PromptStrike Security Compliance Report

Generated: 2025-07-09 19:57:36

Target Model: GPT-4

Report Type: Comprehensive Security Assessment

OWASP LLM Top 10 Coverage

✓ LLM01: Prompt Injection
✓ LLM02: Insecure Output Handling
✓ LLM03: Training Data Poisoning
✓ LLM04: Model Denial of Service
✓ LLM05: Supply Chain Vulnerabilities
✓ LLM06: Sensitive Information Disclosure
✓ LLM07: Insecure Plugin Design
✓ LLM08: Excessive Agency
✓ LLM09: Overreliance
✓ LLM10: Model Theft

Compliance Frameworks

✓ NIST AI Risk Management Framework (AI-RMF)
✓ EU AI Act Requirements
✓ SOC 2 Control Objectives
✓ ISO 27001 Information Security Management
✓ GDPR Data Protection Requirements
✓ PCI DSS Payment Card Industry Standards

Security Assessment Results

• Vulnerability assessment completed
• Risk analysis performed
• Threat modeling executed
• Security controls evaluated
• Compliance mapping verified