Section A: Topic Completeness

Subtotal: 13 / 15

Element	Score	Feedback
WHAT	3	"Lightweight Adversarial Defenses" and "Malware Detection" are clearly named.
WHO	2	Implied as "organizations" or "resource-constrained environments," but could specify the user type (e.g., mobile users, IoT devices).
WHERE	3	Clearly situated in the context of Machine-Learning-Based Malware Detection.
WHEN	2	While timeframe is often less critical in technical topics, a mention of "modern" or "current" attack signatures would tighten this.
HOW	3	Methodology (Evaluating/Testing/Building a classifier) is clearly indicated.

Peer Comment: The "WHO" is a bit broad. Are you targeting enterprise servers, or specifically low-power edge devices? Defining the "resource-constrained environment" more specifically will help your evaluation criteria later.

Section B: Appropriateness (Quality & Research Value)

Subtotal: 14 / 15

Criterion	Score	Feedback
Discipline Fit	3	Perfectly aligned with Cybersecurity and Data Science requirements.

Theory Link	2	You mention "Adversarial Attacks," which is the theoretical base, but explicitly naming the theory (e.g., Evasion attacks) would be stronger.
Clarity	3	Aim and Objectives are exceptionally well-aligned and logical.
Fresh Insight	3	Evaluating "lightweight" and "combined" defenses offers a practical angle often ignored by theory-heavy papers.
Value	3	Even if defenses perform poorly, the "trade-off" analysis provides useful data for the industry.

Peer Comment: A strong section. The focus on "trade-offs" (robustness vs. cost) is your greatest strength here as it provides immediate industry value.

Section C: Capability (Feasibility)

Subtotal: 11 / 12

Criterion	**Score**	**Feedback**
Skills	3	Building a classifier and testing attacks is standard for this level of research.
Time	3	Using "publicly available datasets" ensures you aren't stuck in data collection hell.
Cost	3	Public datasets and standard ML libraries make this highly affordable.
Data Access	2	While datasets are public, ensure you have the computing power (GPU/RAM) to run adversarial training.

Peer Comment: The main risk is the computational overhead of "Adversarial Training" if that is one of your defenses. Ensure your hardware can handle the training cycles required.

Section D: Fulfillment (Motivation & Relevance)

Subtotal: 6 / 6

Criterion	Score	Feedback
Interest	3	The focus on "practical, deployable protection" suggests a strong interest in real-world application.
Future Goals	3	High relevance for careers in Cyber-AI, SecOps, or Malware Analysis.

Final Coaching Summary

Total Score: 44 / 48 (Strong)

You have a very solid foundation. To move this from "Strong" to "Exceptional," I recommend:

1. **Define "Lightweight":** Quantify what this means for your study (e.g., < 10% CPU overhead).
2. **Specify the Environment:** Are you focusing on Android malware (IoT) or Windows executables? This will dictate your "WHO" and "WHERE" more clearly.

NOTES BASED ON PEER REVIEW

- Quantitative definition of “lightweight” (metrics to measure overhead).
- Clear WHO and WHERE — Windows PE malware on endpoint machines.
- Explicitly connect to adversarial attack theory (evasion attacks).
- Mention modern / current attack signatures to frame relevance.
- Include feasibility/resource considerations (hardware, dataset, cost).
- Emphasize your combined vs individual defense evaluation and trade-off analysis as your unique contribution.