SOPHOS

Perguntas técnicas e de vendas – Sophos Emergency Incident Response

Perguntas frequentes externas

Apresentação geral

O que é Emergency Incident Response?
O Sophos Emergency Incident Response está ao seu dispor para quando uma emergência cibernética entra em ação, trabalhando rápido para avaliar, conter, entender e fornecer recomendações para corrigir o problema. Nossa equipe de especialistas interfuncionais aplica anos de experiência e aprendizado adquiridos para fazer a triagem, contenção e neutralização de ameaças ativas com rapidez, eliminar adversários e evitar danos maiores.

O Emergency Incident Response também o ajuda a determinar se a sua organização foi impactada por um incidente, e compreender o escopo do incidente. O serviço oferece uma variedade de atividades investigativas para ajudar a identificar a causa primária dos incidentes, realizar avaliação de comprometimento para determinar se um comportamento observado é malicioso, conduzir atividades de caça e inteligência de ameaça e prestar assistência nas negociações de resgate.

A quem o Emergency Incident Response atende?
A qualquer organização que esteja passando por um incidente de segurança ativo ou que tenha enfrentado um ataque recente e queira aprofundar a investigação ou investigar uma atividade suspeita para estabelecer se representa uma ameaça.

Preciso ser cliente da Sophos para adquirir o Emergency Incident Response?
Não. O Emergency Incident Response está disponível para os clientes Sophos existentes e para aqueles que não trabalham com a Sophos.

Estou enfrentando uma violação ativa. O que devo fazer?
Ligue para o telefone de contato regional abaixo e fale com um dos nossos consultores de incidentes:

- Austrália: +61 272084454
- Áustria: +43 73265575520
- Canadá: +1 7785897255
- França: +33 186539880
- Alemanha: +49 61171186766
- Itália: +39 02 94752 897
- Suíça: +41 445152286
- Reino Unido: +44 1235635329
- EUA: +1 4087461064

Entre em contato conosco por e-mail: EmergencyIR@sophos.com.

O Emergency Incident Response é remoto ou local?
As duas opções estão disponíveis: remoto e local.

Qual é a velocidade do serviço Emergency Incident Response?
A maioria dos clientes leva em torno de duas horas para ser integrada, e a triagem é feita em 48 horas. Como o serviço pode ser realizado totalmente remoto, a resposta pode começar em algumas horas após seu contato inicial com a Sophos.

Perguntas técnicas e de vendas – Sophos Emergency Incident Response

Qual a agilidade de uso do processo de integração?
A equipe do Emergency Incident Response pode começar o processo de integração e dar início às investigações assim que receba a sua aprovação.

Qual é a metodologia do Emergency Incident Response?
Após aceitar o contrato de serviço, realizamos o contato inicial de engajamento por telefone, que também pode ser feito por e-mail se você preferir. A investigação começa assim que os seus objetivos para o engajamento estejam claros.

O Emergency Incident Response inclui diferentes categorias de trabalho que podemos oferecer. Durante a chamada inicial de reconhecimento, trabalhamos lado a lado com você para identificar as categorias necessárias e estimar o número de horas necessárias.

As categorias de foco incluem: Gestão de engajamento, Resposta a incidente, Análise forense digital, Avaliação de comprometimento, Caça a ameaças, Pesquisa e Inteligência de ameaça, Negociação de resgate, Relatório de engajamento, Suporte no local (se aplicável), Comprometimento de e-mail corporativo e Implantação de software.

Em que idiomas o Emergency Incident Response está disponível?
No momento, o serviço está disponível em inglês e japonês. É necessário que você tenha proficiência técnica em inglês ou japonês para interagir.

A Sophos trabalha com os serviços DFIR de análise forense digital e resposta a incidentes ou os substitui?
O Emergency Incident Response é um serviço DFIR (Digital Forensics and Incident Response). Não há necessidade de se engajar com outra empresa de segurança para obter os serviços DFIR, pois o escopo dos serviços entregues pelo Emergency Incident Response também inclui análises forenses digitais.

Preciso instalar a tecnologia Sophos em meus endpoints?
Não, não é preciso. O Emergency Incident Response pode ser entregue usando o Sophos XDR, ou podemos implantar o Sophos XDR Sensor juntamente com a solução incumbente. As duas opções nos permitem investigar o incidente com rapidez.

A equipe do Emergency Incident Response não precisa aguardar pela finalização da implantação para agir na contenção e neutralização da ameaça. A equipe analisará e reutilizará os dados disponíveis e utilizará as ferramentas adequadas para auxiliar na resposta.

Como é feito o cálculo de preço?

A Sophos fará uma estimativa do número de horas necessárias para responder ao incidente com base nas questões levantadas durante a análise de escopo. Você paga apenas pelas horas de uso.

Há custos adicionais?
Se for necessário trabalho no local, os custos da viagem serão faturados para você.

É possível implantar o Emergency Incident Response em apenas um segmento do nosso ambiente, ou o ambiente completo deve ser parte integral do escopo?
Em situações específicas, o Emergency Incident Response pode ser aplicado a um segmento do seu ambiente. Um especialista do Emergency Incident Response pode fornecer mais detalhes como parte do escopo do projeto.

A Sophos pode trabalhar com um representante intermediando minha organização, como uma firma de advocacia, estipulado em contrato?
Sim, pode. É possível trabalhar por meio de um intermediário.

A Sophos é capaz de determinar quais arquivos foram exfiltrados ou roubados no ataque?
O serviço Emergency Incident Response inclui nossos melhores esforços para determinar quais arquivos, se algum, foram exfiltrados como parte de um ataque. Contudo, isso não é garantido, pois dependerá dos dados disponíveis na investigação.

A Sophos fará a descriptografia do ransomware para mim?
Não. Isso não faz parte do serviço Emergency Incident Response.

A Sophos me ajudará a negociar ou intermediará no pagamento do resgate?
O Emergency Incident Response inclui peritos para a negociação de resgate com os agentes de ameaça. Contudo, a Sophos não intermedeia o pagamento do resgate, mas, sim, pode recomendar e trabalhar com terceiros caso necessário para posicionar o Sophos MDR ou Taegis MDR.

2025-06-03 (WP-NP)

SOPHOS