

ESCENARIOS DE ATAQUE



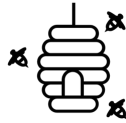
Plataforma IoT basada en GD de monitorización ambiental para simulación y engaño

Una plataforma orientada a la experimentación para evaluar escenarios de amenazas dentro de los ecosistemas del IoT. Aprovechando los GD, este enfoque evalúa tanto la simulación como el engaño para los sistemas de monitorización medioambiental con el objetivo de mejorar la seguridad, la fiabilidad y la robustez de los espacios automatizados.



GD asistido por PV para la atención sanitaria potenciado por detección de anomalías basada en IA

Los GD imitan con precisión los comportamientos del sistema. Además, su combinación con tecnologías PV permite la simulación y el razonamiento basados en la perspectiva de las partes interesadas. Aplicados al ámbito sanitario, los PV pueden contribuir no solo a la toma de decisiones, sino también al análisis de las circunstancias de seguridad.



Honeypots de alta interacción para la protección de redes industriales

Defensa contra amenazas impulsadas por IA en redes industriales basadas en protocolos industriales como Modbus, teniendo en cuenta tanto los ataques a la red como los ataques adversarios. Se aprovechan los HAI y los GD desplegados en la infraestructura industrial para el engaño, mientras que la plataforma AIAS aprovecha la detección y mitigación de los ataques.



Protección de los motores de detección de malware contra ataques adversarios

Identificación y respuesta contra ataques adversarios dirigidos hacia la detección de malware basada en IA utilizando la herramienta weaponizer de AIAS. Mediante la generación de malware sintético y la detección de anomalías impulsada por IA, se detectan los ataques adversarios contra el motor de detección de malware.



Métodos novedosos de engaño para la defensa de pymes

Los servicios digitales basados en IA atraen el interés de ataques adversarios por parte de los atacantes. Esta novedosa plataforma examina cómo interactúan los atacantes con los sistemas de las pymes, recuperando información novedosa y patrones de ataque que mejoran aún más la seguridad del sistema.



PLATAFORMA DE CIBERSEGURIDAD ASITIDA POR IA

DICIEMBRE, 2025



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

PÁGINA WEB: [HTTPS://WWW.AIAS-PROJECT.EU/](https://www.aias-project.eu/)
INICIO DEL PROYECTO: 1 de enero de 2024
DURACIÓN: 48 meses
ACUERDO: 101131292
FONDOS EUROPEOS: EUR 1 564 000
COORDINACIÓN: University of Piraeus Research Center (Grecia)

MÉTODOS DE ENGAÑO INTELIGENTES

El proyecto AIAS se basa en los siguientes métodos de engaño punteros con el fin de extraer conocimiento sobre amenazas en sistemas críticos:

Gemelos Digitales (GD)

Los GD son replicas digitales de activos físicos que reflejan con precisión su comportamiento en tiempo real, lo que permite estudiar el sistema e identificar estados anormales que pueden comprometer el sistema.

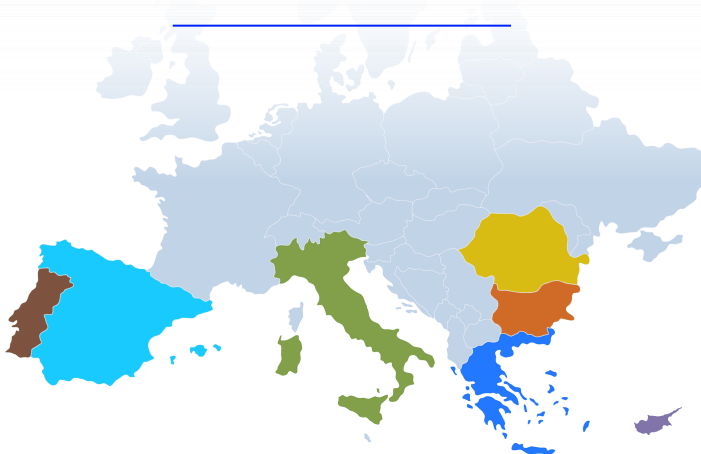
Personas Virtuales (PV)

Las PV son una representación digital de los distintos actores del sistema. Imitan con precisión la interacción de identidades reales, respondiendo a los eventos del sistema y proporcionando una capa adicional de realismo en la producción de señuelos virtuales.

Honeypots de Alta Interacción (HAI)

Los HAI son implementaciones que imitan sistemas reales para crear una falsa sensación de vulnerabilidades abiertas, ofreciendo un alto grado de realismo. Mientras los atacantes concentran sus esfuerzos en explotar estas características, el honeypot los atrae para extraer información valiosa sobre sus acciones y patrones. Los HAI no solo extraen inteligencia de la actividad adversaria, sino que también desvían a los atacantes de los componentes críticos.

COLABORACIÓN INTERNACIONAL



METODOLOGÍA

Fase 1: Identificación de los principales componentes y requisitos del sistema:

- Identificar y definir los requisitos
- Revisión del estado del arte en: métodos de engaño, detección basada en IA y métodos de mitigación
- Especificación de las herramientas y aplicaciones necesarias para la implementación de cada módulo de AIAS

Fase 2: Implementación y validación de los componentes principales de la plataforma:

- Capa de engaño
- Motor de IA adversaria
- Fusión de datos de ciberseguridad
- Módulo de detección basada en IA
- Módulo de mitigación de ataques de IA adversaria

Fase 3: Integración, estudio de prueba de concepto y evaluación en entornos reales.

Para más información visita nuestra web o síguenos en:

