Creating Detection Protocols:

1. Identify Critical Assets:
   * Pinpoint the systems, applications, and data most crucial to your business operations.
   * Focus your detection efforts on these high-value assets to maximize protection.
2. Prioritize Threats:
   * Assess the likelihood and potential impact of various threats based on your industry, threat landscape, and security posture.
   * Focus on threats that pose the greatest risk to your critical assets.
3. Select Relevant Plugins:
   * Choose plugins that effectively detect the prioritized threats, considering:
     + Vulnerability assessment plugins for known vulnerabilities.
     + Compliance check plugins for regulatory requirements.
     + Malware detection plugins for malicious activity.
     + Custom plugins for unique threats or specific environments.
4. Configure Scans:
   * Tailor scan settings to align with your detection goals and environment:
     + Target specific assets or network segments.
     + Adjust plugin preferences for accuracy and depth.
     + Schedule regular scans for continuous monitoring.
5. Implement Active Monitoring:
   * Consider using Nessus agents or continuous scanning for real-time threat detection.
   * Integrate with SIEM or other security tools for centralized monitoring and correlation.

Response Mechanisms:

1. Prioritize Findings:
   * Assess the severity of detected threats based on their potential impact and exploitability.
   * Focus remediation efforts on the most critical vulnerabilities first.
2. Plan Remediation:
   * Develop detailed remediation plans, including:
     + Patching vulnerable systems or applications.
     + Reconfiguring security settings.
     + Isolating or quarantining compromised systems.
     + Reinstalling or restoring affected systems.
3. Assign Responsibilities:
   * Clearly define roles and responsibilities for different response tasks, ensuring timely and efficient execution.
4. Communicate Effectively:
   * Establish clear communication channels for reporting findings, escalating incidents, and coordinating response efforts.
   * Keep stakeholders informed of progress and risks.
5. Monitor Effectiveness:
   * Track the progress of remediation efforts and the effectiveness of detection protocols.
   * Adjust strategies as needed to address new threats or evolving vulnerabilities.