# Cybersecurity Industry Call for Innovation 2021

**Supported by**

CSA SINGAPORE

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

**Powered by**

NUS National University of Singapore | Enterprise

TNB VENTURES

# CONTENTS

## A. Artificial Intelligence for Cybersecurity

## B. Cloud Security

## C. Internet of Things (IoT) Security

## D. Operational Technology (OT) Security

## D. Privacy-enhancing Technologies

## Open Category

# A. Artificial Intelligence for Cybersecurity

## CS01: Cybersecurity Risk Assessment and Audit Data Analytics

| | |
|---|---|
| **Challenge** | Build an application to be able to take in data files, perform query, data extraction, analytics, dashboarding and reporting capabilities. |
| **Background** | Our organisation receives approximately 70 cybersecurity risk assessment reports annually and at least 80 audit reports every two years. Over time, the amount of reports builds up and would be a useful repository to reference for insights. The submitted reports can be in form of MS Word, Excel, PDF and hardcopy.<br>It is a time consuming and resource-intensive extensive to manually review and validate that the submitted reports meet the submission criteria before the reports are reviewed, corelated identified and insights pulled together for reporting purposes. |
| **Requirements** | We are seeking a data analytics solution that, minimally, is able to query and analyse the data sources and pull together the information to address specific questions that we have from a data source completeness-standpoint and separately from an data insight-standpoint. The use of Artificial Intelligence and Natural Language Processing in the solution will be an added advantage.<br>Some of the questions on data completeness and insights that the data analytics application would need to address include the following:<br>1. Completeness and comprehensiveness of data sources whether they include the relevant sections/information, risk assessment methodology used, definition of risk, risk treatment options put in place, outliers, etc.<br>2. Existing/trending cybersecurity risk profile of each cluster, sectors and system in considerations of the risk scenarios, risk category, appropriateness of risk treatment/control measures, risk treatment status/timeliness, etc.<br>3. Risk and controls universe for each sectors and cluster including the mapping of risk scenarios to risk category and risk treatment/control measures<br>Note that a fuller list of questions can be separately shared during the in-depth discussion on the detailed requirements. |
| **Limitations** | 1. The solution provider is free to propose additional insights on risk assessment, audit report and format for dashboard and reports.<br>2. Proposals with solution development being completed in 12 months will have an added advantage. |

## CS02: 360 Cyber Fusion Analytics for IT/OT/IoT Convergence

| **Challenge** | Develop a cyber fusion analytics engine that correlates, converges and contextualise information, reports and threats from IT, OT and IoT devices and sectors to allow for automated response and operations. |
|---|---|
| **Background** | Traditional approaches to cybersecurity fall short in keeping up with today's rapidly evolving threat landscape. In the haste to get products out the door, there has been little consideration placed in developing security capabilities capable of working holistically with one another. This resulted in security silos that prevent an understanding of the full landscape that prevents effective protection against today's advanced and sophisticated threat actors.<br>A decentralised approach to cybersecurity results in organisational silos and overly complex products and solutions just to integrate and sense make data collected. Analysts are often swamped by an overwhelming amount of data that does not provide a clear insight nor an action plan, and there could be duplicated efforts wasted when a threat hit multiple systems, causing everyone to conduct a similar investigative process, wasting valuable time that could have been used to more actively respond to the threat.<br>A collaborative and combined effort like a cyber fusion centre would allow both SOC and Ops to share intelligence and data in order to facilitate the effective response to threats. Bringing together staff from various departments working and collaborating under one roof would drive an integrated response to threats and crisis, resulting in faster response time, reduce cost, and increased productivity and better intelligence. |
| **Requirements** | The proposed Cyber Fusion Analytics engine should:<br>1. Power a single dashboard for all assets, vulnerabilities, intelligence, intrusions, security events and incidents for a tiered SOC investigation, compliance monitoring and reporting.<br>2. Ingest and process information from threat intelligence sources (e.g. OSINT, insider threat, fraud, brand reputation, physical, geopolitical, supply chain) to better detect known or unknown cyber threats at early stage to drive incident prioritisation or remediation. Intelligence feeds must adhere to STIXX/TAXI structures, in the scenario that unstructured data is required, it will be discussed separately during the clarification session.<br>3. Collect security telemetry or intel at various sources via API interfaces including but not limited to Asset Management, Vulnerability Assessment and Penetration Testing, Endpoint Protection, Identity-Email-Collaboration, Network Security, Application Security, Data Security, Cloud Security, IoT/OT Security, Threat Hunting, Threat Intelligence, Attack Surface Monitoring, Managed Detection & Response, SIEM/SOAR and SOC services.<br>4. Cloud-first deployment, natively support cloud orchestration to provide automated build enhancements and configuration updates in real time.<br>5. Create a new cost-effective data lake or the relevant data model (for existing data lake) for data ingression, security analytics and retention. |

| | |
|---|---|
| | 6. Be able to integrate with (or replace) exiting SIEM/SOAR and/or MDR/NDR platform to improve automation and cost-effective security operations. Telemetry, events and intelligence feeds must be vendor agnostic and the reuse of existing security solutions is preferred.<br>7. Detect security incidents via known security patterns or anomalies via behavioural analysis, and confirm the validity of detected events with ML/AI data analytic capabilities to support incident response efforts.<br>8. Have security playbooks for various business domains - Digital Workplace, Digital Cloud Application (e.g. eCommerce, CRM) Manufacturing & Supply Chain, Connected IoT Platform, Data Analytics Platform to define end to end security monitoring, incident response and crisis management capabilities.<br>9. Complement existing Security Operation Centre (as a managed service) to drive cost efficiency via the new innovative technology and automated processes.<br>10. The cyber security operations must adhere to NIST Cybersecurity and MITRE ATT&CK framework.<br>11. Proposed solutions should consume minimum production network bandwidth and should not impact existing IT/OT/IoT system and network performance and operations. |
| **Limitations** | 1. If it is not possible to deliver above requirements by single vendor, a partnership with an XDR provider can be considered to deliver integrated and cost-effective operations.<br>2. At minimum the 50% of requirements must be delivered within 6 to 12 months, where the remaining 50% to be completed within 24 months. |

## CS03: Integrated Cybersecurity Risk Assessment and Remediation Management System

| | |
|---|---|
| **Challenge** | Develop a solution to conduct cybersecurity risk and compliance assessments – tracking from identification to remediation, and leverage on the same data set to calculate the return of security investment. |
| **Background** | With the adoption of digital technology, cyber risk is one of the most important consideration for many companies as they went through the digital transformation. We are building up a more risk-aware culture which can be adopted in the cyber space when dealing with cyber security risk.<br>In a data driven world, we need to leverage on huge amount of data to make informed decision. This could apply to cyber security risk by collecting relevant data sets, correlating their asset criticality/value, and analysing them with threat, and vulnerabilities data sets to prioritize security investment.<br>While current commercial-off-the-shelf (COTS) solutions provide severity rating for the vulnerabilities based on CVSS and proprietary threat intelligence, asset criticality/value is not considered. In addition, the potential impact for breaching compliance standards is not considered.<br>The current process of providing advisory services and risk assessments remain highly manual. Hence, a scalable and self-service cybersecurity risk assessment and remediation management system could address this need. Having the feature to track return of security investment would also help in reporting to the management. |
| **Requirements** | The ideal vulnerability management solution should contain, but are not limited to the following:<br>1. Track return of security investment.<br>2. Conduct comprehensive risk assessment through:<br>a. Vulnerability scanning of assets as they are added or changed<br>b. Use of Artificial Intelligence / Machine Learning to detect zero-day vulnerabilities<br>c. Use of threat intelligence and verify the vulnerability in real-time<br>d. Identifying gaps between current controls and standards / best practice<br>e. Calculating severity with consideration of user-specified criticality levels of assets and agreed risk appetite<br>f. Recommending security controls based on industry best practices.<br>g. Providing the option to implement the remediation automatically.<br>3. Adopt AI / ML to improve risk assessment (e.g. Classification, feature selection of various attributes) to allow real time alerting and pro-active intervention.<br>4. Conduct compliance assessment in addition to risk assessment. |

| | |
|---|---|
| | 5. Integrate with asset management / CMDB system to retrieve and incorporate asset value and asset ownership information into the report.<br>6. Distribute the report automatically to the respective asset owners and allow asset owners and security managers to include action plans/target timelines in the vulnerability instance.<br>7. Allow customisation of the required remediation timeline based on severity and include the remediation timeline in the report for each vulnerability.<br>8. Monitor the remediation timelines, and highlight deviations in the management dashboard. Notify the asset owners if necessary.<br>9. Allow asset owners to raise risk deviation / acceptance directly in the dashboard.<br>10. Develop an opt-in feature for organisations to leverage on collective knowledge collected via this solution, to provide a semi-automated method of risk advisory. |

## CS04: Purple Team Email Filter and Phishing Platform

| | |
|---|---|
| **Challenge** | Develop a comprehensive anti-phishing solution to identify and filter phishing emails with a high degree of accuracy based on machine learning, and leverage on the same data set to implement an intelligent phishing simulation platform capable of generating realistic phishing drills that adapt to the phishing attacks targeting the organization. |
| **Background** | Phishing continues to be one of the most common causes of cybersecurity breaches today, and the attacks are on an escalating trend year on year. While user education and awareness are important in mitigating this threat, technology can also play a part to assist in the identification of phishing threats, especially when attackers are getting more sophisticated.<br>Today, most email security solutions are able to filter out basic phishing emails, but it is not difficult for attackers to craft the content in a way to evade detection. One reason for this is the lack of advanced filtering algorithms such as one that uses machine learning to identify phishing emails specific to an organisation by getting their users to help in the collection and classification of phishing emails in an automated way.<br>With the real phishing emails collected and classified, they can also be used as inputs to generate phishing drill content using adaptive machine-learning techniques. Currently, most phishing simulation platforms utilize a standard library of phishing drill content which are too generic in nature, and the effectiveness diminishes over time. With this new method, phishing drills can evolve automatically and reflect on the real phishing threats faced.<br>Also, current phishing drill platforms only track if users have clicked on a link, and use that to determine the fall-prey rate. Though this is a good measure, it could be further enhanced if users were brought to a functional but fake login page where their actual credentials could be captured and verified. This would provide another dimension of analysis and reporting to allow the prescription of appropriate follow-up actions for those who fall prey. |
| **Requirements** | The proposed solution should have the following capabilities and features:<br>1. Allows users to submit phishing emails with the primary objective of using the data to train the machine learning model. The plugin should be integrated with popular email clients (e.g. Microsoft Outlook).<br>2. Leverage advanced machine learning, sophisticated feature engineering, threat intelligence, and potentially other new web security techniques, to achieve high identification accuracy of phishing emails in the potential presence of wrongly submitted samples in training data. Essentially, the algorithm should cater for wrongly submitted samples as much as possible.<br>3. identify phishing emails, and integrate with common email providers (e.g. Office 365). Assign visual tags to emails based on confidence level, instead of blocking emails suspected to be phishing emails.<br>4. Develop a phishing drill emails content generator which leverages machine learning, threat intelligence and other similar inputs as with (2) using the submitted samples as training data. Generated emails should replicate the style |

| | |
|---|---|
| | and content of training data, but should not be restricted to only the reported threats.<br>5. Create campaigns to send out phishing drill email to users.<br>a. Customise campaigns for different groups of users, with varying parameters (i.e. Frequency of sending, different email content). This includes designing of spear-phishing campaigns, tailored to the most vulnerable roles and departments.<br>b. Utilise results of phishing campaigns to tailor future campaigns (i.e. Users who have fallen prey will get more phishing campaigns).<br>c. Generate comprehensive reports that uniquely identifies users who fell prey to phishing emails.<br>6. Integrate with enterprise logins (i.e. Microsoft ADFS) to create fake but functional login pages to capture (but not collect) credentials of users who have fallen prey. |
| **Limitations** | The solution must run on-premise in the end-user's environment as it involves the potential capture of the users' credentials. |

# B. Cloud Security

## CS05: Integrated Solution using Automation, Analytics and AI in Defence Model for Cloud

| | |
|---|---|
| **Challenge** | Design and build an integrated solution using automation, analytics and AI to enhance threat detection capability, improve asset protection using automated response and increase visibility of cloud environment for a holistic defence of the Cloud. |
| **Background** | There is a growing trend towards utilising the Cloud platform for a whole host of services including the common infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS), to the more niched security-as-a-service (SecaaS). Even malicious entities are using these established avenues to run their nefarious ransomware-as-a-service to enable ransomware attacks based on a subscription model.<br>Commercial off-the-shelf solutions (COTS) offering detection and protection capabilities are often tailored to commercial entities with deep financial resources or cater only to specific IaaS/PaaS setups. Most of these solutions offer restricted dashboard views and limited analytical functionality (i.e. rule-based) to cover security gaps, often with intricate knowledge in architecting different COTS and expected pre-requisite. Thus, this breaks down the holistic defence model into disparate parts covered by different solutions, resulting in misconfigurations, potential software conflicts and inconsistent/duplicative protection coverage.<br>To further compound these issues, many of the solutions also require manual/human intervention to check and validate high volume of alerts, slowing down incident response times and allowing the perpetrator to exfiltrate data or spread malware through to other connected workloads, databases and domains across the organisation. |
| **Requirements** | We are seeking to work with the industry to design and build an innovative solution that is both cost-effective and comprehensive to address the challenges when utilising Cloud services. This new solution should be Cloud Service Provider (CSP) agnostic and can offer detection and response capability for all cloud models (E.g. IaaS, PaaS and SaaS), through the following features with the use of Artificial Intelligence:<br>1. Perform User Entity Behaviour Analytics on asset information to determine baseline and detect anomalies (E.g.: activities that deviate from the baseline).<br>2. Constantly self-adjust/balance, to reduce false positive and generate alerts with high fidelity.<br>3. Propose response/actions to suspected incidents. Consider allowing an option to enable automated responses, to reduce manual validation times and protect against breaches. Interoperability with other existing security solutions in the environment for automated incident response is required to enable ease of configuration for such automated responses.<br>4. Use machine learning to analyse responses to threats/intrusions and provide feedback to improve defence model. (This is suitable for national implementation where the analytical sample size is large)<br>The listed features above should be done both within a single CSP, as well as across various CSPs. |

## CS06: Forensic Acquisition in the Cloud

| | |
|---|---|
| **Challenge** | Design and develop a web-based platform that conducts triage to search, preserve and analyse forensic artifacts from various cloud service providers (CSP). |
| **Background** | Criminals are increasingly leveraging on web technology to advance and expand their vice operation, facilitate communications, and to conduct digital transactions. Oftentimes, their modus operandi relies on any one of the major CSPs – Amazon Web Service (AWS), Microsoft Azure or Google Cloud. These companies account for more than half of the worldwide market share of cloud infrastructure service providers.<br>A key concern for digital forensic examiners is the ability to ensure that any digital evidence triaged from the cloud can be proven to be tamper-proof, so that they are admissible in a court of law. A proper chain-of-custody should also be maintainable as proof of accountability when the proceedings necessitate the transfer of ownership of said evidence.<br>While CSPs may offer native logging and monitoring services (e.g. AWS CloudTrail, Azure Log Analytics, GCP Audit Logs), these services target user actions and server logs primarily while leaving the hosted content (e.g. VM instances, storage, database) untouched. |
| **Requirements** | The proposed solution should offer the following capabilities or characteristics, with the use of Artificial Intelligence and Machine Learning:<br>1. Acquire the front-end of a website including but not limited to:<br>a. Screen capture of the web façade<br>b. Scraping of hosted content<br>c. Parsing of text and metadata<br>2. Access the back-end of a website and traverse through all accessible endpoints or running services on a CSP to search for potential sources of forensic artifacts (e.g. storage, VM images, databases, identity access management portal, etc)<br>3. Remotely triage and export selected data (potentially going into terabytes or petabytes of information) in whole or in part seamlessly onto a local or remote storage<br>4. Log down each step in the forensic acquisition process to ensure integrity of digital evidence, and produce a court admissible audit trail<br>5. Generate hash value for each exported forensic artifacts<br>6. Process collected data to perform evidence discovery (e.g. indexing for keyword search, link analysis, sentiment analysis, image/video classification)<br>7. Provide a basic case management system with user access control<br>8. Deployed in the cloud, ideally on a serverless or containerised architecture<br>a. Or otherwise be proven to be scalable, flexible in choice of deployment environment and self-provisioned |

| | |
|---|---|
| | 9. Designed modularly with appropriate level of abstraction for potential inclusion of new native features as required by end-user<br>10. Designed with relevant API endpoints exposed for potential integration of external tools or services as required by end-user<br>The solution provider is to state clearly in the proposal, if the solution will only be able to fulfil the requirements for a certain cloud model (i.e. SaaS, PaaS, IaaS) or a specific CSP (i.e. AWS, Microsoft Azure or Google Cloud). Pre-requisites that are necessary for the solution to meet the requirements above are to be documented in the proposal. |
| **Limitations** | The end-user is not able to provide operational data. Applicants are advised to source for or generate their own test cases / dataset. |

# C. Internet of Things (IoT) Security

## CS07: Unified IoT Security for Connected Products Utilising Edge Computing

| | |
|---|---|
| **Challenge** | Develop a centralised IoT Hub and its corresponding security architecture that integrates connected products and its ecosystem together for efficient security operations |
| **Background** | Digital security must be designed into IoT devices from the group up and at all points in the ecosystem to prevent vulnerabilities in one part from jeopardising the security of the whole. As smart products become increasingly interconnected, they rely on a centralised hub connected to other services to provide a feature-rich, sophisticated, and personalised experience.<br>The processing and transfer of large volumes of personal data makes it an attractive target for attackers. The protection of consumer privacy data must be strictly adhered to according to the relevant laws at the point of collection, in-transit, and at rest to prevent misused or exfiltration at the device or network level.<br>Traditional perimeter security defence models are no longer sufficient or practical for the exponentially increasing number of connected devices. Intelligent systems with the sentient capabilities that can actively detect, monitor, predict and respond needed to defend against the growing landscape of threats.<br>The tipping point for security has always been cost, and while certain industries are willing to spend large amounts, the consumer segment is extremely competitive and cost sensitive, and the right balance must be found for it to be commercially viable in a large-scale global deployment. |
| **Requirements** | A secure IoT system (consisting of backend hub, gateway, IoT devices etc) must have the following capabilities:<br>1. An integrated approach in the detection of security configurations, detection and assessment of vulnerabilities and centralised reporting.<br>2. Monitoring of end to end connections between connected devices and the entire hub<br>3. Have edge computing/federated learning abilities at the connected device to secure data before it is being transmitted out.<br>4. Automatically detect and alerts a central controller upon detection of intrusion, tampering of firmware, algorithm or data within the connected devices.<br>5. Provide telemetry in industry standard formats for integration into a Fusion Centre’s platform for end-to-end monitoring of the entire ecosystem.<br>6. The centralised hub should be able to identify compromised devices and anomalous network activities based on an AI/ML engine’s analysis of a reference model derived from historical (empirical) data and the normal operating characteristics of connected devices. Such devices should be isolated to protect core services and other uncompromised devices, while still remaining functionally operational for the end-user. |

| | |
|---|---|
| | 7. Ability to detect and tag personal identifiable information, personal sensitive information or environmental information automatically.<br>8. Be able to attest to independent accreditation of applicable IoT security standards.<br>9. Solution needs to be developed in a cloud-first approach for scalability, and automation is to be the key guiding principle for the solution.<br>10. A shared library with open API approach embedded into the connected devices for data ingestion and integration is preferred over an embedded agent-based approach.<br>11. Solution should optimise use of connected device's bandwidth and should not adversely impact the system and network performance and operations. |
| **Limitations** | 1. If the goal to protect every device is cost prohibitive or technically infeasible, but to protect the majority of devices and central ecosystem thereby maintain an cost effective operational service, then an alternative approach which is at lower cost, but still remain good level of trustworthiness can be considered.<br>2. At minimum the 50% of requirements must be delivered within 6 to 12 months, where the remaining 50% to be completed within 24 months. |

# D. Operational Technology (OT) Security

## CS08: Threats Detection and Risk Profiling system for Maritime Vessels

| | |
|---|---|
| **Challenge** | Build a threat detection and risk profiling system catered for maritime vessels systems that can analyse, correlate and provide a coherent overview of threat spans across the IT, OT and IoT systems networks in real time. |
| **Background** | A ship's system is complex and runs on IT (Information Technology), OT (Operational Technology – Navigation, propulsion and machinery, access control, cargo management systems) and IOT (Internet of Things – sensors for performance and preventive maintenance systems).<br>With increasing digitalisation, integration, and automation onboard, the originally isolated systems are now moving to a converged network. This introduces higher risk of unauthorised access or malicious attacks to the ships' systems and network and may result to potential safety, environmental and commercial consequences.<br>A real time solution that profiles cybersecurity risk, detect threats, and protect critical assets across all 3 systems will be beneficial to ship operators to mitigate these risks. |
| **Requirements** | We are seeking for an innovative converged security solution that includes but not limited to the following capabilities:<br>1. Identify known cyber threats (malicious code or traffic. This should be based on known threats/ anomalous activities).<br>2. Protect or isolate critical assets from detected known threats based on (1).<br>3. Learning and discovery of data points, data traffic and do assets' risk profiling in real time using AI / ML methods.<br>4. Establish baseline for operating states and detect anomalies in the network. (Unusual data traffic, new traffic events etc)<br>5. Identify events that increases risk score (Unauthorised access, attempt to modify settings, unusual traffic between critical assets onboard vessels etc..) and recommend remediation.<br>6. Provide alert to local operators and administrator to carry out checks.<br>7. Simple UI that can be operated by personnel with only basic training<br>8. Provide dashboard, periodic compliance report for audit verification.<br>9. Ability to aggregate vulnerabilities to a risk scoring system to better understand internal security gaps and external threats.<br>10. Solution may need to be ship-class certified. |
| **Limitations** | 1. Solution may not have consistent and/or reliable data/internet connections.<br>2. Solution should not impact OT systems and IoT Systems.<br>3. Solution cannot be installed directly on the OT systems. |

## CS09: Operational Technology (OT) Honeypot

| | |
|---|---|
| **Challenge** | Construct a honeypot system to collect cyber-attack information for Operational Technology (OT) network which serves as an early warning system, and has the capability to analyse cyber attackers' tactics, techniques and procedures (TTPs), detect new malware and zero-day exploits, as well as confuse potential cyber attackers. System should trace the intruder to its source or origin where the attack is launched. |
| **Background** | The volume of cyber-attacks on the power industry has escalated in recent years as threat actors seek to infiltrate energy infrastructure for cyber-espionage and sabotage purposes. Protecting these critical Operational Technology (OT) networks from exploitation requires a multi-layered security approach that involves physical controls, firewalls, intrusion detection/prevention systems (IDS/IPS), a highly trained security team, and more.<br>However, these tools (and the human teams managing them) have limitations (e.g. new malware may not be detected, inability to detect internal threats), which results in some level of cyber risk for critical power networks.<br>One way to mitigate these limitations and continuously monitor the OT network is through the use of honeypots. OT honeypots can emulate a range of common industry control protocols to appear like a large facility, allowing hostile scanning and other activity to be detected without modifying existing network and system configurations. They provide a means to gather data on attacker trends and tools, research potential countermeasures and test protocol implementations. Well-designed and deployed honeypots can serve as an early warning system, detect new malware and zero-day exploits, uncover insider threats and confuse cyber attackers. |
| **Requirements** | The proposed solution should have the following capabilities and features:<br>1. Emulate devices and control protocols to appear like a power facility<br>2. Adaptable to any ICS environment (e.g. if models change, easily configurable such as using mass-heat balance thermodynamic model or a generic simulator for operator with capability to do start up, steady state and shutdown of a power plant process)<br>3. Acts as an indicator of attack (i.e. a tripwire)<br>4. Appear as a fully functional power facility to cyber attackers in order to delay the actual discovery and compromise of the actual power facility<br>5. Apply relevant industry knowledge to improve the deception and increase the stickiness of the honeypot to better analyse cyber attackers' kill chain, trends and tools<br>6. Detect both internal and external anomalies that may indicate an attack<br>7. Collect and analyse information on interactions/ intrusions (e.g. actions taken, uploaded malware, exploits used) that can be translated into actions to improve existing cyber defences<br>8. Provide alerts and notifications in case of attacks. |

| | |
|---|---|
| | 9. (Optional) Trace the intruder to its source or origin where the attack was launched.<br>10. Honeypot should be tested via a hackathon or similar event to prove its functionality |
| **Limitations** | 1. The honeypot must be appropriately sandboxed in the event it is to be integrated into one of standalone process control system to mitigate the risk of intrusion attempts into current operating OT systems.<br>2. No sensor or appliance should be installed in the existing OT system<br>3. The honeypot infrastructure shall remain at the test site after the conclusion of project. |

## CS10: Intelligent & Adaptive Detection Models for OT Systems

| | |
|---|---|
| **Challenge** | Build a digital twin with a detection engine model to detect security incidents and unauthorised commands through packet inspection. The detection engine should be able to adapt to different SCADA network setups, data types and network that can be scaled up through virtualisation with detailed simulation using hardware-in-the-loop (e.g. PLC). |
| **Background** | An OT plant contains many processes that generate a large amount of process data that is difficult for operators to detect when values are spoofed, especially if the spoofed value is within the allowed range.<br>Such anomalies will result in plant operators having an inaccurate picture of their systems, which can result in attackers being able to traverse through the plant network without being detected and this presents a serious security breach.<br>Legacy OT communication protocols do not have mechanism to authenticate and encrypt communication packets, allowing an attacker to freely launch attacks on PLC networks once they have manage to gain access into the PLC network which can severely impact operations and have catastrophic consequences.<br>This challenge seeks an innovation solution that is able to predict process values and automatically trigger alerts if a deviation is detected, and to be able to detect anomalies in a wide variety of process data based on historical behaviour and data. |
| **Requirements** | We are looking at building a digital twin with anomaly detection and machine learning capabilities that can:<br>1. Predict expected output and sensor values based on input values in comparison to historical data and the ability to withstand anomalous data due to machine failure/maintenance<br>2. Correlate data from analogue and digital data points to detect anomalies<br>3. Automatically learn baseline plant process through historical data and automatically trigger alerts when deviations between predicted and actual data collected is detected.<br>4. Utilises AI/ML to detect security incidents based on anomalies in the process data and the detection of unauthorised commands through deep packet inspection.<br>5. Automatically improve the AI/ML model in term of detection accuracy and false alarm through reinforced learning when more data is available.<br>6. Detect manipulation and/or spoofed data from data collected by SCADA I/O servers through machine learning of historical behaviour by operators<br>7. Automatically filter out relevant OT communications protocol (e.g. Modbus, DNP3 for machine learning to monitor network traffic, learning the plant’s behaviour<br>8. Differentiate between maintenance/equipment failures and Cyber attacks<br>9. Ability to score and rank alerts to reduce false alarms and operator load<br>10. Be able to detect suspicions traffic (e.g. illegal file transfer, malicious packets, scanning traffic, download of PLC logic) that should not be present in the automation network |

| | |
|---|---|
| | 11. Interface with common SCADA system (e.g. OPC)<br>12. (Optional) The ability to block spoofed commands and not become a risk to plant operations will be considered in the evaluation criteria |
| **Limitations** | 1. Proposed implementation should not impact the operations of any plant.<br>2. Internet connection to external systems are not allowed. |

## CS11: Breach and Attack Simulator (BAS) for an Internet of Things (IoT) connected Power Grid

| | |
|---|---|
| **Challenge** | Develop a Breach and Attack Simulator (BAS) for IoT devices like AMI and EV charging points to continuously identify potential vulnerabilities and weakness in deployed end-point devices at remote sites that are unattended |
| **Background** | Part of Singapore's Smart Nation Initiatives is to push for more connectivity in the daily touch points of the citizens. One such way was the proliferation of connected devices in the form of the Advanced Metering Infrastructure (AMI). AMIs, or "smart meters" are connected to the grid that is able to provide real time data. While previously offline, the new connected meters offer advantages in the form of real time consumption tracking, allowing for better load balancing and generation forecast. However, this brings along a new set of problems that did not exist previously, which was being connected meant that it was open to threats on the internet.<br>With the global trend towards electrification, charging points/stations for electric vehicles (EVs) are being rapidly deployed, and such charging points need to be connected to the grid for its advanced functions to work.<br>As more devices are connected to the grid, the number of access points increases as well, raising the possibility of hackers gaining access to it the private grid network. The current method of securing the IoT devices before they are deployed will not be feasible when deployment ramps up, and there is also the requirement to keep them secure at all times against charging threats. A BAS for IoT devices is required to keep up with the threats. |
| **Requirements** | The proposed solution should be able to identify potential vulnerabilities through automated, continuous assessments and ideally should take into consideration integrations including:<br>1. Develop and Maintain a database of vulnerabilities for IoT systems<br>2. Identify and flag vulnerabilities detected<br>3. Continuously scan, identify and flag new vulnerabilities<br>4. Provide remediation and mitigation suggestions on detected vulnerabilities.<br>5. Be resilient and fail-secure, isolating faults without affecting the entire grid<br>6. Be compatible with all relevant IoT devices in use |
| **Limitations** | 1. Solution providers should have a portable setup, which allows them to connect to the network and run the simulation on SP Group's test site.<br>2. Solution providers will be able to run the simulation on a living lab test-site, which is a lab environment with real devices accessible to consumers, such as EV charging stations and smart meters. |

## CS12: Supply Chain Security: Detection of Malicious Code and Vulnerabilities within Software Patches for IT/OT Environments

| | |
|---|---|
| **Challenge** | Provide a solution that can scan and review software and system patches of commercial software and applications commonly used in an IT/OT environment so as to identify malicious code and vulnerabilities, as well as provide recommendations on remediation actions |
| **Background** | Every organization adopts various commercial software and system tools for day to day operations (e.g. Windows, SCOM, Altris, Ansible). Most software vendors published regular patches and updates. However, increasingly we see threat actors embedding malware into patches through compromises in these product companies.<br>These "loaded" patches are pushed out to the customers of these companies and thus compromised the end users. These incidents results in credential theft, privileged escalation and lateral movements, ransomware, data exfiltration and data theft which results in major disruptions to businesses.<br>One recent example is the SolarWinds incident where the company released a "rogue" software update of their Orion platform solution which resulted in malicious codes being pushed down to 18,000 of their customers (which includes Microsoft, Intel, Cisco and FireEye). This compromise not only impacted SolarWinds products but also their customer's own products. For example, Microsoft pushed out security advisories and patches for their own product lines to their own customers.<br>Another example of a Supply Chain attack is the recent Kaseya ransomware attack that was triggered over the American Independence Day weekend. The attack carried out by threat actors leveraged on a vulnerability within Kaseya's virtual management software. Ransomware was then pushed via an automated, fake, and malicious software update to multiple managed service providers (MSP) who in turn passed it onwards to their customers. |
| **Requirements** | The proposed solution should address these key requirements:<br>1. Scan Commercial Software patches and releases and detect malicious code/functions, vulnerabilities and suspicious behaviours<br>2. Handle a wide variety of software and system tools<br>3. Efficient execution of scan (i.e. able to be completed in a short time)<br>4. Little or no impact on day to day functionality of software and applications being tested<br>5. Use machine learning (ML)/artificial intelligence (AI) to improve review process |
| **Limitations** | Proposed solutions should not excessively load production system resources and impact business operations. |

# E. Privacy-enhancing Technologies

## CS13: Protection of PII and Data Sharing in Healthcare

| | |
|---|---|
| **Challenge** | Automated detection and de-identification of Personal Identifiable Information (PII), and manage secure data sharing in a scalable and efficient manner |
| **Background** | Data collected in healthcare systems are mostly highly sensitive information, which includes personal information and health records. These data are often transmitted to other digital systems for research and audit purposes via automated batch processing or as live streamed data. Current measures are taken to restrict availability of information through the following:<br>1. Containment of data within Intranet,<br>2. Controlled access to only authorised personnel,<br>3. De-identification and encryption for data-at-rest and data-in-transit, and<br>4. Complete anonymisation of data and generation of synthetic data for use in unsecured instances<br>These measures, though effective, are highly restrictive and reduce the efficiency of secure data sharing.<br>Currently, the deidentification and anonymisation are heavily reliant on human effort to apply these codes on multiple datasets, which is tedious and prone to error. The activities such as tokenisation of PII before transmission, setting cryptographic keys are manually performed. In addition, the periodic changing of cryptographic keys, and maintaining change logs often takes a long time to complete. Implementation could be further delayed or non-operational, if there were any changes in personnel.<br>This challenge seeks an innovative solution, which can detect and automatically de-identify PIIs of various datasets at scale; and to manage secure data cryptographic keys in a scalable and efficient manner. |
| **Requirements** | The proposed solution must provide (but is not limited to) the following functionalities:<br>1. Manage and protect cryptographic keys (Automated Key Management System), in alignment with NIST's definition of cryptographic key lifecycle management and best standards<br>2. Perform cryptography functions for large volumes of data at high speed<br>3. Generate, deploy and test cryptographic keys automatically, for enrolment of new users between data stream owner, data stream recipients and IT personnel<br>4. Authenticate and authorize users, according to end-user's requirements (i.e. Principle of least-privilege)<br>5. Implement algorithms and protocols in a modular basis, to allow for upgrading to new, emerging industry standard cryptographic algorithms and supporting of various types of communication protocols<br>6. Create a set of gradated policies for users to select levels of pseudonymization of healthcare data, which are compliant to government regulations (i.e. PDPA and GDPR)<br>7. Be able to automatically identify PII from data collected in the healthcare systems. This means identifying data which are: |

| | |
|---|---|
| | a. PII by itself (i.e. NRIC)<br>b. PII data, which is formed from aggregating various non-PII data (i.e. First Name, Age, Gender)<br>8. Collect audit trails of events, such as user logon activities, changing of cryptographic keys and failed authentication of non-interactive operations.<br>9. Flexible to be deployed in either on-prem and cloud environments.<br>Scalability of the proposed solution will be an important consideration for evaluation. |
| **Limitations** | 1. Data and the solution must remain in Singapore.<br>2. Solution providers must sign a NDI with the end-user.<br>3. Project is to be completed within 12 months.<br>4. Solution must be installed on user's servers for testing<br>5. Proposed solution should not consume significant network bandwidth or impact operational systems.<br>6. The user will fully own and configure the automated deidentification code once the project is completed.<br>7. Proposals with solution development being completed in 12 months will have an added advantage. |

# 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:

1. AI For Cybersecurity
2. Cloud Security
3. IoT Security
4. OT Security
5. 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.