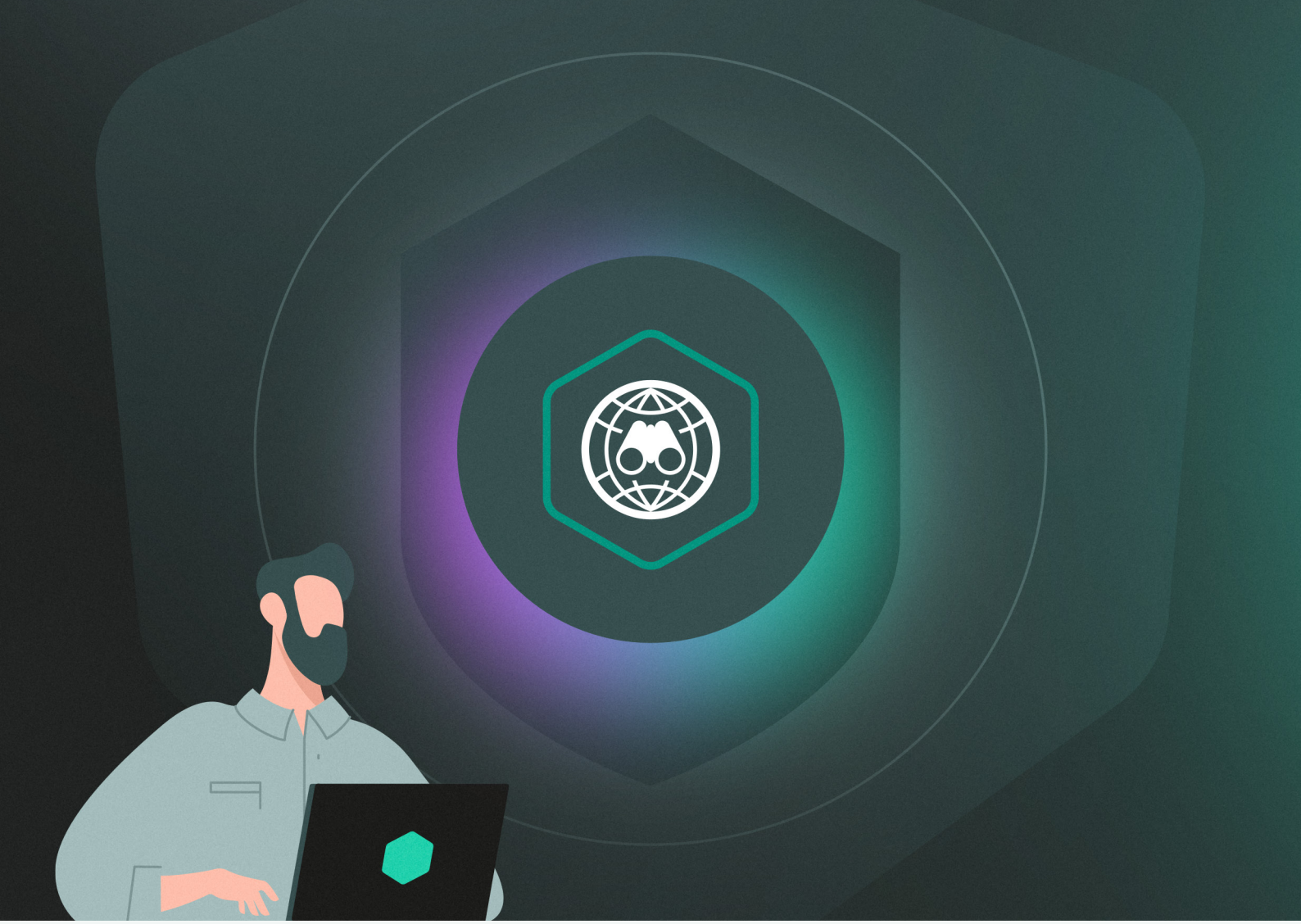


Kaspersky
Threat Intelligence

Avaliando fontes de inteligência de ameaças

kaspersky PREPARADOS PARA O FUTURO

Saiba mais em kaspersky.com.br
#bringonthefuture

Introdução

Com a superfície de ataque em expansão e as ameaças cada vez mais sofisticadas, apenas reagir a um incidente não é suficiente. Os ambientes cada vez mais complexos fornecem múltiplas oportunidades para invasores. Cada setor e cada organização têm seus próprios dados únicos para proteger e utilizam seus próprios conjuntos de aplicativos, tecnologias, etc. Tudo isto introduz um número enorme de variáveis em possíveis métodos de execução de um ataque, com novos métodos a emergir diariamente.

Nos últimos anos, observamos a indefinição de limites entre diferentes tipos de ameaças e diferentes tipos de agentes de ameaças. Os métodos e as ferramentas que antigamente eram uma ameaça para um número limitado de organizações se espalharam para um mercado mais amplo. Um exemplo disso é a divulgação de código pelo grupo Shadow Brokers, que colocou exploits avançados à disposição de grupos criminosos, que de outro modo não teriam tido acesso a esse tipo de código sofisticado. Outro exemplo é o surgimento de campanhas de ameaça persistente avançada (APT) focadas não em espionagem virtual, mas em furto, roubando dinheiro para financiar outras atividades em que o grupo de APT está envolvido. E a lista continua.

É necessária uma nova abordagem

Os métodos e as ferramentas que antigamente eram uma ameaça para um número limitado de organizações se espalharam para um mercado mais amplo.

Com o aumento crescente do número de ataques avançados e direcionados às empresas, é evidente que uma defesa bem-sucedida requer novos métodos. Para se protegerem, as empresas precisam adotar uma abordagem proativa, adaptando constantemente seus controles de segurança ao ambiente de ameaça em constante mudança. A única forma de acompanhar estas mudanças é criar um programa de inteligência de ameaças eficaz.

A inteligência de ameaças já se tornou um componente essencial das operações de segurança implementadas por empresas de várias dimensões em todos os setores e regiões. Disponível em formatos de leitura tanto por máquinas como por humanos, a inteligência de ameaças pode auxiliar as equipes de segurança com informações relevantes durante o ciclo de gestão do incidente e fornecer informações para a tomada de decisões estratégica (Figura 1).

No entanto, a procura crescente por inteligência de ameaças externa originou uma abundância de fornecedores de inteligência de ameaças, cada um oferecendo um conjunto de serviços diferentes. Um mercado vasto e competitivo com imensas e complexas opções pode tornar a escolha da solução certa para a sua organização altamente confusa e extremamente frustrante.

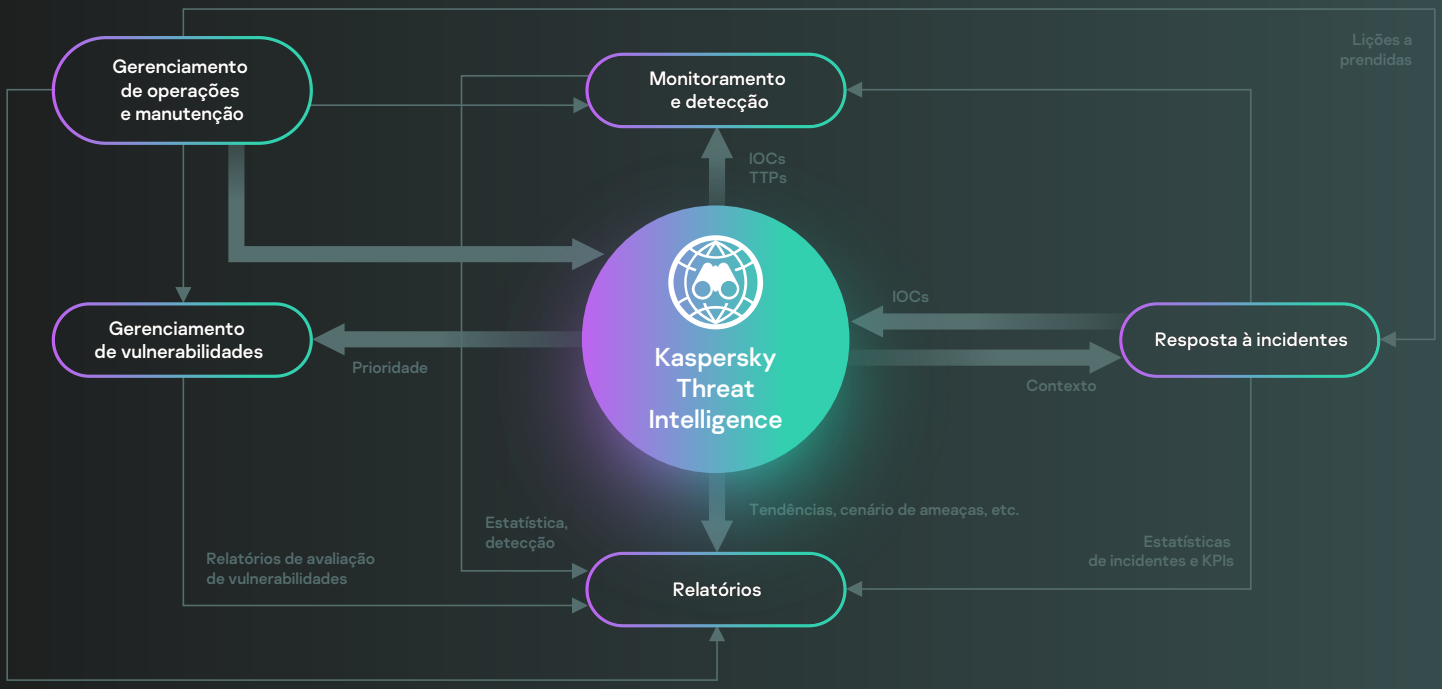


Figura 1

Operações de segurança orientadas por inteligência de ameaças

A inteligência de ameaças que não é concebida de acordo com as especificidades da sua empresa pode agravar a situação. Atualmente, em muitas empresas, os analistas de segurança passam mais de metade do seu tempo classificando falsos positivos ao invés da busca e resposta a ameaças proativa, levando a um aumento significativo nos tempos de detecção. Alimentar suas operações de segurança com inteligência irrelevante ou imprecisa irá aumentar ainda mais a quantidade de alertas falsos e ter um impacto negativo grave nas suas capacidades de resposta e na segurança global da sua empresa.

Onde reside a melhor inteligência...

Então, como você avalia as inúmeras fontes de inteligência de ameaças, identifica aquelas que são mais relevantes para a sua organização e as operacionaliza de forma eficaz? Como você navega pelas enormes quantidades de marketing irrelevante com quase todos os fornecedores alegando que sua inteligência é a melhor?

Estas perguntas, embora válidas, definitivamente não são as primeiras que você deveria fazer. Atraídas por mensagens chamativas e promessas grandiosas, muitas organizações acreditam que um fornecedor externo pode fornecer a eles uma espécie de superpoder de visão raio X, ignorando completamente o fato de que a inteligência mais valiosa reside no perímetro das suas próprias redes empresariais...

Os dados de sistemas de detecção e prevenção de intrusão, firewalls, registros de aplicativos e registros de outros controles de segurança podem revelar muito sobre o que acontece dentro da rede de uma empresa. Pode identificar padrões de atividade maliciosa específicos da organização. Pode distinguir entre um usuário normal e um comportamento de rede, ajudando a manter um rastro de atividade de acesso a dados.

Figura 2

Operacionalizando a inteligência de ameaças externa

Pense como um invasor

Para criar um programa de inteligência de ameaças eficaz, as empresas, incluindo as que têm Centros de Operações de Segurança, devem pensar como um invasor, identificando e protegendo os alvos mais prováveis. Para obter valor real de um programa de inteligência de ameaças é necessário saber muito bem quais são os principais ativos e quais os conjuntos de dados e processos de negócios são essenciais para alcançar os objetivos da organização. Identificar estas "joias da coroa" permite às empresas estabelecer pontos de coleta de dados ao seu redor para mapear ainda mais os dados coletados com informações sobre ameaças disponíveis externamente. Considerando os recursos limitados que os departamentos de segurança da informação normalmente têm, criar o perfil de uma organização inteira é uma tarefa enorme. A solução é adotar uma abordagem baseada no risco, centrando-se primeiro nos alvos mais suscetíveis.

Assim que as fontes internas de inteligência de ameaças estiverem definidas e operacionalizadas, a empresa pode começar a pensar em adicionar informações externas aos fluxos de trabalho existentes.

É uma questão de confiança

As fontes de inteligência de ameaças externas variam em níveis de confiança:

As fontes abertas são gratuitas, mas muitas vezes carecem de contexto e devolvem um número significativo de falsos positivos.

As fontes de inteligência de ameaças comerciais são muito mais confiáveis, embora comprar o acesso a elas possa custar caro.

Uma boa opção para começar, é acessar comunidades de compartilhamento de inteligência específicas do setor, como o Financial Services Information Sharing and Analysis Center (FS-ISAC). Essas comunidades fornecem informações extremamente valiosas, embora muitas vezes sejam vedadas e seja necessária uma assinatura para obter acesso.

O princípio orientador para escolher fontes de inteligência de ameaças externas, deve ser a qualidade e não a quantidade. Algumas organizações podem pensar que quanto mais fontes de inteligência de ameaças conseguirem integrar, melhor será a visibilidade obtida. Isso pode ser verdade em alguns casos, como quando se trata de fontes altamente confiáveis, incluindo as comerciais, que fornecem inteligência de ameaças adaptada ao perfil de ameaças específico da organização. Caso contrário, existe o risco significativo de sobrecarregar suas operações de segurança com informação irrelevante.

A sobreposição de informação fornecidas por fornecedores especializados de inteligência de ameaças pode ser muito pequena. Como suas fontes de inteligência e métodos de coleta variam, os insights que eles fornecem serão únicos em alguns aspectos. Por exemplo, um fornecedor, por ter uma presença significativa numa região específica, fornece mais detalhes sobre ameaças provenientes dessa região, enquanto outro fornece mais detalhes sobre tipos de ameaças específicos. Por isso, ter acesso a ambas as fontes pode ser vantajoso. Quando utilizadas em conjunto, podem ajudar a revelar um contexto geral e a orientar missões de busca de ameaças e resposta a incidentes mais eficazes. No entanto, lembre-se que esses tipos de fontes fidedignas também necessitam de uma avaliação prévia cuidadosa para assegurar que a inteligência fornecida é adequada às necessidades e casos de uso específicos da sua organização, como operações de segurança, resposta a incidentes, gerenciamento de risco, gerenciamento de vulnerabilidades, Red Teaming, etc.

Questões a serem consideradas ao avaliar as ofertas de inteligência de ameaças comerciais

Ainda não existem critérios comuns para avaliar diferentes ofertas de inteligência de ameaças, mas apresentamos aqui algumas coisas a serem lembradas ao fazê-lo:

Supõe-se que sua empresa já tem alguns controles de segurança implementados, com os processos associados definidos, e que você considera importante usar inteligência de ameaças com as ferramentas que já utiliza e conhece. Por isso, procure métodos de fornecimento, mecanismos de integração e formatos que suportem uma integração simples de inteligência de ameaças nas suas operações de segurança existentes.

Procurar inteligência com alcance global. Os ataques não têm fronteiras – um ataque direcionado a uma empresa na América Latina pode ser iniciado na Europa e vice-versa. O fornecedor tem fontes de informação globais e agrupa atividades aparentemente desconexas em campanhas coesas? Esse tipo de inteligência vai ajudar você a tomar medidas apropriadas.

O contexto cria inteligência a partir de dados. Indicadores de ameaças sem contexto não têm valor. Você deve procurar fornecedores que o ajudem a responder às perguntas importantes do tipo: "por que isso importa?" O contexto de relacionamento (por exemplo, domínios associados aos endereços IP ou URLs de onde o arquivo específico foi baixado, etc.) fornece valor adicional, impulsionando a investigação de incidentes e apoiando um melhor escopo de incidentes através da descoberta de Indicadores de Comprometimento relacionados recém-adquiridos na rede.

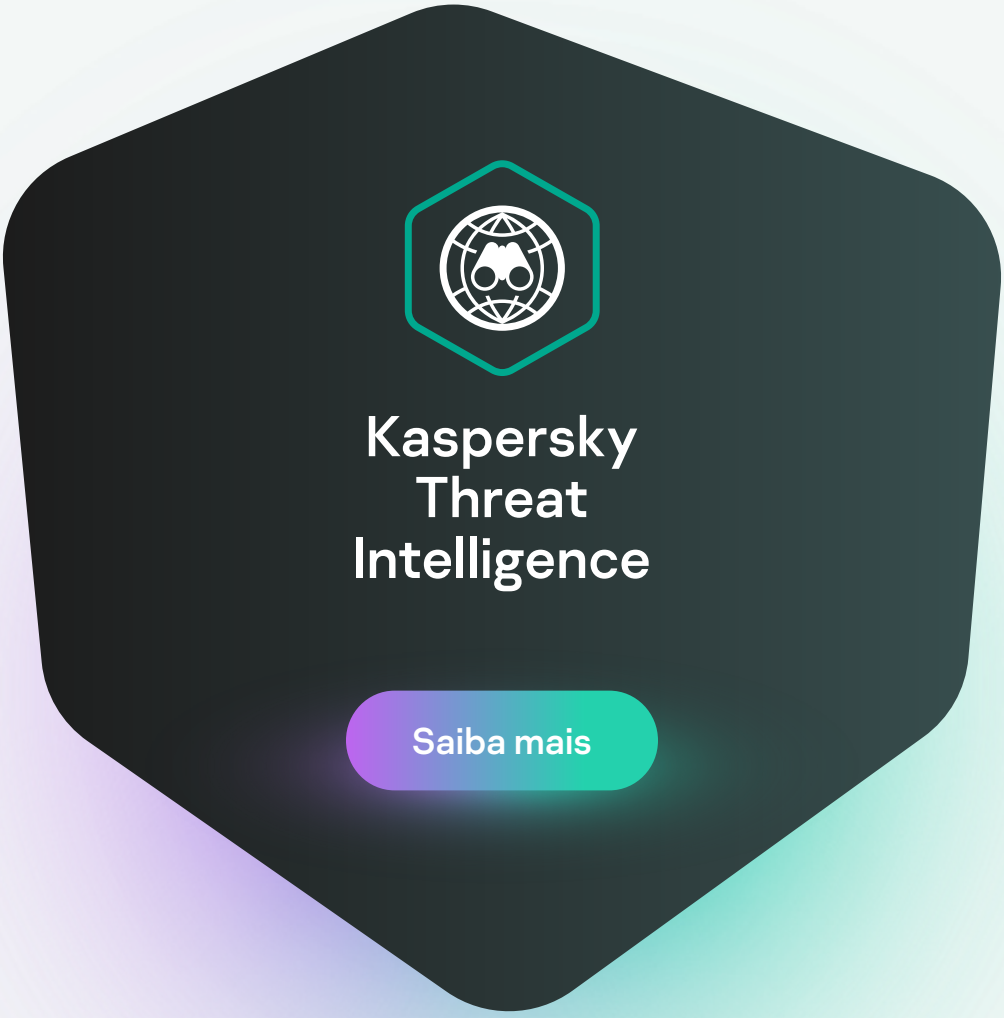
Se procura conteúdo mais estratégico para informar seu planejamento de segurança a longo prazo, como:

- Visão de alto nível das tendências de ataque
- Técnicas e métodos utilizados pelos invasores
- Motivações
- Atribuições, etc.,

então, procure um fornecedor de inteligência de ameaças com um histórico comprovado de descoberta e investigação de ameaças complexas na sua região ou indústria. A capacidade do fornecedor de adaptar seus recursos de investigação às especificidades da sua empresa também é fundamental.

Conclusão

Na Kaspersky, nos concentramos na pesquisa de ameaças há mais de duas décadas. Com petabytes de dados avançados de ameaças para explorar, tecnologias avançadas de machine-learning e um grupo exclusivo de especialistas globais, trabalhamos para apoiar você com a mais recente inteligência de ameaças de todo o mundo, ajudando a manter você imune até a ciberataques nunca vistos.



www.kaspersky.com.br