

SecOps agêntico

Um novo modelo operacional de SOC

Evite e impeça as ameaças. Amplie a defesa com agentes de IA.
Gerencie a segurança como um sistema.

Os centros de operações de segurança (SOCs) de hoje estão presos entre a grande quantidade de ameaças impulsionadas por IA e o atrito persistente de suas próprias ferramentas fragmentadas e processos manuais. O resultado é um revés oculto sobre seu recurso mais valioso — a equipe orientada a missões que mantém tudo funcionando.

Uma pesquisa recente da Microsoft revelou a dura realidade dessa lacuna operacional. É algo quase generalizado, com **91% dos líderes de segurança**¹ confirmando que essas lacunas resultaram diretamente em um incidente grave que afetou os negócios. Seus analistas passam um dia inteiro por semana (mais de **20% do seu tempo**²) agregando dados manualmente. Sobrecarregadas com trabalho manual, as equipes deixam **42% dos alertas de segurança**³ sem investigação. Cada alerta ignorado é um possível ponto de entrada, permitindo que um atacante opere sem detecção e transforme um problema menor em uma grande violação.

Esse modelo fica mais insustentável a cada dia, exigindo uma mudança operacional em um nível fundamental. Essa mudança não está só chegando: ela está sendo liderada por uma nova classe de “Empresas Fronteiriças”,

organizações que, segundo o Índice de Tendências de Trabalho da Microsoft para 2025, já estão reconstruindo seus negócios em torno da IA. Na área de segurança, essas empresas são definidas por seu avanço rumo ao SOC baseado em agentes, onde agentes semiautônomos se integram de forma direta aos fluxos de trabalho de segurança.

Isso não é um conceito futuro; é uma realidade das operações atuais. Como prova disso, a equipe interna de segurança da Microsoft agora usa agentes personalizados de IA para investigar de forma autônoma **75% dos incidentes recebidos**.⁴ Esta é a mudança crucial: migrar da análise manual para a contenção automatizada, liberando especialistas para se concentrar no que fazem melhor, que é arquitetar defesas e buscar ameaças inéditas.

Este white paper fornece um guia fundamental para essa transformação. Para os profissionais, ele promete a transição do trabalho reativo para uma operação de alto impacto. Para os líderes, ele oferece uma perspectiva clara sobre como navegar por essa mudança, desde a construção de uma fundação de dados unificada até o cultivo das equipes do futuro, compostas por um misto de pessoas e IA.



Sumário

- A urgência agêntica
- Fases de maturidade do SOC agêntico
- Criação do modelo operacional agêntico
- Escolha do seu caminho agêntico

¹“Estado do SOC: unifique agora ou pague mais tarde: o que a nova pesquisa revela”, página 8, Microsoft, 2026

²Ibid., página 6

³Ibid., página 7

⁴Com base em dados de pesquisa da Microsoft. Atualizado em fevereiro de 2026

A urgência agêntica

O cronograma para a modernização do SOC foi drasticamente comprimido por três forças poderosas:



Ameaças de IA em escala industrial

Os adversários agora ampliam seus ataques com IA, usando ferramentas generativas para criar iscas de phishing convincentes e automatizar o reconhecimento, o que aumenta drasticamente o volume, a velocidade e a eficácia de ataques sofisticados de engenharia social.



A superfície de ataque de nuvem e os agentes estão em constante mudança

A infraestrutura de nuvem tornou-se o alvo principal, e a superfície de ataque está crescendo rapidamente. À medida que aplicativos SaaS, agentes de IA e implantações em várias nuvens se multiplicam, os invasores ganham novos pontos de entrada que contornam totalmente os pontos de extremidade. Ao comprometer diretamente contas de nuvem ou o acesso de agentes, eles exploram pontos cegos que ferramentas de segurança centradas em dispositivos, como o EDR, simplesmente não foram projetadas para detectar.



Aumento da pressão regulatória

Em resposta a esses novos riscos, conselhos de administração e órgãos reguladores agora exigem governança fortalecida, supervisão humana documentada e relatórios rápidos e precisos de incidentes.

Essas forças tornaram os modelos tradicionais de SOC, caracterizados por ferramentas em silos e playbooks rígidos e manuais, insuficientes. As equipes de segurança estão sobrecarregadas, e **75% dos líderes de segurança**⁵ estão preocupados de que seu SOC não possa acompanhar o ritmo de ameaças novas e emergentes.

O modelo agêntico lida diretamente com essas pressões, ampliando a capacidade do SOC de detectar, decidir e agir na velocidade que as ameaças modernas exigem. Os agentes absorvem a carga operacional criada por ataques industrializados, automatizam investigações rotineiras em ambientes de nuvem e identidade, onde as ferramentas tradicionais enfrentam dificuldades, e fortalecem a governança com ações consistentes e auditáveis. Essa mudança operacional eleva os analistas humanos, levando-os da triagem reativa para o trabalho estratégico de alto impacto.



DADOS DA LINHA DE FRENTE

Concentre-se no que importa

Agentes automatizam o ruído da triagem (correlacionando dados e filtrando alertas) para liberar você para tarefas estratégicas: investigar ataques complexos e caçar novas ameaças.

⁵ "Estado do SOC: unifique agora ou pague mais tarde: O que uma nova pesquisa revela", página 9, Microsoft, 2026

Fases de maturidade do SOC agêntico

A evolução em direção a um SOC agêntico não é uma série de etapas sequenciais em um roteiro linear, mas uma progressão por meio de três estágios interconectados em uma estrutura dinâmica. O progresso em uma etapa acelera diretamente o valor das demais, criando um ciclo virtuoso de modernização, no qual dados aprimorados permitem uma IA mais inteligente, que revela novas oportunidades para o enriquecimento de dados. No cenário de ameaças atual, esperar para aperfeiçoar uma etapa antes de iniciar a próxima é um atraso estratégico que não cabe no contexto do SOC moderno.

SOC I

Unifique sua fundação de dados

Uma plataforma de segurança unificada é o alicerce arquitetônico do SOC agêntico. Sem ela, os agentes tornam-se apenas mais um silo digital, treinados isoladamente e incapazes de correlacionar insights entre domínios. O verdadeiro valor da unificação está no que ela previne: as intermináveis investigações em que analistas alternam entre consoles apenas para juntar as peças de um ataque. Ao integrar sinais de identidade, pontos de extremidade e infraestrutura de nuvem, você fornece o contexto holístico de que humanos e IA precisam para ações decisivas em diversos domínios. Esse princípio arquitetônico é o que separa a automação experimental das operações de segurança prontas para produção.

SOC II

Acelere as operações com a IA generativa

O foco desta etapa é elevar o SOC integrando IA generativa para fornecer contexto instantâneo, acelerar a tomada de decisões dos analistas e simplificar cargas de trabalho de alto volume. A síntese de sinais em toda a malha de segurança (da nuvem e da identidade aos pontos de extremidade) reduz o ruído, melhora a exatidão e capacita os analistas a se concentrarem em investigações de maior impacto. O resultado é um SOC mais eficiente e confiante, que estabelece os padrões operacionais e os modelos de colaboração entre humanos e IA necessários para a próxima etapa.

SOC III

Implante a automação agêntica

Esta etapa final marca a transição da assistência da IA para a verdadeira automação agêntica. Aqui, agentes de IA especializados param de apenas aumentar fluxos de trabalho individuais e começam a orquestrar tarefas específicas de forma autônoma (como isolar dispositivos comprometidos ou realizar a triagem de phishing relatado por usuários). Com o tempo, executam cenários complexos, como simular ataques e coordenar respostas em múltiplas etapas. Isso eleva os analistas humanos a supervisores estratégicos, focados em direcionar a performance dos agentes, orientar iniciativas de segurança e desenvolver expertise organizacional em operações autônomas.

Criação do modelo operacional agêntico

Com os estágios tecnológicos definidos, o foco muda para o modelo operacional. Isso significa criar novas capacidades para as pessoas que supervisionarão os agentes e para os processos de governança que geram confiança na automação.

Cultivo da sua equipe para a era agêntica

À medida que a IA começa a assumir mais análises críticas, as equipes de segurança estão redefinindo o conceito de expertise humana, priorizando o julgamento, a validação e a supervisão em vez da execução repetitiva. Essas tendências emergentes estão remodelando a forma como as equipes aprendem, crescem e desenvolvem confiança com seus novos colegas digitais.

Essa evolução eleva a expertise humana, criando novas funções essenciais para analistas experientes: **orquestradores**, que projetam e dirigem frotas de agentes de IA, **validadores**, que revisam e aprovam ações orientadas por IA, e **truth-setters (definidores de verdade)**, que lidam com incidentes inéditos que exigem intuição humana profunda.



DADOS DA LINHA DE FRENTE

Do tratador de alertas ao orquestrador de agentes

O modelo agêntico transforma sua função: em vez de reagir à fila de alertas, você passa a supervisioná-la. Você pode se concentrar na busca de novas ameaças e na resolução de problemas complexos, um trabalho que só um humano pode fazer.

No entanto, isso apresenta um novo desafio: as tarefas comuns e repetitivas em que a IA se destaca são o principal campo de aprendizado para analistas juniores. Os líderes devem definir um novo caminho para o desenvolvimento de analistas assistidos por IA, criando programas de treinamento que evitem a degradação das habilidades e formem a próxima geração de "truth-setters".

Organizações visionárias estão respondendo com a criação de ambientes de aprendizagem ampliados pela IA, onde analistas juniores treinam ao lado de agentes, aprendendo a validar decisões de IA, identificar casos extremos e desenvolver julgamento por meio de interações supervisionadas com IA, em vez de análises puramente manuais.

Salvaguardas para criar confiança em operações agênticas

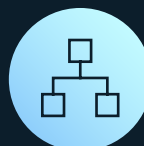
O uso eficaz da IA agêntica depende do controle verificável. A criação desse controle requer uma estrutura de governança alinhada com os requisitos emergentes, desde a [Estrutura de Gerenciamento de Riscos de IA do NIST](#) até as classificações [de alto risco](#) da Lei de IA da UE.

Conforme detalhado no [Guia da Microsoft para proteger a empresa baseada em IA: governança de dados e segurança](#), a governança eficaz de agentes aplica princípios comprovados de segurança do ciclo de vida dos dados a uma nova classe de identidades não humanas por meio de três princípios essenciais:



Trate os agentes como funcionários digitais

Todo agente requer um humano "[líder de agentes](#)" responsável por direcionar seu trabalho e garantir alinhamento com os objetivos do negócio. As equipes de segurança devem criar inventários abrangentes desses colaboradores digitais, verificar o acesso e as interações de cada agente com o sistema e aplicar permissões de privilégio mínimo, restritas a tarefas específicas.



Defina a autoridade do agente conforme o risco

Classifique as ações em três níveis: autônomas (tarefas de baixo risco, como enriquecimento de alertas), aprovadas por humanos (ações de risco médio, como isolamento de contas) e executadas por humanos (decisões de alto risco, como declarações de violação). Essa estrutura alinha o nível necessário de supervisão humana ao risco de cada ação.



Implemente trilhas de decisão verificáveis

Toda ação realizada por um agente deve gerar um registro de auditoria inalterável, detalhando qual decisão foi tomada, quais dados a fundamentaram, os níveis de confiança do agente e se ocorreu uma revisão humana. Isso satisfaz os requisitos regulamentares ao mesmo tempo que permite a melhoria contínua da performance.

Esse arcabouço de confiança, no entanto, não pode existir isoladamente. Ele deve ser respaldado por uma arquitetura tecnológica integrada que forneça [a visibilidade e o controle necessários](#) para operações agênticas seguras e eficazes.

Escolha do seu caminho agêntico

A jornada para um SOC agêntico começa com uma decisão estratégica fundamental: se é necessário adotar agentes prontos para uso para obter valor imediato ou investir em um ambiente de estúdio para criar soluções personalizadas. Projetamos nossa plataforma para possibilitar os dois caminhos, oferecendo uma estrutura flexível que se amplia com a maturidade da sua organização.

O caminho pronto para uso

Para organizações que buscam ganhos imediatos de eficiência, o roteiro se concentra na implantação de agentes pré-construídos para automatizar tarefas comuns e de alto volume.

- **Identifique tarefas repetitivas de alto volume**
Comece identificando as tarefas mais repetitivas e demoradas no seu SOC, como fazer a triagem manual de emails de phishing reportados por usuários ou aprimorar alertas com contexto básico.
- **Implante agentes pré-construídos**
Implante dezenas de agentes interecossistemas da Microsoft para lidar com esse trabalho repetitivo. Por exemplo, o Agente de Triagem de Phishing pode analisar os relatos dos usuários de forma autônoma, descartar mensagens benignas e lidar com ameaças reais, enquanto o Agente de Informações sobre Ameaças pode fornecer resumos instantâneos de novas campanhas ou vulnerabilidades sob demanda.
- **Reinvista a capacidade dos analistas**
Com a redução do trabalho manual, direcione seus analistas para iniciativas de maior valor, como busca proativa de ameaças, ajuste de regras de detecção e fortalecimento das defesas contra riscos emergentes.

O caminho do estúdio

Para organizações maduras que desejam adaptar a IA aos seus fluxos de trabalho, o roteiro se concentra na criação de soluções sob medida usando estruturas governadas.

- **Escolha um fluxo de trabalho empresarial único**
Identifique um desafio de segurança único para sua organização. Para um provedor de saúde, isso pode ser um agente personalizado que monitora acessos anômalos a sistemas de registro de pacientes. Para uma instituição financeira, pode ser um agente desenvolvido para identificar padrões de negociação com informações privilegiadas, correlacionando o acesso a dados com comunicações externas.
- **Crie e implante com governança**
Use estruturas como Microsoft Agent 365 para construir seu agente personalizado dentro dos limites de segurança. Atribua ao agente uma identidade exclusiva, restrinja suas permissões ao mínimo necessário para sua função e garanta que cada ação seja auditável.
- **Itere e expanda**
Use o sucesso do seu primeiro agente personalizado para criar expertise organizacional. Expanda gradualmente suas capacidades ou identifique o próximo fluxo de trabalho exclusivo para automatizar, tornando seu SOC um centro de inovação em segurança.



DADOS DA LINHA DE FRENTE

Vitória instantânea contra a fadiga de alertas

Recupere horas da fila de análise de phishing. Agentes prontos para uso automatizam a triagem repetitiva de emails relatados pelos usuários, liberando você para se concentrar na caça de ameaças em vez de lidar com alertas irrelevantes.

Combinação de abordagens e definição de expectativas

O mais importante é que esses caminhos não são mutuamente exclusivos. Muitas organizações começam com agentes prontos para uso e evoluem para soluções personalizadas à medida que amadurecem. Independentemente do ponto de partida, a governança vem em primeiro lugar. Os líderes devem definir um padrão mínimo de agente com finalidade documentada, proprietário e ações permitidas antes de implantar qualquer agente pré-criado ou personalizado.

O mais importante é que os líderes devem definir o que "de ponta a ponta" significa para sua organização, a fim de estabelecer expectativas claras. Mesmo uma solução pronta para uso requer ajustes e monitoramento para assegurar confiança. O objetivo não é eliminar a participação humana, mas permitir que as pessoas se dediquem ao trabalho mais importante.

Seu parceiro para a nova era da segurança

O SOC baseado em agentes representa uma mudança fundamental e necessária nas operações de segurança. Navegar nessa nova era requer mais do que simplesmente adotar ferramentas; exige um novo modelo operacional, novas habilidades e uma nova parceria entre a expertise humana e a inteligência de máquina.

A Microsoft não apenas compreende esse novo cenário, como também possui um plano claro e confiável para o futuro, comprovado em escala dentro do nosso próprio SOC. Nossa abordagem oferece uma plataforma unificada para visualizar todo o seu ecossistema digital, estruturas agênticas prontas para produção para agir com velocidade e precisão e orientação estratégica para você construir uma base adaptável de confiança e governança. Esse é o futuro da defesa resiliente, impulsionada por agentes, e a Microsoft é o parceiro estratégico para ajudá-lo a construí-la com confiança.



Saiba mais sobre as soluções de SOC capacitadas por IA



Acesse o conteúdo mais recente sobre SOC agêntico