Cybersecurity Industry Call for Innovation
June 2024 Edition (Virtual)

By

CSA SINGAPORE

Uplifting the development of Singapore's cybersecurity ecosystem

Powered by

CyberSG TIG COLLABORATION CENTRE

www.cybercall.sg

Introduction

Cybersecurity is a fast-paced evolving industry involving deep technologies, and companies / end users are under constant pressure to protect their systems. Consistent innovation is the only way to defend against the rising scale and sophistication of cyber-attacks and innovation is at the heart of cybersecurity.

The CyberCall initiative seeks to catalyse the development of innovative cybersecurity solutions to strengthen cyber resilience, and at the same time, provide opportunities for cybersecurity companies to develop new cybersecurity products.

The Call is split into a segment with user driven challenge statements, as well as an open category. Companies are welcome to submit proposals in any of the areas outlined in the document attached.

Thank you and we look forward to receiving your proposals.

A. USER DRIVEN CHALLENGE STATEMENTS

2024JUN-CS01: Trusted Collaboration Partner Assurance Platform

Challenge	Develop a platform/service that provides assurance of the security postures of connected systems from partners/vendors. Some expected capabilities are for the solution to automatically monitor and update on possible breaches in partners/vendors systems, provide secure channels for info exchange and collaboration, and facilitate the identification and remediation of the vulnerabilities of the systems to mitigate risks effectively. The platform/service should also provide assurance that all connected systems have a basic level of security to mitigate against threats in the future.
Background	Organisations today collaborate and work with a wide range of vendors and partners to conduct business. These often result in the need for connected systems which raises the risks and results in a widened attack surface. However, not all partners/vendors have in-house cybersecurity expertise to continually monitor and maintain the security posture of their systems. Therefore, this end user is seeking the development of a platform / service that can provide assurance of the security postures of connected vendor / partner systems.
Requirements	The solution should have end-to-end coverage of every system connected in the collaboration, support tasks to understand the threats/vulnerabilities as they appear and alert every participant to take necessary actions to minimise the risks. While companies are invited to propose innovative ways of addressing the problem described that are not limited to the descriptions in this write-up, some of the expected functions of the solution are also as follows. This system should have the ability to: 1. Collect the logs of the system and conduct vulnerability scan of the system and have a backend platform, that allows uploads of the security data collected from end-point solutions. This backend platform should also consolidate vendor security data and conduct a risk assessment to alert users on the potential risk/impact. Have the ability to produce a risk score based on an internationally recognised framework and recommend remediation/mitigation. 2. Provide an alert when there are new vulnerabilities and conduct an assessment on systems to identify those that may be affected and at risk. 3. Be extendable to integrate with state-of-the-art/ leading AI-enabled security suites in the market (e.g. Microsoft Security Copilot, Google Cloud Security AI Workbench, etc), using API or other means, to enrich the vulnerability management capabilities of the platform. 4. It could be designed with Privacy Enhancing Technology with the option to wipe out the previous end-point results as needed as per user and/or vendor's request. 5. The solution should be simple to configure and deploy without the need of cybersecurity professionals, and be cost effective enough to be adopted by Small/Medium Enterprises (SMEs). *Note: This end-user is not looking for a full-fledged Third-Party Risk Management (TPRM) product or Supply Chain Risk Management (SCRM) product.*

2024JUN-CS02: Cross Domain File Transfer to High Trust Network

Challenge	Operational Technology (OT) environments have traditionally used manual processes and portable storage devices for data/file transfer in the OT environment. Much of these tasks are labour-intensive and consistent and proper access control is necessary. The challenge is to establish a secure environment for cross domain file transfer of files into a high-trust network. The solution should allow the secure transfer of files from external networks to a high-trust network, and come with access control, encryption, authentication, continuous monitoring and auditing mechanisms. It should also prevent communications initiated from the high trust network to the external network and allow the enforcement of policies and rules that govern data sharing between different domains.
Background	Critical Systems like CII need the ability for cross-domain file transfer into high-trust networks. The high-trust network is a critical asset that hosts sensitive information, and it is imperative that the transfer mechanism is robust, secure, and reliable. It is also important to have the ability to ensure that the integrity and confidentiality of information are maintained when files are transferred from external networks. The solution should mitigate potential cyber threats and prevent unauthorized access or data breaches. It should also be suitable for sending patch files or malware definitions from an external network into the high trust network.
Requirements	The solution must facilitate the secure transfer of files from external network to one or more high-trust networks. It should contain, but not be limited to the following: 1. Access Control: • Comprehensive access control system to manage permissions and ensure that only authorized users can initiate transfers. • Define the access control model and specify the granularity of permissions. • Include the ability to manage user roles and access rights. 2. Encryption: • Strong encryption standards to protect data during transit. • Specify the encryption protocols and standards to be used for securing files during transfer. • Include requirements for end-to-end encryption to prevent data exposure. 3. Authentication: • Robust authentication mechanism to verify the identity of users and systems involved in the file transfer. • Detail the authentication methods that will be supported (e.g., multi-factor authentication, public key infrastructure). 4. Continuous Monitoring and Auditing: • Continuous monitoring and have an auditing mechanism to track all file transfer activities. • Provide specifications for real-time monitoring tools to detect and alert on suspicious activities. • Include requirements for comprehensive logging of all file transfer activities, including timestamps, user identities, file metadata, and transfer status. • Specify the retention period for audit logs and the format in which they should be stored.

5. Prevention of Outbound Communication:
    - The solution must prevent any initiation of file transfers from the high-trust network to external networks.
    - Include mechanisms to enforce this policy and detail how violations will be handled.

6. Policy and Rule Enforcement:
    - Define the framework for creating, managing, and enforcing policies and rules that govern data sharing between different domains.
    - Include the ability to update and modify policies as per evolving security needs.

7. Compliance and Standards:
    - To state its expected compliance with relevant International or Singapore security standards.

8. Scalability and Maintenance:
    - The solution should be scalable to accommodate future growth in data transfer needs.
    - Include provisions for regular updates, patches, and maintenance activities.

Note: This end-user is not looking for a USB-storage product, Data-Diode product, or man-in-the-loop solution.

2024JUN-CS03: Automated Cybersecurity Risk Management for Cloud Applications Change Request

Challenge	Develop a solution that can automate, simplify, and provide recommendation for cybersecurity risk management for cloud application change requests. The change requests can be for enterprise's functional (e.g. new features) and non-functional (e.g. cybersecurity patches) updates.
Background	Alterations to cloud applications carry cybersecurity risks, including coding errors and unintended logic faults. Implementing new cloud applications may require changes to the configuration management such as the firewall rules and the routing tables which might affect the security posture of the system. Implementing changes requires rigorous risk assessments to mitigate these risks. An automated risk management solution is needed to perform dynamic risk assessments based on the change request, provide a recommendation for appropriate change schedules, and notify stakeholders. The dynamic nature of these operations demand swift turnaround times, but the current manual effort is inefficient to handle the volume of change requests.
Requirements	The solution should contain, but not be limited to the following: 1. Develop an automated risk management solution that can understand a ticketing system using Large Language Model (LLM) and conduct a risk framing from the information provided in the ticket. It should include identifying the scope of the process, asset inventory affected, prioritization, and any legal/regulatory requirement involved. The first ticketing system to be tested will be JIRA. 2. It should perform dynamic risk assessment to aggregate risks arising from multiple changes, analyse past incidents arising from the changes, and identify the threats, vulnerabilities, and impacts. 3. It should recommend a change schedule based on information such as the criticality of the assets and systems affected. 4. It should provide a summarised and easy to understand information using Generative AI to notify the stakeholders. It should also collect response from the stakeholders after the information has been sent. 5. The solution must be scalable to support different ticketing products, such as having a common interface design for the integration to different ticketing products. 6. The first ticketing tool to be integrated and tested is JIRA. 7. The solution must be designed to support different Cloud Service Providers including AWS, Azure and GCP

B. CSOC: OPEN CATEGORY SEGMENT

The Open Category segment is for cybersecurity proposals that do not fulfil any of the Challenge Statements listed. Proposals should clearly explain the problem, specific issue(s) that it aims to address, articulate the innovation required for solving the identified problem and have concrete go-to-market plans. Proposal for innovation development must result in new product development and not be an existing solution / improvement(s) on existing solutions.

For proposals submitted under the Open Category, the applicant company must secure at least one committed end-user by the third milestone. This end-user must be interested to deploy the solution if the project is successful. The company can leverage on "minimum viable products"[1] and/or market ready technologies to develop cybersecurity applications with new features and functionalities that would meet new and emerging demands of cybersecurity users.

The broad areas for this year's call are as follows:

1. **2024JUN-CSOC1: Cybersecurity for Artificial Intelligence (AI)**
   Safeguarding AI systems and the data they process from various cyber adversarial attacks to maintain the integrity, confidentiality, trustworthiness and reliability of AI applications in an increasingly connected and digital world.

2. **2024JUN-CSOC2: AI for Cybersecurity**
   Harnessing the power of AI to strengthen cyber defences, improve threat detection, and respond more effectively to the evolving and sophisticated nature of cyber threats, thereby helping organisations protect their systems, data and networks from cyber attacks.

3. **2024JUN-CSOC3: Quantum Safe**
   Protecting 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 defense-in-depth.

4. **2024JUN-CSOC4: Operational Technology (OT) / Internet of Things (IoT) Security**
   Safeguarding critical infrastructure, Industrial Control Systems (ICS) and internet-connected devices from cyber threats and vulnerabilities.

5. **2024JUN-CSOC5: Cloud Security**
   Safeguarding data, applications, resources and infrastructure hosted in cloud environments, while maintaining the confidentiality, integrity and availability of resources in the cloud.

6. **2024JUN-CSOC5: Privacy-Enhancing Technologies (PET)**
   Safeguarding the privacy of individuals and confidentiality of their data while using systems and digital services, to empowering individuals to manage their data securely and in compliance with privacy regulations.

[1] A minimum viable product is a product with just enough features to satisfy early customers, and to provide feedback for future product development.