Design Phase 1

Baisc factors that we have to keep in mind

External Entities:

- Network
- Hosts
- Users

Data should flow in this direction

- Network traffic
- Host logs
- User reports

Processes:

1. Data Collection and Scanning: This process collects data from the network, hosts, and users. The data is collected using a variety of tools, such as Nessus, configuration checks, and regular scans.
2. Result Analysis: This process analyzes the results of the data collection and scanning process. The results are analyzed to identify malware signatures, vulnerabilities, and their severity.
3. Reports and Alerts: This process generates reports and alerts based on the results of the result analysis process. The reports and alerts are sent to users so that they can take appropriate action.
4. Response and Mitigation: This process takes action to respond to and mitigate the malware infections and vulnerabilities that have been identified. This may involve notifying users, patching vulnerabilities, or quarantining infected hosts.

Data Stores:

- Database: This data store stores the results of the data collection and scanning process, as well as the results of the result analysis process.
- SIEM System: This data store stores the results of the data collection and scanning process, as well as the results of the result analysis process. The SIEM system also stores alerts and incidents.

Technology Selection:

Nessus: Nessus is a vulnerability scanner that can be used to scan for vulnerabilities on hosts and networks.

Database (MySQL): MySQL is a relational database management system that can be used to store the results of the data collection and scanning process, as well as the results of the result analysis process.

SIEM System (IBM QRadar): IBM QRadar is a security information and event management (SIEM) system that can be used to collect, analyze, and respond to security events.

Security:

- Tool Security: The tools that are used in the malware detection and classification system must be secure. This means that they should be patched regularly and that they should be configured securely.
- Data Encryption: The data that is stored in the database and in the SIEM system must be encrypted. This will protect the data from unauthorized access.
- Access Control: Access to the malware detection and classification system must be controlled. This means that only authorized users should be able to access the system.
- Audit Logging: All activity in the malware detection and classification system should be logged. This will help to investigate security incidents.

Scalability:

- Horizontal Scaling: The malware detection and classification system can be scaled horizontally by adding more servers. This will increase the capacity of the system to handle more data and more users.
- Monitoring and Alerting: The malware detection and classification system should be monitored for performance and security. Alerts should be generated when problems are detected.
- Cloud Services: The malware detection and classification system can be deployed in the cloud. This will provide a scalable and reliable platform for the system.

Data Flow:

The data flow in the malware detection and classification system is as follows:

- Data is collected from the network, hosts, and users.
- The data is analyzed to identify malware signatures, vulnerabilities, and their severity.
- Reports and alerts are generated based on the results of the analysis.
- The reports and alerts are sent to users so that they can take appropriate action.
- Users may respond to the reports and alerts by patching vulnerabilities, quarantining infected hosts, or taking other actions.