Proposed Solution Template :-

To effectively understand and mitigate cyber threats, organizations need a structured approach using Nessus and other vulnerability scanning tools. Below are solution templates that provide a step-by-step framework for implementing vulnerability management and threat mitigation strategies.

1. ### General Cybersecurity Framework Using Nessus & Beyond

   #### Objective :

   To create a robust cybersecurity framework using vulnerability scanning tools to detect and mitigate cyber threats efficiently.

   #### Solution Approach :

Step	Action	Tools Used
Step 1	Identify and classify assets (networks , servers , databases).	Nessus , OpenVAS , Qualys.
Step 2	Perform automated vulnerability scans.	Nessus , Nexpose , Burp Suite.
Step 3	Analyze and prioritize risks based on severity.	CVSS Scoring , Threat Intelligence Platforms.
Step 4	Apply patches and security updates	Patch Mangagement Systems.
Step 5	Conduct penetration testing for deeper assessment.	Metasploit , Burp Suite.
Step 6	Implement continuous monitoring & reporting.	SIEM (Splunk , IBM Qradar).

   Expected Outcome : Reduced security vulnerabilities and faster threat detection.Enhanced compliance with industry standards like ISO 27001, GDPR, and PCI-DSS.

2. ### Automated Vulnerability Management Plan

   #### Objective :

   To create an automated vulnerability detection and remediation system using Nessus and complementary tools.

Solution Approach :

Phase	Action Plan	Tools Used
Assessment Phase	Run periodic Nessus scans to identify vulnerabilities.	Nessus , OpenVAS.
Prioritization Phase	Rank vulnerability based on risk level and exploitability.	CVSS , Tenable.io
Remediation Phase	Automate patch deployment for critical vulnerability.	SCCM , WSUS , Ansible.
Verification Phase	Re-scan and validate fixes to ensure security gaps are closed.	Nessus , Nexpose.
Monitoring Phase	Set up real-time alerts and incident response automation.	SIEM , SOAR (Splunk , IBM Resilient).

Expected Outcome :

Automated detection and patching of vulnerabilities.Fewer security breaches and reduced attack surface.

3. Cloud Security Strategy with Nessus & Other Scanners
   Objective :

   To secure cloud-based infrastructures by integrating vulnerability scanning tools into cloud environments.

Solution Approach :

Step	Action	Tools Used
Step 1	Identify and map cloud assets.	AWS Inspector , Nessus , Qualys.
Step 2	Perform regular vulnerability scans on cloud instances.	Nessus , Tenable.io
Step 3	Secure APIs and web applications	Acunetix , Burp Suite.
Step 4	Implement cloud security posture management (CSPM).	Prisma Cloud , Microsoft Defender for Cloud.
Step 5	Continuously monitor threats and automate response.	AWS Security Hud , SIEM.

Expected Outcome :

Enhanced visibility into cloud security risks.Proactive detection and response to cloud-based cyber threats.

4. Zero Trust Security Model Using Nessus & Beyond

Objective :

To implement a Zero Trust architecture using Nessus and other security tools to prevent unauthorized access.

Solution Approach :

Components	Implementation Strategy	Tools Used
Identity & Access Control	Enforce MFA & Least Privilege.	Okta , Microscoft Azure AD.
Vulnerability Scanning	Regular scans for misconfigurations & threats.	Nessus , Qualys , Nexpose.
Network Segmentation	Restrict access to sensitive data.	Firewalls , SD-WAN.
Continous Monitoring	Real-time threats detection & response.	SIEM , SOAR
Incident Response	Automated attact mitigation.	CrowdStrike , IBM Resilient.

Expected Outcome :

Stronger access control and zero-trust enforcement.Continuous verification of network security to prevent breaches.