Project Title: SplunkSec AI - An AI-Driven Cybersecurity Monitoring Platform

Track: AI/ML (Track 4)

What Problem Does It Solve?

Security teams face alert fatigue, noise, and missed threats due to traditional SIEM limitations.

SplunkSec AI uses machine learning and NLP to detect anomalies, correlate events, and summarize incidents in real-time.

Target Users:

- SOC analysts
- Security engineers
- Incident response teams using Splunk

How It Integrates with Splunk:

- Ingests logs via Splunk Universal Forwarder
- Uses CIM mapping for indexing and model input
- Runs unsupervised ML via MLTK (Isolation Forest, Autoencoder)
- Summarizes threats using LLMs through Splunk DSDL
- Outputs to dashboards, alerts, and Splunk ES Notable Events

Optional: Architecture diagram provided separately.