kaspersky

Acertar na primeira vez: implementação do SOC sem arrependimentos

Introdução: quando é o momento certo para implantar um SOC?

Não existe um momento "eureca" universal em que as organizações percebem que precisam de um centro de operações de segurança (SOC). As empresas, assim como as pessoas, são entidades distintas que enfrentam desafios únicos e amadurecem em ritmos diferentes. Em nenhum outro campo isso é tão verdadeiro quanto na cibersegurança, em que a transformação digital e a complexidade tecnológica trazem novos riscos com o tempo, desde a mitigação de ataques direcionados até o gerenciamento da conformidade em escala global.

Contudo, existem gatilhos comuns que colocam em prática o processo de criação de um SOC. Alguns deles são lógicos e proativos, incluindo:

Requisitos regulatórios, especialmente em uma infraestrutura crítica

Conscientização proativa sobre riscos, entendimento de que as operações do negócio podem ser interrompidas por ataques cibernéticos

Aumento observado de ameaças cibernéticas, enfrentamento de ataques cibernéticos mais frequentes e/ou sofisticados que exigem uma equipe dedicada para a sua mitigação

Alguns outros gatilhos são reativos e, portanto, menos desejáveis. Um exemplo é uma empresa atacada que percebe que não tinha a capacidade de responder de forma eficaz. Ela pode começar sua jornada SOC a partir de uma posição de insegurança financeira, enquanto luta para desfazer os danos à sua reputação.

> A razão mais lamentável para estabelecer um SOC é que a empresa sofreu um incidente e teve que enfrentar as consequências. A abordagem correta é entender que você pode ser atacado e se preparar antes que isso aconteça.

Roman Nazarov, chefe de consultoria de SOC da Kaspersky

As violações de dados, vale a pena notar, geralmente custam milhões de dólares às organizações, mas é menos provável que as organizações que fazem uso intensivo de IA e automação na sua defesa gastem quantias tão altas.

É evidente que, do ponto de vista econômico, é mais viável implantar um SOC de forma proativa do que descobrir que seus controles de segurança são insuficientes em meio a um ataque.

Competências essenciais exigidas desde o primeiro dia

Uma vez que sua organização tenha identificado que precisa de um SOC e confirmado que é viável do ponto de vista financeiro, é fundamental começar com o pé direito. Isso significa identificar cedo o que é necessário para que o SOC funcione, e construir as bases que podem ser escaladas.

No topo da lista está a capacidade humana: cada SOC depende de três funções principais e sem elas o sucesso não é possível:

Analistas de segurança (investigação, triagem e resposta): defensores da linha de frente que fazem a triagem de alertas, investigam atividades suspeitas e executam a resposta inicial. Eles separam falsos positivos de ameaças reais e garantem um tratamento rápido e eficaz de incidentes.

Engenheiros (manutenção e suporte técnico): responsáveis pela implementação, manutenção e otimização de ferramentas e infraestrutura de segurança. Eles garantem que sistemas como o gerenciamento de eventos e informações de segurança (SIEM), plataformas de inteligência de ameaças (TIP) e orquestração, automação e resposta de segurança (SOAR) funcionem e sejam escaláveis.

Pesquisadores de ameaças (conscientização moderna sobre ameaças, desenvolvimento de detecção): Concentram-se na identificação de ameaças emergentes e no desenvolvimento de estratégias de detecção. Eles analisam a inteligência de ameaças, criam regras de detecção e ajudam o SOC a permanecer atualizado com relação às táticas em evolução.

Essas funções abrangem **operações**, **manutenção técnica** e **desenvolvimento para proteção contra ameaças**. Cada um deles requer uma experiência única sem a qual um SOC incipiente falhará.

> As três principais competências para qualquer SOC são analistas de segurança, engenheiros e pesquisadores de ameaças. Todos eles precisam estar cientes das ameaças modernas e estar preparados para combatê-las.

Roman Nazarov, chefe de consultoria de SOC da Kaspersky

Mas, embora essas contratações sejam cruciais, elas não são simples. A contratação de pessoas com a experiência e o conhecimento certos para trabalhar nos SOCs está sendo prejudicada pela lacuna de habilidades em segurança cibernética, com uma escassez estimada de quatro milhões de pessoas em todo o mundo.[1] E resumindo o mercado: apenas 14% das organizações acreditam ter as pessoas e as habilidades necessárias para atingir seus objetivos de segurança cibernética.[2]

Isso significa que você deve levar em consideração tempo e orçamento substanciais ao buscar talentos.

---

[1]World Economic Forum, Why Closing the Cyber Skills Gap Requires a Collaborative Approach, (World Economic Forum, 2024).

[2]World Economic Forum, Global Cybersecurity Outlook 2025, (World Economic Forum, 2025).

Viabilidade do SOC e preparação para escalar

Falamos sobre as habilidades e conhecimentos necessários em um SOC, mas o número de funcionários também é importante. O número mínimo viável é de cerca de 10 a 12 pessoas. Por quê? Porque um SOC precisa funcionar 24 horas por dia, 7 dias por semana, com uma equipe fundamental de pelo menos dez pessoas: um gerente, cinco analistas, dois engenheiros e dois pesquisadores.

Equipes pequenas logo enfrentam cargas de trabalho insustentáveis e fadiga de alertas (sendo que muitos deles podem ser falsos positivos). Isso pode levar a equipe a sofrer de burnout e, assim, aumentar a probabilidade de ameaças perdidas. É comum que os profissionais de segurança de TI cometam erros devido ao burnout que levam a violações de segurança.

A mão de obra é claramente importante. Se uma organização não tiver os meios apropriados para contratar pessoas para trabalhar no SOC, é melhor procurar um provedor externo que possa realizar o monitoramento de ameaças no seu lugar (falaremos sobre isso mais tarde). Mas se sua empresa estiver apta a implantar um SOC, o foco muda para a escalabilidade. Garantir que suas tecnologias possam ser dimensionadas horizontalmente, como pipelines de telemetria, mecanismos de correlação e outros sistemas principais, torna-se fundamental. Também é importante antecipar os limites de arquitetura desde o início, para que você esteja preparado para o crescimento e possa considerar necessidades futuras, como custos de recuperação de desastres.

Atalhos de SOC que funcionam (exceto um)

Como na maioria dos empreendimentos comerciais, é possível pegar alguns atalhos para atingir o objetivo mais rapidamente (neste caso, a funcionalidade do SOC). Um deles é aproveitar o conhecimento de terceiros na forma de estruturas, que atuam como um modelo para o seu SOC e podem acelerar o processo de design. Você pode pegar os processos definidos deles, adaptá-los à sua infraestrutura e começar a trabalhar.

O próximo não é exatamente um atalho, mas economizará tempo a longo prazo: é o ajuste contínuo e engenharia de detecção, essenciais para evitar a sobrecarga de alertas. A tecnologia deve ser ajustada, especialmente o conteúdo padrão, e adaptada à sua infraestrutura exclusiva. Isso requer processos claros para engenharia de detecção e refinamento contínuo da lógica de detecção.

> Não é possível simplesmente implementar ferramentas de segurança para fazer o monitoramento como o SIEM faz sem ajustá-las e pensar que isso o ajudará a combater ameaças. Tudo deve ser ajustado e adaptado à sua infraestrutura.

Roman Nazarov, chefe de consultoria de SOC da Kaspersky

Confiar demais no conteúdo padrão levará a um excesso de falsos positivos. Esse é um grande problema para as equipes do SOC porque cria um ruído esmagador que pode obscurecer os sinais de um ataque genuíno.

A resiliência de longo prazo requer revisão, refinamento e validação de alertas contínuos contra incidentes reais.

Processos que devem ser estabelecidos para garantir valor

Um SOC bem-sucedido sabe como implantar não apenas pessoas e tecnologia, mas também processos. E há uma ordem em que eles devem acontecer.

1

Inventariação da infraestrutura: um grande problema para muitos SOCs é que eles não entendem o que estão protegendo. A inventariação pode estar relacionada à área de TI, mas é um processo fundamental do SOC, porque é necessário saber o que precisa ser protegido para fazer isso com eficiência. Entender a infraestrutura a ser protegida é fundamental para definir como um ataque pode ocorrer, o que permite implementar controles de detecção e prevenção de forma proativa.

2

Monitoramento de ameaças: o próprio SOC deve começar a fazer o monitoramento de segurança. É preciso definir como adquirir telemetria, detectar sinais de ameaças e, então, gerenciá-las.

3

Operações maduras: é necessário, então, executar atividades mais avançadas, como identificação proativa de ameaças, pesquisa e engenharia de detecção contínua. O crescimento da experiência humana também deve se tornar uma prioridade, assim como o estabelecimento de processos definidos, a implantação de métricas, o investimento na resiliência da infraestrutura do SOC e a manutenção da melhoria contínua.

Implantar um SOC requer essa abordagem estruturada, começando com a inventariação da infraestrutura para garantir que você saiba exatamente o que está protegendo. O monitoramento de segurança então se torna o foco. E à medida que seu SOC amadurece, você deve priorizar o refinamento das operações e a integração de recursos avançados. Cada etapa se baseia na anterior.

> A primeira coisa que deve ser feita é a inventariação. Muitos SOCs descobrem anos depois que estão monitorando apenas parte da sua infraestrutura.

Roman Nazarov, chefe de consultoria de SOC da Kaspersky

Quando trazer MSSPs e consultores externos

MSSPs

Nem toda empresa deve implantar um SOC próprio. Aquelas que não têm tempo, vontade ou recursos para estabelecer um SOC devem considerar um provedor de serviços gerenciados de segurança (MSSP). É um provedor externo que pode fornecer monitoramento e resposta a incidentes adequados ao setor, capacidade e orçamento da organização.

Nas grandes empresas, os MSSPs podem fornecer conteúdo de detecção durante a implantação de um SOC interno, o que costuma levar mais de nove meses. Eles também podem ajudar a preencher a lacuna de habilidades, atuando como uma solução temporária enquanto você contrata pessoas para trabalhar no SOC e as treina.

Os MSSPs também podem ser incorporados em um modelo de transferência em fases, em que vocês executam operações em conjunto por 6 a 12 meses. Enquanto isso, você aprende com seu MSSP, até que o SOC interno esteja apto a funcionar de forma independente.

Consultores externos

É uma boa ideia trazer consultores externos desde o início da sua jornada de SOC para evitar cometer erros que possam custar caro. Eles podem fornecer abordagens e projetos testados que já foram comprovados em ambientes semelhantes e compartilhar percepções sobre o que funciona e o que não funciona, mostrando como adaptar os processos do SOC de forma eficaz.

Preparar e medir o sucesso do SOC

Um SOC deve agregar valor em pouco tempo. Você deve se preparar com objetivos claros, manuais definidos e as pessoas, processos e tecnologia certos. É essencial provar a prontidão do SOC por meio de testes rigorosos. Um dos métodos para isso são os exercícios de equipe vermelha para validar a detecção de cada etapa do ataque, e exercícios e simulações de ataque para confirmar a cobertura total. Esses exercícios podem expor lacunas (e ajudá-lo a preenchê-las) antes que incidentes reais ocorram.

Você pode medir o sucesso do SOC usando o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR). A queda do MTTD mostra uma descoberta de ameaças mais rápida, enquanto um MTTR mais baixo mostra que há uma contenção e correção mais rápidas. Testes constantes e rastreamento de métricas garantirão que seu SOC esteja melhorando desde o primeiro dia.

Erros comuns em SOCs recém-implantados

SOCs recém-implantados geralmente dependem muito da tecnologia e do conteúdo padrão do fornecedor, supondo que as ferramentas funcionarão de forma eficaz sem precisar de ajustes ou operadores qualificados. Esperar resultados instantâneos de soluções prontas para uso leva a ameaças perdidas e a uma confiança falsa. Não cometa esse erro.

Outra armadilha comum é negligenciar a melhoria contínua, tratando o SOC como estático em vez de uma capacidade em evolução, o que impede a adaptação a novas técnicas de ataque.

> O erro mais comum é considerar as tecnologias de detecção de um SOC como soluções fechadas que não requerem ajuste e adaptação.

Roman Nazarov, chefe de consultoria de SOC da Kaspersky

Principais pontos de aprendizado

Um SOC bem-sucedido começa com uma equipe central de analistas, engenheiros e pesquisadores. As estruturas podem acelerar a configuração, mas o ajuste e a personalização são essenciais. Você deve começar com a inventariação dos ativos, a compreensão do possível vetor de ataque e o monitoramento básico antes de implementar processos avançados. MSSPs e consultores podem apoiar as operações iniciais, ajudar a preencher suas lacunas de habilidades e fornecer experiência contínua.

Lembre-se: é importante planejar a escalabilidade desde o primeiro dia, considerando a tecnologia e o orçamento. Acima de tudo, as pessoas são fundamentais. Sem capacidade humana e experiência suficientes, mesmo as melhores ferramentas e estruturas não impedirão que o SOC falhe.

Sobre a Kaspersky

A Kaspersky é uma empresa de privacidade digital e segurança cibernética global fundada em 1997. Com mais de um bilhão de dispositivos protegidos contra ameaças cibernéticas emergentes e ataques direcionados, a inteligência de ameaças profunda e a expertise em segurança da Kaspersky estão constantemente se transformando em soluções e serviços inovadores para proteger empresas, infraestrutura crítica, governos e consumidores em todo o mundo. O portfólio abrangente de segurança da empresa inclui proteção de endpoint líder, produtos e serviços de segurança especializados, bem como soluções de imunidade cibernética para combater ameaças digitais sofisticadas e em constante evolução. Ajudamos mais de 200.000 clientes corporativos a proteger o que mais importa para eles. Saiba mais em www.kaspersky.com.

www.kaspersky.com.br