Problem Statements

PYHack 01:-Air and water quality index and environment monitoring

Description:-

Considering the importance of air and water to human existence, air pollution and water pollution are critical issues that require collective effort for prevention and control. Different types of anthropogenic activities have resulted in environmental dilapidation and ruin. One of the tools that can be used for such a campaign is Air Quality Index (AQI). The AQI was based on the concentrations of different pollutants: We are also familiar with the Water Quality Index (WQI), which in simple terms tells what the quality of drinking water is from a drinking water supply. There is a need for constant and continuous environment monitoring of air quality and water quality for the development of AQI and WQI, which in turn will enable clear communication of how clean or unhealthy the air and water in the study area is.

PYHack02:-Cybersecurity Portal for Effective Management of Servers and Firewalls

Description:-

The All India Council for Technical Education (AICTE) is responsible for managing and safeguarding critical infrastructure and data related to technical education institutions across India. To ensure robust cybersecurity measures, AICTE requires a centralized and comprehensive portal dedicated to managing servers, firewalls, load balancers, software licenses, user access, and other data center hardware components is commonly known as a Data Center Management Portal or Data Center Infrastructure Management (DCIM) Portal. However, the current infrastructure management practices face various challenges that hinder efficient and secure operations. The existing problem can be defined by the following factors: Fragmented Infrastructure Management: AICTE's infrastructure management practices may be fragmented, resulting in disparate systems and tools for managing servers, firewalls, load balancers, and other hardware components. This lack of centralized control leads to inefficiencies, inconsistencies, and potential security vulnerabilities. 1. Manual and Time-Consuming Processes: The absence of an integrated portal leads to manual and time-consuming processes for managing various infrastructure components. Activities such as provisioning, monitoring, patching, and license management are often performed manually, consuming significant human resources and increasing the risk of errors or oversights. 2. Limited Visibility and Control: Without a dedicated portal, AICTE may face challenges in gaining comprehensive visibility into the status, performance, and security of servers, firewalls, load balancers, and other hardware components. This limitation hampers effective monitoring, maintenance, and proactive identification of potential security threats or vulnerabilities. 3. Compliance and License Management: The absence of a centralized portal makes it difficult to track and manage software licenses and ensure compliance with licensing agreements. This may result in the misuse of licenses, unintentional non-compliance, or unnecessary expenses due to duplicate purchases or inadequate license usage tracking. 4. User Access Management: AICTE needs an efficient mechanism to manage user access to various infrastructure components. This includes defining user roles and permissions, ensuring secure authentication and authorization mechanisms, and maintaining an auditable log of user activities. Without a dedicated portal, managing user access becomes challenging and increases the risk of unauthorized access or privilege abuse. Addressing these challenges and implementing an AICTE Cybersecurity Portal has these specific feature need to be developed 5. Server Management: The portal allows administrators to manage servers, including provisioning, configuration, monitoring, and maintenance tasks. It provides an overview of server health, resource utilization, and performance metrics. 6. Firewall and Network Device Management: The portal enables management and configuration of firewalls, switches, routers, and other network devices. It provides a central interface to set up and monitor network policies, security rules, and traffic management. 7. Load Balancer Management: Load balancers play a critical role in distributing network traffic across multiple servers. The portal allows configuration, monitoring, and scaling of load balancers to ensure optimal performance, high availability, and efficient resource utilization. 8. Software License Management: It provides a centralized repository to manage software licenses for various applications and operating systems. The portal helps track license usage, compliance, renewal dates, and license allocation to specific servers or users. 9. User Access and Identity Management: The portal facilitates user access control, authentication, and authorization. Administrators can define user roles, permissions, and access levels for different components and resources within the data center environment. 10. Hardware Inventory and Asset Tracking: The portal maintains an inventory of data center

hardware components, including servers, switches, firewalls, load balancers, and more. It tracks hardware configurations, warranties, and maintenance schedules, helping with resource planning and optimizing hardware lifecycle management

PYHack03:-Efficient enumeration of URLs of active hidden servers over anonymous channel (TOR)

Description:-

The Onion Routing (TOR) is an overlay anonymous network over internet, which not only anonymizes clients accessing the TOR network or internet but also facilitate hosting of servers anonymously. These servers have been reported to be hosting various hidden services involved in malicious activities. The goal of this problem statement is to develop Proof of Concept (PoC) to enumerate URLs (.onion) of active hidden servers hosted over TOR. Teams are supposed to examine the cryptographic security controls and survey existing vulnerabilities in underlying security architecture of TOR network to develop PoC for efficient enumeration of URLs of active hidden services hosted over TOR.

PYHack 04:-Create an intelligent system using AI/ML to detect phishing domains which imitate look and feel of genuine domains

Description:-

Phishing attack is the most prevalent attack technique to compromise users worldwide. Phishing links/websites are shared through number of mediums like email, SMS etc. to target users. These domains are at times host user login page that imitates the genuine target websites. Login attempts on such pages can lead to compromise of user credentials and may also download malicious payload in user computers. The objective of the problem is to identify such phishing domains from the newly registered websites based on open source databases (Example WHOIS Database). Such databases provide list of newly registered domains. The tool should be automated and harness power of AI/ML to identify phishing domains from genuine domains. It may use the following techniques: (a) Backend code / content similarity in web pages. (b) Web page image analysis (i.e. analysis between genuine and phishing site web page images; more the similarity better is the probability score of being a lookalike phishing site). The evaluation would be based on the toolÃƒÂ¢Ã¢â€šÂ¬Ã¢â€žÂ¢s ability with regard to the following: (e) Probability scores of phishing domains on how close they are to the genuine domain. (f) Ability to detect new phishing domains in reasonable time. (g) Ease of use and flexibility in output formats.

PYHack05:-Develop Ransomware Readiness Assessment tool.

Description:-

Ransomware is a type of malicious software designed to block access ICT devices by encryption of data until ransom is paid to attacker. It is of paramount importance to increase awareness regarding such attacks and assess readiness of the ICT infrastructure of any organisation to thwart these attacks or atleast recover at the earliest. The developer should design and deploy a methodology to evaluate posture and preparedness of an organization towards stopping / mitigating threat from ransomware attack. The developed tool shall be evaluated based on following: (a) Depth of the tool to assess readiness of organization to hinder / stop /mitigate ransomware attack. (b) Assessment of organization towards detection of early signs of ransomware. (c) Ease of use and awareness imparted by the tool. (d) Visualization and reporting of the maturity assessment of the organization.

PYHack06:-Develop a AI/ML tool to detect whether a system / firewall /router / network is compromised. The technique should not rely only on IoCs (Indicators of Compromises) detection.

Description:-

Early detection of a compromise of any compute device is critical for security of critical information infrastructure. While most of infections on ICT are detected using IoCs (Indicators of Compromises), the objective of this problem is to explore techniques for detection of compromise on devices using AI / ML models when the IoC of the compromise

is not known. The developer should employ innovative models for non-IoCs based detection of compromise on devices. The evaluation of the solution will be based on the following: (a) Innovation and ruggedness of the method of detection of compromise. (b) Utility of the method developed over various types of devices including system / firewall / router / network. (c) Ease of deployment and method of reporting of detected compromise. (d) Ability to minimize false alarms of compromise.

PYHack07:-**De-anonymisation for monitoring and tracking of illegal activities performed using cryptocurrency transaction technology**

Description:-

Whatever the darkest corner of diabolical human mind can conceive, Dark-Web can deliver with anonymity and impunity. Dark web markets and forums are filled with illicit activities such as counterfeit currency, fake documents, contraband drugs, ransomware attacks etc. In India, Dark-web crimes have proliferated in recent times especially in the arena of Cyber terrorism, drug trafficking, counterfeit documents, currency and sale of classified Government documents. Governments have also recently raised concern over digital currency and use of Dark-Web for drug trafficking. It is important that appropriate tools and techniques may be developed to monitor and track anti-national activities carried out behind the shield of anonymity by using dark web and cryptocurrency technology.

PYHack 08:-To develop centralised information security .Log-collection facility' or 'security operation centre (soc)' in the power sector, considering cEA cybersecurity (Power sector) Guidelines, 2021 to keep lr and or networking System isolated and air-gapped.

Cyber intrusion attempts and cyber-attacks in any critical sector are carried out with a malicious intent. ln Power sector, it's either to compromise the power Supply system or to render the grid operation in-secure. Any such compromise may result in maloperation of, equipment damages or even in a cascading grid brownout/blackout. The Description:-

much-hyped air gap myth between lr and or systems now stands shattered. The artificial air gap created by deploying firewalls between any lr and or system can be jumped by an insider or an outsider through social engineering. Cyber-attacks are staged through tactics and techniques of initial Access, Execution, persistence, privilege Escalation, Défense Evasion, Command and Control, Exfiltration. After gaining an entry inside the system through privilege escalation, the control of lr network and operations of or systems can be taken over even remotely by any cyber adversary. The gain of sensitive operational data through such intrusions may help the Nation/State sponsored or non-sponsored adversaries and cyber-attackers to design more sinister and advanced cyber-attacks. How to develop centralized information security log-collection facility or Security Operation Canter (SoC) in the Power Sector, considering cEA cybersecurity (power Sector) Guidelines- 2021, to keep lT and OT networking System isolated and air-gapped?

PYHack 09:-**Detection of Malware Trojan in software’s used in Power Sector.**

Description:-

The power system networks are getting automated and software are being updated or new Software are being used in the network for various purposes including SCADA, Head End System, Meter Data Management System, Billing System, etc. Most of these software’s are loaded in demilitarized zones; regular patch updates and penetration tests are normally avoided on the live systems. These systems become vulnerable, and hackers try to exploit such systems using various attack vectors. The challenge is to validate presence of malicious codes if any in the software’s which could exploit specific attacks including the zero day attack.

PYHack 10:-**Detection of embedded Malware/ Trojan in hardware devices used in Power Sector**.

Description:-

We know that the technology is changing fast and so are the devices used in Power Systems network. The hardware devices used in the sector are also having fast processing capacity and are intelligent. They also communicate data

either periodically or on request or if some logic is met or at programmed intervals, to control canter's or to local / zonal SCADA system. The devices could be Intelligent Electronic Devices (IEDs) like Relay, BCU, Smart Meters, or Remote Terminal Units (RTU) etc. As these are electronic devices, they are prone to security threats. To make sure these devices are free from security threats, it is required to test them for malware / Trojan or alike of malicious codes present in the devices/ hardware systems (like System on Chip/ Microcontrollers / Microprocessors/ DSP /FPGA based products) which has inbuilt firmware and dedicated application programs running within available and constraint memory. The challenge is to validate such electronic equipment's for vulnerability assessment tests and for presence of suspicious or malicious codes present if any, in the devices; such codes could otherwise exploit specific attacks which may cause damage to process/ system or harm the environment and living beings on certain conditions or may trigger on logics including the zero day attack.

PYHack11:-Analysis and identification of malicious mobile applications

Description:-

ln today's world, using different mobile applications for specific tasks is very common. This leads to smart phone users accumulating too many applications over a period. Seldom do users delete unused applications. Any application performing malicious tasks can very easily go unnoticed. So, there is a need to develop a mobile app tool that can use open-source intelligence and threat feeds to detect various indicators of compromise in the smartphones. The tool can check network communication to various lP addresses that are suspicious, various URLs that are suspicious, inbound connections or packets from applications that are suspicious.

PYHack12:-Online Blockchain based certificate generation and validation system for government organization.

Description:-

Currently large no of training programs is organized, and certificates are provided. There is no mechanism to validate digital certificate.so create a system in which custom digital certificate generate. User can store certificate in digital locker system other organization will validate certificate. Use opensource software and blockchain technology. Expected Output: Blockchain Based Certificate generation and validation Certificate can be added in Digital Loker System Users: Government Office, Student, Industry, Institutes.

PYHack13:-Design of CYBER-SECURITY ENABLED SMART CONTROLLER for grid-connected Microgrid

Description:-

This aims to develop a cybersecurity-enabled smart controller specifically designed for grid-connected microgrids. The smart controller will play a crucial role in ensuring the secure and efficient operation of the microgrid, protecting it from cyber threats and unauthorized access. Key Objectives: Secure Communication: Design a communication framework that employs robust encryption protocols to safeguard the data transmitted between the smart controller and various components within the microgrid. This framework should prevent unauthorized access, tampering, and eavesdropping. Intrusion Detection and Prevention: Implement advanced intrusion detection and prevention mechanisms within the smart controller to identify and mitigate potential cyber attacks in real-time. Develop algorithms and techniques to detect anomalies, malicious activities, and vulnerabilities within the microgrid system. Access Control: Create an access control mechanism for the smart controller that regulates user access based on roles and privileges. This mechanism should prevent unauthorized configuration changes and ensure only authorized personnel can modify or interact with the microgrid system. Cybersecurity Auditing: Develop a logging and auditing system within the smart controller to track and monitor all activities and events related to the microgrid's cybersecurity. This system should provide detailed logs, alerts, and reports to facilitate post-incident analysis and forensic investigations. Security Patch Management: Implement a mechanism within the smart controller to manage and deploy security patches and updates across the microgrid system. This will ensure that vulnerabilities are promptly addressed, reducing the risk of potential cyber attacks. Scalability and Compatibility: Design the smart controller to be scalable, allowing it to accommodate the increasing complexity and size of grid-connected microgrids. Ensure compatibility with different microgrid components, protocols, and standards to facilitate seamless integration into existing infrastructure. Usability and User Interface: Develop a user-friendly interface for the smart controller that enables efficient monitoring, configuration, and management of the microgrid's cybersecurity settings. The interface should be intuitive and accessible to both cybersecurity experts and non-technical users. This PS encouraged to explore innovative cybersecurity methodologies, including encryption algorithms, anomaly detection techniques, and secure communication protocols. The resulting smart controller will contribute significantly to the protection and

reliable operation of grid-connected microgrids, ensuring the stability and security of the power distribution system in the face of evolving cyber threats.

PYHack14:-**A mobile app that crowd sources water-related problems from around a community, open sources data, etc. and display them on a map.**

Description:-

The use of social media data in disaster and crisis management is increasing rapidly. Particularly in connection to flooding events, water quality issues in ponds/lakes, urban flooding, and drainage problem, etc., geo-referenced images shared by citizens can provide situational awareness to emergency responders, as well as assist with financial loss assessment, giving information that would otherwise be very hard to collect through conventional sensors or remote sensing products. Discussion about such events can also be found on various social media platforms. Further, recent advances in computer vision and deep learning can perhaps support the automated analysis of these data. In this problem, software/ algorithm to be developed focusing on ground-level images taken by humans. Considering distinct datasets from different sources, the algorithm of the developed mobile app should be able to categorize water-related problems at different administrative. Further, the mobile app should serve as a valuable tool for the administrators for planning and managing water-related problems.

PYHack 15:-Self-identifying the mental health status and get guidance for support.

Description:-

Considering the increasing burden of the mental disorders (as evidenced in National Mental Health Survey-2016), it is important to identify the people at the risk of developing mental disorder at early stage to take the necessary action. Primary Health Care centre is a gate-keeper of the Indian public health care delivery system and also an opportunity to screen patient for the risk of developing mental disorders. There are some validated tools are available for screen of the person for risk of developing psychiatric disorders, however, ready availability, taking response from patients, interpretation and quick guide for taking action based on the interpretation of the tool score is still challenge for effective and efficient utilization of the screening tool. Expected Output: Mobile application for screening of mental health. Users: Public as well as Frontline Health worker.

PYHack16:-Developing a GUI based hardening script for Ubuntu operating system with flexibility to cater for organisational security policies

Description:-

Hardening of an operating system involves implementation of security measure to make the system compliant with the security policies of the organization. The procedure for hardening should be intuitive to allow ease of use by personnel with minimal IT skills. The goal of this problem statement is to generate a script which is undertakes hardening of Ubuntu OS using an GUI based approach. During the hardening process, the user should have the flexibility to make settings based on the organisations IT security policy provision like blocking ssh, usb, ToR etc. The grading of tool will be based on hardening functions implemented, attention to user experience and flexibility to take user settings. Developer should remember that security is of utmost importance.

PYHack 17:-Community Based Reporting and Monitoring Tool for Women's Safety in Colleges/Universities.

Description:-

Campuses of colleges and universities are meant to be vibrant, free-flowing, and dynamic in nature. An accommodating campus supports idea exchange, personal growth, and soft skill development. The safety of students, especially women's students, is a pillar of an accommodating campus. In the present scenario, the measures available to college administrators and students, such as the installation of CCTV cameras, increased security on campuses, and the establishment of police outposts, are reactive in nature, i.e., they are pressed into action only after the occurrence of a mishap. The objective of the problem statement is to develop predictive analytic models to prevent mishaps even before they occur. The second issue pertaining to women's safety is the lack of manpower for proactive interventions to prevent mishaps. Another objective is to develop, monitor, predict, and provide actionable intelligence for the prevention of mishaps. The solution can explore the contours of anonymous and non-anonymous data collection mechanisms, point-to-point reporting systems, and predictive data analytics for providing actionable intelligence.

Further, the collected data can be leveraged to develop and mark probable black spots and red time zones for pin-pointed actions to be taken by administrators. To promote a community-based system, the system may be designed in such a way that it not only gathers information from students but also involves the entire student community in the prevention of mishaps. The data collected from the participants can be populated into the system, and real-time monitoring can be done with an interactive dashboard and charts. It can also be used to develop real-time rapid intervention by the student community, college administration, and local authorities. Further to this, a companion model can also be developed for students that helps them travel through black spots and during red time zones. This will not only ensure the community participation of students but also develop a responsibility-sharing framework for campus safety.

PYHack 18:-AI-powered Legal Documentation Assistant

Description:-

Legal documentation can be a complicated and time-consuming process, especially for individuals and small businesses who may not have access to legal resources. In addition, the language and jargon used in legal documents can be difficult for non-lawyers to understand, which can lead to errors and misunderstandings. Objective: The objective of this hackathon challenge is to develop an AI-powered solution that can simplify legal documentation for individuals and small businesses in India, by automatically drafting legal documents in plain language and using easy-to-understand terms. Potential Features: 1. User-friendly interface for inputting relevant information such as parties involved, terms of the agreement, and other necessary details. 2. AI-powered document generation that automatically drafts legal documents in plain language and using easy-to-understand terms. 3. Ability to customize legal documents based on the specific needs of the user. 4. Integration with existing legal resources and databases to ensure accuracy and completeness of the legal documents. 5. Option for users to seek legal advice from an expert in case of complex legal issues. Impact: The proposed solution can greatly benefit individuals and small businesses in India, who often face challenges with legal documentation due to limited access to legal resources. By simplifying legal documentation, this solution can potentially save time, reduce errors, and increase access to justice. Data: Participants can use publicly available legal databases and resources to train the AI model for document generation. Deliverables: 1. A working prototype of the AI-powered legal documentation assistant, demonstrating its functionality and ease of use. 2. A presentation outlining the features and potential impact of the solution, as well as its technical architecture and data requirements. 3. Code and documentation for the solution, along with instructions for deployment and maintenance. Note: Participants are encouraged to consider the ethical implications of their solution and to prioritize data privacy and security.

PYHack 19:-Design, develop and implement a software bill of materials (SBOM) generation tool that can generate the complete SBOM of custom-developed software (including in-house developments by organisations)

Description:-

SBOM stands for Software Bill of Material and lists out all the packages / modules used from various repositories to make the final solution. This list is essential for identification of vulnerabilities that may impact the final solution. This is critical for supply chain vulnerability management of solutions deployed within the organisation. Thus the task for developers is to develop a software which automatically lists various libraries, dependencies and modules that have been used for making of a given application and generates underlying SBOM. There would be added focus on creating features which can red flag anomalies with an ability to lay out the context to the user. The evaluation shall be based on automation, granularity and accuracy of the SBOM generated. Example, if the developer can identify the version of the libraries used, it shall be graded higher. Ease of use and user experience are other important metrics of evaluation.

PYHack 20:-Making career choices and AI based counselling accessible to every child at secondary level along with aptitude tests and detailed career paths.

Description:-

The project team shall establish an interactive AI based model that will help students to to choose from careers. The model should handhold student in assessing his capabilities and subsequently help him in deciding a career path.