

NCIS. Neutralización colaborativa de ciberataques en sistemas industriales preservando la privacidad

Consorcio: ITS; Fagor Automation; S2grupo; Ibermatica; Savvy; JAKINCODE; Tecnalía; Ikerlan

Tecnología: Blockchain; Ciberseguridad; Espacio de Datos

Descripción general:

El objetivo principal del proyecto es dotar al sector industrial de un espacio digital colaborativo que posibilite a las empresas desplegar mecanismos de ciberdefensa en ecosistemas de empresas industriales, a través de la compartición y explotación de datos y procedimientos de prevención, detección mitigación y remediación de forma colaborativa.

- NCIS tiene como objetivo realizar investigaciones avanzadas en ámbitos tecnológicos que impliquen novedades disruptivas en los siguientes dos ejes principales: la confidencialidad del dato y la compartición de estrategias de seguridad en nuevos entornos industriales conectados, contribuyendo así el pleno desarrollo de la industria 4.0 en entornos seguros, sostenibles y conectados.
- El proyecto plantea definir un marco común colaborativo que permita establecer los requisitos de privacidad, confidencialidad y confiabilidad de datos contribuyendo así al desarrollo de nuevos servicios basados en el intercambio de datos y su explotación.
- El proyecto tiene como objetivo proponer un marco de referencia para la colaboración en cuatro funciones fundamentales de cualquier sistema de gestión de ciberseguridad en ecosistemas industriales: prevención, detección, respuesta y recuperación.

<https://proyectosi3b.wixsite.com/ncis>

Programa: MISIONES Grandes Empresas – CDTI (MIG-20221060)

Duración: 36 meses (2022-2025)

Presupuesto global proyecto: 4.277.084,00 €

Presupuesto Grupo Ayesa: 567.725,00 €

Proyecto Subvencionado por el CDTI y apoyado por el Ministerio de Ciencia e Innovación



NCIS. Neutralización colaborativa de ciberataques en sistemas industriales preservando la privacidad

Consortio: ITS; Fagor Automation; S2grupo; Ibermatica; Savvy; JAKINCODE; Tecnalía; Ikerlan

Tecnología: Blockchain; Ciberseguridad; Espacio de Datos

Rol de Ayesa:

Ibermática desempeña en este proyecto un papel técnico relevante centrado en la gestión segura del dato, la integración de tecnologías avanzadas y la validación de soluciones en entornos reales de ciberseguridad industrial.

Su participación se inicia en el desarrollo e investigación de modelos avanzados de inteligencia artificial para la detección de ciberataques en infraestructuras industriales, colaborando en la adaptación de algoritmos para identificar tanto ataques conocidos como de día cero, y aplicando técnicas avanzadas de protección de datos como cifrado homomórfico o computación multipartita.

Además, contribuye al diseño y adaptación de arquitecturas basadas en aprendizaje colaborativo, participando en la integración de modelos de aprendizaje federado y técnicas de boosting para mejorar la eficiencia y precisión de los modelos en entornos distribuidos.

Ibermática tiene también un papel clave en el ámbito del gobierno del dato, investigando e implementando mecanismos que, combinados con tecnologías DLT, permitan garantizar la trazabilidad, integridad y confidencialidad de la información. En este contexto, trabaja con tecnologías como smart contracts, oráculos descentralizados y esquemas de autorización distribuida para automatizar respuestas ante incidentes de ciberseguridad.

Asimismo, participa en la integración de estos mecanismos dentro de plataformas operativas, facilitando la ejecución automatizada de procesos de detección, respuesta y recuperación frente a incidentes.

Finalmente, colabora en la validación del sistema en entornos de laboratorio, contribuyendo a la definición del escenario de experimentación y a la ejecución de pruebas de rendimiento, evaluando tanto la calidad de los resultados como aspectos clave como la latencia y la eficiencia de las soluciones desarrolladas.

