Sophos Rapid Response

Perguntas Frequentes

Preciso ser cliente ativo da Sophos para ser um ciente do serviço Rapid Response?
Não. O serviço Sophos Rapid Response está disponível para os clientes Sophos existentes e para aqueles que não trabalham com a Sophos.

Estou observando uma violação em atividade, o que devo fazer?
Ligue para o telefone de contato regional abaixo e fale com um dos nossos consultores de incidentes.

EUA +1 4087461064

Austrália +61 272084454

Canadá +1 7785897255

França +33 186539880

Alemanha +49 61171186766

Reino Unido +44 1235635329

Suécia +46 858400610

Itália +39 0287317993

Qual a velocidade do serviço Rapid Response?
Muito rápida. A maioria dos clientes é integrada em questão de horas, e a triagem é feita em 48 horas. Como o serviço é totalmente remoto, a resposta pode começar em algumas horas após o contato com a Sophos.

Como é o processo de integração?
A equipe do Rapid Response pode começar o processo de integração e dar início às investigações assim que receba a aprovação. Para as organizações que não tenham o Sophos XDR instalado em seus ambientes, a Sophos oferece a opção Rapid Deployment. A equipe do Rapid Deployment é composta por especialistas em instalação rápida em ambientes que estejam sob um ataque ativo.

Há custos adicionais associados ao Rapid Deployment?
Não. O Rapid Deployment está incluído como parte do serviço.

Qual é a metodologia do Rapid Response?
Após a aprovação do Rapid Response e a aceitação do nosso contrato de serviços pelo cliente, já entramos em ação. São quatro as principais etapas do Rapid Response: integração, triagem, neutralização e monitoramento.

Integração

- Realizar chamada inicial para estabelecer preferências de comunicação e confirmar quais etapas de correção já foram tomadas, se alguma
- Identificar a escala e o impacto do ataque
- Definir plano de resposta mutuamente
- Iniciar implantação do software de serviço

Triagem

- Avaliar o ambiente operacional
- Identificar indicadores de comprometimento conhecidos e atividade adversa
- Realizar a coleta de dados e iniciar atividades de investigação
- Criar plano de colaboração para o início das atividades de resposta

Neutraliza

- Retirar o acesso dos invasores
- Parar danos maiores a informações e dados
- Impedir a exfiltração de mais dados
- Recomenda ações preventivas em tempo real para resolver o problema

SOPHOS

Perguntas Frequentes sobre o Sophos Rapid Response

Monitorar

- Fazer a transição para o serviço MDR Advanced
- Realizar monitoramento contínuo para detectar a recorrência
- Fornecer um resumo da ameaça pós-incidente

Em que idiomas o Rapid Response está disponível?
No momento, o serviço está disponível apenas em inglês.

A Sophos trabalha com serviços DFIR de análise forense e resposta a incidentes ou os substitui?
A Sophos trabalha lado a lado com os serviços DFIR e assim tem feito em múltiplas ocasiões. O Sophos Rapid Response se concentra no aspecto da resposta ao incidente dos serviços DFIR e não fornece todos os serviços oferecidos por um engajamento DFIR tradicional.

A Sophos envia equipamentos físicos? Especialistas em incidentes são deslocados para a localidade do cliente?
Não. Todas as respostas a incidentes são realizadas remotamente.

Os clientes precisam instalar o Sophos em seus endpoints?
Sim. O Rapid Response é entregue usando o agente padrão Managed Detection & Response / Sophos XDR para que possamos garantir monitoramento e resposta eficientes, 24 horas por dia, sete dias por semana. Sendo assim, será necessário que desinstalem ou desativem temporariamente a proteção de endpoint atual que tenham.

A equipe Rapid Response não precisa aguardar pela finalização da implantação para começar a 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?
Os preços são calculados com base no número total de usuários e servidores, fixo por um período de 45 dias.

Há custos adicionais?
Não. Não há nenhum custo extra para o serviço.

O que acontece ao término do período do Rapid Response?
Ao final do período, os clientes podem fazer a transição para a versão completa do Sophos Managed Detection & Response (MDR), do contrário a licença irá expirar.

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

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

A Sophos é capaz de determinar quais arquivos foram exfiltrados/roubados no ataque?
O serviço Rapid 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 descriptografia do ransomware para o cliente?
Não. Isso não faz parte do serviço Rapid Response.

A Sophos ajudará o cliente a negociar ou intermediará no pagamento do resgate?
Não. Isso não faz parte do serviço Rapid Response.

2022-09-14 (FAQ-PC)

SOPHOS