DOCUMENTOS SiC
Nº 37
SEPTIEMBRE 2022

SIEMENS Ciberseguridad industrial a la medida de la transformación

Karen Gaines

Global Head of Cybersecurity Defense de Siemens

"Aspiramos a ser el referente global de ciberprotección en el mercado"

Protección de sistemas críticos e infraestructuras estratégicas

Vilocify: servicio inteligente para identificar vulnerabilidades en tiempo real

ENTREVISTA

Pedro Martín

Gerente de Servicio del Centro de Ciberdefensa (CDC) de Siemens CYS

Protección holística e integrada como componente esencial de la transformación digital

Siemens CYS: la experiencia probada en ciberseguridad del gran referente industrial europeo

Presente en todos los países, Siemens es la compañía tecnológica industrial más grande de Europa, con más de 2.000 millones de personas que usan sus servicios. Por ello, también es uno de los referentes en protección de entornos ciberfísicos y sus tecnologías de operaciones (OT), una apuesta que se plasma en productos y servicios que tienen en su ADN enfoques como la confianza cero, una estrategia de defensa en profundidad, holística y la capacidad para anticiparse a las ciberamenazas a través de su área de Defensa y de su Centro de Defensa Cibernética (CDC).

'We sell what we use' ('Vendemos lo que utilizamos'). Bajo este lema, esta multinacional y su división de ciberseguridad (CYS), reforzada en 2018, marcan la diferencia con sus rivales en lo que atañe a protección industrial y sus sistemas operativos (OT). Con un equipo dedicado de más de 1.300 especialistas, repartidos en centros globales (*hubs)* de ciberseguridad en Alemania, China, Canadá, Portugal, EE.UU. y España (más de 80 expertos, en Tres Cantos, Madrid), la compañía apuesta por la protección industrial y, también, de los sectores que estén sumergidos en la transformación digital, con un enfoque holístico y granular, incluyendo la seguridad cibernética como un pilar fundamental. Para ello, cuenta con cinco áreas especializadas: Ciberdefensa, Protección OT/IT, Seguridad en la Nube, Gestión del Riesgo y Cumplimiento y Consultoría. Todas comparten una filosofía de protección global permeable a toda la organización, con soluciones y estrategias adaptadas a cada cliente, sector y vertical. Buena prueba de la importancia que da la compañía a la ciberseguridad es que su CISO, **Natalia Oropeza,** depende directamente del CEO global, **Roland Busch.**

Seguridad proactiva e inteligencia

En su enfoque destaca la capacidad de anticipación a través de su Centro de Ciberdefensa (CDC), desplegado entre Lisboa, Madrid y Cincinnati (EE.UU.), que trabaja en coordinación con el equipo CERT (equipo de respuesta a incidentes) y el Product CERT (encargado de la seguridad de los productos de la compañía, de uso interno y también por parte de sus clientes). Además, desde abril de 2022, también cuenta con un nuevo Centro de Ciberseguridad para Infraestructuras Críticas, en Canadá.

Todos ellos basan su protección en el ciclo de vida de productos y servicios (identificar, proteger, responder y recuperar) y una apuesta por la 'mejora continua' de la ciberseguridad. Un valor al que se suma su experiencia y conocimiento en el ámbito industrial. Y es que, nada que ofrezca Siemens CYS se comercializa sin haber sido probado con éxito antes, de forma intensiva, en sus infraestructuras. Un buen ejemplo es la oferta plasmada en soluciones como Vilocify, SiESTA y Osa.

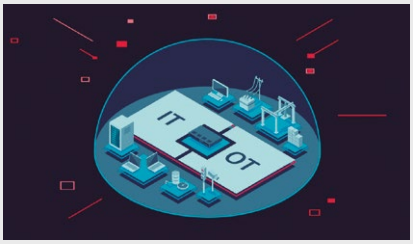
Además, su sistema global también cuenta con un marco certificado IEC 62443, diseñado para entornos industriales con un "enfoque integrado de experiencia en redes OT, software certificado y hardware resistente".

Alianzas internacionales

Su apuesta para llevar la ciberseguridad más allá de su compañía y cliente es fuerte. La empresa impulsó, en 2018, la alianza internacional **'Charter of Trust'** a la que se han sumado grandes referentes, como Airbus, Daimler o IBM. También, tiene una presencia activa en organismos internacionales como el **Centro Europeo de Análisis e Intercambio de Información sobre Energía** (EE-ISAC) o el **Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN** (NATO CCDCOE). ●

Socio confiable para cumplir con las grandes regulaciones como NIS2

Los ataques cibernéticos ya no se dirigen solo a empresas, sino también a particulares, comunidades, infraestructuras críticas e incluso países, por lo que la inversión en su protección es esencial para la creación de un ciberespacio seguro. A ello se suma la acción normativa, marcada por la vigente NIS1 y por la casi lista NIS2, al objeto de regular de forma común en todos los estados



miembros los sistemas y medidas de ciberseguridad. Entre otros aspectos, NIS2 busca incrementar el nivel de ciberresiliencia de un gran conjunto de empresas que operan en la UE en diversos sectores, a través de normas y medidas de ciberseguridad que las organizaciones estarán obligadas a implementar. Una de estas medidas será que las empresas deberán tener conocimiento de los ataques que sufren, para lo que es esencial la monitorización.

Propuesta de Siemens CYS

Asimismo, la NIS2 se propone reducir incoherencias en tema de resistencia en los sectores ya cubiertos por la directiva, para lo cual se invertirán esfuerzos en alinear el ámbito de aplicación, los requisitos de seguridad y notificación de incidentes, entre otros aspectos.

Precisamente, en esta línea Siemens ha situado la monitorización como una de sus prioridades y desde CYS se ha desarrollado el **Cyber Defense Center de tecnología OT (CDC OT),** para dicha labor. Asimismo, para finales de 2022 está previsto la comercialización del sistema propio de monitorización de Siemens bautizado como OSA. Un reto para el que la compañía también cuenta con áreas de negocios especializadas, tanto en soluciones integradas de Ciberseguridad de Siemens como de consultoría que cubre elementos tecnológicos, procedimentales y personales y servicios integrales a lo largo de todo el ciclo de vida de los activos.

Karen Gaines, Global Head of Cybersecurity Defense de Siemens A.G.

"Nos estamos enfocando especialmente en los entornos OT debido al incremento de ciberataques que registran"

Es una de las ejecutivas que mejor conoce la protección en los entornos IT e industriales y, también, cómo sacar el máximo partido a las tecnologías y estrategias más innovadoras. Responsable de una de las áreas de mayor proyección en Siemens CYS, su reto es convertirla en "el referente global de ciberprotección en el mercado".

"Nuestra extensa experiencia en la gestión de la ciberseguridad de Siemens hace que estemos especialmente preparados para evaluar el ecosistema de los clientes y ayudarles a crear un entorno controlado de protección global".

– **¿Cómo está evolucionando el enfoque de Siemens CYS y, sobre todo, su área de Defensa?**
– Nuestra estrategia en el área de Defensa se está enfocando intensamente a los entornos OT, dado el crecimiento de los ataques en ellos.
– **Como responsable de dicha área, ¿cuáles son sus pilares y retos?**
– Uno de los grandes retos es seguir perfeccionando la gestión de la protección de todos los activos IT/OT de Siemens bajo nuestra responsabilidad. Ser capaces de monitorizar, proteger y responder a entornos que van desde la nube hasta la maquinaria industrial. También, lo es impulsar iniciativas con base en *Zero Trust,* una pieza angular en nuestra estrategia para lograr una seguridad efectiva.
– **¿Cómo va perfeccionándose el modelo de 'defensa en profundidad' y protección holística?**
– El mejor motor es el aprendizaje constante al hacer frente a los riesgos día a día. Hay que reaccionar y eso significa que estamos poniendo a prueba nuestro método y capacidades.
– **¿Qué peso tiene, en la propuesta de Siemens CYS, el Hub de Ciberseguridad situado en Tres Cantos (Madrid)?**
– Muy relevante, ya que en los últimos tres años ha crecido hasta conformar un equipo de unos 80 profesionales. Su motor principal es el talento que hay en ciberseguridad en España y, también, su colaboración con los centros del resto del mundo. Eso sí, nuestro *hub* se caracteriza por tener el mayor número de expertos y especialidades. El objetivo, a medio plazo, es que Siemens España, de la mano de nuestras unidades de negocio, sea un referente global de ciberprotección en el mercado.
– **¿Qué propuesta tiene Siemens CYS en el ámbito industrial para ayudar a los CISO?**
– El aspecto más crítico en este momento es que los entornos OT, tradicionalmente, no han sido concebidos, construidos y operados pensando en la ciberseguridad. Por ello, hay que apoyar a los CISO para que extiendan su función a tales entornos de una manera no disruptiva y comunicando, a los que en ellos trabajan, la necesidad de tener en cuenta la ciberseguridad, que para los mismos representa un nuevo factor, y posicionarla como uno de los pilares más importantes de la industria.
– **También son notables los importantes cambios normativos que se están produciendo, por ejemplo, en Europa, con la NIS2, la Ley de Resiliencia…**
– El hecho de que los responsables políticos identifiquen la ciberseguridad como una prioridad es algo positivo. La Comisión Europea, en particular, ha estado muy activa en los últimos años con la Ley de Ciberseguridad, la NIS2 y la próxima Ley de Resiliencia Cibernética (por nombrar solo algunas). Estamos interactuando de manera proactiva con los responsables de la formulación de políticas en todos los niveles para garantizar que las prioridades clave para nuestras industrias, especialmente cuando se trata de OT, se aborden adecuándose a esas leyes. En algunos casos, la Comisión también ha acudido directamente a nosotros en busca de asesoramiento sobre ciertos temas normativos, especialmente desde que iniciamos el Charter of Trust (CoT), en 2018. En colaboración con nuestros socios del CoT, podemos brindar una perspectiva industrial única sobre temas clave, como la seguridad de la cadena de suministro, la certificación o la educación en ciberseguridad.
– **¿Cuáles son las grandes ventajas de Siemens como *partner* de ciberseguridad de cualquier organización?**
– Nuestro valor es una gran experiencia en ciberseguridad, protegiendo a nuestra propia organización. Por ello, al ofrecer servicios lo hacemos con un *know-how* muy amplio que, a su vez, se extiende a muchas áreas. Nuestra historia protegiéndonos con éxito e, incluso nuestros retos, nos permiten evaluar mucho mejor el ecosistema de nuestros clientes de forma holística para ofrecerles una seguridad integral pensada y adaptada a su entorno.
– **¿Qué no se está contando de protección OT y ciberdefensa que, desde la experiencia de Siemens, tiene que ser la prioridad?**
– Uno de los mayores retos es priorizar la ciberseguridad en las industrias. Para muchos profesionales esto es un concepto muy nuevo y, a veces, lo ven lejano. Por lo tanto, la comunicación es un factor clave a la hora de extender la ciberdefensa a los entornos OT. Es importante explicar bien a sus responsables por qué, quién, cómo y cuándo vamos a hacer las cosas para generar un clima de confianza y colaboración con ellos y lograr que la ciberseguridad sea parte del ADN de la industria. ●

Pedro Martín

Gerente de Servicio del Centro de Ciberdefensa (CDC) de Siemens CYS

Le gusta destacar que en protección OT "cada día es distinto, por la variedad de entornos a los que te enfrentas". Ingeniero de Telecomunicaciones, Martín es actualmente uno de los grandes impulsores de las capacidades más proactivas de la compañía en ciberprotección, centrando sus esfuerzos, a través del CDC de Siemens CYS, en adelantarse a posibles amenazas. Algo de lo que se muestra especialmente orgulloso, ya que si "en algo destacamos es en nuestra fiabilidad: sólo se ofrece a los clientes lo que ya hemos probado nosotros en nuestras infraestructuras".

"La protección cibernética es determinante en todas las propuestas de Siemens en los entornos OT y también en las orientadas a la transformación digital IoT"

– ¿Cómo han evolucionado las ciberamenazas tras lo peor de la pandemia y, también, con la guerra de Ucrania, en entornos OT y TI?

– A raíz de la pandemia y la clara tendencia al teletrabajo, se ha observado un aumento en los ataques a los sistemas de acceso remoto a través de la explotación de vulnerabilidades, debilidades en las configuraciones y robos de credenciales a través de la ingeniería social. Prestamos mucha atención a la guerra de Ucrania, desde el inicio de las tensiones previas, antes del conflicto armado. Esto nos permitió poner foco en la 'securización' de las infraestructuras críticas y seguir de cerca a los actores de amenazas. Sí hay que poner en valor cómo la comunidad, en general, se ha unido compartiendo información, indicadores y análisis para neutralizar estas amenazas.

– Como Gerente de Servicio del CDC de Siemens CYS, ¿cuál es el principal error de los clientes en estos ámbitos?

– En cuanto a la ciberseguridad en los entornos OT, observamos tres grandes desafíos: por un lado, muchos de estos ámbitos no están concebidos inicialmente teniendo en cuenta la ciberseguridad. Por otro, existe una gran diversidad en los mismos, desde la gestión energética hasta la construcción de trenes, pasando por la gestión de residuos, lo que implica tener que amoldar las soluciones de ciberprotección a muchos casos distintos. Además, es fundamental adaptar la comunicación sobre ciberseguridad a los responsables de los entornos OT para hacernos entender sobre la importancia de la misma, ganarnos su confianza y entrar en sus dominios.

– ¿Qué capacidades diferenciales ofrecen a través de Siemens CYS y sus Centros de Ciberdefensa tanto en servicios, como en consultoría?

Nuestra gran capacidad diferencial a la hora de ofrecer estos servicios es que están testados, afinados y probados primero internamente. Es decir, no vendemos nada fuera que no estemos utilizando nosotros y sin que haya pasado los estándares de excelencia de nuestros clientes internos. Esto, unido a la gran variedad de entornos IT/OT que tenemos en Siemens, nos da un nivel de calidad muy alto y una gran cobertura.

– A través de iniciativas como Siemens Advanta o Xcelerator también se está reforzando la presencia de Siemens CYS en todo tipo de sectores que apuesten por la transformación digital. ¿Qué peso tiene la ciberseguridad en estas propuestas?

– La protección cibernética es determinante en todas las propuestas de Siemens, incluidas las orientadas a la transformación digital. No se percibe la ciberprotección como algo que hay añadir al final, ni como un agente externo al que llamar solamente en determinado momento de los desarrollos.

– El Centro de Ciberdefensa de Siemens es, sin duda, una gran apuesta. ¿Cuál es su capacidad más innovadora y eficaz ante los riesgos críticos en entornos industriales?

– Nuestro fuerte es el conocimiento interno y el 'expertise' con el que ya contamos dada nuestra experiencia al llevar ya tiempo trabajando con nuestras factorías, así

como el apoyo del resto de nuestros compañeros del área de CYS, lo que nos hace tener una visión muy completa del entorno OT desde el punto de vista de la ciberseguridad.

– ¿Con cuántos clientes cuentan ahora en España, públicos y privados, y en qué sectores espera ganar mercado a medio y largo plazo?

– Estamos centrados en estos momentos en nuestros clientes internos (empresas de Siemens, tanto Siemens Energy como Siemens Healthineers, al igual que nuestras grandes unidades de negocio, como Smart Infrastructures, Digital Industries y Siemens Mobility). Por tanto, estamos presentes en sectores muy variados como son el de las comunicaciones, salud, movilidad, automotriz, energético, de desarrollo software, etc.

– ¿Cuál es el servicio o capacidad más demandado y por qué, y en cuál esperan crecer más durante este próximo año?

– Estamos creciendo en el área de monitorización y respuesta de OT y la previsión es continuar con este crecimiento en un futuro próximo. Pero todos los sectores relacionados con OT, definitivamente, tienen una alta demanda por las razones comentadas, como la necesidad de una mayor preparación, la amenaza creciente y una gran diversidad.

– ¿Qué es lo más complejo de proteger en OT y qué ofrece Siemens CYS?

– Es importante no descuidar dos aspectos claves: el primero es que tenemos que ser capaces de comunicar de manera eficiente e inteligible la necesidad de soluciones de ciberseguridad a interlocutores en el mundo OT que no conocen y no están acostumbrados a lidiar con este tipo de problemas. El segundo es que lo que sirve para una factoría/sector puede no funcionar para otro por el gran nivel de diversidad de digitalización y de tecnologías OT en el sector industrial.

– El enfoque *Zero Trust* está cobrando un gran protagonismo tras apostar por él EE.UU. para sus agencias federales. ¿Qué peso tiene en la propuesta de Siemens?

– Estamos trabajando activamente con nuestros compañeros dentro de CYS encargados del despliegue del enfoque *Zero Trust* en las factorías para asegurarnos de que las soluciones de monitorización y respuesta que ofrecemos son compatibles con el mismo.

– Uno de los grandes valores de Siemens en ciberseguridad reside en el análisis, inteligencia de amenazas y *threat hunting*…

“Nuestro valor diferencial a la hora de ofrecer servicios es que están testados, afinados y probados primero internamente. Es decir, no vendemos nada fuera que no estemos utilizando nosotros y sin que haya pasado los estándares de excelencia de nuestros clientes internos”.

– Sí, contamos con un gran equipo distribuido en distintos *hubs* alrededor del mundo, principalmente en ciudades de Europa, Estados Unidos y México, así como con un sistema de monitorización global construido y mantenido por Siemens.

– También, está el problema de cómo atraer talento en un mercado que es escaso. ¿Cuál es la fórmula de Siemens CYS para conseguirlo?

– Nuestra propuesta es ofrecer un entorno en el que los técnicos estén cómodos y sientan que pueden aportar y crecer dentro de la compañía. Hacemos un gran esfuerzo en el *onboarding* de los nuevos contratados para que se sientan arropados por todos sus compañeros y eso hace que tengamos una rotación muy baja. Al ser equipos distribuidos, procuramos que no todas las reuniones sean virtuales y hacemos un esfuerzo en juntarnos físicamente siempre que es posible para compartir experiencias más allá del trabajo diario.

– Su oferta de ciberseguridad aúna tecnología propia y acuerdos con terceros. ¿Qué peso tiene el área de I+D de la compañía en la conformación de esta oferta y cuál es su política de alianzas con fabricantes y MSSPs?

– Tenemos acuerdos con varios fabricantes globales, tanto de soluciones EDR como de distintas plataformas tecnológicas que usamos como parte de nuestro sistema de monitorización global. Colaboramos activamente con el área de I+D para ir evolucionando nuestra respuesta de manera adaptativa a las amenazas cambiantes para nosotros y nuestros clientes. ●

“Estamos creciendo en el área de monitorización y respuesta de OT y la previsión es continuar con tal crecimiento en un futuro próximo. Todos los sectores de actividad relacionados con los entornos industriales, definitivamente, tienen una alta demanda por la falta de preparación en ciberprotección, la amenaza creciente y su gran diversidad”.

Objetivo: convertirse en el socio idóneo a la hora de proteger las infraestructuras industriales

Servicios de ciberseguridad: la construcción de una línea de detección y defensa en profundidad

Desde hace más de tres décadas, Siemens viene aprovechando los avances en seguridad OT de sus propias plantas y filiales para obtener un valioso conocimiento que comparte con clientes y socios, a través de productos y servicios destinados a construir una línea de detección y defensa en profundidad. La compañía ha desarrollado así un potente portafolio de ciberprotección de ciclo completo cuyo principal valor diferencial reside en adaptarse a la casuística específica de cada infraestructura y cliente.

La ciberseguridad se ha convertido en una de las áreas prioritarias de Siemens, consciente de los problemas que se derivan de la cada vez mayor convergencia entre IT y OT y de la digitalización de estos entornos. Por ello, la compañía se ha conformado como un socio tecnológico que comprende cómo los productos, los sistemas y las soluciones tecnológicas se integran con los procesos y las personas.

La multinacional dispone en la actualidad de una gama de servicios de protección gestionada que presta con tecnologías propias y acuerdos con terceros, fruto de su profundo conocimiento de las instalaciones industriales, su experiencia en gobernanza, riesgo y cumplimiento y el desarrollo de soluciones que la compañía también utiliza para protegerse. Entre ellas, destacan: **SiESTA** (Siemens Extensible Security Testing Appliance), un inventario de activos en tiempo real y generación de topología de red; **OSA**, (OT Cybersecurity Appliance) para la monitorización y detección de amenazas; y **Vilocify**, que alerta en tiempo real sobre vulnerabilidades, tanto en el software como en el hardware, de la infraestructura OT. Asimismo, las facilita a su Equipo de Respuesta a Emergencias Informáticas (CERT) para que actúe en consecuencia.

Con todo ello, la compañía ha sabido construir una oferta que se adapta a las necesidades del cliente, ya que cada fábrica se enfrenta a unos retos concretos debido, entre otros aspectos, a su grado de madurez y a la complejidad de los sistemas heredados con los que cuenta que, en no pocas ocasiones, son muy específicos.

Protección testada

La compañía destaca asimismo por su **servicio para proteger sus fábricas y filiales** a través de las capacidades de detección, análisis y respuesta que ofrece su Centro de Ciberdefensa (CDC) y el de Detección de Anomalías y Monitorización de la Seguridad OT (CDC-OT), que aprovechan los datos ofrecidos por la plataforma de detección, Argos, y que, además, son complementados con sus capacidades de inteligencia y caza de amenazas.

Así, esta propuesta se plasma en cuatro módulos: (1) Evaluación del grado de madurez IT/ OT de la fábrica y determinación del alcance del servicio; (2) Supervisión de la seguridad de OT 24x7; (3) Análisis de seguridad OT; y, (4) Alojamiento y gestión de infraestructuras e ingeniería de detección, incluyendo tanto el despliegue de servicios de hardware y software como la operación remota de la solución.

Además, se ofrece en tres modalidades: Essential, Enhanced y Customized, para adaptarlo a las necesidades de cada ámbito. El primer nivel de cobertura está pensado para entornos industriales con un nivel de complejidad y de madurez OT medio y bajo, con pocos dispositivos ICS y una red sencilla. Enhanced está diseñado para entornos de mayor complejidad y madurez, en los que, además de la tecnología incorporada en el nivel Essential, se añaden soluciones de monitorización y detección de amenazas específicas de protocolos OT. En el corazón de esta cobertura están las tecnologías OSA y Claroty. El nivel Customized, por su parte, "está diseñado para entornos críticos y en él se hace un análisis profundo para poder construir *parsers* de *logs*, reglas de detección e informes adaptados al mismo para conseguir aumentar al máximo el grado de detección y respuesta a incidentes", resaltan desde la compañía.

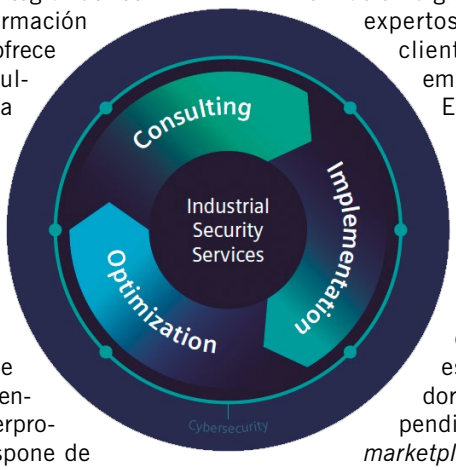
Propuesta a terceros

En el portafolio de Siemens también destacan **los servicios de ciberprotección que forman parte de los proyectos de transformación digital segura**, que la compañía

La multinacional dispone de un catálogo de servicios de protección gestionada que presta con tecnologías propias y acuerdos con terceros, fruto de su conocimiento de las instalaciones industriales y en el desarrollo de soluciones que la compañía también utiliza para protegerse

ofrece para todo tipo de industrias, sobre todo en áreas como edificios y redes inteligentes, sanidad y transporte. En este sentido, la multinacional aprovecha sus avances para compartirlos con clientes y socios poniendo a disposición de terceros soluciones como SiESTA, OSA y Vilocify, además de ofrecer sus servicios de evaluación de la seguridad de los activos OT, para identificar riesgos, amenazas y vulnerabilidades incluyendo, si es necesario, consejos sobre las contramedidas inmediatas que hay que adoptar para evitar interrupciones de la producción. También dispone de servicios de protección y consultoría, con evaluaciones para garantizar el cumplimiento normativo y el establecimiento de conceptos de protección para mitigar los riesgos cibernéticos.

Cabe recordar, además, que la ciberseguridad es una parte integral de los proyectos de transformación que esta compañía ofrece a través de su consultora Advanta, con la que Siemens desarrollará servicios de digitalización para clientes industriales externos.



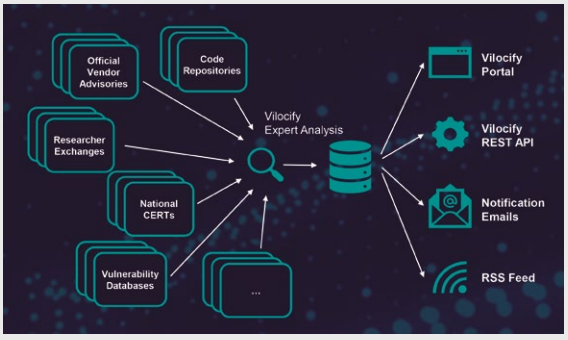
IoT seguro

A ello se suma, que como parte de su intensivo esfuerzo en ciberprotección, también dispone de la plataforma de negocios digital abierta **Siemens Xcelerator**, presentada en junio, para ayudar a acelerar la transformación digital, segura, a socios, expertos, desarrolladores y clientes de todo tipo de empresas y sectores.

En ella, la empresa incluye desde una cartera seleccionada de hardware y software habilitado para IoT, hasta un poderoso ecosistema de socios certificados, hiperescaladores, proveedores de software independientes e, incluso, un *marketplace* en evolución que permite explorar, educar, intercambiar y comprar todo tipo de soluciones y capacidades. ●

Vilocify: la importancia de contar con capacidades de última generación para identificar vulnerabilidades en los productos e infraestructuras más críticos

"En Siemens, el cuidado de los clientes y la garantía de su protección es prioritario para todo el equipo de ciberseguridad, y con el desarrollo de sistemas inteligentes y de mitigación de vulnerabilidades en entornos IT y OT, convertimos la ciberseguridad en una pieza fundamental de nuestro catálogo de servicios", destacan desde la compañía. Asimismo, recuerdan que cada vez es más crítico para las empresas contar con capacidades para identificar amenazas y puntos débiles, en tiempo real. Y no es sencillo. Los sistemas ciberfísicos (CPS) presentan vulnerabilidades únicas debido a su naturaleza que conecta los mundos digital y físico. Y esto es preocupante teniendo en cuenta que se calcula que, de media, las organizaciones tardan entre 100 y 120 días en corregir o mitigar las vulnerabilidades debido a su incapacidad de escanear, identificar y parchearlas de forma rápida y eficaz. Para ayudarlas a hacer frente a este reto, Siemens ha desarrollado un sistema, Vilocify, para "asegurar la protección de las infraestructuras inteligentes de sus clientes y garantizar el conocimiento de las vulnerabilidades".



Es evidente que las empresas que sean capaces de identificar las vulnerabilidades y detectar amenazas con anticipación contarán con mayores ventajas, no solo competitivas, sino funcionales, también a largo plazo, para garantizar su supervivencia y superación frente a ataques cibernéticos, un aspecto en el que Siemens se considera un referente, al tener el rol de constructor de sistemas propios completos, a lo que se suma la experiencia en la gestión de sus propias plantas e infraestructura IT/OT. Estos dos aspectos están completamente integrados en la cartera de servicios de la organización y, por supuesto, en uno de los más innovadores y exitosos, como es Vilocify.

Fiabilidad y rapidez de detección

El valor de esta solución/servicio estriba en su fiabilidad en la detección de vulnerabilidades y amenazas que afectan al software y hardware de las infraestructuras, así como en el envío de alertas en tiempo real para que la supervisión sea efectiva y permita una rápida solución. Para ello, el equipo de Vilocify supervisa miles de fuentes de información de seguridad, así como webs de empresas de software, de fabricantes de hardware y, también, repositorios de código *open source.* También, ofrece una implementación rápida y optimizada de parches y mitigaciones individualizadas.

Por ello, sus impulsores destacan que este servicio es hasta un 76% más rápido en monitorización de emisión de información y alertas que los habituales motores de búsqueda, contando ya con 20 años de prestación de servicios entre cientos de usuarios que confían en él para el seguimiento de los sistemas de seguridad implementados en sus infraestructuras críticas y estratégicas.

Así, reduciendo la complejidad de monitorizar las vulnerabilidades publicadas cotidianamente, contando con una *single source of truth* de calidad, los clientes de Vilocify pueden enfocar sus recursos críticos en mantener al día el inventario IT/OT de su empresa y acelerar las medidas de reducción de riesgo frente a ciberataques.

Ventaja competitiva y resiliencia

"El desarrollo de Vilocify es un ejemplo de colaboración para proporcionar una gran ventaja a nuestros clientes en el conocimiento inmediato de las vulnerabilidades, sobre todo en entornos OT", destaca la Global Head of Cybersecurity Defense de Siemens, **Karen Gaines**, a la vez que recuerda la intención de la compañía de "replicar este modelo de productos y servicios altamente escalables y de uso sencillo para abarcar otras áreas de actividad de nuestros clientes". Por ello, Vilocify es compatible con todo tipo de componentes de terceros, y permite planificar con antelación el ciclo de vida de cualquier elemento para proceder a su reemplazo antes de que se convierta en un riesgo para la seguridad de las infraestructuras.

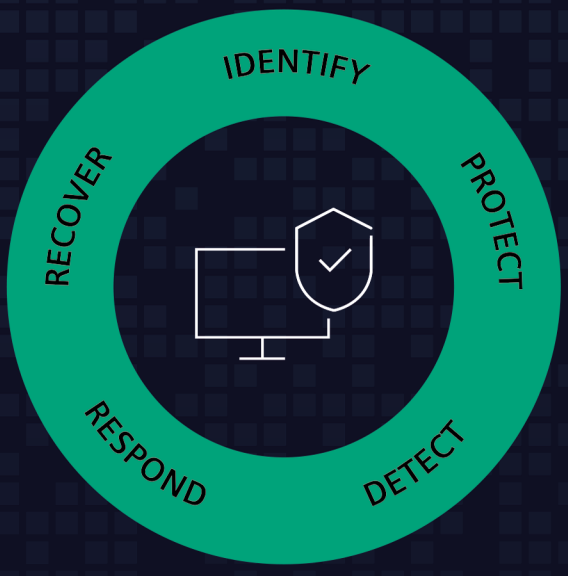
SIEMENS

We addressed the **OT cybersecurity** challenge in 3 steps

Holistic ownership for cybersecurity

Ensure the people & budget to make it real, together

Central services & continuous improvement



Cybersecurity

www.siemens.com