SUBTÍTULO

Buenas prácticas en Ciberseguridad Industrial

tecnalia

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

11 de junio de 2024
TECNALIA

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

ÍNDICE

TECNALIA y las buenas prácticas en Ciberseguridad Industrial

TECNALIA: ¿Quiénes somos?

- Ámbitos de actuación
- Tecnologías de Ciberseguridad

Buenas prácticas en ciberseguridad industrial: proyectos e iniciativas

- La importancia de sensibilizar y formar
- Investigación y desarrollo en tecnologías de ciberseguridad industrial

PRESENTACIÓN

TECNALIA: ¿Quiénes somos?

TECNALIA es el **mayor centro de investigación aplicada y desarrollo tecnológico de España**, un referente en Europa y miembro de *Basque Research and Technology Alliance*.

Con **1.520** personas expertas de **27** nacionalidades, orientadas a transformar la investigación tecnológica en prosperidad, ejerciendo de agentes de transformación de las **empresas** y de la **sociedad** para su adaptación a los retos de un futuro en continua evolución.

ÁMBITOS DE ACTUACIÓN

Nuestros ámbitos de actuación están alineados con los **Objetivos de Desarrollo Sostenible (ODS)**

Con una perspectiva **multisectorial** y **multitecnológica** escuchamos y trabajamos junto a las empresas e instituciones para dar respuesta a los **grandes desafíos globales**.

Transformación digital

Nos apasiona diseñar y desplegar cómo serán los procesos, productos y servicios digitales en un mundo cada vez más interconectado e interactivo. Para ello, desplegamos nuestra estrategia digital sobre tres drivers: inteligencia, seguridad y nuevos modelos de generación de valor.

Gracias a ellos desarrollamos una propuesta diferencial en la “economía del dato” para fabricantes e integradores de productos en base a ciberseguridad, *blockchain* e inteligencia artificial.

Más información

¿Qué podemos hacer por ti?

- Tecnologías cuánticas
- Inteligencia artificial
- Robótica y sistemas cognitivos
- Sistemas avanzados de interacción y trabajador 4.0
- Computación de alto rendimiento para datos masivos
- Ciclo de vida de sistemas y *DevOps*
- **Ciberseguridad y confianza**
- Internet de las cosas
- Sensórica y actuación
- Visión artificial
- Mantenimiento inteligente

tecnalia

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

PROYECTOS E INICIATIVAS

La importancia de sensibilizar y formar

Cyber Ranges

Laboratorios para ejercitarse y algunas iniciativas de interés realizadas

Cyber Range Lab

- Espacio físico que permite simular una infraestructura real IT/OT y ejecutar ejercicios de ciberseguridad.
- El objetivo final es entrenar, validar y experimentar en ciberseguridad.
- **Iniciativas desde la administración vasca** para integrar competencias en estudiantes de Formación Profesional del ámbito industrial.
- **Colaboración con el BID** para mejorar competencias de personal de infraestructuras críticas de energía en LATAM.

Smart Grid Cybersecurity Lab

- Orientado al diseño y operación de subestaciones eléctricas seguras, mejorando la detección de ciberataques.
- Colaboración con empresas del sector eléctrico como (**Ingeteam, Arteche, ZIV, Fanox, Isotrol**) y Proveedores de ciberseguridad i (**S2 Grupo, Grupo Ayesa**)
- Definición de arquitecturas, topologías y elementos seguros para la Smart Grid (**General Electric, Schneider, Ormazabal, ZIV, Arteche, Ingeteam**)
- Ethical Hacking

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

PROYECTOS E INICIATIVAS

I+D en tecnologías de ciberseguridad industrial

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Ciberseguridad y confianza:

Tecnologías

Applied Cryptography & IoT Security

Privacy-Preserving Computation

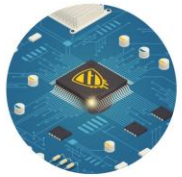
Técnicas de procesado seguro para proteger la confidencialidad de los datos y algoritmos.

Secure Virtualization

Políticas y entornos seguros para proteger los entornos virtuales de ejecución.

Trusted Execution Environment

Despliegue de chips criptográficos para la custodia de claves y ejecución de algoritmos criptográficos en dispositivos embebidos.



Lightweight Cryptography

Criptografía ligera para entornos críticos en tiempo real.

Detection & Cyberintelligence technologies

Threat and Anomaly Detection

Inteligencia artificial aplicada a la detección de anomalías.

SOAR
(Security Orchestration, Automation and Response)

Inteligencia artificial aplicada a la automatización y respuesta de incidentes.

Honeypots & Honeynets

Herramientas de seguridad e infraestructuras de señuelo utilizadas para atraer intentos de ataque y detectar actividades malintencionadas.

Threat Intelligence Federation

Sistema de registro distribuido diseñado para federar información de ciberinteligencia.

Distributed Ledger Technologies

Self-Sovereign Identity

Sistemas de gestión descentralizados para devolver al usuario el control total de su identidad.

Web3, tokens & oracles

Tecnologías para la creación de la nueva Internet descentralizada.

Decentralized Data Spaces

Técnicas criptográficas para la descentralización de la gobernanza y la operación en espacios de datos.

Zero Knowledge Protocols

Protocolos criptográficos para probar y verificar de forma fiable que una información es cierta.

Compliance & Certification

Diseño de herramientas de certificación

Protocolos de redes y sistemas para que las certificaciones sean ciberseguras.

Conformidad de normas industriales

Requisitos y especificaciones para garantizar el cumplimiento normativo.

Cyber Ranges

Desarrollo de escenarios de ataque

Escenarios para distintos tipos de ejercicio que permiten entrenamientos que mejoren las competencias y conciencien sobre ciberseguridad.

Ejecución de ataques en laboratorios industriales BDIH

Laboratorios industriales y cyber-ranges combinados para que la experiencia sea más completa y real.

Quantum Security & Post Quantum Cryptography

Post-Quantum Cryptography

Criptografía resistente al adversario cuántico que tiene como objetivo proteger la información almacenada y en tránsito.

Quantum Cryptography

Criptografía basada en estados cuánticos que permiten cifrar y descifrar mensajes y mejorar la seguridad de los sistemas de comunicación.

Quantum Key Distribution

Técnicas para la distribución de claves cuánticas en comunicaciones seguras.

Inteligencia Artificial aplicada a Ciberseguridad

Buenas prácticas en “Ciber-inteligencia”

Algunos ejemplos de dónde estamos aplicamos ML, IA Generativa, …

Extracción de datos de ciberseguridad de **fuentes de información abiertas sobre ciberamenazas**.

Inspección de la Deep/Dark web y otros canales para obtener información de ciberincidentes.

Perfilado de Sistemas OT en redes industriales.

Priorización de tickets en SOCs para maximizar la eficiencia en la respuesta antes un incidente.

Preparación

Automatización de búsquedas y **priorización de vulnerabilidades (CVE)** según el inventario de activos de la compañía**.**

Simulación de ciberataques basados en IA capades de emular ataques avanzados contra sistemas IT, OT and IoT systems

Respuesta

Detección

Anomalías en el comportamiento de usuarios, a través del análisis de logs del Sistema que pueden dar indicios sobre actividades sospechosas.

Anomalías en redes de comunicación OT en tiempo real a través del análisis y correlación de datos de los flujos de información.

Anomalías en Sistemas ciberfísicos a través del análisis del comportamiento de parámetros que den indicios de problemas asociados a su diseño y/o potenciales ataques.

MAK 21: Hacia la máquina del siglo XXI

Máquina eficiente y segura con capacidad de aprendizaje y toma de decisiones para el ahorro de materia prima y energía (*)

Caso de Uso: máquina CNC de DENN

(Industrias Puigjaner)

CONSORCIO DE EMPRESAS

DENN · DIMECO · asai INDUSTRIAL · CodeSyntax · RKL integral

Objetivo:

Detectar problemas en el comportamiento de los elementos digitales de una máquina de repulsado con el fin de identificar:

- Ciberataques.
- Posibles errores de diseño.

Solución:

- Tipología de anomalías de interés:
  - Uso de recursos del sistema
  - Cambios y accesos no autorizados a ficheros sensibles.
  - Transferencia de datos segura entre máquina y servidor.
  - Intento de inicios de sesión no autorizados.
- Uso de modelos de Machine Learning sobre parámetros relativos al uso de los recursos del sistema (consumo de CPU, RAM total, RAM por aplicación,…)

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

(*) Este proyecto se enmarca bajo el programa MISIONES del Centro de Desarrollo Tecnológico Industrial (CDTI) y será posible gracias a los fondos europeos asignados al Mecanismo de Recuperación y Resiliencia nacional.

Gobierno de España · Ministerio de Ciencia e Innovación · Plan de Recuperación, Transformación y Resiliencia · CDTI Innovación · Financiado por la Unión Europea NextGenerationEU

BCSSD: Espacios de datos de ciberseguridad

Basque Cyber Security Shared Data

Caso de Uso: compartición de datos de ciberseguridad industrial

Objetivo:

Crear un espacio descentralizado para compartir información de ciberseguridad entre las empresas y organizaciones del sector industrial vasco, con el fin de mejorar su ciberresiliencia y competitividad:

- Provisión de Indicadores de Compromiso (IoCs)
- Alerta temprana de TTPs
- Vigilancia de Vulnerabilidades
- Alerta Empresa Vulnerable
- Resumen Ejecutivo de Informes de Ciberseguridad

Solución:

- Uso de LLM y NLP para extracción de conocimiento de ciberseguridad.
- Arquitectura alineada con iniciativas IDS y GAIA-X sobre espacios de datos

(*) Programa de ayudas de apoyo a la i+d empresarial - HAZITEK
Actuación cofinanciada por el Gobierno Vasco y la Union Europea a través del fondo europeo de desarrollo regional 2021-2027 (FEDER)

tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

¡Muchas gracias!

Para cualquier consulta o más información:

www.tecnalia.com

maite.alvarez@tecnalia.com

tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL