Ciberseguridad Industrial:

protege tus activos de ataques cibernéticos

JORNADAS FP DE ELECTRICIDAD Y ELECTRONICA
Vigo, 10/05/2025

SIEMENS

Antes de comenzar una breve introducción histórica

Los ataques cibernéticos han cambiado la historia, y estos han evolucionado a lo largo de los años, convirtiéndose en una de las principales amenazas para la seguridad digital a nivel mundial, y para la industria en particular.

A medida que avanza la tecnología, también avanzan las tácticas de los ciberdelincuentes.

Os comento 3 ataques cibernéticos relevantes en nuestra historia contemporánea;

- El gusano de Morris, el primer gran ataque cibernético (1988)
- Stuxnet, un malware dirigido a infraestructuras nucleares (2010)
- WannaCry, el ransomware que logró parar al mundo (2017)

Irán sufre un ataque informático contra sus instalaciones nucleares

El potente virus Stuxnet afecta ya a unos 30.000 ordenadores en el país

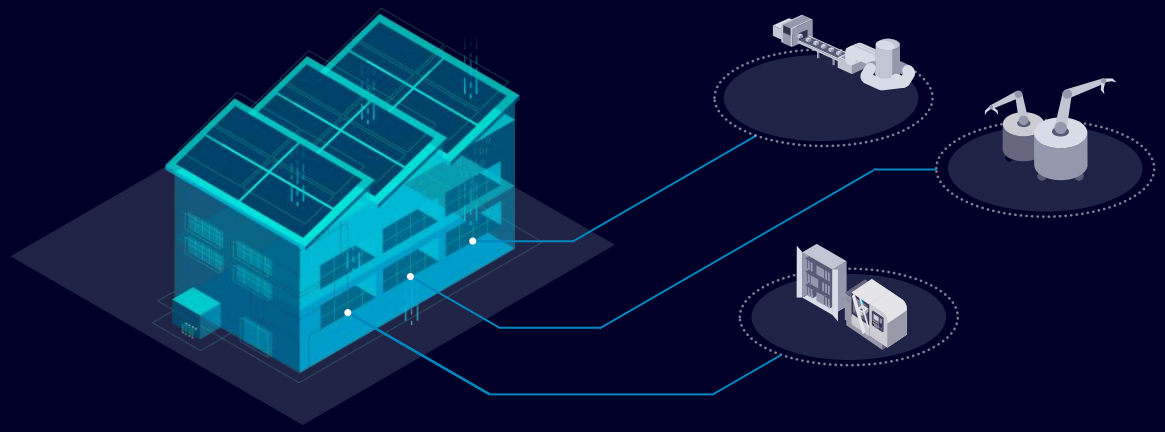
ATAQUES INFORMÁTICOS >

Ciberataque global: últimas noticias del 'ransomware WannaCry'

El virus informático que ha afectado a más de 150 países, tuvo su origen según fuentes del Gobierno de EE UU, en Corea del Norte

"Estamos bajo ataque": se cumplen 34 años del 'gusano Morris', el primer malware de la historia

Porque la Ciberseguridad es más importante ahora que antes!

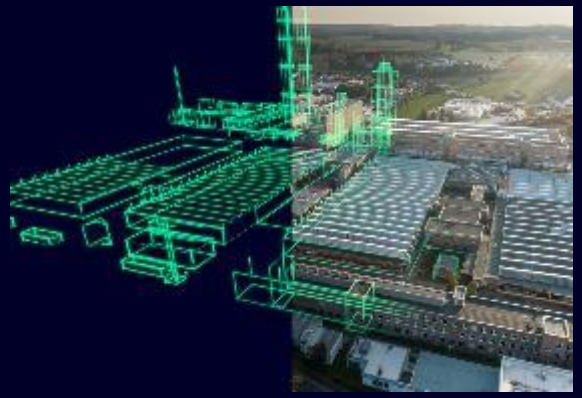


Ayer teníamos islas de comunicación

Hoy todo está conectado y los riesgos aumentan

SIEMENS

Las mega tendencias plantean grandes retos en la mayoría de las industrias



Digitalización

Falta de personal cualificado

Aumento de normativas legales

Globalización

Retos

- Hacer frente al aumento de ataques de ciberseguridad procedentes de una conectividad cada vez mayor
- Mayor complejidad del uso de datos y redes abiertas

- Falta de conocimientos sobre cómo afrontar los retos de la ciberseguridad
- Falta de personal cualificado en el mercado debido a las numerosas competencias específicas necesarias.

- Aumento de normativas de seguridad con las que cumplir.
- Dificultad para entender la situación de las instalaciones y evitar errores humanos que afecten a la seguridad.

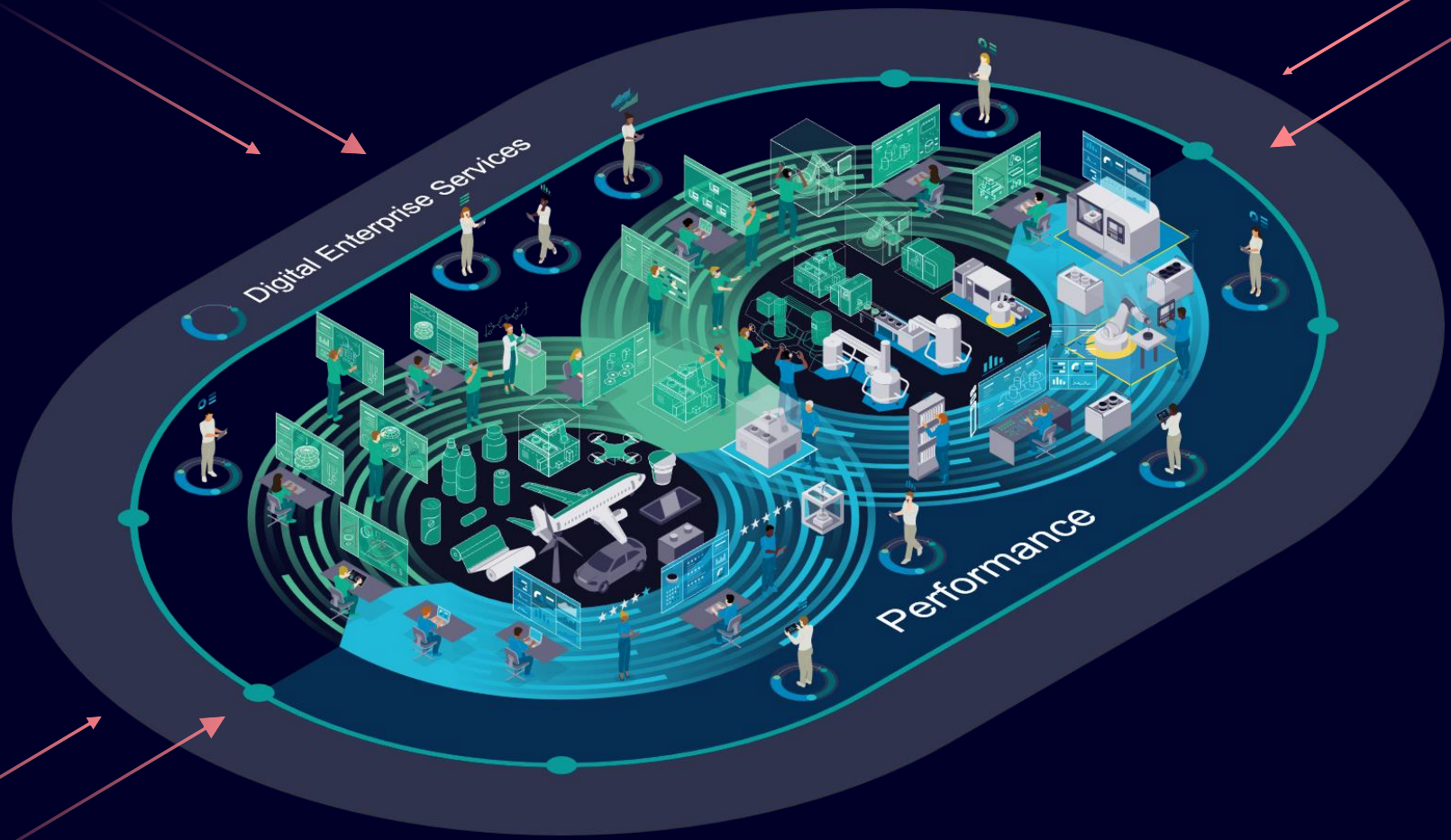
- Garantizar el trabajo a distancia independientemente de la ubicación
- Asegurar el intercambio de datos y la comunicación entre y dentro de las empresas que trabajan a escala mundial.

SIEMENS

Esto significa integración OT/IT en todas las áreas y capas

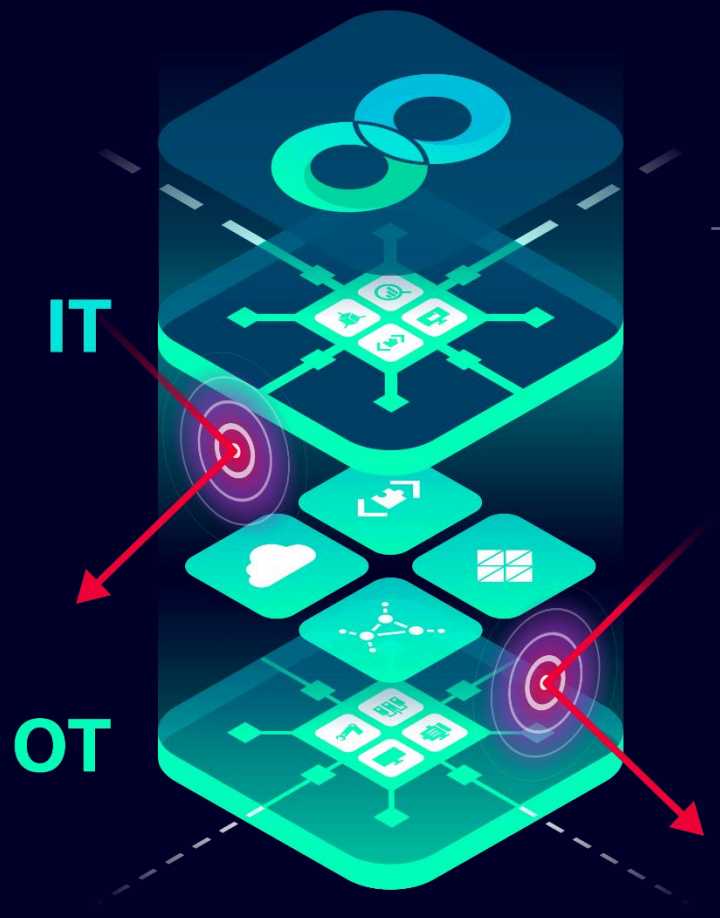
Convergencia OT/IT significa:

- **Mayor conectividad**
- **Más datos**
- **Nuevas amenazas de seguridad**



SIEMENS

A diferencia de IT, OT no se suele estar debidamente protegido y no cumple la legislación vigente.



Seguridad solo en IT

Interfaz IT/OT no segura.

Entorno OT no seguro

Requisitos de seguridad distintos para OT.

Uso de componentes obsoletos.

Incompatibilidad de medias de IT en OT.

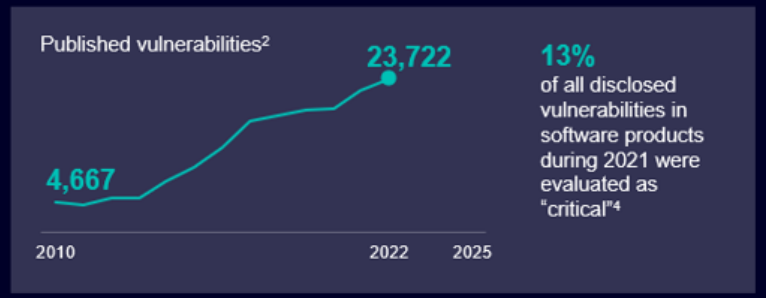
Conectividad IT/OT

SIEMENS

El transcurso de la ciberseguridad en OT

***60%** de orgs. están aquí* | ***30%** de orgs. están aquí* | ***10%** de orgs. están aquí*

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6
Concienciación	**Compromiso/Análisis de ventajas/Estudio Topológico de la Red**	**Momento… Oh Wow!**	**Apagafuegos**	**Integración**	**Optimización**



Sources: 1 IoT Analytics | 2 NIST | 3 ITAM (IT Asset Management) | 4 BSI

61%

de las fábricas inteligentes han sufrido un **incidente de ciberseguridad**.[1]

33%

De los incidentes de seguridad ocurren en producción.[2]

72%

De los **ataques de ransomware tienen lugar en áreas de producción**.[3]

87%↑

Incremento de ataques de ransomware en entornos industriales entre 2021 y 2022. [4]

Fuentes: 1 Manufacturing Automation – Growing cybersecurity risks for smart factories | **2** PMMI 2021 Assess your risk white paper | **3** Dragos 2022 ICS/OT Cybersecurity year in review | **4** Dragos 2022 ICS/OT Cybersecurity year in review

SIEMENS

Perfiles en ciberseguridad. Formación

Crece demanda de talento especializado en Ciberseguridad

El auge de la ciberseguridad en España: aumento de incidentes y demanda de perfiles especializados

Por Redacción / 3 diciembre, 2024

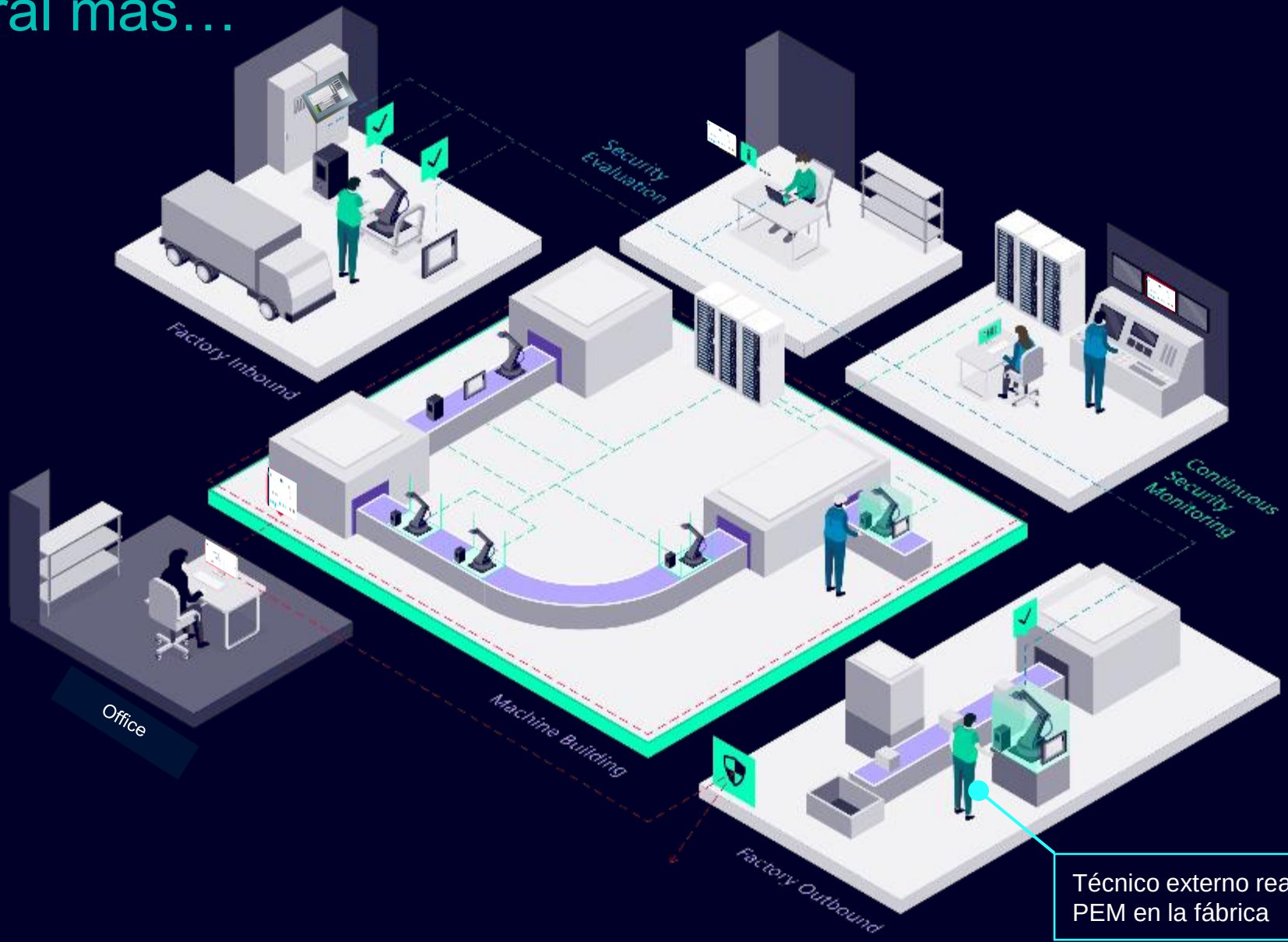
La demanda de profesionales en ciberseguridad en España supera con creces la oferta

Seguridad 13 FEB 2025

SIEMENS

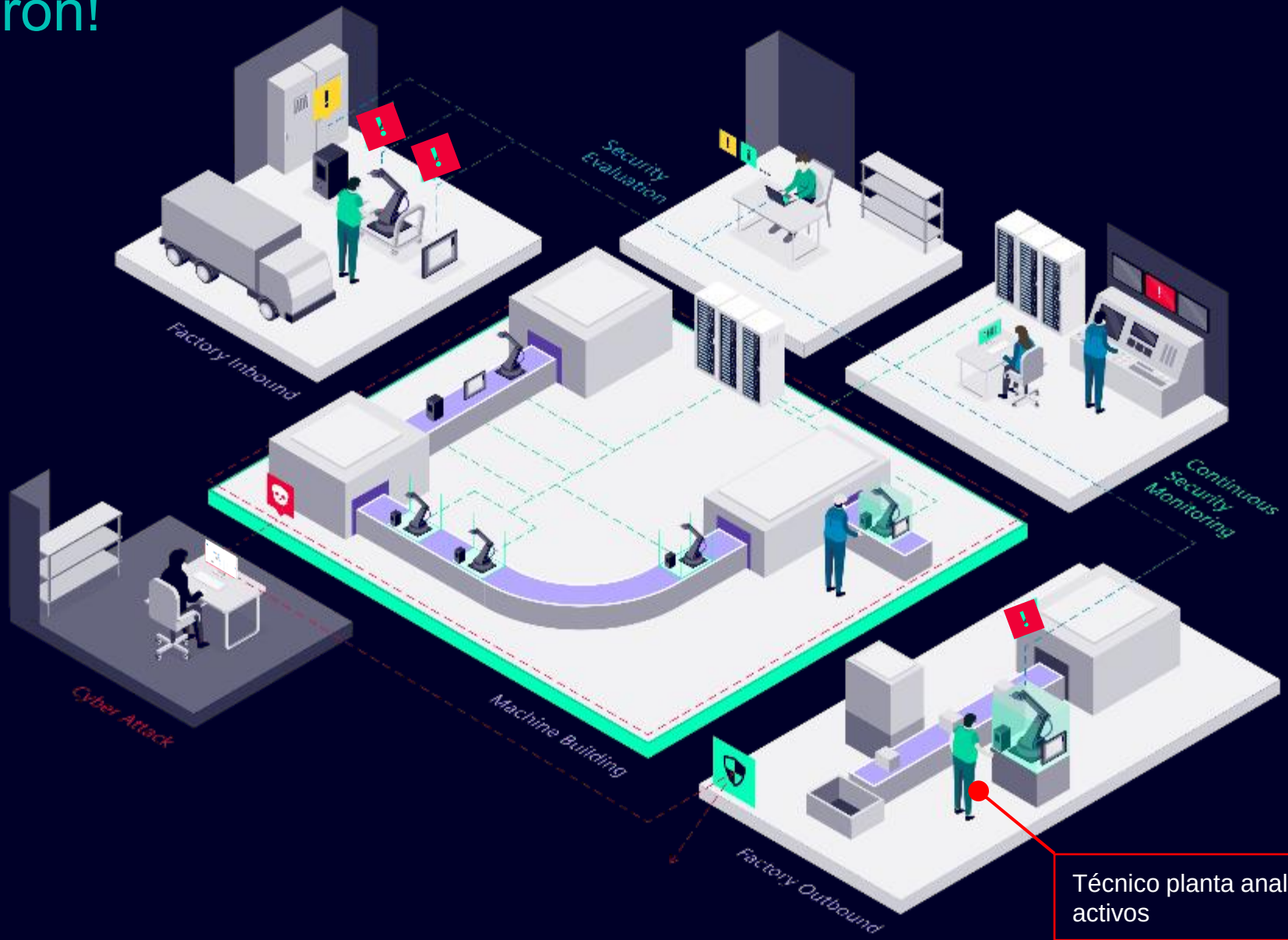
¡Esto es la Tormenta Perfecta!

Un día laboral mas…



SIEMENS

…nos atacaron!



SIEMENS

Toca legislar, y se está realizando en muchas partes del mundo

Las normativas **CIRCIA** y **SEC** en **EE.UU.** cambiarán la forma en que las empresas abordan la ciberdelincuencia La atención se centra en: la información, los criterios de divulgación y la transparencia

Fuente: McKinsey, 2022

Endurecimiento de las obligaciones de ciberseguridad en toda **Europa**: Directiva **NIS2**
Foco en: nuevas normas y más sectores incluidos

Fuente: European Parliament, 2023

Cambios relevantes en la legislación sobre privacidad de datos y ciberseguridad en el **Sudeste Asiático** en 2022

Fuente: Herbert Smith Freehills, 2022

SIEMENS

¿Que es la directiva NIS2?

!

Es la directiva europea más completa en materia de ciberseguridad.

Con requisitos más estrictos para la gestión de riesgos y la notificación de incidentes, una cobertura más amplia de los sectores y sanciones más contundentes en caso de incumplimiento, cientos de miles de organizaciones de la UE tendrán que reevaluar su postura en materia de ciberseguridad.

Entidades Esenciales

Inspecciones in situ y supervisión externa, incluidos controles aleatorios y auditorías periódicas.

Multas: máx de **10M€**, hasta el 2% del volumen de negocios total anual

Energía

electricidad, calefacción y refrigeración urbanas, petróleo, gas and hidrógeno

Bancos

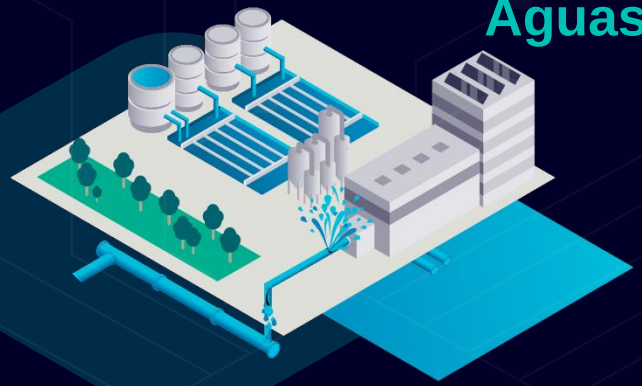
Infraestructuras del mercado financiero

Transporte

aire, vías, agua and carreteras

NUEVO

Agua Potable



Aguas Residuales

NUEVO

Salud incluyendo la fabricación de

productos farmacéuticos

como las vacunas

Infraestructura digital

NUEVO

Espacio

NUEVO

SIEMENS

Entidades importantes

Inspecciones in situ y supervisión externa

Multas: máx de **7M€** hasta un 1,7% del volumen de negocios total anual.

NUEVO

Fabricación

de dispositivos médicos, ordenadores y electrónica, maquinaria y vehículos de motor

Servicios postales y de mensajería

Investigación

NUEVO

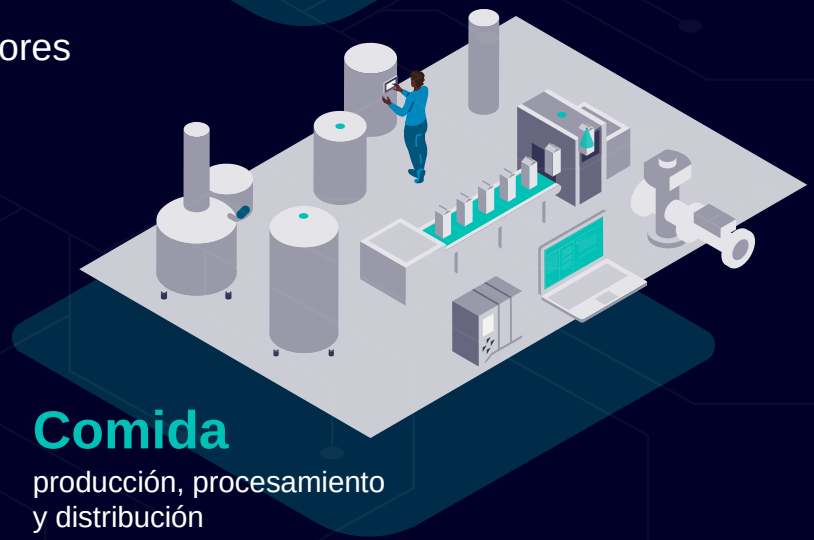
Gestión de residuos

NUEVO

Proveedores digitales

Químicos

NUEVO



Comida

producción, procesamiento y distribución

NUEVO

SIEMENS

Responsabilidades y obligaciones en materia de gestión de riesgos de ciberseguridad (CRM)

La dirección puede hacerse responsable personalmente de los daños

Las medidas CRM **Incluirán al menos** requisitos técnicos y metodologías definidos

La **alta dirección** de las entidades esenciales e importantes **debe aprobar la gestión de riesgos** para la ciberseguridad, **debe comprobar su cumplimiento. Añadiendo obligaciones a la hora de reportar.**

SIEMENS

Obligación de informar

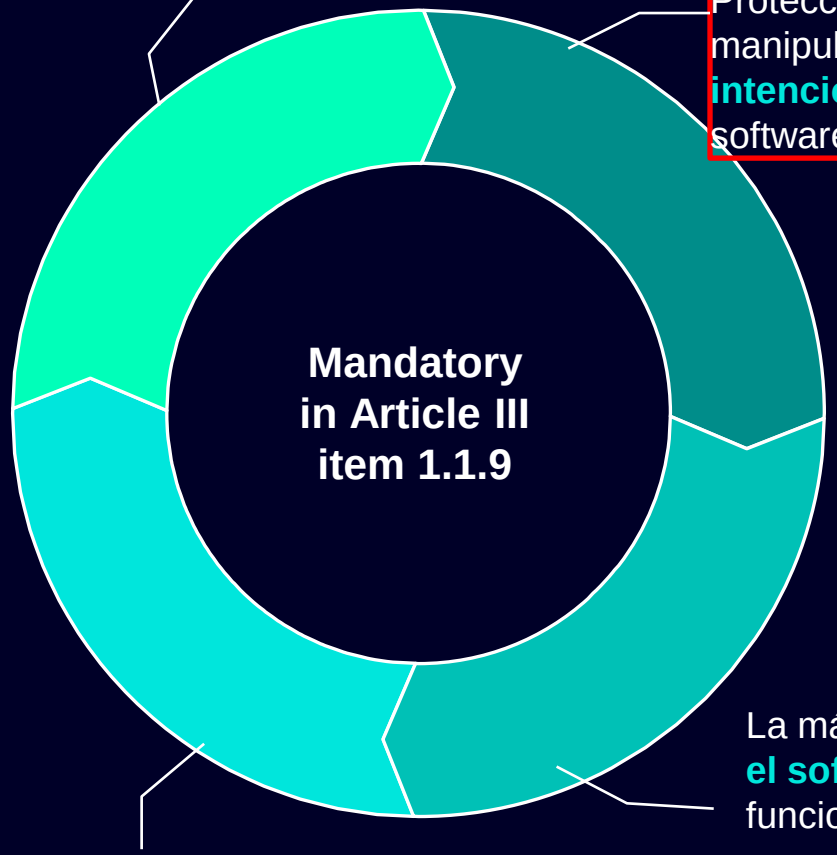
Qué? Cuando?

- Alerta temprana dentro de las 24 h siguientes al conocimiento del incidente
- Después de 72 h, notificación del incidente, incluyendo su gravedad y su impacto
- Informe final del progreso a más tardar 1 mes después de la presentación de dicho incidente

¿Qué va a cambiar? Ciberseguridad de las máquinas en el Reglamento de seguridad de las máquinas

Medidas de ciberseguridad obligatorias

- Requisitos para la interacción hombre-máquina
- Obligatorio en caso de cambio de maquinaria
- Incluye guía para Inteligencia Artificial



Se evitará el **acceso no autorizado** a la máquina, tanto local como remoto

Protección de la máquina contra la manipulación **intencionada o no intencionada** **ya sea** hardware o software

La máquina deberá **identificar el software instalado** para un funcionamiento seguro

registrar los cambios tanto hardware como software

SIEMENS

Se necesitan soluciones… IEC62443

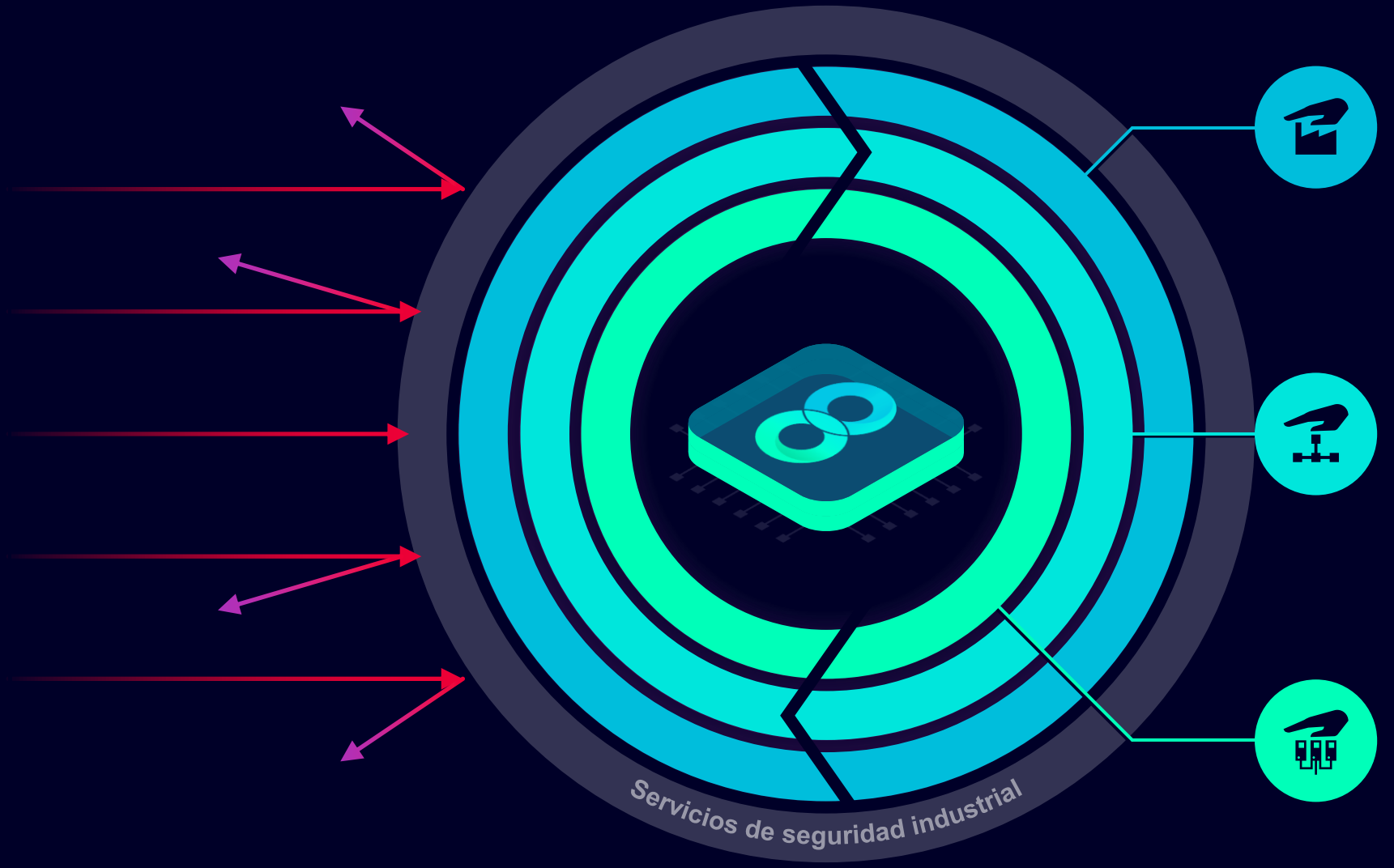
	Publicación	Activación		Fin transición
NIS2	27 dic 2022	16 ene 2023		18 oct 2024

Basadas en una arquitectura de referencia OT

Encuéntrala aquí

SIEMENS

Sólo un modelo de Defensa en Profundidad con multicapa protege en todos los aspectos



Seguridad de planta

- Protección de acceso físico
- Políticas de seguridad
- Monitorización de seguridad

Seguridad de red

- Protección de celdas, zonas de seguridad y redes perimetrales.
- Firewalls y VPN

Integridad de sistema

- Bastionado del sistema
- Gestión de parches
- Autenticación y protección de acceso

SIEMENS

Ciberseguridad OT paso a paso

Paso 1

¡Conozca lo que tiene!

Acciones

- Análisis pasivo de las redes y realizar un inventario de activos

→ **Consultoría**

Paso 2

¡Conozca lo que hace!

Acciones

- Realizar chequeos de posibles vulnerabilidades en los activos

→ **Consultoría**

Paso 3

¡Conozca lo que ha de hacer!

Acciones

- Realizar una evaluación de seguridad y una consultoría de seguridad

→ **Consultoría**

Paso 4

¡Conozca como hacerlo!

Acciones

- Formación del personal, instalación de Firewall Industrial, crear DMZ Industrial, etc

→ **Implementación**

Paso 5

¡Conozca cómo mejorar!

Acciones

- Disponer de sistemas que detecten vulnerabilidades y sistemas que gestionen los parches

→ **Optimización**

¡Vuelta al paso 1!

FINALIDAD

"El objetivo es que las empresas se centren en su actividad principal".

SIEMENS

Ciberseguridad OT paso a paso

***60%** de orgs. están aquí* | ***30%** de orgs. están aquí* | ***10%** de orgs. están aquí*

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6
Concienciación	**Análisis de ventajas y estudio de la Red**	**Momento… Oh Wow!**	**Apagafuegos**	**Integración**	**Optimización**

Paso 1	Paso 2	Paso 3	Paso 4	Paso 5
¡Conozca lo que tiene!	**¡Conozca lo que hace!**	**¡Conozca lo que ha de hacer!**	**¡Conozca como hacerlo!**	**¡Conozca cómo mejorar!**
Acciones • Análisis pasivo de las redes y realizar un inventario de activos	**Acciones** • Realizar chequeos de posibles vulnerabilidades en los activos	**Acciones** • Realizar una evaluación de seguridad y una consultoría de seguridad	**Acciones** • Formación del personal, instalación de Firewall Industrial, crear DMZ Industrial, etc	**Acciones** • Disponer de sistemas que detecten vulnerabilidades y sistemas que gestionen los parches
→ Consultoría	**→ Consultoría**	**→ Consultoría**	**→ Implementación**	**→ Optimización**

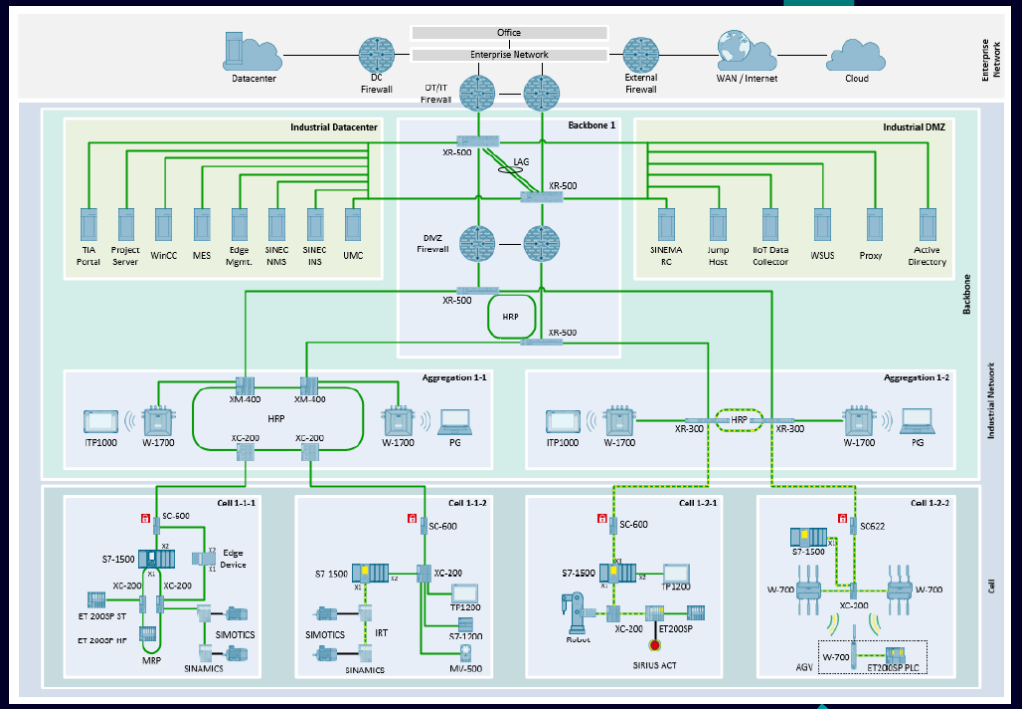
¡Vuelta al paso 1!

FINALIDAD

"El objetivo es que las empresas se centren en su actividad principal".

SIEMENS

La ciberseguridad es un concepto circular



SIEMENS

¿Por dónde **empezar?**

Seguridad en Planta

- Descubrimiento y gestión de activos de red
- Evaluación y consultoría de seguridad
- Asesoramiento en las políticas
- Formaciones de ciberseguridad
- Gestión de Backups
- Seguridad de la cadena de suministro

Seguridad en la Red

- Detección de Anomlías
- Cryptografía y Cifrado
- Seguridad IT/OT basada en Zero Trust
- Seguridad perimetral de la integración IT/OT

Integración del sistema

- Integración de sistemas OT en un SIEM de IT existente
- Gestión de usuarios para OT
- Gestión de vulnerabilidades y parches

Y habrá más …

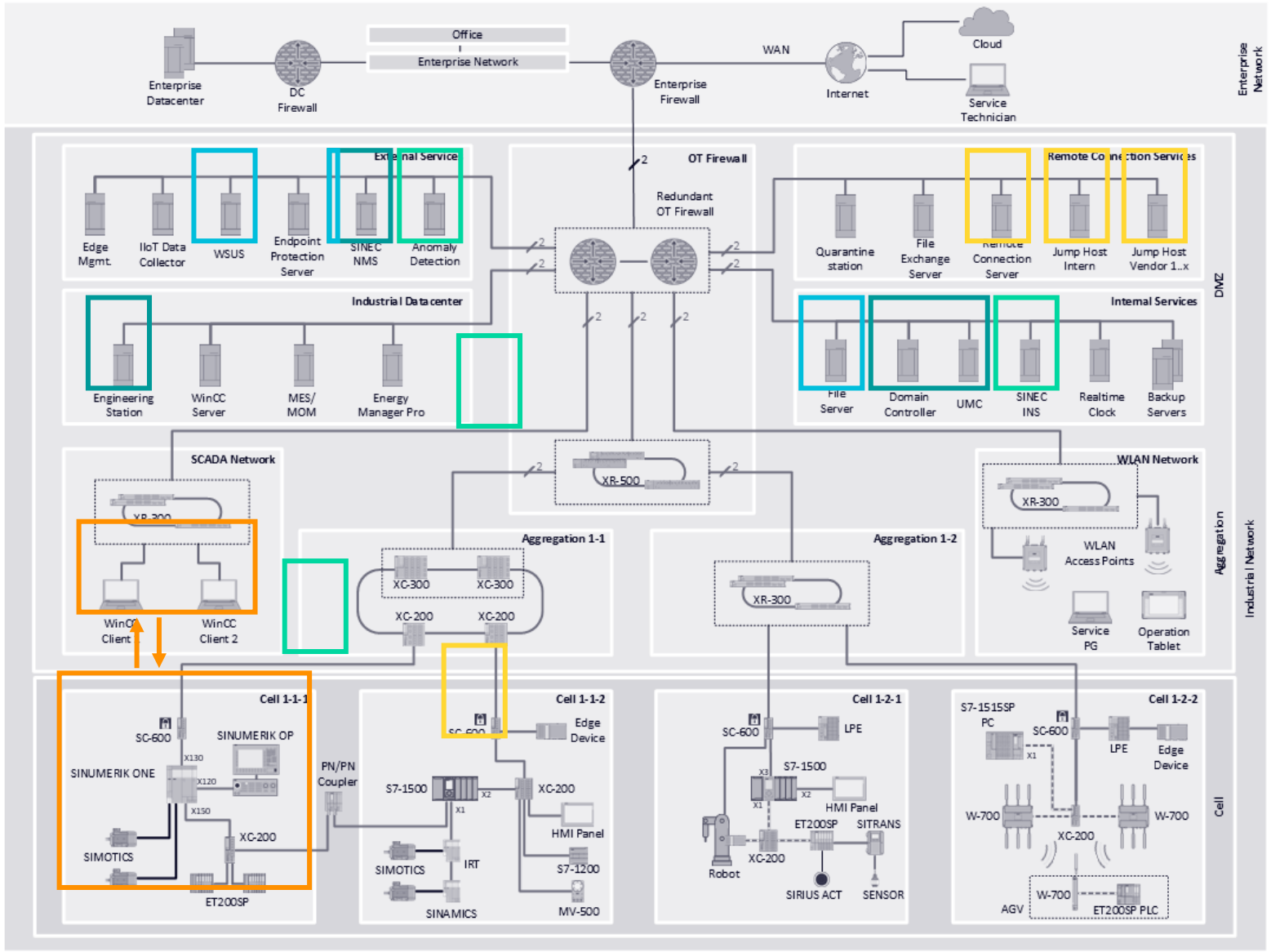
Solución basada en la “Secure Reference Architecture”

- Descubrimiento y gestión de activos
- Gestión de usuario
- Detección basada en anomalías/intrusiones
- Gestión de vulnerabilidades y parches
- Comunicación cifrada para OT
- Acceso remoto Seguro/Zero Trust

Y más…

SIEMENS

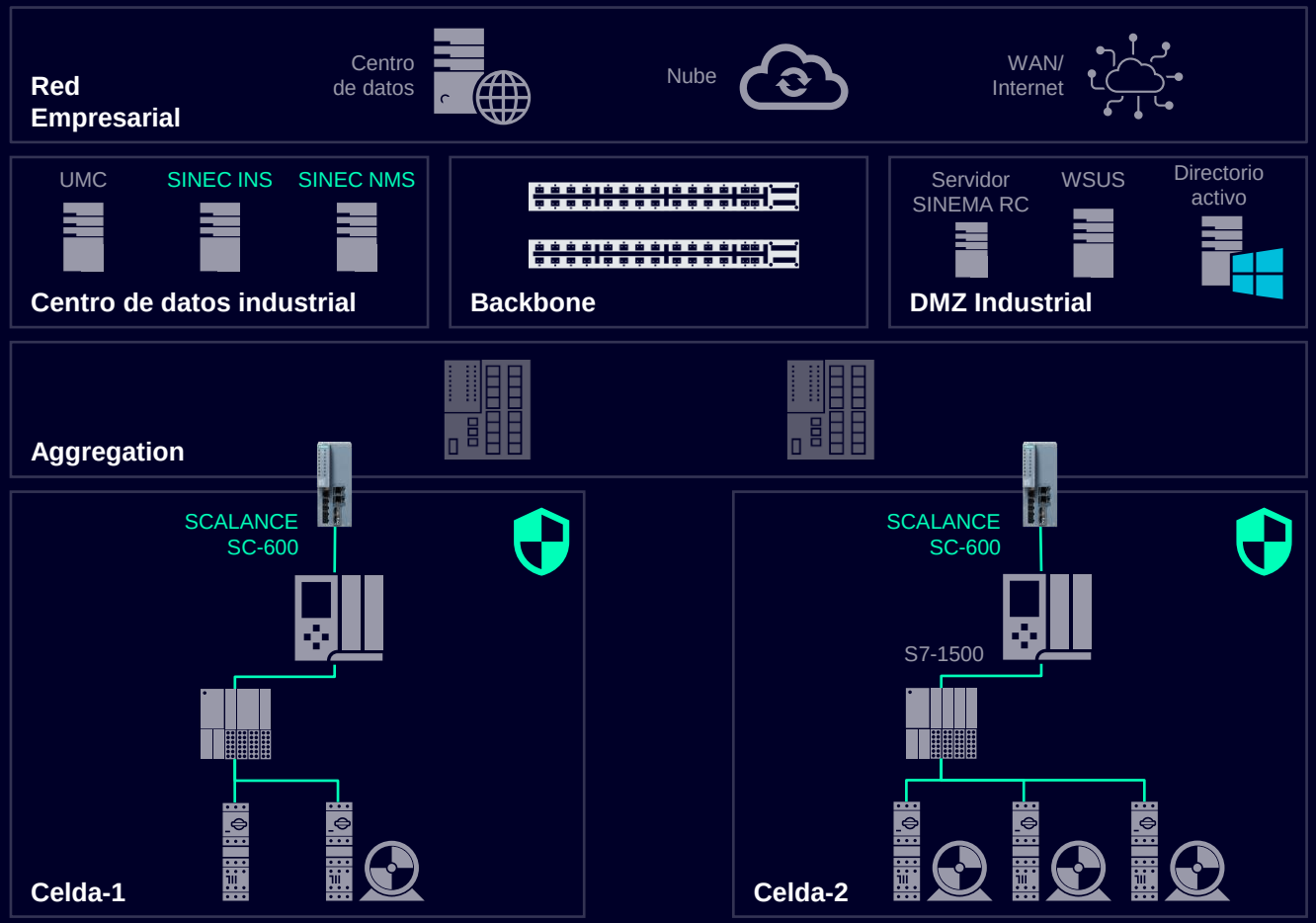
Secure Reference Architecture



- Descubrimiento y gestión de activos
- Gestión de usuario
- Detección basada en anomalías/intrusiones
- Gestión de vulnerabilidades y parches
- Comunicación cifrada para OT
- Acceso remoto Seguro/Zero Trust

SIEMENS

Soluciones NIS2
Segmentación OT



Solución

Seguridad perimetral con productos SCALANCE y SINEC

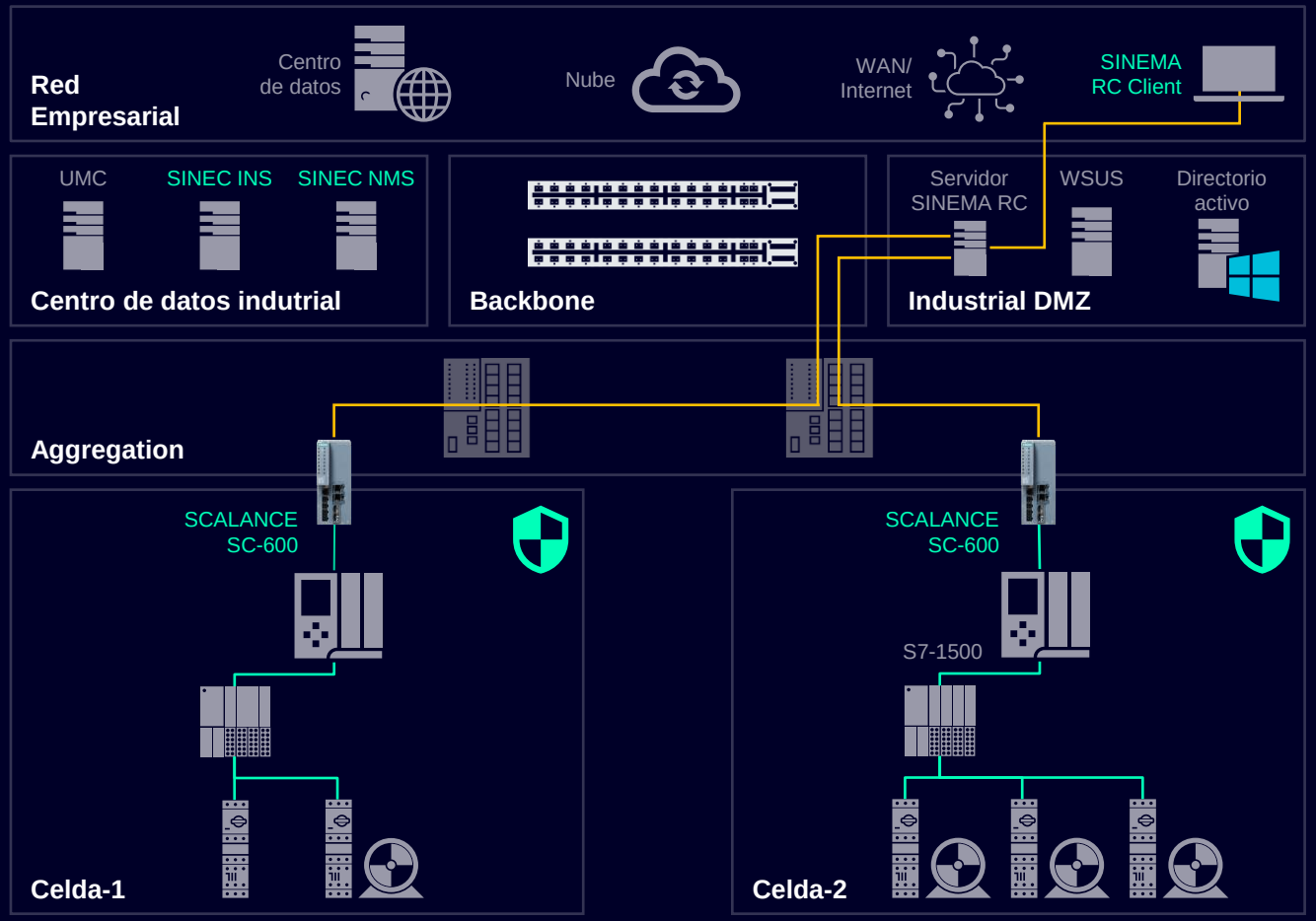
El comienzo pasa por el enfoque de la solución.
El concepto de seguridad de celda mediante dispositivos SCALANCE S protegiendo cada máquina siendo gestionados de forma centralizada con SINEC NMS. SINEC INS proporciona servicios adicionales para la autenticación de usuarios y la recopilación centralizada de eventos.

Los puntos clave de este enfoque son:

- Segmentación de la red
- Protección de los límites de las zonas
- Protección de la comunicación entre las zonas de seguridad
- Gestión centralizada

SIEMENS

Soluciones NIS2
Acceso remoto



Solución

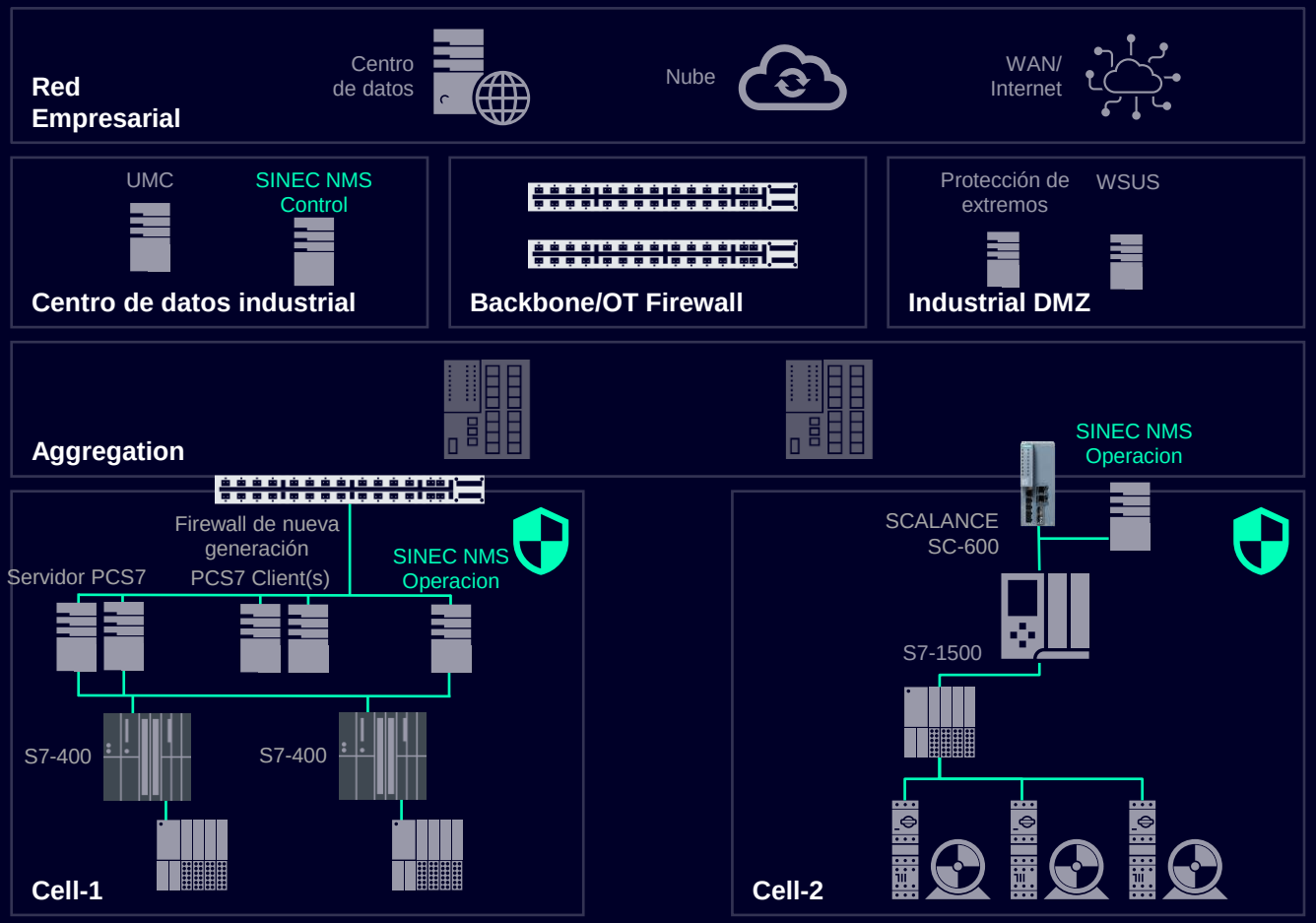
Cómo establecer conexiones remotas seguras

Desde SINEMA RC Client y la máquina a la que se va a dar servicio con el SCALANCE S se establecen conexiones separadas a un SINEMA RC Server.
La identidad de los participantes determinada mediante certificados permite gestionar el acceso remoto a la máquina.

Los puntos clave de este enfoque son:

- Comunicación segura mediante VPN
- Fácil de implantar
- Fácil de gestionar

Soluciones NIS2
Descubrimiento y gestión de activos



Solución

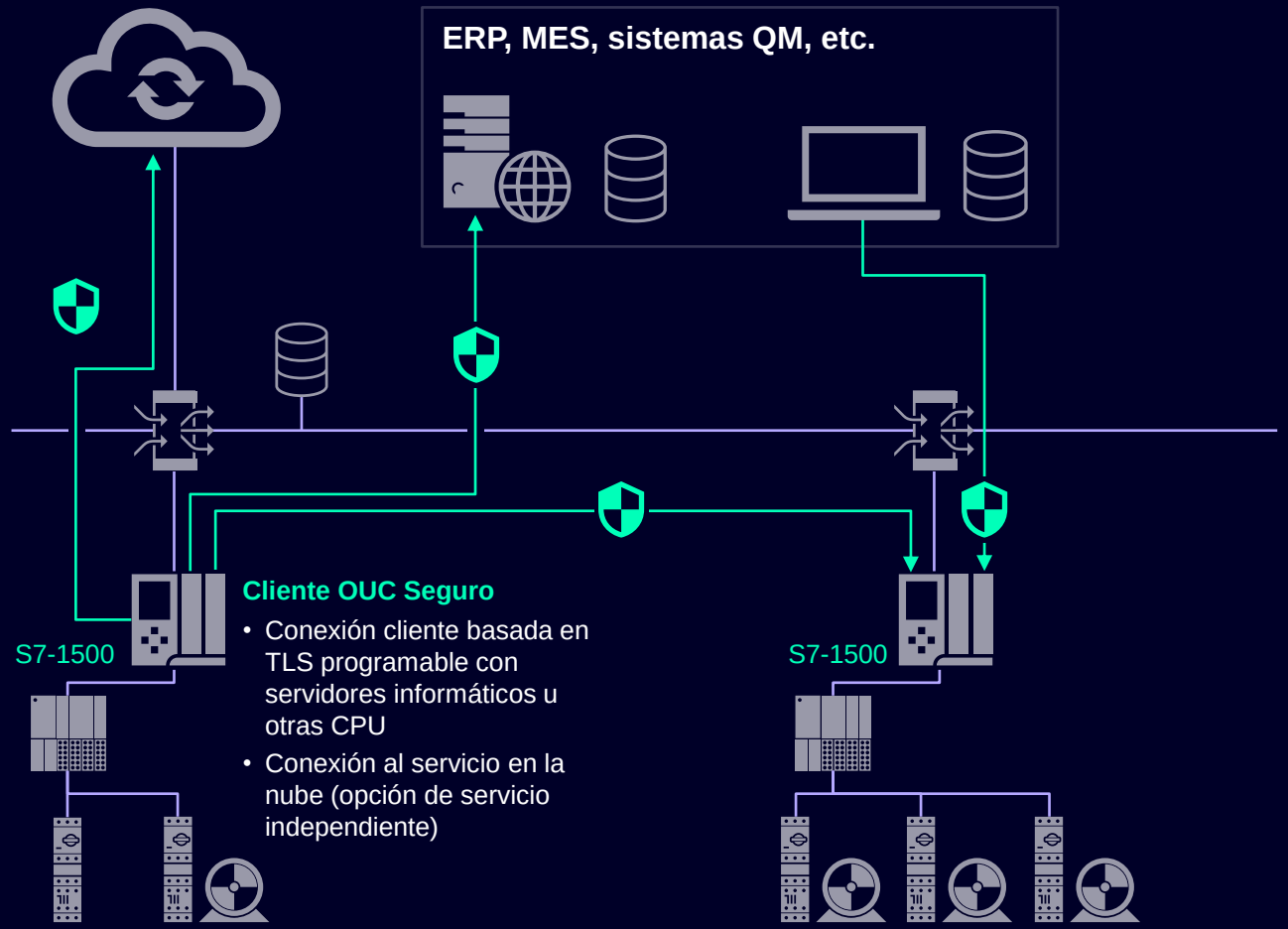
La solución de Siemens hace uso del sistema centralizado SINEC NMS (Network Management System) o PRONETA para proporcionar:

- Monitorización de red
- Descubrimiento automático de la topología
- Gestión de configuración de dispositivos

SINEC Security Inspector ofrece un escaneado para generar una visión general de la instalación y la seguridad de los componentes.

La evaluación de dichas soluciones a través de consultoría es igualmente un valor para el cliente final.

NIS2 Solutions
Criptografía y Cifrado, así como endurecimiento del sistema con una sola herramienta



1 Transport Layer Security

Solución

Integridad mediante autenticación y cifrado
Cifrado de extremo a extremo entre activos de OT
Comunicación segura de última generación basada en TLS1 V1.3

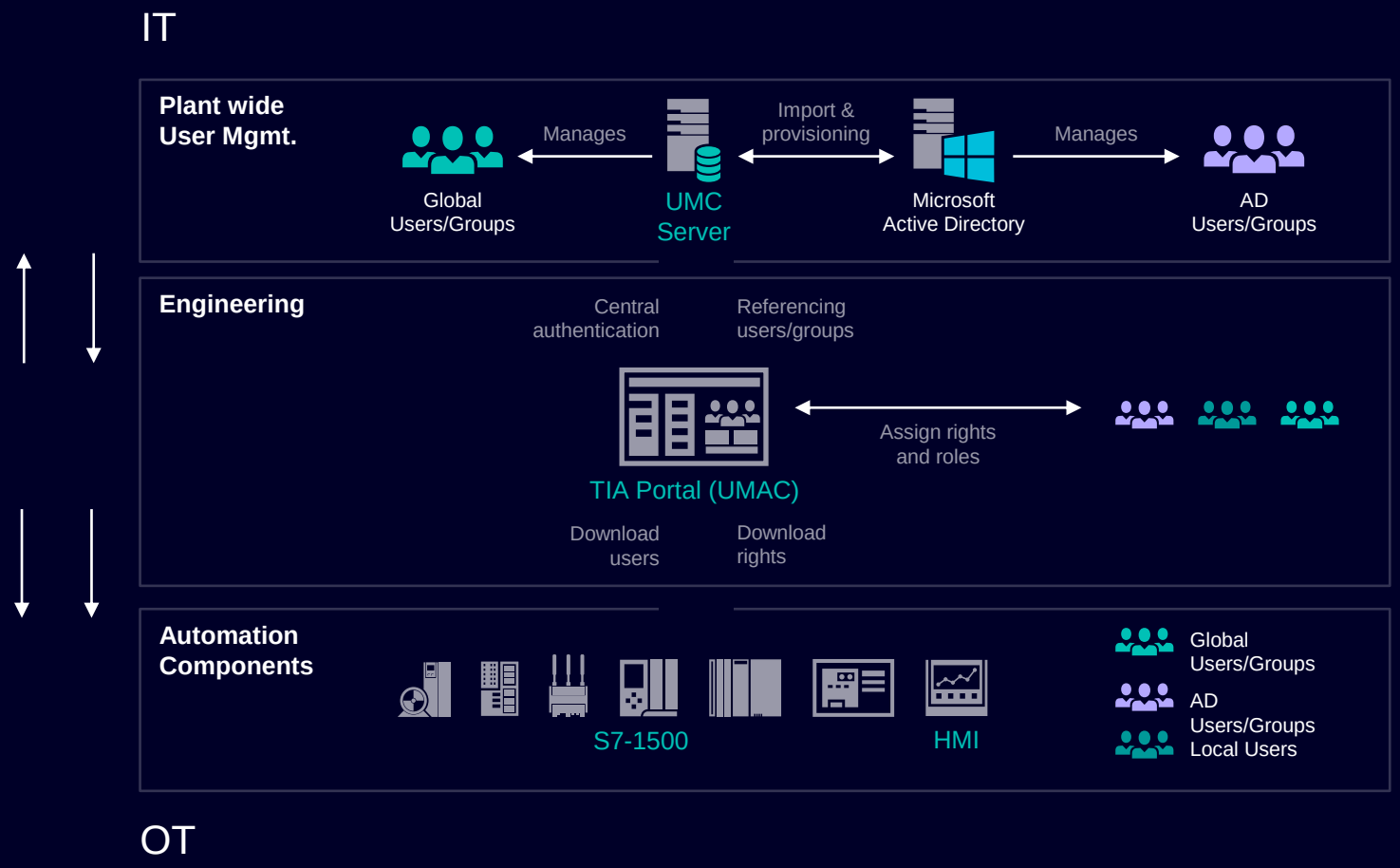
Simplificación del proceso de puesta en servicio en lo que respecta a las configuraciones de seguridad

Valor para el cliente
- Identificación única de los componentes basada en certificados individuales que reducen los riesgos de seguridad.
- Confidencialidad de las comunicaciones gracias al intercambio de datos cifrados.
- Autenticación de los interlocutores de comunicación para evitar que partes no autorizadas establezcan una comunicación con los componentes.

Productos & Servicios
- TIA Portal
- S7-1500, S7-1200
- HMI

SIEMENS

NIS2 Solutions
Gestión de usuarios para OT



Solución

Importar usuarios y grupos de Microsoft Active Directory al servidor UMC del componente de gestión de usuarios.
Importar usuarios y grupos del servidor UMC al proyecto TIA Portal, SINEMA RC...
Asignación local de derechos y funciones a través del sistema local de gestión de usuarios y control de acceso UMAC.
Usa los usuarios importados para controlar el acceso a las CPUs, HMIs

Valor para el cliente

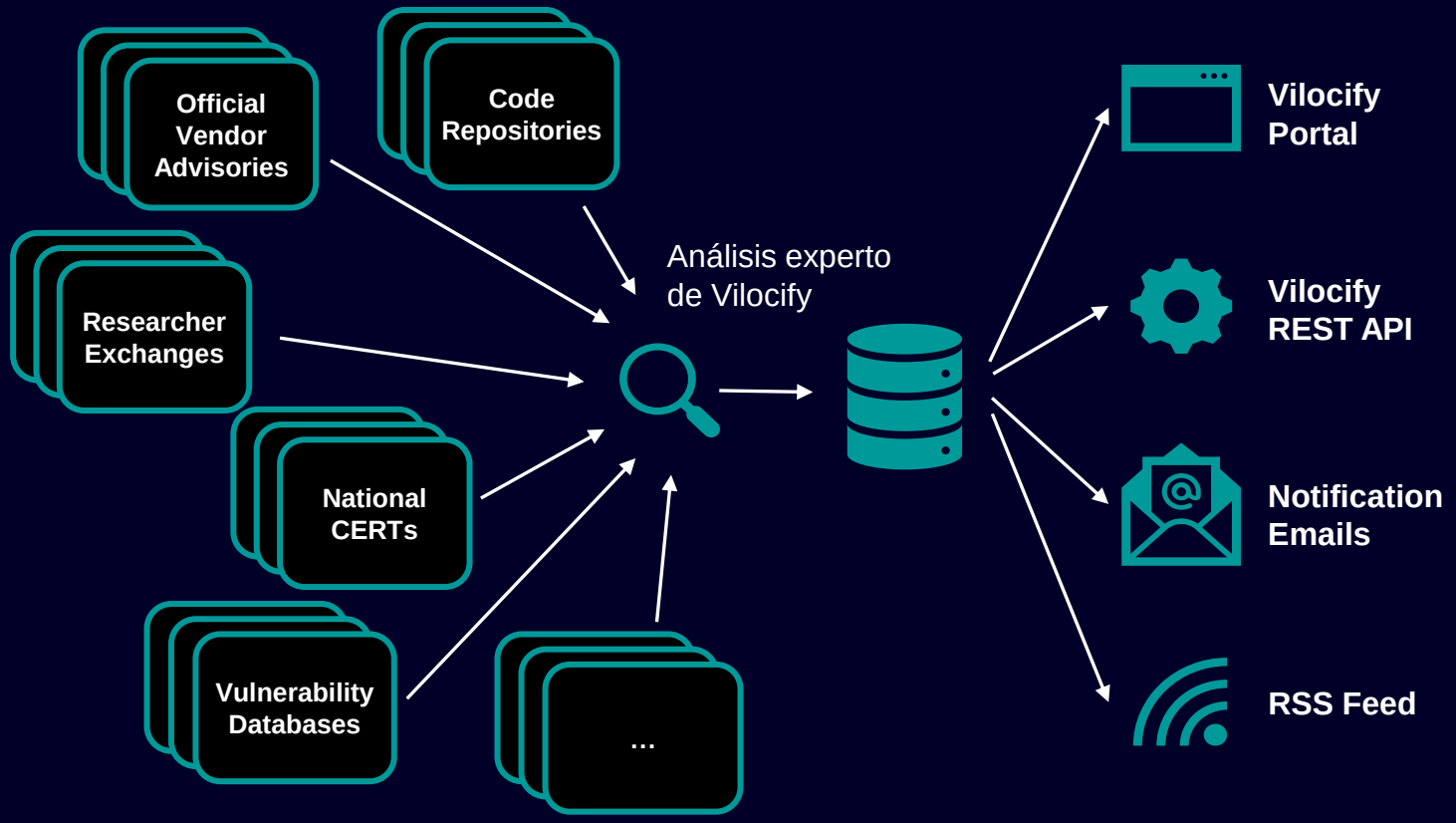
- Gestión centralizada de usuarios para toda la planta.
- Los usuarios/grupos pueden importarse de servidores Microsoft AD ya disponibles, lo que ahorra tiempo y esfuerzo.
- Acceso personalizado en lugar del acceso genérico mediante contraseña

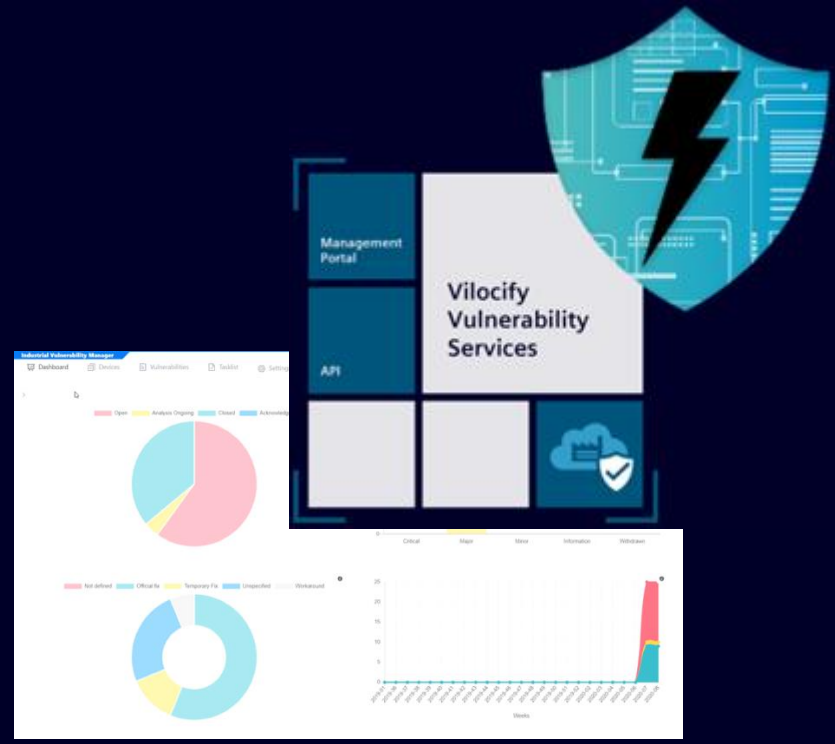
Productos & Servicios

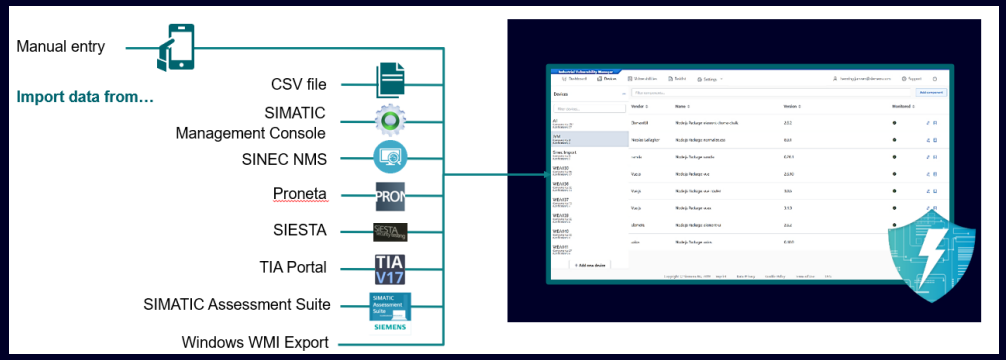
- User Management Component (UMC)
- TIA Portal
- S7-1500, S7-1200, HMI…
- SINEMA RC, SINEC NMS
- …

SIEMENS

Soluciones NIS2
Gestión de vulnerabilidades







SIEMENS

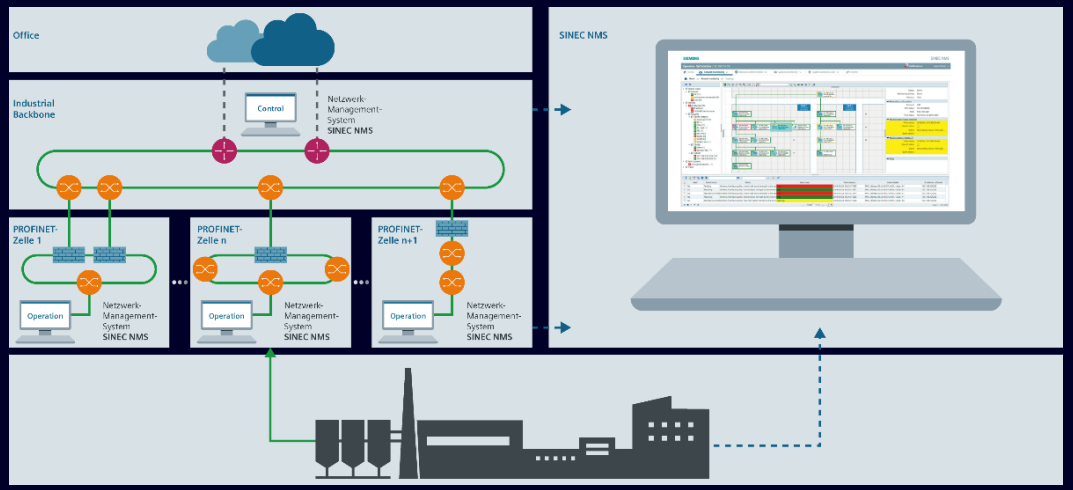
Soluciones NIS2
Parcheado del sistema y actualizaciones de versiones

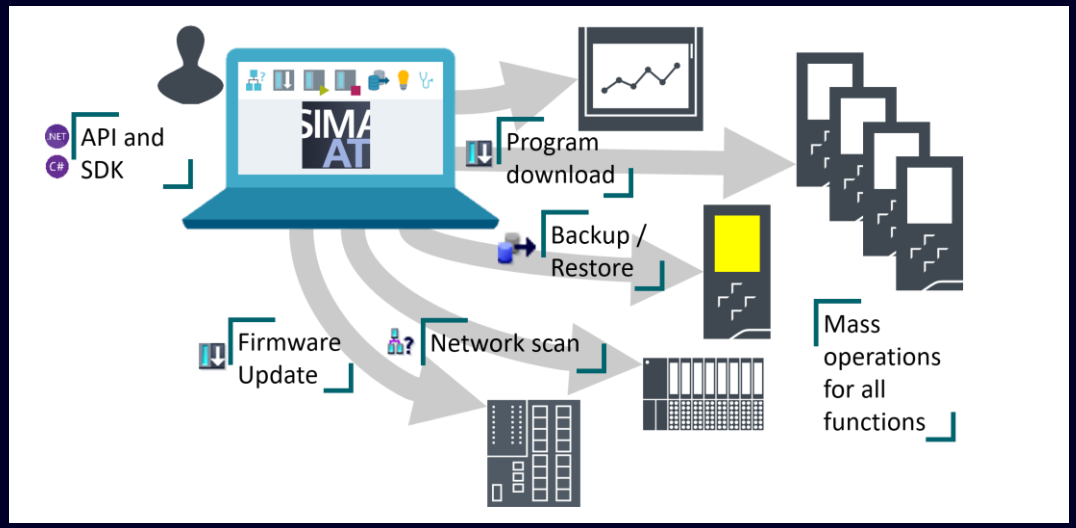
Caso de uso en el ciclo de vida

- El conocimiento de nuevas amenazas requiere igualmente una ágil respuesta a las mismas.
- Disponer de las herramientas oportunas puede reducir el tiempo de exposición enormemente elevando la madurez de nuestras máquinas.

El reto

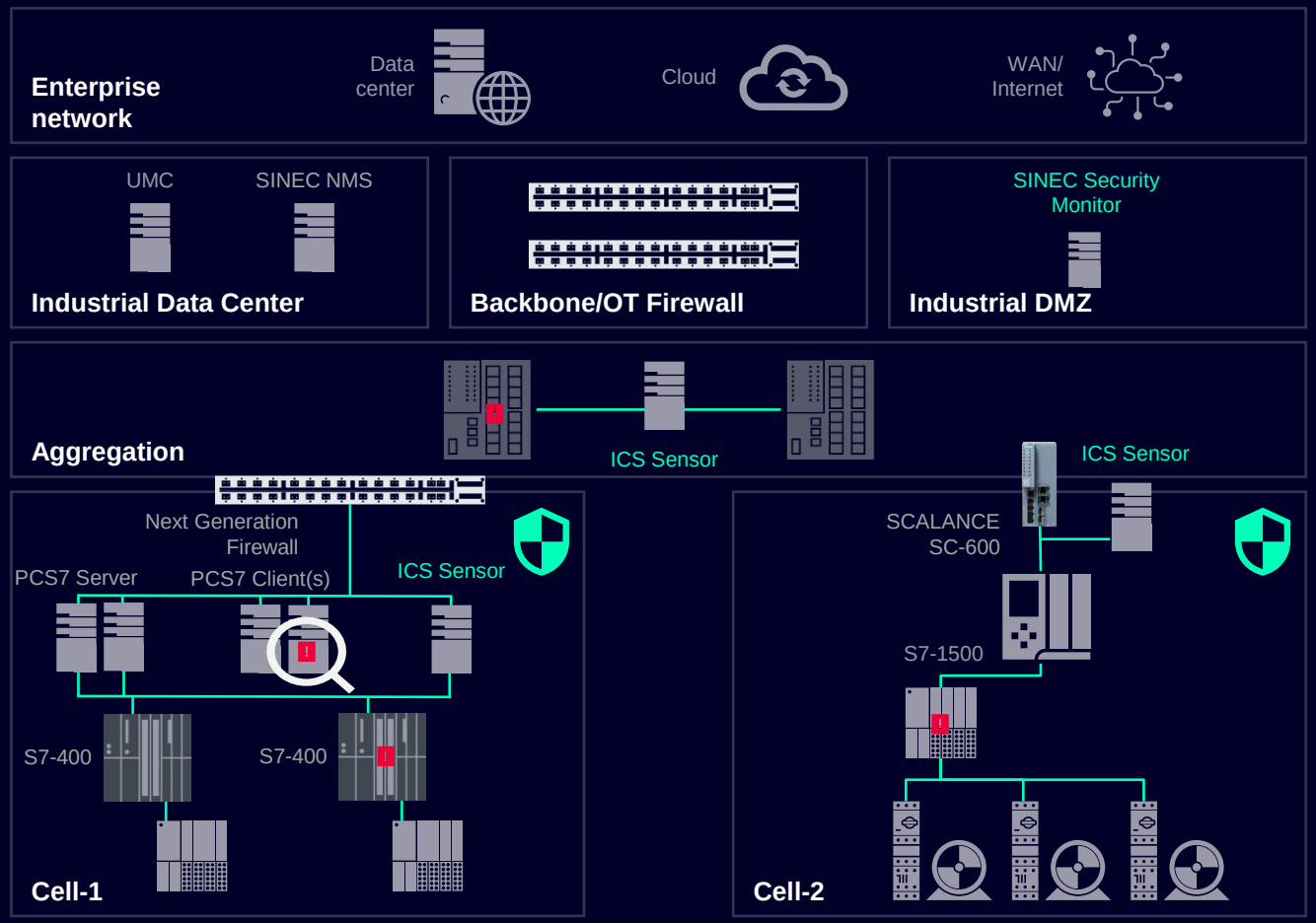
- Utilización de SAT, despliegue WSUS, NMS son soluciones que han de integrarse para posteriormente ser capaces de responder a los parches de seguridad existentes y que necesitan ser desplegados.





SIEMENS

NIS2 Solutions
Detección de Anomalías



Solución

SINEC Security Monitor, supervisa el tráfico de la red, crea una línea de base de funcionamiento normal y detecta anomalías a partir de esa línea de base.
Los operadores pueden reaccionar rápidamente y atajar las amenazas en fase temprana.

Valor para el cliente

- La transparencia en el intercambio de datos dentro de las redes industriales facilita la detección de anomalías en la fabricación.
  Detección temprana de anomalías y amenazas para aumentar la ciberseguridad industrial.
- Solución de supervisión 100 % pasiva para una mayor ciberseguridad sin impacto en los sistemas de control industrial supervisados.

Productos & Servicios

- SINEC Security Monitor

SINEC
Security Monitor

SINEC
Security Inspector

Monitorización del acceso remoto

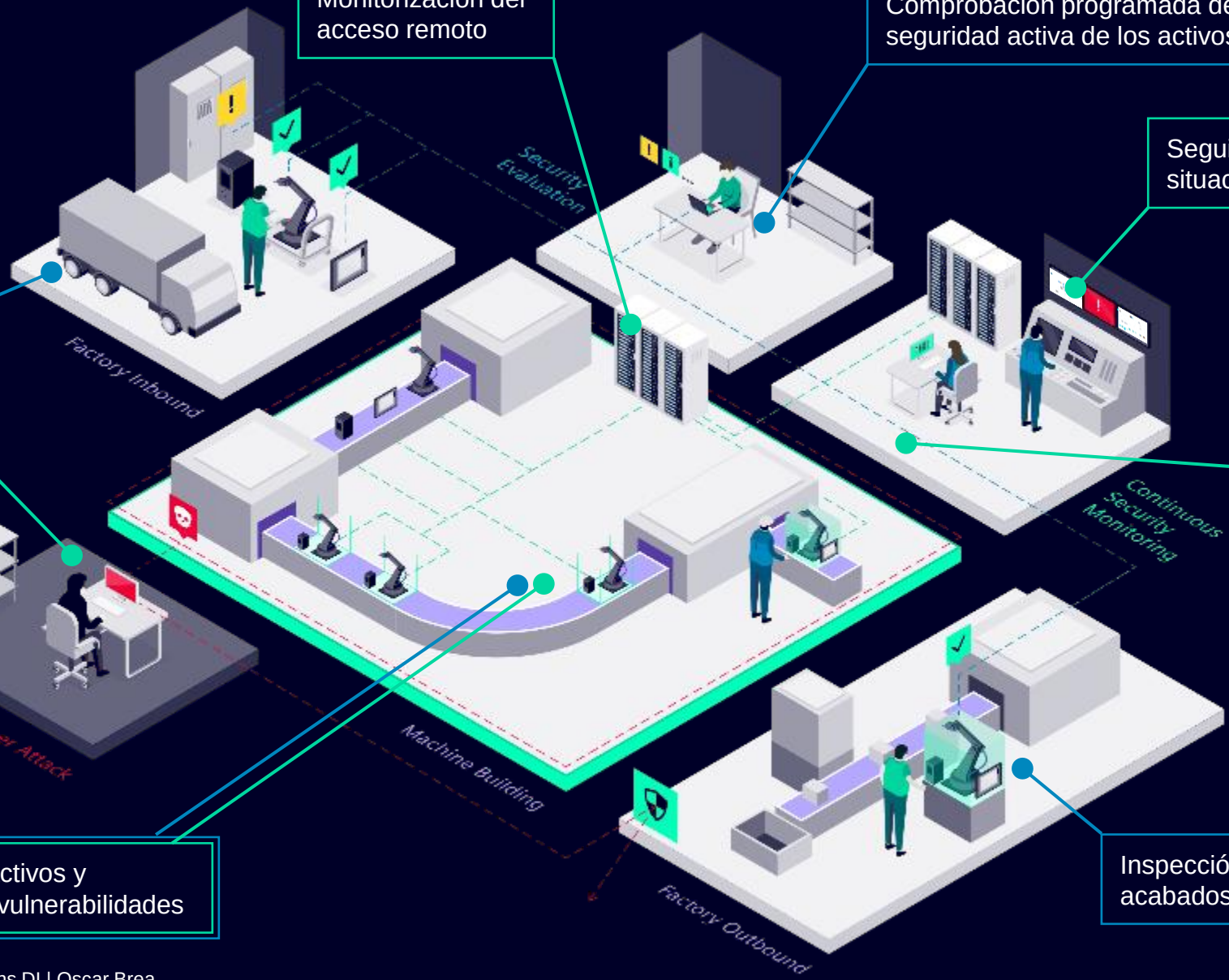
Comprobación programada de la seguridad activa de los activos

Seguimiento constante de la situación de la ciberseguridad

Inspección de mercancías entrantes

Detección de ataques para iniciar contramedidas

Evitar riesgos mediante la supervisión de los PC



Detección de activos y correlación de vulnerabilidades

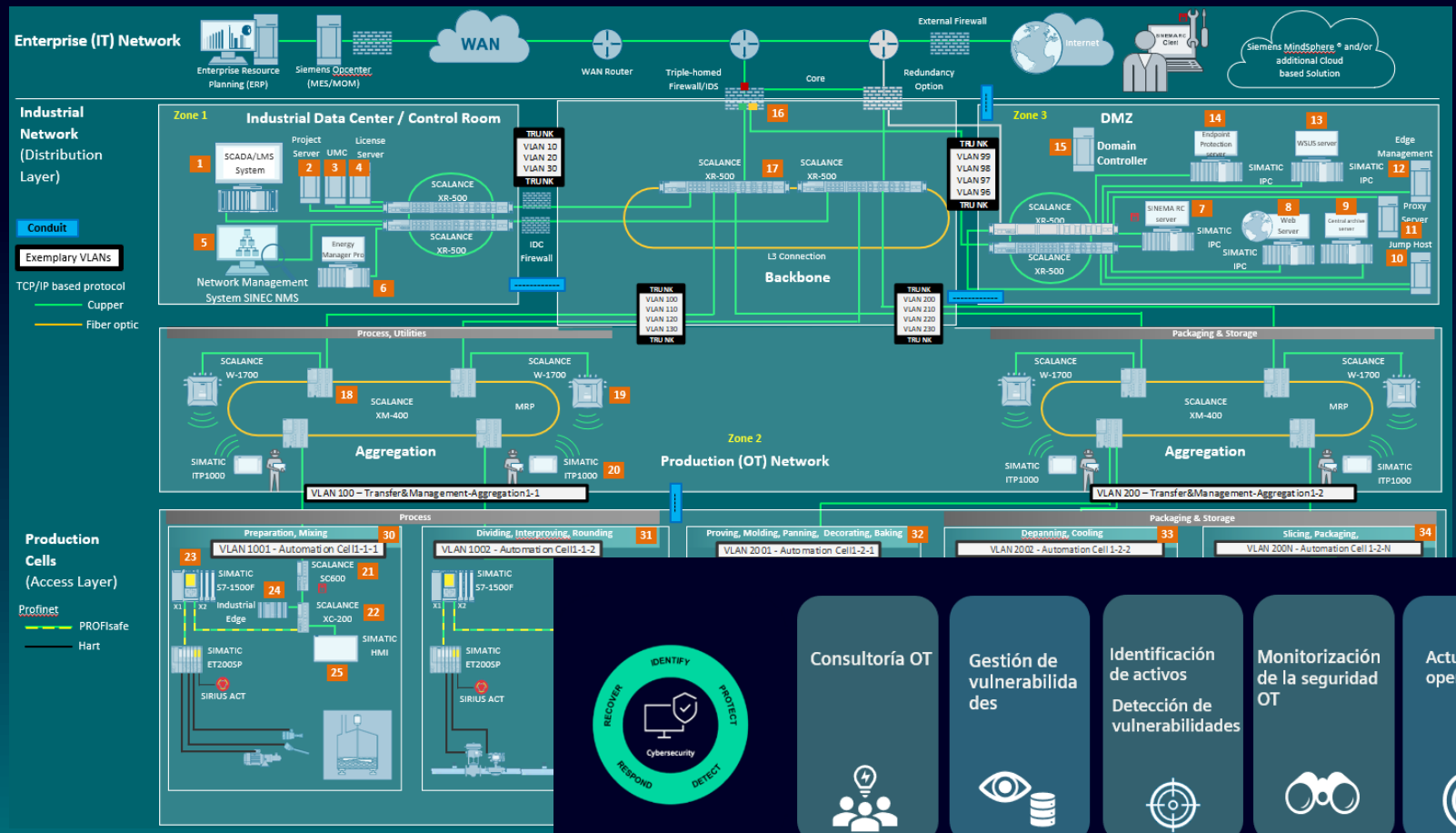
Inspección de los productos acabados antes de la entrega

SIEMENS

Nuestros expertos le ayudan a crear arquitecturas seguras para su actividad industrial

Seguridad integral, desde la consultoría hasta la implantación de productos y soluciones:

Hecho a medida para sus operaciones industriales completas: desde el sensor hasta la nube



SIEMENS

MUCHAS GRACIAS

Oscar Brea Castro
Sales Manager
Siemens DI Galicia-Asturias-Cantabria

Fernando Casas Novoa s/n
15890 Santiago de Compostela,
España
Mobile +34 670 929 899
E-mail oscar.brea@siemens.com

SIEMENS