Cybersecurity Industry Call for Innovation 2019

Supported by

Uplifting the development of Singapore's cybersecurity ecosystem

Powered by

CONTENTS

A. Cyber Readiness

CS01: Integrated Cooperative Cyber Defence

Challenge	Develop a fully integrated threat mitigating solution based on CSA's Be Safe Online measures with automated threat identification, protection, detection and response
Background	Despite the abundance of available security solutions, the volume and frequency of data breaches and serious ransomware incidents continue to rise. One key cyber defence strategy involves the mapping of all existing assets to enable continuous monitoring of unauthorised behaviour. This strategy aims to map assets' details comprehensively and accurately as the source of truth and trust, enabling every unauthorised/unknown element in the environment to be identified so that threats may be detected. Data should be protected with an 'encrypt everywhere' policy to prevent exfiltration of data in unencrypted form. This concept requires components to cooperate to provide mutual protection. In the event that any component is disabled (regardless of malicious intent), decryption of data should be disabled to ensure that data remains encrypted. CSA has published the Be Safe Online (https://www.csa.gov.sg/news/publications/be-safe-online) measures to help companies enhance their cyber defence capabilities. This challenge seeks an integrated implementation of the Be Safe Online measures in order to provide automated threat mitigation.
Requirements	The proposed solution must implement the Be Safe Online measures with the following functions: a. Keep track of system assets (software and hardware information) b. Analyse asset list for Common Vulnerabilities and Exposures (CVEs) to allow users to prioritise patching and updating c. Allow only authorised software to work (using asset information) and investigate unauthorised elements using multiple anti-virus engines, Artificial Intelligence and behavioural analysis to detect threats d. Integrate solution components to enable communications between them to increase chances of detecting breaches promptly and mitigating threats e. Detect and block anomalous behaviour and known/unknown threats through continuous monitoring of assets f. Automatically analyse any anomalies and provide an incident response g. Perform automated log and account analysis to detect potential threats and provide consolidated compliance/management reporting h. Encrypt data i. Disable decryption of data if any component of the security system is disabled (regardless of malicious intent) j. Secure systems and user devices on premise and cloud environments k. Provide alerts in case of potential system breaches (e.g. if any component is disabled by a threat) l. Provide an integrated dashboard for SOC analysis (e.g. triaging) and management view that can work with third-party ticketing systems (e.g. Remedy)

CS02: Real-time Risk Scoring of Data Centres

Challenge	Provide robust real-time scoring of the cybersecurity posture of colocation data centres based on agreed-upon cyber risk indicators
Background	Data centres store, manage and disseminate large volumes of sensitive customer or proprietary information. Data centres are complex facilities that combine Information Technology (IT) and Operation Technology (OT) (e.g. power, cooling, surveillance) to provide high availability with minimal downtime. The continuous operations of a data centre's OT systems is critical for the non-stop support of customer IT workloads. However, originally isolated OT networks now need to communicate with IT networks (e.g. to allow customers to view system performance). This has necessitated a certain amount of IT-OT convergence and introduced risk. Due to the high concentration of mission-critical assets on their premises, data centres face a wide range of security risks, ranging from physical theft to cyberattacks. A combination of physical and virtual (cyber) security is required to ensure the confidentiality, integrity and availability of the hosted data. The cybersecurity posture of a data centre facility consists of all OT and IT security controls. There are currently no industry standards and frameworks available to assess and manage data centres' cybersecurity posture. A holistic solution to monitor and score the cybersecurity posture of data centre facilities in real-time will be highly beneficial to data centre providers and their customers.
Requirements	We are looking for a solution with the following capabilities: a. Define key cyber risk indictors for data centre facilities that includes all OT and IT security controls b. Define the architecture and cybersecurity controls (Technology and Solutions) that can meet the highest cybersecurity standards (e.g. in terms of defined risk indicators) c. Collect all data points relevant to the identified risk indicators in real-time d. Allow identified risk indicators to be monitored over the Internet e. Calculate a real-time cyber risk score based on agreed-upon risk indicators f. Use Artificial Intelligence (AI) / Machine Learning (ML) to improve risk assessment (e.g. accuracy, indicator weightage) and provide alerts before the threshold is reached g. Identify the reason (e.g. location of missing controls) in the event of any change in risk scoring and recommend remediation actions to mitigate any detected increase in risk h. Improve and enhance security controls progressively based on AI/ML learnings on (g)
Limitations	There are currently no industry standards and frameworks available to assess (score) and manage data centres' cybersecurity posture in real-time

B. Industrial Protection

CS03: Identify Cybersecurity Threats by Context-aware Power Plant Simulation

Challenge	Provide a simulated process model of a power plant that can differentiate between cyberattacks and operational issues
Background	The Distributed Control System (DCS) within a power plant consists of sensors, controllers and associated computers to monitor and control physical equipment and processes. The DCS comprises many operating parameters (e.g. temperature, heat rate, heat balance, efficiency, pressure, equipment vibrations), some of which are displayed and can be controlled by the plant operator. Current industrial Intrusion Detection System (IDS) solutions in the market establish baselines by monitoring network traffic for a limited duration. However, the behaviour of the system and network differs during various operating states (e.g. start-up, steady state, shut-down, outage). These differing plant states have distinct baselines that could lead to an increase in false positive alarms. Operators are usually alerted to abnormal conditions by alarms and warnings. Due to the large number of operating parameters displayed in the centralized controller, even a highly experienced operator may have difficulty differentiating between a cyberattack and equipment fault. Cyber attackers can also display fictitious values in the DCS or suppress the alarms to disguise system compromise.
Requirements	We are looking for a simulation of the entire power plant system that can fulfil the following requirements: a. Model processes within the plant[1] b. Establish baselines/profiles for different operating states (e.g. start-up, steady state, shut-down, outage) c. Monitor key parameters (e.g. temperature, heat rate, heat balance, efficiency, pressure, equipment vibrations) to detect any abnormalities d. Model and account for changes due to equipment aging to reduce false positives e. Allow for flexible data input to calibrate model (e.g. import historical data, upload/modify planned schedule, remarks for any unplanned state changes) f. Simulate/Forecast output values based on specified inputs g. Compare actual value against forecasted value and trigger alert in case of anomalies (i.e. deviation exceeds threshold) h. Differentiate if the anomaly is due to a cyberattack or operational issues i. Support different OT networks implemented by various vendors j. Alert operators to carry out the necessary checks

[1] Schematic diagram will be provided to shortlisted applicants

CS04: 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.
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. 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. 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: a. Emulate devices and control protocols to appear like a power facility b. Adaptable to any ICS environment (e.g. if models changes, easily configurable) c. Acts as an indicator of attack (i.e. a tripwire) d. Appear as a fully functional power facility to cyber attackers in order to delay the actual discovery and compromise of the actual power facility e. 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 f. Detect both internal and external anomalies that may indicate an attack g. 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 h. Provide alerts and notifications in case of attacks

CS05: Secure Autonomous Prime Movers (APMs)

Challenge	Detect and protect against potential cyber threats to local Autonomous Prime Movers (APMs) platform systems and communication with infrastructure layers in a scalable and implementable manner
Background	Terminal prime movers operate within the port confines to transport shipping containers from ships to onshore cranes and container yards, and vice versa. The user is presently exploring the automation of this transport process via the development of Autonomous Prime Movers (APM) for driverless container operations in mixed traffic conditions within the port. The APM is a cyber-physical system with embedded control systems and multiple interactions with the port environment. Operational safety is of paramount importance as the APM will be moving heavy loads at speed in a live environment. For example, tampering of data transmissions between various APM hardware components (e.g. CANBUS message spoofing) could result in vehicle control being impaired. A compromised APM system (e.g. due to a cyberattack) could result in human injury or property damage. Protecting the APM's potential attack surfaces is essential to maintain operational safety within the port.
Requirements	We are seeking vehicle-level APM solutions with the following characteristics: a. Propose and explain potential APM vulnerabilities and/or attack vectors b. Demonstrate the proposed vulnerability exploit(s) and/or attack(s) on an APM (or similar system) c. Design and develop countermeasures against described APM vulnerabilities and/or attacks d. Work with user-appointed APM vendor/supplier for system integration e. Be scalable with reasonable implementation effort as it has potential impact on fleet proliferation of the APM for port use
Limitations	End-user intends to negotiate ownership of foreground IP

C. Secure Access

CS06: Authentication and Detection for Industrial HMI Systems

Challenge	Provide a robust and out-of-band authentication, logging and detection solution that allows power plant operators to seamlessly access Human-Machine Interface (HMI) systems
Background	Human-Machine Interface (HMI) systems within a power plant provide schematic representations of plant processes and are critical to plant operations. The HMI enables the operator to control the plant systems (e.g. gas turbines) and monitor plant operating data. These systems operate continuously (24/7) and can be configured to provide alarms and event notifications. Existing HMI access controls are managed through logins with usernames and passwords assigned to individual operators. While it is not operationally feasible to require repeated authentication (e.g. login/logout of operating system) whenever an operator performs any action on the HMI, there needs to be a way to log the actions performed by individual operators for security and audit purposes. In addition, it is of utmost importance to prevent disruption to plant operations.
Requirements	We are looking for an out-of-band authentication, logging and detection solution with the following characteristics: a. Hardware solution for input devices (e.g. keyboard, mouse, touchscreen) that is robust enough to operate in an industrial environment b. Incorporate some form of biometric or nearfield communication (NFC) authentication to provide the operator with quick and seamless access c. Work for all HMI systems from various vendors d. Ability to manage access rights e. Capture and log the actions performed by individuals on the HMI systems, e.g. login attempts (success/failure), control operations f. Ability to detect anomalies and provide alerts in case of such detections g. Block compromised accounts to prevent access to other HMI systems
Limitations	Software **CANNOT** be installed on the HMI systems

CS07: Integrated User Access Monitoring

Challenge	Design a user access monitoring and control system which can integrate information across multiple sources, and intelligently and automatically monitor user access and behaviour to detect potential unauthorised access to sensitive records.
Background	Traditional user access management systems require manual mapping of personnel records and information with required roles to establish extensive user access matrices. This is often a tedious process requiring regular manual reviews of user accounts and access rights, and extremely unwieldy when personnel records and information on user roles come from multiple sources. While user access can be logged, effective monitoring of access logs can be challenging. Traditional user access management systems depend on pre-defined rules which are manually defined and often difficult to calibrate appropriately across different users. Above-threshold accesses and exceptions also have to be manually reviewed which is tedious and time-consuming and may not be sufficiently responsive to unauthorised accesses. This challenge seeks an innovative user access monitoring solution which can integrate user information from multiple sources, and intelligently and automatically analyse user behaviour to identify and detect potential unauthorised access.
Requirements	We are seeking an innovative user access monitoring and control solution that can: a. Authenticate users securely b. On-board new records (e.g. users, patients) in a seamless and secure manner c. Integrate personnel records and information on user roles across multiple sources d. Incorporate AI capabilities to monitor and learn user access behaviour across different users and roles e. Dynamically establish anomalous user access patterns and thresholds for identifying potential unauthorised Electronic Medical Records (EMR) access f. Raise alerts when such unauthorised user accesses are detected g. Provide a flexible dashboard with customisable settings and views (e.g. charts) to enable easy reporting h. Allow administrators to drill into alerts to investigate detailed access by users i. Centralized control to manage and limit access based on the principle of least privilege (e.g. read-only access for auditors)

CS08: Multi-Factor Authentication (MFA) for Different Healthcare Operating Environments

Challenge	Develop a Multi-Factor Authentication (MFA) solution to support healthcare workers in their use of clinical applications (without any change to these applications) with adaptive authentications that vary according to medical environment
Background	Healthcare software provides a spectrum of benefits, enabling healthcare providers to manage organization data, access patient records and operate clinical equipment. Most healthcare organisations end up using a wide variety of applications from different vendors based on their suitability for specific use cases. Software from different companies may have disparate credential policies and authentication rules. Healthcare providers end up having to memorize a wide range of credentials. In addition, some of these applications may only support single-factor authentication, making them susceptible to an increasing range of cyber-attacks. The use of Multi-Factor Authentication (MFA) will help to address some of these security issues, but there are several operational and deployment limitations in time-sensitive medical environments. For example, biometric solutions may not be compatible where the use of clinical masks and gloves are routine, while physical tokens may not be compatible in sterile environments (e.g. Operating Theatre). Multiple medical applications may be installed on a single machine. A flexible MFA solution is required to manage these third-party applications in a cost-effective manner with minimal impact to existing systems and applications, while allowing varying authentication requirements to be enforced depending on the operational constraints of the healthcare environment.
Requirements	The proposed solution should have the capability to: a. Perform user authentication using at least two factors with Single Sign On (SSO) for existing applications (without modifying the applications) b. Store user credentials of all the software applications securely c. Achieve near real-time authentication for legitimate users d. Prevent bypass of the proposed solution (i.e. users should not be able to access the protected applications directly) e. Fail secure mode to be triggered should authentication fail to work f. Manage the credential policies of all software applications (e.g. password change frequency, complexity requirements) g. Removal of an authentication factor should trigger proper logout from account or application h. Flexible and configurable authentication policy i. Vary authentication policy dynamically based on operational constraints (e.g. physical location) j. Support multiple user profiles (i.e. different users may see different apps) k. Be seamlessly integrated into existing electronic medical records software use in healthcare operating environments
Limitation	The software applications to be protected must not be modified.

CS09: Living Lab: Secure Remote Building Control

Challenge	Devise a solution to remotely control buildings and extract building systems data that is secure, practical and affordable
Background	Smart facilities management (FM) systems enable functions such as building optimisation, estate monitoring and workflow automation. A centralised and integrated building and estate operations command centre (Ops Centre) allows for remote monitoring of buildings and optimisation of building systems (e.g. air conditioners, lighting). The Ops Centre currently only has monitoring capabilities. Control capabilities for Building Management System (BMS) are currently disabled due to security concerns (e.g. remote building controls may be hacked, resulting in BMS compromise and potential failure of mission critical facility operations). In addition, to analyse and troubleshoot any issues that arise within a particular building, data extraction has to be done on-site due to perceived security issues with remote data extraction. It will greatly increase the efficiency and efficacy of the Ops Centre and BMS if secure means of remote building control and data extraction can be implemented.
Requirements	We are seeking a solution to provide the following functions within the stated desired parameters: a. Remotely monitor and control BMS in a cyber-secure manner (e.g. hardened, able to prevent hacking of the remote connection) b. Remotely extract and use data from BMS for analysis and troubleshooting in a cyber-secure manner while retaining or increasing system flexibility c. Describe potential vulnerabilities and/or attack vectors that may impact building systems (e.g. remote control of BMS, remote data extraction) d. Test the proposed solution with various attack methods to demonstrate its resilience to cyberattacks e. Practical (e.g. impractical to lay fiber cables from all buildings to achieve “remote” data extraction), with reasonable cost and implementation effort f. Flexible (e.g. allows for changes in cloud suppliers and/or other service providers, changes to BMS without security impact and incurring costs)

D. Smart Detection

CS10: Advanced Malware Forensic using AI

Challenge	Build an advanced malware detection solution that can detect, dissect and analyse malware (including new versions and fileless varieties)
Background	Cyber threats are continuously evolving and increasing in both frequency and sophistication. Today's advanced malware may have the capability to alter their signatures to avoid detection. Fileless malware do not use executable payloads but instead make use of built-in tools in the operating system to carry out attacks. Since fileless malware are executed in-memory, traditional methods of malware detection (e.g. signature-based static analysis) are no longer effective on their own. Dynamic malware analysis (e.g. behaviour analysis) and detection is rapidly gaining traction. Artificial Intelligence (AI) or Machine Learning (ML) techniques are increasingly used to perform malware behaviour analysis due to their scalability and ability to handle large datasets and create a baseline to detect cyberattacks. A combination (hybrid) of static and dynamic analysis is generally accepted to be more efficient and accurate in detecting cyber-attacks.
Requirements	We are looking for an advanced malware detection system that can detect and analyse malware with the following capabilities: a. Dissect files or binaries to identify code similarities and classification of malware automatically b. Detect in-memory fileless malware by analysing memory / process dumps or any other combination of methods c. Automate extraction of Indicators of Compromise (IOCs) d. Correlate the findings with past incidents or logs e. Detect malicious files and classify them to the relevant malware families f. Link to threat actors/groups based on detected Tactics, Techniques and Procedures (TTPs) g. Use AI or machine learning to study the behaviour of malware h. Reduce false positives
Limitations	User is not able to provide sample data (e.g. malware samples) Solution must be installed on user's premises for testing

CS11: Routing Monitoring Suite

Challenge	Design and develop a monitoring software suite that will apply Artificial Intelligent(AI) /Machine Learning (ML) to detect and analyse any anomalies in the routing of data traffic
Background	Routing protocols are used determine how packets can be sent from one Autonomous System (AS) to another to reach their final destination, which may traverse across AS owned by different organisations. Organisations publish information about their connectivity to various networks and routers exchange this routing information to map the most efficient path. One of the major concerns related to the exchange of routing information is the lack of robust security mechanisms, with the exchanges being largely based on trust between network administrators. However, there are varying levels of trust among networks and there are no efficient methods to detect and prevent routing paths towards untrusted networks.
Requirements	We are seeking innovative solutions for a route monitoring suite that can: a. Build a dynamic process model to predict routing values b. Detect and analyse anomalies in routing based on Artificial Intelligent(AI) /Machine Learning (ML) c. Identify cause(s) of variation between predicted results versus actual routing paths d. Correlate anomalies from routing and networks to detect malicious activities e. Inspect integrity of data registries f. Provide alerts in case of anomaly detection g. Be scalable to support commonly deployed routing protocols for large networks
Limitations	Proposed solution should not consume significant network bandwidth, impact operational systems or alter routing

CS12: Detection and Handling of Malicious Code

Challenge	Scan and review software and applications (developed in-house and commercial products) to identify malicious code and vulnerabilities, as well as provide recommendations on remediation actions
Background	There are numerous network and business applications which are custom-built or coded by in-house or third-party developers. However, some codes may not be well-written and may contain security vulnerabilities. Every organization also adopts various commercial software for day to day operations (e.g. Windows, Microsoft Office, ERP Systems). While most software vendors publish regular patches and updates, there may still be vulnerabilities within these applications that pose potential security risks to the internal network. All applications and software, regardless of their source, may include malicious functions (e.g. backdoors for future unauthorized access in the event of an unhappy/disgruntled developer). Such codes may be well-hidden and may not be picked up by ad-hoc and/or basic code review process.
Requirements	The proposed solution should address these key requirements: a. Internal Code Review – automated and thorough source code review to identify potential malicious code, vulnerabilities or compare against industry best practices b. Scan Commercial Software and test binary applications and detect malicious code/functions c. Perform black-box testing of software/applications/code for OT systems d. Able to scan and review existing software/applications/code that has already been deployed as well as in development e. Handle a wide variety of programming languages f. Ability to evolve over time to include new programming languages that may potentially be use in within the organization g. Efficient execution of scan (i.e. able to be completed in a short time) h. Little or no impact on day to day functionality of software and applications being tested i. Use machine learning (ML)/artificial intelligence (AI) to improve code review process j. Provide recommendations on remediation actions

CS13: Early Warning of Cyber Threats

Challenge	Build a system which is able to detect new or imminent cyber threats from public conversations on blogs, Twitter and Dark Web forums
Background	Threat Actors may discuss vulnerabilities, exploits and upcoming cyberattack campaigns on Dark Web social media (e.g. forums, marketplaces). On the other hand, cybersecurity personnel (e.g. security vendors, White Hat hackers, researchers) may discuss vulnerabilities and potential defensive measures on Internet social media (e.g. Twitter, blogs). For example, exploits may first be discussed on Dark Web forums followed by Twitter before they are publicly disclosed. Relevant Dark Web and World Wide Web social media sites/accounts can be monitored and the collected data processed and analysed to detect new and/or imminent cyber threats. The timely detection of such threats can serve as a form of early warning to cybersecurity professionals, enabling them to come up with and deploy appropriate countermeasures to defend against impending attacks and mitigate their impact.
Requirements	The envisioned system should be able to: a. Acquire data from Dark Web and World Wide Web social media (e.g. forums, marketplaces, Twitter, blogs) based on applicant-proposed sources (subject to user's agreement) b. Store acquired (raw) and processed data in a flexible format to facilitate analysis and visualization c. Process acquired data to enable further analysis d. Propose and implement a method to detect new and/or imminent cyber threats (e.g. vulnerabilities, malware names, threat actors, data breaches) e. Correlate data from different sources to verify authenticity and reduce false positives f. Use Artificial Intelligence (AI) / Machine Learning (ML) techniques to reduce false positives of detected threats g. Correlate findings from different data sources to discover linkages (if any) h. Design an interactive dashboard to display analysis results (e.g. trends) i. Provide alerts in case of such detections (e.g. via email) j. Include other data sources (e.g. Telegram)
Limitations	Only publicly available data may be collected, but user is willing to work with successful applicant to tag training data (where applicable)

CS14: Validate AI Robustness against Adversarial Attacks

Challenge	Develop a tool and propose technical guidelines to validate the robustness of Artificial Intelligence (AI) and Machine Learning (ML) models and systems against adversarial attacks
Background	Artificial Intelligence (AI) and Machine Learning (ML) are rapidly becoming mainstays in cyber defence systems due to their ability to help security teams identify threats accurately and in a timely fashion. However, researchers have demonstrated that it is technically feasible to conduct adversarial attacks on AI systems through data poisoning and evasion techniques. For example, Domain Generated Algorithms (DGA) require AI/ML detection (instead of signature-based) due to the rapid rotation of DGA seeds and algorithm complexity. An attacker can introduce perturbations to skew the training dataset and change detection parameters, eventually generating DGAs that can bypass the AI/ML system. Effective validation of such AI/ML models for cyber threat detection is essential to identify model weaknesses prior to deployment as well as validate attack resistance and system robustness against AI adversarial attacks.
Requirements	We are seeking a solution with the following capabilities in the cybersecurity context: a. Perform black-box testing for robustness (i.e. attack resistance) of AI models without the need to access the AI models' source code b. Propose parameters to quantify the robustness of tested AI models c. Analyse the robustness of tested AI models based on proposed parameters d. Report on tested models' accuracy (e.g. precision, recall) e. Identify and report on tested models' weaknesses (e.g. deviations from expected output based on known input, point of deviation) f. Generate the training/testing datasets (automatically and/or on-demand) that can mislead the AI models to allow practitioners to examine and rectify the AI models g. Propose a list of technical guidelines that can be applied to AI solution providers (e.g. provision of models in a standard format with APIs to allow for black-box testing) h. Develop demo scenarios to test the AI models used for detection against at least three (3) different techniques documented in MITRE ATT&CK i. Provide analysis of tested AI models to explain the models' behaviour
Limitations	Applicant companies shall provide own AI models and datasets

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. Protection against Ransomware
2. Protection against Phishing
3. Secure Messaging/VOIP application
4. 5G Security
5. Protection of homes from cyber threats
6. Protection of SMEs from cyber threats
7. Protection of medical devices from cyber threats