

SCENARII DE ATAC



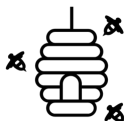
Platformă DT-IoT pentru monitorizarea mediului – simulare și decepție

O platformă orientată spre experimentare, destinată evaluării scenariilor de amenințare din ecosistemele IoT. Folosind tehnologii Digital Twin (DT), această abordare integrează atât simularea, cât și tehnici de decepție pentru sistemele de monitorizare a mediului, cu scopul de a îmbunătăți siguranța, fiabilitatea și robustețea spațiilor automatizate.



DT asistat de VP pentru asistență medicală – detectarea anomaliilor bazată pe inteligență artificială

În timp ce Digital Twin reproduce cu acuratețe comportamentul sistemului, combinarea sa cu tehnologiile Virtual Persona (VP) permite simularea și raționamentul bazate pe perspectiva părților interesate. Aplicată în domeniul asistenței medicale, această abordare contribuie atât la sprijinirea deciziilor clinice, cât și la analiza situațiilor care pot afecta siguranța pacienților.



Honeypot cu interacțiune ridicată pentru protecția rețelelor industriale

O soluție de apărare împotriva amenințărilor bazate pe inteligență artificială în rețele industriale care utilizează protocolul Modbus, luând în considerare atât atacurile la nivel de rețea, cât și pe cele adversariale. Honeypot-urile cu interacțiune ridicată (HIH) și Digital Twins (DT) implementați în infrastructura industrială sunt folosiți pentru decepție, în timp ce platforma AIAS contribuie la detectarea și atenuarea atacurilor.



Protecția sistemelor de detectare a malware-ului împotriva atacurilor adversariale

Identificarea și răspunsul la atacurile adversariale asupra sistemelor de detecție a malware-ului bazate pe inteligență artificială sunt realizate cu ajutorul instrumentului AIAS Weaponizer. Prin generarea de mostre sintetice de malware și utilizarea detectării anomaliilor bazate pe IA, sistemul poate identifica și contracara atacurile adversariale îndreptate împotriva motorului de detecție.



Tehnici inteligente de decepție pentru apărarea serviciilor IMM-urilor

Serviciile digitale atrag tot mai des atacuri bazate pe inteligență artificială ostilă. Această platformă inovatoare analizează modul în care atacatorii interacționează cu sistemele IMM-urilor, extrăgând informații și modele de atac ce contribuie la dezvoltarea unor mecanisme de securitate mai eficiente și adaptabile.



PLATFORMA DE SECURITATE CIBERNETICĂ ASISTATĂ DE AI

DECEMBRIE, 2025



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

PROJECT WEBSITE: <https://www.aias-project.eu/>
PROJECT START: 1st January 2024
DURATION: 48 months
GRANT AGREEMENT: 101131292
EU CONTRIBUTION: EUR 1 564 000
COORDINATION: University of Piraeus Research Center (Greece)

METODE INOVATOARE DE DECEPTIE INTELIGENTĂ

Proiectul AIAS se bazează pe soluții de ultimă generație pentru evaluarea și analiza informațiilor privind amenințările, integrând tehnologii avansate precum Digital Twin (DT), Virtual Persona (VP) și Honeypot-uri cu interacțiune ridicată (HIH).

Digital Twin (DT)

Reprezintă replici digitale ale activelor fizice, care reflectă cu acuratețe comportamentul acestora în timp real. Prin intermediul DT-urilor, este posibilă monitorizarea, simularea și analiza dinamică a sistemului, facilitând identificarea timpurie a stărilor anormale ce pot compromite funcționarea optimă sau securitatea infrastructurii.

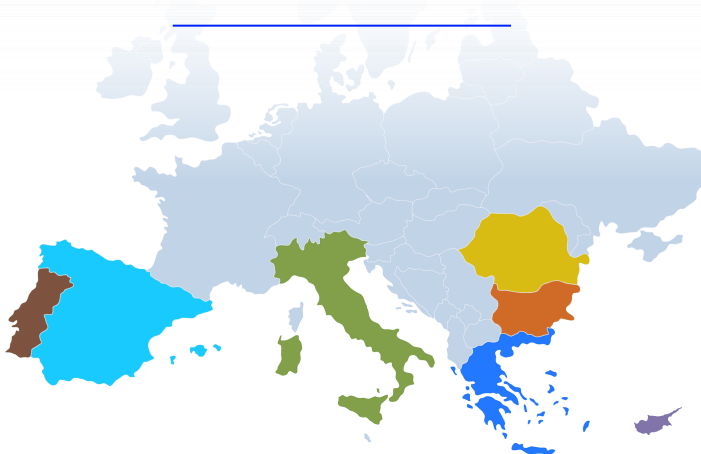
Virtual Persona (VP)

Sunt reprezentări digitale ale părților interesate din cadrul sistemului, capabile să imite comportamente și interacțiuni specifice identităților reale. VP-urile răspund în mod autonom la evenimentele din sistem, oferind un plus de realism și complexitate în cadrul proceselor de simulare și generare de momeli virtuale utilizate în strategiile de deceptie.

Honeypot-uri cu interacțiune ridicată (HIH)

Sunt implementări de sistem concepute pentru a simula vulnerabilități reale, oferind un grad ridicat de realism și implicare a atacatorilor. În timp ce aceștia își concentrează eforturile pe exploatarea acestor puncte aparent slabe, honeypot-ul captează și analizează comportamentele și modelele de atac. Astfel, HIH contribuie nu doar la colectarea de informații valoroase despre activitatea adversarilor, ci și la distragerea atenției acestora de la componentele critice ale infrastructurii.

COLABORARE INTERNAȚIONALĂ



METODOLOGIE

Faza 1: Definirea cerințelor sistemului și a componentelor principale ale platformei:

- Identificarea și definirea cerințelor funcționale și nefuncționale ale sistemului
- Realizarea unei analize state-of-the-art (SOTA) privind: metode de deceptie, tehnici de detectare bazată pe inteligență artificială (IA) și strategii de atenuare a atacurilor adversariale
- Specificarea instrumentelor, tehnologiilor și aplicațiilor utilizate pentru implementarea fiecărui modul AIAS

Faza 2: Implementarea și validarea componentelor principale ale platformei:

- Stratul de deceptie
- Modulul motorului AI adversarial
- Fuziunea datelor de securitate
- Modulul de detectare bazat pe IA
- Modulul de atenuare a atacurilor AI adversariale

Faza 3: Integrare, validare a conceptului și evaluare în condiții reale.

Pentru mai multe informații, vizitați site-ul nostru web sau urmăriți-ne

