**Methods of inquiry of cybersecurity:**

In cybersecurity, the main methods include risk assessment, threat intelligence, vulnerability assessment, penetration testing, and forensic analysis.

**Appendixes:**

**Appendix A: Risk Assessment Procedures**

Objective: Identify and evaluate potential risks to MASE Inc.'s information assets.

1. Risk Identification: Process for identifying threats and vulnerabilities.

2. Risk Analysis: Techniques for assessing the likelihood and impact of risks.

3. Risk Evaluation: Criteria for prioritising risks based on potential impact.

4. Mitigation Strategies: Approaches for mitigating identified risks.

**Appendix B: Threat Intelligence Gathering**

Objective: Collect and analyze information about potential threats to MASE Inc.

Data Sources: Internal and external sources for threat intelligence (e.g., OSINT, commercial threat feeds).

Analysis Techniques: Methods for analyzing and interpreting threat data (e.g., pattern recognition, trend analysis).

Integration: Process for integrating threat intelligence into MASE Inc.'s security posture.

**Appendix C: Vulnerability Assessment**

Objective: Identify and assess vulnerabilities within MASE Inc.'s systems and networks.

Scanning Tools: List and description of automated vulnerability scanning tools.

Manual Testing Procedures: Guidelines for manual vulnerability assessments.

Reporting and Remediation: Process for documenting findings and implementing remediation measures.

**Appendix D: Penetration Testing Protocols**

Objective: Simulate attacks to discover and address security weaknesses.

Methods:

- Testing Scope: Define scope and objectives of penetration tests.

- Testing Types: Describe different types of penetration tests (black-box, white-box, gray-box).

- Execution: Procedures for conducting penetration tests, including pre-test preparation and post-test reporting.

**Appendix E: Forensic Analysis Guidelines**

Objective: Investigate and analyze security incidents and breaches.

Evidence Collection: Procedures for collecting and preserving digital evidence.

Analysis Techniques: Methods for analyzing digital evidence (e.g., file analysis, log analysis).Reporting: Guidelines for documenting findings and creating forensic reports.

**Solutions:**

**Risk Assessment Solutions:**

- Introduce a risk management framework

- Use risk management tools like RiskWatch or Qualys for automated risk assessments

- Adopt structured risk management frameworks like NIST RMF or ISO/IEC 27005

- Develop a formal risk assessment process covering identification, analysis, evaluation, and treatment of risks

- Update risk assessments regularly to reflect environmental changes

**Threat Intelligence Solutions:**

* Remember to utilize advanced threat intelligence platforms and integrate threat intelligence feeds with your SIEM system to enhance detection capabilities. Establish a threat intelligence program for gathering, analyzing, and disseminating relevant threat information.

**Vulnerability Assessment Solutions**

Use automated tools like Nessus, Qualys, or OpenVAS for vulnerability scans. Conduct manual assessments with tools like Burp Suite or Nmap. Establish a vulnerability management process with regular scans and prioritized remediation efforts.

**Penetration Testing Solutions:**

Conduct regular and comprehensive penetration testing using tools like Metasploit, Kali Linux, or Core Impact. Engage with professional penetration testing service providers for thorough and independent testing. Develop a penetration testing schedule and use results to improve security.

**Forensic Analysis Solutions:**

Implement a forensic investigation process and use digital forensic tools like EnCase, FTK Imager, or Sleuth Kit for evidence collection and analysis. Establish a forensic response plan covering evidence preservation, analysis, and reporting, and ensure your team is well-trained in forensic methods and legal considerations.