Slide 1: Title Slide

SplunkSec AI - An AI-Driven Cybersecurity Monitoring Platform

Track 4 - AI/ML

Team Name: [Your Team Name]

Member(s): [Your Name]

Slide 2: The Problem

SOC teams are overwhelmed with noisy, low-priority alerts.

Static rule-based SIEMs miss stealthy or multi-stage attacks.

Need for contextual, intelligent, real-time detection.

Slide 3: The Solution

SplunkSec AI provides ML-powered anomaly detection,

behavior profiling, alert clustering, and NLP summaries.

It works natively within Splunk and enhances analyst workflows.

Slide 4: Architecture Overview

[See architecture.png]

Data -> Indexing -> ML Pipeline (MLTK + DSDL) -> Dashboards & Alerts.

Slide 5: Key Features

- Anomaly Detection
- User Behavior Analytics (UEBA)
- Clustering & Summarization
- Custom Dashboards & Alerts
- Splunk-native Integration

Slide 6: Tech Stack

Splunk, MLTK, DSDL, Python, ONNX, Autoencoder, Isolation Forest,

DBSCAN, LLMs, GitHub, JSON/CSV Logs.

Slide 7: Demo Snapshots

[Include dashboard, alert, NLP summary images]

Video demo shows full pipeline from logs to alerts.

Slide 8: Value Proposition

- Reduces Alert Fatigue

- Detects Advanced Threats

- Accelerates Response

- Works with Existing Splunk Workflows

Slide 9: Future Scope

- Generative AI Playbooks

- Threat Intel Integration

- Federated Learning

- Explainable AI

Slide 10: Thank You

GitHub: [Your Link Here]

Demo Video: [Your YouTube Link Here]