1. Anomaly & Threat Detection Models

These models address the core requirement of identifying "unusual" behavior in network logs or system telemetry.

- **Isolation Forest:** The industry standard for unsupervised anomaly detection in tabular log data. It is computationally efficient and excels at finding "outliers" (anomalies) by isolating them in a tree structure.
- **Graph Neural Networks (GNNs):** Specifically models like **GraphSAGE** or **Log2Vec**. Since cyber threats are often relational (e.g., an IP connecting to multiple servers), GNNs treat network traffic as a graph, making them superior for detecting lateral movement and sophisticated botnet patterns.
- **LSTM-Autoencoders:** A deep learning approach for time-series logs. The model learns to "reconstruct" normal traffic; a high reconstruction error indicates a potential zero-day threat or a sudden spike in malicious activity.

---

2. Threat Classification & MITRE ATT&CK Mapping

These models turn raw detections into actionable intelligence by labeling them with specific tactics and techniques.

- **XGBoost / CatBoost:** Gradient-boosted decision trees are the best performers for structured security data. They can be trained on datasets like **UNSW-NB15** or **CIC-IDS2017** to classify attacks (e.g., DDoS, SQL Injection, Brute Force) with very high precision.
- **Random Forest:** Excellent for transparency. It provides **Feature Importance** scores, which can be visualized in your dashboard to show analysts exactly which log attributes (like payload size or destination port) triggered the alert.

---

3. Temporal Trend & Forecasting Models

To identify "seasonality" or "spikes" in the threat landscape, use specialized time-series forecasting.

- **Prophet (by Meta):** The best choice for business-ready trend analysis. It automatically handles holidays, seasonality, and missing data, providing clear "uncertainty intervals" that are perfect for your **Trend and Anomaly Detection** module.

- **NeuralProphet:** A hybrid model that combines the interpretability of Prophet with the power of Neural Networks (PyTorch). It is better at capturing complex, non-linear dependencies in high-frequency attack logs.

---

4. Geospatial & Hierarchical Models

For the interactive map and treemap components, these models help in grouping and prioritizing risks.

- **DBSCAN (Clustering):** Unlike K-Means, DBSCAN does not require you to pre-specify the number of clusters. It is ideal for identifying **Geographical Hotspots** (e.g., a high density of attack origins in a specific region) while ignoring low-density "noise."
- **H3 (Geospatial Indexing):** Developed by Uber, this isn't a "model" in the ML sense, but a hexagonal hierarchical spatial index. It is the gold standard for aggregating global attack data into "bins" for high-performance geospatial rendering.