kaspersky

Otimização das operações do SOC com manuais personalizados: recursos do desenvolvimento eficaz

Introdução: o que é (e o que não é) um manual de SOC

Muitos cenários que as equipes encontram em um centro de operações de segurança (SOC) acabam ressurgindo, como ondas retornando à costa da praia. Eles podem parecer únicos, mas os padrões subjacentes são os mesmos. Os manuais do SOC, que são instruções passo a passo vinculadas a categorias de incidentes, são ferramentas que otimizam o trabalho e ajudam você a lidar com esses cenários.

Um manual oferece aos analistas um caminho claro a seguir quando há restrições de tempo e pressão. No entanto, ele não deve ser confundido com um plano de resposta a incidentes (RI), que define a estrutura, as funções e as políticas de alto nível de uma organização. Embora o plano de RI oriente a estratégia, como quais reguladores devem ser notificados após uma violação, ele carece da orientação detalhada e prática exigida por um analista durante um evento.

Os manuais auxiliam na divisão de categorias complexas de ameaças em ações específicas e consistentes nas quais os analistas podem confiar. Em última análise, isso acelera a resposta e reduz o risco. Sem eles, os analistas precisariam converter políticas amplas em ações, muitas vezes em meio a uma crise. E se eles não conseguirem entender o próximo passo a ser dado, podem ficar estagnados e desperdiçar segundos valiosos.

Os SOCs que adotam manuais junto com um plano de RI abrangem tanto a estratégia quanto a execução. O plano define quem faz o quê e por quê, enquanto o manual descreve como fazer. Juntas, essas ferramentas ajudam a construir resiliência diante de ameaças recorrentes.

A sequência importa: Plano de RI → capacidade de detecção → manuais

A sequência de preparação é importante ao desenvolver manuais, e ela deve fazer sentido. Primeiro, você deve desenvolver o plano de RI em coordenação com os departamentos de TI, gerenciamento de riscos e outras partes interessadas importantes. Cada grupo tem responsabilidades quando um incidente afeta sistemas, pessoas ou reputação, por isso é importante que eles estejam alinhados.

O SOC pode, então, se concentrar em desenvolver suas capacidades de detecção, porque faz pouco sentido elaborar manuais para ameaças que você não consegue identificar. No entanto, isso não significa que um SOC deva apenas analisar um conjunto restrito de detecções e considerar que "o trabalho já está feito". Uma visão limitada das ameaças deixa os analistas despreparados, e uma resposta inadequada a qualquer possível incidente é um fracasso.

> Antes de desenvolver manuais, é necessária uma compreensão completa dos seus recursos de detecção. No início, você não precisa de manuais para algo que não consegue detectar.

Andrey Tamoykin, especialista em segurança cibernética da Kaspersky

A prioridade deve ser elaborar manuais para lidar com incidentes que a equipe consegue detectar com confiança antes de expandir a cobertura para mais cenários à medida que a visibilidade melhora. Essa abordagem lógica equilibra prontidão com realismo:

- O plano de RI garante um alinhamento amplo.
- A detecção define as ações imediatas a serem tomadas.
- Os manuais convertem essas capacidades em ações consistentes.

A biblioteca dos manuais cresce junto com a capacidade de detecção ao longo do tempo, abrangendo não apenas o que é conhecido e esperado, mas também o que é menos comum e mais complexo.

Quem os manuais beneficiam e como?

Os manuais agregam valor em todo o SOC, mas seu principal impacto é na execução do dia a dia, pois eles fornecem estrutura e eficiência. As equipes podem, assim, responder de forma coordenada sem perder tempo debatendo quais seriam os próximos passos. Isso é importante no cenário atual, com tantos SOCs sobrecarregados.

Em termos de indivíduos, os analistas são os que mais se beneficiam porque os manuais fornecem instruções claras e consistentes vinculadas a cenários específicos. Isso significa que, em vez de adivinhar ou reinventar o processo a cada alerta, eles podem seguir um caminho que já foi testado. A incerteza é reduzida e os analistas mais novos ou juniores conseguem se adaptar mais rapidamente. (Para se ter uma perspectiva, 46% dos profissionais de Segurança da Informação disseram que demoraram mais de um ano para se sentirem confortáveis ou confiantes na sua primeira função de segurança cibernética.[1])

> Ao otimizar a área de resposta, o desempenho geral de todo o SOC aumenta, mas os analistas se beneficiam mais do que os outros.

Andrey Tamoykin, especialista em segurança cibernética da Kaspersky

Os manuais também limitam a fadiga causada pela tomada de decisões. Durante um turno longo ou incidente que requer uma resposta rápida, ter uma sequência predefinida de ações reduz o esforço mental. O resultado é que a equipe consegue gerar respostas mais rápidas e consistentes. Com o tempo, essa consistência fortalece a confiabilidade do SOC e permite que os líderes se concentrem em melhorar a estratégia geral e a resiliência.

[1] Kaspersky, Portrait of Modern Information Security Professional, (Kaspersky Daily, 2024).

Melhoria contínua e gatilhos para revisão

Um manual que nunca é atualizado rapidamente perde o seu valor. As ameaças evoluem, as ferramentas mudam e lições são aprendidas com incidentes do mundo real. Os manuais devem ser revisados com frequência, idealmente pelo menos uma vez por ano. Isso garante que eles reflitam os processos, a tecnologia e as prioridades de negócios atuais.

> Quase todas as atividades em um SOC geram uma melhoria contínua, e os manuais não são exceção.

Andrey Tamoykin, especialista em segurança cibernética da Kaspersky

As revisões baseadas em eventos são igualmente importantes. Sempre que houver uma mudança na lógica de detecção, uma mudança na infraestrutura ou um incidente significativo, o manual correspondente deve ser revisado. Esses são os momentos em que as lacunas são expostas e as melhorias se tornam evidentes. A atualização em resposta a esses eventos garante que o SOC sempre se fortalecendo.

Ao combinar revisões frequentes com atualizações orientadas a eventos, as organizações podem manter manuais que melhoram junto com o SOC. O resultado é um recurso que permanece confiável e eficaz ao longo do tempo.

O que é "bom": as métricas que realmente importam

Um manual bem estruturado não é apenas claro e prático, mas também oferece resultados mensuráveis. As métricas corretas mostram se um manual está funcionando conforme o esperado. Uma medida importante é o tempo médio de triagem: a rapidez com que os analistas conseguem confirmar se um alerta é um verdadeiro positivo ou um falso positivo, para que os recursos possam ser direcionados para onde importa. A qualidade da triagem também se reflete nas taxas de falsos positivos e falsos negativos. Muitos falsos positivos desperdiçam tempo, enquanto falsos negativos significam que ameaças reais estão sendo perdidas.

> O tempo de triagem é uma das métricas mais importantes, pois os incidentes de segurança precisam ser validados o mais rápido possível.

Andrey Tamoykin, especialista em segurança cibernética da Kaspersky

O tempo médio de resposta é outra métrica fundamental, pois ele rastreia a rapidez com que o SOC consegue conter um incidente e fornece recomendações para a sua mitigação. Atrasos aumentam o risco, enquanto a velocidade prova a eficácia da equipe.

Como acertar na automação do manual

A abrangência da automação também é importante. Acompanhar a porcentagem de tarefas automatizadas em cada manual mostra onde a eficiência está melhorando e onde o esforço manual ainda prevalece.

Mas, embora a automação possa transformar os manuais, ela não deve ser o ponto de partida. Um manual bem testado é a base que garante a solidez dos processos antes da automatização das tarefas. Partindo dessa base, a automação pode ser feita em etapas. O enriquecimento básico acelera o acesso ao contexto, enquanto a orquestração das tarefas vincula as ações entre as ferramentas. O fator humano garante que os analistas atuem onde o julgamento é necessário.

> É melhor começar a desenvolver manuais sem automação do que não ter nenhum.

Andrey Tamoykin, especialista em segurança cibernética da Kaspersky

A automação total é possível, mas apenas em cenários de baixo risco e bem conhecidos. A confirmação humana é essencial para ações de alto impacto, como isolamento de hosts críticos para os negócios ou exclusão de contas. Nesses casos, a automação sem critérios pode causar mais danos do que a própria ameaça. O objetivo é o equilíbrio: a automação deve substituir o trabalho repetitivo enquanto os analistas continuam supervisionando as decisões sensíveis. Essa abordagem, quando executada corretamente, cria um SOC em que a tecnologia amplifica o julgamento humano em vez de substituí-lo.

Escopo e estrutura do manual

O escopo do manual começa com as categorias de incidentes. Normalmente, o SOC consegue detectar de 20 a 30 incidentes de forma confiável. Cada categoria deve ter seu próprio manual, com possíveis ramificações para abranger variantes comuns. Um manual sólido equilibra as principais etapas compartilhadas, como triagem e contenção, com ações personalizadas para ameaças específicas, como vírus ou backdoors. Isso garante consistência sem perder a precisão.

> Não precisamos de um manual para lidar com um backdoor. Precisamos de um manual para lidar com infecções por malware, com instruções especiais para um backdoor, se for realmente necessário no seu caso específico.

Andrey Tamoykin, especialista em segurança cibernética da Kaspersky

Nos SOCs menores, o gerente geralmente lidera o desenvolvimento e a aprovação. Nos SOCs maiores, um líder de pesquisa ou especialista no assunto valida cada manual quanto à relevância, necessidade e alinhamento com as capacidades de detecção, garantindo a eficácia da biblioteca.

Implementação prática: comece de forma simples e cresça com sua capacidade

A implementação de manuais deve começar de forma simples. Comece listando algumas tarefas no estilo de lista de verificação que abordam os incidentes mais comuns e repetidos. À medida que sua capacidade e tecnologia de detecção amadurecem, expanda a biblioteca para abranger mais categorias e introduza a automação onde ela agrega valor óbvio. O segredo é aumentar a quantidade de manuais no mesmo ritmo que a capacidade do SOC aumenta.

> Você não precisa gastar mais tempo elaborando um manual do que o necessário.

Andrey Tamoykin, especialista em segurança cibernética da Kaspersky

Você deve evitar investir tempo em manuais complexos ou teóricos que trazem pouca eficiência na prática. Uma abordagem focada e em constante evolução garante que os manuais permaneçam úteis, gerenciáveis e alinhados com as necessidades do mundo real da equipe.

Principais pontos de aprendizado

A resposta eficaz a incidentes começa com a preparação na ordem certa: crie o plano de RI, avalie as capacidades de detecção e, depois, crie manuais. O sucesso deve ser medido com métricas claras, incluindo tempo de triagem, tempo de resposta, taxas de falsos positivos e negativos, e abrangência da automação.

Lembre-se de que os manuais não são estáticos. Eles devem ser revisados com frequência e após qualquer alteração importante nas suas ferramentas ou infraestrutura. Embora a automação possa trazer velocidade e eficiência, ela deve ser equilibrada com a experiência humana para a tomada de decisões críticas.

Os melhores resultados são obtidos ao começar de forma simples, comprovar valor logo no início e dimensionar os manuais de acordo com a maturidade e a capacidade do SOC.

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