Mitos sobre a resposta a incidentes

Vamos dar um passo atrás e examinar alguns dos mitos em torno da crescente área de preocupação com a segurança corporativa.

Mito nº 2

A resposta está na contenção das ameaças

Mito Também conhecida como armadilha de pensar a curto prazo. Mais especificamente, a resposta a incidentes está relacionada ao gerenciamento das consequências de uma violação de segurança, incluindo o constante combate a incêndios que arruínam a vida de muitos especialistas em segurança de TI. Infelizmente, o escopo de "consequências" é frequentemente subestimado. Entre outras coisas, ele pode incluir uma investigação mais profunda e uma reconstrução completa da linha de tempo e da lógica de um incidente.

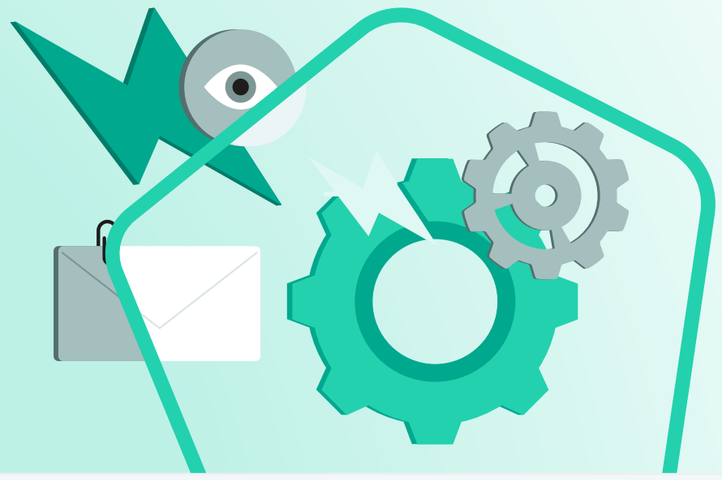
Em vez disso **Não tenha pressa de voltar ao descanso depois de corrigir os danos causados por um incidente. Investigue mais para desenvolver uma compreensão mais profunda da causa básica, de modo que incidentes semelhantes possam ser evitados no futuro com um mínimo de preocupação.**

Mito nº 4

Os serviços de resposta a incidentes são uma proposição do tipo ou isso ou aquilo

Mito Em vez de definir que a pergunta sobre de terceirização da resposta a incidentes deve ser "fazemos isso internamente OU contratamos um suporte externo?", considere usar uma abordagem mista. Sua equipe interna é composta pelos especialistas mais importantes nesta situação, e isso não muda quando você contrata serviços externos de resposta a incidentes.

Em vez disso **Procure por serviços de resposta a incidentes que aumentem os esforços gerais de sua equipe interna. Nesse sentido, os serviços de resposta a incidentes devem ser compreendidos como uma das muitas ferramentas vitais que seus especialistas podem utilizar na defesa contra incidentes complexos.**



Mito nº 1

Qualquer correção é melhor do que nada

Mito Conhecida também como "não fique aí parado, faça alguma coisa!". Esse mito é parcialmente verdadeiro, mas somente se presumirmos que "qualquer correção" resulte em algum nível de solução. Mas analisar um alerta individual abordando cada fragmento do incidente é ineficaz. Muitas equipes não têm uma abordagem sistêmica geral para a resposta a incidentes e, por isso, perdem a oportunidade de tirar o máximo proveito do seu talento interno.

Em vez disso **Crie uma abordagem mais holística de cibersegurança para que você possa responder de modo rápido e eficaz, sem sacrificar um em detrimento do outro. Desenvolva uma abordagem sistêmica de longo prazo para uma resposta a incidentes compreensiva que leve o futuro em consideração, assim como a ameaça presente no momento.**

Mito nº 3

O sucesso pode ser medido pelo número de incidentes solucionados

Mito A segurança de TI no século 21 é uma atividade emocionante, de alto risco e cheia de suspense, com as equipes de especialistas responsáveis perante diversas partes interessadas, incluindo CEOs, acionistas e agências reguladoras. É também um campo altamente complexo e de elite e, por isso, não é nenhuma surpresa que os especialistas em segurança de TI frequentemente medem a eficácia em termos de "contagem de mortes" de incidentes cibernéticos.

Em vez disso **Meça o valor dos processos de resposta a incidentes usando as métricas de Tempo médio até a detecção e Tempo médio de resposta (MTTD/MTTR), e leve em conta métricas mais amplas, como economia de custos e nível de prevenção de danos (à reputação e operacional).**

Mito nº 5

Se precisa de serviços de resposta a incidentes, você deve estar fazendo algo errado

Mito Isso pode ter sido verdadeiro para organizações muito grandes com segurança de TI madura duas décadas atrás, mas está longe de ser verdade hoje, devido ao horizonte de ameaças complexas, à necessidade de inteligência global de ameaças e à necessidade de aproveitar o ecossistema de cibersegurança mais amplo.

Em vez disso **Estimule o poder da cibersegurança de sua equipe com tecnologia líder do setor, colocando-a em uma posição melhor para conduzir seus próprios processos de resposta a incidentes e, ao mesmo tempo, fortalecendo-a com especialistas externos quando necessário.**

A Kaspersky entende os desafios envolvidos na defesa contra APTs e ataques complexos. O Kaspersky Expert Security permite que sua equipe tenha menos trabalho com as ameaças sofisticadas e os ataques do tipo APT, atendendo aos desafios de discrição, persistência, silos e talento. Ele foi projetado e criado em torno da plataforma de XDR e apresenta recursos que aumentam os superpoderes da equipe interna de segurança de TI, incluindo inteligência de ameaças compreensiva, treinamento e orientação de especialistas.

go.kaspersky.com/pt_br_expert

kaspersky