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  κύκλο ζωής και κάθε στοιχείο του συστήματος ΤΝ ,  βρείτε τις απειλές (χρησιμοποιώντας την βάση του [OWASP](https://owaspai.org/)) .

4) Προτείνετε τα αντίμετρα για κάθε απειλή

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

Το σύστημα Τεχνητής Νοημοσύνης που αναλύουμε είναι ένα σύστημα ελέγχου χάλυβα. Ο χάλυβας είναι ένα κράμα σιδήρου και άνθρακα, το οποίο αποτελεί ένα από τα πιο σημαντικά υλικά στην κατασκευή και τη βιομηχανία. Ο χάλυβας περιέχει κυρίως σίδηρο, ενώ το ποσοστό του άνθρακα κυμαίνεται συνήθως μεταξύ 0,02% και 2%. Ο χάλυβας έχει ποικιλία εφαρμογών σε πολλές κατασκευές, με κυριότερες την κατασκευή μεγάλων κτηρίων και γεφυρών, τα οποία αποτελούν κρίσιμες υποδομές.