CSC 116 Introduction of Cybersecurity

Assignment 4

Notes: Write your answers in a new word document including your team number and members, and share it with our TA Caden before **03/31/2025.** email: crh873@miami.edu.

1. **Why are hospitals often targeted by cyber attackers?**
   - ☐ A. Healthcare data is highly valuable on black markets
   - ☐ B. Hospital systems are often outdated and vulnerable
   - ☐ C. Hospitals have too many staff trained in cybersecurity
   - ☐ D. Cyberattacks can disrupt critical operations like ICU
   - ☐ E. Attackers can easily guess patients' medical conditions
2. **Which behaviors could indicate a suspicious login event in a hospital system?**
   - ☐ A. Login from an unusual location
   - ☐ B. Access from a new device at odd hours
   - ☐ C. Login from a known user at a regular time
   - ☐ D. Login attempts exceeding normal frequency
   - ☐ E. Multiple failed login attempts before success
3. **What are potential AI-based solutions for detecting fake prescriptions?**
   - ☐ A. Using BERT to analyze prescription text
   - ☐ B. Matching prescriptions to patient medical history using AI
   - ☐ C. Detecting typos in medication names manually
   - ☐ D. Comparing against a standard list of approved treatments
   - ☐ E. Training AI models on past fraudulent prescription patterns
4. **What are common types of malicious activity in hospital systems?**
   - ☐ A. Phishing attacks requesting login credentials
   - ☐ B. Unauthorized access to sensitive records
   - ☐ C. Polishing attacks slowly changing data
   - ☐ D. Installation of useful software updates
   - ☐ E. Fake doctor orders submitted digitally
5. **Which methods improve the accuracy and trust in AI security systems?**
   - ☐ A. Human-in-the-loop feedback
   - ☐ B. De-identification of sensitive training data
   - ☐ C. Model training with clean labeled data
   - ☐ D. Random guessing to explore new patterns
   - ☐ E. Regular review and tuning of AI models

Part 2: Short Answer Questions

Instructions: Answer the following briefly in 3-5 sentences each.

6. **Explain how a "poisoning attack" works in a hospital setting and why it's difficult for traditional anomaly detection to catch it.**
7. **Imagine a nurse receives a suspicious email claiming to be from hospital IT support. How can AI help in this situation, and what should the nurse do?**