Sophos Rapid Response

Resposta imediata a ameaças ativas

O Sophos Rapid Response oferece assistência imediata à sua organização com a identificação e neutralização de ameaças ativas através de uma equipe especializada de resposta a incidentes.

Durante um ataque, cada segundo conta

Ao responder a uma ameaça ativa, é imperativo que o tempo entre o indicador inicial de comprometimento e a mitigação total da ameaça seja o menor possível. Conforme seu adversário avança pela estrutura kill chain, começa a corrida contra o tempo para garantir que ele não seja capaz de atingir seus objetivos.

Com o Sophos Rapid Response, conseguimos tirar você da zona de perigo rapidamente com a nossa equipe remota 24/7 de caçadores de ameaças, analistas e defensores que:

- Age rapidamente na triagem, contenção e neutralização de ameaças ativas
- Ejeta os adversários do seu patrimônio para prevenir danos maiores a seus ativos
- Realiza monitoramento e resposta contínuos 24/7 para aprimorar a sua proteção
- Recomenda ações preventivas em tempo real para tratar da causa primária
- Implanta rapidamente um armamento tecnológico baseado na nuvem da Sophos a todo o seu patrimônio
- Analisa dados suplementares de tecnologias de terceiros
- Oferece um resumo detalhado da ameaça pós-incidente que descreve nossa investigação

Destaques

- Identificação e neutralização rápida de ameaças ativas
- Resposta a incidentes e monitoramento 24/7 por 45 dias
- Ponto de contato e resposta dedicado
- Resumo da ameaça pós-incidente detalhando todas as ações tomadas
- Preço previsível com custos fixos e sem taxas extras
- Projetado para reembolso da seguradora
- Transição descomplicada para uma assinatura com o Sophos Managed Detection and Response (MDR) após o Sophos Rapid Response

Recursos do Sophos Rapid Response

O Sophos Rapid Response inclui todos os benefícios do Sophos MDR Complete, além de vários outros benefícios adicionais.

	Sophos Rapid Response
MDR Complete no modo de resposta a ameaças "Autorizar"	✓
Monitoramento, busca e resposta a ameaças 24/7	✓
Líder de resposta dedicado durante a ameaça ativa e acesso a chamada direta	✓
Análise de dados suplementares de tecnologias de terceiros	✓
Orçamento expresso e ativação da conta no mesmo dia	✓
Resumo da ameaça pós-incidente formal detalhando a investigação	✓

SOPHOS

Neutralização de ameaça ativa

A equipe do Sophos Rapid Response é especializada na neutralização de ameaças ativas. Seja uma infecção, um comprometimento ou um acesso não autorizado a seus ativos que esteja tentando burlar os seus controles de segurança, nós já vimos de tudo e paramos tudo.

Nossa equipe de peritos em resposta a incidentes é parte do Sophos Managed Detection and Response (MDR), nosso serviço 24/7 de caça, detecção e resposta a ameaças que sai no encalço, identifica, investiga e responde a ameaças proativamente em nome de nossos clientes como parte de um serviço totalmente gerenciado.

Incentivos alinhados

Os serviços IR convencionais de resposta a incidentes são cobrados por hora, o que pode deixá-lo vulnerável ao subestimar o tempo necessário para mitigar completamente uma ameaça. Isso fará com que você precise adquirir mais horas, ou, pior ainda, isso pode encorajar o serviço IR convencional a maximizar o número de horas que demoram para responder ao incidente.

O Sophos Rapid Response oferece um modelo de preços com taxa fixa, sem custos ocultos, determinado pelo número de usuários e servidores do seu patrimônio. Ele é oferecido remotamente, de modo que podemos iniciar as ações de resposta no mesmo dia da aquisição. O interesse é nosso, e seu, de sair da zona de perigo o mais rápido possível, pois o tempo nunca é um fator no custo.

Implantação Rapid

Para garantir a resposta mais rápida possível, o processo de implantação do Sophos Rapid tem foco direto na distribuição imediata dos agentes Sophos MDR para endpoints e servidores detectáveis.

Após desenvolver uma estratégia de substituição usando utilitários de remoção para substituir produtos existentes, uma equipe remota de engenheiros de implantação conversa com cada cliente do Rapid Response para estabelecer um plano de ação personalizado, aproveitando as ferramentas de automação para a implantação em massa em toda a rede.

A equipe trabalha em colaboração para otimizar o status de integridade do agente Sophos MDR em toda a rede, garantindo as configurações recomendadas para uma investigação acelerada.

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
- Recomendar ações preventivas em tempo real para tratar da causa raiz

Monitorar

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

Documento detalhado da ameaça

Assim que tivermos neutralizado a ameaça ativa contra a sua organização, entregaremos a você um resumo formal da nossa investigação, detalhando as ações que tomamos, as descobertas que fizemos, bem como oferecendo orientação e recomendações sobre como mitigar a recorrência de ameaças semelhantes no futuro.

Monitoramento e resposta pós-incidente 24 horas diárias

No momento em que o incidente é resolvido e a ameaça imediata à sua organização é neutralizada, fazemos a transição para o nosso serviço Sophos MDR de nível superior, o Sophos MDR Complete, para oferecer captura, investigação, detecção e resposta ininterruptas a ameaças.

Caso a ameaça retorne ou se uma nova ameaça surgir, estaremos prontos para responder sem custos adicionais para você. Se você ficar sob ataque por 45 dias, nós o defenderemos por 45 dias durante a vigência da sua assinatura.

Enfrentando uma violação ativa?

Ligue para o telefone de contato regional abaixo e fale com um dos nossos consultores de incidentes.

Austrália +61 272084454

Canadá +1 7785897255

França +33 186539880

Alemanha +49 61171186766

Itália +39 02 873 17993

Reino Unido +44 1235635329

EUA +1 4087461064

Suécia +46 858400610

Se todos os consultores estiverem ocupados, deixe uma mensagem e alguém entrará em contato com você o mais rápido possível.

Enfrentando uma violação ativa?

Para obter mais informações, acesse sophos.com/rapidresponse

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

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

22-05-12 DS-PTBR (DD)

SOPHOS