SOPHOS

Casos de uso do Sophos EDR e XDR

Disponível com o Intercept X Advanced with XDR, Intercept X Advanced with EDR, Intercept X Advanced for Server with XDR e Intercept X Advanced for Server with EDR

Responda a operações de TI críticas aos negócios e questões de caça a ameaças e entre em ação quando for preciso. Administradores de TI e analistas de segurança cibernética podem aproveitar as vantagens dessa poderosa funcionalidade.

Desempenhe operações de segurança de TI críticas e tarefas de caça a ameaças

- Escolha entre consultas SQL pré-gravadas e totalmente personalizáveis
- Aja rapidamente quando tiver as informações de que precisa
- Cobre endpoints, servidores, firewalls, e-mail, hosts na nuvem e mais

Sophos XDR

Casos de Uso de Operações de TI

Casos de Uso de Operações de TI mantêm a higiene das suas operações de TI em perfeitas condições. Veja aqui alguns casos de uso de exemplo:

Verificações de integridade do dispositivo

Identifique dispositivos que tenham problemas de desempenho e acesse-os remotamente para tomar as medidas necessárias.

- Localize dispositivos com pouco espaço em disco, alto consumo de memória/CPU ou que exigem reinicialização
- Acesse dispositivos remotamente para liberar espaço em disco, investigue as causas de uso intenso e reinicialize conforme necessário

Vulnerabilidades

Detecte dispositivos que têm problemas ou vulnerabilidades que podem ser explorados por malware ou invasores.

- Localize dispositivos que apresentam vulnerabilidades de software, serviços desconhecidos em execução ou extensões de navegadores não autorizadas e detecte credenciais de contas compartilhadas ou roubadas
- Acesse dispositivos remotamente para instalar patches, investigar e encerrar serviços desconhecidos, desinstalar extensões de navegadores e atualizar credenciais de contas na nuvem

Softwares indesejados

Rastreie softwares que possam causar problemas de conformidade ou produtividade.

- Localize programas indesejados, como Spotify, Steam e Bittorrent
- Acesse dispositivos remotamente para desinstalar softwares

Configuração supervisionada

Localize dispositivos e cargas de trabalho que apresentam problemas de configuração que representam risco à segurança.

- Identifique servidores com RDP e SSH habilitados, grupos de segurança na nuvem com portas à rede abertas, monitore e faça o inventário de hosts na nuvem pública, contêineres e mais
- Acesse servidores remotamente, desabilite RDP/SSH e verifique se há servidores escutando as portas abertas

Conformidade

Identifique e corrija problemas de conformidade no local e na nuvem.

- Localize arquivos confidenciais, avalie configurações dos ambientes AWS, Azure e GCP
- Acesse dispositivos remotamente para remover arquivos confidenciais, compare as configurações de segurança da nuvem com CIS Benchmarks

Implementação de projetos

Verifique se os projetos são implementados em todos os dispositivos.

- Veja se o software foi implantado nos dispositivos para medir o progresso durante todo o processo
- Acesse dispositivos remotamente para assegurar uma implantação de sucesso e para reinicialização, caso seja necessário fazer alguma alteração

Problemas de rede de escritório (requer XDR)

Veja e retifique problemas de rede em todos os seus escritórios e filiais.

- Entenda por que uma localidade está tendo problemas de rede que deixa seu desempenho lento
- Identifique qual aplicativo está causando o problema

Gerenciamento de dispositivo (requer XDR)

Identifique e reconheça os dispositivos no ambiente de TI da sua organização.

- Veja dispositivos não gerenciados e não protegidos, como notebooks, dispositivos móveis e equipamentos IoT
- Veja dados adicionais sobre dispositivos legados ou não gerenciados, como equipamentos médicos especializados

Espere pelo inesperado (requer XDR)

Com 30 dias de armazenamento na nuvem, não seja pego de surpresa por eventos inesperados.

- Retroceda 30 dias e verifique atividades incomuns em um dispositivo que foi perdido
- Veja o que aconteceu com um dispositivo mesmo que tenha sido limpo ou destruído

Casos de Uso de Caça de Ameaças

Rastreie ameaças sutis e evasivas e elimine-as rapidamente. Veja aqui alguns casos de uso de exemplo:

Ataques à Rede

Identifique processos fazendo tentativas incomuns de acesso à rede.

- Detecte processos tentando se conectar a portas fora do padrão ou tráfego de saída irregular de uma carga de trabalho da nuvem
- Analise grupos de segurança na nuvem para identificar recursos expostos à internet pública
- Acesse remotamente dispositivos e cargas de trabalho, encerre processos e verifique se há presença de movimentos laterais no sistema

Arquivos modificados

Localize itens que foram modificados de uma maneira inesperada.

- Identifique processos que tiveram arquivos ou chaves de registro recém-modificados
- Acesse o dispositivo remotamente, examine as probabilidades e adote medidas adequadas

Scripts ofuscados

Ataques sem arquivo baseados na memória são um vetor de ataque comum.

- Aprofunde-se nos detalhes de execuções PowerShell inesperadas
- Acesse o dispositivo remotamente, execute ferramentas forenses adicionais e encerre processos suspeitos

Processos disfarçados

Alguns processos maliciosos se disfarçam para evitar a detecção.

- Detecte processos que se disfarçaram
- Acesse o dispositivo remotamente, encerre processos suspeitos e execute ferramentas forenses

Estrutura MITRE ATT&CK

A estrutura MITRE ATT&CK é um modelo usado regularmente para identificar técnicas de ataque.

- Use suas próprias consultas ou as consultas da Sophos para identificar as táticas e técnicas de ataque usadas pelos adversários
- Baseado na técnica identificada, canalize sua investigação na espreita de possíveis ataques subsequentes ou em áreas para reavaliar

Escopo do incidente

Entenda o impacto de um incidente e quais dispositivos e usuários foram afetados.

- Identifique dispositivos que clicaram em um link presente em um e-mail de phishing
- Veja quais dispositivos baixaram arquivos do site de phishing, acesse-os remotamente e realize a limpeza

SOPHOS

Prolongue os períodos de investigação (requer XDR)

Use 30 dias de dados na nuvem além de 90 dias de armazenamento de dados no dispositivo.

- Investigue 30 dias de dados sem precisar colocar o dispositivo online
- Veja o que aconteceu a dispositivos incapacitados durante um ataque

Use dados de rede detalhados (requer XDR)

Incorpore dados de rede à sua caça e investigação de ameaças.

- Faça uma análise entre tráfegos maliciosos bloqueados e outros IoCs para entender a amplitude de um ataque
- Use detecções ATP e IPS do firewall para investigar hosts e dispositivos suspeitos

Use dados de e-mail detalhados (requer XDR)

Integre informações de e-mails para obter insight adicional de seu ambiente.

- Compare informações de cabeçalho de e-mail com outros IoCs para obter um melhor entendimento de um incidente
- Identifique arquivos suspeitos e remova-os rapidamente de dispositivos e caixas de correio do O365

Para saber mais sobre o Sophos XDR, EDR e as poderosas funcionalidades de proteção do Intercept X, visite o site Sophos.com.

21-03-26 UC-PTBR (MP)

SOPHOS