DOCUMENTO TÉCNICO

# Navegando na segurança cibernética com um centro de operações de segurança eficiente

Descubra qual modelo de SOC é o mais indicado para as necessidades da sua organização.

SOPHOS

# Sumário executivo

O cenário da segurança cibernética segue em um estado de constante fluidez, com ameaças cada vez mais sofisticadas e penetrantes. Nesse ambiente, os centros de operações de segurança (SOCs) são essenciais para as organizações detectarem, analisarem e responderem rapidamente a incidentes cibernéticos. As organizações precisam decidir qual modelo de SOC é o mais indicado: interno, híbrido ou terceirizado, e então assegurar o uso das métricas adequadas para medir seu desempenho em segurança continuada e mantê-lo alinhado com seus objetivos de negócios.

### 63% das empresas

tornam-se vítimas de ransomware devido à falta de pessoas ou habilidades.[1]

# O papel do SOC no atual panorama da segurança cibernética

A era digital atrelou a si um aumento em ameaças cibernéticas, com ataques sofisticados lançados por criminosos cibernéticos e agentes patrocinados pelo Estado. As tendências atuais indicam uma redução preocupante no tempo entre a violação inicial e a implantação do ransomware, que hoje revolve em uma média de apenas 2 dias.[2] O setor de segurança cibernética contínua a encontrar um mercado defasado de profissionais para suprir as necessidades, o que complica ainda mais o estabelecimento e manutenção de um SOC interno.

### Escassez de talentos

O setor da segurança cibernética continua enfrentando uma escassez significativa de talentos profissionais.

SOC é uma funcionalidade organizacional dedicada ao gerenciamento de processos para identificar, investigar e remediar incidentes de segurança. Responsabilidades específicas incluem o gerenciamento de ativos, o gerenciamento de mudanças, o gerenciamento de vulnerabilidades, o gerenciamento de eventos de segurança, o gerenciamento de incidentes, bem como a incorporação de inteligência de ameaça e de diversas atividades DevOps, como automação e garantia da qualidade. Ainda que os SOCs não controlem todos os aspectos da segurança de uma organização, eles desempenham um papel crucial na coordenação de suas respostas com as questões de segurança. A missão específica e as metas de um SOC podem variar imensamente, influenciadas por diferentes fatores, como a tolerância de risco da organização, o setor da indústria, o nível de maturidade e as ferramentas e processos empregados.

# Tipos de modelos de SOC

As organizações podem escolher entre modelos variados de SOC, cada qual com o seu próprio conjunto de características e benefícios:

**SOCs internos** são normalmente encontrados em organizações com capital elevado para manter sua operação com uma equipe dedicada. Esses SOCs podem ainda terceirizar certas funções especializadas, como pentest, caça a ameaças ou inteligência de ameaça. Organizações maiores ou geograficamente dispersas podem usar um modelo em camadas com vários SOCs operando sob uma estrutura de comando unificada.

**SOCs híbridos** estão se popularizando, combinando recursos internos com serviços externos para criar uma funcionalidade de segurança personalizada seguindo um modelo de parceria. O provedor de serviços de segurança é, normalmente, responsável pelo monitoramento e triagem de alertas 24/7, investigação de incidentes, caça a ameaças e fornecimento de suporte especializado. Isso permite à equipe interna maximizar seus recursos através de atividades como arquitetura e design de segurança, gerenciamento de políticas e conformidade, mitigação de riscos, treinamento e conscientização em segurança, e execução de ações de resposta, quando a organização opta por manter a remediação internamente. Isso é particularmente atraente devido à flexibilidade que oferece e a capacidade de lidar com a falta de pessoal competente e restrições orçamentárias.

**Um SOC totalmente terceirizado** é um serviço independente que oferece funcionalidades abrangentes de monitoramento e resposta à segurança cibernética. As organizações que precisam estabelecer uma linha de base de SOC rapidamente sem a expertise interna necessária podem se voltar para esse modelo, colocando a sua confiança em um provedor de detecção e resposta gerenciadas (MDR). A organização pode permitir que o fornecedor externo se integre a suas tecnologias existentes de TI e segurança para obter uma visibilidade mais ampla do ambiente e para coordenar as atividades de resposta a incidentes.

## Você sabia?

88% dos ataques de ransomware são lançados fora do horário comercial.[2]

# Qual é o modelo certo para você?

Determinar o modelo certo de SOC para a sua organização depende de múltiplos fatores, incluindo o seu perfil geral de risco. Você deve ponderar o nível de risco aceitável da organização versus o orçamento direcionado à segurança cibernética. São várias as considerações que entram nessa equação:

1. Constrições de recursos internos (a disponibilidade de expertise ou pessoas e habilidades)
2. O equilíbrio entre o que precisa ser mantido internamente e o que pode ser terceirizado
3. A atual maturidade das suas operações de segurança
4. O desafio de contratar, treinar e manter profissionais especializados com habilidades específicas
5. A necessidade de um envolvimento contínuo com tecnologias emergentes e de se manter à frente no cenário evolutivo das ameaças e técnicas de adversários ativos
6. Dependências interdepartamentais: TI, jurídico, conformidade e outros departamento comerciais

Qualquer que seja o modelo que você busque, é importante desenvolver um estudo de caso para justificar o modelo e os recursos exigidos para proporcionar sustentabilidade de longo prazo. Avaliações regulares do potencial do seu SOC são cruciais para garantir o seu alinhamento com o design pretendido e as metas operacionais.

A maioria das organizações enfrenta a escassez de profissionais, e muitos orçamentos simplesmente impossibilitam montar e manter um SOC interno operando 24 horas por dia. CISOs experientes também entendem o valor de manter o controle estratégico das operações de segurança cibernética, e, por extensão, a sustentabilidade de longo prazo da organização, acompanhando e mantendo o controle.

# Benefícios de um modelo híbrido de SOC

O modelo do SOC híbrido oferece uma combinação atraente de benefícios gerados pelas abordagens de trabalho interno e terceirizado. Isso permite que as organizações utilizem a expertise e a eficiência de um provedor terceirizado e mantenham um nível de personalização e controle de suas operações de segurança.

Um dos principais benefícios de um SOC híbrido é o acesso e a escala que ele oferece a peritos em segurança mais experientes e inteligência de ameaça validada. Esses profissionais são parte de um grande grupo de talentos que é exposto continuamente a uma extensa gama de ameaças, permitindo que se mantenham a par dos últimos desenvolvimentos no campo de segurança cibernética. Essa exposição é algo a que uma equipe interna autônoma dificilmente conseguiria equiparar-se, dada a rápida evolução do panorama de ameaças.

Além disso, a parceria com um provedor terceirizado assegura uma cobertura contínua — 24 horas por dia, sete dias por semana, 365 dias por ano —, incluindo noites, fins de semana e feriados, quando as equipes internas muito provavelmente estarão offline.

Um SOC híbrido pode reduzir significativamente a fatiga de alertas ao ajudar as organizações a ajustarem seus sistemas de detecção, consequentemente reduzindo o tempo médio de resposta (MTTR) a incidentes. As organizações também podem evitar os custos substanciais associados à pesquisa de ameaças dedicada, pois seus parceiros externos farão isso por você, adicionando continuamente novas habilidades de detecção conforme são desenvolvidas.

Outra vantagem é a capacidade de direcionar os recursos internos nas questões básicas de TI, tecnologia e conformidade, enquanto o parceiro de SOC se concentra nos incidentes de segurança. Essa divisão de trabalho permite uma alocação mais eficiente de recursos e expertise, podendo, também, permitir que outros departamentos foquem em suas responsabilidades adicionais relativas à segurança.

O treinamento em segurança cibernética, que pode ser caro e demorado, é reformulado no modelo híbrido. O provedor externo garante que suas equipes estejam atualizadas sobre todos os aspectos da segurança cibernética, desde a análise forense e de malware até a resposta a incidentes e segurança da nuvem. Isso alivia o peso imposto ao pessoal interno de manter a expertise em cada faceta da segurança cibernética, o que permite que foquem em áreas que são mais relevantes aos negócios.

O modelo de SOC híbrido oferece flexibilidade para operar em camadas, de acordo com a abordagem da organização a riscos, e ajustar as metodologias de resposta a tal cenário. Isso pode levar a medidas de segurança mais efetivas e direcionadas. Além do mais, a economia de custos associada a um SOC híbrido faz dele uma opção atraente não apenas para as pequenas e médias empresas, mas também para as grandes organizações que pretendem terceirizar certas funções de segurança.

# Medindo a eficiência do SOC

Qualquer que seja o seu modelo ideal, para medir a eficiência de um SOC é essencial empregar um conjunto de métricas que reflitam o panorama da segurança e a eficácia dos recursos do SOC. As métricas sugeridas abaixo, acrescidas de outras mais, podem ser adicionadas a um painel de controle para mostrar contagens em tempo real, além de estatísticas semanais, mensais e trimestrais, para demonstrar tendências com foco na qualidade da capacidade de resposta e investigação do SOC.

Para o panorama da segurança, as métricas devem oferecer insights do escopo e do volume de ameaças potenciais, os pontos de vulnerabilidade da organização e a exposição geral a riscos. Exemplos incluem o volume de e-mails suspeitos ou maliciosos recebidos, o número de tentativas de varredura e exploração de sistemas externos, e o número de incidentes de segurança por origem.

Quando analisamos a eficácia do SOC, as métricas deveriam demonstrar a performance em comparação a políticas e metas de postura estabelecidas, que estão associadas aos resultados comerciais, como risco reduzido e conformidade regulatória. Isso inclui a qualidade da capacidade de resposta e investigação, o detalhamento do tempo despendido pelo pessoal de segurança em atividades diversas, o número de incidentes por categoria de conformidade e a quantidade de trabalho de engenharia associado à redução da superfície de ataque. As métricas-chave também incluem o tempo de triagem na investigação, o número de investigações em que foram adotadas ações corretivas, o número de ações corretivas baseadas em caça a ameaças proativa e o número de vulnerabilidades com patches definidas por severidade.

Ao monitorar essas métricas com regularidade, as organizações podem garantir que o SOC não opere apenas com eficiência, mas também contribua para a postura de segurança geral e os objetivos comerciais.

## As métricas devem:

- Oferecer uma representação do escopo e do volume de ameaças potenciais
- Encontrar os pontos de vulnerabilidade de uma organização
- Mostrar a exposição geral a riscos
- Rastrear o desempenho comparado a políticas e metas de postura estabelecidas

## Principais métricas:

- Tempo de triagem na investigação
- Número de investigações em que foram adotadas ações corretivas
- Número de ações corretivas baseadas em caça a ameaças proativa
- Número de vulnerabilidades com patches definidas por severidade

# Encontre uma solução de SOC avançada

Cada empresa é diferente, com níveis variados de maturidade de segurança. Com o crescente panorama evolutivo das ameaças, o acesso a um SOC competente é necessário para toda organização que leve a sério a sua segurança cibernética. Independentemente de a organização optar por desenvolver habilidades internas, trabalhar com um provedor externo ou adotar uma abordagem híbrida, o parceiro ideal pode assegurar uma defesa eficiente alinhada às metas de negócios.

Muitas empresas estão tendendo para os modelos de SOC com gerenciamento híbrido ou completo para resolver a escassez de talentos, as restrições orçamentárias e a complexidade crescente das ameaças cibernéticas. Esses modelos oferecem flexibilidade, expertise e cobertura 24/7, capacitando as equipes internas a manter o foco em iniciativas estratégicas enquanto parceiros de confiança cuidam das operações de segurança progressivamente.

Sophos MDR exemplifica a potencial dessa abordagem. Com ofertas em camadas projetadas para atender às organizações em qualquer ponto de sua jornada na segurança cibernética, a Sophos fornece as funcionalidades avançadas de detecção, investigação e resposta personalizadas para as necessidades dos seus negócios. Como respaldo à sua equipe de SOC ou operando como um parceiro terceirizado completo, o Sophos MDR aprimora a visibilidade e resposta, ajudando as organizações a fortalecer suas defesas e proteger o que importa.

[1] Sophos, Relatório O Estado do Ransomware 2025
[2] Sophos, Relatório de Adversários Ativos 2025

SOPHOS

# Saiba mais sobre nossos serviços de detecção e resposta gerenciadas em sophos.com/mdr.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com