Annexure 1

Request for Proposal (RFP): Development of Cyber Security Enhancement Web Application for general Public

Introduction:

We are seeking proposals from forward-thinking start-ups to participate in the development of a cutting-edge web-based application focused on bolstering cyber security measures for the general public. Our primary objective is to address the increasing threats posed by users navigating through malicious fake trading websites with the goal of providing users with real-time scam alerts through their web browsers.

Objective:

The objective of this project is to improve the efficiency and accuracy of our team's daily task of identifying and reporting suspected fake trading/investment websites. Through the incorporation of Artificial Intelligence (AI) and Deep Learning (DL) technologies, in collaboration with start-ups specializing in AI and DL, we aim to automate the current manual processes involved in website analysis. This automation will save time and enhance the precision of identifying potential threats.

Project Overview:

The proposed solution entails the development of a web application that employs advanced website analysis techniques, including but not limited to IP series examination, source code scrutiny, signature comparison, and trust score evaluation. The ultimate aim is to empower users with real-time scam alerts seamlessly integrated into their web browsers.

Key Focus Areas:

Advanced Website Analysis: Leverage sophisticated techniques such as IP series analysis, source code examination, signature comparison, and trust score evaluation to identify potential threats on websites.

Real-time Scam Alerts: Provide users with instantaneous alerts through their web browsers, enabling proactive measures against potential cyber threats.

We believe that collaboration with KSUM and its network of innovative start-ups will bring fresh perspectives and expertise to this crucial project. By working together, we can contribute to the development of a solution that not only addresses current challenges but also sets a new standard for cyber security in the digital landscape.

Current Workflow:

1. Identification: Manually identify suspected fake trading/investment websites through the websites and links registered at the National Cybercrime Report Portal.

2. Analysis: Conduct reverse engineering on identified websites, retrieving WHOIS domain details, including IP information, registrar, registrant, and age of the website. Utilize open-source tools for review, trust scores, and technical parameters.
3. Reporting: Compile a detailed report for higher officials with findings and recommendations.

Proposed Automation:

1. AI-powered Analysis: Collaborate with AI and DL-based companies to develop a system that automates the analysis of suspected websites, mimicking the current manual analysis, including review scores and technical parameter evaluation.
2. Automated WHOIS Lookup: Integrate tools to automatically retrieve WHOIS domain details, eliminating the need for manual searches. AI-driven analysis and automated WHOIS lookup will enhance the accuracy of identifying fake trading/investment websites, minimizing the risk of oversight.
3. Scalable Infrastructure: Develop a scalable and robust infrastructure to handle the increasing volume of suspected websites, ensuring quick and efficient processing.
4. Real-time Reporting: Implement an automated system to generate reports in real-time, allowing for quicker response and proactive measures against potential scams.
5. Artificial Intelligence for Phishing Link Detection: Utilize AI to identify phishing links based on factors such as URL structure and domain characteristics. Populate a comprehensive database of fraudulent websites and links.
6. Browser Extension Development: Create browser extensions for popular browsers to seamlessly integrate the database. Enable API calls to our database for every search, or collaborate with browsers that maintain their own databases for phishing/scam websites.
7. User Alerts: If a link is identified as phishing, generate alerts to warn users. Include educational content in alerts to inform users about potential risks involved.

Proposal Submission:

Interested start-ups are requested to submit proposals no later than [Insert Deadline] through Kerala Startup Mission. Proposals should include:

- Company profile and relevant experience.
- Details of past projects related to software development and security.
- Technical approach and methodology.
- Proposed timeline and milestones.
- Cost estimate with a breakdown.
- Team composition and qualifications.
- Certifications from past clients for the last five completed projects.
- Any additional relevant information.

Deliverables:

1. **Web Application Development:**
   - Creation of a user-friendly web application with advanced website analysis capabilities.
   - Implementation of IP series examination, source code scrutiny, signature comparison, and trust score evaluation features.
2. **Real-time Scam Alert System:**
   - Integration of a robust system for providing users with instantaneous scam alerts.
   - Seamless integration into web browsers to ensure a user-friendly experience.
3. **Documentation:**
   - Comprehensive documentation outlining the technical aspects and functionalities of the developed web application.
   - User manuals and guidelines for effective utilization of the real-time scam alert system.

Evaluation Criteria:

Proposals will be evaluated based on:

- Experience and expertise.
- Technical approach and methodology.
- Cost-effectiveness.
- Compliance with government guidelines.
- Timeliness and project management capabilities.
- Additional recommended services.

Timeline:

- RFP Issuance Date: 12/01/2024
- Proposal Submission Deadline: 22/01/2024
- Evaluation and Selection: 22/01/2024 to 25/01/2024
- Project Commencement: 01/02/2024

Contact Information: For inquiries, please contact Mr. Nighil.S (9020351631) or Email: webadminscrb.pol@kerala.gov.in.

****