Why is AI critical in cybersecurity, and what excites me about building SentinelNet?

Cybersecurity today faces an arms race between defenders and attackers. Traditional systems rely heavily on static rules and manual monitoring, which makes them ineffective against rapidly evolving and sophisticated cyberattacks. This is where **Artificial Intelligence (AI)** becomes critical. AI enables automated learning from massive amounts of network traffic, identifying hidden patterns that humans or rule-based systems might miss. By using machine learning and deep learning models, AI can detect anomalies in real time, classify different types of attacks, and even predict potential intrusions before they cause harm. This makes AI not just a tool but a **necessity** in modern cybersecurity.

What excites me about working on **SentinelNet** is the opportunity to combine cutting-edge AI with real-world applications. Instead of simply studying datasets in theory, SentinelNet gives me the chance to build something that could protect real systems and users. The idea of designing a system that continuously adapts to new threats—like an immune system for networks—is both intellectually challenging. Furthermore, working with datasets such as NSL-KDD and CICIDS2017 allows me to explore both classical and modern perspectives of network intrusions. SentinelNet is not just an academic exercise but a step toward solving one of the most pressing challenges in today's digital world: securing data and systems from ever-evolving cyber threats.