Countermeasures:

Exploratory, Targeted, Integrity attacks can be defended by randomization of the decision boundary because boundary movement is likely to change classification of the relevant points.

Causative, Indiscriminate, Privacy attacks can be defended with regularization. Regularization is a technique used in statistics to smooth complex data by multiplying it by a term J(f).

Exploratory, Indiscriminate, Integrity attacks can be defended by information hiding. If the attacker’s probe can’t interpret any information about the decision boundary it will not be able to attack the system.