Table 1

Technology	Description	Usage
React	A JavaScript library for building user interfaces	Front-end development (user interface)
Bootstrap	A CSS framework for making responsive and mobile-friendly websites	Front-end development (styling)
Chart.js	A JavaScript library for creating charts and graphs	Front-end development (data visualization)
Python	A general-purpose programming language	Back-end development (server-side logic), machine learning model development
Flask	A lightweight web framework for Python	Back-end development (server-side logic)
SQLAlchemy	An object-relational mapper (ORM) for Python	Back-end development (database access)
scikit-learn	A machine learning library for Python	Machine learning model development (classification, regression, etc.)
MySQL	A relational database management system (RDBMS)	Data storage (malware samples, machine learning model parameters)
Docker	A tool for containerizing applications	Deployment and administration (packaging the malware detection and classification system as a container)
Kubernetes	A tool for orchestrating containerized applications	Deployment and administration (deploying and managing the malware detection and classification system at scale)
Prometheus	A tool for monitoring system performance	Deployment and administration (monitoring the performance of the malware detection and classification system)
Grafana	A tool for visualizing system performance data	Deployment and administration (visualizing the performance of the malware detection and classification system)
Cloud-based platform	A platform for deploying and managing cloud-based applications	Deployment and administration (deploying the malware detection and classification system to the cloud)

Table 2

Technology	Description	Usage
Nessus	A vulnerability scanner	Data collection and scanning (identifying vulnerabilities on hosts and networks)
Configuration checks(Nmap)	Tools for checking the configuration of hosts and networks	Data collection and scanning (identifying vulnerabilities on hosts and networks)
IBM QRadar	A security information and event management (SIEM) system	Data collection and scanning (collecting security events from hosts and networks), result analysis (correlating security events to identify threats), reports and alerts (generating reports and alerts based on security events), response and mitigation (responding to and mitigating security threats)