SOPHOS
Cybersecurity made simple.

Os 5 principais m
para precisar de EDR

As ferramentas de detecção e resposta de endpoints (EDR) são criadas para complementar a segurança de endpoints com recursos aprimorados de detecção, investigação e resposta. NNo entanto, o hype surrounding a ferramentas de EDR pode dificultar a compreensão de como exatamente elas podem ser usadas e por que são necessárias. Para piorar as coisas, as soluções de EDR atuais muitas vezes têm dificuldade em agregar valor para muitas organizações, pois podem ser difíceis de usar, não têm funcionalidades de proteção suficientes e exigem muitos recursos.

O Sophos Intercept X Advanced with EDR integra o EDR inteligente com a proteção de endpoints mais bem avaliada da indústria em uma única solução, tornando-o a maneira mais fácil para as organizações responderem às difíceis perguntas sobre incidentes de segurança. Aqui estão outros motivos para considerar uma solução de EDR.

Comunique com confiança a sua postura de segurança a qualquer momento

As equipes de TI e segurança geralmente são motivadas por métricas de ataque e defesa, mas a pergunta mais difícil para a maioria das equipes é "estamos seguros neste momento?" Isso ocorre porque a maioria das redes têm pontos cegos consideráveis que faz com que as equipes de TI e segurança tenham dificuldade em ver o que está acontecendo em seus ambientes.

A falta de visibilidade é a principal razão pela qual as organizações têm dificuldade para entender a abrangência e o impacto dos ataques. Esta situação geralmente se manifesta quando ocorre um incidente e a equipe supõe que está segura por este incidente já ter sido detectado. O Intercept X Advanced with EDR fornece informações adicionais que determinam se outras máquinas foram afetadas. Por exemplo, se um arquivo executável suspeito fosse encontrado na rede, ele seria corrigido. No entanto, o analista pode não saber se o executável está presente em algum outro lugar do ambiente. Com o Intercept X Advanced with EDR, essas informações estão facilmente disponíveis. A capacidade de visualizar os outros locais onde existam ameaças permite que a equipe de segurança priorize incidentes para realizar investigações adicionais e potenciais correções.

A geração de uma visão clara da postura de segurança de uma organização também oferece a vantagem da possibilidade de comunicar o status de conformidade. Esta informação ajudará a identificar áreas que podem estar vulneráveis a ataques. Também permite que os administradores determinem se a abrangência de um ataque afetou as áreas onde os dados confidenciais estão armazenados. Por exemplo, se fosse detectado um malware que vazasse dados da rede, um analista precisaria determinar se as máquinas afetadas armazenavam informações médicas que estavam sujeitas ao HIPAA (Health Insurance Portability and Accountability Act: Lei de portabilidade e responsabilidade de seguros de saúde – regulamentação dos EUA). Esta seria uma prática muito mais simples com o Intercept X Advanced with EDR. Como um benefício adicional de conformidade, também seria muito mais fácil demonstrar que as informações do paciente estão sendo protegidas graças à maior visibilidade de endpoints.

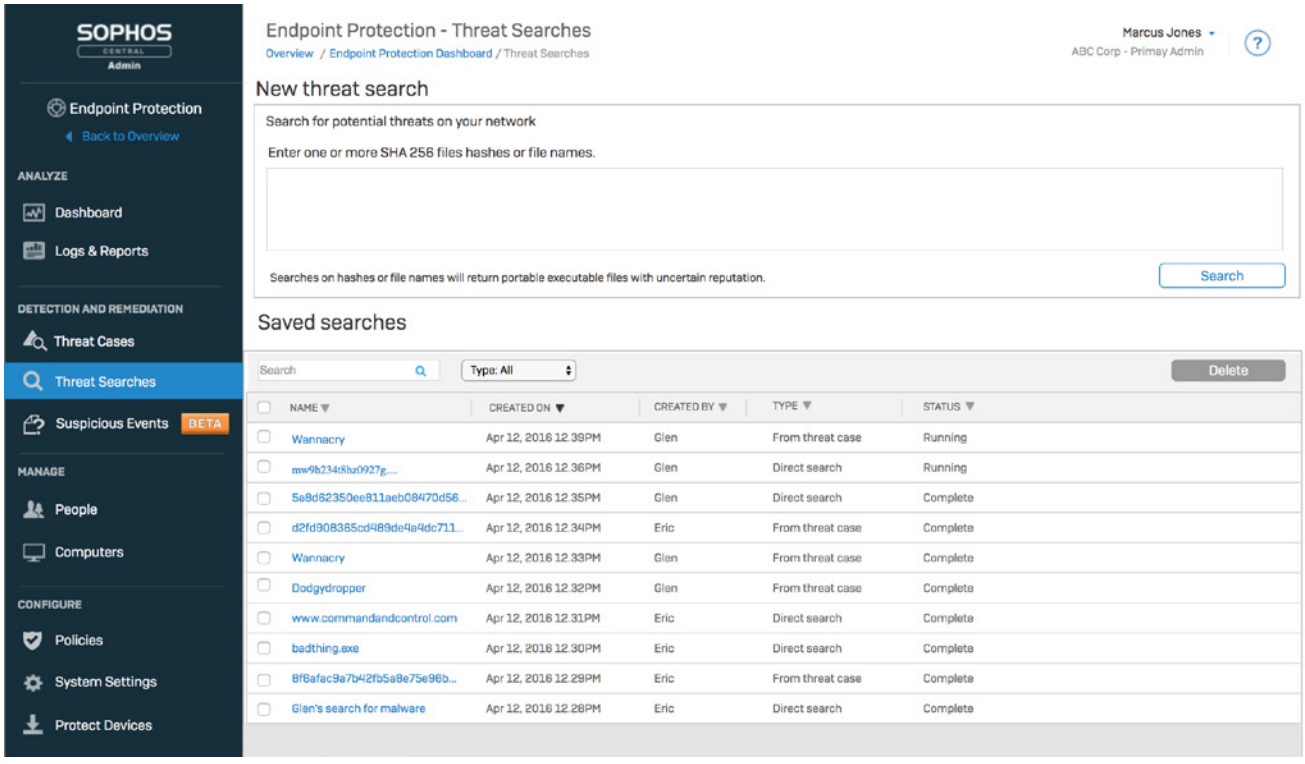


Figura 1: O Sophos Intercept X Advanced with EDR exibe todos os locais adicionais onde uma ameaça está presente

Detecte ataques que passaram despercebidos

Quando se trata de segurança cibernética, se houver tempo e recursos suficientes, até mesmo as ferramentas mais avançadas podem ser derrotadas, o que dificulta a compreensão real de quando acontecem os ataques. As organizações geralmente dependem exclusivamente da prevenção para que permaneçam protegidas e, embora a prevenção seja fundamental, o EDR oferece outra camada de recursos de detecção para possivelmente encontrar incidentes que passaram despercebidos.

As organizações podem aproveitar o EDR para detectar ataques ao buscar indicadores de comprometimento (IOCs). Esta é uma maneira rápida e simples de buscar por ataques que possam ter passado despercebidos. As pesquisas de ameaças frequentemente são iniciadas após uma notificação de inteligência de ameaças de terceiros: por exemplo, uma agência do governo (como a US-CERT, CERT-UK ou CERT Austrália) pode informar uma organização de que há atividade suspeita em sua rede. A notificação pode vir acompanhada por uma lista de IOCs, que pode ser usada como ponto de partida para determinar o que está acontecendo.

O Sophos Intercept X Advanced with EDR fornece uma lista dos principais eventos suspeitos e, assim, os analistas sabem exatamente o que devem investigar (disponível em 2019). Aproveitando os recursos de Machine Learning do SophosLabs, uma lista dos principais eventos suspeitos é apresentada e classificada de acordo com a pontuação da ameaça deles. Aos analistas, isso facilita a priorização de suas cargas de trabalho e permite que se concentrem nos eventos mais importantes.

Eventos suspeitos também destacam um cenário comum, no qual analistas são chamados para determinar se algo é realmente mal-intencionado. Isso diz respeito a atividades que não parecem ser mal-intencionadas o suficiente para serem bloqueadas de forma automática, mas que ainda se mostram suspeitas o bastante para justificar uma análise mais profunda. Para exemplificar, imagine estar numa "área indefinida", onde é necessária uma análise adicional para confirmar se algo é mal-intencionado, benigno ou indesejado.

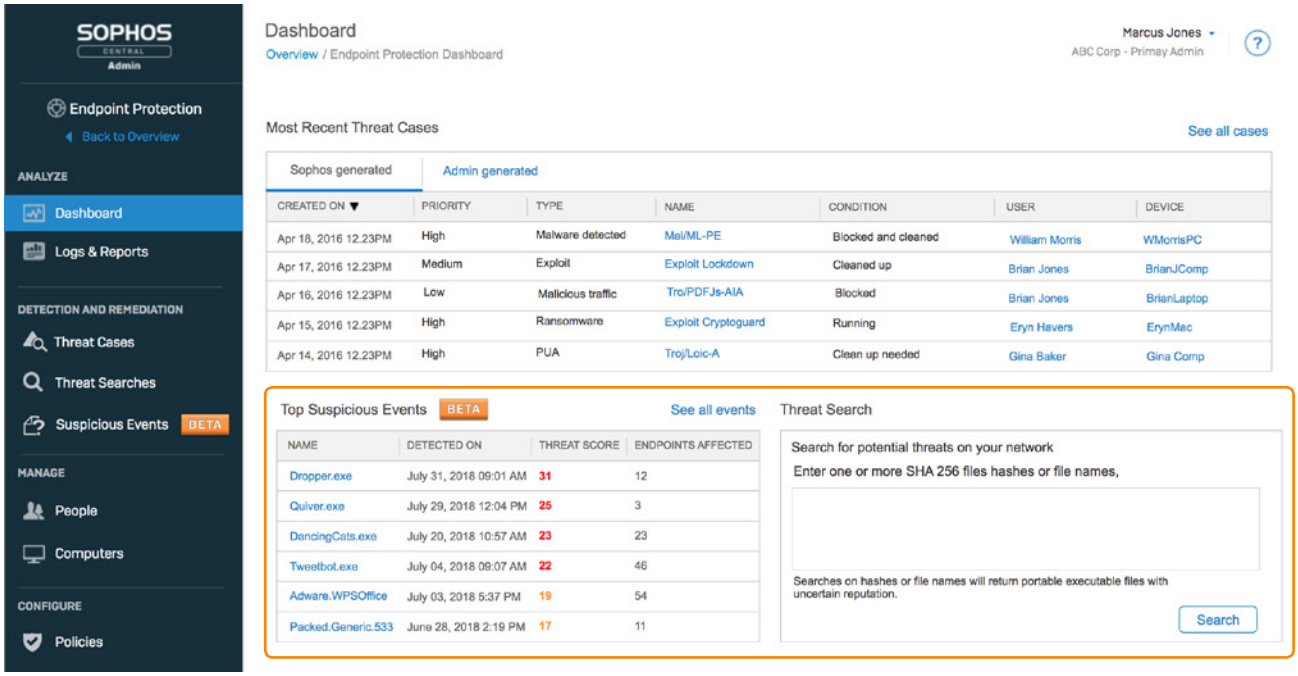


Figura 2: O Sophos Intercept X Advanced with EDR oferece a capacidade de buscar indicadores de comprometimento em toda a rede. Também aproveita o Machine Learning para determinar os principais eventos suspeitos que devem ser investigados (a funcionalidade de eventos suspeitos estará disponível em 2019)

Responda rapidamente a possíveis incidentes

Uma vez que os incidentes são detectados, as equipes de TI e de segurança geralmente têm dificuldade em corrigi-los o quanto antes para reduzir o risco dos ataques se alastrarem e para limitar qualquer possível dano. Naturalmente, a pergunta mais pertinente a ser feita é como se livrar de cada ameaça. Em média, as equipes de segurança e de TI gastam mais de três horas tentando corrigir cada incidente. O EDR pode acelerar significativamente este processo.

O primeiro passo que um analista poderia tomar durante o processo de resposta a incidentes seria impedir o alastramento de um ataque. O Intercept X Advanced with EDR isola os endpoints sob demanda, o que é um passo fundamental para impedir que uma ameaça se alastre por todo o ambiente. Os analistas costumam fazer isso antes de investigar, o que os faz ganhar tempo enquanto determinam a melhor estratégia.

O processo de investigação pode ser lento e complicado. Este caso obviamente pressupõe uma investigação. A resposta a incidentes sempre dependeu muito de analistas humanos altamente qualificados. A maioria das ferramentas de EDR também depende muito dos analistas para saber quais perguntas fazer e como interpretar as respostas. No entanto, com o Intercept X Advanced with EDR, equipes de segurança de todos os níveis de habilidade podem responder rapidamente a incidentes de segurança graças às investigações guiadas, que oferecem sugestões dos próximos passos, representações visuais claras dos ataques e conhecimentos integrados.

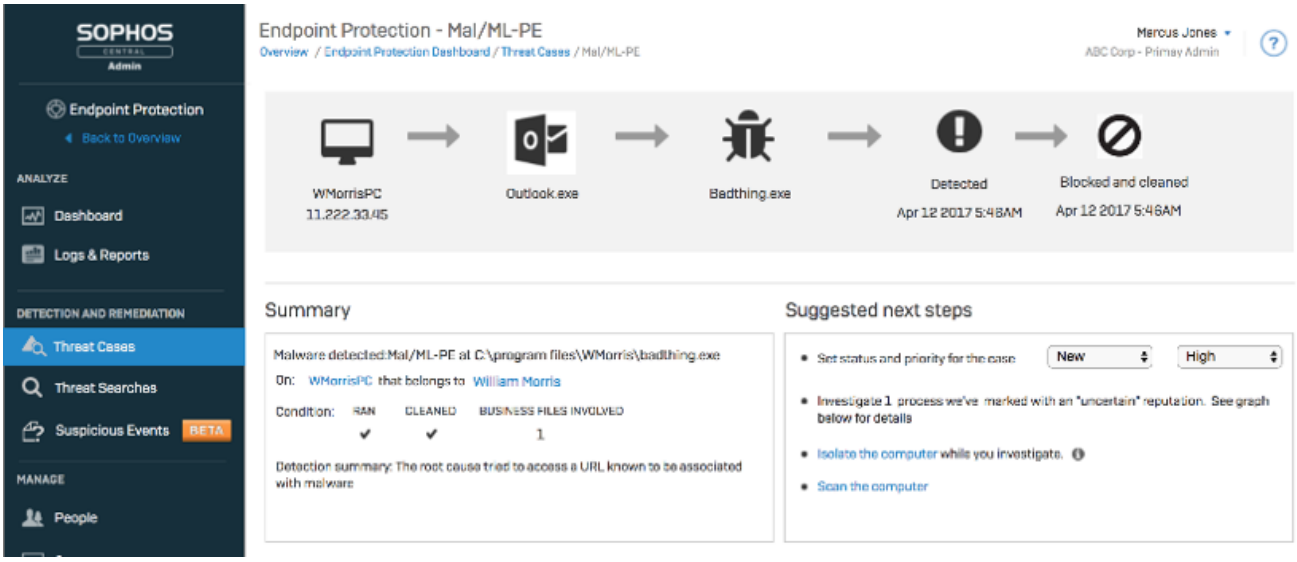


Figura 3: A resposta guiada a incidentes oferece as próximas etapas sugeridas e o isolamento de endpoints sob demanda para resolver os incidentes com rapidez e segurança.

Ao concluir uma investigação, os analistas podem responder com apenas um clique. Dentre as opções de resposta rápida estão a capacidade de isolar os endpoints para correção imediata, realizar a limpeza e o bloqueio de arquivos e criar instantâneos forenses. E se um arquivo for bloqueado por engano, ele pode ser facilmente revertido.

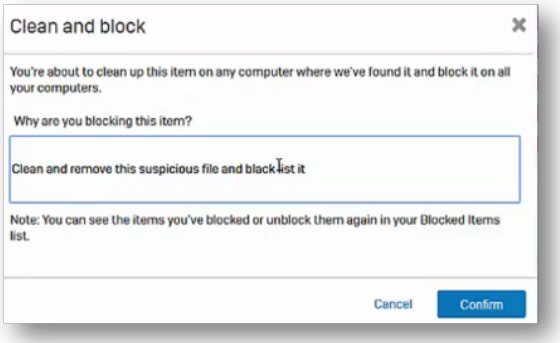


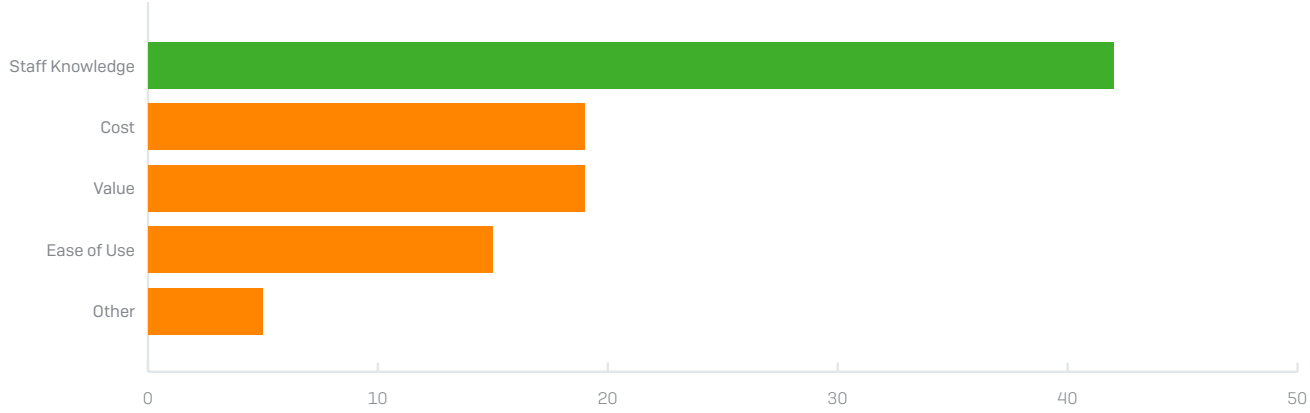
Figura 4: Os botões de ação estão localizados em todo o Intercept X Advanced with EDR e oferecem várias opções de correção, sendo as mais comuns "eliminar e bloquear".

Agregue experiência sem aumentar o headcount

A grande maioria das organizações que buscam adicionar recursos de detecção e resposta de endpoints mencionam o "conhecimento dos funcionários" como o principal impedimento para a adoção do EDR. Isso não deve ser nenhuma surpresa, já que a lacuna de talentos para encontrar profissionais qualificados em segurança cibernética tem sido amplamente discutida há vários anos. Esta barreira é especialmente nítida quando se trata de pequenas organizações.

Principais motivos pelos quais as organizações não implementaram o EDR

Figura 5: O conhecimento dos funcionários foi citado como o principal motivo pelo qual as organizações não adotaram uma solução de detecção e resposta de endpoints (EDR) (Fonte: Estudo da Sapio realizado em conjunto com a Sophos, outubro de 2018)



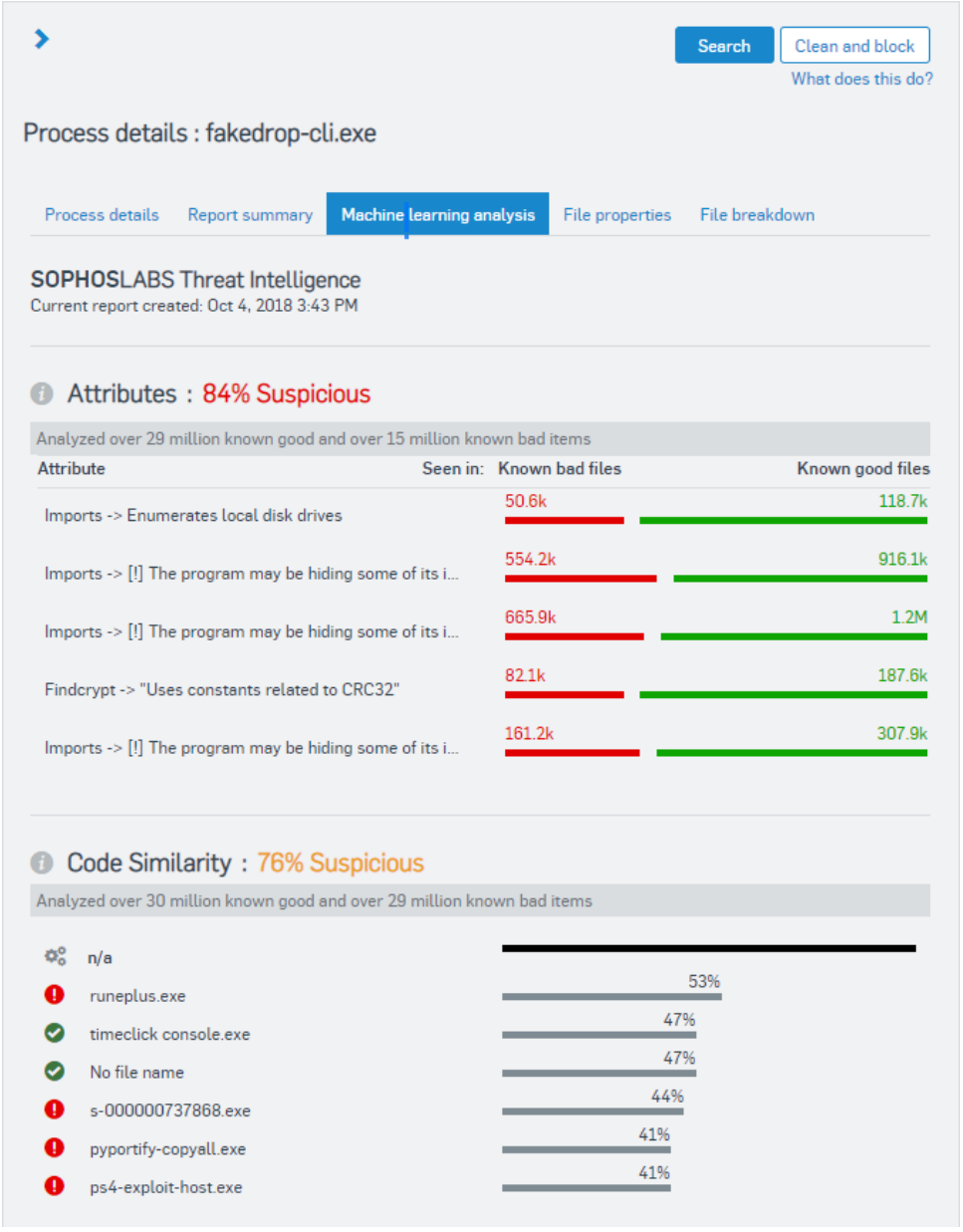
Para combater a lacuna de conhecimentos dos funcionários, o Intercept X Advanced with EDR replica os recursos associados a analistas raros de encontrar. Ele aproveita o Machine Learning para integrar informações aprofundadas de segurança e é aprimorado com a SophosLabs Threat Intelligence, para que você possa agregar experiência sem ter que aumentar o número de funcionários. As capacidades inteligentes de EDR ajudam a preencher as lacunas causadas pela falta de conhecimentos dos funcionários, o que reproduz as funções de vários tipos de analistas:

- **Analistas de segurança**: Esses são os analistas da linha de frente, encarregados da triagem de incidentes e da determinação de quais alertas precisam ser imediatamente endereçados. O ideal é que eles também sejam capazes de proativamente caçar e detectar ataques que possam ter passado despercebidos. O Intercept X Advanced with EDR detecta e prioriza automaticamente possíveis ameaças (disponível em 2019). Com o uso do Machine Learning, eventos suspeitos são identificados e recebem uma pontuação de ameaças. Os eventos com as pontuações mais altas são os mais imediatamente importantes. Os analistas podem descobrir rapidamente onde concentrar sua atenção e iniciar a investigação.
- **Analistas de malware**: As organizações podem depender de especialistas em malware especializados em engenharia reversa de arquivos suspeitos para que possam analisá-los. Essa abordagem não apenas é demorada e difícil de ser realizada, como também pressupõe um nível de sofisticação de segurança cibernética que a maioria das organizações não possui. É necessário que haja analistas de malware para decidirem se um arquivo que não foi bloqueado é realmente mal-intencionado. Também podem examinar arquivos que foram bloqueados, mas que podem ser falsos-positivos. O Intercept X Advanced with EDR oferece uma melhor abordagem à análise de malware ao empregar o Machine Learning. Com o uso do melhor motor de detecção de malware de endpoints do mercado, o malware é analisado de forma automática nos mínimos detalhes ao dividir-se os atributos de arquivo e componentes de código e compará-los com milhões de outros arquivos. Os analistas podem facilmente ver quais atributos e segmentos de código são semelhantes aos arquivos "sabidamente bons" e "sabidamente ruins", para que possam

determinar se um arquivo deve ser bloqueado ou permitido.

- **Analistas de inteligência de ameaças**: As investigações podem depender da inteligência de ameaças prestada por terceiros (geralmente a um custo adicional) para adicionar informações e contexto às ameaças. Os analistas são necessários para interpretar e integrar esses dados, a fim de garantir que agreguem valor. A inteligência de ameaças pode ser usada como ponto de partida para investigações, como um meio de perguntar à comunidade de segurança a sua opinião sobre um arquivo suspeito ou para determinar se um ataque está sendo direcionado contra a organização. O Intercept X Advanced with EDR fornece aos administradores de TI e de segurança a capacidade de coletar mais informações ao acessar dados sob demanda sobre ameaças, selecionados pelo SophosLabs. Para manter a visibilidade total do cenário de ameaças, o SophosLabs rastreia, desconstrói e analisa 400.000 ataques de malware únicos e inéditos, todos os dias, em uma busca constante pelas mais recentes e melhores técnicas de ataque. Essa inteligência de ameaças é coletada, agregada e resumida de modo a facilitar a análise, para que as equipes que não possuam analistas dedicados à inteligência de ameaças ou o acesso aos feeds de ameaças, que são caros e difíceis de compreender, possam se beneficiar de uma das melhores equipes de pesquisa sobre segurança cibernética e ciência de dados do mundo.

Figura 6: A análise de Machine Learning exibe os atributos, a semelhança entre códigos e a análise de caminho de arquivo para que seja obtida uma análise poderosa, porém simples.



Entenda como um ataque aconteceu e como impedir que ele ocorra novamente

Os analistas de segurança têm pesadelos frequentes depois de sofrerem um ataque: um executivo grita: "Como isso aconteceu?!" e tudo o que eles podem fazer é encolher os ombros. Identificar e remover arquivos mal-intencionados resolve o problema imediato, mas não esclarece como ele chegou lá ou o que o invasor fez antes do ataque ser neutralizado.

Os casos de ameaças, incluídos no Intercept X Advanced with EDR, destacam todos os eventos que levaram a uma detecção, o que facilita a compreensão de quais arquivos, processos e chaves de registro foram afetados pelo malware para, assim, determinar o impacto de um ataque. Ele fornece uma representação visual de toda a cadeia de ataque, o que garante a emissão de relatórios confiáveis sobre como o ataque começou e para onde foi o invasor. Mas o mais importante, ao entender a causa primária de um ataque, é que a equipe de TI terá muito mais chances de impedir que ele ocorra novamente.

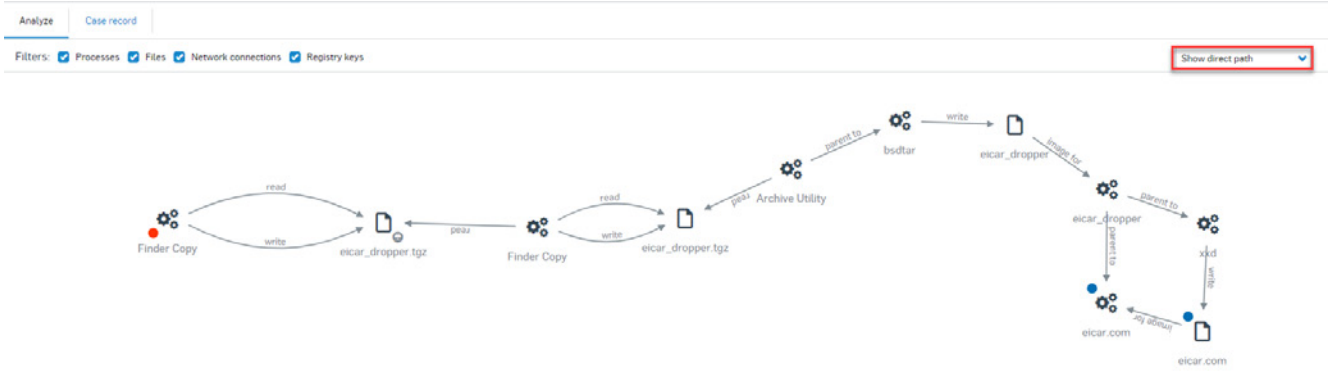


Figura 7: Os casos de ameaças fornecem uma representação visual e interativa da cadeia de ataque.

Experimente agora gratuitamente

Registre-se para uma avaliação gratuita de 30 dias em sophos.com/interceptx

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

Vendas na Brasil
E-mail: Brasil@sophos.com

2018-11-14 (PC)

SOPHOS