

Cybersecurity Industry Call for Innovation 2025 Edition

By



*Uplifting the development of Singapore's
cybersecurity ecosystem*

Powered by



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

2025-CS01: AI-Powered Automated Analysis of Privileged Access Management Session Logs and Screen Recordings

| | |
|---------------------|--|
| Challenge | Develop a cost-effective, standalone AI component that seamlessly integrates with existing Privileged Access Management (PAM) 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. |
| Background | <p>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. The system records user sessions through logs and screen video captures.</p> <p>Whenever there is a requirement to perform changes to the system (such as patches or updates to certain component), the administrator or the vendor will do it through the organisation's PAM setup. The PAM solution will perform recording of the entire session from logon to the completion of the change. This is required as a regulation for CII (OT).</p> <p>Analysing these recordings is currently done manually, which is tedious and time-consuming. The commands are difficult to interpret because they are not written in natural language (system commands) and operators could open multiple command prompt in a single terminal. The video recordings are long and cumbersome to review, making it easy for important details to be overlooked. In addition, there are a lot of videos accumulated in the organisation over the past few years, manual review of these videos will take a long time. Therefore, there is a clear need for a cost-effective, private AI driven internal solution that can be easily integrated into the existing PAM framework to automate and improve the analysis process (extract, analyse, classify, and alert/report). The AI solution should operate across the four stages from the analysis process.</p> <p>For example, in an OT environment, when data diode bypass occurs, a vendor will RDP to the terminal server and access the target device for troubleshooting or maintenance. The AI should be able to review the vendor's actions via screen recordings after the session has ended and flag any suspicious activities during a post-event audit. This includes identifying malicious actions such as attempting to access devices other than the intended target, or deviations from standard plant activities like the creation of new accounts or changes to firewall rules.</p> <p>Another example is in an IT environment, where users typically access servers to perform upgrades or patching in accordance with release notes. The AI should be capable of reviewing the user's actions via session recordings after the event has concluded and flagging any deviations from the release notes or unexpected and suspicious activities during the post-event audit.</p> |
| Requirements | The solution should encompass, but not be limited to, the following features: |

1. Extract and process data from PAM solutions, handling both text-formatted logs and screen recording videos.
2. Conduct behavioural analysis after PAM sessions to ensure compliance with benchmarks.
3. Identify and flag anomalies from internal administrator and third-party support staff during post-session analyses.
4. Recognise acceptable behaviours that may deviate from benchmarks but are not considered security risks.
5. Allow for benchmark and configuration settings to be input in various formats, including change management request (could be in document or email format) release notes and natural language instructions.
6. Performance standards: Achieve minimum 80% accuracy with maximum 20% false positive rate for deployment; 95% accuracy with maximum 5% false positive rate for production usage.
7. Utilise User and Entity Behaviour Analytics (UEBA) training with 'golden images' and typical user behaviour patterns as references.
8. Operate efficiently without excessive bandwidth, time, or processing power consumption.
9. Classify the confidence level of detected anomalies into categories such as HIGH, MEDIUM, and LOW.
10. Provide post-session alerts for detected anomalies.
11. Enable querying of recording contents using natural language.
12. Generate analysis reports in a user-friendly format.
13. An advantageous feature would be the capability for the solution to automatically conduct real-time behavioural analysis, assess user actions against established benchmarks or blacklisted processes, and where necessary, proactively manage and restrict user access to specific assets.

Additional Information

1. Compatible with various PAM solutions on the market. Integrate smoothly with existing PAM systems without complex setup procedures or loss of existing PAM features.
2. Be compatible with both Information Technology (IT) and OT environments, accommodating one-way data transfer from OT to IT using Data Diodes.
3. Function in offline environments, particularly in Operational Technology (OT) settings.
4. The solution may be a non-video analytic tool, provided it meets the requirement.
5. Training of the AI model would be executed with sensitive data privacy and concerns.
6. Operate efficiently without excessive bandwidth, time, or processing power consumption.

2025-CS02: Artificial Intelligence (AI) assisted Automated Patch Management and Testing Across Diverse Information Technology Environments

| | |
|---------------------|---|
| Challenge | Develop an automate patch management, pre- and post-patch testing activities across both Windows and Linux systems, aiming to reduce manual effort and enhance operational efficiency. |
| Background | <p>Modern Information Technology (IT) environments consist of large and diverse technology stacks, supporting a wide array of systems and applications. The infrastructure team regularly receives numerous patch requests, impacting critical business services and security posture.</p> <p>Currently, patch management and testing are performed manually, involving extensive coordination, planning, and prioritisation among team members. Each day typically begins with manual task assignments, followed by patch application, system verification, and planned production rollouts. This process is time-consuming, resource-intensive, and subject to human error.</p> <p>Given the increasing volume and frequency of patches, there is a strong need for automation to streamline patch management, improve turnaround time, and reduce operational risks. Automating both the patch deployment and subsequent testing phases presents a significant opportunity for time savings and efficiency gains.</p> <p>Ideally, the operating system services and applications after patch applied should be fully functional, before application team does their regression testing. Any technical errors should be clearly reported for the product vendor to resolve.</p> |
| Requirements | <p>The solution should include, but not be limited to, the following:</p> <ol style="list-style-type: none"> 1. Automated patch management and AI assisted pre and post deployment testing capabilities that operate across both Windows and Linux environments, supporting a wide range of market-leading IT products and technologies. 2. Static analysis of patch file to provide insights prior actual testing in actual environment. 3. Generation of detailed testing reports pre and post deployment, specifically highlighting failed use cases and other actionable insights. 4. Monitoring dashboards that provide real-time visibility of patch status, enabling effective coordination and workflow management across teams. 5. Solutions that help reduce the time to patch as a quantifiable metric of improvement. 6. (Good to have) Additional patch verification controls, such as malware detection on patch files, to enhance security and trust in automated patching. 7. The solution must be adaptable and extensible to support integration with various IT products and technologies in the market. 8. Adhere to industry best practices and relevant regulations where applicable. |

2025-CS03: Inter-Agency Cryptocurrency Investigation Collaboration Platform

| | |
|---------------------|--|
| Challenge | 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. |
| Background | <p>Singapore and the surrounding region face increasing illicit activities including money laundering, fraud, ransomware attacks and cross-border crimes, which increasingly leverage digital assets/cryptocurrencies.</p> <p>Currently, authorities conduct cryptocurrency investigations independently, leading to duplication of efforts when multiple agencies unknowingly investigate the same wallet addresses or entities. This siloed approach creates inefficiencies that strain agencies' resources as cryptocurrency crime volume increases and investigations get more complex.</p> <p>Existing market solutions are primarily blockchain analysis tools for individual users rather than secure, multi-agency collaboration platforms that can support sensitive information sharing whilst maintaining strict access controls and operational security requirements.</p> |
| Requirements | <p>The solution should contain, but not limited to the following:</p> <ol style="list-style-type: none"> 1. Secure database with bulk upload functionality for cryptocurrency information such as wallet addresses with associated investigation metadata 2. Wallet address clustering and relationship mapping functionality 3. Quick wallet address lookup to verify existing agency interest 4. Real-time duplicate detection and alert notification when multiple agencies input identical wallet addresses or associations with known wallet address clusters 5. Automated OSINT enrichment for wallet addresses of interest 6. Real-time newsfeed on crypto security incidents, exploits and local crypto news 7. Configurable role-based access control by agencies, departments and user roles. 8. User authentication integration with official authentication system 9. Comprehensive analytics dashboard with metrics on wallets, duplicates detected, and platform usage statistics 10. Comprehensive audit trail for all logins and data access 11. Knowledge base repository for investigation 12. API integration with user-specified commercial blockchain intelligence databases for deeper insights on wallet addresses and wallet clustering relationships. 13. Darknet monitoring to identify compromised or exposed agency-controlled wallet addresses. 14. Secure wallet seed phrase management with encryption and multi-level access control |

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. 2025-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. 2025-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. 2025-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. 2025-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. 2025-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. 2025-CSOC6: 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.