I+D+i

DOMINION

ZIBERURA (2024-2026)

Investigación y desarrollo en ciberseguridad industrial para el sector del agua como infraestructuras críticas.

Nº de expediente ZE-2024/00033 y otros del programa de ayudas de apoyo a la I+D empresarial HAZITEK.

Actuación cofinanciada por el Gobierno Vasco y la Unión Europea a través del Fondo Europeo de Desarrollo Regional 2021-2027 (FEDER)

Europar Batasunak kofinantzatua

Cofinanciado por la Union Europea

EUSKO JAURLARITZA GOBIERNO VASCO

En el marco del proyecto **ZIBERURA** se van a investigar las tecnologías de ciberseguridad industrial orientada al sector del agua, considerado una infraestructura crítica. El proyecto evaluará el impacto de los ciberataques desde el punto de vista social, económico y ambiental, así como la eficacia de los controles de seguridad aplicados.

El objetivo principal del proyecto **ZIBERURA** es la investigación en ciberseguridad industrial tomando como referencia el sector del agua, sobre el que se pretende normalizar una arquitectura de referencia mediante un entorno de preproducción híbrido que incorpore activos reales, virtuales y gemelos digitales para desarrollar enfoques ofensivos y defensivos en ciberseguridad. Este objetivo se obtendrá mediante la consecución de los siguientes objetivos particulares:

A) Definir la arquitectura de referencia e identificar las principales amenazas, técnicas y tácticas asociadas al dominio del agua tanto en ámbitos de depuración (WWTP) como de distribución (WDS).
B) Desarrollar un entorno híbrido de preproducción que integre activo reales sobre infraestructura virtualizada y gemelos digitales de procesos industriales tanto en ámbitos de depuración (WWTP) como de distribución (WDS).
C) Desarrollar un conjunto de pruebas de seguridad ofensivas basadas en frameworks como MITRE ATT&CK y modelos de seguridad como TARA sobre el entorno híbrido de preproducción.
D) Desarrollar y automatizar el despliegue de soluciones ciberseguras cubriendo todo el ciclo de vida de desarrollo del software (SDLC) y su monitorización.
E) Analizar la evolucionabilidad de las contramedidas hacia soluciones basadas en Automated Moving Target Defense (AMTD).
F) Evaluar el impacto económico, ambiental y social tanto en ámbitos de depuración (WWTP) como de distribución (WDS) del conjunto de técnicas y tácticas empleadas en el enfoque ofensivo.
G) Evaluar la madurez de las soluciones de ciberseguridad integradas en la infraestructura de preproducción con base a estándares como ISA/IEC 62443.
H) Definir directrices y buenas prácticas de seguridad de manera que puedan ser metodológicamente trasladadas sobre entornos de producción tanto en ámbitos de depuración (WWTP) como de distribución (WDS).

DOMINION