## 

## 

## 

## 

## **CY650–Cyber Security Capstone**

## **Title: Assignment 1: Project Plan Narrative (Product Concept)**

## **Team Name: NeuraShield**

## **Semester: Fall 2024**

## **Date Submitted: 09/23/2024**

## 

**Team Roles and Responsibilities:**

1. **Sagar - Project Manager:** Oversees execution and ensures project goals are met.
2. **Vamsi - Lead Developer:** Develops and maintains platform functionality.
3. **Abhigna - UI/UX Designer** : Ensures user-friendly platform design.
4. **Bhanu Prakash - Content Strategist** : Manages content and website updates.
5. **Hari Prashanth Reddy - Security Expert** : Oversees security systems and testing.
6. **Bhanu Mahesh - QA Tester**: Ensures platform quality and performance.

**Project Narrative:**

**NeuraShield - AI-Driven Security for the Modern Digital Age**

NeuraShield provides enterprises with advanced AI-driven security operations to protect their networks, data, and digital assets 24/7. As cyber threats become more sophisticated, NeuraShield simplifies security management, enabling businesses to operate with confidence in an increasingly hostile cyber landscape.

**AI-Driven Security Operations:**

NeuraShield leverages AI and machine learning for real-time threat detection, proactive defense mechanisms, and rapid responses. Key features include:

* Advanced Threat Detection: Analyzes network traffic and behaviors to identify anomalies.
* Automated Response: Delivers rapid automated threat responses, minimizing downtime.
* Predictive Analytics: Uses machine learning to predict emerging threats based on historical data.

**Key Services and Features:**

* Comprehensive Monitoring: 24/7 monitoring of networks and endpoints, ensuring real-time security visibility.
* Threat Intelligence Integration: Incorporates global threat intelligence feeds for enhanced AI-driven analysis.
* Automated Threat Hunting: Actively searches for indicators of compromise across digital infrastructure.
* Security Operations Center (SOC): Managed SOC-as-a-Service to help businesses offload security management while maintaining visibility.

**Common Cybersecurity Threats Addressed by NeuraShield :**

* Phishing and Social Engineering: Detects and blocks phishing attempts by analyzing communication patterns.
* Insider Threats: Monitors user behavior to detect malicious or accidental insider activity.
* Ransomware: Isolates affected systems quickly, preventing the spread of ransomware.
* DDoS Attacks: Detects and mitigates DDoS attacks in real-time to ensure business continuity.

### **Onboarding Plan:**

1. **Account Setup:** To maintain security, users must establish an account using their organizational email address. This is followed by email verification.
2. **Initial Configuration:** Users explore the dashboard, configure permissions and user roles, and integrate firewalls and IDS/IPS, among other security technologies.
3. **Feature Overview:** An extensive introduction to the main features, including automated incident response and AI-driven threat identification, is provided to users.
4. **AI Feature Configuration:** Users can establish alarm levels, adjust detection parameters to suit their needs, and upload historical data for AI training.
5. **Support and Feedback:**  A feedback mechanism and access to extensive documentation and support channels are provided in order to continuously enhance the platform's usability and onboarding process.

**Why Choose NeuraShield?**

NeuraShield adapts to evolving cyber threats by utilizing the latest AI and machine learning technology. Key benefits include:

* **Reduced Response Time:** Accelerated threat detection and response, minimizing damage.
* **Expert Support:** 24/7 access to cybersecurity professionals for incident handling and system security.
* **Cost-Effective Security:** Automation reduces the need for large in-house security teams, offering a more affordable solution for businesses of all sizes.