Cybersecurity Industry Call for Innovation (CyberCall) 2022

Supported by

Uplifting the development of Singapore's cybersecurity ecosystem

Powered by

CONTENTS

Introduction

This year's CyberCall is looking for solutions in the following areas:

- Artificial Intelligence (AI) for cybersecurity
- Cloud security
- Internet of Things (IoT) security
- Operational Technology (OT) security
- Privacy-enhancing technologies

For a start, CSA has put together a list of end-users who are looking for solutions in some of the areas mentioned above. We welcome more ideas and submissions from industry partners who have innovative ideas that address cybersecurity concerns in sectors like manufacturing, maritime, healthcare etc.

A. Artificial Intelligence for Cybersecurity

CS01: End-to-End Normalised Threat-based Cybersecurity Risk Management System

Challenge	Develop a platform or tool to support end-to-end, threat-based cybersecurity risk management that assist in threat modelling and uses data from existing IT and security tools.
Background	Cybersecurity risk management is often disjointed. It needs to be integrated to the enterprise risk management and to conduct assessment at each business unit (BU) to ensure sufficient granularity. The importance of dimensions of risks other than vulnerabilities, like the cyber supply chain have emerged and must be addressed as well. In addition, new regulations (e.g., CCOP 2.0) have been published by the regulatory authority. Companies understand that cyber is an existential risk and the need shift from the compliance-based approach to a threat-based approach in cybersecurity risk assessments (RA). Commercial off-the-shelf solutions typically focus on a specific dimension of risk like vulnerabilities integrated with proprietary threat intelligence, asset criticality or value. This is no longer sufficient. The current practice uses advisory services and RA remain highly manual. Some platforms do support the process, track compliance, and follow up remediation. However, this is not end-to-end, and compliance to CCOP 2.0 which is a Singapore regulation for Critical Information Infrastructure (CII) is not included. The use of advisory services is also not scalable especially for companies with multiple BUs. A platform or tool that can enable self-service cybersecurity RA by BUs, assisted by the cybersecurity team, could be required. The platform or tool should also have intelligence to suggest risk reduction by re-engineering business process or by adjusting controls (not really implementing new controls) and be able to contextualise risk based on the latest industry-specific and geo-political threats.

Requirements	The proposed solution should contain, but not limited to the following: 1. Consolidated view across BUs 2. CCOP 2.0 compliance benchmarking or scoring 3. Supply chain risk view 4. Intelligent suggestions to reduce risk by re-engineering a business process or by adjusting controls (not really implementing new controls) 5. Contextualization of threat intelligence vertical or industry wise and geo-political wise 6. Ability to ingest data from other tools such as asset management or Configuration Management Database (CMDB) and/or scan the network to derive a cyber digital twin to enable threat modelling for risk-assessment 7. Ability to render the network based on collected data to aid planning 8. Allow for inputs on Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for cyber resilience planning 9. Ability to take in threat intelligence data and suggest the resultant impact on risk 10. Allow asset owners to raise risk deviation or acceptance directly in the dashboard

B. Cloud Security

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. 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. There is currently a need for a 3rd party to ensure that the permissions are not too excessive, e.g. privileges cannot be escalated, application teams do not have access to security logs, or ability to pivot to other accounts outside what they have. 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 properly assigned separation of duties. The in-house system (e.g., AWS) is not able to track overall permissions granted because GIC is using multiple CSPs.
Requirements	The proposed solution should contain, but not limited to the following: 1. Provides a single pane of glass platform 2. Integrates with multiple Cloud Service Providers (starting with AWS and Azure) to track IAM permissions 3. Provides an intuitive User Interface (UI) to present IAM permissions in organisation hierarchical level 4. Issues multi-cloud permanent and temporary rights to the user through the platform 5. Detects automatically and alerts central controller upon detection of suspicious activities 6. Extracts IAM logs to provide usage activity 7. Utilises UEBA to advise permission rights based on user's profile and department usage history 8. Provides automatic detection of excessive permission or violation of access policy 9. Updated when the CSPs change their query mechanism

CS03: Automated Prioritization of Cloud Drift Remediation in Multi Cloud Environment

Challenge	Develop a solution to detect, evaluate, prioritize, and remediate configuration drifts (CDs) in the multi-cloud environment.
Background	With mainstream Cloud Service Providers (CSPs) such as AWS, Azure and GCP, it is possible to generate reports of CDs detected in the various services utilised by organisations. These reports categorise CDs based on severity levels High/Medium/Low (or equivalent, depending on each provider's terminology). This categorization is based on the CSP's standard assessment and inevitably overlooks several important parameters. For example, a CD may be categorised as High severity, but may be occurring within a completely sandboxed service thus have a lower remediation priority. Vice-versa, a CD with Medium or Low severity may have a higher remediation priority if the service is exposed to the Internet or is critical to the business. On top of this, the assessment criteria for CD varies between CSPs, further increases the difficulty of CD categorisation. Because of these difficulties, manpower is required for manual analysis of each CD. This process is time-consuming, prone to human error, and may not be sufficiently comprehensive. As a result, critical CDs may not be properly prioritised, if left exposed and it could potentially lead to security breaches.
Requirements	The proposed solution should contain, but not limited to the following: 1. A single intuitive dashboard to view all the CDs from different CSPs 2. Normalised CD reports from multiple CSPs to get a common assessment across the CSPs 3. Automated analysis on the CD severity level provided by multiple CSPs (starting with AWS and Azure) 4. CD prioritization based on CSPs' reports and user's parameter such as potential exploitability of the drifts that could compromise the security of the environment, as well as business criticality of the services impacted, and any compensating controls in place 5. Embedded CII CCoP requirements from out-of-the-box 6. Prioritized remediation and automated remediation process upon approval a. Address misconfigured cloud resources by reverting them to their last known correct configuration b. Prompt detection to the relevant individual or team 7. "Change history" record to capture when, who, what configuration have been changed, including the remediation information
Limitations	Automatic remediation might not be possible as the organisation would have to provide the proposed solution with write permissions. Thus the solution should offer both options: 1. Manual remediation with detailed remediation steps listed 2. Automatic remediation

C. Operational Technology (OT) Security

CS04: Non-Intrusive Data Collection from Isolated OT System

Challenge	Develop a data enrichment layer for critical systems that allow remote response teams, with no physical connection to the network nor physical visibility, to better support organizations during the incident response process.
Background	Data is today at the core of a unified IT/OT Security Operation Centre. Increasing the diversity of data flow through the network due to the digitalization of industrial systems (IoT, OT, IT and on-cloud systems) and the spread of attacks via legitimate vectors [1], have made it clear that today's SOCs can't only rely on thresholds and indicator of compromise, but also have to understand, analyse and correlate the whole data which is shared across an operating network. Besides, OT systems can be safety critical and therefore the incident response cannot be automated. Therefore, contextualization of data is necessary to enrich the security events (e.g., evaluate the criticality of the incident) and make them understandable by an operational. Finally, sharing information across an organization (SOC, ICT team, Operational team) within a unique referential (like Digital Twin) is key for the timely incident response as SOC and Operation team must work closely. For instance, since they are most knowledgeable on the systems, operational team are much able to detect any anomaly. Their sharing of relevant information to the SOC is therefore critical. Example of this background is rail transport rolling stock OT networks with Grade of Automation (GOA) Level 4 technology or any autonomous buses/vehicles that are composed of assets that communicate with proprietary protocols but also of standard OT assets, network equipment or IoT components on the shelf. Getting clear visibility on data flow within this critical system is a priority for an operator who fears malicious command injection or loss of availability: any detected event requires contextualization and data enrichment so that the head of operations can take the right decision, in collaboration with the SOC team. [1] https://securityintelligence.com/news/cybersecurity-attacks-legitimate-services/
Requirements	The solution should contain, but not limited to the following: 1. Collect data and security information across various critical SMRT components (starting with the train network, such as platform screen door and rolling stock) from air-gapped system side channels 2. The solution should consider the extraction of data in a cluttered and noisy environment 3. Provide an aggregated view of data collected from the components
Limitations	Proposed implementation should not impact the OT system. Solution provider may not have access to certain OEM hardware and software built.

CS05: OT Kernel Prevention of Cyber Attacks

Challenge	Construct a system within Operational Technology (OT) environment that stops cyber-attacks at the kernel level. Using data provenance and machine learning, the system should reliably identify and shut out cyber intrusions based on the behaviour and signatures of related events they, in near real-time.
Background	OT networks are highly vulnerable to cyber-attacks. Most attacks pivot into the OT environment through the IT systems connected to them. Because all existing tools only monitor IT systems, visibility or situation awareness of the OT threat vectors is lost or at most, a best-effort collection of provenances. Currently, the so-called OT cyber security tools focus on network data packet inspection for anomalous packets. These tools use deep packet inspection to find signatures of anomalous behaviour. Most intrusions go undetected as cyber intruders mimic regular network behaviour and packets. For example, false data injections cannot be detected by such techniques. A further complication will be the introduction of encrypted protocols to OT networks by the major equipment vendors. All the current tools only inspect datasets after the attack event(s). This post-mortem analysis is not good enough for critical infrastructure and should be complemented by near-real-time, time-series machine learning capabilities to provide early warning detection – much like a weather forecast.
Requirements	The proposed solution should contain, but not limited to the following: 1. An OT kernel solution that is using machine learning and global intelligence feeds, the system should be able to identify new tactics techniques and procedures (TTPs) to maintain the operational effectiveness of the system 2. The system should be able to use AI/ML and data provenance to discover, close and stop cyber intrusion based on behaviour patterns and signatures of related events 3. The system should be able to alert operators through various communication channels in the event of suspected malicious activity 4. The system should be able to perform on-demand threat-hunting of malicious codes and content residing in the PLC and generate score analytics that provide insights into the composition of the cybersecurity score 5. Sanity checks on the new PLC code (text or byte) 6. The OT kernel management application shall complement existing controls and not directly connected to OT in production. It shall draw no bandwidth from operating OT networks
Limitations	The solution should not take up bandwidth within the network/environment.

CS06: OT Threat Vector Path Discovery on Digital Asset Map

Challenge	Develop an automated solution that extracts the current network asset map and vulnerabilities, conduct penetration test (PT) on the digital asset, discover path of intrusion of the asset without operating on the actual OT system based on MITRE attack framework and suggest remediation.
Background	Under the new CSA CCoP released in July 2022, CII owners are required to conduct periodic PT on OT CII environment at least once every 24 months. Such PT would typically be sending commands to the field controllers which are monitoring and/or controlling the physical processes to exploit vulnerabilities that can potentially cause disruption. While conducting an offline Vulnerability Assessment (VA) prior to a PT helps to discover known vulnerabilities on field controllers, there are certain limitations to this approach e.g., VA does not state if there is a potential path of intrusion from the engineering workstation to the field controllers for pen-testers to exploit. PT could be conducted on a digital twin to overcome such limitation, but a digital twin is expensive to build and maintain. Therefore, an automated PT solution that can be conducted on the digital asset map and can achieve similar outcome as PT on the production system is needed. It would be beneficial to have a tool to discover the potential path of intrusion before the conduct of a PT on the production system.
Requirements	The solution should contain, but not limited to the following: 1. A non-intrusive solution which can extract the current network asset map and vulnerabilities to discover if there is a potential path of intrusion to the field controllers based on MITRE attack framework and suggest remediation which would help to identity and reduce the surface area of attack on these assets during the actual pen-testing 2. Capture information from third party tools such as OT NADS, firewalls, and network routers/switches to create a comprehensive map of assets and interconnections on-site in an organisation 3. Offer a smart system to categorise and analyse the digital asset maps and discover new vulnerabilities and attack paths to create a threat model 4. Deploy the MITRE attack framework to present the identified vulnerabilities in a structured actionable report, linking to available dataset bases of remediation actions, such as overdue firmware upgrades etc 5. The findings from this PT on the digital asset maps should be similar to the findings from a PT on the production environment
Limitations	Proposed solutions should not consume significant production network bandwidth and should not impact OT system operation.

D. Privacy-enhancing Technologies

CS07: Privacy Preserving Digital Forensics

Challenge	Preserving privacy of victim while allowing digital forensic searches and analytics to be performed on Personally Identifiable Information (PII) data and sensitive images or videos
Background	Digital Forensics is a rapidly growing capability for examining the contents of computers and other digital devices. It raises many challenges to the conventional notions of privacy because it involves a more considerably detailed search of digital data than is possible with other manual techniques. Digital Forensics, especially on cybercrime, for law enforcement agencies is experiencing an exponential increase in the amount of digital data to be processed, analysed, and stored for evidential purpose. Moving to the cloud is one of the key solutions but there is much concern on the storage of sensitive data on cloud, especially PII and sensitive images or videos such as sexual content.
Requirements	The proposed solution should contain, but not limited to the following: 1. Keep sensitive data and PII private but allowing for keyword search and entity matching 2. Allow image or video analytics such as AI/ML categorization to execute properly on the privacy-preserved data 3. Allow investigators to locate critical evidence from the privacy-preserved data 4. Provide an access control mechanism which allows only authorized investigators to access and view private data and identified digital evidence 5. Preserve the chain-of-custody of digital evidence 6. Ensure the authenticity, confidentiality, and reliability of the evidence 7. Propose a Privacy Preserving Digital Forensics (P2DF) framework that is suitable for the end-user use case 8. Support major Cloud Service Providers (CSPs) in the market for deployment
Limitations	Real or actual data is not provided for development but can be leveraged upon for testing at user's premise.

Open Category

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.

Examples of areas for cybersecurity innovation include but are not limited to:

- Artificial Intelligence (AI) for cybersecurity
- Cloud security
- Internet of Things (IoT) security
- Operational Technology (OT) security
- Privacy-enhancing technologies

For proposals submitted under the Open Category, the applicant company must secure at least one committed cybersecurity end-user by the third milestone. 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.