**CIRCUIT 25**

**Team Members:**

* **KALASH BHEDA**
* **ARNAV BHANDARI**
* **JASON DSOUZA**
* **HEET BHARADWA**

**Git hub-** [**GITHUB**](https://github.com/Mercurius13/codeclash2025-uno)

**Project Overview**

This project is an AI-driven cybersecurity framework that detects, responds to, and adapts to security threats in real-time using machine learning and reinforcement learning techniques. The self-healing capability allows the system to take automated actions to mitigate threats dynamically.

**Problem Statement**

* Growing cyber threats exploiting unseen vulnerabilities.
* Traditional rule-based security systems struggle to detect and mitigate real-time threats.
* Need for an AI-driven self-healing security framework to handle evolving cyberattacks autonomously.

**Our Approach**

**Part 1: Threat Detection**

* Trained on data from the **TON IoT dataset**.
* Uses **Graph Neural Networks (GNNs)** for enhanced accuracy.
* **Adam optimizer** for efficient model training.
* Simulates **network problems like jitter and packet loss** to test resilience.
* Implements a **basic Reinforcement Learning (RL) algorithm** to improve over time.
* Continuously receives **simulated attacks (real or fake)** to refine detection.
* Effectively distinguishes between **true and false positives**.

**Part 2: Security Dashboard**

* Implements a **self-healing algorithm** for automated threat mitigation.
* Provides **real-time updates** on attack locations and logs.
* **Map-based visualization** to identify the origin of cyber attacks.
* Identifies intrusion types from:
  + **IoT Botnet**
  + **Ransomware**
  + **DDoS**
  + **Malware**
  + **Brute Force**
  + **SQL Injection**
* Classifies threats based on **severity levels (low to critical)**.

**Frameworks Used:**

* **AI & ML**: PyTorch, Graph Neural Networks, Stable-Baselines3 PPO.
* **Backend**: Flask, FastAPI, Uvicorn, NumPy, Pandas, SHAP (Explainable AI).
* **Visualization**: Plotly.js, Leaflet.js for geolocation mapping.
* **Cybersecurity Features**: Secure Firmware Rollback, OS Recovery.
* **Webapp:** Next JS, TypeScript, JavaScript, HTML

**Market Potential**

* **$500+ billion cybersecurity market by 2030** due to rising AI-powered cyber threats.
* **Growing demand for AI-based security solutions** in enterprises.
* **Expanding IoT ecosystem requires automated, real-time security.**

**Conclusion**

This AI-powered self-healing framework has the potential to revolutionize cybersecurity by making **threat detection, response, and mitigation fully autonomous**. By leveraging **real-time monitoring, automation, and adaptive AI**, this project aims to create a **self-healing defense system** against cyber threats.