

Literary Criticism RCS813 – Task 2

Prepared by
Abdulaziz Alarfaj



Part
01

Research Title

Assignment : Critique of Research Paper in Terms of
Research Methodology

Article Chosen :

Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation

<https://www.sce.carleton.ca/faculty/wainer/papers/1-s2.0-S0268401222000548-main.pdf>

Published in 2023

1. Research Methodology

A. Data Collection - Sources of Data
Human-Generated Policies:

Industry Reports: Policies from cybersecurity vendors (Trend Micro, SANS Institute, Symantec).

Government Guidelines: Documents from NIST (USA), NCSC (UK), and NCSC (Netherlands).

GPT-4-Generated Policies:

1. Research Methodology – coniu'ed

Data Selection Criteria

Relevance: Focused on ransomware attacks involving data exfiltration (e.g., Maze, REvil, Ryuk).

Timeliness: Reports published between 2021–2023 to ensure up-to-date threat intelligence.

Diversity: Policies from both private sector (vendors) and public sector (government agencies).

Field Study Components

A. Expert Review & Validation

Human Moderators: Cybersecurity and GRC experts reviewed GPT-4 outputs for:

Accuracy: Are recommendations technically sound?

Practicality: Can they be implemented in real-world settings?

Legal/Ethical Risks: Does the policy comply with regulations?

B. Case Study Simulation

Scenario: A mid-sized financial firm hit by REvil ransomware (data exfiltration variant).

Field Study Components – continued

Approach:

Baseline Policy: Existing human-generated incident response plan.

GPT-4 Policy: Generated using optimized prompts.

Comparison: Effectiveness in reducing attack success rate, cost savings, coverage gaps.

Recommendations for Future Field Studies

Expand Data Sources: Include sensitive/classified GRC documents (with permissions).

Real-World Deployment: Test GPT-5 policies in live corporate environments.

Longitudinal Analysis: Track policy performance against evolving ransomware tactics.