

# AI security threats and controls navigator

from the OWASP AI Exchange at [owaspai.org](https://owaspai.org)

LEGEND:

Group of controls, ordered by threat or type (clickable)

▶ Standard information security CONTROL (with attention points)

▶ Runtime Data science CONTROL

▶ Development-time Data science CONTROL

▶ Other CONTROL

Impact on Confidentiality, Integrity or Availability

