Sophos Compromise Assessment

Descubra indícios de violações antes que elas possam impactar os seus negócios

No ano passado, as empresas gastaram uma média de 37 dias e US$ 2,4 milhões para encontrar brechas na segurança e restaurar sistemas. Mas agora, com a perícia em resposta a incidentes de nossos especialistas, oferecemos o Sophos Compromise Assessment, o meio mais rápido e eficiente de identificar atividades passadas e ativas de invasores em seus ambientes que permite à sua organização tomar decisões rápidas e decisivas.

Identifique atividades ativas ou recentes de um invasor

Fornecido por uma equipe de profissionais especializados em ameaças e resposta a incidentes, o Sophos Compromise Assessment identifica rapidamente se um invasor transpôs suas defesas, quantifica a intensidade do risco para a organização e fornece diretrizes detalhadas das ações necessárias para eliminar a ameaça.

A grande experiência em resposta às mais avançadas ameaças permite que a equipe de resposta a incidentes do Sophos Incident Response (IR) Services identifique indicadores de comprometimento (IoC) por meio de uma investigação direcionada a recursos e máquinas com o potencial de estarem comprometidos. O resultado é uma avaliação rápida e completa que ajuda a sua organização a gerenciar riscos e conformidades enquanto mantém a eficiência operacional.

Metodologia do Sophos Compromise Assessment

A equipe do Sophos IR Services se mantém em comunicação direta com a sua organização durante todas as fases de avaliação do Compromise Assessment, proporcionando esclarecimentos sobre a ameaça, risco de exposição e ações a serem tomadas para resolver o incidente e tratar da sua causa primária.

1. **Chamada de coordenação inicial** – a avaliação começa com a troca eficiente de informações sobre o potencial da ameaça, a identificação dos principais pontos de contato e a confirmação do escopo de implantação e do processo de investigação a ser seguido.
2. **Implantação de ferramentas de investigação** – uma instalação guiada pela plataforma premiada da Sophos e entregue via nuvem garante que os dados nos dispositivos designados sejam capturados imediatamente, permitindo que a equipe do Sophos IR Services realize uma avaliação completa da integridade do dispositivo.
3. **Investigação de ameaça e avaliação de risco** – se for confirmada uma ameaça ativa, a equipe do Sophos IR Services acionará uma Chamada de Ameaça Ativa imediata com os seus principais pontos de contato para tratar do risco de disseminação do incidente de segurança e das ações urgentes a serem tomadas.
4. **Resumo da chamada e relatório publicado** – entrega da documentação técnica e de um resumo executivo não técnico detalhando os indícios da atividade do invasor, a exposição ao risco e as diretrizes para a eliminação da ameaça e tratamento da causa primária.

Todas as quatro fases de avaliação do Sophos Compromise Assessment são normalmente concluídas em sete dias da chamada de coordenação inicial.

Destaques

- Identifique rapidamente se um há invasor oculto operando no seu ambiente
- Quantifique o potencial de risco de disseminação do incidente de segurança
- Comunique-se diretamente com uma equipe de especialistas em caça a ameaças e resposta a incidentes durante todos os estágios da investigação
- Receba uma análise detalhada da atividade do invasor, exposição ao risco e diretrizes para a eliminação da ameaça e tratamento da causa primária
- Suporte ao gerenciamento de risco e a iniciativas de conformidade, bem como a atividades de diligência prévia associadas a fusões e aquisições

SOPHOS

Investigação rápida e completa

O Sophos Compromise Assessment investiga e identifica o espectro completo das atividades do invasor, incluindo:

- Atividade suspeita na rede
- Movimento lateral
- Arquivos maliciosos ou anômalos
- Execução automatizada de malware
- Acesso não autorizado
- Escalonamento de privilégio
- Evasão de defesas
- Roubo de credenciais
- Exfiltração de dados
- Scripts não verificados

Depois da avaliação

Se a equipe do Sophos IR Services confirmar que um invasor atravessou suas defesas, comprometendo seus dados e o seu negócio, existe a opção para a integração priorizada ao Sophos Rapid Response. Esse serviço de resposta a incidentes de grande escala fará a triagem, contenção e neutralização da ameaça ativa em todo o seu ambiente de TI. Uma equipe 24 horas de peritos em incidentes e resposta remota atuará rapidamente para eliminar o adversário do seu ambiente e recomendar ações preventivas em tempo real para tratar da causa primária.

Se não forem encontrados sinais de violação, o Sophos Managed Detection and Response (MDR) pode equipar a sua organização com serviços 24 horas de detecção e resposta. Nossa incansável equipe de caçadores de ameaças e peritos em resposta busca incessantemente possíveis ameaças e incidentes para então validá-los. Nosso pessoal continua trabalhando para interromper, conter e neutralizar as ameaças e oferecer medidas acionáveis para tratar da causa primária dos incidentes e melhorar a higiene da sua segurança.

Enfrentando uma violação ativa?

O Sophos Rapid Response tira você rapidamente da zona de perigo com uma equipe pronta para responder a incidentes, analisar ameaças e sair em seu encalço 24 horas por dia. A integração é iniciada em horas, e a maioria dos clientes é averiguada em 48 horas. Se estiver no meio de uma ameaça ativa, ligue para o telefone de contato regional abaixo e fale com um dos nossos consultores de incidentes.

Se estiver no meio de uma ameaça ativa, envie um e-mail à equipe Rapid Response para rapidresponse@sophos.com ou ligue para o telefone da sua região abaixo:

EUA: +1 4087461064

Austrália: +61 272084454

Canadá: +1 7785897255

França: +33 186539880

Alemanha: +49 61171186766

Reino Unido: +44 1235635329

Suécia:+46 858400610

Itália: +39 02 947 52897

Áustria: +43 73265575520

Suíça: +41 445152286

Países Baixos: +31 162708600

Espanha: +34 913758065

Enfrentando uma violação ativa?

Use o suporte acelerado do Sophos Rapid Response

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

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

2023-06-27 DS-PTBR (PC)

SOPHOS