SOPHOS
Cybersecurity delivered.

Quatro grandes dicas de peritos em resposta a incidentes

Saiba antecipadamente como responder a um ataque cibernético crítico

Responder a um incidente cibernético crítico pode ser extremamente estressante e desgastante. Ainda que nada possa aliviar por completo a pressão de lidar com um ataque, entender essas dicas de nossos peritos em respostas ajudará a sua equipe a romper barreiras para defender a sua organização.

O documento destaca as lições que todos deveríamos saber quando se trata de responder a incidentes de segurança cibernética. Elas se baseiam em experiências reais vivenciadas pelas equipes Sophos Managed Detection and Response e Sophos Rapid Response, que coletivamente já responderam a milhares de incidentes de segurança cibernética.

Dica 1: Reaja com extrema rapidez

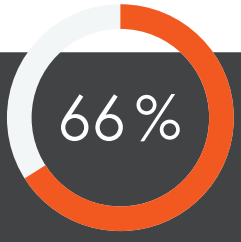
Quando uma organização está sob ataque, cada segundo conta.

São poucos os motivos que justificam a demora de reação das equipes. O mais comum deles é não perceberem a gravidade da situação em que se encontram – e a falta de entendimento leva à falta de percepção da urgência do momento.

Os ataques costumam chegar nos momentos mais inoportunos: férias, fins de semana e no meio da noite. Como a maioria das equipes de resposta a incidentes tem falta de pessoal, é fácil entender a atitude do "amanhã a gente resolve". Mas, infelizmente, amanhã pode ser tarde demais para tentar minimizar o impacto do ataque.

A sobrecarga faz com que reajam mais lentamente aos indicadores de ataque porque a exaustão das equipes afeta seu tempo de reação aos alertas, e é assim que os sinais se perdem nos ruídos. Mesmo no momento em que o caso é aberto, pode acontecer de ele ser priorizado incorretamente devido à falta de visibilidade e contexto. Isso custa tempo – e o tempo não está a favor das equipes de defesa quando se trata de responder a incidentes.

Até mesmo nas situações em que a equipe de segurança está ciente de estar sob ataque e sabe que algo precisa ser feito de imediato, pode ser que eles não tenham experiência para saber o que fazer a seguir, e isso também desacelera o tempo de resposta. A melhor forma de combater esse tipo de situação é se planejar para enfrentar os desafios.



Quase dois terços das organizações foram atingidas por ransomware no último ano, e os invasores tiveram êxito na criptografia dos dados em 65% dos casos.[1]

Dica 2: Não cante vitória antes da hora

Quando se trata de responder a um incidente, não basta apenas tratar dos sintomas, é importante tratar da doença também.

Quando uma ameaça é detectada, a primeira coisa a fazer é a triagem do ataque imediato, que pode ser eliminar o executável de um ransomware ou cavalo de Troia bancário ou bloquear a exfiltração de dados, por exemplo. Contudo, grande parte das vezes, as equipes interrompem o ataque inicial sem se darem conta de que não solucionaram a causa primária.

A remoção bem-sucedida de um malware para eliminar um alerta não significa que o invasor foi extirpado do ambiente. É possível ainda que aquilo que você detectou tenha sido apenas um "teste" do invasor para constatar quais defesas encontrará. Se o invasor ainda tiver acesso, certamente atacará novamente, mas de maneira mais destrutiva.

As equipes de resposta a incidentes precisam garantir que chegarão à causa primária do incidente original que interpelaram. O invasor ainda mantém uma base operacional no ambiente? Há planos de uma segunda onda de ataques? Os operadores de resposta a incidentes que já corrigiram milhares de ataques sabem quando e onde investigar mais a fundo. Eles procuram por outras coisas que os invasores estejam fazendo, fizeram ou planejam fazer na rede – e neutralizam isso também.

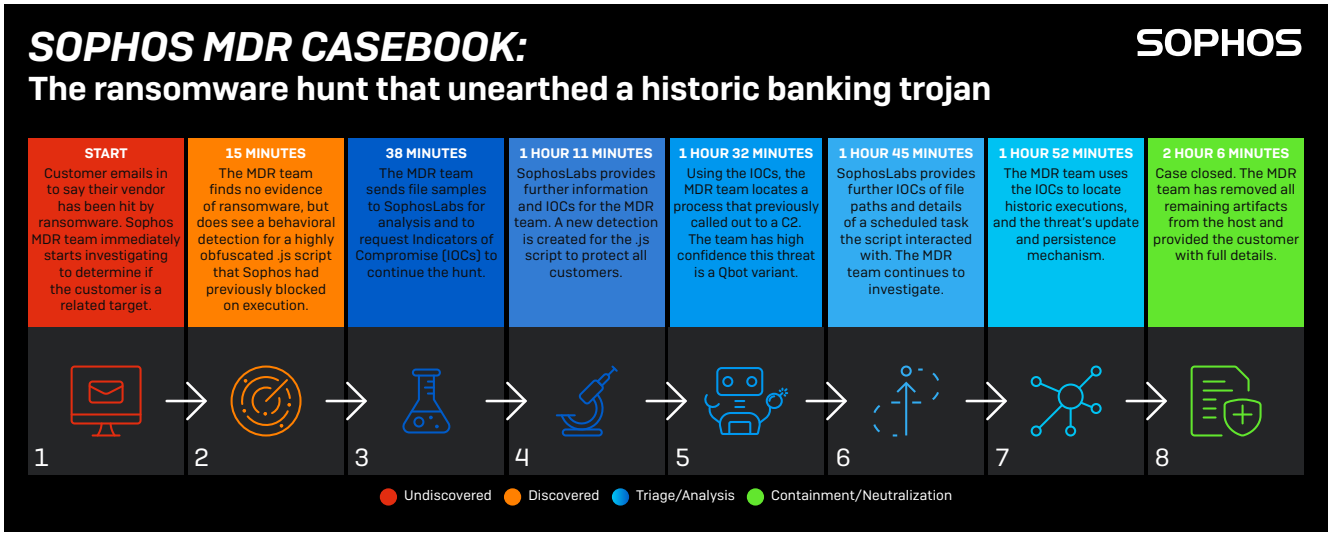
Por exemplo, houve uma situação em que os especialistas em resposta a incidentes da Sophos foram capazes de frustrar um ataque que durou nove dias e três tentativas separadas de atingir uma organização com um ransomware.

Como não eram ainda um cliente Sophos MDR, a equipe do Sophos Rapid Response foi a primeira a arregaçar as mangas.

Na primeira onda de ataques (que foi bloqueada pela solução de proteção de endpoint da organização), os invasores tiveram sob sua mira 700 computadores com o ransomware Maze e uma demanda de resgate de US$ 15 milhões. Sabendo que estavam sob ataque, o pessoal da segurança empregou habilidades avançadas de resposta a incidentes da equipe do Sophos Managed Detection and Response (MDR).

Os especialistas de resposta a incidentes da Sophos identificaram rapidamente a conta administrativa que foi comprometida e removeram vários arquivos mal-intencionados e bloquearam as comunicações de comandos de ataque e de C2 (comando e controle). A equipe Sophos MDR foi capaz de interceder contra duas ondas de ataques pelo adversário. Se os invasores tivessem tido sucesso e a vítima tivesse feito o pagamento, esse teria sido um dos resgates de ransomware mais altos até hoje.

Em outro exemplo, a equipe Sophos MDR respondeu a uma possível ameaça de ransomware, mas logo se deu conta de que não havia indícios de ransomware. Nesse ponto, muitas equipes talvez fechassem o caso e o dessem por encerrado. Contudo, a equipe Sophos MDR continuou investigando e descobriu um cavalo de Troia histórico. Felizmente, para o cliente, a ameaça nunca mais ficou ativa, e isso serviu de lição sobre a importância de olhar além dos sintomas iniciais na intenção de determinar a causa primária em sua totalidade, pois isso poderia ser um indicador de um ataque maior.



Dica 3: Visibilidade completa é essencial

Enquanto navega por um ataque, nada dificulta mais a defesa de uma organização do que voar às cegas. É importante ter acesso a dados de alta qualidade, o que possibilita uma identificação precisa dos possíveis indicadores do ataque para determinar a causa primária.

Equipes eficientes coletam os dados certos para ver os sinais, separá-los dos ruídos e distinguir quais sinais são os mais importantes a priorizar.

Coletando sinais

A visibilidade limitada de um ambiente é um modo infalível de deixar passar ataques de risco. Por anos, muitas ferramentas de big data despontaram no mercado para tentar solucionar esse desafio específico. Algumas trabalham com dados centrados em eventos, como logs; outras utilizam dados centrados em ameaças, e outras apostam em uma abordagem híbrida. Em qualquer uma dessas abordagens, o objetivo é o mesmo: coletar dados suficientes para gerar insights significativos a fim de investigar e responder a ataques que, do contrário, teriam passado despercebidos.

Coletar os dados certos e de alta qualidade de uma grande variedade de fontes garante total visibilidade das ferramentas, táticas e procedimentos (TTP) utilizados pelo invasor. Do contrário, seria como se apenas uma parte do ataque fosse vista.

Reduzindo ruídos

Com medo de não obterem os dados de que necessitam para traçar a imagem completa de um ataque, algumas organizações (e as ferramentas de segurança com que trabalham) coletam tudo. Porém, isso não ajuda a encontrar a agulha no palheiro – na verdade, só estão colocando mais palha no palheiro. Isso não apenas aumenta o custo de coleta e armazenamento de dados, mas também cria muito mais ruído, o que leva à exaustão de alertas e ao desperdício de tempo perseguindo falsos positivos.

Aplicando contexto

Existe um ditado entre os profissionais de detecção e resposta a ameaças que diz: "Conteúdo é rei, mas o contexto é a rainha". Os dois são necessários para executar um programa eficiente de resposta a incidentes. Aplicar metadados significativos associados a sinais permite que os analistas determinem se tais sinais são malignos ou benignos.

Um dos componentes mais críticos da detecção e resposta eficiente a ameaças é priorizar os sinais que mais interessam. A melhor maneira de selecionar os alertas que realmente importam é combinando o contexto oferecido pelas ferramentas de segurança (ou seja, soluções de resposta e detecção de endpoint), inteligência artificial, inteligência de ameaças e a base de conhecimentos dos operadores humanos.

O contexto ajuda a distinguir o ponto onde um sinal se originou, o estágio atual do ataque, os eventos relacionados e o potencial de impacto nos negócios.

Dica 4: Se precisar, peça ajuda

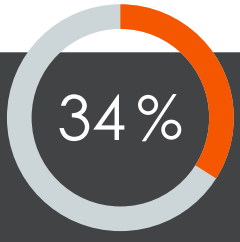
Nenhuma organização quer lidar com tentativas de violação. Contudo, não existe substituto para a experiência quando se trata de responder a incidentes, o que significa que as equipes de TI e segurança, geralmente incumbidas de responder a incidentes intensos para os quais não têm preparo para lidar, são postas frente a frente com situações que muitas vezes têm um impacto colossal nos negócios.

A falta de recursos humanos capacitados para investigar e responder a incidentes é um dos maiores problemas que o setor de segurança cibernética enfrenta atualmente. Esse problema é tão grande que, de acordo com a ESG Research2, "34% dizem que seus desafios maiores são a falta de pessoal capacitado para investigar um incidente de segurança virtual envolvendo um endpoint para determinar a causa primária e a sequência de ataque".

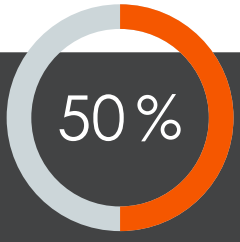
Esse dilema deu vez a uma nova alternativa: os serviços de segurança gerenciada. Mais especificamente, os serviços de detecção e resposta gerenciada (MDR). Os serviços MDR são operações de segurança terceirizadas fornecidas por uma equipe de especialistas que atuam como uma extensão da equipe de segurança do cliente. Esses serviços combinam investigações conduzidas por humanos, caça a ameaças, monitoramento em tempo real e resposta a incidentes com abundância tecnológica para coleta e análise de inteligência. De acordo com a Gartner, "até 2025, 50% das organizações usarão serviços MDR"3, o que mostra a tendência de que as organizações estão se dando conta de que precisarão de ajuda para executar um programa completo de operações de segurança e resposta a incidentes.

Para as organizações que ainda não empregam um serviço MDR e que estão em meio a um ataque ativo, os serviços especializados de resposta a incidentes são uma excelente opção. As equipes de resposta são inseridas no cenário quando a equipe de segurança está sobrecarregada e precisa de peritos externos para a triagem do ataque e para garantir que o adversário seja neutralizado.

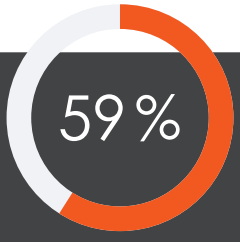
Mesmo as organizações com equipes de analistas de segurança altamente treinados podem se beneficiar da colaboração de um serviço de resposta a incidentes para tapar as lacunas em cobertura (noites, fins de semana e feriados, por exemplo) e especialização necessária para responder aos incidentes.



De acordo com a firma de pesquisa e análises ESG, "34% das organizações dizem que seus desafios maiores são a falta de pessoal capacitado para investigar um incidente de segurança virtual envolvendo um endpoint para determinar a causa primária e a sequência de ataque".[2]



Até 2025, 50% das organizações usarão serviços MDR (acima dos menos de 5% de 2019).[3]



Em uma pesquisa de 2022 com 5.600 profissionais de TI, 59% disseram que a complexidade dos ataques a suas organizações aumentou em comparação ao ano anterior.[4]

Como a Sophos pode ajudar

Serviço Sophos Managed Detection and Response (MDR)

Preocupado com a capacidade de resposta da sua organização a incidentes graves? Nesse caso, o serviço Sophos Managed Detection and Response (MDR) é uma opção que merece atenção.

O Sophos MDR oferece busca, detecção e resposta a ameaças, 24 horas por dia, sete dias por semana, ditadas por um time de especialistas como um serviço totalmente gerenciado. Indo além da simples notificação sobre ataques ou comportamentos suspeitos, a equipe de MDR da Sophos age de modo determinado para neutralizar ameaças complexas e ultrassofisticadas para você. Se ocorrer um incidente, a equipe MDR iniciará ações remotas para interromper, conter e neutralizar a ameaça. A equipe de peritos em operações de segurança oferece conselhos práticos para tratar das causas primárias dos incidentes recorrentes.

Saiba mais em www.sophos.com/mdr

Serviço Sophos Rapid Response

Se a sua organização está sob ataque e precisa de assistência imediata para responder ao incidente, a Sophos pode ajudar.

Entregue por uma equipe especializada de resposta a incidentes, o Sophos Rapid Response oferece assistência imediata à organização com identificação e neutralização de ameaças ativas. A integração é iniciada em horas, e a maioria dos clientes é averiguada em 48 horas. O serviço está disponível para os clientes Sophos existentes e para aqueles que não trabalham com a Sophos.

A equipe remota de resposta a incidentes do Sophos Rapid Response entra em ação rapidamente para fazer a triagem, contenção e neutralização de ameaças ativas. Os adversários são extirpados do seu patrimônio para prevenir danos maiores a seus ativos.

Saiba mais em www.sophos.com/rapidresponse

Sophos XDR

O Sophos XDR é a única solução XDR da indústria que sincroniza a segurança nativa de endpoint, servidor, firewall, e-mail, nuvem e M365. Veja um quadro holístico do ambiente da sua organização com um rico conjunto de dados e uma análise profunda para detecção, investigação e resposta a equipes de SOC dedicadas e administradores de TI.

Saiba mais e experimente gratuitamente em www.sophos.com/xdr

[1] O Estado do Ransomware 2022 – baseado em uma pesquisa independente com 5.600 gerentes de TI em 31 países: https://www.sophos.com/pt-br/whitepaper/state-of-ransomware
[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1
[3] Gartner, Market Guide for Managed Detection and Response Services, 26 de agosto de 2020. Analistas: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider
[4] O Estado do Ransomware 2022 – baseado em uma pesquisa independente com 5.600 gerentes de TI em 31 países: https://www.sophos.com/pt-br/whitepaper/state-of-ransomware

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

22-08-08 WPPTBR (PC)