**- Cybersecurity Threat Detection System**

**Introduction**

In today’s digital age, cybersecurity threats are increasingly sophisticated, posing significant risks to organizations of all sizes. A Cybersecurity Threat Detection System aims to proactively identify and mitigate these threats by monitoring network activities and analysing user behaviours. This project seeks to develop an efficient and effective system capable of detecting anomalies indicative of potential security breaches.

**Objectives**

The primary objectives of the Cybersecurity Threat Detection System are:

* To implement real-time monitoring of network traffic and user activities.
* To develop detection algorithms that identify both known and unknown threats.
* To provide automated alerts and response mechanisms to enhance incident management.
* To offer a user-friendly interface for security analysts to monitor and analyze threats effectively.

**System Components**

1. **Data Collection Module**: Gathers data from various sources, including firewalls, intrusion detection systems (IDS), and logs from servers and applications.
2. **Data Processing Engine**: Cleans and prepares the collected data for analysis, ensuring accuracy and relevance.
3. **Threat Detection Engine**: Utilizes machine learning and heuristic algorithms to analyse data and detect potential threats, distinguishing between normal and suspicious behaviour.
4. **Response System**: Automates responses to detected threats, such as alerting administrators, logging incidents, or blocking malicious activities.
5. **User Interface**: A dashboard providing real-time insights, alerts, and detailed reports for effective threat management.

**Methodology**

The development process will involve:

* Defining the scope and types of threats to detect.
* Setting up the necessary development environment and tools.
* Collecting historical data for training detection models.
* Implementing and testing detection algorithms using machine learning techniques.
* Developing a response framework for effective incident management.
* Creating a user-friendly interface for monitoring system status and alerts.

**Challenges**

The project will address challenges such as minimizing false positives, managing large volumes of data, and keeping pace with evolving threats. Continuous refinement of detection algorithms will be crucial to enhance system effectiveness.

**Expected Outcomes**

The Cybersecurity Threat Detection System will provide:

* A robust solution for identifying and responding to cybersecurity threats in real-time.
* Improved security posture for organizations by enhancing threat visibility and response capabilities.
* A practical tool for security analysts, enabling informed decision-making based on real-time data.

**Conclusion**

This project will contribute significantly to the field of cybersecurity by providing an innovative approach to threat detection and response. By leveraging advanced algorithms and a user-centric design, the Cybersecurity Threat Detection System aims to enhance organizational resilience against the growing landscape of cyber threats.

Name: Bhakti Raskar.

Department: Cyber Security.

PRN No: 2124UCSF1002.