Folheto de soluções

Sophos Emergency Incident Response

Assistência completa a serviços — da investigação até a recuperação

Resposta imediata a ameaças ativas

Cada segundo conta quando sua empresa está sob ataque. Quando acontece um incidente, você precisa de velocidade, eficiência, habilidades interdisciplinares em segurança e expertise. Você também precisa de visibilidade e conhecimento do cenário global de evolução da ameaça e das mais recentes táticas e técnicas do agente de ameaça.

O Sophos Emergency Incident Response está ao seu dispor para quando uma emergência cibernética entra em ação, trabalhando rápido para avaliar, conter, entender e 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. A Sophos se respalda nas lições aprendidas de milhares de engajamentos realizados para direcionar melhorias recomendadas e ações preventivas que não apenas tratam da causa primária do incidente, mas que ajudam a aumentar a sua resiliência contra futuras investidas.

Reforça suas defesas e a postura de segurança proativamente

O Sophos Emergency Incident Response emprega uma abordagem de colaboração interativa, trabalhando com a sua equipe para avaliar rapidamente a situação, conter e eliminar a ameaça conforme necessário e fornecer diretrizes acionáveis de recuperação. Nossa equipe oferece análise forense digital e de malware, caça a ameaça e inteligência de ameaça das equipes de pesquisas Sophos X-Ops e Counter Threat Unit para localizar e eliminar as ameaças. Trabalhamos com especialistas interdisciplinares, como profissionais de pentest e pesquisadores, para garantir a mitigação total do risco e a recuperação.

Detectar e investigar

Contato inicial e investigação

Para garantir a resposta mais rápida possível, a Sophos foca diretamente na distribuição imediata de agentes a ativos detectáveis. A assistência remota para resposta a incidentes permite a captura de dados forenses para embasar à análise inicial, desenvolver ações de contenção apropriadas e determinar a necessidade de tecnologias adicionais para expandir rapidamente a visibilidade por todo o processo de engajamento.

Benefícios aos clientes

- Aumenta a sua equipe com recursos interfuncionais de análise forense digital e resposta a incidentes, e expertise.
- Diminui o impacto de um incidente e o risco de recorrência com o entendimento completo da ameaça.
- Expande a visibilidade, reúne fatos e define respostas rápidas para definir as ações certas.

Investigação profunda

Captura de dados: ativos, serviços afetados, impacto nos negócios e outros vetores de ataque.

Processo forense iterativo e análise de ameaças: pesquisadores, caçadores, testadores e analistas ajudam a entender completamente a ameaça.

Plano de remediação: planejamento inicial para remediação, em paralelo e dando seguimento à investigação.

Redução da superfície de ataque: a Sophos fornece insights interativos sobre o agente de ameaça para validar controles e identificar pontos de reentrada, gerando uma mitigação de risco mais abrangente.

Negociação de resgate: negociadores experientes utilizam-se do conhecimento profundo dos agentes de ameaças de ransomware para facilitar as negociações e oferecer diretrizes para que a recuperação dos dados das mãos dos agentes de ransomware seja feita de forma segura e economicamente viável.

Remediação

Garantir e validar

Fortalecimento focado da segurança: a equipe IR indica e dá suporte aos esforços voltados ao fortalecimento tático do controle de segurança que evita a reentrada do agente de ameaça.

Contenção: dar fim às tentativas de ataques de comando e controle.

Remoção do agente de ameaça: exterminar o adversário em uma rede autônoma exige a eliminação orquestrada de seus artefatos e a reprogramação dos domínios comprometidos.

Recuperar

Recuperação de dados e sistemas: para ajudar a reconstruir sistemas, higienizar dados e recolocar os sistemas em operação, a equipe Sophos IR trabalha com parceiros confiáveis que fornecem serviços de recuperação de modo seguro e imperceptível.

Validação do host: usando nossa tecnologia de agente — e que desponta como líder do setor — ajudamos a garantir que os hosts restaurados estejam prontos para produção.

Acompanhamento

Melhorar

A Sophos reúne um arsenal de aprendizados compilados dos milhares de engajamentos vivenciados e as ações adotadas para levar melhorias ao processo de respostas recomendadas, bem como recomendações estratégicas para ajudar a encaminhar a transformação em segurança. No fim de um engajamento, entregamos a você um relatório formal do incidente da nossa investigação, detalhando as ações que tomamos, as descobertas que fizemos, bem como oferecendo recomendações sobre como mitigar a recorrência de ameaças semelhantes no futuro.

Recursos do serviço

- Identificação e neutralização rápida de ameaças ativas.
- Implantação rápida de tecnologias.
- Captura e análise de dados forenses digitais para identificar indicadores de comprometimento e rastrear a atividade adversária.
- Caça a ameaças para identificar uma atividade relacionada do agente de ameaça.
- Recurso remoto e local para consultoria, direcionamento e diretrizes de comando do incidente.
- Equipe global de profissionais de resposta a incidentes experientes e credenciados, com experiência em cenários cibernéticos comuns e também não muito comuns.
- Insights e inteligência de ameaça específica ao incidente aplicados aos artefatos operacionais do adversário.
- Perito em negociação de resgate.
- Relatório pós-incidentes detalhando as ações adotadas, as descobertas e as recomendações.

Por que usar a Sophos para responder a incidentes?

A Sophos coloca em ação sua extensa experiência em cada engajamento de emergência de segurança cibernética. Oferecemos assistência completa para os serviços de resposta a incidentes a uma diversidade de organizações que atendem diferentes mercados e enfrentam qualquer tipo de incidente — desde uma simples preocupação com um sistema comprometido até situações de crise que impedem o andamento das operações comerciais.

Nossa equipe de resposta a incidentes conta com profissionais experientes que combinam especializações em áreas administradas pelo governo, departamento militar, equipes de resposta a incidentes Computer Security Incident Response Teams (CSIRTs), autoridades legais e agências de inteligência governamental. Esses profissionais combinam sua experiência prática nas principais interpelações de segurança cibernética com a resposta a incidentes da equipe da linha de frente, a inteligência de ameaça do nosso serviço X-Ops e das equipes de pesquisa da Counter Threat Unit, as descobertas feitas em testes de segurança e engajamentos de avaliação, e as análises de dados de segurança para acelerar as investigações e recompor-se com confiança.

Enfrentando uma violação ativa?

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

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

E-mail: EmergencyIR@sophos.com

Para saber mais, visite

sophos.com/emergency-response

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

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

2025-06-04 BRPTBR (MP)

SOPHOS