Relatório Anual 2022: Segurança Cibernética para os Sistemas de Controle Industrial (ICS)

Novembro de 2022

Mensagem do Presidente

Caros colegas,

Aqui estamos e mais um ano atípico se passou. Todos temos enfrentado desafios compartilhados significativos em todo o mundo e, embora certamente não se limite à segurança cibernética, sabemos que ainda temos muito trabalho a fazer para proteger nossa sociedade moderna e conectada.

Em nome do incansável comitê diretor do relatório anual (CS)²AI, tenho o orgulho de apresentar o segundo **Relatório Anual de Segurança Cibernética do Sistema de Controle 2022 (CS)²AI -KPMG**. Este relatório é o resultado da participação significativa de nossa parceira de aliança estratégica, a KPMG, a quem devemos um sincero "obrigado" por ajudar a dar vida a isso. Devemos também agradecer à Fortinet, à Waterfall Security Solutions e a muitos parceiros de apoio (consulte a página 57) e ao comitê diretor (páginas 54–55) por suas importantes contribuições desde a fase de pesquisa até o relatório final. Por meio de seu apoio direto ao (CS)²AI e a esse projeto conjunto, tais empresas e indivíduos continuam demonstrando seu compromisso em ajudar a resolver os desafios que a força de trabalho de segurança cibernética dos sistemas de controle enfrenta hoje.

O relatório foi baseado nos resultados da pesquisa de mais de 580 membros da indústria em geral e uma amostra representativa da associação mundial da **(CS)²AI** (aproximando-se de 25.000 membros da comunidade hoje), com perguntas sobre eventos de segurança do sistema de controle, tendências em atividades de ataque e proteção tecnológicas e como as organizações estão priorizando seus esforços para enfrentar esse desafio.

A maioria de nós não pode "fazer tudo" e precisa escolher sabiamente para onde vai o nosso foco. O objetivo dest relatório anual é dar aos indivíduos uma visão mais clara do que seus pares estão fazendo e servir como uma ferramenta de apoio anual para as muitas decisões difíceis que sabemos que estão sendo tomadas.

Boa sorte!

Espero sinceramente que muitos considerem este relatório valioso e agradecemos *feedback* de todos os tipos. Embora todos nós adoraríamos ouvir coisas positivas, a crítica construtiva também é um ingrediente necessário para tornar esse recurso o melhor possível. Para *feedback* ou se você quiser se envolver no projeto do relatório de 2023 ou em qualquer uma de nossas iniciativas, envie-nos uma mensagem para **GetInvolved@cs2ai.org**

Derek Harp
Fundador e Presidente
(CS)2 AI

Relatório anual
Prefácio do patrocinador titular

Desafios significativos continuam a impactar a segurança cibernética na indústria e, à medida que a frequência e a sofisticação das ameaças aumentam, as empresas devem mobilizar seus recursos e conhecimentos de maneiras novas e ousadas de se proteger.

De fato, foi um ano alarmante para a segurança cibernética OT em meio a ataques de alto perfil que dominaram as manchetes internacionais, incluindo o Colonial Pipeline, a instalação de água Oldsmar e os casos de *ransomware* da JBS Foods, para citar apenas alguns.

Vimos muitas empresas, em resposta, se apressarem para revisar e remediar seus ambientes de OT — normalmente dedicando alguns investimentos, talentos e tecnologia necessários para soluções imediatas enquanto trabalham para manter suas operações críticas e agilidade. O foco aprimorado na segurança OT inclui uma lente particularmente nítida sobre a crescente ameaça do *ransomware* em meio ao seu potencial alarmante de interromper ambientes OT sensíveis e alvos industriais.

Enquanto o ransomware e outras ameaças cibernéticas estão ganhando força, as empresas também estão voltando sua atenção para incidentes e ameaças potenciais entre atores estatais. Embora os entrevistados de nossa pesquisa citem *"insiders negligentes"* como o ator de ameaça mais comum em comprometimentos de segurança do sistema de controle, os ataques patrocinados pelo estado também se tornaram uma preocupação significativa.

Conforme observado, essas tendências perturbadoras estão levando mais empresas a continuar sua busca por novos investimentos em programas de segurança cibernética de OT que possam ajudá-los a combater os adversários persistentes e cada vez mais agressivos de hoje. Mas o investimento geral para proteger a infraestrutura de OT está mostrando evidências de restrições orçamentárias.

A maioria dos entrevistados relatou um aumento no orçamento de cerca de 10%, abaixo dos aproximadamente 30% em nossa pesquisa anterior, enquanto 10% das empresas relataram uma redução no orçamento, em comparação com cerca de 1% no ano anterior.

Enquanto isso, os obstáculos ao verdadeiro progresso permanecem na área de conhecimento e experiência, conforme revelado na pesquisa. Cerca de metade dos entrevistados (49,1 %) citou "experiência insuficiente em segurança cibernética do sistema de controle" como o maior obstáculo para reduzir a superfície de ataque cibernético do sistema de controle, enquanto mais de um terço também citou "pessoal insuficiente".

Falta, também, treinamento em meio a uma tendência à terceirização de terceiros, que está fornecendo soluções limitadas, pois as empresas de serviços também lutam com a escassez de pessoal e habilidades em meio à interrupção do fornecimento de mão de obra da pandemia global. Embora as organizações estejam combinando conhecimentos internos limitados com pessoal terceirizado para resolver os desafios atuais, é importante observar que os serviços gerenciados ainda não são uma aposta certa no espaço de OT, com poucas ofertas de serviços SOC, por exemplo, projetadas adequadamente para as complexidades de necessidades críticas de Cibersegurança de OT de hoje.

Isso nos traz de volta à inevitável — e cada vez mais urgente — necessidade de treinamento interno. A boa notícia aqui é que algumas empresas estão realmente progredindo em meio à falta geral de investimento nessa área crucial, com uma variedade de métodos de treinamento sendo usados. Embora as organizações de menor maturidade ainda dependam de programas tradicionais baseados em computador e conduzidos por instrutores, vemos jogadores mais maduros se voltando para exercícios de simulação de incidentes de mesa "ao vivo". Em última análise, isso permite que eles passem da simples compreensão da segurança de OT para a compreensão de quão bem preparados estão para gerenciar o cenário de ameaças em expansão de hoje.

Essa tendência fala da necessidade crítica de treinamento de "conscientização de segurança". Ao contrário do treinamento de segurança — desenvolvendo as habilidades e as capacidades de profissionais de segurança especializados — o treinamento de conscientização de segurança visa melhorar a cultura de segurança em toda a organização, permitindo que todos os funcionários reconheçam seu papel na redução de exposições a riscos. Enquanto o progresso está se desenrolando, no entanto, ainda vemos quase uma em cada cinco organizações (18%) sem treinamento de conscientização de segurança cibernética. Isso é preocupante quando você considera a alta ameaça de incidentes de *"insider negligente"* que podem envolver algo tão simples quanto um funcionário desinformado clicando em um *link* de *e-mail* perigoso.

Quanto ao estado atual do planejamento organizacional, é encorajador observar que mais de 85% das organizações dizem ter planos de gerenciamento/resposta em algum estágio de desenvolvimento. E, embora as porcentagens de implementação e teste permaneçam baixas, isso ainda é uma melhoria significativa em relação a 2020, quando 18% a 27% nem tinham esse planejamento em vigor.

Como mostra a pesquisa abrangente mais recente, ainda há um terreno considerável a ser coberto no ambiente perigoso de hoje, à medida que o cenário de ameaças cresce e o ritmo das mudanças acelera. Um maior senso de urgência tornou-se crítico e a necessidade de profissionais de segurança de OT altamente qualificados não pode ser exagerada. O verdadeiro progresso exigirá um ato de equilíbrio estratégico que gerencie custos, disponibilidade do sistema e medidas modernas para combater as ameaças crescentes de hoje — e acreditamos que não há tempo a perder.

Walter Risi
Líder Global de Cyber IoT,
KPMG da Argentina

Conteúdo

Sumário executivo

Este relatório é o mais recente de uma série de projetos anuais, elaborados a partir de pesquisas em andamento pela Control System Cyber Security Association International [(CS)² AI] e sua comunidade de membros e Parceiros de Aliança Estratégica (SAPs). Com base em décadas de desenvolvimento, pesquisa e análise de pesquisas de segurança do Sistema de Controle (CS) liderada pelo fundador e presidente da (CS)² AI Derek Harp e cofundador e presidente Bengt Gregory-Brown, a equipe da (CS)² AI convidou a participação de nossos mais de 24.000 membros globais e milhares de outros em nossa comunidade estendida. Fizemos a eles perguntas importantes sobre suas experiências nas linhas de frente de operação, proteção e defesa de sistemas e ativos de Tecnologia Operacional (OT) que custam de milhões a bilhões em desembolsos de capital, impactando tanto ou mais nas receitas contínuas e afetando a vida diária e operações comerciais de empresas em todo o mundo. Mais de 580 deles responderam à nossa pesquisa primária e muitos outros participaram de várias ferramentas secundárias de coleta de dados que executamos periodicamente.

Esse conjunto de dados, enviado anonimamente para garantir a exclusão de políticas organizacionais e influências de fornecedores, ofereceu *insights* sobre as realidades enfrentadas por indivíduos e organizações responsáveis por operações e ativos de CS/OT além do que poderia caber neste relatório. Esperamos que os detalhes que selecionamos para incluir atendam à necessidade de suporte à decisão que nos propusemos a responder.

Objetivo do projeto

O (CS)² AI-KPMG Control System Cyber Security Report Steering Committee lançou o projeto para coletar, analisar e relatar dados de profissionais que trabalham em segurança cibernética de sistemas de controle no primeiro semestre de 2021, com o objetivo de produzir outro em nossa série de ferramentas informativas de tomada de decisão para todos os envolvidos com este trabalho, sejam usuários finais, sejam fornecedores, líderes ou operacionais.

Para coletar nossos dados, convidamos a participação no componente de pesquisa por meio de uma ampla variedade de canais de transmissão e diretos, visando todas as partes envolvidas ativamente na segurança cibernética dos Sistemas de Controle. Nossos entrevistados incluíram profissionais em todos os níveis organizacionais: especialistas em segurança cibernética e especialistas no assunto (SMEs), bem como aqueles cujo trabalho inclui — mas não consiste necessariamente em — apenas proteger sistemas de controle.

Este Relatório usa o termo abrangente "Sistemas de Controle" para se referir a qualquer/todos os sistemas que gerenciam, monitoram e/ou controlam dispositivos e processos físicos. CS ou (CS) deve ser considerado para incluir Sistemas de Controle Industrial (ICS), Controle de Supervisão e Aquisição de Dados (SCADA), Sistemas de Controle de Processo (PCS), Domínios de Controle de Processo (PCD), Controle de Edifício/Instalação, Automação e Sistemas de Gerenciamento (BACS/ BAMS/FRCS…), dispositivos médicos conectados à rede etc.

Da mesma forma, o termo (CS)² refere-se a campo, profissão e força de trabalho da Segurança Cibernética do Sistema de Controle.

Principais destaques

Os entrevistados de organizações que se identificaram como tendo programas de segurança cibernética do sistema de controle de maturidade mais alta ("Alta M") se destacaram daqueles em organizações de Baixa M de várias maneiras. De particular interesse, os participantes de Alta M têm:

- Quase duas vezes mais probabilidade de incluir a conformidade com IEC62443-4-1 em suas avaliações de risco de pré-aquisição de produtos/serviços do sistema de controle (**34,8%** Alta M vs. **17,6%** Baixa M).
- Mais que o dobro da probabilidade de usar equipes de segurança interna sob CISO/CSO/CTO (**49,3%** vs. **21,4%**).
- Quase quatro vezes mais probabilidade de alavancar os serviços de segurança do sistema de controle gerenciado (**44,3%** Alta M vs. **12,8%** Baixa M).
- Quase três vezes mais probabilidade de ter implementado o monitoramento de rede de todas as atividades de rede do sistema de controle (**35,7%** Alta M vs. **13%** Baixa M) e planejar aumentar o grau desse monitoramento nos próximos 18 meses (**17,1%** Alta M vs. **6,5%** Baixa M).
- Mais do que o dobro de probabilidade de monitorar continuamente todos os dispositivos, usuários e aplicativos em suas redes (**27,5%** Alta M vs. **12,5%** Baixa M).

Metodologia de pesquisa

A Pesquisa e Relatório de Segurança Cibernética do Sistema de Controle (CS)^2 AI-KPMG foi um esforço colaborativo das seguintes entidades:

- **(CS)^{2}AI:** como criadora do projeto, a (CS^2 AI ocupou o papel principal no desenvolvimento, na liderança e na implementação do projeto, incluindo a produção da entrega do projeto de autoria deste relatório.
- **KPMG:** omo patrocinadora do projeto de título, a KPMG forneceu suporte primário na forma de financiamento e recursos humanos e organizacionais para aumentar as próprias capacidades da (CS)^{2}AI.
- **Patrocinadores adicionais:** patrocinadores não titulares forneceram financiamento adicional e recursos humanos e organizacionais sempre que possível (consulte o Apêndice D: Patrocinadores de relatórios).

De acordo com os objetivos do projeto declarados acima, a (CS)^{2}AI e os patrocinadores do projeto distribuíram várias pesquisas *on-line* para membros do CS/OT que trabalham em campo durante o segundo e terceiro trimestres de 2021, coletando dados importantes sobre eventos, atividades e tecnologias de CS, bem como sobre como as organizações estão respondendo aos desenvolvimentos em andamento no threatscape1. A (CS)^{2}AI convidou seus membros associados, conhecidos defensores e pesquisadores de segurança de OT a participar, distribuiu a pesquisa por meio de vários canais de mídia social e a promoveu em sites que atendem à força de trabalho de segurança cibernética da CS, com a intenção de coletar uma amostra tão ampla quanto possível. Os entrevistados se autosselecionaram, afirmando seu envolvimento com a área de CS Cyber Security.

A capacidade de analisar nossos participantes em diferentes grupos e considerar suas respostas à luz de suas associações de grupo é fundamental para os *insights* derivados deste projeto de pesquisa anual. Em nossa opinião, a maturidade do programa de segurança cibernética do sistema de controle dos participantes da pesquisa é a dimensão mais importante. Pedimos a cada participante que escolhesse qual dos seguintes descritores melhor se adequava à situação em sua organização.

[1] Threatscape: a soma de todas as ameaças possíveis às operações e ativos de CS/OT. O cenário de ameaças é dinâmico, mudando continuamente à medida que as vulnerabilidades são descobertas e as proteções são desenvolvidas para combater sua exploração.

Nível 1 — Combate a incêndios. Os processos de segurança cibernética são desorganizados e não documentados, não organizados em um "programa". O sucesso depende de esforços individuais; não é repetível ou escalável porque os processos não são suficientemente definidos e documentados. Defesa passiva.

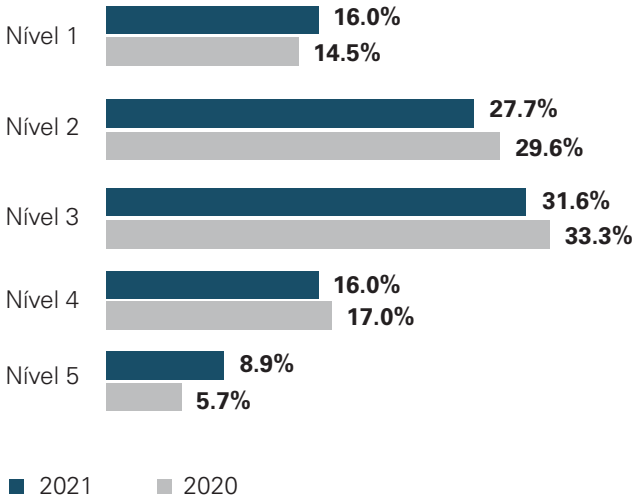
Nível 2 — As práticas básicas de gerenciamento de projetos são seguidas nas implementações de segurança cibernética; o sucesso continua a exigir pessoas-chave, mas um corpo de conhecimento está se desenvolvendo. As melhores práticas são executadas, mas podem ser *ad hoc*. Defesa passiva.

Nível 3 — A segurança cibernética produz e funciona a partir de processos e procedimentos documentados. As principais partes interessadas são identificadas e envolvidas. Recursos adequados são fornecidos para apoiar o processo (pessoas, financiamento e ferramentas). Padrões e/ou diretrizes foram identificados para orientar as implementações. Defesa passiva.

Nível 4 — O programa de segurança cibernética usa, coleta e analisa dados para melhorar seus resultados. As atividades são guiadas por diretrizes organizacionais documentadas; políticas incluem requisitos de conformidade para padrões e/ou diretrizes especificados. O pessoal responsável pelas funções de segurança do sistema de controle tem treinamento e experiência. O programa é gerenciado, proativo, acompanha métricas e alguma automação. Active Defense, SIEM, Anomaly and Breach Detection.

Nível 5 — Processos de segurança cibernética continuamente aprimorados por meio de *feedback* dos processos existentes e adaptando-se para atender melhor às necessidades organizacionais. O pessoal que executa os processos possui habilidades e conhecimentos adequados. Otimizado, automatizado, integrado e previsível. Defesa Ativa, Inteligência de Ameaças e Gerenciamento de Incidentes.

Na sua opinião, qual delas melhor descreve o programa de segurança cibernética do seu sistema de controle?



Quando observamos como as respostas daqueles que se identificam como Nível 1 ou Nível 2 ("Maturação inferior" ou "M Baixa") diferem daqueles que se identificam como Nível 4 ou Nível 5 ("Maturidade Alta" ou "M Alta"). Os dois grupos não diferem significativamente nas respostas a todas as perguntas, mas, quando diferem, mostramos isso em gráficos comparando os dois.

O ciclo anual desses projetos de pesquisa também nos permite examinar nossos dados longitudinalmente em busca de tendências e mudanças de ano para ano. O refinamento e a revisão das pesquisas e suas perguntas componentes às vezes impedem comparações diretas, mas, sempre que possível e quando são encontrados deltas interessantes entre conjuntos de dados anuais, nós os levamos ao conhecimento de nossos leitores.

> *"O intervalo nas respostas do conjunto de dados em relação à maturidade do programa de segurança cibernética é consistente com a experiência da Industrial Defender. Os setores/verticais que escolheram um padrão por meio de decreto corporativo ou regulatório tendem a se enquadrar na categorização de Nível 3 de Programas de Segurança Cibernética. Infelizmente, verticais da indústria, como água e gás midstream, normalmente tendem a pousar nas categorias de Nível 1 e Nível 2 devido à falta de financiamento e supervisão regulatória."*
>
> **George Kalavantis**
> COO na Industrial Defender

Resultados da pesquisa

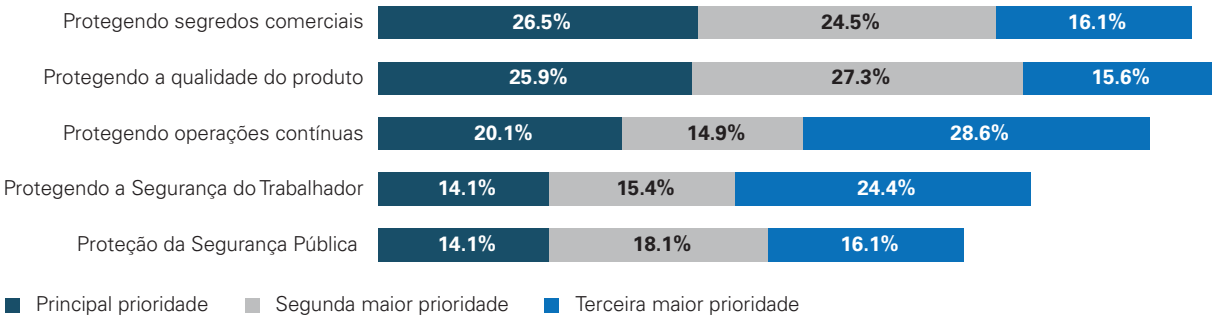
Principais prioridades

Para aumentar a utilidade desta pesquisa como ferramenta de tomada de decisão, incorporamos mais questões de categorização do que em seu antecessor. Notavelmente, isolamos as respostas dos usuários finais para analisá-las separadamente da tecnologia de segurança e dos fornecedores de serviços. Em muitas perguntas, encontramos respostas desses grupos bastante semelhantes, mas, em áreas com maior divergência, podemos apresentar as respostas do usuário final especificamente.

O tópico das principais prioridades de segurança cibernética do sistema de controle é um deles. Com todas as opções recebendo algum apoio de vários usuários finais, é claro que continua a haver uma forte priorização na proteção da segurança dos trabalhadores e do público.

Alguns de nossos membros do Comitê Diretivo de Especialistas no Assunto ficaram surpresos com o fato de Segurança não ter recebido uma classificação muito mais alta, pois sempre foi fundamental para as considerações de segurança de OT. Como muitas vezes é verdade, a questão subjacente do porquê de os participantes responderam dessa maneira não é totalmente clara. Pode ser que muitos não considerem seus Sistemas Instrumentados de Segurança expostos a ameaças cibernéticas (apesar das amplas evidências de que muitos estão) e casos bem conhecidos de ataques cibernéticos ao SIS[2].

Classifique as principais prioridades de segurança cibernética do sistema de controle da sua organização (usuários finais)



> *Quando a infraestrutura crítica é invadida diariamente, não é surpresa que haja uma preocupação cada vez maior entre as partes interessadas de OT relacionadas a operações seguras e contínuas. Vemos que as soluções de rede que funcionavam no passado, como adicionar mais um firewall, não são mais eficazes. Esses fatores por si só apontam para uma necessidade contínua de soluções de segurança cibernética, como confiança zero e acesso remoto seguro, para reduzir as superfícies de ataque e mitigar o impacto financeiro negativo para uma organização.*
>
> **Keith Beeman**
> CEO na Tempered Networks

[2] https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

Indicadores-chave de desempenho (KPIs) rastreados

As métricas que uma organização usa para rastrear o desempenho de seu programa de segurança cibernética podem conter informações valiosas sobre suas prioridades, seu nível de maturidade, prováveis experiências de incidentes anteriores e postura de segurança atual. Por exemplo, uma olhada na tabela abaixo mostrará que as organizações Alta M usam muitos indicadores-chave de desempenho, mais do que programas menos maduros, com alguns KPIs rastreados quase duas vezes mais pelo primeiro (por exemplo, redução do número de incidentes de segurança: 50,7% Alta M vs. 25,6% Baixa M). Ao mesmo tempo, as organizações Baixa M têm duas vezes mais probabilidade de não rastrear nenhum KPI (minha organização não acompanha KPIs, 10,4% de Baixa M vs. 4,2% de Alta M). As organizações Alta M têm uma visibilidade muito maior de seus ambientes, permitindo que calculem métricas mais significativas, identifiquem e rastreiem seus KPIs de forma mais consistente.

Em apenas algumas áreas os grupos de "inquiridos" abordam a paridade, nomeadamente reduzir o custo financeiro dos incidentes de segurança, reduzir o número de contas partilhadas e reduzir o número de falsos positivos de incidentes de segurança

Embora os níveis de maturidade do programa de segurança tenham sido distribuídos uniformemente entre as organizações respondentes de todos os tamanhos, observamos que as entidades maiores acompanharam um subconjunto de KPIs mais do que as menores, conforme mostrado na tabela a seguir.

Os dois grupos relataram o uso de outros KPIs de forma bastante semelhante, mas encontramos diferenças distintas no uso desses 11 indicadores específicos.

Examinamos como as respostas de outros subconjuntos de participantes diferiram em várias perguntas. Foi encontrada uma correlação estatisticamente útil, e usamos o símbolo "p" para chamar a atenção dos leitores.

p

Identifique todos os principais indicadores de desempenho do programa de segurança que sua organização usa (Alta M vs. Baixa M)

Identifique todos os principais indicadores de desempenho do programa de segurança que sua organização usa (grandes vs. pequenas organizações)

Muitas dessas métricas se alimentam umas às outras, criando um ciclo de feedback positivo. As organizações que são proativas na redução de sistemas não corrigidos e aplicativos/configurações expiradas encontrarão ocorrências mais baixas de ransomware e resolução mais rápida.

Um caso semelhante pode ser feito para o comportamento do usuário — as organizações que rastreiam o treinamento do usuário e os resultados de exercícios cibernéticos (como phishing) provavelmente verão uma queda no número de pessoas clicando em links suspeitos (uma ou várias vezes) e os incidentes decorrentes da engenharia social vetores de ataque.

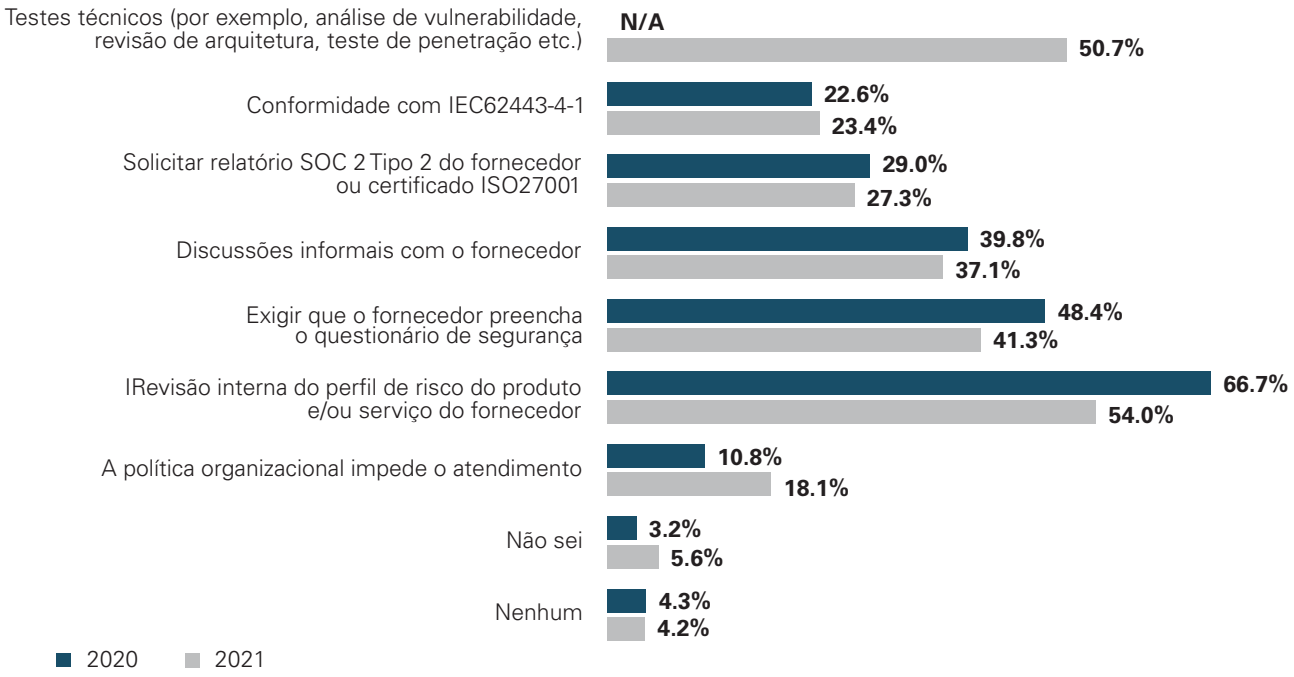
Brad Raiford
Diretor de Segurança Cibernética
da KPMG nos EUA

Avaliações de risco de pré-aquisição

A revisão interna do perfil de risco do produto e/ou serviço do fornecedor ainda é a forma de avaliação de risco pré-aquisição mais usada para proprietários de sistemas de controle (54% agora vs. 67% em 2020). Adicionamos "Testes Técnicos" como uma nova opção este ano, e é encorajador ver que pelo menos metade das organizações participantes faz isso. Desse grupo, a maioria (69,2%) também realiza análises internas de perfis de risco de produtos e/ou serviços de fornecedores e 50,6% exigem que os fornecedores preencham questionários de segurança. Sendo os impactos potenciais o que são em muitas configurações do sistema de controle, os autores recomendam o uso de várias abordagens para medir e gerenciar riscos.

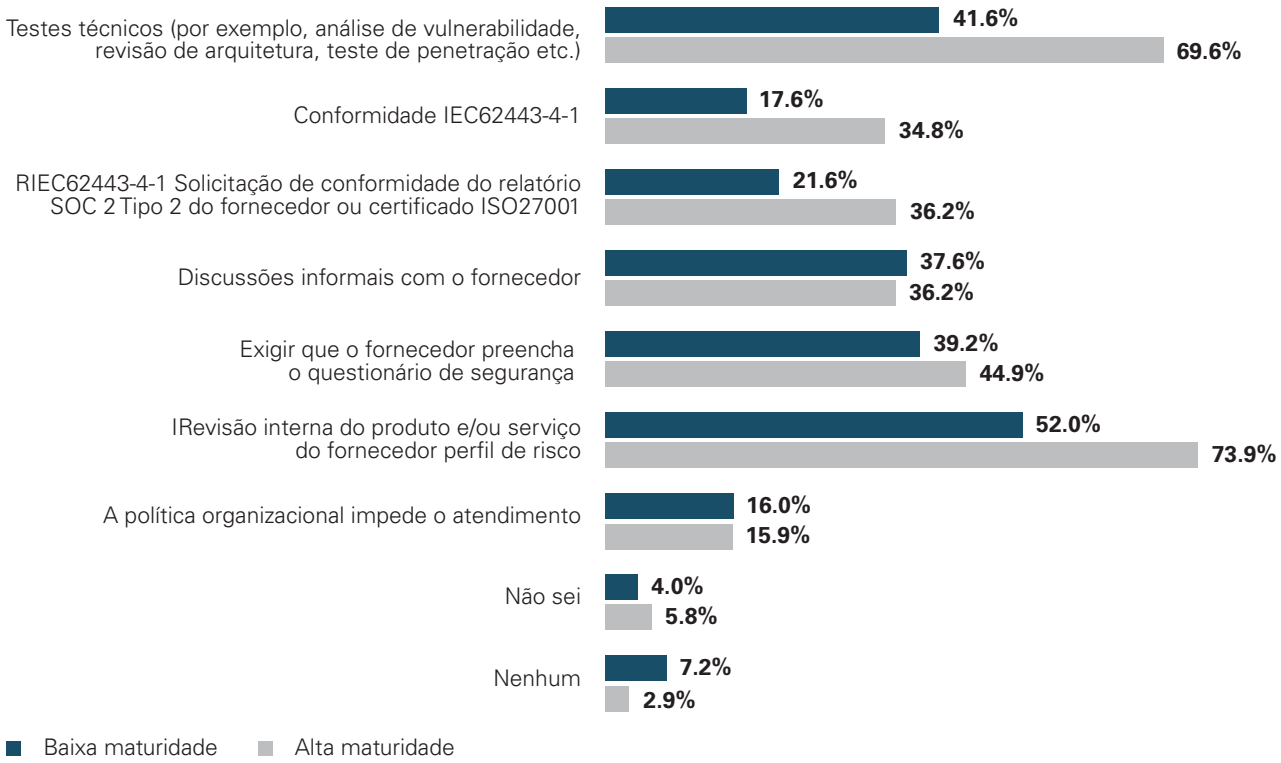
De particular interesse em comparação com organizações de Alta e Baixa M são as grandes diferenças em suas avaliações de conformidade com a IEC62443-4-1 (34,8% Alta M vs. 17,6% Baixa M) e sua inclusão de Testes Técnicos (69,6% Alta M vs. 41,6% Baixa M). A frequência significativamente maior de uma revisão interna do perfil de risco do produto e/ou serviço do fornecedor também se destacou (73,9% Alta M vs. 52% Baixa M).

Identificar todas as avaliações de risco que sua organização realiza antes de adquirir produtos ou serviços do sistema de controle



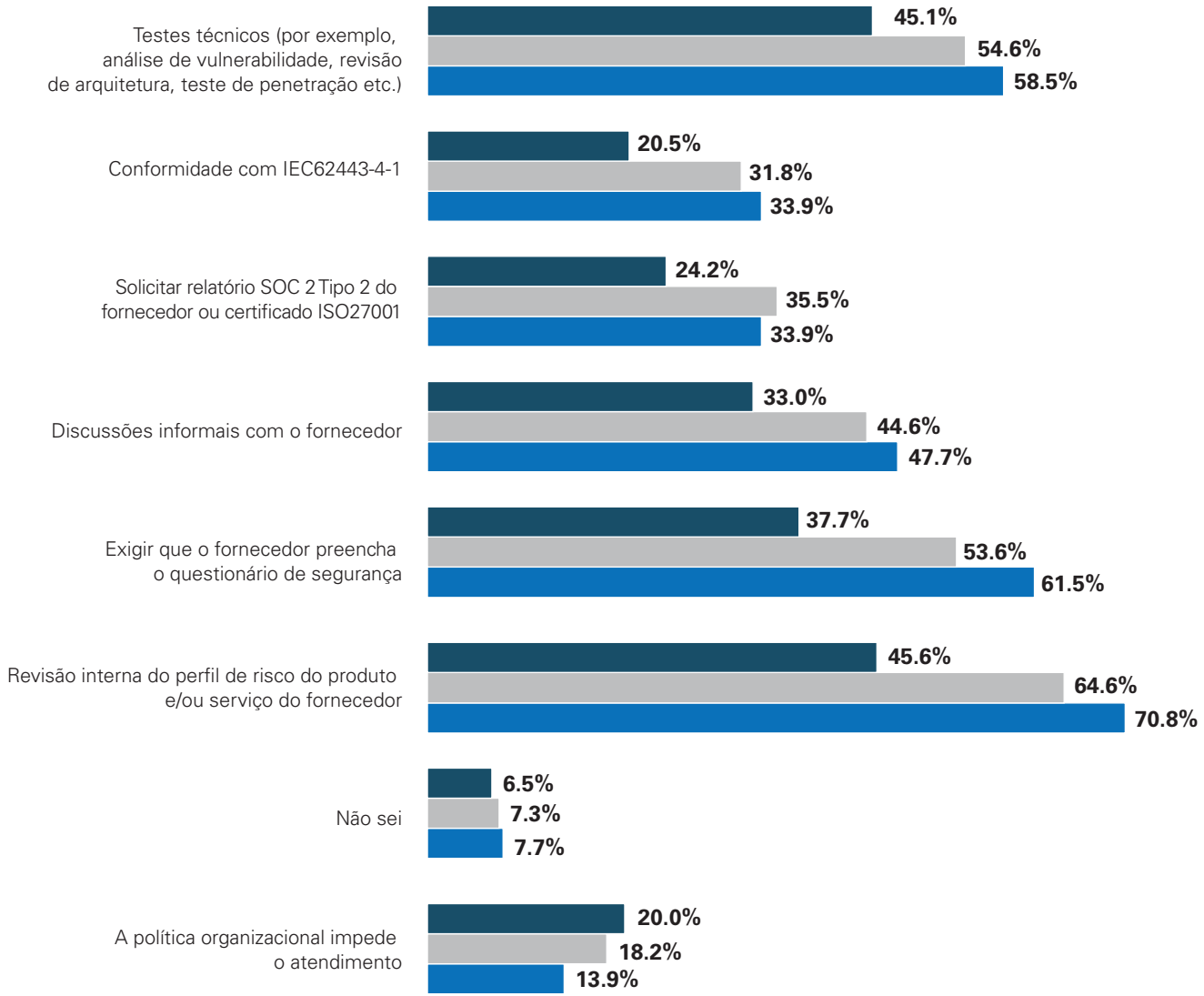
O tamanho das organizações respondentes (conforme definido pelo tamanho da força de trabalho) também influenciou claramente as avaliações de risco realizadas antes da aquisição de produtos ou serviços do sistema de controle. Mesmo controlando os níveis de maturidade do programa de segurança cibernética, as organizações maiores são mais propensas a realizar todo tipo de avaliação de risco. Talvez essas entidades, com maiores recursos, possam e optem por ser mais criteriosas nesse aspecto de sua gestão de risco.

Identifique todas as avaliações de risco que sua organização realiza antes de adquirir produtos ou serviços do sistema de controle (Alta M vs. Baixa M)



Apesar dos recursos disponíveis, os desafios que aumentam de forma confiável com o tamanho da organização são o tamanho do portfólio do fornecedor e a manutenção de um conhecimento atual dos riscos. As avaliações de risco pré-aquisição podem ser solicitadas apenas uma vez, mas as avaliações periódicas pós-aquisição de uma lista cada vez maior de fornecedores e seus equipamentos, *software* e serviços podem aumentar para milhares ou dezenas de milhares ao longo do tempo.

Identifique todas as avaliações de risco que sua organização realiza antes de adquirir produtos ou serviços do sistema de controle (por tamanho da organização)



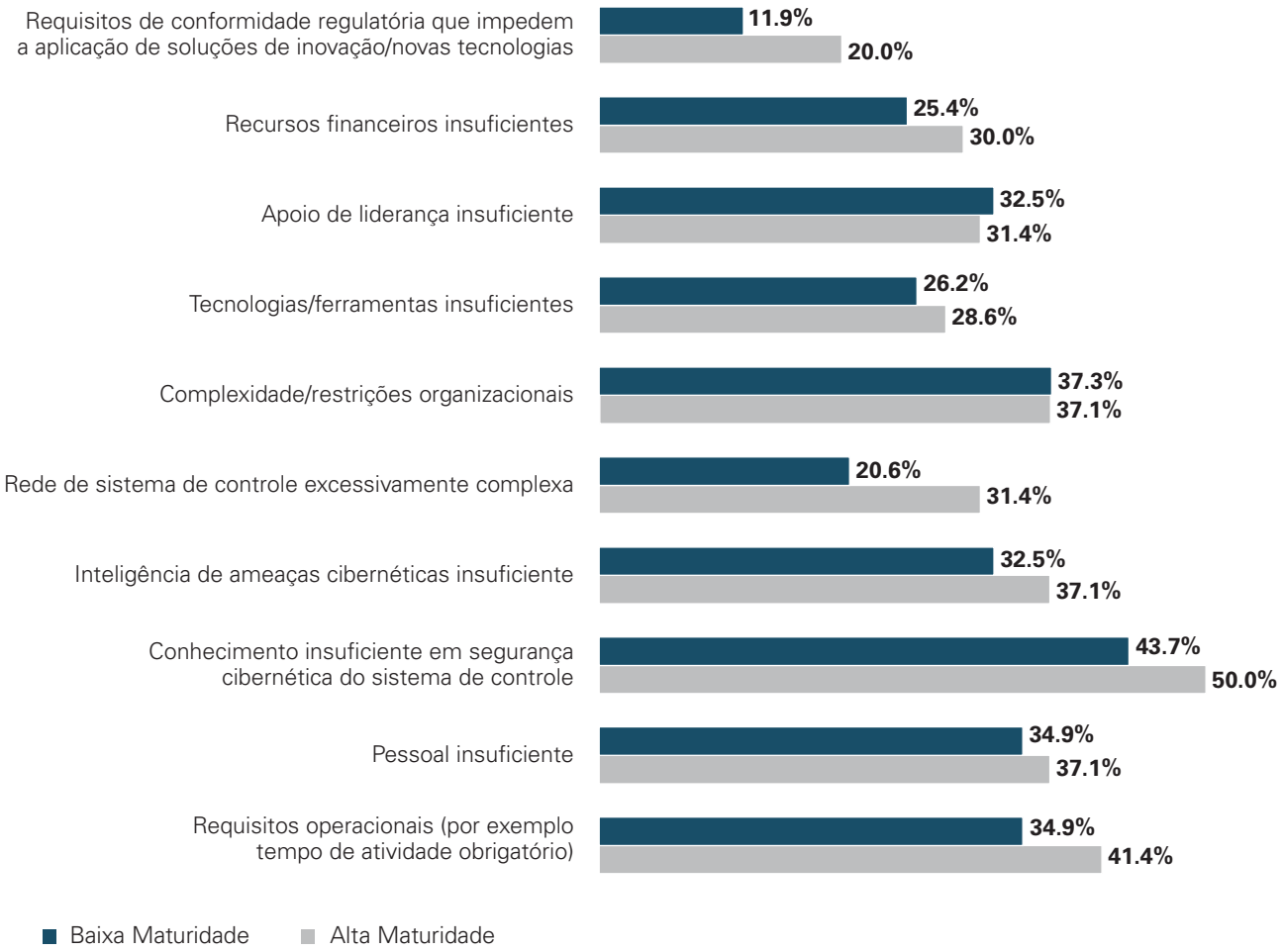
Selecione os maiores obstáculos para reduzir a superfície de ataque de segurança cibernética do sistema de controle (2020 *vs.* 2021)

Maiores obstáculos para reduzir a superfície de ataque (CS)[2]

A especialização insuficiente em segurança cibernética do sistema de controle continua sendo amplamente considerada o maior obstáculo para reduzir a superfície de ataque de segurança cibernética do sistema de controle.

Na análise longitudinal, quase todos os fatores receberam uma porcentagem de respostas menor do que em nosso relatório de 2020, um efeito não surpreendente de termos adicionado duas novas opções de resposta a essa pergunta este ano. Vale a pena notar que as Tecnologias/Ferramentas Insuficientes ficaram praticamente inalteradas (27,2% este ano vs. 28,0% em 2020) e outros dois receberam uma parcela maior de respostas. A inteligência insuficiente de ameaças cibernéticas saltou para 32,8% (2021) de 12,9% (2020) e a Rede de Sistema de Controle Excessivamente Complexa aumentou ligeiramente para 26,9% (2021) de 22,6% (2020). Muitas organizações, é claro, ficam frustradas com a maior complexidade administrativa e novas barreiras à visibilidade da rede ao implementar níveis maiores de segmentação de rede.

Selecione os maiores obstáculos para reduzir a superfície de ataque de segurança cibernética dos sistemas de controle



As inscrições comuns (inseridas pelos entrevistados usando nosso campo Outro nesta pergunta) incluíram problemas na cadeia de suprimentos, falta de produtos de OT seguros e suporte insuficiente abaixo do nível de liderança da organização.

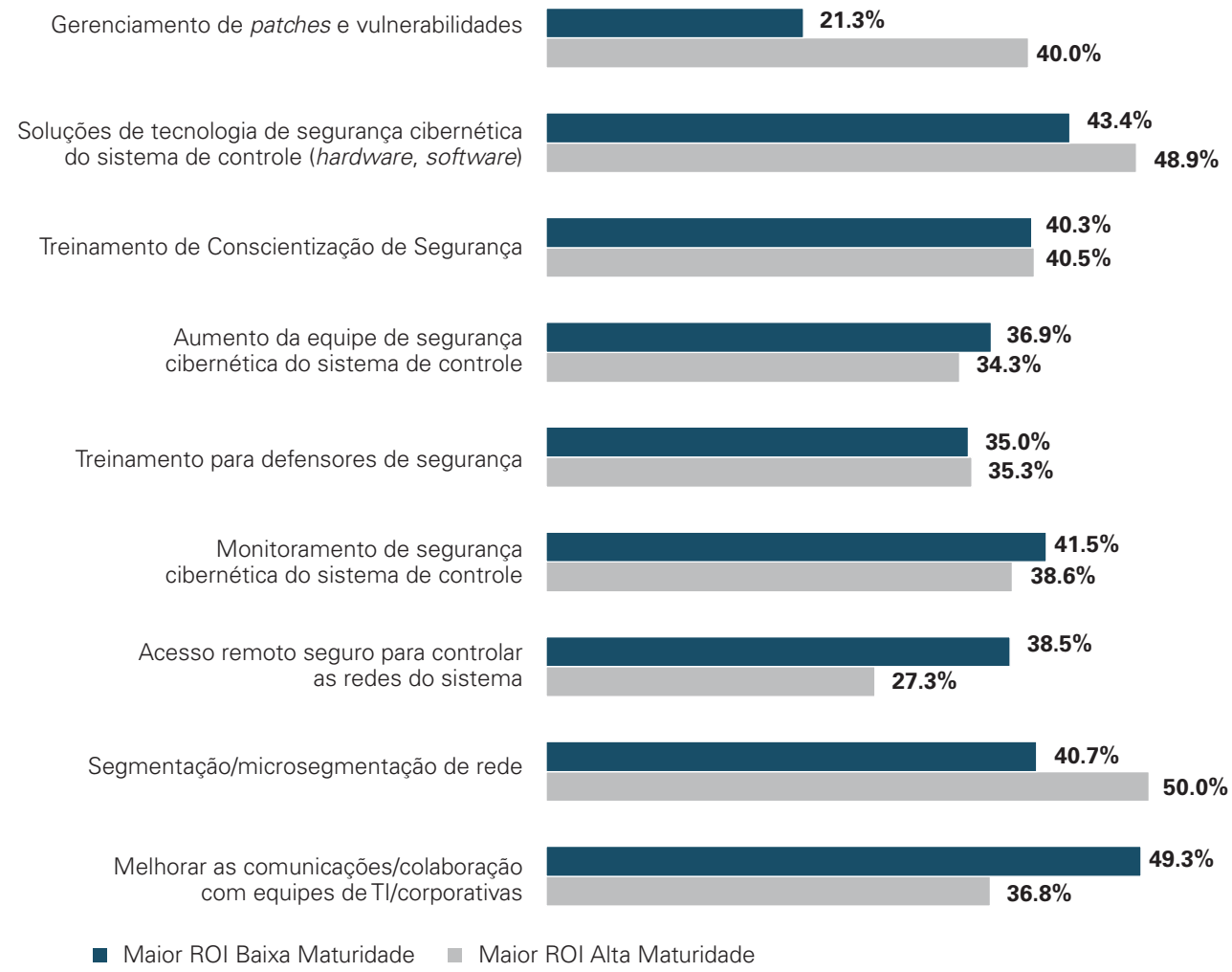
> A partir deste resultado da pesquisa, podemos ver que, à medida que TI e OT continuam em rede, a complexidade da organização relacionada à segurança de OT é um grande obstáculo, juntamente com a falta de experiência em segurança cibernética da ICS..

William Malik
Vice-Presidente de Estratégias de Infraestrutura, Trend Micro

As três principais áreas para ROI em investimentos (CS)[2]

s entrevistados diferiram significativamente sobre onde consideraram os melhores lugares para gastar seus dólares em segurança cibernética com base na maturidade relativa de seus programas de segurança cibernética do sistema de controle. Ambos os grupos colocam ênfase muito semelhante no treinamento de conscientização de segurança, treinamento para defensores da segurança e aumento da equipe de segurança cibernética do sistema de controle. Fora dessas três áreas relacionadas, vemos deltas que variam de quase 3 pontos percentuais (Monitoramento de segurança cibernética do sistema de controle: 38,6% Baixa M vs. 41,5% Alta M) até quase 20 (Gerenciamento de *patches* e vulnerabilidades: 21,3% Baixa M vs. 40% Alta M).

Qual área oferece os maiores retornos sobre os investimentos em segurança cibernética do sistema de controle? (Alta M vs. Baixa M)



As organizações de alta maturidade têm quase duas vezes mais chances de acreditar que o gerenciamento de patches e vulnerabilidades fornece alto ROI.

“O estudo sugere que uma análise mais detalhada é necessária para determinar se há expectativas de ROI mais baixas na melhoria da comunicação e colaboração entre as organizações de OT e suas contrapartes corporativas de TI. No relatório de pesquisa The State of Operational Technology and Cybersecurity de 2021 da Fortinet, os resultados indicaram que a convergência de TI-OT estava bem encaminhada antes da pandemia, e a pandemia apenas acelerou a transformação digital e aumentou a necessidade de conectividade.

O estudo também revelou que as poucas empresas que relataram zero intrusões eram mais propensas a aderir a várias práticas recomendadas. Eram:

— Mais propensas a usar orquestração e automação e ter rastreamento e relatórios de segurança em vigor

— Mais propensas a ter visibilidade 100% centralizada em seu centro de operações de segurança

— Mais preparadas, mais cedo, para acomodar o trabalho em casa durante a pandemia.

Como diz o velho ditado, o que é medido é melhorado. As implicações financeiras para vulnerabilidades de segurança foram rastreadas e relatadas por 74% das organizações de primeira linha. Também rastreiam vulnerabilidades encontradas e bloqueadas (74%) e resultados tangíveis de gerenciamento de risco (60%).”

William Noto
Líder Global de Marketing de Produto para Tecnologia Operacional, Fortinet

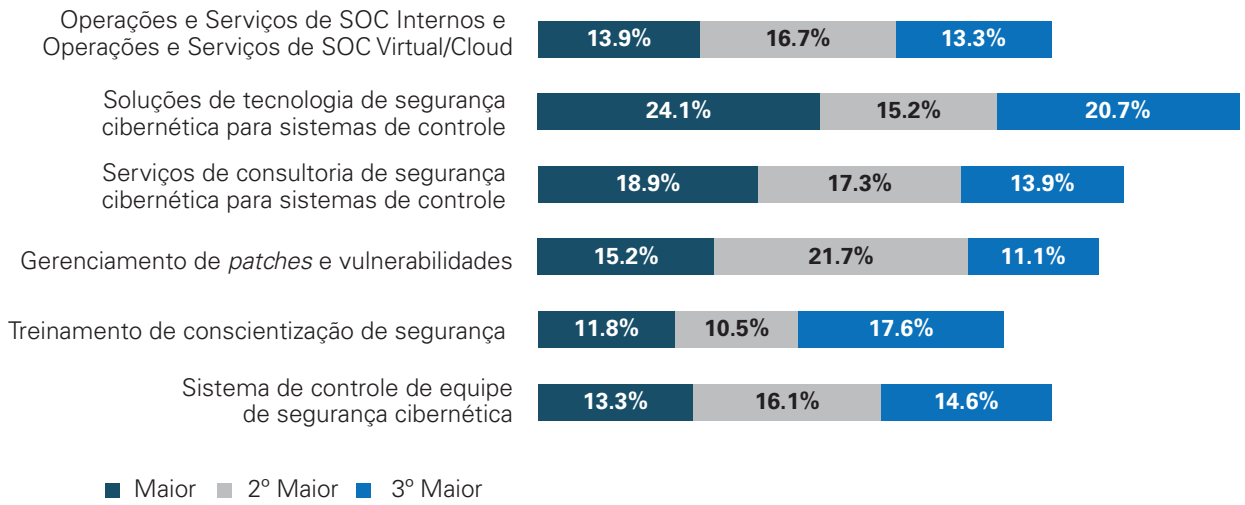
Além de reconhecer de onde programas de diferentes níveis de maturidade obtêm seus melhores retornos, vale a pena considerar por que eles o fazem. As organizações com programas de segurança cibernética menos maduros se concentram mais no acesso remoto por que essa é uma área problemática para elas ou por que dependem mais da segurança terceirizada? As organizações com programas de segurança cibernética mais maduros colocam expectativas de ROI mais baixas na melhoria das comunicações/colaboração com equipes de TI/corporativas por que estabeleceram protocolos e processos superando amplamente os desafios dessa atividade e estão seguindo em frente, por que o trabalho anterior nessa área foi decepcionante resultados ou por outros motivos? Mais pesquisas para investigar as razões subjacentes serão necessárias para responder a essas perguntas.

As três principais áreas de maior gasto em (CS)[2]

As soluções de tecnologia de segurança cibernética do sistema de controle continuam a ser relatadas como a área em que a maior quantidade de recursos de segurança cibernética do sistema de controle é gasta, embora com uma porcentagem significativamente menor de entrevistados selecionando isso como seu maior gasto (24,1% este ano vs. 48,3% anteriormente). Os serviços de consultoria de segurança cibernética do sistema de controle, gerenciamento de patches e vulnerabilidades mantiveram as mesmas posições relativas de 2020.

Treinamento de conscientização de segurança e sistema de controle: a equipe de segurança cibernética trocou de lugar como a segunda área mais baixa e a mais baixa de recursos gastos, respectivamente. Em geral, algum efeito de diluição deve ser reconhecido pela adição de Operações e Serviços de SOC Internos e Operações e Serviços de SOC Virtual/Cloud como uma nova opção na pesquisa deste ano. Também é possível que estejamos vendo o impacto de processos aprimorados e implementações de tecnologia diminuindo a quantidade de trabalho humano necessário para executar funções de segurança. Vemos isso como uma área interessante para novas pesquisas.

Identifique as três principais áreas nas quais sua organização gasta mais recursos de segurança cibernética do sistema de controle



Orçamentos

Mais de 43% dos nossos entrevistados que forneceram dados orçamentários relataram orçamentos de segurança cibernética do sistema de controle superiores a US$ 1 milhão para o ano fiscal de 2020, o que é comparável ao nosso relatório anterior.

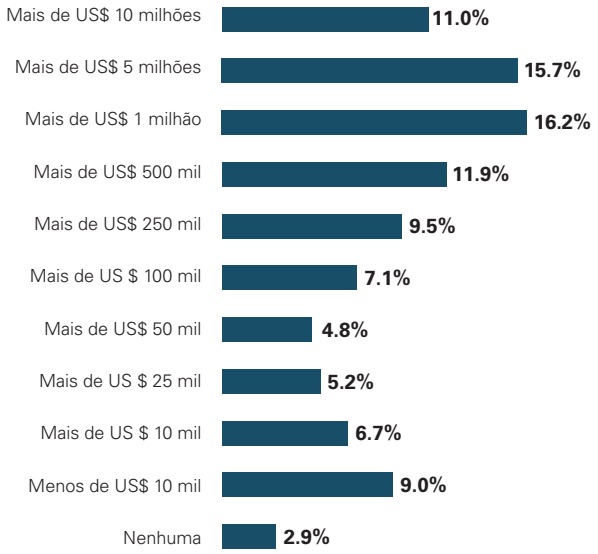
Encontramos algumas evidências de restrições nos orçamentos no ano passado. A maioria dos entrevistados indicou que suas organizações aumentaram os orçamentos de segurança cibernética do sistema de controle no ano passado, mas um total de 10% dos entrevistados indicou uma queda em 2020, muito mais do que o 1,1% do estudo anual anterior, que analisou os orçamentos de 2019. Além disso, a concentração do crescimento do orçamento diminuiu da faixa de 30% a 50% para a faixa de 10% a 30%, para um aperto geral dos orçamentos de segurança cibernética, provavelmente derivando pelo menos em parte dos impactos da pandemia no mercado.

As tendências gerais continuaram em alta, com quase dois terços (60,4%) relatando um aumento de pelo menos 10% nas alocações de recursos, e as pressões orçamentárias para muitas organizações incluirão o rápido aumento da necessidade de acesso remoto do trabalhador impulsionado pela COVID-19, exigindo maior segmentação de rede e gastos com Gerenciamento de Acesso de Identidade.

> “Acho que a mensagem de 'sem bala de prata' está finalmente começando a ser absorvida. Muitos fornecedores afirmaram ter 'a' solução para melhorar a cibernética de forma holística ou dentro de uma capacidade específica e com grande efeito. O que não estava acontecendo era um mergulho profundo na compreensão da verdadeira natureza do espaço do problema que a organização precisava resolver.
> A tecnologia possibilita processos executados/administrados/supervisionados por pessoas; a tecnologia não resolve lacunas/imaturidades do processo; a tecnologia não resolve inerentemente as lacunas/escassez de pessoas e habilidades.”

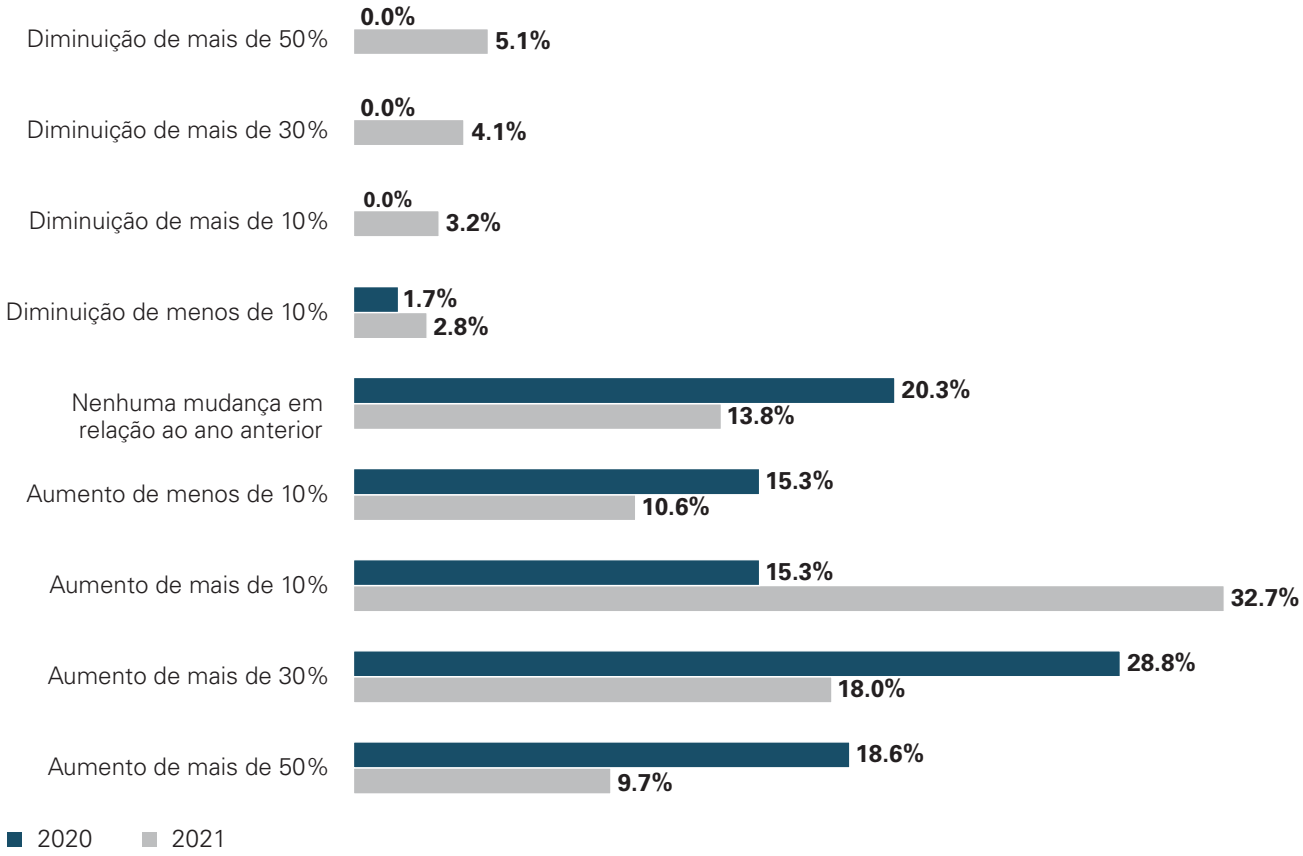
Brad Raiford
Diretor de Segurança Cibernética da KPMG nos EUA

Forneça sua melhor estimativa de orçamento de segurança cibernética anual total do sistema de controle de sua organização



Sendo esse o caso, mergulhamos mais fundo nos dados para descobrir o que pudemos sobre os impactos relativos em diferentes organizações e encontramos alguns padrões distintos nos deltas orçamentários com base no tamanho da força de trabalho da empresa. O aperto de cinto mais significativo, com queda de 50% ou mais, ocorreu quase exclusivamente nas pequenas e médias empresas, aquelas com até 1.000 funcionários. Essas SMBs eram bastante diversificadas, obviamente, pois também são altamente representadas nos grupos de aumento de mais de 10% e mais de 30%. As maiores entidades, aquelas com força de trabalho superior a 15.000, não ficaram imunes aos ventos contrários econômicos, mas os programas que apresentam o maior crescimento vêm principalmente desse subconjunto, com 12,9% relatando um aumento de 50% ou mais.

Forneça sua melhor estimativa de como o orçamento de segurança do sistema de controle deste ano se compara ao ano passado (2020 x 2021)

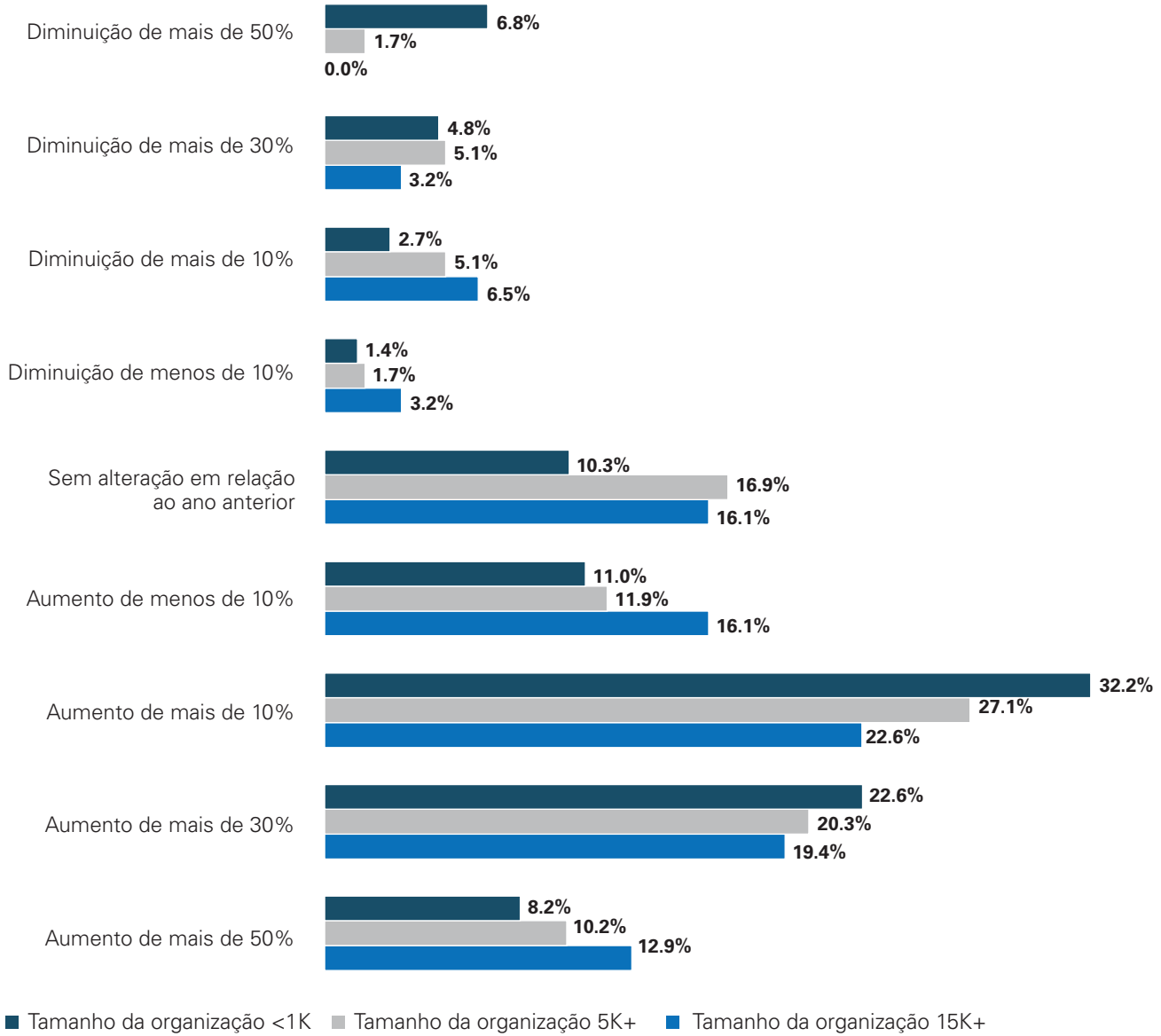


“Qualquer organização com responsabilidade de proteger a infraestrutura crítica deve levar a segurança a sério. Os dados da pesquisa CS2AI de 2022 ilustram que limitações orçamentárias, conhecimento insuficiente e a necessidade de sistemas de controle permanecerem on-line 24 horas por dia, 7 dias por semana, podem se tornar grandes obstáculos para uma segurança cibernética forte.

Mas não precisa ser desse jeito. Veremos uma tendência nos próximos 12 meses em direção à segurança baseada em hardware, pois os líderes de segurança exigem a proteção mais forte sem a necessidade de manutenção ou correção. Há uma fome real por soluções elegantes que possam proteger a infraestrutura crítica do futuro contra todos os tipos de ataques remotos.”

Dr. Ron Indeck
CEO, Q-Net Security

Forneça sua melhor estimativa de como o orçamento de segurança do sistema de controle deste ano se compara com o ano passado (por tamanho da organização)



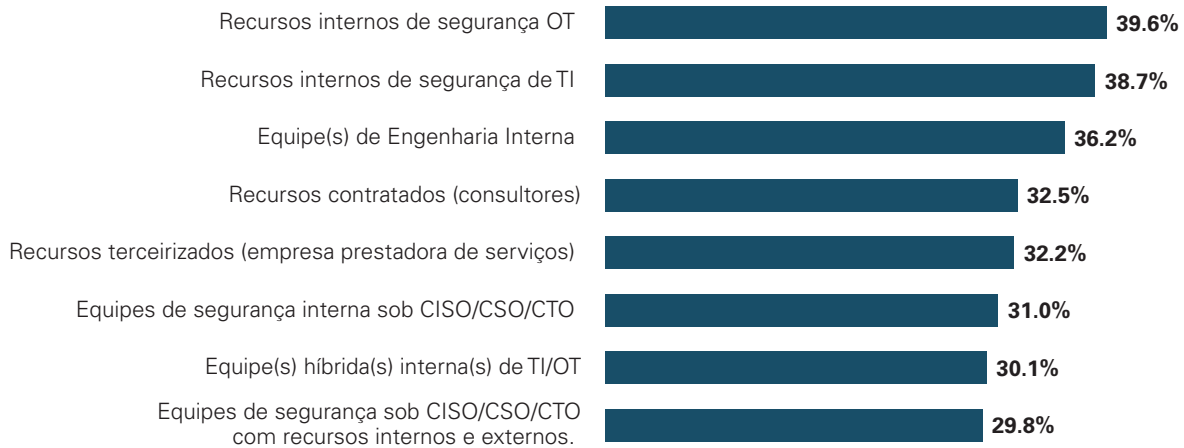
Serviços em uso

Não observamos grandes mudanças em relação aos resultados da pesquisa do ano passado sobre a questão dos serviços de segurança cibernética do sistema de controle em uso. As organizações continuam a depender mais fortemente de seus recursos internos para serviços de segurança cibernética do sistema de controle, com recursos internos de segurança de TI em 38,7% e recursos internos de segurança OT em 39,6 % como as respostas mais comuns.

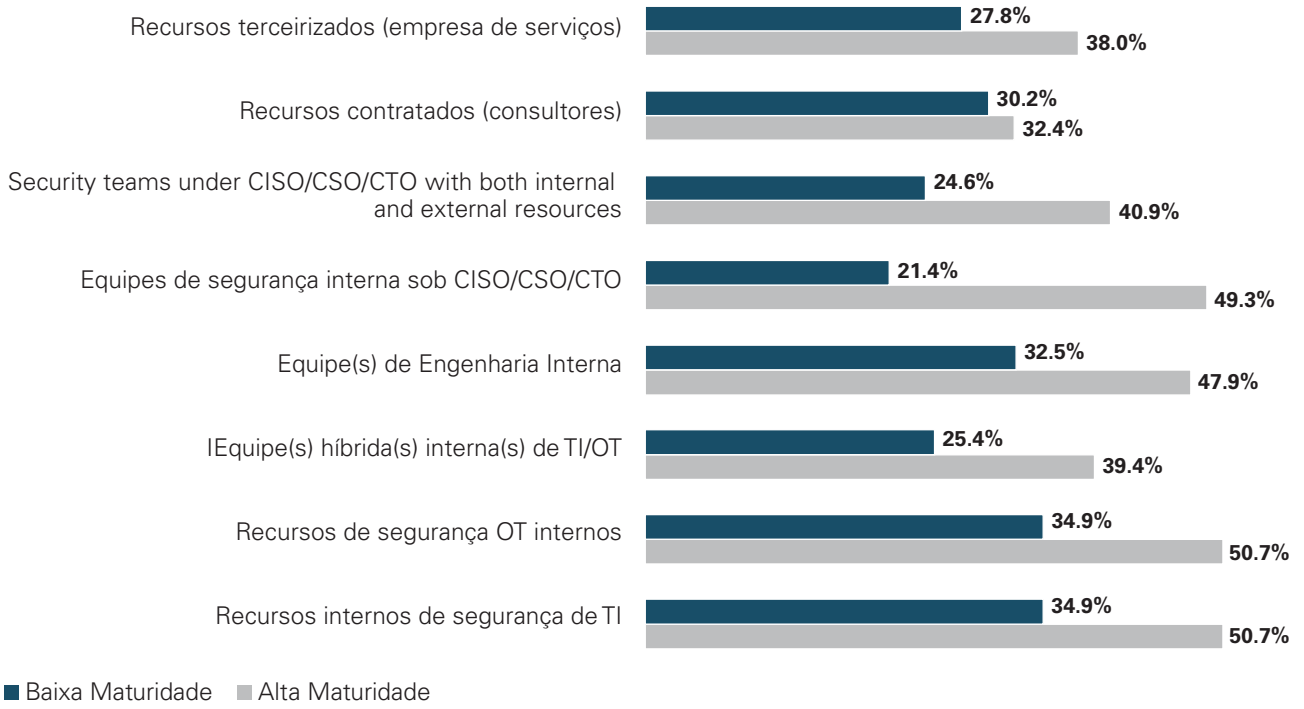
Uma observação feita é que cada entrevistado, em média, relatou uma combinação de 2 a 3 serviços diferentes em uso em sua organização.

Dividindo nossos entrevistados em subconjuntos por maturidade de seus programas de segurança cibernética do sistema de controle, ficou imediatamente claro que os programas de maturidade mais alta têm uma abordagem muito mais abrangente, usando **todos** os serviços com mais frequência do que seus equivalentes em programas de maturidade mais baixa, muitas vezes por uma ampla margem.

Selecione todas as fontes de serviços de segurança do sistema de controle que sua organização usa



Selecione todas as fontes de serviços de segurança do sistema de controle que sua organização usa (Alta M vs. Baixa M)



As organizações de Alta M são duas vezes mais propensas que o grupo de Baixa M de usar equipes de segurança interna sob CISO/CSO/CTO.

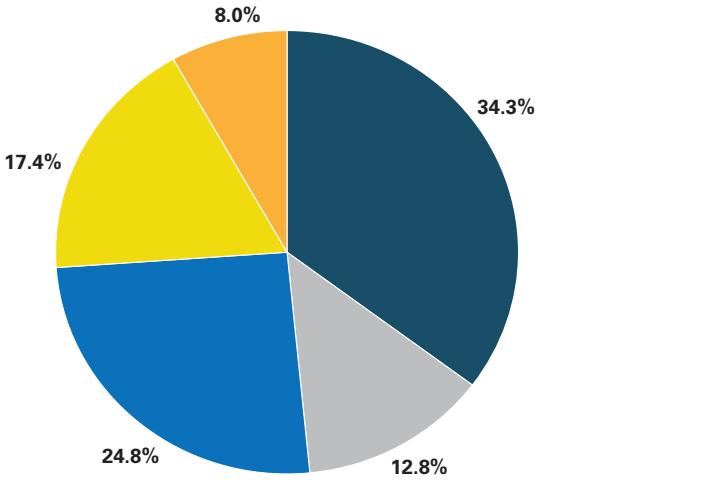
Treinamento de conscientização

Treinamento de conscientização de segurança, que visa a melhorar a cultura de segurança de uma organização e permitir que todos os funcionários reconheçam seu papel na redução da exposição ao risco, em oposição ao treinamento de segurança que é projetado para desenvolver as habilidades e capacidades dos profissionais de segurança especializados na defesa da organização, seus ativos e recursos, é um campo em amadurecimento nas configurações do sistema de controle. O treinamento para conscientização de segurança de TI e conscientização de segurança de OT geralmente tem histórias de desenvolvimento mais profundas.

O raciocínio e a importância dos conceitos de conscientização de segurança de TI, como validar fontes de e-mail antes de clicar em *links* desconhecidos, são amplamente conhecidos e compreendidos, por exemplo. Menos bem compreendidas são as exposições frequentemente criadas ao conectar os sistemas de negócios à tecnologia operacional, e é crucial que todas as organizações resolvam essa falta de conscientização fornecendo treinamento de conscientização de segurança cibernética do sistema de controle a todos os seus funcionários, se eles conseguirem isso integrando esse treinamento com um programa mais amplo ou como um produto autônomo.

A principal preocupação dos autores é com mais de um sexto (17,4%) dos entrevistados cujas organizações não possuem nenhum treinamento de conscientização de segurança do sistema de controle. Embora haja uma melhora muito pequena (20,6% no relatório de 2020), devemos enfatizar a importância de educar todo o pessoal sobre suas responsabilidades em manter os sistemas de controle seguros.

O treinamento de conscientização de segurança do sistema de controle da minha organização é...



- Integrado ao Treinamento de Conscientização de Segurança de TI
- Integrado ao Treinamento de Segurança Física
- Não sei
- Um programa separado de TI ou Treinamento de Segurança Física
- Inexistente (minha organização não tem treinamento de conscientização sobre segurança cibernética do sistema de controle).

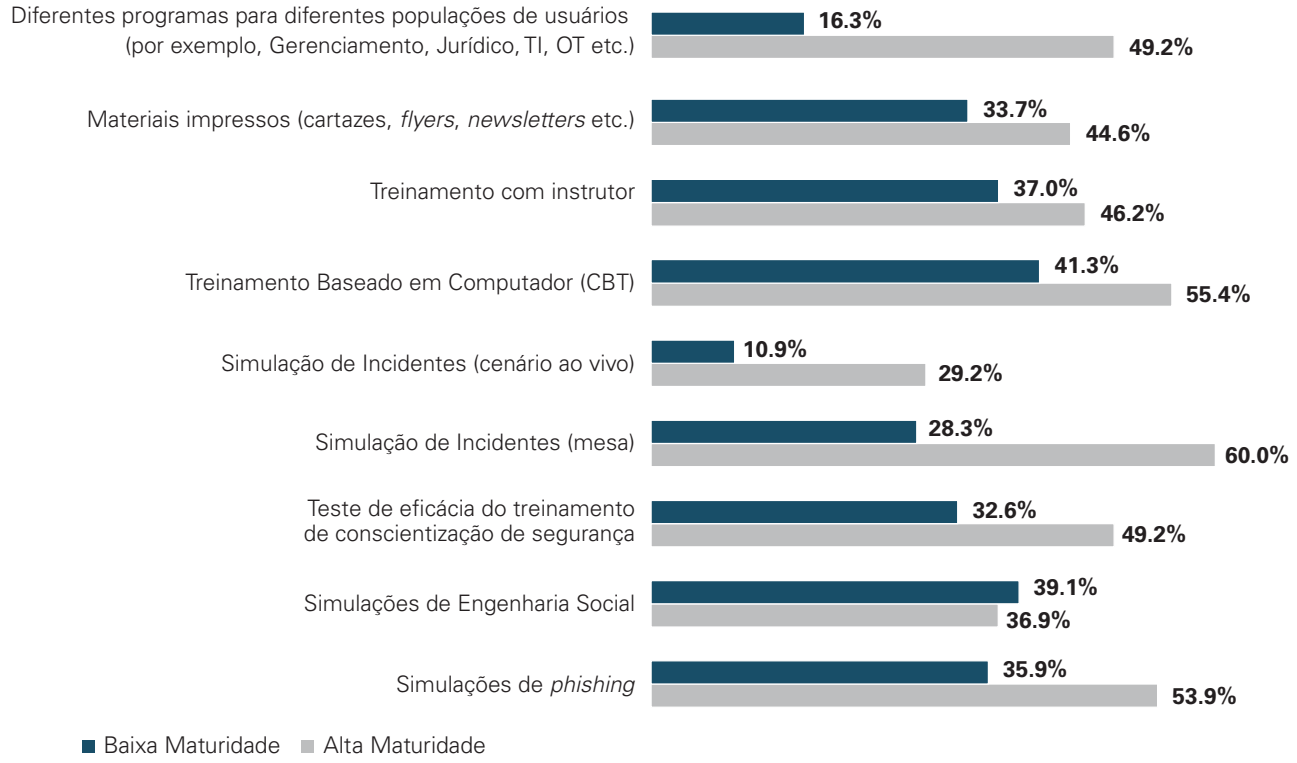
Treinamento

Os entrevistados relataram, em média, mais de três componentes de treinamento incluídos em seus respectivos programas de treinamento. Com diferenças conhecidas na utilidade de diversos métodos de treinamento em diferentes populações, essa combinação de abordagens é definitivamente recomendada, com conteúdo e mensagens semelhantes entregues em vários canais, esperançosamente em um sistema eficaz de reforço.

A Simulação de Incidentes (cenário ao vivo) foi selecionada pelo menor número de participantes, principalmente nos programas menos maduros (Nível de Maturidade 1–2). Embora reconheçam que estes são certamente os exercícios de treinamento mais complexos e caros, os autores desejam enfatizar que eles também são geralmente muito mais eficazes do que outros, particularmente na descoberta de lacunas na resposta a incidentes e nos planos de continuidade de negócios.

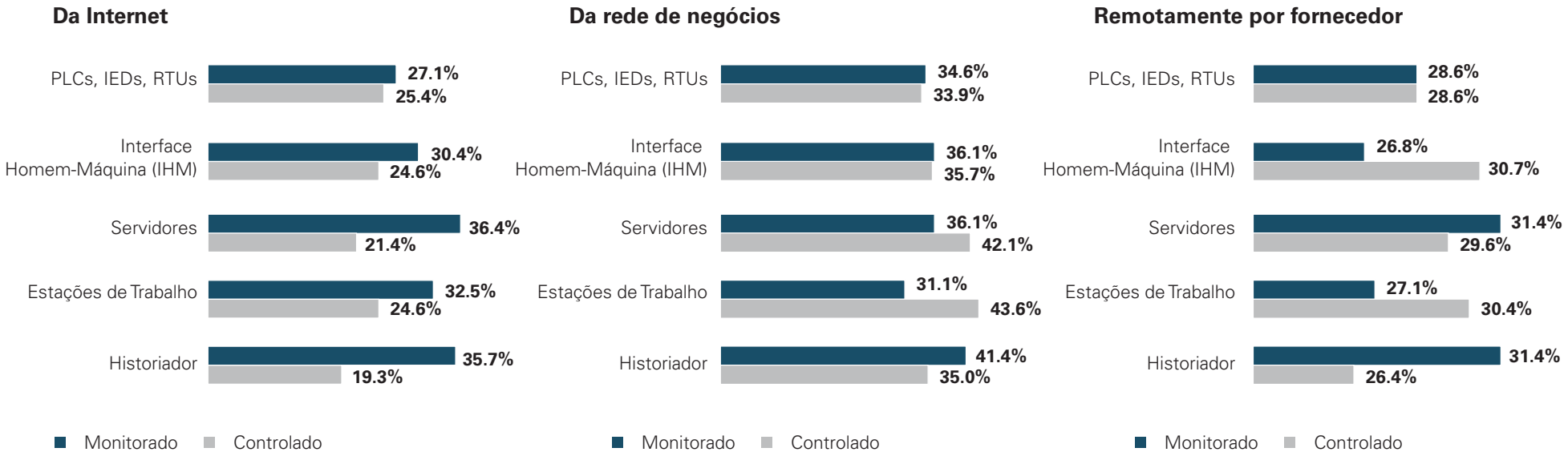
Uma razão clara pela qual os programas de Alta Maturidade são muito mais propensos a realizar Simulações de Incidentes é que não é fácil começar do zero. Como precursor, os Planos relevantes (por exemplo, DR/BC/IR) devem existir e ser relativamente maduros em termos de documentação, com todos os papéis definidos e compreendidos por todas as entidades com papéis a desempenhar antes que as simulações de mesa se tornem possíveis. Estes devem ser praticados várias vezes (com lições aprendidas e melhorias/atualizações feitas nos planos a cada iteração) antes de avançar para cenários ao vivo, com o envolvimento de sistemas operacionais.

Selecione todos os componentes incluídos em seu treinamento relacionado à segurança do sistema de controle (Alta M vs. Baixa M)



Acessibilidade dos componentes do sistema de controle

Com isso já bem estabelecido, de que pelo menos alguma acessibilidade de fora da rede de controle é comum na maioria dos ambientes, pedimos aos entrevistados que identificassem se cada componente do sistema de controle pode ser monitorado ou controlado remotamente.



Componentes do sistema de controle mais suscetíveis a comprometimento

Seja qual for o progresso feito na proteção de sistemas no ano passado, nossos entrevistados continuam a considerar as conexões com outros sistemas internos (redes de escritório/negócios) e ativos de computador (IHM, servidor, estações de trabalho) seus pontos mais fracos. Os dispositivos de comunicação sem fio receberam quase 50% mais atenção do que há um ano, sugerindo uma maior conscientização sobre a proliferação de dispositivos sem fio inseguros ou de segurança fraca durante esse período.

Estado dos planos organizacionais

O lado positivo é que mais de 85% têm todos os seus planos em algum estágio de desenvolvimento, com cerca de 20% Documentados e 26–30% Implementados. Essa é uma melhoria significativa em relação a 2020, quando descobrimos que 18% a 27% nem tinham os vários planos de gerenciamento/resposta em suas organizações.

Vale ressaltar que poucos relataram ter realmente testado algum de seus planos, principalmente em Gestão de Vulnerabilidades e Gestão de Riscos da Cadeia de Suprimentos. Os planos de teste são essenciais para encontrar e fechar as lacunas antes que se tornem falhas durante incidentes reais com consequências.

Identifique quais componentes do sistema de controle sua organização considera MAIS suscetíveis a comprometimento com base nas proteções e configurações atuais

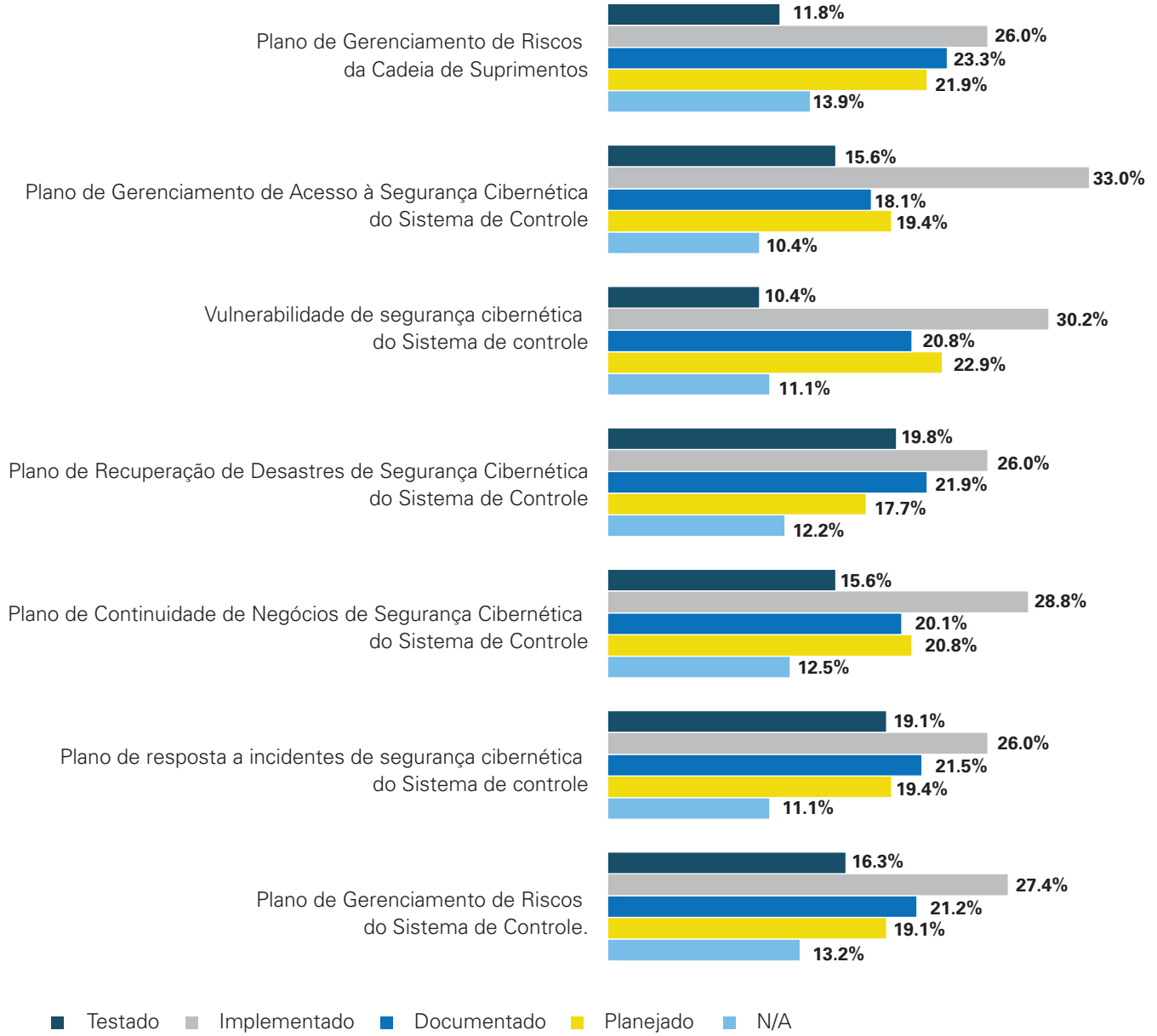
"'Conexões com outros sistemas' é o principal resultado para a pergunta 'mais suscetível a comprometimento' confirma a premissa do meu livro Secure Operations Technology de 2019. Todas as conexões e outros fluxos de informação são vetores de ataque. As instalações industriais seguras trabalham arduamente para minimizar o número e os tipos de fluxos de informações que entram em seus sistemas de controle a partir de redes menos críticas. E esses sites implantam universalmente *gateways* unidirecionais somente de saída entre redes críticas de controle e de negócios."

Andrew Ginter
VP Industrial Security, Waterfall Security Solutions

“O OT apresenta um ambiente de segurança mais complicado do que o de TI, pois existem dispositivos de TI (servidores baseados em SO) e dispositivos de OT industriais puros. Essa separação de dispositivos cria uma divisão interessante de propriedade, conjunto de habilidades e orçamento entre as equipes de TI e OT. A 'lacuna' de TI e OT é real, mas existem empresas voltadas para o futuro que estão preenchendo essa lacuna ao se integrarem para dar às equipes de TI exposição a dispositivos industriais para auxiliar no gerenciamento dos controles básicos necessários nos espaços de OT relativamente imaturos enquanto as equipes industriais estão tendo acesso a pessoal adicional, práticas de segurança estabelecidas e orçamento muito necessário. Como testemunhamos no ano passado, o risco cibernético e o risco de produção estão misturados e cabe às empresas abordar esses riscos juntos, fechando rapidamente a lacuna de TI e OT.”

Richard Springer
Diretor de Desenvolvimento de Negócios, Industrial, Tripwire

Selecione o melhor descritor para o estado atual de cada um de seus planos organizacionais

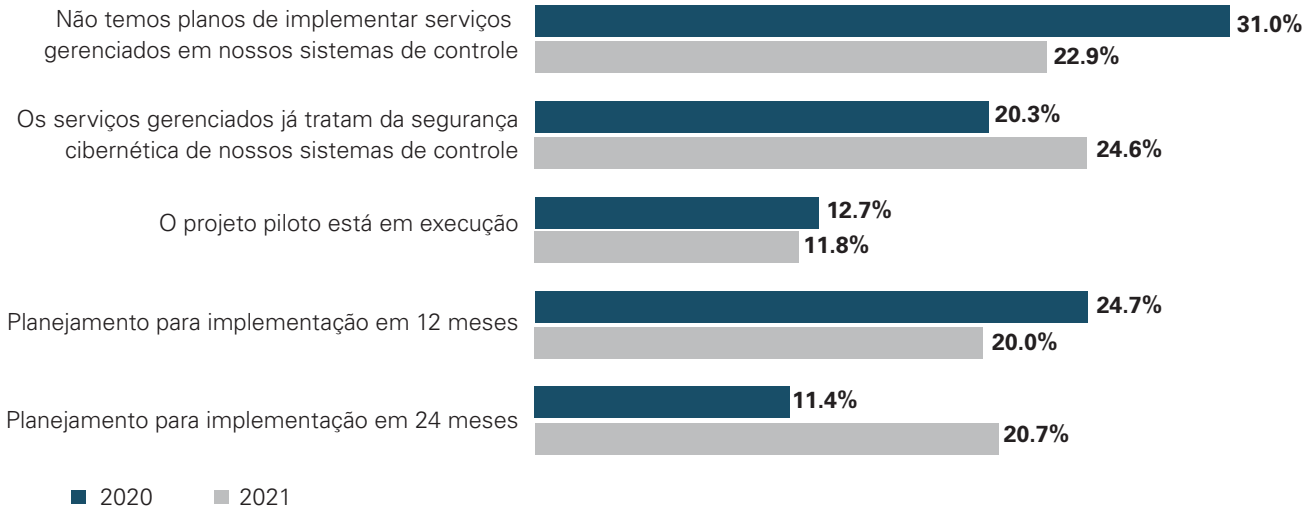


Serviços gerenciados

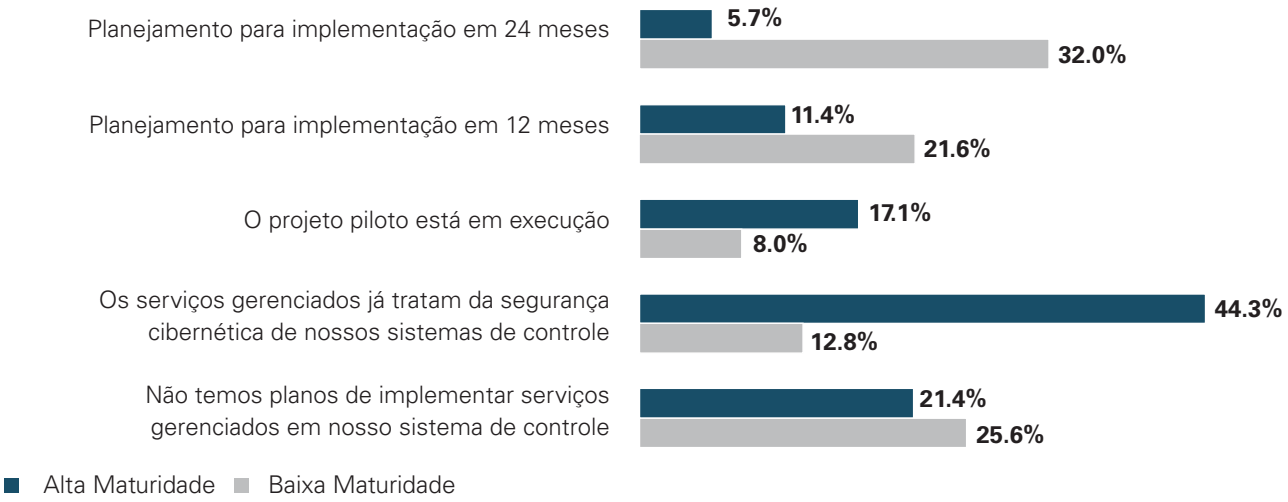
Estamos vendo uma pequena mudança nos entrevistados que planejam implementar serviços de segurança cibernética de sistema de controle gerenciado (cerca de 5% de aumento) e menos que não têm planos (mais de 8% de redução em "Não temos planos para implementar serviços gerenciados... sistemas"), com algumas diferenças entre os programas de Baixa Maturidade e Alta Maturidade. Não havia tendências claras entre as organizações com base no tamanho de sua força de trabalho.

A falta de recursos internos com treinamento e experiência suficientes continua sendo o principal motivador para as organizações implementarem serviços de segurança cibernética de sistema de controle gerenciado, selecionado como o único fator por quase 44% e por 68% dos entrevistados. Ao comparar os dados longitudinalmente, parece que mais entidades estabeleceram um suporte de fator único claro do que anteriormente. Isso é apoiado pelo número de entrevistados que, ao selecionar Outros no relatório de 2020, especificaram que não tinham casos de negócios claros para implementar serviços gerenciados.

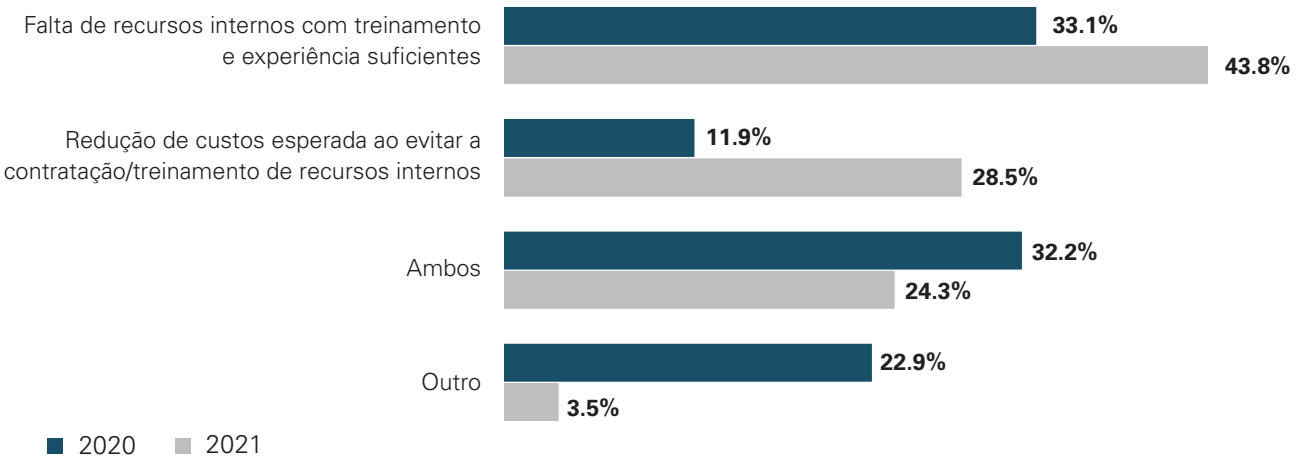
Qual é o estado atual dos serviços de segurança do sistema de controle gerenciado em sua organização?



Qual é o estado atual dos serviços de segurança do sistema de controle gerenciado em sua organização? (Maturidade Alta vs. Maturidade Baixa)



Por que você tem (ou planeja ter) serviços de segurança do sistema de controle gerenciado?



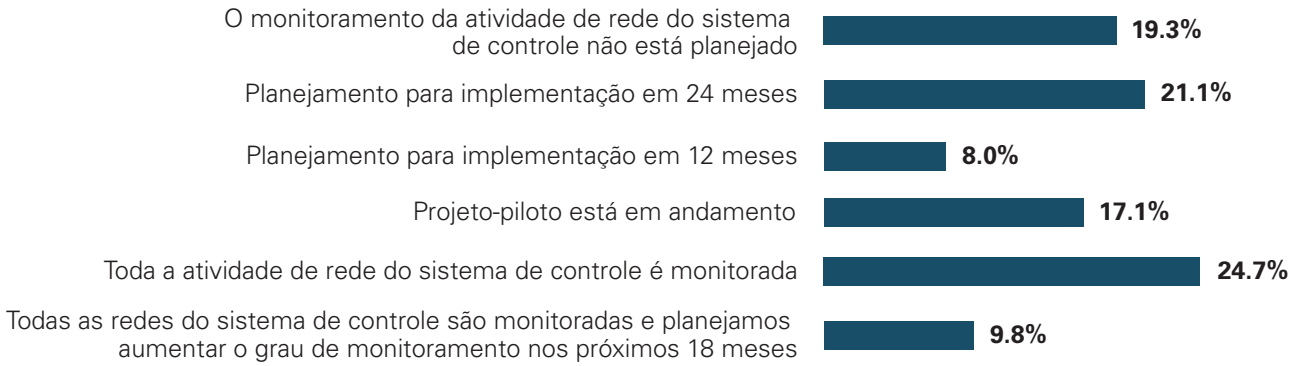
Monitoramento de atividade de rede do sistema de controle atual

A visão positiva de nossos dados é que mais da metade das organizações respondentes pelo menos começaram a monitorar sua atividade de rede do sistema de controle (51%) e quase outro terço (29%) está planejando implementar essa importante ferramenta de conscientização. Infelizmente, o restante de quase um quinto (19,1%) não é monitorado e não tem planos de mudar isso. A falta de conhecimento do tráfego nessa área significa que a primeira indicação de comprometimento dessas organizações serão interrupções operacionais, quando os atores de ameaças terão uma quantidade indeterminada de tempo em seus sistemas para reconhecer e estabelecer sua presença com o ambiente de rede. Muitos estudos de caso mostraram que os invasores muitas vezes passam despercebidos por vários meses exatamente por esse motivo, com a extensão dos danos e a dificuldade em removê-los muito maior devido ao longo período de ação livre concedido por sua invisibilidade.

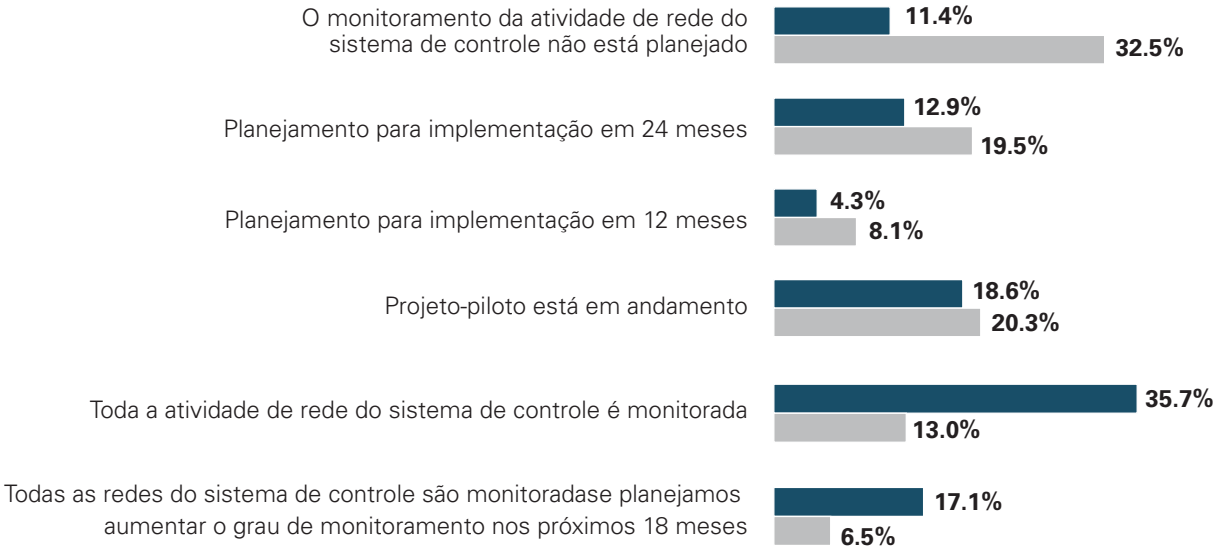
Talvez mais interessantes sejam as diferenças distintas entre os insumos dos respondentes de Baixa Maturidade e Alta Maturidade, e os últimos têm significativamente mais chances de ter implementado o monitoramento da rede do sistema de controle e até mesmo estar aumentando o que já está em vigor.

Sabe-se que muitos profissionais de sistemas de controle experientes permanecem cautelosos com as soluções de monitoramento, em alguns casos decorrentes de problemas históricos na aplicação de ferramentas de varredura derivadas de TI para ambientes OT. O que deve ser reconhecido, no entanto, é que as ferramentas de detecção e prevenção de intrusão específicas do sistema de controle (IDS/IPS) fizeram grandes avanços nos últimos anos e, com profissionais experientes envolvidos, têm pouco risco associado a elas. Eles são cada vez mais considerados um componente básico essencial na proteção de ativos e operações do sistema de controle.

Qual é o estado atual do monitoramento da atividade de rede do sistema de controle em sua organização?



Qual é o estado atual do monitoramento da atividade de rede do sistema de controle em sua organização? (Alta M vs. Baixa M)



Avaliações

Frequência

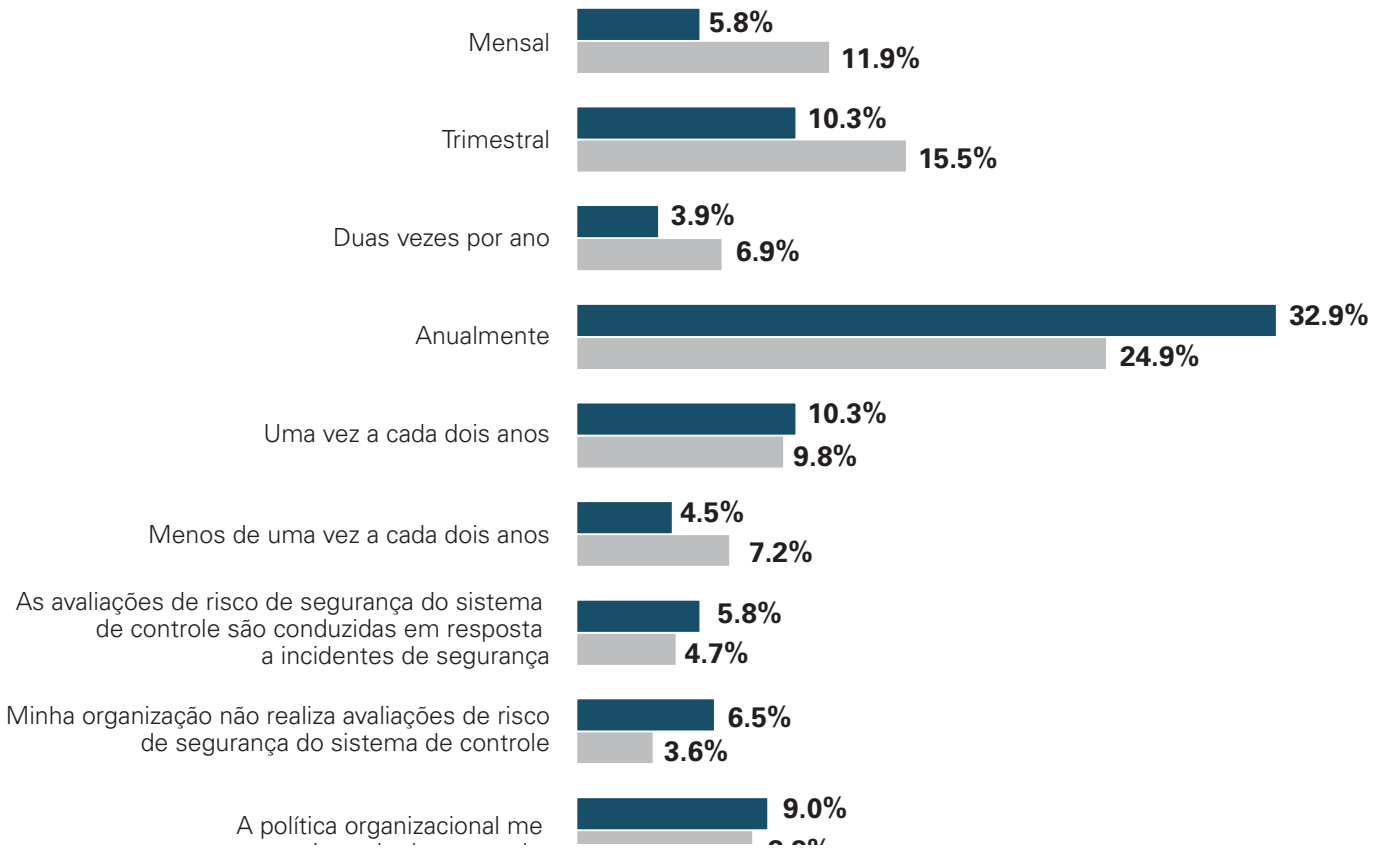
Embora a maior frequência de avaliações de segurança cibernética do sistema de controle relatadas continue sendo anual (24,9%), houve um aumento geral em cada taxa mais alta de ocorrência, o que só pode ser visto como positivo. O número de entrevistados que conduzem as Mensais aproximadamente dobrou (para 11,9%), e as Trimestrais aumentaram quase pela metade (para 15,5%).

Não observamos uma diferença significativa na frequência de avaliações realizadas por organizações com programas de segurança cibernética altamente maduros em relação aos menos maduros. A distinção tornou-se mais evidente quando consideramos a questão do que estava incluído nessas avaliações.

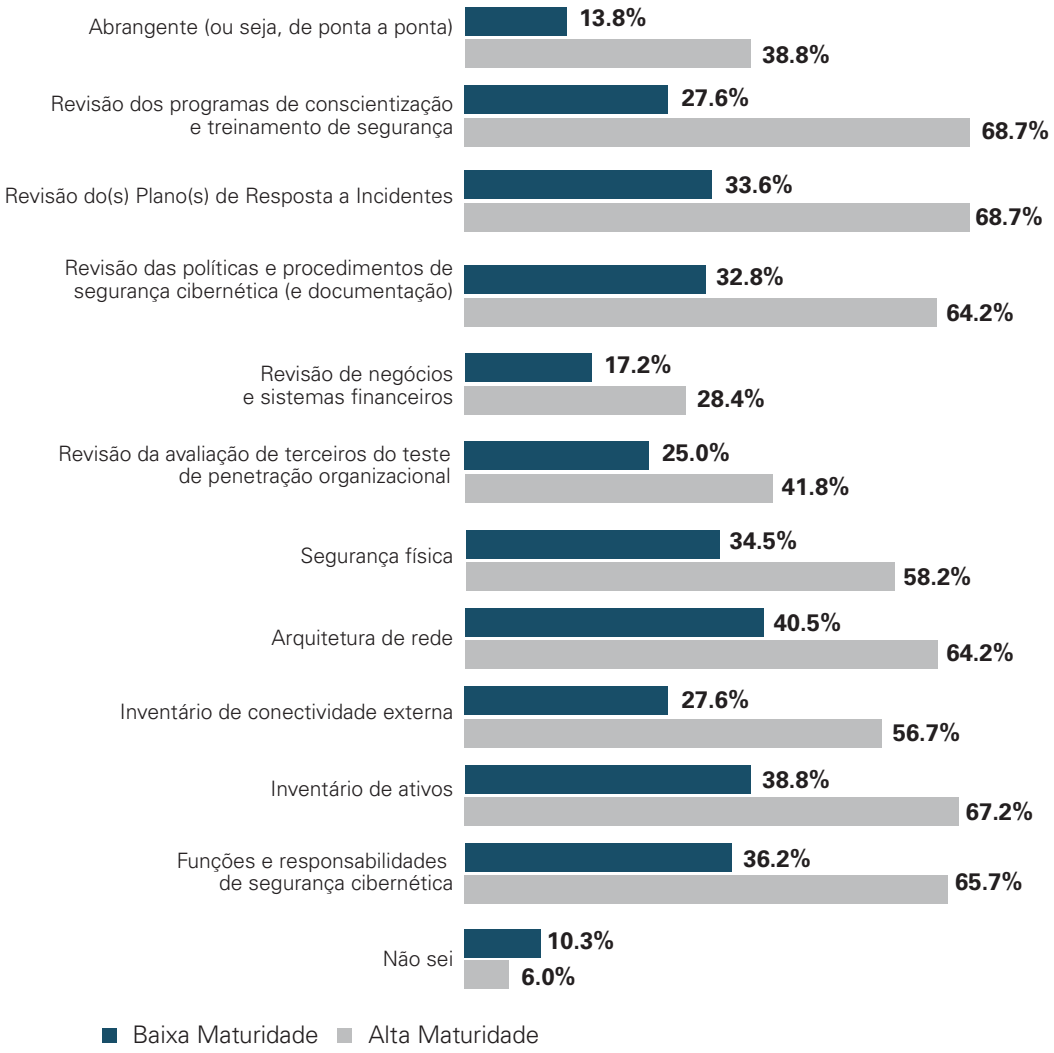
Inclusões

No entanto, as organizações com programas de segurança mais maduros evidentemente conduzem avaliações de segurança cibernética mais completas, não apenas incluindo cada componente com mais frequência do que aquelas com programas menos maduros, geralmente por margens amplas, mas também quase três vezes mais propensas a realizar Abrangente (ou seja, de ponta a ponta).) (Alta M 38,8 % vs. Baixa M 13,8 %).

Com que frequência sua organização realiza avaliações de segurança do sistema de controle?



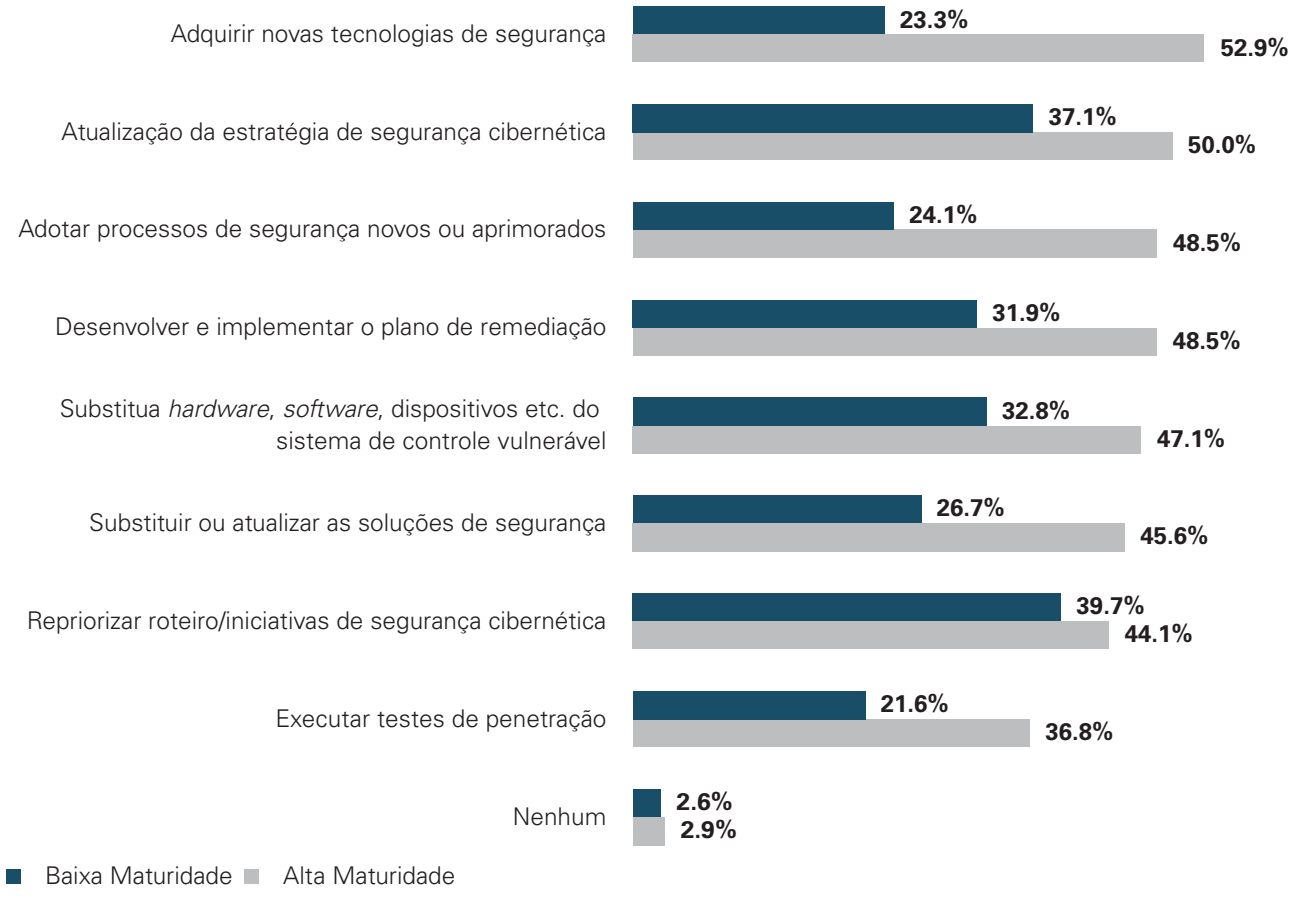
Identifique todos os componentes incluídos nas avaliações de segurança do sistema de controle da sua organização (Alta M vs. Baixa M)



Atividades de acompanhamento

Da mesma forma, os programas de maior maturidade são mais propensos a realizar uma ampla gama de ações de acompanhamento que respondem às conclusões dessas avaliações de segurança.

Selecione todas as atividades que sua organização realizou (ou planeja) em resposta às avaliações de segurança realizadas nos últimos 12 meses (Alta M *vs.* Baixa M)



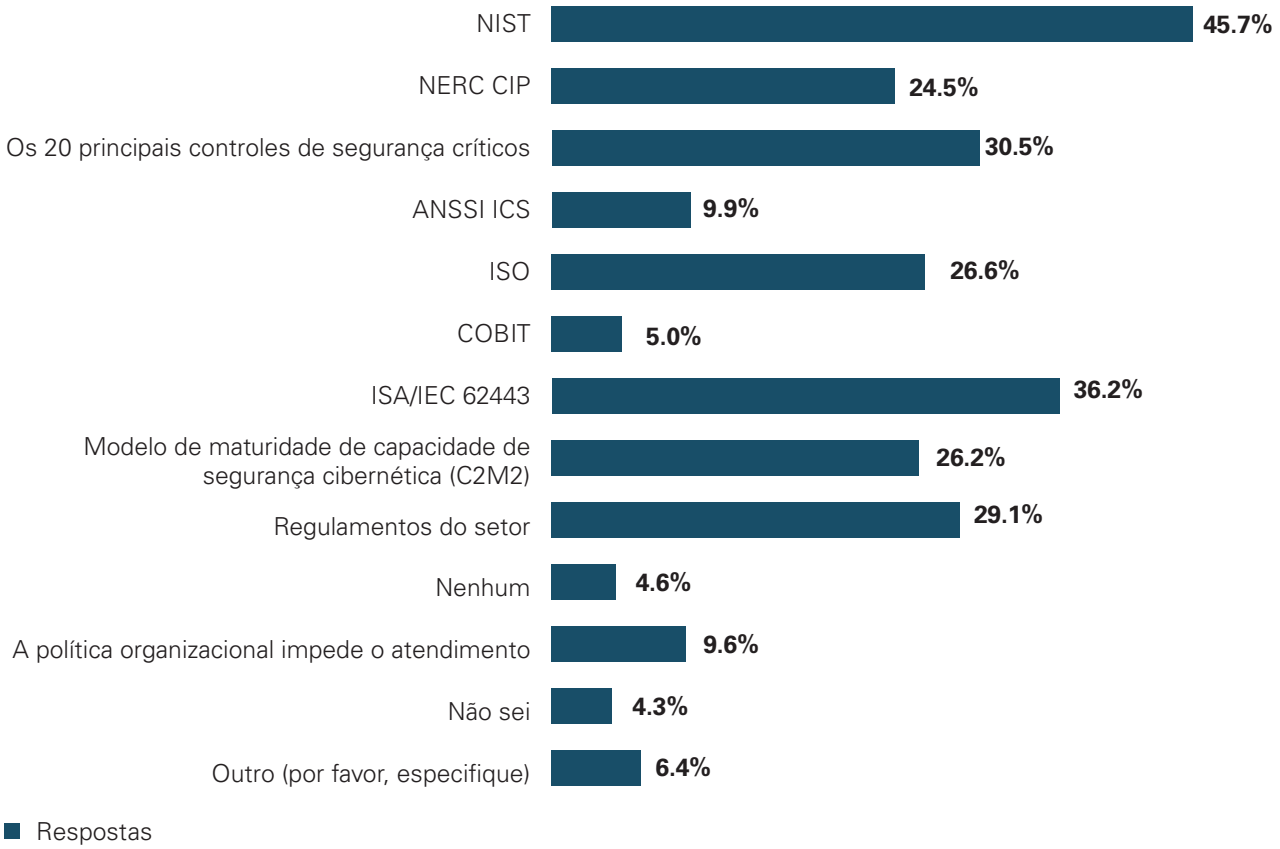
Frameworks em uso

O *framework* de segurança cibernética do NIST continua sendo o mais utilizado. A comparação direta com o nosso relatório anterior não é possível devido a mudanças nessa questão, mas vale a pena notar que duas opções de resposta não oferecidas em nossa pesquisa original, o Cybersecurity Capability Maturity Model (C2M2) e o ISA/IEC 62443, também estão em uso generalizado (26,2% e 36,2%, respectivamente).

Os 20 principais controles de segurança críticos se destacaram como o único *framework* citado com mais frequência pelos entrevistados com programas de segurança de baixa maturidade do que os de alta maturidade (30,1% vs. 28,6%). Os participantes do programa de segurança Alta Maturity relataram usar outros *frameworks* em taxas mais altas, sugerindo fortemente que suas organizações usem várias fontes de conhecimento para orientar seus programas com mais frequência do que suas contrapartes.

A conclusão clara não é que todos os programas de baixa maturidade devem adotar frameworks específicos para melhorar sua postura de segurança, mas que essas organizações devem incorporar **mais** fontes de orientação às melhores práticas e processos.

Selecione todos os seguintes *frameworks* usados por sua equipe de segurança do sistema de controle



Tecnologias em uso

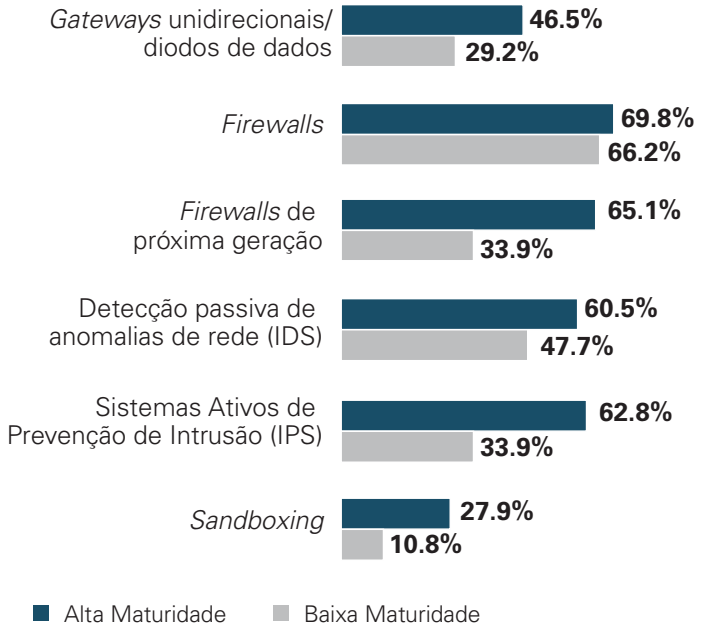
Encontramos várias tendências notáveis no uso de tecnologia de segurança entre as organizações de programas de segurança de alta maturidade. Elas têm aproximadamente metade da probabilidade de usar *gateways* unidirecionais/diodos de dados (46,5% Alta M vs. 29,2% Baixa M), quase duas vezes mais propensas a usar firewalls NextGen (65,1% Alta M vs. 33,9% Baixa M) e sistemas de prevenção de intrusão ativa (IPS) (62,8% Alta M vs. 33,9% Baixa M) e duas vezes mais probabilidade de usar Sandboxing (27,9% Alta M vs. 10,8% Baixa M).

Incidentes recentes

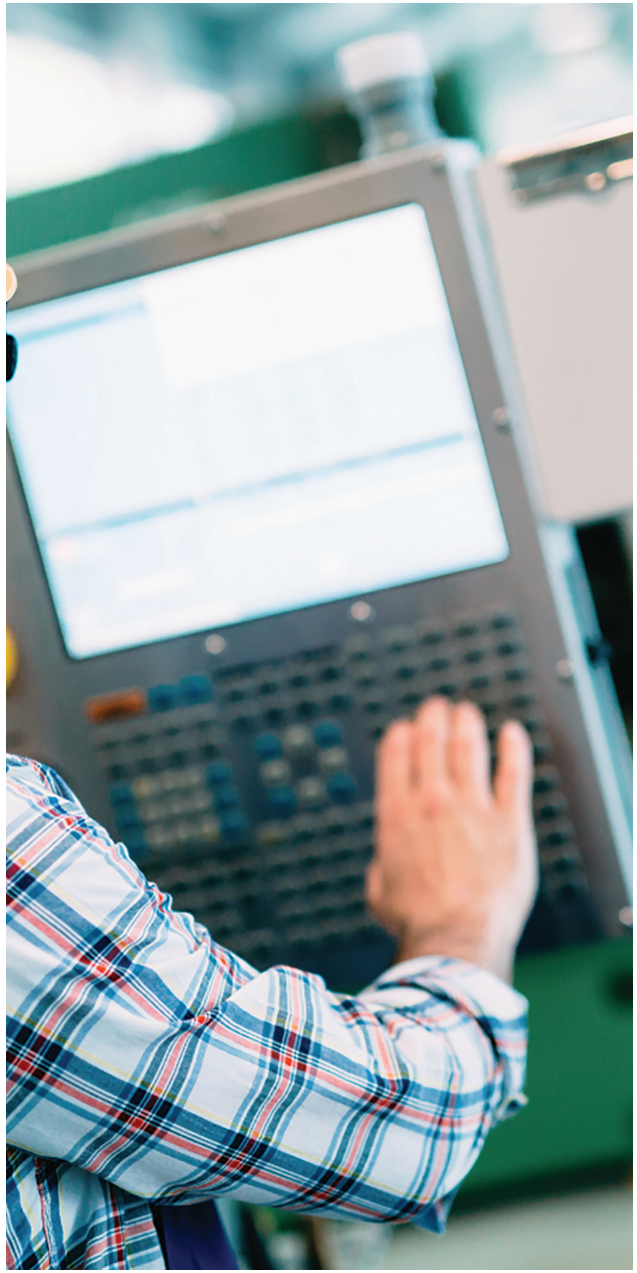
A análise longitudinal revelou um salto estatístico nos entrevistados que relataram mais de dez incidentes de segurança cibernética do sistema de controle no ano passado (4,6% em 2020 vs. 9,0% em 2021) e uma queda nos relatórios em cinco incidentes (26,2% em 2020 vs.17,4% em 2021).

Ao dividir as organizações dos entrevistados em subconjuntos por tamanho da força de trabalho, rapidamente fica claro que suas experiências eram diferentes. O número nitidamente maior de entidades na faixa de 500 a 1.000 funcionários relatando mais de 25 incidentes de segurança cibernética do sistema de controle nos últimos 12 meses (40,9%), agrupados por números muito semelhantes nas faixas de 100 a 500 e 1.000 a 5.000 (28,6 % e 28%, respectivamente), juntamente com a queda acentuada fora desse intervalo, sugere a possibilidade de que os malfeitores estejam mirando empresas desse porte.

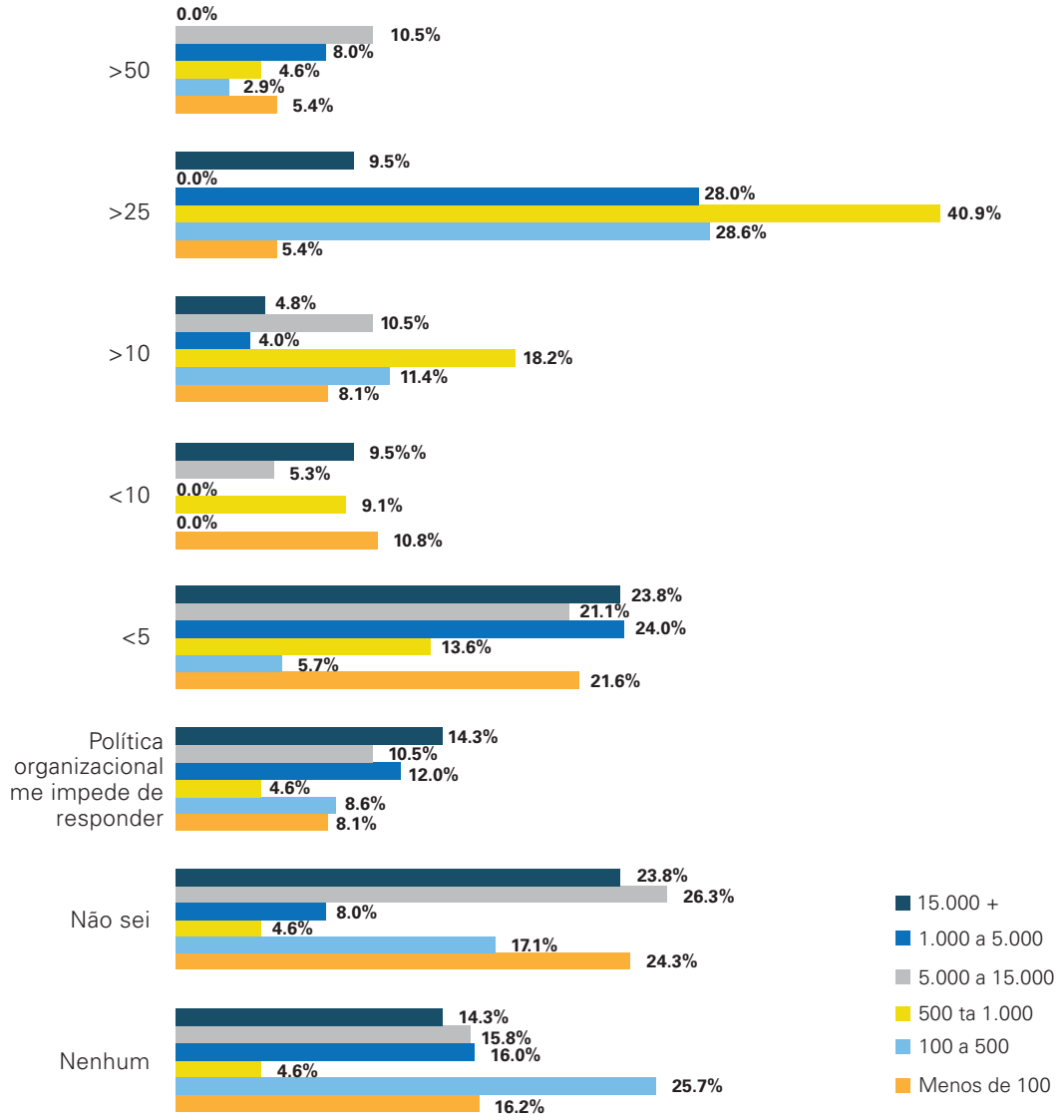
Indica todas as tecnologias de segurança em uso para proteger os ativos do sistema de controle de sua organização contra ameaças cibernéticas? (Alta M vs. Baixa M)



Qual é a sua melhor estimativa de quantos incidentes de segurança cibernética do sistema de controle ocorreram em sua organização nos últimos 12 meses?



Qual é a sua melhor estimativa de quantos incidentes de segurança cibernética do sistema de controle ocorreram em sua organização nos últimos 12 meses? (por tamanho da organização)



Impactos de incidentes recentes

Embora comparações diretas entre a pesquisa deste ano e o relatório anterior sobre essa questão não sejam possíveis devido a mudanças no design da pesquisa, há um claro aumento no número de entrevistados indicando "Lesão" (de 1,3% para 6,9%) e "Perda de Life" (de 1,3% para 6,2%) resultante de um incidente de segurança do sistema de controle no ano passado. Parte disso pode ser atribuída à maior representação de participantes na área de saúde (mais de 12% dos entrevistados em 2021 fazem pelo menos parte de seu trabalho com ou em hospitais) e ao enorme crescimento de ataques de ransomware em sistemas de saúde[3] na história recente.

As tendências adicionais observadas incluíram menos entrevistados citando políticas organizacionais ou falta de conhecimento que os impediam de responder (de 30,9% para 19,0% e de 34,9% para 13,1%, respectivamente). Que mais pessoas estão contribuindo com informações para esta pesquisa, tanto em números gerais quanto em dados reais fornecidos, só pode ser visto positivamente.

Selecione todos os impactos resultantes de incidentes de segurança de sistemas de controle nos últimos 12 meses

[3] https://thecrimereport.org/2021/08/18/hospitals-cyberattacks/

> “Em julho de 2021, a TSA ordenou que os operadores de dutos dos EUA melhorassem a segurança até o ponto em que os dutos continuassem operando, mesmo quando suas redes de TI estivessem comprometidas. Afinal, o que significa ‘encerrar com muita cautela’? Isso significa que não confiamos na força de nossos programas de segurança OT. Chegou a hora de adicionar uma camada de *gateways* unidirecionais reforçados por *hardware* em nossa defesa em profundidade, projetos de segurança OT/ICS.”

Andrew Ginter
VP Industrial Security, Waterfall Security Solutions

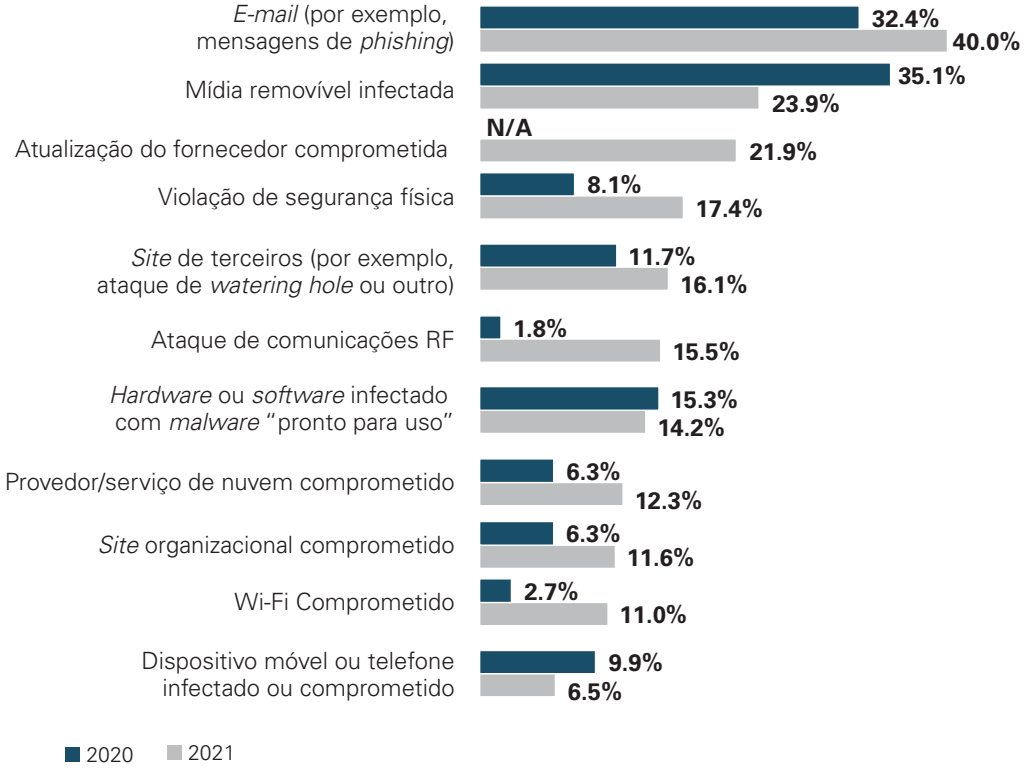
> Organizações de operações bem-sucedidas funcionam com base em métricas, metas, procedimentos detalhados e resultados táticos monitorados de hora em hora, diariamente e semanalmente. Os objetivos de segurança cibernética tendem a ser sutis ou aspiracionais: reduzir vulnerabilidades, identificar malware em potencial, identificar invasores, melhorar a resposta a incidentes etc., gráficos verdes.

Rick Kaun
VP Solutions na Verve Industrial Protection

Vetores de ataque recentes

Compromised Vendor Update, um vetor recém-adicionado em nossa pesquisa este ano, impactou um número maior de entrevistados do que o previsto, em 21,9%. Ao contrário de algumas perguntas que mostraram um possível efeito de diluição de opções de resposta adicionais, vários outros vetores aumentaram acentuadamente, particularmente Ataque de comunicações de RF (1,8% em 2020 vs.15,5% em 2021), Comprometimento de Wi-Fi (2,7% em 2020 *vs.* 11,0% em 2021), Violação de segurança física (8,1% em 2020 *vs.* 17,4% em 2021) e provedor/serviço de nuvem comprometido (6,3% em 2020 vs. 12,3% em 2021).

Selecione todos os vetores de ataque usados em qualquer um dos incidentes de segurança cibernética do sistema de controle que ocorreram em sua organização nos últimos 12 meses



“A pandemia da COVID-19 tornou ainda mais imperceptíveis as linhas entre os mundos físico e digital, expondo falhas na infraestrutura de segurança cibernética e desvendando uma série de novos desafios. No contexto pós-pandemia, a escassez de mão de obra no local é um desses desafios. Uma das principais razões para a falta de pessoal nos locais é que as empresas estão adotando acordos de trabalho híbridos e equipes divididas em meio a restrições relacionadas à COVID-19. Isso geralmente leva a ciclos de manutenção estendidos e soluções alternativas, como suporte de serviço remoto do contratado. Como resultado, os riscos da cadeia de suprimentos também aumentaram.

As comunicações sem fio apresentam outro caminho para os invasores entrarem em uma rede ICS. Frequências de rádio como 5G foram implantadas para facilitar as comunicações entre dispositivos/equipamentos que são móveis ou implantados em longas distâncias. Outras frequências de rádio podem ser usadas para controle manual no dia a dia ou para solução de problemas. O risco de usar frequências de rádio para comunicações é que elas geralmente são transmitidas e podem ser gravadas, submetidas à engenharia reversa, manipuladas e reproduzidas de maneiras que podem ter impacto na segurança e na produção. Um ponto de acesso Wi-Fi, comumente usado em rede doméstica, quando implantado em rede ICS, pode prejudicar o uso de diodo de dados destinado a estabelecer um airgap. Saber qual tecnologia está implantada em nossa rede ICS e entender quais riscos eles apresentam para os negócios não pode ser subestimado.”

Eddie Toh
Sócio, Head de Forensic Technology, Ásia-Pacífico, Advisory, Cyber, Advisory, KPMG Singapore

Fatores de ameaças

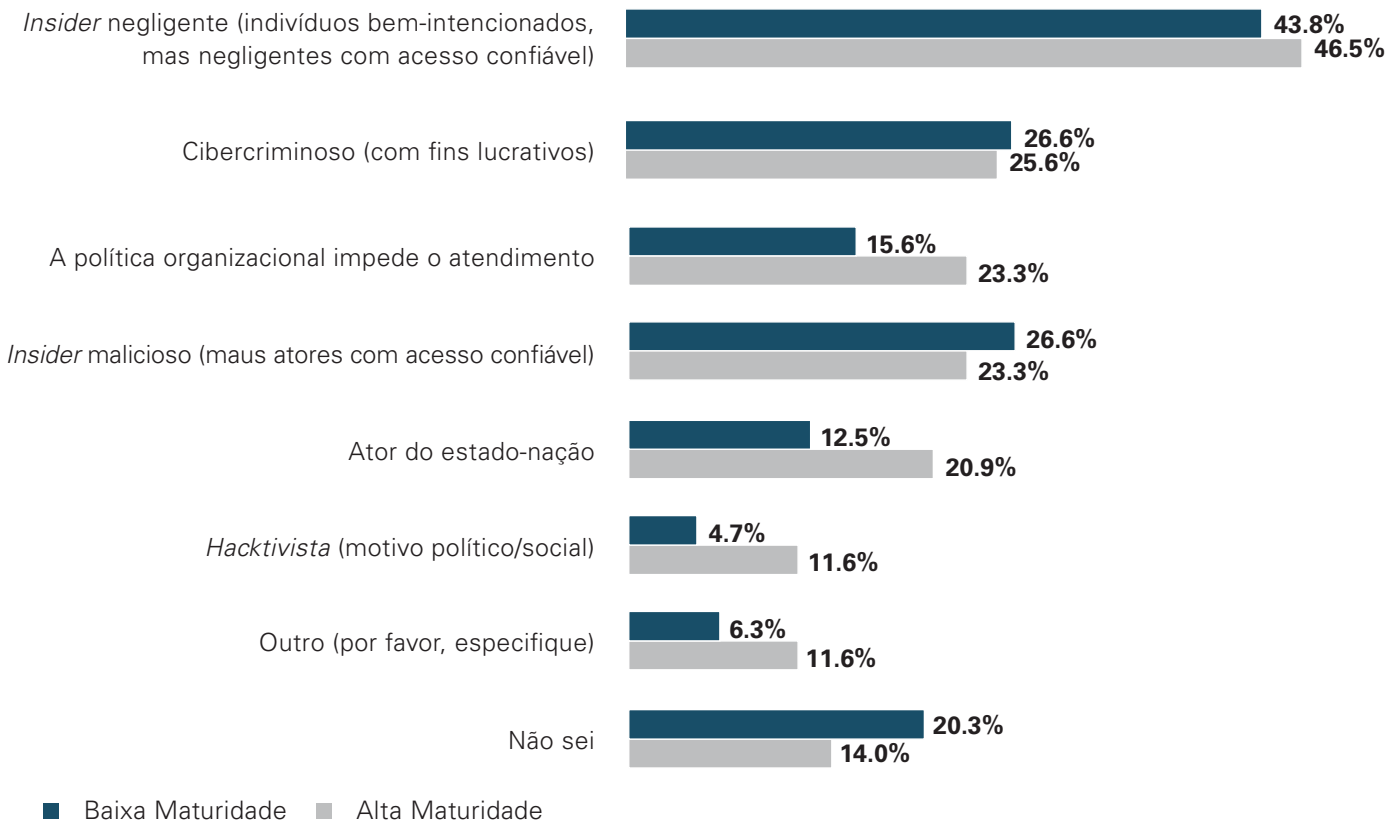
O *insider* negligente continua a ser o agente de ameaças mais comumente identificado em comprometimentos de segurança do sistema de controle. Faz parte de nossos ambientes de trabalho que esses indivíduos bem-intencionados, mas negligentes, com acesso confiável, possam causar interrupções em sistemas e processos devido à natureza de suas funções.

Reduzir a probabilidade de eles fazerem isso exige uma abordagem em duas frentes:

— Sempre que possível, implementar salvaguardas para forçar a confirmação de ações potencialmente disruptivas. Dependendo da situação/ambiente, eles podem assumir formas como limites de parâmetros, controles físicos ou verificações de autorização que exigem aprovação de segunda parte para entrar em vigor.

— Treinamento, incluindo operações técnicas e componentes de conscientização de segurança, para garantir que aqueles com acesso confiável saibam como desempenhar suas funções sem interrupções e os possíveis impactos de erros se forem negligentes.

Selecione todos os itens a seguir que descrevem os agentes de ameaças em seus recentes comprometimentos de segurança cibernética do sistema de controle (Alta M vs. Baixa M)

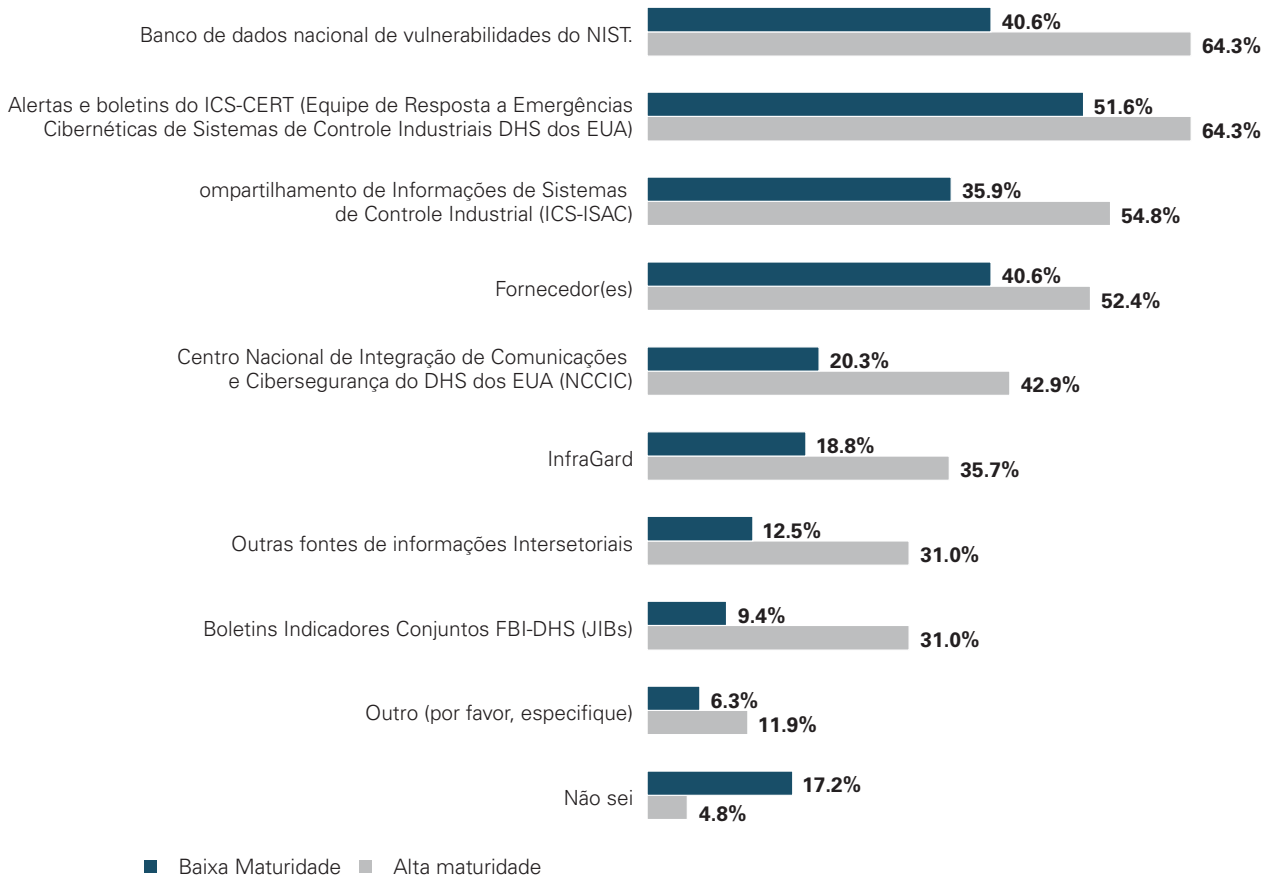


Fontes de informações sobre ameaças cibernéticas

It iÉ claro que os entrevistados dos programas de segurança cibernética do sistema de controle de alta maturidade utilizam mais fontes de informações sobre ameaças do que aqueles em programas de baixa maturidade, são muito menos propensos a não ter conhecimento das fontes em uso em suas organizações (4,8% de Alta Maturidade vs. 17,2% de Baixa Maturidade) e quase duas vezes mais propensos a usar fontes adicionais além da nossa lista (11,9% de Alta Maturidade vs. 6,3% de Baixa Maturidade).

A maior visibilidade de seus ambientes disponíveis para as organizações Alta M provavelmente é um fator para isso, pois permite que elas façam maior uso da inteligência de ameaças das várias fontes disponíveis.

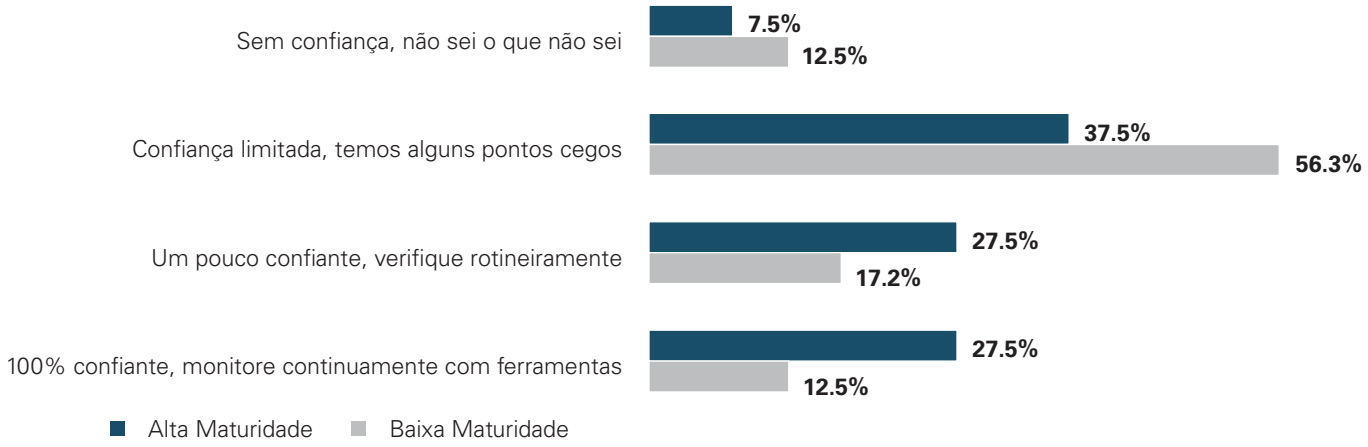
Indique qual das seguintes fontes de segurança cibernética do sistema de controle informações de ameaças que sua organização usa (Alta Maturidade *vs* Baixa Maturidade)



Confiança na visibilidade da rede

A maior parte dos entrevistados reconhece ter alguns pontos cegos em suas redes, discutindo dispositivos, aplicativos ou usuários. Aqueles de programas de segurança cibernética mais maduros costumam ter níveis mais altos de confiança em sua visibilidade sobre o que está acontecendo nas áreas pelas quais são responsáveis, mas é bom ver que quase dois terços desse grupo reconhecem que ainda há trabalho a ser feito (total de 65 % dos entrevistados de Alta Maturidade indicaram Confiança Limitada ou Um Pouco Confiante). Conjecturas baseadas em incidentes em andamento e avaliações de PMEs no campo sugerem que aqueles que estão 100% confiantes devem ser mais cautelosos em suas estimativas, mas desejamos a todos sucesso.

Quão confiante você está com a visibilidade dos dispositivos, usuários e aplicativos em sua rede? (Alta M vs. Baixa)

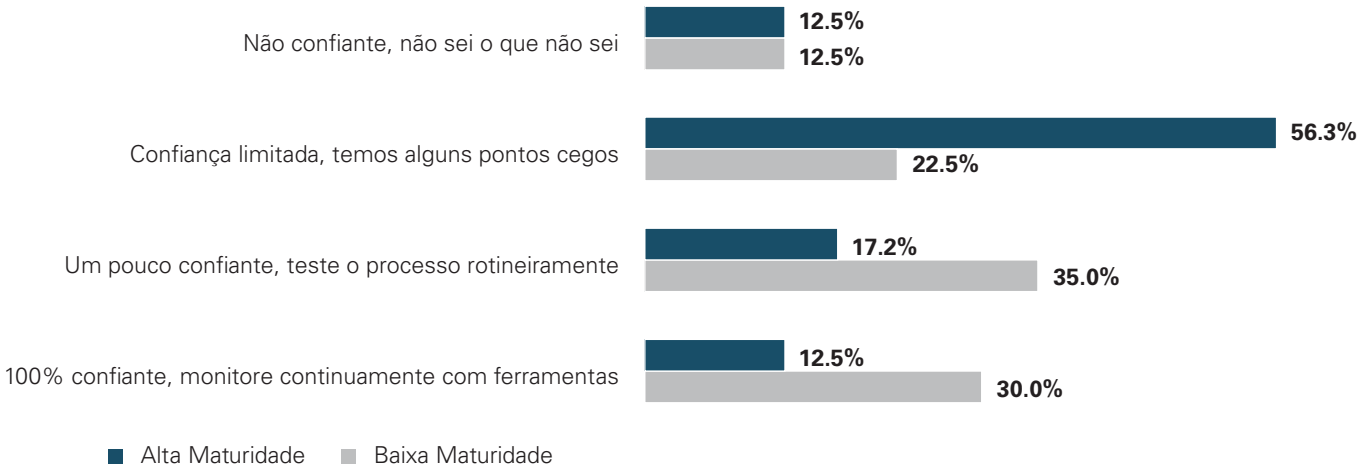


> A maioria das organizações tem pouca ou nenhuma confiança na visibilidade de sua rede e ativos devido à crescente complexidade e tamanho de seu ambiente. É importante entender que existem dois tipos de visibilidade de rede: monitoramento de tráfego ativo e revisão de arquitetura independente. O primeiro requer a implantação de sensores em campo, o que geralmente leva anos para ser concluído. Este último pode ser alcançado com uma solução de modelagem de rede sem sensor que requer apenas os arquivos de configuração de firewalls e roteadores, o que significa que as organizações podem aproveitá-la para obter visibilidade em sua arquitetura de rede muito mais rapidamente e com menor custo.

Robin Berthier
CEO, Network Perception

Confiança nos processos de resposta a ataques cibernéticos

Quão confiante você está em seus processos de resposta caso sua organização sofra um ataque cibernético? (Alta M vs. Baixa M)



Investimentos no próximo ano

Como um ponto de interesse particularmente importante para muitos de nossos leitores, analisamos as respostas à questão dos investimentos planejados em segurança cibernética de OT. Talvez a maior surpresa, dado o número de incidentes de cadeia de suprimentos bem divulgados e impactantes no ano passado, seja como poucos de nossos entrevistados pretendem concentrar recursos nessa área.

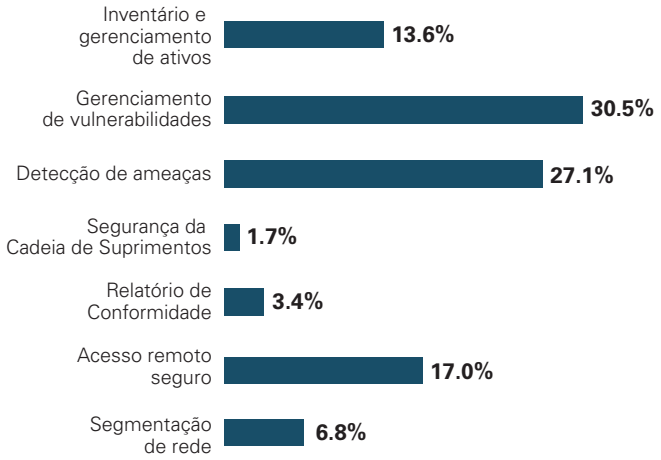
Visto através de uma lente de maturidade do programa de segurança cibernética, fica claro que os programas menos maduros percebem a necessidade de abordar o inventário e gerenciamento de ativos básicos, bem como o gerenciamento de vulnerabilidades (20,6% e 30,2%, respectivamente) mais do que seus equivalentes em ambientes mais maduros (15,4% e 15,4%, respectivamente). Ambos os grupos pretendem abordar deficiências na detecção de ameaças (20,6% de Baixa Maturidade e 23,1% de Alta Maturidade), e o grupo avançado está enfatizando a implementação da segmentação de rede (6,4% de Baixa Maturidade vs. 18% de Alta Maturidade).

“Apesar das crescentes ameaças e da crescente pressão pública, as organizações muitas vezes permanecem despreparadas. Como resposta, o setor de segurança cibernética inclui uma infinidade de serviços, muitos dos quais são relativamente novos e às vezes não testados. Confundidas por escolhas, muitas organizações acabam até desprotegidas. Portanto, investir na segurança de áreas de OT é um pré-requisito para os negócios industriais futuros e para a preparação de cultura, processo, pessoas e tecnologia. Os recursos de segurança cibernética precisam ser implementados para avaliar os sistemas existentes quanto a ameaças e monitorá-los continuamente no futuro.”

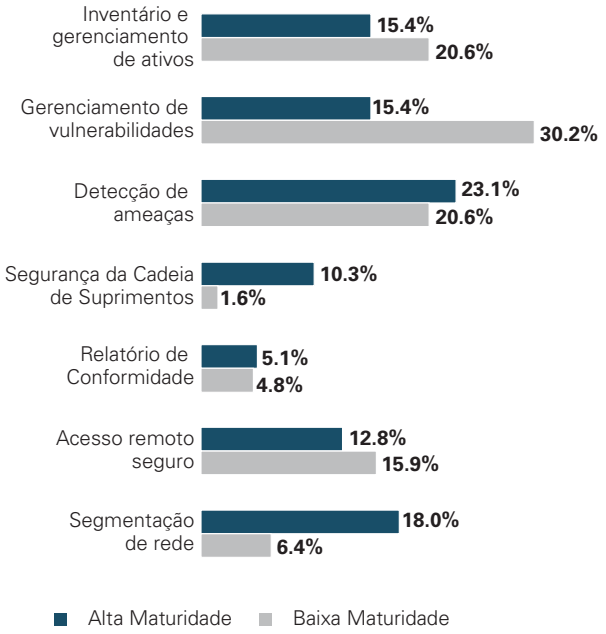
Hossain Alshedoki
Diretor associado, líder de ENR de segurança cibernética e privacidade de dados de TI/OT, KPMG na Arábia Saudita

Olhando especificamente para nossos tomadores de decisões financeiras e respondentes aprovadores, que deveriam ter o melhor conhecimento sobre o assunto, vemos uma concordância mais estreita, com mais da metade visando apenas a duas áreas: Gerenciamento de Vulnerabilidades (30,5%) e Detecção de Ameaças (27,1%).

Em qual elemento de segurança cibernética OT você investirá mais durante o próximo ano? (Tomadores de Decisões Financeiras e Aprovadores)



Em qual elemento de segurança cibernética OT você investirá mais durante o próximo ano? (Alta M vs. Baixa M)



Principais recomendações

Existem alguns conceitos-chave subjacentes à nossa abordagem sugerida para proteger seu ambiente de CS. Em primeiro lugar, a segurança é uma busca contínua e não um destino. O estado ideal de estar completamente seguro é apenas hipotético e provavelmente não alcançável no mundo de hoje. Decorrente disso, assumimos que a missão central da segurança é gerenciar o risco, ou seja, reduzi-lo a níveis aceitáveis. Os parâmetros dessa missão são estabelecidos pelos líderes organizacionais, que definem a tolerância ao risco e devem fornecer os recursos necessários para alinhar os riscos a esse apetite.

A ausência de uma solução "tamanho único" limita a especificidade das recomendações para orientar esses líderes, mas podemos sugerir e sugerimos que cada organização busque alguns objetivos básicos na medida do possível:

- Desenvolva sua força de trabalho, por meio de treinamento, educação e criação/melhoria de uma cultura de segurança em sua organização. Isso reduzirá o risco de ocorrência de incidentes, impactos e tempo de recuperação.
- Aumente sua percepção sobre seus ambientes de sistema de controle, melhorando o inventário de ativos e o monitoramento da atividade de tráfego de rede. Isso reduzirá a probabilidade e a duração das interrupções.
- Segmente seus sistemas de controle, tanto de redes não operacionais quanto, quando possível, entre si. Isso reduzirá o escopo dos incidentes, limitando sua capacidade de propagação.
- Investigue a segurança de sua cadeia de suprimentos e implemente controles em torno dos pontos de entrada em seus ambientes. Isso reduzirá o potencial de ataques a seus fornecedores que afetem você.

Apêndice A: Dados demográficos dos participantes

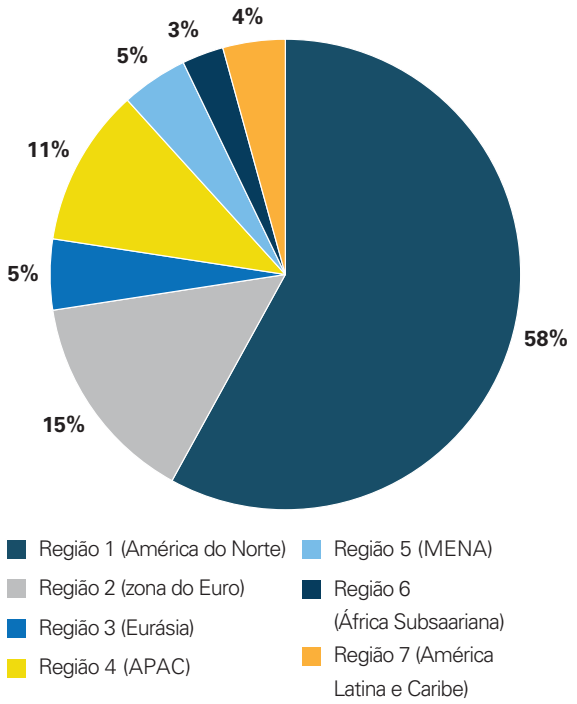
Dados demográficos dos respondentes

Localização

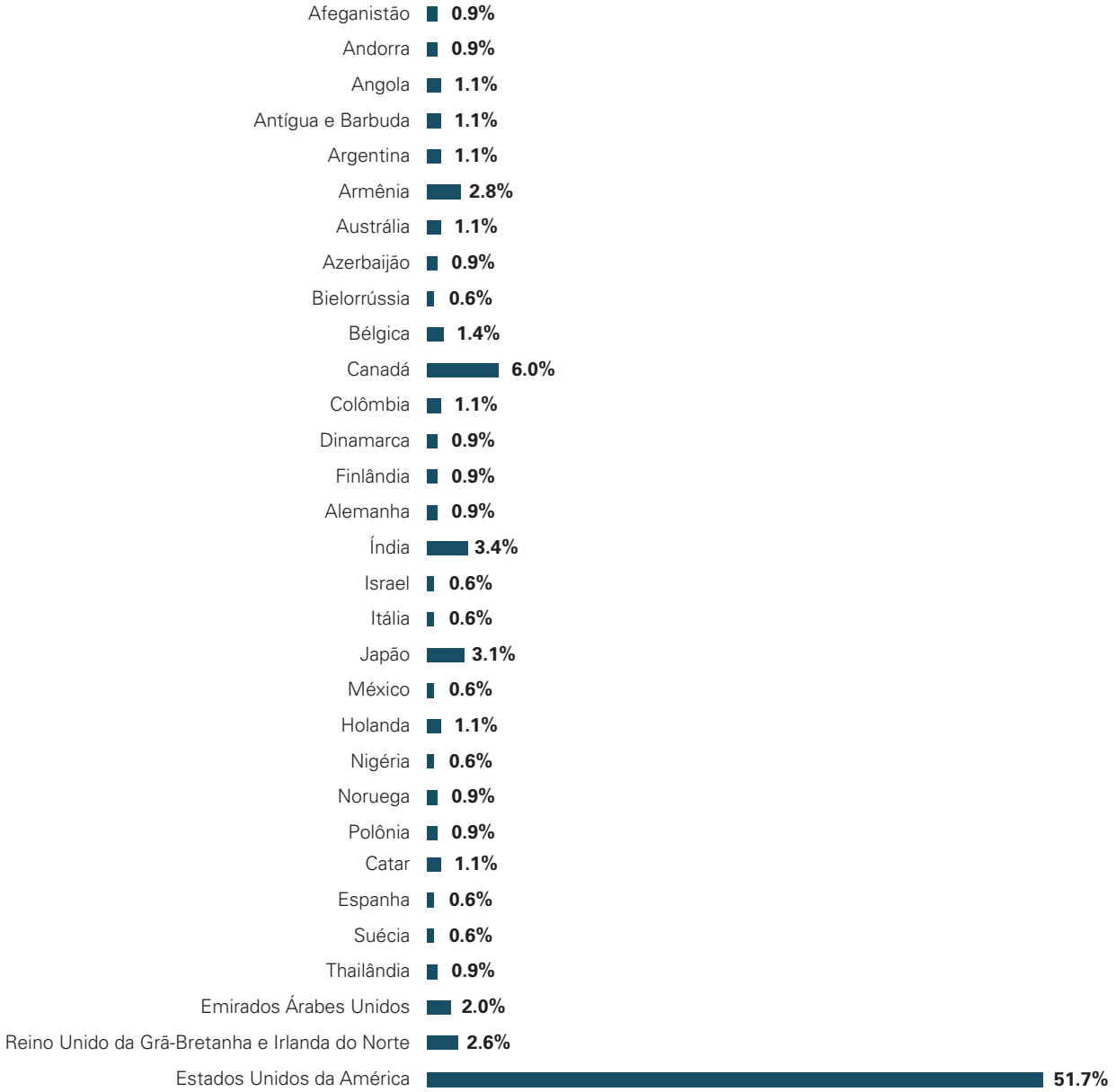
(CS)2AI viu seu número de membros crescer mais de 20% no ano passado, mas o grupo de participantes envolvidos em nossos projetos de pesquisa se estende muito além desse grupo, e é claro que esse corpo maior cresceu mais rapidamente na América do Norte. Em números absolutos, a resposta internacional aos nossos convites de pesquisa aumentou significativamente, como era nosso objetivo. No entanto, a participação dos EUA e do Canadá cresceu tanto que, em termos percentuais, essa região já representa mais da metade de nossos participantes.

Observe que a lista de países é parcial; muitos foram excluídos para fins de legibilidade.

Respostas por região



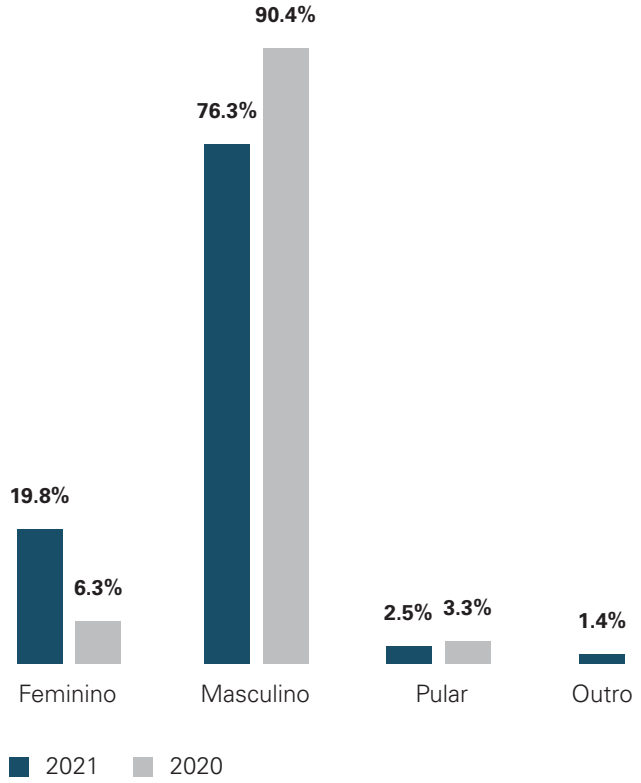
Por favor, identifique o país em que você trabalha principalmente



Participação de gênero

Entende-se que abordar a escassez dessa força de trabalho exigirá o recrutamento de todas as populações. Ficamos satisfeitos por ter alcançado um número muito maior de mulheres no campo de segurança cibernética CS este ano, com um número significativamente maior de participantes na pesquisa do que anteriormente. Isso nos oferece a oportunidade de considerar as diferenças de perspectivas entre esses grupos. Uma observação interessante sobre a representação aqui: descobrimos que as mulheres estão cerca de 50% mais propensas a trabalhar para organizações com tamanho de força de trabalho entre 100 e 1.000.

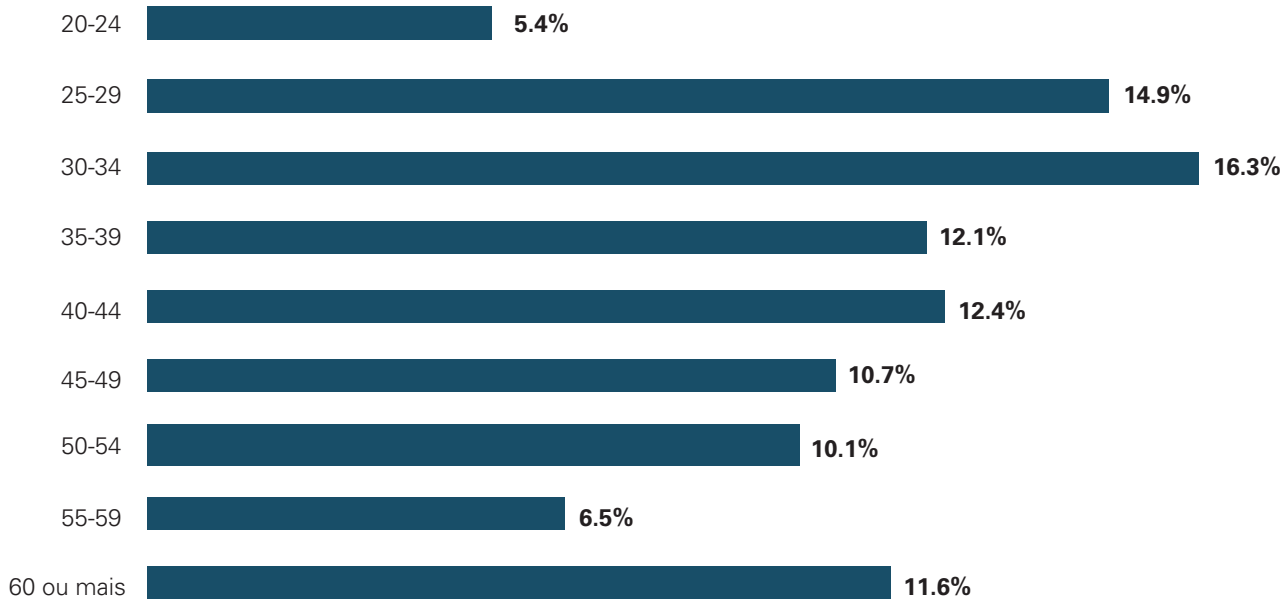
Por favor selecione seu gênero



Distribuição etária

Tomamos como sinal positivo de que o número de respondentes nas faixas etárias mais jovens aumentou acentuadamente este ano. O envelhecimento da força de trabalho de ciência e engenharia, da qual os profissionais de segurança cibernética de CS fazem parte, tem sido frequentemente relatado e apresenta preocupações tanto pela perda de conhecimento institucional quanto pelo efeito redutor nos recursos humanos disponíveis diante da crescente demanda . O efeito é particularmente pronunciado em nações altamente desenvolvidas, como os Estados Unidos, onde estamos vendo a combinação de níveis crescentes de infraestrutura interconectada e cadeias de suprimentos com rotatividade de gerações entre engenheiros profissionais. Com tudo isso em mente, estamos muito felizes em ver que a maioria (61,1%) de nossos participantes está na primeira metade de suas carreiras, com décadas restantes para contribuir com nossa missão compartilhada.

Selecione sua faixa etária



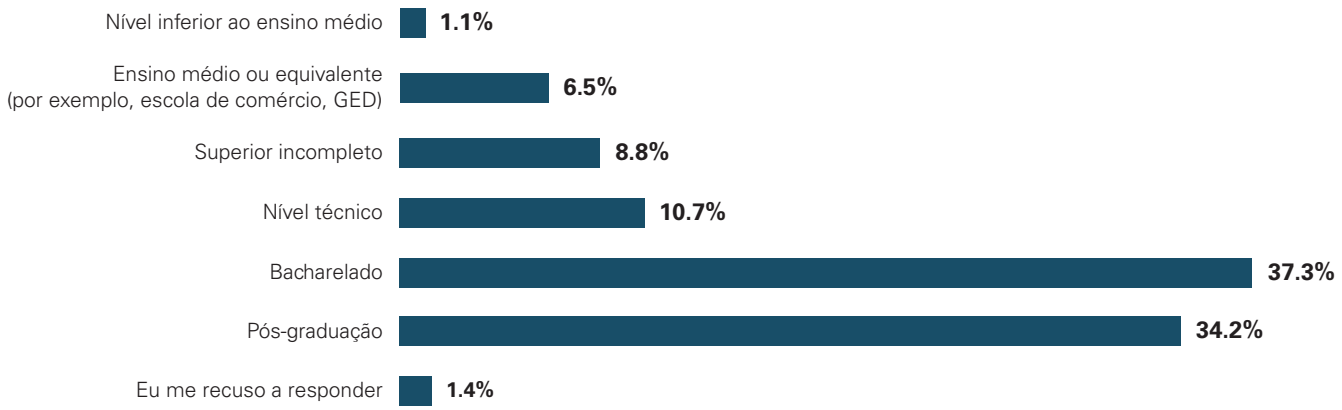
Tipo de emprego dos respondentes

Com acesso restrito ao aprendizado em sistemas de OT caros e os custos de treinamento técnico altos, a maioria dos profissionais os obtém por meio de seus empregadores, para os quais isso faz parte dos custos de fazer negócios. Continuamos a ver a grande maioria (59,8%) dos entrevistados trabalhando como funcionários da organização para a qual desempenham suas funções de segurança cibernética.

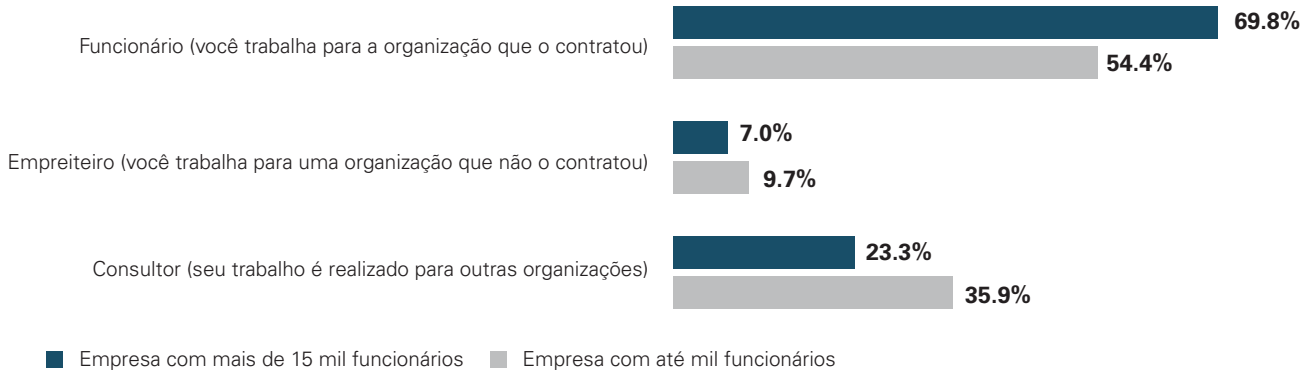
Observamos alguma diferença entre as organizações com base em seu tamanho, no entanto mostrando um aumento no uso de Consultores e Empreiteiros entre entidades com força de trabalho abaixo de 1.000. Isso pode refletir o efeito de restrições financeiras mais apertadas, reduzindo a capacidade dessas organizações na dedicação de recursos permanentes às tarefas de segurança cibernética.

Nível educacional dos respondentes

Por favor, selecione o nível mais alto de educação que você concluiu ou o grau mais alto que você recebeu



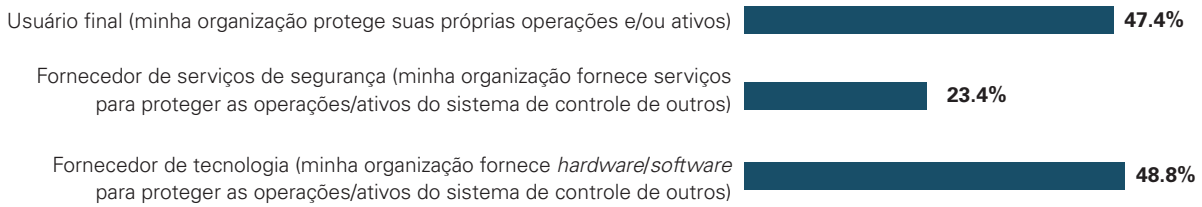
Selecione a descrição que melhor se adapta à sua posição de trabalho



Categoria da organização

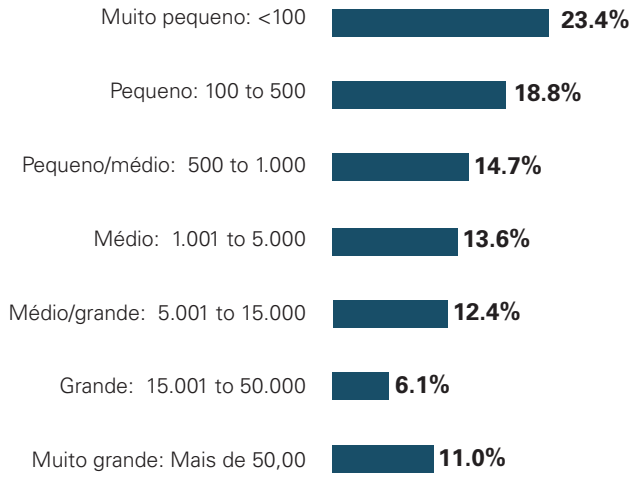
Observe que os entrevistados puderam escolher mais de uma categoria. Enquanto poucos o fizeram, as respostas nesta tabela somam mais de 100% devido a isso.

Identifique a categoria da sua organização em relação à segurança cibernética do sistema de controle



Forneça sua melhor estimativa da força de trabalho da sua organização

Forneça sua melhor estimativa da força de trabalho da sua organização



Apêndice B: Comitê de direção do relatório anual

Derek Harp

(CS)2AI Fundador e Presidente: Presidente de Pesquisa e Relatório Anual, Coautor

Bengt Gregory-Brown

(CS)2AI Cofundador e Presidente: Diretor de Pesquisa e Relatório Anual, Designer e Analista Líder, Coautor

John Merkel

(CS)2AI Analista de Dados Líder, Cientista de Dados Líder de Pesquisa e Relatório Anual

Walter Risi

(CS)2AI Strategic Alliance Partner Liaison, Survey Design e Report Analysis Teams Líder Global de Cyber IoT KPMG na Argentina

Em nome de toda a comunidade, a (CS)2AI gostaria de estender um sincero **agradecimento** ao Comitê Diretor do Relatório Anual de 2022. Desde a revisão de perguntas, ajudando na divulgação da ferramenta de pesquisa, estudando resultados, fornecendo ou editando conteúdo e distribuindo o relatório final. Esse grupo de profissionais viabiliza esse esforço anual. É um dos melhores exemplos de (CS)2AI **Membros Ajudando Membros.**

Brad Raiford
Equipes de Design de Pesquisa e Análise de Relatório KPMG nos EUA

Hossain Alshedoki
Equipe de Análise de Relatórios KPMG na Arábia Saudita

Eddie Toh
Equipe de Análise de Relatórios KPMG em Cingapura

Jaco Benadie
Equipe de Análise de Relatórios KPMG na Malásia

Sandra Cusato
Líder de Produção de Relatórios KPMG International

Andrew Ginter
(CS)2AI Strategic Alliance Partner Liaison, Survey Design e Equipes de Análise de Relatórios

Soluções de segurança em cascata

Bryan Singer
Equipe de Análise de Relatórios Accenture

William Noto
Equipe de Análise de Relatórios Fortinet

George Kalavantis
Equipe de Análise de Relatórios Industrial Defender

Robin Berthier
Percepção de rede da equipe de análise de relatórios

William Malik
Equipe de Análise de Relatórios Trend Micro

Ron Indeck
Equipe de Análise de Relatórios Q-Net Security

Keith Beeman
Equipe de análise de relatórios temperada

Rick Kaun
Equipe de Análise de Relatórios Verve Industrial

Richard Springer
Equipe de Análise de Relatórios Tripwire

Apêndice C: Sobre (CS)²AI

VISÃO

Fortalecer a infraestrutura crítica global promovendo a rede e o desenvolvimento ponto a ponto da segurança cibernética do sistema de controle.

MISSÃO

Uma organização internacional que capacita organizações *Peer-to-Peer* e apoia seus esforços de base.

METAS

- Rede profissional
- Alianças globais
- Desenvolvimento profissional
- Alcance da comunidade
- Oportunidades de liderança

(CS)²AI ("*See-Say*" para abreviar) é uma associação global sem fins lucrativos em rápido crescimento, com cerca de 24.000 membros em todo o mundo, a principal organização global sem fins lucrativos de desenvolvimento de força de trabalho que apoia profissionais de todos os níveis encarregados de proteger sistemas de controle. Fornecemos a plataforma para que os membros ajudem os membros, promovam trocas significativas entre pares, continuem a educação profissional e apoiem diretamente o desenvolvimento profissional de segurança cibernética em todos os sentidos.

Rede *Peer-to-Peer* em escala global

Como membro do (CS)²AI, você se junta a uma comunidade global de profissionais de segurança cibernética do sistema de controle que estão motivados a melhorar e se desenvolver pessoal e profissionalmente nesta área altamente crítica e campo consequente.

(CS)²AI oferece um local para conexões ponto a ponto, interações em pequenos grupos com os principais especialistas do setor, compartilhamento de experiências, desafios e práticas recomendadas e recursos que você precisa para desenvolver e crescer. Explore a crescente variedade de oportunidades exclusivas para membros (CS)²AI projetadas para ajudá-lo a alcançar o próximo nível em sua jornada de carreira.

Se você ainda não é um membro ativo da Associação Internacional de Segurança Cibernética do Sistema de Controle, convidamos você a se juntar aos nossos esforços de "membros-ajudando-membros" envolvendo-se hoje. Nossa associação tem muitas maneiras de contribuir como membro global, palestrante, professor, mentor, parceiro, colaborador, membro de comitê, (CS)2AI companheiro ou participante de pesquisa.

Apêndice D: Patrocinadores de relatórios

A (CS)²AI deseja estender nossos sinceros agradecimentos aos seguintes Parceiros da Aliança Estratégica por suas contribuições contínuas para este relatório anual e, mais importante, por seu apoio aos profissionais de segurança cibernética em todo o mundo que estão se esforçando para proteger os sistemas críticos em que todos confiamos.

Patrocinador Titular

KPMG

Patrocinador da Edição

Fortinet

Waterfall Security

Sable Lion Cyber

Patrocinadores

Applied Risk

Network Perception

Trend Micro

GBQ Partners

Q-Net Security

Tripwire

Industrial Defender

Tempered

Verve Industrial

Fale com o nosso time

Rodrigo Milo
Sócio de Cyber Security da KPMG no Brasil
rodrigomilo@kpmg.com.br

kpmg.com.br

/kpmgbrasil