Annex A - List of CyberCall 2022 Recipients

SN	Recipients	Description
1	Custodio Technologies Pte. Ltd.	**Company:** Custodio Technologies was first established in 2014 as a Cybersecurity R&D Centre of Israel Aerospace Industries (IAI) Ltd for Asia. In 2016, it turned into a fully-fledged cybersecurity company providing proactive defence solutions that was successfully translated from R&D programmes. Custodio Technologies continues to participate in R&D innovation projects as well as develop customised solutions for customers with specific needs. **Project:** OT Threat Vector Path Discovery on Digital Asset Map The project is to develop an innovative solution that performs non-intrusive threat discovery on Operational Technology (OT) network. The solution creates a comprehensive digital map of the intended network based on logs and data collected from multiple sources. Coupled with advanced machine learning models, the solution will perform virtual penetration testing on the digital map and automatically generate results. This is a cost-effective solution for companies to continue scanning for irregularities.
2	Scantist Pte. Ltd.	**Company:** Scantist is a Singaporean company specialising in application security tools and services. It was founded in 2016 as a spin-off from Cyber Security Lab at Nanyang Technology University (NTU). Scantist strives to provide comprehensive software application protection against both known and unknown vulnerabilities and code across applications, ensuring enhanced security for their clients' software solutions. **Project:** Secure Open-Source Supply Chain via AI-enabled Patching and Delivery The project aims to automate 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 Model (LLM)s to create security-hardened versions of open-source packages at scale, ensuring fast and effortless mitigation of open-source risks for software development teams.

SN	Recipients	Description
3	Simulation Software & Technology (S2T) Pte. Ltd.	**Company:** Simulation Software & Technology (S2T) is a Singapore-headquartered company which specializes in cyber intelligence software. Their key product offerings are in the areas of Open Source Intelligence (OSINT) and data fusion for investigative agencies. These products are powered by advanced algorithms and AI, enabling users to extract, analyse, and utilise digital intelligence to deliver actionable insights to customers. **Project:** <u>Privadence – Privacy Preserving Digital Forensics</u> The project aims to address the conflict between law enforcement investigation and privacy needs by leveraging AI to rapidly identify evidence that includes personal data and redacts it to ensure privacy. It provides the tools to allow investigators to do their work efficiently while proactively safeguarding privacy and addressing the growing privacy challenges in digital forensics.
4	First Watch Singapore Pte. Ltd.	**Company:** First Watch was formed in 2019 by CTEK, a New Zealand's leading industrial automation company in partnership with University of Waikato. They developed a cybersecurity platform that is the first of its kind, designed to prevent attacks on the Operational Technology (OT) network. With cyberattacks on the rise and critical infrastructure increasingly vulnerable, First Watch would play a critical role in protecting businesses and communities around the world. The University of Waikato is well known for its competence in cybersecurity research and education, hence their participation in the collaboration that founded First Watch gave access to leading researchers and experts in the field of cybersecurity. **Project:** <u>OT Kernel Prevention of Cyber Attacks</u> The project leverages machine learning mechanism to detect the tactics, techniques, and procedures (TTPs) in the industrial environment and minimise the risk of a cyber-attack. First Watch, in collaboration with University of Waikato, use patterns of legitimate behaviour produced in computer-made policies, in the environment where actions are filtered with the aid of human-made policies. Users of the solution would be able to attribute unusual behaviour to the TTPs and monitor the derived threat score relative to the threshold where action is required.