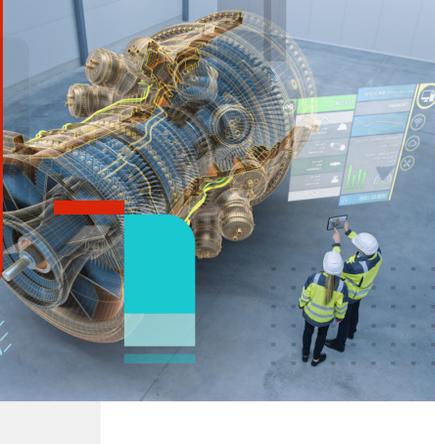


RELATÓRIO

Do estado da tecnologia operacional e cibersegurança de 2023



Pontos chave

Personas

En sua todas las organizaciones encuestadas, los CISO son ahora un terço 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.

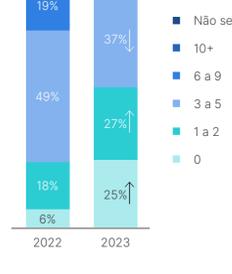
Cibersegurança estará sob controle do CISO nos próximos 12 meses



Incidentes de cibersegurança

Embora o número de organizações que não sofreram uma invasão de cibersegurança tenha melhorado drasticamente em relação ao ano anterior (de 6% em 2022 para 25% em 2023), ainda há espaço significativo para melhorias. Na verdade, três quartos das organizações OT relataram pelo menos uma invasão no ano passado e quase um terço dos entrevistados relataram ter sido vítimas de um ataque de ransomware (32%, inalterado desde 2022). As invasões de malware e phishing aumentaram 12% e 9% respectivamente.

Número de invasões no ano passado



Por Maturidade em Cibersegurança

	Nível 0-2	Nível 3	Nível 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

O impacto das invasões

Quando um ataque cibernético ocorreu no início deste ano, quase um terço (32%) dos entrevistados indicou que os sistemas de TI e OT foram afetados – acima dos 21% do ano passado.

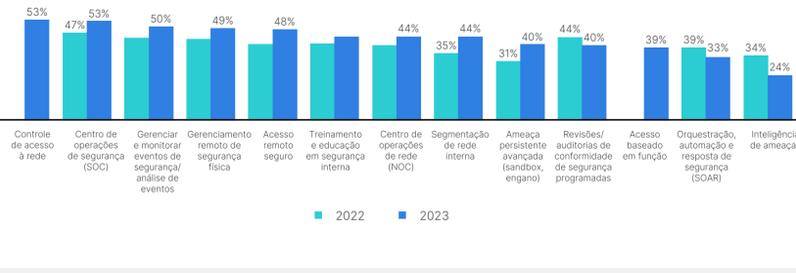
Para combater invasões, os profissionais de OT estão aumentando as soluções de cibersegurança em suas redes industriais.

Ambientes impactados



Ameaças persistentes avançadas, segmentação de rede interna e acesso remoto seguro foram os que mais aumentaram, enquanto a inteligência de ameaças diminuiu como solução.

Recursos de cibersegurança e segurança implementados



Como a cibersegurança ajuda

Embora os resultados da pesquisa revelem que as soluções de cibersegurança continuam a ajudar no sucesso da maioria (76%) dos profissionais de OT, principalmente melhorando a eficiência (67%) e a flexibilidade (68%), os dados também mostram que a expansão da solução torna mais difícil proteger seu cenário convergente de TI/TO.

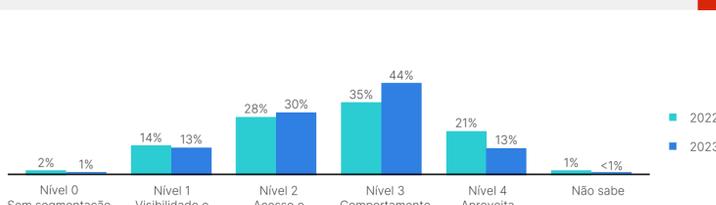
Como as soluções de cibersegurança ajudam no sucesso (no top 3)



Postura de cibersegurança

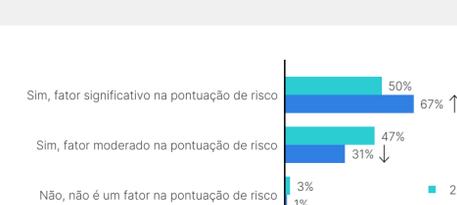
Embora menos indivíduos caracterizem a postura de cibersegurança OT de suas empresas como nível 4 (“altamente maduro”) este ano em comparação com 2022 (reduziu para 13% de 21%), 44% de todas as organizações agora se classificam no nível 3, acima do último ano de 35%. Isso pode refletir uma abordagem de amadurecimento para avaliar as capacidades, resultando em uma visão mais realista do estado de sua postura.

Maturidade da postura de segurança OT



Quase todas as organizações (98%) agora incluem sua postura de cibersegurança OT na pontuação de risco mais ampla compartilhada com liderança executiva e conselhos de administração.

Postura de segurança OT incluída na pontuação de risco mais ampla



Sumário executivo

O relatório do estado da tecnologia operacional e cibersegurança de 2023 é o nosso quinto estudo anual, baseado em dados de uma pesquisa mundial aprofundada com 570 profissionais de TO realizada por uma empresa de pesquisa terceirizada respeitada.

Proteger os sistemas OT agora é mais crítico do que nunca, pois mais organizações conectam seus ambientes OT à internet.

Embora a convergência de TI/TO tenha muitos benefícios, ela está sendo dificultada e prejudicada por ameaças cibernéticas avançadas e destrutivas. O transbordamento desses ataques é cada vez mais direcionado a ambientes OT. Por esses motivos, os dados da pesquisa deste ano indicam que a cibersegurança OT é agora mais central e crucial no portfólio de riscos de uma organização do que nunca.

Uma análise dos dados de 2023 revela que atualmente existem quatro tendências globais proeminentes:

Houve um declínio geral nas invasões devido a menos violações internas

embora o ransomware e o phishing ainda sejam as principais ameaças. Em vez de uma diminuição no risco cibernético, no entanto, isso pode ser devido aos cibercriminosos adotarem uma abordagem

Quase todas as organizações colocaram as responsabilidades pela cibersegurança OT

com um diretor de segurança da informação (CISO) em vez de um executivo ou equipe de operações.

Organizações e profissionais de OT contêm de uma ampla gama de soluções de cibersegurança para combater invasões.

Há indicações de que produtos pontuais e expansão de soluções podem tornar mais desafiador aplicar políticas e aplicá-las de forma consistente em todo o cenário convergente de TI/TO.

O número de entrevistados que consideram a maturidade de cibersegurança de sua organização no nível 4 caiu

de 21% há um ano para 13% hoje, enquanto aqueles que consideram sua cibersegurança no nível 3 aumentaram de 35% para 44%.

Essa oscilação de dados parece indicar que os profissionais de TO agora têm uma autoavaliação mais realista dos recursos de cibersegurança de TO de sua organização.

Após cinco anos pesquisando profissionais de OT, a notícia mais animadora é que a cibersegurança agora parece estar finalmente fora das sombras.

A cibersegurança da tecnologia operacional agora recebe atenção total e frequente da liderança corporativa e dos C-suites.

No entanto, a maioria das organizações ainda tem muito trabalho a fazer e nunca há tempo para “descansar sobre os louros” em relação à cibersegurança.

Para ajudar sua organização a melhorar sua postura de segurança OT, o relatório do estado da tecnologia operacional e cibersegurança deste ano conclui com uma lista das melhores práticas comuns que organizações de primeira linha empregam para manter seus sistemas OT seguros.