ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Πληροφορικής



Εργασία Μαθήματος ***Ασφάλεια Δικτύων και Επικοινωνιών***

|  |  |
| --- | --- |
| Αρ. Άσκησης – Τίτλος Ασκησης |  |
| Όνομα φοιτητή – Αρ. Μητρώου  (όλων σε περίπτωση ομαδικής εργασίας) |  |
|  |
|  |
|  |
| Ημερομηνία παράδοσης |  |

**Εκφώνηση της άσκησης**

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

Contents

[Νοητό Case Study: SteelInspectAI 4](#_Toc187498760)

[1.Εισαγωγή 4](#_Toc187498761)

[2. Ανάλυση Στοιχείων του Συστήματος 5](#_Toc187498762)

[3. Κύκλος Ζωής και Εμπλεκόμενοι Χρήστες 5](#_Toc187498763)

[4. Αναγνώριση Απειλών 6](#_Toc187498764)

[5. Ανάλυση Επικινδυνότητας (Risk Assessment) 6](#_Toc187498765)

[6. Σχέδιο Αντιμετώπισης Κινδύνων (Risk Treatment Plan) 7](#_Toc187498766)

[7. Ανάλυση Επικινδυνότητας για Κάθε Φάση του Κύκλου Ζωής 8](#_Toc187498767)

# Νοητό Case Study: SteelInspectAI

Η "SteelInspectAI" είναι ένα σύστημα ΤΝ που χρησιμοποιείται σε ένα εργοστάσιο χάλυβα για την αυτοματοποιημένη αξιολόγηση της ποιότητας των παραγόμενων προϊόντων. Το σύστημα εφαρμόζει αλγόριθμους μηχανικής μάθησης και τεχνητής νοημοσύνης για τη βελτιστοποίηση της διαδικασίας ελέγχου ποιότητας και τη μείωση αποβλήτων.

# **1.Εισαγωγή**

Το σύστημα ΤΝ "SteelInspectAI" αξιολογεί την ποιότητα του χάλυβα που παράγεται σε πραγματικό χρόνο, εντοπίζοντας ελαττώματα και αποκλίσεις από τα πρότυπα. Το σύστημα ενσωματώνεται στην παραγωγική διαδικασία και παρέχει αναφορές στους διαχειριστές του εργοστασίου.

Kύριες Λειτουργίες:

* Ανάλυση οπτικών δεδομένων από αισθητήρες και κάμερες.
* Συγκριτική αξιολόγηση με πρότυπα ποιότητας.
* Παροχή συστάσεων για διορθωτικές ενέργειες.

# 2. Ανάλυση Στοιχείων του Συστήματος

Το σύστημα αποτελείται από κρίσιμα περιουσιακά στοιχεία όπως τη βάση δεδομένων SteelData\_v1, το μοντέλο QualityAI\_v2 και κάμερες υψηλής ανάλυσης. Αυτά συνεργάζονται μέσω ασφαλούς υποδομής για την παροχή άμεσων και ακριβών αποτελεσμάτων ελέγχου. Παράλληλα, η προστασία δεδομένων διασφαλίζεται με χρήση προηγμένων τεχνολογιών όπως κρυπτογράφηση και firewalls.

**Περιουσιακά Στοιχεία:**

1. **SteelData\_v1:** Βάση δεδομένων με ιστορικά δεδομένα παραγωγής και ποιότητας.
2. **QualityAI\_v2:** Μοντέλο ΤΝ για την αξιολόγηση ποιότητας.
3. **FactoryServer01:** Εξυπηρετητής επεξεργασίας δεδομένων παραγωγής.
4. **InspectionCameras:** Κάμερες υψηλής ανάλυσης για την ανάλυση προϊόντων.
5. **FactoryControlPortal:** Διαδικτυακή πλατφόρμα παρακολούθησης και αναφορών.
6. **Backup\_Storage\_AWS:** Αντίγραφα ασφαλείας δεδομένων.
7. **Firewall\_FORTINET01:** Προστασία δικτύου εργοστασίου.
8. **MaintenanceBot:** Αυτοματοποιημένος μηχανισμός διαγνωστικών και συντήρησης.
9. **John Greek (AI Engineer):** Υπεύθυνος ανάπτυξης και συντήρησης του μοντέλου ΤΝ.

# 3. Κύκλος Ζωής και Εμπλεκόμενοι Χρήστες

Το σύστημα ακολουθεί έναν πλήρη κύκλο ζωής που περιλαμβάνει τον σχεδιασμό, την ανάπτυξη, την εφαρμογή, τη συντήρηση και την απόσυρση. Κατά τη φάση συντήρησης, διασφαλίζεται η συνεπής απόδοση και η συμμόρφωση με τις απαιτήσεις της βιομηχανίας. Οι εμπλεκόμενοι περιλαμβάνουν μηχανικούς ΤΝ, διαχειριστές συστημάτων, και υπευθύνους συμμόρφωσης.

**Φάσεις Κύκλου Ζωής:**

1. **Σχεδιασμός:** Καθορισμός απαιτήσεων και ανάπτυξη του συστήματος.
   * **Εμπλεκόμενοι:** Αναλυτές συστημάτων, διαχειριστές έργων.
2. **Ανάπτυξη:** Δημιουργία και εκπαίδευση του μοντέλου ΤΝ.
   * **Εμπλεκόμενοι:** Προγραμματιστές, ειδικοί ΤΝ.
3. **Εφαρμογή:** Εγκατάσταση και ενσωμάτωση στο εργοστάσιο.
   * **Εμπλεκόμενοι:** Διαχειριστές συστημάτων.
4. **Συντήρηση:** Παρακολούθηση, αναβάθμιση και βελτιστοποίηση.
   * **Εμπλεκόμενοι:** Υπεύθυνοι τεχνικής υποστήριξης.
5. **Απόσυρση:** Αντικατάσταση ή παύση λειτουργίας του συστήματος.
   * **Εμπλεκόμενοι:** Υπεύθυνοι συμμόρφωσης.

# 4. Αναγνώριση Απειλών

Το σύστημα αντιμετωπίζει διάφορες απειλές, όπως διαρροές δεδομένων, επιθέσεις DDoS, και SQL injections. Για κάθε περιουσιακό στοιχείο έχουν αναγνωριστεί συγκεκριμένες απειλές που θα μπορούσαν να επηρεάσουν τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων.

|  |  |  |
| --- | --- | --- |
| **Περιουσιακό Στοιχείο** | **Απειλή** | **Περιγραφή** |
| SteelData\_v1 | Διαρροή δεδομένων | Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα παραγωγής. |
| QualityAI\_v2 | Δηλητηρίαση δεδομένων | Εισαγωγή ανακριβών δεδομένων εκπαίδευσης. |
| FactoryServer01 | Επιθέσεις DDoS | Υπερφόρτωση εξυπηρετητή. |
| InspectionCameras | Κακόβουλη παρέμβαση | Παραποίηση δεδομένων μέσω κακόβουλης πρόσβασης. |
| FactoryControlPortal | SQL Injection | Εισαγωγή κακόβουλων εντολών. |
| Backup\_Storage\_AWS | Απώλεια δεδομένων | Αδυναμία ανάκτησης αντιγράφων ασφαλείας. |
| Firewall\_FORTINET01 | Παραβίαση προστασίας δικτύου | Παράκαμψη του firewall από εξελιγμένες απειλές. |
| MaintenanceBot | Μη εξουσιοδοτημένη πρόσβαση | Παρέμβαση στη λειτουργία του μηχανισμού συντήρησης. |

# Ανάλυση Επικινδυνότητας (Risk Assessment)

Η εκτίμηση των κινδύνων έγινε με βάση την πιθανότητα εμφάνισης απειλών και τη σοβαρότητα των επιπτώσεων. Τα κρίσιμα περιουσιακά στοιχεία όπως το SteelData\_v1 και το FactoryServer01 έχουν υψηλό επίπεδο κινδύνου λόγω της πιθανής διαρροής δεδομένων και των επιθέσεων DDoS, ενώ προτάθηκαν στοχευμένα μέτρα μετριασμού.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Περιουσιακό Στοιχείο** | **Απειλή** | **Πιθανότητα** | **Σοβαρότητα** | **Κίνδυνος** |
| SteelData\_v1 | Διαρροή δεδομένων | Υψηλή | Υψηλή | Υψηλός |
| QualityAI\_v2 | Δηλητηρίαση δεδομένων | Μέτρια | Υψηλή | Μέτριος |
| FactoryServer01 | Επιθέσεις DDoS | Μέτρια | Υψηλή | Μέτριος |
| InspectionCameras | Κακόβουλη παρέμβαση | Μέτρια | Μέτρια | Μέτριος |
| FactoryControlPortal | SQL Injection | Υψηλή | Υψηλή | Υψηλός |
| Backup\_Storage\_AWS | Απώλεια δεδομένων | Χαμηλή | Υψηλή | Μέτριος |
| Firewall\_FORTINET01 | Παραβίαση προστασίας δικτύου | Μέτρια | Υψηλή | Μέτριος |
| MaintenanceBot | Μη εξουσιοδοτημένη πρόσβαση | Χαμηλή | Μέτρια | Χαμηλός |

# Σχέδιο Αντιμετώπισης Κινδύνων (Risk Treatment Plan)

Προτάθηκαν συγκεκριμένα μέτρα για κάθε απειλή, όπως κρυπτογράφηση δεδομένων, εγκατάσταση Anti-DDoS λύσεων, και εφαρμογή προετοιμασμένων ερωτημάτων SQL. Τα μέτρα αυτά διασφαλίζουν την ασφάλεια του συστήματος και τη συνεχή λειτουργία του.

|  |  |  |
| --- | --- | --- |
| **Περιουσιακό Στοιχείο** | **Απειλή** | **Μέτρα Μετριασμού** |
| SteelData\_v1 | Διαρροή δεδομένων | Κρυπτογράφηση AES-256, RBAC, τακτικοί έλεγχοι ασφαλείας. |
| QualityAI\_v2 | Δηλητηρίαση δεδομένων | Έλεγχος ποιότητας δεδομένων, ανίχνευση ανωμαλιών. |
| FactoryServer01 | Επιθέσεις DDoS | Anti-DDoS λύσεις, χρήση CDN, παρακολούθηση σε πραγματικό χρόνο. |
| InspectionCameras | Κακόβουλη παρέμβαση | Ασφαλής διαμόρφωση συσκευών, έλεγχος πρόσβασης. |
| FactoryControlPortal | SQL Injection | Χρήση προετοιμασμένων ερωτημάτων SQL, WAF. |
| Backup\_Storage\_AWS | Απώλεια δεδομένων | Τακτικές δοκιμές ανάκτησης, γεωγραφικά απομακρυσμένα αντίγραφα. |
| Firewall\_FORTINET01 | Παραβίαση προστασίας δικτύου | Τακτικές ενημερώσεις, δοκιμές αντοχής. |
| MaintenanceBot | Μη εξουσιοδοτημένη πρόσβαση | Πολιτικές ελέγχου πρόσβασης, έλεγχοι ταυτότητας. |

Η SteelInspectAI αποτελεί κρίσιμο στοιχείο της παραγωγικής διαδικασίας του εργοστασίου χάλυβα. Με τη χρήση προηγμένων αλγορίθμων ΤΝ, εξασφαλίζει υψηλή ποιότητα προϊόντων και μειώνει την πιθανότητα σφαλμάτων. Η συνεχής αναθεώρηση και παρακολούθηση του συστήματος είναι απαραίτητες για την αντιμετώπιση μελλοντικών προκλήσεων και την προσαρμογή σε νέες απειλές.

# Ανάλυση Επικινδυνότητας για Κάθε Φάση του Κύκλου Ζωής

**1. Σχεδιασμός**

**Απειλή:** Ελλιπής προδιαγραφή απαιτήσεων ασφαλείας.

**Περιγραφή:** Κακή διατύπωση ή μη ενσωμάτωση απαιτήσεων ασφαλείας κατά τη φάση του σχεδιασμού.

**Πιθανότητα:** Μέτρια.

**Σοβαρότητα:** Υψηλή.

**Κίνδυνος:** Μέτριος.

**Μέτρα Μετριασμού:** Ενσωμάτωση αρχών Security by Design, τακτικοί έλεγχοι απαιτήσεων, και ανασκόπηση από ειδικούς ασφαλείας.

**2. Ανάπτυξη**

**Απειλή:** Δηλητηρίαση δεδομένων εκπαίδευσης (Data Poisoning).

**Περιγραφή:** Χρήση μη αξιόπιστων δεδομένων για την εκπαίδευση του μοντέλου ΤΝ, οδηγώντας σε μη ακριβείς προβλέψεις.

**Πιθανότητα:** Μέτρια.

**Σοβαρότητα:** Υψηλή.

**Κίνδυνος:** Μέτριος.

**Μέτρα Μετριασμού:** Ανίχνευση ανωμαλιών στα δεδομένα, χρήση επαληθευμένων πηγών δεδομένων, και περιοδικές αξιολογήσεις του μοντέλου.

**3. Εφαρμογή**

**Απειλή:** SQL Injection στο FactoryControlPortal.

**Περιγραφή:** Εισαγωγή κακόβουλων εντολών μέσω των φορμών εισαγωγής δεδομένων της πλατφόρμας.

**Πιθανότητα:** Υψηλή.

**Σοβαρότητα:** Υψηλή.

**Κίνδυνος:** Υψηλός.

**Μέτρα Μετριασμού:** Εφαρμογή προετοιμασμένων ερωτημάτων SQL, τακτική παρακολούθηση της εφαρμογής, και χρήση WAF (Web Application Firewall).

**4. Συντήρηση**

**Απειλή:** Επιθέσεις DDoS στο FactoryServer01.

**Περιγραφή:** Μαζικές αιτήσεις που προκαλούν υπερφόρτωση του διακομιστή, με αποτέλεσμα την παύση της υπηρεσίας.

**Πιθανότητα:** Μέτρια.

**Σοβαρότητα:** Υψηλή.

**Κίνδυνος:** Μέτριος.

**Μέτρα Μετριασμού:** Εγκατάσταση Anti-DDoS λύσεων, χρήση CDN για απορρόφηση του φορτίου, και παρακολούθηση του δικτύου σε πραγματικό χρόνο.

**5. Απόσυρση**

**Απειλή:** Απώλεια δεδομένων κατά τη διαδικασία απόσυρσης.

**Περιγραφή:** Μη ασφαλής διαγραφή δεδομένων που μπορεί να οδηγήσει σε διαρροές.

**Πιθανότητα:** Χαμηλή.

**Σοβαρότητα:** Υψηλή.

**Κίνδυνος:** Μέτριος.

**Μέτρα Μετριασμού:** Χρήση προτύπων ασφαλούς διαγραφής (π.χ. DoD 5220.22-M), επιβεβαίωση διαγραφής, και δημιουργία αναφορών συμμόρφωσης.

Η παραπάνω ανάλυση επικεντρώνεται στην αξιολόγηση της επικινδυνότητας σε κάθε φάση του κύκλου ζωής του συστήματος. Οι κίνδυνοι κατηγοριοποιήθηκαν με βάση την πιθανότητα και τη σοβαρότητα, και προτάθηκαν κατάλληλα μέτρα μετριασμού για τη διασφάλιση της ασφάλειας του συστήματος.