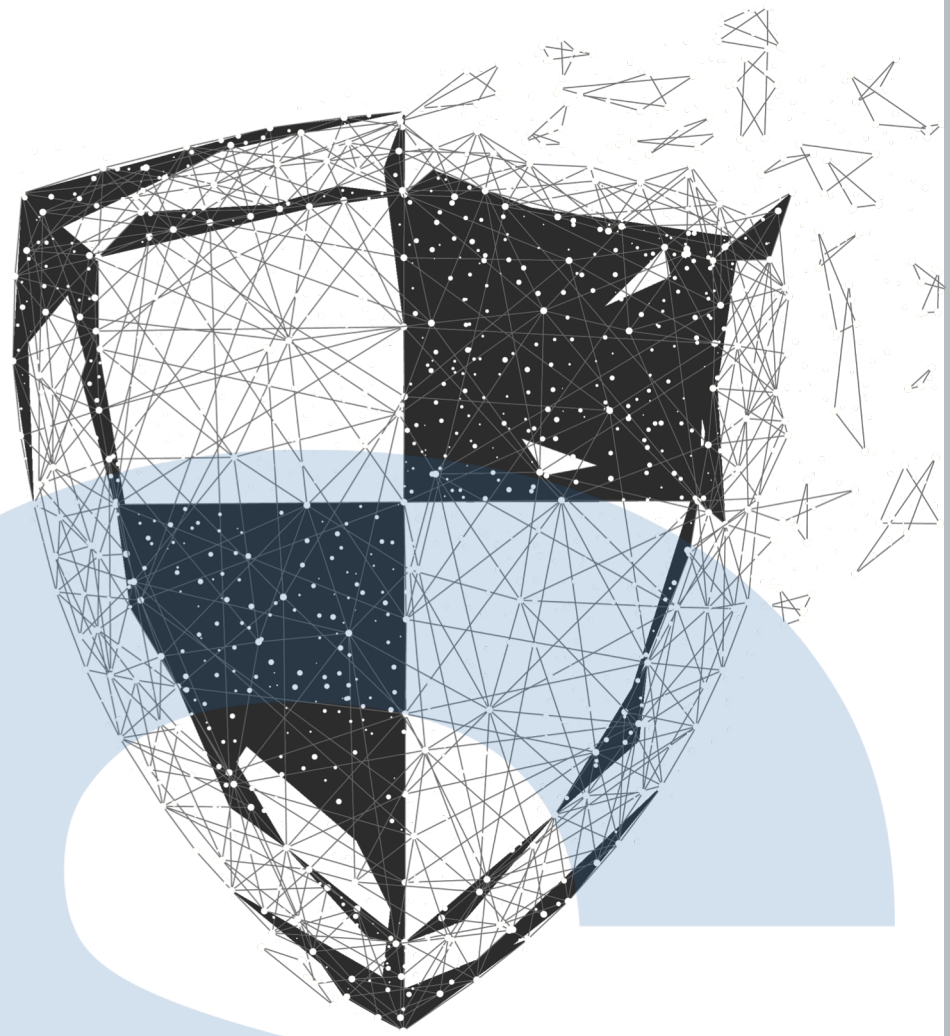
S21SEC

CYBERSECURITY YOU CAN TRUST

Infraestructuras críticas sanitarias

www.s21sec.com

CARACTERÍSTICAS DEL SECTOR HOSPITALARIO



“Datos extremadamente sensibles y cuyo valor en el mercado negro es más alto que el de las tarjetas de créditos.

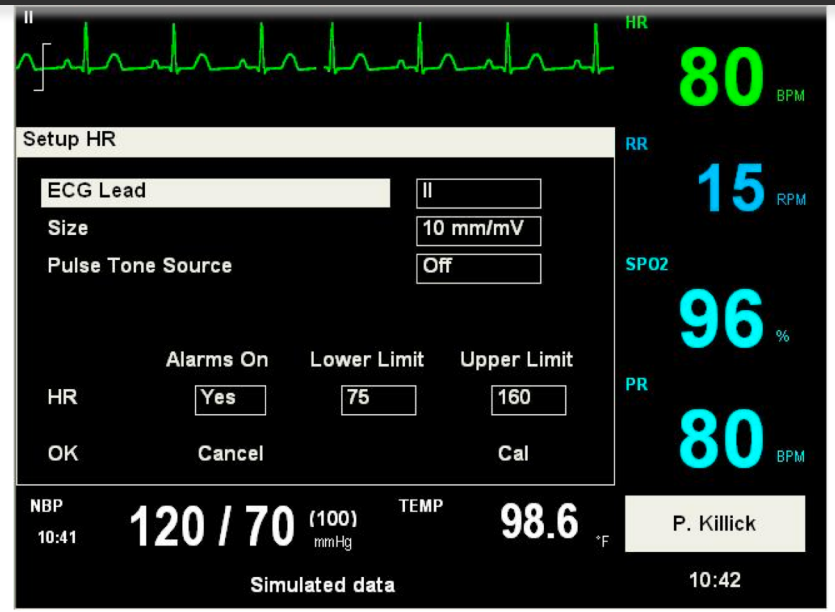
Sistemas antiguos y obsoletos cuyo coste de sustitución es muy alto.

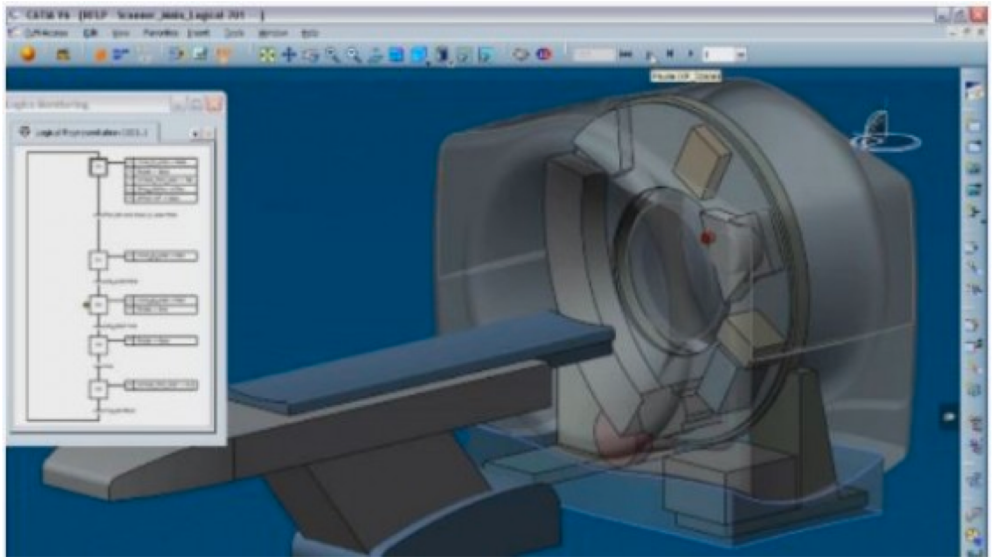
Un ataque a su infraestructura puede causar grandes daños, incluso físicos.”

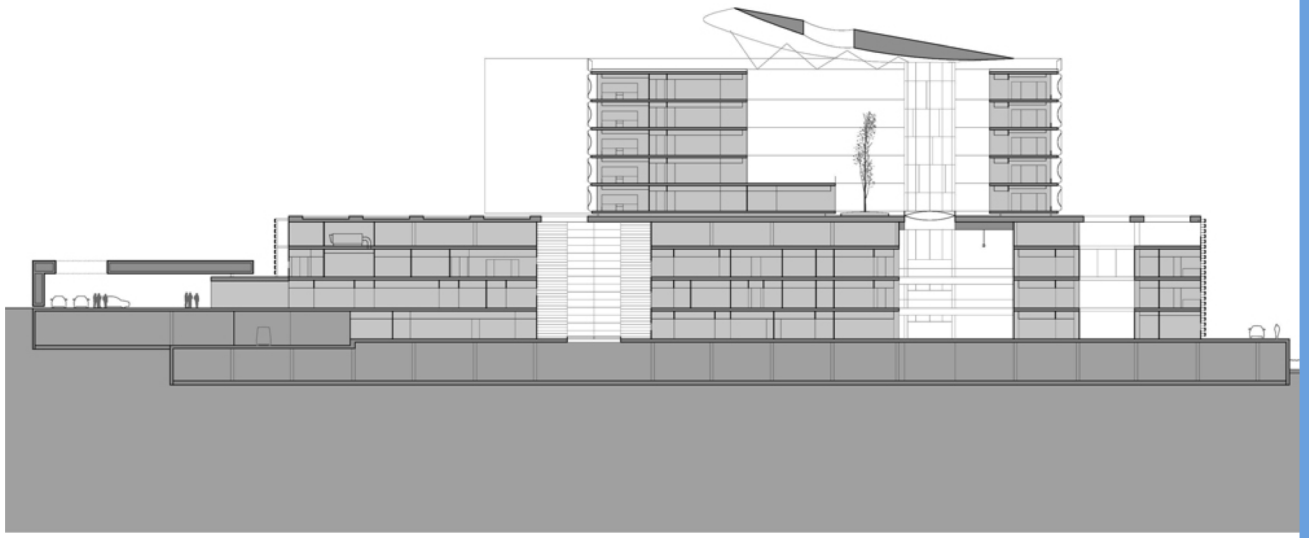
S21SEC

Hospital

- Edificio – BMS (Building Management System)
- Centro de producción industrial – SCADA
- Banco de información – GDPR, ISO 27001
- Nodo de comunicaciones

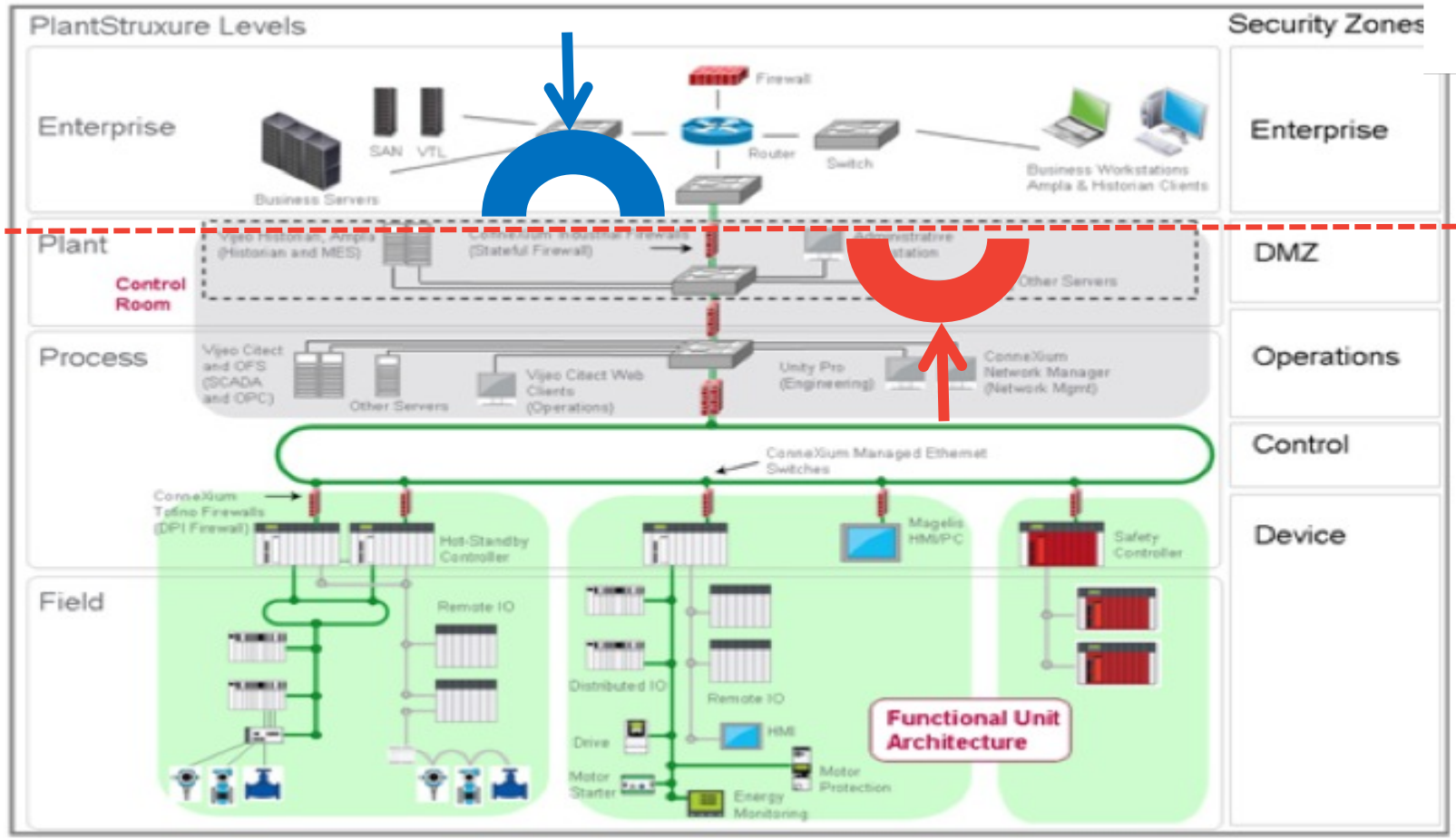




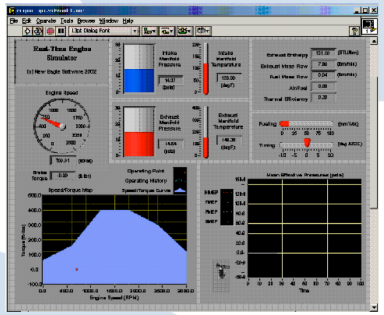


Hospital

A medida que avanza la digitalización en la salud, aumenta el número de tecnologías digitalmente conectadas. Esto está acompañado por un número creciente de **Incidentes de ciberseguridad**



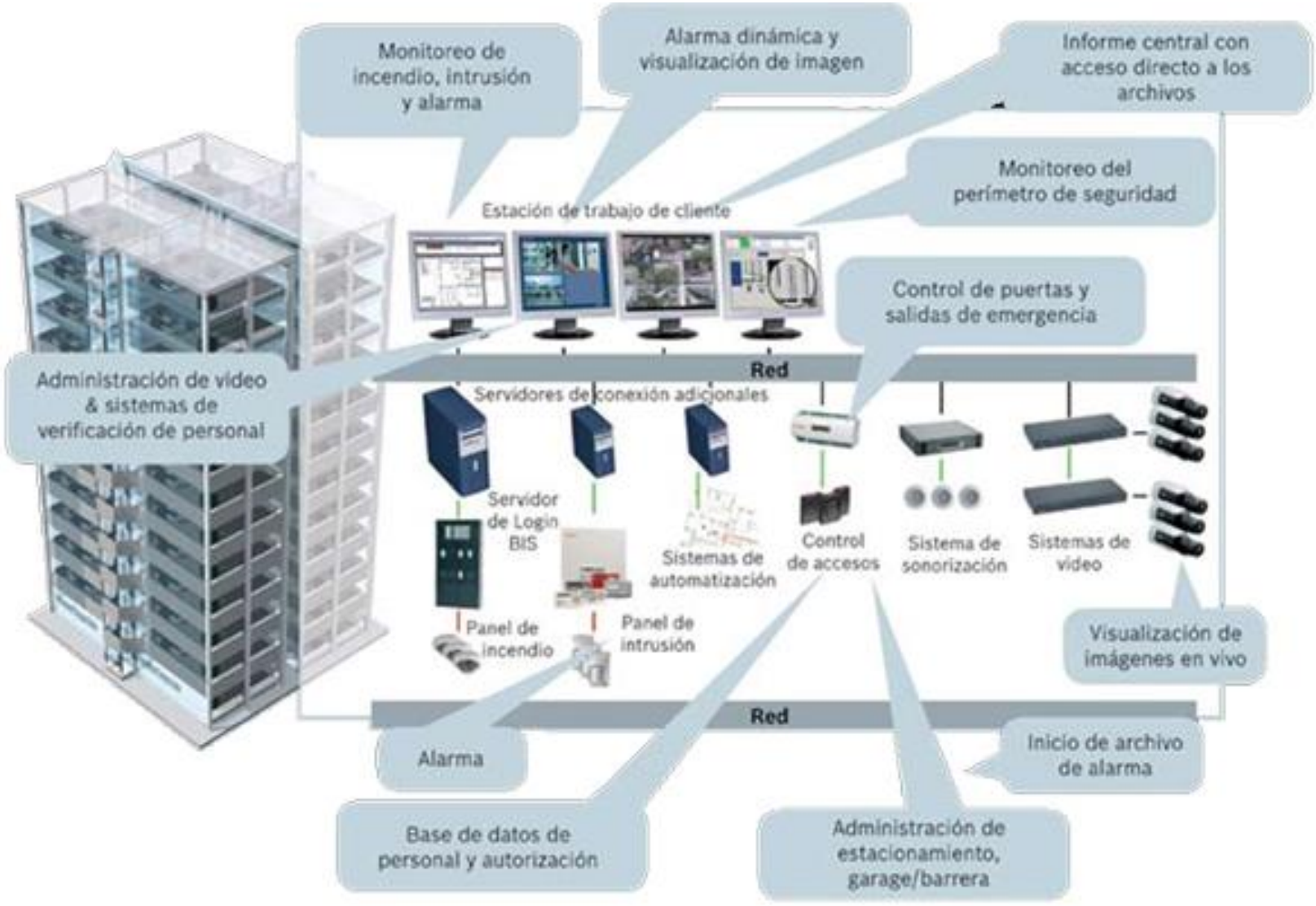
Red OT



NUEVAS AMENAZAS

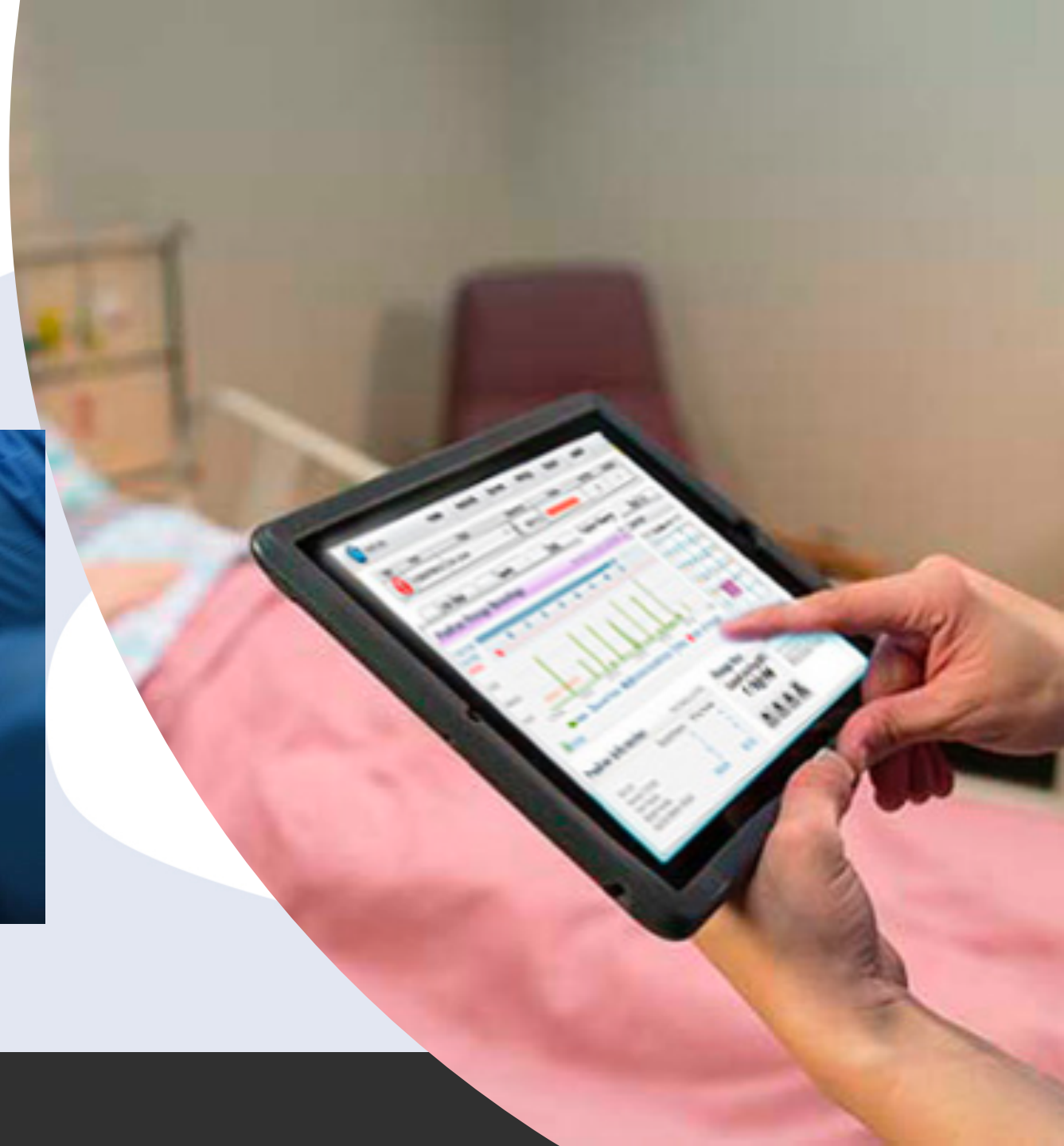
S21SEC
Your Cybersecurity Company

Complejidad y Variedad de dispositivos

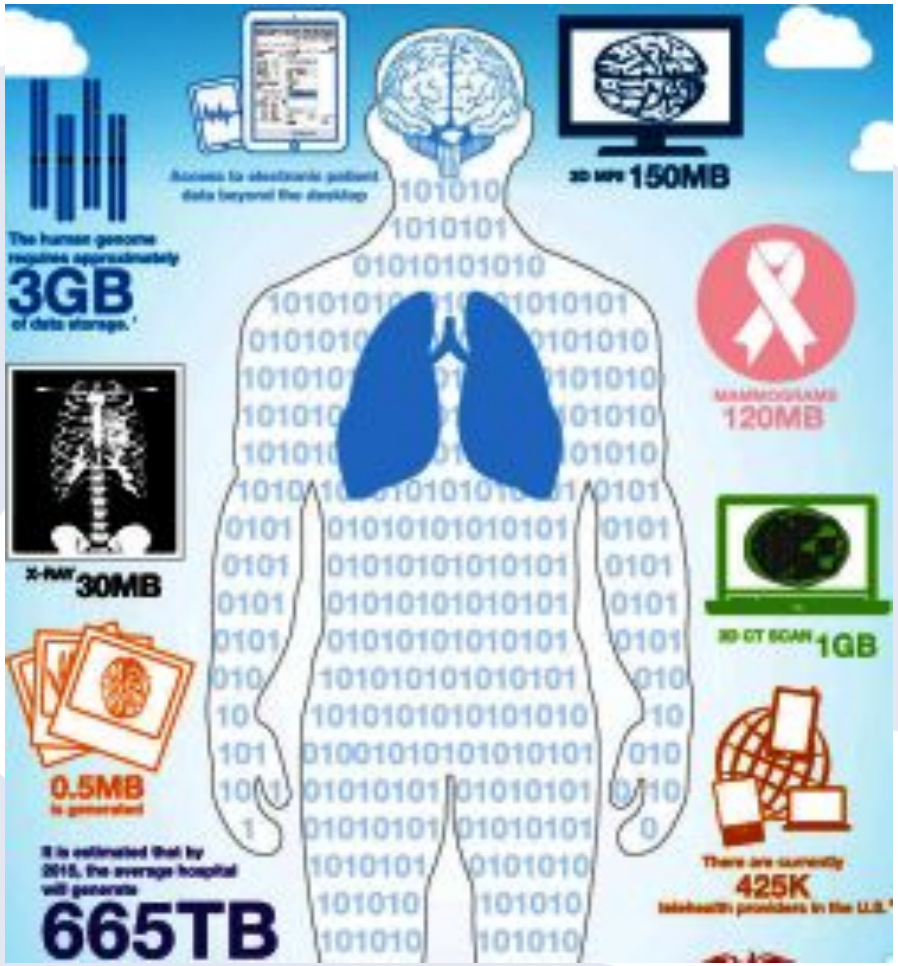


. Toda la Información en la palma de la mano

. Mejoras en el control IOT



Incorporación de Software Cloud y Big Data



E-health en Aplicaciones y Sistemas

Integración de Robótica e I.A

ATAQUES

S21SEC
Your Cybersecurity Company

Ataques de Ransomware a Nivel Global

El Gobierno británico confirma un ataque informático a gran escala en sus hospitales públicos

» La primera ministra Theresa May se muestra convencida de que todo forma parte de un «ataque internacional»en el que se han visto implicados otros países y organizaciones.

3 Compartir Compartido 87 veces

Un ciberataque ha afectado este viernes a los equipos informáticos de diversos **hospitales y centros médicos en Inglaterra**, según ha confirmado a Efe un portavoz del departamento de tecnología del sistema de salud público británico (NHS Digital).

Al respecto, la primera ministra de Reino Unido, Theresa May, confirmado las acciones lanzadas este viernes por 'hackers' instituciones médicas y ha asegurado que **todo forma parte internacional»**en el que se han visto implicados otros países organizaciones. La 'premier' ha aclarado que, hasta el mome Gobierno no tiene constancia de filtraciones de datos de paci Europa Press.

May ha explicado en un comunicado, en el que ha aludido a ataque que exige el pago de un rescate a cambio de recuper que «estamos al corriente de que varias organizaciones del **alertado de un ataque 'ransomware'»**.

Urology Austin Ransomware Attack Possibly Affects 279K

A Texas-based provider recently announced that it was the victim of a ransomware attack were data stored on servers was encrypted.

March 29, 2017 - Urology Austin recently announced on its ransomware attack on January 22, 2017, which potentially exposed patient data that was stored on the compromised server.

The OCR data breach reporting tool states that 279,663 individuals were possibly impacted by the incident.

Urology Austin said that it became aware of the incident within minutes of the attack, shut down its computer network, and started an investigation.

Healthcare IT News GLOBAL EDITION TOPICS SIGN UP MAIN MENU

HEALTHCARE DATA BREACHES

The biggest healthcare data breaches of 2018 (so far)

Healthcare continued to be a lucrative target for hackers in 2017 with weaponized ransomware, misconfigured cloud storage buckets and phishing emails dominating the year. In 2018, these threats will continue and cybercriminals will likely get more creative despite better awareness among healthcare organizations at the executive level for the funding needed to protect themselves.

This collection highlights some of the biggest breaches across the industry – and points to some mistakes to avoid in the future.

Staff

Hospitals are hit with 88% of all ransomware attacks

July 27, 2016 | Print | Email

Share Tweet 41 Share G+

Hospitals and health systems have more to lose than organizations in other sectors when it comes to hacks. Patient data sells for more money than any other kind of information on the black market. Adding insult to injury, a new report suggests that the healthcare industry is hit significantly harder by ransomware than in any other — 88 percent of attacks hit hospitals.

Of the 88 percent of ransomware attacks that occurred in healthcare organizations, 94 percent were linked to a specific variant of software called Cryptowall, according to Solutionary's Security Engineering Research Team Quarterly Threat Report for Q2 2016.

One reason hospitals may be particularly vulnerable is they use so many systems and devices that there are more entry and pivot points for cybercriminals to exploit, according the report.

"The most important steps in protecting your company's and your customers' data from the growing malicious ransomware onslaught are ensuring that you have a robust backup and recovery process, and that your security software is up-to-date and able to detect the most recent ransomware variants," Rob Kraus, director of research for Solutionary's SER team, said in a statement. "As the threat continues to evolve, it will be crucial for organizations to have defined incident-response procedures and proper detective and preventive controls in place to reduce ransomware's impact."

Some of the most high-profile hospital data breaches in 2016 have been due to ransomware. In March, Hollywood Presbyterian Medical Center in California was locked out of its EHR for a week, and providers were forced to revert to pen and paper until the decision was made to pay hackers $17,000.

Necesidad de recuperar los datos a cualquier precio

Robo de Datos Personales (pacientes y menores)

DATA OF 500,000 CHILDREN STOLEN FROM PEDIATRICIANS, SOLD ON DARK WEB

POSTED BY: JOSEPH YOUNG MAY 17, 2017 IN FEATURED, NEWS UPDATES LEAVE A COMMENT

A hacker who operates with the online alias Skyscraper revealed that 500,000 records of patients have been stolen from various healthcare companies and are currently being sold on the dark web. According to Skyscraper, all of the stolen records and identities are that of children and they include sensitive information such as the names of the children and their parents, social security numbers, addresses, phone numbers and complete medical records.

Healthcare IT News GLOBAL EDITION TOPICS

Officials discovered unauthorized access on an employee email account on Aug. 13 and immediately secured the account and launched an investigation with help from a third-party forensic firm. The investigation determined it was not one but two accounts hacked for more than a month between July 4 and August 17.

The investigation found those email accounts included patient names, dates of birth, medical data and health insurance information, according to officials. Social Security numbers were included for some patients.

Catawba Valley began notifying patients on Oct. 12 and created a dedicated call center to handle patient questions about the breach. Officials are recommending patients review any statements they receive from their insurance carrier to make sure they're not billed for any services they didn't receive.

Healthcare IT News GLOBAL EDITION TOPICS S

205,000 patient records exposed on misconfigured FTP server

MedEvolve, a practice management software vendor, left its FTP server open to the public without the need for a login.

By Jessica Davis | May 18, 2018 | 01:03 PM

Necesidad de recuperar los datos a cualquier precio

Vulnerabilidades en Aplicaciones

Layer 8

FBI raids dental software researcher who discovered private patient data on public server

Dissent Doe—2016-05-27 08:00 am | Last updated 2017-02-24 06:36 pm

Update: Misconfigured database breaches thousands of MedCall Advisors patient files

A researcher discovered the North Carolina-based tech vendor is leaking protected, personal data through its Amazon S3 bucket twice in a month.

By Jessica Davis | October 10, 2018 | 12:17 PM

Healthcare IT News GLOBAL EDITION TOPICS

LifeBridge Health reveals breach that compromised health data of 500,000 patients

Discovered on March 18, the health system was infected with malware that infected its EMR server, patient registration and billing systems for more than a year.

Robo de datos, daños en los servicios

Dispositivos Móviles

Descuidos y sistemas móviles desprotegidos. Políticas deficientes

Dispositivos Conectados

Healthcare IT News

GLOBAL EDITION TOPICS

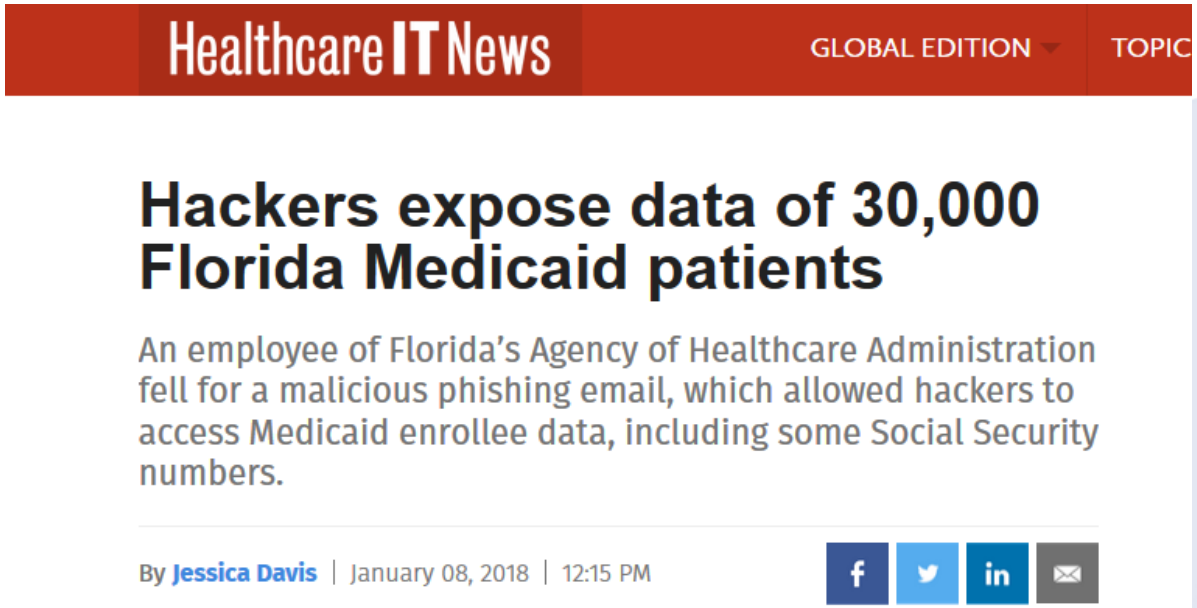
California medical device manufacturer reports breach of 30,000 consumers

Inogen reports a hacker accessed an employee email account for more than two months, according to an SEC filing.

By Jessica Davis | April 17, 2018 | 12:11 PM

Crecimiento de dispositivos conectados para mejoras de los servicios médicos.

PHISHING



Ingeniería social.

APT , Malware

Symantec Corporation (US) | https://www.symantec.com/blogs/threa | Buscar

Security Response Attack Investigation Team

POSTED: 23 APR, 2018 | 4 MIN READ | THREAT INTELLIGENCE

SUBSCRIBE FOLLOW

New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia

Symantec has identified a new attack group dubbed Orangeworm deploying the Kwampirs backdoor in a targeted attack campaign against the healthcare sector and related industries.

HARE

Healthcare IT News | GLOBAL EDITION | TOPICS

Malware attack causes breach of 134,512 patient records

St. Peter's Surgery and Endoscopy Center was hit with the second-largest healthcare breach of 2018.

By Jessica Davis | March 12, 2018 | 03:26 PM

incibe-cert_ | Alerta | Incidentes | Serv

Inicio / Alerta Temprana / Bitacora Ciberseguridad / Orangeworm, nueva APT orientada al sector sanitario

Orangeworm, nueva APT orientada al sector sanitario

23/04/2018

Symantec ha realizado una publicación sobre una APT (Amenaza Persistente Avanzada) cuyo objetivo es el sector y los proveedores del mismo, principalmente EE.UU, Europa y Asia. Según Symantec, el grupo que está detrás de amenaza, denominado Orangeworm, utiliza un malware llamado Trojan.Kwampirs. La primera evidencia de este data del 2015 y en la actualidad apenas ha sufrido modificaciones por lo que las medidas tomadas para su mitigación no han resultado efectivas.

Según la información publicada, una vez que los atacantes obtienen acceso a la red de la organización intentan obtener información de dispositivos médicos como máquinas de resonancia magnética, para robar información confidencial presumiblemente con fines de espionaje industrial.

Referencias:

23/04/2018	symantec.com	New Orangeworm attack group targets the healthcare sector in ...
23/04/2018	forbes.com	Advanced Hackers Infect X-Ray Machines In Healthcare Espionag...
23/04/2018	zdnet.com	Mysterious cyber worm targets medical systems, is found on X-r...
23/04/2018	bleepingcomputer.com	Orangeworm Hackers Infect X-Ray and MRI Machines In Their Q...

Etiquetas: APT Ciberespionaje

Orientado al sector salud (+ 40% de sus victimas)

Detectado en equipos de X-Ray , MRI, máquinas para pacientes donde puedes rellenar consentimiento.

No está claro el motivo.

Sistemas obsoletos que facilitan los ataques

VULNERABILIDADES

CISA
CYBER+INFRASTRUCTURE

CASA | ACERCA DE | ICSJWG

Asesoramiento médico (ICSMA-19-080-01)

Más avisos

Protocolo de telemetría por radiofrecuencia de Medtronic Conexus

Fecha de lanzamiento original: 21 de marzo de 2019.

Print | Tweet | Send | Share

Aviso Legal

Todos los productos de información incluidos en http://ics-cert.us-cert.gov se proporcionan "tal cual" con fines informativos únicamente. El Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) no ofrece ninguna garantía de ningún tipo con respecto a la información contenida en este documento. DHS no respalda ningún producto o servicio comercial, mencionado en este producto o de otra manera. La difusión adicional de este producto se rige por el marcado del Protocolo de semáforos (TLP) en el encabezado. Para obtener más información sobre TLP, visite http://www.us-cert.gov/tlp/ .

---

1. RESUMEN EJECUTIVO

- CVSS v9.3
- **ATENCIÓN:** explotable con acceso adyacente / bajo nivel de habilidad para explotar
- **Vendedor:** Medtronic
- **Equipo:** monitor MyCareLink, monitor CareLink, programador CareLink 2090, dispositivos cardíacos implantados específicos de Medtronic que se enumeran a continuación
- **Vulnerabilidades:** control de acceso incorrecto, transmisión de texto claro de información sensible

2. EVALUACIÓN DEL RIESGO

La explotación exitosa de estas vulnerabilidades puede permitir que un atacante con acceso adyacente de corto alcance a uno de los productos afectados interfiera, genere, modifique o intercepte la comunicación de radiofrecuencia (RF) del sistema de telemetría Conexus patentado por Medtronic, lo que podría afectar la funcionalidad del producto. y / o permitir el acceso a datos sensibles transmitidos. La explotación exitosa requiere: (1) un dispositivo de RF capaz de transmitir o recibir comunicaciones de telemetría Conexus, como un monitor, programador o radio definida por software (SDR); (2) tener acceso de corto alcance adyacente a los productos afectados; y (3) para que los productos se encuentren en estados donde la funcionalidad de RF está activa. Antes del procedimiento de implantación del dispositivo y durante las visitas clínicas de seguimiento, las sesiones de telemetría de Conexus requieren el inicio de un protocolo inductivo. Fuera de estos entornos de uso, la radio RF en el dispositivo implantado afectado se habilita por breves períodos de tiempo para admitir transmisiones de seguimiento programadas y otras notificaciones operacionales y de seguridad. El resultado de la explotación exitosa de estas vulnerabilidades puede incluir la capacidad de leer y escribir cualquier ubicación de memoria válida en el dispositivo implantado afectado y, por lo tanto, afectar la función prevista del dispositivo.

Sistemas obsoletos que facilitan los ataques

REGULACIÓN

S21SEC
Your Cybersecurity Company

- Los reguladores europeos están avanzando mediante la introducción de requisitos de ciberseguridad para dispositivos, sistemas e infraestructura en diversos marcos regulatorios, que abordan específicamente el sector de la salud.

- Guía de recomendaciones para garantizar que los dispositivos y servicios médicos en Europa permanezcan seguros ante posible ataque de ciberseguridad.

- El uso de sistemas conectados puede amenazar la capacidad de dar Servicios de Salud. Por lo tanto, la administración de la seguridad debe ser una parte importante en las estrategias de seguridad en los proveedores y organización de prestación de asistencia sanitaria.

- Notificación de incidente de Ciberseguridad, existen varias autoridades competentes en un solo país, por ejemplo, para privacidad (GDPR), Infraestructuras críticas (NIS), dispositivos médicos (MDR) deben ser informados.

- Debería haber una orientación clara sobre cómo las organizaciones nacionales y europeas comunican a través de los Equipos de Respuesta a Emergencias Informáticas (CERT)

- Promover Auditar la capacidad de una organización para detectar, responder y recuperarse de nuevas vulnerabilidades.

CERTIFICADOS DE CIBERSEGURIDAD

El Parlamento Europeo aprueba el nuevo sistema de certificados de ciberseguridad

Por amplia mayoría, el **Parlamento Europeo** ha aprobado la **nueva norma comunitaria sobre ciberseguridad**, cuya novedad más relevante es el nuevo **sistema de certificación** para garantizar que los productos, procesos y servicios respetan los **estándares** de ciberseguridad.

DATOS

S21SEC
Your Cybersecurity Company

Resultado análisis activo de sistemas:

- Ejecución de comandos con permiso de administrador en sistemas
- **Software desactualizado** (S.O. Windows, PHP, Apache)
- **Credenciales transmitidas en texto claro** (HTTP).
- Protocolos inseguros o algoritmos de cifrado débiles (SSL v3, RC4, certificados autofirmados, etc.)
- **Inyección de código SQL**
- Cross-Site scripting (es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript
- Redes IT y OT no segmentadas (Sistema anti-incendios accesible desde red IT)
- Contraseñas cifrado débil (LM)
- Servidor FTP abierto

Análisis pasivo de las comunicaciones:

- Equipos infectados por **botnet** malware Qakbot
- Uso de protocolos inseguros (HTTP, SMB, SNMP)
- Detección de redes privadas 169.254.x.x fuera de direccionamiento de la red LAN del Hospital.
- Tráfico protocolo IPv6 (volumen superior a IPv4)
- Vulnerabilidades en servicios IPv6 (p.ej. DHCPv6

DIAGNÓSTICO DETECTADO

¿RECETA PARA LA CURA?

S21SEC
Your Cybersecurity Company

SERVICIOS CIBERSEGURIDAD

- ✓ Plan Director de Ciberseguridad para analizar los entonos IT - OT y aplicar soluciones.
- ✓ Servicios de Monitorización, Detección y Protección ante amenazas
- ✓ Actualización de los Sistemas
- ✓ Escaneos de vulnerabilidades
- ✓ Servicios de Red Team – Resilencia
- ✓ Medir para Mejorar

OFFICES

Madrid
C/Ramírez de Arellano, 21, CP 28043

Pamplona
P.E. La Muga, CP 31160, Orcoyen

Barcelona
C/Tarragona, 141-157, Piso 14, CP 08014

Vitoria - Gasteiz
Edificio AzucareraAvda. de los Huetos 75, oficina 38

Porto
Lugar do Espido, via norte 4470-177. Maia

San Sebastián
P.E. Zuatzu, Ed. Urgull, 2º, CP 20018

León
Edificio CEBT, Calle Santos Ovejero 1. Oficina PB08

Bilbao
C/ Camino de Laida Edificio 207, Bloque B 1º planta

Lisboa
Rua do Viriato, 13B, 4º Andar. 1050-233, PT

Ciudad de Mexico
Calle Río Pánuco, 108. Colonia Renacimiento, Ciudad de México

MUCHAS GRACIAS

facebook.com/pages/S21sec

linkedin.com/company/s21sec

twitter.com/@S21sec

instagram.com/s21_sec