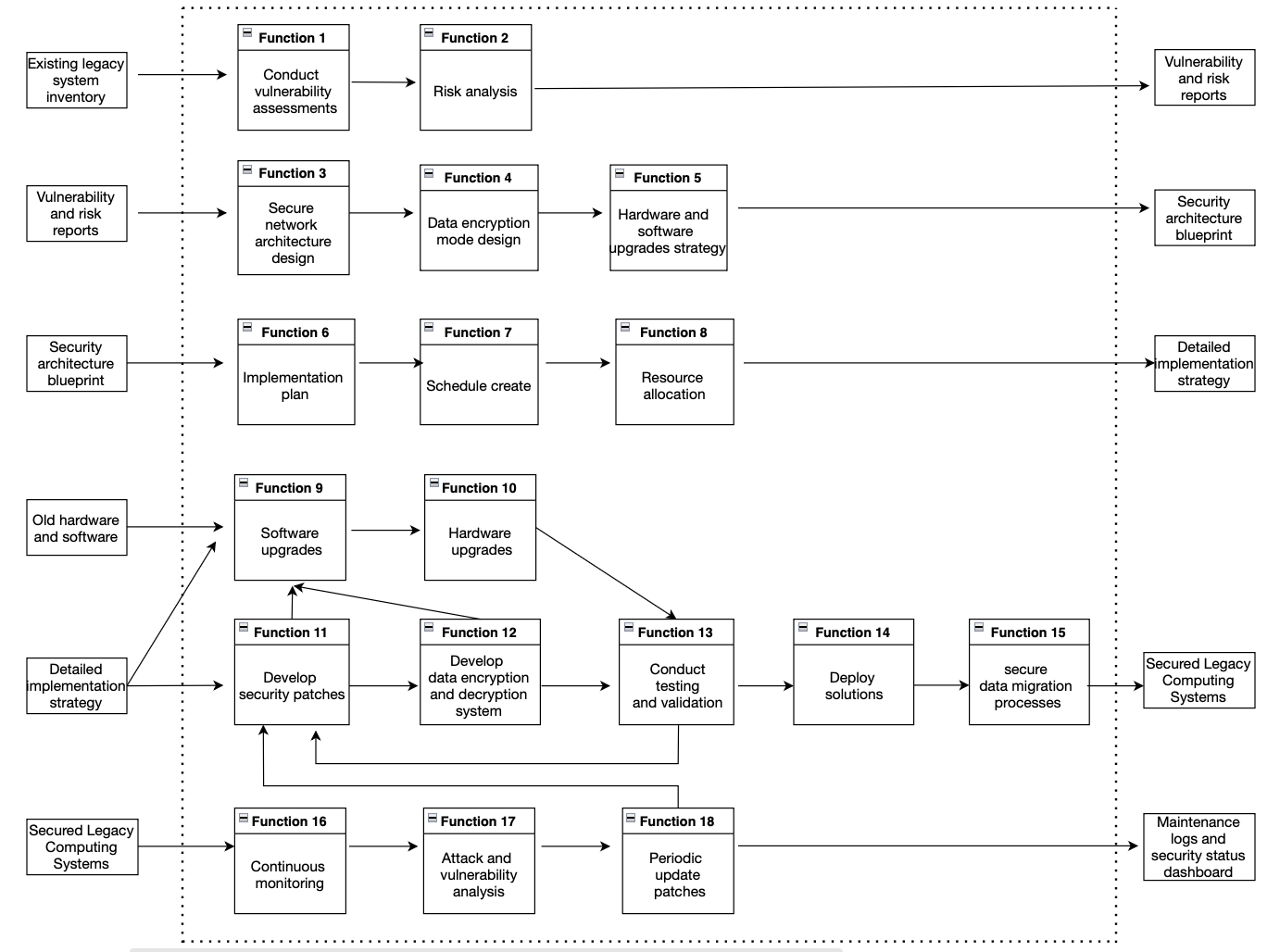
# ***Summary***

# ***Stakeholders / Requirements***

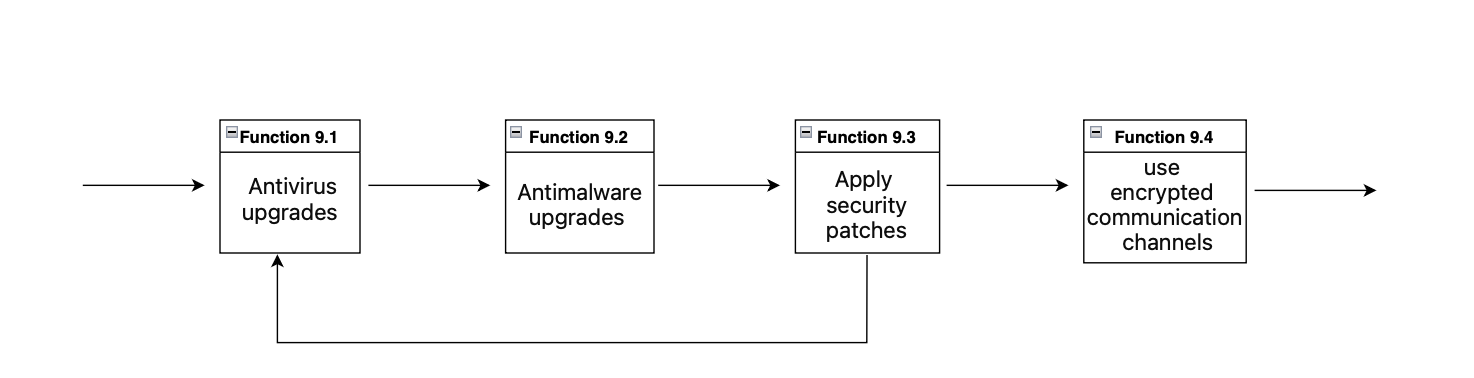
# ***FFBD***

## ***First-Level:***

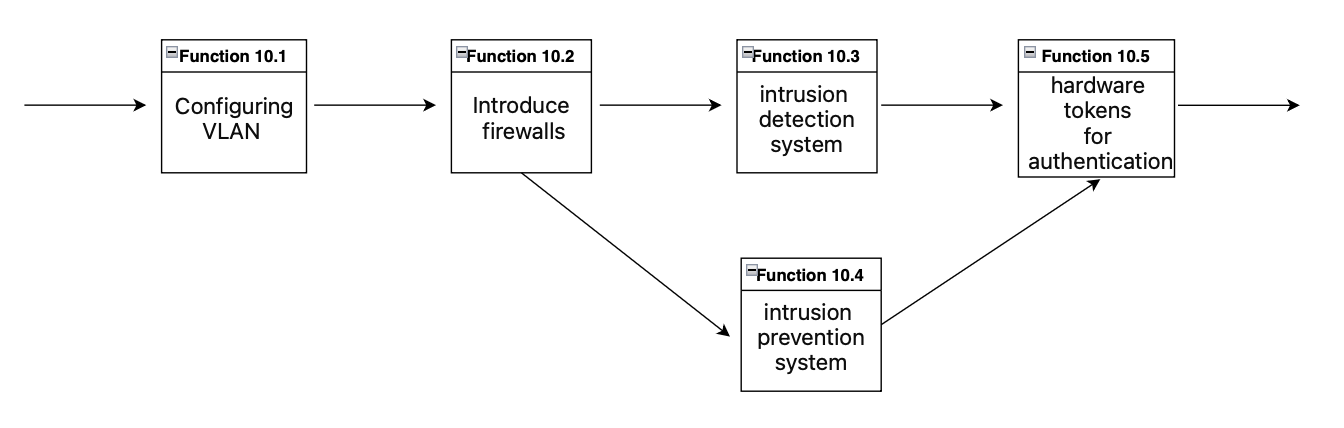
*How *

|  |  |  |
| --- | --- | --- |
| *Function No.* | *Function Description* | *Notes* |
| *Function 1* | *Conduct vulnerability assessments* | *Comprehensive review of legacy systems to identify potential security vulnerabilities.* |
| *Function 2* | *Perform risk analysis* | *Assess risks that could threaten system security.* |
| *Function 3* | *Design secure network architecture* | *Build an enhanced network structure that can withstand cyber threats.* |
| *Function 4* | *Design data encryption modes* | *Create encryption schemes to protect sensitive data transmission and storage.* |
| *Function 5* | *Devise hardware and software upgrades strategy* | *Plan how to upgrade old hardware and software to improve overall security.* |
| *Function 6* | *Create implementation plan* | *Determine the timeline and resources required for implementing security measures.* |
| *Function 7* | *Create schedule* | *Arrange detailed scheduling for the deployment of the security system.* |
| *Function 8* | *Allocate resources* | *Allocate the necessary personnel and technical resources for security upgrades.* |
| *Function 9* | *Software upgrades* | *Update the software of legacy systems to patch security vulnerabilities.* |
| *Function 10* | *Hardware upgrades* | *Replace or enhance hardware components of legacy computing systems to support new security measures.* |
| *Function 11* | *Develop security patches* | *Create software patches specifically for identified vulnerabilities.* |
| *Function 12* | *Develop data encryption and decryption system* | *Implement encryption to secure data during transmission and storage.* |
| *Function 13* | *Conduct testing and validation* | *Ensure that newly deployed security measures and upgrades do not disrupt hospital operations.* |
| *Function 14* | *Deploy solutions* | *Implement the new security architecture and protocols in the hospital's legacy systems.* |
| *Function 15* | *Secure data migration processes* | *Ensure facts isn't always exposed or corrupted all through migration to updated structures.* |
| *Function 16* | *Continuous monitoring* | *Continuously screen legacy systems for protection threats and manage them in actual-time..* |
| *Function 17* | *Perform attack and vulnerability analysis* | *Regularly assess the system for new security threats and vulnerabilities.* |
| *Function 18* | *Periodic update patches* | *Regularly update security patches to address emerging security risks.* |

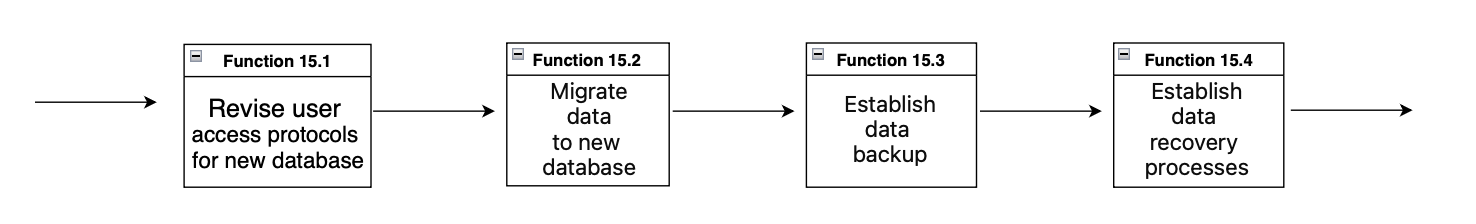
## *Second-Level:*

**

|  |  |  |
| --- | --- | --- |
| *Function No.* | *Function Description* | *Notes* |
| *Function 9.1* | *Antivirus upgrades* | *Upgrading antivirus software program involves no longer best updating virus definitions but additionally improving heuristic analysis and conduct-based totally detection capabilities to combat evolving malware threats efficaciously.* |
| *Function 9.2* | *Antimalware upgrades* | *Updating antimalware software guarantees that the ultra-modern kinds of malware, such as ransomware and spyware, are recognized and blocked, thinking of the modern danger intelligence and advanced detection algorithms.* |
| *Function 9.3* | *Apply security patches* | *Applying security patches is vital for closing vulnerabilities that might be exploited by way of attackers. This system includes patch control regulations to make sure timely updates to all systems and programs.* |
| *Function 9.4* | *Use encrypted communication channels* | *Establishing encrypted communication channels entails imposing protocols such as SSL/TLS for secure net traffic, VPNs for faraway connections, and end-to-give up encryption for touchy communications to shield information from eavesdropping and guy-in-the-middle assaults.* |

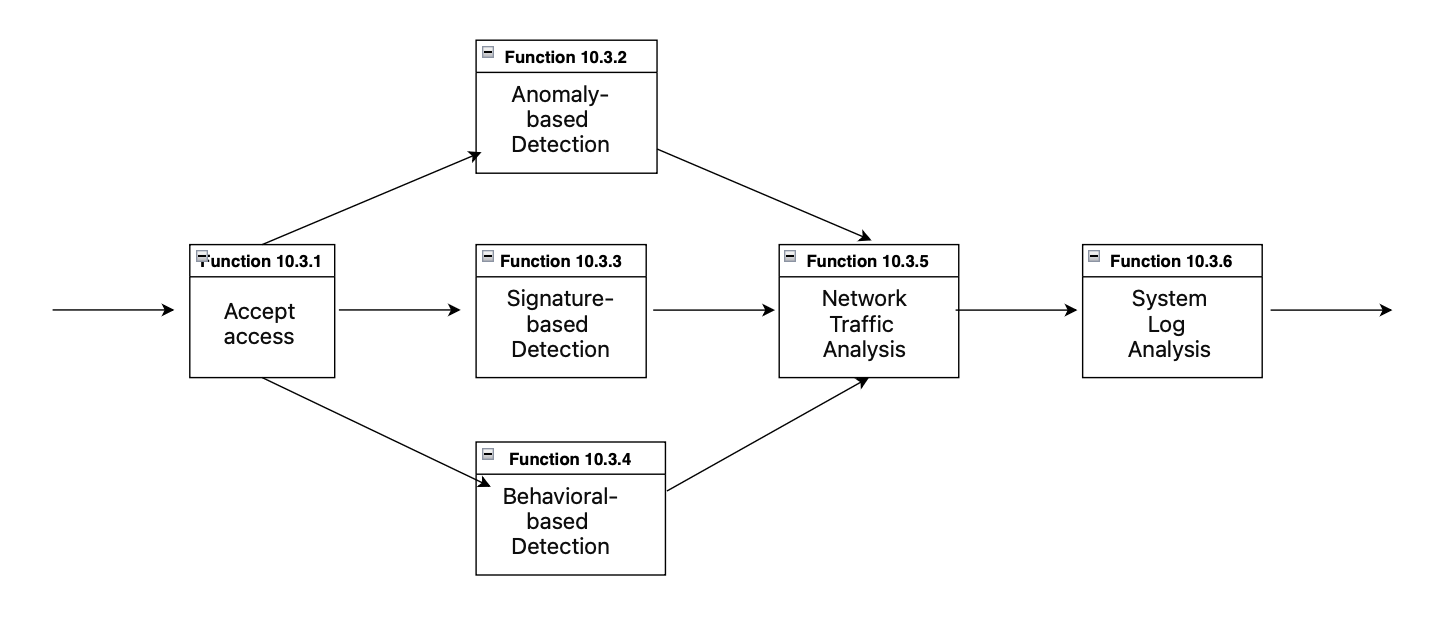
**

|  |  |  |
| --- | --- | --- |
| *Function No.* | *Function Description* | *Notes* |
| *Function 10.1* | *Configuring VLAN* | *Virtual Local Area Network (VLAN) configuration segregates community site visitors, enhancing protection by isolating touchy regions of the network. It requires setting up VLAN IDs and assigning them to an appropriate ports on switches, and probably reconfiguring network structure to support VLAN routing.* |
| *Function 10.2* | *Introduce firewalls* | *The creation of firewalls involves deploying hardware or software program-primarily based firewalls to create a barrier between secure inner networks and untrusted outside networks. Firewall policies want to be defined to govern traffic primarily based on the level of believe, protocols, ports, and IP addresses.* |
| *Function 10.3* | *Intrusion detection system (IDS)* | *Implementing an IDS calls for installing structures that reveal community and gadget activities for malicious activities or policy violations. This ought to involve setting up community-primarily based IDS (NIDS) for network site visitors analysis or host-based IDS (HIDS) for man or woman system tracking.* |
| *Function 10.4* | *Intrusion prevention system (IPS)* | *Intrusion prevention structures are proactive safety answers that now not most effective stumble on capability threats but also take movement to dam them. Deploying an IPS entails putting it inline with community site visitors, configuring regulations for hazard prevention, and integrating it with current protection infrastructure.* |
| *Function 10.5* | *Hardware tokens for authentication* | *Utilizing hardware tokens introduces a physical detail to the authentication process, which can be biometric devices or protection tokens. This step includes distributing tokens to legal personnel, integrating them with the authentication system, and training users on their operation.* |

**

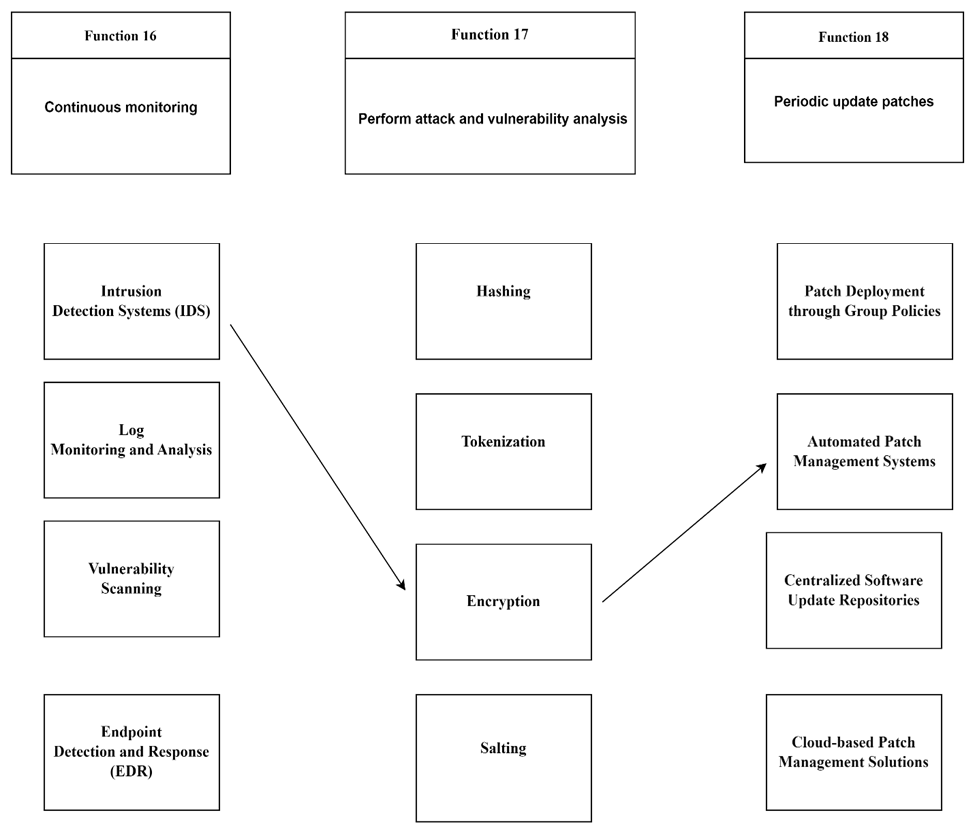
|  |  |  |
| --- | --- | --- |
| *Function No.* | *Function Description* | *Notes* |
| *Function 15.1* | *Revise user access protocols for new database* | *Revising user access protocols involves assessing current security policies, determining necessary updates, and redefining user permissions and authentication methods for the new database environment. This includes the establishment of roles, privileges, and auditing controls to comply with data protection regulations.* |
| *Function 15.2* | *Migrate data to new database* | *Data migration requires careful planning to ensure data integrity and availability. This process typically includes data mapping, cleansing, and the actual transfer while minimizing downtime. Verification and validation post-migration are crucial to confirm the data's integrity.* |
| *Function 15.3* | *Establish data backup* | *Establishing a data backup strategy involves selecting appropriate backup methods (full, incremental, differential), scheduling the backup jobs, and securing backup storage locations, whether on-premises or cloud-based, to ensure data redundancy and quick recovery in case of data loss.* |
| *Function 15.4* | *Establish data recovery processes* | *Creating data recovery processes entails developing a comprehensive plan to restore systems and data in the event of data corruption or loss. This includes the establishment of recovery objectives, testing recovery procedures, and maintaining recovery tools and environments.* |

## ***Third-Level:***

**

|  |  |  |
| --- | --- | --- |
| *Function No.* | *Function Description* | *Notes* |
| *Function 10.3.1* | *Accept access* | *Refers to the initial step of allowing network traffic to be assessed by the intrusion detection system. This could include authenticating access credentials or simply beginning the monitoring process for incoming traffic.* |
| *Function 10.3.2* | *Anomaly-based Detection* | *This characteristic entails studying community behavior towards a baseline of what is considered regular. Any deviations from this baseline might also indicate capacity protection incidents, prompting further research or computerized responses.* |
| *Function 10.3.3* | *Signature-based Detection* | *Signature-based detection is based on a database of known danger signatures. It fits found activities towards this database to become aware of and flag recognized malicious patterns, making it a vital part of any IDS.* |
| *Function 10.3.4* | *Behavioral-based Detection* | *Goes past signatures with the aid of analyzing the conduct of customers and community entities. It uses heuristics and algorithms to hit upon unusual pastime that could advocate a security risk, even supposing that threat hasn't been previously diagnosed.* |
| *Function 10.3.5* | *Network Traffic Analysis* | *Entails a radical examination of incoming and outgoing network statistics packets. It seems for suspicious styles, uncommon data flows, or different indicators of potential compromise.* |
| *Function 10.3.6* | *System Log Analysis* | *This project analyzes device logs for signs of unauthorized access attempts, system configuration changes, or various abnormalities that could compliment cybersecurity which is violated.* |

## ***Concept:***

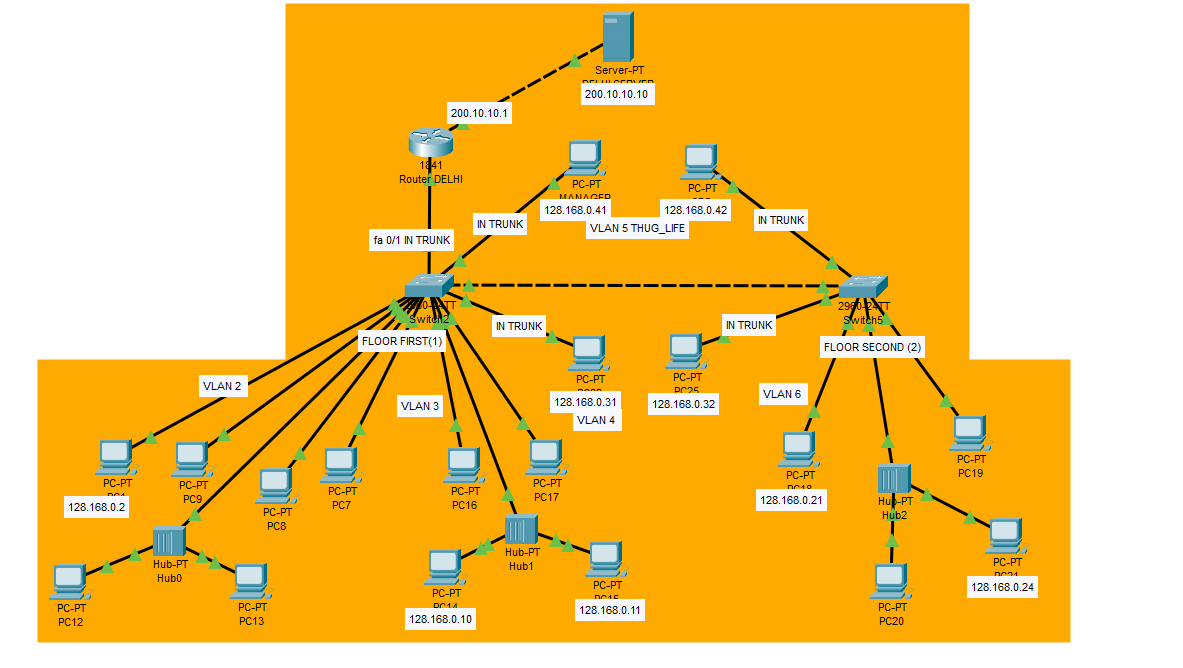
**

# ***System Structure / Subsystem Baseline***

*Device architecture proposed to enhance cybersecurity in hospital legacy systems follows a layered approach, commonly referred to as a "defense in depth" architecture This design uses multiple types of security controls for protection away from threats and provide redundancy in case of a layer breach:*

## ***1. Network Security:***

* *Firewalls: These gateways switch website visitors between internal and external networks, control access, and prevent unauthorized access.*
* *Intrusion Detection and Prevention Systems (IDS/IPS): Provides constant vigilance, systems that reflect local and machine gaming activity, all at once to detect and activate power threats.*
* *Encrypted Communication Channels: Using encryption protocols such as SSL/TLS and VPNs, tactile information flowing locally remains masked to the eyes of analysts.*
* *VLAN Configuration: Network website online traffic isolation enhances security, prevents unauthorized get access and monitors potential rules.*

**

## ***2. Data Security:***

* *Data Encryption and Decryption: Sensitive information is indecipherable through both transmission and storage for unauthorized information, protecting privacy.*
* *Data backup and recovery: Robust backup strategies ensure data resilience, allowing for rapid recovery in the event of data loss or corruption.*
* *User access control: Granular access controls manage database access, reduce the threat of account breaches and ensure security compliance.*

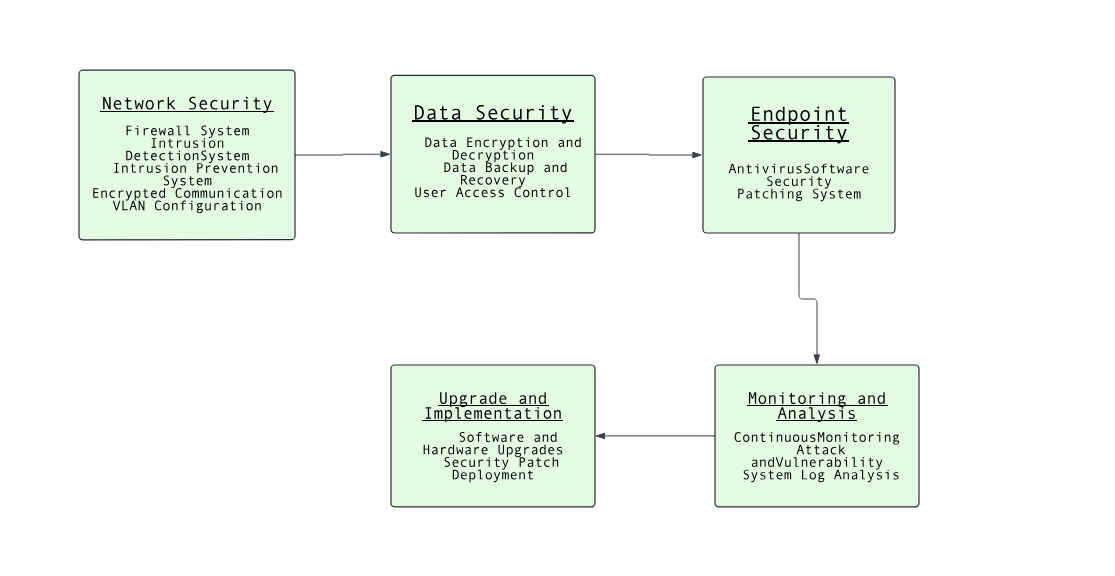
## ***3. Endpoint Security:***

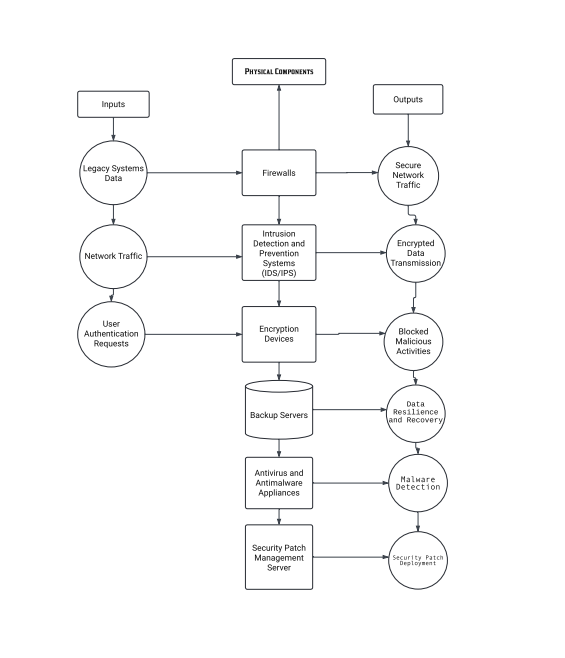
* *Antivirus software: Constantly updating antivirus solutions gives them a competitive edge against malware threats, and fear and stop them from doing anything before they wreak havoc.*
* *Security patching system: During security patches, software coast vulnerabilities in software and hardware, and strengthen endpoint defenses.*

## ***4. Monitoring and Analysis:***

* *Continuous monitoring: Real-time analysis of environmental and device activity can quickly detect and respond to security incidents.*
* *Attack and Risk Analysis: Routine testing identifies growing threats and vulnerabilities, and identifies countermeasures.*
* *System log analysis: Parsing equipment logs for anomalous gaming activities identifies power security violations and correctly addresses them.*

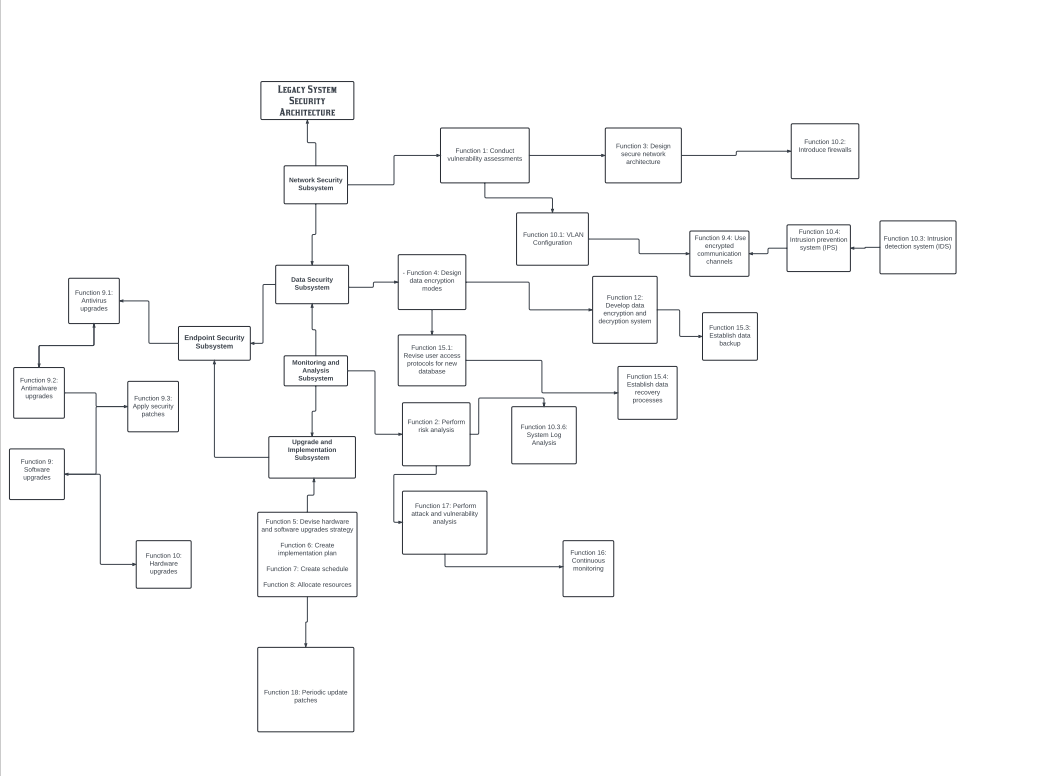
## ***5. Upgrade and Implementation:***

* *Updated software and hardware: Legacy systems are strengthened through upgrades, ensuring resilience to evolving threats.*
* *Security patch application: Regular application of security patches strengthens systems, reducing the window of vulnerability to cyber threats.  
    
  *

***Based on the requirements, I have created a physical design diagram for the first layer of the FFBD.******Physical Design Diagram for the First Layer of FFBD:*** **

***[Hospital Legacy Systems Cybersecurity Reinforcement - First Layer Diagram](https://i.imgur.com/Q2V7Q7X.png" \t "https://www.blackbox.ai/_blank)***

*This diagram illustrates the relationship between the first-level functions and the subsystems in the context of the Defense in Depth architecture. Each subsystem plays a crucial role in securing the hospital's legacy systems against cybersecurity threats, encompassing network, data, endpoint, monitoring, and upgrade elements.*

***First-Level Function Allocation to Subsystems:****I have allocated each function in the first layer of the Function Flow Block Diagram (FFBD) to a corresponding subsystem.*

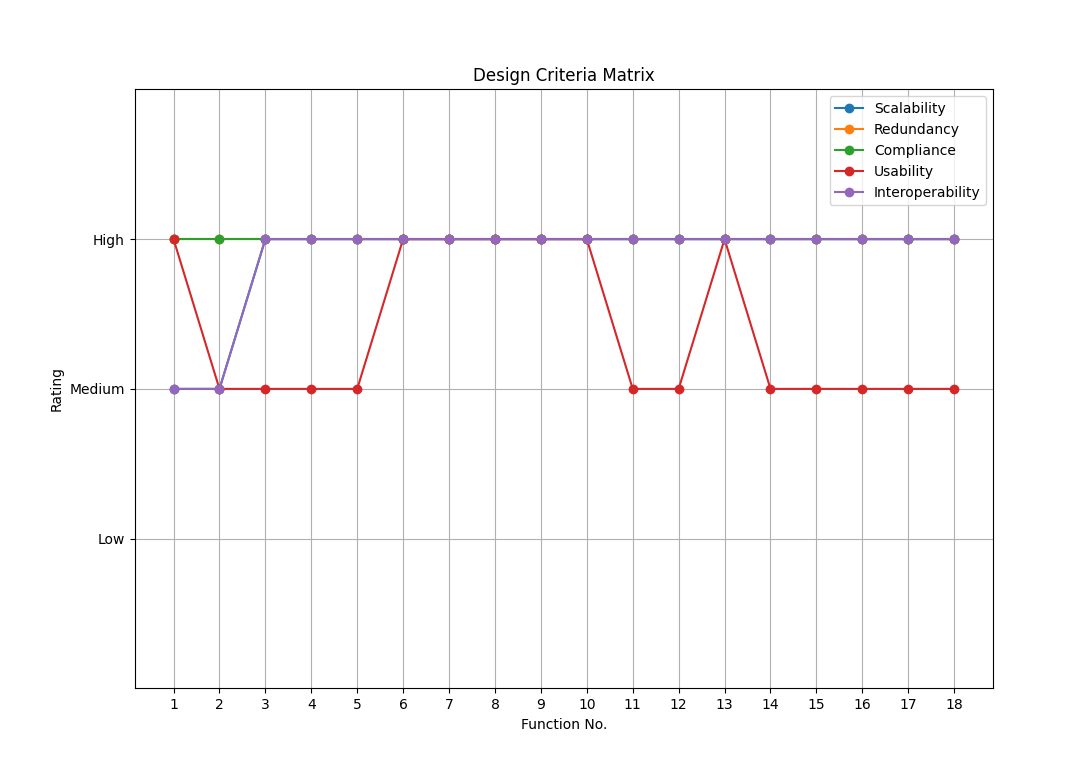
| *Function No.* | *Function Description* | *Subsystem* |
| --- | --- | --- |
| *Function 1* | *Conduct vulnerability assessments* | *Network Security* |
| *Function 2* | *Perform risk analysis* | *Monitoring and Analysis* |
| *Function 3* | *Design secure network architecture* | *Network Security* |
| *Function 4* | *Design data encryption modes* | *Data Security* |
| *Function 5* | *Devise hardware and software upgrades strategy* | *Upgrade and Implementation* |
| *Function 6* | *Create implementation plan* | *Upgrade and Implementation* |
| *Function 7* | *Create schedule* | *Upgrade and Implementation* |
| *Function 8* | *Allocate resources* | *Upgrade and Implementation* |
| *Function 9* | *Software upgrades* | *Endpoint Security* |
| *Function 10* | *Hardware upgrades* | *Endpoint Security* |
| *Function 11* | *Develop security patches* | *Upgrade and Implementation* |
| *Function 12* | *Develop data encryption and decryption system* | *Data Security* |
| *Function 13* | *Conduct testing and validation* | *Network Security, Data Security, Endpoint Security, Monitoring and Analysis* |
| *Function 14* | *Deploy solutions* | *Network Security, Data Security, Endpoint Security* |
| *Function 15* | *Secure data migration processes* | *Data Security* |
| *Function 16* | *Continuous monitoring* | *Monitoring and Analysis* |
| *Function 17* | *Perform attack and vulnerability analysis* | *Monitoring and Analysis* |
| *Function 18* | *Periodic update patches* | *Upgrade and Implementation* |

***Design Criteria and Performance Measures Matrices***

***Design Criteria Matrix****:*

| *Function No.* | *Function Description* | *Scalability* | *Redundancy* | *Compliance* | *Usability* | *Interoperability* |
| --- | --- | --- | --- | --- | --- | --- |
| *1* | *Conduct vulnerability assessments* | *Medium* | *High* | *High* | *High* | *Medium* |
| *2* | *Perform risk analysis* | *Medium* | *High* | *High* | *Medium* | *Medium* |
| *3* | *Design secure network architecture* | *High* | *High* | *High* | *Medium* | *High* |
| *4* | *Design data encryption modes* | *High* | *High* | *High* | *Medium* | *High* |
| *5* | *Devise hardware and software upgrades* | *High* | *High* | *High* | *Medium* | *High* |
| *6* | *Create implementation plan* | *High* | *High* | *High* | *High* | *High* |
| *7* | *Create schedule* | *High* | *High* | *High* | *High* | *High* |
| *8* | *Allocate resources* | *High* | *High* | *High* | *High* | *High* |
| *9* | *Software upgrades* | *High* | *High* | *High* | *High* | *High* |
| *10* | *Hardware upgrades* | *High* | *High* | *High* | *High* | *High* |
| *11* | *Develop security patches* | *High* | *High* | *High* | *Medium* | *High* |
| *12* | *Develop data encryption and decryption* | *High* | *High* | *High* | *Medium* | *High* |
| *13* | *Conduct testing and validation* | *High* | *High* | *High* | *High* | *High* |
| *14* | *Deploy solutions* | *High* | *High* | *High* | *Medium* | *High* |
| *15* | *Secure data migration processes* | *High* | *High* | *High* | *Medium* | *High* |
| *16* | *Continuous monitoring* | *High* | *High* | *High* | *Medium* | *High* |
| *17* | *Perform attack and vulnerability analysis* | *High* | *High* | *High* | *Medium* | *High* |
| *18* | *Periodic update patches* | *High* | *High* | *High* | *Medium* | *High* |

*This matrix evaluates each function in opposition to the design criteria to make sure they align with the overall dreams of the cybersecurity reinforcement plan.*

** ***Performance Measures Matrix:***

*This matrix evaluates the performance measures for every function to make sure that each feature meets the specified standards of performance.*

| *Function No.* | *Function Description* | *Detection Rate* | *Response Time* | *System Uptime* | *Data Integrity* | *User Satisfaction* |
| --- | --- | --- | --- | --- | --- | --- |
| *1* | *Conduct vulnerability assessments* | *High* | *High* | *High* | *High* | *Medium* |
| *2* | *Perform risk analysis* | *High* | *High* | *High* | *High* | *Medium* |
| *3* | *Design secure network architecture* | *High* | *Medium* | *High* | *High* | *Medium* |
| *4* | *Design data encryption modes* | *High* | *Medium* | *High* | *High* | *Medium* |
| *5* | *Devise hardware and software upgrades* | *High* | *Medium* | *High* | *High* | *Medium* |
| *6* | *Create implementation plan* | *High* | *High* | *High* | *High* | *High* |
| *7* | *Create schedule* | *High* | *High* | *High* | *High* | *High* |
| *8* | *Allocate resources* | *High* | *High* | *High* | *High* | *High* |
| *9* | *Software upgrades* | *High* | *Medium* | *High* | *High* | *High* |
| *10* | *Hardware upgrades* | *High* | *Medium* | *High* | *High* | *High* |
| *11* | *Develop security patches* | *High* | *Medium* | *High* | *High* | *Medium* |
| *12* | *Develop data encryption and decryption* | *High* | *Medium* | *High* | *High* | *Medium* |
| *13* | *Conduct testing and validation* | *High* | *High* | *High* | *High* | *High* |
| *14* | *Deploy solutions* | *High* | *Medium* | *High* | *High* | *Medium* |
| *15* | *Secure data migration processes* | *High* | *Medium* | *High* | *High* | *Medium* |
| *16* | *Continuous monitoring* | *High* | *High* | *High* | *High* | *Medium* |
| *17* | *Perform attack and vulnerability analysis* | *High* | *Medium* | *High* | *High* | *Medium* |
| *18* | *Periodic update patches* | *High* | *Medium* | *High* | *High* | *Medium* |

# ***Key:***

# *High: The feature completely meets or exceeds the criterion/degree.*

# *Medium: The feature partially meets the criterion/degree.*

# *Low: The characteristic does now not effectively meet the criterion/degree.*

# ***Interpretation:***

# *From the matrices, it's miles clean that each one capabilities are designed to fulfill high standards of scalability, redundancy, compliance, and interoperability. The usability of some features, including those related to network structure and statistics encryption, may additionally need further optimization to make certain they do no longer disrupt hospital operations.*

# *The overall performance measures indicate that maximum features are notably effective in terms of detection price, reaction time, machine uptime, and information integrity. User satisfaction is generally high, specifically for functions that directly contain the IT department and health facility body of workers in planning and aid allocation. However, user delight for technical implementations (e.G., encryption and migration approaches) is mild and might be advanced with better consumer training and assist.*

# ***Conclusion:***

# *By the usage of these matrices, we can ensure that each function inside the cybersecurity reinforcement plan is thoroughly evaluated in opposition to key design standards and overall performance measures. This complete evaluation enables in optimizing the general safety strategy and making sure that the clinic’s legacy systems are robustly covered in opposition to cyber threats.* ***References***

*National Institute of Standards and Technology. (2018). NIST Cybersecurity Framework Version 1.1. [Online] Available at: [https://www.nist.gov/publications/nist-cybersecurity-framework](https://www.nist.gov/publications/nist-cybersecurity-framework" \t "https://chat.openai.com/c/_new) .*

*Pfleeger, C. P., and Pfleeger, S. L. (2012). Security in Computing (4th ed.). Prentice Hall.*

*Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and McQuaid, R., 2019. Developing cyber resilient systems: a systems security engineering approach (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology.*

*Vacca, J. R. (2013). Computer and Information Security Handbook (2nd ed.). Morgan Kaufmann.*

*Whitman, M. E., Mattord, H. J.,and Green, A. (2014). Principles of Information Security (5th ed.). Cengage Learning.*