# Cybersecurity Industry Call for Innovation 2026 November Edition

**By**

CSA SINGAPORE

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

**Powered by**

CyberSG TIG COLLABORATION CENTRE

[tig.cybersg.sg](tig.cybersg.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

### 2026NOV-CS01: Risk-Aware, Autonomous and Reversible Containment of Fast-Moving Intrusions

| | |
|---|---|
| **Challenge** | Develop an innovative cybersecurity solution capable of detecting and autonomously containing fast-moving cyber intrusions at machine speed, before an attacker can establish significant lateral movement or cause material operational impact.<br><br>The solution should dynamically determine the appropriate containment action based on the assessed cyber risk and potential blast radius, applying graduated and reversible controls rather than relying solely on the current industry's rule-based binary allow/block decisions. Actions should be automatically reversible where the assessed threat subsides or is subsequently determined to be benign, thereby reducing the operational impact of false positives.<br><br>The solution should be designed for deployment in high-availability aviation operational environments, where cybersecurity containment must balance the need for rapid response against the need to maintain continuity and safety of operational services. |
| **Background** | Cyber intrusions are occurring at increasing speed, significantly reducing the time available for human analysts to investigate and respond before lateral movement occurs. Attackers may also operate through legitimate accounts, applications and trusted channels, making malicious activity difficult to distinguish immediately from legitimate activity.<br><br>Existing security operations typically require alerts to be investigated and validated before containment actions can be taken. This creates a fundamental challenge: waiting for greater confidence reduces the risk of disrupting legitimate operations but gives attackers more time to move laterally, while acting too quickly may cause operational disruption.<br><br>A new decision and orchestration layer is therefore needed to take proportionate action as confidence in a cyber threat increase. The underlying concept proposes a continuously updated risk score that would trigger progressively stronger measures, such as additional authentication, restricting connectivity or access, and ultimately freezing credentials, with automatic reversal when the risk subsides.<br><br>For the aviation sector, this is particularly important because cyber containment must not create an operational disruption greater than the cyber incident it is intended to contain.<br><br>Two potential environments for developing and validating the proposed capability are **Aeronautical Information Management (AIM)** and **Air Traffic Flow Management (ATFM)**:<br><br>• **AIM** supports the management and dissemination of aeronautical information required for aviation operations, such as information concerning airspace, airports, routes and other operational data. It presents a useful development context because cyber controls must protect the integrity and availability of operational information while avoiding unnecessary disruption to legitimate information flows. |

| | |
|---|---|
| | • **ATFM** supports the management of air traffic demand and available airspace or airport capacity so that traffic flows can be planned and managed efficiently. It presents a useful development context for testing machine-speed containment because system and user interactions can be operationally important and time-sensitive, making conventional blanket isolation potentially undesirable.<br><br>Accordingly, AIM and ATFM provide potential aviation use cases for developing and validating risk-aware containment that can progressively restricts access or connectivity before resorting to full isolation. |
| **Requirements** | The solution should contain, but not limited to the following:<br><br>1. **Real-time risk and blast-radius assessment**: Continuously assess cyber risk associated with users, identities, endpoints, workloads, sessions and/or network connections using multiple security signals and estimate the potential impact or blast radius of suspected compromise.<br><br>2. **Machine-speed autonomous containment**: Automatically initiate containment without waiting for manual analyst intervention where predefined risk thresholds and conditions are met.<br><br>3. **Graduated containment actions**: Support multiple containment levels corresponding to different confidence and impact levels, instead of a single binary "isolate/not isolate" response. For example, lower-confidence events could result in enhanced monitoring or authentication, while higher-confidence events could result in progressively tighter access or network restrictions. This follows the confidence-to-action approach in the underlying problem statement.<br><br>4. **Automatic and safe reversibility Containment actions**: should be designed to be reversible. Where corroborating threat evidence does not emerge within an appropriate timeframe, or where authorised personnel determine that an event is benign, the solution should be capable of returning affected entities to their previous operational state in a controlled manner. Automatic reversal is a defining characteristic of the proposed concept.<br><br>5. **Operational-context awareness**: Allow containment policies to take into consideration the criticality of affected systems, identities and services, so that the response to a suspected intrusion is proportionate to both cyber risk and potential operational impact.<br><br>6. **Pre-authorised containment policies and guardrails**: Allow end users to define in advance which autonomous actions may be performed for particular systems, asset classes and risk levels, including actions that require human authorisation. The source concept specifically identifies pre-authorised response playbooks as a means of addressing the accountability barrier to automation.<br><br>7. **Integration with existing cybersecurity controls**: Integrate, where applicable, with existing security capabilities such as SIEM, EDR/XDR, IAM/PAM, network security and security orchestration platforms rather than requiring wholesale replacement of existing security infrastructure. The proposed flagship concept is explicitly positioned as a decision/orchestration layer over existing security tools. |

| | |
|---|---|
| | 8. **Transparent and explainable decision-making**: Record the security signals, risk assessment, policy and conditions that resulted in each autonomous action, together with the actions taken, their duration and any subsequent reversal or escalation. The source concept specifically requires autonomous actions to log the signals that triggered them.<br><br>9. **Human override and emergency restoration**: Permit authorised personnel to immediately stop, override or reverse automated containment actions where operational circumstances require intervention.<br><br>10. **Aviation operational environment applicability**: Demonstrate the solution in one or more aviation operational use cases, with AIM and/or ATFM proposed as candidate development and validation environments, subject to the availability of suitable test environments and end-user approval.<br><br>11. **False-positive resilience**: Demonstrate that erroneous or low-confidence detections do not unnecessarily result in prolonged denial of legitimate operational services. Particular emphasis should be placed on the ability to contain provisionally, reassess continuously and restore automatically.<br><br>12. **Measurable effectiveness**: Provide measurable indicators covering, at minimum:<br><br>a) time from detection/signal generation to containment;<br>b) time required to reverse containment;<br>c) false-positive containment rate;<br>d) percentage of containment actions successfully reversed to the previous known operational state; and<br>e) operational impact produced by containment actions. |
| **Limitations** | The solution should not autonomously perform containment actions that could directly compromise aviation safety or create an unacceptable operational impact.<br><br>Autonomous containment should operate only within predefined policies, asset scopes, authority levels and risk thresholds agreed with the end-user.<br><br>For highly critical operational functions, implementation may initially be limited to monitoring, recommendation, simulation or lower-impact containment actions until sufficient confidence has been demonstrated through testing.<br><br>The solution should not assume that every detected anomaly represents malicious activity. Legitimate operational activities, maintenance activities and exceptional operational circumstances may deviate from normal behavioural baselines.<br><br>Full autonomous isolation may not be appropriate for all AIM or ATFM components. The innovation should therefore focus particularly on progressive degradation of attacker capability, such as restriction of identity privileges, connectivity or reachable resources, rather than indiscriminate shutdown of an operational system.<br><br>Development and testing should use an appropriate non-production, simulated, test or otherwise approved environment where autonomous containment could affect operational availability. |

**2026NOV-CS02: Trustworthy ADS-B verification that safely coexists with operational surveillance**

| | |
|---|---|
| **Challenge** | Develop an innovative, operationally viable solution to verify Automatic Dependent Surveillance–Broadcast (ADS-B) messages and detect spoofed, forged or unauthorised transmissions within a timeframe suitable for the intended operational use, without adversely affecting aviation safety, surveillance performance or existing air-traffic operations. |
| **Background** | ADS-B is widely used for aviation surveillance, but its open broadcast design does not inherently authenticate the origin or integrity of transmitted messages. ADS-B signals can therefore be spoofed through the use of readily available hardware and software tools, potentially introducing false or manipulated aircraft information into surveillance systems. There is a need to preserve backward compatibility, minimise additional use of the 1090 MHz channel and support phased deployment across existing transmitters and receivers.<br>Existing aviation infrastructure includes a diverse installed base of airborne and ground equipment. A practical solution must therefore operate safely during a transition period in which authenticated and legacy ADS-B systems coexist. It should also account for the operational need for timely verification. |
| **Requirements** | The solution should contain, but not limited to the following:<br><br>1. Identify suspected spoofed, forged, replayed or altered transmissions.<br><br>2. Provide timely and actionable authentication status, confidence indicators and/or alerts, including, where appropriate, states such as authenticated, authentication-pending, unverifiable and suspected malicious, to authorised aviation users.<br><br>3. Preserve compatibility with existing ADS-B operations and support phased deployment alongside legacy transmitters and receivers.<br><br>4. Operate within the bandwidth, latency, availability and reliability constraints of aviation surveillance communications.<br><br>5. Remain resilient to message loss, duplication, delay and out-of-order delivery.<br><br>6. Provide secure and scalable management of cryptographic identities, credentials, keys and trust relationships.<br><br>7. Protect sensitive aircraft identity or movement information where operationally appropriate.<br><br>8. Support integration with relevant airborne, ground-based or surveillance-processing systems without compromising safety-critical functions.<br><br>9. Be demonstrated through measurable tests covering detection/authentication effectiveness, false-positive and false-negative performance, authentication latency, channel occupancy and impact, processing overhead, resilience to packet loss/duplication/out-of-order delivery, backward compatibility, and behaviour during authentication or credential failure. |

| | |
|---|---|
| **Limitations** | 1. **Safety and operational continuity**: The solution must not interfere with, degrade or create unsafe dependencies within existing ADS-B surveillance and air-traffic operations. Authentication failure, missing credentials, loss of connectivity or temporary inability to verify a message should not, by itself, cause the loss or suppression of surveillance information required for safe operations.<br><br>2. **Backward compatibility and mixed-mode operation**: The solution should support a transition environment in which authenticated and legacy ADS-B transmitters and receivers coexist. It should not assume fleet-wide or region-wide modification or replacement of existing airborne and ground equipment from the outset.<br><br>3. **1090 MHz spectrum constraints**: The solution should minimise additional transmissions and channel occupancy on 1090 MHz and demonstrate that authentication-related overhead does not materially degrade surveillance performance under representative traffic conditions.<br><br>4. **Timeliness of authentication**: Authentication mechanisms may introduce processing, cryptographic or verification latency. The solution should therefore distinguish between information that is authenticated, authentication-pending, unverifiable or suspected to be malicious, and provide these states to downstream users without compromising operational use of surveillance data.<br><br>5. **Imperfect communications**: ADS-B messages may be lost, duplicated, delayed or received out of order. The authentication approach must tolerate such conditions and should not assume reliable or ordered delivery.<br><br>6. **Installed-equipment constraints**: Some existing airborne or ground ADS-B equipment may not have sufficient processing capability, secure key storage, software/firmware upgradeability or support for new message/modulation mechanisms. Solutions requiring modifications to certified avionics should clearly identify such dependencies and provide a practicable migration path.<br><br>7. **Cryptographic trust infrastructure**: Approaches relying on digital credentials, certificates or cryptographic keys must address credential issuance, provisioning, renewal, revocation, compromise, interoperability, and operation across multiple aviation stakeholders and jurisdictions.<br><br>8. **Standards and certification dependency**: Any proposed modification to airborne ADS-B transmission, reception or safety-related surveillance processing may be subject to applicable aviation standards, technical validation, regulatory acceptance and certification before operational deployment. Demonstration under this project should therefore not be taken as approval for operational use.<br><br>9. **Cybersecurity detection is not separation assurance**: The solution should provide authentication, confidence indicators or alerts to support authorised aviation users. It should not assume that a cyber assessment alone can automatically reject, suppress or alter surveillance data used for safety-critical air-traffic functions without appropriate operational safeguards and validation. |

**2026NOV-CS03: Automated Cyber Readiness & Assurance System**

| | |
|---|---|
| **Challenge** | Develop an innovative, affordable and scalable solution that enables Small and Medium Enterprises (SMEs), including those with limited cybersecurity expertise and resources, to identify, prioritise, implement and independently verify cybersecurity improvements, without requiring extensive manual assessments or reliance on a single security vendor.<br><br>The solution should go beyond conventional vulnerability scanning, cybersecurity posture dashboards and compliance monitoring. It should translate identified cybersecurity weaknesses into practical, environment-specific remediation actions, guide SMEs through their implementation and verify whether the underlying risks have been adequately addressed.<br><br>A key objective is to enable SMEs to sustain and build upon their cybersecurity improvements over time, regardless of whether they remain connected to the platform, change IT service providers or discontinue a subscription. The solution should explore innovative approaches to maintaining portable, reusable and independently verifiable cybersecurity assessment and remediation records.<br><br>The solution should support continuous or periodic reassessment, detect cybersecurity regressions, and allow SMEs to resume their cybersecurity improvement journey without restarting previous assessments.<br><br>The intended outcome is a scalable solution that moves SMEs beyond understanding their cybersecurity risks towards demonstrably improving and sustaining their cyber resilience. |
| **Background** | As organisations increasingly adopt digital technologies, cloud services and AI, their digital attack surfaces expand, exposing them to threats such as phishing, ransomware, business email compromise and exploitation of vulnerable systems.<br><br>Many SMEs lack the cybersecurity expertise, manpower and resources to identify their most important vulnerabilities, determine appropriate remediation measures and implement them effectively.<br><br>Existing cybersecurity solutions increasingly offer automated scanning, continuous monitoring, compliance assessment, evidence collection and remediation tracking. However, some solutions may require technical expertise, extensive integrations or continued subscription access, while SMEs may still depend on external IT service providers to implement and verify recommended improvements.<br><br>For resource-constrained SMEs, identifying a cybersecurity gap does not necessarily translate into resolving it. Technical reports and recommendations may remain unactioned because SMEs lack the expertise, confidence or resources to implement the required changes.<br><br>Even when remediation is completed, SMEs may not have a reliable means of confirming its effectiveness or maintaining an accurate record of their improvements over time. |

| | |
|---|---|
| | There is therefore an opportunity to develop a solution that bridges the gap between cybersecurity assessment and verified implementation, while reducing technical complexity, recurring assessment effort and unnecessary vendor dependency. |
| **Requirements** | The solution should encompass, but need not be limited to, the following capabilities:<br><br>1. **Automated and Low-Friction Cybersecurity Assessment**: Identify relevant vulnerabilities, configuration weaknesses, exposure risks and cyber hygiene gaps using automated assessments, authorised integrations or existing digital evidence wherever feasible, minimising manual SME inputs.<br><br>2. **Context-Aware Cybersecurity Prioritisation**: Prioritise identified risks based on exploitability, exposure, business criticality, potential operational impact and remediation effort, providing SMEs with clear explanations of what should be addressed first and why.<br><br>3. **Actionable and Environment-Specific Remediation**: Translate cybersecurity findings into practical remediation actions tailored to the SME's technology environment, available resources and technical capabilities, rather than generic recommendations.<br><br>4. **Safe and Assisted Remediation**: Support guided remediation and, where feasible, authorised automated remediation, with appropriate validation, safeguards and rollback mechanisms to minimise unintended operational impact or data loss.<br><br>5. **Independent Remediation Verification**: Reassess identified weaknesses using fresh technical evidence, where feasible, to confirm whether remediation has successfully addressed the underlying risk, distinguishing verified improvements from self-declared or unverified actions.<br><br>6. **Continuous Reassessment and Regression Detection**: Support periodic or event-driven reassessment to identify newly introduced vulnerabilities, configuration changes or regression in previously implemented cybersecurity measures, and provide appropriate alerts and corrective recommendations.<br><br>7. **Portable and Reusable Cybersecurity Records**: Enable SMEs to securely export, retain, update and re-import assessment records, remediation history and supporting evidence, allowing them to resume their cybersecurity improvement journey without restarting previous assessments.<br><br>8. **Platform-Independent Cybersecurity Continuity**: Enable SMEs to maintain access to their cybersecurity improvement records and conduct subsequent reassessments without mandatory reliance on a single vendor, proprietary security product or uninterrupted subscription. Innovative approaches to offline updates, reusable evidence and lightweight reassessment are encouraged.<br><br>9. **Integration with Existing SME Environments**: Support commonly used technology environments, such as Microsoft 365, Google Workspace, endpoints, cloud services and internet-facing systems, leveraging existing security capabilities without unnecessarily duplicating or replacing them. |

| | |
|---|---|
| | 10. **Measurable Cybersecurity Improvement**: Provide SMEs with visibility of current and historical cybersecurity posture, identified and resolved gaps, verified remediation, newly introduced risks and regressions, with capabilities to generate and export periodic progress reports.<br><br>11. **SME-Friendly Experience and Collaboration**: Present findings and remediation actions in plain language suitable for non-technical business owners, while allowing authorised IT service providers to access relevant technical guidance and support remediation activities.<br><br>12. **Scalable and Extensible Architecture**: Support large-scale adoption across SMEs with minimal manual intervention, secure organisational authentication where required, and the flexibility to incorporate additional security tools, assessment methods and technology environments. |
| **Limitations** | The solution should minimise disruption to SMEs' existing systems and business operations, avoid destructive testing and not introduce material cybersecurity, privacy or data-loss risks.<br><br>Automated remediation should require appropriate user authorisation and safeguards. Assessment and remediation records should be protected against unauthorised access, modification and disclosure.<br><br>The solution should clearly distinguish between current, technically verified findings and historical or SME-declared information. Where continuous monitoring is not active, the solution should indicate when a finding was last verified rather than imply that the organisation's present cybersecurity posture remains unchanged. |

## 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. **2026NOV-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. **2026NOV-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. **2026NOV-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. **2026NOV-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. **2026NOV-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. **2026NOV-CSOC6: Privacy-Enhancing Technologies (PET)**
   Safeguarding the privacy of individuals and confidentiality of their data while using systems and digital services, to empower 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.