DEFENCE INNOVATION ORGANISATION

(Under Aegis of Department of Defence Production)

Ministry of Defence, Government of India

New Delhi -110002

Summary of Defence India Startup Challenge-9 Cyber Security (Disc 9)

Problem Statements

Overall No. of challenges proposed: 28 (Twenty-Eight)

S.No	Name of Agency	Number of Problem Statements
1	Indian Army	3
2	Indian Navy	3
3	Indian Air Force	7
4	MIDHANI	2
5	GRSE	1
6	BEML	1
7	MDL	1
8	BEL	3
9	MHA - I4C	7

CHALLENGES

Problem Statement – 1 (ARMY)

Organization Name	**Army Cyber group/DGMO (MO-12)**
Problem Statement/ Challenge title	Drone Forensics
Challenge domain	Forensics
Challenge brief/definition	In today's scenario, the variety of COTS (Commercial Off The Shelf) drones including locally manufactured drones is vast and its support to carry out forensics investigation is very limited.
Key Specifications	Industrial & Commercial grade Drones
Future Expectation from the prototype / Technology developed	It should be able to provide support at raw data level of a drone, like the flight data extraction from physical storage, cloud data access if available.

Problem Statement – 2 (ARMY)

Organization Name	**Dte. Gen of Mil Ops (Army Cyber Gp.)**
Problem Statement/ Challenge title	Website Defacement Detection & Mobile App scanner.
Challenge domain	Cyber Threat Intelligence
Challenge brief/definition	Requirement of an integrated platform to carry out vulnerability assessment and defacement detection of organization's internet facing websites and to carry out scanning of organization related mobile apps hosted in open domain to detect any vulnerabilities or malicious content.
Key Specifications	Design and implement a GUI based integrated platform for 'Vulnerability Assessment' and 'Defacement Detection' of websites/domains/subdomains and scanning android mobile apps. The platform must scan the website for the under mentioned issues and generated a report of the identified vulnerabilities and also suggest required mitigation. Moreover, the platform should be able to scan an android mobile app to detect any vulnerability or malicious content. (a) Website Defacement Detection. 1. Monitors website integrity

	2. Detect any attack. (b) App misconfiguration (c) SSL Scan. (d) Port Scan.
Future Expectation from the prototype / Technology developed	A user friendly, GUI based website and mobile app, vulnerability assessment platform for risk detection.

Problem Statement – 3 (ARMY)

Organization Name	**Dte Gen of Mil Ops (Army Cyber Gp.)**
Problem Statement/ Challenge title	Design and Implementation of a GUI-based Social Media Monitoring Platform for Intelligence and Operations purpose
Challenge domain	Cyber Threat Intelligence
Challenge brief/definition	Requirement of indigenous, social media monitoring tool.
Key Specifications	Design and implement a GUI based 'Social Media Monitoring Platform' for periodic/user defined crawling of various social media platforms like Twitter, Facebook, Instagram, Discord, etc. based on user input queries/watch words and present the results in a tabulated form. The platform should have the capability to analyze the crawled data and classify the data as per user defined attributes
Future Expectation from the prototype / Technology developed	A user friendly, GUI based portal for user social media monitoring.

Problem Statement – 4 (NAVY)

Organization Name	**NAVY**
Problem Statement/ Challenge title	Development of an indigenous Security Information and Event Management (SIEM) solution based on open-source framework
Challenge domain	**NIL**

Challenge brief/definition	Non- availability of an indigenous SIEM solution developed based on open-source framework for monitoring the endpoints which are not connected to Naval Unified Domain (NUD) Development of an indigenous SIEM solution based on open-source framework primarily compatible with Windows and NasvIOS endpoints. The solution, in addition to the core feature facilitating endpoint monitoring, should comprise multiple modules such as a built-in Network Monitoring System, Threat intelligence, Forensic Analysis, Behavioural Analysis etc.
Future Expectation from the prototype / Technology developed	**NIL**

Problem Statement – 5 (NAVY)

Organization Name	**NAVY (DNI)**
Problem Statement/ Challenge title	Development of an advanced open-source framework sanitisation tool facilitating secure transfer of data between multiple air-gapped networks.
Challenge domain	
Challenge brief/definition	➢ Non-availability of a proper advance sanitisation tool for sanitising data transferred between multiple air-gapped networks. ➢ Development of an advanced open-source framework sanitisation tool facilitating secure transfer of data between multiple air-gapped networks.
Future Expectation from the prototype / Technology developed	NIL

Problem Statement – 6 (NAVY)

Organization Name	**NAVY**
Problem Statement/ Challenge title	Autonomous AI based threat detection and threat elimination engine to block ransomware and zero-day attacks
Challenge domain	**NIL**
Challenge brief/definition	Ransomware attacks poses great threat to Cloud services and are capable of locking the service with or without damage of system files. Further, zero-day attacks can exploit the vulnerability in the cloud service till the vulnerability is detected by developer and fixed. The solution must provide an AI-powered alert management system that can automatically detect problem ransomware & zero-day attacks and help reduce the workload of security analyst. The solution must have analytics section to measure its performance by evaluating false positives.
Future Expectation from the prototype / Technology developed	NIL

NAVY FAQs

1. Are cyber security threats increasing?

Ans. Yes, threats are imminent and increasing exponentially in sophistication, intensity, diversity and volume. Cyber experts report significant escalation in external cyber-attacks, especially from criminal organizations and foreign state sponsored activities.

2. What are the top five barriers in addressing cyber security?

Ans. Even as CISOs better define their roles and become an integral part of state government, they continue to face challenges, particularly in securing the resources they need to combat ever-evolving cybersecurity threats. The following are the major barriers considered post survey:-

a. Lack of adequate funds.

b. Inadequate availablity of cyber security professionals.

c. Lack of documentation process.

d. Increasing sophistication of threats.

e. Lack of visibility and influence within the enterprise

3. Any guiding principles for implementation of cyber security for Naval

requirement?

Ans. Cyber security design should follow these principles:-

a. Establish the context before designing a system.

b. Make compromise difficult.

c. Make disruption difficult.

d Make compromise detection easier.

e. Reduce the impact of compromise.

4. What tool are to be used?

Ans. Any tools can be used but are to focus on network security monitoring, encryption, web vulnerability, penetration testing, antivirus software, network intrusion detection, and packet sniffers.

5. What are the most common types of cyber risk expected?

Ans. Cyber Security Breaches, a quantitative-qualitative survey revealed 66% of businesses / organization has faced breaches or attacks.

The most common types are:

a. Phishing attacks

b. Viruses, spyware or malware, including ransomware attacks

Problem Statement – 7 (AIRFORCE)

Organization Name	**INDIAN AIRFORCE**
Problem Statement/ Challenge title	Development of a multi-engine AV (anti-virus) solution
Challenge domain	NIL
Challenge brief/definition	1. Development of a multi-engine AV solution that is capable of handling and identifying present day complex malware. Presently, there is no standardized, indigenous AV solution with long term support for use by Defence institutions. Proposal is to develop a multi-engine AV solution that is capable of handling and identifying present day complex malwares. 2. The envisaged solution should be for enterprise level deployment with central control and management of end point devices. 3. The solution should provide round the clock support and regular updates keeping it up-to date, to reduce the window of vulnerability.

Future Expectation from the prototype / Technology developed	1. Minimum Order Quantity (MOQ) Once the prototype for a multi-engine solution is acceptable along with the plan of action for continuous support at least for 10 years, a MOQ for one enterprise solution would be considered.
FAQs	**1. How many antivirus solutions need to be integrated?** Ans. At least four AV solution need to be integrated for threat feeds. **2. Can commercial AV solutions be integrated?** Ans.No, all AV solutions need to be indigenised. As on date we are dependent on the industry predominantly from the West. There is a need to be Atmanirbhar in this area. **3. What kind of support is expected?** Ans. All the AV solutions need to be in active development with constant updates for IOCs and threat feeds. This support is required for at least ten years. **4. What are the desired features of the AV solution?** Ans. Salient aspects of desired features are as follows: - (i) Multi-AV engines are to be integrated (ii) The solution need to be a next generation AV solution with both behaviour and signature analysis. (iii) Differential scanning of hard disks (iv) Scanning to be done at endpoints by all AV engines **5. What would be the order quantity for the IAF?** Ans. One enterprise solution is the present need. The solution would be acceptable after necessary tests and POC are successful.

Problem Statement – 8 (AIRFORCE)

Organization Name	**INDIAN AIRFORCE**
Problem Statement/ Challenge title	Creation of a browser plug-in for Chrome and Firefox, which is able to detect phishing mails and take appropriate action.
Challenge domain	
Challenge brief/definition	Currently the Defence network is air gapped, however there is an internet presence in all three services where nic emails are used to exchange information as well as other email services are being used by

	personals for various personal and official requirement. This poses a big risk of phishing attacks which is not being mitigated by standard security tools (Antivirus / firewalls) as the user has clicked undesired link and allowed the phishing malware to be downloaded. It is proposed to create a browser plug-in for chrome and Firefox, which is able to detect phishing mails and take appropriate action
Future Expectation from the prototype / Technology developed	The solution should provide live detection of any malicious code being received on mail and alert / block it, even before the user has clicked on mail. Minimum Order Quantity (MOQ) This tool can be procured for deployment on many Internet PCs of IAF.
FAQs	**1. Would this solution be e-mail vendor specific?** Ans. No, the solution would not be email vendor specific. It should be able to detect phishing mails based on the context, header, body and links of the email. **2. How will it be deployed on the endpoint?** Ans. It has to be in the form of a browser plugin for chrome and firefox. **3. How would the detection of the phishing mail work?** Ans. The plugin should flag any email automatically but in cases where the email vendor is not compatible with the plugin then there should be a functionality to forward the email to a central email id and for the user to receive back the results. **4. What would be the order quantity for IAF?** Ans. One enterprise solution is the present need. The solution would be acceptable after necessary tests and POC are successful. **5. Can commercial Threat feeds be integrated?** Ans. Yes, seamless integration of top industry standard threat feeds is expected.

Problem Statement – 9 (AIRFORCE)

Organization Name	**INDIAN AIRFORCE**
Problem statement/ Challenge title	Intelligent (AI Based) Document Management System

Challenge Brief/ Definition (Please give details of the Innovation to be done by the Start-Up and expected deliverable at the end of the project)	An integrated solution is required to manage access control, real time classification of data by content (preferably AI driven) encryption in data at client, transit and storage. The solution should also track the files sing Digital rights management policies. Total users of 3,00,000. Project execution to be completed in 12 months. Software solution with all the features mentioned above with an active support for 3 years
Future Expectation from the prototype/ Technology developed	The solution will be used to replace the existing COTS document management systems for the benefit of IAF users.

Problem Statement – 10 (AIRFORCE)

Organization Name	**INDIAN AIRFORCE**
Problem statement/ Challenge title	Mitigating Risks of Unauthorized USB Devices: A custom PC Solution
Challenge Brief/ Definition (Please give details of the Innovation to be done by the Start-Up and expected deliverable at the end of the project)	1. Due to carelessness and lack of adherence to SOPs, many violations are occurring wherein unauthorised USB devices have been erroneously plugged-in to AFNET/ Civil internet PCs, thereby increasing the potential to infect the network, leak confidential information and subsequent administrative actions. 2. Already various software’s have been introduced in the network for protection, however physical measures are also equally essential. 3. Hence in order to mitigate this risk, it is recommended that we should develop a customised PC for IAF. All the USB ports in the PCs (AFNET & Internet) as well as USB devices (i-key, e-token, hard disks and accessories) should be converted to USB B/ C type adapters.
Future Expectation from the prototype/ Technology developed	Development of such customised PCs for IAF will definitely help in reducing the operational risks and occurrences of erroneous/ malafide USB insertion.
FAQs	**1. What is the envisaged scope of customization in the PC?** Ans. A customized cabinet is to be made for all existing AFNET/ Internet PCs in the IAF. This cabinet will replace the existing cabinet of the desktop PCs. All female connector ports in

	the new cabinet for the accessories are to be converted to Type Micro B (excluding HDMI/ DVI/ DP ports and one port of the service issued i-key/ e-token/ ex-HDD). One female connector port earmarked for service issued external devices (i-key/ e-token/ ex-HDD) to be converted to Type A/ C (A for AFNET devices and C for internet PCs). Each cabinet should also have an external lock with customized key. **2. Any other additional requirement for the accessories/ service issued devices?** Ans. Removable male connector Micro B ports are to be provided for accessories and Type A/ C ports are also to be provided for the service issued external devices for AFNET/ Internet devices respectively. These connectors will be permanently fixed to all the existing accessories and service issued external devices.

Problem Statement – 11 (AIRFORCE)

Organization Name	**INDIAN AIRFORCE**
Problem statement/ Challenge title	Indigenous software to avoid unauthorised access of data from smart devices
Challenge Brief/ Definition (Please give details of the Innovation to be done by the Start-Up and expected deliverable at the end of the project)	A software may be developed which when installed in any smart device can detect and avoid any type of unauthorised access for any data from that device
Future Expectation from the prototype/ Technology developed	Security of data on smart devices of all service personnel.
Minimum Order Quantity (MOQ)	For all service personnel.
FAQs	**1. Can this software stop all unauthorised access of data in smart devices?** Ans. Yes.

	2. Can this software detect and block phone calls from a specific country code? Ans. Many people who are unaware pick-up fraud phones calls from adversary leading to either sharing of data or location. If phone calls from a specific country code will be blocked this problem will be solved **3. Can this software detect a particular IP address?** Ans. Different versions of the software should be made to install in smart phone and PCs. Any file containing malware which can have access to data will be detected. **4. Will this software have access to private content of a person in smart devices?** Ans. No, the user will have the access to grant permission for private content. **5. Can this software be installed in all smart devices of service personnel?** Ans. Yes, this will be made available to all station IT sections and in turn installed in all devices. This would scan for any threat which is sharing information to adversary. **6. Do we have a database of such blocked phone numbers and IP address which have been found to steal data from service personnel?** Ans.Yes, A database need to be made and updated periodically. This would be made available to all users as a software update so as to scan for any new cyber threat. **7. What is end state with such system in place?** Ans. This would ensure Security of data on smart devices of all service personnel.

Problem Statement – 12 (AIRFORCE)

Organization Name	**INDIAN AIRFORCE**
Problem statement/ Challenge title	Development of a Smartphone Security solution/ Application

Challenge Brief/ Definition (Please give details of the Innovation to be done by the Start-Up and expected deliverable at the end of the project)	Development of a Smartphone Security solution/ Application which when installed on smart phone will facilitate utilisation of smart mobile phones in IAF Establishments without infringing upon security aspects of IAF In advanced countries like Israel, smart mobile phones are not prohibited from usage inside most of the sensitive locations, including their defence locations. To ensure similar environment in IAF, it is suggested that an application be designed / developed which should be mandatorily installed on individual's smart phone (whosoever wishes to carry them inside IAF establishments), and it should cater to all security needs of the organization.
Future Expectation from the prototype/ Technology developed	Besides obviating expenditure on AFCELs (savings to exchequer) it will also result in optimum utilisation of smart mobile phones in a controlled environment with real time monitoring. This will also enable the organization to effectively track all the activities of individuals who have installed ibid application thereby ensuring better security environment. Monitoring will also be effective and thus, before an avoidable event occurs, it can be obviated.
Minimum Order Quantity (MOQ)	Smartphone Security Application (Software) with adequate no. of licences
FAQs	**1. What all functions/ hardware should be disabled?** Ans. Camera, Location (GPS) & Bluetooth. **2. What all apps should be disabled?** Ans. Facebook, Whatsapp and similar ones; particularly of Chinese origin like Truecaller. **3. What is the origin of the idea?** Ans. Practice that is in vogue at Rafael and IAI. **4. The proposed IAF software should work on what all OSs?** Ans. Only Android. **5. Any other Suggestions/ ideas?** Ans. Following suggestions may be incorporated:- (i) SIM to be purchased through IAF, so that necessary sanitization / data capture, can be achieved (can get into a contract with operators like BSNL). (ii) The IAF app should activate & deactivate certain features / apps at the entrance of the IAF premises only. (iii) RAT can be remotely and automatically run, once, the mobile is inside the IAF's premises. (iv) Mobile to be tweaked for having hardware encryption. (v) Have CUG network on the rreferred service provider, calls

	within CUG network will be encrypted and outside CU Gamy be open (R&S Germany had something similar in year 2005) (vi) Have a system in place to monitor incoming and outgoing media data with help of service provider.

Problem Statement – 13 (AIRFORCE)

Organization Name	**INDIAN AIRFORCE**
Problem statement/ Challenge title	Innovative decision support system (DSS) for analysis of unstructured database
Challenge Brief/ Definition (Please give details of the Innovation to be done by the Start-Up and expected deliverable at the end of the project)	Current Scenario Dte of Int is flooded with various reports (hard & soft copies) in structured/unstructured formats (word, ppt, pdf, images, excel, Maps etc) and also from internet. The reports from different agencies have repeated information of an event. Processing such information in shortest time is humongous task and also tends to miss certain critical points of information. There is a need for innovative solution which can read & analyse the voluminous reports and aid as decision support system. A customized innovative software solution with structured and readable database, for IAF with associated hardware, which can reduce human effort in extracting the useful intelligence from the reports received at Air HQs and also from open source (internet). The system should run on network internal to organization with air gap/ isolation solutions to internet ensuring data security. The software should able to read and understand the defence terminology/ jargons/ acronyms etc and carry out change detection, temporal and predictive analysis. The end product should be user friendly Geo-Int solution. The analysis should be presented using geo visualization tools. The system should aid as operational decision support system

Future Expectation from the prototype/ Technology developed	The development of system to be within IAF premises. The software, database and hardware should have redundancies. The IP rights and source code to remain with IAF. The system should be able to process huge volumes of textual data. The system should use advanced text/data analysis tools and able to generate reports as per IAF service formats and the user defined formats
Minimum Order Quantity (MOQ)	The product will be a unique server- client based software enterprise system customized for IAF's requirement. Quantity required will be one with provisions for scalability and periodic up gradation of software and hardware.
FAQs	**1. Do the reports that need to be processed have a standard format?** Ans. The IAF receives inputs from several agencies each of which follow different formatting standards. In addition, several unstructured/ raw inputs are also received from time to time. The system should be able to analyse all such inputs and assimilate requisite information. **2. Will the data be provided by user for development and testing?** Ans. The vendors/ developers are expected to provide a Proof of Concept using open-source information. Thereafter, all development/ testing activities requiring access to information available with IAF would be exclusively carried out within IAF premises. **3. Can the end product be deployed remotely with user terminals at IAF premises?** Ans.The end product will need to be deployed mandatorily at IAF premises. Further, IAF would require to be given access to the source code.

Problem Statement – 14 (MIDHANI)

Organization Name	Mishra Dhatu Nigam Limited (DPSU)
Problem Statement/ Challenge title	Integration of GeM portal to ERP in compliance with cyber security norms.
Challenge domain	System integration, Data handling, phishing attacks, cyber security.
Challenge brief/definition	Being the Defence PSU, maintaining 100% air gap is mandatory as per the cyber security policy. ERP is in intranet and GeM is in Internet. Currently Communication between ERP and GeM is not established. There is a direction from MoD to integrate the GeM with ERP. There is a challenge in integrating GeM with ERP by maintaining 100% air gap and cyber security.
Future Expectation from the prototype / Technology developed	Solution to mentioned challenges are expected inline with MoD cyber security policy.

Problem Statement – 15 (MIDHANI)

Organization Name	Mishra Dhatu Nigam Limited (DPSU)
Problem Statement/ Challenge title	Secure USB solution
Challenge domain	System integration, Data handling, phishing attacks, cyber security.
Challenge brief/definition	As per certain business requirements sharing of data between the networks is inevitable. USB are being used for data transfer. Ensuring the secure data transfer is challenge using USB.
Future Expectation from the prototype / Technology developed	Solution to mentioned challenges are expected inline with MoD cyber security policy.

Problem Statement- 16 (GRSE)

Organization Name	Garden Reach Shipbuilders and Engineers Limited. (DPSU)
Problem Statement/ Challenge title	Implementing Industry 4.0 for shipyard without WiFi connectivity.
Challenge domain	Information Technology, Automation and Industry 4.0

Challenge brief/definition	GRSE being operated under the administrative control of Ministry of Defense, as per the cyber security policy of “Cyber Security Group, Department of Defense Production”, the **WiFi** connectivity is strictly prohibited with the organization for connecting its IT infrastructure and related devices and equipment. However, in order for embracing modern technologies, machineries and automation in the shipbuilding processes, Industry 4.0 solutions are inevitable. But, because of **WiFi** restriction most of the solution could not be effectively implemented & utilized to its fullest features. Innovative solutions may be derived to overcome mentioned challenges where Industry 4.0 & Automation solutions can effectively be implemented in on-premise model (without WiFi and Cloud adoption).
Future Expectation from the prototype / Technology developed	The solution should be able to solve the GRSE challenges w.r.t. implementing Industry 4.0 & Automation in the shipyard processes and ensures compliance to Ministry requirement of WiFi restriction.

Problem Statement – 17 (BEML)

Organization Name	**BEML LIMITED (DPSU)**
Problem Statement/ Challenge title	Automation of Security Orchestration, Automation, and Response (SOAR)
Challenge domain	Many Advisories come regularly from MoD for Cyber Security compliance for blocking of Malicious IPs which are being done manually and takes a lot of manhours.
Challenge brief/definition	Presently we are doing blocking of IPs in Firewall & User ends manually, which should happen automatically through security operations center (SOC).
Future Expectation from the prototype / Technology developed	NIL
FAQs	**1) What are Basic features of SOAR?** a) Automated Phishing Investigation and Remediation b) Threat Intelligence Lifecycle Automation c) Threat Hunting with SOAR d) Incident Response with SOAR **2) Is there a Manual Human Action in SOAR?**

	SOAR is a fully automated with No human intervention to perform repetitive and mental tasks. Incident response teams are now in constant defense mode as the number of security alerts being generated is hitting an all- time high. Humans, even when very skilled, do have limitations on how fast they can react and access, collect, analyze and correlate the information to gather proper threat intelligence. 3) **Is there a False alarm?** Too many alerts may raise innumerable false positives that is generating noise. To combine and correlate SOAR Solution alerts to reduce further false positives and address real threats. 4) **Will it Mitigate alerts on own & intimate SOC Team?** It should mitigate most of the threats on its own & generate areport of the real threats & the action taken. 5) **Will SOAR meet Compliance requirements?** SOAR products meet MoD & CERT compliance, SOAR products and solutions follow industry best practices and standards, suchas ISO, NIST, CERT, SOA, COBIT, OWASP, MITRE, OASIS, PCI, HIPAA. 6) **Will it help in investigation process?** It should even deal with the investigation process & find the root cause of the attack all by itself.

Problem Statement – 18 (MDL)

Organization Name	**Mazagon Dock Shipbuilders Ltd (DPSU)**
Problem Statement/ Challenge title	Linux desktop in Windows Environment
Challenge domain	Cyber Security

Challenge brief/definition	As a security measure “Linux desktop on internet facing machines” is recommended by Cyber security agencies in the Defence environment. MDL has implemented security controls which are based on the Windows environment. Challenges are to implement Security controls like Active Directory (AD) Authentication, Antivirus (AV) implementation, Network Access Control) NAC client installation, Group Policy implementation, eToken or Class IIIB certificate for using the dongle based authenticate software, Pen Drive white listing, printer installation, encryption on a Linux Desktop in a windows environment.
Future Expectation from the prototype / Technology developed	Expectation from the prototype is to develop Hardware/Software mechanism wherein, the Linux desktops also can be centrally controlled like any other windows desktop in Windows environment.
FAQs	**1. Does Linux machine are envisaged over Windows OS?** No, Linux Machines in a LAN where all other machines and security control are Windows based. **2. Which flavor of Linux is envisaged?** Any flavor, preferably Ubuntu, Suse, Redhat, BOSS etc. **3. What is NAC?** It is Network Access Control used for MacID and user authentication with the Windows AD (Active Directory) to Allow and disallow the machine and user in LAN. **4. What is eToken or Class IIIB Certificate?** This refers to Dongle based 2 factor authentication with application like eProcurement application etc. **5. Pen Drive white listing – What is expected?** In a LAN, pen drive white listing should be able to achieve centrally controlling pen drive and its access to specific machine. **6. What do you mean by Group Policy implementation?** In windows environment, Windows AD controls security or any other policies by applying Group Policy centrally.

Problem Statement -19 (BEL)

Organization Name	**Bharat Electronics Ltd**
Problem Statement/ Challenge title	Attack surface monitoring tool for continuous discovery, analysis, remediation and monitoring of cyber security vulnerabilities and potential attack vectors for inventory.
Challenge domain	**Cyber security**
Challenge brief/definition	Attack surface monitoring tool for continuous discovery, analysis, remediation and monitoring of cyber security vulnerabilities and potential attack vectors for inventory. Tool shall protect the inventory of Critical systems by discovering vulnerabilities periodically and provide remediation.
Future Expectation from the prototype / Technology developed	1. Fully automated solution 2. Integrity and configuration checker 3. Patch management 4. On premises and cloud based 5. Standard APIs to integrate solution

Problem Statement -20 (BEL)

Organization Name	**Bharat Electronics Limited**
Problem Statement/ Challenge title	Intelligent system for identification of phishing emails, fake websites and sand-boxing targeted entity
Challenge domain	**Cyber Security**
Challenge brief/definition	Problem of protection against phishing attacks, in which attackers send fake emails / create fake websites that mimic legitimate ones in an attempt to trick users to reveal sensitive information are critical. Though it is important to educate users about how to identify and avoid phishing attacks and strong technical measures required to reduce / eliminate risk of successful phishing attacks. Solution with intelligent mechanisms required to automatically detect and identify phishing emails, fake web sites. Even if user is tricked to click email links or attachments fake websites, solution to provide mechanisms to isolate and sandbox process / executable / file system to contain damage / impact.
Future Expectation from the prototype/ Technology developed	1. Fully automated solution 2. On premises and cloud based 3. Standard APIs to integrate solution

Problem Statement -21 (BEL)

Organization Name	**Bharat Electronics Limited**
Problem Statement/ Challenge title	Enhancing Security for Any POS, Banking and ATM based transaction
Challenge domain	**Cyber Security – Banking**
Challenge brief/definition	Transactions using ATM card / Debit Card / Credit card and PIN / OTP based verification being compromised through attacks. Solution to enhance security is required, during transactions employing ATM card / Debit Card / Credit card, by drastically reducing the related frauds during usage at POS or other touch points.
Future Expectation from the prototype / Technology developed	Solution shall provision for future customization and to be supplied along with other security products, shall be subjected to evaluation and certification, by external agencies for BFSI sector
FAQs	1. **Whether the solution will be centralized for all POSand ATMs of all banks in India?** No. Each bank has its own data center and security features in place. So the solution will have to be deployedfor particular bank. 2. **How GPS coordinates are associated to banking transactions?** If the location of transaction is linked to location of user/subscriber, many varieties of cyber attacks can be prevented. 3. **Will this call for Credit/debit cards with GPS chip andchange of existing cards?** Not necessarily, alternate solution for assessing subscriber location to be considered for solution architecture. 4. **Does it call for any standards to be met?** Yes. Relevant PCI-DSS standards should be met. 5. **Support for what kind of POS is expected?** It shall support all variants of POS like GPRS, PSTN, WiFi and Mobile POS.

Problem Statement – 22 (MHA-I4C)

Organization Name	**MHA - I4C**
Problem Statement/ Challenge title	Voice Recognition Software to mitigate cyber frauds
Challenge brief/definition	Current Scenario: Many of the cyber frauds happen over voice communication. Fraudsters communicate with potential victims either through GSM or VoIP calls. On several occasions the victim is able to record the voice of the fraudsters. The voice sample has certain noise and distortions in it. However, this is the only identifier with which the crime or attempted crime can be connected to the criminal. The goal of this project is to design and develop a Voice Recognition System (VRS) that can assist Law Enforcement Agencies (LEAs) in identifying and tracking individuals who have committed or attempted to commit cyber fraud through voice communication. The VRS will be used to analyze voice samples that have been recorded by victims of cyber fraud, which may contain background noise and distortions. The VRS will be able to store voice samples of different individuals of interest that can be uploaded by LEAs and match them with test samples in order to identify suspects. The system should have the following features: i. The ability to store voice samples of different individuals of interest, along with additional information that can be imported through an API from another system. ii. The ability to group voice samples based on their similarity. iii. The ability to match individual test samples with the samples available in the database, and display near matches in decreasing order of similarity. iv. The ability to eliminate background noise and other distortions from the voice samples. v. A high level of voice fingerprinting and matching accuracy to ensure reliable results. This system will help in identifying the criminals and can be used as a evidence in the court of law.
FAQs	**1. Which formats should the VRS system support?**

	Software should support all the prominent audio codecs / formats like .mp3, .aac, .wav etc. 2. **Should the application interface be a desktop based or web based?** Application software could be either desktop based or web based.

Problem Statement – 23 (MHA-I4C)

Organization Name	**MHA - I4C**
Problem Statement/ Challenge title	A tool to analyse Bank Statements to assist in cybercrime detection
Challenge brief/definition	The goal of this project is to design and develop a tool that can analyze bank statements of individuals and organizations who may be involved in cybercrime and other forms of fraud. The tool will be used to assist law enforcement agencies and other organizations in their efforts to prevent and detect these crimes. The tool will need to be able to handle bank statements in various formats and columns provided by different banks and be able to convert them into a common, structured format. This will enable the tool to analyze transactions and generate intelligence using traditional analytical methods. The tool should also be able to decipher narrations and provide capabilities for link analysis, timeline analysis, and other standard reports and queries. Additionally, the tool should be available on a cloud-based platform to support multiple concurrent logins and be accessible to multiple agencies and organizations. The tool should be able to handle large amount of data and should be able to scale with the growing need of the user.
FAQs	1. **Is it desired to host software On-premise or on cloud?** An On-premise version as well as cloud version of software is needed for Bank Statement Analysis

	2. **Which Bank formats should be accepted by the Software?** Bank formats not limited to PDF, CSV and Excel would be required as an input. Tool should also be able to identify scanned account statements. 3. **Is there a restriction on software technology being used?** No, Software can be made in any technology; considering in mind the speed of execution of large volume data / account statement.

Problem Statement – 24 (MHA-I4C)

Organization Name	**MHA - I4C**
Problem Statement/ Challenge title	Cryptocurrency Intelligence & Analysis Tool
Challenge brief/definition	Crypto currency like Tether, Bitcoin, Ether etc. is used to perform illegal activities over Dark Web. There is no indigenous crypto analysis tool and auto-updating database of crypto addresses that are used for conducting illegal activities in dark web A comprehensive tool is sought to effectively monitor the usage of cryptocurrencies on darknet websites. The tool should have the ability to crawl these websites on a regular basis and gather information about the public key addresses being used for payments. The collected information should then be organized into records that consist of the website name, date and time of the transaction, type of service offered on the darknet, type of cryptocurrency used as a mode of payment, and the public key address. In addition, the tool should maintain a database of all known cryptocurrency exchanges globally, organized by continent. Tool should also have collection of email addresses of prominent exchange / wallets for sending legal notices. The

	database should also keep track of all known tainted coins to assist investigators in their work. The Crypto tool should have facility to identity the blockchain / type of crypto currency or exchange using addresses provided. The tool should also provide alerts for new transactions on various cryptocurrencies including, but not limited to, Ether, Tether, Monero, Dash, and Tron. This feature should be similar to the one offered by websites such as bitcoinwhoswho.com, which provides alerts for new transactions on the Bitcoin network.
FAQs	1. **What should be the frequency of crawling on Dark web / Surface web to identify suspected crypto addresses?** Crawling must be done on continuous basis to identify surfacing of any new crypto addresses by the tool. 2. **Is there a limitation of number of cryptocurrencies to monitor.** Preliminary requirement is to monitor commonly used crypto currency like Bitcoin, Ethereum, Tether etc. However, if the tool provides support for more number of crypto currencies; it would increase efficiency.

Problem Statement – 25 (MHA-I4C)

Organization Name	**MHA - I4C**
Problem Statement/	Framework platform for identification of phishing domains/URLs
Challenge title	The goal of this project is to design and develop a framework platform for the identification of phishing domains and URLs. Phishing is a major cybercrime that uses social engineering and technical deception to obtain sensitive information such as financial data, emails, and other personal information from users. Cybercriminals create and host phishing websites and domains that appear similar to popular and trusted websites belonging to government and private organizations. The system should have a whitelist of trusted domains commonly used by the public and continuously crawl the web and open-source platforms to find near matches for these whitelisted domains and flag them. The system should also generate reports with relevant information such as WHOIS records, Internet Protocol (IP) address, SSL certificate attribution, domain hosting details, source code, similar websites, and other domains hosted on the same domain. The system should be able to handle large amount of data and should be able to scale with the growing need of the user. Additionally, the system should be able to categorize the domains as malicious and non-malicious for further analysis. The system should also be able to automatically notify the relevant authorities and organizations about the malicious domains.

FAQs	1. **Is there a specific requirement regarding feeds / engine to identify the phishing URLs.** Threat feeds from various sources may be aggregated and indigenous phishing domain identification may also be developed. This engine should identify phishing domains from Indian context. 2. **What are the data formats that need to be analysed by the framework / tool?** Phishing campaigns not limited through emails, SMS, android apps, URL Shorteners, Hyperlinks should be analysed.

Problem Statement – 26 (MHA-I4C)

Organization Name	**MHA - I4C**
Problem Statement/ **Challenge title**	**Portable Mobile Forensic Suite and a cloud version**
Challenge domain	NIL
Challenge brief/definition	Current Scenario Mobile phones are in used most of modern-day crimes. Presently there is a high dependency on international mobile forensic tools with very high license cost. Portal mobile forensic tools are required at every cyber cell for investigation - forensics. Full-fledged mobile forensic suite with features at par with International Mobile forensic suite.

	Features: - Support for iPhone and Android Device. - Support all latest mobile processors. - A cloud-based solution along with standalone setup is required to help and reach the remotest law enforcement officer. - Feature to unlock the smart phones with and without password. - Physical and logical data extraction facility. - Capability to analyse damaged phones.
FAQs	**1. Is it required to have a battery backup for the portal tool?** Yes; battery backup would be required for the portal mobile forensic tool. **2. Any specific requirement related to the physical / logical image?** The extracted forensic image quality must match the international standards. **3. Is it required for portable suite to support multiple devices.** Support of multi device parallel imaging would be desired for faster forensic imaging.

Problem Statement – 27 (MHA-I4C)

Organization Name	**MHA - I4C**
Problem Statement/ **Challenge title**	Plug and Play Agent based Cyber Security and compromise assessment Audit Tool
Challenge domain	MHA has released National Information Security Policy and Guidelines (NISPG) for Ministries that includes various aspect of Information & Cyber Security.

	There are a Large number of Government IT assets which includes Laptop, Desktop & Servers. Owing to absence of periodic audits and manpower, there are major lapses in cyber security. Configuration level vulnerably may increase the chance of Cyber Attacks. Also there is an absence of centralized dashboard for Senior Officials to assess the state of organization.
Challenge brief/definition	Audit results should be displayed against NISPG, MeitY guidelines on cybersecurity on various domains like Patch management, Antivirus Management, Hardening, Internet Security Configuration, Removable device management etc. Light weight agent will be deployed in system which will send final status of report to centralized server. The software should have capability of auditing various versions of operating systems not limited to Windows, Android, Linux (Debian, Red Hat etc.), Mac OS, Chrome OS etc. Dashboard should give an overall rating to an organization mapped against all its IT assets.
FAQs	**1. Apart from NISPG guidelines, is it required to integrate any other cyber security standards?** Auditing software may support various international standards along with NISPG guideline. This would be an add-on for the software. **2. Is it required to perform security assessment of the tool?** Yes, the assessment tool must be checked thoroughly for presence of any vulnerable code or vulnerability. **3. What is scope of product expansion?**

	Agents must be capable of upgrading the check list automatically based on inputs provided from server regarding new attacks / standards.

Problem Statement – 28 (MHA-I4C)

Organization Name	**MHA - I4C**
Problem Statement/ **Challenge title**	Cyber security and cyber investigation training courseware
Challenge brief/definition	Current Scenario Lack of quality and updated cyber security and cyber investigation training courseware built for Indian scenarios. Large number of Police force gets recruited by States/UTs or are posted in cyber investigation who needs practical – hands on training. The goal of this project is to design and develop a comprehensive, quality, and up-to-date cyber security and cyber investigation training courseware that is specifically tailored to Indian scenarios. The training courseware will be aimed at addressing the lack of practical, hands-on training for police force personnel who are recruited by States/UTs or are posted in cyber investigation. The courseware should be delivered through a cloud-based, browser-based platform that offers a range of attack-defense and investigation labs that align with Indian investigations. The courseware should include a range of topics such as cyber forensics, server/system log analysis, Distributed Ledger Technology (DLT) - Blockchain Forensics, Cloud Investigation, Crypto currency investigation, API Forensics, IoT Forensics, Ransomware Investigation, SIEM, Vulnerability Analysis & Penetration Testing, Compromise Assessment and First Responder training. This will help in providing hands-on experience to the police force and also making them aware of the latest trends and technologies in cyber security and cyber investigation. The courseware should be designed in a way

	that it can be accessed by multiple users and should be able to scale with the growing need of the user.
FAQs	1. **How would the training module & labs be accessed?** Training labs will be accessed using browser based interface. 2. **Is there a need of training handout /** Standard Operating Procedure **(SOP)** Structured Training content on various practical investigation techniques along with instruction to perform on the laboratory is required. 3. **Where will the vulnerable machines / lab infrastructure hosted?** Vulnerable / Infected machines used in lab would be hosted in sandbox environments ensuring other systems don't get infected.