Enterprise Strategy Group | Getting to the bigger truth.™

Modernização do SOC e a função do XDR

Jon Oltsik, analista sênior principal, membro da ESG
Dave Gruber, analista principal

JUNHO DE 2022

Objetivos da **pesquisa**

As operações de segurança demandam grande escala para coletar, processar, analisar e agir em grandes quantidades de dados. O XDR inicial estava ancorado em duas fontes de dados principais: endpoints e redes. Embora isso tenha sido uma melhoria nas ferramentas desconectadas de EDR e NDR, a detecção e a resposta a ameaças em todas as empresas exigem uma abertura mais ampla, incluindo cargas de trabalho na nuvem, feeds de inteligência de ameaças, aplicações de SaaS e visibilidade de gerenciamento de identidade e acesso. Ao mesmo tempo, para modernizar os centros de operações de segurança e acompanhar o volume de alertas de segurança, as empresas de grande porte precisam de análises avançadas para ajudar a automatizar as tarefas do analista de nível 1, como alertas de triagem, correlacionando alertas com IoCs e preparando incidentes para investigações.

Para obter informações sobre essas tendências, a ESG entrevistou 376 profissionais de TI e segurança cibernética em empresas na América do Norte (EUA e Canadá) pessoalmente responsáveis por avaliar, comprar e utilizar produtos e serviços de segurança de resposta e detecção de ameaças.

O OBJETIVO DESTE ESTUDO FOI:

Analisar as pessoas, os processos e a tecnologia que oferecem suporte à modernização das operações de segurança.

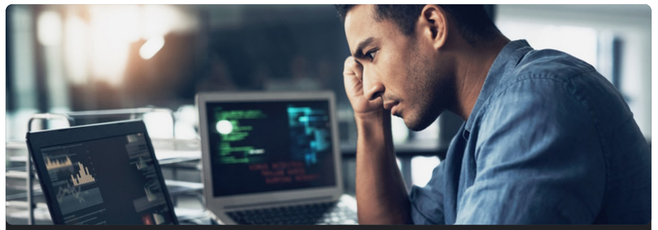
Determinar a percepção e a função atuais do XDR como um componente dos esforços de modernização das operações de segurança.

Identificar os principais pontos de valor, as métricas necessárias para fazer o backup desses pontos de valor e o que é esperado dos produtos e serviços gerenciados para modernização de XDR e SOC.

Explorar as estratégias usadas para automatizar a triagem, acelerar as investigações e ajudar as empresas a encontrar ameaças desconhecidas.

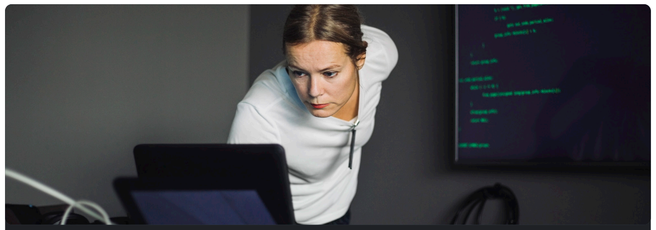
PRINCIPAIS DESCOBERTAS

CLIQUE PARA SEGUIR



As operações de segurança continuam sendo desafiadoras.

O aumento da dificuldade se deve à crescente superfície de ataque, ao cenário de ameaças perigosas e ao aumento do uso da computação em nuvem.



Os profissionais de segurança querem mais dados e melhores regras de detecção.

Apesar da grande quantidade de dados de segurança em uso, deseja-se mais, assim como melhores regras de detecção.

Os investimentos em automação de processos SecOps estão demonstrando serem valiosos.

Embora as estratégias de implementação variem, os investimentos em automação estão valendo a pena para a maioria.

A estrutura MITRE ATT&CK tem demonstrado ser valiosa para a maioria.

No entanto, muitos ainda estão descobrindo como e onde aplicá-la para obter valor.

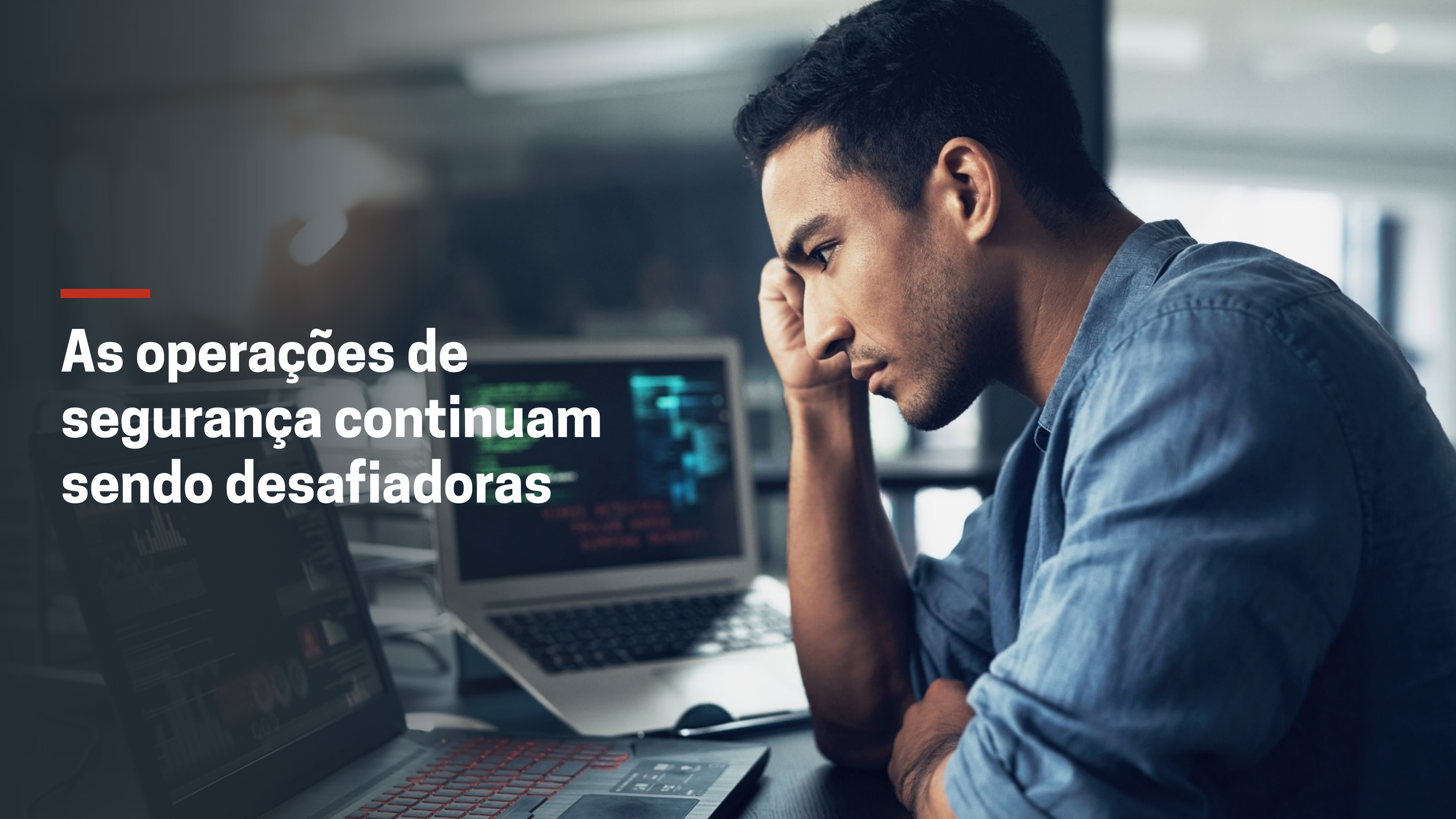
A dinâmica do XDR continua crescendo.

Embora haja confusão sobre o que é XDR, o investimento no suporte à detecção avançada de ameaças é significativo.

O MDR é popular e está em expansão.

Embora os casos de uso variem, os serviços MDR são amplamente adotados em empresas de todos os portes e maturidade.

Voltar ao índice



As operações de segurança continuam sendo desafiadoras

As operações de **segurança** se tornaram mais difíceis na maioria das empresas nos últimos anos. Especificamente, mais da metade (52%) dos respondentes acreditam que se tornou mais difícil gerenciar o ambiente de operações de segurança da empresa nos últimos dois anos. Isso se deve a fatores como o cenário de ameaças cada vez mais perigoso, uma superfície de ataque crescente, o volume e a complexidade dos alertas de segurança e a proliferação da nuvem pública. Como esses desafios só aumentarão no futuro, muitos CISOs percebem que as estratégias de SOC atuais são inadequadas. Para lidar com o crescente volume de ameaças e a expansão de TI, as empresas têm diversas iniciativas focadas na modernização do SOC.

52%

das empresas acreditam que as operações de segurança estão mais difíceis hoje do que há dois anos.

As operações de segurança estão mais difíceis hoje do que há dois anos porque:

O cenário de ameaças está crescendo e mudando rapidamente,

41%

A superfície de ataque cresceu,

40%

A superfície de ataque está mudando e evoluindo constantemente,

39%

O volume e a complexidade dos alertas de segurança aumentaram,

37%

O uso de serviços na nuvem pública aumentou,

34%

> “As empresas têm várias iniciativas **focadas na modernização do SOC.”**

Voltar ao índice

As operações de segurança são afetadas pela falta de habilidades global

Além dos desafios gerais das operações de segurança, é importante observar que 81% das empresas concordam que as operações de segurança foram afetadas pela falta de habilidades global em segurança cibernética. Normalmente, isso gera um aumento na carga de trabalho da equipe atual, bem como o desgaste da equipe. Os profissionais de segurança indicam várias áreas onde a equipe e as habilidades são insuficientes, incluindo arquitetos de segurança, engenheiros de segurança, analistas de nível 3 e analistas de avaliação/priorização de vulnerabilidades.

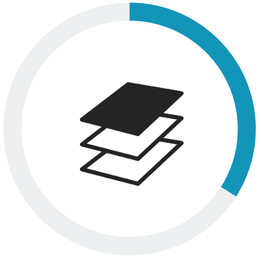
81%

das empresas concordam que suas operações de segurança **foram afetadas pela falta de habilidades em segurança cibernética.**

A maioria das áreas de operações de segurança tem escassez de funcionários.

Arquiteto de segurança,
37%

Engenheiros de segurança,
35%



Analistas de nível 3,*
34%

Analistas de avaliação/ priorização de vulnerabilidades,
33%

** Ou seja, semelhantes aos analistas de nível 2, porém mais experientes e focados em problemas difíceis/graves.*

Voltar ao índice

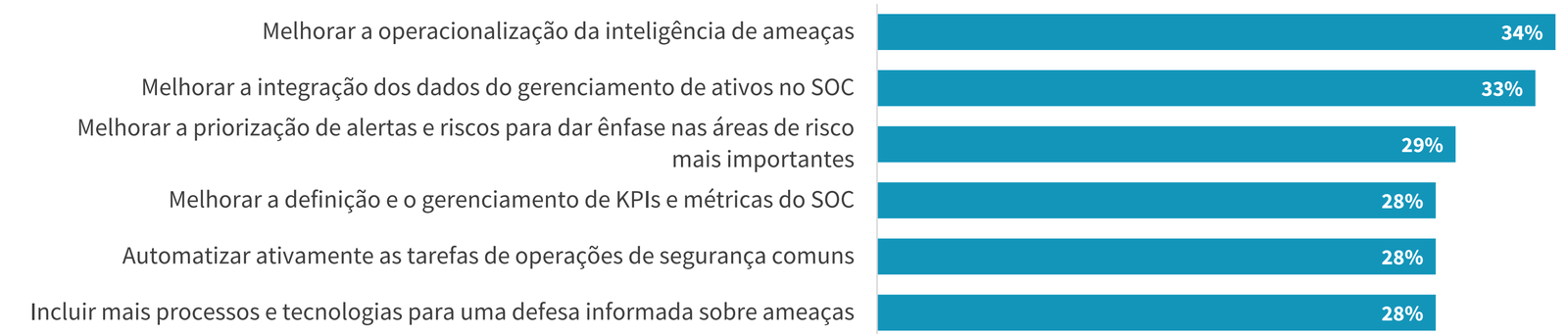
Prioridades de modernização do SOC de curto prazo

Como as empresas planejam lidar com ambientes de operações de segurança cada vez mais difíceis, incluindo níveis insuficientes de equipe? A modernização do SOC é uma iniciativa importante do programa, com 88% das empresas aumentando os gastos com operações de segurança este ano. No curto prazo, as equipes do SOC planejam concentrar seus esforços em áreas como melhoria da operacionalização da inteligência de ameaças, melhoria da integração dos dados de gerenciamento de ativos no SOC, melhoria da priorização de riscos e alertas, melhoria da definição e do gerenciamento de KPIs do SOC e automatização de tarefas comuns de operações de segurança.

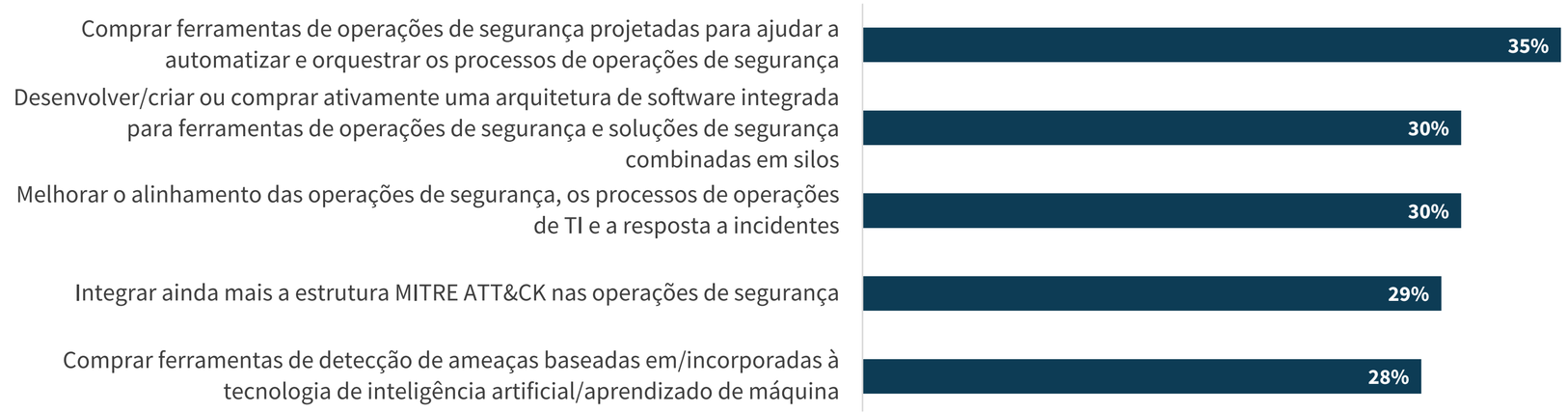
No futuro, as empresas darão muitos passos adicionais para modernização do SOC, como a compra de ferramentas de automação dos processos de segurança, o desenvolvimento/criação de uma arquitetura de plataforma de análise e operações de segurança integrada (SOAPA), a melhoria do alinhamento das operações de segurança e TI, a integração ainda maior da estrutura MITER ATT&CK em operações de segurança e a compra de ferramentas de análise avançadas para detecção de ameaças.

Esses avanços não serão imediatos e podem exigir suporte dos serviços de segurança. No entanto, eles devem ser vistos como paradas ao longo de uma jornada em direção à modernização do SOC. O objetivo é criar um SOC que possa oferecer escalabilidade, desempenho, inteligência, automação e capacidade de gerenciamento para prevenir, detectar e responder a ameaças, gerenciar riscos e oferecer suporte à missão da empresa.

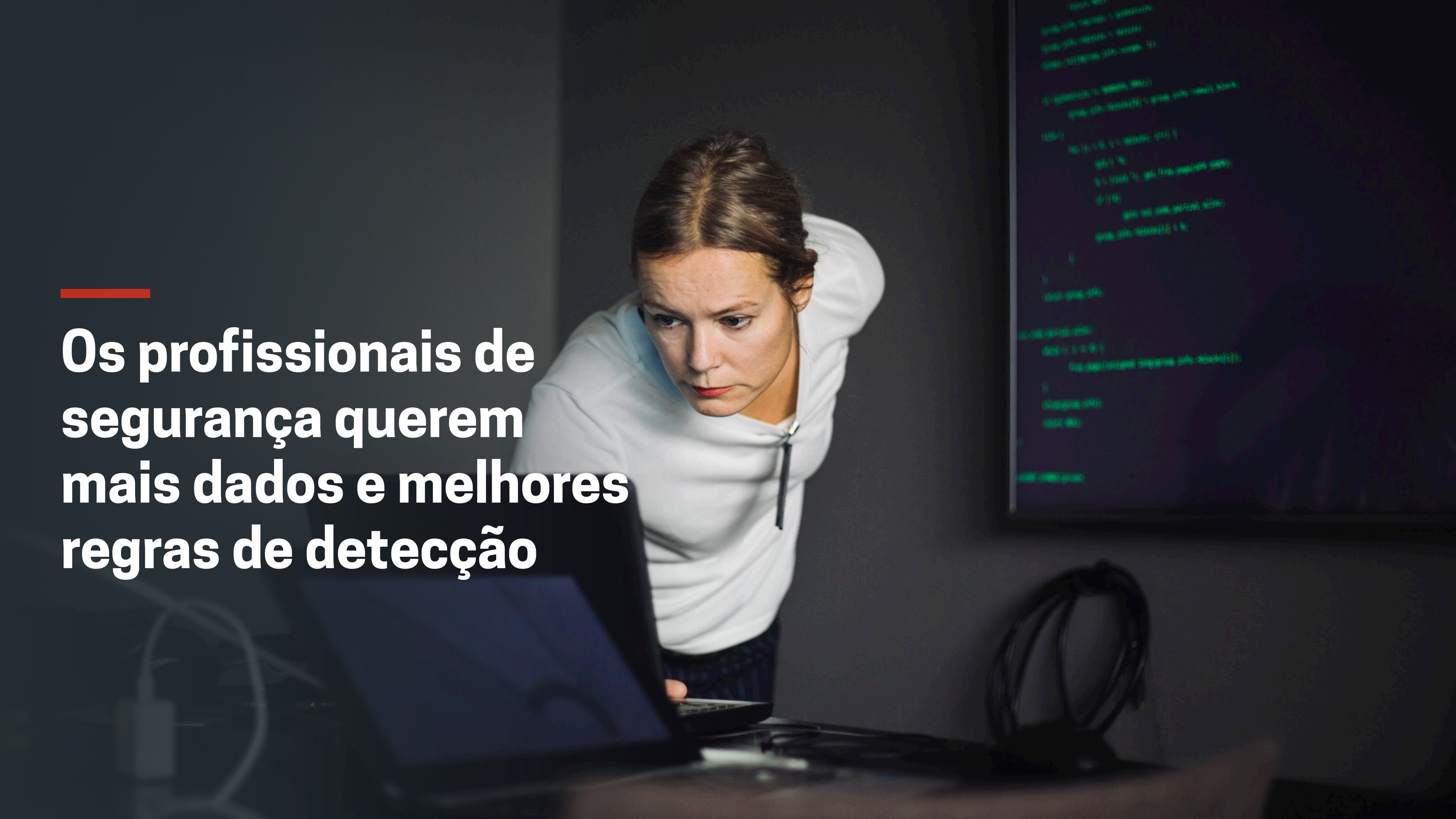
Objetivos esperados com foco no SOC para os próximos 12 meses.



Ações previstas para melhorar as operações de segurança nos próximos 12-18 meses.



Voltar ao índice



Os profissionais de segurança querem mais dados e melhores regras de detecção

Apesar da mudança para XDR, os dados de endpoint ainda são os mais valiosos

Oito em cada dez empresas coletam, processam e analisam dados de operações de segurança de mais de dez fontes de dados. Os profissionais de segurança acreditam que as fontes mais importantes são dados de segurança de endpoint, feeds de inteligência de ameaças, logs de dispositivos de segurança, dados de gerenciamento de postura da nuvem e logs de fluxo de rede. Embora isso pareça ser uma grande quantidade de dados, os respondentes da pesquisa querem usar mais dados para operações de segurança, gerando a necessidade de repositórios de dados de back-end escalonáveis, de alto desempenho e baseados na nuvem.

80%

das empresas usam mais de 10 fontes de dados como parte das operações de segurança.

> “Os respondentes querem usar **mais dados para operações de segurança.**”

Fontes de dados mais importantes para operações de segurança.

24%
Dados de segurança de endpoint

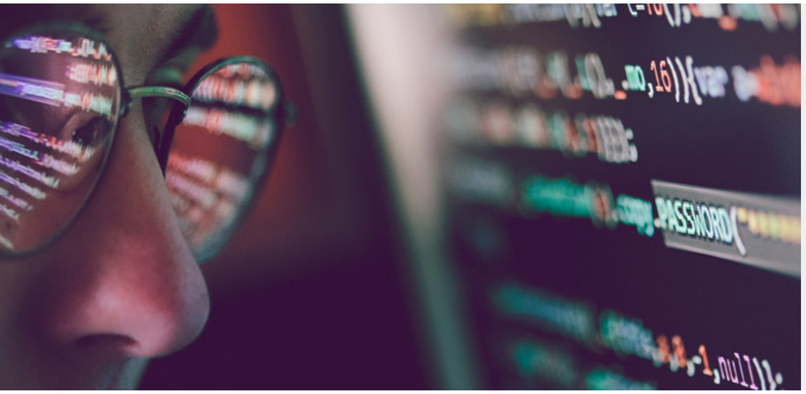
21%
Feeds de inteligência de ameaças

20%
Dados de log em dispositivos de segurança

20%
Sistemas de gerenciamento de postura de segurança na nuvem

18%
Dados NetFlow e/ou IPFIX e/ou logs de fluxo VPC

Voltar ao índice

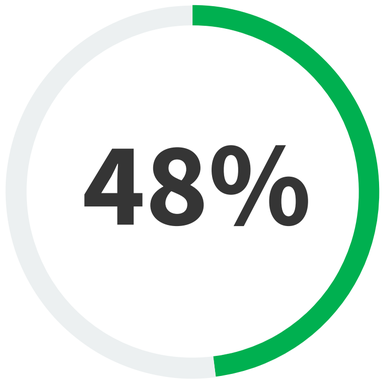


A maioria das empresas desenvolve as próprias regras personalizadas de detecção

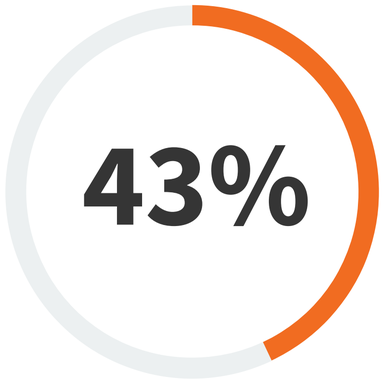
Embora os fornecedores ofereçam volumes cada vez maiores de conteúdo pronto para uso para detecção de ameaças, 91% das empresas complementam esses esforços com sua própria engenharia de detecção. Na verdade, as equipes do SOC coletam, processam e analisam uma variedade de telemetria de segurança para ajudá-las a determinar os pontos fracos da detecção onde as regras personalizadas são necessárias. As equipes de segurança personalizam os conjuntos de regras do fornecedor para atender às suas necessidades e desenvolvem regras personalizadas para detectar ameaças direcionadas ao setor ou à empresa. Para apoiar essa tendência, os fornecedores devem facilitar a cooperação de rede do usuário e, ao mesmo tempo, adotar padrões abertos, como Sigma e YARA, com o suporte estabelecido no setor.

Extensão das regras personalizadas de detecção de ameaças.

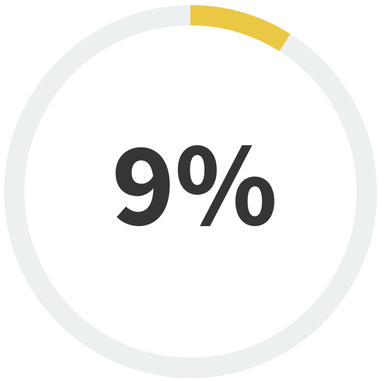
A empresa desenvolve um número significativo de regras personalizadas para complementar as regras de detecção informadas pelos fornecedores



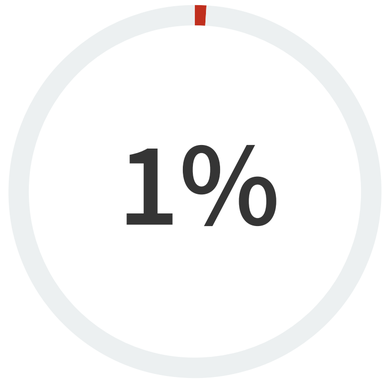
A empresa desenvolve algumas regras personalizadas para complementar as regras de detecção informadas pelos fornecedores



A empresa pode desenvolver um pequeno número de regras personalizadas de detecção, mas depende principalmente daquelas informadas pelos fornecedores



A empresa não desenvolve regras personalizadas de detecção e depende totalmente das regras informadas pelos fornecedores



Voltar ao índice

Os investimentos em automação de processos SecOps estão demonstrando ser valiosos

Muitas empresas perceberam os benefícios da automação do processo de segurança, mas os desafios continuam

A automação do processo de segurança é popular, conforme evidenciado por 90% das empresas que automatizam os processos de operações de segurança, com 46% descrevendo seus esforços de automação como demorados. Aqueles envolvidos na automação do processo de segurança relatam benefícios, como detecção aprimorada de ameaças usando manuais, MTTR e priorização de incidentes, bem como a capacidade de isolar mais rapidamente os ativos infectados. Considerando os desafios das operações de segurança, como a crescente superfície de ataque, as tempestades de alertas e o cenário de ameaças perigosas, a automação do processo de segurança continuará e provavelmente se fundirá com a automação do processo de TI para oferecer eficiência em toda a TI e na segurança.

Embora a automação do processo de segurança continue sendo popular e benéfica, ela traz alguns desafios. Quase duas a cada cinco (39%) empresas afirmam que a equipe de operações de segurança não tem as habilidades de programação adequadas para desenvolver runbooks/fluxos de trabalho nas ferramentas SOAR, enquanto 21% afirmam que os processos de operações de segurança são imaturos e precisam de reengenharia antes de serem automatizados. Nesses casos, as empresas precisam de mais para avaliar os fluxos de trabalho do processo, procurando gargalos antes de passar para a automação. Aqueles com habilidades de programação limitadas devem investigar as opções de SOAR com baixo código/sem código ou usar a funcionalidade de automação de processo integrada em outras ferramentas de operações.

Benefícios mais comumente observados da automação do processo de operações de segurança.

Melhoria na detecção de ameaças usando manuais

51%

Melhoria no tempo médio de resposta

49%

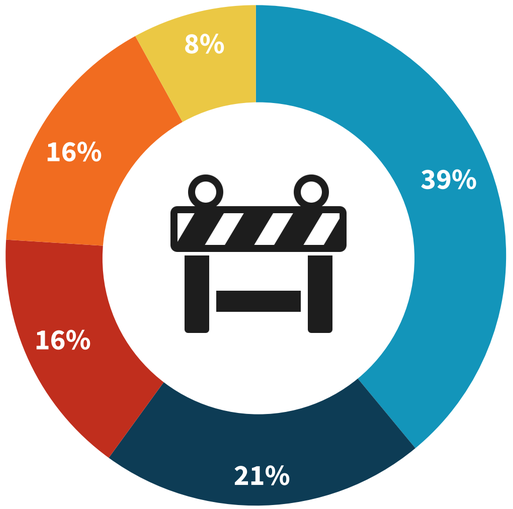
Melhoria na priorização de incidentes

44%

Ativos infectados isolados com mais rapidez

44%

Maiores impedimentos à automação do processo de operações de segurança.



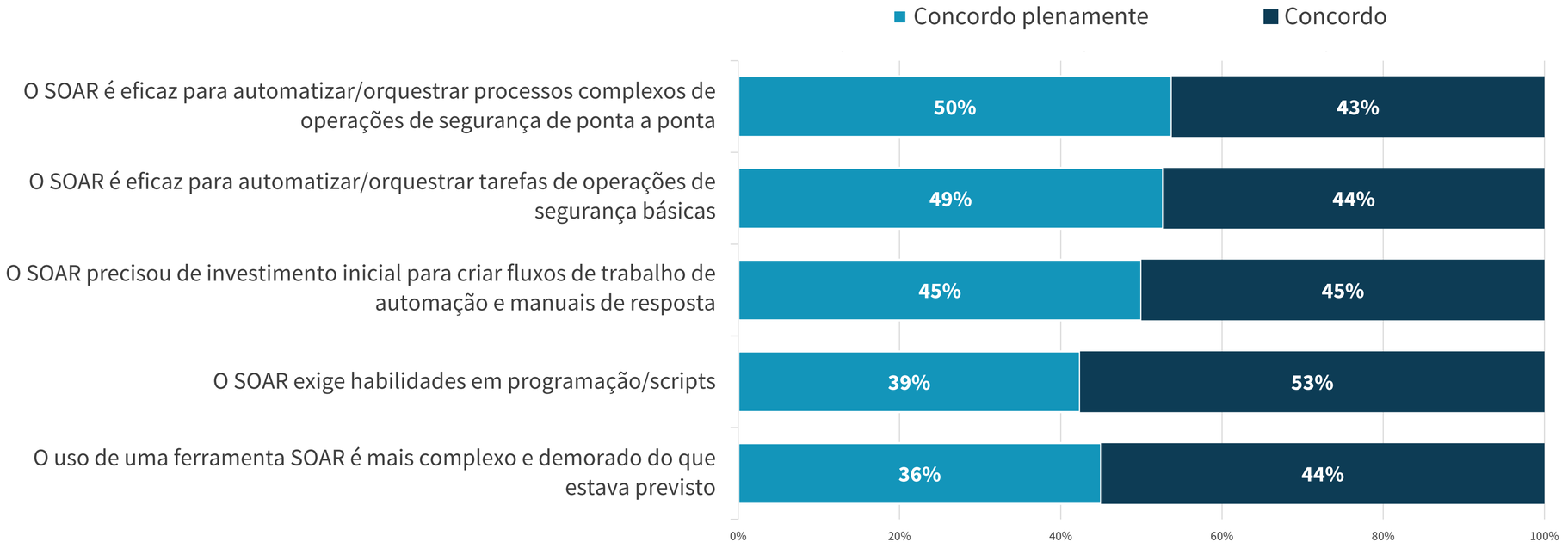
- Habilidades de desenvolvimento de software: a equipe de operações de segurança não possui habilidades de programação para desenvolver runbooks/fluxos de trabalho
- Imaturidade do processo: os processos de operações de segurança são relativamente imaturos. Portanto, seria necessário reformulá-los antes de prosseguir com a automação do processo
- Tempo: a equipe de segurança não tem tempo suficiente para trabalhar na automação do processo
- Ferramentas: a empresa não possui as tecnologias, como o SOAR, necessárias para a automação do processo de segurança
- Sem impedimentos

Voltar ao índice

As ferramentas SOAR podem produzir resultados com os investimentos e as expectativas iniciais corretas

Mais de um quarto (29%) das empresas usa algum tipo de ferramenta de orquestração, automação e resposta de segurança (SOAR) para automação de processos. O uso do SOAR pode ser benéfico: 93% dos profissionais de segurança concordam que o SOAR é eficaz para automatizar processos de operações de segurança complexos e para automatizar/orquestrar tarefas de operações de segurança básicas. No entanto, o SOAR não é simples. O sucesso depende de planejamento inicial, investimentos e das habilidades certas. Por exemplo, 90% dos profissionais de segurança afirmam que o SOAR precisou de investimento inicial para criar fluxos de trabalho de automação e manuais de resposta, 92% concordam que o SOAR exige habilidades de programação/script e 80% concordam que o uso de uma ferramenta SOAR é mais complexo e demorado do que o esperado. Com base nesses dados, as empresas devem reconhecer que o SOAR deve ser considerado um projeto, não uma panaceia. Os benefícios do SOAR só podem ser obtidos com o nível certo de planejamento, treinamento e gerenciamento de projetos.

Opinião sobre as ferramentas de orquestração, automação e resposta de segurança (SOAR).



> “O uso do SOAR pode ser benéfico.”

Voltar ao índice

A estrutura MITER ATT&CK tem demonstrado ser valiosa para a maioria

A maioria das empresas usa e considera a estrutura MITER ATT&CK valiosa para operações de segurança

A popularidade da estrutura MITER ATT&CK cresceu a ponto de quase nove em cada dez empresas a utiliza atualmente. Os gerentes do SOC esperam uma utilização ainda maior do MITER. Na verdade, 97% dos profissionais de segurança acreditam que o MITER ATT&CK (e projetos derivados) será fundamental, muito importante ou importante para a estratégia de operações de segurança da empresa.

Uso da estrutura MITER ATT&CK para operações de segurança.

As empresas usam a estrutura MITER ATT&CK para operações de segurança?

Importância da estrutura MITER ATT&CK para operações de segurança.

97%

dos profissionais de segurança acreditam que o MITER ATT&CK (e projetos derivados) será fundamental, muito importante ou importante para a estratégia de operações de segurança da empresa.

Voltar ao índice

Os casos de uso do MITER ATT&CK crescem

O MITER ATT&CK também se tornou fundamental em vários processos de operações de segurança. Das empresas que adotam a estrutura MITER ATT&CK, 38% a usam para ajudá-las a aplicar a inteligência de ameaças na triagem de alertas ou no processo de investigações, 37% como uma diretriz para engenharia de segurança, 35% para entender melhor as táticas, as técnicas e os procedimentos de criminosos cibernéticos, e 34% para ajudá-las a verificar toda a extensão dos ataques com mais rapidez.

Dessa forma, as empresas estão operacionalizando o MITER ATT&CK na prevenção, detecção e resposta a ameaças.

Formas de utilização da estrutura MITER ATT&CK pelas empresas.

Para ajudar a aplicar melhor a inteligência de ameaças aos processos de triagem de alertas e/ou investigações,

38%

Como uma diretriz para a engenharia de segurança,

37%

Para entender melhor as táticas, as técnicas e os procedimentos dos criminosos cibernéticos,

35%

Para ajudar as empresas a verificar mais rapidamente a extensão total dos ataques,

34%

Para garantir a coleta dos dados corretos das fontes de dados corretas,

33%

> “O MITER ATT&CK também se tornou **fundamental em vários processos de operações de segurança.”**

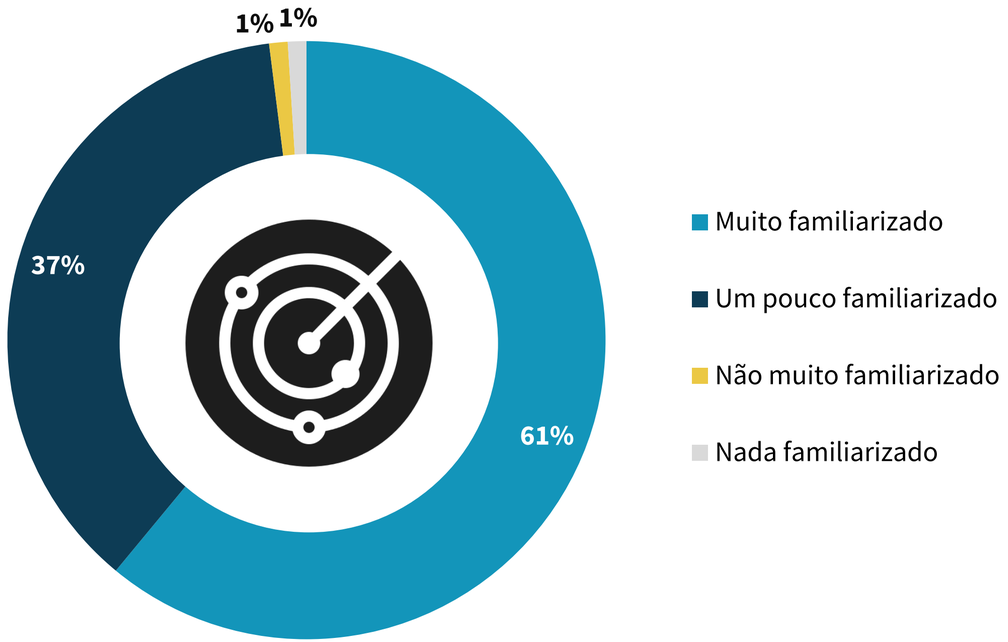
Voltar ao índice

O dinamismo do XDR continua crescendo

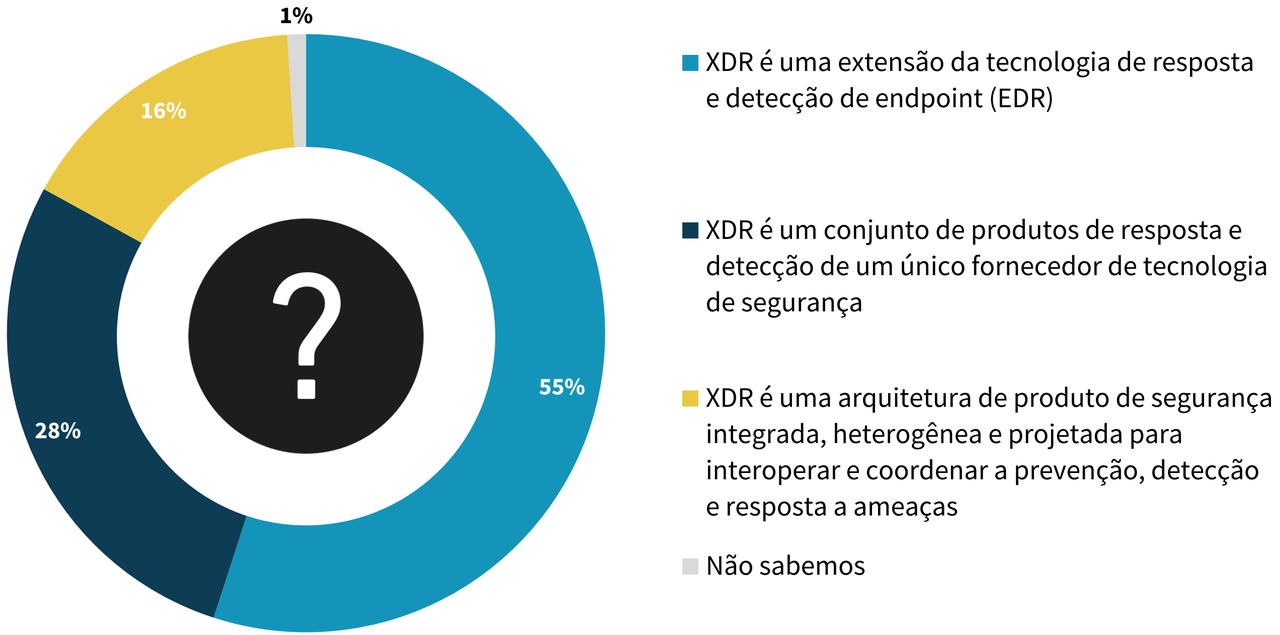
A conscientização do XDR continua crescendo, embora a maioria considere que o XDR suplemente ou consolide as tecnologias SOC

Embora o XDR tenha ganhado mais atenção do setor, ele continua sendo um conceito amorfo com diferentes componentes e definições. Isso se reflete no fato de que 61% dos profissionais de segurança afirmam estar muito familiarizados com a tecnologia XDR. Embora isso represente uma melhoria em comparação à pesquisa da ESG de 2020 (quando apenas 24% dos profissionais de segurança estavam muito familiarizados com o XDR), 39% ainda estão um pouco familiarizados, não estão muito familiarizados ou não estão familiarizados de forma alguma com o XDR. Os usuários também estão confusos sobre o conceito de XDR. Enquanto 55% dos respondentes dizem que o XDR é uma extensão do EDR, 44% acreditam que o XDR é um produto de detecção e resposta de um único fornecedor de tecnologia de segurança ou uma arquitetura de produto de segurança integrada e heterogênea projetada para interoperar e coordenar a prevenção de ameaças, detecção e resposta. É seguro dizer que o XDR continua sendo um trabalho em andamento.

Familiaridade com a tecnologia XDR.



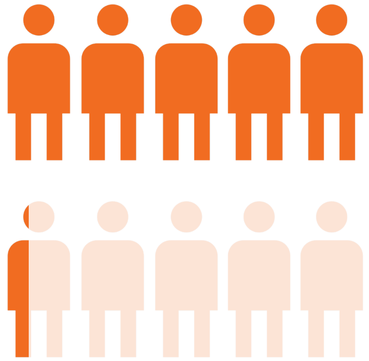
Definições organizacionais da tecnologia XDR.



Voltar ao índice

A maioria considera que o XDR suplemente ou consolide as tecnologias SOC

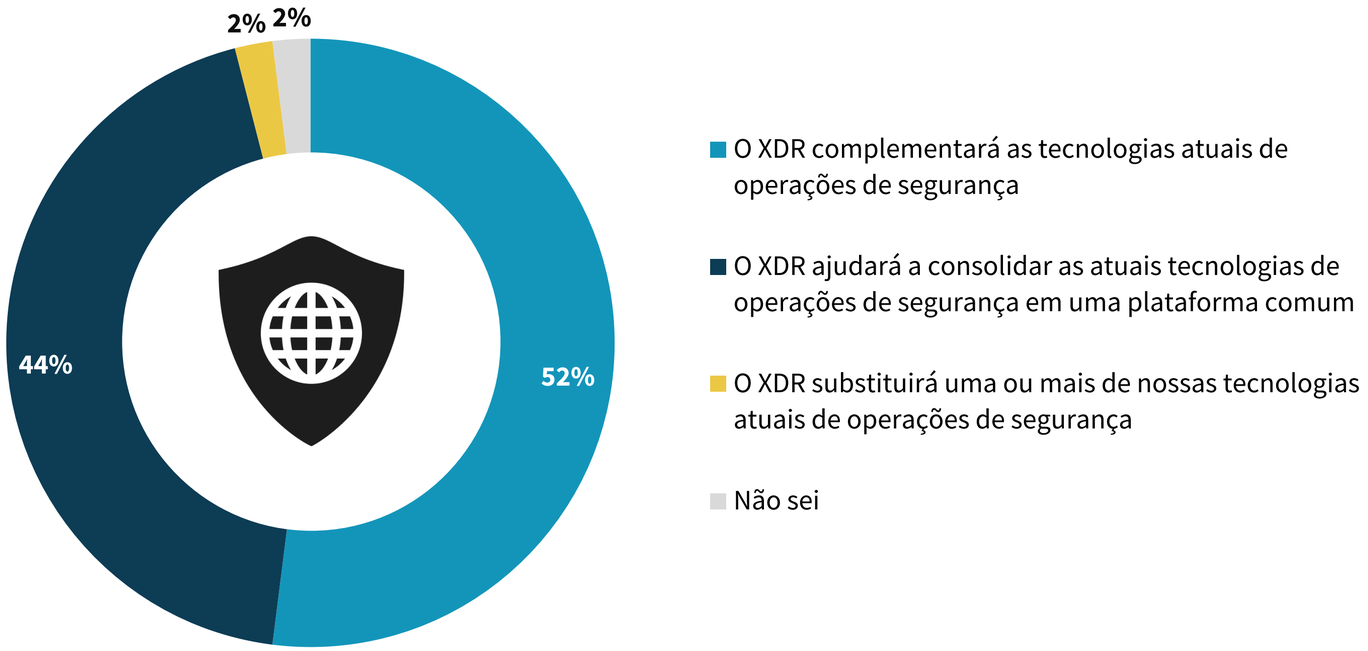
Neste momento, o XDR não é visto como um possível substituto para as tecnologias SOC, como SIEM, SOAR e TIP. Em vez disso, mais da metade (52%) dos profissionais de segurança acreditam que o XDR complementará as tecnologias de operações de segurança atuais, enquanto 44% consideram o XDR como uma consolidação das tecnologias de operações de segurança atuais em uma plataforma comum. Apenas 2% acreditam que o XDR substituirá qualquer tecnologia de operações de segurança atual.



MAIS DA METADE

dos profissionais de segurança acreditam que o **XDR complementará as tecnologias de operações de segurança atuais.**

Impacto esperado do XDR em ambientes de operações de segurança.



Voltar ao índice

Os usuários desejam que o XDR aborde a detecção de ameaças comuns e os desafios de resposta

Independentemente de como o XDR é definido, os profissionais de segurança estão interessados em usar o XDR para ajudá-los a lidar com vários desafios de detecção e resposta a ameaças. O XDR parece uma opção atraente, pois as ferramentas atuais se esforçam para detectar e investigar ameaças avançadas, exigem habilidades especializadas e não são eficazes na correlação de alertas. Em resumo, os CISOs desejam ferramentas de XDR que possam melhorar a eficácia da segurança, especialmente em relação à detecção avançada de ameaças. Além disso, eles querem que o XDR otimize as operações de segurança e aumente a produtividade da equipe.

Os profissionais de segurança parecem ter vários casos de uso de XDR comuns. Por exemplo, 26% dos profissionais de segurança querem que o XDR ajude a priorizar alertas de acordo com o risco, 26% buscam detecção aprimorada de ameaças avançadas, 25% desejam investigações forenses/de ameaças mais eficientes, 25% desejam uma adição em camadas às ferramentas de detecção de ameaças atuais e 25% acham que o XDR pode melhorar a detecção de ameaças para reforçar os controles de segurança e evitar ataques futuros semelhantes. Claramente, os usuários querem que o XDR preencha as lacunas na pilha de segurança e, ao mesmo tempo, melhore a eficácia da detecção e resposta a ameaças.

Cinco desafios mais comuns que geram interesse pelo XDR.

51%
As ferramentas atuais se esforçam para detectar e investigar ameaças avançadas

38%
As ferramentas atuais exigem muitas habilidades especializadas

36%
As ferramentas atuais não são eficazes na correlação de alertas

35%
Lacunas específicas nos recursos de resposta e detecção de nuvem

32%
A abordagem atual das ferramentas é muito cara

Cinco casos de uso de XDR de maior prioridade.

26%
Uma solução XDR que pode ajudar a priorizar alertas de acordo com o risco

26%
Melhoria na detecção de ameaças avançadas

25%
Investigações forenses/de ameaças mais eficientes

25%
Adição em camadas às ferramentas de detecção de ameaças atuais, com o objetivo de identificar ameaças avançadas ou mais complexas

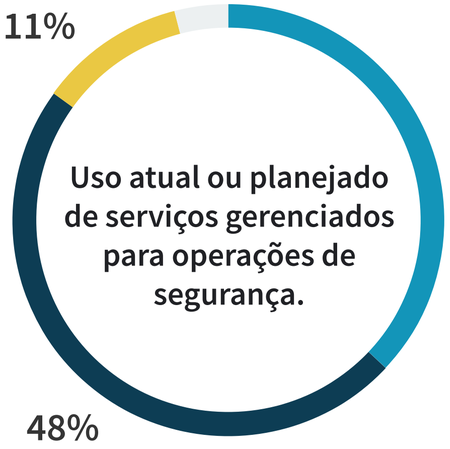
25%
Uso de detecção de ameaças aprimorada para reforçar os controles de segurança e evitar ataques futuros semelhantes

Voltar ao índice

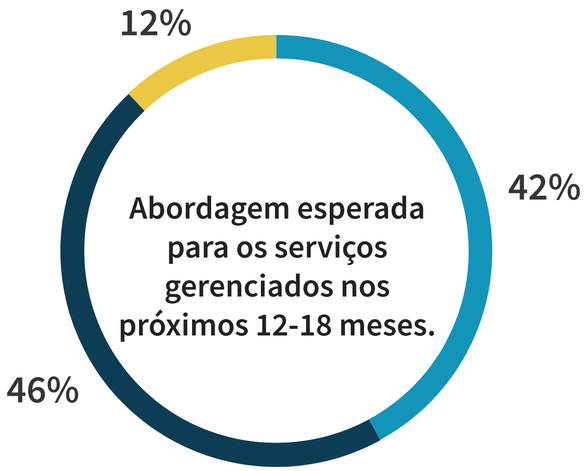
O MDR é popular e está em expansão

O uso de MDR é popular... e está crescendo

Independentemente das definições de tecnologia ou estratégias de implementação, os dados da ESG demonstram uma verdade quase universal: as empresas precisam da ajuda dos provedores de serviços nas operações de segurança. Oitenta e cinco por cento das empresas usam serviços gerenciados para uma parte ou a maioria das operações de segurança atuais. E das empresas que utilizam serviços de segurança gerenciados, 88% aumentarão o uso de serviços gerenciados para operações de segurança no futuro.



- Usamos serviços gerenciados na maioria das operações de segurança
- Usamos serviços gerenciados para uma parte de nossas operações de segurança
- Usamos serviços gerenciados para operações de segurança em uma capacidade limitada



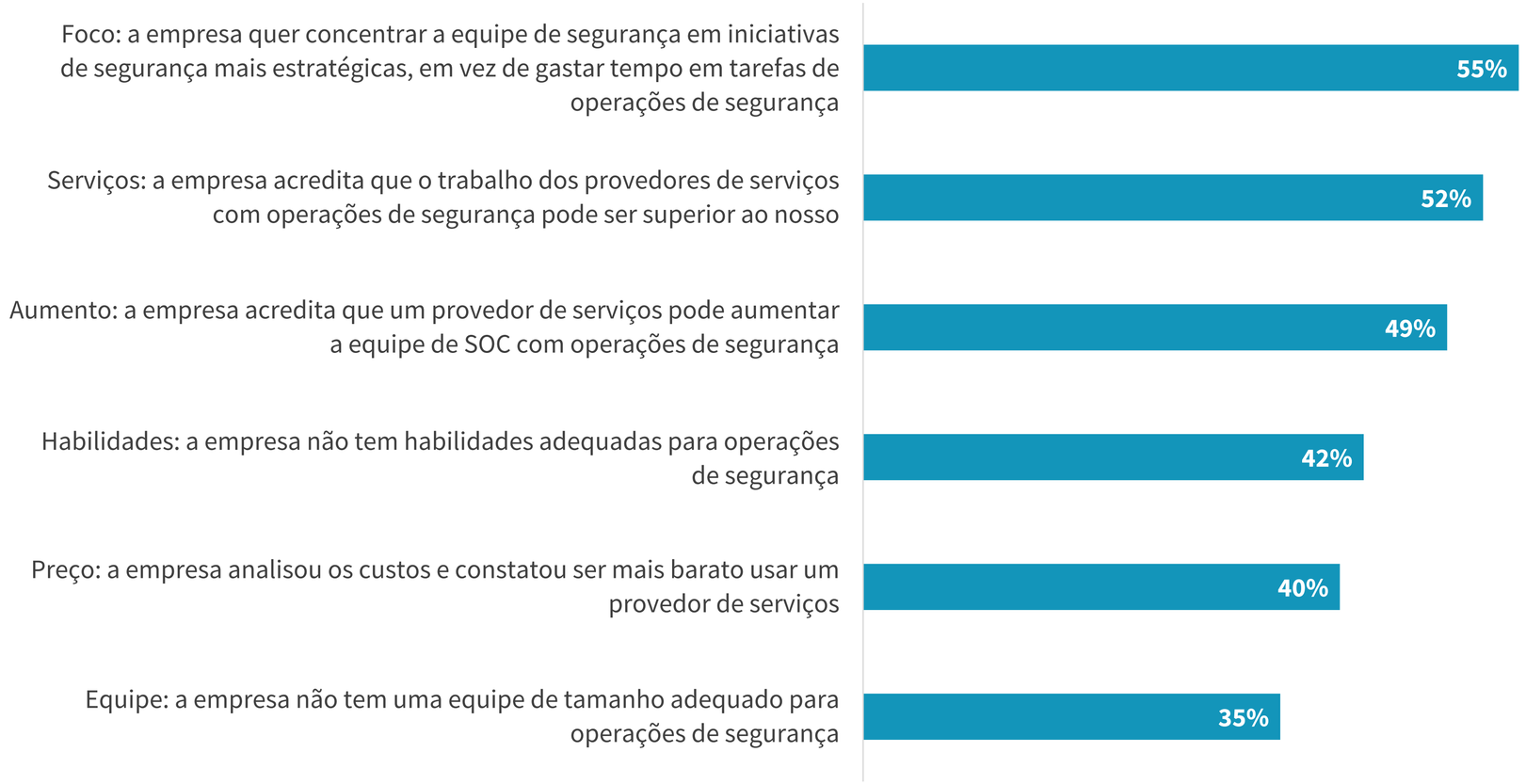
- Aumentaremos significativamente o uso de serviços gerenciados nas operações de segurança
- Aumentaremos um pouco o uso dos serviços gerenciados nas operações de segurança
- Manteremos o uso atual de serviços gerenciados nas operações de segurança

Voltar ao índice

O MDR ajuda as empresas a concentrar os esforços de segurança e a lidar com habilidades e escassez de pessoal

Por que as empresas precisam de serviços gerenciados para operações de segurança? Mais da metade (55%) deseja serviços de segurança para que possam concentrar a equipe de segurança em iniciativas de segurança estratégicas. Outros acreditam que os provedores de serviços gerenciados podem concretizar coisas que a empresa não pode, com 52% acreditando que os provedores de serviços podem fornecer operações de segurança melhores do que a empresa, 49% afirmando que um provedor de serviços gerenciados pode aumentar sua equipe de SOC e 42% admitindo que a empresa não tem habilidades adequadas para operações de segurança.

Principais razões por trás do uso ou planos de serviços gerenciados para operações de segurança.



Voltar ao índice

cisco SECURE

Uma coisa é certa: o XDR terá um papel fundamental na modernização do SOC. A definição de como isso ajudará a equipe de segurança e com quais parceiros trabalhar conforme a abordagem de XDR é desenvolvida determinará o nível de sucesso. Não basta coletar mais dados. Procure uma solução que possa ajudar a transformá-los em dados melhores e práticos com contexto. A automação pode ajudar a preencher as lacunas de habilidades, reduzindo o tempo necessário para detectar, investigar e resolver incidentes para que a responsabilidade possa ser transferida para analistas menos experientes. Isso permite que as empresas realoquem o tempo dos analistas de segurança seniores para amadurecer as operações de segurança. E nunca subestime a importância de um parceiro confiável.

Incluindo a segurança da rede para o endpoint e do e-mail para a nuvem, o portfólio do Cisco Secure conecta detecções a respostas confiáveis com recursos integrados em cada ponto de controle, alcançando o XDR mais amplo do setor. A abordagem XDR da Cisco transforma a infraestrutura de uma série de soluções desconexas em um ecossistema totalmente integrado, evitando que ameaças ignorem as equipes de segurança sobrecarregadas. E como pode ser atestado por mais de 300 mil clientes em todo o mundo, a Cisco oferece uma experiência na qual os CISOs podem confiar. Vamos conversar hoje.

SAIBA MAIS

SOBRE A ESG

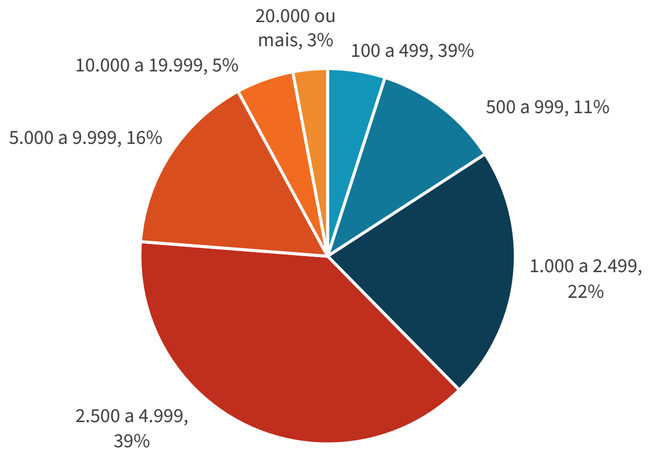
A Enterprise Strategy Group é uma empresa de estratégia, pesquisa e análise de tecnologia integrada que fornece inteligência de mercado, informações práticas e serviços de conteúdo de entrada no mercado para a comunidade de tecnologia global.

Metodologia de pesquisa

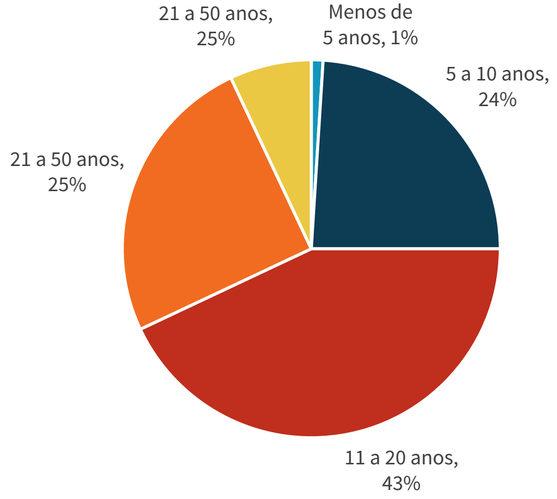
Para coletar dados para este relatório, a ESG realizou uma pesquisa on-line abrangente com profissionais de TI e segurança cibernética de empresas dos setores público e privado na América do Norte entre 4 de abril de 2022 e 15 de abril de 2022. Para se qualificar para esta pesquisa, os respondentes deveriam ser profissionais de TI ou segurança cibernética responsáveis por avaliar, comprar e utilizar produtos e serviços de segurança de resposta e detecção de ameaças. Todos os respondentes receberam um incentivo para concluir a pesquisa na forma de prêmios em dinheiro e/ou equivalentes em dinheiro.

Após filtrar os respondentes não qualificados, remover respostas duplicadas e rastrear as respostas completas restantes (em vários critérios) quanto à integridade de dados, o resultado foi uma amostra total final de 376 profissionais de TI e segurança cibernética.

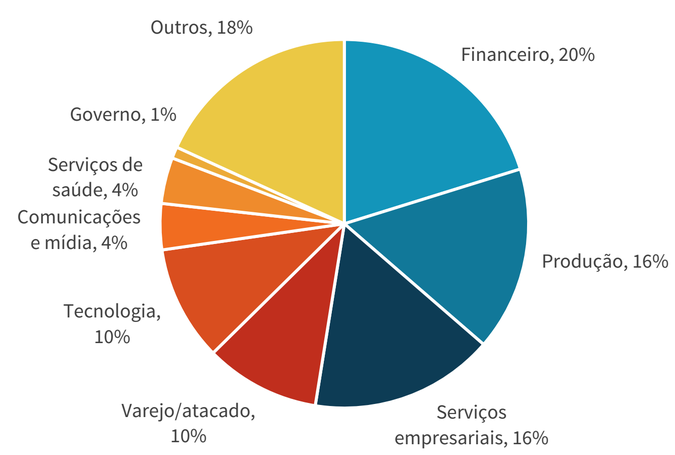
RESPONDENTES POR NÚMERO DE FUNCIONÁRIOS



RESPONDENTES POR TEMPO NA EMPRESA



RESPONDENTES POR SETOR



Voltar ao índice

A **Enterprise Strategy Group** é uma empresa de estratégia, pesquisa e análise de tecnologia integrada que fornece inteligência de mercado, informações práticas e serviços de conteúdo de entrada no mercado para a comunidade de tecnologia global.