Model Research for Cyber Threat Visualization

1. Descriptive Statistical Modeling

- Transforms unstructured security logs into analyzable numerical summaries
- Helps establish a baseline understanding of normal vs abnormal activity
- Enables quick comparison between different attack categories
- Reduces data complexity before advanced analysis is applied
- Improves clarity for non-technical and executive stakeholders

2. Time-Series Analysis Model

- Captures short-term and long-term attack behavior patterns
- Helps identify recurring attack windows and seasonal trends
- Supports comparison of current activity against historical baselines
- Assists analysts in correlating attacks with real-world events
- Enables dynamic time-based filtering in the dashboard

3. Statistical Anomaly Detection Model

- Highlights deviations without requiring labeled attack data
- Minimizes false alarms by using historical thresholds
- Allows analysts to investigate anomalies rather than auto-blocking
- Works well with simulated and incomplete datasets
- Enhances situational awareness during sudden threat escalations

4. Hierarchical Threat Modeling

- Structures Complex attack data into meaningful layers
- Improves understanding of relationships between tactics and techniques
- Enables efficient prioritization of frequently exploited techniques
- Aligns well with cybersecurity frameworks such as MITRE ATT&CK
- Simplifies visualization of large and complex threat datasets

5. Geospatial Risk Analysis Model

- Reveals regional concentration of cyber attacks
- Supports identification of high-risk source and target locations
- Enables comparison of threat intensity across different regions
- Improves strategic planning and geo-based security policies
- Enhances visual impact and intuitive understanding for analysts

6. Visual Analytics Model

- Encourages human-in-the-loop analysis rather than blind automation
- Allows interactive exploration instead of static reporting
- Improves decision accuracy through visual context
- Supports drill-down analysis from high-level to detailed views
- Makes complex cybersecurity data accessible and actionable

7. Logistic Regression Risk Model

- Produces probability-based outputs useful for risk estimation
- Serves as a transparent baseline for comparing advanced models
- Helps identify influential features affecting risk scores
- Performs well on smaller and well-structured datasets
- Supports explainable and audit-friendly decision-making

8. Decision Tree Model

- Provides clear, rule-based logic for threat categorization
- Helps analysts understand how feature thresholds influence decisions
- Useful for validating assumptions made by complex models
- Easy to interpret and visualize in decision paths
- Acts as a reference explainability model

9. Random Forest Ensemble Model

- Reduces overfitting compared to single decision trees
- Handles noisy and imbalanced cybersecurity data effectively
- Provides feature importance across multiple decision paths
- Performs reliably across different attack scenarios
- Suitable for benchmarking against gradient boosting models

10. XGBoost Threat Prediction Model

- Handles missing and imbalanced security data efficiently
- Provides high accuracy with optimized training performance
- Supports explainable AI through feature importance and SHAP values
- Produces probabilistic threat scores ideal for dashboards
- Balances prediction performance with real-time usability

11. Neural Network (ANN) Model

- Learns complex non-linear relationships in attack data
- Adapts well to evolving threat patterns
- Performs better when large datasets are available
- Useful for experimental comparison with traditional ML models
- Demonstrates deep learning capabilities in cybersecurity research

12. LSTM Temporal Model

- Captures long-term dependencies in attack sequences
- Helps analyze multi-stage or slow-moving attacks
- Improves understanding of attack progression over time
- Useful for modeling attacker behavior patterns
- Best suited for advanced or future extensions of the system