Webinar Gratuito

Fundamentos de Ciberseguridad ICS para Lideres

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 26 Agosto 2026

Alonso Eduardo Caballero Quezada

Cuento con más de diecinueve años de experiencia en el área y desde hace quince años me especializo en la áreas de Hacking, Forense, OSINT, Ciberseguridad y temas relacionados.

https://www.linkedin.com/in/alonsocaballeroquezada/

https://x.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

https://wa.me/reydes

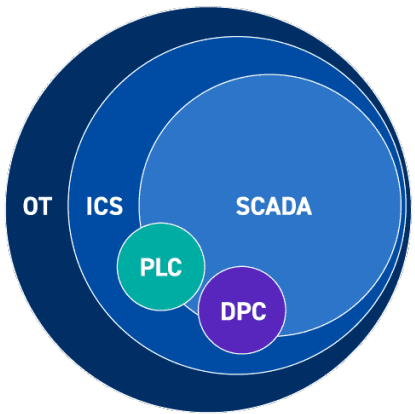
https://t.me/ReYDeS

Introducción

Estrategias de Ciberseguridad en OT/ICS (Operational Technology/Industrial Control Systems) para Líderes y Directivos

Fundamentos para proteger la Infraestructura Crítica y Entornos Industriales.

Alinear los riesgos cibernéticos industriales con los objetivos del negocio (empresa).



La Brecha Fundamental entre IT y OT

C-I-A vs. A-I-C

- En IT priorizamos la Confidencialidad; en OT la Disponibilidad y la Integridad son la máxima prioridad

Ciclo de vida del activo

- Servidores IT (3 a 5 años) vs. Maquinaria OT (15 a 30+ años)

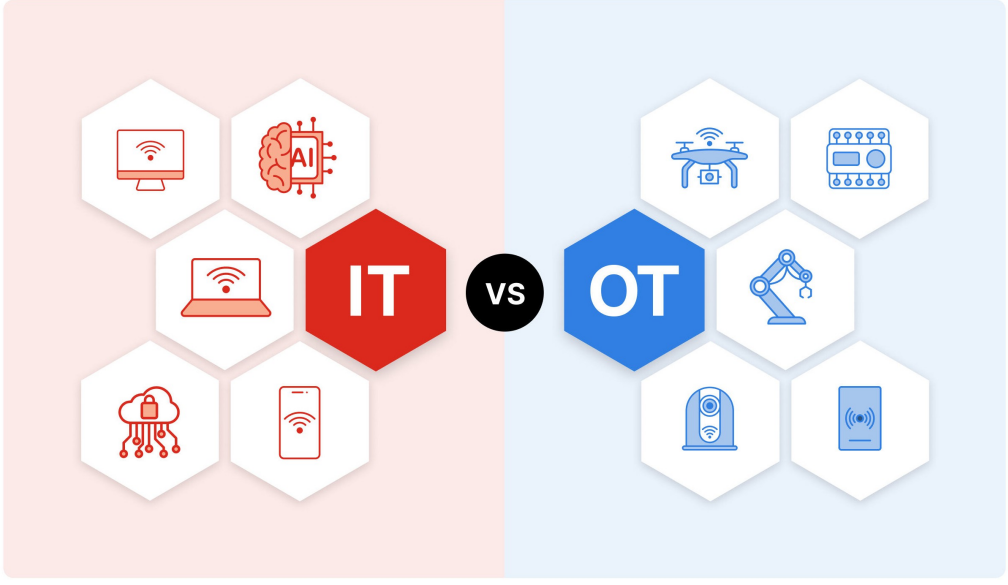
Sistemas Legacy (heredado)

- Protocolos industriales diseñados originalmente sin autenticación ni cifrado (Modbus, S7, BACnet)

La Brecha Fundamental entre IT y OT (Cont.)

Consecuencias

- Un ciber incidente en OT no únicamente destruye datos, impacta el entorno físico, y la vida humana.



Caso: Inseguridad por Diseño en Protocolos OT

Demostración de reconocimiento e inspección en un protocolo industrial (Modbus TCP / Port 502).

Objetivo

- Mostrar la facilidad con la cual un ciberatacante mapea e interactúa con un Controlador Lógico Programable (PLC) sin controles de seguridad.

Herramientas a utilizar

- Kali Linux, Nmap e Interfaz SCADA/PLC simulada.

Reconocimiento y Manipulación de Modbus

- **Paso 1:** Escaneo de la red para detección de dispositivos industriales

  $ sudo nmap -sV --script modbus-discover 192.168.0.200

- **Paso 2:** Lectura de registros de memoria del PLC mediante Scripts de Kali Linux.

- **Paso 3:** Manipulación de valores de control de proceso.

- **Lección Clave para Líderes:** La visibilidad de la red OT es el primer paso crítico antes de poder defenderla.

Estructura del Programa de Ciberseguridad OT

Modelo GOES

- **Governance** (Gobernanza): Definición de políticas adaptadas a OT y gestión de cumplimiento regulatorio
- **Oversight** (Supervisión): Evaluación continua de riesgos e integración de Inteligencia de Amenazas (Threat Intelligence)
- **Execution** (Ejecución): Detección, vigilancia de activos, y respuesta ante incidentes en tiempo real
- **Support** (Soporte): Capacitación, cultura organizacional, y presupuesto estratégico

Traducir Ciberseguridad OT a Riesgo Financiero

Como comunicar el valor de la ciberseguridad a los ejecutivos y juntas directivas.

Métricas que importan

- Cobertura e inventario de activos OT
- Tiempo de detección y contención en la red industrial
- Frecuencia y resultados de simulaciones de respuesta ante incidentes (Tabletops).

El retorno de inversión (ROI) en OT es el Evitar Pérdidas de Producción y Accidentes.

Preparación y Respuesta ante Incidentes ICS/OT

- Integración de Inteligencia de Amenazas específica para entornos industriales
- Implementación de “Tabletop Exercises” para probar planes de respuesta
- Estrategias de contención sin interrumpir procesos críticos
- Lecciones aprendidas e ingeniería inversa de incidentes pasados.

Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Construir Equipos Seguridad OT y Cultura Interna

- Cerrando la brecha de habilidades: Integración entre ingenieros de planta y analistas de ciberseguridad
- Superando restricciones culturales entre los equipos de IT, OT, y Seguridad Física
- Estrategias para atraer, capacitar, y retener talento capacitado en ciberseguridad industrial
- Creación de una cultura orientada a la Seguridad, Confiabilidad, y Resiliencia.

Hoja de Ruta para Líderes de Ciberseguridad OT

1. **Visibilidad:** Mapear e inventariar el 100% de los activos de la red OT

2. **Segmentación:** Implementar arquitecturas defensivas (Modelo Purdue / Zona y Conductos).

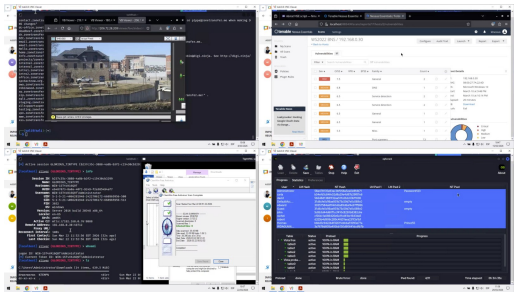
3. **Vigilancia pasiva:** Detectar anomalías sin alterar las comunicaciones en tiempo real.

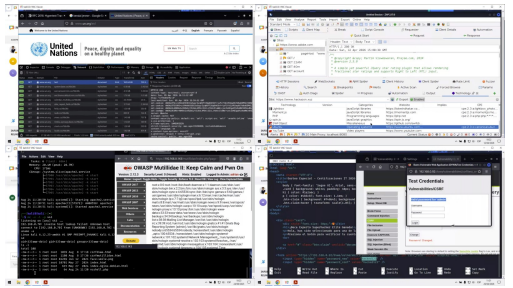
4. **Capacitación:** Dotar a los líderes y operadores con herramientas especializadas para gestión de riesgo

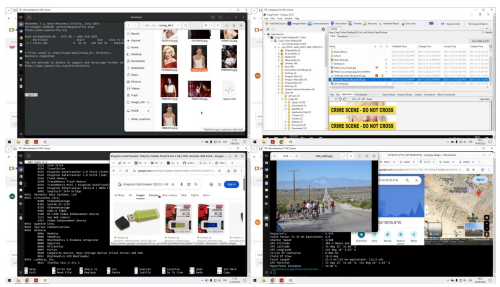
Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

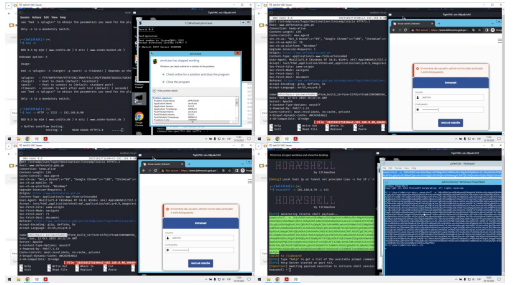
Cursos (Aula Virtual)

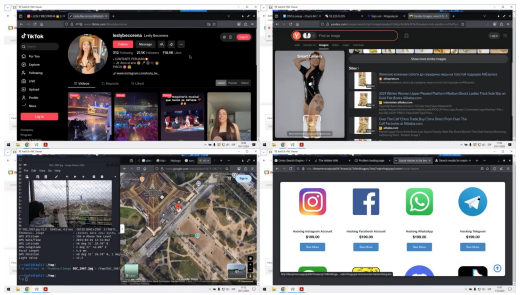
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Ciberseguridad Windows y Linux
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego Graph CE
- Y más...

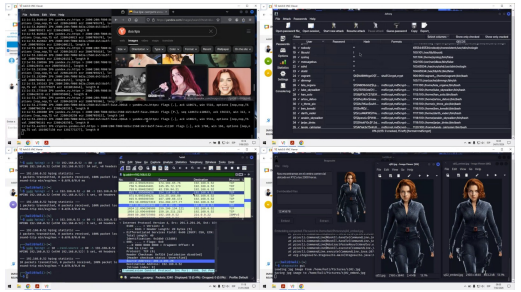












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Webinar Gratuito

Fundamentos de Ciberseguridad ICS para Lideres

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 26 Agosto 2026