SOPHOS

O Estado da Segurança Cibernética 2023: O impacto comercial dos adversários

Resultados de um estudo independente com 3.000 líderes responsáveis pela segurança cibernética distribuídos em 14 países realizada em janeiro e fevereiro de 2023.

Documento técnico Sophos. Abril, 2023

Metodologia da pesquisa

Para explorar o verdadeiro impacto comercial da segurança cibernética, a Sophos contratou uma pesquisa independente com 3.000 líderes responsáveis pela segurança cibernética distribuídos em 14 países. Todos os entrevistados eram de organizações com entre 100 e 5.000 funcionários. A pesquisa foi conduzida em janeiro e fevereiro de 2023 pela Vanson Bourne.

3000
entrevistados

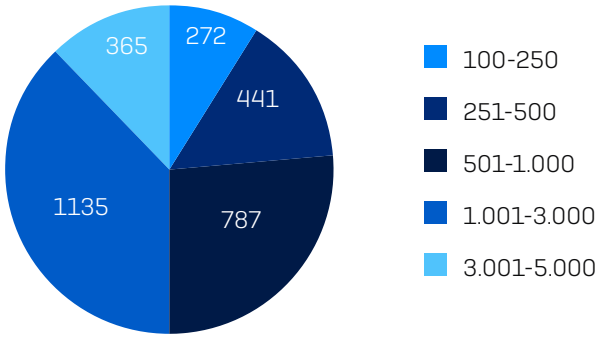
100 a 5.000
funcionários

14
países

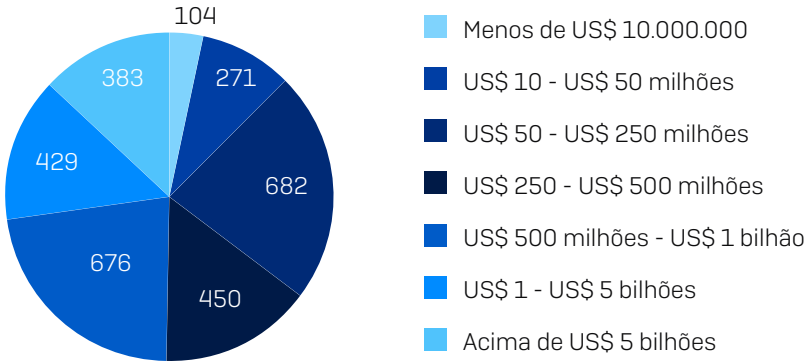
<US$ 10M - US$ 5B+
Receita anual

Jan/Fev 23
elaboração da pesquisa

Entrevistados por tamanho da organização (nº de funcionários)



Entrevistados por tamanho da organização (receita anual)



Entrevistados por país

PAÍS	NÚMERO DE ENTREVISTADOS	PAÍS	NÚMERO DE ENTREVISTADOS
Estados Unidos	500	Reino Unido	200
Alemanha	300	África do Sul	200
Índia	300	França	150
Japão	300	Espanha	150
Austrália	200	Áustria	100
Brasil	200	Singapura	100
Itália	200	Suíça	100

Sumário executivo

Situação: os adversários estão tomando a dianteira, e as defesas estão ficando para trás

O estudo sobre a realidade da segurança cibernética atual revela um sistema desalinhado, com adversários e defesas se movendo a diferentes velocidades. Utilizando a automação, modelos de crimes cibernéticos "as-a-service", clonagens furtivas e adaptação, os adversários estão avançando e se especializando na execução de uma grande diversidade de ataques sofisticados e em grande escala. No ano passado, 94% das organizações registraram alguma forma de ataque cibernético, o que nos permite presumir que, independentemente do tamanho da receita, todas as empresas serão um alvo na mira em 2023.

Presas a um grande volume de alertas, tempo excessivo respondendo a incidentes e falta de profissionais especializados, as defesas não conseguem acompanhar o ritmo. Operacionalizar a detecção e resposta a ameaças é algo difícil para a maioria das organizações, com 93% delas considerando a execução de tarefas e operações essenciais de segurança algo desafiador.

Investigar alertas de segurança é um problema generalizado. Em média, um pouco menos da metade (48%) dos alertas são investigados para determinar se são sinais de atividades maliciosas, e a maioria das organizações tem dificuldade para identificar (71%) e priorizar (71%) quais alertas e eventos devem ser investigados. Para os alertas que exigem atenção, o processo completo de detecção, investigação e resposta leva, em média, nove horas para as organizações com 100 a 3.000 funcionários, subindo para 15 horas naquelas com uma média de 3.001 a 5.000 funcionários.

Do ponto de vista operacional, as defesas não confiam muito em seus processos, que colocam a configuração incorreta das ferramentas de segurança no topo da lista de riscos de segurança observados em 2023. Mais da metade (52%) dos profissionais de TI dizem que os ataques cibernéticos estão agora muito avançados para as suas organizações lidarem com eles por conta própria, subindo para 64% quando se trata das pequenas empresas (100 a 250 funcionários).

Impacto nos negócios: a situação traz consequências para as finanças, operações e recursos

Esse sistema em desalinho tem um impacto considerável na organização como um todo. As repercussões financeiras diretas de um incidente cibernético são imensas e muito bem conhecidas, chegando a um custo médio de US$ 1,4 milhão para uma organização de pequeno ou médio porte reparar um ataque de ransomware[1]. Os custos de limpeza desses incidentes são apenas parte da história.

A capacidade de operação geral da TI fica reduzida, com 55% dos entrevistados declarando que lidar com as ameaças cibernéticas teve um impacto negativo no trabalho das equipes de TI em outros projetos. A natureza urgente e imprevisível da segurança cibernética também atrapalha o empenho que se coloca nos negócios: 64% gostariam que as equipes de TI pudessem gastar mais tempo em questões estratégicas e menos tempo apagando incêndios.

A quantidade de tempo gasta em detectar, investigar e remediar alertas de segurança também tem um impacto financeiro considerável quando se trata dos custos gastos com recursos.

A situação também é um fardo pesado para os funcionários. 57% dos profissionais de TI dizem que a preocupação de que a organização possa vir a ser atingida por um ataque cibernético por vezes lhes tira o sono, subindo para 65% quando se trata de organizações com 3.001 a 5.000 funcionários. Dado o alto custo de recrutar, treinar e reter esse pessoal especializado, as repercussões criam outros desafios e custos extras para os negócios.

1 O Estado do Ransomware 2022, Sophos

Recomendação: acelere seu carrossel de defesas e deixe seus adversários para trás

Permitir que as suas defesas ultrapassem os invasores na corrida da segurança cibernética de 2023 requer uma abordagem ampla, porém direcionada. Primeiramente, as organizações precisam estabelecer um processo de resposta a incidentes que possa ser escalado – obtido através da minimização da superfície de ataque e do volume de alertas que exigem atenção e da otimização do tempo de resposta por meio do uso de serviços especializados.

Elas também precisam implementar defesas adaptáveis que se ajustem automaticamente à situação. Isso permite desacelerar os adversários e ganhar tempo para a resposta de suas defesas.

Por fim, precisam criar um ciclo virtuoso que combine tecnologia e expertise humana para turbinar as defesas, capacitando um aumento em velocidade, eficácia e impacto. Quando em conjunto, elas aceleram o seu carrossel de defesas, gerando um impulso maior.

Uma peça central para o sucesso dessa abordagem é o uso de especialistas terceirizados. A boa notícia é que as organizações já têm uma abordagem que mescla processos de segurança cibernética, com 94% das empresas trabalhando com especialistas externos em determinadas posições para escalar suas operações. Conforme os adversários intensificam seu empenho, unir forças com um pessoal dedicado à segurança de suas operações torna-se essencial.

Principais descobertas

94% das organizações passaram por alguma forma de ataque cibernético no ano passado

Exfiltração de dados é a preocupação de segurança número 1 de 2023

93% acham a execução de tarefas e operações essenciais de segurança algo desafiador

48% dos alertas de segurança são investigados

15 horas é o tempo médio para detectar, investigar e responder a um alerta em organizações com 3.001 a 5.000 funcionários.

A configuração incorreta das ferramentas de segurança está no topo da lista de riscos de segurança observados em 2023

52% dizem que as ameaças cibernéticas estão muito avançadas para suas organizações lidarem com elas por conta própria

55% dizem que lidar com as ameaças cibernéticas teve um impacto negativo no trabalho das equipes de TI em outros projetos

64% gostariam que as equipes de TI pudessem dedicar mais tempo a questões estratégicas e menos tempo apagando incêndios

57% dos profissionais de TI dizem que a preocupação de que a organização venha a ser atingida por um ataque cibernético lhes tira o sono

Ameaças cibernéticas de 2023: a realidade nas linhas de frente

Ameaças cibernéticas mais preocupantes de 2023

99% dos profissionais de TI estão preocupados com as ameaças cibernéticas que afetam suas organizações em 2023. A exfiltração de dados (roubo por um invasor externo) encabeça a lista das ameaças que mais preocupam os profissionais de TI e o efeito que têm em suas organizações, seguida de perto pelo phishing (incluindo spear phishing). O ransomware ocupa a terceira posição.

É importante lembrar que essas três ameaças estão geralmente interligadas: um e-mail de phishing costuma iniciar um ataque que resulta em exfiltração de dados e ransomware.

AMEAÇA CIBERNÉTICA	PORCENTAGEM DE ENTREVISTADOS QUE A CONSIDERAM UMA DAS PRINCIPAIS PREOCUPAÇÕES
Exfiltração de dados (roubo por um invasor externo)	41%
Phishing (incluindo spear phishing)	40%
Ransomware	35%
Extorsão cibernética	33%
Ataque de negação de serviço (DDoS)	32%
Comprometimento de e-mail corporativo (BEC)	31%
Adversários ativos (hackers humanos que atuam via teclado)	30%
Malwares móveis	30%
Criptomineradores	22%
Wipers	16%
Outros	0%
Não me preocupo com ameaças cibernéticas que possam afetar minha organização em 2023	1%
Não sabe	0%

Pensando em 2023, quais as ameaças cibernéticas mais preocupantes que podem vir a afetar a sua organização? (n=3.000)

Agora os adversários executam uma infinidade de ataques em grande escala

As preocupações que tiram o sono dos profissionais de TI se aproximam do que a realidade tem mostrado nas linhas de frente, com 94% das organizações vitimadas por pelo menos um ataque cibernético no último ano. Ainda que o ransomware tenha sido o ataque mais difundido, os adversários executam uma ampla gama de ataques em grande escala. A intensidade e diversidade dos ataques cria um desafio crescente e considerável para as defesas.

Por trás desses números está o aumento do profissionalismo da economia do crime cibernético, incluindo o crescimento do modelo "as a service", como "access-as-a-service", "phishing-as-a-service" e "scamming-as-a-service". Essa evolução nas operações cibernéticas criminosas facilitou a entrada de aspirantes a malfeitores no mundo do crime cibernético. [Para obter mais informações, leia o Relatório de Ameaças 2023 da Sophos.]

Registro de ataques cibernéticos não pertinentes a ransomwares que vitimaram as organizações e o percentual de relatos

Ataques por adversários ativos agora são corriqueiros

23%
das organizações passaram por um ataque envolvendo um adversário ativo no último ano

30%
dizem que os adversários ativos são uma das ameaças cibernéticas mais preocupantes de 2023

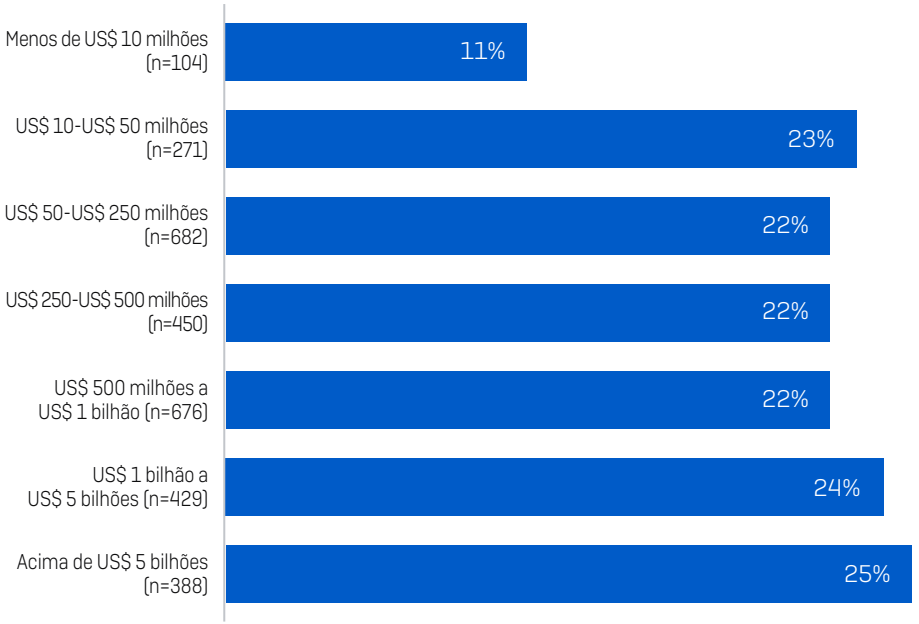
Adversários ativos são agentes de ameaças que adaptam suas técnicas, táticas e procedimentos (TTPs) atuando através de ações práticas e imediatas em resposta às tecnologias de segurança utilizadas pelas equipes de defesa e como forma de escapar da detecção. Esses ataques, que geralmente resultam em incidentes devastadores de ransomware e violação de dados, estão entre os mais difíceis de conter.

23% dos entrevistados relatam que suas organizações passaram por um ataque envolvendo um adversário ativo no último ano. O índice de ataque foi consistente, independentemente do tamanho da organização, variando em apenas dois pontos percentuais entre todas as segmentações por porte das organizações.

É interessante constatar que, para as organizações com menos de US$ 10 milhões em receita anual, o índice de ataques registrados de adversários ativos caiu para apenas 11%, o que pode indicar que os invasores estão focando deliberadamente em alvos mais endinheirados. Detectar adversários ativos requer grandes habilidades, e muito provavelmente o índice real de incidentes é bem maior.

Refletindo sobre o potencial devastador desses ataques, 30% dos entrevistados registraram que os adversários ativos são uma das ameaças cibernéticas mais preocupantes de 2023.

Experiência com ataques de adversários ativos por receita

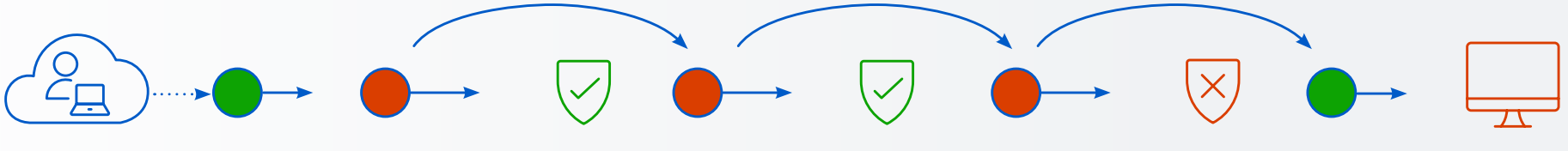


Você passou por algum ataque cibernético no ano passado? Sim. Adversários ativos (hackers humanos que atuam via teclado)

Entendendo os adversários ativos

Para entender o tamanho do desafio enfrentado pelas equipes de defesa, é essencial entender que bloquear os adversários ativos não é o suficiente para frustrar suas artimanhas. Esses agentes habilidosos e persistentes aplicam várias técnicas, táticas e procedimentos (TTPs) para atingir seus objetivos:

- Explorar pontos fracos na segurança para penetrar nas organizações e mover-se lateralmente pelas redes utilizando-se de credenciais roubadas, vulnerabilidades sem patches e ferramentas de segurança configuradas incorretamente.
- Abusar de ferramentas de TI legítimas usadas pelas defesas para evitar disparar detecções.
- Modificar seus ataques em tempo real em resposta a controles de segurança e continuar alternando entre novas técnicas até que encontrem uma maneira de atingir seus objetivos.



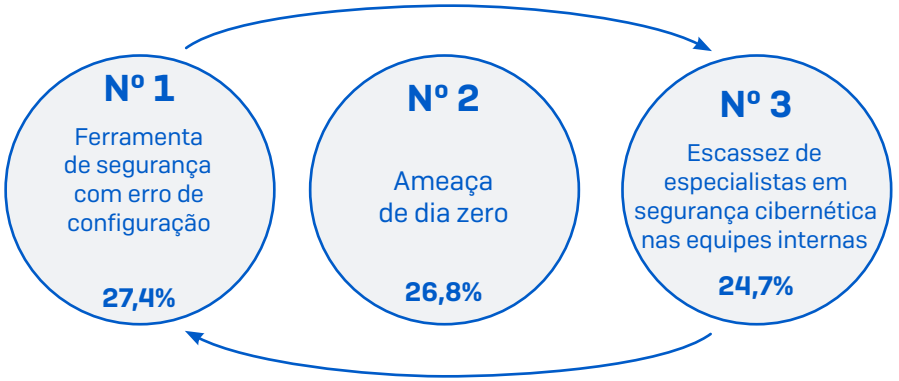
Segurança cibernética 2023: O Estado das Defesas

Riscos cibernéticos mais preocupantes

Configurações incorretas nos controles de segurança (por exemplo, em uma solução de endpoint ou firewall) são o risco mais amplamente percebido, com 27,4% dos entrevistados incluindo esse risco entre os três principais riscos cibernéticos. Essa alta posição no ranking ilustra os desafios enfrentados pelas equipes de TI para garantir que seus controles de segurança permaneçam corretamente configurados e operando continuamente, e o nível de preparo dos adversários em prontidão para explorar as possíveis lacunas nas defesas de uma organização.

Ataques de dia zero, ou seja, ataques que exploram uma vulnerabilidade de segurança ou uma falha de software até então desconhecida, ocupam a segunda posição, sendo responsáveis por 26,8% dos riscos à segurança. A escassez de profissionais especializados em segurança cibernética nas equipes internas ocupa a terceira posição na lista, contabilizando 25% das respostas dos entrevistados.

Existe uma relação direta entre falta de competências profissionais e erros nas configurações das ferramentas de segurança: sem tempo, conhecimento e experiência para configurar os controles corretamente, criam-se deficiências em suas defesas.



RISCO À SEGURANÇA CIBERNÉTICA	PORCENTAGEM NO RANKING DAS TRÊS PRINCIPAIS PREOCUPAÇÕES
Configurações incorretas nos controles de segurança (por exemplo, em uma solução de endpoint ou firewall)	27%
Ameaças de dia zero (uma ameaça que se aproveita de uma técnica de ataque até então desconhecida)	27%
Escassez de especialistas em segurança cibernética nas equipes internas	25%
Credenciais e dados de acesso roubados	24%
Dispositivos desprotegidos (incluindo dispositivos desconhecidos)	24%
Falta de ferramentas de segurança cibernética	23%
Vulnerabilidades sem patches	22%
Habilitar o acesso a usuários remotos	20%
Rede sem fio desprotegida	20%
Usuários internos (acidentais)	18%
Cadeia de suprimentos/parceiros	18%
Ferramentas de acesso remoto	18%
Usuários internos (propositais)	17%
Dispositivos IoT	17%
Outros	0%
Nenhum desses riscos de segurança cibernética é representativo para a minha organização	0%
Não sabe	0%

Quem ou quais você considera como sendo os três principais riscos à segurança cibernética da sua organização? Combinação de respostas classificadas em primeiro, segundo e terceiro lugares (n=3.000)

Diferentes abordagens ao investigar alertas

Organizações investigam
48% de seus alertas de segurança
para identificar se são sinais de atividades maliciosas

Um dos desafios para as equipes de defesa é identificar quais alertas investigar e como usar seus recursos limitados da melhor forma possível.

Em média, um pouco menos da metade (48%) dos alertas de segurança são investigados para identificar se são sinais de atividades maliciosas, subindo para 54% nas organizações com 3.001 a 5.000 funcionários. Contudo, as abordagens diferem imensamente: 16% das organizações investigam mais de três quartos de seus alertas (incluindo 5% que dizem investigar todos os alertas), enquanto 18% investigam um quarto ou menos.

Analisando sob o ponto de vista dos setores, o governo central/federal investiga a mais baixa porcentagem de alertas (39%) (n=89); já os setores de energia, petróleo/gás e serviços de utilidade investigam a mais alta taxa (55%) (n=69).

Gasto indireto com detecção, investigação e resposta

O tempo médio para detectar, investigar e responder a um alerta é de nove horas para organizações com 100 a 3.000 funcionários, aumentando para 15 horas para aquelas com uma média de 3.001 a 5.000 funcionários – um provável reflexo da maior complexidade de seus ambientes operacionais.

A pesquisa revelou uma variação considerável por indústria, com as organizações nos setores de manufatura e produção (15 horas) e energia, petróleo/gás e serviços de utilidade pública (18 horas) levando mais do dobro de tempo em comparação com os setores de TI, tecnologia e telecomunicações (6,75 horas).

Vale notar que a maioria dos alertas não chegarão ao estágio de resposta. A maioria dos ataques será bloqueada proativamente pelas tecnologias de segurança, com um subconjunto de alertas averiguado e posteriormente investigado. As ações de resposta também apresentarão consideráveis variações devido à natureza do evento que exige ser remediado – desde remover um e-mail de phishing da caixa de entrada dos usuários até recompilar a totalidade de um farm de servidores.

Tempo médio para detectar, investigar e responder a um alerta

ATIVIDADE	100-3.000 FUNCIONÁRIOS (n=2.460)	3.001-5.000 FUNCIONÁRIOS (n=350)	TI, TECNOLOGIA E TELECOMUNICAÇÕES (n=98)	MANUFATURA E PRODUÇÃO (n=331)	ENERGIA, PETRÓLEO/GÁS E SERVIÇOS DE UTILIDADE PÚBLICA (n=66)
Detecção	3 horas	3 horas	1,5 horas	3 horas	6 horas
Investigação	3 horas	6 horas	2,25 horas	6 horas	6 horas
Resposta	3 horas	6 horas	3 horas	6 horas	6 horas
Total	**9 horas**	**15 horas**	**6,75 horas**	**15 horas**	**18 horas**

Quanto tempo leva para a sua organização detectar, investigar e, se necessário, corrigir um possível incidente?
(n=2.812 entrevistados que investigam alertas internamente)

As organizações são carentes em pessoal capacitado em operações essenciais de segurança

Como já foi visto, os profissionais de TI consideram a falta de especialistas em segurança cibernética em suas equipes internas um dos grandes riscos à segurança em 2023. Indo mais a fundo, a pesquisa revela que a maioria das organizações tem dificuldade com suas tarefas diárias e operações básicas de segurança, com 93% classificando pelo menos uma das seguintes atividades como "desafiadora":

- Distinguir sinais de ruídos (71% acham desafiador)
- Priorizar quais sinais/alertas investigar (71% acham desafiador)
- Reunir dados suficientes para identificar se um sinal é maligno ou benigno (71% acham desafiador)
- Remediar alertas ou incidentes maliciosos com rapidez (71% acham desafiador)
- Identificar a causa principal de um incidente (75% acham desafiador)
- Manter registros precisos das investigações (68% acham desafiador)

Identificar a causa principal de um incidente é o problema mais genérico entre todos, com 75% dos entrevistados dizendo que acham isso desafiador.

Organizações com receitas anuais mais baixas (abaixo de US$ 10 milhões) são as mais propensas a sentirem o peso das tarefas operacionais de segurança, seguidas pelas de mais alta receita (acima de US$ 5 bilhões). As duas extremidades do espectro enfrentarão diferentes obstáculos, com complexidades organizacionais e sistemas que muito provavelmente desempenharão um papel de maior peso para as grandes organizações.

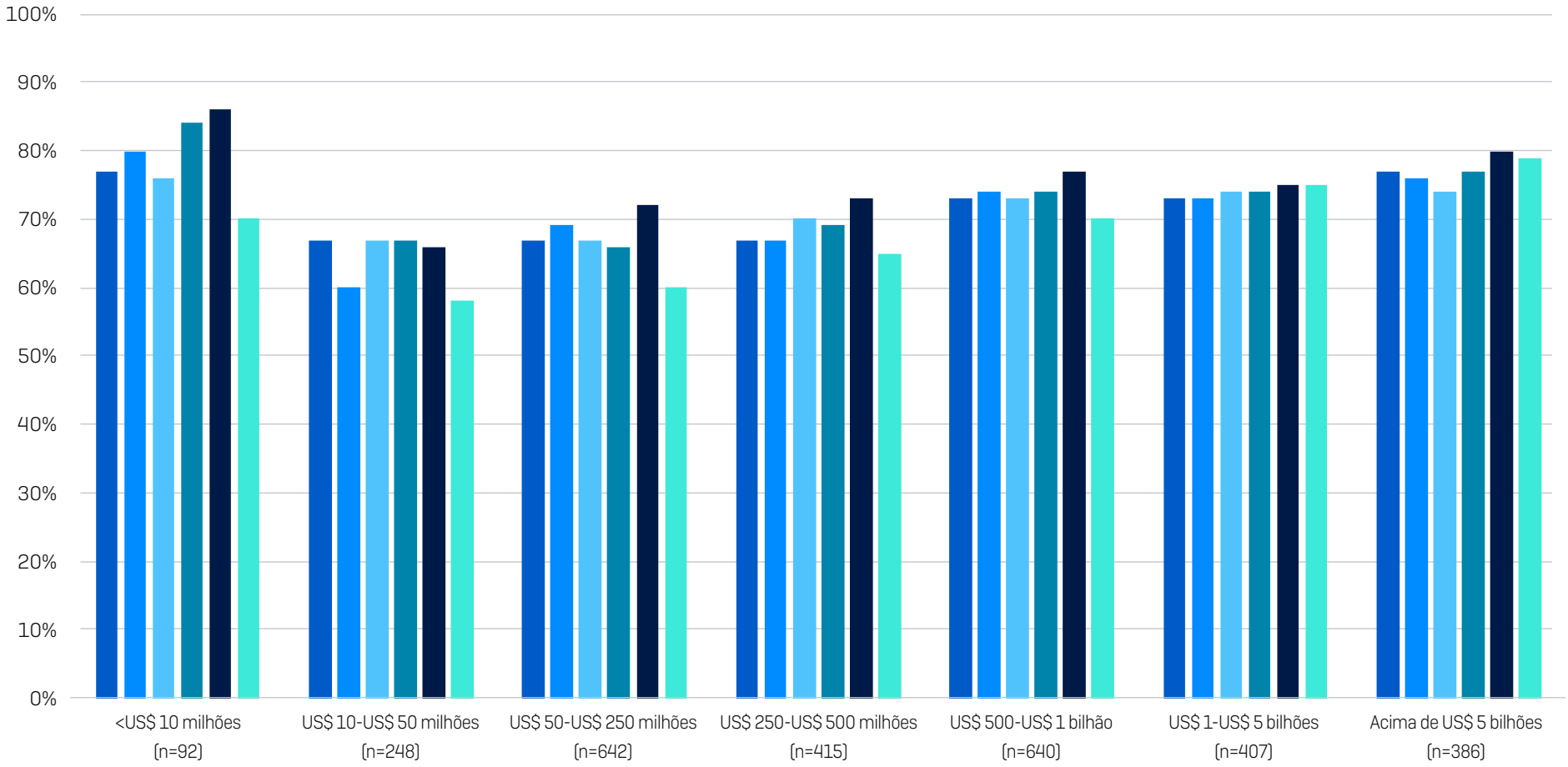
A escassez de recursos humanos especializados cria um efeito dominó: a investigação de alertas demora mais, o que, por sua vez, diminui a capacidade da equipe e aumenta a exposição a riscos.

93%
acham as operações de segurança desafiadoras

75%
acham difícil identificar a causa principal de um incidente

71%
têm dificuldades para identificar quais alertas investigar

Organizações que acham as tarefas e operações de segurança “desafiadoras” por receita



Entrevistados cujas organizações acham as tarefas e operações de segurança algo “muito desafiador” ou “um pouco desafiador” quando investigam alertas suspeitos (n=2.812 entrevistados que investigam alertas internamente)

- Distinguir sinais de ruídos, ou seja, entender quais sinais/alertas investigar
- Priorizar quais sinais/alertas investigar
- Reunir dados suficientes para identificar se um sinal é maligno ou benigno
- Identificar a causa principal de um incidente, ou seja, como o adversário entrou na organização
- Remediar alertas ou incidentes maliciosos com rapidez
- Manter registros precisos das investigações

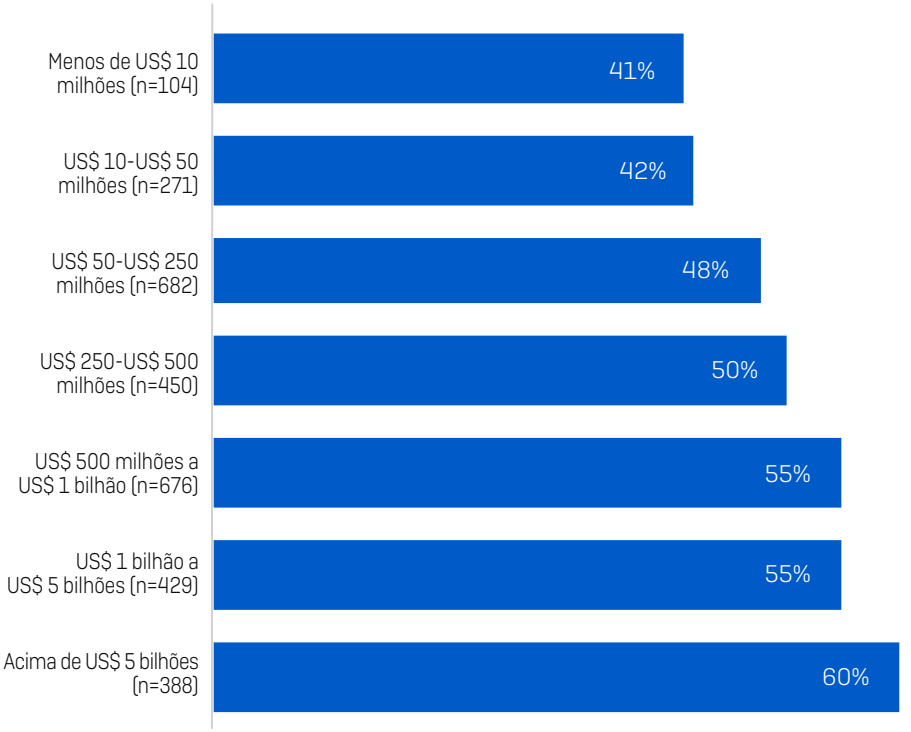
Os adversários desbancaram as defesas

52%
dizem que as ameaças cibernéticas estão muito avançadas para suas organizações lidarem com elas por conta própria

Mais da metade (52%) dos profissionais de TI dizem que os ataques cibernéticos estão agora muito avançados para as suas organizações lidarem com eles por conta própria, subindo para 64% quando se trata das pequenas empresas (100 a 250 funcionários).

O aumento da receita das organizações é proporcional à maior possibilidade das equipes internas não conseguirem acompanhar o ritmo. Isso reflete a maior complexidade do ambiente interno da segurança cibernética das organizações com altas receitas e a maior propensão a engajarem serviços de segurança especializados. Reflete também um maior entendimento sobre o ambiente da ameaça e os desafios para se defenderem contra ameaças avançadas.

Ataques cibernéticos estão muito avançados para a minha organização lidar com eles por conta própria



Quanto você concorda ou discorda da afirmação: "as ameaças cibernéticas estão muito avançadas para a nossa organização lidar com elas por conta própria"? Concordo totalmente, concordo parcialmente (número de base no gráfico)

O impacto nos negócios

Impacto na operação geral

64%
gostariam que as equipes de TI pudessem dedicar mais tempo a questões estratégicas e menos tempo apagando incêndios

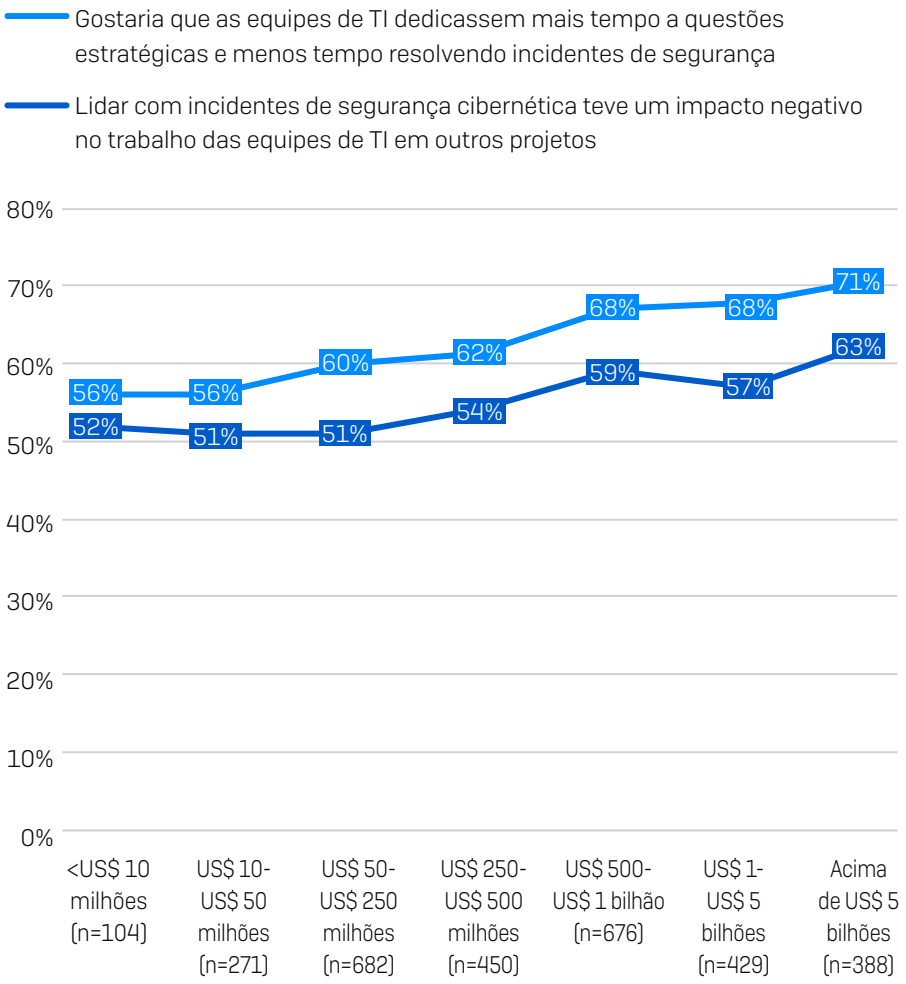
55%
dizem que lidar com ameaças cibernéticas teve um impacto negativo no trabalho das equipes de TI em outros projetos

Para 60% das organizações, a segurança cibernética e as diversificações em suas funções de TI estão estreitamente ligadas: 52% têm uma equipe de segurança cibernética incorporada na equipe de TI, enquanto que, para os outros 8%, são as equipes de TI que gerenciam a segurança cibernética. Os 40% restantes têm equipes de TI e de segurança cibernética separadas. O tempo e o esforços necessários para promover a segurança cibernética resulta em consequências consideráveis para a organização de TI.

Mais da metade (55%) das organizações dizem que lidar com ameaças cibernéticas teve um impacto negativo no trabalho das equipes de TI em outros projetos, com as organizações de maior receita registrando os maiores impactos.

A natureza urgente e imprevisível da segurança cibernética também atrapalha o empenho que se coloca nos negócios: 64%, em média, gostariam que as equipes de TI pudessem dedicar mais tempo a questões estratégicas e menos tempo apagando incêndios. E aqui o fato se repete: conforme a receita aumenta, aumenta também o impacto na capacidade de operação geral.

A segurança cibernética causa um impacto negativo na operação geral de TI



Em que medida você concorda ou discorda de cada afirmação? a) Lidar com incidentes de segurança cibernética teve um impacto negativo no trabalho das equipes de TI em outros projetos; b) Gostaria que as equipes de TI gastassem mais tempo em questões estratégicas e menos tempo resolvendo incidentes de segurança (números de base no gráfico)

Impacto financeiro

O ambiente desafiador da segurança cibernética causa vários impactos financeiros para uma organização. Os grandes custos incorrem nos casos de incidentes cibernéticos de grande impacto. Como destacado no relatório Estado do Ransomware 2022 da Sophos, o custo médio para remediar um ataque de ransomware gira em torno de US$ 1,4 milhão.

Contudo, o impacto financeiro de se lidar com os ataques cibernéticos não se limita ao custos com a limpeza. Com um salário médio anual atualmente na casa dos US$ 100.000,00 nos EUA para um especialista em segurança de TI[2], o custo com recursos humanos por hora para investigar cada alerta de segurança é considerável. Ainda que os salários variem com base nas condições do mercado de trabalho local, o impacto financeiro de um processo de investigação prolongado é considerável.

2 Baseado no salário médio de especialistas em segurança de TI em março de 2023, https://www.indeed.com/career/it-security-specialist/salaries

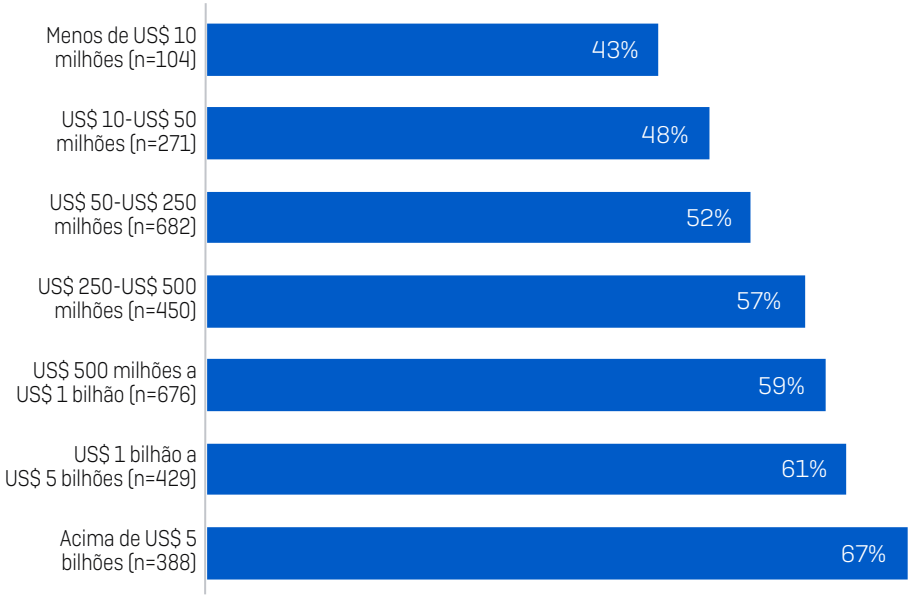
Impacto nas equipes

57% dos entrevistados dizem que a preocupação de que a organização venha a ser atingida por um ataque cibernético por vezes lhes tira o sono. Dado o alto custo de recrutar e reter esse pessoal especializado, isso causa preocupações tanto econômicas quanto sociais, o que sugere também que o pessoal responsável pela defesa não confia em suas ferramentas de segurança.

O desgaste da imagem é um dos grandes problemas na segurança cibernética. Muitos alertas e muitos afazeres colocam um estresse considerável nos funcionários. Uma força de trabalho desgastada está mais propensa a perder sinais importantes, o que aumenta ainda mais a pressão sobre as equipes. No fim, o sistema quebrará, e, com ele, o seu pessoal chegará à exaustão.

A propensão das preocupações com a segurança cibernética interferirem nas noites de sono aumenta no mesmo ritmo que a receita das organizações, chegando a 43% nas organizações com receita anual inferior a US$ 10 milhões e aumentando para 67% nas organizações com rendimentos acima de US$ 5 bilhões.

Porcentagem de entrevistados que dizem que a preocupação de que a organização venha a ser atingida por um ataque cibernético lhes tira o sono



Em que medida você concorda ou discorda da afirmação? A preocupação de que a organização venha a ser atingida por um ataque cibernético por vezes me tira o sono (números de base no gráfico)

Recomendações

Lidar com a situação exige uma abordagem precisa de três estágios: a) implementar um processo escalável de resposta a incidentes que acelere o tempo de resposta, b) utilizar defesas adaptáveis para desacelerar os adversários e c) criar um ciclo virtuoso que melhore a proteção e baixe os custos.

Uma analogia com a campanha "Shields Up" é uma boa maneira de retratar isso. Bloquear adversários avançados e persistentes exige que as organizações otimizem a eficiência de suas defesas (protejam-se), incluindo tecnologias sensíveis ao contexto que elevem o nível de proteção proporcionalmente à situação. É crucial também que usem o tempo destinado a suas defesas para aplicar a expertise humana na análise da causa principal.

Uma proteção forte é essencial

A qualidade de suas tecnologias de segurança cibernética é fundamental, e os controles de segurança devem:

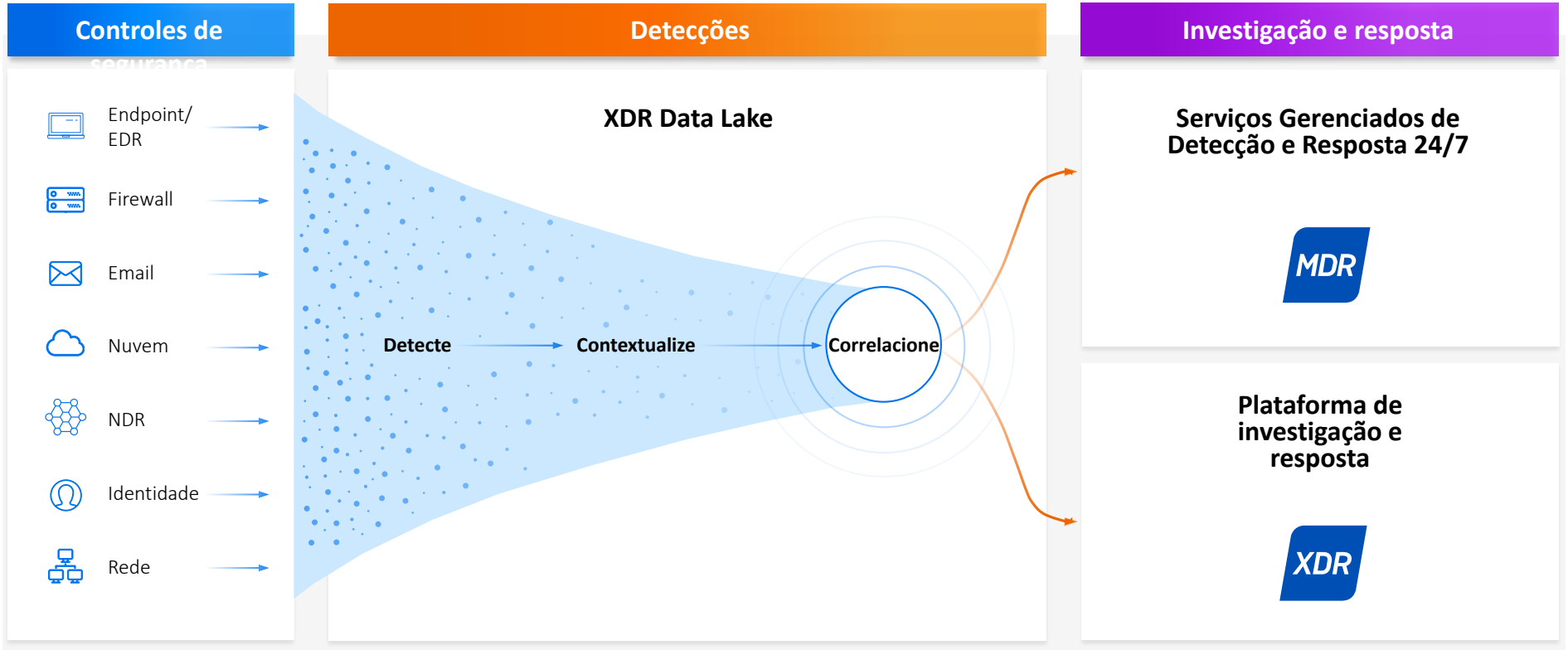
- **Otimizar a prevenção**, detectando e bloqueando automaticamente o máximo possível de ameaças nos estágios iniciais da cadeia de ataque. Dessa forma, você reduz o risco à organização e retira os incidentes do foco de trabalho de sua equipe de defesa.
- **Reduzir a exposição**, garantindo que os investimentos em segurança sejam correta e adequadamente implantados e que os erros de configuração sejam evitados.
- **Interceptar os adversários**, usando tecnologias que detectem e interpelem automaticamente as atividades adversárias para frustrar os ataques e ganhar tempo para que a defesa neutralize o incidente.

Trate da causa primária com pessoas e tecnologia

Uma boa proteção dá à equipe de defesa um tempo valioso para investigar e responder aos ataques. Mas isso não garante 100% de proteção, o que faz da análise rápida, bem-informada e bem executada um fator essencial na prevenção.

Pesquisas mostram que os adversários não seguem um caminho pré-estabelecido. Portanto, utilizar dados de telemetria de diferentes ambientes de segurança usando os controles de segurança que as organizações já têm permite que as equipes de defesa vejam e respondam às ameaças mais rapidamente enquanto aumenta o retorno de investimentos existentes.

Localizar uma atividade maliciosa em meio a alertas benignos é como tentar encontrar uma agulha no palheiro. Processar os sinais por meio de uma plataforma XDR (Extended Detection and Response), que adiciona insights contextuais e os correlaciona a alertas, permite que as equipes internas de defesa foquem rapidamente no que realmente importa. A investigação e resposta podem ser desempenhadas através de uma plataforma XDR pelo próprio pessoal interno. Ou as organizações podem trabalhar com um serviço MDR externo especializado para detecção, investigação e resposta gerenciadas.



Acelere o seu carrossel de defesas

Assim que o carrossel atingi uma velocidade alta, ele mantém o giro. Quanto mais força o giro concentra, mais rápido é o movimento, como em um pêndulo. As organizações podem acelerar o movimento de sua segurança cibernética combinando tecnologias de segurança com perícia humana. Controles abrangentes de segurança diminuem o volume de alertas com que a defesa precisa lidar, permitindo manter o foco em neutralizar os ataques e elevar sua postura de segurança. Por sua vez, isso aumenta a eficiência de seus controles de segurança, criando um ciclo virtuoso.

A maioria das organizações planeja adotar os controles de segurança e serviços necessários

A pesquisa revelou que a maioria das organizações planeja incluir soluções de detecção e resposta em seus modelos de segurança nos próximos 12 meses. Mais de três quartos (78%) planejam adicionar as ferramentas EDR (Endpoint Detection and Response) e/ou XDR (Extended Detection and Response) no próximo ano.

Investigar e responder a ameaças cibernéticas avançadas é uma habilidade especializada, e fornecer cobertura 24 horas diárias exige, no mínimo, de cinco a seis pessoas. Com a falta de especialistas em segurança cibernética nas equipes internas classificada no ranking dos três riscos cibernéticos mais proeminentes de 2023, muitas organizações estão buscando contratar peritos externos para suporte: 44% das organizações planejam começar a trabalhar com provedores de MDR (Managed Detection and Response) dentro dos próximos 12 meses.

Porcentagem de organizações que planejam adotar soluções de detecção e resposta nos próximos 12 meses

78%	44%
EDR/XDR	MDR

A Sophos pode ajudar

A Sophos fornece serviços e tecnologias que capacitam as organizações a acelerar seu carrossel de defesas e se manter à frente dos adversários. Defendemos mais de 550.000 organizações contra ameaças avançadas, e o Sophos MDR é o serviço MDR mais confiável do mundo.

Comece com uma proteção robusta

Nossas soluções de endpoint/EDR, firewall, e-mail, rede e nuvem debilitam os invasores e dão às suas defesas tempo e insights para concretizar suas respostas.

- **Otimize a prevenção:** a Sophos bloqueia 99,98% das ameaças automaticamente, de imediato, minimizando riscos e possibilitando que seu pessoal foque em menos incidentes que exigem a intervenção humana.
- **Reduza a exposição:** as configurações de proteção ideais são implantadas automaticamente, de imediato, eliminando lacunas na segurança. A ferramenta interna de verificação da integridade da conta destaca problemas de configuração e softwares ausentes que poderiam levar a infecções totalmente evitáveis.
- **Intercepte os adversários:** a Proteção Adaptativa de Adversário Ativo aciona imediatamente altas defesas quando uma invasão a um endpoint, executada "via teclado por mãos humanas", é detectada, frustrando a ação dos invasores e dando às equipes de defesa tempo para responder.

Otimize a detecção, investigação e resposta

Quanto mais rápido as defesas vêm, mais rápido podem agir. Na Sophos, trabalhamos com dados de detecção obtidos de diferentes ambientes de segurança, integrando-os à telemetria de controles de segurança da Sophos e de outros fornecedores para acelerar a detecção e resposta e aumentar o retorno de investimentos existentes.

O serviço Sophos MDR reúne mais de 500 peritos em caça a ameaças, investigação e resposta a adversários ativos e outros ataques que trabalham por você 24 horas por dia, sete dias por semana, durante os 365 dias do ano. Com um tempo médio de resposta a ameaças de apenas 38 minutos, o Sophos MDR é imbatível quando comparado à média das equipes internas. Alternativamente, as organizações podem usar a plataforma Sophos XDR, que inclui a funcionalidade EDR completa para investigar e responder a ataques diretamente, ou trabalhar em colaboração com a equipe Sophos MDR.

Onde quer que sua organização se encontre hoje – e onde quer que queira chegar no futuro –, a Sophos pode ajudar a acelerar o seu carrossel de defesas e a se colocar à frente dos adversários mais avançados. Para obter mais informações, acesse www.sophos.com ou fale com um consultor em segurança.

Obtenha resultados excelentes em segurança cibernética com a Sophos

2023-03-29 (WP-NP)

SOPHOS