# Cybersecurity Industry Call for Innovation (CyberCall) 2023

**Supported by**


***Uplifting the development of Singapore's cybersecurity ecosystem***

**Powered by**

## Introduction

This year's CyberCall is looking for solutions in the following (but not limited to) areas:

a. Cybersecurity for Artificial intelligence (AI)
   Safeguarding AI systems and the data they process from various cyber adversarial attacks in order to maintain the integrity, confidentiality, trustworthiness and reliability of AI applications in an increasingly connected and digital world.

b. 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.

c. Operational Technology (OT) / Internet of Things (IoT) security
   Safeguarding critical infrastructure, Industrial Control Systems (ICS) and internet-connected devices from cyber threats and vulnerabilities.

d. Cloud security
   Safeguarding data, applications, resources and infrastructure hosted in cloud environments, while maintaining the confidentiality, integrity and availability of resources in the cloud.

e. Privacy-Enhancing Technologies (PET)
   Safeguarding 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.

For a start, CSA has put together a list of end-users who are looking for solutions in some of the areas mentioned above.

## CSOC: Open Category

Innovative cybersecurity proposals that do not fulfil any of the Challenge Statements can be submitted under the "Open Category". The proposal should clearly explain the issue(s) that it aims to address, demonstrate innovation in solving the identified problem (e.g., no existing solution, improvement(s) on existing solutions), and have concrete go-to-market plans.

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 the new and emerging demands of cybersecurity users.

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

## CS01: Lightweight Security Gateway for IP-based camera and Network Video Recorders (NVR)

| | |
|---|---|
| **Challenge** | Lightweight defence to prevent exploitation of IP-based camera and NVR vulnerabilities. |
| **Background** | IP-based CCTV cameras and NVR typically use web servers for serving H.264/H.265 video encoders and web-based management interface, which in turn receives HTTP and RTSP requests. Zero-day and unpatched security vulnerabilities in web servers and web applications such as improper authorisation, buffer overflow, and arbitrary code execution, can therefore be exploited (e.g using maliciously crafted HTTP/RTSP requests). Cameras and NVRs are typically deployed at edge networks situated near the physical area under video surveillance, hence not protected by Web Application Firewalls (WAF) in data centres. |
| **Requirements** | The solution should contain, but not limited to the following:<br>1. Develop lightweight defences that can be deployed in edge networks to detect and prevent exploitation of IP-based camera and NVR vulnerabilities (E.g using malicious HTTP and RTSP requests). |
| **Limitations** | Expand the usage of Web Application Firewalls (WAF) to edge networks is currently not feasible due to costs and physical space constraints. In addition, WAF does not detect malicious injections like Real Time Streaming Protocol (RTSP) headers and payloads. |

## CS02: Automated Governance of Users' Permissions in Multi Cloud Environment

| | |
|---|---|
| **Challenge** | Develop a solution that can connect to multiple Cloud Service Providers (CSPs) to track and monitor Identity & Access Management (IAM) permissions automatically using User and Entity Behaviour Analytics (UEBA), allowing for easy governance and permission updates. |
| **Background** | As more applications are moving to the public cloud, the platform needs to be properly secured. IAM is relatively mature in the on-premises space but not in cloud environment. Also, management of IAM today is cloud vendor-centric, limiting its effectiveness across different CSPs.<br>As a result, it is difficult to define user permissions properly, whereby users could end up with excessive access to the environment. IAM permission changes are often requested by the application teams. As permissions are usually added and rarely removed, there is no way to keep track of the permissions to determine if they are too excessive.<br>There is currently a need for a 3rd party to ensure that privileges cannot be escalated, application teams do not have access to security logs, or ability to pivot to other accounts outside what they have.<br>Users could be a member of multiple roles. For example, the user could have both access to the code and ability to merge the code to production. This should not be allowed with proper separation of duties.<br>The AWS in-house system is not able to track overall permissions granted because the end-user is using multiple CSPs. |
| **Requirements** | The proposed solution should contain, but not limited to the following:<br><br>1. Provides a single pane of glass platform<br>2. Integrates with multiple Cloud Service Providers (starting with AWS and Azure) to track IAM permissions<br>3. Provides an intuitive UI to present IAM permissions in organisation hierarchical level<br>4. Detects automatically and alerts the security operations team upon detection of suspicious activities<br>5. Extracts IAM logs to provide usage activity<br>6. Utilises UEBA to advise permission rights based on user's profile and department usage history<br>7. Provides automatic detection of excessive permission or violation of access policy<br>8. Updated when the CSPs change their query mechanism<br>9. Connect to the on-premise Active Directory to get information from the organisation's users and groups<br>10. Flags out risky and unutilised IAM permissions<br>11. Ideally perform auto-remediation where possible |

## CS03: Bot Traffic Detection

| | |
|---|---|
| **Challenge** | To build a machine learning model that can accurately detect malicious online and offline bot traffic in event tracking data while adhering to privacy requirements for the e-commerce industry. |
| **Background** | Bot usage has given rise to and enabled a variety of automated threats that pose risks to businesses, for instance, payment fraud, voucher abuse, ads fraud, data scraping and credential stuffing attacks. Bot traffic can also lead to misleading event tracking data, as it is mixed with real human behaviour, resulting in poor-quality and inaccurate data that hinders decision-making by businesses.<br><br>There are three types of attack scenarios, 1) Credential Stuffing, 2) Mass Collection of Vouchers and 3) Web Scraping. In credential stuffing, the attacker will obtain the account name and password from the dark web and perform a mass login test. Once successful, they can request refund and transfer the money from the customer's e-wallet to other accounts. They can also utilise customer accounts that have credit card information to place orders and then re-sell the products on other e-commerce platforms. Next, in mass collection of vouchers attacks, attackers will use bots to create multiple new accounts to collect vouchers and make purchases at discounted prices. The attackers can resell the merchandise at a slightly lower price on another e-commerce site to gain financial benefits. In web scraping attacks, attackers will use bots to extract large amount of content and data from a website. Competitors can use this information to understand what the best-selling products are (e.g., from users' reviews or items sold), or what new products are coming. This will allow competitors to adapt their strategy or even identify the victim's suppliers, affecting sales.<br><br>While the industry currently deploys both real-time and offline measures to detect bot traffic and mitigate threats, there is no industry-wide, standardised solution to detect offline bot traffic in event tracking data. Privacy requirements that limit the available data points pose additional challenges for the development of solutions targeted at bot traffic detection. |
| **Requirements** | The solution should contain, but not be limited to the following:<br><br>1. Be able to leverage browse and click data to detect bot traffic in an offline environment, with real-time detection ability a bonus<br><br>2. Provide either a unified or different models applicable to PC, app, and PWA<br><br>3. The models should have a high accuracy and coverage rate, and they will be compared with the insights metrics of organizations with similar business strategies.<br><br>4. To be accurate, the machine model must be trained in the e-commerce environment utilizing different scenarios and models. |

| | |
|---|---|
| | 5. Various business matrices will be offered to solution providers to assess the accuracy of the detection. |
| **Limitations** | Total data volume is over 1 billion records per day, so efficiency in the model's ability to process high data volumes is critical.<br><br>For the start due to the sensitive of the data extracted from voucher attack. We will start with the data scrapping attack first. This kind of attack is normally conducted via highly skilled ecommerce competitors. |