: Detection and Handling of Malicious Code

Scantist developed an AI-enabled Application Security Testing Framework that combined AI-based techniques with program analysis to create a scalable and extensible malicious code/vulnerability identification framework. The platform is now available as a Software-as-a-Service (SaaS) offering for small and medium-sized enterprises (SMEs), enterprises and government users.



SCANTIST

Scantist, a Singaporean company specialising in application security tools and services, was a spin-off of Nanyang Technology University (NTU). Scantist's main focus is on providing comprehensive software application protection against both known and unknown vulnerabilities and code across applications, ensuring enhanced security for their clients' software solutions.

https://www.scantist.com/

jeremy@scantist.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

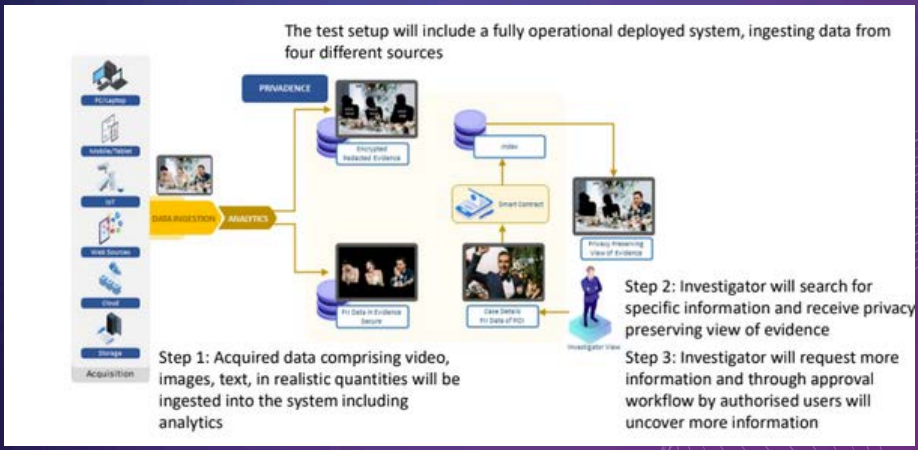
CYBERCALL INNOVATOR

Challenge Statement:

Develop a solution to preserve the privacy of victims while allowing digital forensic searches and analytics to be performed on Personally Identifiable Information (PII) data and sensitive images or videos.

Solution: Privadence

Privadence provides a timely solution to growing privacy challenges in digital forensics. It addresses the conflict between law enforcement investigation and privacy needs. Leveraging AI, it rapidly identifies evidence which includes personal data and redacts it to ensure privacy. It provides tools to allow investigators to do their work efficiency while proactively safeguarding privacy.



S2T
Unlocking Cyberspace

Stimulation Software & Technology (S2T) specialises in cyber intelligence software. Our key offerings are Deep Webint, a suite of open-source intelligence (OSINT), and Deep Fusion, our innovative data fusion platform enabling in-depth investigations. Both products are powered by advanced algorithms and AI, enabling users to extract, analyse, and utilise digital intelligence. Our products deliver actionable insights to customers worldwide.

https://www.s2t.ai/

ori@s2t.ai

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

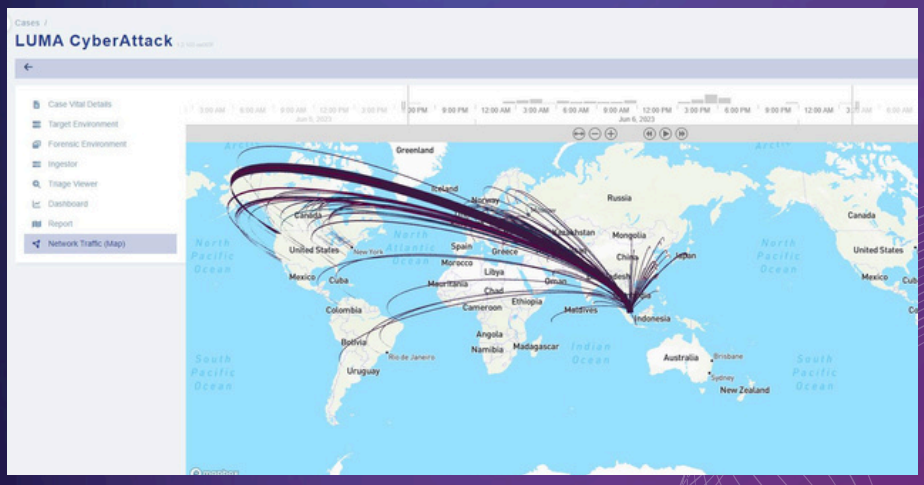
CYBERCALL INNOVATOR

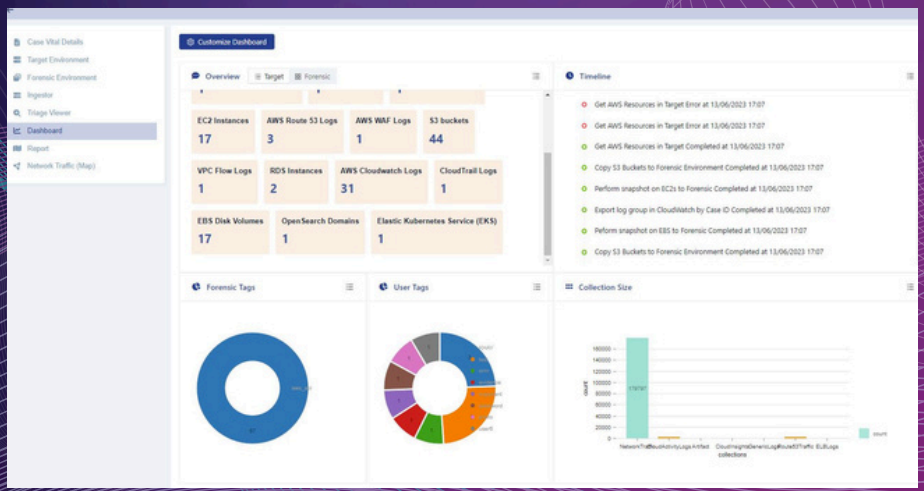
Challenge Statement:

Design and develop a web-based platform that conducts triage to search, preserve and analyse forensic artifacts from Cloud Service Providers (CSP).

Solution: Anvil Crawler

Anvil Crawler is a sophisticated platform designed for efficient digital cloud forensic investigations. It allows investigators to access information from CSP such as AWS and Azure. Leveraging on cutting-edge algorithms, it rapidly sifts through data to pinpoint crucial digital evidence, and maintain its integrity for further scrutiny.





S2T
Unlocking Cyberspace

Stimulation Software & Technology (S2T) specialises in cyber intelligence software. Our key offerings are Deep Webint, a suite of open-source intelligence (OSINT), and Deep Fusion, our innovative data fusion platform enabling in-depth investigations. Both products are powered by advanced algorithms and artificial intelligence (AI), enabling users to extract, analyse, and utilise digital intelligence. Our products deliver actionable insights to customers worldwide.

https://www.s2t.ai/

ori@s2t.ai

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

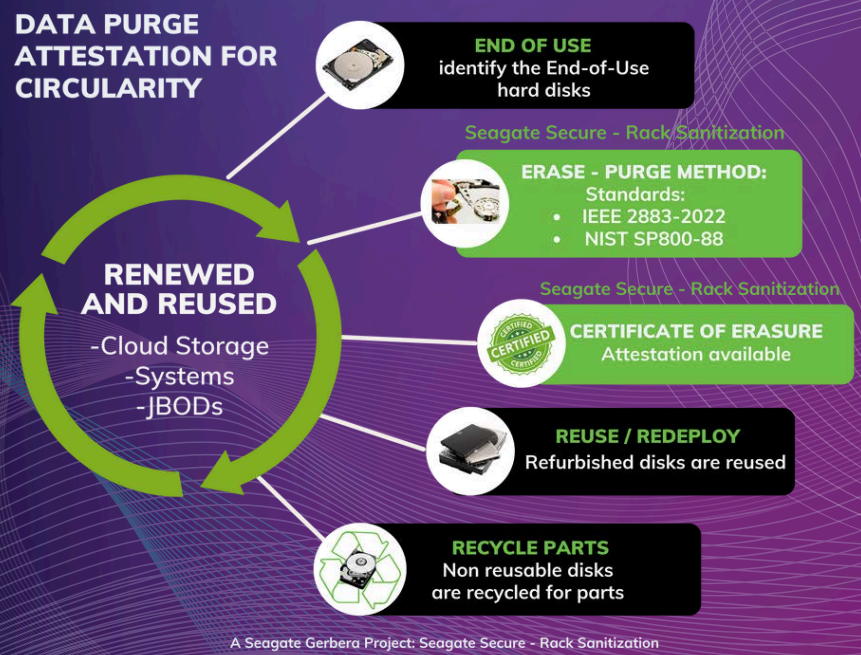
CYBERCALL INNOVATOR

Challenge Statement (Open Category):

Data-bearing device destruction techniques (such as degauss, shredding) wastes precious resources and the solution is not green as many of these devices end up in landfills. This is not a sustainable solution. The challenge is how do we promote the reuse, redeployment and recycling of data-bearing storage devices while complying with growing privacy and data sanitisation requirements?

Solution: Data Sanitisation Attestation - Certified Erase

Seagate's Certified Erase technology enables Seagate's Hard Disk Drives (HDD) and Solid State Drives (SSD) to perform firmware-based (instead of software-based) data erasure with attestation. Public Key Infrastructure (PKI) parameters established within the firmware during manufacturing can be used to produce a digitally signed certificate to prove data erasure at the drive's redeployment or end-of-life.



SEAGATE

Seagate is a world leader in data storage, shipping over 4 Zettabytes of storage systems in our 40-year history.

https://www.seagate.com/

Reach us through our website

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

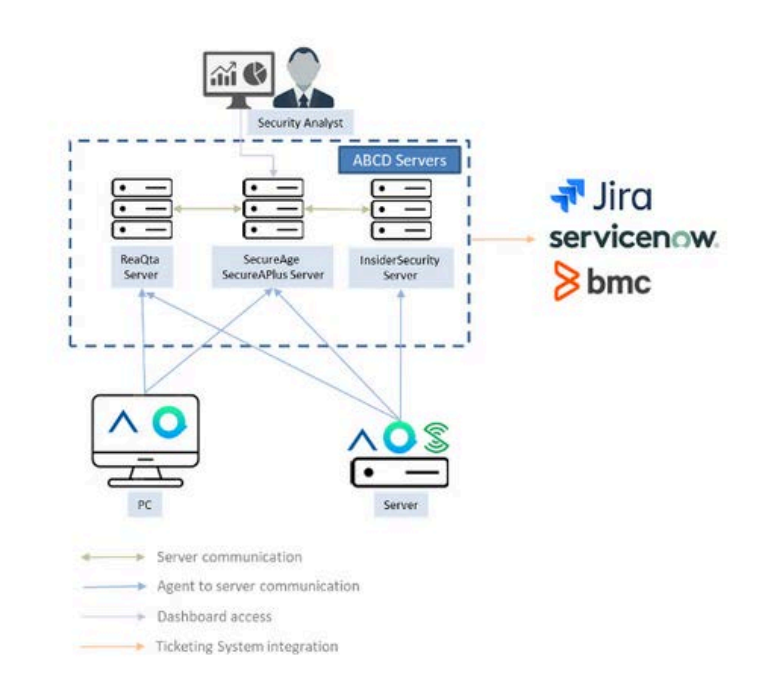
CYBERCALL INNOVATOR

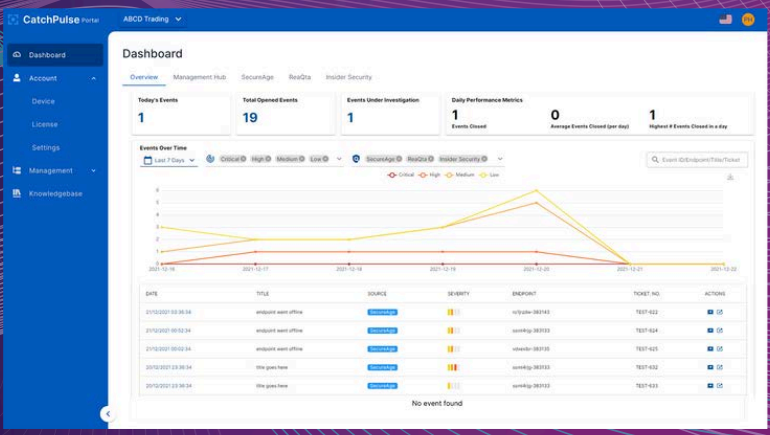
Challenge Statement:

Develop a fully integrated threat mitigating solution based on CSA's 'Be Safe Online' measures with automated threat identification, protection, detection and response.

Solution: Asset Based Cyber Defence (ABCD)

As part of the CSA Cybersecurity Industry Call for Innovation and in updating their integrated Cybersecurity measures, SecureAge Technology, Insider Security and Reaqta come up with Asset Based Cyber Defence, also known as ABCD. ABCD helps small and medium-sized enterprises (SMEs) and enterprises protect themselves against ransomware, data breaches, and insider threats.





SecureAge

SecureAge specialises in providing data security for the home and corporate organisations. With a 20-year history of zero plain data breaches, we are trusted by governments, research institutes and organisations across the globe to protect them from the most advanced and persistent cyber threats.

https://www.secureage.com/

pennyheng@secureage.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

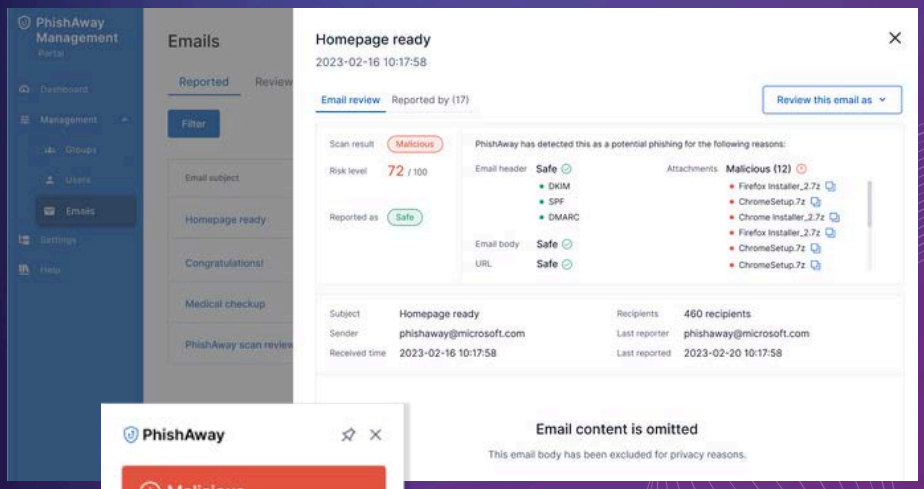
CYBERCALL INNOVATOR

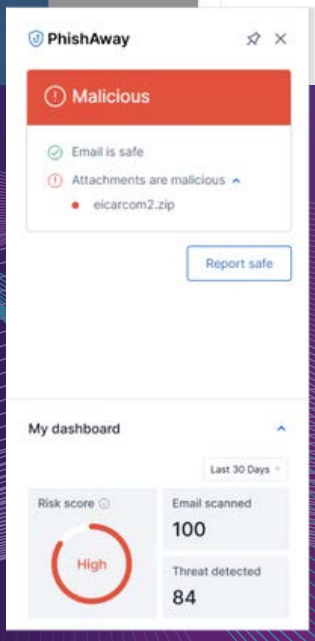
Challenge Statement:

Develop a comprehensive anti-phishing solution to identify and filter phishing emails with a high degree of accuracy based on machine learning, and leverage on the same data set to implement an intelligent phishing simulation platform capable of generating realistic phishing drills that adapt to the phishing attacks targeting the organization.

Solution: Phish-Away

SecureAge's Phish-Away is an AI-powered solution that detects and simulates email phishing attacks. Instead of using reactive deny-list solutions against three billion phishing emails daily, Phish-Away pits detector and simulator against each other to build machine learning engines with comprehensive zero-day detection against email phishing attacks.





SecureAge

SecureAge specialises in providing data security for the home and corporate organisations. With a 20-year history of zero plain data breaches, we are trusted by governments, research institutes and organisations across the globe to protect them from the most advanced and persistent cyber threats.

https://www.secureage.com/

pennyheng@secureage.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

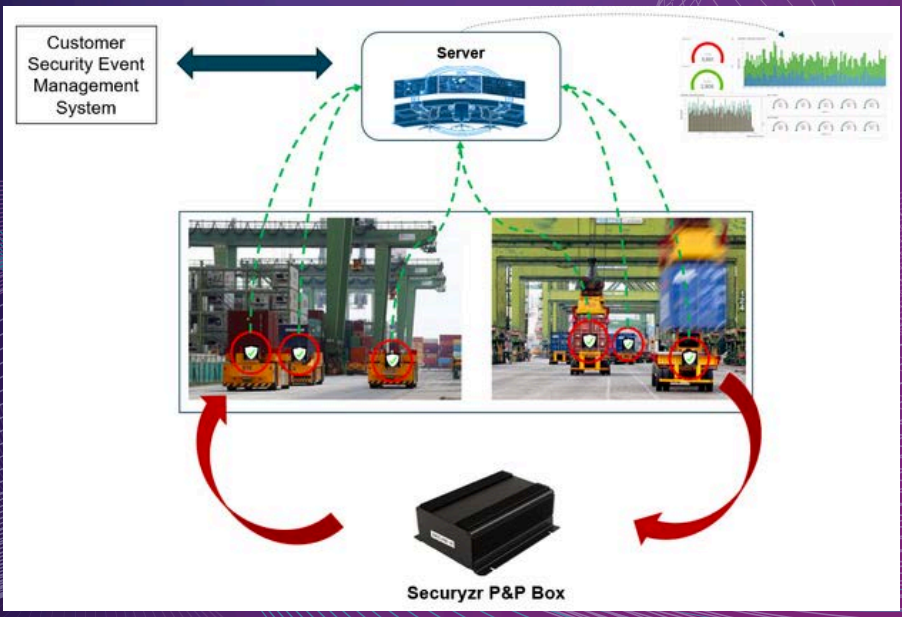
CYBERCALL INNOVATOR

Challenge Statement:

Detect and protect against potential cyber threats to local Autonomous Prime Movers (APMs) platform systems with infrastructure layers in a scalable and implementable manner.

Solution: Securyzr™ P&P Solution

As part of the 'Secure Autonomous Prime Movers' project, Secure-IC has provided a cybersecurity solution called 'Securyzr™ Plug & Play' solution for detection and protection against cyber threats to local Autonomous Prime Movers (APMs) platform systems and for communication with infrastructure layers in a scalable and implementable manner.



SECURE-IC
THE SECURITY SCIENCE COMPANY

Founded in 2010, Secure-IC is a Spin-off of Télécom Paris University and benefits directly from 15 years of research results conducted by ones of the best scientists in the embedded cybersecurity field. Leadership, innovation and creative intelligence constitutes the DNA of Secure-IC, which displays proudly this legacy in the company's baseline: "The Security Science Company".

https://www.secure-ic.com

contact@secure-ic.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

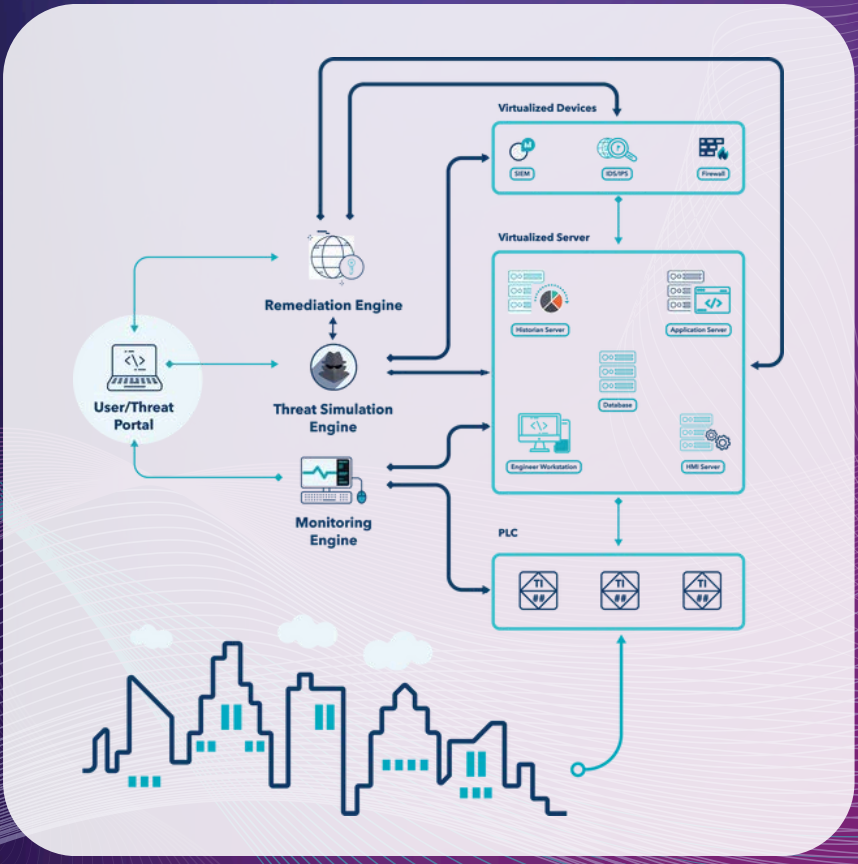
CYBERCALL INNOVATOR

Challenge Statement:

Develop a solution that addresses the challenges related to software patch management for Operational Technology (OT) environments. The goal is to ensure timely and secure application of patches to production systems, minimising the risk of cyber-attacks and maximising system safety and functionality.

Solution: Threat Simulation and Validation Platform for Industrial Control Systems (ICS)

SkillSpar's 'Automated Attack & Remediation Engine – for Critical Infrastructure' offers a unique threat simulation and validation platform for Industrial Control Systems (ICS). It uses a digital replica of physical assets to validate patches, updates, and configurations. The solution requires minimal user intervention and conducts continuous ICS threat simulations, detecting vulnerabilities and providing remediation recommendations.



SkillSpar is an innovative company that bridges the gap between knowledge and practical skills. At our platform, we firmly believe in the power of "Knowledge to Skills." That's why we offer a unique learning experience that includes simulations, assessments, and training to help learners elevate their skills and propel their careers forward. We strive to create an engaging and interactive environment for educators and learners.

https://www.skillspar.com

ssp-sales@skillspar.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

POWERED BY:

CYBERSECURITY INNOVATION DAY 2023

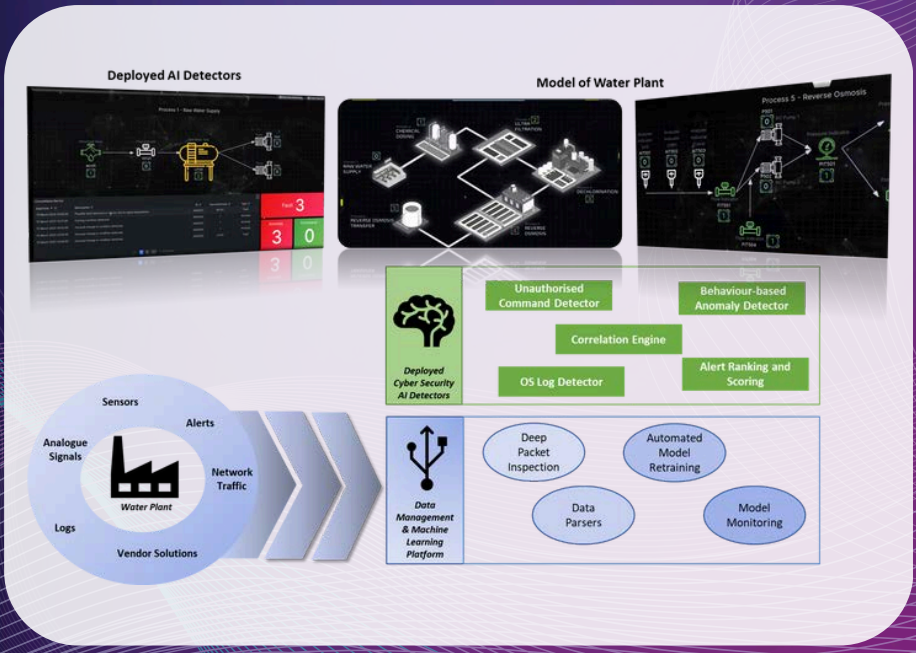
CYBERCALL INNOVATOR

Challenge Statement:

Build a detection engine model to detect security incidents and unauthorised commands through packet inspection. The detection engine should be able to adapt to different supervisory control and data acquisition (SCADA) network setups, data types and networks that can be scaled up through virtualisation with detailed simulation using hardware-in-the-loop (e.g. Programmable Logic Controller (PLC).

Solution: Adaptive and Intelligent Cyber Monitoring for Operational Technology (OT), AICYMO

AICYMO uses techniques and algorithmic detectors built on an machine learning operation (MLOps) platform to make sense of various sources of OT system data from SCADA network and engineering workstations to complete the cyber picture for an OT system. Methods include modelling a digital twin of the SCADA system to simulate plant behaviour, and detect anomalies when actual observations deviate from the simulation.



ST Engineering

ST Engineering is a global technology, defence and engineering group serving customers in more than 100 countries. Backed by indigenous capabilities and deep domain expertise, the Cyber Business is an industry leader in cybersecurity with over two decades of experience, delivering a holistic suite of trusted cybersecurity solutions to empower cyber resilience for government and ministries, critical infrastructures, and commercial enterprises.

https://www.stengg.com/en/digitaltech/cybersecurity/

cybersecurity@stengg.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS Enterprise

CYBERSECURITY INNOVATION DAY 2023

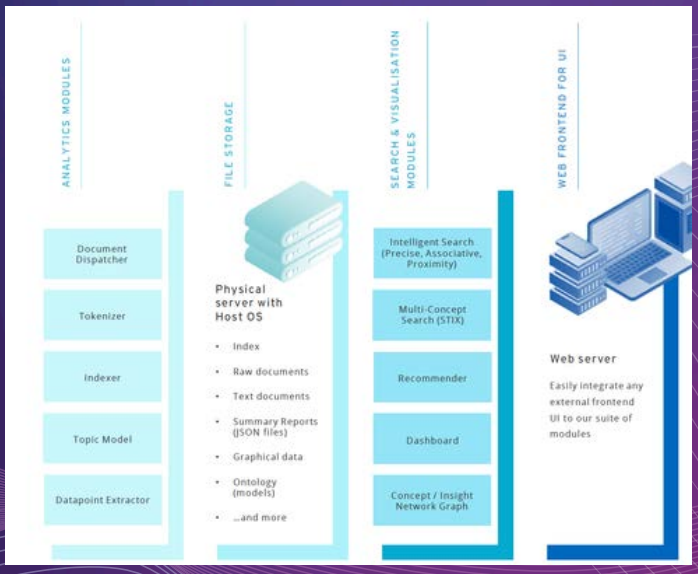
CYBERCALL INNOVATOR

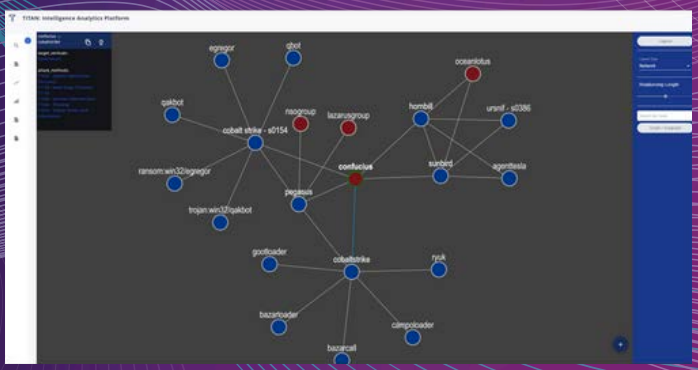
Challenge Statement:

Develop an advanced threat monitoring solution that enables Security Operation Centers to deal with big datasets and identify noteworthy correlation from all data points. It should help security analysts identify both "known" and "unknown" threats based on historical and real-time insights.

Solution: Smart Cyber Intelligence Management Tool

SCIM (Smart Cyber Intelligence Management) is a robust artificial intelligence (AI) platform that ingests and processes open-source intelligence (OSINT) data from various sources. The platform promotes collaboration and enables quick discovery of reports via AI-assisted search. Routine tasks like data extraction and classification are automated, allowing analysts to focus on strategic work. SCIM utilises machine learning (ML) and AI to conduct in-depth analysis to find and visualise hidden links between entities.





TAU EXPRESS

TAU Express was co-founded in 2018 by Professor Lam Kwok Yan, Associate Vice President (Strategy and Partnerships) at Nanyang Technological University (NTU) Singapore. Together with a team of AI experts, TAU developed TITAN, which applies AI and ML techniques to process and analyse large volumes of unstructured data to aid in decision-making and intelligent information retrieval across a wide range of industries, including cybersecurity.

https://www.tauexpress.com/

info@tauexpress.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

CSA SINGAPORE

POWERED BY:

NUS National University of Singapore | Enterprise

CYBERSECURITY INNOVATION DAY 2023

CYBERCALL INNOVATOR

Challenge Statement:

Detect and de-identify PII automatically, and manage secure data sharing in a scalable and efficient manner.

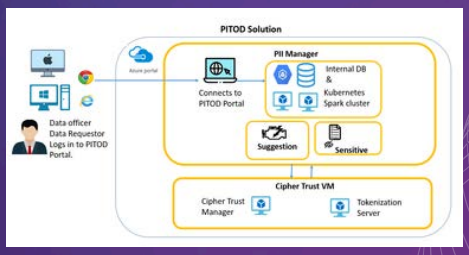
Solution: Personal Identifiers Tokenized On Demand (PITOD)

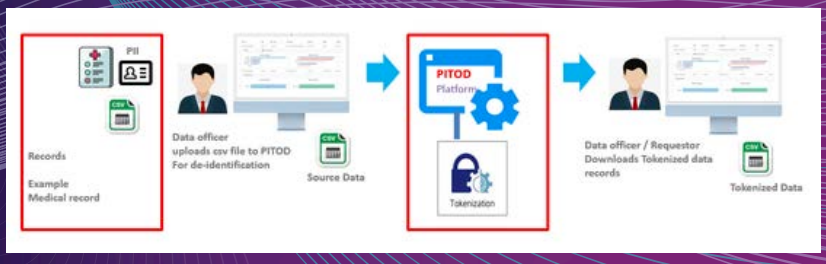
Medical data is often transmitted to other digital systems for research and audit purposes. The currently available products are heavily reliant on manual efforts for encryption, which is tedious and prone to error.

With PITOD System , data will be securely processed and automatically tokenized, saving IT security team's efforts to manually check and reducing error, allowing users to conduct secure data sharing efficiently and automatically, reducing human efforts. This will reduce any potential delays or operational issues that could arise out of personnel changes or human errors.

To reduce risk of accidental exposure of PII, Quasi-PII data can also be further identified and tokenised. Thus, ensuring secure sharing of sensitive data confidently and effectively.

PITOD is able to re-identify original data easily when required.





THALES

Thales has been present in Singapore since 1973 originally supporting aerospace-related activities in the Asia-Pacific region. Since then, the company has expanded and is today involved in the primary businesses of Aerospace (including Air Traffic Management), Defence & Security and Digital Identity & Security. Thales employs close to 2,000 employees across 3 sites in Singapore providing solutions that help customers make critical decisions. As a people-centred company, Thales was ranked 50th out of 200 on The Straits Times Singapore's Best Employers 2021 list, a recognition of our investment in nurturing talent.

https://www.thalesgroup.com/en/countries/asia-pacific/thales-singapore

ruren.siak@thalesgroup.com
eric.tan@thalesgroup.com

CYBERSECURITY INDUSTRY CALL FOR INNOVATION

AN INITIATIVE BY:

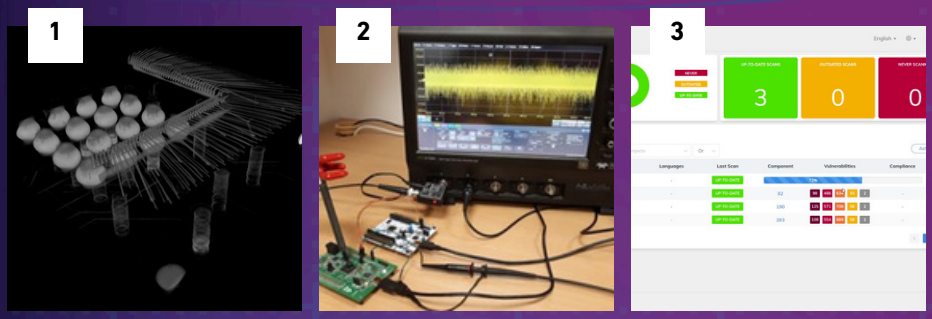
CSA SINGAPORE

POWERED BY:

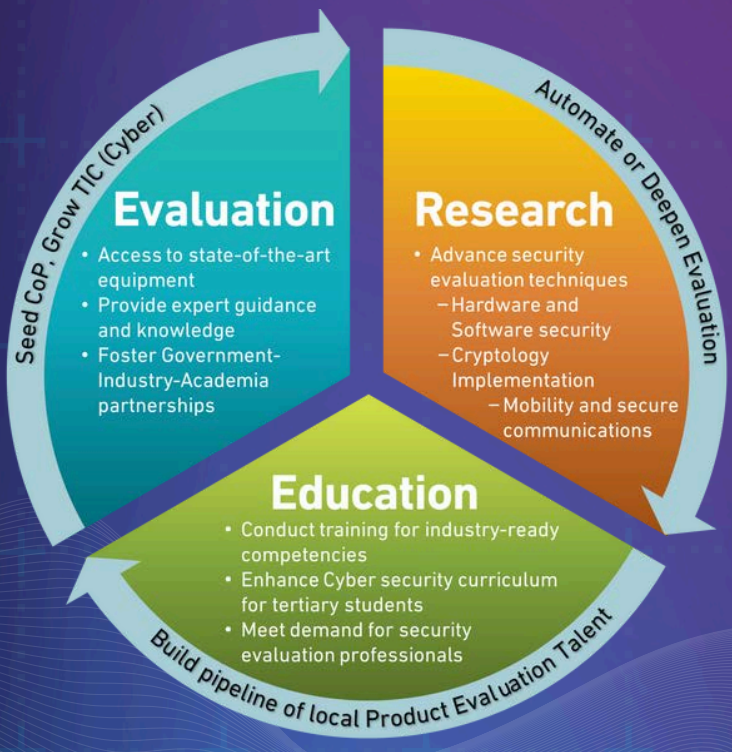
NUS National University of Singapore | Enterprise

NiCE

National Integrated Centre for Evaluation (NiCE) @ NTU



NiCE is a collaboration between CSA and Nanyang Technological University, Singapore (NTU). With its collection of state-of-the-art equipment, NiCE is strategically located in NTU for its knowledge, expertise and experience in hardware and software assurance.



One-Stop Centre Supporting the TIC (Cyber) Industry

NiCE aims to lower the barrier of entry in areas of hardware and software certification, for product developers and evaluation companies. NiCE also supports research, having supported programmes such as 'SOCure: Assuring Hardware Security by Design in Systems on Chip'. Lastly, NiCE also provides training and education opportunities for talent development in this developing and trending field.

CSA SINGAPORE

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

KEY CAPABILITIES

1. **Sample preparation & Imaging**: Exposing the microelectronic chip for circuit analysis, fault injection (FI) and side-channel analysis (SCA) evaluation. Circuit editing and non-destructive 3D computed tomography imaging of circuit board.
2. **Fault injection (FI) and side-channel analysis (SCA)**: Overcoming countermeasure in circuitry and recovering encryption key through non-invasive and semi-invasive methods.
3. **Software**: Binary code and software composition analysis tools to scan for vulnerabilities in source code.

https://www.ntu.edu.sg/nice

nice_enquiries@ntu.edu.sg

iTrust

iTrust Centre for Research in Cyber Security

iTrust was jointly established by Singapore University of Technology and Design (SUTD) and Ministry of Defence (MINDEF) in 2012 to improve its understanding of cyber threats to cyber-physical systems (CPS) and develop translatable technologies to mitigate such threats. iTrust's approach is based on the interdisciplinary fields of control theory, artificial intelligence, axiomatic design and software engineering.

iTrust and its sister lab, the National Cybersecurity R&D Laboratories (NCL), together form the Cyber Security R&D Laboratories of Singapore. This national effort of co-joining both labs' Operational Technology (OT) and Information Technology (IT) expertise and infrastructure provides a high-fidelity and hyper-realistic network of IT-OT platforms for cyber security practitioners to conduct cyber research, drills and training.

Featured Project

NSoE in DeST-SCI Phase 2

Funded by the Cyber Security Agency of Singapore for Phase 2 of the National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure (NSoE-DeST-SCI), iTrust will build upon the research outcomes of the previous phase, enhance the scalability and robustness of existing tools, and facilitate rapid technology transfer in four domains: electric power, IoT, maritime, and water.

ACADEMIC COLLABORATORS: PI: Professor Aditya Mathur; Co-PIs: Professor Jianying Zhou, Associate Professor Binbin Chen, Assistant Professor Sudipta Chattopadhyay

INDUSTRY PARTNERS: American Bureau of Shipping (ABS), Ensign Infosecurity (Singapore) Pte Ltd, Pacific Light Power Pte Ltd, Power Automation Pte Ltd, Resync Technologies Pte Ltd

iTrust Centre for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

KEY CAPABILITIES

iTrust hosts several world-class testbeds and training platforms:

1. Electric Power Intelligent Control (EPIC)
2. Internet of Things Automatic Security Testbed (IoT)
3. Secure Water Treatment (SWaT)
4. Water Distribution (WADI)

The interconnected testbeds support R&D, technology validation, international cyber exercises, education and training programmes towards the safety and security of cyber-physical systems.

The testbeds have been conceived, designed and built collaboratively by a group of SUTD faculty, international consultants, and engineers from public utilities in Singapore.

The testbeds are available to SUTD and its partners across the world.

https://itrust.sutd.edu.sg/

itrust@sutd.edu.sg

NCL

National Cybersecurity R&D Lab (NCL)

NCL offers computing resources and controlled experimentation environments to facilitate collaborative research among academia, government bodies, and industry. The NCL Cybersecurity Compute Infrastructure (CCI) comprises a cluster of 300+ nodes with diverse provisioning mechanisms, security data, and security services. The NCL CCI provides a realistic and safe environment to test and validate before the systems are deployed in production.

Featured Project

CRITICAL INFRASTRUCTURE DEFENCE EXERCISE (CIDEX) 2022

The cyber defence exercise involved over 100 participants from the Digital and Intelligence Service (DIS) and 16 other national agencies across the Critical Information Infrastructure (CII) sectors.
To strengthen Whole-Of-Government (WoG) cyber capabilities, the project focused on detecting and tackling cyber security threats posed to Information Technology (IT) and Operational Technology (OT) networks within critical infrastructure.
NCL hosted an Enterprise IT network of VMs that was integrated with three OT testbeds contributed by iTrust — the Secure Water Treatment (SWaT), Water Distribution (WaDi) and Electric Power and Intelligent Control (EPIC) OT testbeds.

COLLABORATORS: Ministry of Defence (MINDEF), Cyber Security Agency of Singapore (CSA), iTrust, Singapore University of Technology and Design & ST Engineering

National Cybersecurity R&D Laboratory

KEY CAPABILITIES

NCL Testbed is set up to support cyber-security researchers engaged in the research, development, experimentation, and testing of innovative cybersecurity technology.

NCL's cloud services include:

- Compute & Baremetal
- GPUs
- Custom cybersecurity environments such as replaying APT & various cyberattacks
- Capture the Flags (CTFs), Cyber-Exercises

NCL supports a wide range of training and cyber exercises, including CTF events. The recent events include NUS GreyHats CTF 2023, AYCEP, and YCEP.

https://ncl.sg/

support@ncl.sg

Cyber Security Agency of Singapore
www.csa.gov.sg

NUS Enterprise
enterprise.nus.edu.sg