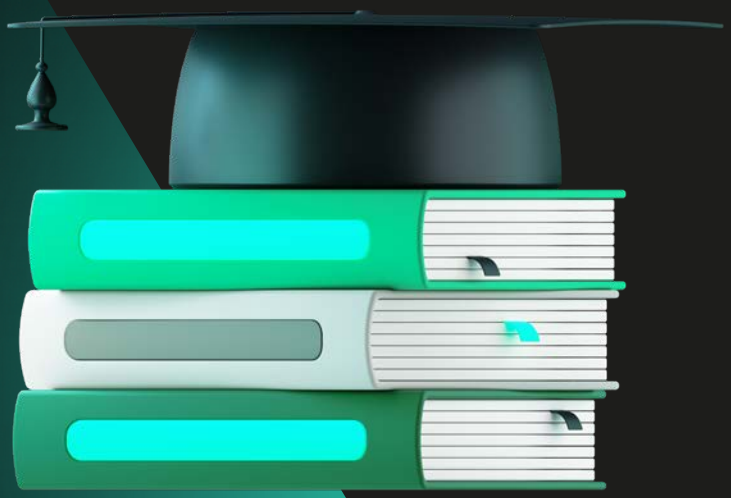
kaspersky



Integração e mentoria efetivas nas equipes de SOC

Este artigo foi escrito por **Renat Gimadiev, especialista em soluções de SOC no departamento de Soluções de segurança especializadas da Kaspersky**. Ele destaca o papel essencial da integração estruturada e da mentoria nos SOCs modernos, mostrando como programas intencionais podem acelerar a prontidão dos analistas, melhorar a retenção e reduzir o burnout.

O artigo se baseia em desafios do mundo real para destacar estratégias fáceis de serem implementadas e que ajudam os novos contratados a se tornarem produtivos, incluindo:

- Planos de integração estruturados (por exemplo, modelos de 30/60/90 dias com equilíbrio entre teoria e prática)
- Funções e responsabilidades de mentoria definidas (mentor, colega, supervisor e mentorado)
- Técnicas práticas de transferência de conhecimento, incluindo aprendizado por observação, práticas guiadas e ciclos de feedback
- Indicadores-chave de desempenho (por exemplo, tempo até a independência, taxa de erro de controle de qualidade e satisfação do mentor)

Ao usar essas abordagens, as organizações podem desenvolver gradualmente os novos contratados, transformando-os em analistas confiantes, capazes de fortalecer a detecção, a resposta e a resiliência de um SOC.

Por que a integração e a mentoria são importantes

Em um centro de operações de segurança (SOC), as pessoas são o ativo mais importante. Ferramentas avançadas e processos bem definidos são fundamentais, mas é o fator humano que, em última análise, determina a eficácia com que as ameaças são detectadas, investigadas e neutralizadas.

As primeiras semanas de um novo analista no SOC são as mais importantes. Sem um caminho claro de integração, empatia e apoio dos colegas, eles correm o risco de ficar sobrecarregados, ter um desempenho baixo ou pedir demissão em pouco tempo. Da mesma forma, a ausência de uma mentoria estruturada deixa a transferência de conhecimento ao acaso, o que pode levar a uma qualidade de investigação inconsistente, tempos de resposta mais lentos e incidentes críticos perdidos.

Os dados confirmam esse risco: no Estudo sobre a Força de Trabalho da Segurança Cibernética (ISC) de 2023, mais de 20% dos analistas de SOC relataram níveis altos de estresse e burnout, com muitos deixando suas funções no período de dois anos. [1] Estudos também mostram que normalmente são necessários entre seis e nove meses para um analista atingir uma produtividade independente caso a integração não seja estruturada. Por outro lado, as organizações que investem em programas estruturados de mentoria podem aumentar as taxas de retenção em 20 a 30%, em média. Na prática, isso pode significar que cada novo contratado será acompanhado por um mentor para fazer suas primeiras investigações.

Programas eficazes de integração e mentoria abordam esses desafios, fornecendo clareza, estrutura e orientação contínua. Eles ajudam os novos contratados a se tornarem produtivos mais rapidamente, tornam a equipe mais resiliente durante incidentes de alta pressão e evitam que as pessoas deixem a empresa cedo demais. Igualmente importante, eles incentivam o aprendizado contínuo, em vez de um esforço de treinamento único.

Funções e expectativas claras

O sucesso da integração e da mentoria depende da existência de funções claramente definidas. Embora cada SOC possa ter sua própria estrutura de pessoal, as seguintes funções são altamente recomendadas:

1

Supervisor (Gerente de SOC/CISO): Supervisiona o programa de integração e mentoria, alinhando-o com os objetivos da empresa e com os requisitos de conformidade, e analisa o progresso ao longo do tempo.

2

Mentor (Analista sênior): Orienta o novo contratado sobre os processos, as ferramentas e a cultura da equipe, fornece feedback regular e compartilha experiências do mundo real.

3

Colega (Analista de turno): Atua em um contexto informal para perguntas do dia a dia, ajudando na orientação dos fluxos de trabalho e ferramentas.

4

Mentorado (Novo contratado): Participa ativamente do aprendizado, busca feedback, documenta as lições aprendidas e assume mais responsabilidades conforme seu progresso.

[1] ISC. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. (ISC 2023).

Projeto da jornada de integração

Um processo de integração bem estruturado garante que o novo analista de SOC ganhe conhecimento e confiança sem ser sobrecarregado com tarefas rotineiras e casos difíceis. Um dos modelos mais populares e comprovados é o **plano de 30/60/90 dias**, que equilibra o aprendizado teórico com a exposição prática durante o período de experiência. Aqui está uma breve demonstração:

Primeiros 30 dias - Orientação e observação:

Introdução à missão do SOC, à estrutura da equipe e a caminhos de escalonamento, aprendizado básico sobre as ferramentas, observação dos mentores, reunião com diferentes equipes como TI, departamento jurídico, entre outros. Nessa fase, os novos contratados também podem participar de exercícios simulados ou minicenários gamificados que os ajudam a praticar sem a pressão causada por incidentes em tempo real.

ias 31 a 60 - Prática guiada:

Lidar com alertas de baixa gravidade sob supervisão, executar consultas predefinidas, redigir chamados e contribuir com artigos para a base de conhecimento. Essa fase também deve incluir sessões virtuais de aprendizado por observação e exposição a outras funções de segurança para fornecer um contexto mais amplo (por exemplo, breves rotações com equipes de identificação proativa de ameaças ou de perícia digital).

Dias 61 a 90 - Operações independentes:

Assumir a responsabilidade pela triagem de primeiro nível, conduzir investigações com a supervisão dos mentores e começar a orientar o próximo grupo de mentorados. A essa altura, os analistas devem demonstrar adaptabilidade, mas a velocidade de progressão pode variar: alguns podem estar prontos em 60 dias, enquanto outros podem precisar de até 120 dias. O segredo é manter ciclos de feedback semanais entre o mentorado, o mentor e o gerente do SOC para garantir o alinhamento dos objetivos e evitar que informações importantes sejam perdidas.

Concluindo, cada analista de SOC aprende de maneira diferente, alguns aprendem o básico em semanas, enquanto outros precisam de mais tempo para absorver todos os novos conceitos.

Desenvolvimento de um programa de mentoria efetivo

É evidente que a mentoria é um processo estruturado com etapas definidas e resultados mensuráveis. Não se esqueça de seguir estas etapas na sua jornada de mentoria:

Observar → atuar em conjunto → liderar: primeiro, o mentorado acompanha o mentor, depois, atua junto nas tarefas e, finalmente, passa a liderar os incidentes com intervenção mínima.

Cadência: reuniões semanais presenciais, relatórios diários de turno, verificação formal de habilidades, visão geral de obstáculos etc.

Melhores práticas: limitar o número de mentorados por mentor, por exemplo, no máximo dois; documentar o feedback, comemorar as conquistas e solicitar feedback com frequência.

KPIs

Métrica	Definição	Infraestrutura	Por que é importante
Tempo até a independência	Dias até que um novo contratado possa lidar com incidentes básicos sozinho	60 a 90 dias	Reduz a carga de trabalho da equipe
Taxa de erro de controle de qualidade	Porcentagem de chamados de incidentes com desvios dos padrões	<5% após 90 dias	Garante qualidade e conformidade
Taxa de retenção	Porcentagem de novos contratados que permanecem no cargo após 6 a 12 meses	>85%	Reduz os custos de recrutamento e treinamento
Satisfação do mentor/mentorado	Feedback de estudos estruturados	≥4/5	Indica engajamento e valor do programa
Adesão ao manual de procedimentos	Porcentagem de etapas seguidas corretamente	>95%	Mantém a consistência e a prontidão para auditoria

Melhores práticas: combinar o treinamento de ferramentas com o contexto do processo, manter e atualizar com frequência uma base de conhecimento dinâmica, reconhecer e recompensar os melhores mentores e combinar formatos de aprendizado.

Armadilhas comuns: sobrecarregar os mentores, focar apenas nas habilidades técnicas, dar um feedback inconsistente aos mentorados e tratar a integração como um processo único em vez de contínuo.

Conclusão

A integração e a mentoria vão muito além de simples listas de verificação de RH: são investimentos estratégicos que geram um impacto direto no desempenho do SOC e na qualidade do serviço. Com um programa estruturado, os analistas se adaptam mais rapidamente e são menos propensos a sofrer de burnout. Essa estabilidade significa menos contratações e custos mais baixos para a organização.

Essas iniciativas melhoram não só a produtividade, mas também a qualidade da detecção e da resposta. Os analistas integrados de forma eficaz têm mais confiança em lidar com incidentes, seguem os manuais de procedimentos com maior precisão e contribuem para a melhoria contínua da base de conhecimento do SOC. Sem mentoria, conhecimentos essenciais podem ser perdidos quando alguém deixa a empresa, como aquele analista que se lembra de todas as peculiaridades e truques de SIEM.

Do ponto de vista comercial, isso se traduz em resultados mensuráveis: tempo médio de detecção (MTTD) mais rápido, tempo médio de resposta (MTTR) mais curto, melhor prontidão para auditoria e uma postura de conformidade mais sólida. Para a liderança da empresa, investir em pessoas cria uma cultura resiliente no SOC, fazendo com que os analistas se sintam apoiados, valorizados e motivados a crescer.

No fim das contas, as melhores ferramentas não servirão de nada se as pessoas não estiverem devidamente preparadas. Uma integração e mentoria eficazes constroem o tipo de equipe que consegue reagir rapidamente quando a próxima ameaça surgir. Ninguém sabe exatamente quando isso poderá acontecer. Portanto, a equipe precisa estar sempre preparada e aprimorar continuamente suas habilidades.

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