ManageEngine
Log360

CASO DE USO

Use o Log360 para detecção de malware

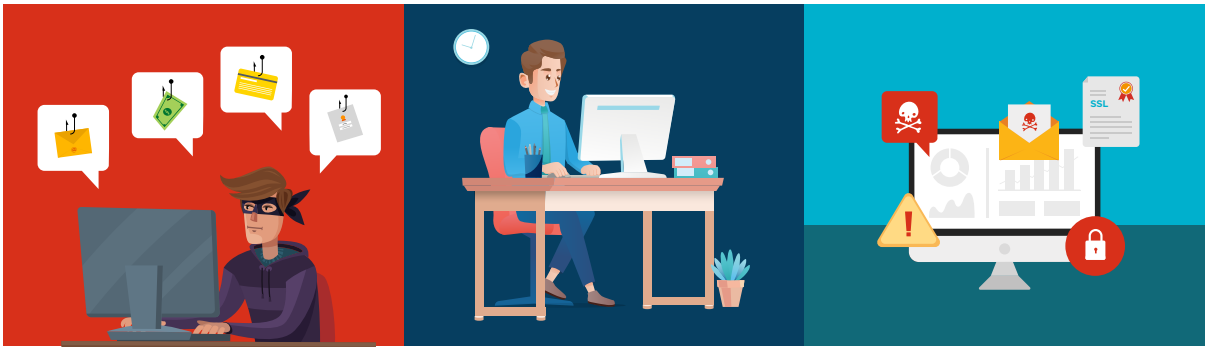
Use o Log360 para detecção de malware

Os ataques de malware continuam a atormentar as empresas ano após ano. De acordo com um estudo da Statista, o número total de novas detecções de malware em todo o mundo chegou a 677,66 milhões de programas em março de 2020.

O combate ao malware começa com sua detecção. Malwares como o ransomware e o adware criptografam imediatamente os arquivos do sistema e transmitem anúncios. Outros, como cavalos de Troia e spyware, são notoriamente indetectáveis. Os vírus e worms podem operar furtivamente até resultarem em arquivos excluídos, desligamentos repentinos, alto uso do disco e até mesmo falhas de hardware.

Considerando que os ataques de malware evoluem rapidamente, como você pode garantir que o sistema de detecção em sua rede esteja combatendo efetivamente essa ameaça dinâmica?

Como o malware funciona?



1. O malware é entregue ao seu sistema via

- Emails de spam
- Vulnerabilidades
- Links maliciosos
- Propagação de rede

2. Ele é instalado em seu sistema com ou sem ação do usuário

3. Possíveis consequências:

- Criptografa o sistema
- Rouba ou manipula dados
- Estabelece backdoors
- Rouba credenciais, senhas bancárias e muito mais

Embora a implantação de uma solução antimalware seja altamente eficaz, pode não ser suficiente, pois não forneceria uma visão de segurança holística de sua rede. Além disso, ele pode não levar em conta fatores como o comprometimento da conta, que às vezes pode preceder a instalação de um software legítimo que é realmente malicioso.

É por isso que você precisa de uma solução de gerenciamento de eventos e informações de segurança (SIEM) que possa correlacionar eventos. Construir um forte sistema de correlação e análise de log ajuda você a tomar medidas proativas contra ataques de malware.

Como o Log360 pode detectar malware

O Log360, uma solução SIEM abrangente e fácil de usar, pode ajudá-lo a detectar e interromper ataques de malware.

Mecanismo de correlação baseado em regras para detectar malware

O Log360, uma solução SIEM abrangente e simples de usar, vem com um poderoso mecanismo de correlação que permite definir regras para identificar padrões suspeitos em seus logs de rede recebidos. Com uma série de regras integradas, ele correlaciona vários eventos e alerta você sobre instalações suspeitas de software, de serviços e muito mais.

Análise comportamental para detectar malware

O Log360 leva vários fatores em consideração antes de sinalizar uma instalação de software como maliciosa. Isso é possível com a análise de comportamento realizada pelo complemento Log360 UEBA, que detecta anomalias com base em tempo, contagem e padrão. Isso elimina efetivamente os falsos alarmes, que são um grande desafio na detecção de ameaças.

Investigação de incidentes com Log360

O Log360 não se limita apenas à detecção de malware; também ajuda na investigação e mitigação eficazes. Uma vez sinalizado, você pode investigar facilmente o incidente com os relatórios de correlação. A linha do tempo detalhada do incidente e os relatórios de análise de segurança apresentam informações de log que servem como evidência para o incidente.

O sistema de gerenciamento de incidentes de ponta a ponta da solução vem com um módulo de ticket integrado que ajuda a atribuí-los a administradores de segurança, rastrear seu status e garantir a responsabilidade no processo de resolução de incidentes. Esse sistema também possui uma estrutura de correção automática que pode associar perfis de fluxo de trabalho a regras de correlação. Esses perfis de fluxo de trabalho podem ser executados automaticamente quando o alerta de é acionado para corrigir instantaneamente o incidente.

O mais recente Gartner Magic Quadrant para SIEM está disponível!

ManageEngine foi reconhecido no Gartner's Magic Quadrant para Gerenciamento de Informações e Eventos de Segurança, 2021.

Obter relatório

Escolha dos clientes do Gartner Peer Insights, 2021

A ManageEngine foi reconhecida como a escolha dos clientes do Gartner Peer Insights para SIEM em 2021.

Saiba como

O Log360 é uma solução SIEM unificada com recursos integrados de DLP e CASB que detecta, prioriza, investiga e responde a ameaças à segurança. Ele combina inteligência contra ameaças, detecção de anomalias baseada em machine learning e técnicas de detecção de ataques baseadas em regras para detecção sofisticadas, além de oferecer um console de gerenciamento de incidentes para corrigir com eficácia as ameaças detectadas. O Log360 oferece visibilidade holística da segurança em redes on-premises, na nuvem e híbridas com seus recursos intuitivos e avançados de análise e monitoramento de segurança.

Para mais informações sobre o Log360, visite https://www.manageengine.com/br/log-management/

ManageEngine Log360

$ Obter lançamento

Download