

ΣΕΝΑΡΙΑ ΕΦΑΡΜΟΓΗΣ



Honeyrot Υψηλής Αλληλεπίδρασης για την Προστασία Βιομηχανικών Δικτύων

Άμυνα απέναντι σε επιθέσεις που καθοδηγούνται από Τεχνητή Νοημοσύνη (AI) σε βιομηχανικά δίκτυα βασισμένα στο πρωτόκολλο Modbus.

Τα Honeyrots Υψηλής Αλληλεπίδρασης και οι Ψηφιακοί Δίδυμοι αναπτύσσονται εντός της βιομηχανικής υποδομής για την υλοποίηση στρατηγικών παραπλάνησης, ενώ η πλατφόρμα AIAS αξιοποιεί τα δεδομένα που συλλέγονται για τη βελτίωση των μηχανισμών ανίχνευσης και αντιμετώπισης επιθέσεων.



Προστασία Συστημάτων Ανίχνευσης Κακόβουλου Λογισμικού από Επιθέσεις Adversarial AI

Ανίχνευση και απόκριση σε adversarial AI επιθέσεις κατά συστημάτων ανίχνευσης κακόβουλου λογισμικού (malware detection) μέσω του εργαλείου AIAS Weaponizer.

Με τη δημιουργία συνθετικού κακόβουλου λογισμικού και την ανίχνευση ανωμαλιών καθοδηγούμενη από Τεχνητή Νοημοσύνη, εντοπίζονται και μετριάζονται στοχευμένες επιθέσεις κατά των μηχανών ανίχνευσης malware.



IoT-Πλατφόρμα Περιβαλλοντικής Παρακολούθησης με Ψηφιακούς Δίδυμους για Προσομοίωση και Παραπλάνηση

Μια πειραματική πλατφόρμα για την αξιολόγηση σεναρίων απειλών σε οικοσυστήματα Internet of Things (IoT). Αξιοποιώντας Ψηφιακούς Δίδυμους, η προσέγγιση αυτή επιτρέπει την προσομοίωση και την παραπλάνηση σε συστήματα περιβαλλοντικής παρακολούθησης, με στόχο τη βελτίωση της ασφάλειας, της αξιοπιστίας και της ανθεκτικότητας αυτοματοποιημένων χώρων.



Συνδυασμός Ψηφιακών Διδύμων και Ψηφιακών Προσωπικότητων στον Τομέα της Υγείας για Ανίχνευση Ανωμαλιών με χρήση Τεχνητής Νοημοσύνης

Ενώ οι Ψηφιακοί Δίδυμοι αναπαριστούν με ακρίβεια τη συμπεριφορά των συστημάτων, ο συνδυασμός τους με Ψηφιακές Προσωπικότητες (VPs) επιτρέπει τη μοντελοποίηση και ανάλυση από την οπτική των ενδιαφερόμενων μερών. Εφαρμοσμένο στον τομέα της υγείας, το μοντέλο αυτό συμβάλλει όχι μόνο στη λήψη αποφάσεων, αλλά και στην ανάλυση παραμέτρων ασφάλειας.



Καινοτόμος Ευφυής Μηχανισμός Παραπλάνησης για την Προστασία Συστημάτων Μικρομεσαίων Επιχειρήσεων (SMEs)

Οι ψηφιακές υπηρεσίες των ΜΜΕ αποτελούν στόχο πολλών επιθέσεων που αξιοποιούν Τεχνητή Νοημοσύνη.

Η πλατφόρμα AIAS εξετάζει τον τρόπο με τον οποίο οι επιτιθέμενοι αλληλεπιδρούν με τα συστήματα των επιχειρήσεων, συλλέγοντας νέα δεδομένα και μοτίβα επιθέσεων, ώστε να ενισχύεται συνεχώς η ασφάλεια των υπηρεσιών.



AI-ASSISTED CYBERSECURITY PLATFORM

Δεκέμβριος 2025



HORIZON-MSCA-2022-SE-01-01;
HORIZON.1.2 - Marie Skłodowska-Curie Actions
(MSCA)

Ιστοσελίδα έργου: <https://www.ias-project.eu/>

Έναρξη έργου: 1η Ιανουαρίου 2025

Διάρκεια: 48 μήνες

GRANT AGREEMENT: 101131292

EU CONTRIBUTION: EUR 1 564 000

Συντονιστής έργου: Κέντρο Ερευνών Πανεπιστημίου Πειραιώς
(ΕΛΛΑΔΑ)

ΚΑΙΝΟΤΟΜΕΣ ΕΥΦΥΕΙΣ ΜΕΘΟΔΟΙ ΠΑΡΑΠΛΑΝΗΣΗΣ

Το έργο AIAS βασίζεται σε πρωτοποριακές λύσεις παραπλάνησης (deception) για την αξιολόγηση πληροφοριών απειλών (threat intelligence).

Ψηφιακοί Δίδυμοι (Digital Twins)

Ψηφιακά αντίγραφα φυσικών πόρων ή συστημάτων που απεικονίζουν με ακρίβεια τη συμπεριφορά τους σε πραγματικό χρόνο. Επιτρέπουν τη λεπτομερή μελέτη λειτουργίας και τον εντοπισμό ανωμαλιών που μπορεί να υποδηλώνουν κινδύνους ή αστοχίες.

Ψηφιακές Προσωπικότητες (Virtual Personas)

Ψηφιακές οντότητες που αναπαριστούν ενδιαφερόμενους (stakeholders) του συστήματος. Μιμούνται την αλληλεπίδραση πραγματικών χρηστών, ανταποκρίνονται σε γεγονότα και προσθέτουν ένα επιπλέον επίπεδο ρεαλισμού στη δημιουργία εικονικών δολωμάτων (decoys).

Honeybots Υψηλής Αλληλεπίδρασης (High-Interaction Honeybots)

Συστήματα που δημιουργούν την ψευδαίσθηση εκτεθειμένων ευπαθειών, προσφέροντας υψηλό βαθμό ρεαλισμού. Ενώ οι επιτιθέμενοι επικεντρώνουν τις προσπάθειές τους στην εκμετάλλευση αυτών των «αδυναμιών», τα honeybots τους εμπλέκουν ώστε να εξαχθούν πολύτιμες πληροφορίες σχετικά με τις τακτικές και τα πρότυπα συμπεριφοράς τους. Παράλληλα, αποσπούν την προσοχή των επιτιθέμενων μακριά από κρίσιμα συστήματα και δεδομένα.

ΔΙΕΘΝΗΣ ΣΥΝΕΡΓΑΣΙΑ



ΜΕΘΟΔΟΛΟΓΙΑ

1η Φάση: Ορισμός Απαιτήσεων και Κύριων Συνιστωσών της Πλατφόρμας

- Προσδιορισμός των απαιτήσεων του συστήματος
- Διεξαγωγή ανασκόπησης ερευνητικής και τεχνολογικής προόδου (State of the Art) στους τομείς: Μεθόδων παραπλάνησης (deception methods), Ανίχνευσης καθοδηγούμενης από Τεχνητή Νοημοσύνη, και Μεθόδων αντιμετώπισης και περιορισμού επιθέσεων
- Καθορισμός εργαλείων και εφαρμογών για την υλοποίηση κάθε επιμέρους συνιστώσας του AIAS

2η Φάση: Υλοποίηση και Επικύρωση των Κύριων Συνιστωσών της Πλατφόρμας

- Deception Layer
- Adversarial AI engine Module
- Security Data Fusion
- AI-based Detection Module
- Mitigation of Adversarial AI Attacks Module

3η Φάση: Ενοποίηση, Απόδειξη Λειτουργικότητας και Αξιολόγηση σε Πραγματικές Συνθήκες

For more information
visit our website or follow us

