Εργασία Α : Διαχείρηση Ασφάλειας Συστημάτων Τεχνητής Νοημοσύνης (ΤΝ)

**Περιγραφή:**

Επιλεξτε ένα συστημα ΤΝ που χρησιμοιπειται σε κάποιο κρίσιμο  οργανισμό (πχ υγείας, χρηματοοικονομικό, παιδείας, κλπ)  και

1) Αναλύστε τα στοιχεία του συστήματος

2) Προσδιορίστε το κύκλο ζωής τους και τους εμπλεκόμενους χρήστες..

3) Σε κάθε φάση του  κύκλοθ ζωής και καθε στοιχείο του συστήματος ΤΝ ,  βείτε τις απειλές (χρησιμοποιώντας την βάση του [OWASP](https://owaspai.org/)) .

4) Προτείνετε τα αντίμετρα για κάθε απειλή

5) Ακολουθήστε τα βήματα ανάλυσης επικινδυνότητητας και υπολογίστε την επικνδυνότητα για κάθε απειλή, για κάθε στοιχείο του TN συστήματος για κάθε φάση του κύκλου ζωής του συστήματος .