Brainstorm & Idea Prioritization

Team – 9.2

Problem Statement

The problem addressed by this project is the unauthorized access into home networking systems, which poses a serious threat to the privacy and security of home users. Traditional security measures such as firewalls and antivirus software are often insufficient to protect against determined attackers. As a result, there is a pressing need for a dedicated intrusion detection system (IDS) tailored for Windows-based home networks. This IDS aims to detect and prevent unauthorized access, thereby reducing downtime and safeguarding private and confidential information for home users.

Ideation

Intrusion Detection Software:

Develop user-friendly intrusion detection software that is compatible with Windows operating systems. This software could continuously monitor network traffic and alert users to any suspicious activity.

Machine Learning-Based Anomaly Detection:

Implement machine learning algorithms to create a system that can learn and detect unusual patterns of network behaviour. This can help in identifying unauthorized access attempts.

Behavioural Analysis:

Create a system that not only detects known threats but also analyses user and device behaviour to identify anomalies. For example, if a device suddenly starts accessing a lot of sensitive information, it could trigger an alert.

Real-time Notifications:

Design a system that provides realtime notifications to users when it detects potential threats. These notifications could be in the form of mobile app alerts or emails.

User-Friendly Dashboard:

Build a user-friendly dashboard for the intrusion detection system, allowing users to monitor their network's

security easily. They should be able to see network activity and potential threats in a comprehensible manner. **Automatic Quarantine:** Implement a feature that, when a threat is detected, automatically quarantines the affected device, preventing it from accessing the network until the user confirms its legitimacy.

Regular Software Updates:

Ensure the intrusion detection software is regularly updated to stay ahead of evolving threats. Provide users with automated updates to keep their network security current. **Network Traffic Encryption:**

Promote the use of encrypted connections (e.g., VPNs) to add an extra layer of security to the network. Integrate this with the intrusion detection system.

Collaboration with ISPs:

Partner with Internet Service Providers (ISPs) to offer intrusion detection as part of their service package to residential customers.

Cloud-Based IDS:

Consider implementing a cloudbased intrusion detection system that can provide enhanced security features and scalability.

Community Monitoring:

Create a community-based approach where users can share information about potential threats and collectively enhance network security.

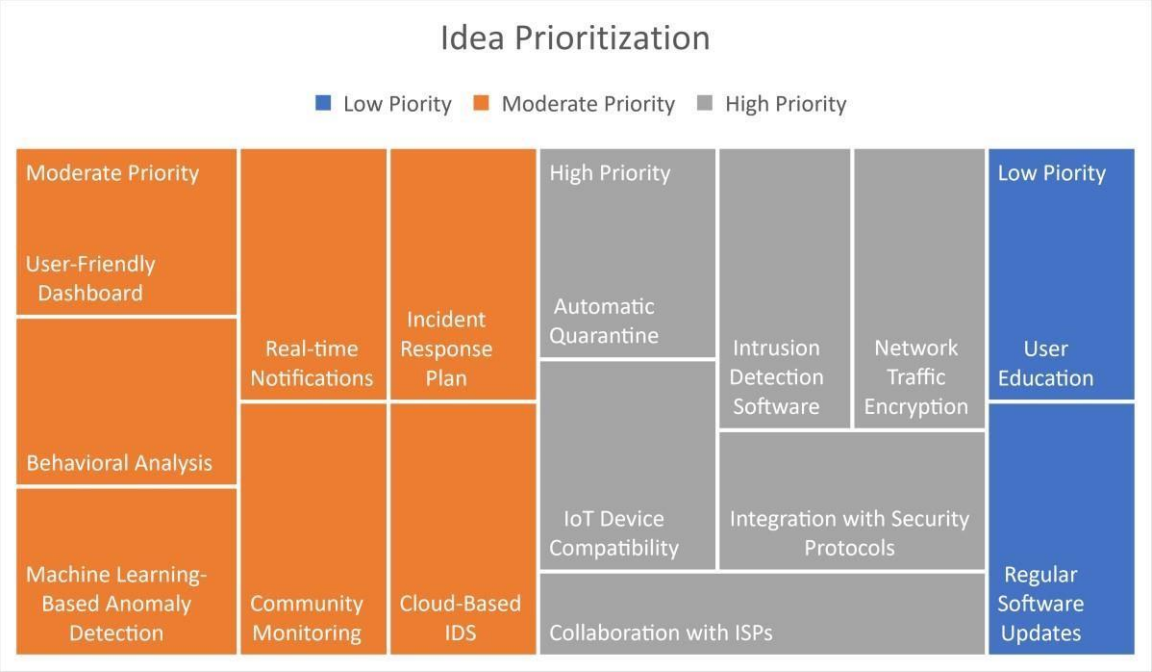
IoT Device Compatibility:

Ensure that the intrusion detection system is compatible with the increasing number of IoT devices in home networks. **Incident Response Plan:**

Develop a clear incident response plan for users, guiding them on what to do if a breach is detected, including contacting support and reporting the incident to authorities if necessary.

Integration with Security Protocols:

Ensure the intrusion detection system integrates seamlessly with existing security protocols and standards to enhance overall network security.


Idea Prioritization
Low Piority
Moderate Priority
High Priority
Moderate Priority
User-Friendly Dashboard
Behavioral Analysis
Machine Learning-Based Anomaly Detection
Real-time Notifications
Community Monitoring
Incident Response Plan
Cloud-Based IDS
High Priority
Automatic Quarantine
IoT Device Compatibility
Collaboration with ISPs
Intrusion Detection Software
Network Traffic Encryption
Integration with Security Protocols
Low Piority
User Education
Regular Software Updates