SOPHOS
Cybersecurity evolved.

A Equipe de Segurança de TI: 2021 e além

Resultados de uma pesquisa com 5.400 gerentes de TI em 30 países

Documento técnico Sophos. Junho, 2021

As equipes de TI têm se mantido na linha de frente para responder à pandemia em praticamente todas as organizações. A TI tem desempenhado um papel direto e essencial, capacitando as organizações a continuarem trabalhando apesar das restrições e limitações que a COVID-19 exigiu. Em grande parte, é graças ao comprometimento e à paixão das equipes de TI em todo o globo que tantas organizações conseguiram se manter em operação durante a pandemia. Elas ajudaram as instituições de ensino a entregar aprendizado online, permitiram que o varejo comercializasse via online e assegurou que os órgãos públicos pudessem continuar a providenciar os serviços básicos, e esses são apenas alguns poucos exemplos.

Esse relatório, baseado no feedback direto de 5.400 gerentes de TI distribuídos em 30 países, coloca em evidência a realidade que as equipes de TI têm enfrentando nos últimos 12 meses. Ela revela as mudanças pelas quais as equipes de TI passaram no decorrer de 2020, com foco especial na segurança cibernética, e o impacto dessas mudanças no pessoal das equipes de TI. O relatório também analisa o futuro das equipes de segurança de TI, expondo as expectativas para a TI nos próximos cinco anos e ajudando as organizações a desenvolver hoje a equipe de TI do futuro.

Principais descobertas

Mudanças pelas quais as equipes de TI passaram no decorrer de 2020

- **A carga de trabalho de segurança cibernética E TI cresceu:** 63% viram um aumento em cargas de trabalho não relacionadas à segurança, enquanto 69% experimentaram um aumento na carga de trabalho de segurança de TI
- **Os ataques cibernéticos ficaram mais predominantes:** 61% registraram um aumento no número de ataques cibernéticos em suas organizações
- **As equipes de TI foram capazes de aprimorar suas capacidades em segurança cibernética:** 70% das equipes de TI disseram ter desenvolvido suas habilidades e conhecimentos em segurança cibernética durante esse período
- **A adversidade uniu as equipes:** 52% disseram que o moral da equipe aumentou no decorrer do ano, e as vítimas de ransomware foram consideravelmente mais propensas a ter sentido um aumento no moral do que aqueles que não foram afetados (60% x 47%)

O presente estado do momento

- **As equipes de TI precisam de ajuda para lidar com ataques complexos:** 54% dizem que os ataques cibernéticos estão muito avançados para as suas equipes de TI lidarem com eles por conta própria
- **As equipes de TI se sentem bem equipadas para os desafios à frente:** 82% acreditam ter as ferramentas e conhecimentos para investigar atividades suspeitas completamente

A equipe de TI do futuro

- **As equipes de segurança de TI estão destinadas a crescer em tamanho**
  - 68% preveem um aumento de pessoal interno de segurança de TI até 2023, e 76% até 2026
  - 56% esperam um aumento no número de pessoal terceirizado de segurança de TI até 2023, e 64% até 2026.
- **A tecnologia de IA é a chave para as estratégias de segurança do futuro**
  - 92% esperam que a IA ajude a lidar com o crescente número de ameaças e sua complexidade

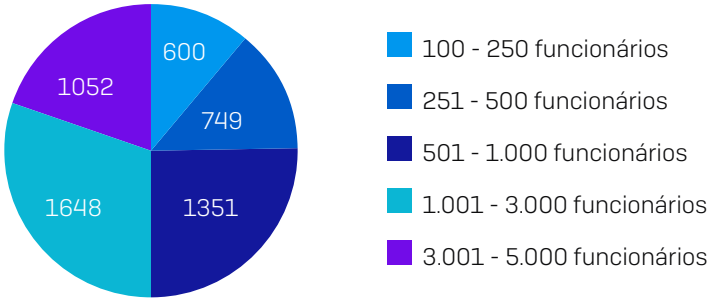
Sobre a pesquisa

A Sophos encarregou uma firma independente de pesquisa de opinião, a Vanson Bourne, para realizar um estudo com 5.400 tomadores de decisão de serviços de TI em 30 países. A pesquisa foi conduzida em janeiro e fevereiro de 2021.

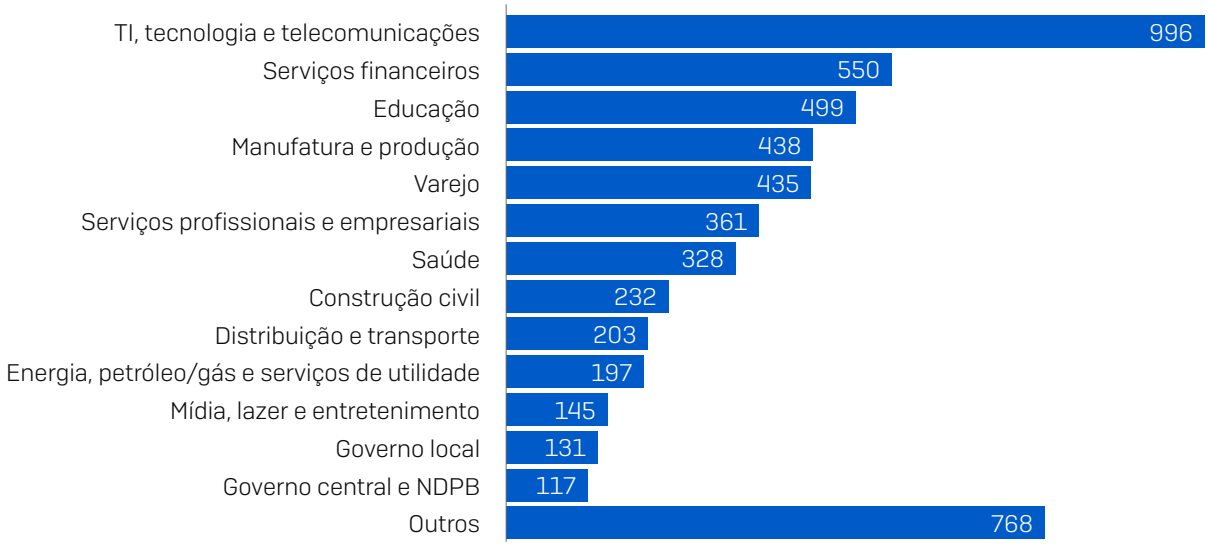
País	Nº de respondentes	País	Nº de respondentes	País	Nº de respondentes
Austrália	250	Índia	300	Arábia Saudita	100
Áustria	100	Israel	100	Singapura	150
Bélgica	100	Itália	200	África do Sul	200
Brasil	200	Japão	300	Espanha	150
Canadá	200	Malásia	150	Suécia	100
Chile	200	México	200	Suíça	100
Colômbia	200	Países Baixos	150	Turquia	100
República Tcheca	100	Nigéria	100	EAU	100
França	200	Filipinas	150	Reino Unido	300
Alemanha	300	Polônia	100	EUA	500

50% dos respondentes de cada país vieram de organizações com entre 100 e 1.000 funcionários e 50% vieram de organizações com entre 1.001 e 5.000 funcionários. Os respondentes também vieram de uma grande diversidade de setores.

Quantos funcionários a sua organização tem em âmbito global? [5.400]



Em que setor se encontra a sua organização? [5.400]



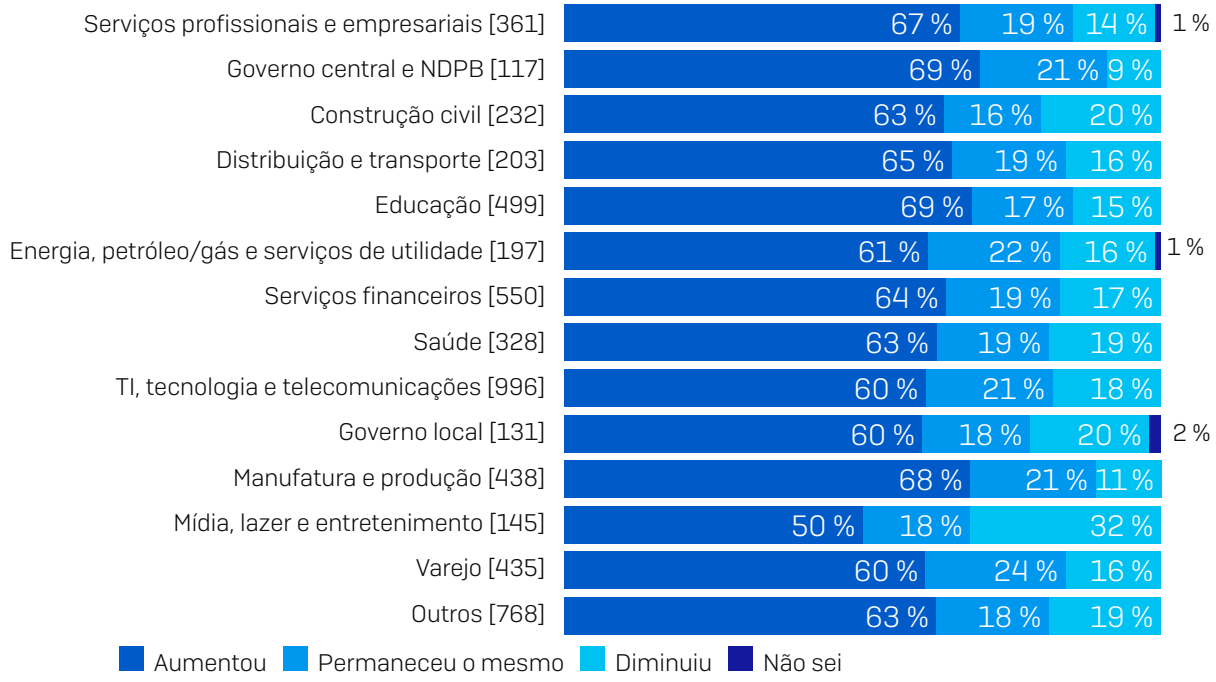
2020: um ano de mudanças

O ano de 2020 foi irrefutavelmente um ano inesquecível para as equipes de TI que tomaram a linha de frente para capacitar as organizações a adaptarem suas operações em resposta à pandemia, e não surpreende que isso tenha tido um considerável impacto na carga de trabalho.

A carga de trabalho de TI não relacionada à segurança cresceu...

2020 trouxe muito trabalho extra às equipes de TI: 63% dos gerentes de IT disseram que suas cargas de trabalho não relacionadas à segurança aumentaram no decorrer de 2020, e apenas 17% experimentaram uma diminuição. Os respondentes na Turquia (84%), Áustria (81%) e EUA (75%) foram mais propensos a registrar aumento na carga de trabalho.

Como a carga de trabalho de TI (não relacionada à segurança) mudou no decorrer de 2020



Durante o ano de 2020, nossa carga de trabalho de TI (não relacionada à segurança) diminuiu/aumentou/permaneceu a mesma [tamanhos de base no gráfico], dividido por setor

Analisando os dados por setor, podemos ver que as equipes de TI em **governo central e NDPB** e **educação** foram as que sofreram mais impacto, com 69% dos respondentes dizendo que a carga de trabalho aumentou durante o ano, provavelmente devido ao papel central que as organizações governamentais e educacionais desempenharam na resposta à pandemia. De modo recíproco, **mídia, lazer e entretenimento** tiveram a mais alta porcentagem de respondentes que registraram uma diminuição (32%), provavelmente devido, em parte, à pandemia, que forçou muitos deles a limitar seus serviços.

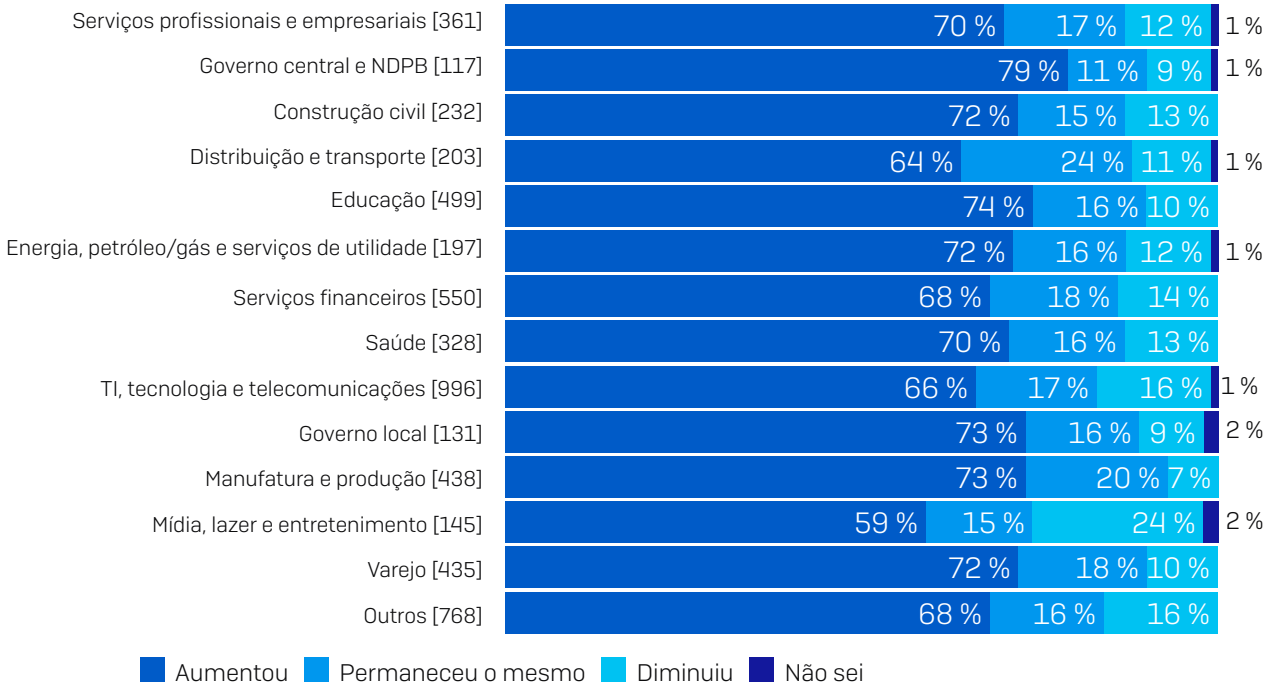
...e a carga de trabalho de segurança cibernética cresceu ainda mais

Como a carga de trabalho de segurança cibernética mudou no decorrer de 2020

Durante o ano de 2020, nossa carga de trabalho de segurança cibernética diminuiu/aumentou/permaneceu a mesma [5.400], omitindo "Não sei"

69% dos respondentes registraram um aumento em suas cargas de trabalho de segurança cibernética em comparação ao ano anterior, 13% registraram uma diminuição e 17% disseram que suas cargas de trabalho permaneceram as mesmas. Mais uma vez, a Turquia (82%) registrou o maior índice de aumento, seguida pela Suécia (80%), Israel e Brasil (ambos 78%). Por outro lado, os respondentes nos EAU tendenciaram a registrar uma diminuição na carga de trabalho de segurança cibernética (26%), seguidos pela Suíça (22%) e pela Nigéria e Filipinas (ambos 19%).

Como a carga de trabalho de segurança cibernética mudou no decorrer de 2020



Durante o ano de 2020, nossa carga de trabalho de segurança cibernética diminuiu/aumentou/permaneceu a mesma [tamanhos de base no gráfico], dividido por setor

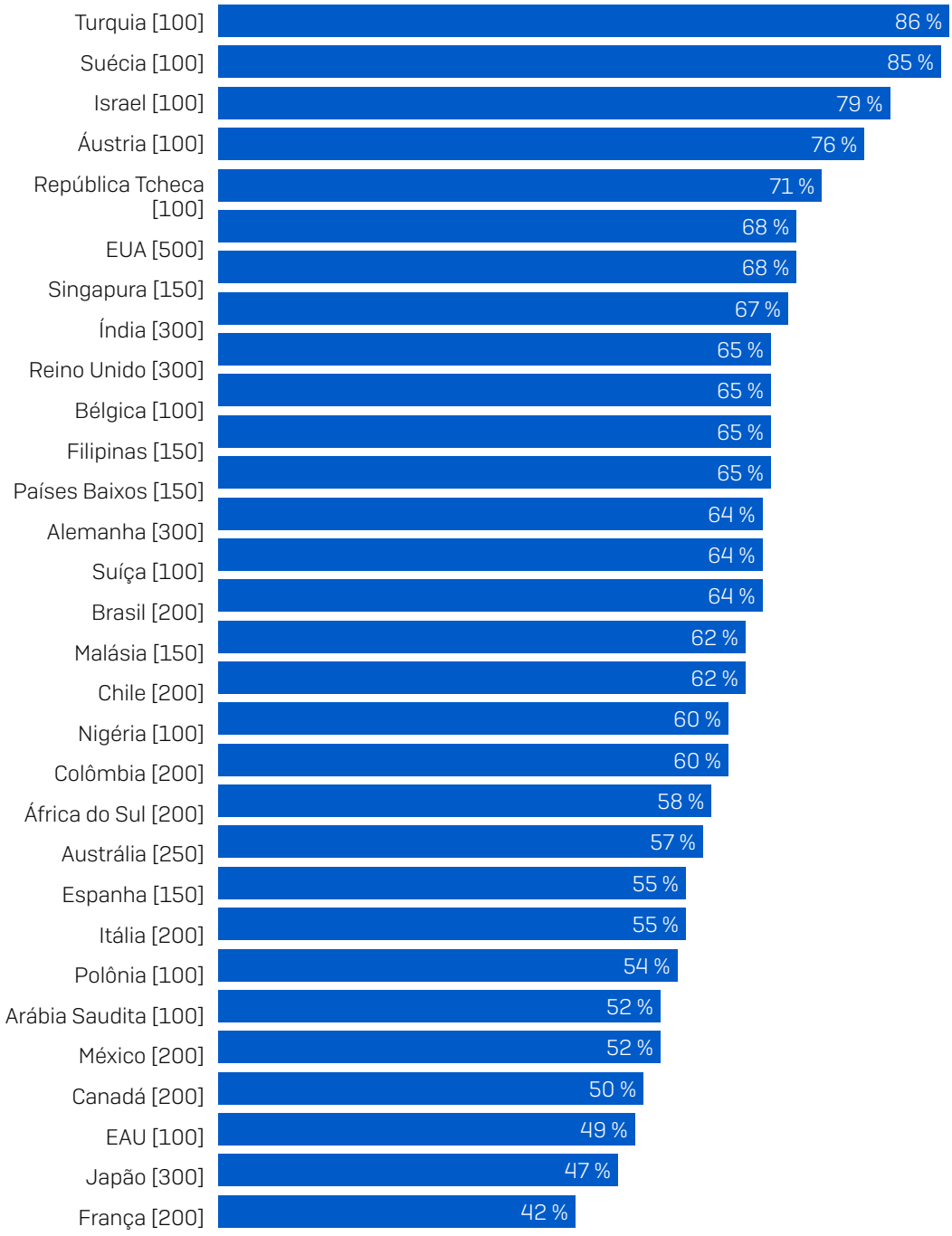
Ressonando a tendência do setor que vimos anteriormente, os gerentes de TI em **governo central e NDPB** (79%) e **educação** (74%) foram os que mais registraram aumento na carga de trabalho de segurança cibernética durante o último ano, enquanto o setor de **mídia, lazer e entretenimento** foi mais propenso a registrar uma diminuição (24%). Novamente, isso provavelmente se deve ao fator de esses setores estarem entre os mais afetados pela pandemia, ainda que de modos bastante diferentes.

Ataques cibernéticos aumentaram em frequência

Esse peso extra à carga de trabalho de segurança cibernética durante 2020 foi levado, em parte, pelo aumento em ataques cibernéticos: mais de seis em dez (61%) respondentes registraram aumento nos ataques às suas organizações no ano passado. Apenas 19% registraram queda.

Esse crescimento ocorreu em todos os setores, e a variação entre aqueles que sentiram o maior aumento **(governo central e NDPB)** e o menor aumento **(TI, tecnologia e telecomunicação** e **mídia, lazer e entretenimento)** foi de apenas 16 pontos percentuais (74% x 58%).

Porcentagem de organizações respondentes que experimentaram aumento em ataques cibernéticos no decorrer de 2020

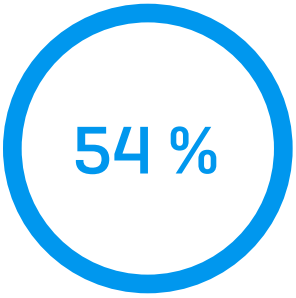


No decorrer de 2020, os ataques cibernéticos aumentaram [tamanhos de base no gráfico], omitindo algumas opções de resposta, dividido por país

Contudo, quando analisamos os dados por país, notamos uma variação bem maior no número de experiências, com mais do dobro de respondentes na Turquia registrando um aumento nos ataques em comparação com a França (86% x 42%). Altas porcentagens de respondentes na Suécia (85%), Israel (79%) e Áustria (76%) também registraram um aumento em ataques cibernéticos em suas organizações no decorrer de 2020. De modo recíproco, na França, Japão e EAU, um pouco mais da metade registraram um aumento.

Os ataques estão ficando mais difíceis de deter

Os ataques cibernéticos são complexos e ocorrem em múltiplos estágios, com os adversários usando uma infinidade de Táticas, Técnicas e Procedimentos (TTPs) durante o incidente. Lidar com esses ataques é laborioso, e para mais da metade dos respondentes (54%) os ataques agora estão muito avançados para as suas equipes de TI lidarem com eles por conta própria.

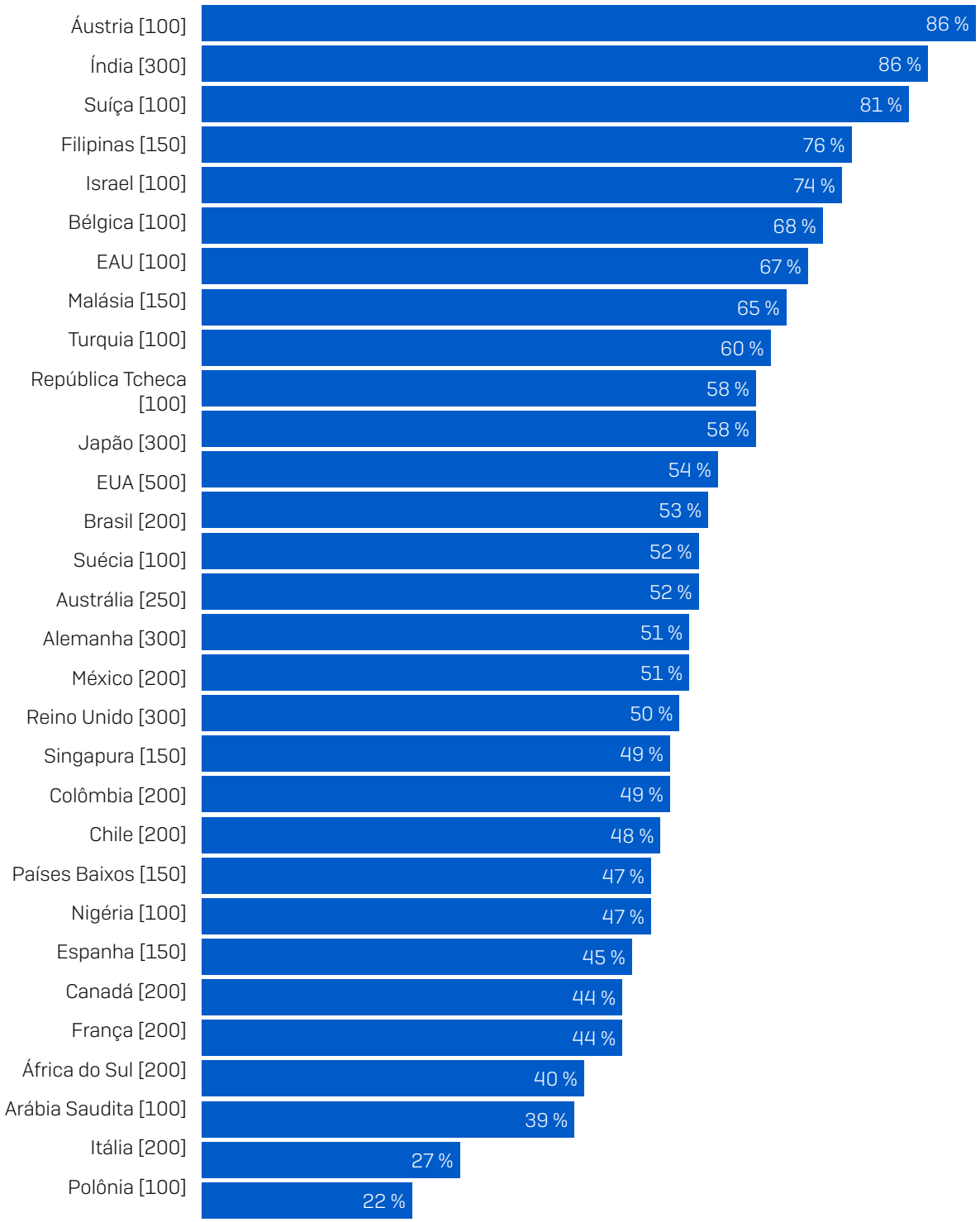


Dizem que os ataques estão muito avançados para a equipe de TI de suas organizações lidar com eles por conta própria

Esse desafio é mais acirrado no setor de **negócios e serviços profissionais**, onde 63% dos respondentes acreditam não serem mais capazes de lidar com ataques cibernéticos por conta própria, seguidos de perto por **governo central e NDPB** (62%) e pela **área de saúde** (60%). De modo recíproco, **construção civil** e **governo local** foram os que menos concordaram (47%). No caso do governo local, o resultado surpreendeu porque, como registrado no Estado do Ransomware 2021, o setor é o mais propenso a ter seus dados criptografados em um ataque de ransomware.

Entre os países participantes da pesquisa, notamos uma variação considerável nos níveis de confiança em lidar com ataques complexos.

Respondentes que acham que os ataques cibernéticos estão muito avançados para suas equipes de TI lidarem com eles por conta própria



Respondentes que concordam que os ataques cibernéticos estão muito avançados para as equipes de TI de suas organizações lidarem com eles por conta própria [tamanhos de base no gráfico], omitindo algumas opções de resposta, dividido por país

Aqueles baseados na Áustria e Índia demonstraram menos confiança em lidar com os ataques, com 86% dizendo que agora eles são muito complexos para suas equipes de TI lidarem por conta própria, seguidos por Suíça (81%), Filipinas (76%) e Israel (74%).

Reconhecer a complexidade do ataque e identificar quando é necessária expertise externa são etapas essenciais na defesa contra os avançados ataques cibernéticos da atualidade. As equipes do SophosLabs e do Sophos Managed Threat Response observaram um aumento uniforme no número de ataques que combinam automação com hackers atuantes, em um esforço de burlar as defesas das organizações. Deter esses ataques sofisticados requer pessoal capacitado, e as organizações são prudentes em reconhecer quando esses talentos precisam ser terceirizados.

Por outro lado, a Polônia registra menos dificuldade em lidar com ataques cibernéticos internamente, com apenas 22% dos respondentes que dizem que os ataques são muito avançados para suas equipes de TI lidarem com deles, seguidos de perto pela Itália (27%). Essa confiança, em face ao número crescente de ataques, pode ser devida a investimentos em contratação e desenvolvimento de profissionais capazes de se mantarem na dianteira dos adversários. Porém, isso também pode refletir uma confiança enganosa, considerando-se os ataques avançados de hoje. Com a constante evolução da abordagem dos adversários, é importante se manter realista quanto ao nível de expertise necessária para detê-los.

O tempo de resposta caiu

Dado o imenso aumento na carga de trabalho no decorrer de 2020, somado aos desafios de adaptação à pandemia, não é de surpreender que uma significativa maioria de respondentes (61%) registrou um aumento no tempo de resposta aos casos de TI durante esse período. 20% disseram que o tempo de resposta diminuiu durante esse período, enquanto 19% disseram que permaneceu o mesmo.

Mudanças no tempo de resposta aos casos de TI no decorrer de 2020

Durante o ano de 2020, nosso tempo de resposta aos casos de TI diminuiu/aumentou/permaneceu o mesmo [5.400], omitindo "Não sei"

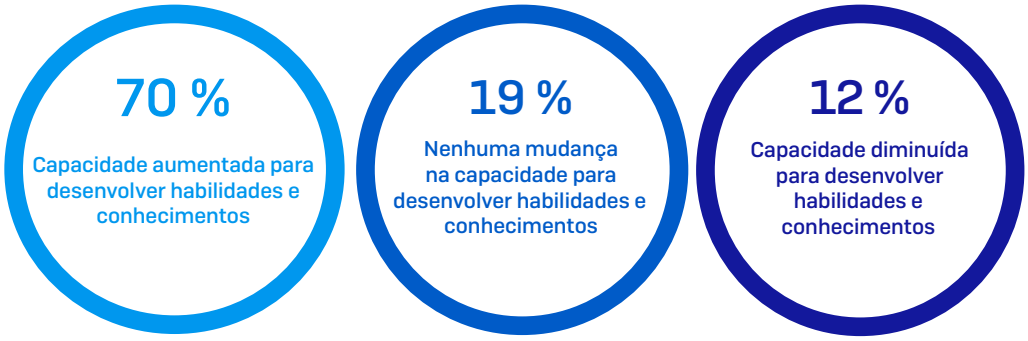
O aumento no tempo de resposta foi mais intenso no setor de **educação**, onde 65% dos respondentes registraram uma subida. A necessidade dos estabelecimentos de educação, na maioria dos países, se voltarem para o ensino online durante 2020 gerou um trabalho considerável às equipes de TI, o que causou, certamente, um impacto à capacidade de resposta rápida aos tíquetes de problemas.

Mídia, lazer e entretenimento registrou a maior queda no tempo de resposta, com quase um terço (32%) dizendo que foram capazes de responder aos tíquetes com maior rapidez. Do novo, isso muito provavelmente se deve à pandemia, um fator de peso por trás da redução na produção organizacional, que liberou a equipe de TI para oferecer respostas mais rápidas.

O impacto de 2020 na equipe de TI

Mas não são só más notícias. Quando se trata do estado das equipes de TI, temos muito a aplaudir. 70% dos gerentes de IT disseram que a capacidade de desenvolvimento de suas equipes em relação às suas habilidades e conhecimentos aumentou no decorrer de 2020, e apenas 12% experimentaram uma queda.

Mudanças na capacidade de desenvolvimento das equipes em relação às suas habilidades e conhecimentos no decorrer de 2020



Durante o ano de 2020, a capacidade de desenvolvimento das nossas habilidades e conhecimentos em segurança cibernética diminuiu/aumentou/permaneceu a mesma [5.400], omitindo "Não sei"

Devido ao arredondamento, os resultados não somam 100%

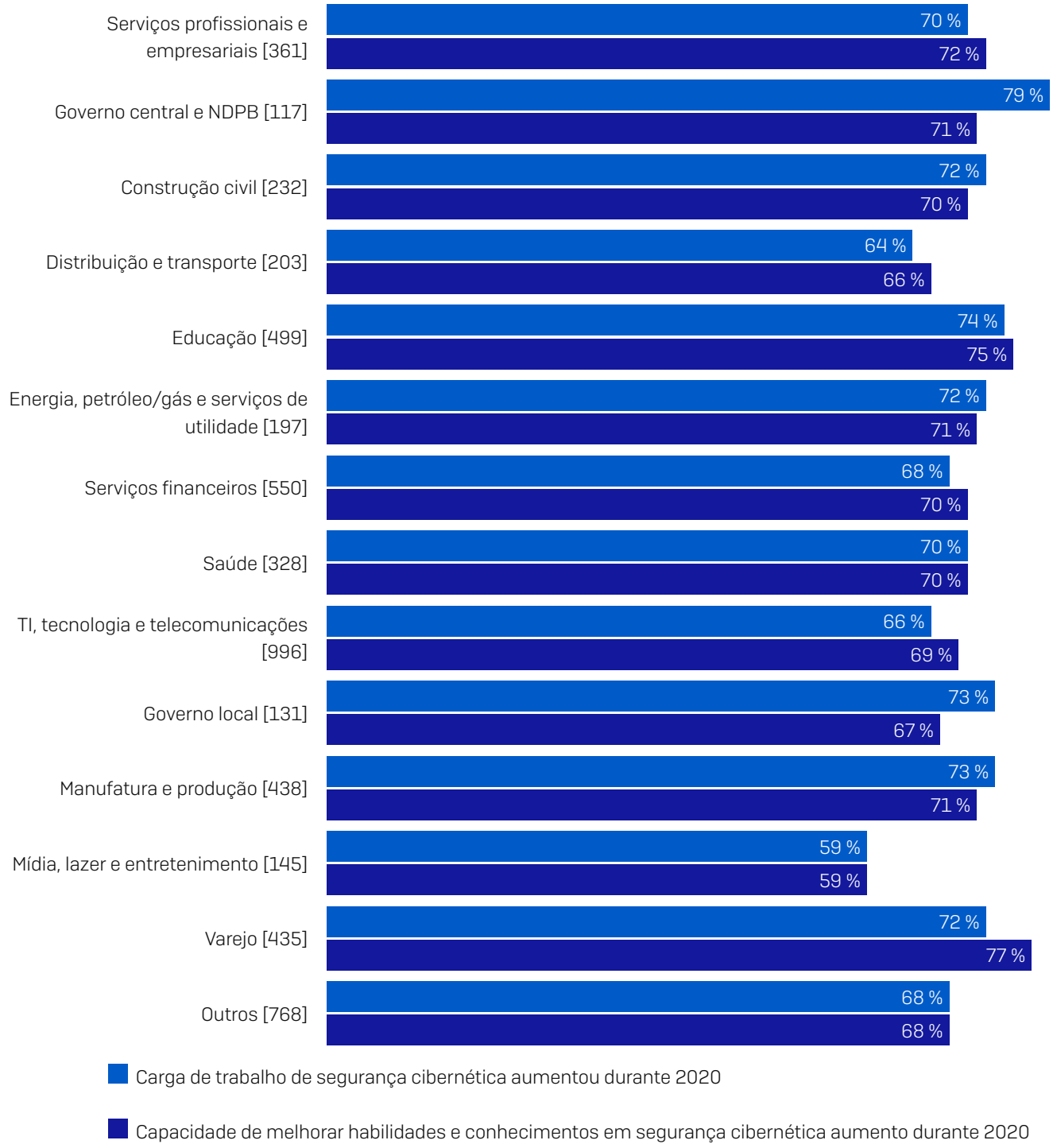
É interessante notar que vários setores que foram particularmente afetados pela pandemia registraram experiências contrastantes:

- **Varejo** foi o setor com maior capacidade de aumentar as habilidades e conhecimentos em segurança cibernética (77%). É provável que a grande virada para o varejo online durante os períodos de lockdown criou novos desafios e oportunidades para as equipes de TI nesse setor.
- **Educação** foi o setor com o segundo maior aumento em capacidade de melhorar em habilidades e conhecimentos de segurança cibernética (75%). Esse é outro setor que experimentou uma grande transformação durante o ano passado, e ainda que, indubitavelmente, a mudança para o ensino e aprendizado online tenha apresentado um grande desafio às equipes de TI, isso também criou uma excelente oportunidade de aprendizado.
- **Mídia, lazer e entretenimento** registrou o menor crescimento (59%). Como esse setor também mostrou o maior declínio em cargas de trabalho não relacionadas à segurança e de segurança cibernética, é provável que a redução nas atividades tenha restringido as oportunidades de desenvolvimento.

Aumento na carga de trabalho leva ao aumento de habilidades e conhecimentos

No geral, os dados revelaram uma clara correlação entre o aumento da carga de trabalho de segurança cibernética e o aumento da capacidade de desenvolvimento de habilidades e conhecimentos em segurança cibernética em todos os setores.

Aumento na carga de trabalho de segurança cibernética e aumento na capacidade de desenvolver habilidades e conhecimentos em segurança cibernética



Durante o ano de 2020, nossa carga de trabalho de segurança cibernética aumentou/ Durante o ano de 2020, nossa capacidade de desenvolver nossas habilidades e conhecimentos em segurança cibernética aumentou [tamanhos de base no gráfico], dividido por setor

Entre os respondentes que experimentaram um aumento na carga de trabalho de segurança cibernética durante 2020, 84% também disseram que a capacidade de desenvolvimento de suas habilidades e conhecimentos em segurança cibernética aumentou. Tal qual, mais de oito em dez (82%) dos que registraram um aumento em ataques cibernéticos às suas organizações também disseram que a capacidade de desenvolvimento de suas habilidades e conhecimentos em segurança cibernética aumentou. Isso faz sentido: enquanto o aumento em carga de trabalho e ataques cibernéticos aumenta a pressão, também proporciona oportunidades de desenvolver novas habilidades.

O moral da equipe melhorou

Mais da metade dos gerentes de TI entrevistados (52%) disseram que o moral da equipe subiu no decorrer de 2020. 26% disseram que caiu e 22% disseram que permaneceu o mesmo.

Mudanças no moral da equipe no decorrer de 2020

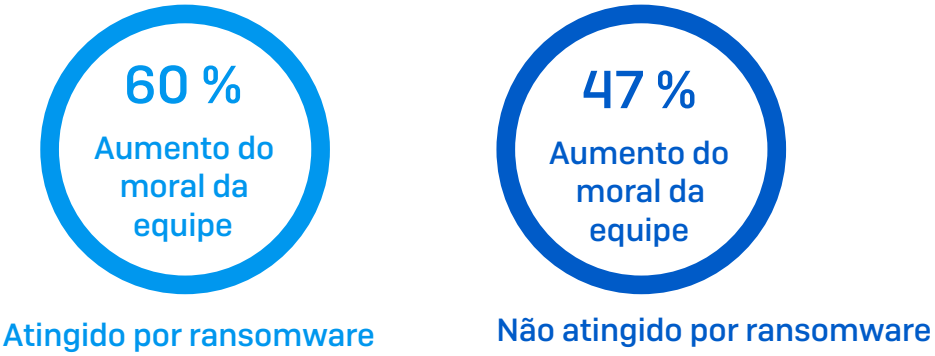
Durante o ano de 2020, o moral da nossa equipe diminuiu/aumentou/permaneceu o mesmo [5.400], omitindo "Não sei"

Geograficamente, os maiores aumentos no moral foram registrados na Turquia (75%), Áustria (71%) e Índia e África do Sul (ambos 69%). No outro lado da balança, as equipes de TI em Israel (26%), França (31%), Itália (33%) e Polônia (36%) foram as que menos observaram melhoras no moral da equipe.

Você deve ter notado que vários países em destaque aqui também despontaram nas seções anteriores. Turquia e Áustria, que apresentaram a maior proporção de respondentes que disseram que o moral da equipe aumentou, estavam entre os quatro principais países que registraram aumento em ataques cibernéticos. Semelhantemente, a França apresentou a segunda mais baixa porcentagem de respondentes que registraram um aumento no moral e também o menor aumento em ataques cibernéticos entre todos os países entrevistados. Essa correlação entre experiências de ataques cibernéticos e moral da equipe é um dos resultados mais notáveis da pesquisa.

Para demonstrar esse ponto com mais clareza, 60% dos respondentes cujas organizações foram atingidas por um ataque de ransomware nos 12 meses anteriores registraram um aumento no moral da equipe, comparado aos 47% daqueles que não foram atingidos.

Mudanças no moral da equipe no decorrer de 2020

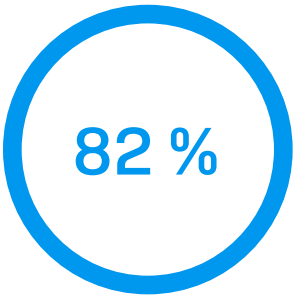


Durante o ano de 2020, o moral da nossa equipe diminuiu/aumentou/permaneceu o mesmo [5.400], omitindo algumas opções de resposta, dividido por respondentes cujas organizações foram atingidas por um ataque durante o ano passado

Há uma variedade de fatores prováveis por trás dessa correlação. A adversidade – nesse caso ataques cibernéticos – geralmente se concretiza em oportunidades para as pessoas se unirem e trabalharem em prol de um objetivo único, aumentando o moral da equipe. Além disso, ser capaz de dar suporte à organização em face ao aumento dos ataques dá a sensação de satisfação. O maior índice de aumento do moral foi registrado pelos dois setores que foram mais afetados pela pandemia, com a **educação** sentindo a maior melhora (58%), seguida de perto pela **saúde** (57%).

Ao mesmo tempo, a mudança no papel que as equipes de TI desempenharam em capacitar a continuidade dos negócios em face à pandemia pode ter resultado na maior percepção e reconhecimento da contribuição dada por elas, o que também ajuda a subir o moral. Se as equipes de TI ainda não foram devidamente reconhecidas, essa é a hora.

As equipes de TI se sentem bem equipadas para os desafios à frente



Dizem ter as ferramentas e conhecimentos para investigar atividades suspeitas completamente

Respondentes que concordam que se detectarem atividades suspeitas em suas organizações terão as ferramentas e o conhecimento necessários para investigá-las completamente [5.400], omitindo algumas opções de resposta

Em face ao aumento da carga de trabalho e frequência dos ataques cibernéticos durante 2020, é animador notar que 82% dos gerentes de TI dizem ter as ferramentas e o conhecimento necessários para investigar atividades suspeitas completamente se forem detectadas em suas organizações. As oportunidades oferecidas para desenvolver habilidades e conhecimentos durante 2020 foram equipar bem essas equipes para os desafios à frente. Continuar esse investimento em ferramentas e treinamento é essencial para que as equipes de TI sejam capazes de acompanhar a crescente evolução dos ataques cibernéticos.

Contudo, quando analisamos as respostas a essa pergunta por setor, há dois que claramente se destacam: **governo central e NDPB** (67%) e **governo local** (64%). Em todo o mundo, o setor governamental foi intensamente afetado pela pandemia. Ele teve que garantir a continuidade dos serviços essenciais durante um extenso período de ruptura e, ao mesmo tempo, providenciar apoio adicional para cidadãos e organizações. Além disso, os cofres públicos são um eterno desafio em muitos países, o que pode limitar os recursos disponíveis. Com agentes de ransomware focados intensamente em organizações governamentais, é essencial que tenham os recursos e habilidades necessários para investigar as atividades suspeitas completamente.

O futuro da equipe de segurança de TI

Como já vimos, o ano que passou foi uma árdua contenda para muitos na área de TI. Contudo, as equipes de TI ascenderam de modo admirável, resultando no aumento de suas habilidades e do seu moral. Essas experiências, juntamente com mudanças mais abrangentes no cenário da TI, como o aumento do trabalho flexível e do uso da nuvem, terão um impacto direto na equipe de segurança de TI do futuro.

As equipes de segurança de TI estão destinadas a crescer – rápido

Em face às exigências de crescimento das equipes de TI, os respondentes preveem um crescimento considerável em tamanho do pessoal de segurança de TI interno e terceirizado, especialmente nos próximos dois anos:

- 68% esperam que o pessoal interno aumente nos próximos dois anos, com 76% prevendo um aumento durante os próximos cinco anos
- 56% esperam que o pessoal de TI terceirizado aumente nos próximos dois anos, com 64% prevendo um aumento durante os próximos cinco anos
- Apenas 8% esperam que o número de funcionários internos caia nos próximos cinco anos

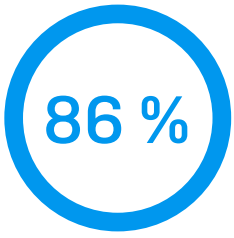
Recursos à segurança de TI	Mudança esperada	Até 2023	Até 2026
Pessoal interno de segurança de TI	Aumentar	68 %	76 %
	Diminuir	11 %	8 %
Pessoal terceirizado de segurança de TI	Aumentar	56 %	64 %
	Diminuir	14 %	10 %

Como você acha que o tamanho da equipe de segurança de TI da sua organização mudará até 2023 e 2026? [5.400] excluindo algumas opções de resposta

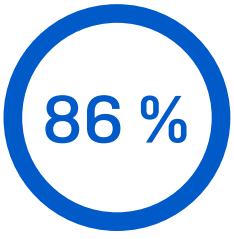
Um ponto interessante é que o crescimento em pessoal de TI terceirizado não se traduz na perda de equipes internas. Quase metade (46%) dos respondentes esperam um aumento de pessoal de segurança de TI tanto interno quanto terceirizado até 2023, e 55% até 2026.

No geral, 77% dos respondentes esperam o crescimento em pelo menos uma área de recursos (interna ou terceirizada) durante os próximos dois anos, subindo para 85% até 2026.

IA é a chave



Esperam que a IA ajude a lidar com o crescente número de ataques



Esperam que a IA ajude a lidar com a crescente sofisticação dos ataques

Respondentes que concordam que esperam que as tecnologias de IA ajudarão a lidar com o número crescente de ataques e/ou que esperam que as tecnologias de IA ajudarão a lidar com a crescente sofisticação dos ataques [5.400], omitindo algumas opções de resposta

Quase que universalmente, as equipes de TI estão buscando tecnologias de IA para ajudá-las a combater o aumento em ameaças cibernéticas. 86% esperam que as tecnologias de IA ajudem a lidar com o número crescente de ataques, enquanto a mesma porcentagem espera que as tecnologias de IA ajudem a lidar com a crescente sofisticação dos ataques, com 92% selecionando pelo menos uma dessas opções.

Crie a equipe de segurança de TI do futuro, hoje

Para criar a equipe de TI do futuro você tem começar agora. As organizações devem usar as perspectivas e insights gerados pela linha de frente para garantir o sucesso da segurança cibernética em 2023 e além. Baseado no aprendizado obtido com este relatório, a Sophos oferece cinco recomendações:

1. Implemente ferramentas e abordagens que reduzam a carga de trabalho administrativa de segurança de TI

O aumento das cargas de trabalho não relacionadas à segurança e de segurança durante o último ano ficou bastante claro para todos. As organizações devem ponderar a implementação de ferramentas e abordagens que reduzam a carga de trabalho de segurança de TI, liberando suas equipes para outras atividades.

- **Automatize.** Aproveite a automação para reduzir a carga diária com tarefas que consomem tempo e energia inestimáveis dos profissionais de TI e remaneje-os para outros projetos estratégicos. Invariavelmente, as máquinas são capazes de reagir mais rápido do que operadores humanos, acelerando o tempo de resposta e reduzindo a exposição.
- **Consolide.** Simplifique a administração do dia a dia gerenciando todas as suas soluções de segurança cibernética por meio de um painel de controle unificado. Ter tudo à mão em um só lugar elimina a necessidade de pular de painel para painel para gerenciar a segurança e correlacionar dados entre diferentes sistemas, economizando tempo e esforços valiosos das equipes de TI. Consolidar a segurança de TI também reduz os encargos de gerenciar fornecedores.
- **Integre.** Escolha soluções que se integrem e sejam projetadas para trabalhar em conjunto. Isso aumenta a sua capacidade de automatizar tarefas, facilitando a condução de investigações entre produtos e oferecendo insights mais profundos à sua postura de segurança.

2. Invista em ferramentas e treinamento para capacitar as equipes de TI a usar suas habilidades crescentes

As equipes de TI observaram um desenvolvimento significativo em suas habilidades e conhecimentos no último ano. As organizações devem ser criteriosas e investir em ferramentas e treinamento que as capacitem a usar essas novas habilidades e a continuar aprendendo. Esses recursos irão também ajudar a contratar novos talentos para a equipe.

3. Combine a expertise da equipe de TI interna e terceirizada

Os ataques cibernéticos já são bastante complexos para mais da metade dos gerentes de TI lidarem com eles por contra própria – e eles simplesmente ficarão cada vez mais complexos. Ao combinar o pessoal interno e especialistas terceirizados em suas equipes de segurança, você terá o melhor dos dois mundos: profissionais com conhecimentos profundos sobre ameaças e sobre a sua organização. Essa estrutura combinada também facilita a adaptação e resposta a mudanças, aproveitando os melhores talentos em cada situação. As organizações devem procurar por parceiros de segurança que possam revigorar suas equipes de TI com habilidades e capacidades não disponíveis internamente, e ao mesmo tempo oferecer flexibilidade para se adaptarem a seus modelos operacionais.

4. Prepare-se para atrair os melhores talentos globais

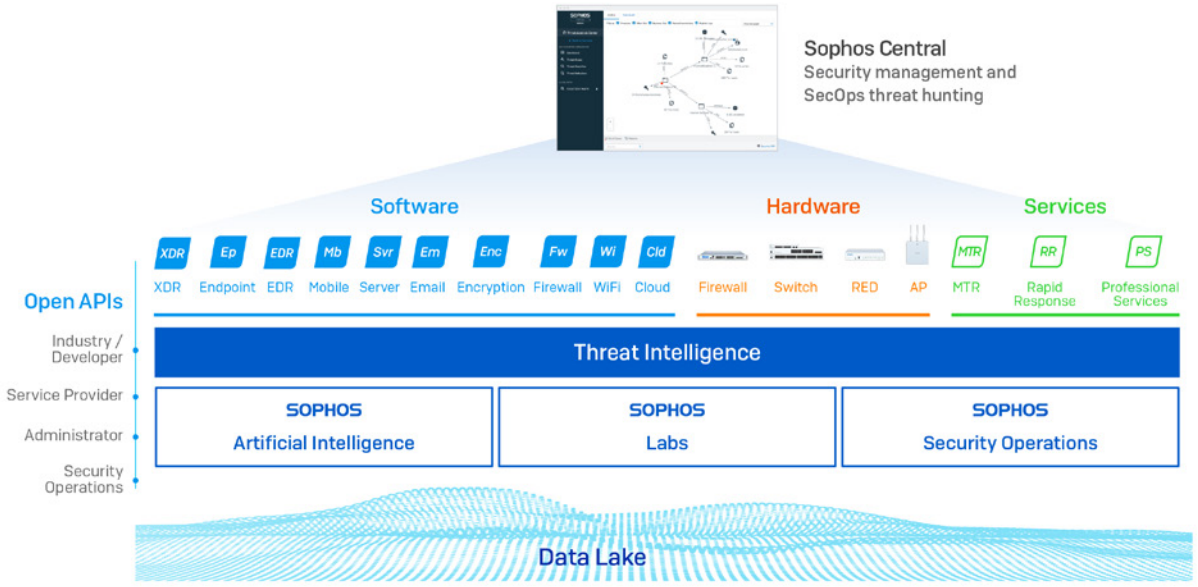
Com a maioria das organizações procurando expandir suas equipes de TI, a competição para conquistar os melhores talentos ficará acirrada. A adoção de tecnologias inovadoras que podem ser gerenciadas de qualquer lugar ajuda a aumentar a sua opção de profissionais talentosos. A pandemia nos ensinou que quase todas as funções de TI podem ser desempenhadas remotamente, se necessário. Mais ainda, a oferta de ferramentas de alta qualidade aumentará o seu poder de atração sobre a maioria dos candidatos a uma vaga.

5. Construa um canal para a sua equipe interna de segurança de TI

Talentos em segurança de TI já estão escassos. Além de expandir seu pool de talentos, as organizações também devem buscar programas internos para incentivar o progresso e a criação de um canal de crescimento para a sua equipe de TI, como estágios e programas de treinamento. Ainda que a imagem de um jovem de capuz no quarto debruçado sobre o computador seja um estereótipo, também serve para nos lembrar de que muitas pessoas desenvolvem habilidades cibernéticas avançadas seguindo outros caminhos que não os tradicionais.

Como a Sophos pode ajudar

A Sophos ajuda as equipes de TI de mais de 500.000 organizações em 150 países a defender suas organizações contra ameaças cibernéticas.



O Ecossistema de Segurança Cibernética Adaptativa (ACE) da Sophos

- Oferecemos um portfólio completo de **tecnologias next-gen** com **inteligência artificial.** Nossos produtos são desenvolvidos para trabalharem em conjunto, automatizando tarefas manuais e reduzindo a exposição a ameaças – chamamos isso de Segurança Sincronizada. Clientes com a nossa proteção de endpoint e firewall registram consistentemente uma redução na administração diária de pelo menos 50%, e menos incidentes de segurança.
- O **Sophos Extended Detection and Response (XDR)** e o **Sophos Endpoint Detection and Response (EDR)** proporcionam às equipes de TI as ferramentas necessárias para identificar e remediar rapidamente as ameaças e os problemas de higiene de TI. O Sophos EDR é o primeiro EDR desenhado para analistas de segurança e administradores de TI. Ele capacita as equipes de TI para desenvolverem expertise sem aumentar seu pessoal.
- Todas as tecnologias next-gen da Sophos são gerenciadas através da plataforma de segurança **Sophos Central** – uma ferramenta baseada na web que o capacita a usar os melhores profissionais, independentemente de sua localização.
- As equipes do **Sophos Managed Threat Response (MTR)** e do **Sophos Rapid Response** oferecem expertise para a caça a ameaças avançadas e resposta a incidentes para dar suporte às equipes internas, tudo entregue como um serviço totalmente gerenciado. Você controla como e quando escalonar possíveis incidentes e quais medidas (se houver) devemos tomar por você.
- Toda a nossa proteção é respaldada pela inteligência de ameaças coletiva do **SophosLabs, Sophos Security Operations** e da equipe do **Sophos AI**, além do **Sophos Data Lake.**
- **APIs abertas** permitem que seus clientes se beneficiem da ciência e da telemetria de nossos parceiros em todo o mundo.

Para saber mais sobre o que fazemos e conversar sobre os desafios que a sua equipe enfrenta, visite nosso site ou fale com um representante da Sophos.

Para saber mais sobre o que fazemos e conversar sobre os desafios que a sua equipe enfrenta, visite nosso site ou fale com um representante da Sophos.

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2021-05-20 (WP-NP)

SOPHOS