SANS

Analyst Program

Enquete

Uma pesquisa SANS 2021: OT/ICS Cibersegurança

Escrito por **Mark Bristow**

Agosto 2021

Cisco Umbrella
DRAGOS
KEYSIGHT TECHNOLOGIES
network perception
NOZOMI NETWORKS
tenable

©2021 SANS™ Institute

Sumário Executivo

O mundo da segurança da Tecnologia Operacional (OT) e dos Sistemas de Controle Industrial (ICS) está continuamente se adaptando para fazer frente a novos desafios e ameaças. Esta pesquisa SANS 2021 de Cibersegurança OT/ICS explora como os defensores da OT (também conhecida como Tecnologia de Automação – TA), de todos os setores, encaram esses desafios e olham para áreas onde podemos concentrar esforços para ajudar a defender as nossas infraestruturas críticas no futuro. A pesquisa deste ano foca nos riscos reais e reconhecidos, ameaças, fontes de informação e desafios de implementação operacional, bem como os níveis de investimento neste importante tópico. Este ano, os resultados mostram claramente o aumento de ransomware, impactando as infraestruturas críticas como uma ameaça significativa e com isso uma área de preocupação entre os entrevistados.

Os profissionais de cibersegurança e as salas do conselho da OT mantêm as ameaças e os riscos reconhecidos em mente. Incidentes recentes, como o ataque de ransomware da Colonial Pipeline e o ransomware que atingiu a empresa JBS Foods, destacam o ambiente de ameaças complexo que esses sistemas enfrentam. Os resultados confirmam que ransomware e cibercrimes com motivação financeira estão no topo da lista de vetores de ameaças que mais preocupam os entrevistados, seguidos pelo risco de ciberataques de estado-nação (43,1%). O mais interessante é que a elevação dos vetores de ameaças não intencionais representam 34,5% do total de escolhas para os três principais vetores de ameaças.

O cenário de ameaças e riscos permanece um tanto obscuro e os incidentes geralmente não são reportados e são insuficientemente investigados. Quando solicitados a identificar o setor em maior risco, a maioria dos setores entrevistados não escolheu o seu próprio. Quando questionados sobre vulnerabilidades em seu setor, no entanto, eles relataram desafios significativos. A autoconsciência de incidentes na forma de monitoramento e detecção também teve uma classificação relativamente baixa, com apenas 12,5% dos entrevistados confiantes de que não haviam experimentado um comprometimento no ano passado e 48% dos participantes da pesquisa não sabiam se sofreram um incidente. A conectividade com os sistemas externos continua sendo a causa raiz esmagadora dos incidentes, uma indicação de que as organizações ainda falham em seguir as melhores práticas de segmentação de rede. Além disso, 18,4% dos vetores iniciais de infecção estão relacionados ao aproveitamento da estação de trabalho de engenharia, um fato altamente preocupante porque poucos correlacionam dados cibernéticos e de processo para analisar violações no sistema. Canais publicamente disponíveis subnotificam incidentes; por exemplo, quase todos os entrevistados indicaram ter pelo menos um incidente, com 90% tendo algum nível de impacto no processo, mas apenas incidentes de alto perfil, como o ocorrido no Colonial, ganham manchetes.

O panorama da cibersegurança da OT mudou significativamente nos últimos dois anos. Temos visto uma atenção significativa e um crescimento geral em investimento na proteção de nossos sistemas críticos de ICS/OT, mas ainda precisamos de algum progresso em áreas-chave. Os principais destaques desta pesquisa em todo o setor incluem:

- Crescimento constante em posições de cibersegurança com foco em ICS
- Aumento geral na alocação de orçamento para esforços de cibersegurança em ICS
- Aumento constante na influência dos regimes regulatórios para impulsionar os investimentos em cibersegurança
- Aumento na adoção da nuvem (e uso primário para resultados operacionais)
- Adoção significativa da estrutura do MITRE ATT&CK® para ICS (devido ao seu lançamento relativamente recente)
- Adoção contínua de tecnologias de monitoramento de ICS e metodologias de caça a ameaças
- Suporte contínuo para gerenciamento de patches (pela maioria) e processos de avaliação de vulnerabilidade se não forem aplicados uniformemente
- Os estoques de ativos continuam a desafiar a maioria das organizações, com apenas 58,2% tendo um processo formal (progresso, mas progresso insuficiente)

No geral, ocorreu um progresso significativo nas áreas de profissionalização da força de trabalho, monitoramento da OT, análise, avaliação, remediação, e resposta. No entanto, embora que ainda precisemos de melhorias na gestão de inventário e ativos, e segmentação/interconectividade do sistema OT, os últimos dois anos demonstraram um grande progresso (com mais por vir).

Introdução

A pesquisa SANS 2021 de ICS/OT recebeu 480 respostas, um aumento de 42% em relação à pesquisa de 2019. Os entrevistados representam uma ampla gama dos principais setores da indústria[1], com entrevistados adicionais subclassificados em 62 grupos singulares, que vão desde a área de jogos a aviação, a sistemas espaciais e sistemas de pagamento.

A pesquisa representa uma visão equilibrada em todo o setor, capturando as respostas daqueles cujas responsabilidades principais enfatizam as operações em ICS ou TI/empresa de negócios. A maioria dos entrevistados passa a maior parte do tempo focada na cibersegurança do ICS. Metade deles (50%) relataram que gastam 50% ou mais do seu tempo em cibersegurança de ICS, ao contrário da pesquisa de 2019, onde 45% dos entrevistados relataram que gastam pelo menos 50% de seu tempo em cibersegurança de OT/ICS. Em 2021, mais de 50% têm funções que enfatizam as operações de ICS, exclusivamente ou em conjunto com TI/empresa de negócios. Veja a Figura 1.

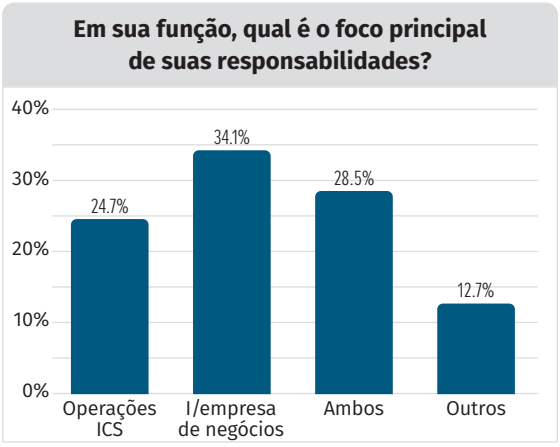

Figura 1. Foco da função de TI/OT

[1] Opções de pesquisa baseadas nas definições críticas do setor de infraestrutura da CISA, com alguns modificadores para elementos específicos do ICS, www.cisa.gov/critical-infrastructure-sectors

Isso representa um aumento significativo no número de profissionais de cibersegurança de ICS em um período de tempo relativamente curto. Embora alguns tenham se concentrado na cibersegurança de ICS por mais de 15 anos, agora vemos um aumento de recursos dedicados e da atenção dos operadores neste espaço que reconhecem a importância dessas funções com foco em OT. Essa tendência pode ter relação direta com o número de entrevistados que possuem certificações de segurança cibernética específicas de ICS; 54% dos entrevistados possuem uma certificação na pesquisa de 2021 contra apenas 38% em 2019. Este investimento em certificação indica que a indústria reconhece e valoriza as certificações, especialmente as certificações do SANS. Veja a Figura 2.

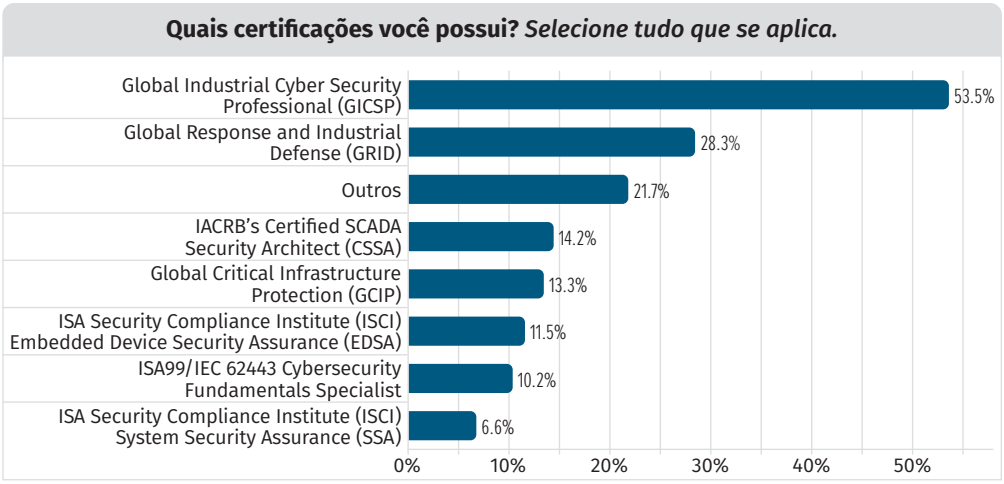

Figura 2. Certificações dos entrevistados

A Figura 3 fornece um registro ativo da demografia dos entrevistados.

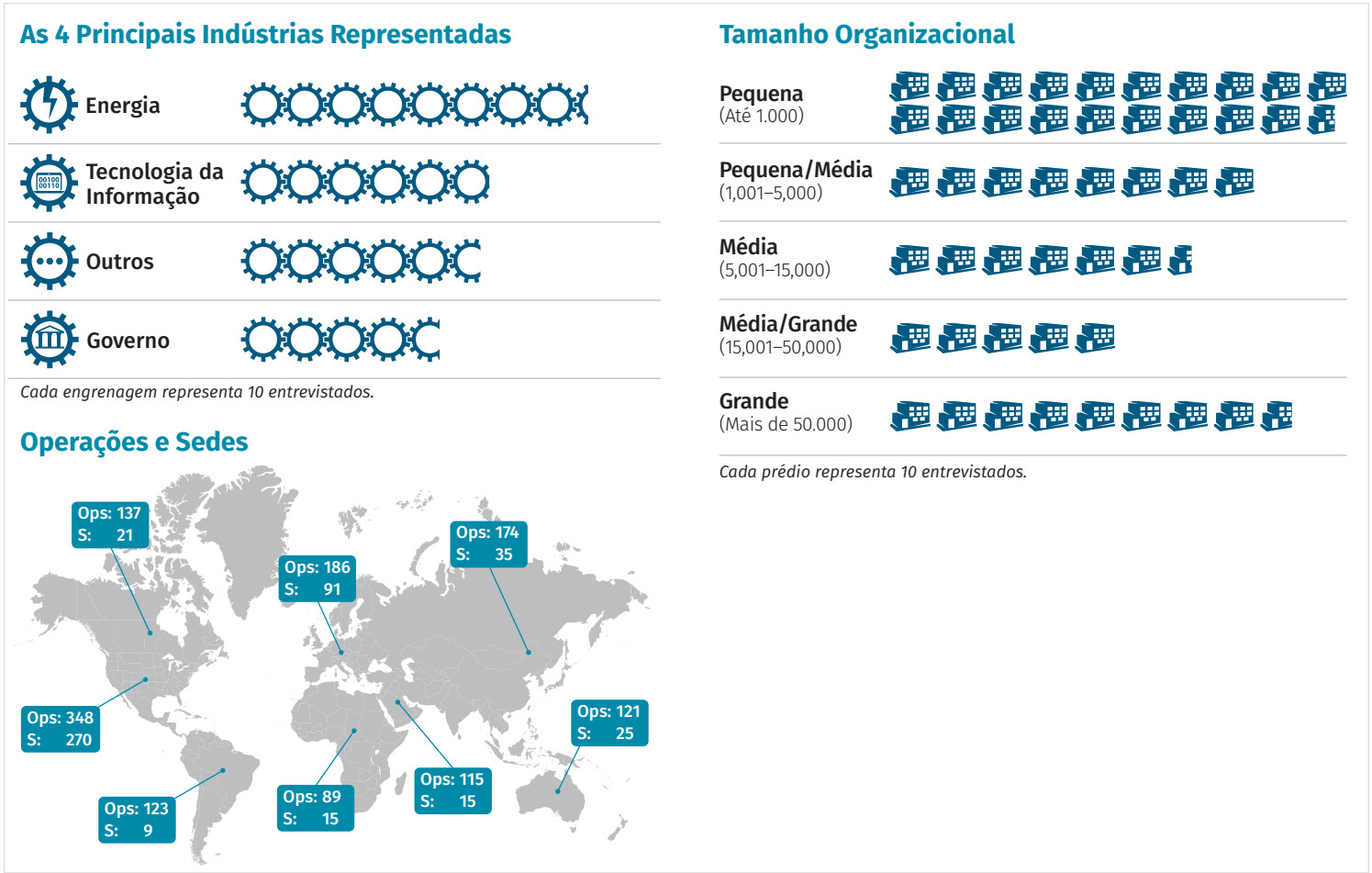

Figura 3. Dados demográficos dos entrevistados na pesquisa

O Negócio de Segurança de ICS

As organizações agora reconhecem a segurança de seus ativos de ICS como fundamental para seus negócios e expressaram-na como sua preocupação número 1 em garantir a confiabilidade e a disponibilidade de sistemas de controle. Veja a Tabela 1.

Os maiores desafios enfrentados pela segurança da OT dizem respeito, como sempre, a pessoas, processos e tecnologia. As respostas dos entrevistados são relativamente equilibradas entre essas três áreas no que diz respeito ao que eles consideram os maiores desafios que suas organizações enfrentam. Veja a Figura 4.

- **Tecnologia—**TA integração técnica representa um desafio. As organizações precisam garantir que as implementações técnicas integrem de forma mais eficaz os ambientes legados de OT com tecnologias de segurança modernas. A inovação dos provedores de soluções pode dar suporte nesta área.
- **Pessoas—**Enfrentamos uma escassez significativa de mão de obra de segurança de OT. Embora esta pesquisa mostre que atualmente temos mais profissionais de segurança de OT do que nunca, ainda precisamos fazer mais para acrescentar profissionais para a indústria para realizar este trabalho crítico. Precisamos de investimentos em treinamento formal e informal e desenvolvimento profissional para treinar e requalificar a força de trabalho para atender a essa demanda crescente.

Tabela 1. Principais preocupações empresariais

	2021		2019		Mudança na Classificação
	%	Classificação	%	Classificação	
Garantir a confiabilidade e disponibilidade de sistemas de controle	50.3%	1	52.3%	1	—
Reduzindo o risco/Melhorando a segurança	45.5%	2	34.8%	3	+1
Prevenindo danos aos sistemas	27.2%	3	27.7%	4	+1
Protegendo conexões com sistemas externos	23.3%	4	11.7%	10	+6
Cumprindo a conformidade regulatória	19.8%	5	22.3%	5	—
Prevenindo o vazamento de informações	18.1%	6	14.8%	9	+3
Garantir a saúde e segurança dos funcionários	17.7%	7	42.2%	2	-5
Protegendo pessoas externas e propriedades	15.2%	8	20.7%	6	-2
Criação, documentação e gerenciamento de políticas e procedimentos de segurança	13.1%	9	8.2%	13	+4
Protegendo a reputação e a marca da empresa	11.6%	10	17.6%	8	-2
Fornecer ou coordenar programas de conscientização e educação sobre cibersegurança para funcionários	11.2%	11	10.5%	11	—
Prevenindo perdas financeiras da empresa	7.9%	12	18.8%	7	-5
Protegendo segredos comerciais e propriedade intelectual	6.0%	13	7.8%	14	+1
Minimizar o impacto sobre os acionistas	3.3%	14	9.8%	12	-2

Surpreendentemente, para as indústrias, historicamente, com foco em segurança de pessoas, garantir a saúde e a segurança dos funcionários e do pessoal externo caiu em importância, do segundo para o quinto lugar. A prevenção de perdas financeiras também caiu em importância, outro fato surpreendente, uma vez que muitas concessionárias são de propriedade de investidores e responsáveis perante os acionistas. A pandemia global de COVID-19 pode ter impactado essas perspectivas, com o quadro de funcionários muito reduzido nos últimos dois anos e um mercado financeiramente restrito resultante de uma mudança para minimizar o risco de negócios de longo prazo de modo a resistir à desaceleração impulsionada pela COVID.

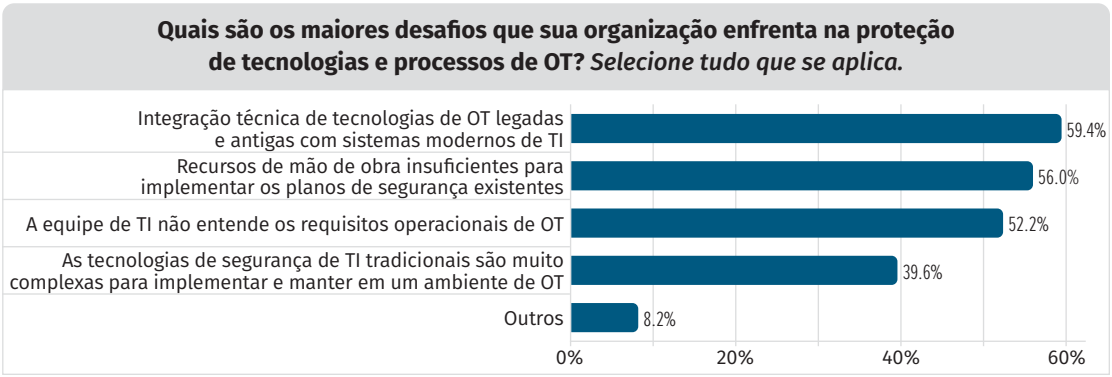

Figura 4. Desafios da OT

- **Processos—**Os líderes de segurança precisam desenvolver uma cultura de compreensão mútua e de visão e execução compartilhadas por meio da liderança e integração de processos. Por ter especialistas em TI e OT trabalhando mais próximos, cada um pode entender melhor a perspectiva do outro e, por fim, gerar resultados favoráveis para o negócio. Sem esse entendimento compartilhado, todos os nossos outros esforços podem dar em nada.

Sem recursos, não podemos garantir nada. Quarenta e sete por cento dos entrevistados relataram que seus orçamentos de segurança de ICS aumentaram nos últimos dois anos, com 16% diminuindo o orçamento e 32% sem mostrar nenhuma alteração. Quando visto em comparação com o orçamento geral de 2021 a 2019, ocorreu um crescimento significativo na maioria das categorias, com um aumento na resposta "sem orçamento" (talvez por causa da eliminação da opção "desconhecida" em 2021). Veja a Tabela 2.

Tabela 2. Comparação de Orçamento de 2021 vs. 2019

Budget	2021	2019	% Change
Não temos um orçamento	23.7%	9.9%	13.8% ▲
Menos de $100.000 USD	19.1%	11.5%	7.6% ▲
$100.000–$499.999 USD	24.2%	8.9%	15.3% ▲
$500.000–$999.999 USD	10.8%	8.3%	2.5% ▲
$1 milhão–$2.49 milhões USD	10.8%	6.3%	4.5% ▲
$2.5 milhões–$9.99 milhões USD	5.2%	3.7%	1.5% ▲
Mais que $10 milhões USD	6.2%	7.3%	-1.1% ▼

Os proprietários de ativos continuam a investir na segurança de seu ambiente de ICS, e esse investimento precisa atingir os resultados de segurança discutidos nesta pesquisa.

Riscos para Nossos Ambientes de ICS

O risco, a força que direciona a maior parte dos esforços em torno da proteção e segurança do ICS, está diretamente correlacionado com o vetor de ameaça que insere o risco. Em 2021, crimes com motivação financeira – incluindo ransomware e extorsão – subiram para o topo na classificação geral de vetores que preocupam os entrevistados, seguidos por ciberataques de estados-nação além de dispositivos e "coisas" (que não podem se proteger) sendo adicionados à rede. Veja a Figura 5.

Selecione os três principais vetores de ameaças com que você está mais preocupado.
Observação: a lógica da pesquisa requer que você selecione exatamente três opções da lista abaixo.

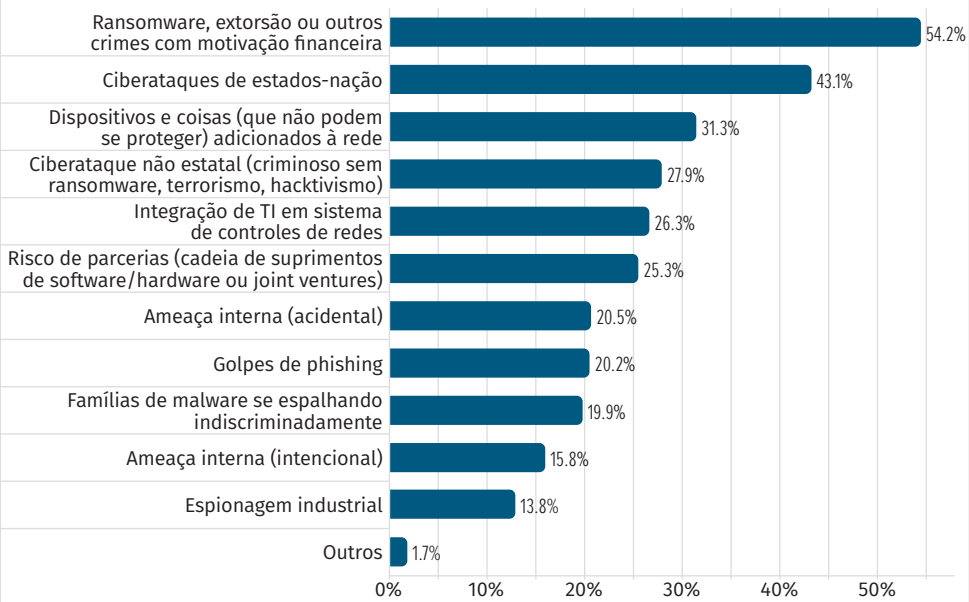

Figura 5. Principais vetores de ameaça

Curiosamente, no entanto, quando solicitados a identificar o vetor de ameaça mais importante nesta lista, a ordem daqueles com maior preocupação diferiu um pouco, indicando que os entrevistados acreditam que os vetores de ameaça não intencionais também desempenham um papel importante na segurança do ICS:

1. Ransomware, extorsão ou outros crimes com motivação financeira
2. Ciberataques de estados-nação
3. Dispositivos e coisas (que não podem se proteger) adicionados à rede
4. Ciberataque não estatal (criminoso sem ransomware, terrorismo, hacktivismo)

Preste atenção aos vetores de ameaça não intencionais (ou seja, um vetor de ameaça que não é malicioso por natureza, mas ainda apresenta riscos). Esses vetores de ameaça – incluindo ameaça interna acidental, dispositivos não autorizados na rede e o risco de redes de parceiros e integração de TI/OT – foram responsáveis por 35% dos principais vetores de ameaças em geral.

Para testar a hipótese de que a percepção de risco varia de acordo com o setor industrial, colocamos esta questão: "Com base em sua compreensão do cenário de ameaças de ICS, quais setores são mais propensos a ter um comprometimento bem-sucedido do ICS, impactando a segurança e a confiança na operação do processo?" Nossa intenção era direcionar para o risco reconhecido da indústria não somente para os setores em que os entrevistados participam, mas também para outros setores.

A Figura 6 na próxima página mostra os resultados. O setor de energia liderou, seguido por assistência médica (privado) e saúde pública, ambos tradicionalmente alvo de múltiplos atores de ameaças. O setor de água/esgoto seguiu, não surpreendentemente, como suas margens baixas frequentemente criam um atraso nos fundamentos de segurança. Observe que, embora esses resultados possam mostrar algum viés de pesquisa relacionado aos dados demográficos, a equipe de analistas destaca que esses resultados são consistentes com a percepção de risco dos participantes setoriais e não setoriais.

Com base em sua compreensão do cenário de ameaças em ICS, quais setores são mais propensos a ter um comprometimento bem-sucedido do ICS, impactando a segurança e a confiança na operação do processo? ***Escolha seus três primeiros.***

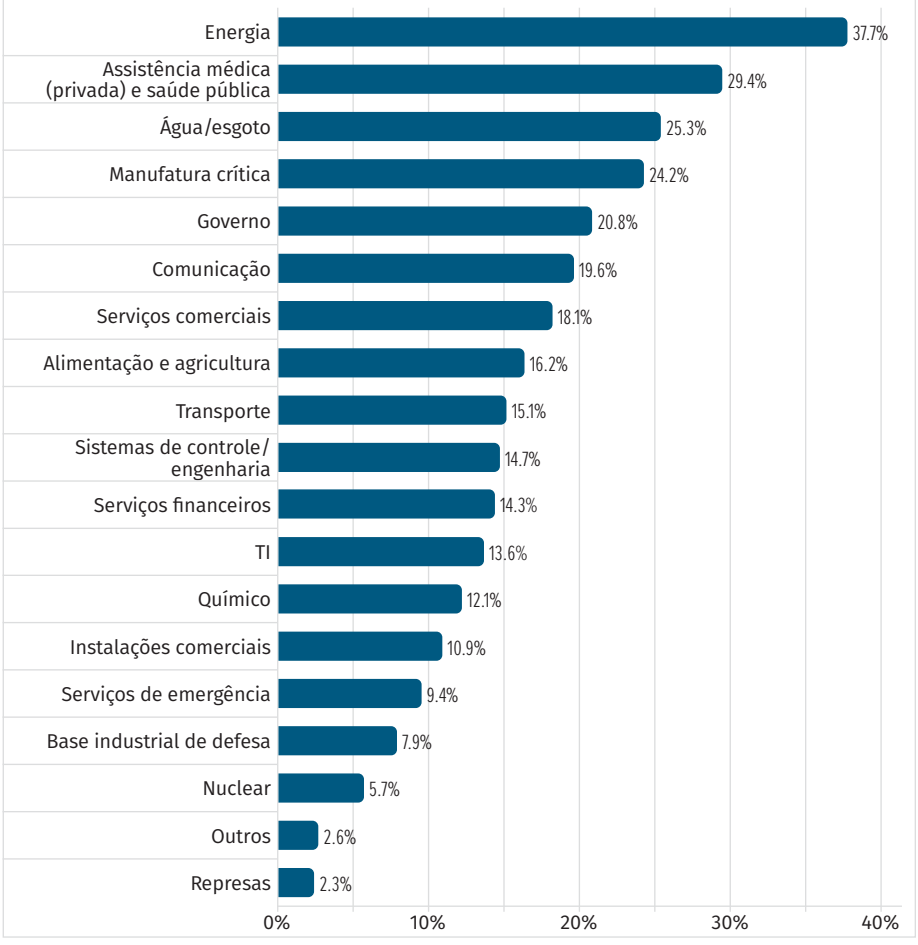

Figura 6. Percepção do setor de maior risco

Algumas observações interessantes indicam que precisamos de mais dados para informar melhor o quadro geral de risco, especialmente porque não está claro se as motivações para essas respostas resultam de confiança ou excesso de confiança nas próprias posturas de segurança:

- A maioria das indústrias parece confiante na postura de segurança de OT de sua indústria. Das 18 opções disponíveis, apenas cinco avaliaram seu próprio setor como o mais provável de ter um ciberataque bem-sucedido: serviços comerciais, comunicações, base industrial de defesa (DIB), energia e água/esgoto.
- Para os entrevistados que não escolheram seu próprio setor, a energia e a assistência médica privada e saúde pública foram as principais escolhas.
- Inconsistências relacionadas a setores que os entrevistados consideraram relativamente livres de risco. Por exemplo, adversários sofisticados geralmente visam os sistemas DIB para comprometer e mantê-los em risco.Além dos próprios entrevistados do DIB, no entanto, quase nenhum outro selecionou o DIB como um alvo provável.

A segurança do ICS realmente entrou na consciência do público nos últimos anos, e a percepção de ameaças altas e graves/críticas aumentou dramaticamente de 2019 a 2021 (consulte a Figura 7). Os eventos de 2020 e 2021 podem ter influenciado essa percepção. Considerando que o ransomware foi classificado como a sexta maior preocupação em 2019, ransomware, extorsão e cibercrimes com motivação financeira agora estão no topo da lista de vetores de ameaças que preocupam os entrevistados.

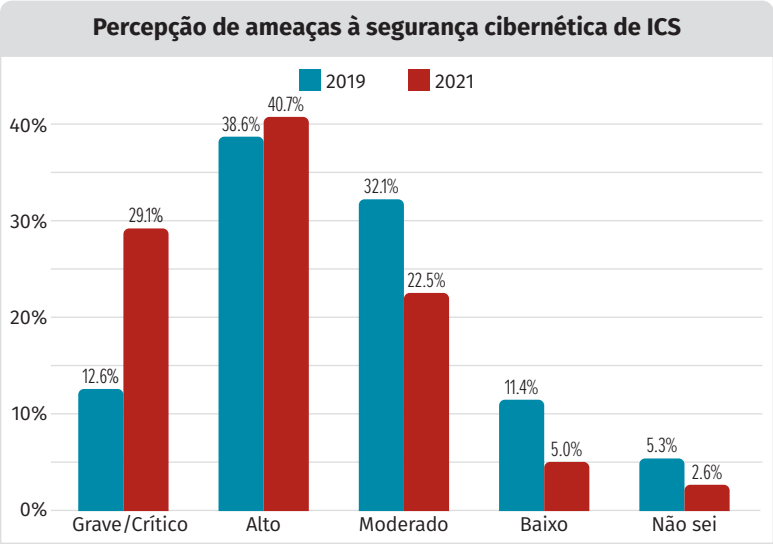

Figura 7. Percepção de risco de 2019 vs. 2021

INCIDENTES EM ICS: IMPACTOS E LACUNAS

Como em 2019, os hackers continuam sendo a fonte mais prevalente de intrusão na rede ICS (como esperado, porque em muitos casos os níveis adicionais de atribuição são impossíveis ou de utilidade organizacional limitada). O crime organizado subiu três posições para a fonte número dois na pesquisa de 2021, provavelmente consequência do aumento de incidentes de ransomware, enquanto as fontes de estados-nação estrangeiros caíram três posições, do número quatro em 2019 para o número sete em 2021. Consulte a Tabela 3.

Um foco nos últimos anos no treinamento de funcionários, programas de ameaças internas e validação de parceiros de negócios para cibersegurança pode ter contribuído para a redução desses conceitos entre as pesquisas. Curiosamente, os serviços de inteligência domésticos subiram três posições, para a preocupação número oito em 2021.

Como em 2019, 15% dos entrevistados relataram que tiveram um incidente de cibersegurança em seu ambiente de OT nos últimos 12 meses. No entanto, podemos estar perdendo terreno na área de detecção e resposta a incidentes. Em comparação com 42% em 2019 dizendo que estavam incertos, 48% dos participantes da pesquisa não sabiam se haviam tido um incidente, indicando uma clara necessidade de melhorar nossos recursos de detecção e resposta como comunidade. Veja a Figura 8.

Tabela 3. Risco de atores de ameaça ao longo do tempo

Opções de resposta	Classificação 2021	2019 Rank	Mudança
Hackers	1	1	—
Crime organizado	2	5	+3 ▲
Prestadores de serviços atuais, consultores, contratos	3	3	—
Funcionários atuais	4	2	-2 ▼
Ativistas, organizações ativistas, hacktivistas	5	6	+1 ▲
Não sei (as fontes não foram identificadas)	6	7	+1 ▲
Estados-nação estrangeiros ou grupos patrocinados pelo Estado	7	4	-3 ▼
Serviços de inteligência doméstica	8	11	+3 ▲
Ex-fornecedores de equipamentos	9	12	+3 ▲
Ex-funcionários	10	10	—
Fornecedores de equipamentos atuais	11	8	-3 ▼
Concorrentes	12	9	-3 ▼
Fornecedores ou parceiros	13	13	—
Ex-prestadores de serviços, consultores, contratos	14	14	—
Outros	15	15	—

Lembre-se sempre de relacionar a percepção de risco com a realidade. Por exemplo, a diminuição nos ataques de estados-nação estrangeiros (caindo do número quatro em 2019 para o número sete em 2021) é inconsistente com a classificação dos ciberataques de estado-nação como o segundo maior vetor de ameaça que preocupa os entrevistados.

Você experimentou um ou mais incidentes de segurança (por exemplo, acesso não autorizado; violação de segurança; perda de dados relevantes da OT; interrupção operacional, dano, destruição de produto, processo ou propriedade) envolvendo sua OT/sistemas de controle durante os últimos 12 meses?

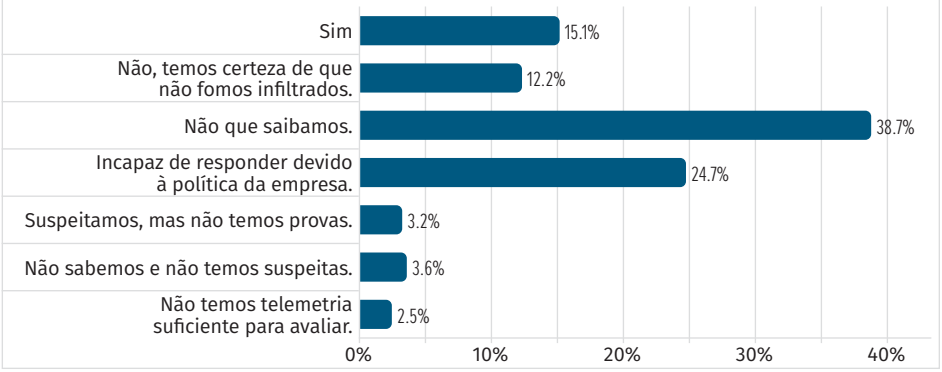

Figura 8. Incidentes nos últimos 12 meses

Dos 15% que relataram um incidente, a maioria experimentou menos de 10 incidentes. Mesmo com esse número relativamente baixo, no entanto, os incidentes ainda podem ser disruptivos: 26% relataram que pelo menos 10% dos incidentes impactaram nas operações. Esses dados indicam que devemos questionar a percepção de que a maioria dos incidentes não tem impacto operacional. Veja a Figura 9.

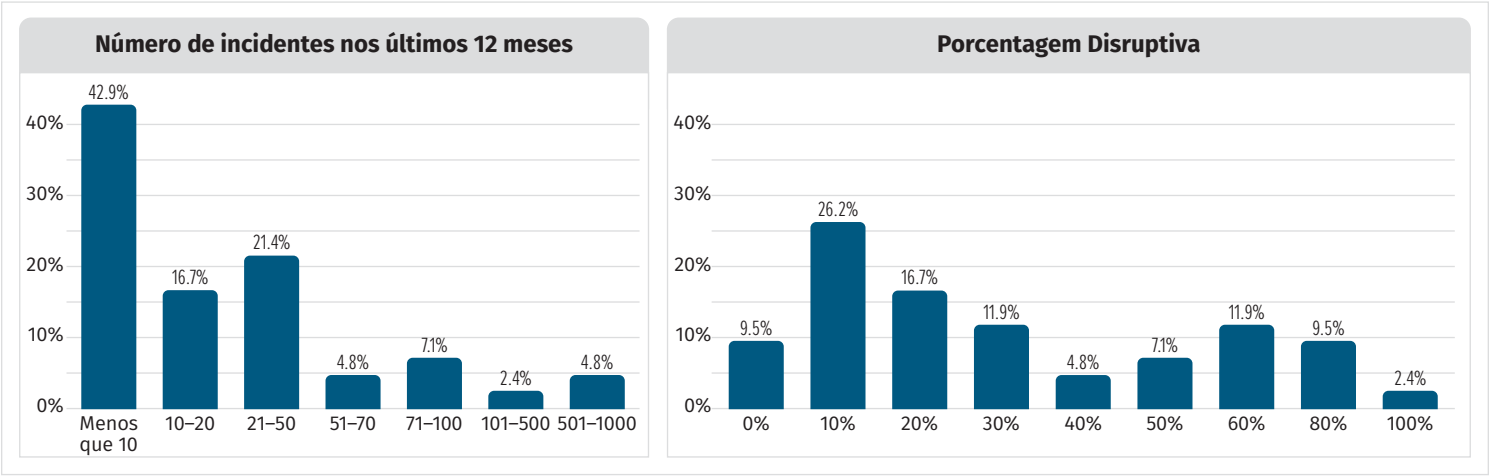

Figura 9. Frequência de incidente e interrupção do processo

Um dado positivo, o tempo entre o comprometimento e a detecção melhorou significativamente desde 2019. A categoria de 6 a 24 horas passou de 35% em 2019 para 51% em 2021 (veja a Figura 10), e a taxa de menos de 6 horas na pesquisa de 2021 (não perguntada na pesquisa de 2019) está em 30%.

O investimento contínuo em tecnologias de detecção de incidentes em OT, monitoramento e analistas de segurança cibernética de OT, além de centros de operação de segurança provavelmente impulsionaram essas melhorias. Essa tendência também representa uma interrupção significativa em casos históricos de intrusão de OT, como Havex[2] e BlackEnergy[3], em que o tempo de permanência do adversário era de mais de três anos antes da detecção. A contenção também mostra resultados promissores, com a maioria dos incidentes sendo contidos no primeiro dia do incidente.

Relatórios públicos sobre incidentes cibernéticos que afetam as redes OT não estão amplamente disponíveis. A comunidade se beneficiaria com relatórios de dados mais transparentes, o que poderia nos permitir estudar esses incidentes mais detalhadamente para implementar melhores medidas defensivas para proteger nossas operações.

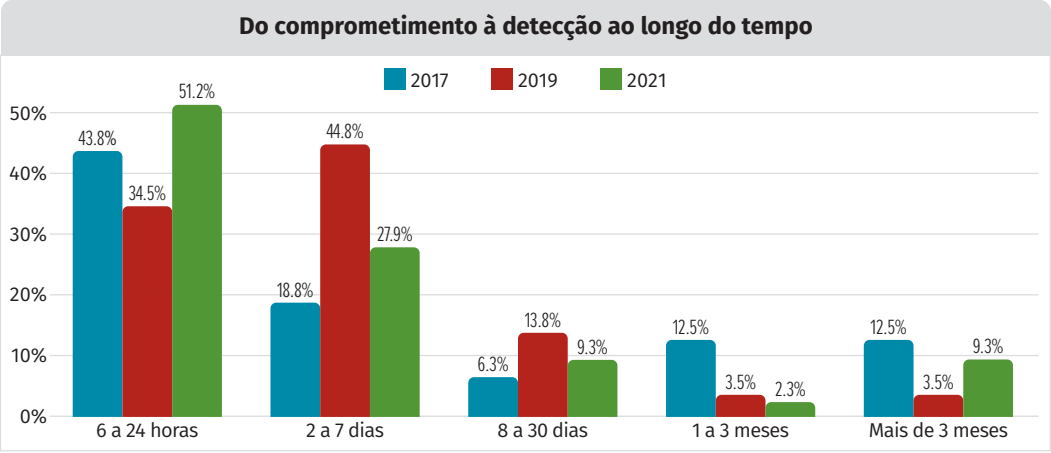

Figura 10. Velocidade de detecção de comprometimento ao longo do tempo

[2] "Havex," https://en.wikipedia.org/wiki/Havex

[3] "BlackEnergy," https://en.wikipedia.org/wiki/BlackEnergy

Contudo, os problemas persistem. O número de incidentes que atingem ou impactam o ambiente de OT ainda é preocupante porque, potencialmente, tem efeitos imediatos nesse cenário, mesmo que uma organização consiga conter o incidente rapidamente. Como esperado, os esforços de remediação parecem estar um pouco atrasados, com a maior parte ocorrendo na primeira semana de contenção.

Quais foram os vetores de ataque iniciais envolvidos em seus incidentes de OT/sistemas de controle? ***Selecione tudo que se aplica.***

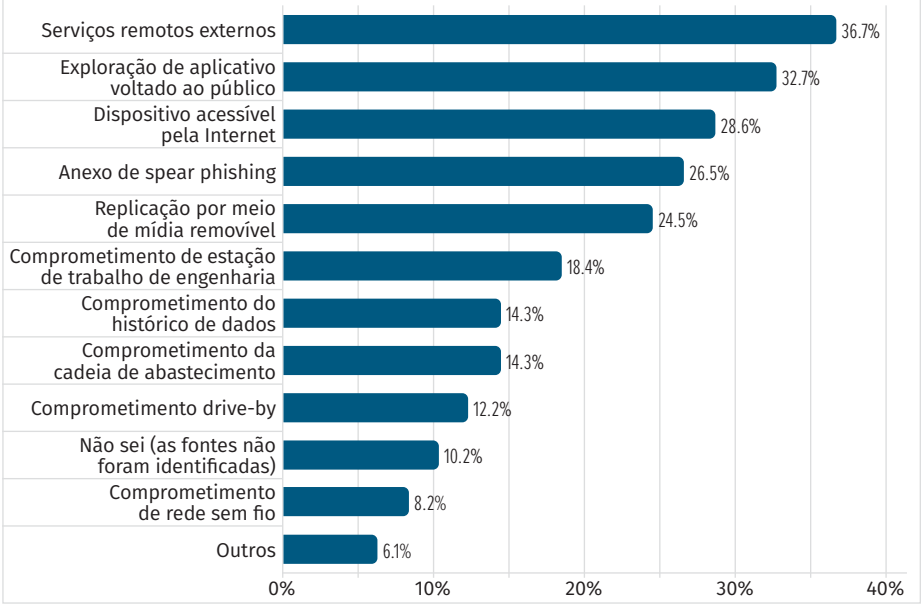

Figura 11. Vetores de ataque inicial de incidente

Os serviços de acesso remoto (37%) lideraram o relatório de vetores de acesso inicial, que está alinhado com o risco reconhecido (descrito na próxima seção) de fontes de conectividade externas quando os entrevistados classificaram suas fontes de risco agudo reconhecido. Com o aumento do foco da indústria na proteção de tecnologias de acesso remoto, esperávamos uma queda mais significativa em relação a 2019, quando o acesso remoto representou 41% dos vetores de ataque iniciais. Claramente, precisamos promover mais fortemente a adoção de tecnologia de acesso remoto seguro. Veja a Figura 11.

Com relação aos outros principais vetores de ataque, achamos interessante que, embora não sejam considerados tecnologias de acesso remoto, eles aproveitam a interconectividade como uma função habilitadora:

- **Exploração de aplicativos voltados ao público—**Que nível de conectividade ou controle é possível a partir de aplicativos expostos à Internet e que arquitetura existe para reduzir os riscos ao ICS?
- **Dispositivos acessíveis pela Internet—**A conectividade do dispositivo está contornando a DMZ?
- **Anexo de spear phishing—**O ambiente de OT devidamente configurado não deve ter acesso direto aos serviços de e-mail, porém o phishing continua a ser um vetor apresenta índices relativamente altos nessa classificação.

Uma preocupação particular são os 18% dos vetores iniciais que se aproveitam da estação de trabalho de engenharia. Essa porcentagem levanta alguma preocupação porque as estações de trabalho de engenharia representam um terreno importante para realizar uma variedade de efeitos no estágio 2 do ICS Cyber Kill Chain e pode ter contribuído para o alto número de incidentes com impacto nos processos.

Risco, impacto e exploração de componentes

Considerando esses resultados em relação aos vetores de ataque iniciais, vamos revisar a questão da percepção de risco do ponto de vista dos componentes de ICS. Não surpreendentemente, a maioria dos entrevistados concorda que os terminais – estações de trabalho de engenharia e ativos de servidor ICS – apresentam o maior risco de comprometimento. Veja a Figura 12.

Quais componentes do sistema de controle você considera com maior risco de comprometimento? ***Selecione os três primeiros em cada categoria, sem ordem específica.***

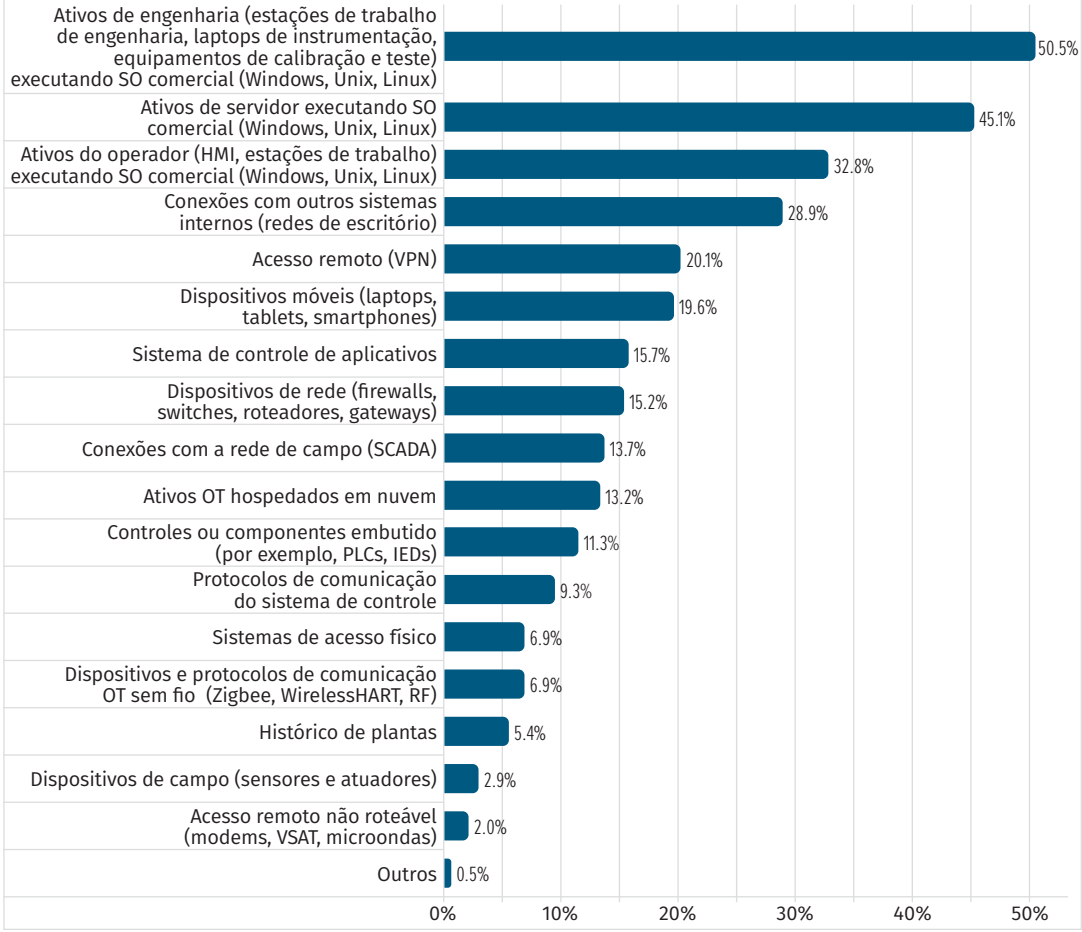

Figura 12. Risco de componente do sistema

Coletivamente, no entanto, os problemas de conectividade são responsáveis pela segunda maior preocupação de risco (ao considerar as conexões do sistema interno, o acesso remoto, as conexões à rede de campo e sem fio). Portanto, as organizações precisam se concentrar no acesso remoto e nas conexões com outras redes como uma fonte de risco. Esta avaliação de risco está de acordo com os incidentes relatados que se aproveitam do acesso remoto como um vetor inicial. No entanto, os controles de segurança aplicados atualmente não reduzem esse risco de forma adequada.

A percepção de risco se correlaciona bem com o impacto estimado nas operações de ativos fixos (terminais), mas tende a divergir quando a conectividade e a mobilidade entram em jogo. Por exemplo, as conexões com as redes internas do escritório estão em quarto lugar em risco, mas ficam em nono lugar em impacto, se forem comprometidas. Da mesma forma, os dispositivos móveis estão em sexto lugar em risco, mas em décimo primeiro em impacto, se comprometidos. Finalmente, o risco do comprometimento de controles embutidos está em décimo primeiro lugar, mas o impacto está em quarto lugar. Esse desalinhamento leva a uma abordagem sistemática para desenvolver planos integrados que levam em consideração tanto a probabilidade quanto a gravidade. Consulte a Tabela 4 na próxima página.

Por sua natureza, as vias de comunicação sem fio e não roteáveis (modems, VSAT, microondas) correm o risco de serem manipuladas por pessoal externo. Relativamente, poucas ferramentas de segurança nos permitem monitorar ou proteger essas vias de comunicação. No entanto, esses ativos recebem uma classificação de risco relativamente baixa quando se considera o fator comprometimento. Dada essa desconexão aparente, as organizações devem investir em pesquisas e inovações técnicas para aprender como proteger melhor esses ativos.

Tabela 4. Risco de componente comparado ao impacto

Componente	Classificação de Risco	Classificação de Impacto
Ativos de engenharia (estações de trabalho de engenharia, laptops de instrumentação, equipamentos de calibração e teste) executando SO comercial (Windows, Unix, Linux)	1	1
Ativos de servidor executando SO comercial (Windows, Unix, Linux)	2	2
Ativos do operador (HMI, estações de trabalho) executando SO comercial (Windows, Unix, Linux)	3	3
Conexões com outros sistemas internos (redes de escritório)	4	9
Acesso remoto (VPN)	5	8
Dispositivos móveis (laptops, tablets, smartphones)	6	11
Sistema de controle de aplicativos	7	7
Dispositivos de rede (firewalls, switches, roteadores, gateways)	8	6
Conexões com a rede de campo (SCADA)	9	5
Ativos OT hospedados em nuvem	10	10
Controles ou componentes embutido (por exemplo, PLCs, IEDs)	11	4
Protocolos de comunicação do sistema de controle	12	12
Sistemas de acesso fisico	13	14
Dispositivos e protocolos de comunicação OT sem fio (Zigbee, WirelessHART, RF)	14	16
Histórico de plantas	15	15
Dispositivos de campo (sensores e atuadores)	16	13
Acesso remoto não roteável (modems, VSAT, microondas)	17	17

Resposta ao incidente: Para quem ligar?

Os entrevistados identificam uma combinação de recursos terceirizados e internos como seus três principais recursos a serem consultados: um provedor terceirizado de soluções de cibersegurança para suporte de resposta primária, bem atrás estão os recursos internos e, em terceiro, um consultor de TI. Veja a Figura 13.

Quarenta por cento dos entrevistados indicam que utilizam um consultor de TI para apoiar seus esforços de resposta de OT. A equipe SANS ICS testemunhou isso muitas vezes, geralmente quando chamada para remediar uma tentativa falha de tratamento de uma empresa focada em resposta a incidentes de TI tradicional. Ao examinar parceiros para suporte de resposta a incidentes, certifique-se de perguntar sobre históricos de casos anteriores (anônimos) e experiência em resposta em ambientes de OT.

Quem você consulta ou recorre quando detecta sinais de uma infecção ou infiltração no seu sistema de controle de ativos cibernéticos ou na rede? ***Selecione tudo que se aplica.***

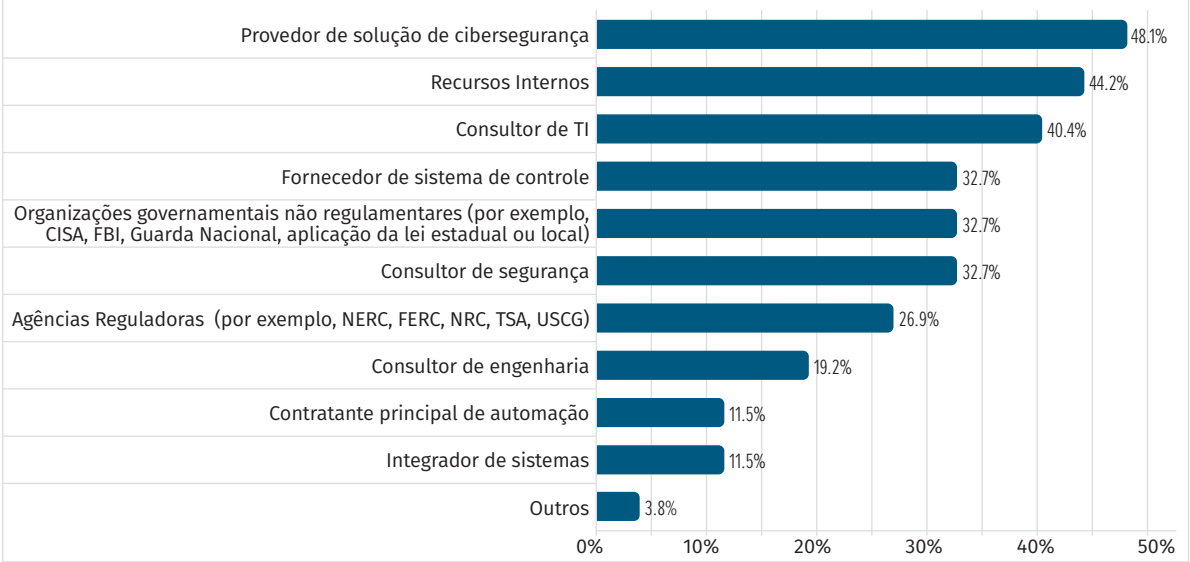

Figura 13. Organizações de Apoio à Resposta a Incidentes

Esses resultados apresentam um contraste interessante com os resultados da pesquisa de 2019. A Tabela 5 mostra uma queda acentuada na dependência de recursos internos, com o aumento para o uso de consultores de TI e provedores de soluções de cibersegurança.

Tabela 5. Tendências em Suporte à Resposta a Incidentes 2019 e 2021

Suporte à Resposta a Incidentes	2019	2021
Provedor de solução de cibersegurança	35.6%	48.1%
Recursos Internos	59.0%	44.2%
Consultor de TI	18.4%	40.4%
Fornecedor de sistema de controle	45.6%	32.7%
Organizações governamentais não regulamentares (por exemplo, CISA, FBI, Guarda Nacional, aplicação da lei estadual ou local)	40.6%	32.7%
Consultor de segurança	37.2%	32.7%
Consultor de engenharia	13.4%	19.2%
Contratante de automação principal	8.4%	11.5%
Integrador de sistemas	15.1%	11.5%
Outros	2.1%	3.8%

Defesas de hoje e Segurança de Amanhã

As organizações aproveitam uma variedade de tecnologias e soluções de segurança em seu ambiente de OT. A Tabela 6 mostra as principais soluções atuais:

1. Controles de acesso (82%)
2. Soluções de antivírus (77%)
3. Programas de avaliação/auditoria (65%)

O planejamento de investimento para soluções novas e antigas abrange os próximos 18 meses, com os principais concorrentes identificados da seguinte forma:

1. Centro de operações de segurança (SOC) para sistemas de OT/controle (37%)
2. Orquestração, automação e resposta de Segurança (SOAR) (33%)
3. Na terceira posição temos um empate de quatro soluções: IDS industrial, EDR, prevenção de perda de dados (DLP) e princípios de confiança zero (zero trust) (31%)

A Tabela 6 também compara 2019 e 2021 em termos de tecnologias em uso e planejadas. As principais tendências incluem:

Tabela 6. Soluções com mudança na taxa de adoção (2019 a 2021)

Suporte à Resposta	Mudança em uso	Mudança planejada
Controles de acesso	9.5% ▲	4.31% ▲
Anti-malware/antivirus	23.9% ▲	-3.39% ▼
Avaliação e auditoria	5.2% ▲	10.47% ▲
Identificação e gestão de ativos	8.3% ▲	4.18% ▲
Monitoramento e análise de log	6.4% ▲	1.62% ▲
Treinamento de conscientização de segurança para funcionários, contratados e fornecedores	-5.7% ▼	4.83% ▲
Verificação de vulnerabilidade	1.5% ▲	5.93% ▲
Controles de acesso de usuário e aplicativo	-4.2% ▼	4.90% ▲
Ferramentas de detecção de anomalias	19.3% ▲	0.89% ▲
Lista de comunicações permitidas	15.2% ▲	2.98% ▲
Lista de aplicações permitidas	8.2% ▲	8.78% ▲
Soluções de monitoramento de segurança de rede OT/ICS e detecção de anomalias	14.1% ▲	-8.51% ▼
Gerenciamento de configuração OT/ICS	12.7% ▲	-1.28% ▼
Controles de acesso à dispositivo e lista de permissões baseada em política	6.7% ▲	4.58% ▲
Melhorias do sistema de controle/serviços de atualização	10.9% ▲	0.88% ▲
IDS industrial	-0.9% ▼	3.89% ▲
Lista de dispositivos permitidos	5.9% ▲	-0.63% ▼
Sistemas de prevenção de intrusão industrial (IPS)	4.1% ▲	6.44% ▲
Prevenção de perda de dados (DLP)	15.1% ▲	6.36% ▲
Segmentação de rede definida por software	10.7% ▲	1.77% ▲
Gateway unidirecional entre sistemas de controle e redes de alto risco	5.5% ▲	7.54% ▲
SOC para OT/sistemas de controle	11.1% ▲	2.71% ▲
Política de orquestração baseada em identidade	5.3% ▲	6.17% ▲
Ocultação dos endereços IP de dispositivos	10.3% ▲	10.59% ▲

- **Movimento em direção a um modelo de caça de ameaças e baseado em hipóteses para OT—**Um aumento (14%) na implementação de monitoramento de segurança de rede de OT e detecção de anomalias evidencia esta tendência, bem como o crescimento de 19% no uso de ferramentas para detecção de anomalias , sinalizando uma mudança bem-vinda dos recursos de defesa baseados em indicadores tradicionais. O suporte para essa tendência também mostra aumentos na lista de permissões para comunicações, aplicativos e dispositivos, bem como controles de acesso a dispositivos e listas de permissões baseadas em políticas.

- **Investimento adicional e foco em cibersegurança, detecção e resposta de OT—**A adoção de SOC para OT aumentou drasticamente de 2019 a 2021, assim como a adoção de tecnologias de prevenção de perda de dados (DLP). Os recentes incidentes de ransomware de alto nível provavelmente contribuíram para essa tendência, assim como as intrusões cada vez mais comuns no estilo hack-and-leak. Curiosamente, os entrevistados indicam a adoção de EDR e ferramentas de análise comportamental do usuário, apesar das ofertas específicas de OT limitadas no mercado.
- **Aumento do uso de soluções anti-malware/antivírus—**A pesquisa de 2021 mostra um aumento acentuado (24%) em relação a 2019, o que pode sugerir que as defesas gerais da comunidade de OT baseadas em tecnologias de análise passiva estão acompanhando o ambiente de TI, uma tendência positiva.

Surpreendentemente, os entrevistados relataram uma baixa adoção de automação (28%), uma ironia em uma comunidade que é focada na automação de processos físicos. No entanto, 22% planejam implementar, nos próximos 18 meses, o SOAR em suas arquiteturas de defesa de OT. Como comunidade, queremos aumentar os índices de automação em segurança cibernética, para garantir que teremos uma proteção melhor com o mínimo de intervenção manual possível.

O uso de gateway unidirecional permanece relativamente constante (aumento de 6%). Com foco na indústria em tecnologias de isolamento, esperávamos uma porcentagem bem maior aqui.

As empresas em crescimento sempre precisam aumentar as capacidades existentes e atualizar a funcionalidade com novas soluções de OT. Com relação à implantação de novas tecnologias, 71% dos entrevistados consideram como obrigatório ou altamente importante pré-qualificar as posturas de segurança cibernética do fornecedor ou do provedor de soluções antes de trazer novos recursos. A maioria das organizações (65%) adota uma abordagem baseada em padrões para essas avaliações, com apenas uma minoria usando uma abordagem adhoc. Veja a Figura 14.

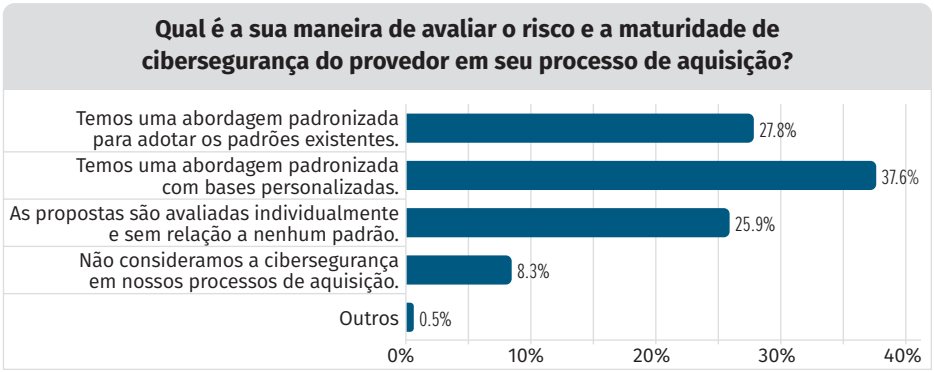

Figura 14. Processo de avaliação do fornecedor

A Indústria Vai para a Nuvem

Cada vez mais, as tecnologias e serviços nativos da nuvem impactam os ambientes de OT. Quarenta por cento dos entrevistados relataram o uso de alguns serviços baseados em nuvem para sistemas OT/ICS, com muitos usando tecnologias de nuvem para apoiar diretamente as operações ICS, bem como funções de cibersegurança (serviços NOC/SOC, BCP/DR e MSSP). Veja a Figura 15.

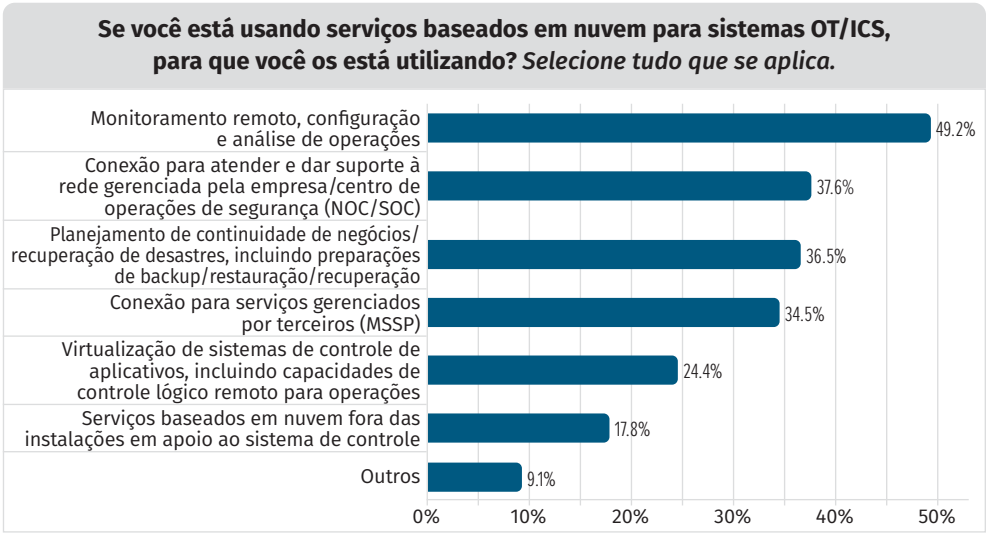

Figura 15. Uso funcional de tecnologias de nuvem

O uso de tecnologias externas para suportar a funcionalidade central do ICS representa um desenvolvimento recente na indústria. As organizações precisam estar cientes desses novos riscos potenciais, especialmente quando combinados com as recentes invasões de alto nível à cadeia de suprimentos em seus serviços de nuvem e provedores de serviços gerenciados, invasões estas realizadas por atores avançados.

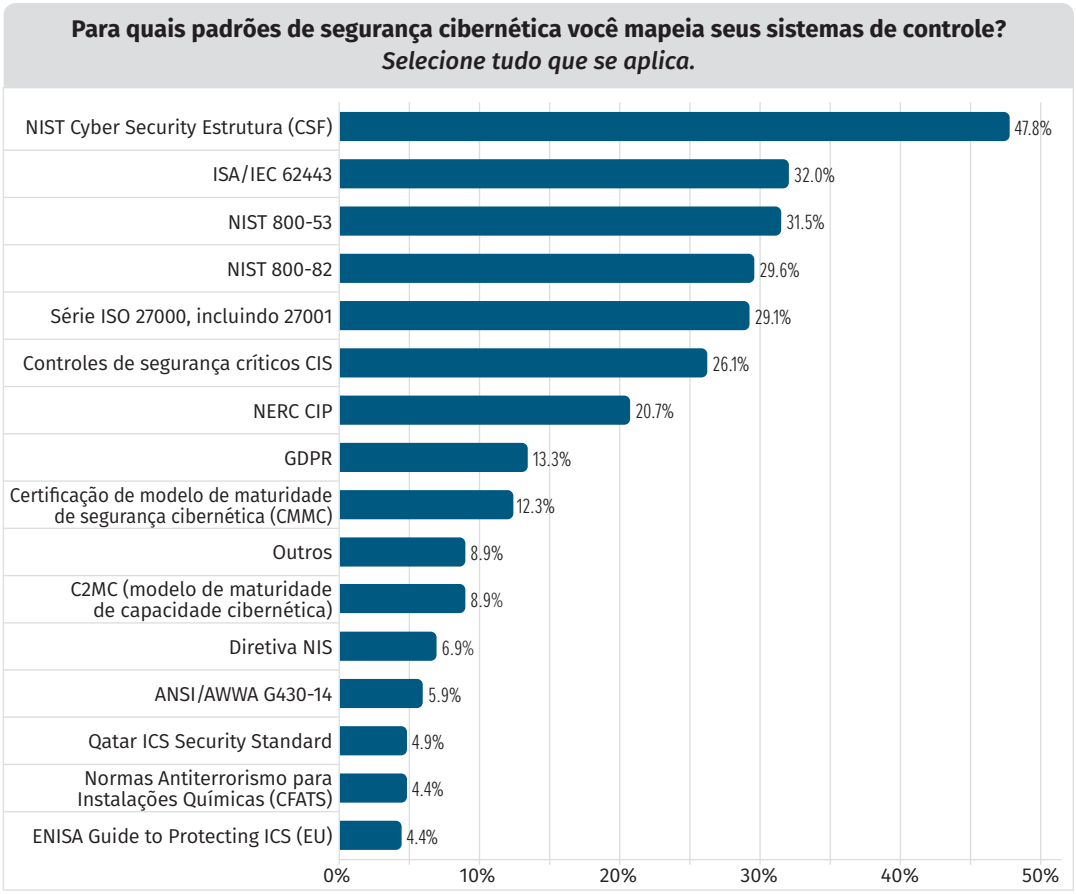

Figura 16. Uso de padrões de segurança cibernética

Estruturas e Padrões

As organizações buscam estruturas (frameworks) e padrões para ajudar a garantir uma defesa estruturada dos sistemas de controle. A maioria das organizações mapeia seus sistemas de controle para o NIST Cyber Security Framework para ajudar a apoiar e estruturar suas práticas de segurança, e com IEC 62443 como a segunda escolha mais popular. Algumas organizações também devem usar padrões específicos da indústria (por exemplo, NERC CIP) ou específicos da localidade (por exemplo, Diretiva NIS) para governar suas práticas de cibersegurança. Veja a Figura 16.

O cenário de segurança de OT mudou significativamente desde 2019 após o lançamento do framework MITRE ATT&CK® ICS[4]. Esta nova estrutura fornece um léxico comum para descrever o comportamento do adversário e as consequências em um contexto de ICS como uma extensão do ATT&CK para o modelo Enterprise[5]. Na pesquisa de 2021, 47% dos entrevistados aproveitam o MITRE ATT&CK® para ICS de alguma forma como parte de sua estrutura de segurança: 43% apenas para avaliação, 31% usando-o como parte de teste de invasão, 16% para atividade de ameaça e 11% para emulação de adversário.

[4] https://collaborate.mitre.org/attackics/index.php/Main_Page

[5] https://attack.mitre.org/

Daqueles que usam ICS ATT&CK, 50% completaram um MITRE ATT&CK® para avaliação de cobertura de ICS. A cobertura foi distribuída de maneira relativamente uniforme considerando as áreas mapeadas pelo framework, contudo o acesso inicial, o movimento lateral e a persistência foram as áreas que tiveram uma das coberturas mais abrangentes. Veja a Figura 17.

Inteligência de Ameaças

O mercado de inteligência de ameaças de ICS amadureceu nos últimos dois anos. Em 2019, várias organizações de pequeno porte forneciam inteligência de ameaças específicas de ICS. Em 2021, esse mercado se expandiu. Embora a maioria dos entrevistados ainda use inteligência de ameaças disponível publicamente, metade possui fontes (feeds) de inteligência de ameaças específicas de ICS fornecidas por empresas especializadas e dependem cada vez menos de provedores de inteligência de ameaças de TI (36%). Veja a Figura 18.

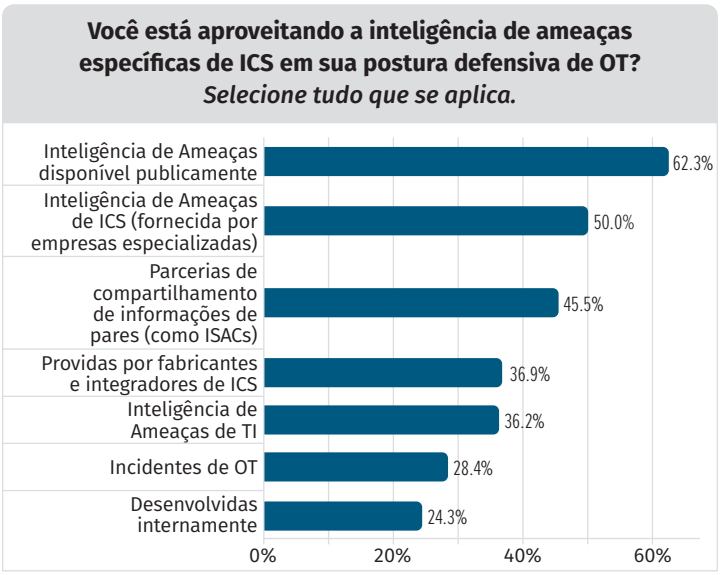

Figura 18. Fontes de Inteligência de Ameaças

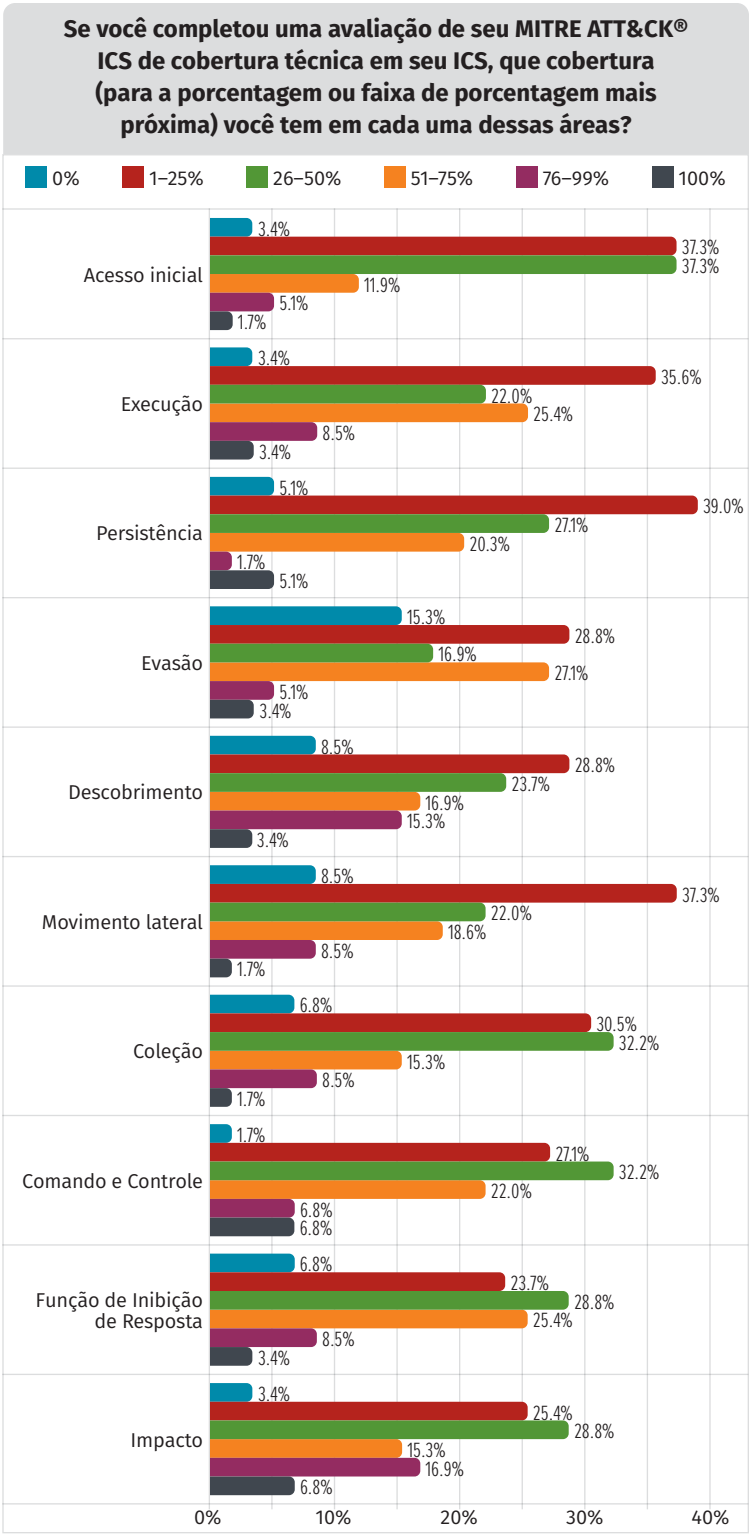

Figura 17. MITRE ATT&CK® para avaliação de cobertura ICS

Melhorando as Defesas

Monitoramento

Quase 70% dos entrevistados na pesquisa de 2021 têm um programa de monitoramento em vigor para a segurança de OT. A maior parte desse monitoramento (56%) vem da equipe de segurança de TI, que também monitora o ambiente de OT. Trinta e dois por cento dos entrevistados relataram que têm um SOC de OT dedicado para monitorar seus ativos de OT e 25% usam um MSSP de OT terceirizado para monitoramento. Com relação ao SOC de OT e MSSP de OT, 57% dos entrevistados usam um recurso de monitoramento específico do OT. Veja a Figura 19.

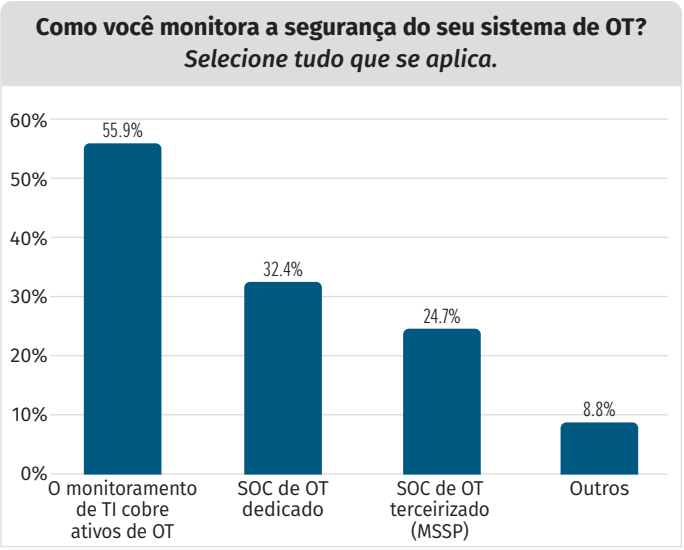

Figura 19. Monitoramento de segurança de OT

A maior parte do monitoramento da telemetria vem de dispositivos de rede ou ativos de servidor que se assemelham mais aos ativos de TI. Grande parte da telemetria de monitoramento de dispositivos específicos do ICS não parece ter uma adoção mais ampla. Apenas 24% dos entrevistados correlacionam dados de seu histórico de processos com seus dados de segurança cibernética. Correlacionar os dados cibernéticos relevantes com os dados do processo é um aspecto crítico da investigação do incidente cibernético de OT, especialmente quando esse incidente tem um impacto no processo (consulte a Figura 20). Sem comparar esses conjuntos de dados, identificar a(s) causa(s) raiz torna-se mais desafiador; mesmo assim, poucas soluções no mercado facilitam essa correlação.

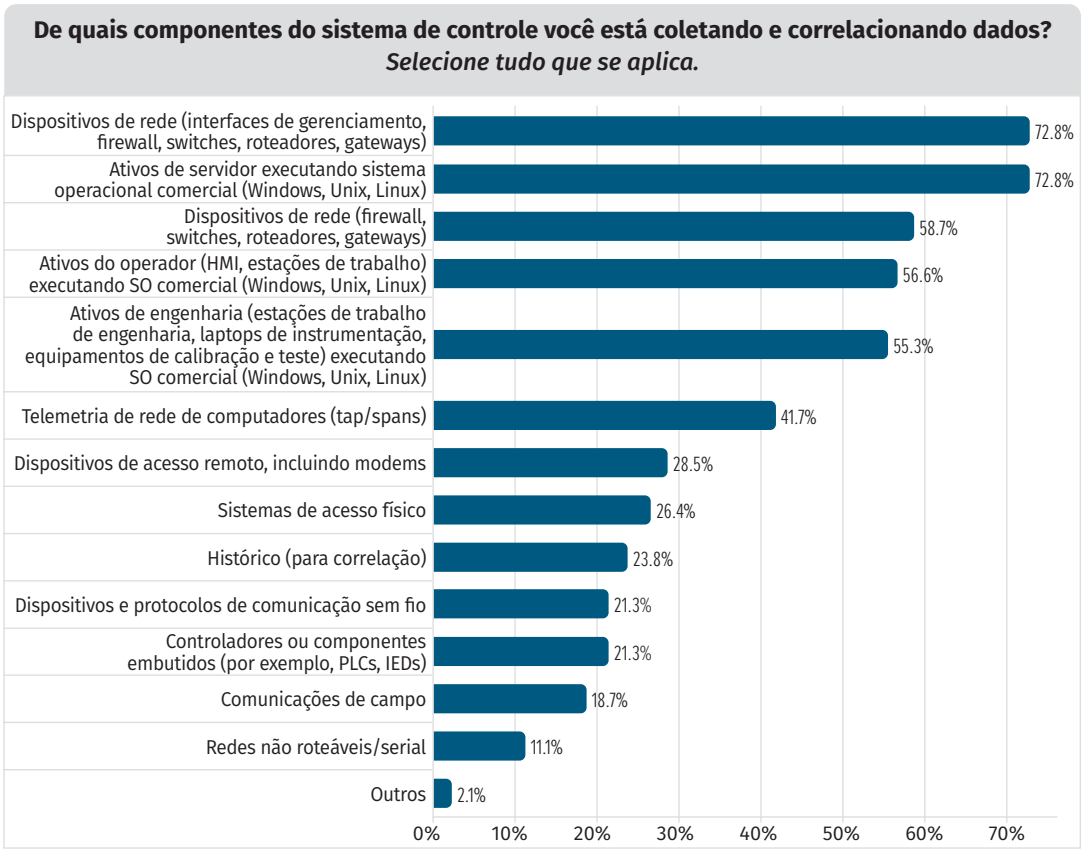

Figura 20. Fontes de monitoramento de OT

Embora as organizações monitorem a maioria dos ativos, muito desse monitoramento ainda depende de detecções e assinaturas automatizadas, como AV e IDS, para identificar os riscos ativos. Uma parte significativa dos entrevistados também usa uma metodologia de caça a ameaças (35%) ou detecções baseadas

em anomalias (30%) para pesquisar ameaças ativas em seus ambientes de OT. Vinte e quatro por cento não têm um processo formal de caça a ameaças e 17% não procuram por ameaças em seus ambientes de OT (indicando algumas áreas para a adoção de melhorias). Veja a Figura 21.

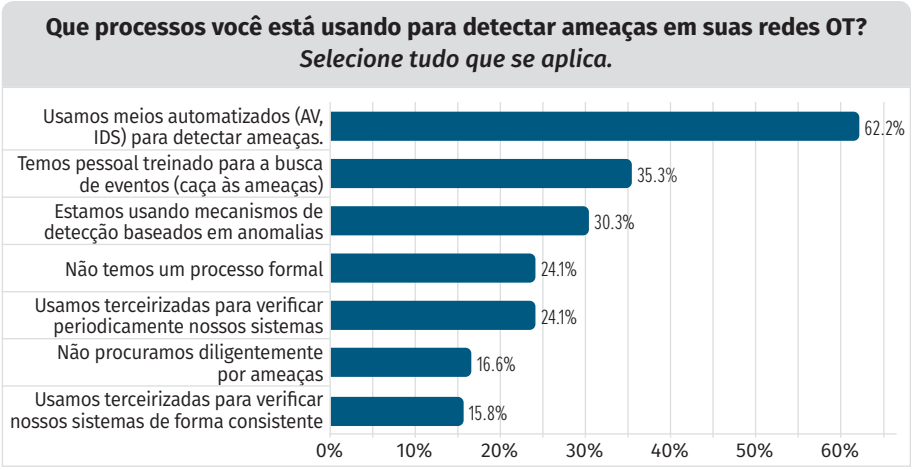

Figura 21. Metodologia de Análise de Segurança OT

Inventário de Ativos

Sem um conhecimento sólido dos ativos em sua rede de ICS, você não pode desenvolver e implementar uma estratégia para gerenciar riscos e garantir operações confiáveis. Embora a maioria dos entrevistados (58%) indique que sua organização tem um programa formal para inventariar ativos de OT, devemos trabalhar mais para ter uma maior adoção desta etapa fundamental.[6] A pesquisa não cobriu as metodologias usadas para desenvolver o inventário de ativos, nem foi perguntado quais mudanças na alocação de recursos financiam esse trabalho.

Dos ativos que compõem uma rede de OT, os servidores e dispositivos de ICS foram os ativos mais inventariados no ambiente, com 29% e 22% dos entrevistados indicando que tinham 100% de cobertura, respectivamente. O monitoramento desses ativos, no entanto, apresentou um atraso de 7% para cada categoria, indicando que mesmo em ambientes bem inventariados, o monitoramento dos ativos conhecidos continua sendo um desafio. Os ativos e aplicativos de software ficaram significativamente para trás nas categorias de inventário e monitoramento. Veja a Figura 22.

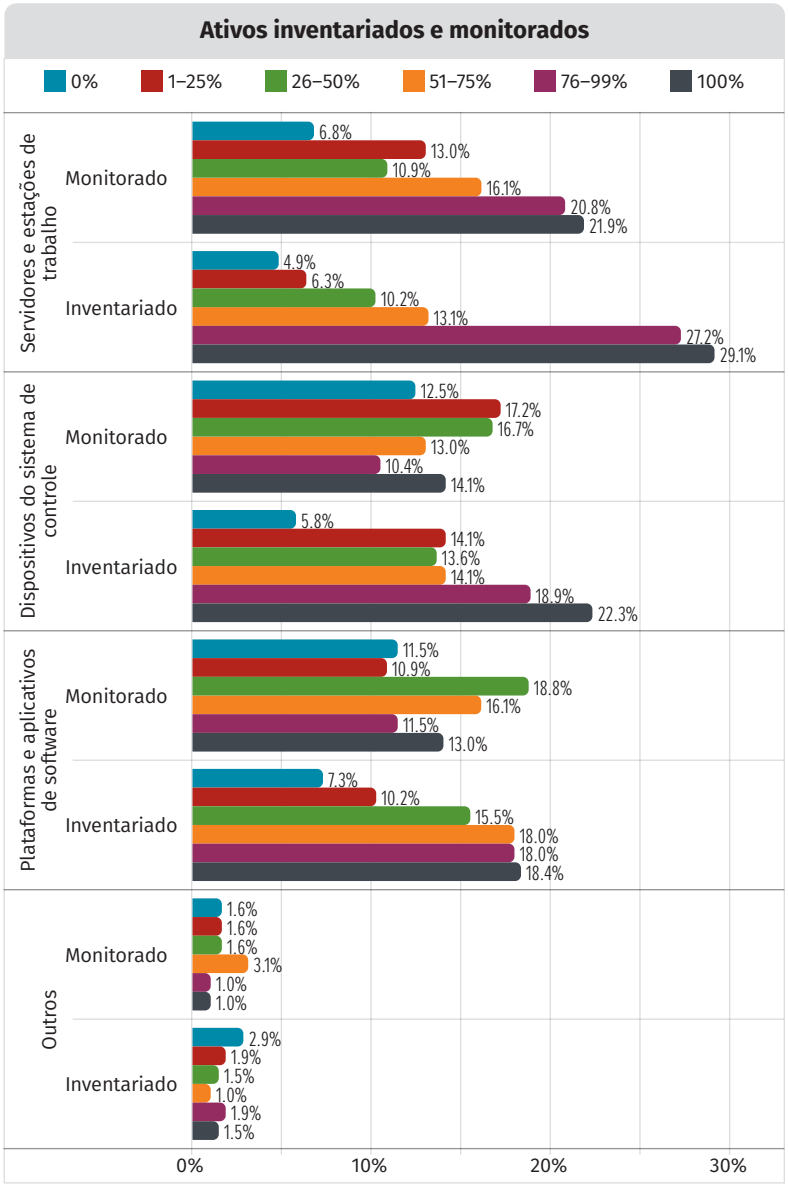

Figura 21. Metodologia de Análise de Segurança OT

Inventários de Conexão

Semelhante aos resultados de inventário de ativos, apenas 57% dos entrevistados documentaram todas as conexões de saída do ambiente de OT, contra 62% em 2019. Esta diminuição talvez resulte de os entrevistados compreenderem melhor a complexidade das redes ICS e sendo, portanto, menos inclinados a indicar que tinham todas as conexões documentadas. Essa tendência continua preocupante e provavelmente contribui para a prevalência de incidentes relacionados à conectividade.

[6] Você pode encontrar informações adicionais sobre os estoques de ativos do ICS no whitepaper SANS "ICS Asset Identification: It's More Than Just Security", de Mark Bristow, www.sans.org/white-papers/39650/

Uma vez que uma organização tem um limite bem definido e é responsável por todas as vias de comunicação, as organizações precisam avaliar como elas protegem essas comunicações. Como em 2019, a maioria dos entrevistados relata o uso de uma DMZ entre a rede de OT e a rede corporativa para separar as comunicações. A porcentagem de entrevistados nesta categoria, no entanto, caiu de 57% em 2019 para 49% em 2021.

Os especialistas em segurança consideram ter uma DMZ entre a rede de OT e a rede corporativa uma prática recomendada se a conectividade for necessária. Em 2019, 28% dos participantes da pesquisa relataram ter sistemas 100% isolados. Em 2021, esse número cai para 8%. Vários fatores podem ter influenciado essa queda; talvez dados mais abrangentes tenham se tornado disponíveis, indicando a conectividade onde antes se supunha que não existia, ou talvez as organizações tenham adotado tecnologias adicionais baseadas em nuvem que precisam de comunicações. Na pesquisa de 2021, 42% indicam que seus sistemas de controle tinham conectividade direta com a internet contra uma taxa de 12% em 2019. Mais uma vez, essa mudança pode resultar de uma melhor compreensão dos canais de comunicação, em oposição a uma mudança na conectividade real para a internet.

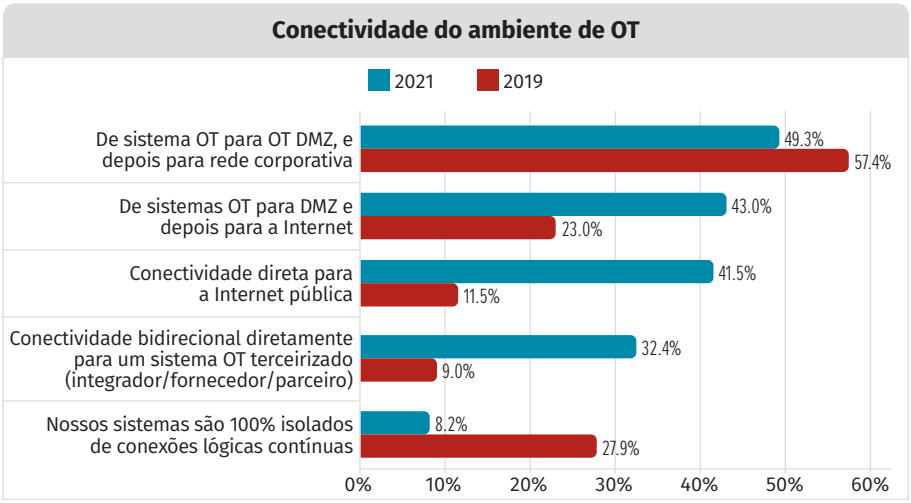

Figura 23. Conectividade do ambiente de OT para redes externas

Porém essa tendência permanece preocupante. Vinte e seis por cento relatam apenas a conectividade de saída com a internet, com minúcias adicionais sobre detalhes de verificação indisponíveis. Veja a Figura 23.

Os métodos de conectividade também representam um indicador importante no sistema de segurança em geral. Os circuitos dedicados e os mecanismos de comunicação naturalmente oferecem mais segurança (exigindo acesso físico ao meio) do que comunicações alugadas, por satélite ou sem fio. Com base nas respostas desta pergunta, as organizações usam uma ampla variedade de tecnologias da Camada 1 do Modelo OSI para mover dados para dentro e para fora de suas redes de controle. A maioria usa fibra dedicada ou alugada, mas muitos usam sistemas de Internet pública (cabo, DSL) ou tecnologias parecidas. E Sete por cento relatam que ainda usam comunicações dial-up. Veja a Figura 24.

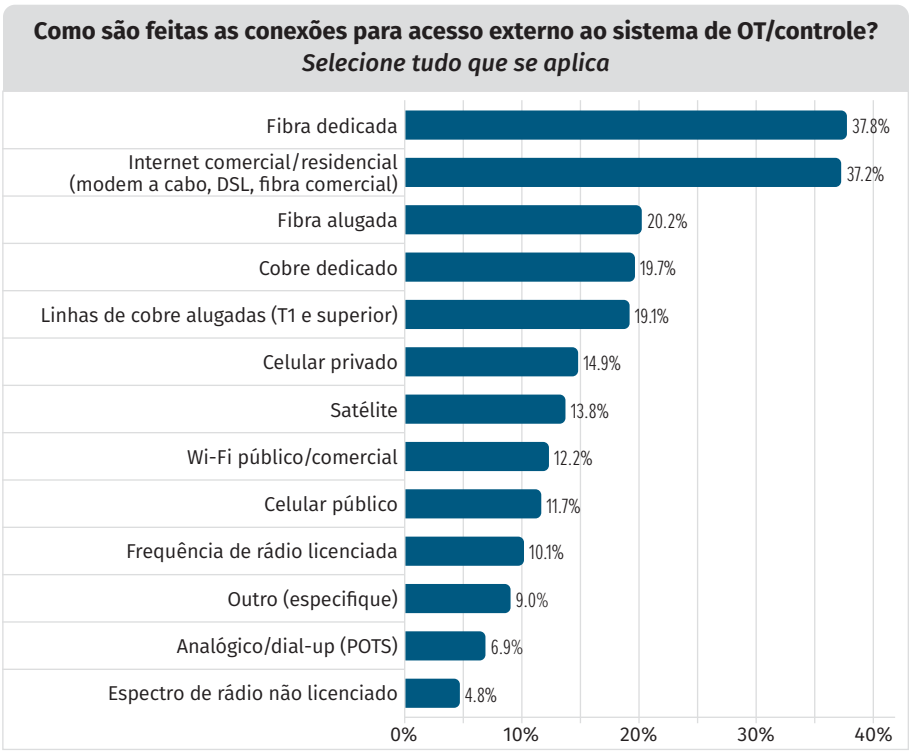

Figura 24. Meios de conexão OT

Avaliando e Corrigindo Vulnerabilidades

As organizações fizeram grandes melhorias em relação às avaliações de ambientes de ICS. Trinta por cento dos entrevistados implementaram um programa de avaliação contínua e 76% fizeram uma avaliação no ano passado, com apenas 10% dos entrevistados que nunca fizeram uma avaliação da rede do sistema de controle.

Para aqueles que estão concluindo as avaliações, a maioria aproveita os recursos com a técnica específica de OT – um testemunho do amadurecimento de ofertas robustas de avaliações de segurança de OT. Veja a Figura 25.

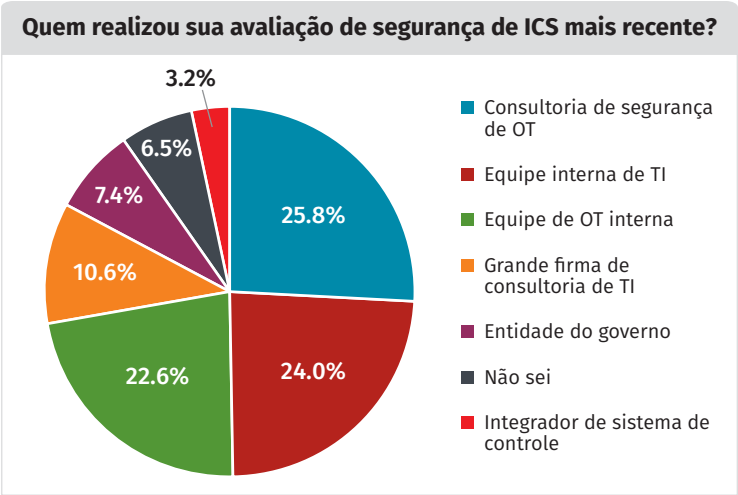

Figura 25. Assessores de segurança

Depois de realizar uma avaliação, as organizações precisam identificar vulnerabilidades em seus ambientes de sistema de controle. Para isso, os entrevistados que responderam aproveitam esses processos para detectar vulnerabilidades em seus sistemas. A maioria (61%) usa avisos públicos de vulnerabilidades assim que as informações se tornam disponíveis. Veja a Figura 26.

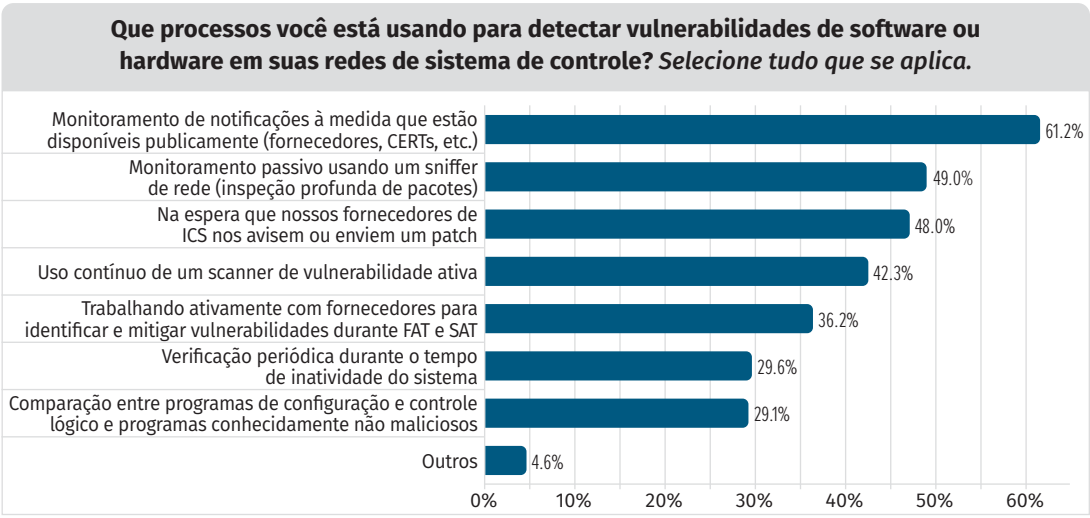

Figura 26. Fontes de dados de vulnerabilidade

O SANS foi motivado a ver alguns desenvolvimentos:

- Forte adoção (42%) de tecnologias de varredura de vulnerabilidade ativas, historicamente consideradas arriscadas ambientes de controle antigos. Essa adoção indica confiança adicional dos proprietários de ativos em relação à implementação dessas tecnologias em um ambiente de ICS moderno.
- Adoção mais ampla (36%) de organizações aproveitando oportunidades para descobrir vulnerabilidades em testes de aceitação de fábrica (FAT) e testes de aceitação de local (SAT) para mitigar os riscos antes que eles sejam colocados em campo.
- Aproximadamente 30% usam configurações conhecidamente boas combinadas com as configurações e lógica atuais para validar que os processos sejam executados conforme o esperado.

Depois de identificar as vulnerabilidades, a maioria usa um plano de mitigação para reduzir o risco, com apenas 6% não tomando nenhuma ação. Veja a Figura 27.

Até recentemente, a maioria dos ambientes de processo não podia aplicar patches continuamente. Consequentemente, os 16% dos entrevistados que aplicam patches continuamente representam um ótimo sinal da melhoria na confiabilidade nos ciclos de gerenciamento de patches do ICS. Os entrevistados do setor de energia foram os mais propensos a ter um ciclo de patch contínuo, mas também mais propensos a não corrigir a vulnerabilidade (demonstrando um paradoxo).

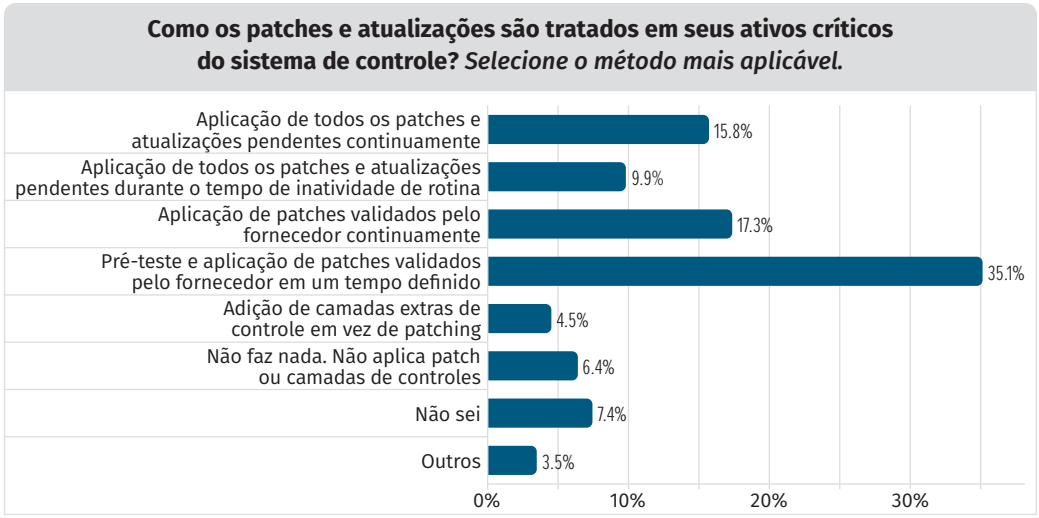

Figura 27. Métodos de correção de vulnerabilidade

Pessoas Motivam Processos

Junto com a tecnologia, pessoas e processos representam elementos críticos de um programa robusto de cibersegurança de ICS. A liderança que entende de ICS é fundamental.

Trinta e seis por cento dos entrevistados indicam que o CISO define a política de segurança de ICS. Apenas 8% dos entrevistados relataram que essas políticas derivam do nível da fábrica, e o diretor de tecnologia (CTO) é classificado como o segundo diretor corporativo mais alto definindo política. Veja a Figura 28.

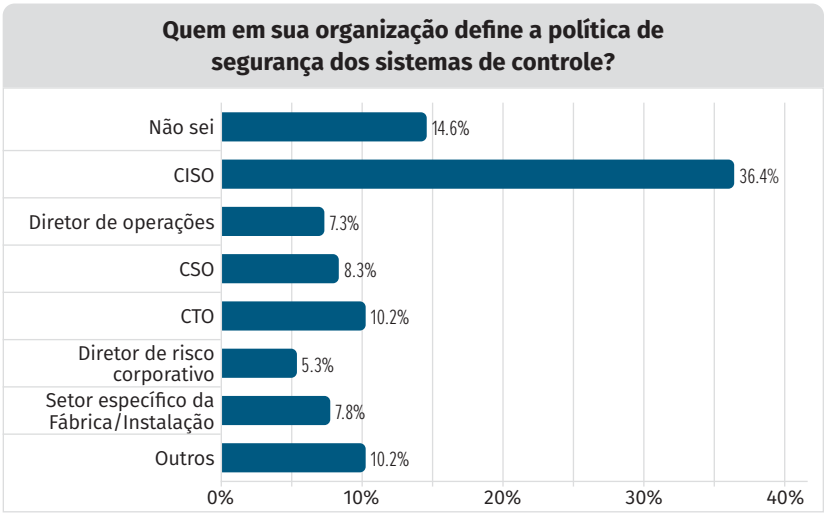

Figura 28. Responsabilidade da Política de Segurança

A implementação, no entanto, permanece em grande parte nas mãos da gestão de TI (39%), embora 35% indique que o CISO tem uma função de "mão na massa" na implementação dos processos e estratégias que eles definem para a organização. Veja a Figura 29.

Como OT e TI geralmente têm filosofias diferentes, a distinção entre política e implementação pode ter implicações significativas. Então, para criar uma equipe sólida de segurança deICS, as organizações precisam continuar priorizando as comunicações, divulgação e educação entre os dois grupos.

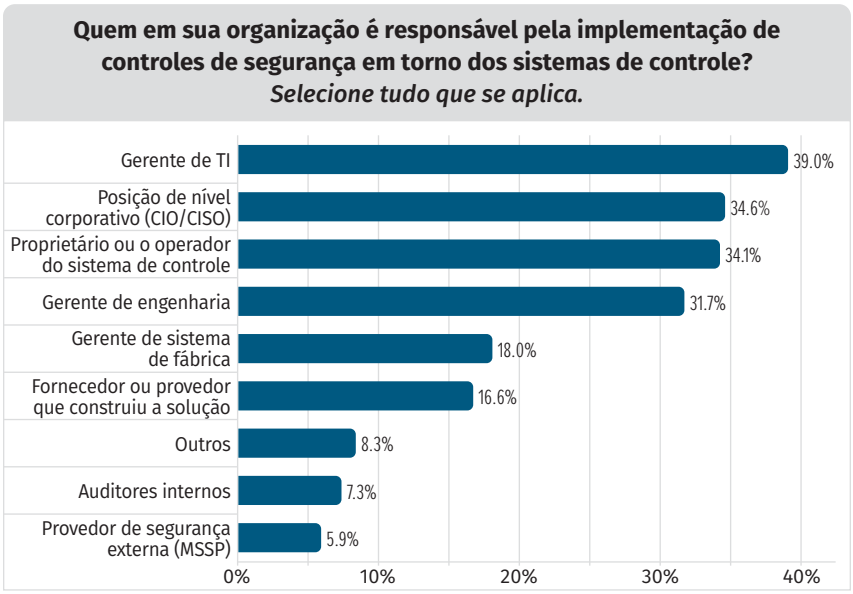

Figura 29. Implementação do controle de segurança

Para Onde Vamos Daqui?

A defesa eficaz dos ambientes de OT requer uma estratégia multifacetada e integrada que considere os riscos internos e externos, que entenda a vulnerabilidade desses riscos e priorize as medidas de mitigação por meio de pessoas, processos e tecnologia para gerenciar os riscos identificados. Essa abordagem requer uma compreensão sólida da situação entre entidades semelhantes e parcerias-chave internamente, especialmente com equipes de segurança de TI e com colegas em outras organizações.

As lacunas e desafios que a comunidade ICS precisa abordar incluem:

- Melhor compreensão do cenário de ameaças, com compartilhamento aprimorado de incidentes para aperfeiçoar a defesa coletiva
- Compreender os impactos de incidentes relacionados ao processo
- Correlacionando a telemetria de controle de processo com a telemetria de cibersegurança para análise de causa raiz
- Atender aos atuais fundamentos de higiene de segurança de ICS – identificação de ativos aprimorados e gerenciamento de conectividade
- Melhorar a visibilidade do endpoint OT/ICS conforme as tecnologias-chave continuam a amadurecer

A comunidade de ICS enfrenta um ponto de inflexão. Continuamos a ver o crescimento de investimentos e de resultados dos esforços de segurança de OT, mas os fatores de risco não permanecem estáticos. A segurança da OT domina a conversa cibernética nacional de maneiras nunca imaginadas. Embora a comunidade de segurança ICS/OT tenha feito grandes avanços, ainda temos muito trabalho pela frente.

Sobre o Autor

Mark Bristow, um instrutor do SANS para ICS515: ICS Active Defense e Incident Response, é um membro ativo da comunidade de segurança cibernética ICS em nível de operações e de política. Mark é apaixonado em fazer crescer o "exército de pessoas inteligentes em cibersegurança do ICS" e em ajudar a defender os sistemas essenciais que sustentam a vida moderna. Ao longo de sua carreira, Mark esteve na linha de frente dos esforços de resposta a incidentes que ocuparam as manchetes, como o ataque à rede elétrica ucraniana, invasões na infraestrutura eleitoral dos Estados Unidos e tentativas russas de obter acesso à rede elétrica dos Estados Unidos. Mark é bacharel em engenharia da computação pela Pennsylvania State University e atualmente trabalha para a Cybersecurity and Infrastructure Security Agency, que faz parte do Departamento de Segurança Interna dos EUA.

Mark gostaria de agradecer a Lindsey Cerkovnik, Jason Dely e Dean Parsons por suas contribuições e revisão por pares deste artigo.

Patrocinadores

SANS gostaria de agradecer aos patrocinadores deste artigo: