PROPOSED SOLUTION

S.NO	PARAMETER	DESCRIPTION
1	**Scanning tool**	Nessus,OpenVAS, nexpose, and other vulnerability scanning tools.
2	**Threat categories**	Malware, phishing,ransomware, dos/ddos attacks,insider threats,zero-day vulnerabilities
3	**Scanning techniques**	Network-based,host-based,credentialed and non-credentialed scans,compliance checks.
4	**Risk assessment**	Identifying severity levels(low, medium, high, critical)based on CVSS(common vulnerability scoring system).
5	**Remediation strategies**	Patch management,firewall configurations,IDS/IPS integration,zerotrust model implementation.
6	**Automation and AI**	Use of AI- driven threat detection, automated patching, behaviour-based anomaly detection.
7	**Parameter Reporting and compliance**	Generating security reports,aligning with frameworks like NIST,ISO 27001, GDPR,HIPAA.
8	**Integration with SIEM**	Connecting Nessus and other tools with security information and event management(SIEM)solutions
9	**Continuous monitoring**	Implementing real-time threat monitoring and periodic security audits.