Webinar Gratuito

Fundamentos de Ciberseguridad ICS/SCADA

Alonso Eduardo Caballero Quezada

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

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

Miércoles 2 Setiembre 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

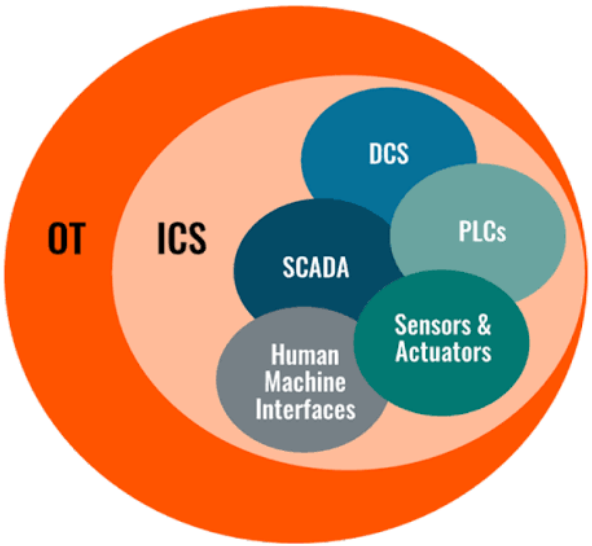
https://wa.me/reydes

https://t.me/ReYDeS

Introducción

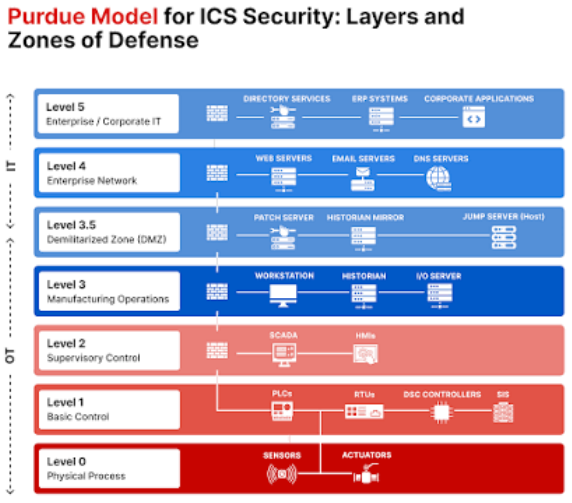
Estrategias de defensa activa, visibilidad, y protección de sistemas para control industrial.

Mapeo de riegos en infraestructuras críticas y redes para automatización.



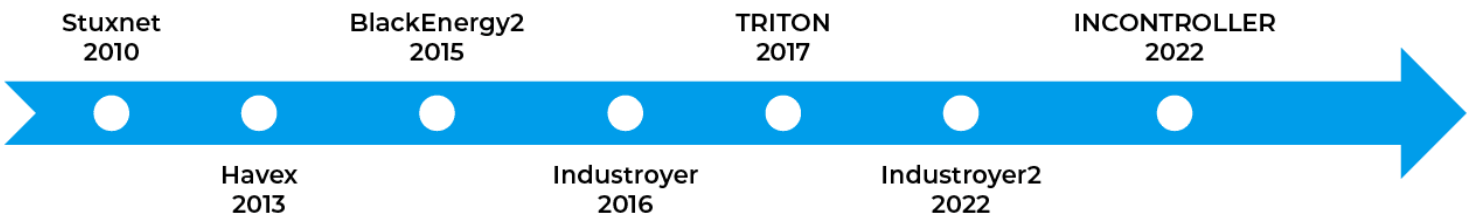
La Estructura de Red en Entornos Industriales

- **Nivel 0 - 1 (Proceso y Control):** Sensores, actuadores, PLCs, y RTUs operando el proceso físico
- **Nivel 2 (Supervisión):** Estaciones HMI, servidores SCADA, y consolas de control local
- **Nivel 3 (Operaciones de Planta):** Servidores “Historian” (Historiadora), gestión de mantenimiento, y redes de producción
- **DMZ Industrial (Nivel 3.5):** La frontera crítica de separación entre la red corporativa (TI) y la red de control (OT)



Anatomía de las Intrusiones Industriales

- **Interconexión IT/OT no autorizada:** Accesos remotos, modems de soporte, y portátiles de contratistas
- **Inseguridad por Diseño:** Protocolos ICS (Modbus, DNP3, Profinet, EtherNet/IP) sin encriptación ni autenticación
- **Malware Específico de ICS:** EVILPLANT, Industroyer, PIPEDREAM/Incontroller y cargas (payloads) de Ransomware dirigidas a la continuidad operativa

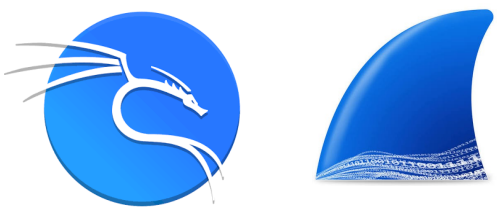


Reconocimiento Activos ICS/SCADA

Caso Práctico

Demostrar como un profesional en ciberseguridad /ciberatacante descubre dispositivos industriales, audita funciones y detecta falta de autenticación en protocolos ICS mediante herramientas en Kali Linux.

- **Propósito:** Identificar dispositivos activos, recolectar información, leer / escribir registros en PLCs
- **Herramientas:** Kali Linux, nmap, mbpoll para análisis, interacción, evaluación de Modbus



Demo: Inspección Pasiva y Análisis de Tráfico ICS

- **Paso 1:** Utilizar los filtros de Shodan para encontrar dispositivos con servicios modbus en funcionamiento
- **Paso 2:** Escanear con Nmap el dispositivo para obtener mayor información
- **Paso 3:** Utilizar la herramienta mbpoll para leer / escribir de manera no autorizada en el PLC

Lección importante: Facilidad de reconocimiento de activos en redes OT no segmentadas. Y riesgo inherente de los protocolos industriales legados.

Pasando de Defensa Pasiva a Vigilancia Continuaa

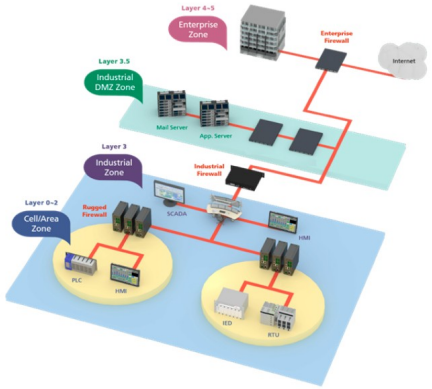
- **Inventario Automatizado de Activos:** Mapeo de dispositivos, versiones de firmware, y topología real
- **Detección de Anomalías en Protocolos:** Análisis de comportamiento “baseline” linea base frente a comandos atípicos en la red OT
- **Caza de Amenazas (ICS Threat Hunting):** Búsqueda proactiva de TTPs (Tácticas, Técnicas y Procedimientos) alineados al marco ATT&CK para ICS

Desafío de la Actualización en Plantas Operativas

- **Inviabilidad del parcheo inmediato:** Los ciclos de parches de TI no se pueden aplicar a sistemas los cuales operan 24/7

- **Controles Compensatorios:** Segmentación mediante Firewalls Industriales, reglas de IDS/IPS, y restricción de puertos

- **Pruebas en Entornos de Simulación:** Validación rigurosa de actualizaciones en laboratorios antes de desplegar en producción



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

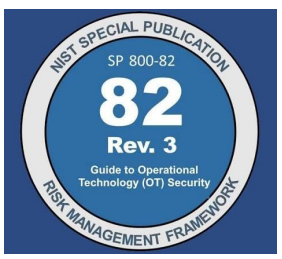
Protocolos Contención sin Interrupción Operativa

- **Diferencia con TI:** En OT no se puede aislar o apagar un segmento de red si compromete la seguridad física (Salvaguarda)
- **Playbooks Adaptados:** Procedimientos de respuesta paso a paso según la severidad del proceso afectado
- **Preservación Forense:** Captura de volúmenes de memoria y logs de red sin detener controladores ni interfaces HMI

Estándares Internacionales Seguridad Industrial

- **ISA/IEC 62443:** Implementación del concepto de Zonas y Conductos para una segmentación efectiva
- **NIST SP 800-82:** Guía de ciberseguridad para Sistemas de Control Industrial

Matriz de Riesgo Integrada: Evaluación del impacto cibernético cruzado con el impacto ambiental y de seguridad del personal



Plan Acción para Protección Sistemas ICS/SCADA

1. **Segmentar:** Aislar la red de control mediante DMZ industrial y arquitectura IEC 62443

2. **Visibilizar:** Desplegar sensores de monitoreo pasivo de tráfico en los switches de la planta.

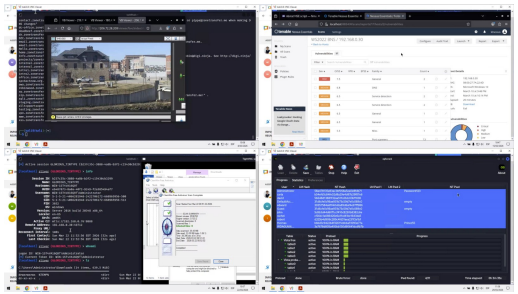
3. **Controlar accesos:** Eliminar conexiones directas a Internet y aplicar MFA en todos los accesos remotos de soporte.

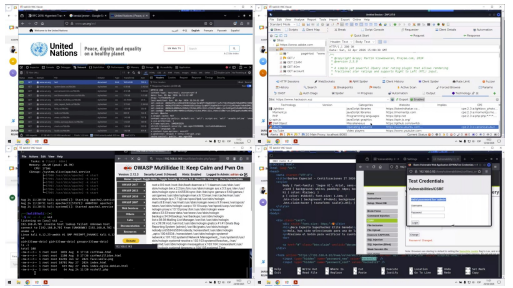
4. **Capacitar:** Formar al personal de planta y ciberseguridad en el manejo de incidentes OT.

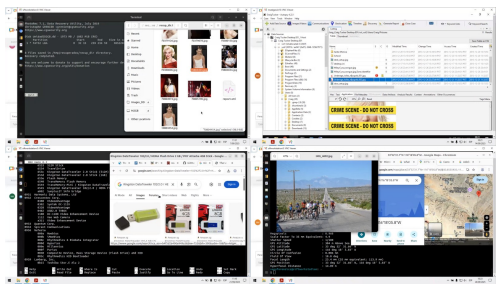
Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

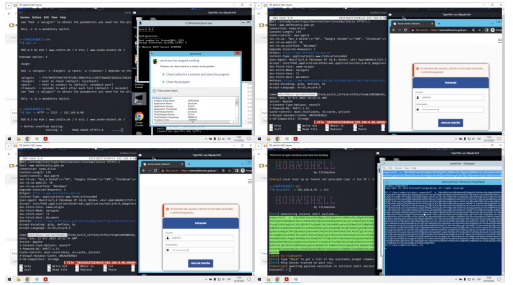
Cursos (Aula Virtual)

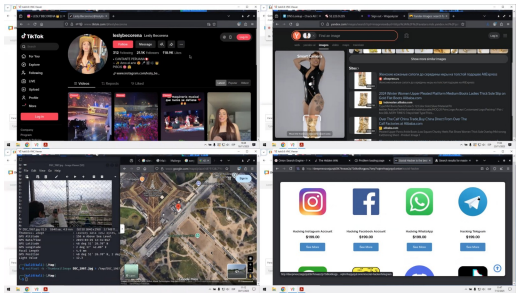
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Ciberseguridad Windows y Linux
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking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

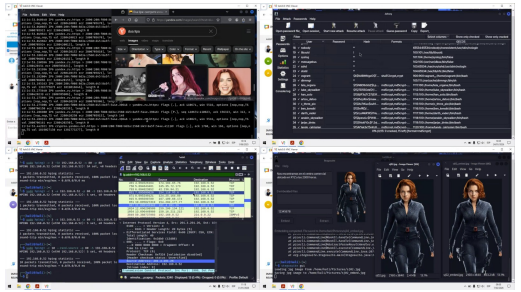












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Webinar Gratuito

Fundamentos de Ciberseguridad ICS/SCADA

Alonso Eduardo Caballero Quezada

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

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

Miércoles 2 Setiembre 2026