CLAIMS

What is claimed is:

1. A computer-implemented defensive cybersecurity system for discovering vulnerabilities in post-quantum cryptographic implementations within the MWRASP (Total) framework, comprising:

a vulnerability discovery engine operated by defensive AI agents that identifies implementation weaknesses undetectable by classical cryptanalysis;

a GPU-accelerated quantum attack simulator executing parallel simulations through AI agent swarms against target cryptographic implementations for defensive purposes;

a side-channel analysis module employing quantum-enhanced correlation techniques guided by monitoring AI agents;

a compliance validation engine with AI agents automatically generating reports for multiple international standards;

a migration recommendation system with planning AI agents implementing algorithmic risk assessment based on Mosca's theorem; and

an integrated MWRASP AI agent network coordinating all defensive operations.

2. A method for automated defensive security validation of post-quantum cryptographic implementations through AI agents comprising:

deploying defensive AI agent swarms to load cryptographic implementations;

executing parallel adversarial quantum attack simulations via protection agents on GPU hardware;

performing quantum-enhanced side-channel analysis by monitoring agents;

identifying vulnerabilities through AI agent pattern recognition;

validating compliance via specialized certification agents;

generating risk assessments through planning AI agents;

producing comprehensive security reports from the MWRASP network; and

coordinating all operations through integrated defensive AI agent systems.

3. A computer-readable medium storing instructions for defensive vulnerability discovery through AI agents, that when executed cause a computing system to:

configure GPU resources for defensive AI agent testing operations;

simulate quantum attacks via protection agent networks;

detect vulnerabilities through discovery AI agents;

assess compliance via certification AI agents;

calculate risk scores through planning AI agents;

generate recommendations from the MWRASP agent network; and

coordinate all defensive operations through integrated AI agent swarms.

4. The system of claim 1, wherein the defensive AI agents test but do not implement cryptographic algorithms for production use.

5. The system of claim 1, wherein GPU acceleration is optimized for defensive AI agent adversarial testing operations.

6. The system of claim 1, designed to validate implementations through defensive AI agent networks testing libraries including NVIDIA cuPQC, LibOQS, and other frameworks.

7. The system of claim 1, wherein defensive quantum attack simulators operated by AI agents implement Grover's algorithm, Shor's algorithm, quantum collision finding, and amplitude amplification for protection purposes.

8. The system of claim 1, wherein discovery AI agents employ early termination upon finding vulnerabilities to optimize defensive testing throughput.

9. The system of claim 1, wherein monitoring AI agents use quantum superposition principles to enhance correlation sensitivity for protection.

10. The system of claim 1, wherein compliance AI agents simultaneously evaluate NIST FIPS 203, FIPS 204, FIPS 205, ETSI TR 103 619, and ISO/IEC 18033-2 requirements.

11. The system of claim 1, wherein planning AI agents implement Mosca's theorem through algorithmic calculation of data sensitivity periods, migration time estimates, and quantum threat timelines for defensive purposes.

12. The method of claim 2, wherein defensive AI agents utilize tensor cores for cryptanalytic operations in protection scenarios.

13. The method of claim 2, wherein vulnerability identification by AI agents includes detection of timing variations, power consumption patterns, electromagnetic emanations, and error handling flaws for comprehensive protection.

14. The method of claim 2, further comprising defensive AI agents testing GPU-specific implementation vulnerabilities unique to hardware-accelerated cryptographic libraries.

15. The computer-readable medium of claim 3, wherein instructions cause defensive AI agent systems to operate as a validation layer above existing PQC implementation libraries within the MWRASP framework.

16. The system of claim 1, wherein the MWRASP AI agent network comprises specialized agents for discovery, monitoring, protection, planning, and compliance operating in coordinated swarms.

17. The system of claim 1, wherein defensive AI agents communicate through encrypted channels within the MWRASP platform to coordinate vulnerability discovery and protection deployment.

18. The system of claim 1, wherein the AI agent architecture supports dynamic scaling across multiple GPU nodes for enterprise-wide defensive testing.

19. The method of claim 2, wherein AI agents employ machine learning models trained on known vulnerabilities to predict novel attack vectors for defensive purposes.

20. The system of claim 1, wherein the MWRASP framework provides real-time threat intelligence sharing between defensive AI agents across multiple organizations while preserving data privacy.