kaspersky

Da sobrecarga à eficiência – como a IA transforma as operações de SOC

O burnout do SOC está se tornando um problema de segurança crítico

> Observamos continuamente muitas organizações enfrentando dificuldades para contratar e reter pessoal, pois muitos analistas de SOC ficam tão sobrecarregados que muitas vezes procuram mudar de emprego ou migrar para uma área totalmente diferente.

No Reddit ocorrem discussões sobre o tema. O SANS Institute comentou que, como resultado,

E um relatório de 2024 da Osterman Research descobriu que os Centros de Operações de Segurança (SOCs) estão enfrentando um número crescente de alertas diários para investigar, com 97% das organizações observando aumentos anuais no número de alertas gerados.

O burnout do SOC está se tornando um problema de segurança crítico. Mas felizmente, como em muitas áreas, a ajuda está disponível na forma de inteligência artificial (IA) que, ao automatizar tarefas de rotina, filtrar falsos positivos e muito mais, pode reduzir o burnout e melhorar a eficácia geral da equipe do SOC.

Por que o burnout do SOC está acontecendo?

O crescimento no número de alertas diários, apontado pela Osterman Research, sobrecarrega os analistas encarregados de triá-los e investigá-los, agravando-se à medida que os alertas e incidentes não tratados se acumulam. O relatório constatou, por exemplo, que 89,6% das organizações estão observando um aumento contínuo nos backlogs de segurança e que, à medida que o número de alertas cresce, a pressão sobre as equipes do SOC para gerenciá-los também aumenta. No entanto, como apenas 19% dos alertas costumam ser resolvidos, a carga de trabalho se torna um ciclo vicioso, levando a uma pressão implacável sobre os analistas envolvidos.

Não surpreende o SANS Instituteter dito,

> Essa constante troca de profissionais de segurança leva a um problema enorme — e não é algo com que apenas os profissionais de cibersegurança devem se preocupar. A constante rotatividade dos funcionários inevitavelmente interrompe o fluxo de trabalho do SOC e, por fim, a eficácia do SOC. Tudo isso pode expor uma organização a um risco maior. Se o seu SOC não conseguir fugir dessa interrupção, um cibercriminoso poderá passar despercebido. É um ciclo do qual acreditamos que não conseguimos escapar. Mas precisamos. É nossa obrigação.

A questão é: que medidas práticas você pode implementar para reduzir problemas como estes?

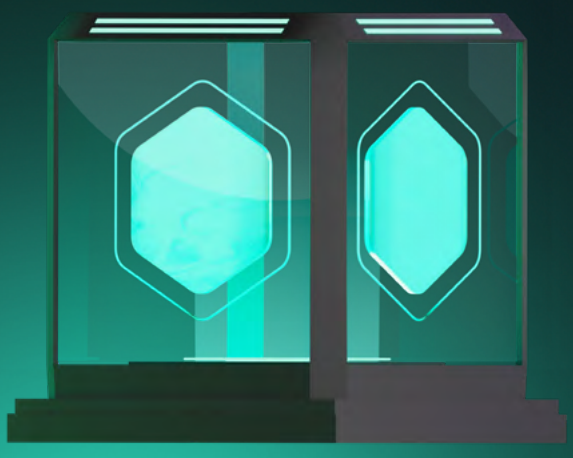
Reduzir o burnout e aprimorar a eficácia do SOC

Vladislav Tushkanov, gerente de grupo no Kaspersky AI Technology Research Center, diz,

> Uma maneira óbvia de reduzir o esgotamento do SOC é facilitar a vida dos analistas do SOC automatizando tarefas de rotina, como triagem de alertas e investigação.
>
> Muitos analistas gastam tempo excessivo em tarefas repetitivas que podem ser facilmente automatizadas. Isso pode levar ao "boreout" e ao burnout, fazendo com que tarefas mais importantes não sejam iniciadas ou permaneçam inacabadas e aumentando o risco de ameaças perigosas prejudicarem sua organização.

Como a KPMG observa,

> A IA permite a automação eficiente de muitas tarefas manuais que atualmente são realizadas por humanos, resultando na redução do tempo gasto nessas tarefas e na melhor utilização dos recursos humanos. O uso de algoritmos de aprendizado de máquina (ML) ajuda computadores a identificar padrões e detectar anomalias mais rapidamente que qualquer ser humano, aumentando as taxas de detecção de atividades maliciosas e ameaças à infraestrutura de rede ou à privacidade de dados da sua empresa. A IA também permite que as organizações respondam de forma mais eficaz às ameaças, com interrupção mínima nas operações comerciais, ao mesmo tempo que ajuda a proteger ativos valiosos contra violações por hackers ou outros agentes mal-intencionados que buscam informações confidenciais, como números de cartão de crédito ou números de previdência social.



Tushkanov acrescenta,

> Muitos SOCs estão explorando formas de reduzir as cargas de trabalho dos analistas com a ajuda de ML – melhorando a eficiência da triagem e evoluindo a automação de tarefas ao filtrar falsos positivos do fluxo de alertas resultante.
>
> Uma maneira eficiente de conseguir isso é por meio de um "analista automático" baseado em IA — um modelo de ML supervisionado que aprende com alertas processados pela equipe do SOC e, em seguida, tenta replicar seu comportamento de forma independente. Ao reduzir o número de alertas que exigem investigação dos analistas do SOC, isso não apenas economiza recursos da equipe, mas também lida com os alertas mais comuns e rotineiros, permitindo que os analistas do SOC se concentrem nos casos mais interessantes que exigem investigação mais profunda por especialistas humanos.

A Kaspersky pode te ajudar

IA e ML são recursos amplamente utilizados nas soluções de cibersegurança da Kaspersky, com o desenvolvimento contínuo dessas tecnologias sendo conduzido por um dos cinco centros especializados da Kaspersky, o Kaspersky AI Technology Research Center, o qual é dedicado a essa tarefa.

> O Kaspersky AI Technology Research Center se concentra na detecção de ameaças e soluções com tecnologia de IA, cibersegurança com IA e pesquisas em IA generativa.
>
> Isso abrange desde a aplicação de ciência de dados e algoritmos de IA para detectar ameaças cibernéticas, como malware, spam, phishing e ataques direcionados, até a pontuação de risco de IA, que evidencia comportamentos suspeitos de hosts com base em dados de correlação em produtos como XDR e SIEM.
>
> Também estamos envolvidos várias atividades de desenvolvimento, como estudar métodos de aplicação de IA generativa para desenvolver instrumentos baseados em LLM para operações de segurança, criar instrumentos de análise de comportamento e detecção de anomalias baseados em IA para ambientes industriais de TI – TO e formular abordagens, metodologias e soluções de IA seguras, todas as quais beneficiam nossos parceiros e clientes.

Tushkanov explica,

Sobre a Kaspersky

A Kaspersky é uma empresa global de cibersegurança e privacidade digital fundada em 1997. Com mais de um bilhão de dispositivos protegidos contra ameaças cibernéticas emergentes e ataques direcionados, a inteligência de ameaças profunda e o 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 de segurança abrangente da empresa inclui proteção de endpoint líder, produtos e serviços de segurança especializados e 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