Security Architecture Recommendations

- For NexaCart Inc.

- Prepared by: Ifeanyi Christian Edeh

- Date: 29 April, 2025

Executive Summary

- Rapid business growth exposed security gaps.

- Key threats: weak access controls, outdated endpoint security, unsegmented network.

- Goal: Protect customer data, achieve compliance, support secure growth.

- Framework used: NIST Cybersecurity Framework.

Introduction

- Purpose: Recommend solutions based on prior assessment findings.

- Scope: Focused on digital assets, networks, endpoints, and cloud services.

- Limitations: No physical security audit; limited penetration testing.

Current Security Landscape

- Flat network architecture — no segmentation.
- Basic firewall protection — lacks advanced threat prevention.
- No MFA; weak password policies.
- Outdated antivirus; limited monitoring tools.

Security Architecture Goals

- Protect customer and payment data.
- Ensure PCI DSS and GDPR compliance.
- Support future growth securely.
- Minimize business disruption risks.

Assessment Findings

- High-risk vulnerabilities:
  - Unsecured endpoints
  - Poor access control
  - No network segmentation
  - Lack of monitoring/detection
- High-impact threats: data breaches, financial loss, reputational damage.

Action Plan (NIST Cybersecurity Framework)

- **Identify**: Asset inventory, risk assessments.
- **Protect**: Network segmentation, MFA, encryption.
- **Detect**: SIEM, IDS/IPS deployment.
- **Respond and Recover**: Incident response plan, regular backups.

Task Prioritization Based on Risk

- **High Priority**:
  - Network segmentation
  - MFA deployment
  - EDR rollout

- **Medium Priority**:
  - Encryption upgrades
  - Employee security training
  - Cloud security hardening

Implementation Roadmap

- **Short-term (1–3 months)**:
  - Network segmentation
  - MFA and RBAC
- **Medium-term (3–6 months)**:
  - Endpoint protection upgrades
  - SIEM/IDS implementation
- **Long-term (6–12 months)**:
  - Incident response exercises
  - Continuous monitoring improvements

Conclusion

- Investing in cybersecurity is critical.
- Protect customer trust and company reputation.
- Reduce legal/regulatory exposure.
- Strengthen foundation for future growth.

Thank You!!!