Annex B – Details of Cybersecurity Industry Call for Innovation (CyberCall) 2025 and Awardees of CyberCall 2024

1) CyberCall 2025 Call for Proposals

The CyberCall 2025 was launched by Mr Tan Kiat How, Senior Minister of State for Digital Development and Information at the CyberSG Innovation Day 2025 held on 14 November 2025. It consists of two categories: i) Open Call Category, and ii) User-Driven Category.

i) Open Call Category: The CyberCall is seeking proposals in these focus areas:

1. Cybersecurity for Artificial Intelligence (AI)

   To safeguard AI systems and maintain the integrity, confidentiality, trustworthiness and reliability of AI applications in an increasingly connected and digital world.

2. AI for Cybersecurity

   To harness the power of AI to strengthen organisations' cyber defences in protecting their systems, data and networks; improving threat detection and responding more effectively to cyber-attacks.

3. Quantum Safe

   To protect critical digital systems, data, and infrastructure from the potential threat of cryptographically relevant quantum computers by transitioning to quantum-resistant solutions and enabling cryptographic agility and defence-in-depth.

4. Operational Technology or Internet of Things Security

   To safeguard critical infrastructure, Industrial Control Systems, and internet-connected devices from cyber threats and vulnerabilities.

5. Cloud Security

   To safeguard infrastructure, data and applications hosted in cloud environments, while maintaining the confidentiality, integrity and availability of resources in the cloud.

6. Privacy-Enhancing Technologies

   To safeguard the privacy of individuals and confidentiality of their data while using systems and digital services, thereby empowering individuals to manage their data securely and complying with privacy regulations.

ii) **User-Driven Category:** Companies are also invited to address user-driven challenge statements provided by end-users – YTL Power Seraya, Pacific International Lines, and Home Team Science and Technology Agency. The aim is to leverage technologies to improve the efficacy of cybersecurity management processes in sectors such as maritime and energy.

The challenge statements are:

1. To develop a cost-effective, standalone AI component that seamlessly integrates with existing Privileged Access Management systems to autonomously analyse session screen recordings and log data for irregular or suspicious user behaviour. The solution should address the inefficiencies and potential for oversight in manual reviews, whilst overcoming the interpretive challenges of non-natural language logs to provide accurate, actionable security insights.

2. To develop an automated patch management, pre- and post-patch testing activities across both Windows and Linux systems, aiming to reduce manual effort and enhance operational efficiency.

3. To develop a secure, real-time information sharing platform that enables multiple agencies to collaborate on cryptocurrency investigations while maintaining operational security and avoiding duplication of investigative efforts across blockchain addresses and entities.

The closing date for submission is **13 January 2026.** More information on the CyberCall, including the latest challenge statements can be found on the website.

2) CyberCall 2024 Awardees

At the CyberSG Innovation Day, the CyberSG Talent, Innovation and Growth Collaboration Centre (TIG Centre) also announced the results of CyberCall 2024, with five cybersecurity companies awarded for the Open Category, a total of approximately S$3 million in funding. The projects were selected through a rigorous evaluation process that assessed the quality of the proposed solution, its wider applicability and benefits, and team competency.

CyberCall 2024 awardees are:

1. **Betterdata**

- **Company description:** A Singapore-based generative AI and privacy company that uses advanced deep learning and privacy-preserving methods to create synthetic data with no personally identifiable information. These methods allow organisations to securely share high-quality, privacy-compliant data for AI development and data collaboration. Betterdata was also awarded a contract by the US Department of Homeland Security to enhance its cyber defence simulations using synthetic data, a global validation of its technology.

- **CyberCall 2024 solution:** To develop a Tabular Foundational Model (TFM) for synthetic data generation. The project aims to safeguard individuals' privacy and the confidentiality of their data. The TFM will be designed to generate synthetic data in no-, low-, and high-data environments for various enterprise applications, including AI, machine learning, analytics, and testing.

2. **Ensign InfoSecurity**

   - **Company description:** One of Asia's largest comprehensive cybersecurity service providers, Ensign offers tailored solutions to meet clients' cybersecurity needs. Headquartered in Singapore, Ensign specialises in advisory, assurance, architecture design, systems integration, and managed security services, including advanced threat detection, threat hunting, and incident response. With two decades of proven experience and in-house R&D, Ensign serves both public and private sector clients across the Asia Pacific region.

   - **CyberCall 2024 solution:** To develop an end-to-end pipeline that provides comprehensive, evidence-based malware analysis insights in a timely and automated manner using generative AI technologies.

3. **Goldilock Secure Asia**

   - **Company description:** The UK-based company is developing a product that enables authorised users to instantly and remotely disconnect their systems from any network, without relying on an internet connection. This form of physical isolation is particularly useful for securing critical infrastructure in complex environments such as defence, utility, transport and other critical asset security. Reinforcing its commitment to the region, Goldilock has established its Asia Pacific headquarters in Singapore, investing S$1.2 million to open a local office, with plans to hire about 20 engineers over the next three years.

   - **CyberCall 2024 solution:** To develop a flexible out-of-band trigger for physical network segmentation to be deployed into OT systems. This will be rolled out as an Original Equipment Manufacturer solution first and later through licensing a system-on-module, ensuring compliance with regulatory standards and initiating the testing phase to evaluate the functionality and performance of the prototypes solution and later through licensing a system-on-module, ensuring compliance with regulatory standards and initiating the testing phase to evaluate the functionality and performance of the prototypes.

4. **Ryzome**

- **Company description:** A cybersecurity company that provides runtime security and forensics for virtualised environments, Ryzome was founded on the principle that effective security requires a tamper-resistant monitoring approach. Its customer base primarily consists of organisations with virtualised IT infrastructure that needs to secure sensitive data and critical business operations against advanced adversaries.

- **CyberCall 2024 solution:** To create a tamper-resistant threat detection solution that provides organisations with a trusted security layer for real-time protection of Linux workloads, and provide the appropriate level of cybersecurity protection.

5. **SpeQtral**

    - **Company description:** A pioneer in quantum communications with a vision to build and deploy global quantum networks, SpeQtral develops quantum-secure products and services designed to protect sovereign and enterprise telecommunication networks against both classical and future quantum-based cyberattacks. Combining terrestrial and space-based solutions, SpeQtral aims to secure the world's networks against the threats posed by the imminent quantum revolution and to drive innovation in quantum communications that will serve as the building blocks of the future quantum internet.

    - **CyberCall 2024 solution:** To accelerate quantum-safe migration by developing a cost-effective Quantum Key Distribution system that optimises the trade-off between cost and security, addressing an existing product gap in the quantum security market.

3) About CyberCall

The CyberCall was first launched in 2018 by the Cyber Security Agency of Singapore (CSA), helps catalyse the development of innovative cybersecurity solutions in Singapore. It brings together cybersecurity companies and end-users by matching industry proposals to real-world challenges and supporting the co-development of innovative cybersecurity solutions. Awarded companies will receive funding support of up to S$1,000,000 for up to 24 months under CSA's Cybersecurity Co-Innovation and Development Fund.

The CyberCall aims to uplift Singapore's cybersecurity landscape and strengthen organisations' cyber resilience. Specifically, it seeks to:

- Catalyse the development of innovative cybersecurity solutions to meet national and strategic needs;
- Develop a vibrant local cybersecurity ecosystem by building advanced cybersecurity capabilities and growing the talent pipeline; and
- Identify and articulate mid- to long-term cybersecurity challenges to encourage the trial and adoption of novel solutions.

Starting from 2024, the CyberCall has been organised by the TIG Centre, a joint initiative between the National University of Singapore and CSA. The TIG Centre, which officially opened in July 2024, aims to establish Singapore as the premier global cybersecurity innovation hub by uplifting talent, innovation, and growth programmes.