Grupo de Estratégia Empresarial | Getting to the bigger truth.™

Modernização do SOC e a importância do XDR

Jon Oltsik, Analista-Chefe Sênior, ESG Fellow
Dave Gruber, Analista-Chefe

JUNHO DE 2022

Objetivos da pesquisa

As operações de segurança exigem grande escala para coletar, processar, analisar e acionar grandes quantidades de dados. O XDR original era ancorado em duas fontes de dados primárias: endpoints e redes. Embora isso tenha representado uma melhoria nas ferramentas EDR e NDR desconectadas, a detecção e resposta de ameaças para as organizações corporativas exige uma abertura mais ampla, incluindo cargas de trabalho na nuvem, feeds de inteligência contra ameaças, aplicativos 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 grandes organizações precisam contar com análises avançadas, para automatizar tarefas de analistas juniores, como triagem de alertas, correlação de alertas com IoCs e preparação de incidentes para investigações.

Para obter insights sobre essas tendências, a ESG entrevistou 376 profissionais de TI e cibersegurança em organizações da América do Norte (EUA e Canadá), encarregados pessoalmente de avaliar, comprar e utilizar produtos e serviços de segurança de risco e detecção de ameaças.

ESTE ESTUDO BUSCOU:

Examinar pessoas, processos e tecnologia que apoiam a modernização das operações de segurança.

Determinar a percepção e o papel atual do XDR como um componente nos esforços de modernização das operações de segurança.

Identificar os principais pontos de valor agregado, as métricas necessárias para sustentar esses pontos de valor e o que é esperado de ambos os produtos e serviços gerenciados para a modernização do XDR e do SOC.

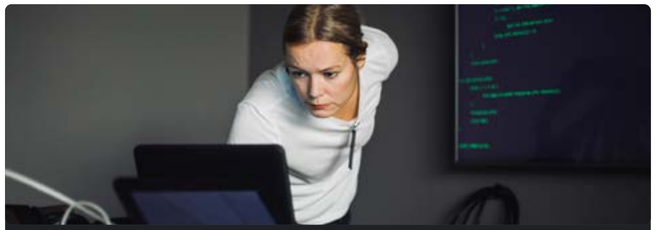
Explorar estratégias usadas para automatizar a triagem, acelerar investigações e ajudar as organizações a detectarem ameaças desconhecidas.

PRINCIPAIS RESULTADOS

CLIQUE PARA SEGUIR

As operações de segurança continuam sendo um desafio.

A dificuldade progressiva se deve à crescente superfície de ataque, ao cenário geral de ameaças perigosas e ao uso crescente de serviços de computação em nuvem.



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

Apesar da enorme quantidade de dados de segurança sendo acionados, a expectativa é contar com ainda mais e o mesmo vale para melhores regras de detecção.

Os investimentos em automação de processos de SecOps estão se mostrando importantes.

Embora as estratégias de implementação variem, os investimentos em automação têm compensado para a maioria dos que apostam na solução.

A estrutura MITRE ATT&CK está se mostrando muito valiosa para muitos no setor.

Mas, muitos ainda estão descobrindo como e onde aplicá-la para conquistar valor agregado.

O impulso do XDR continua a se manter.

Embora haja confusão sobre o que é o XDR, o investimento em suporte à detecção avançada de ameaças é considerado significativo.

O MDR é o padrão e está expandindo.

Embora os casos de uso variem, serviços de MDR são amplamente adotados por organizações de todos os tamanhos e níveis de experiência.

Voltar ao Sumário

As operações de segurança continuam sendo desafiadoras

As operações de segurança tornaram-se mais difíceis na maioria das organizações nos últimos anos. Especificamente, mais da metade (52%) dos entrevistados acredita que o ambiente de operações de segurança de sua organização tornou-se mais difícil de gerenciar nos últimos dois anos. O motivo são fatores como o cenário de ameaças cada vez mais perigoso, uma superfície de ataque em expansão, o volume e a complexidade dos alertas de segurança e a proliferação de nuvens públicas. Como esses desafios só tendem a acelerar no futuro, muitos CISOs percebem que as estratégias atuais do SOC são inadequadas. Para lidar com o aumento no volume de ameaças e escala/expansão de TI, as organizações desenvolvem várias iniciativas focadas na modernização do SOC.

52%

das organizações afirmam que as operações de segurança são mais difíceis hoje do que há dois anos.

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

O cenário de ameaças está em rápida expansão e transformação,

41%

A superfície de ataque se expandiu,

40%

A superfície de ataque está continuamente se transformando e evoluindo,

39%

O volume e a complexidade dos alertas de segurança aumentaram,

37%

Houve um aumento no uso de serviços de nuvem pública,

34%

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

Voltar ao Sumário

Operações de segurança são impactadas pela escassez global de talentos

Além dos desafios gerais das operações de segurança, vale a pena frisar que 81% das organizações concordam que as operações de segurança foram impactadas pela escassez global de talentos de cibersegurança. Normalmente, isso leva ao aumento da carga de trabalho na equipe existente, bem como ao esgotamento mental e físico das equipes. Os profissionais de segurança apontam para várias áreas onde faltam sobretudo pessoal especializado, incluindo arquitetos de segurança, engenheiros de segurança, analistas de nível 3 e analistas de avaliação/priorização de vulnerabilidades.

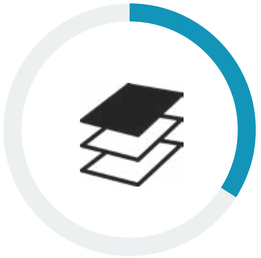
81%

das organizações concordam que suas operações de **segurança foram impactadas pela escassez de habilidades em cibersegurança.**

Áreas com mais deficiência de pessoal.

Arquiteto de segurança,
37%

Engenheiros de segurança,
35%



Analistas nível 3,*
34%

Analistas de avaliação/ priorização de vulnerabilidades,
33%

** semelhante aos analistas nível 2, mas mais experientes e focados em questões difíceis/críticas.*

Voltar ao Sumário

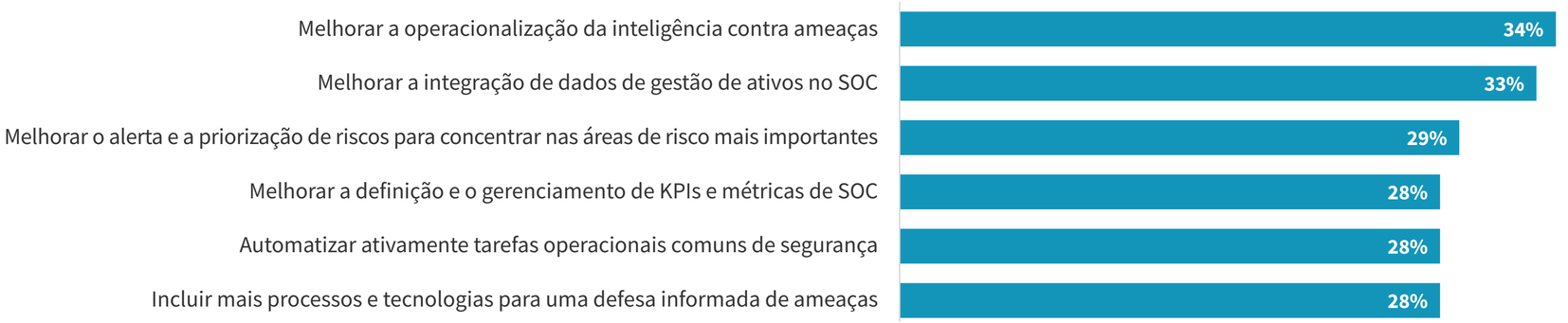
Prioridades de modernização do SOC de curto prazo

Como as organizações planejam lidar com ambientes de segurança operacionais cada vez mais desafiadores, incluindo níveis insuficientes de pessoal? A modernização do SOC é uma iniciativa fundamental do programa, com 88% das organizações incrementando os gastos com operações de segurança este ano. Em curto prazo, as equipes do SOC planejam concentrar seus esforços em áreas como melhorar a operacionalização da inteligência contra ameaças, melhorar a integração de dados de gerenciamento de ativos no SOC, melhorar a priorização de riscos e alertas, melhorar a definição e o gerenciamento de KPIs de SOC e automatizar tarefas comuns de operações de segurança.

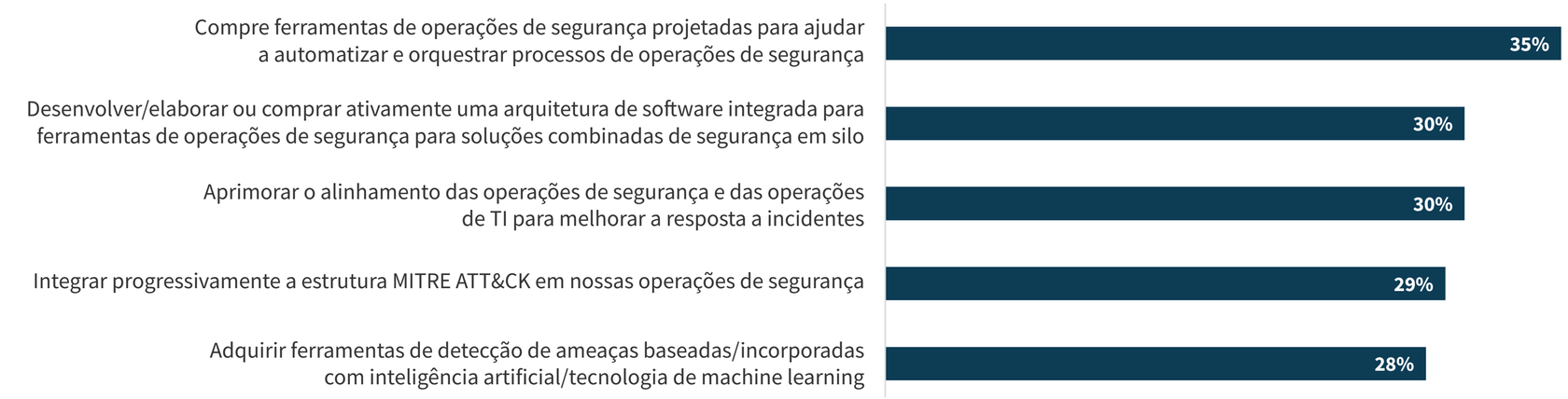
Além disso, as organizações esperam avançar para a modernização do SOC, com a compra de ferramentas de automação de processos de segurança, o desenvolvimento/construção de uma arquitetura integrada de plataformas de segurança e análise (SOAPA), melhorando o alinhamento das operações de segurança e TI, integrando ainda mais a estrutura MITRE ATT&CK em operações de segurança e comprando ferramentas avançadas de análise e detecção de ameaças.

Esses avanços levarão tempo e podem exigir suporte aos serviços de segurança. No entanto, devem ser vistos como incrementos ao longo de uma jornada em direção à modernização do SOC. O objetivo é criar um SOC que possa oferecer a escalabilidade, desempenho, inteligência, automação e capacidade de gerenciamento para prevenir, detectar e responder a ameaças, além de gerenciar riscos e apoiar a missão da organização.

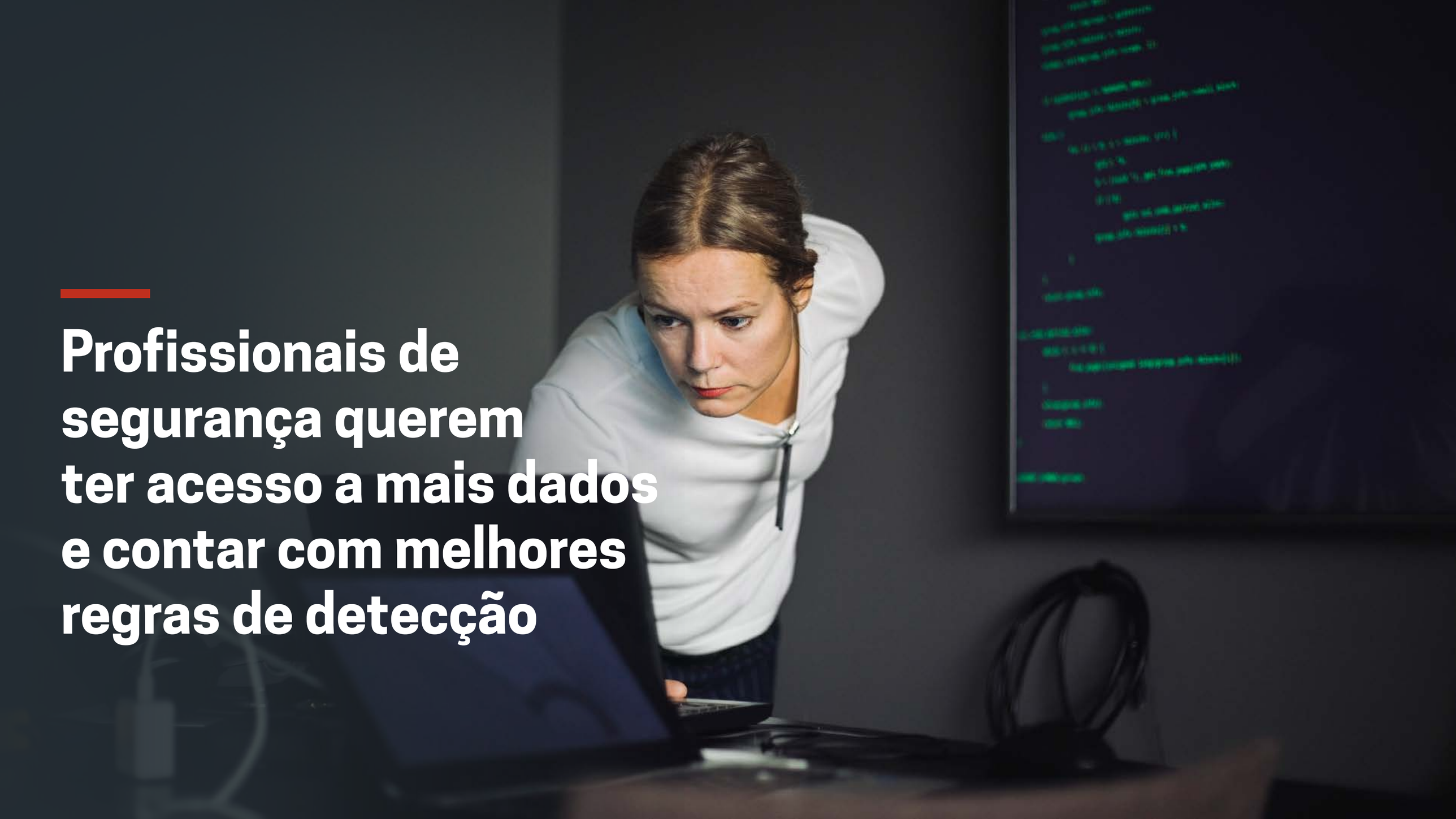
Objetivos esperados focados no SOC nos próximos 12 meses.



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



Voltar ao Sumário



Profissionais de segurança querem ter acesso a mais dados e contar com melhores regras de detecção

Apesar da mudança para o XDR, os dados sobre endpoints ainda são os mais valorizados

Oito em cada dez organizações coletam, processam e analisam dados de operações de segurança de mais de dez fontes. Os profissionais de segurança acreditam que as fontes mais importantes são dados de segurança de endpoints, feeds de inteligência sobre ameaças, logs de dispositivos de segurança, dados de gerenciamento de postura de segurança na nuvem e logs de fluxo de rede. Embora isso pareça um grande volume de dados, os entrevistados realmente querem usar mais dados para operações de segurança, impulsionando a necessidade de repositórios de dados de back-end escaláveis, com alto desempenho e baseados na nuvem.

80%

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

> “Os entrevistados demonstram que realmente querem usar **mais dados para operações de segurança.”**

Fontes de dados mais importantes para operações de segurança.

24%
Dados de segurança de endpoints

21%
Feeds de inteligência contra ameaças

20%
Log de dados de dispositivos de segurança

20%
Sistemas de gerenciamento de postura de segurança na nuvem

18%
Registros de fluxo NetFlow e/ou IPFIX e/ou VPC

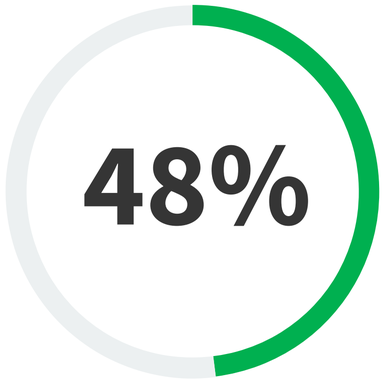
Voltar ao Sumário

A maioria das organizações desenvolvem suas próprias regras de detecção personalizadas

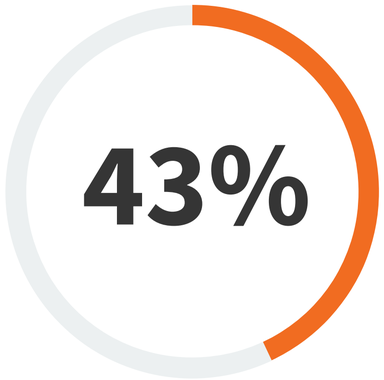
Embora os fornecedores disponibilizem volumes crescentes de conteúdo fora da caixa para detecção de ameaças, 91% das organizações complementam esses esforços com sua própria engenharia de detecção. Na realidade, as equipes do SOC coletam, processam e analisam uma variedade de dados de telemetria de segurança para ajudá-las a determinar as fraquezas de detecção onde as regras personalizadas são necessárias. As equipes de segurança personalizam os conjuntos de regras dos fornecedores para atender às suas necessidades e desenvolvem regras personalizadas para detectar ameaças direcionadas ao seu setor ou organização. Para apoiar essa tendência, os fornecedores devem facilitar a cooperação entre a rede de usuários, ao mesmo tempo em que adotam padrões abertos como Sigma e YARA com suporte estabelecido ao setor.

Extensão das regras personalizadas de detecção de ameaças.

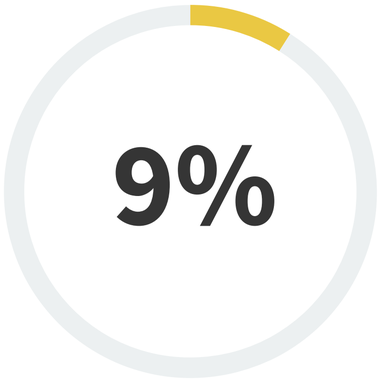
Minha organização desenvolve um número significativo de regras personalizadas para complementar as regras de detecção fornecidas pelos fornecedores



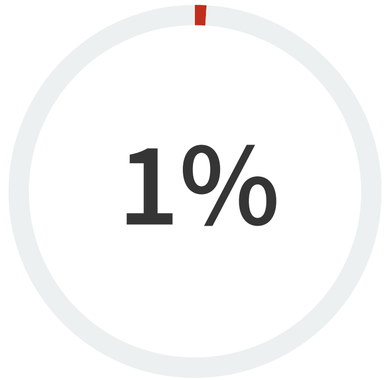
Minha organização desenvolve algumas regras personalizadas para complementar as regras de detecção disponibilizadas pelos fornecedores



Minha organização é capaz de desenvolver um pequeno número de regras de detecção personalizadas, mas depende principalmente daquelas disponibilizadas pelos fornecedores

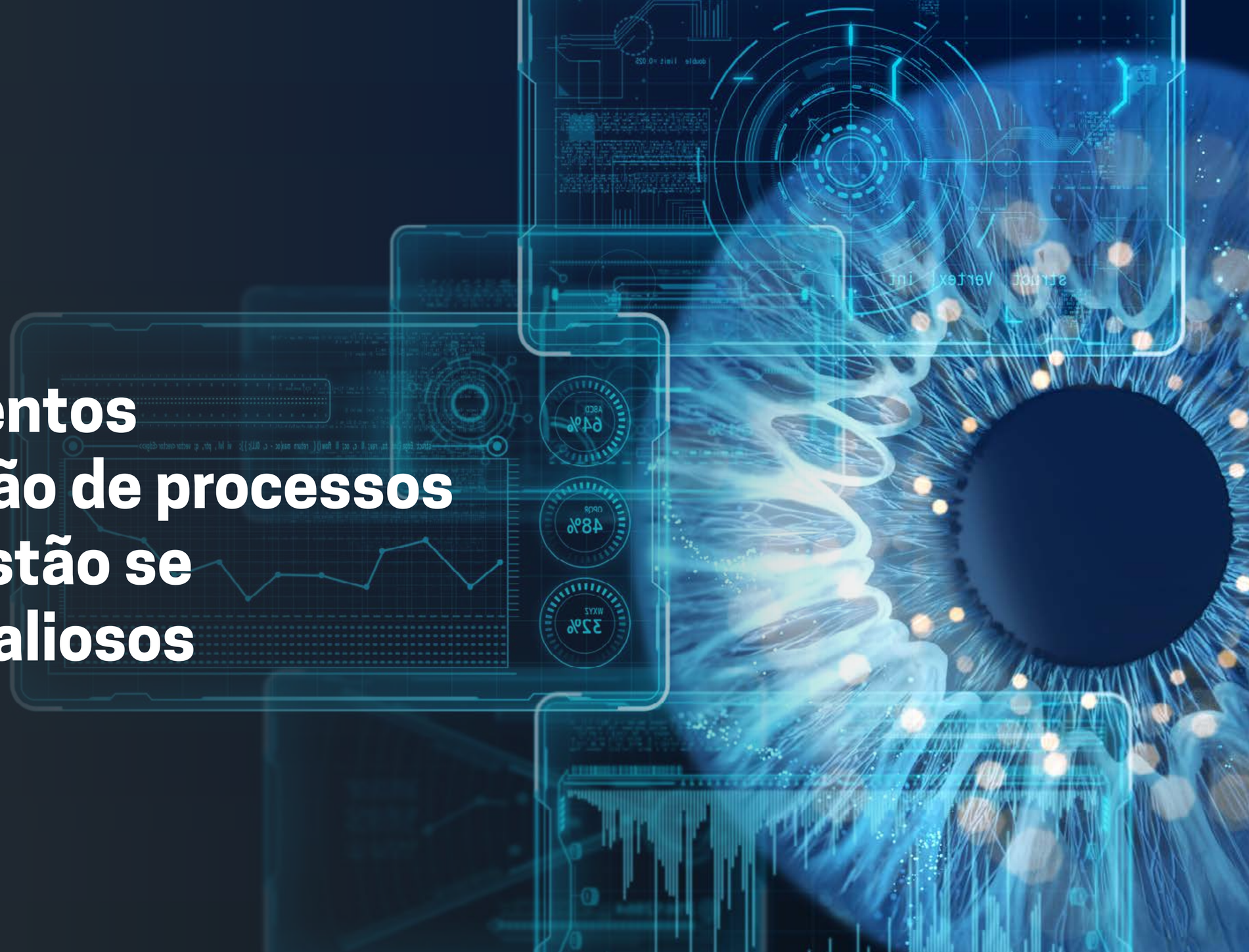


Minha organização não desenvolve nenhuma regra de detecção personalizada e depende completamente daquelas disponibilizadas pelos fornecedores



Voltar ao Sumário

Os investimentos em automação de processos da SecOps estão se mostrando valiosos



Muitas organizações têm conquistado benefícios da automação de processos de segurança, mas os desafios persistem

A automação de processos de segurança é muito buscada, como evidenciado por 90% das organizações que atualmente automatizam processos de operações de segurança, e 46% descrevendo seus esforços de automação como abrangentes. Aqueles envolvidos em automação de processos de segurança relatam benefícios, como a melhor detecção de ameaças usando cartilhas, estrutura MTTR e priorização de incidentes, bem como a capacidade de isolar mais rapidamente os ativos infectados. Devido aos desafios das operações de segurança, como a crescente superfície de ataque, tempestades de alerta e o cenário de ameaças perigosas, a automação de processos de segurança continuará e provavelmente se fundirá com a automação de processos de TI para fornecer eficiências em TI e segurança.

Embora a automação de processos de segurança permaneça muito procurada e vantajosa, envolve alguns desafios. Quase duas em cada cinco (39%) organizações afirmam que sua equipe de operações de segurança não dispõe das habilidades de programação ideais para desenvolver roteiros de execução/fluxos de trabalho em ferramentas SOAR. Outras 21% afirmam que seus processos de operações de segurança são imaturos e precisam de reengenharia antes que possam ser automatizados. Nesses casos, as organizações precisam de apoio extra para avaliar fluxos de trabalho de processos, procurando gargalos antes de passar para a automação. As organizações com limitação de competências de programação devem investigar opções SOAR de pouco código/sem código ou usar a funcionalidade de automação de processos incorporada em outras ferramentas de operações.

Vantagens mais comuns da automação de processos de operações de segurança.

Detecção aprimorada de ameaças com uso de roteiros

51%

Tempo médio de resposta aprimorado

49%

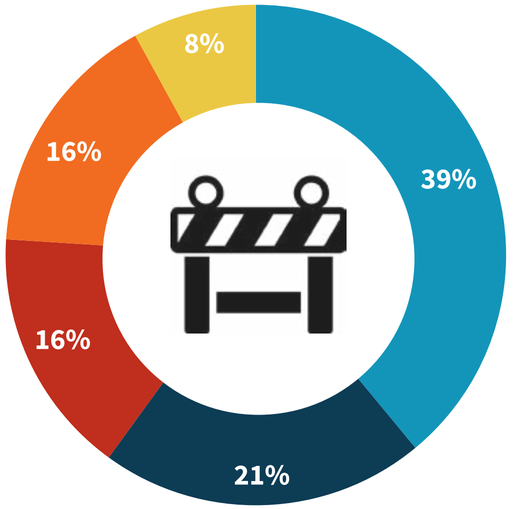
Priorização de incidentes aprimorada

44%

Ativos infectados são isolados mais rapidamente

44%

Maiores obstáculos à automação de processos de operações de segurança.



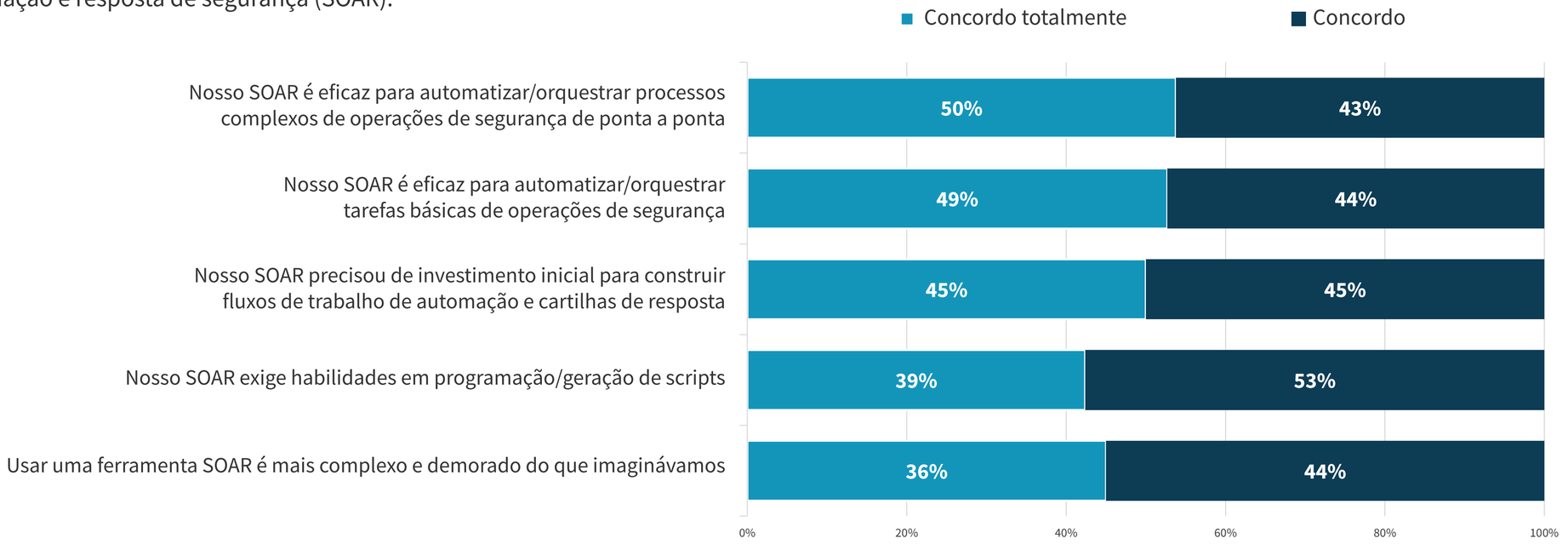
- Habilidades de desenvolvimento de software: Nossa equipe de operações de segurança não dispõe das habilidades de programação para desenvolver roteiros de execução/fluxos de trabalho
- Imaturidade de processos: Nossos processos de operações de segurança são relativamente imaturos, então seria realmente preciso reprojetá-los antes da automação de processos
- Tempo: A equipe de segurança não tem tempo suficiente para se dedicar à automação de processos
- Ferramentas: Nossa organização não dispõe de tecnologias, como o SOAR, necessárias para automação de processos de segurança
- Sem impedimentos

Voltar ao Sumário

Ferramentas SOAR podem produzir resultados com os investimentos e expectativas iniciais

Mais de um quarto (29%) das organizações usam algum tipo de ferramenta de orquestração, automação e resposta de segurança (SOAR) para automação de processos. O uso de SOAR pode ser vantajoso: 93% dos profissionais de segurança concordam que sua solução de SOAR é eficaz para automatizar processos complexos de operações de segurança de ponta a ponta e para automatizar/orquestrar tarefas básicas de operações de segurança. No entanto, o SOAR não dá resultados sem esforços. O sucesso depende de algum planejamento inicial, investimentos e habilidades ideais. Por exemplo, 90% dos profissionais de segurança afirmam que o SOAR precisou de investimento inicial para construir fluxos de trabalho de automação e cartilhas de resposta. 92% concordam que o SOAR exige habilidades de programação/geração de scripts e 80% concordam que o uso de uma ferramenta SOAR é mais complexo e demorado do que o previsto. Com base nestes dados, as organizações devem reconhecer que o SOAR deve ser visto como um projeto, não como uma saída rápida para os problemas. As vantagens do SOAR só podem ser conquistadas com o nível ideal de planejamento, treinamento e gerenciamento de projetos.

Impressão das ferramentas de orquestração, automação e resposta de segurança (SOAR).



“O uso do SOAR pode ser vantajoso.”

Voltar ao Sumário

A estrutura MITRE ATT&CK está se mostrando muito valiosa para muitos no setor

A maioria das organizações usa e reconhece o valor agregado da estrutura MITRE ATT&CK para operações de segurança

A estrutura MITRE ATT&CK cresceu em popularidade a ponto de quase nove em cada dez organizações usá-la de alguma maneira hoje em dia. À medida que os gestores do SOC vislumbram o futuro, prevêem uma utilização ainda maior da MITRE. Em realidade, 97% dos profissionais de segurança acreditam que a MITRE ATT&CK (e projetos de derivados) será indispensável, muito importante ou importante para a estratégia de operações de segurança de sua organização.

Uso da estrutura MITRE ATT&CK nas operações de segurança.

As organizações usam a estrutura MITRE ATT&CK nas operações de segurança?

Importância da estrutura MITRE ATT&CK nas operações de segurança.

97%

dos profissionais de segurança acreditam que a MITRE ATT&CK (e projetos derivados) será indispensável, muito importante ou importante para a estratégia de operações de segurança de sua organização.

Voltar ao Sumário

Explosão de casos de uso do MITRE ATT&CK

A estrutura MITRE ATT&CK também se tornou indispensável para uma variedade de processos de operações de segurança. Dentre as organizações que adotam a estrutura MITRE ATT&CK, 38% usam para apoio na aplicação de dados de inteligência sobre ameaças em seu processo de triagem de alerta ou investigações, 37% usam como diretriz para engenharia de segurança, 35% usam para entender melhor as táticas, técnicas e procedimentos dos cibercriminosos e 34% usam para entender toda a extensão dos ataques mais rapidamente.

Dessa forma, as organizações estão operacionalizando o MITRE ATT&CK por meio da prevenção, detecção e resposta de ameaças.

Maneiras de utilização da estrutura MITRE ATT&CK pelas organizações.

Para aplicar melhor a inteligência de ameaças em nossos processos de triagem de alerta e/ou investigações,

38%

Como diretriz para a engenharia de segurança,

37%

Para entender melhor as táticas, técnicas e procedimentos de cibercriminosos,

35%

Para entender mais rapidamente toda a extensão dos ataques,

34%

Para garantir a coleta de dados certos das fontes certas,

33%

> “A estrutura MITRE ATT&CK também se tornou **indispensável para uma variedade de processos de operações de segurança.”**

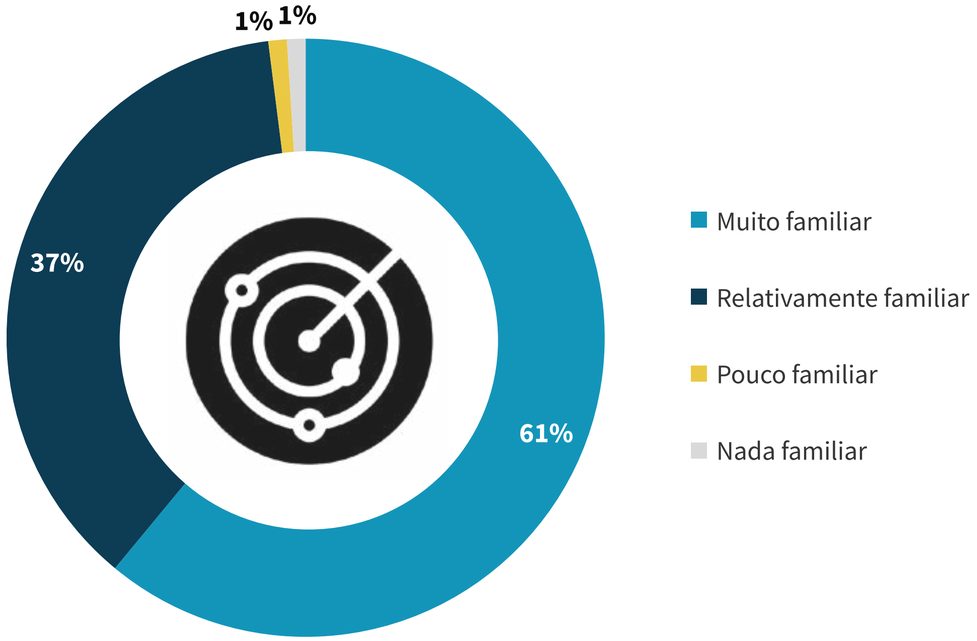
Voltar ao Sumário

O impulso do XDR continua a se manter

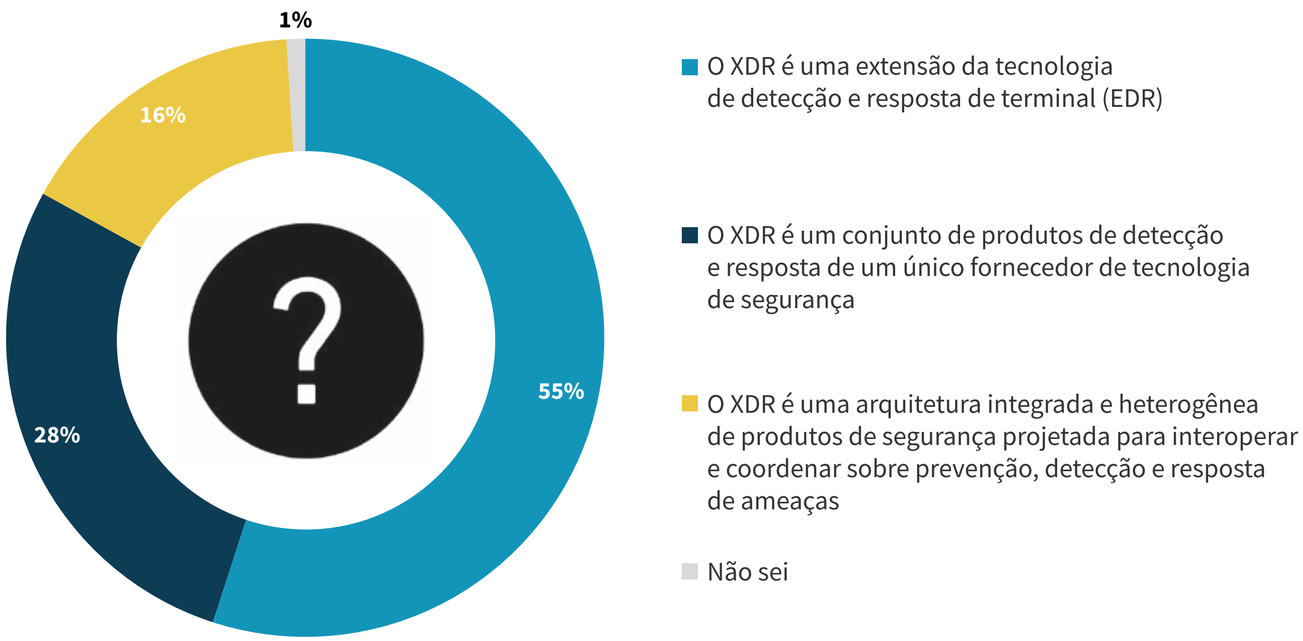
A conscientização sobre o XDR continua a crescer, embora a maioria vislumbre uma complementação ou uma consolidação de tecnologias SOC XDR

Embora o XDR tenha ganhado mais atenção do setor, continua sendo um conceito amorfo com diferentes componentes e definições. Isso se reflete no fato de que 61% dos profissionais de segurança afirmam estarem muito familiarizados com a tecnologia XDR. Embora isso seja uma melhoria da pesquisa de 2020 da ESG (quando apenas 24% dos profissionais de segurança estavam muito familiarizados com o XDR), 39% ainda são apenas relativamente familiarizados, muito pouco familiarizados ou não familiarizados com XDR. Os usuários também não têm clareza sobre o que é XDR. Enquanto 55% dos entrevistados dizem que o XDR é uma extensão do EDR, 44% acreditam que o XDR é um produto de detecção e resposta exclusivo de um fornecedor de tecnologia de segurança ou de uma arquitetura de produto de segurança integrada e heterogênea, projetada para interoperar e coordenar sobre prevenção, detecção e resposta de ameaças. É possível afirmar com segurança que o XDR continua a ser um projeto em andamento.

Familiaridade com a tecnologia XDR.



Definições organizacionais da tecnologia XDR.



Voltar ao Sumário

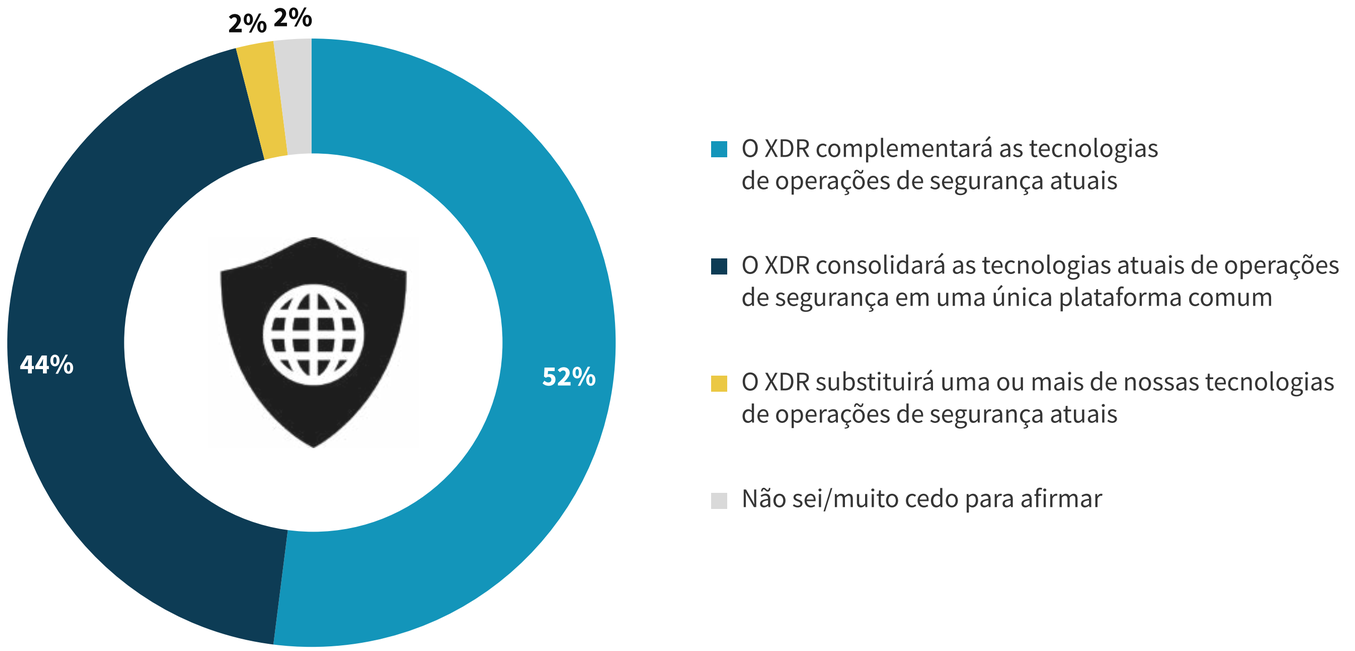
A maioria vê o XDR como complementar ou consolidando tecnologias SOC

Assim, no momento, o XDR não é visto como um potencial substituto das 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 existentes, enquanto 44% acham que o XDR consolida as tecnologias atuais de operações de segurança em uma plataforma comum. Apenas 2% acreditam que o XDR substituirá todas as tecnologias atuais de operações de segurança.

MAIS DA METADE

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

Impacto esperado do XDR nos ambientes de operações de segurança.



Voltar ao Sumário

Os usuários esperam que o XDR resolva desafios comuns de detecção e resposta de ameaças

Independentemente de como o XDR é definido, os profissionais de segurança estão interessados em usar o XDR para ajudá-los a enfrentar vários desafios de detecção e resposta de ameaças. O XDR se mostra como uma opção atraente, já que as ferramentas atuais lutam para detectar e investigar ameaças avançadas, exigem habilidades especializadas e não são eficazes em correlacionar alertas. Em suma, os CISOs querem ferramentas XDR que possam melhorar a eficácia da segurança, especialmente na detecção avançada de ameaças. Além disso, querem que o XDR agilize as operações de segurança e reforce a produtividade da equipe.

Os profissionais de segurança parecem perceber uma série de casos comuns de uso de XDR. Por exemplo, 26% dos profissionais de segurança querem que o XDR ajude a priorizar alertas baseados em riscos, 26% buscam uma melhor detecção de ameaças avançadas, 25% querem investigações mais eficientes de ameaças/análises forenses, 25% desejam incluir camadas às ferramentas de detecção de ameaças existentes e 25% acham que o XDR poderia melhorar a detecção de ameaças para reforçar os controles de segurança e prevenir futuros ataques semelhantes. Claramente, os usuários querem que o XDR supra as deficiências no stack de segurança, melhorando a eficácia e a eficiência da detecção e resposta de ameaças.

Cinco desafios mais comuns que impulsionam o interesse pelo XDR.

51%

As ferramentas atuais têm dificuldade de detectar e investigar ameaças avançadas

38%

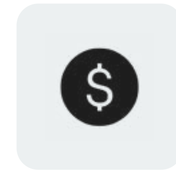
As ferramentas atuais exigem muitas competências especializadas

36%

As ferramentas atuais não são eficazes na correlação de alertas

35%

Deficiências específicas nos recursos de detecção e resposta na nuvem



32%

A abordagem das ferramentas atuais é muito onerosa

Cinco casos de uso prioritário do XDR.

26%

Uma solução XDR capaz de ajudar a priorizar alertas com base no risco

26%

Detecção aprimorada de ameaças avançadas

25%

Investigações de ameaças/ análises forenses mais eficientes

25%

Inclusão de camadas às ferramentas de detecção de ameaças existentes, para identificar ameaças avançadas ou mais complexas

25%

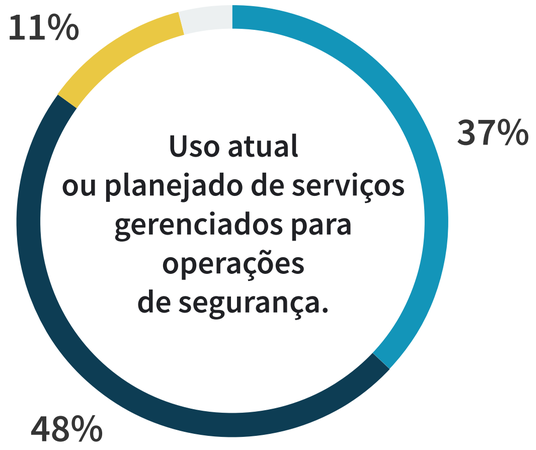
Uso de uma melhor detecção de ameaças para reforçar controles de segurança e prevenir futuros ataques semelhantes

Voltar ao Sumário

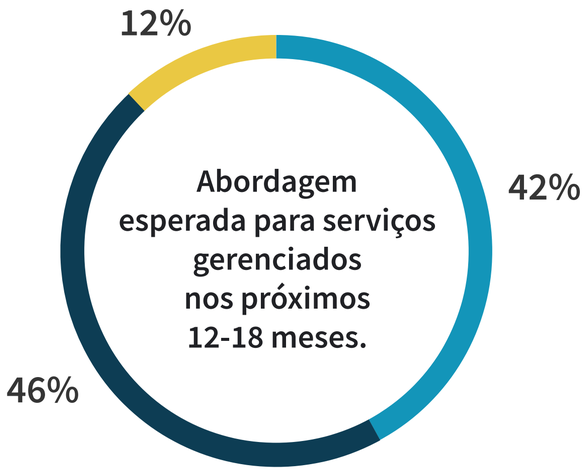
MDR é o padrão e está expandindo

O uso de MDR é padrão... e está expandindo

Independentemente das definições de tecnologia ou estratégias de implementação, os dados da ESG revelam uma verdade quase universal: As organizações precisam da ajuda dos provedores de serviços para as suas operações de segurança. 85% das organizações usam serviços gerenciados para uma parte ou a maioria de suas operações de segurança na atualidade. E dentre os que utilizam serviços de segurança gerenciados, 88% aumentarão o uso de serviços gerenciados para operações de segurança que estão avançando.



- Usamos serviços gerenciados para a maioria de nossas operações de segurança
- Usamos serviços gerenciados em parte de nossas operações de segurança
- Usamos serviços gerenciados nas operações de segurança com uma capacidade limitada



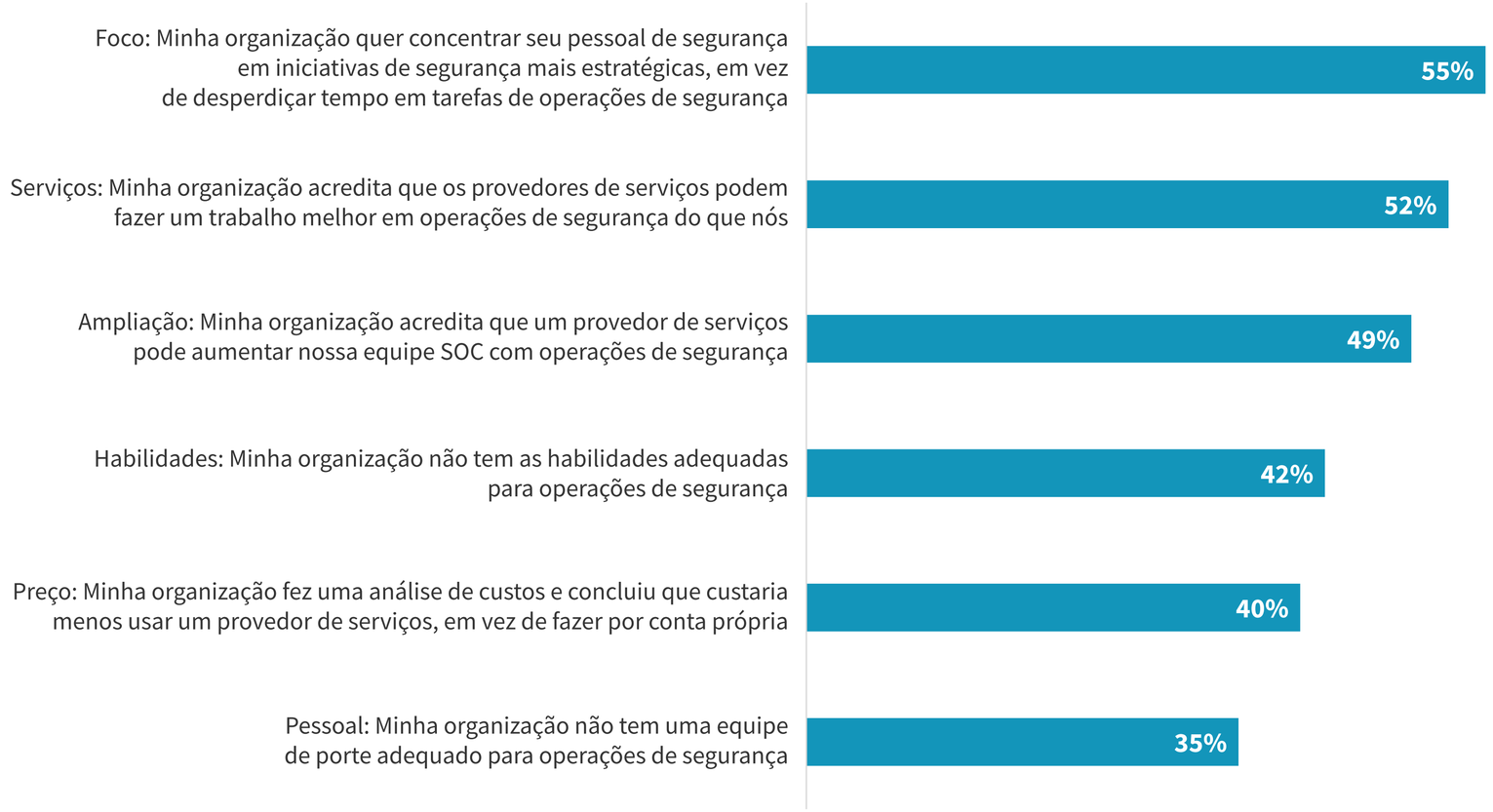
- Aumentaremos significativamente nosso uso de serviços gerenciados para operações de segurança
- Aumentaremos relativamente nosso uso de serviços gerenciados para operações de segurança
- Manteremos nosso uso atual de serviços gerenciados para operações de segurança

Voltar ao Sumário

O MDR ajuda organizações a concentrarem esforços de segurança e lidar com habilidades e escassez de pessoal

Por que as organizações precisam de serviços gerenciados para operações de segurança? Mais da metade (55%) quer contar com serviços de segurança para que possam concentrar o pessoal de segurança em iniciativas estratégicas de segurança. Outros acreditam que os provedores de serviços gerenciados podem executar tarefas que suas organizações simplesmente não podem. 52% acreditam que os provedores de serviços podem fornecer melhores operações de segurança do que sua organização, 49% acham que um provedor de serviços gerenciado pode aumentar sua equipe de SOC e 42% admitem que sua organização não tem habilidades adequadas para operações de segurança.

Principais razões para o uso ou planos de uso de serviços gerenciados para operações de segurança.



Voltar ao Sumário

SOBRE A ESG

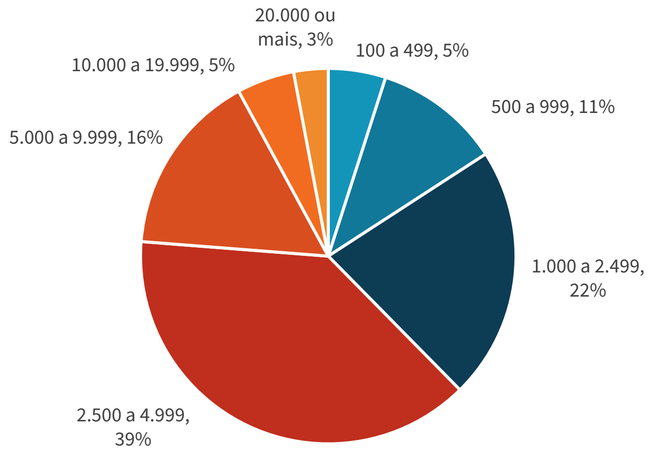
A Enterprise Strategy Group é uma empresa integrada de análise, pesquisa e estratégia de tecnologia que fornece inteligência de mercado, insights acionáveis e serviços de conteúdo de mercado para a comunidade global de tecnologia.

Metodologia da pesquisa

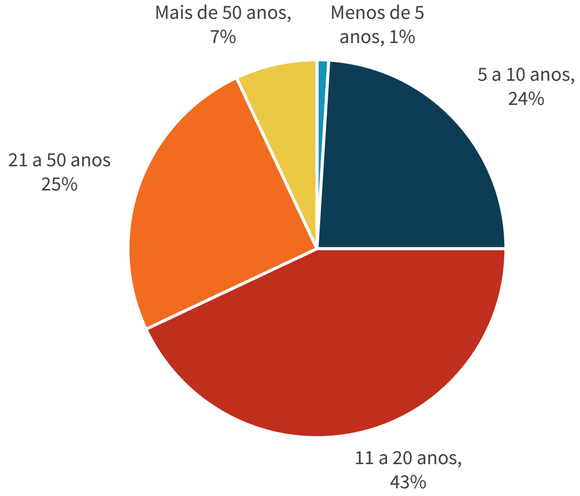
Para coletar dados para este relatório, a ESG realizou uma pesquisa online abrangente com profissionais de TI e de cibersegurança de organizações privadas e do setor público na América do Norte, no período de 4 de abril de 2022 a 15 de abril de 2022. Para se qualificarem para esta pesquisa, os entrevistados atenderam aos critérios de serem profissionais de TI ou de cibersegurança responsáveis por avaliar, comprar e utilizar produtos e serviços de segurança de detecção e resposta de ameaças. Todos os entrevistados receberam um incentivo para responder à pesquisa na forma de prêmios em dinheiro e/ou equivalentes em dinheiro.

Depois de excluir os respondentes não qualificados, remover respostas duplicadas e selecionar as respostas completas restantes (em vários critérios) para a integridade dos dados, ficamos com uma amostra total final de 376 profissionais de TI e cibersegurança.

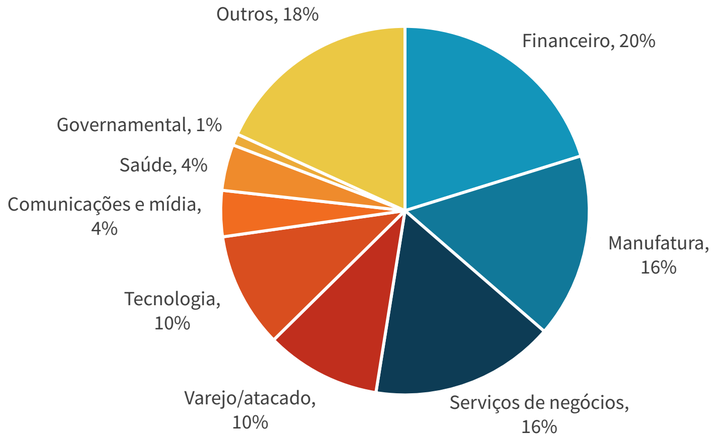
ENTREVISTADOS POR QUANTITATIVO DE PESSOAL



ENTREVISTADOS POR IDADE DA EMPRESA



ENTREVISTADOS POR SETOR



Voltar ao Sumário

A EnterpriseStrategy Group é uma empresa integrada de análise, pesquisa e estratégia de tecnologia que fornece inteligência de mercado, insights acionáveis e serviços de conteúdo de mercado para a comunidade global de tecnologia.