Cybersecurity Industry Call for Innovation

Supported by

CSA
SINGAPORE

Uplifting the development of Singapore's cybersecurity ecosystem

Powered by

TNB
VENTURES

Challenge Statements

Table of Contents

Introduction

The Cyber Security Agency of Singapore (CSA) and partner TNB Ventures have launched a Cybersecurity Industry Call for Innovation in collaboration with participating companies - Ascendas-Singbridge, PacificLight Power, Singapore LNG Corporation (SLNG), SMRT Corporation (SMRT) and Singapore Press Holdings (SPH).

The Call for Innovation invites solution providers to submit proposals for innovative solutions that address cybersecurity challenges articulated by these users in the areas of Advanced Protection and Detection and Advanced Security Operations. These solutions should be ready for testing and deployed within a year or two (Level 6 and above in terms of Technology Readiness Level).

We have compiled a set of 10 challenge statements highlighted in the next section. These challenge statements were articulated and distilled based on the Value Proposition Canvas and the US National Institute of Standards and Technology (NIST) cybersecurity framework. The Framework served as guidance for end-users from different sectors and individual organisations to articulate their risks, situations and needs.

The 5 key areas for innovation opportunities were:

1. **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
2. **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
3. **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4. **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
5. **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

These challenge statements were further classified into the two main themes of Advanced Protection and Detection, and Advanced Security Operation.

Solution providers whose proposals are shortlisted will have the opportunity to discuss their proposals further with end-users for potential adoption, co-innovation, investment, and test-bedding opportunities.

Selected solutions which fulfil the eligibility criteria[1] may also be awarded with Proof-of-Concept (POC) funding of up to S$500,000 under CSA's Co-innovation and Development POC Scheme.

[1] For more information on the eligibility criteria, please refer to https://www.csa.gov.sg/programmes/proof-of-concept-scheme

1. Advanced Protection and Detection

1.1. Operational Technology Intrusion Detection Systems

In Information Technology (IT) systems, the main security consideration is to protect sensitive data, whereas the Operational Technology (OT) Systems that process operational data e.g. Industrial Control Systems, such as Supervisory Control and Data Acquisition systems (SCADA), Distributed Control Systems (DCS) are often designed to ensure high availability and safety. Breaches in IT system would result in loss of data while breaches in OT system may affect critical operations which may cause safety issues and property damage.

In addition, OT system has not traditionally been a network technology. For example, IT system uses standard communication protocols such as TCP/IP, whereas OT system, which consists of various devices from different OEM, uses proprietary or industrial communication protocols such as IEC and Modbus. It is a challenge to detect security breaches in such OT system with a large number of different proprietary communication systems

We are seeking innovative OT intrusion detection solutions based on the normalcy of known process models, abnormality of networks and system traffic between field devices and HMI. These may include, but not be limited to:

a. Profile network communication
b. Identification of “first seen” events
c. Identification of unusual manipulation of critical perimeters
d. Identification of unusual traffic between controllers/devices in the OT system which are not part of the baseline on behavior, time, value and threshold (e.g high volume, or abnormal hour)
e. Identification of anomalies in the traffic in a wide variety of vendors’ proprietary controllers/devices
f. Comparison of predicted dynamic process model data[2] against sensors data
g. Identification of comparison deviations in (f)
h. Periodic controllers’ program/functions/firmware validation
i. Data/data registers’ integrity inspection
j. Correlation of field devices anomaly with network layer anomaly to detect malicious activities.

Proposed solutions should not have any consumption of production network bandwidth and should not have impact to the operation of the OT system. The scalability of proposed solutions will also be an important consideration for evaluation. Artificial intelligence in detecting abnormality behavior of monitored traffic is also recommended.

[2] Not system baseline

1.2. Operational Technology Log Analysis

The Operational Technology (OT) networks (e.g. industrial control and supervisory control and data acquisition systems, ICS/SCADA) are a collection of devices designed to work together as an integrated and homogenous system. If one of these systems fails, it will generate a catastrophic domino effect.

Many of these OT systems comprise of various components that require system engineers to collect and monitor logs from different devices. The system engineers have to manually check logs and contact third party vendors for assistance for the OT systems or other non-documented legacy system issues.

A key challenge lies in insufficient documentation or knowledge for interpreting logs, alongside different logs with various formats that may prevent timely interventions. Different systems also have different command sequences, logic and protocols, resulting in logs unique to each system. Other challenges include having low quality and conflicting data points that affect timely triage across multiple systems, thus potentially leading to several costly false investigations.

We are seeking innovative solutions including but not limited to:

a. A platform to collect and translate logs from different OT system to a common language (the underlying semantics of the logs) that can be easily understood by the operators.

b. The ability to automatically and accurately generate alerts of abnormal network behavior

c. The ability to analyse logs from different parts of a system, and to trace and identify the root cause of an event

1.3. Advanced Threat Monitoring

Security Operation Centres are dealing with a large variety of big datasets everyday. Some information sources are structured (eg. security logs), while others are unstructured (eg. intelligence reports on new threats). The current process of security analysis starts from sifting through all information sources (internal and external) to identifying noteworthy correlation from all data points. In a swath of irrelevant noise, security analysts are expected to focus on relevant data and venture to identify known and unknown threats.

We are seeking innovative solutions that will address all challenge areas as follows:

a) The first area is building an adversary behavioural and Tactics, Techniques and Procedures (TTP) knowledge base using known "attacker" datasets from all sources of information (both structured and unstructured). The knowledge base should also include modus operandi and adversarial actions of persistent threat actor over time. This shall aid the tracking, all-source analysis and assessment of emerging and evolving threats and allow organisations to proactively defend against these threats.

b) The second area is identifying "known" threat/anomalous activities. With the insights from the knowledge base in (1), similarities in "known bad behaviour" can be used to surface "known" threat/anomalous activity flows from network telemetry datasets, such as malware "beaconing"/callback activities, covert channels and possible data exfiltration etc. Analytics should be applied on both successful and failed/blocked attempts to gain further insights to the threat landscape specific to the organisation. This shall also further build up the knowledge base in (a).

c) The third area is discovering "unknown" threat/anomalous activities. With the "known" threat/anomalous activities formed, how can it be used to identify "undiscovered" or "unknown" attack processes from network telemetry datasets, e.g. new attack campaigns.

d) The fourth area is pinpointing precursors to a potential cyber-attack. Insights derived from "known" and "unknown" threat/anomalous activities will allow analysts to understand the cyber threat landscape over time (i.e. historical as well as real-time). This will allow pre-emptive measures to be put in place to mitigate against potential cyber-attacks.

We are seeking solutions to develop a coherent solution to address the aforementioned areas. This will aid organisations to achieve an efficient and effective way of deriving insights from very large dataset to better forewarn against eminent threats.

Solution providers should assume that no sample data will be shared by the sponsored organisation, and solution providers will have to source for relevant datasets to demonstrate the capabilities in solving the above challenge areas.

1.4. Securing Social and Digital Platforms from Phishing and Malicious URL Redirects

With increasing business demands for creating new digital & social media channels via partnerships, end-users need to enhance digital security by securing platforms (including third party platforms) against URL redirects and fake content.

A key challenge lies in insufficient real-time analysis and detection capabilities of malicious or fake user comments via uploading of files and phishing URL(s). A common example is when a user is deceived by trusting a redirected source by disclosing confidential information.

We are seeking innovative solutions to improve real time analysis and detection capabilities including but not limited to the:

a. Identification of malicious posting on a single or cross platform, and automatic removal of the posting;

b. Identification of “bad” users and the automatic blacklisting of such bad users;

c. Identification of unusual high volume postings from single user;

d. Identification of attack profiles (e.g. by region, attack hours etc.).

1.5. Customer / User Data Security and Privacy

Incomplete customer data are often misleading and result in poor marketing decisions. Moreover, these data are mostly stored and managed in different databases and systems; thereby increasing the risk of data misuse and leakage.

As such, many organizations are increasingly looking to incorporate a single customer overview (also known as a ‘360’ or ‘unified’ customer view) where all customer data are consolidated into a single record.

We are seeking innovative solutions including but not limited to:

a. Efficient customer data collection and consolidation from various touch points; to alleviate the need for customers to do multiple data entries;

b. Effective protection of customer privacy and sensitive data;

c. Detection and blocking of abnormal access of customer data;

d. The ability to trace and monitor the digital path of customer data;

e. The ability to prevent customer data from leaving the organization’s system.

1.6. Reducing Human Vulnerabilities in Security Systems to Achieve Better Security Compliance

Human vulnerabilities such as carelessness, ignorance, mistakes and even “curiosity” remain the ‘achilles’ heel of cybersecurity and it has been reported that an estimated 60% of enterprise companies have been the target of socially engineered attacks.

The current method of periodic training and informative sessions is expensive, consuming, ineffective and often reactive. With a growing number of touch points and security compliance requirements, providing timely and effective user training becomes a daunting challenge; especially in an extensive workforce present in multiple locations and geographies.

End-users are seeking innovative tools to educate their users and provide for timely interventions in the event of unfavourable user behaviour.

We are seeking innovative scalable solutions to provide for:

a. Timely and contextualised training and guidance across multiple use environments to address vulnerabilities such as phishing and vishing, whilst remaining compliant (eg. handling consumer data) and nurturing a more ‘security-aware’ culture.

b. Automated and highly accurate tools that provide timely interventions as users conduct their daily business. These tools should have the intelligence to evolve alongside changing threats and be easily incorporated into various touch points and applications (eg. emails and marketing software).

2. Advanced Security Operation

2.1. Patch Management and Vulnerability in Operational Technology Environment

Software patches are applied to update systems and deal with vulnerabilities or security gaps. Software vendors routinely deliver patches for products to ensure system safety whilst updating systems. Without these patches, new functionalities remain undelivered and systems can be vulnerable to cyber-attacks.

One of the key challenges is the risk of applying these patches to a production system. Every OT system is different, and even though patches have been tested in the OEM setup, it is still necessary to thoroughly review patch management documentation, and perform proper risk assessment before allowing patches to be released into the production environment. This is important particularly given that the high cost of setting up mirrored staging sites.

Another key challenge is the delay in patch execution. In critical systems, some patches can only be applied during maintenance period; thereby leaving the organization at risk to the vulnerabilities for months or even a year. The process of patch execution remains time consuming and requires dedicated personnel – downloading and updating patches manually takes a long time.

We are seeking innovative solutions including but not limited to:

a. The cost effective assessment of the interdependency impact of the patches and patched systems

b. The identification of vulnerabilities (especially known or zero-day attacks) on an existing in-situ OT landscape to form a risk decision matrix for end-user to decide if it is critical for patching.

c. To prevent vulnerabilities being exploited without a patch; and

d. A more effective and efficient patch management methodology/system for silo and multi-site operating environments.

2.2. Securing IoT/Cloud Systems in Building Management

The end-user develops and manages numerous buildings within technology parks in multiple countries and has seen an emergence of estate monitoring and building management solutions that are IoT and/or cloud based.

The end-user wishes to adopt these new innovative offerings at the earliest feasible time to improve efficiency, sustainability and overall manageability. However, these IOT/Cloud solutions are also possible launching grounds for cyber-attacks and/or a catalyst for more broad based building-wide failures; thereby increasing collateral damage.

We are seeking frameworks and innovative solutions that would reduce the risk and at the same time allow for quicker adoption of these IOT/Cloud systems in a scalable way across multiple buildings in multiple locations. We are seeking solutions including but not limited to:

a. The systematic and rigorous evaluation of cyber risks posed by the adoption of these systems;

b. Scalable solutions to monitor and provide timely notifications when these systems turn vulnerable and become cybersecurity threats;

c. Scalable solutions to expeditiously isolate these systems in the event of potential threats.

2.3. Effective evaluation of the Security Posture of Outsourced Partner's Systems

Outsourcing network services is a common business practice for most large organisations. Although these digital/network services often undergo rigorous contract reviews, content audits and extensive access control; they lack real-time risk identification and protection.

Due to the lack of visibility in engaging security implementation outside contractual specifications; outsourcing can pose a serious risk to proprietary information, especially protected user data. With the rise of cloud service providers from niche to global providers, there is also a lack of a real time security assessment, governance and certification of these providers for end-users to evaluate the cloud provider's actual security posture in areas of operations, systems, networks and data protection.

Nevertheless, there are potential new vulnerabilities given the data sharing with third parties as well as the multi-layer interconnect between independently operated systems. These threats are exemplified by any changes and updates that are independently conducted by each party.

We are seeking proposals on innovative solutions to:

a. Improve the assurance mechanism and gain insights into the outsourced partners/providers' internal security controls in the area of data security and privacy for all 3rd party; including cloud providers;

b. Provide threat risk assessments on systems access and connections and impose a need to know basic when granting access rights to external outsourced vendors.

2.4. Intelligent management of Identity Access Management and Governance

Large corporates have thousands of users island-wide scaling across many core departments IT based applications and OT physical card access system. Current identity management and governance is based on a manual process where department managers are required to signoff individual users and access rights on an annual basis. This not only results in unproductive man-hours, but also causes an outstanding audit challenge.

Moreover, a lack of transparency exists as the current identity platform and process does not provide unified management and baseline visibility of its privilege administers, normal users, groups and access permissions.

With the rise of cloud and mobile channels, digital business applications are outgrowing traditional network boundaries; alongside the pressure to scale faster. This phenomenon becomes a constant spectre of hacking, insider threats and consumer fraud – thereby necessitating identification-based access controls throughout the different environment.

We are seeking innovative identity access management and governance solutions based on the AI concept of including but not limited to:

a. Learning and discovery of users, groups and access including privilege user accounts across various operational and information systems, operating systems, networks and applications including 3rd party outsource & partner cloud environments

b. Identification of anormalcy or abnormality of identity access and management across network, application and system traffic

c. Monitor abnormal user access to system accounts

d. Intelligence assessment of user rights assignment