SOAIR
School Of Artificial Intelligence & Robotics

SOAIR Hub, Nigeria Airforce Base Ikeja
www.soairafrica.com
08065089535
soairafrica

Prepared for: Pleroma Inc.
Prepared by: School of Artificial Intelligence & Robotics (SOAIR)
Date: May 5th, 2025.

Proposal from SOAIR to Pleroma Inc. for Cybersecurity Software Development

Executive Summary

The School of Artificial Intelligence & Robotics (SOAIR), a leader in affordable tech education and robotics development in Nigeria, proposes a strategic partnership with Pleroma Inc. to develop its innovative Petri net-based cybersecurity software. Pleroma's unified framework, which uses Petri nets to model organizational networks, detect cyber threats via machine learning trained on the CAPEC database, and optimize defenses through stochastic game theory, addresses the critical need for compositional cybersecurity in an interconnected world. SOAIR offers its expertise in software development, AI, and project-based training to build a scalable, intuitive platform that aligns with Pleroma's vision. This collaboration will deliver a prototype within six months, leveraging SOAIR's cost-effective development model and Pleroma's cutting-edge research to create a market-ready solution that protects small and large firms from diverse cyber threats.

About SOAIR

SOAIR, operating under Learners Technology NIG LTD, is a trailblazing institution dedicated to empowering Africans through affordable education in AI, robotics, and coding. Since 2021, SOAIR has trained over 500 Nigerians and engaged 2,500+ young learners through its Code Learners initiative. Key strengths include:

- **Software Development Expertise**: SOAIR's team has delivered robust web and AI applications, including student accommodation software and robotics control systems.
- **Project-Based Approach**: Hands-on training ensures practical, industry-relevant solutions, with students contributing to real-world projects.
- **Affordable Innovation**: SOAIR's cost-effective model makes high-quality tech solutions accessible, aligning with Pleroma's goal of affordable consulting for SMEs.
- **Robotics and AI Leadership:** SOAIR manufactures Africa-centric robotics, equipping its team with skills in concurrent systems akin to Petri net modeling.

SOAIR's experience in developing scalable software and fostering tech talent positions it as an ideal partner to bring Pleroma's cybersecurity vision to life.

Understanding Pleroma's Vision

Pleroma Inc. aims to revolutionize cybersecurity by using Petri nets a graphical and mathematical language for concurrent systems to provide a unified framework for detecting and preventing cyberattacks. Key components include:

- **Network Modelling:** Creating Petri net models from business process data to represent organizational systems and their interactions.
- **Threat Detection**: Using machine learning trained on the CAPEC database to identify attack patterns and assign costs to network nodes.
- **Defence Optimization**: Applying stochastic game theory and reinforcement learning to simulate attack scenarios and devise optimal protection strategies.
- **Compositional Security**: Modeling small and large firms independently and combining them to address interdependencies, critical for supply chains.
- **Intuitive Interface:** Translating complex models into diagrams for non-experts, ensuring accessibility.

Pleroma's current priorities include developing a prototype, scaling from toy models to realistic scenarios, and integrating cloud-based computing for performance. SOAIR's proposal addresses these needs with a structured development plan.

Market Opportunity

Cybercrime costs Canada $3.12 billion annually and globally extracts 13-20% of the $3 trillion internet economy, with SMEs facing significant risks (average data breach cost: $6.03 million). The cybersecurity market is projected to reach $177 billion by 2025, driven by rising threats like ransomware, phishing, and IoT vulnerabilities. Pleroma's Petri net approach is uniquely positioned to:

- Address the gap in unified cybersecurity frameworks, unlike fragmented tools.
- Serve SMEs, which account for 98% of Canada's economy and 75% of data breaches.
- Capitalize on the 1.8 million global cybersecurity job gap by offering intuitive tools for non-experts.

SOAIR's development capabilities will accelerate Pleroma's market entry, delivering a solution that meets the growing demand for compositional, scalable cybersecurity.

Proposed Development Plan

SOAIR proposes to develop Pleroma's Petri net-based cybersecurity platform, delivering a functional prototype within six months. The plan includes:

1. Requirements Analysis and Planning (Weeks 1-4)

- Objective: Define technical specifications and align with Pleroma's vision.
- **Activities:**
  - Collaborate with Pleroma's team to map business process data integration needs.
  - Specify Petri net modeling requirements, including CAPEC integration and stochastic game theory algorithms.
  - Design an intuitive graphical interface for non-expert users.
- **Deliverables**: Requirements document, project roadmap, and UI/UX wireframes.

2. Prototype Development (Weeks 5-16)

- **Objective:** Build a cloud-based prototype with core functionalities.
- **Technology Stack:**
  - **Front-End:** React.js for a responsive, graphical interface displaying Petri net diagrams.
  - **Back-End:** Node.js with Express for API management and cloud integration (e.g., AWS or Azure).
  - **Machine Learning**: Python with TensorFlow for CAPEC-trained threat detection.
  - **Database**: PostgreSQL for storing network models and attack patterns.
- **Activities:**
  - Develop Petri net modeling module to infer organizational structures from business data.
  - Implement machine learning algorithms to identify attack patterns and assign node costs.
  - Build stochastic game theory and reinforcement learning components for defense strategies.
  - Create a user-friendly dashboard with diagrammatic visualizations.
- **Deliverables**: Functional prototype with core features, cloud infrastructure setup.

3. Testing and Iteration (Weeks 17-22)

- **Objective**: Ensure reliability, scalability, and usability.
- **Activities:**
  - Conduct unit, integration, and stress testing to validate performance under simulated cyberattacks.
  - Test anomaly and misuse detection accuracy using CAPEC-based scenarios.
  - Gather feedback from Pleroma's team and potential users via beta testing.
  - Refine interface and algorithms based on feedback.
- **Deliverables**: Tested prototype, bug reports, and user feedback summary.

4. Deployment and Training (Weeks 23-24)

- **Objective**: Prepare Pleroma for market entry.
- **Activities**:
  - Deploy the prototype on a cloud platform with scalable architecture.
  - Provide training for Pleroma's staff on platform operation and maintenance.
  - Deliver comprehensive documentation, including API guides and user manuals.
- **Deliverables**: Deployed prototype, training sessions, and documentation.

5. Ongoing Support (Post-Deployment)

- **Objective**: Ensure long-term success and scalability.
- **Activities**:
  - Offer six months of technical support for bug fixes and minor updates.
  - Train Pleroma's team to extend the platform for diverse industries (e.g., healthcare, retail).
  - Provide consulting on integrating the platform with existing cybersecurity tools.

SOAIR's Value Proposition

- **Cost-Effective Development**: SOAIR's affordable model, honed through training 500+ Nigerians and developing robotics, ensures high-quality deliverables within budget.
- **Expertise in AI and Concurrent Systems**: SOAIR's experience with robotics control systems aligns with Petri nets' concurrent modelling, ensuring technical proficiency.
- **Project-Based Talent**: SOAIR's student developers, trained in real-world projects, contribute to cost-efficient, innovative solutions.
- **Alignment with Pleroma's Mission:** Both organizations prioritize accessibility, with SOAIR's affordable education mirroring Pleroma's goal of serving SMEs.

and large firms from diverse cyber threats.

Expected Outcomes

- A functional prototype modeling organizational networks as Petri nets, detecting threats, and optimizing defenses.
- An intuitive interface for non-experts, enhancing Pleroma's market appeal.
- A scalable, cloud-based platform ready for beta testing and free trials.
- Strengthened Pleroma-SOAIR partnership, with potential for future collaborations (e.g., training programs for Pleroma's clients).