Task: Lilan Weng’s blogpost distillation!

Adversarial Attacks

SubTasks

* Motivation
* Methodology
* Main Conclusions and Rationale behind them
* Critique the paper (unanswered questions, any limitations that the paper didnʼt address, and anything that you are skeptical about)