ManageEngine
Log360

Inteligência contra ameaças e a vantagem do SIEM

Por que as soluções SIEM são a escolha ideal para obter capacidades de inteligência contra ameaças.

www.manageengine.com/br/log-management/

Introdução

A Inteligência de ameaças (IA) é a arma não tão secreta que o setor de segurança cibernética está usando para intensificar seu jogo contra ataques. Embora já exista há algum tempo, a inteligência de ameaças foi amplamente reconhecida apenas recentemente. De acordo com a Pesquisa de inteligência de ameaças Cibernéticas SANS 2018, 81% dos profissionais de segurança acreditam que investir na IA ajudou a melhorar a postura de segurança de sua organização, em comparação com 64% em 2016.

No entanto, apesar do crescente interesse, também há muito debate em torno desse tópico. O que exatamente envolve a inteligência de ameaças? Quais capacidades são necessárias para uma organização afirmar que possui um sistema maduro de inteligência de ameaças? Quais ferramentas são melhores para fornecer essas capacidades?

Neste relatório oficial, discutiremos:

- Inteligência de contra ameaças e seus vários aspectos.
- Como a inteligência de ameaças é incorporada à estrutura de segurança de uma organização.
- As vantagens de usar uma solução SIEM para implementar um sistema abrangente de inteligência de ameaças em sua organização.
- Casos de uso corporativo.

Desmistificando a inteligência de ameaças

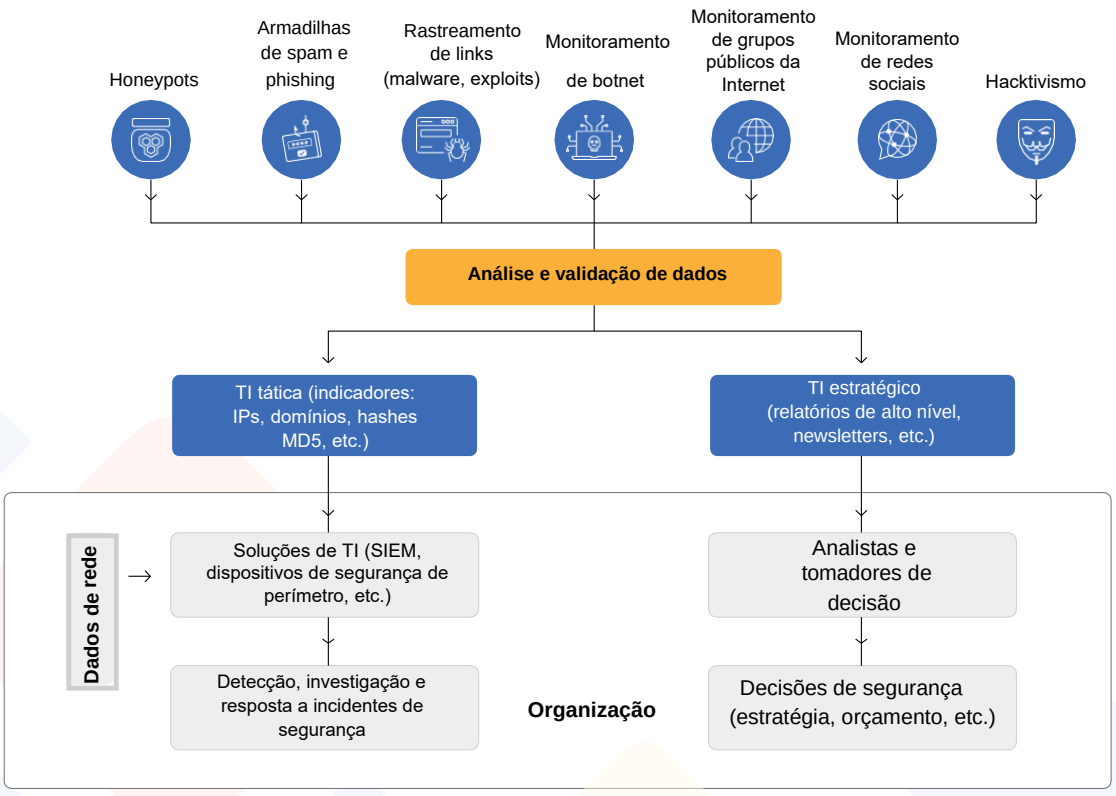
O Gartner, instituto líder mundial em pesquisa e consultoria, define inteligência de ameaças como "conhecimento baseado em evidências, incluindo contexto, mecanismos, indicadores, implicações e conselhos acionáveis, sobre uma ameaça ou risco existente ou emergente para ativos, que pode ser usado para fundamentar decisões em relação à resposta de quem está sujeito a essa ameaça ou perigo".

Essa definição nos ajuda a observar os seguintes aspectos da inteligência de ameaças:

- Com base em uma abordagem "conhecidamente ruim", a inteligência de ameaças ajuda as organizações a detectar ameaças com base no conhecimento observado em outras partes do mundo.
- A inteligênciade ameaças não é apenas uma lista de IPs ruins. Ela também inclui perfis detalhados de agentes, mecanismos de ataque e instruções sobre como responder a uma ameaça.
- Ela está em constante evolução e fornece informações sobre ameaças existentes e emergentes.
- Seu principal objetivo é equipar melhor as organizações na luta contra as ameaças globais.

O ciclo de inteligência de ameaças

A definição de inteligência de ameaças nos ajuda a avaliar o que é a ameaça; no entanto, ainda não aborda duas questões importantes: de onde ela vem? E como ela é incorporada no contexto da segurança de rede de uma organização? O diagrama a seguir pode nos ajudar a visualizar as respostas para essas perguntas:



Usando uma combinação de técnicas automatizadas e manuais, os dados de inteligência de ameaças são coletados de toda a internet. Esses dados são então processados por equipes de pesquisa resolutas que analisam e validam as informações antes de publicá-las na forma de inteligência de ameaças estratégica ou tática.

A inteligência de ameaças estratégica destina-se principalmente ao consumo humano e orienta as decisões estratégicas de segurança, como decidir em quais áreas de segurança cibernética focar, lançar programas de conscientização dos funcionários sobre as ameaças mais recentes e assim por diante.

A inteligência de ameaças tática é mais publicada na forma de feeds de ameaças e é lida por uma ou mais soluções de segurança. É mais útil no dia a dia, pois ajuda as organizações a detectar e combater incidentes de segurança em suas redes. Alguns feeds de ameaças populares incluem AlienVault OTX, FireEye iSight Threat Intelligence e Symantec Deepsight.

A vantagem do SIEM

Entre a ampla gama de soluções de segurança disponíveis hoje que fornecem recursos de inteligência de ameaças, nenhuma é tão abrangente quanto as oferecidas pelas soluções SIEM. Elas são a escolha mais popular entre aqueles que desejam desenvolver capacidades de inteligência de ameaças. A esse respeito, os seguintes fatores dão uma vantagem às soluções SIEM:

Qualidade da inteligência de ameaças

Os alertas de segurança têm a qualidade das informações nas quais se baseiam. Conforme mostrado no diagrama acima, há um grande esforço humano envolvido no processamento de dados de ameaças. Isso significa que a qualidade da inteligência de ameaças pode variar entre os provedores.

As soluções SIEM processam inteligência de ameaças de fontes confiáveis e algumas até oferecem a opção de adicionar feeds personalizados aos quais sua organização se inscreve independentemente. Como muitos feeds de ameaças são específicos de um setor ou de certos tipos de ameaças, os personalizados podem fazer mais sentido para sua organização.

Uma visão abrangente da sua rede

O conhecimento sobre ameaças globais não é bom se você não puder usá-lo no contexto de sua rede. Com uma visão abrangente de todos os dispositivos e aplicações, as soluções SIEM podem notificá-lo se entidades maliciosas forem detectadas em qualquer sistema da rede.

As soluções SIEM usam resultados de dados de rede para triagem de alertas com eficácia. Eles podem reduzir os falsos positivos levantando um alerta apenas se um agente de ameaça detectado estiver envolvido em padrões de atividade específicos e suspeitos.

Necessidade de menos integrações

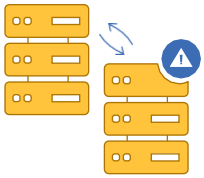
O objetivo da inteligência de ameaças é tornar a detecção de incidentes e o ciclo de resposta o mais eficiente e rápido possível. Quando essas funções estão espalhadas por várias soluções que não se integram bem, isso anula seu objetivo.

As soluções SIEM superam esse problema fornecendo a maioria das funções necessárias a partir de um console único com provisões para uma integração suave quando necessário. Depois que um incidente de segurança é detectado, você pode investigá-lo, gerenciá-lo e responder minuciosamente a ele. Isso ajuda a agilizar o processo de resolução de incidentes, garantindo que sua organização permaneça protegida contra qualquer ameaça.

Inteligência contra ameaças e SIEM em ação: Casos de uso corporativo

Comunicação com servidores de callback

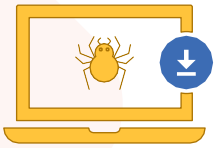
Às vezes, se um sistema em sua rede for infectado, ele pode ficar sob o controle de um servidor externo, também conhecido como callback ou servidor de comando e controle. Esse servidor de callback pode usar esse sistema para extrair dados confidenciais ou infectar outros servidores críticos em sua rede.



As soluções SIEM verificam constantemente os logs de tráfego de saída de sua rede e capturam as comunicações enviadas para esses tipos de servidores. Você pode iniciar uma investigação para descobrir como e quando o sistema foi infectado e verificar se há outros sistemas potencialmente infectados que tiveram contato com esse servidor de callback.

Tentativas de injeção de SQL de fontes maliciosas

Os invasores podem explorar vulnerabilidades em seu servidor web e injetar código SQL malicioso para recuperar registros comerciais confidenciais de seus bancos de dados. Para evitar tais violações de dados, as soluções SIEM ficam de olho em todas as conexões de entrada para seus servidores da web e sinalizam quaisquer IPs ou domínios maliciosos. Isso permite conter a perda de dados importantes e identificar e corrigir vulnerabilidades em seu servidor web.



Downloads de malware em potencial

Os invasores estão sempre procurando maneiras de se infiltrar em sua rede e baixar malware em seus sistemas. Como ele não é facilmente distinguível do software comum, você precisa ficar atento a indicadores de ataque que apontem para softwares problemáticos.

Por exemplo, se um agente maicioso conhecido fizer logon remotamente em sua rede após um ataque de força bruta na VPN de sua organização, acessar um sistema na rede e baixar software nele, é provável que seja um ataque de malware. As soluções SIEM utilizam módulos de correlação que podem verificar padrões de atividade como esse, permitindo detectar ataques com alta precisão e reduzir alertas com falsos positivos.

Destaques: Módulo de inteligência de ameaças do Log360

O módulo de inteligência de ameaças do Log360 da ManageEngine oferece as vantagens a seguir:

- **Atualizações dinâmicas:** O processador de feed de ameaças da solução recupera automaticamente a inteligência de ameaças mais recente de código aberto altamente confiáveis.
- **Não requer configurações:** O perfil de alerta do feed de ameaças é pré-configurado. O Log360 começa a escanear sua rede em busca de ameaças no momento em que você adiciona fontes de log para monitoramento.
- **Capacidade de adicionar feeds personalizados:** Adicione facilmente feeds personalizados de ameaças baseados em STIX/TAXII para serem comparados com seus logs de rede.

- **Construtor de regras de correlação:** Crie regras de correlação personalizadas que detectam atividades suspeitas de um agente de ameaça e geram alertas.
- **Mecanismo de busca poderoso:** Pesquise milhões de logs em segundos e crie uma trilha de log da atividade de qualquer agente malicioso em sua rede.
- **Gerenciamento de incidentes:** Rastreie o status dos alertas de ameaças usando o console de emissão de tickets integrado da solução ou encaminhe alertas para consoles de help desk externos.
- **Resposta automatizada:** Atribua scripts personalizados para serem acionados automaticamente quando um alerta de ameaça é gerado.

Conclusão

A inteligência de ameaças é realmente um divisor de águas na luta contra o número cada vez maior de ataques cibernéticos que as organizações enfrentam. Ela é um esforço colaborativo global do setor de segurança cibernética e, quando usada corretamente, ajuda as organizações a detectar e derrotar ameaças logo após a detecção.

Devido aos seus recursos de segurança abrangentes, as soluções SIEM são a escolha ideal para implementar sistemas de inteligência de ameaças nas empresas. E, com alertas de ameaças robustos, você poderá manter sua organização sempre segura.