FORTINET

INFORME

Informe del estado de la tecnología operativa y ciberseguridad de 2023

Puntos clave

Personas

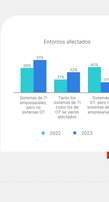
En casi todas las organizaciones encuestadas, los CISO son ahora o pronto serán responsables de la ciberseguridad de OT.

También cabe destacar que ahora más profesionales de ciberseguridad de OT provienen del liderazgo de seguridad de TI en lugar del equipo de operaciones.

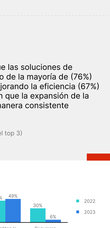
Incidentes de ciberseguridad

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.



# 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 añopasado.

Para combatir las intrusiones, los profesionales de OT están incrementando las soluciones de ciberseguridad en sus redes industriales.

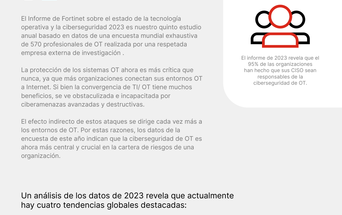
Las amenazas persistentes avanzadas, la segmentación de la red interna y el acceso remoto seguro es lo que más han aumentado, mientras que la inteligencia de amenazas ha disminuido como solución.

Ciberseguridad y funciones de seguridad implementadas

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.

Cómo las soluciones de ciberseguridad ayudan al éxito (en el top 3)

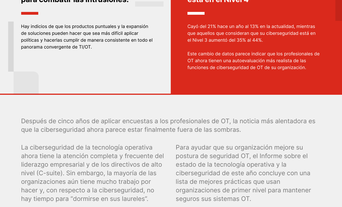


Postura de ciberseguridad

Si bien menos personas caracterizan la postura de ciberseguridad OT de sus empresas como Nivel 4 ("altamente madura") 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.

Madurez de la postura de seguridad OT



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.

Postura de seguridad de OT incluida en una puntuación de riesgo más amplia

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.

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

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

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, 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.