1. Overview
   Project Title: Network Traffic Monitoring and Analysis System
   Project Description:
   This project is actually about the design of a system for the purpose of monitoring and analyzing
   network traffic in providing timely detection against potential cyber threats. This system will be
   supported through monitoring tools and data analysis software, which will highlight abnormal
   activities and trigger immediate alerts to security teams for the protection of the network and
   reduction of cyber-attack risks.
   Main Objectives:
   Detection of Network intrusion and other suspicious activities
   Generation of instant alert on detection of potential threats in the network to the network administrators
   Reporting of the patterns of network traffic and its activities in detail
2. Project Deliverables
3. Live Data Analysis: live data analysis in search of abnormal patterns that indicate a possible
   threat.
4. User Interface Display: The real-time alerts generated along with the reports of the network
   traffic should be displayed on a user interface.
5. Training Machine Learning Models: The AI mechanism is developed by training the machine.
6. Enhancing network security through providing recommendations along with analytical insights to reduce vulnerabilities.

---

3. Project Phases

Phase	Details	Tools Used

System Analysis	Collect and analyze project requirements	Requirements documentation
Design	System architecture and user interface design	Visio or Lucidchart
Development	System building and module programming	Python, Snort, Zeek
Testing	Performance and threat detection testing	Penetration testing, K-means
Documentation	Write user guide and team training	Training documentation

1. System Design
   System Architecture:
   Monitoring Module: Snort would be implemented as a part of this module to acquire the data from routers and analyze it for packet discrepancies.
   Analysis Module: The machine learning algorithm would sort through the found patterns and detect the anomalies by the application of K-means and other algorithms.
   Alerting Module: Provides instant alerts to the user when a threat is detected via e-mail or app.
   User Interface:
   Realtime alert notifications
   Detailing reports on network flow and patterns
2. Project Tools and Technologies
3. Monitoring Tools: Snort, Zeek - real-time data gathering and analysis.
4. Software Development: Python - Algorithm development and other development in functionality analysis.
5. Machine Learning: Scikit-learn library for the implementation of K-means along with other machine learning models.
6. Database: MySQL or MongoDB - packet data storage and detected pattern storage.

6. Timeline

Phase	Estimated Duration

Analysis and Requirements Gathering	2 weeks
Design	1 week
Development	4 weeks
Testing	2 weeks
Documentation and Training	1 week
Total	10 weeks

1. Test Plan
2. Performance of System: Whether it can process network traffic without affecting network speed.
3. Threat testing: Attack by DOS, malware etc. to ensure system detect them.
4. Response testing: Alerts are delivered to administrators on time.
5. Risk Analysis
6. Inability of System to Identify Complex Threats: These systems may have difficulty in identifying unidentified threats, which can be minimized by refreshing
   AI models periodically.
7. System Integration Challenges: It may not be able to integrate with other security systems, therefore, APIs need to be prepared in advance or readied for easy integration.

10. Maintenance and Update Plan

1. **Regular security updates**: To stay up-to-date with new threats.
2. **System maintenance**: Perform periodic checks to ensure optimal functionality.