Solution Architecture :-

A well-structured solution architecture is essential for effectively identifying, assessing, and mitigating cyber threats using Nessus and other scanning tools. Below is a comprehensive architecture that integrates vulnerability scanning, risk management, automated remediation, and continuous monitoring into a single security framework.

1. Solution Architecture Overview :

The architecture consists of four key layers:

1. Data Collection & Threat Intelligence Layer – Gathers security data from networks, applications, and external threat intelligence sources.
2. Vulnerability Assessment & Risk Prioritization Layer – Uses scanning tools to detect vulnerabilities and prioritize risks.
3. Automated Remediation & Incident Response Layer – Applies security patches, mitigates threats, and integrates with SOAR systems.
4. Continuous Monitoring & Compliance Layer – Ensures real-time security monitoring, compliance management, and reporting.

2. Workflow of the Solution :

1. Data Collection → Security logs and external threat intelligence are collected.

2. Vulnerability Scanning → Nessus, OpenVAS, and Qualys scan for security weaknesses.

3. Risk Prioritization → Identified threats are classified based on severity.

4. Remediation & Response → Automated patching and real-time mitigation occur.

5. Continuous Monitoring → SIEM tools track security events and generate compliance reports.

3. Key Benefits of the Architecture :

✓ Proactive Cyber Threat Detection – Identifies vulnerabilities before attackers exploit them.

✓ Automated Threat Remediation – Reduces response time to cyber threats.

✓ Real-Time Security Monitoring – Provides live tracking of security events and potential breaches.

✓ Regulatory Compliance – Ensures adherence to standards like ISO 27001, GDPR, and PCI-DSS.

✓ Scalability & Integration – Supports integration with cloud security, AI-driven threat analysis, and SOAR automation.

4. Future Enhancements :

✅ AI-Powered Threat Detection – Use machine learning to predict and prevent cyber threats.

✅ Cloud-Native Security Tools – Enhance AWS, Azure, and Google Cloud security with native scanning solutions.

✅ Zero Trust Security Integration – Implement continuous user authentication and least privilege access for better security.