McAfee Enterprise Log Search

Detecção rápida com pesquisa de bilhões de eventos em alta velocidade

As equipes de segurança precisam de ferramentas para se movimentar com mais velocidade em ambientes que geram alertas em quantidades cada vez maiores. Os analistas dessas equipes precisam de acesso a um contexto mais rico, além da capacidade de identificar detalhes relevantes de eventos relacionados a um incidente. O McAfee® Enterprise Log Search acelera a caça a ameaças com uma pesquisa ultrarrápida de dados de eventos brutos e não compactados. Um backend viabilizado pela Elasticsearch otimiza o desempenho das consultas, proporcionando acesso imediato a logs brutos. Sua funcionalidade de pesquisa aprimorada permite consultas com entrada em linguagem natural (palavras-chave simples) ou com padrões de expressões regulares mais sofisticados para recuperação de dados direcionada.

Otimize o gerenciamento de logs

O McAfee Enterprise Log Search baseia-se na Elasticsearch, uma tecnologia que utiliza um índice invertido para armazenar dados. O índice invertido cataloga dados em uma estrutura que facilita a recuperação eficiente de termos de pesquisa. Como a Elasticsearch foi desenvolvida para assimilação e indexação com alto desempenho, o McAfee Enterprise Log Search disponibiliza os dados brutos para pesquisa em alta velocidade após eles serem capturados e catalogados.

O McAfee Enterprise Log Search é um componente do McAfee® Enterprise Security Manager, uma solução de gerenciamento de eventos e informações de segurança (SIEM). Um outro componente complementar é o McAfee® Enterprise Log Manager, desenvolvido para ser o armazenamento de registro aplicando hashing (MD5) a logs brutos de entrada para fins de integridade forense e compactando esses logs brutos para conseguir eficiência no armazenamento. Quando combinados, esses dois componentes proporcionam soluções de armazenamento para fins específicos que maximizam pesquisas rápidas (via McAfee Enterprise Log Search) e retenção de logs para fins de conformidade (via McAfee Enterprise Log Manager), evitando que os usuários tenham de priorizar uma capacidade em detrimento da outra.

Principais vantagens

- Gerenciamento de logs otimizado para retenção dos logs e rapidez nas pesquisas
- O backend viabilizado pela Elasticsearch permite um desempenho de alta velocidade na assimilação, indexação e consulta
- Pesquisa em linguagem natural
- Alternância rápida e fácil de visualizações de dados analisados para logs brutos
- Integração total com o McAfee Enterprise Security Manager
- Opções de distribuição flexíveis, como appliances virtuais e físicos (prontos para serem combinados entre si)

Conecte-se conosco

Com o McAfee Enterprise Log Search, as políticas de retenção podem ser personalizadas para armazenar dados não compactados por diferentes durações em anos (365 dias), trimestres (90 dias) ou meses (30 dias). Os usuários podem identificar quais fontes de dados devem ser associadas ao McAfee Enterprise Log Search e podem adicionar até seis políticas de retenção individuais.

Funcionalidade de pesquisa aprimorada

A função de pesquisa dentro do McAfee Enterprise Log Search é como a de mecanismos de pesquisa populares, possibilitando entradas em linguagem natural. Resultados de pesquisa podem ser recuperados de texto simples ou palavras-chave. Além disso, é possível realizar pesquisas com padrões mais sofisticados que incluam lógica booleana, caracteres curinga e expressões regulares (RegEx). Para estreitar ainda mais os resultados da pesquisa, os usuários podem aplicar filtros por data e fonte de dados. O filtro de data permite aos usuários selecionar períodos de tempo nos quais os eventos do log foram gerados, como na última hora, no dia atual, no ano passado ou em intervalos personalizados.

Integração com o McAfee Enterprise Security Manager

A forte integração com o McAfee Enterprise Security Manager permite aos analistas passar de dados analisados para dados brutos com um único clique. Quando um evento é gerado dentro do McAfee Enterprise Security Manager, os arquivos do evento analisado são vinculados diretamente ao arquivo de log de origem e ao registro de log bruto correspondente.

Os analistas que desejarem visibilidade adicional sobre esse registro ou sobre partes do mesmo podem simplesmente selecionar o log em questão para realizar uma pesquisa de log bruto. Não há uma etapa, aplicativo ou interface extra a ser iniciado para se aprofundar com a pesquisa de log bruto.

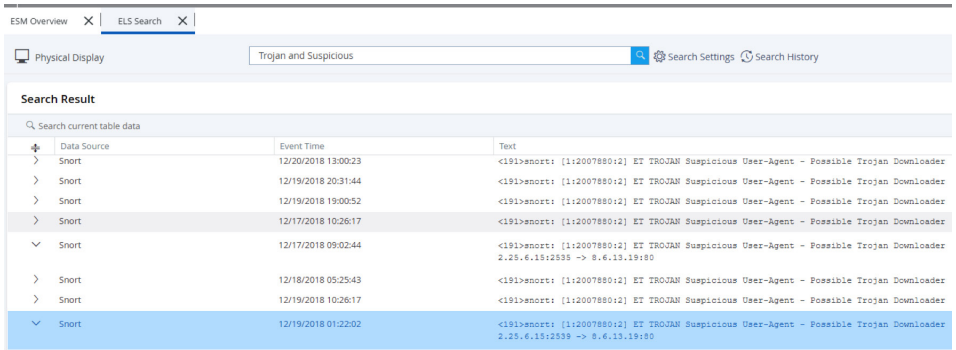

Figura 1. Pesquise palavras-chave utilizando lógica booleana para revelar eventos que contenham um cavalo de Troia e que sejam suspeitos.

Preço e distribuição flexíveis

Opções de distribuição flexíveis incluem appliances físicos e virtuais. Os appliances são avaliados e vendidos conforme sua capacidade de assimilar uma determinada capacidade em eventos por segundo (EPS), em vez de um preço por fonte de dados, preço por EPS ou preço por volume de dados indexados. Máquinas virtuais (VMs) são licenciadas com a mesma filosofia e vendidas pelo número de núcleos de CPU necessários para suportar um determinado EPS. Isso permite que os usuários acrescentem núcleos adicionais conforme a necessidade, sem substituir hardware.

Colete e pesquise rapidamente os dados necessários

Ao se distribuir o McAfee Enterprise Log Search, existem seis tipos de logs que costumam ser utilizados para caçar ameaças. Esses logs podem proporcionar contexto e insights específicos para incidentes de segurança.

Tipo de log	Dados comumente disponíveis
Logs de DNS	▪ Nome de domínio consultado ▪ Endereço IP de origem da consulta de DNS ▪ Sucesso ou falha das consultas de DNS ▪ Endereço IP resolvido, caso a consulta seja bem-sucedida ▪ Valor TTL da resposta ▪ Servidor DNS utilizado
Logs de proxy	▪ Domínio/endereço IP ao qual se está conectando ▪ Bytes transferidos ▪ Data e hora da conexão ▪ URI sendo utilizado ▪ Referenciador ▪ Sequência de caracteres do agente de usuário
Logs SMTP	▪ Domínio do remetente de e-mail ▪ Assunto do e-mail ▪ Endereço IP do remetente
Logs do Windows	▪ Eventos do log de segurança do Windows ▪ Eventos do log de aplicativos do Windows ▪ Eventos do log de sistema do Windows ▪ Eventos do log de integridade de código do Windows
Logs DHCP	▪ Endereço MAC de origem ▪ Endereço IP concedido ▪ Período de concessão ▪ Data e hora da solicitação e concessão
Logs de VPN	▪ Endereço IP de origem ▪ Identidade autenticadora ▪ Data e hora do estabelecimento da conexão VPN ▪ Tipo de conexão: restabelecida ou nova ▪ Tentativas de autenticação falhas — caso tenha havido alguma — e identidades correspondentes

Saiba mais

Para obter mais informações, visite **www.mcafee.com/enterprise/pt-br/products/siem-products.html**.

McAfee Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br