19° URUMAN 2° INGURU

# Riesgos de Ciberseguridad en la convergencia de mundos IT y OT

A/P ETHEL KORNECKI, CISA,CISM,CDPSE


# EVOLUCION

Tradicionalmente las tecnologías de Información IT y las centradas en las Operaciones OT, se mantenían aisladas

La **convergencia IT/OT**:

Ha sido impulsada por la creciente necesidad de coordinación y eficiencia en las operaciones empresariales.

Permite a las organizaciones recopilar y analizar datos en tiempo real, lo que puede **mejorar la toma de decisiones y la capacidad de responder a los cambios** en el entorno de la empresa.

KRAV MAGA HACKING

# ¿Qué es la Ciberseguridad Industrial ?

- La ciberseguridad industrial, también conocida como ciberseguridad OT (Tecnologías de Operación), es una rama de la ciberseguridad que se focaliza en la protección de los sistemas y procesos que se utilizan en la producción, fabricación y otros tipos de actividades industriales frente a las amenazas cibernéticas.

KRAV MAGA HACKING

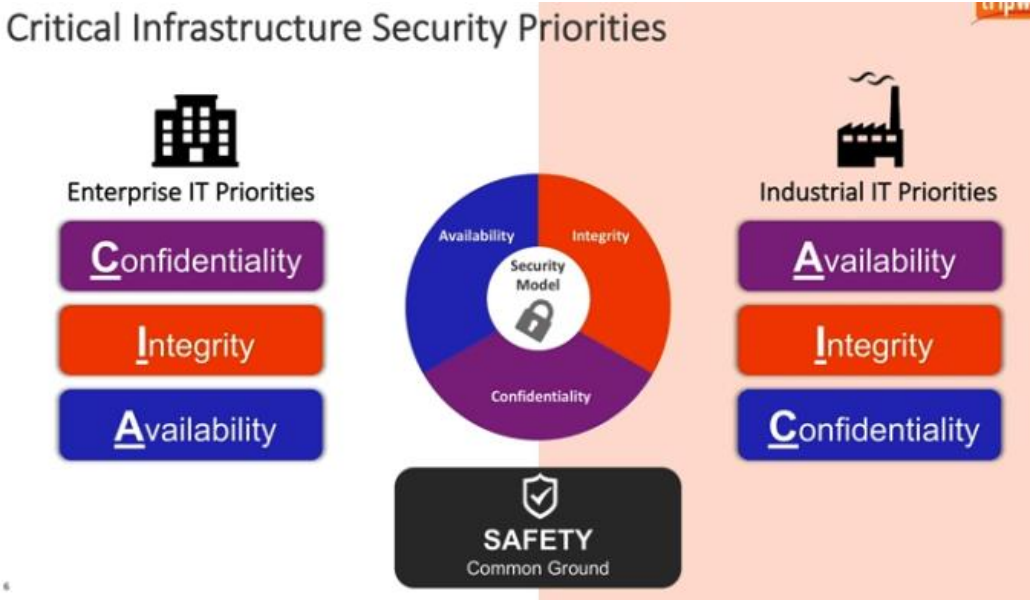

- Como expertos en ciberseguridad, entendemos que la protección de los sistemas de control y adquisición de datos (SCADA) es esencial para garantizar la operación segura de las instalaciones industriales.

- La convergencia ha abierto un nuevo campo de batalla en el que amenazas cibernéticas pueden tener impactos físicos devastadores.

KRAV MAGA HACKING

- **¿Qué es diferente entre IT y OT?**
  Especialización y foco de ambos mundos

  Son sistemas y departamentos de naturaleza y misión diferentes, la integración y convergencia de ambos grupos es un problema de interés general para la industria.





KRAV MAGA HACKING

# ¿Qué está pasando en el ámbito industrial?

- Todos sabemos que las infraestructuras industriales se están convirtiendo en blancos potenciales para ciberataques a medida que se va incrementando su conexión a otras redes. Los fabricantes y operadores de sistemas SCADA y DCS cada vez reportan más casos de ataques a sus sistemas.

- Años atrás los sistemas de control se encontraban aislados

- Las necesidades de comunicación han hecho que esto vaya mutando, aumentando los riesgos y vulnerabilidades que puedan ocasionar eventos indeseados como shutdowns o afectar la seguridad física en un entorno de producción.

- El incremento de ataques viene dado, principalmente, por la interconexión de redes empresariales/corporativas con redes de control de procesos y producción, utilizando protocolos de tecnologías estándar como Ethernet, TCP/IP, etc

KRAV MAGA HACKING

# Durante una consultoría

## Nos encontramos con:


La infraestructura obsoleta da como resultado redes y soluciones propietarias que aumentan la complejidad de la red

Los enfoques de seguridad tradicionales no son lo suficientemente robustos para mitigar las amenazas de seguridad más recientes

Los trabajadores necesitan incorporar nuevos conocimientos para administrar redes OT modernas

La escala y el volumen de datos que se generan son difíciles de capturar y administrar

Confusión por un exceso de productos y soluciones disponibles en el Mercado

KRAV MAGA HACKING


# Amenazas de la convergencia

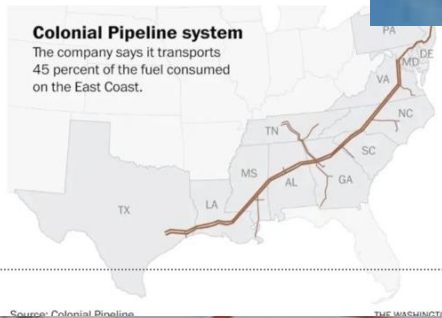
- Falta de colaboración (trabajos aislados, necesidad de comunicar)
- Políticas , procedimientos y cultura inadecuada
- Sistemas obsoletos (sin seguridad, necesario adicionar)
- Falta de Visibilidad (Garantizar conocimiento y visibilidad)
- Criticidad en la disponibilidad (7x 24 x 365)
- Instalación inapropiada de aplicaciones
- Software vulnerable
- Falta de herramientas forenses y métodos de auditoria

KRAV MAGA HACKING

# Los ciberataques están ocurriendo...

## Ransomware attack leads to shutdown of major U.S. pipeline system

The attack on top U.S. operator Colonial Pipeline appears to have been carried out by an Eastern European-based criminal gang

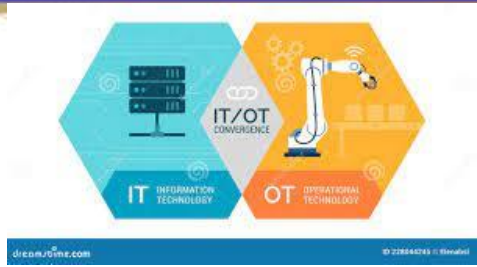

SEGURIDAD Y PRIVACIDAD

## El ataque de JBS fue llevado a cabo por el grupo de hackers REvil

por **Rafael Arbulu**, editado por **Rafael Rigues** | 04/06/2021 12h04, actualizado 07/06/2021 10h10

KRAV MAGA HACKING

# Convergencia organizacional:




- Convergencia de Procesos (flujos de trabajo y compartir información relevante)
- Convergencia de Software e información (adaptado al punto anterior)
- Convergencia física (integrar dispositivos para implementar la misma)



KRAV MAGA HACKING

# Retos convergencia IT OT

- Ventana de tiempo para introducir parches de seguridad, o instalar nuevas funcionalidades. "Operaciones no puede parar "

- Ciclos de vida de los sistemas OT mucho mayores que los de los sistemas IT.

- Sistemas OT no conectados a internet, como lo están hoy sin seguridad implementada.

# Acciones a realizar

- Estrategia de ciberseguridad que abarque tanto IT como OT. (Acceso remoto seguro , y acceso de usuarios de dominio dedicado)

- Capacitar en seguridad del lado de las redes y sistemas OT.

- La convergencia de IT/OT ( oportunidad para impulsar la innovación , contar con capacitación en defensa y en ataque)

KRAV MAGA HACKING

# Planificación de la estrategia


- Formalización de la comunicación y sus objetivos.
- Destacar sinergias y solapamientos.
- Definición de roles y responsabilidades.
- Formación, concienciación y capacitación continua
- Tecnologías y análisis de riesgos en la incorporación de las mismas

# Crear un Sistema de Gestión de la Ciberseguridad Industrial

Sistema de gestión implementado por una organización para garantizar la adopción de buenas prácticas en ciberseguridad respecto a los sistemas de control y automatización industrial

Alcance del SGCI

- Roles y responsabilidades
- Evaluación de riesgos
- Plan de acción
- Marco normativo de la seguridad
- Implementación de medidas de seguridad
- Monitorización
- Mejora continua


KRAV MAGA HACKING

# Factores críticos del éxito

| | |
|---|---|
| Apoyo de la dirección | 01 |
| Cultura de la ciberseguridad | 02 |
| Identificación del riesgo | 03 |
| Monitorización y detección de amenazas | 04 |

# Impementar medidas de ciberseguridad

1 –Segmentación de Red

2– Controles de acceso y autenticación

3– Actualizaciones y parches

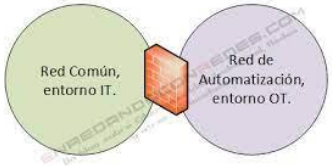
4– Respaldo y restauración de datos

5– Monitorización y registro de eventos

6– Protección contra malware

7– Respuesta a incidentes

KRAV MAGA HACKING




# Segmentación de red

- Aislar el tráfico entre líneas de producción con distintas finalidades para que ante un fallo de una no pueda afectar a las demás.
- Restringir el flujo de información, con HW o SW, evita la propagación entre las mismas .
- Proporcionar seguridad con control de entrada y salida de cada tramo



KRAV MAGA HACKING

# Control de acceso y autenticación

- Comprobar e implementar la autenticación multi factor (MFA) correctamente
- Cuentas con accesos privilegiados
- Eliminar todas las cuentas de usuarios antiguas
- Control y supervisión de acceso remoto, a través de Firewall y que se definan DMZ donde se alojan los servicios de conectividad hacia los SCI .
- Bloquear cualquier protocolo innecesario para dichas tareas y dejar trazas de todo

KRAV MAGA HACKING

# Actualización, parcheo y gestión de vulnerabilidades


- Primordial el mapa de los activos a los efectos del escaneo de los mismos.(prioridad los críticos)
- Las actualizaciones y parches de seguridad en los ICS es un problema en el ambiente OT.(downtime)
- Continuas amenazas en ciberseguridad (Cumplimiento y Privacidad)

KRAV MAGA HACKING


# Respaldo y Restauración

- Plan de backup y recovery
- Puntos de roll back claros.



KRAV MAGA HACKING

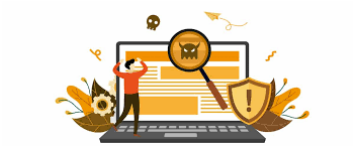
# Monitorización y registro de eventos

- Sistema de monitoreo para detectar comporta mientos anómalos .
- Medir la capacidad y los servicios que consumen el ancho de banda de la red y administrar los focos de problemas.

- Registro de cada actividad , quien la realiza, cuando y sobre qué información



KRAV MAGA HACKING



# Protección contra malware

- Las medidas para prevenir que los SCI puedan infectarse con malware y evitar su propagación.

- Controles a nivel procedural y técnico, destinados a detectar malware y prevenir infecciones.

- Herramientas de detección o de prevención de intrusión ( análisis de tráfico).


# Respuesta a Incidentes

- Reporte de incidentes exitosos o sospechosos, y la escala de notificación
- Planes de respuesta con personal capacitado y procedimientos para informar partes interesadas
- Personal activamente involucrado en el diseño, elaboración y pruebas de los planes



KRAV MAGA HACKING


# Respuesta a Incidentes

- Reporte de incidentes exitosos o sospechosos, y la escala de notificación
- Planes de respuesta con personal capacitado y procedimientos para informar partes interesadas
- Personal activamente involucrado en el diseño, elaboración y pruebas de los planes



KRAV MAGA HACKING

# Riesgos en OT

- Amenazas que reducirían la seguridad operativa (seguridad física de bienes y personas, impacto medioambiental) y la disponibilidad o incluso la integridad física de las herramientas de producción.
- El robo de datos industriales importantes.
- Los impactos son económicos, pero también sociales; la responsabilidad civil y penal de los líderes también se ve comprometida.
- Inserción de USB comprometidos
- Accesos remotos inseguros

# Evaluación de riesgos en la red OT

- **Identificación de los activos de OT**. Todo hardware, software y dispositivo conectado a la red es identificado junto con cualquier interconexión o punto de integración entre las redes de OT e IT.

| ID | MAC / fabricante | Nº Serie | Modelo | Propietario | Responsable | Localización física | Firmware versión | Valoración del activo | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Confidencialidad | Integridad | Disponibilidad | Criticidad | Coste (€) |
| S21sec001 | 00:1C:06:00:BC:37/Siemens | V-LA263238 | SIMATIC S7 1200 | Paco Pérez | Luis Alfonso | Sala de máquinas | V.04.02.03 | 5 | 4 | 8 | 5 | 960 |
| S21sec002 | 00:1C:06:00:BB:38/Siemens | V-L3B62271 | SIMATIC S7 1200 | Juan Martín | Luis Alfonso | Sala de máquinas | V.04.02.03 | 4 | 6 | 7 | 5 | 960 |
| S21sec003 | AC:64:17:4C:CA:F2/Siemens | V-PJ9133606 | SCALANCE M874-3 | Paco Pérez | Luis Alfonso | Sala de máquinas | V.04.03.01 | 3 | 5 | 8 | 6 | 1500 |
| S21sec004 | AC:64:17:4D:A3:8A/Siemens | C-C1VJ54042012 | SIMATIC S7 1500 | Juan Martín | Ataulfo López | Sala de máquinas | V.03.03.01 | 4 | 4 | 9 | 7 | 3467 |
| S21sec005 | 00:80:F4:18:42:82/Schneider Electric | X-4398dsa786 | M340 | Paco Pérez | Ataulfo López | Sala de máquinas | v2.9 | 5 | 5 | 9 | 7 | 3345 |
| S21sec006 | 00:80:F4:18:35:83/Schneider Electric | X-4398dsb5423 | M340 | Juan Martín | Ataulfo López | Sala de máquinas | v2.9 | 6 | 5 | 9 | 8 | 6780 |

KRAV MAGA HACKING

# Evaluación de riesgos en la red OT

- **Evaluación de vulnerabilidades.** Todos los activos analizados para identificar sus vulnerabilidades de seguridad, sistema operativo, aplicaciones, protocolos de comunicación, interfaces de hardware, etc.

# Evaluación de riesgos en la red OT

- **Patrón de amenazas.** Comparativa entre las vulnerabilidades detectadas y las amenazas y “malwares” conocidos y se consigue una evaluación de los escenarios posibles de ciberataque.

KRAV MAGA HACKING

# Evaluación de riesgos en la red OT

- **Evaluación de riesgos general.** Las vulnerabilidades y la evaluación de amenazas proporcionan la evaluación de riesgos general, y permite la creación de un plan de acción con las prioridades definidas.

# Plan de Gestión de riesgos OT

- **Gestión de activos del ICS.** Un sistema de gestión de activos hace seguimiento del ICS, de sus componentes y de su nivel de seguridad, e identifica nuevos componentes en la red.

- **Monitorización de la red OT.** Los sistemas de monitorización de redes OT protegen el entorno de operaciones identificando posibles ataques y alertando al personal de supervisión.

Guardian – Nozomi: Tenable OT, etc.

# Estándares de ciberseguridad en OT

- Los **estándares de ciberseguridad** son herramientas utilizadas para fomentar la **disponibilidad y tolerancia a fallos** en redes de operación, y evitar posibles incidencias de ciberseguridad.

| | |
|---|---|
| ISA | ISA/IEC 62443 |
| NIST | NIST CSF<br>NIST SP 800-82 |
| ISO | ISO 27001, 27002<br>& 27005 |
| enisa | NIS-2 Directive |

KRAV MAGA HACKING

# ISA/IEC 62443

- **Sistema:** establecen guías para la evaluación de riesgos, requisitos de seguridad y tecnologías tenemos a nuestro alcance para incrementar el nivel de protección.

- **Componentes**: describe los requisitos para diseñar productos y subcomponentes de forma segura.

- Realización de evaluaciones de riesgos cibernéticos de OT
- Creación de equipos de gestión de seguridad cibernética de OT
- Parcheado y otras capacidades/controles de protección
- Requisitos estructurados tanto en soluciones como en productos
- Ciclo de vida de seguridad de activos y sistemas

KRAV MAGA HACKING

- Aislamiento, segmentación y protección de zonas de red
- Procesos derivados y gobernanza
- Creación de roles y responsabilidades apropiados para usuarios o recursos
- Evaluación de los factores de reducción del riesgo cibernético (CRRFs)
- La utilización del modelo de **PURDUE**

# ¿Qué es el modelo de Purdue?


El modelo de referencia de Purdue, adoptado por ISA-99, es un modelo para la segmentación de redes del Sistema de control industrial (ICS), que proporciona un enfoque estructurado para organizar y gestionar estos sistemas complejos, particularmente en industrias donde el control preciso, la confiabilidad, la seguridad y la eficiencia son primordiales.

KRAV MAGA HACKING

# Modelo de Purdue

Level 5 - DMZ Internet: La primera línea de defensa, donde se encuentra el firewall de perímetro. NGFS

Level 4 - Red Interna: La red interna principal, con servidores y conmutadores.

Level 3.5 - Planta DMZ: Zona intermedia para el control de acceso y autenticación.

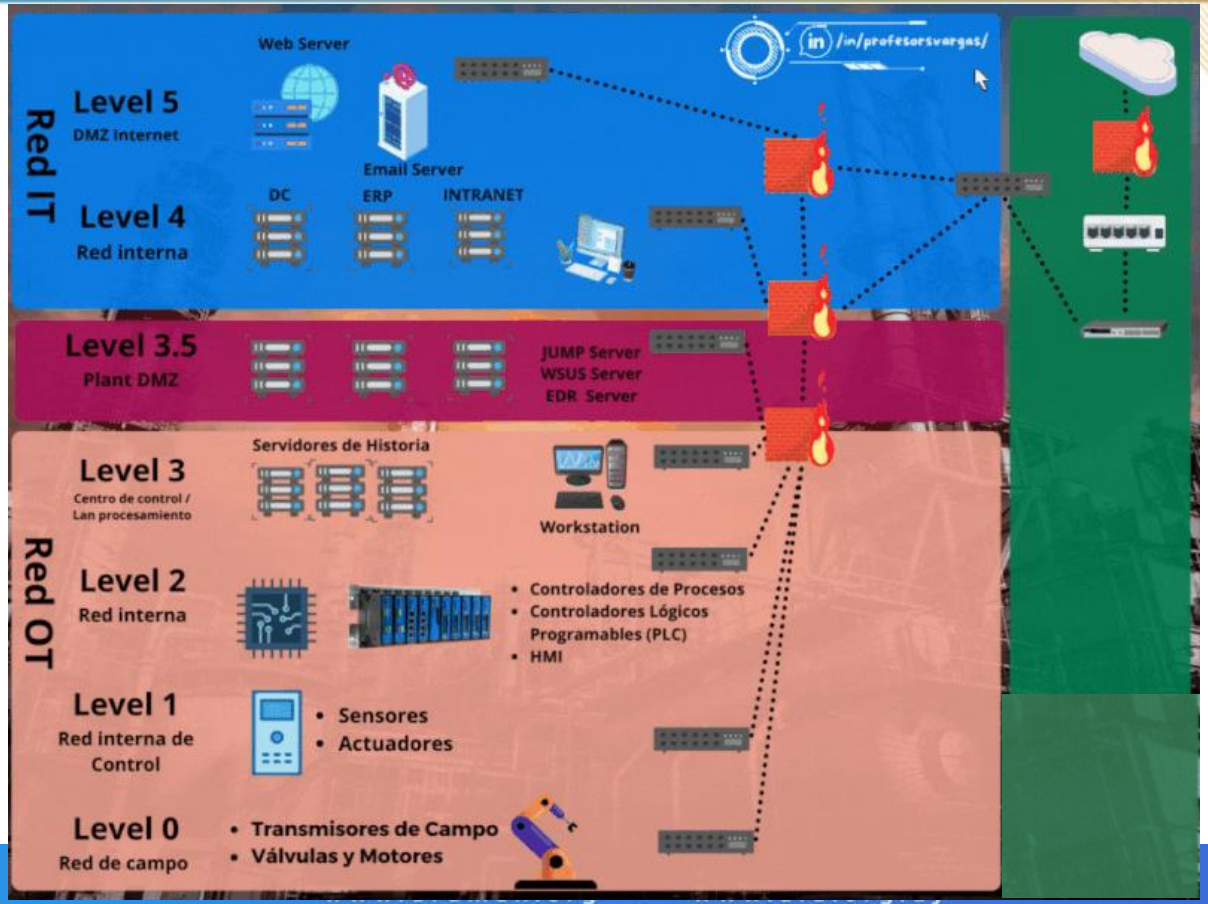
Level 3 - Centro de Control / LAN de Procesamiento: Donde operadores y servidores de historia gestionan procesos.

Level 2 - Red Interna: Con controladores de proceso y PLC.

Level 1 - Red Interna de Control: Aquí están los sensores y actuadores.

Level 0 - Red de Campo: La base, con transmisores de campo y dispositivos físicos.

# Modelo Purdue




KRAV MAGA HACKING

# Amenazas en crecimiento para 2024 - 2025




KRAV MAGA HACKING

## Espionaje industrial

- Ciberataques  efectuados para obtener información de las operaciones de otras empresas. Los ataques para espionaje industrial necesitan de altos conocimientos, y son llevados a cabo por medio de acceso a correos, redes o malware.

KRAV MAGA HACKING

## Ingeniería social.

Las amenazas de ingeniería social seguirán siendo uno de los principales riesgos para las empresas del sector OT, ya que mayoritariamente tienen alguna relación con entornos IT.

KRAV MAGA HACKING


## Ransomware SCI

Ataques basados en el cifrado de las configuraciones de los SCI que se desarrollan en procesos físicos como los procesos en una línea de producción.
El fin del ransomware SCI es hacer colapsar un sistema.

KRAV MAGA HACKING


## Ransomware SCI

Ataques basados en el cifrado de las configuraciones de los SCI que se desarrollan en procesos físicos como los procesos en una línea de producción.
El fin del ransomware SCI es hacer colapsar un sistema.

KRAV MAGA HACKING

**Rápida migración a la nube.**

La utilización de diferentes proveedores para los servicios en la nube derivará en una inconsistencia sistemática y a su vez en diferentes problemas de seguridad.

**Selección de proveedores más crítica.**

Con el aumento y riesgo de ataques a la cadena de suministro, los sistemas industriales buscarán elevar las exigencias mínimas en los criterios de selección de los proveedores. (resistencia cibernética, evaluaciones de vulnerabilidades y capacidad para asegurar los dispositivos, etc.)

## Utilización de la Inteligencia Artificial

Las empresas y usuarios han decidido aumentar sus presupuestos dedicados a la ciberseguridad poniendo especial énfasis en la implementación de herramientas con Inteligencia Artificial .

.. Pero no somos los únicos....

**La seguridad no es un destino sino un camino**. Y para elegir hacia donde daremos nuestros pasos en este camino, es **fundamental estar informados.**

KRAV MAGA HACKING

19° URUMAN 2° INGURU

# ¡Muchas gracias!

A/P ETHEL KORNECKI, CISA,CISM,CDPSE