AI in Cybersecurity - Detect Threats with Machine Learning

Study Plan Overview
- Course Duration: 8 Weeks
- Total Study Hours: Approximately 50 hours (6-7 hours per week)
- Assessment Method: Quizzes, assignments, final project

Week 1: Introduction to Cybersecurity and AI
- Objectives:
- Understand fundamental concepts of cybersecurity and AI
- Explore AI's role in enhancing cybersecurity measures
- Milestones:
- Read introductory materials
- Complete quiz on basic terminology and concepts
- Activities:
- Watch introductory videos on AI and cybersecurity
- Read articles on AI's role in cybersecurity
- Join online forums for discussion

Week 2: Threat Landscape and Types of Cyber Threats
- Objectives:
- Identify types of cyber threats and their characteristics
- Understand threat landscape and AI's role in threat detection
- Milestones:
- Create detailed list of common cyber threats
- Submit assignment on a selected threat type
- Activities:
- Read research papers on current cybersecurity threats
- Review case studies of real-world cyber attacks
- Participate in discussions on AI detection of specific threats

Week 3: Fundamentals of Machine Learning
- Objectives:
- Understand machine learning concepts and algorithms
- Explore supervised, unsupervised, and reinforcement learning
- Milestones:
- Complete tutorials on basic machine learning algorithms
- Take quiz on machine learning concepts
- Activities:
- Watch tutorials explaining machine learning algorithms
- Practice running ML models on platforms like Google Colab
- Discuss importance of data quality in training models

Week 4: Data Collection and Preprocessing
- Objectives:
- Learn importance of data in AI applications
- Understand data collection and preprocessing for machine learning
- Milestones:
- Collect dataset related to cyber threats (e.g., Kaggle, UCI)
- Submit report on preprocessing steps
- Activities:
- Perform data cleaning using Python libraries (Pandas, NumPy)
- Read documentation on data preprocessing best practices
- Share challenges encountered during preprocessing

Week 5: Feature Engineering and Model Selection
- Objectives:
- Understand feature engineering to improve model effectiveness
- Learn model selection for specific problems
- Milestones:
- Create engineered features from dataset
- Complete assignment comparing different threat detection models
- Activities:
- Watch tutorials on feature engineering techniques
- Use Scikit-learn to implement models such as decision trees, random forests
- Discuss model performance and reasons

Week 6: Model Training, Evaluation, and Tuning
- Objectives:
- Learn to train, evaluate, and tune machine learning models
- Understand metrics for assessing model performance
- Milestones:
- Train models and evaluate performance using metrics
- Submit comparison report on model performance
- Activities:
- Implement evaluation techniques like confusion matrix, precision, recall
- Read articles on hyperparameter tuning
- Share insights from model evaluations

Week 7: Deploying AI Models in Cybersecurity
- Objectives:
- Understand AI model deployment in real-world cybersecurity scenarios
- Learn integration of AI within cybersecurity frameworks
- Milestones:
- Create project plan for AI model deployment
- Complete case study on deployed AI system
- Activities:
- Read research papers on AI deployment strategies and frameworks
- Watch masterclasses by industry experts
- Discuss challenges and considerations in AI deployment

Week 8: Ethical Considerations and Future Trends
- Objectives:
- Discuss ethical issues surrounding AI in cybersecurity
- Explore future AI trends and implications for cybersecurity
- Milestones:
- Participate in roundtable on ethical implications
- Submit reflection paper on future AI and cybersecurity trends
- Activities:
- Read articles on ethical AI, bias, responsible deployment
- Engage in discussions on emerging technologies shaping cybersecurity future
- Prepare final project integrating course elements

Final Project: Building a Custom Threat Detection Model
- Project Overview:
- Develop custom AI-based threat detection model using chosen dataset
- Document all stages: data collection, preprocessing, model selection, training, evaluation, ethics
- Submission Requirements:
- Project report (10-15 pages)
- Presentation (10-15 minutes) summarizing findings
- Code repository on GitHub or similar platform

Presented with xmind