Track 6: GreenGuard: Cybersecurity for Critical Eco-Infrastructure

Case Study

As Delhi races to build a smarter, more sustainable future, it is deploying thousands of connected devices. IoT sensors monitor our water pipelines, smart meters manage our energy grid, and automated systems optimize our waste collection. But this hyper-connected infrastructure creates a new, invisible layer of risk. What happens if a malicious actor hacks into the smart grid to cause a targeted blackout during a heatwave? What if they manipulate water quality data from sensors, either hiding a real contamination event or faking one to cause mass panic? If the data from a food traceability system can be altered, the entire platform becomes worthless. Without a foundation of robust security, our smart and sustainable city is dangerously fragile.

Call for Innovation

This track is a mission for the cybersecurity experts, the ethical hackers, and the security architects. While other teams build the future, your job is to defend it. We are not looking for simple firewalls; we are challenging you to design the **next-generation security frameworks** for complex, city-scale IoT networks. Your mission is to build resilient, proactive, and intelligent defense systems that can protect our critical eco-infrastructure from sophisticated threats. Think zero-trust architecture, AI-powered threat detection, and end-to-end data encryption. Become a GreenGuard and ensure that the technology built to save our planet is safe, secure, and trustworthy.

Problem Statements

1. The Smart City IoT Honeypot

Design and deploy a **honeypot** to simulate a network of environmental IoT devices, such as smart water meters or air quality sensors. Your system must be designed to attract, detect, and analyze cyberattacks in a controlled environment. You will need to build a security dashboard that provides real-time alerts on intrusion attempts (like brute-force logins or malware uploads), classifies the type of threat, and provides forensic data that would help an operator strengthen the defenses of the real-world network.

2. Zero-Trust Architecture for the Smart Grid

A modern smart grid has no traditional perimeter, making it vulnerable to attack if even one device is compromised. Your challenge is to design a **zero-trust access control system** for a simulated smart grid network. Your solution must enforce strict identity verification and

micro-segmentation, ensuring that every device (like a smart meter or a grid controller) and every API request is authenticated and authorized before any communication is permitted. The goal is to create a framework where trust is never assumed, effectively preventing attackers from moving laterally across the network.

3. AI-Powered Anomaly Detection for Data Integrity

The data from environmental sensors is the lifeblood of a smart city, but it can be manipulated. Your task is to build an **unsupervised machine learning model** that continuously analyzes the data streams coming from a network of sensors. Your AI must learn the normal operational patterns and statistical signatures of the data. Its primary function is to identify subtle anomalies and deviations that could indicate either a malfunctioning sensor or a sophisticated, low-and-slow data tampering attack, thereby ensuring the integrity and reliability of the city's environmental data.