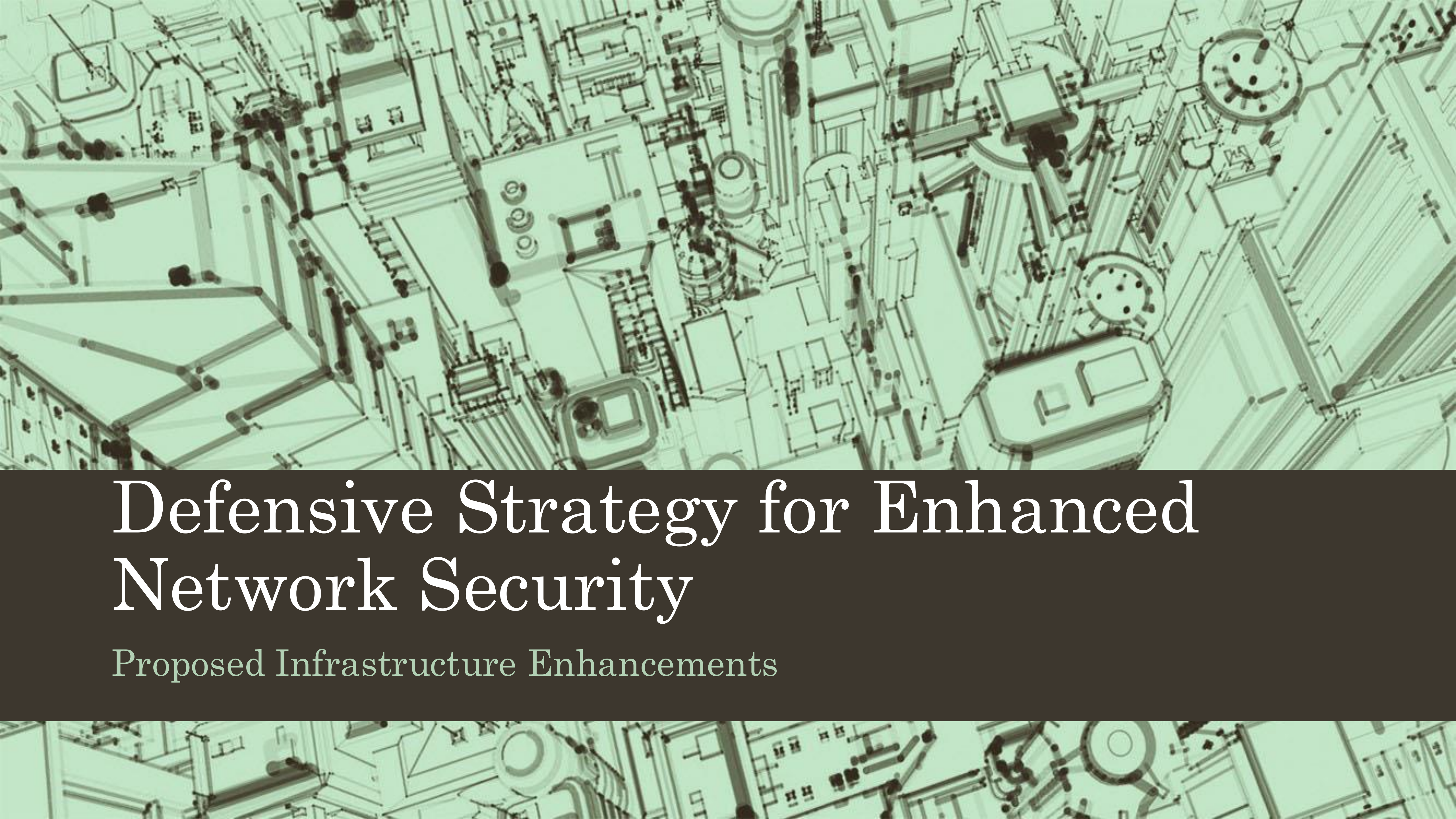


Defensive Strategy for Enhanced Network Security

Proposed Infrastructure Enhancements

Itinerary

Current Network Architecture

Target Network Architecture

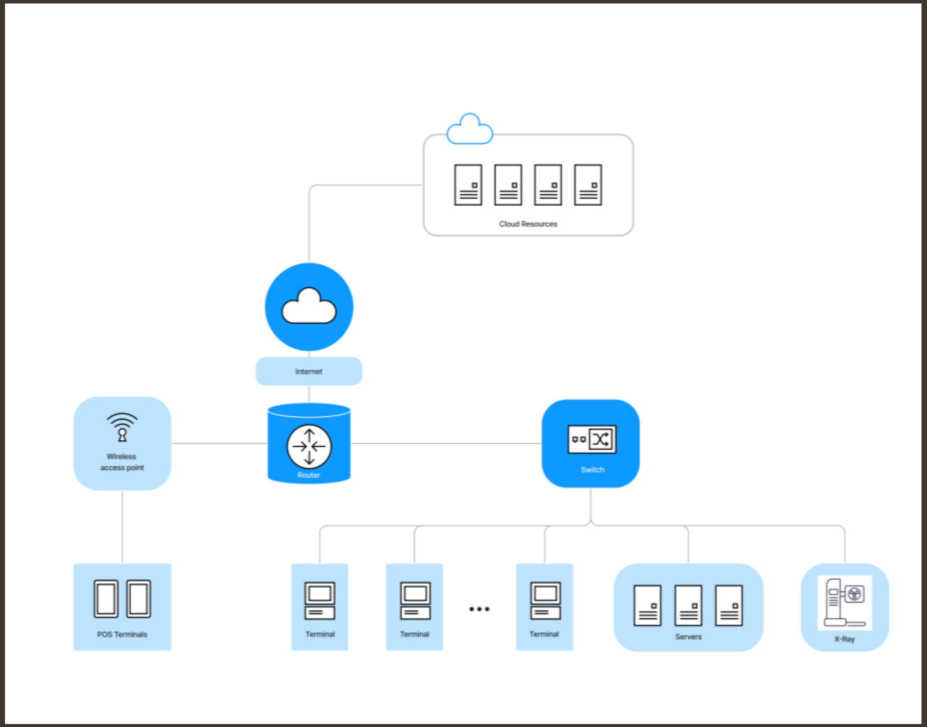
Infrastructure Components

Roles and Responsibilities

Documentation Requirements

Cost Analysis

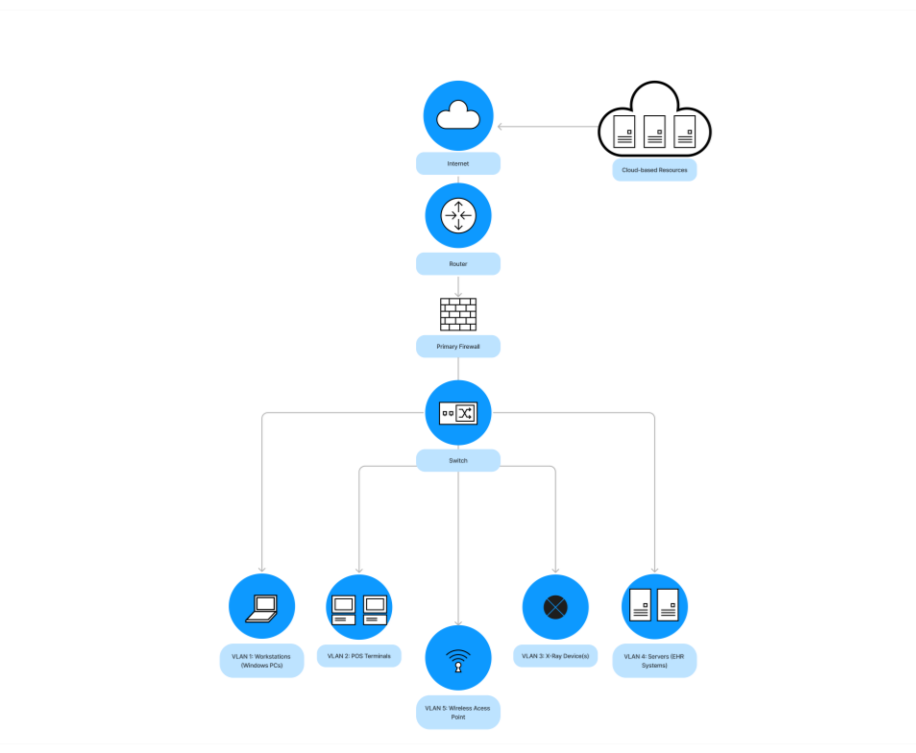
Conclusion and Next Steps



Current Network Architecture

- In the original flat network design, all devices are connected to the same external-facing router via a network switch or wireless access points. This includes:
  - Network Router
  - Network Switch
  - Front desk workstations
  - Digital X-ray sensors and imaging devices
  - Point-of-sale (POS) terminals for handling payments
  - Wireless access points
  - Servers for Patient health records storage system

Target Network Architecture

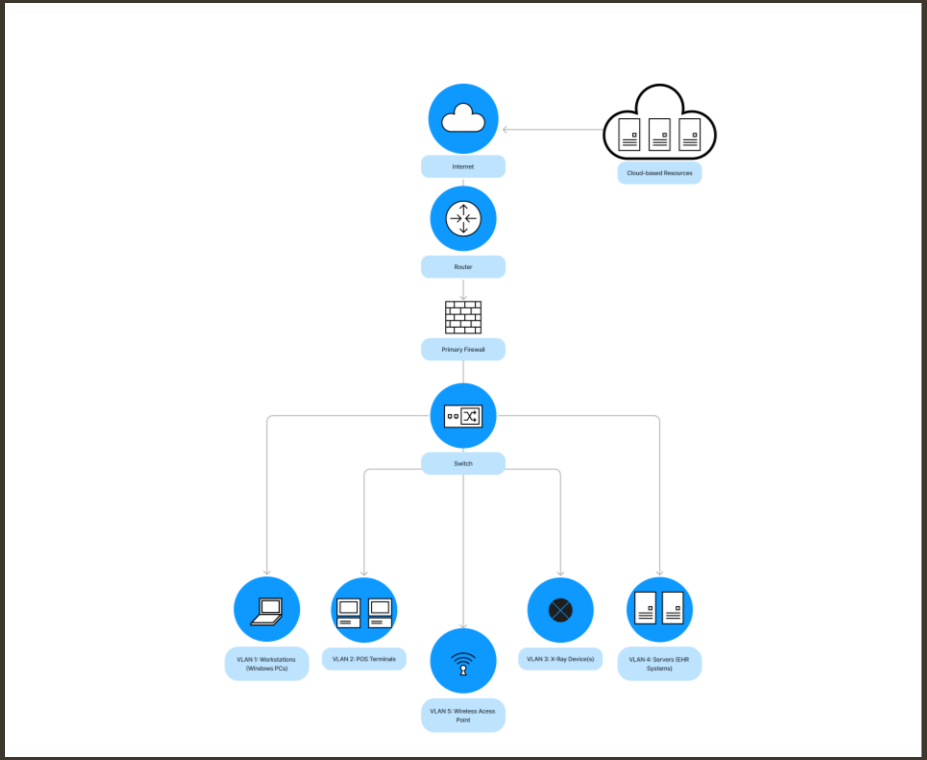


- Diagram Explanation:

• Router: Connects the internal network to the internet.
• Firewall: Positioned after the router to inspect and filter incoming and outgoing traffic.
• Switch: Central device connecting different VLANs.

VLANs:
• VLAN 1: Front Desk Workstations (Windows PCs)
• VLAN 2: POS Terminals
• VLAN 3: Digital X-ray Devices
• VLAN 4: Servers (EHR System)
• VLAN 5: Wireless Access Points

Target Network Architecture



Network Segmentation and Security:

Network Segmentation:

Different categories of devices are placed in separate VLANs to limit broadcast domains and reduce potential attack vectors.

Firewalls are used to control and monitor traffic between VLANs. Ingress/Egress Protection:

The firewall ensures that only authorized traffic enters or leaves the network.

o Firewall rules and Access Control Lists (ACLs) provide an additional layer of security.

Data Protection:

o Sensitive data is encrypted both at rest and in transit.

o Implementing role-based access controls (RBAC) and multi-factor authentication (MFA) enhances data security.

Business-Critical Equipment Protection:

o Dedicated firewalls and continuous monitoring protect critical systems like the EHR.

o Regular security audits help maintain the integrity and security of the network.

This upgraded network architecture improves security by isolating different device categories, minimizing the risk of lateral movement by attackers, and ensuring sensitive data and critical systems have additional layers of protection.

Infrastructure Components

- **Firewalls:**
  - **Description:** Placement at network boundaries and between segments.
  - **Justification:** Prevents unauthorized access and limits the spread of threats.
- **Intrusion Detection and Prevention Systems (IDPS):**
  - **Description:** Monitors network traffic for malicious activities.
  - **Justification:** Enhances detection and response to threats.
- **Network Access Control (NAC):**
  - **Description:** Controls device access to the network.
  - **Justification:** Ensures only authorized devices can connect.

Infrastructure Components

- **Security Information and Event Management (SIEM):**
  - **Description:** Centralized logging and analysis of security events.
  - **Justification:** Provides comprehensive visibility and incident response capabilities.
- **Data Encryption Solutions:**
  - **Description:** Encrypts data at rest and in transit.
  - **Justification:** Protects sensitive data from unauthorized access.
- **Endpoint Protection Platforms (EPP):**
  - **Description:** Provides advanced threat protection for endpoints.
  - **Justification:** Safeguards against malware and other endpoint threats.

Roles and Responsibilities

Existing Roles:

- **IT Manager:**
  - **Responsibilities:** Oversee overall IT and security strategy.
- **System Administrators:**
  - **Responsibilities:** Maintain and secure IT infrastructure.

Roles and Responsibilities

New Roles:

- **Network Security Engineer:**
  - **Responsibilities:** Design and implement network security measures.
- **Security Operations Center (SOC) Analyst:**
  - **Responsibilities:** Monitor and respond to security incidents.

Roles and Responsibilities

Additional Responsibilities:

- **Patch Management Team:** Ensure timely patching of vulnerabilities.
- **Application Security Team:** Conduct security assessments and ensure secure coding practices.

Roles and Responsibilities

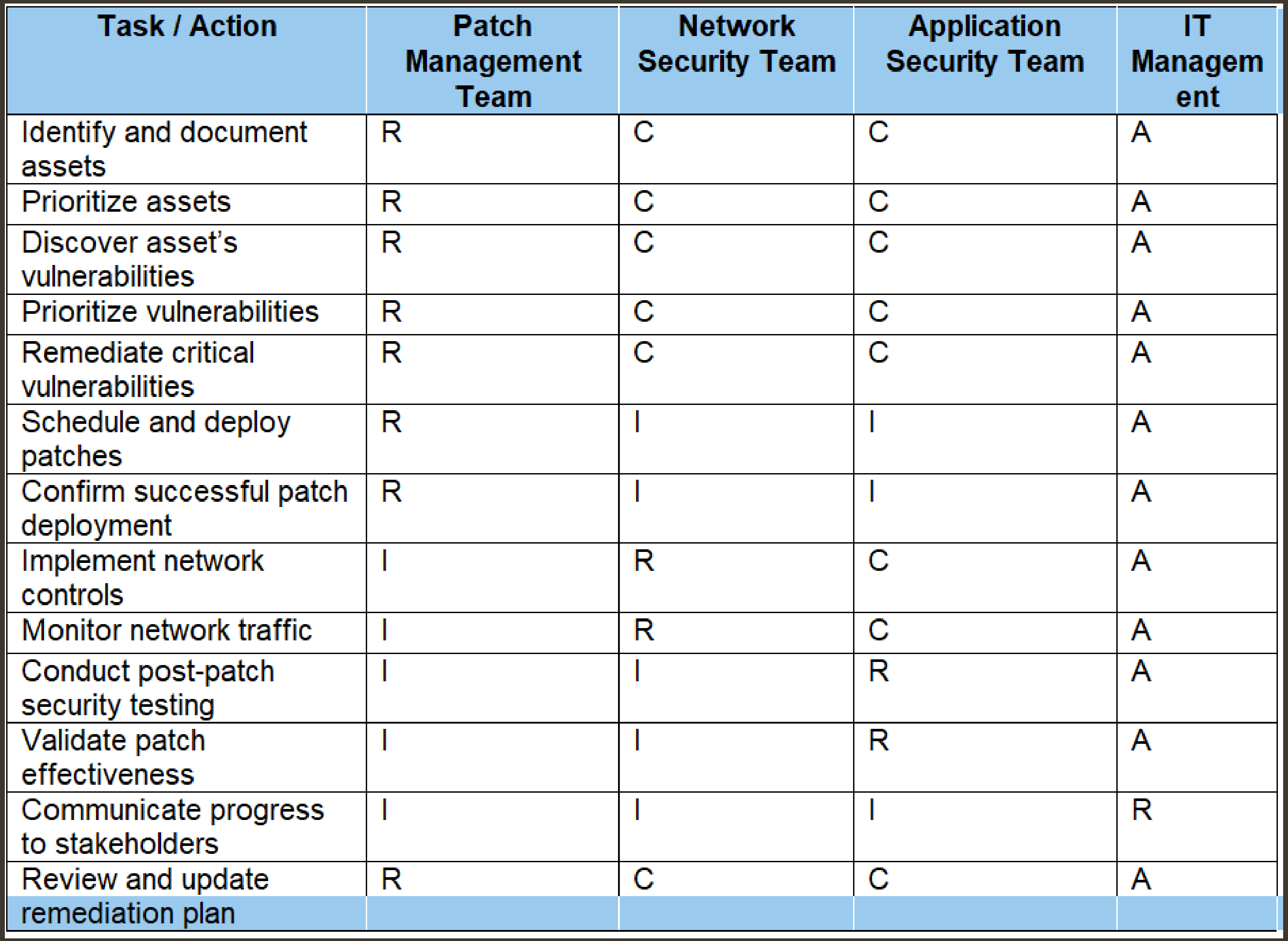
Additional Responsibilities:

- **Patch Management Team:** Ensure timely patching of vulnerabilities.
- **Application Security Team:** Conduct security assessments and ensure secure coding practices.

Roles and Responsibilities

Explanation of RACI Roles:

- **Responsible (R)**: The team or individual who is responsible for completing the task.
- **Accountable (A)**: The team or individual who is ultimately accountable for the task's completion and the final outcome.
- **Consulted (C)**: The team or individual whose opinions or expertise are sought.
- **Informed (I)**: The team or individual who needs to be kept informed of progress and results.



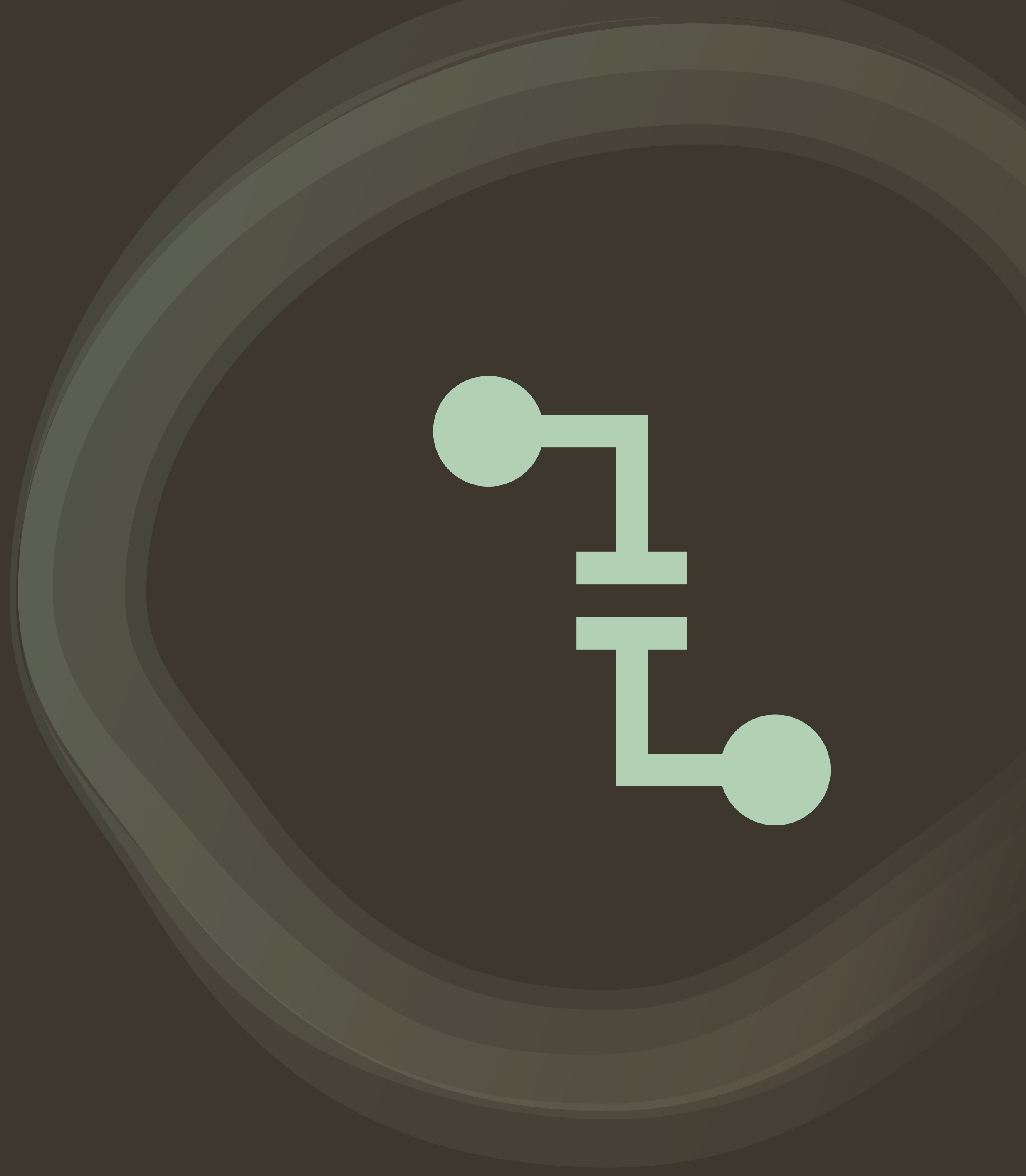
Task / Action	Patch Management Team	Network Security Team	Application Security Team	IT Management
Identify and document assets	R	C	C	A
Prioritize assets	R	C	C	A
Discover asset's vulnerabilities	R	C	C	A
Prioritize vulnerabilities	R	C	C	A
Remediate critical vulnerabilities	R	C	C	A
Schedule and deploy patches	R	I	I	A
Confirm successful patch deployment	R	I	I	A
Implement network controls	I	R	C	A
Monitor network traffic	I	R	C	A
Conduct post-patch security testing	I	I	R	A
Validate patch effectiveness	I	I	R	A
Communicate progress to stakeholders	I	I	I	R
Review and update remediation plan	R	C	C	A

Documentation Requirements

- **Network Security Policy:** Define rules and procedures for network security.
- **Incident Response Plan:** Procedures for detecting, responding to, and recovering from security incidents.
- **Access Control Policy:** Guidelines for user access and authentication.
- **Data Encryption Policy:** Standards for encrypting sensitive data.
- **Patch Management Policy:** Process for applying software updates and patches.
- **Backup and Recovery Plan:** Procedures for data backup and recovery.

Cost Analysis

- **Firewall:**
  - **Cost:** $10,000 (Source: Palo Alto Networks, Cisco)
  - **Justification:** Essential for network segmentation and access control.
- **IDPS:**
  - **Cost:** $8,000 (Source: McAfee, Snort)
  - **Justification:** Enhances threat detection and response.
- **NAC:**
  - **Cost:** $5,000 (Source: Cisco, Forescout)
  - **Justification:** Ensures secure device access.



Cost Analysis

- **SIEM:**
  - **Cost:** $15,000 (Source: Splunk, IBM QRadar)
  - **Justification:** Provides centralized monitoring and incident response.
- **Data Encryption Solutions:**
  - **Cost:** $7,000 (Source: Symantec, Vormetric)
  - **Justification:** Protects sensitive data.
- **EPP:**
  - **Cost:** $6,000 (Source: Symantec, CrowdStrike)
  - **Justification:** Secures endpoints from advanced threats.

Cost Analysis

- **Total Cost:** $51,000
- **Investment Justification:** Enhanced security posture, reduced risk of data breaches, compliance with regulations.

Conclusion and Next Steps

Summary of Proposed Enhancements

Target Network Architecture

- The proposed enhancements aim to transition the network from a flat design to a segmented architecture. Key improvements include:
- **Network Segmentation:**
  - **Firewalls:** Deployed at network boundaries and between segments to prevent unauthorized access and contain threats within specific network zones.
  - **Intrusion Detection and Prevention Systems (IDPS):** Monitors network traffic for malicious activities and enhances threat detection and response.
- **Enhanced Access Controls:**
  - **Network Access Control (NAC):** Ensures that only authorized devices can connect to the network, providing an additional layer of security.
  - **Security Information and Event Management (SIEM):** Centralizes logging and analysis of security events, offering comprehensive visibility and incident response capabilities.

Summary of Proposed Enhancements

Data Protection:

- **Data Encryption Solutions:** Encrypts sensitive data at rest and in transit, safeguarding it from unauthorized access.
- **Endpoint Protection Platforms (EPP):** Provides advanced threat protection for endpoints, securing them against malware and other endpoint threats.

- **Documentation and Policies:**
  - **Network Security Policy:** Establishes rules and procedures for maintaining network security.
  - **Incident Response Plan:** Outlines procedures for detecting, responding to, and recovering from security incidents.
  - **Access Control Policy:** Defines guidelines for user access and authentication.
  - **Data Encryption Policy:** Sets standards for encrypting sensitive data.
  - **Patch Management Policy:** Details the process for applying software updates and patches.
  - **Backup and Recovery Plan:** Ensures procedures for data backup and recovery.

Summary of Proposed Enhancements

Roles and Responsibilities

To manage and oversee the enhanced infrastructure, new roles and responsibilities are proposed:

- **Network Security Engineer:** Designs and implements network security measures.
- **Security Operations Center (SOC) Analyst:** Monitors and responds to security incidents.
- **Patch Management Team:** Ensures timely patching of vulnerabilities.
- **Application Security Team:** Conducts security assessments and ensures secure coding practices.

.

Summary of Proposed Enhancements

Cost Analysis

The estimated cost for the proposed enhancements is $51,000, covering essential components such as firewalls, IDPS, NAC, SIEM, data encryption solutions, and EPP. This investment is justified by the significant improvement in security posture, reduced risk of data breaches, and compliance with regulatory requirements.

Next Steps

The proposed network enhancements will significantly improve the medical clinic's security posture by addressing current vulnerabilities and implementing robust security measures. The next steps involve presenting the proposal to senior management, allocating the budget, initiating the implementation of security measures, and developing the necessary security documentation.