Como prever o desconhecido

Diretor executivo de segurança da informação (CISO) Relatório de referência

CISCO

Conteúdo

Introdução: não vejo nada de errado, não bloqueio nada 3

Olhe para trás para seguir em frente 6

Status do CISO 7

Descobertas de 2019 8

- Pronto para o sucesso? 8
  - Conheça os riscos 8
  - Como gastar o orçamento 8
  - Colaboração, não isolamento 9
  - Envolvimento dos funcionários: simulações e exercícios 10
- Arquitetura: navegando pelo provisionamento do fornecedor 11
  - Desafio de gerenciamento de alertas: você não entende o que não vê 12
  - Gerencie o que você mede 13
- Preparo e resposta a violações: quando o desconhecido aparece 14
  - Ataques vistos no ano passado 14
  - Custo de uma violação: mais do que apenas dinheiro 15
  - O que você está fazendo para lidar com a ameaça de uma violação 16

Lidar com o desconhecido 17

Sobre a pesquisa comparativa da Cisco 19

Sobre a Cisco Cybersecurity Series 20

Introdução: não vejo nenhum mal, não bloqueio nenhum mal

Imagine se você pudesse ver o futuro. E voltar ao passado, tudo ao mesmo tempo. Imagine ter visibilidade de tudo que já aconteceu e de tudo que vai acontecer em todos os lugares, tudo ao mesmo tempo.

Então, pense no poder de processamento, robusto o suficiente para dar sentido a todos esses dados, em todos os idiomas e em todas as dimensões. A menos que você tenha alcançado esse nirvana de dados digitais (e não tenha nos contado), sempre vai haver algo desconhecido no seu mundo.

No universo da segurança, existem ameaças desconhecidas fora da empresa na forma de agentes mal-intencionados, ataques patrocinados e malware que se move rapidamente e destrói tudo o que atinge. O desconhecido está dentro da empresa na forma de ameaça interna de funcionários desonestos ou fornecedores imprudentes, considerados por 24% dos entrevistados da nossa pesquisa como o risco mais sério para as empresas. O desconhecido existe na forma de novos dispositivos, novos aplicativos na nuvem e novos dados. O desconhecido é o que não deixa os CISOs nem você dormirem à noite, e sabemos disso porque lhe perguntamos.

Este é o 12º ano consecutivo que publicamos nossas descobertas sobre o cenário de segurança cibernética e, no quinto ano, realizamos um estudo comparativo com milhares de líderes de segurança. Este relatório é apenas a ponta do iceberg sobre os dados gerados pela pesquisa. No próximo ano, publicaremos mais dados de referência por setor, localização geográfica, tamanho da empresa e função no trabalho, entre outros filtros. Para este relatório, fizemos uma pesquisa com mais de 3.200 líderes de segurança em 18 países, com perguntas em três categorias:

1. **Preparo**: como você se prepara para obter sucesso com treinamento, orçamento, simulações, práticas recomendadas e outras competências essenciais?
2. **Arquitetura**: qual a sua abordagem para a escolha de solução/fornecedor e gerenciamento de alertas?
3. **Preparo e resposta a violações**: como você gerencia as violações em relação a quais sistemas são afetados, quanto é perdido e quanto tempo leva para recuperar?

Entrevista com Marisa Chancellor Diretora sênior, Security & Trust Organization, Cisco

Você está protegendo 70.000 funcionários da Cisco em 400 escritórios com centenas de milhares de endpoints.

Isso é o que chamo de minha superfície de ataque e, como você pode ver, as pessoas têm muitos recursos para atravessá-la. Sim, existem funcionários e data centers, mas também usamos 600 nuvens e, por isso, temos um verdadeiro cenário de nuvem híbrida e multinuvem para defender.

Conte-nos sobre as responsabilidades da sua equipe.

Somos recrutados para defender a Cisco e estamos focados em equilibrar os riscos da Cisco, como empresa, fazendo tudo o que for necessário diante do risco de ameaças internas e externas. Nós nos concentramos em definir a arquitetura de segurança correta para nosso departamento de TI, analisando os incidentes que surgem para determinar a estabilidade da nossa postura de segurança.

(continuação)

Em seguida, comparamos o desempenho nessas áreas para ver se, desde que começamos a rastreá-lo, você avançou na criação de defesas, na detecção de ameaças cibernéticas e na contenção de violações de dados. Este relatório esclarece quais ações estão gerando resultados para fortalecer a saúde cibernética da empresa, para que você possa aprender com seus colegas.

Por exemplo, quando perguntamos, apenas 35% foram capazes de confirmar que: "é fácil determinar o escopo de um comprometimento, contê-lo e corrigir as explorações", sugerindo que ter visibilidade do desconhecido é claramente o principal desafio. Talvez tenha sido a parte "fácil" que derrubou você, já que os incidentes muitas vezes não são o que parecem. Ainda assim, significa que 65% dos CISOs na pesquisa podem melhorar mais. E, mesmo assim, podemos nos basear nos 46% que disseram: "temos as ferramentas necessárias para analisar e fornecer feedback sobre os recursos da nossa abordagem de segurança". Se você reconhecer que não consegue ver tudo, pelo menos, poderá avaliar e gerenciar sua capacidade de melhorar e ver mais.

Embora o bom combate esteja longe de terminar, também não é feito somente de notícias ruins. Pelo menos, alguns entrevistados em nossa pesquisa parecem estar confortáveis com o trabalho. Perguntamos se estavam enfrentando fadiga digital. Nós classificamos isso como a desistência de enfrentar ameaças e agentes mal-intencionados. Apenas 30% dos entrevistados confirmaram sofrer fadiga digital este ano. Mesmo que quase 1/3 pareça ser um número alto e alarmante, a queda em relação ao ano passado, que foi 46%, indica que estamos indo na direção certa e isso faz a luta valer a pena.

(continuação)

O que faz você perder o sono?

Bem, acho que para a maioria das pessoas que trabalham com segurança, o que nos causa insônia é o desconhecido. Quando penso no que preciso proteger diariamente, temos uma equipe fantástica e uma tecnologia muito qualificada, mas estamos nos concentrando no que é conhecido e a verdadeira ameaça é o desconhecido.

Ouvimos dos CISOs sobre o número de alertas com que eles têm que lidar, você acha que há alertas demais para gerenciar?

Isso é verdadeiro no setor em geral, mas na Cisco, analisamos diariamente 47 TB de eventos de rede e isso se traduz em cerca de 22 incidentes por dia, o que é impossível para uma pessoa entender. E o que chega a nós vem de todo o espectro, por isso temos que entender como analisar essas informações e fazer com que a tecnologia trabalhe para nós. Poder usar aprendizado de máquina e inteligência artificial para examinar muitos desses alertas nos permite aprimorar as áreas mais arriscadas nas quais devemos nos concentrar. Não temos um orçamento ilimitado, portanto, como podemos trabalhar na velocidade da máquina, em vez de na velocidade humana?

Veja mais trechos da entrevista com Marisa Chancellor ao longo deste relatório.

Se você acha que enxergar o futuro e o passado ao mesmo tempo é uma tarefa difícil, vamos melhorar o que podemos ver no momento presente e avaliar de que forma nos comportamos bem, e não tão bem hoje, em comparação com os dados relatados anteriormente.

"Nossa Security & Trust Organization é responsável por proteger a Cisco, simples assim. Mas por outro lado – como podemos ter certeza de que conseguimos acelerar os negócios? Não adianta bloquearmos todo o ambiente onde nada está avançando."

Marisa Chancellor
Diretora sênior, Security & Trust Organization, Cisco

Olhe para trás para seguir em frente

Os CISOs melhoraram ou pioraram no último ano? Escolhemos três áreas que foram tópicos controversos no ano passado e classificamos você de acordo com suas respostas neste ano.

Tecnologia

	Você disse 2018	Você diz 2019	Queremos saber mais porque...
Aprendizado de máquina (ML) Até que ponto você depende do ML para reduzir o nível de esforço necessário para proteger a empresa?	77%	↓67%	As tendências negativas nestas três primeiras perguntas provavelmente resultam da incerteza e da falta de confiança. Ou que o aprendizado de máquina (ML) não está pronto para entrar em ação. De qualquer maneira, gostaríamos de saber mais.
Inteligência artificial (IA) Até que ponto você depende da IA para reduzir o nível de esforço necessário para proteger a empresa?	74%	↓66%	Pode ser que a adoção esteja tão difundida e integrada a seus processos de negócios que você não ache que vale a pena destacar.
Automação Até que ponto você depende da automação para reduzir o nível de esforço necessário para proteger a empresa?	83%	↓75%	Talvez você tenha optado por não ser "dependente", mas ainda assim automatize seletivamente. Mesmo as empresas de grande porte podem não adotar a automação completamente.

Custo de uma violação

Pensando na violação mais impactante que você teve no ano passado, qual foi o custo total?	8% disseram $5MI+	8% disseram $5MI+	As violações continuam a ser um desperdício de recursos e afeta mais do que somente a parte financeira.
	< US$ 500 mil 47%	< US$ 500 mil ↑51%	Mais de 50% de vocês estão determinando os custos de violação em menos de meio milhão, o que é excelente. Os custos estão um pouco mais baixos ou pelo menos sob controle.
Quais melhorias foram feitas para aumentar a proteção da sua empresa contra violações de segurança?			
Separação das funções de TI e segurança	38%	↓35%	Este é um tema controverso e a ausência de uma grande diferença sugere que vocês estão igualmente divididos como um grupo.
Mais treinamento e conscientização de segurança para os funcionários	38%	↑39%	Enquanto as pessoas continuarem sendo o elo mais fraco, permaneceremos sem saber qual a quantidade de treinamento suficiente.
Técnicas de mitigação de riscos implementadas	37%	↑39%	Quando você vê que este ano 20% dos entrevistados afirmaram não ter muito conhecimento sobre risco e conformidade, percebe que as estruturas de risco se tornam procedimentos operacionais padrão.
Aumentou o investimento nas tecnologias ou soluções de defesa para segurança	41%	↑44%	Bom, se combinado com treinamento e medição baseada em resultados. Bom para métricas de segurança.

Nuvem

Transferir a segurança para a nuvem aumentou nossa eficiência, permitindo que a equipe de segurança se concentre em outras áreas	92% concordam	↑93%	Adoção contínua da nuvem pelos motivos certos.
Aproveitar as soluções de segurança na nuvem nos permite ser mais eficientes do que operando localmente	91% concordam	↑93%	Um leve aumento na confiança da segurança da nuvem? Queremos!
É como um desafio para defender a infraestrutura de nuvem contra ataques digitais	55% muito	↓52%	Uma queda maior na dificuldade de proteger a infraestrutura de nuvem? Melhor ainda!

Fonte: Estudo comparativo do CISO - Cisco 2019

Status do CISO

Há algum tempo, uma equipe de especialistas que detectam ameaças falaram sobre conhecer o desconhecido. É hora de estender isso a todo o espectro da segurança cibernética: usuários, aplicativos, dados e nuvens. Você não pode proteger o que não consegue ver.

Você quer colaborar com a empresa e não deixá-la se perder na burocracia. Se você tiver uma abordagem um pouco mais aberta, como vai mitigar o controle? Isso vai ser diferente para todos. Os CISOs precisam lidar com esse equilíbrio da cultura corporativa, enquanto combatem as principais ameaças. Às vezes, bloquear tudo não se encaixa na cultura da empresa. Pode ser apropriado para um banco, mas não para uma universidade.

O CISO enfrenta vários desafios no gerenciamento do risco cibernético, seja qual for o modelo corporativo:

- As violações prejudicam a lucratividade financeira, a reputação da marca, a segurança dos dados do cliente, a satisfação do cliente e a continuidade dos negócios.
- As perdas podem ser substanciais e irrecuperáveis, criando uma classificação de risco mais alta para a empresa em relação ao seguro.
- Ao longo dos anos, as soluções pontuais de fornecedores pareciam promissoras, no entanto, cada um gera seu próprio conjunto de alertas. Muitas soluções pontuais que competem em alertas dificultam a identificação das ameaças que representam o maior risco para a empresa e se tornam um desperdício de recursos.
- A TI geralmente é isolada em toda a empresa, o que aumenta a dificuldade de proteger a rede, a nuvem e os endpoints dos funcionários.

"Você se esforça para entender como obter visibilidade sobre o desconhecido, como as novas ameaças iminentes, ou mesmo as que estão dentro do seu próprio ambiente: dispositivos, aplicativos e dados desconhecidos. Não é possível proteger o que você não vê. Essa é a maior causa da minha insônia."

- São necessárias táticas agressivas para contratar pessoal de TI de segurança, porque mesmo um grupo especializado de candidatos não é suficiente para combater a magnitude do problema em empresas globais. A escassez de talentos, no entanto, está fora de controle e não pode ser resolvida simplesmente preenchendo todas as vagas.
- Novas ameaças aparecem diariamente, até mesmo de hora em hora, e estão empregando métodos cada vez mais furtivos e sofisticados. Recentemente, informamos sobre o Emotet, o Olympic Destroyer e outras ameaças predominantes no Relatório de ameaças da Cisco de 2019. A resposta à ameaça como uma categoria tem que evoluir e é preciso ferramentas para consolidar informações e centralizar a remediação de infecções e outros incidentes.

Outras tecnologias e processos para o CISO considerar são:

- IA e ML, quando usadas da forma correta, são essenciais para a triagem do volume de trabalho.
- O custo de uma violação está caindo, mas ainda não dá para se animar muito.
- Existe espaço para obter benefícios óbvios na melhoria do processo, por exemplo, com treinamento.
- Há mais confiança na segurança fornecida pela nuvem e na proteção da nuvem.

Descobertas de 2019

Nossas descobertas do estudo comparativo revelaram várias áreas que são essenciais para fortalecer a postura de segurança da sua empresa. Esta seção detalha nossas descobertas de onde e como os CISOs e seus colegas estão implementando (ou não) a tecnologia e os processos necessários para mitigar os danos que as violações cibernéticas podem provocar nas empresas, sob os tópicos de práticas recomendadas, abordagem de arquitetura e preparo contra violação.

Pronto para o sucesso?

O que significa ser um CISO diariamente? Qual é sua estratégia? Nossa pesquisa atual revelou várias áreas que, juntas, determinam a integridade cibernética da empresa, incluindo: ser prático sobre os riscos, estabelecer critérios orçamentários, colaborar entre divisões, treinar funcionários, realizar simulações, saber acompanhar os resultados para entender como investir e ser estratégico na implementação do fornecedor e da solução.

Conheça os riscos

O gerenciamento de riscos é uma mesa de apostas? Dificilmente. Entender os riscos dos ataques cibernéticos e o cenário de conformidade que abrange violações de segurança é fundamental para saber como se defender e se preparar para o pior. Quando perguntados sobre quem conhecia muito sobre risco e conformidade, apenas 80% dos entrevistados responderam que sim. Restam 20% dos profissionais de segurança que poderiam aproveitar o treinamento discutido anteriormente. Mais desconhecidos – onde você menos espera.

Como gastar o orçamento

Quase metade, ou 47%, determina como controlar os gastos de segurança com base nos objetivos de resultado da segurança empresarial. A medição de resultados em relação aos investimentos é a melhor abordagem orientada por dados. Além disso, 98% concordam total ou parcialmente que a equipe executiva estabeleceu métricas claras para avaliar a eficácia do programa de segurança. 49% dos entrevistados têm métricas utilizadas por várias áreas da empresa para entender as decisões com base em riscos e melhorar os processos para medir a eficácia da segurança em toda a empresa.

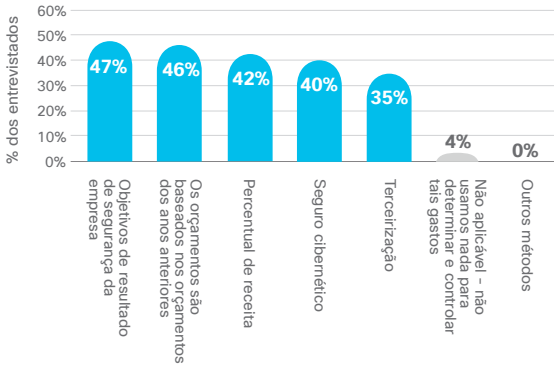
De volta ao orçamento e, além da medição baseada em resultados, conforme mostrado na Figura 1, há algumas opções menos adequadas: controlar os gastos com segurança nos orçamentos dos anos anteriores (46%) e no percentual da receita respectivamente (42%), foram escolhas bastante comuns, mas não estão

"Em algumas áreas, o risco não é tão alto porque a empresa tem práticas de segurança sólidas. Já em outras áreas, podemos fortalecer, minimizar e preencher as defasagens que geram risco. E é dessa forma que fazemos investimentos e nos preparamos para as próximas ameaças. Devemos nos perguntar como podemos construir essa arquitetura fundamental para nos prepararmos melhor para o que enfrentaremos no futuro."

necessariamente associadas à melhor segurança. O cenário de violações muda de ano para ano, e o orçamento do ano anterior ou a porcentagem de receita pode ter pouco a ver com o custo de defesa contra ameaças futuras.

A quarta abordagem mais confiável para determinar os gastos com segurança é o seguro cibernético: 40% usam seguro cibernético, pelo menos parcialmente, para definir os orçamentos. A adoção dessa abordagem começa com uma avaliação de riscos para identificar com precisão os riscos de segurança e garantir que eles possam ser mitigados por um seguro ou protegidos por controles. Para algumas empresas, pode ser que as diretrizes de seguro cibernético influenciem na escolha da tecnologia e/ou na definição do orçamento. De qualquer forma, isso merece mais investigação em relatórios subsequentes.

Figura 1 Qual das seguintes opções a sua empresa usa para determinar e/ou controlar gastos com segurança?
Porcentagem de entrevistados, N=3.259

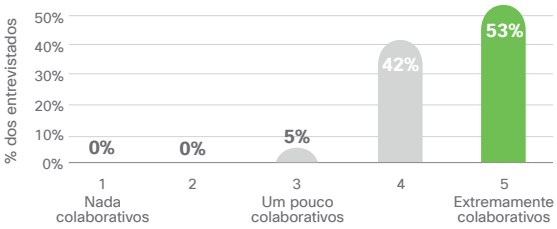


Fonte: Estudo comparativo do CISO Cisco 2019

Colaboração, não isolamento

Em pesquisas anteriores, você nos disse que dividiu a segurança de TI e criou a função do CISO. Felizmente, você se dá bem na área de testes (sandbox) com seus colegas de redes. A Figura 2 nos mostra que 95% de vocês se julgam muito ou extremamente colaborativos no que diz respeito às equipes de redes e segurança. Não trabalha com silos, e isso oferece uma vantagem financeira tangível.

Figura 2 Entrevistados de diferentes cargos relataram bons níveis de colaboração entre redes e segurança em toda a empresa.
Porcentagem de entrevistados, N=3.248



Fonte: Estudo comparativo do CISO Cisco 2019

Quanto de incentivo financeiro? Parece que 59% dos que foram muito/extremamente colaborativos entre redes e segurança tiveram um impacto financeiro inferior a US$ 100 mil com a violação mais importante – a categoria mais baixa de custo de violação.

Isso claramente merece uma análise mais aprofundada e, possivelmente, aponta para uma maior necessidade e possível desenvolvimento de mais equipes de DevSecOps. A colaboração não é uma questão de coincidência, mas uma obrigação, especialmente na era do desenvolvimento ágil.

E isso é reconhecido nos níveis executivos mais altos. De acordo com um estudo recente do CIO publicado pela IDG, "82% dos CIOs esperam que sua estratégia de TI e segurança esteja totalmente integrada nos próximos 3 anos."*

*Fonte: A Secure Alliance: How the CIO-CISO Relationship Strengthens IT and Business, IDG, fevereiro de 2019

Envolvimento dos funcionários: simulações e exercícios

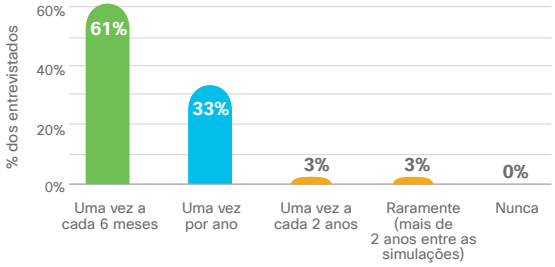
"E se treinarmos nossos funcionários e eles saírem da empresa?", essa às vezes é a dúvida. "Mas e se não treinarmos e eles continuarem na empresa?" O mesmo é válido sob a perspectiva de segurança. Sim, nos concentramos na tecnologia, mas também devemos gastar o mesmo tempo com o processo e as pessoas, porque nosso pessoal é a linha de frente para ajudar a proteger nossas empresas.

Se pessoas/usuários são citados como o elo mais fraco da segurança, ter um processo que começa com a integração de novos funcionários é usar de bom senso. Ou então você pensa: apenas 51% se classificam como fazendo um excelente trabalho de gerenciamento de recursos humanos em segurança, por meio da integração abrangente de funcionários e devidos processos para lidar com transferências e saídas deles. Também parece surpreendente que a tendência de treinar a equipe após um incidente permaneça inalterada, ano após ano, em apenas 39% dos entrevistados.

Um ataque pode ser perigoso sem o preparo adequado. Possivelmente, há espaço para melhorias nessa área quando 61% das empresas realizam uma simulação ou um exercício a cada seis meses para testar planos de resposta a incidentes de segurança cibernética (Figura 3). As simulações podem reforçar a capacidade de ter os controles adequados para detectar e responder o mais rápido possível e mitigar os danos.

"Quando as pessoas são enganadas e caem em golpes geralmente têm uma resposta passional, e é isso que os hackers fazem, eles tentam provocar uma resposta passional, por isso, tentamos simular essas situações de phishing com nossos funcionários. Tudo é baseado em contexto e, portanto, quando um e-mail informa que há uma encomenda esperando por você, você pensa: quem não deseja receber uma encomenda ou um presente? "

Figura 3 Com que frequência a empresa organiza uma simulação ou um exercício para praticar o plano de resposta a um incidente de segurança cibernética?
Porcentagem de entrevistados, N=3.321



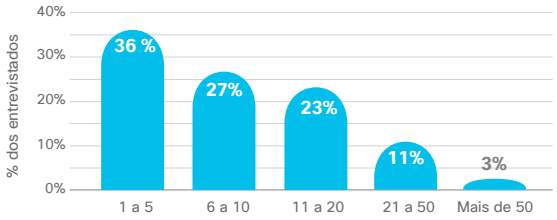
Fonte: Estudo comparativo do CISO Cisco 2019

Arquitetura: navegação no provisionamento do fornecedor

As empresas têm pressa em adquirir várias soluções específicas, pois aumentou a necessidade de ter proteção abrangente contra ameaças digitais. Sabemos disso porque em 2018, 21% dos entrevistados tinham mais de 20 fornecedores e 5% mais de 50. Esse ano, houve uma queda de 14% e 3%, respectivamente. Percebemos a tendência de queda do número de fornecedores e soluções, mas como as soluções de vários fornecedores não são integradas e, portanto, não compartilham a triagem de alertas e a priorização em determinados painéis, nossa pesquisa descobriu que mesmo os CISOs com menos soluções pontuais poderiam gerenciar melhor os alertas por meio de uma abordagem de arquitetura empresarial.

Para gerenciar melhor os alertas, uma prática recomendada de segurança é reduzir o número de fornecedores e soluções. Em 2018, havia 54% dos entrevistados com 10 ou menos fornecedores em seu ambiente, e agora esse número aumentou para 63% (Figura 4). Isso significa que mais entrevistados têm menos fornecedores. A consolidação de fornecedor, devido a uma série de razões possíveis, é real e mensurável.

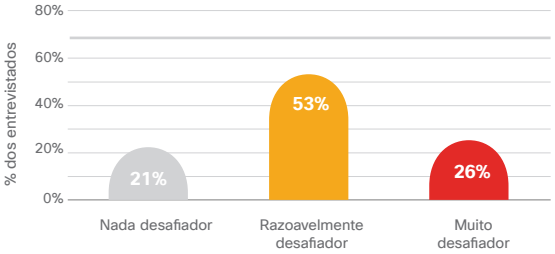
Figura 4 Número de fornecedores de segurança (marcas e fabricantes).
Porcentagem de entrevistados, N=3.248



Fonte: Estudo comparativo do CISO Cisco 2019

Não acredite somente na nossa palavra. Essa abordagem de vários fornecedores (em vez de uma abordagem integrada) faz com que haja um desafio constante de alertas: 79% dos entrevistados disseram que era um pouco ou muito desafiador orquestrar alertas de produtos de vários fornecedores, em comparação com 74% em 2018 (Figura 5). Assim, embora os profissionais de segurança tentem lidar com a expansão de fornecedores e seus problemas de atendimento, o gerenciamento não se tornou mais fácil e precisa de melhorias adicionais para otimizar recursos. É aqui que a análise de segurança, o aprendizado de máquina e a IA podem ajudar muito, automatizando os estágios iniciais de priorização e gerenciamento de alertas. As taxas de adoção muito ruins dessas novas tecnologias parecem ter variado um pouco este ano.

Figura 5 Gerenciamento de alertas de vários fornecedores de segurança.
Porcentagem de entrevistados, N=3.248



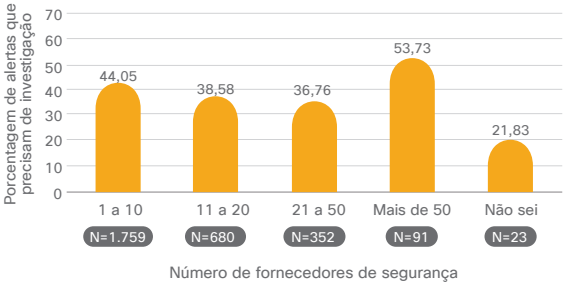
Fonte: Estudo comparativo do CISO Cisco 2019

"Se pudermos reduzir a quantidade de fornecedores e ter uma arquitetura mais integrada, isso nos ajuda muito. Preferiria ter mais automação no back-end com uma arquitetura integrada do que colocar algo em cima dela e escrever alguns novos scripts para consolidar tudo."

Embora o tamanho da empresa possa certamente contribuir para o número de alertas e fornecedores, os dados nos dizem que menos fornecedores podem tornar o gerenciamento de alertas mais eficiente (consulte a Figura 6). No topo do funil, 63% das empresas com apenas 1 a 5 fornecedores e 42% das empresas com 6 a 10 fornecedores receberam menos de 5.000 alertas por dia. Claro que isso também pode nos dizer que há alertas desligados.

A redução do número de fornecedores que você precisa gerenciar ajuda as equipes a se concentrarem em trabalhos mais importantes, como remediação. As empresas com menos de 10 fornecedores tinham uma taxa de resposta média, remediando 44% dos alertas legítimos, em vez de 42%. Você ganha mais eficiência reduzindo o número de fornecedores de segurança, conforme mostrado na Figura 6.

Figura 6 Contraste de quantos alertas precisam ser investigados por quantidade de fornecedor de segurança.
Alertas, N=2.905



Fonte: Estudo comparativo do CISO Cisco 2019

Por fim, descobrimos que 65% das empresas que estão muito atualizadas, e se atualizam constantemente com as melhores tecnologias disponíveis, com mais frequência tiveram uma contagem menor de alertas de segurança diários (até 10.000 por dia). A próxima melhor opção – substituir ou atualizar as tecnologias de segurança em um ritmo regular (mas não necessariamente contar com as melhores e mais recentes ferramentas) – teve 60% de chance de receber até 10.000 alertas por dia.

"No final do dia, o que importa é resolver todas as informações de alerta e é aí que definimos as ações para examinar informações. Então, se começamos a ver um determinado tipo de evento, isso é o que vai desencadear um incidente para nós."

Desafio de gerenciamento de alertas: você não conhece o que não vê

Falar sobre muitos alertas para alguém de segurança é como falar sobre o desafio do trânsito para quem mora em uma cidade grande. Sabemos que é ruim, mas temos que continuar. Você geralmente faz algo a respeito: organiza caronas, evita a hora do rush, trabalha em casa. E os alertas também são a chave para o desconhecido e não podem ser ignorados. No meio da pilha de informações, está escondido o 1% das ameaças que passa até mesmo pela melhor defesa em camadas.

Aqui estão cinco descobertas relacionadas ao cenário de alerta, conforme você nos relatou:

1. Houve uma mudança todos os anos com os entrevistados observando menos alertas, o que significa menos alertas para gerenciar e, em teoria, uma melhor oportunidade de lidar com os alertas importantes. O grupo com o menor volume de alertas recebeu 10.000 ou menos por dia e 59% estão nesse grupo, em comparação com 50% na pesquisa do ano anterior.
2. Dez mil alertas diários ainda é um número muito alto? Claro que sim, mas quando você pensa que 41% recebem mais de 10.000 e que alguns afirmam receber mais de 500.000 alertas (reconhecidamente apenas 1%), o número de 10.000 nos mostra que estamos, no mínimo, caminhando na direção certa.
3. As notícias não são tão boas assim. Você está respondendo a 50,7% dos alertas em comparação com 55,6% em 2018. Isso sugere que, embora alguns de vocês estejam recebendo menos alertas, o que parece facilitar o trabalho, muitos realmente estão respondendo a menos alertas.

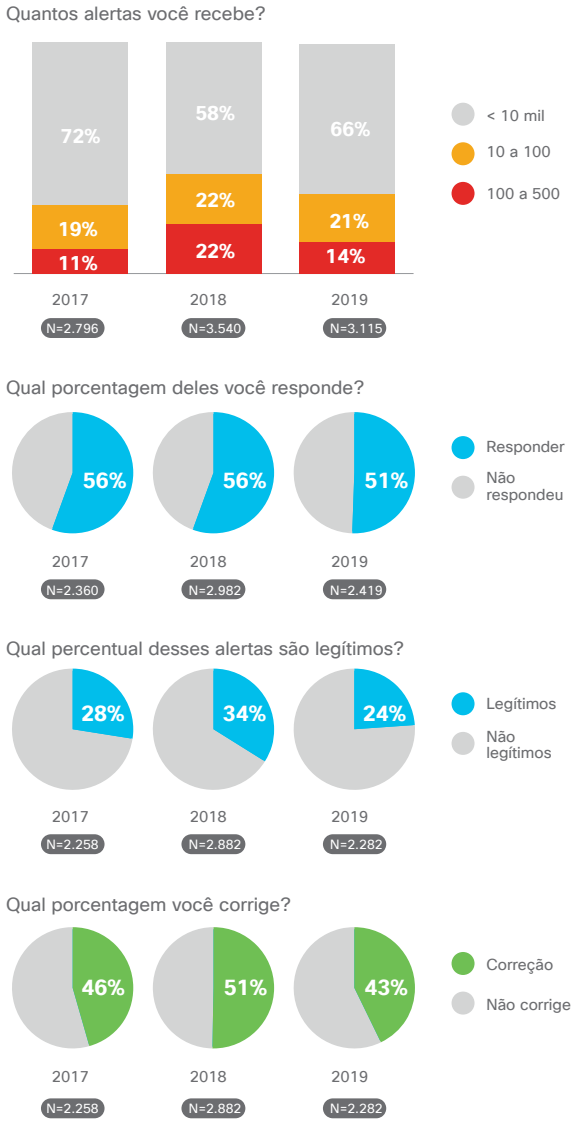
4. Apenas 24,1% dos alertas investigados eram legítimos, em comparação com 34% em 2018. Isso mostra que a precisão das ferramentas utilizadas para determinar quais alertas devem ser investigados não está correta.
5. Há notícias piores quando analisamos a correção de alertas: existe uma grande queda no número de alertas legítimos remediados, em relação à pesquisa de 2018 – de 50,5% para 42,8% este ano.

Colocado de outra forma e ilustrado na Figura 7: se você é uma das empresas que enfrenta até 10.000 alertas por dia, isso deixa 1.000 alertas legítimos desassistidos. Todos os dias. E essa é apenas a metade (50,7%) que você investigou. Nunca foi tão importante ter as ferramentas certas de resposta a ameaças de segurança, que possam incluir amplos conjuntos de dados, dar visibilidade a eles e fornecer meios para agir rapidamente.

Gerencie o que você mede

Essa queda na remediação é crucial, pois muitos de vocês estão passando a considerar a remediação como um indicador-chave da eficácia da segurança. O número de entrevistados que usam o tempo médio de detecção como uma métrica diminuiu de 61% (2018) para 51% (2019) em média. O tempo para correção também caiu de 57% (2018) para 40% (2019). A maior mudança é de entrevistados que se concentram no ***tempo para corrigir*** (48%) como um indicador, que caiu em relação aos 30% de 2018. Isso mostra um novo enfoque na correção como o KPI de um profissional de segurança para medir o procedimentos que ele utiliza. *Quando você compara isso com o aumento do número de alertas legítimos que não estão sendo remediados, uma queda no investimento em aprendizado de máquina e um aumento lento ou uma taxa constante na quantidade de treinamento, concluimos que precisamos de mais inovação no gerenciamento de alertas.*

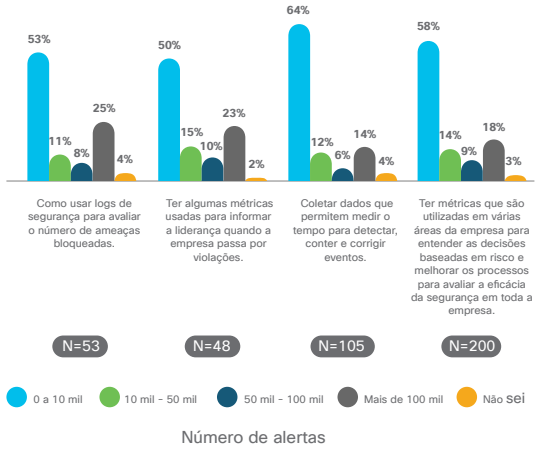
Figura 7 Comparação dos resultados da pesquisa de quantos alertas são identificados, em que porcentagem são respondidos, qual porcentagem desses alertas respondidos são legítimos e qual porcentagem de incidentes é corrigida.



Fonte: Estudo comparativo do CISO – Cisco 2019

Os dados da pesquisa também revelaram que 64% daqueles que coletam dados para permitir a medição do tempo de detecção receberam 10.000 ou menos alertas diários - o maior grupo dessa matriz (veja a Figura 8).

Figura 8 Como sua empresa mede a eficiência da segurança, se comparada ao número de alertas que você enfrenta?
Porcentagem de entrevistados, N=3.259



Fonte: Estudo comparativo do CISO - Cisco 2019

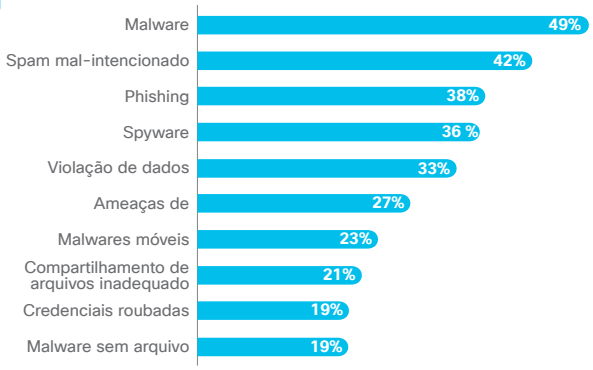
Preparo e resposta a violações: quando o desconhecido aparece

Ataques vistos no ano passado

Pela primeira vez este ano, perguntamos especificamente sobre os tipos de ataques que os CISOs sofreram e fizemos perguntas sobre uma lista de ataques comuns. Embora alguns tenham visto tipos bem específicas de malware, como o WannaCry (11%), ou categorias de ameaças, como malware de remoção (15%), os ataques mais citados são malware e suas variantes, como o ransomware.

"Hoje, 90% dos nossos incidentes ainda estão relacionados a malware, ou à evolução do malware, como ransomware e ataques semelhantes. Ainda não descobrimos exatamente qual é o vetor dessas ameaças persistentes avançadas."

Figura 9 Que tipos de incidentes de segurança/ ataques você enfrentou no ano passado.
Porcentagem de entrevistados, N=2.909



Fonte: Estudo comparativo do CISO - Cisco 2019

Conforme mostrado na Figura 9, dois dos três principais problemas estão relacionados à segurança de e-mail, e esse continua sendo o principal vetor de ameaças. Se você está investindo em proteger a mudança para o Microsoft Office 365 ou tentando proteger melhor o Business Email Compromise (BEC) usando o DMARC, o e-mail ainda é uma área a ser analisada. O fato de 2 dos 10 principais serem problemas de ameaças internas (compartilhamento de arquivos e credenciais roubadas) mostra que você deve olhar para o que está acontecendo dentro e fora, e estar ciente de que alguns criminosos podem entrar ao invés de invadir, mostrando a necessidade de uma melhor autenticação multifatorial (MFA). Em nenhum lugar há tanta necessidade de equilibrar a demanda por

segurança (permitindo a entrada das pessoas certas) como no suporte à continuidade dos negócios (não prejudicando as pessoas que você deixa entrar com uma experiência ruim de autenticação do usuário).

Como a preocupação com outras áreas continua grande, mas é gerenciável (como a mudança para a nuvem), a questão do comportamento do usuário (por exemplo, clicar em links mal-intencionados em e-mails ou sites) agora é a principal preocupação dos CISOs. Quando perguntados sobre o desafio de defender várias partes da sua infraestrutura, a maior preocupação era o comportamento do usuário. Essa percepção de vulnerabilidade se manteve estável nos últimos três anos - entre 56% a 57% dos entrevistados.

Também perguntamos quais desses tipos de ataques resultaram em algum nível de violação (perda de dados) e recebemos a seguinte ordem de prioridade nas respostas:

1. Malware (20%)
2. Violação de dados (19%)
3. Spyware (14%)
4. Phishing (13%)
5. Ransomware (13%)
6. Spam mal-intencionado (13%)

Curiosamente, as percepções de risco variaram entre as funções relacionadas à segurança. Por exemplo, os Diretores de risco e conformidade consideram que a maior vulnerabilidade são os "ataques direcionados". Esses executivos estão bem conscientes das terríveis consequências que um ataque fatal pode ter na continuidade dos negócios.

Para saber mais sobre quais violações ameaçam a estabilidade da empresa, leia o Relatório de ameaças de 2019 da Cisco.

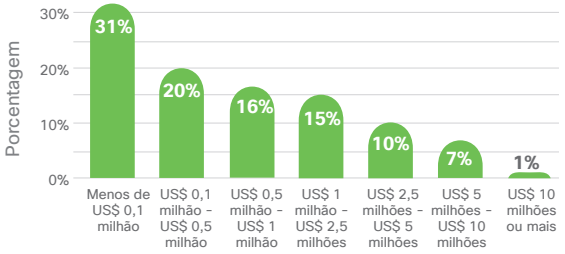
Custo de uma violação: muito mais que dinheiro

Estamos todos cientes das possíveis consequências de uma violação: perda financeira (veja a Figura 10), revés ou destruição da marca e da reputação, abalo na confiança dos acionistas, perda de dados valiosos, multas regulatórias e de não conformidade. A lista é infinita. Analisando a comparação dos dados ano a ano, há uma clara mudança nas questões de percepção. Não há como desistir da necessidade de manter as operações funcionando, mas a experiência do cliente e a reputação da marca passarm a figurar mais como as principais preocupações (Tabela 1).

Tabela 1 Principais preocupações devido a violações.

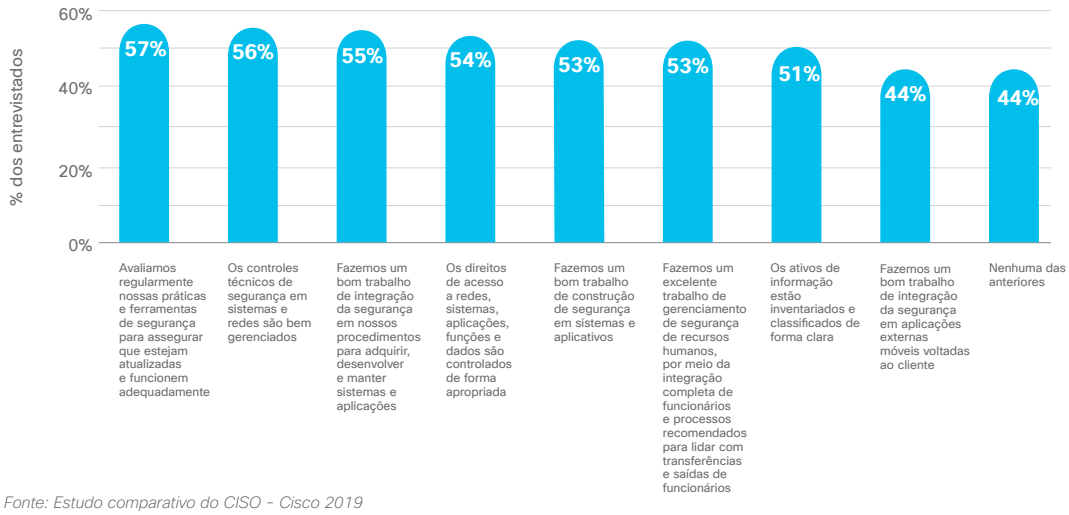
Preocupação devido a violações	Você disse: 2018	Você diz: 2019	
Operações	38%	36 %	Uma leve mudança para menos na preocupação com o operacional é ofuscada por problemas de clientes.
Retenção do cliente	26%	33%	Um sentimento constantemente negativo em relação às violações de dados e à prevalência de malware como o ransomware, tornam os consumidores mais cautelosos.
Reputação da marca	27%	32%	Nomes conhecidos se tornam sinônimos de um grande ataque por anos. Não citamos nenhum aqui, mas acreditamos que os clientes criarão uma lista em breve.

Figura 10 Pensando na violação mais importante que sua empresa sofreu no ano passado, qual foi o impacto financeiro?
Porcentagem de entrevistados, N=2.386



Fonte: Estudo comparativo do CISO Cisco 2019

Figura 11 Que práticas estão sendo empregadas para proteger a empresa?
Porcentagem de entrevistados, N=3.223



Fonte: Estudo comparativo do CISO - Cisco 2019

O que você está fazendo para lidar com a ameaça de uma violação

Perguntamos aos nossos profissionais de segurança até que ponto suas empresas tomaram precauções para instaurar processos, usar produtos e colocar pessoas para proteger a empresa. Os resultados estão demonstrados na Figura 11.

Além disso, perguntamos quais abordagens são adotadas para mitigar os riscos de segurança e esses resultados estão demonstrados na Figura 12.

Com base em mais dados, descobrimos que, embora 85% dos entrevistados estivessem muito bem informados sobre políticas e práticas relacionadas à segurança e proteção da infraestrutura, apenas 74% tinham muito conhecimento sobre continuidade de negócios e recuperação de desastres. Apenas 75% dos entrevistados estavam muito bem informados sobre respostas a incidentes. Isso é um problema. Todos os envolvidos em segurança precisam estar bem informados sobre respostas a incidentes. Na verdade, isso pode ser estendido a todos os funcionários da empresa. É aí que o treinamento se torna vital, e a falta de destaque nos resultados deste ano continua a chamar atenção.

Figura 12 Posturas de segurança: abordagens para reduzir os riscos de segurança.
Porcentagem de entrevistados, N=3.248

Fonte: Estudo comparativo do CISO - Cisco 2019

Como lidar com as incertezas

A ponte entre encontrar ameaças desconhecidas e agir sobre as corretas está em uma postura de segurança eficaz. Aqui estão as recomendações práticas que planejamos para você considerar, de acordo com os resultados da pesquisa:

- Baseie o orçamento de segurança em resultados de segurança medidos com estratégias práticas, junto com seguro cibernético e avaliações de risco, para orientar as decisões de aquisição, estratégia e gerenciamento.
- A única maneira de entender as necessidades de segurança subjacentes de um caso de negócios é colaborar entre os silos – entre os grupos de TI, redes, segurança e conformidade.
- Existem processos comprovados que as empresas podem empregar para reduzir a exposição a violações e a extensão que elas atingem. Prepare-se com simulações. Use métodos investigativos rigorosos e entenda os métodos mais convenientes de recuperação.
- ML, IA e mais automação vão potencializar exponencialmente os esforços de segurança – e no ano que vem, precisamos ver mais entrevistados na fase de implementação e prática "completamente dependente". A Cisco utiliza aprendizado de máquina em vários produtos de segurança, inclusive AMP, Umbrella, Stealthwatch e Cisco Threat Response.
- Construir um Centro de operações de segurança (SOC) para gerenciar a resposta a violações em empresas de todos os portes.
- A segurança na nuvem pode ajudar com o desconhecido. 90% concordam que utilizar a segurança da nuvem aumenta a visibilidade da rede. O Cisco Umbrella é uma solução de segurança fornecida pela nuvem que impede que os usuários se conectem a domínios, IPs e URLs mal-intencionados conhecidos e suspeitos, independentemente de os usuários estarem ou não dentro da rede empresarial.
- Proteção de data centers e com ecossistemas de várias nuvens com soluções integradas, como a solução Cisco Secure Data Center com a visibilidade, segmentação e detecção de ameaças do Tetration, Stealthwatch e NGFW.
- Abordagem do vetor de ameaça principal com proteção contra phishing, filtragem de spam avançada e defesa contra e-mail empresarial comprometido com DMARC. Confira o Cisco Email Security.
- A segurança de endpoint ajuda a lidar com ameaças desconhecidas nos dispositivos de usuários. Experimente o Cisco Advanced Malware Protection para endpoints, também disponível nas soluções de Web, e-mail, nuvem e segurança da rede, criando um ambiente de produtos que trabalhe em conjunto para proteção mais eficaz contra ameaças.
- Conte com rápida detecção de ameaças, acesso altamente seguro e segmentação definida por software com a visibilidade de rede e segmentação da Cisco que combina o Cisco Stealthwatch Enterprise, o Cisco Identity Services Engine e a tecnologia Cisco rustSec.
- Acesso confiável é um componente essencial da segurança. O Duo verifica a confiabilidade do usuário (confirmando se o usuário é legítimo) usando a melhor solução de autenticação multifatorial (MFA) adaptável da categoria.

"Às vezes, pode parecer uma corrida insana descobrir como se manter à frente de hackers mal-intencionados, mas a forma como enxergo o que está por vir, você deve acompanhar a empresa em termos de novas técnicas e tecnologias, e então você vai perceber as defasagens."

"Às vezes, os CISOs recorreram ao medo para estimular algum investimento. O que preferimos analisar é: qual é o risco para a empresa? Há vários níveis de risco aceitáveis, e então nos concentramos onde há o maior risco para a empresa. Temos sorte de a Cisco levar a segurança muito a sério e investir em arquitetura de base para nos preparar melhor."

Marisa Chancellor
Entrevista com Marisa Chanceler diretora sênior, Security & Trust Organization, Cisco

Sobre a pesquisa comparativa da Cisco

A pesquisa duplo-cega, conduzida por um parceiro de pesquisa independente, abrange muitos setores, incluindo varejo, transporte, manufatura, serviços financeiros, bem como governo e ensino superior. Os participantes são funcionários em tempo integral, trabalhando no mercado intermediário (250 a 999 funcionários), em empresas (1.000 a 9.999) e grandes corporações (mais de 10.000).

Os entrevistados ocupam uma série de funções, incluindo Diretores de segurança da informação (CISO), Diretores de informação (CIOs) e outros cargos de nível sênior. Eles são bem informados sobre os procedimentos e as políticas de segurança e estão envolvidos na criação da estratégia de segurança. A maioria tem cargos de CISO, Diretor/Gerente de TI e/ou CTO, e 99% dos entrevistados da pesquisa têm uma equipe na empresa dedicada à segurança cibernética.

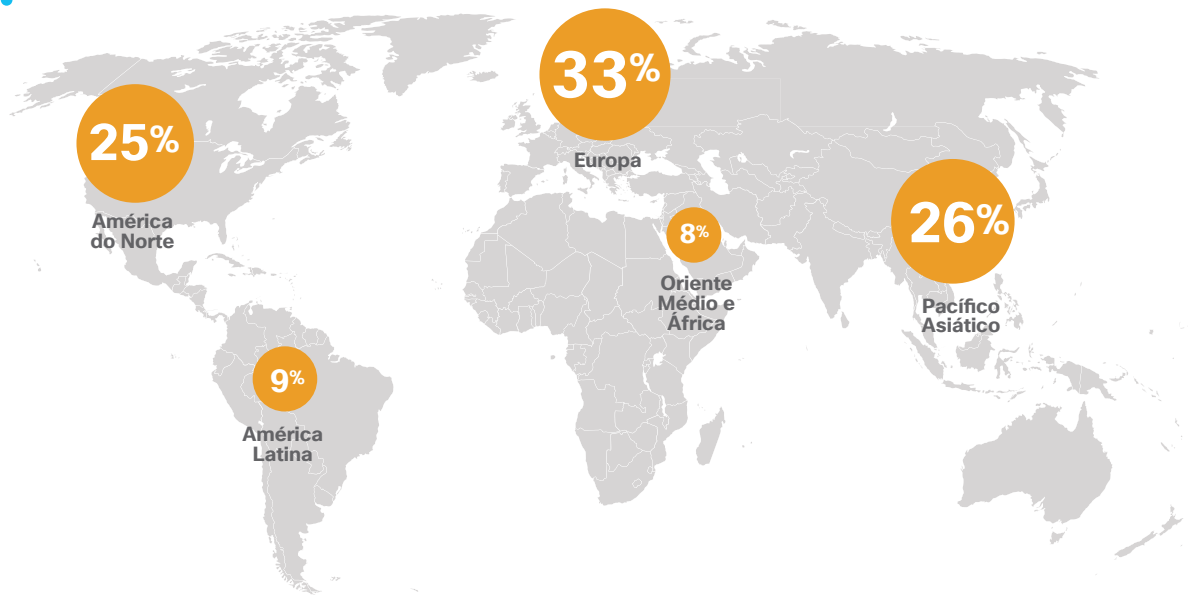
Há entrevistados de todos os continentes e 18 países, incluindo EUA, Canadá, Reino Unido, França, Alemanha, Austrália, Japão e China (Figura 13).

Entrevistados qualificados

Os seguintes critérios foram usados para qualificar os entrevistados:

- Adultos (25 anos ou mais) aprovados na triagem de emprego sensível/competitivo.
- Trabalham em tempo integral para uma empresa com fins lucrativos, no governo ou ensino superior com mais de 250 funcionários em tempo integral e um departamento formal de TI.
- Está envolvido em segurança de TI, além de na aprovação de orçamentos.
- Está muito bem informado sobre práticas e políticas de segurança.

Figura 13 Distribuição dos entrevistados por região, arredondado para o percentual mais próximo.
Porcentagem de entrevistados, N=3.259



Fonte: Estudo comparativo do CISO - Cisco 2019

Sobre a Serie de Relatórios de Cibersegurança

Ao longo da última década, a Cisco publicou uma série de informações sobre inteligência de ameaças para profissionais de segurança interessados no status global da segurança digital. Estes relatórios abrangentes forneciam detalhes dos cenários de ameaças e as implicações para as empresas, bem como as melhores práticas para se defenderem contra os impactos das violações de dados.

Na nova abordagem da nossa liderança de pensamento, a Cisco Security está publicando vários artigos baseados em pesquisas e orientados por dados sob o banner **Serie de Relatórios de Cibersegurança**. Ampliamos o número de títulos para incluir relatórios diferentes para profissionais de segurança com interesses diferentes. Apelando para a profunda e vasta experiência de pesquisadores de ameaças e inovadores no setor de segurança, a coleção de relatórios da série 2019 inclui o Relatório de Privacidade de Dados, o Relatório de Ameaças e o Relatório de Referência do CISO, e outros ainda virão ao longo do ano.

Para obter mais informações acesse www.cisco.com/br/securityreports.

Sede nas Américas
Cisco Systems, Inc.
San Jose, CA

Sede na Ásia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Cingapura

Sede na Europa
Cisco Systems International BV Amsterdam,
Holanda

A Cisco possui mais de 200 escritórios em todo o mundo. Os endereços, números de telefone e de fax estão disponíveis no site da Cisco www.cisco.com/go/offices.

Publicado em março de 2019 CISO_01_0319_r1

© 2019 Cisco e/ou suas afiliadas. Todos os direitos reservados.

Cisco e o logotipo da Cisco são marcas comerciais ou marcas comerciais registradas da Cisco e/ou de suas afiliadas nos EUA e em outros países. Para ver uma lista de marcas comerciais da Cisco, acesse: www.cisco.com/go/trademarks. Todas as marcas de terceiros citadas pertencem a seus respectivos detentores. O uso do termo "parceiro" não implica uma relação de sociedade entre a Cisco e qualquer outra empresa. (1110R)

Adobe, Acrobat e Flash são marcas registradas ou comerciais da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.