**PS-1: Enhancing Cybersecurity with Targeted Vulnerability Prevention**

**Problem:**

Delivering robust and secure software solutions requires actively addressing the OWASP Top 10 vulnerabilities and other common security threats. As the cybersecurity landscape evolves, ensuring that all potential vulnerabilities are effectively identified, mitigated, and resolved remains an ongoing challenge. While existing security measures and processes are typically in place, continually adapting to new and emerging threats demands enhanced vigilance and continuous improvement. The dynamic nature of software development, coupled with the increasing sophistication of cyber threats, makes it crucial for organizations to consistently strengthen their ability to detect, address, and prevent vulnerabilities in code, ensuring compliance with industry standards and the protection of sensitive data.

**Goal:**

* Develop tools/techniques/processes that can automatically detect and flag the specified OWASP top 10, SANS top 25, business logic vulnerabilities, and other emerging threats within the application system during the development cycle
* The application systems for which vulnerabilities need to be identified should be .Net, Java, Eclipse, Android Studio, and IOS.

**Key Challenges:**

* Selecting the right tools and techniques for detecting the specified vulnerabilities.
* Seamlessly integrating these tools into development and deployment workflows.
* Ensuring that the vulnerability detection process is accurate, has no / less false positives, and is effective.
* Balancing security requirements with the need for efficient development and delivery

List of Vulnerabilities to Address: OWASP Top 10, SANS Top 25, business logic vulnerabilities, and other emerging threats within the application system. As a participant, you are encouraged to choose as many vulnerabilities as possible and provide remediation for them.

Participants are free to choose tools of their choice however the tools used should not have any existing, known, published vulnerabilities.

**PS-2: Enhancing Customer Experience and Retention through AI-Driven Personalisation to improve the propensity to purchase**

**Problem**

SBI Life currently relies on a 1000+ user persona-based approach for customer behavior recommendation, which limits the depth of individual-centric analysis and fails to resonate with their unique preference, reducing the likelihood of conversion.

**Goal**

To leverage AI to:

* **Deepen individual-centric insights:** Develop a more personalized understanding of customer behavior, preferences, and needs.
* **Optimize upselling strategies:** Suggest tailored policy terms, ticket prices, and durations to increase customer satisfaction and retention.
* **Improve customer persistency:** Enhance the likelihood of prospective customers closing deals and existing customers maintaining their policies.

**Key Challenges**

* **Data Quality and Availability:** Ensuring the quality, completeness, and ethical sourcing of customer data from both internal and external sources.
* **AI Model Development:** Building robust AI models capable of accurately predicting customer behavior, preferences, and future needs.
* **Integration with Existing Systems:** Seamlessly integrating AI-powered solutions into SBI Life's existing customer relationship management and policy management systems.
* **Ethical Considerations:** Adhering to data privacy regulations and ensuring ethical use of AI to protect customer information and prevent bias.or

Participants are free to choose tools of their choice however the tools used should not have any existing, known, or published vulnerabilities.

**PS-3: AI-Driven Fraud Detection and Prevention in Insurance**

**Problem:**

The insurance industry faces significant challenges in detecting and preventing various types of fraud, including identity theft, premium fraud, and claim inflation. With fraudsters employing increasingly sophisticated techniques and the vast amount of data generated by insurers, it has become difficult to identify and mitigate fraudulent activities effectively.

**Goal:**

The aim is to develop AI-driven solutions that can:

* **Identify trends and anomalies**: Detect unusual patterns or deviations from expected behavior in customer data, policy information, and claim submissions.
* **Detect forgery**: Authenticate documents and signatures to ensure the legitimacy of policy applications, claims, and other relevant documents.
* **Prevent fraud**: Implement proactive measures to prevent fraudulent activities through innovative approaches and advanced techniques.

**Key Challenges:**

* **Complex fraud patterns**: Fraudsters continually evolve their methods, requiring solutions capable of identifying both known and emerging fraud patterns such as identity theft, premium fraud, and claim documentation fraud.
* **Large datasets**: Insurance companies generate vast amounts of data daily, making it challenging to efficiently analyze and extract insights necessary for fraud detection.
* **Data quality**: Ensuring the accuracy, consistency, and completeness of data is crucial for effective fraud detection, as incomplete or inconsistent data can hinder AI model performance.
* **Innovation gap**: The insurance industry facing challenges in adopting cutting-edge AI technologies and promoting innovation in fraud prevention strategies.

Participants are encouraged to use as many generic datasets as available relevant to insurance fraud detection. They will also be provided with a set of key **data points and parameters** that should guide their solution modeling, ensuring alignment with real-world scenarios in the insurance industry. However, participants are expected to **look beyond the provided data** and come up with their approaches to detect emerging, **unknown fraud patterns**, as fraud techniques continually evolve.

Participants are free to choose tools of their choice however the tools used should not have any existing, known, published vulnerabilities.