Hackathon Scenario: "Securing Tomorrow's Healthcare: A Cybersecurity Challenge"

Overview

Welcome to the "MedGuard 360: Hack the Cure!" hackathon, by SMU in collaboration with IMEDRA SPHERE, a leading cybersecurity consulting company. In this intense 12-hour competition, participants will design, build, and secure a cutting-edge healthcare infrastructure. The goal is to ensure robust network security, seamless device integration, and operational efficiency, while crafting a compelling business plan to showcase the viability of their solution.

Scenario

You are a team of cybersecurity engineers at IMEDRA SPHERE tasked by a fictional healthcare organization, **MedSecure Hospitals**, to design and secure their state-of-the-art healthcare facility. This facility heavily relies on connected medical devices, AI-powered tools, and advanced robotics to deliver world-class patient care. However, as technology expands, so do the threats. Your mission is to ensure this interconnected system is impenetrable, compliant with regulations, and resilient against evolving cyber threats.

Infrastructure Components

You will need to integrate and secure the following components:

1. **Life-Saving Equipment**
    - 5 integrated respirators and scopes.
    - 6 ECG machines with AI defibrillator functions.
    - 10 AI-enabled ultrasounds for preliminary reports.
2. **Advanced Diagnostics**
    - 2 scanners (CT) and 1 integrated MRI/PET scanner with AI.
3. **Patient Support**
    - 12 robots for temperature and heart rate monitoring.
    - 2 rehabilitation robots with augmented reality.
4. **Assistive Technology**
    - 34 connected patient-support equipment (PSE).
    - 12 smart glasses with AI for symptom and syndrome filtering.
5. **Administrative and Support Systems**
    - 24 tablets for patient record management and registration.

- 12 connected printers.
- 12 control and biology station computers.

6. **Innovative Tools**
    - 1 3D printer for prosthetic manufacturing.

Objectives

1. **Design a Secure Network Architecture**
    - Create a network topology ensuring secure device communication.
    - Implement Network Security systems and mechanisms.
    - Secure IoT devices and segregate critical systems from non-essential networks.
2. **Develop a Robust Security Plan**
    - Address vulnerabilities in AI-powered and connected devices.
    - Propose encryption and authentication mechanisms for all endpoints.
    - Include proactive monitoring and threat detection strategies.
3. **Craft a Business Plan**
    - Justify the cost-effectiveness of your solution.
    - Highlight ROI for MedSecure Hospitals.
    - Align the solution with healthcare compliance standards (e.g., HIPAA, GDPR).
4. **Prepare for Incident Response**
    - Create a plan for detecting, responding to, and recovering from cyber incidents.
5. **Showcase Scalability**
    - Ensure the infrastructure can expand as the hospital grows.

Deliverables (Should be Presented in one PDF Document MAX 2 without Presentation)

- **Network Diagram**: Visually represent your secure infrastructure.
- **Security Plan**: Detailed steps taken to secure each device and subsystem.
- **Incident Response Plan**: A strategy for cyberattack mitigation and recovery.
- **Business Plan**: Persuasive documentation to gain buy-in from stakeholders.
- **Presentation**: A 10-minute pitch to the judges explaining your solution.