1. Functional Requirements:

• Threat Identification System: Identify various cybersecurity threats like malware, phishing, DDoS attacks, and insider threats.

• Real-time Threat Monitoring: Continuous monitoring of networks and systems for suspicious activities.

• Risk Assessment Tools: Analyzing vulnerabilities and predicting potential attack surfaces.

• Incident Response Mechanism: Automated alerts and response strategies to mitigate attacks.

• User Authentication and Access Control: Implementing multifactor authentication (MFA) and zero-trust architecture.

• Data Encryption and Secure Communication: Safeguarding sensitive data during transmission and storage.

2. Non-Functional Requirements:

• Scalability: Handle large volumes of data and traffic in realtime

.• Performance: Fast response time to detect and respond to threats.

• Reliability: Ensure system uptime and protection against

• User-Friendly Interface: Intuitive dashboards for threat visualization.

• Compliance and Privacy: Adherence to regulations like GDPR, HIPAA, and PCI-DSS.