Cybersecurity Industry Call for Innovation
November 2024 Edition

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 CyberCall 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

2024NOV-CS01: Analysis of Privileged Access Management Session

Challenge	Construct an Artificial Intelligence (AI) module designed to seamlessly amalgamate with current Privileged Access Management (PAM) systems, enabling the scrutiny of PAM session recordings to pinpoint irregularities in user behaviour.
Background	PAM serves as an identity security mechanism that identifies and obstructs unauthorised entry to vital assets while monitoring the activities of privileged users during their access to these critical resources. It maintains a record of the sessions via logs and screen video captures. Presently, the analysis of screen recordings is conducted manually, a process that is both tedious and time-consuming. The log recordings are not exhaustive and are challenging to interpret due to their lack of natural language, while video recordings can be extensive and cumbersome to review, often leading to human oversight. Consequently, there is a pressing requirement for a cost-effective, standalone AI component that can be effortlessly incorporated into existing PAM frameworks.
Requirements	The solution should encompass, but not be limited to, the following features: 1. Extract and process data from PAM solutions, handling both word-formatted logs and screen recording videos. 2. Perform automated real-time behavioural analysis, comparing user actions against benchmarks or blacklisted processes. 3. Control and restrict user access to designated assets. 4. Conduct scheduled behavioural analyses after PAM sessions to ensure compliance with benchmarks. 5. Identify and flag unacceptable behaviours during both real-time and post-session analyses. 6. Recognise acceptable behaviours that may deviate from benchmarks but are not considered security risks. 7. Allow for benchmark settings to be input in various formats, including release notes and natural language instructions. 8. Utilise User and Entity Behaviour Analytics (UEBA) training with 'golden images' and typical user behaviour patterns as references. 9. Operate efficiently without excessive bandwidth, time, or processing power consumption. 10. Classify the confidence level of detected anomalies into categories such as HIGH, MEDIUM, and LOW. 11. Provide real-time and post-session alerts for detected anomalies. 12. Enable querying of recording contents using natural language. 13. Generate analysis reports in a user-friendly format.
Additional Information	1. Integrate smoothly with existing PAM systems without complex setup procedures or loss of existing PAM features. 2. Function in offline environments, particularly in Operational Technology (OT) settings. 3. Be compatible with both Information Technology (IT) and OT environments, accommodating one-way data transfer from OT to IT using Data Diodes. 4. The solution may be a non-video analytic tool, provided it meets the requirement

2024NOV-CS02: Data Security Incident Management

Challenge	Create a data security management tool that autonomously identifies and safeguards data instantaneously, employing Artificial Intelligence to ascertain the sensitivity of data contingent on context as opposed to predefined rules.
Background	New AI technologies such as Copilot enable organisations to operate more efficiently and effectively. These systems can analyse data from both within and outside the organisation, delivering results based on the user's prompts. However, they also introduce new risks to data management and privacy. To integrate new AI technologies like Copilot, our organisation must enhance our capabilities to: 1. Comply with Personal Data Protection Laws in the various countries where our organisation operates. 2. Prevent the spread of data breaches across our global network. 3. Respond to any data breaches as swiftly as possible. Given the vast amount of unstructured data, it is impractical to preprocess and label all data at rest. We need a solution capable of independently identifying and protecting data in real-time. Most solutions on the market rely on precise definitions to identify data, which often results in a low accuracy rate due to a lack of contextual understanding.
Requirements	The solution should encompass, but not be limited to, the following features: 1. Utilising AI to determine data sensitivity based on context rather than predefined rules. For instance, training the system to recognise the nature of documents such as business contracts, personal information, etc. 2. The capability to monitor and detect potential real-time data breaches as they occur. 3. The ability to generate user-friendly summaries of data breach incidents for reporting to senior management and local authorities. 4. The provision of a comprehensive dashboard for reporting on risk and compliance status. Management of data loss prevention strategies (restricting email, USB transfers, printing, etc.) in line with designated data classifications.
Additional Information	The solution could be a standalone end-to-end system or an integration with existing Data Loss Prevention products.

2024NOV-CS03: Incorporating Generative AI into Cybersecurity Incident Management in OT/IoT.

Challenge	Develop a cyber security incident response utility employing GenAI to synthesise the incident details, carry out an impact assessment, offer remediation strategies, and compile a report summary.
Background	Cybercriminals around the world now have access to new AI tools as these become more commercially available. These tools significantly enhance their ability to conduct sophisticated cyber-attacks. The inherent limitations in OT/IoT environments, such as the inability to install agents and security tools, further increase cybersecurity risks. To adapt to these changing times and upgrade our capabilities, our organisation must also embrace AI to bolster our rapid response to cyber-attacks while meeting global regulatory reporting requirements. The solution we seek should not only reduce response times but also improve the accuracy of incident handling in OT/IoT environments. Our organisation requires a swift response to any cybersecurity incidents to enhance our capabilities in responding to cyber-attacks and to comply with reporting requirements from regulators worldwide, thereby protecting our Operational Technology (OT)/Internet of Things (IoT) environments globally.
Requirements	The solution should encompass, but not be limited to, the following features: 1. The ability to collect information on and conduct analysis of a cybersecurity incident. 2. The ability to conduct impact analysis of the cybersecurity incident. 3. Utilising AI to summarise the cybersecurity incident and generate user-friendly reports for management and local authorities. 4. Ensuring that incident summarisation is conducted swiftly, within the response times mandated by local authorities. 5. The ability to identify the point of entry and the path of the cybersecurity incident to pinpoint vulnerabilities within our organisation. 6. The ability to provide recommended remediation and guided responses.
Additional Information	The solution could be an end-to-end system or an integration with existing Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), or extended Detection and Response (xDR) platforms.

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. **2024NOV-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. **2024NOV-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. **2024NOV-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. **2024NOV-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. **2024NOV-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. **2024NOV-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.