Requirement Analysis

The project focuses on strengthening cybersecurity measures by understanding threats, vulnerabilities, and mitigation strategies. The key requirements include:

1. **Web Application Security** – Identifying and mitigating vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and security misconfigurations.
2. **Penetration Testing & Vulnerability Assessment** – Implementing tools like OWASP ZAP, Burp Suite, and Nessus to assess application and network security.
3. **Threat Intelligence & Cyber Threat Hunting** – Analyzing cyber threats using frameworks like MITRE ATT&CK and MISP to enhance proactive defense.
4. **Security Operations & Incident Response** – Understanding SOC (Security Operations Center) workflows, SIEM tools, and digital forensics for real-time threat detection and response.
5. **Cloud & AI-Driven Security** – Implementing Zero Trust Architecture and exploring AI-based threat detection to enhance cybersecurity resilience.