Project Proposal: Security Incident Pattern Recognition and Response Opt

1. Executive Summary

This project applies AI-powered market trend analysis principles to security operations, using Wazuh data to identify incident patterns and optimize automated responses via Shuffle playbooks. The system will detect emerging threats, predict future incidents, and recommend the most efficient responses through ML-driven insights.

2. Problem Mapping & Analogy

We map:

- Product Trends -> Incident Trends (e.g., surge in phishing alerts)
- Customer Behavior -> Asset/Threat Profiling (e.g., frequent targets)
- Pricing Patterns -> Response Cost-Effectiveness (e.g., which playbook offers most ROI)

This parallels the use of AI for Market Trend Analysis in business.

3. Data Pipeline & Enrichment

- Source: Wazuh alerts, logs, integrity/vulnerability data
- Augmentation: Threat intel feeds (e.g., MITRE ATT&CK, public CVE feeds)
- Feature Engineering: Time-series creation, normalization, entity extraction, missing value handling

4. AI Techniques & Use Cases

- Time-Series Forecasting (LSTM/Prophet): Predict threat trends
- Clustering (KMeans/DBSCAN): Group similar threats for reusable playbooks
- Supervised Models (RF/Logistic Regression): Recommend optimal playbooks
- Anomaly Detection (Isolation Forest): Spot novel attacks
- NLP (Transformer/BERT): Extract incident context from logs and messages

5. Output Layer

- Predictive Graphs: Incident volume/type over time
- Playbook Recommendations: Based on alert pattern and response history
- Novelty Alerts: Flag outliers for SOC review

6. Innovation Add-ons

- Explainable AI (SHAP/LIME): Justify model decisions

- Interactive Streamlit Dashboard: Visual trends, model insights, analyst feedback loop
- Feedback Mechanism: Improve recommendations over time

7. Milestone Plan

- Week 1: Define data schema, simulate Wazuh alerts
- Week 2: Implement preprocessing, clustering, basic time series
- Week 3: Supervised model + anomaly detection + dashboard MVP
- Week 4: Add NLP, XAI, finalize system and documentation

System Architecture Diagram