SMART HOSPITAL SECURITY

Cybersecurity Risk Analysis, Penetration Testing & Defense Design

Faculty of Artificial Intelligence
Cybersecurity

Table of Contents

Executive Summary

This project presents a comprehensive cybersecurity assessment of a smart hospital environment. With the increasing reliance on digital systems, medical devices, and interconnected networks, hospitals have become highly attractive targets for cyber attacks.

The objective of this project is to identify critical hospital assets, assess their risk levels, simulate realistic cyber attacks, and propose effective security controls. The assessment includes both offensive security techniques through penetration testing and defensive strategies using Security Operations Center (SOC) principles and Active Directory policies.

The results highlight several high-risk and critical assets that require immediate security controls to ensure patient safety, data confidentiality, and business continuity.

Hospital Overview

The assessed environment represents a modern smart hospital that relies heavily on digital technologies to manage patient care, administrative operations, and emergency services. The hospital utilizes Electronic Medical Records (EMR), Internet of Things (IoT) medical devices, mobile and web applications, and internal networks to ensure efficient healthcare delivery.

Due to the sensitive nature of medical data and the critical role of hospital systems, cybersecurity is considered a fundamental requirement. Any compromise could lead to data breaches, financial losses, service disruption, or even risk to human lives.

Departments & Roles

The hospital consists of several departments, each responsible for specific operational and technical functions. Understanding these roles is essential for identifying potential security risks and asset ownership.

Department	Description
Human Resources (HR)	Manages employee recruitment and personal data
IT & Cybersecurity	Responsible for infrastructure, networks, and security
Medical Labs	Handles laboratory machines and test results
Emergency Department	Manages critical patient care and emergency services
Medical Records (EMR)	Stores and manages patient medical data
Patient App Team	Doctors and nurses interacting with patient systems
Finance	Manages billing, payments, and financial records

Asset Identification

The following assets were identified as key components of the hospital's digital infrastructure. These assets store, process, or transmit sensitive information and therefore require appropriate security controls.

Asset	Description
EMR Server	Stores electronic medical records of patients
PACS Server	Stores and manages radiology images
IoT Patient Monitors	Monitor patient vital signs
Biometric Access System	Controls physical access to hospital areas
Doctors' Laptops	Used for patient diagnosis and reporting
Patient Database	Centralized repository for patient data
Mobile / Web Application	Enables patient and staff interaction
Hospital WiFi Network	Provides internal and guest connectivity
Ambulance GPS System	Tracks emergency vehicles
Backup Server	Stores data backups for disaster recovery

Asset Ownership Mapping

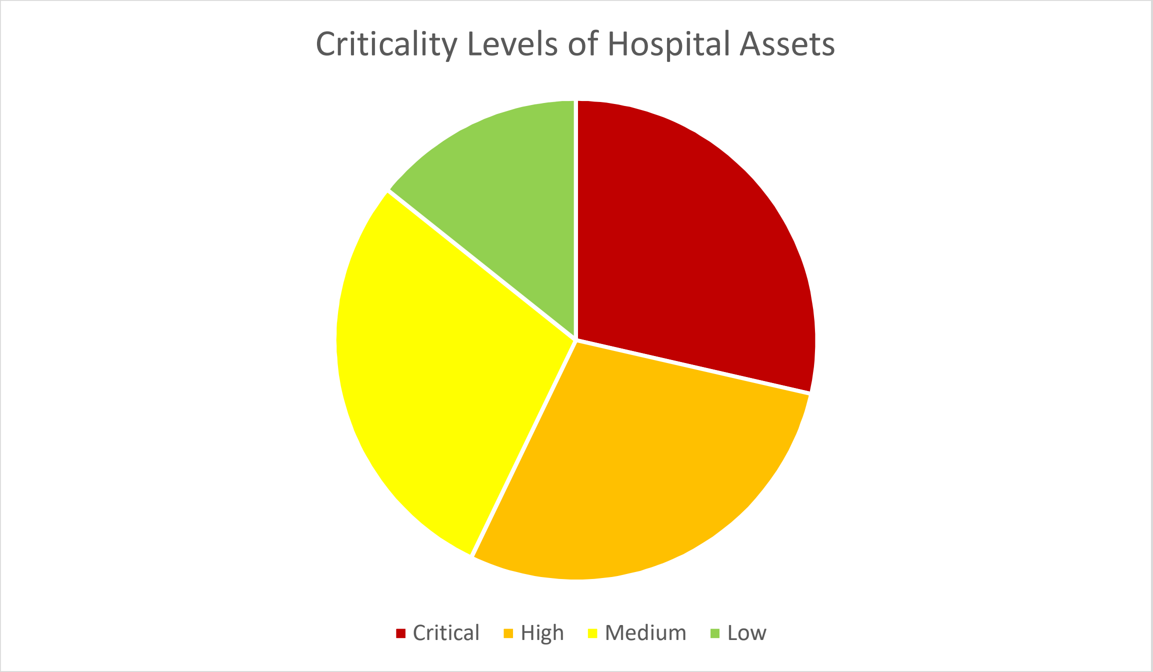
Each department is responsible for managing specific assets. Mapping asset ownership helps identify accountability and potential attack surfaces.

Assets	Department
HR	HR PCs, Emails, Employee Data
IT & Cybersecurity	Active Directory, Backups, Switches, Firewalls
EMR Department	EMR Database, PACS Server
Medical Labs	Laboratory Machines
Emergency Department	IoT Monitors, Ambulance GPS
Finance	POS Systems, Billing System

Risk & Criticality Assessment

To prioritize security efforts, each asset was evaluated based on its impact on confidentiality, integrity, and availability. Assets were classified into four categories: Critical, High, Medium, and Low.

Asset	Criticality
EMR Database	Critical
IoT Patient Monitors	Critical
Doctor Emails	High
Finance POS System	High
HR PCs	Medium
Hospital Website	Medium
Guest WiFi Network	Low



Threat Modeling & Attack Scenarios

Potential attack scenarios were analyzed by adopting an attacker's perspective to identify weaknesses in hospital systems.

Phishing Attack

- **Target:** HR employee
- **Weakness:** Lack of security awareness
- **Impact:** Credential theft and unauthorized access

Weak Password Attack

- **Target:** Internal hospital systems
- **Weakness:** Poor password policies
- **Impact:** Account compromise and lateral movement

ARP Spoofing Attack

- **Target:** IoT patient monitoring devices
- **Weakness:** Lack of network segmentation
- **Impact:** Data interception and device manipulation

SQL Injection Attack

- **Target:** Hospital website and database
- **Weakness:** Insufficient input validation
- **Impact:** Unauthorized database access and data leakage

These attacks were demonstrated practically in a controlled environment for educational purposes.

Note:
These are the links to the applied attacks :

ARP Spoofing Attack & Brute Force

https://drive.google.com/drive/folders/1SulRuIUk2FCgAhMjbSSa5uBbJvBp0bji

SQL Injection Attack & Spear phishing

https://drive.google.com/drive/folders/1JRRA314VT8MjlNBu7PtJz9GuLahBitUH?usp=sharing

Mitigation & Security Recommendations

Based on the identified threats, the following security measures are recommended to reduce risks and improve the hospital's security posture.

Phishing Mitigation

- Security awareness training
- Email filtering solutions
- Multi-factor authentication (MFA)

Password Security

- Strong password policies
- Account lockout mechanisms
- Regular credential audits

Network Security

- Network segmentation
- Secure communication protocols
- Intrusion Detection Systems (IDS)

Application Security

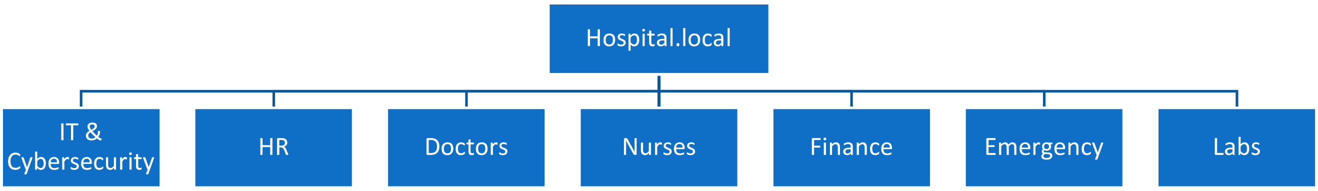
- Secure coding practices
- Input validation
- Regular vulnerability assessments

SOC & Active Directory Design

To enhance detection and response capabilities, a basic Security Operations Center (SOC) model was proposed. The SOC is responsible for monitoring system logs, detecting suspicious activity, and responding to security incidents.

The Active Directory (AD) environment is structured using Organizational Units (OUs) based on hospital departments. Group Policies are applied to enforce password policies, restrict unauthorized device usage, and improve endpoint security.

This centralized approach enables better visibility, access control, and incident response.



The organizational hierarchy illustrated above reflects the logical design of the hospital's Active Directory environment. Each department is assigned a dedicated Organizational Unit (OU), allowing security controls to be applied based on operational roles and data sensitivity.

This structure supports the SOC by enabling centralized monitoring, simplified incident investigation, and faster response to security events affecting specific departments.

Active Directory Hierarchical Structure

The hierarchical OU design improves administrative control and limits the spread of security incidents across the network.

Security Visibility and Incident Response

By combining SOC monitoring with a structured Active Directory design, the hospital achieves improved visibility over user activities, system access, and potential threats. This integration allows quicker detection of anomalies and more effective incident response.

Conclusion

This project demonstrates the importance of a structured cybersecurity approach in smart hospital environments. By identifying critical assets, evaluating risks, simulating realistic attacks, and proposing defensive strategies, the hospital's security posture can be significantly improved.

Implementing the recommended security controls will help protect sensitive medical data, ensure system availability, and enhance patient safety.