QUIZ

Fill in the blank.

Evasion attacks are designed to interrupt AI's ability to perform classification and identification.

You got it!

True or False:

The underlying technology behind AI systems is software and algorithms.

True. The underlying technology behind AI systems IS software and algorithms.

Correct! The underlying technology behind AI systems is software and algorithms.

False. The underlying technology behind AI systems IS NOT software and algorithms.

Fill in the blank.

Data poisoning is when trained data has been tainted and is used for an AI model.

You got it!

What can lead to expected and desired AI behaviors?

Large amount of trained data.

Correct! Large amount of trained data can lead to expected and desired AI behaviors.

Small amount of trained data.

Large amount of untrained data.

Which of these options is an AI systems vulnerability?

Weak Passwords

Input Handling

👏 Correct! One of the vulnerabilities in an AI systems is input handling.

SQL Injection

This type of attack is when a malicious actor feeds data into a model and tracks how the model manipulates the data to steal the underlying model.

Generative attack.

Extraction attack.

👏 Correct. An extraction attack is when a malicious actor feeds data into a model and tracks how the model manipulates the data to steal the underlying model.

Session attack.

Can input manipulation introduce an inference attack?

No, input manipulation CANNOT introduce an inference attack.

Yes, input manipulation CAN introduce an inference attack.

👏 Correct. Input manipulation may unravel and detect specific connections in an AI system which can introduce an inference attack.