INFORME

Informe del estado de la tecnología operativa y ciberseguridad de 2023

FORTINET

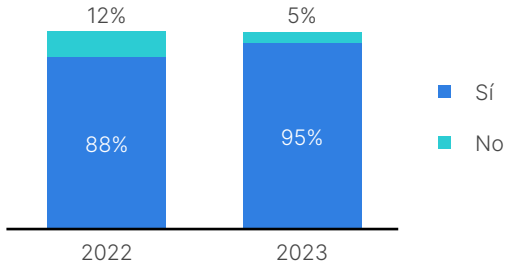
Contenido

Puntos clave

Personas

En casi todas las organizaciones encuestadas, los CISO son ahora o pronto serán responsables de la ciberseguridad de OT.
También cabe destacar que ahora más profesionales de ciberseguridad de OT provienen del liderazgo de seguridad de TI en lugar del equipo de operaciones.

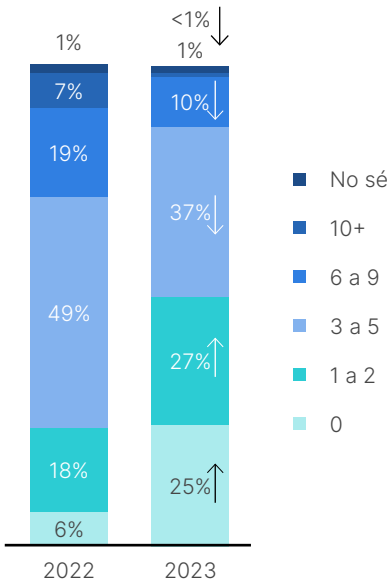
La ciberseguridad estará bajo el CISO en los próximos 12 meses



Incidentes de ciberseguridad

Si bien la cantidad de organizaciones que no sufrieron una intrusión de ciberseguridad mejoró drásticamente año con año (del 6% en 2022 al **25% en 2023**), todavía hay un importante margen de mejora. De hecho, tres cuartas partes de las organizaciones de OT reportaron al menos una intrusión en el último año y casi un tercio de los encuestados reportó haber sido víctima de un ataque de ransomware (**32%**, sin cambios desde 2022). Aumentaron las intrusiones de malware y phishing **12%** y **9%**, respectivamente.

Número de intrusiones en el último año

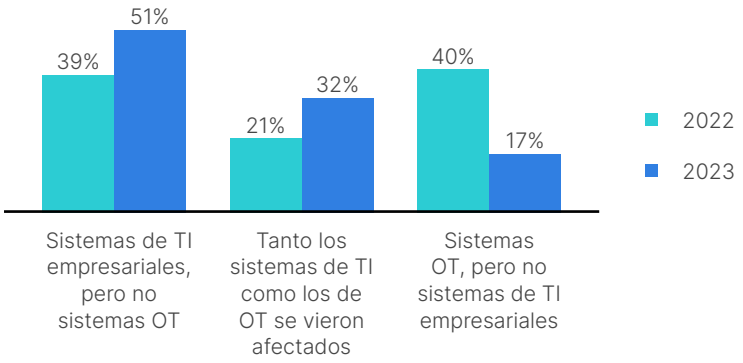


# Por madurez en ciberseguridad	Nivel 0–2	Nivel 3	Nivel 4
No sé	1%	0%	0%
10+	1%	2%	0%
6 a 9	11%	11%	6%
3 a 5	38%	35%	40%
1 a 2	36%[B]	21%	25%
0	14%	31%[A]	29%[A]

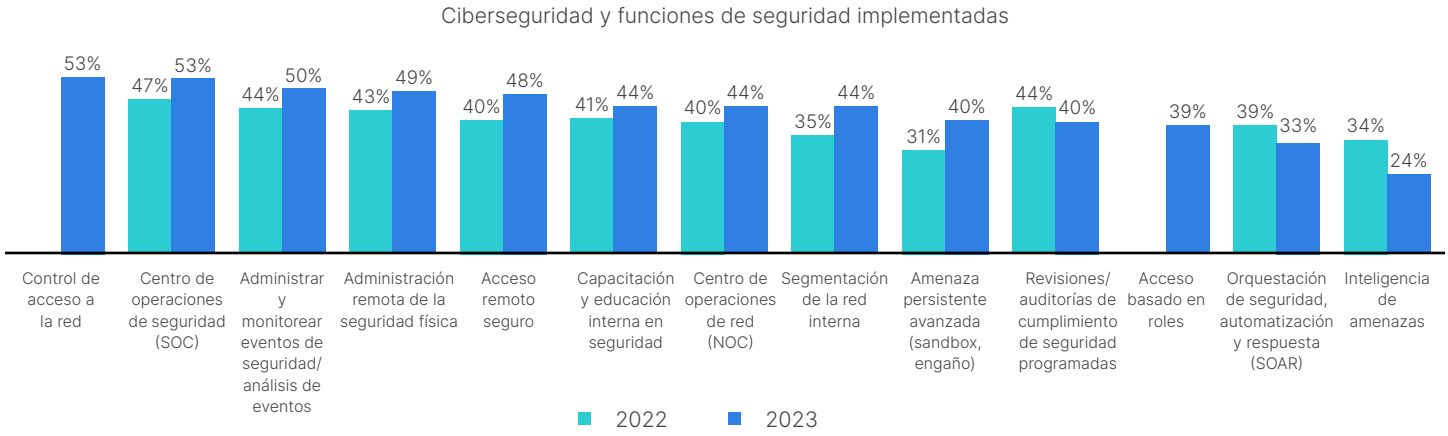
El impacto de las intrusiones

A principios de este año ocurrió un ciberataque y casi un tercio **(32%)** de los encuestados indicó que tanto los sistemas de TI como los de OT se vieron afectados, en comparación con solo el 21% el año pasado. Para combatir las intrusiones, los profesionales de OT están incrementando las soluciones de ciberseguridad en sus redes industriales.

Entornos afectados

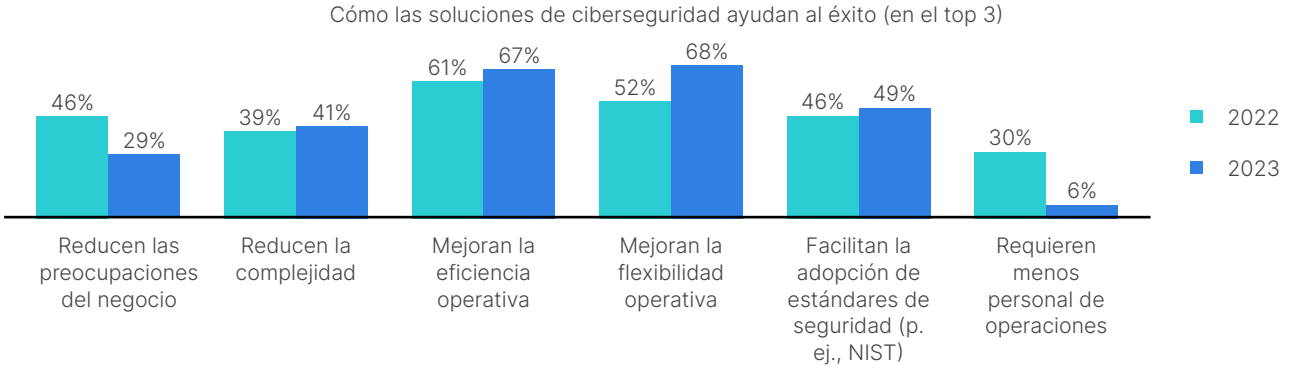


Las amenazas persistentes avanzadas, la segmentación de la red interna y el acceso remoto seguro es lo que más han aumentado, mientras que la inteligencia de amenazas ha disminuido como solución.



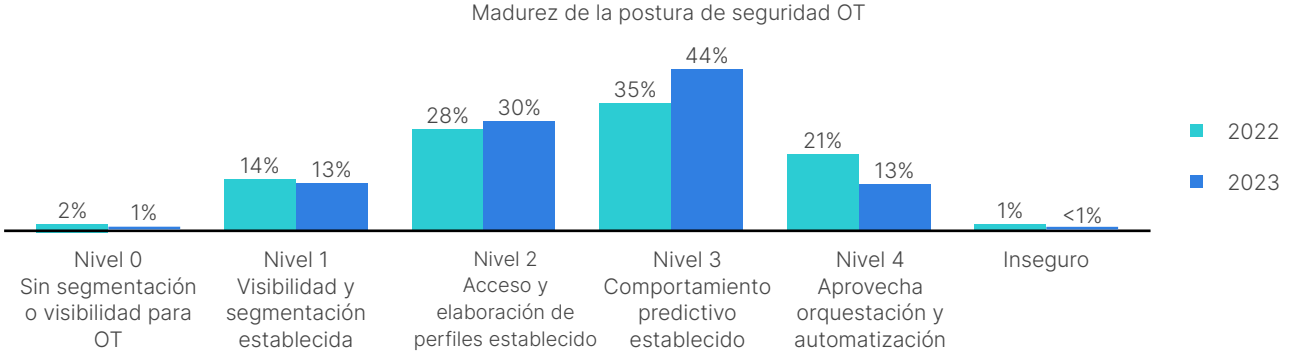
Cómo ayuda la ciberseguridad

Si bien los resultados de la encuesta revelan que las soluciones de ciberseguridad continúan contribuyendo al éxito de la mayoría de **(76%)** de los profesionales de OT, particularmente mejorando la eficiencia **(67%)** y flexibilidad **(68%)**, los datos también muestran que la expansión de la solución hace que sea más difícil proteger de manera consistente su panorama convergente de TI/OT.

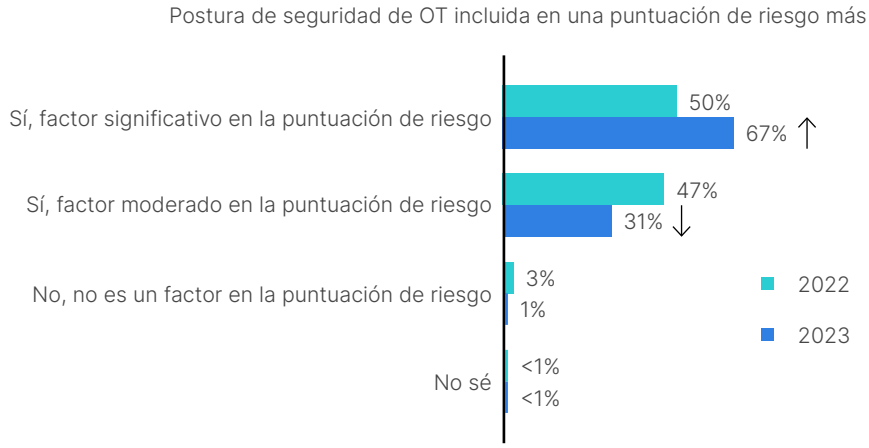


Postura de ciberseguridad

Si bien menos personas caracterizan la postura de ciberseguridad OT de sus empresas como Nivel 4 ("altamente maduro") este año en comparación con 2022 (bajó a **13% de 21%**), **44%** de todas las organizaciones ahora se califica a sí misma en el Nivel 3, frente al 35% del año pasado. Esto puede reflejar un enfoque maduro para evaluar la funcionalidad, lo que da como resultado una visión más realista del estado de su postura.



Casi todas las organizaciones (98%) ahora incluyen su postura de ciberseguridad OT en la puntuación de riesgo más amplia, compartida con el liderazgo ejecutivo y las juntas directivas.

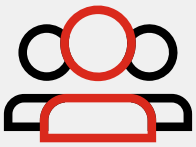


Resumen ejecutivo

El Informe de Fortinet sobre el estado de la tecnología operativa y la ciberseguridad 2023 es nuestro quinto estudio anual basado en datos de una encuesta mundial exhaustiva de 570 profesionales de OT realizada por una respetada empresa externa de investigación .

La protección de los sistemas OT ahora es más crítica que nunca, ya que más organizaciones conectan sus entornos OT a Internet. Si bien la convergencia de TI/OT tiene muchos beneficios, se ve obstaculizada e incapacitada por ciberamenazas avanzadas y destructivas. El efecto indirecto de estos ataques se dirige cada vez más a los entornos de OT. Por estas razones, los datos de la encuesta de este año indican que la ciberseguridad de OT es ahora más central y crucial en la cartera de riesgos de una organización.

Un análisis de los datos de 2023 revela que actualmente hay cuatro tendencias globales destacadas:



El informe de 2023 revela que el 95% de las organizaciones han hecho que sus CISO sean responsables de la ciberseguridad de OT.

- Ha habido una disminución general de las intrusiones debido a menos infracciones internas, aunque el ransomware y el phishing siguen siendo amenazas importantes. Sin embargo, en lugar de una disminución del riesgo cibernético, esto puede deberse a que los ciberdelincuentes adoptan un enfoque más específico.
- Casi todas las organizaciones han puesto la responsabilidad de la ciberseguridad de OT bajo un director de seguridad de la información (CISO) en lugar de un equipo o ejecutivo de operaciones.
- Las organizaciones y los profesionales de OT confían en una amplia gama de soluciones de ciberseguridad para combatir las intrusiones. Hay indicios de que los productos puntuales y la expansión de soluciones pueden hacer que sea más difícil aplicar políticas y hacerlas cumplir de manera consistente en todo el panorama convergente de TI/OT.
- El número de encuestados que consideran que la madurez de ciberseguridad de su organización está en el Nivel 4 cayó del 21% hace un año al 13% en la actualidad, mientras que aquellos que consideran que su ciberseguridad está en el Nivel 3 aumentó del 35% al 44%. Este cambio de datos parece indicar que los profesionales de OT ahora tienen una autoevaluación más realista de las funciones de ciberseguridad de OT de su organización.

Después de cinco años de aplicar encuestas a los profesionales de OT, la noticia más alentadora es que la ciberseguridad ahora parece estar finalmente fuera de las sombras. La ciberseguridad de la tecnología operativa ahora tiene la atención completa y frecuente del liderazgo empresarial y de los directivos de alto nivel (C-suite). Sin embargo, la mayoría de las organizaciones aún tiene mucho trabajo por hacer y, con respecto a la ciberseguridad, no hay tiempo para “dormirse en sus laureles”.

Para ayudar que su organización mejore su postura de seguridad OT, el Informe sobre el estado de la tecnología operativa y la ciberseguridad de este año concluye con una lista de mejores prácticas que usan organizaciones de primer nivel para mantener seguros sus sistemas OT.

Introducción

Hoy nadie puede dudar de la importancia de proteger los sistemas OT. La tecnología operativa controla las infraestructuras críticas de las que todos dependemos, desde la gestión de la red eléctrica hasta la operación de los sistemas de agua y alcantarillado, el funcionamiento de las redes de transporte, la fabricación de bienes esenciales y la habilitación de cadenas de suministro globales. Y para que nadie lo olvide, OT también es un componente clave de los esfuerzos de la aceleración digital de muchas organizaciones industriales.

Las condiciones del mercado actual han hecho que la adopción de metodologías y tecnologías de la Industria 4.0 sea una "era de conectividad, análisis avanzado, automatización y tecnología de manufactura avanzada"[1] esencial para que los fabricantes y otras industrias sigan siendo competitivas.

Amenazas de ciberseguridad para OT

La convergencia de las redes de TI y OT no ha sucedido sin llamar la atención de los ciberdelincuentes y los estados-nación agresivos. Los informes recientes sobre el panorama global de amenazas de FortiGuard Labs señalan una mayor detección de malware y actividad maliciosa en los sistemas OT.[2]

Varios ataques de ciberseguridad de alto perfil destacan este desafío y actúan como llamadas de atención para todos los responsables de proteger los sistemas OT. Un buen ejemplo es la continua agresión de Rusia contra la infraestructura crítica de Ucrania,[3] que se convirtió en una “guerra abierta” física hace más de un año.[4] Pero estos ataques no se limitan a la agresión abierta entre estados-nación. Los sistemas de tecnología operativa en todo el mundo siguen siendo el objetivo de los ciberdelincuentes, especialmente en la manufactura, que sigue experimentando muchos ataques de ransomware dirigidos contra sus sistemas OT.[5]

Desafortunadamente, el porcentaje de organizaciones en la encuesta de este año que experimentó una intrusión de ransomware (32%) es el mismo que el del grupo del año pasado (también 32%). Hay que avanzar en la defensa contra este tipo de ataques. Dada la evolución y sofisticación creciente de las operaciones de ransomware, no es sorprendente que el 84% de las organizaciones representadas en la encuesta del Informe global sobre ransomware 2023 de Fortinet sigan "muy" o "extremadamente" preocupadas por esta amenaza.[6]

Aunque las infracciones internas intencionales y no intencionales han disminuido considerablemente este año, según los encuestados, las intrusiones de malware y phishing aumentaron significativamente, 12% y 9%, respectivamente. Los resultados de esta encuesta están respaldados por el Informe de amenazas globales de FortiGuard Labs más reciente, que afirma que "El malware tiene una forma de dominar los titulares y mantener a las empresas en alerta".[7]

Ya no están aisladas

Ahora que las infraestructuras de TI y OT se han integrado casi universalmente, el aislamiento o *“air gap”* que anteriormente mantenía los sistemas OT casi invulnerables a los ataques cibernéticos ha desaparecido. En consecuencia, las superficies de ataque de las organizaciones industriales se han expandido enormemente. Sumado a esto, el aumento en la implementación de dispositivos del Internet de las Cosas Industrial (IIoT, por sus siglas en inglés), junto con la nueva vulnerabilidad del OT al panorama de amenazas de TI y el alto valor de atacar los entornos de producción, que aumenta la motivación de las organizaciones para pagar un rescate. Es evidente por qué proteger el OT se ha vuelto vital.

Ciberseguridad OT en el punto de mira

El Informe sobre el estado de la tecnología operativa y la ciberseguridad del año pasado[8] indicó que el aumento en el enfoque y la inversión en ciberseguridad OT es un excelente desarrollo. Sin embargo, como se reveló en la encuesta de este año, muchas organizaciones aún tienen un largo camino por recorrer para proteger adecuadamente sus sistemas OT.

Profundicemos en los datos de la encuesta de este año y veamos qué podemos aprender sobre el estado actual de la ciberseguridad de OT. Con suerte, uno de los titulares de nuestro informe del próximo año será sobre el progreso significativo realizado para proteger los sistemas OT.

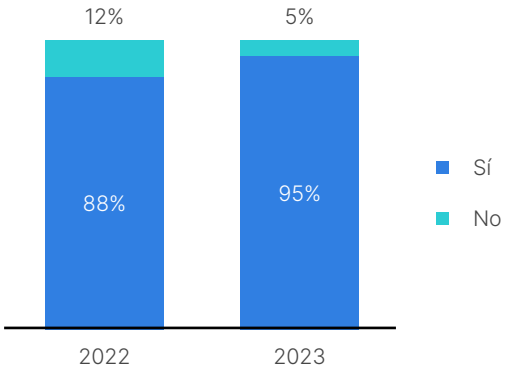
Visiones críticas

Visión crítica # 1: La responsabilidad de la ciberseguridad de OT está pasando del personal de OT a los expertos en ciberseguridad

Las personas que trabajan en OT se pueden encontrar en la mayoría de las principales industrias: manufactura, transporte, logística, atención médica, farmacéutica, petróleo, gas, energía, servicios públicos, química, agua, aguas residuales y otras. Tradicionalmente, estos profesionales de OT también han estado profundamente involucrados en las decisiones de compra de ciberseguridad para sus entornos de OT.

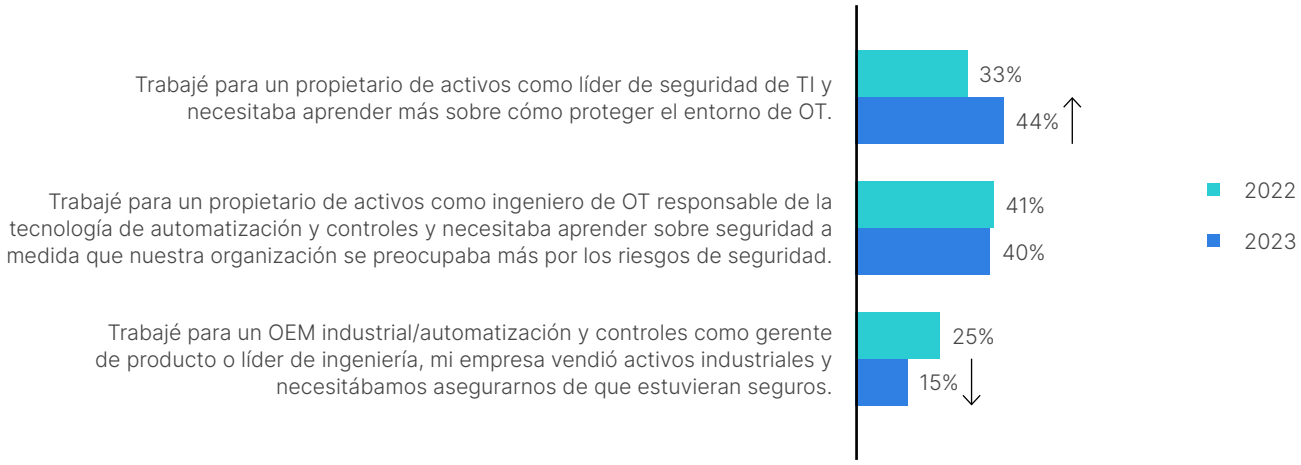
Sin embargo, parece que la continua vulnerabilidad de las redes OT a los ataques cibernéticos ha derivado en que las decisiones de ciberseguridad de OT pasen al CISO. Los datos también muestran que los profesionales de seguridad de OT vienen de las filas del equipo de TI en lugar de aquellos con experiencia laboral en administración de productos. Como resultado, y como indican los datos de la encuesta, los líderes de seguridad tradicionales y de la C-suite, especialmente el CISO/CSO, se están involucrando e invirtiendo más en la toma de decisiones de ciberseguridad.

P: ¿Su organización planea implementar ciberseguridad de OT a cargo del CISO en los próximos 12 meses?



La ciberseguridad estará bajo el CISO en los próximos 12 meses

P: ¿Qué antecedentes profesionales lo llevaron a la seguridad de OT?

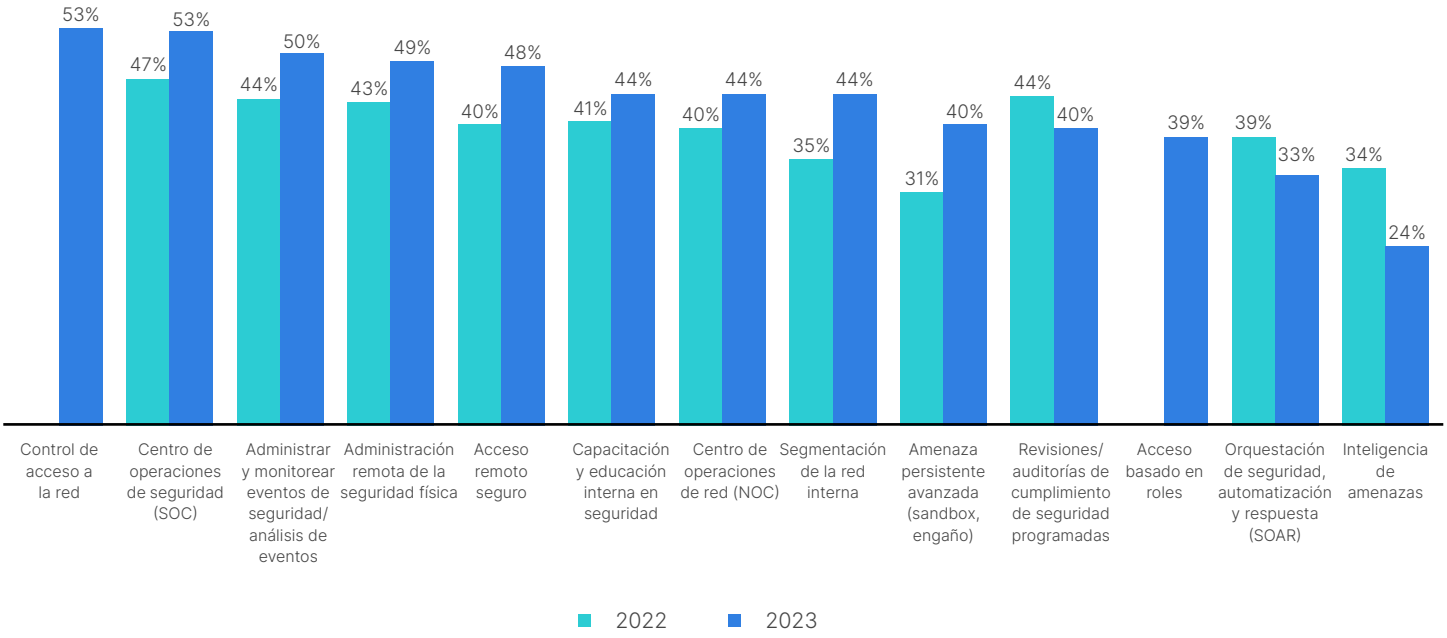


Antecedentes profesionales que llevaron a la seguridad de OT

Visión crítica # 2: Los profesionales de OT confían en una gama de soluciones

Los profesionales de OT encuestados este año buscan soluciones de ciberseguridad que, ante todo, detecten vulnerabilidades conocidas. Un desafío único al que se enfrentan los equipos de OT es que el tiempo de inactividad suele ser mucho más crítico que en los entornos de TI. Como resultado, el éxito en una red OT se mide menos por el mantenimiento de la confidencialidad e integridad de los datos y más por la disponibilidad de los sistemas críticos. Esto otorga una gran importancia al tiempo de respuesta a los ataques, como lo ilustra un aumento generalizado en la implementación de redes OT y soluciones de ciberseguridad.

Sin embargo, igual que con las redes de TI, el simple hecho de contar con soluciones no es suficiente para prevenir todos los ataques a las redes de OT. Parte del desafío puede estar relacionado con la expansión de soluciones y proveedores, lo que dificulta la detección de una amenaza y la prevención de una respuesta coordinada.



Ciberseguridad y funciones de seguridad implementadas

Visión crítica # 3: El número de intrusiones sigue siendo problemático

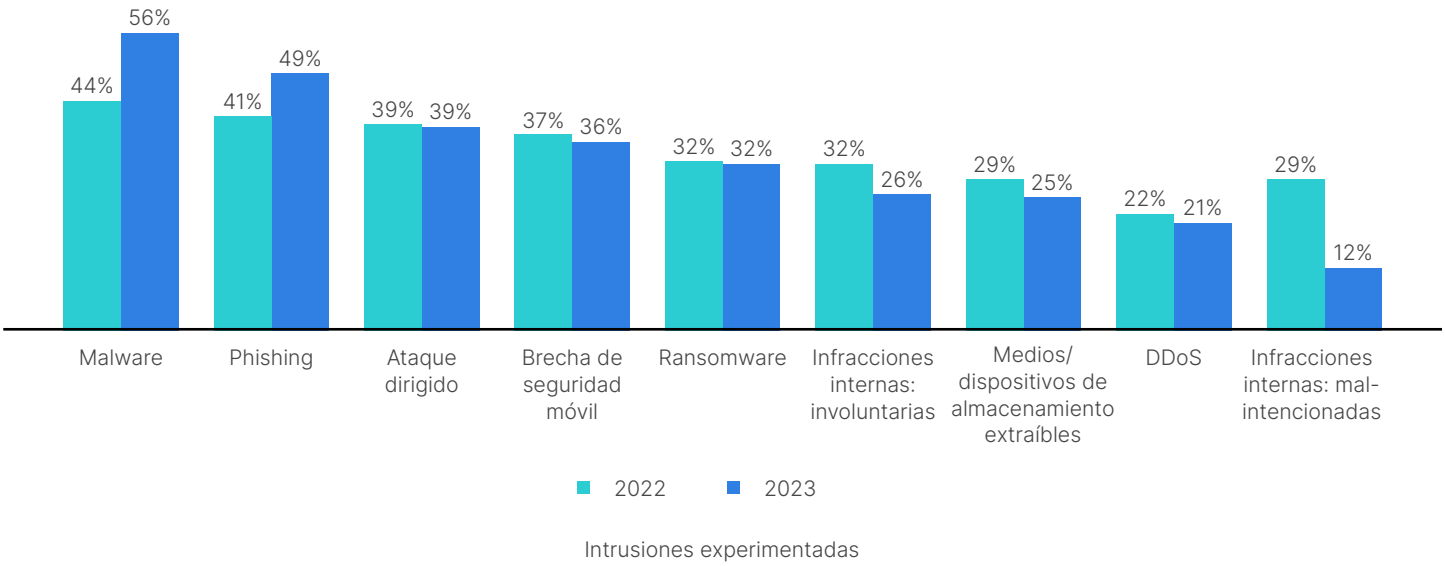
La cantidad de intrusiones experimentadas está disminuyendo, pero aún así el 75% de las organizaciones encuestadas informó haber experimentado al menos una intrusión en los últimos 12 meses. La disminución general se atribuye a menos infracciones internas, no a menos ataques de ciberdelincuentes.

Sin embargo, los incidentes de malware y phishing siguen siendo las amenazas más comunes y aumentaron desde el año pasado, pero el ransomware sigue siendo la mayor preocupación y los incidentes siguen creciendo. Los impactos fueron amplios y afectaron cada vez más a los sistemas de TI y OT, pero tendieron a resolverse en cuestión de horas (cada vez más en minutos).

Algunas de las disminuciones de intrusiones pueden deberse a un cambio en las tácticas de los ciberdelincuentes. Sin embargo, las iniciativas de los atacantes siguen siendo efectivas según los aumentos que hemos visto en el malware y el phishing. Aún así, dado el alto valor de los sistemas OT, podemos prever un cambio hacia ataques más específicos.

Es importante tener en cuenta que el exceso de confianza en la preparación perjudica a las organizaciones tanto como tener la tecnología incorrecta, que, según nuestro último informe de ransomware,[9] es otro problema al que se enfrenta la mayoría de las organizaciones. Aunque la defensa contra el ransomware, por ejemplo, es una alta prioridad para la mayoría de las organizaciones, muchas soluciones que identifican como clave para su estrategia de ciberseguridad brindan poca protección contra los ataques de ransomware.

P: ¿Qué tipo de intrusiones se experimentaron? (marque todo lo que corresponda)



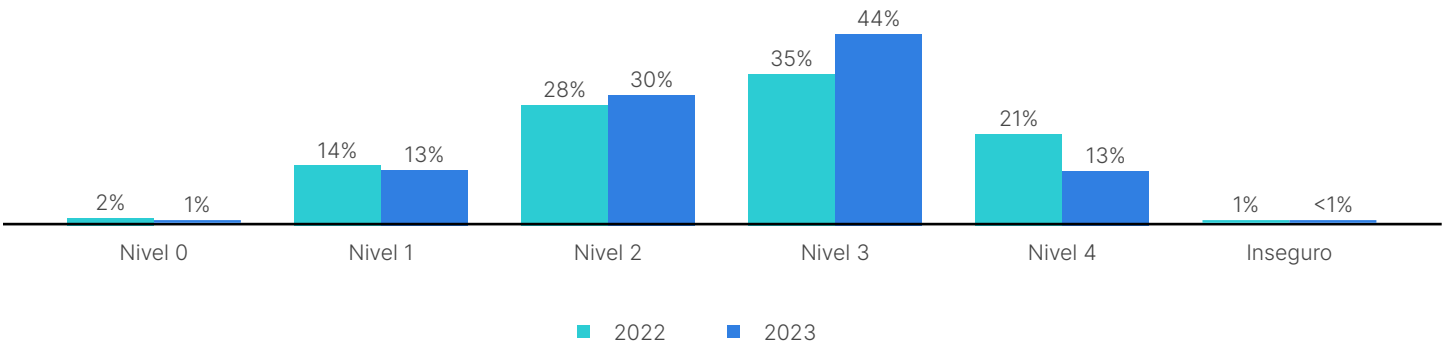
Intrusiones experimentadas

Visión crítica # 4: El nivel promedio de madurez de la ciberseguridad está mejorando

La autoevaluación precisa de la funcionalidad propia de la ciberseguridad y la madurez de la postura es un primer paso fundamental para mejorar las defensas cibernéticas y proteger adecuadamente los entornos de OT. A nivel mundial, menos empresas caracterizan su postura de seguridad OT como muy madura este año, con una disminución del 21% en 2022 al 13% este año. Al mismo tiempo, el 44% de las organizaciones ahora caracterizan la madurez de su postura de ciberseguridad de OT en el Nivel 3, frente al 35% hace un año. Estos datos indican que los encuestados de este año pueden tener una autoevaluación más realista de la funcionalidad de su ciberseguridad de OT.

La escala de madurez	
Nivel 0	Sin segmentación o visibilidad para OT
Nivel 1	Visibilidad y segmentación establecida
Nivel 2	Acceso y elaboración de perfiles establecidos
Nivel 3	Comportamiento predictivo establecido
Nivel 4	Aprovecha la orquestación y la automatización

P: ¿Cómo caracterizaría la madurez de su postura de seguridad de OT?

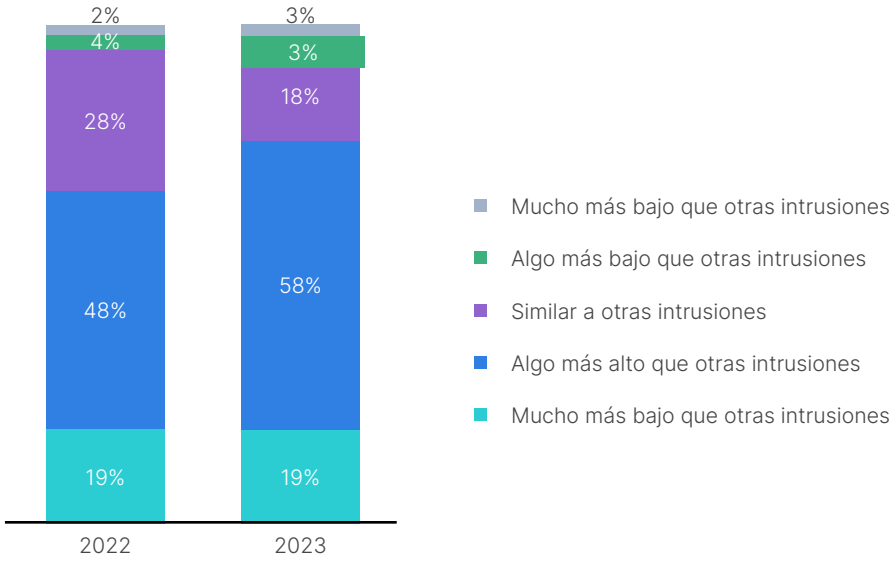


Madurez de la postura de seguridad OT

Un análisis exhaustivo de la encuesta 2023

P: En comparación con otras intrusiones, ¿qué tan preocupado está por el impacto del ransomware en su entorno OT?

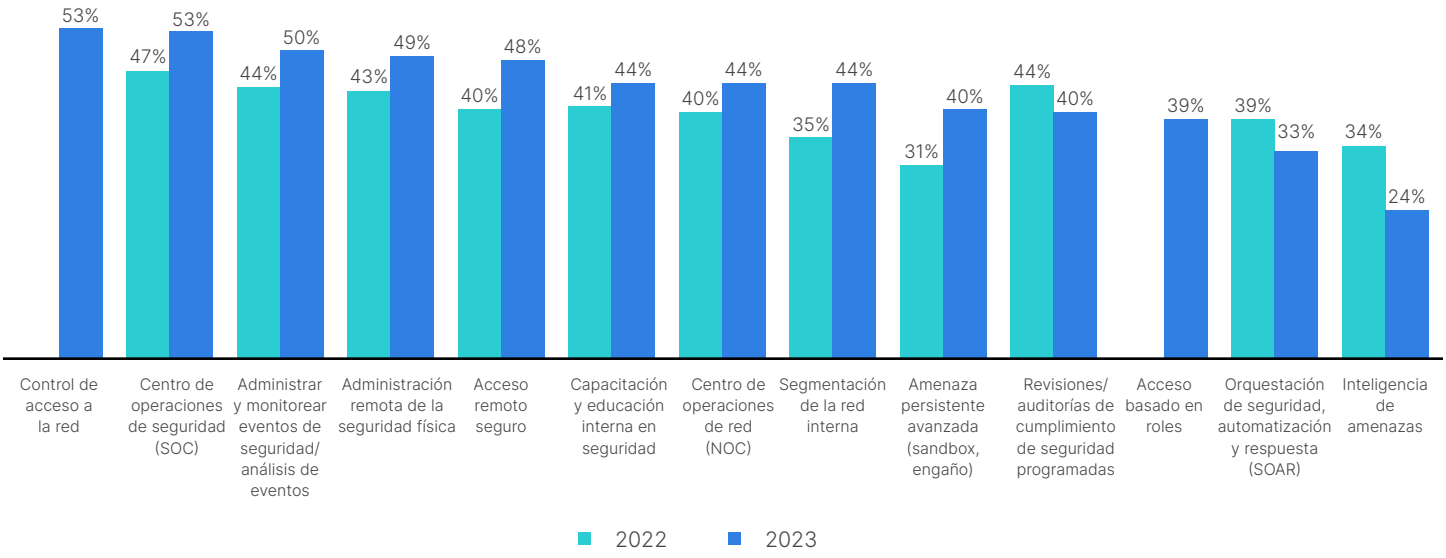
Los incidentes de ransomware que ocurren en la empresa o en la red de TI pueden afectar directa o indirectamente la producción. Las organizaciones están cada vez más preocupadas por esto que por otras intrusiones (a pesar de que el phishing y el malware son más comunes). Por lo tanto, el ransomware sigue siendo una de las principales preocupaciones debido a las implicaciones financieras y de producción.



Preocupación por el impacto del ransomware

P: ¿Qué características de ciberseguridad y seguridad tiene implementadas hoy?

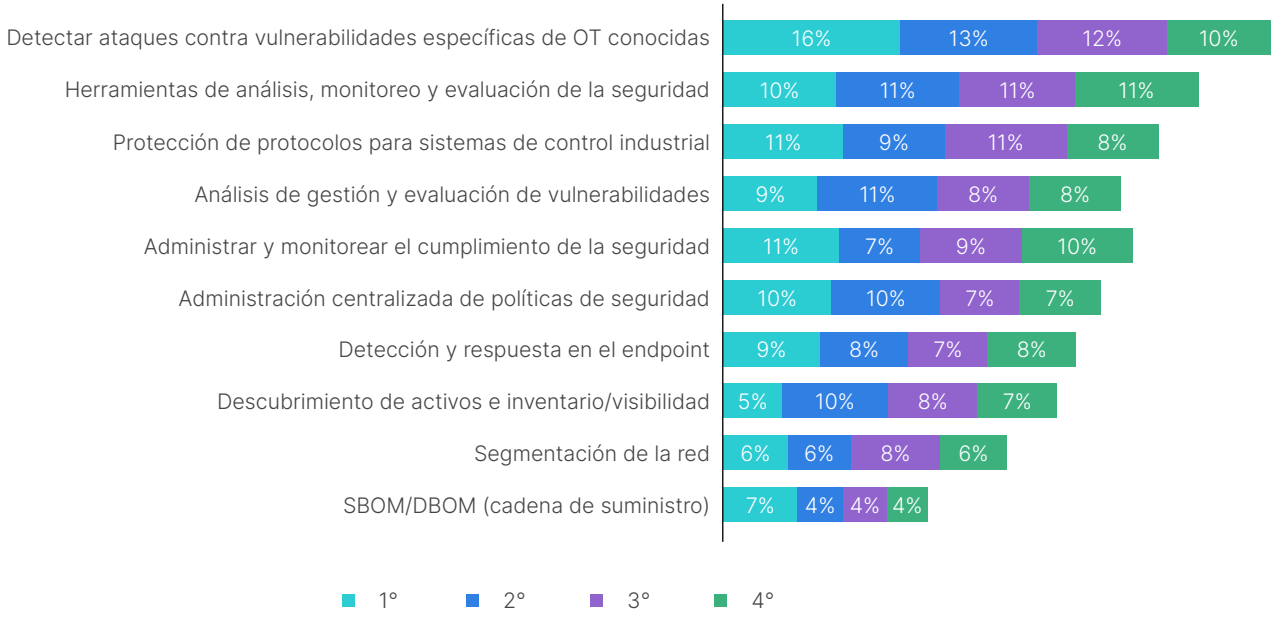
Para combatir las intrusiones, los profesionales de OT están fortaleciendo las muchas funciones defensivas y de ciberseguridad que tienen implementadas. Con el aumento de funciones, sospechamos que las auditorías de seguridad están en declive debido a la proliferación de estas funciones adicionales y las soluciones más avanzadas, como SOAR e inteligencia de amenazas. Una vez que estas nuevas funciones estén firmemente operativas, es probable que las auditorías aumenten a niveles preexistentes.



Ciberseguridad y funciones de seguridad implementadas

P: ¿Qué características son las más importantes en las soluciones de ciberseguridad de OT? (Califique hasta cuatro)

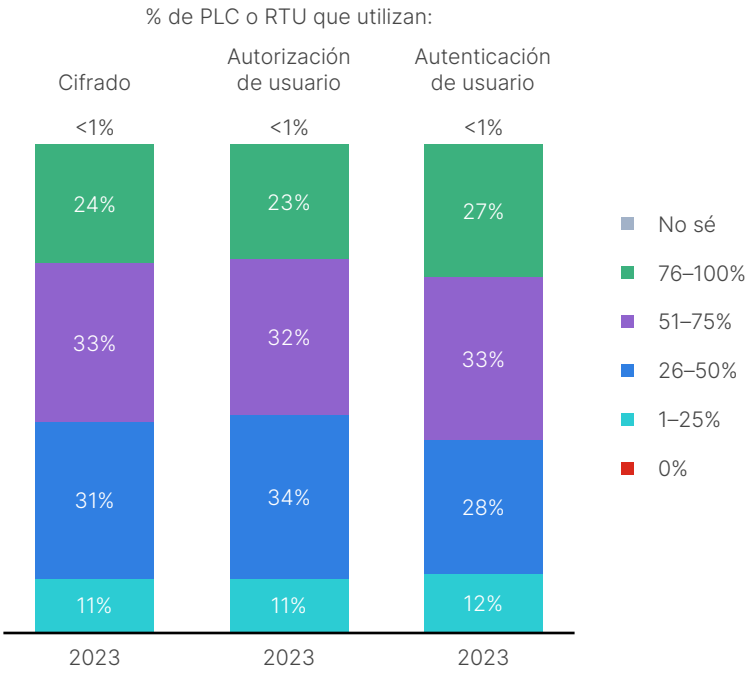
La detección de ataques contra vulnerabilidades conocidas es ahora la característica más esencial de la solución de ciberseguridad y su importancia aumentó durante el último año. Otra indicación de la creciente madurez en la seguridad de OT es la menor prioridad en el descubrimiento y la segmentación de activos. Lo que hemos visto en la industria y es consistente con la Guía Complementaria de Controles de Seguridad Críticos ICS de CIS,[10] es que la mayoría de los clientes han dado estos pasos básicos y están avanzando hacia soluciones fundamentales y organizacionales más avanzadas.



Funciones de soluciones de seguridad más importantes (clasificación)

P: ¿Qué porcentaje de sus PLC o RTU utilizan cada una de las siguientes funciones de seguridad?

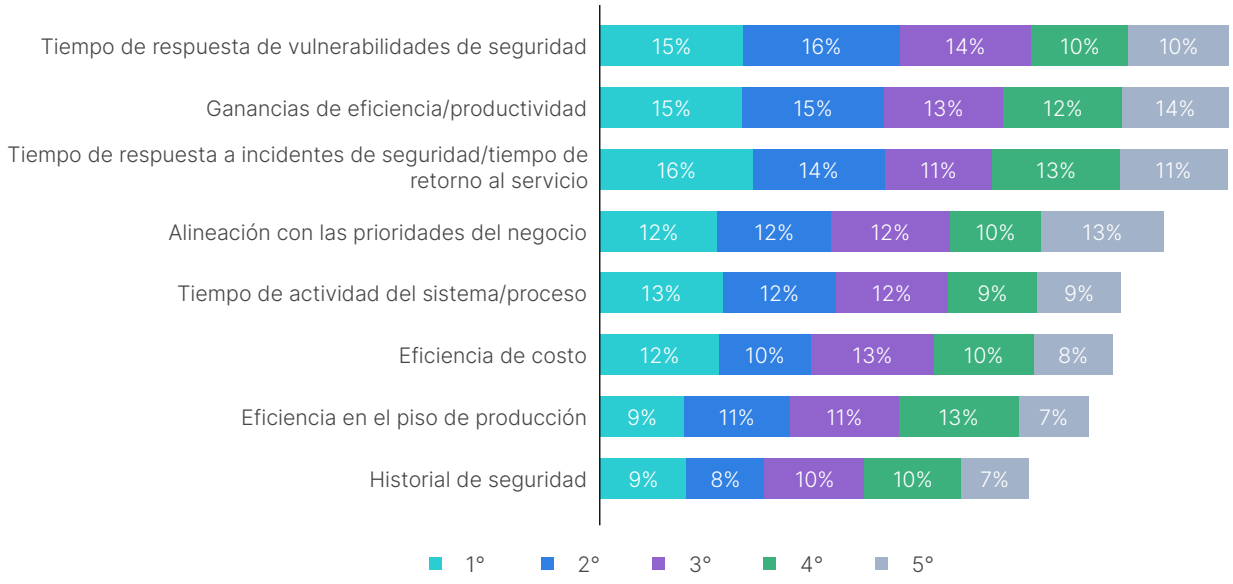
El cifrado, la autorización de usuarios y la autenticación de usuarios suelen utilizarse en más del 50% de los PLC o RTU.



Impacto mundial

P: ¿Cómo mide su éxito? (Califique hasta cinco)

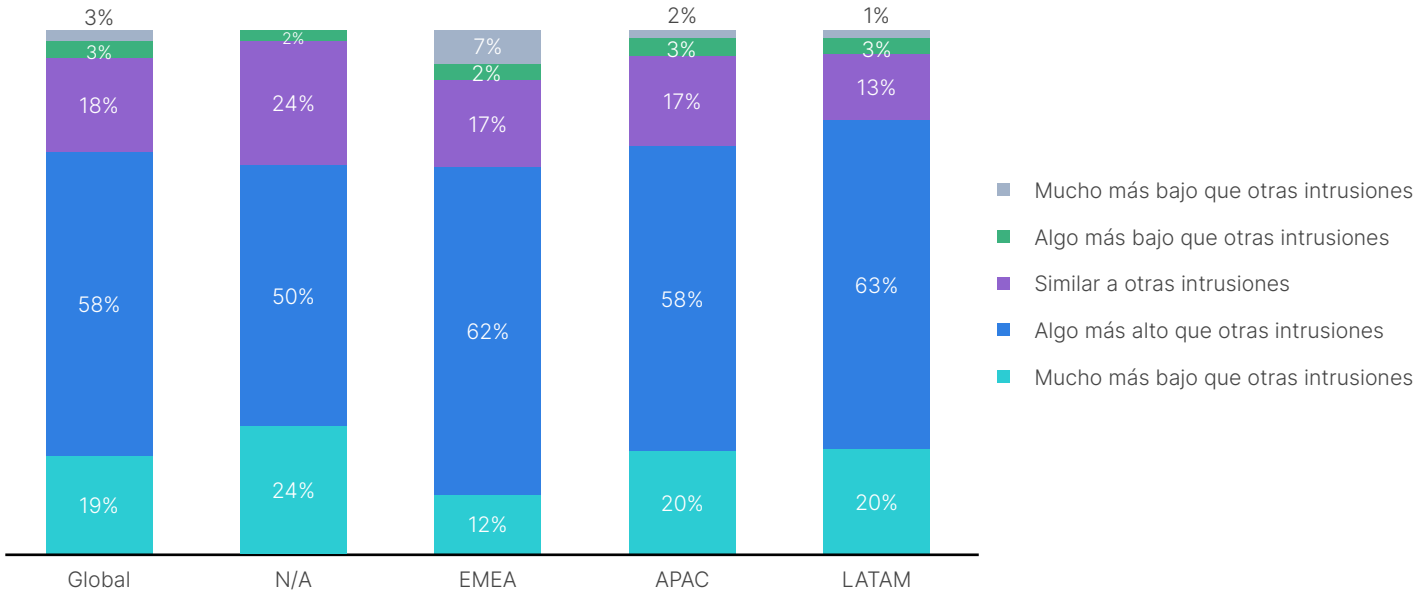
Curiosamente, no existe una definición única de éxito de OT, lo que indica la inmadurez del espacio de seguridad de OT. Sin embargo, como se esperaba para los entornos de OT, el tiempo de respuesta y las ganancias en productividad han llegado a la cima.



Cómo se mide el éxito (clasificación)

P: En comparación con otras intrusiones, ¿qué tan preocupado está por el impacto del ransomware en su entorno OT?

Aunque los ataques de ransomware no son las intrusiones más comunes, son la principal preocupación de la mayoría de las organizaciones a nivel mundial (más que cualquier otra amenaza), probablemente debido a su notoriedad y al alto costo de restaurar los sistemas afectados.



Preocupación por el impacto del ransomware

Mejores prácticas

El setenta y cinco por ciento de las organizaciones en la encuesta de este año reportó al menos una intrusión en los últimos 12 meses. Lo crea o no, esta es una mejora con respecto a 2022, cuando más del 90% reportó al menos una intrusión. Y este año, solo el 11% de los encuestados reportó seis o más intrusiones. El año pasado, el 27% reportó seis o más intrusiones.

Si bien las soluciones de ciberseguridad continúan contribuyendo al éxito de la mayoría (76%) de los profesionales de OT, en particular al mejorar la eficiencia (67%) y la flexibilidad (68%), los datos del informe también indican que la expansión de la solución aún dificulta la incorporación, el uso y la aplicación de las políticas en su panorama de TI/OT cada vez más convergente. Además el problema se ve agravado por el envejecimiento de los sistemas, ya que la mayoría (74%) de las organizaciones reportó que la antigüedad promedio de los sistemas ICS implementados en su organización es de entre seis y diez años. Sin duda, se han logrado algunos avances en la ciberseguridad global de OT, pero las organizaciones deben seguir avanzando.

A continuación se presentan algunas de las mejores prácticas que hemos supuesto están detrás de la pequeña pero significativa mejora encontrada en los resultados de la encuesta de este año.

Desarrolle una estrategia de plataforma de ciberseguridad para proveedores y OT.

La consolidación reduce la complejidad y acelera los resultados. El primer paso es empezar a construir una plataforma a lo largo del tiempo asociándose con proveedores que diseñen sus productos teniendo en cuenta la integración y la automatización. El proveedor adecuado permitirá a las organizaciones incorporar y aplicar políticas de forma consistente en un panorama de TI/OT cada vez más convergente. Además, busque involucrarse con proveedores que tengan un amplio portafolio de soluciones que puedan proporcionar soluciones básicas de inventario de activos y segmentación, así como soluciones más avanzadas, como un SOC de OT o la capacidad para soportar un SOC conjunto de TI/OT.

Implemente tecnología de control de acceso a la red (NAC).

Para resolver los desafíos asociados con la seguridad de los sistemas de control industrial (ICS), control de supervisión y adquisición de datos (supervisory control and data acquisition; SCADA), Internet de las cosas (IoT), traiga su propio dispositivo (BYOD) y otros endpoints, es necesario un NAC avanzado como parte de una arquitectura de seguridad integral. Una solución NAC efectiva también ayuda a mantener el control completo de la red de una organización al administrar nuevos dispositivos que desean conectarse o comunicarse con otras partes de la infraestructura de la organización.

Aplique un enfoque de confianza cero.

Implemente los pasos básicos de inventario y segmentación de activos. El acceso de confianza cero ofrece verificación continua de todos los usuarios, aplicaciones y dispositivos que buscan acceder a activos críticos, independientemente de dónde residan.

Incorpore educación y capacitación en materia de ciberseguridad.

La capacitación en ciberseguridad sigue siendo fundamental porque la batalla contra los ciberdelincuentes requerirá el empoderamiento colectivo de todos los empleados para que tengan el conocimiento y la conciencia de trabajar juntos para protegerse a sí mismos y a los datos de su organización. Las organizaciones deberían considerar incluir capacitación no técnica dirigida a cualquier persona que use una computadora o dispositivo móvil, desde teletrabajadores hasta sus familias.

Principales consejos

1. Continúe implementando los pasos básicos de inventario y segmentación de activos y aplique soluciones de parcheo virtual y microsegmentación más avanzadas para proteger los dispositivos contra vulnerabilidades conocidas y tener tiempo suficiente para parchear los dispositivos correctamente.
2. Colabore en los equipos de TI, OT y producción para evaluar adecuadamente los riesgos cibernéticos y de producción, específicamente los incidentes de ransomware, e informe al CISO para garantizar una concientización, priorización, presupuesto y asignación de personal adecuados.
3. Desarrolle una estrategia de plataforma de ciberseguridad para proveedores y OT. Se están introduciendo muchas soluciones nuevas de seguridad, pero la escasez de personal aumenta. Además, a medida que madure su postura de seguridad, busque involucrarse con proveedores que tengan un amplio portafolio de soluciones que puedan proporcionar soluciones básicas de inventario de activos y segmentación, así como soluciones más avanzadas, como un SOC de OT o la capacidad para soportar un SOC conjunto de TI/OT.

Metodología para este estudio

La mayoría de los encuestados tienen títulos de "operaciones de planta" u "operaciones de manufactura" y casi un tercio son vicepresidentes o directores de operaciones de planta. La mayoría de los encuestados, sin importar su puesto, están profundamente involucrados en las decisiones de compra de ciberseguridad. Y cada vez más son estas personas la que tienen la última palabra en las decisiones de compra de OT. La encuesta de este año reveló que el 91% de los encuestados participa regularmente en las decisiones de compra de ciberseguridad de su organización.

Todos los que participaron en la encuesta de este año trabajaban en alguna de las siguientes industrias:

- Manufactura
- Transportación, logística
- Salud, farmacéutica
- Petróleo, gas, refinación
- Energía, servicios públicos
- Química, petroquímica
- Agua, aguas residuales

Objetivos del estudio

Fortinet contrató a InMoment, una empresa externa con experiencia en investigación, para ayudarnos a desarrollar la personalidad de un profesional de OT.

La encuesta que nos ayudaron a crear está destinada a comprender mejor lo siguiente:

- Cómo encaja la persona en las organizaciones
- Cómo se utilizan las funciones de seguridad
- Cómo se rastrea y reporta la información
- Influencias y factores de éxito

Enfoque

Se utilizó una muestra panel para obtener 570 encuestas completadas con el siguiente tipo de encuestado de una empresa en:

- Manufactura
- Transportación, logística
- Salud, farmacéutica
- Petróleo, gas, refinación
- Energía, servicios públicos
- Química, petroquímica
- Agua, aguas residuales
  - Con más de 1,000 empleados con determinadas excepciones
- La tecnología operativa está dentro de su responsabilidad funcional
- Tiene la responsabilidad de informar sobre las operaciones de manufactura o planta
- Involucrado en las decisiones de compra de ciberseguridad
- Se amplió a alcance global en 2022 y 2023:
  - Los encuestados procedían de diferentes lugares del mundo, entre ellos: Australia, Nueva Zelanda, Brasil, Canadá, Egipto, Francia, Alemania, India, Japón, México, Sudáfrica, Reino Unido y Estados Unidos, entre otros.

Conclusión

El Informe sobre el estado de la tecnología operativa y la ciberseguridad de 2023 revela que las organizaciones están priorizando la ciberseguridad para los entornos de OT. Esta es una tendencia importante y necesaria porque el 75% de las organizaciones encuestadas ha tenido que lidiar con al menos un ciberataque en los últimos 12 meses. Los datos de la encuesta sugieren que la ciberseguridad de OT está mejorando o madurando, y los incidentes parecen estar disminuyendo. Asimismo, los riesgos asociados con los incidentes de OT se están volviendo más evidentes a través de eventos mundiales. Además, las corporaciones ahora son más agresivas en su postura de seguridad de OT y los equipos de TI se involucran más en las redes industriales.

Los datos de nuestra encuesta demuestran un aumento generalizado en varias soluciones de ciberseguridad OT. La ciberseguridad de la tecnología operativa, la propiedad y el riesgo y la implementación de soluciones de seguridad están madurando y teniendo un impacto. Pero todavía queda un largo camino por recorrer para que la mayoría de las organizaciones se protejan adecuadamente contra el malware más común, como el ransomware.

1 "What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?," McKinsey and Company, 17 de agosto de 2022.

2 2022 Global Threat Landscape Report, FortiGuard Labs, 22 de febrero de 2023.

3 "Cyber-Attack Against Ukrainian Critical Infrastructure," CISA, 20 de julio de 2021.

4 "Ukraine: Russian attacks on critical energy infrastructure amount to war crimes," Amnesty International, 22 de octubre de 2022.

5 Jonathan Reed, Pipedream Malware Can Disrupt or Destroy Industrial Systems, Security Intelligence, 19 de abril de 2023.

6 The 2023 Global Ransomware Report, Fortinet, 24 de abril de 2023.

7 2022 Global Threat Landscape Report, FortiGuard Labs, 22 de febrero de 2023.

8 2022 State of Operational Technology and Cybersecurity Report, Fortinet, 21 de junior de 2022.

9 The 2023 Global Ransomware Report, Fortinet, 24 de abril de 2023.

10 CIS Critical Security Controls ICS Companion Guide, Center for Internet Security, Version 7.

FORTINET

www.fortinet.com

mayo 31, 2023 1:40 p. m.

2101968-0-0-EN