CISCO
SECURE

Reporte de la encuesta de seguridad

Las organizaciones industriales aún carecen de visibilidad y preparación para defenderse contra los ataques cibernéticos de TO/ICS

cisco SECURE

Contenido

Resumen ejecutivo

¿Están las organizaciones industriales preparadas para defender sus entornos de tecnología operativa (TO) y el sistema de control industrial (ICS) en caso de un ataque cibernético?

Eso es lo que Cisco se propuso responder en una encuesta que llevó a cabo en el tercer trimestre de 2022 junto con Gartner Peer Insights y Takepoint Research en la que participaron 100 profesionales de TI, TO, ingeniería e infoSec de todo el mundo.

Lo que descubrimos fue sorprendente: el 77 % de las organizaciones industriales aún se encuentra dando los primeros pasos en su recorrido hacia la seguridad de TO. Y ninguno de los encuestados tiene aún que proteger completamente sus entornos de TO/ICS.

Esto es preocupante, teniendo en cuenta las características del mundo posterior a la pandemia en el que nos encontramos hoy.

Se han producido muchos cambios en los últimos tres años. En la pandemia se ha acelerado significativamente la transformación digital de la TO, lo que ha llevado a la mayoría, si no todas, las operaciones críticas de una organización a integrarse con las tecnologías digitales. A su vez, los ataques cibernéticos, como los sufridos por el gasoducto Colonial y JBS en 2021, se han vuelto más frecuentes porque los agentes maliciosos se centran en las vulnerabilidades de las redes de TO/ICS.

A puertas cerradas, la presión se está acumulando en la sala de juntas y las inquietudes sobre la continuidad del negocio y las directivas de seguridad, como Shields Up de CISA, sin duda contribuyen en gran medida. En las conversaciones que tuvimos con ejecutivos de alto nivel quedó claro que la mayoría de las organizaciones reconocen que no están preparadas para un ataque cibernético y que muchas recién están comenzando a priorizar la seguridad de TO.

De cara al futuro, vemos que la tormenta de seguridad de TO perfecta se dirige hacia nosotros. Se espera que en la mayoría de las organizaciones industriales las funciones de seguridad converjan en los entornos de TI y TO durante los próximos tres años, lo que ampliará considerablemente sus superficies de ataque. Y los ataques en entornos de TO/ICS continuarán intensificándose hasta el punto de que se dañarán o perderán vidas, probablemente dentro de la década.

Las organizaciones industriales deben acelerar sus esfuerzos de seguridad de TO ahora para salvaguardar la continuidad del negocio.

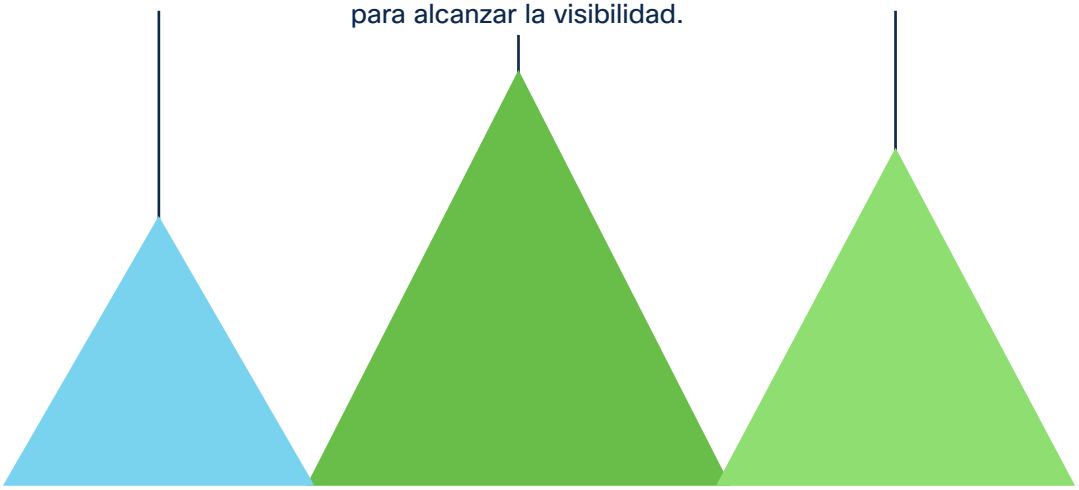
Descubrimientos clave

En nuestra encuesta se puso de manifiesto que la visibilidad integral de los dispositivos de TO y las redes industriales es el objetivo principal y el desafío para proteger las operaciones industriales. Si bien esto no es una sorpresa, teniendo en cuenta la etapa en la que se encuentran la mayoría de las organizaciones en sus procesos de ciberseguridad, es interesante observar sus enfoques y desafíos para lograr este objetivo.

El 58 %
de los encuestados afirma que alcanzar la visibilidad es su principal objetivo a la hora de proteger las operaciones industriales.

El 74 %
de los encuestados afirma que el costo y la complejidad de crear una red de SPAN fuera de banda o implementar los TAP de red son los principales obstáculos para alcanzar la visibilidad.

El 65 %
de los encuestados tiene la intención de obtener el inventario de activos de los equipos de ingeniería de TO para alcanzar la visibilidad.



¿Por qué la visibilidad es la base de la seguridad industrial?

Para comprender lo que se necesita para proteger los entornos de TO/ICS en un entorno digital en constante cambio, solo hay que observar la evolución de la seguridad de TI en los últimos 20 años.

Antes, los esfuerzos de seguridad se centraban en el perímetro y los sistemas sensibles estaban aislados. La visibilidad de la red interna no se consideraba importante porque se suponía que cualquier persona con acceso era un agente legítimo. Todo eso cambió con la suplantación de identidad (phishing) y los ataques de día cero.

Con los enfoques de Zero Trust y defensa en profundidad, el objetivo ahora es mantener la visibilidad total y la segmentación de la red para limitar los efectos de una intrusión. Vemos esto en la proliferación de sistemas de detección y respuesta de red (NDR) y centros de operaciones de seguridad (SOC) disponibles las 24 horas.

La prevención sigue siendo una parte importante de la seguridad, pero también lo son la contención y la corrección rápidas.

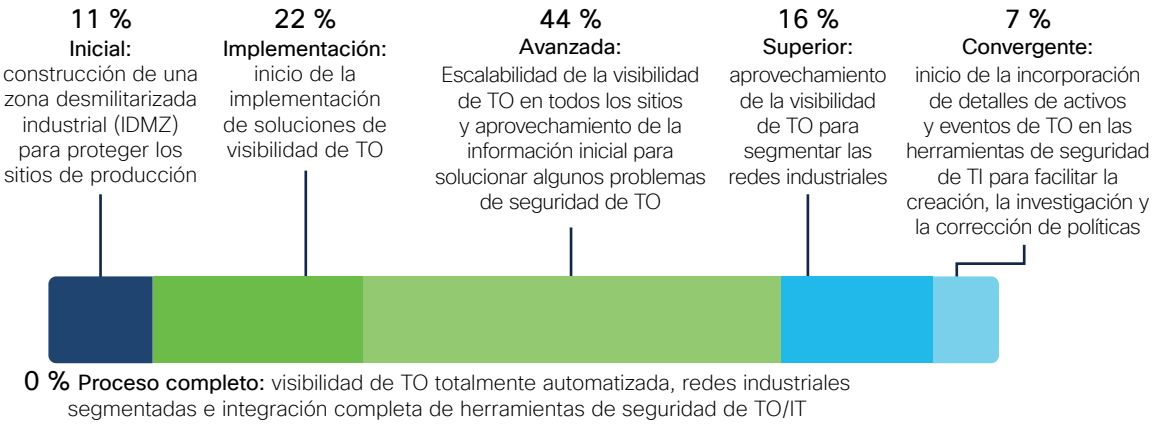
Cuando se trata de proteger sus entornos de TO/ICS, muchas organizaciones han seguido el mismo libro de tácticas: desconectar la red y aislar los sistemas críticos, pero, como hemos visto, esto no funcionará por mucho tiempo.

Las organizaciones sencillamente tienen que establecer una visibilidad completa de sus redes de TI y TO antes de que se puedan tomar medidas correctivas o preventivas.

Estado actual y objetivos

La mayoría de las organizaciones recién están comenzando su recorrido por la seguridad de TO

¿En qué etapa del proceso de seguridad de la tecnología operativa (TO) se encuentra en este momento?



Si bien ninguna organización encuestada tiene aún que alcanzar la madurez completa de la seguridad de TO, la buena noticia es que en los datos se refleja un nivel de autoconocimiento y urgencia para mejorar la situación.

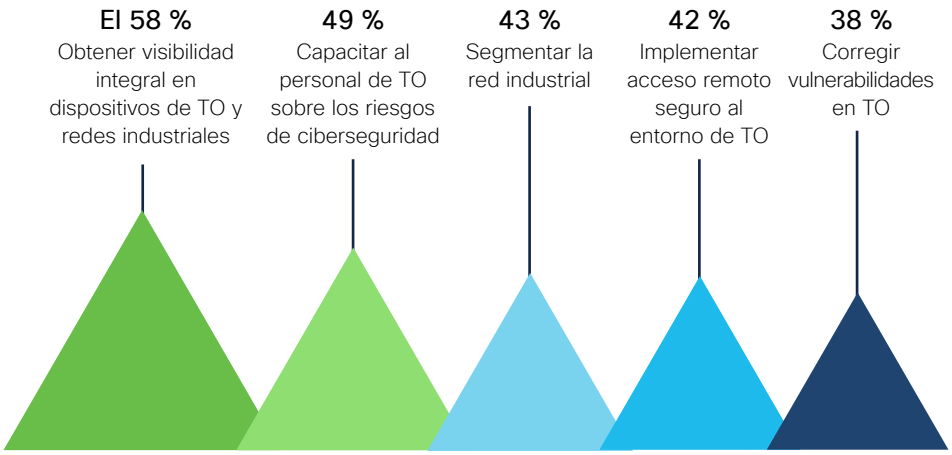
El 11 % de los encuestados ha comenzado su recorrido con zonas desmilitarizadas industriales (IDMZ) para proteger los sitios de producción, el 22 % ha comenzado a implementar soluciones de visibilidad de TO y el 44 % está ampliando la visibilidad de TO en todos los sitios y aprovechando la información inicial para solucionar algunos problemas de seguridad de TO.

Sin embargo, solo el 23 % de los encuestados ha ampliado sus implementaciones de visibilidad de TO. Un porcentaje aún menor está implementando estas herramientas en una estrategia de seguridad avanzada: el 16 % ha segmentado sus redes industriales y solo el 7 % ha comenzado a introducir detalles de activos y eventos de TO en la seguridad de TI herramientas para facilitar la creación, la investigación y la corrección de políticas.

En general, descubrimos que los líderes de seguridad ven los beneficios de las soluciones de visibilidad de TO y las consideran una tecnología madura para implementar a escala.

La visibilidad, la capacitación y la segmentación son prioridades

¿Cuáles son sus principales objetivos para proteger sus operaciones industriales durante los próximos 12 a 24 meses?



Presentar libros de tácticas de respuesta y corrección de TO/TI **27 %**,
Integrar alertas de TO en el centro de operaciones de seguridad (SOC) **25 %**,
Implementar la detección de intrusiones (IDS) en la red industrial **21 %**,
Crear equipos funcionales entre dominios (TO/TI) **6 %**, Otros **0 %**

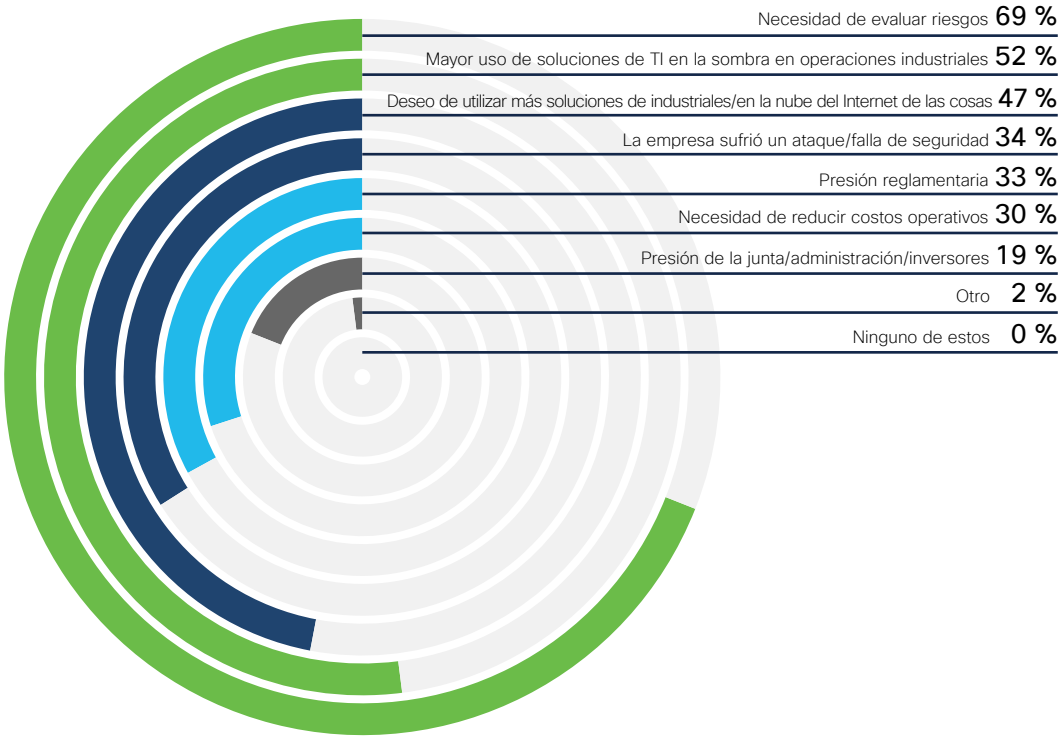
En cuanto a los objetivos, el 58 % de los encuestados afirma que tiene la intención de obtener una visibilidad integral de su red industrial en un plazo de 24 meses y el 49 % indicó que está priorizando la capacitación en ciberseguridad, mientras que el 43 % apunta a segmentar su red industrial.

En cuanto a la segmentación, vale la pena señalar que, aunque los entornos de TO están más conectados con el tiempo, no están optimizados para la seguridad. Las IDMZ, los firewalls y los gateways unidireccionales son medidas de seguridad de gran alcance que pueden proteger el perímetro, pero no protegen el entorno de TO de cualquier persona que ingrese.

Muchas redes de TO aún son planas y no están segmentadas, por lo tanto no es raro que las organizaciones no tengan una contabilidad completa de toda la red.

La gestión de riesgos y la TI en la sombra están impulsando la necesidad de visibilidad

¿Cuáles son los factores principales que impulsan la necesidad de visibilidad de red industrial y ciberseguridad en su organización?



Es interesante observar que los dos principales impulsores de la visibilidad de la red son la necesidad de evaluar los riesgos (69 %) y el mayor uso de soluciones de TI en la sombra en las operaciones industriales (52 %).

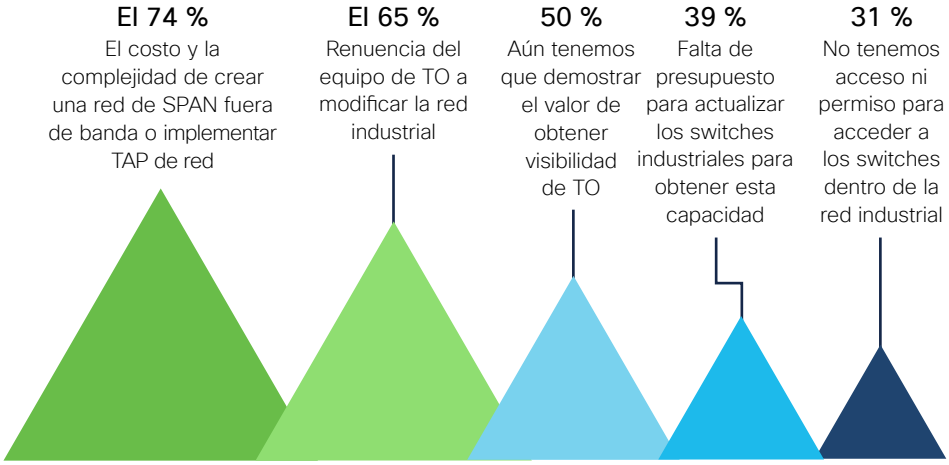
Esto refleja el hecho de que los problemas de seguridad de TO suelen ser mucho más graves de lo que las organizaciones creen y que, anecdóticamente, los líderes de seguridad saben que sus organizaciones son vulnerables. Por ejemplo, no es raro encontrar varios puertos abiertos o sistemas operativos implementados con credenciales predeterminadas o OEM que evalúan máquinas sin supervisión.

Estas vulnerabilidades pueden exponerse y abordarse solo con una visibilidad integral de los activos conectados y las actividades de la red.

Desafíos

Las soluciones convencionales son costosas y complejas

¿Cuáles considera que son los principales obstáculos para obtener una visibilidad integral en dispositivos de TO y redes industriales?



Ninguno de estos **2 %**, Otro **1 %**

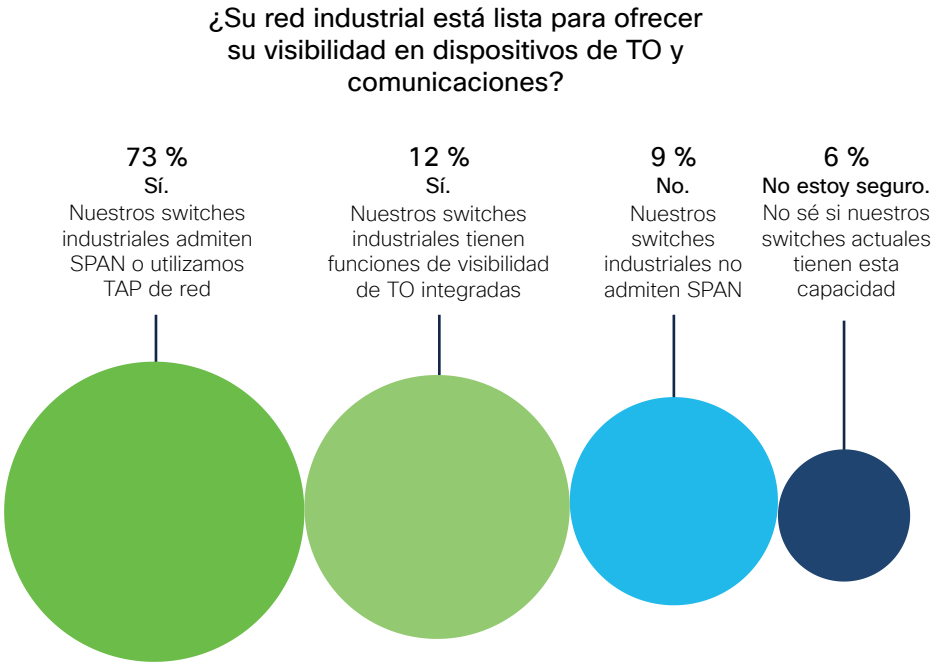
El 74 % de los encuestados afirma que el costo y la complejidad de crear una red de analizador de puertos conmutados (SPAN) para capturar y monitorear el tráfico de red industrial es el principal obstáculo para la visibilidad. No es de extrañar, teniendo en cuenta que esto implicaría la creación de una red duplicada, que simplemente no es escalable.

El 65 % afirma que los equipos de TO son reticentes a modificar la red. Una vez más, esto no es de extrañar si se tiene en cuenta la prioridad de TO de mantener las luces encendidas. Junto a esto, el 50 % dice que demostrar el valor de obtener visibilidad de TO es un desafío.

Además, el 39 % de los encuestados afirma que carece del presupuesto para actualizar los switches industriales, lo que respalda aún más el hecho de que el costo es la principal restricción. Finalmente, el 31 % afirma que no tiene permiso para acceder a los switches dentro de la red industrial.

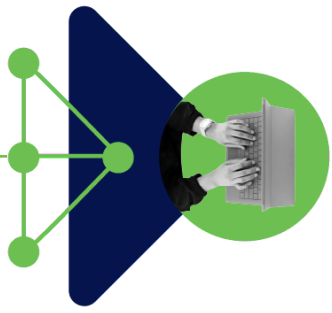
En nuestra experiencia, solo cuando la TI genere confianza con TO y pueda demostrar el valor que tiene la visibilidad para mejorar la confiabilidad operativa, la empresa aumentará sus inversiones en actualizaciones de red. Hasta entonces, la TI debe solucionar estas restricciones.

La escalabilidad sigue siendo un desafío

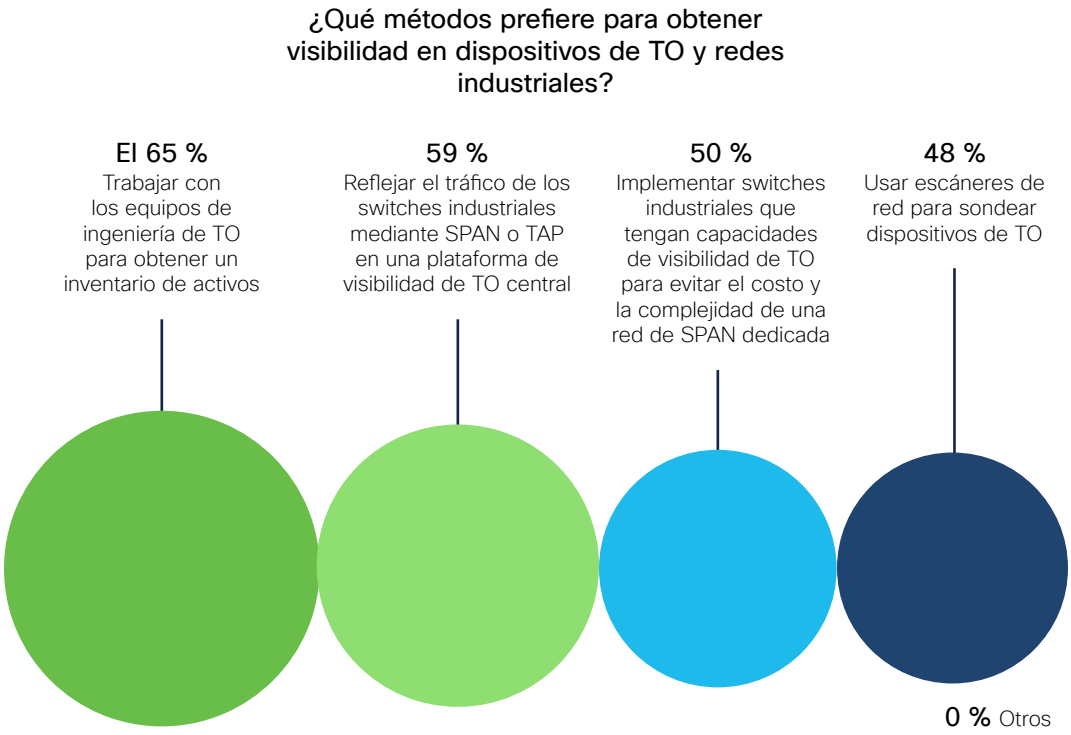


Cuando se les preguntó sobre la preparación de su red para proporcionar visibilidad, el 73 % de los encuestados afirmó que sus switches estaban preparados para SPAN o puntos de acceso de tráfico (TAP). Esto podría explicar la fijación en SPAN o TAP de red como solución de monitoreo, aunque el 74 % de los encuestados afirma que una implementación de este tipo sería demasiado costosa y compleja.

También es revelador que la mayoría de los encuestados no conozcan otros métodos más rentables para monitorear el tráfico de red, como el uso de switches industriales con capacidades integradas de detección de activos e inspección profunda de paquetes (DPI). Solo el 12 % afirma que sus switches industriales tienen funciones de visibilidad de TO integradas.



Las organizaciones deben repensar la visibilidad y la escalabilidad en TO



El 65 % de los encuestados afirma que trabajaría con la ingeniería de TO para obtener un inventario, pero este método no es confiable porque los inventarios de ingeniería generalmente son incompletos y no se actualizan en tiempo real. El problema principal es que dichos inventarios no ofrecen visibilidad de las actividades de comunicación reales y los dispositivos dudosos que se conectan a la red. Tampoco ayuda a detectar amenazas ni a abordar el problema de la TI en la sombra.

El 59 % prefiere duplicar el tráfico con un SPAN o TAP, probablemente debido sus logros iniciales o porque no conocen otras alternativas. Esto será problemático a escala a medida que se sumen los costos y la complejidad.

El 50 % afirma que usaría switches industriales con capacidades de visibilidad de TO. De las tres opciones, esta solución tiene mucho que ofrecer. No requiere la creación de una red de recopilación de datos separada ni ninguna modificación de la red de TO. Esta solución aborda los dos principales desafíos que se analizaron anteriormente.

El 48 % afirma que usaría escáneres de red. Pero esta opción, como obtener un inventario de la ingeniería de TO, no ofrece visibilidad en tiempo real de los activos ni de las comunicaciones. Además, aunque los escáneres de red se utilizan ampliamente para detectar dispositivos de TI en redes empresariales, son inapropiados en redes industriales. La mayoría de los dispositivos de TO son antiguos y agotarán rápidamente sus recursos limitados de CPU y memoria. Es probable que los análisis de red los supriman e interrumpan la producción. Las soluciones de visibilidad de TO capaces de consultar recursos a través de tecnologías semánticas podrían ser una alternativa viable.

Este desafío con los escáneres de red es un buen ejemplo de por qué las organizaciones deben mirar más allá de las mejores prácticas de TI estándar para encontrar soluciones, especialmente cuando se trata de desafíos de TO.

Dentro de banda frente a fuera de banda: ¿cuál es mejor para su organización?

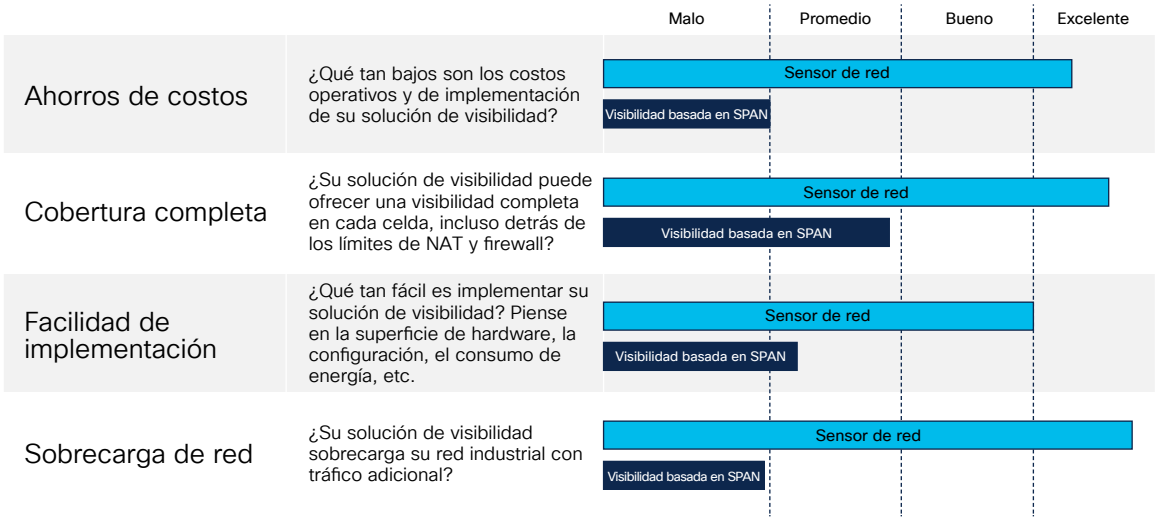
Comparemos las dos formas más comunes de establecer la visibilidad: la creación de una red de SPAN (fuera de banda) o la actualización de equipos de red existentes (dentro de banda) a dispositivos con capacidades de DPI.

En una solución basada en SPAN, el tráfico de red se recopila de los switches industriales y se envía para su análisis a un dispositivo de seguridad dedicado a través de una red fuera de banda. Una solución alternativa es utilizar equipos de red que incorporen funciones de visibilidad, como DPI pasivo y detección dinámico de activos.

Estos elementos de red extraerán información significativa y enviarán solo metadatos livianos a una plataforma de seguridad de TO central para su posterior análisis. Como estos metadatos generalmente representan del 3 % al 5 % del tráfico original, se pueden transmitir dentro de banda sin la necesidad de agregar recursos de red adicionales al entorno industrial.

Las organizaciones deben tener en cuenta los siguientes factores al momento de elegir una solución:

- **Costo:** las soluciones dentro de banda son relativamente económicas porque no requieren el empleo de hardware ni de redes adicionales. Las soluciones fuera de banda requieren el abastecimiento, la instalación y el mantenimiento de dispositivos exclusivos, así como una red completamente nueva, incluidos switches y cableado.
- **Escalabilidad**: las soluciones dentro de banda aprovechan los recursos de red existentes y pueden implementarse rápidamente. Las soluciones fuera de banda requieren mucho tiempo y esfuerzo para desarrollar una red independiente.
- **Visibilidad**: las soluciones fuera de banda tienen un costo, lo que obliga a la mayoría de las organizaciones a monitorear el tráfico solo desde los switches de agregación. Esto limita su visibilidad en el tráfico de norte a sur y restringe su capacidad para detectar activos que se encuentran detrás de firewalls industriales o límites de traducción de direcciones de red (NAT). Con una solución dentro de banda, la visibilidad está integrada en cada switch implementado en el entorno.
- **Complejidad**: las soluciones dentro de banda no requieren que se replantee la topología de la red, solo una configuración adicional. Una red SPAN se hace más compleja cuanto más grande se vuelve.
- **Impacto del ancho de banda:** las soluciones dentro de banda envían metadatos livianos. Las soluciones fuera de banda duplican el tráfico y generalmente requieren la construcción de una red independiente para evitar que se congestionen los bucles de control y que haya fluctuaciones en la red industrial.



Para obtener más detalles sobre cómo obtener visibilidad mediante el uso de una arquitectura dentro o fuera de banda, consulte este informe técnico.

Conclusión

La vulnerabilidad de los entornos de TO/ICS en la actualidad no puede subestimarse. Las organizaciones industriales deben acelerar sus esfuerzos para intensificar la seguridad de TO.

Aunque la mayoría de las organizaciones recién están dando los primeros pasos de su recorrido de seguridad de TO, es alentador verlas encaminarse en la dirección correcta. Tienen un enfoque bastante maduro de la seguridad y comprenden la importancia de la visibilidad para permitir medidas preventivas y correctivas.

Por supuesto, la visibilidad es solo una parte de la solución, pero es el paso fundamental sobre el que se construye todo lo demás. Cualquier solución viable también debe poder segmentar las redes y escalar a varios sitios de manera rentable.

Lo más importante es que las organizaciones deben mirar más allá de las mejores prácticas de TI estándar para encontrar la mejor solución y mejorar la colaboración entre TI, TO y SecOps.

Cisco Industrial Threat Defense aprovecha su red industrial como sensor y ejecutor para ayudarlo a obtener visibilidad a escala y adoptar un enfoque paso a paso para implementar una estrategia integral de seguridad de TO. Para obtener más información, visite cisco.com/go/iotsecurity.

Metodología

Los hallazgos de este reporte surgieron de una encuesta que se llevó a cabo en la industria durante el tercer trimestre de 2022. Esta encuesta, diseñada por TP Research y realizada por Gartner Peer Insights, contó con la participación de 100 profesionales de TI, TO, ingeniería e InfoSec.

Los encuestados provienen de una amplia gama de geografías, sectores y organizaciones:

- El 84 % de los encuestados reside en América del Norte y el 16 % en Europa, Medio Oriente y África (EMEA).
- El 74 % de los encuestados tiene el nivel de director o superior; el 26 % son gerentes.
- El 50 % de los encuestados proviene de empresas con más de 10 000 empleados; el 17 % proviene de organizaciones con 5000 a 10 000 empleados; el 33 % proviene de organizaciones con al menos 1000 empleados.

C11-3411110-00 02/23