McAfee Advanced Correlation Engine

Detecta ameaças de acordo com o que é importante para você

As ameaças sutis da atualidade desafiam a detecção de ameaças padrão com base em regras. Distribua a solução McAfee® Advanced Correlation Engine com o McAfee Enterprise Security Manager para identificar e gerar pontuação de eventos de ameaça em tempo real utilizando a lógica com base em regras e em riscos. Você informa à solução McAfee Advanced Correlation Engine o que considera importante: usuários ou grupos, aplicativos, servidores específicos ou sub-redes, e ela irá alertá-lo caso o seu ativo esteja ameaçado. As trilhas de auditoria e as reproduções dos históricos possibilitam análise forense, conformidade e ajuste de regras.

Principais vantagens

- Simplifica a inicialização: não há atualizações de regras, ajuste de assinaturas ou outras dificuldades
- Alerta caso alguma ameaça vise seus usuários, ativos, aplicativos e atividades mais importantes
- Gera pontuações precisas por meio da correlação simultânea com base em regras ou sem regras
- Permite verificar novos ataques e vulnerabilidades em comparação ao seu histórico para detectar eventos anteriores
- Acrescenta recursos especializados de correlação e processamento ao McAfee Enterprise Security Manager
- Disponível em distribuições virtuais e de appliance

A solução McAfee Advanced Correlation Engine complementa a correlação de eventos do McAfee Enterprise Security Manager, com dois mecanismos de correlação dedicados e de desempenho para fins específicos:

- Um mecanismo de detecção de risco que gera uma pontuação de risco utilizando a correlação de pontuação de risco sem regras.
- Um mecanismo de detecção de ameaças que as detecta utilizando a correlação de eventos convencional com base em regras.

A solução independente McAfee Advanced Correlation Engine proporciona o poder de processamento necessário para permitir essa ampla correlação de eventos em toda a sua empresa. Seu mecanismo de dados pode ser expandido para se adaptar até mesmo às maiores redes.

Detecção de ameaças por histórico e em tempo real

É possível distribuir a solução McAfee Advanced Correlation Engine nos modos de histórico ou em tempo real. No modo em tempo real, a solução McAfee Advanced Correlation Engine analisa os eventos conforme são coletados, proporcionando uma detecção imediata de riscos e ameaças.

- Correlação com base em regras dos dados de evento em tempo real para detectar as ameaças à medida que ocorrem.
- Correlação sem regras dos dados de evento em tempo real para detectar as ameaças à medida que se desenvolvem.

No modo de histórico, qualquer dado coletado pode ser “reproduzido” por meio dos dois mecanismos de correlação, para detecção recursiva de ameaças e riscos. Quando os ataques de dia zero são descobertos, a solução McAfee Advanced Correlation Engine pode ver os antecedentes para verificar se sua empresa já foi exposta àquele ataque no passado, proporcionando uma detecção de ameaças antes do dia zero.

intel Security

Desempenho dedicado onde é necessário

Como a solução McAfee Advanced Correlation Engine é um appliance autônomo ou uma oferta virtual, não há impacto algum no desempenho do McAfee Enterprise Security Manager em termos de coleta e gerenciamento de eventos. Você pode utilizar todos os recursos dos aplicativos McAfee Advanced Correlation Engine sem comprometer o desempenho, ao mesmo tempo que aproveita o utilitário McAfee Enterprise Security Manager ao máximo.

Correlação de eventos com base em regras

A correlação com base em regras utiliza a lógica de correlação convencional para analisar as informações coletadas em tempo real. Todos os registros, eventos e fluxos de rede são correlacionados — juntamente com informações de contexto, como identidades, funções, vulnerabilidades, entre outras — para detectar padrões que indiquem uma ameaça maior. Embora todas as soluções McAfee Enterprise Security Manager já sejam diretamente compatíveis com a correlação com base em regras por toda a rede, o McAfee Advanced Correlation Engine oferece um recurso de processamento dedicado, para correlacionar volumes de dados ainda maiores, seja complementando as iniciativas de correlação existentes ou assumindo total responsabilidade por elas.

Correlação de pontuação de risco sem regras

Apesar de a correlação com base em regras ser um recurso necessário e importante de qualquer SIEM (Security Information and Event Management) convencional, esses sistemas são capazes de detectar somente padrões de ameaça conhecidos, exigindo constantes atualizações e ajustes de assinaturas para que sejam eficazes. A resposta é complementar a correlação de eventos convencional com a tecnologia de correlação "sem regras". Nos sistemas de correlação sem regras, as assinaturas de detecção são substituídas por uma configuração simples e única: basta informar à solução McAfee Advanced Correlation Engine o que é importante para os seus negócios. Pode ser um serviço ou aplicativo específico, um grupo de usuários ou determinados tipos de dados.

Alerta e rastreamento em tempo real

A solução McAfee Advanced Correlation Engine começará a rastrear toda a atividade relacionada a esses itens, criando uma pontuação de risco dinâmica que aumenta ou diminui, de acordo com a atividade em tempo real. Caso uma pontuação de risco ultrapasse um determinado limite, será gerado um evento na solução McAfee Advanced Correlation Engine. Esse evento poderá ser utilizado para alertar um analista de segurança sobre condições de ameaça cada vez mais perigosas ou pelo mecanismo de correlação convencional com base em regras, como uma condição de um incidente maior. A solução McAfee Advanced Correlation Engine mantém uma trilha de auditoria completa de todas as pontuações de risco, para possibilitar análises e investigações detalhadas das condições de ameaça ao longo do tempo.

Casos de uso

Modelagem de risco empresarial

A solução McAfee Advanced Correlation Engine oferece uma plataforma para modelar o risco empresarial de forma eficaz. O acesso de funcionários com autorização de alto nível a documentos de alta confidencialidade pode trazer risco a um órgão de defesa, ao passo que o vazamento do prontuário médico de uma celebridade diagnosticada com uma doença grave pode trazer risco a um hospital. A solução McAfee Advanced Correlation Engine proporciona uma modelagem impecável dos riscos de sua empresa, pontuando os atributos que são importantes, desenvolvendo uma linha de base e enviando notificações caso os limites normais sejam ultrapassados.

Avaliações proativas de risco para dados críticos

Como a solução McAfee Advanced Correlation Engine monitora os dados em tempo real, é possível utilizar os dois mecanismos de correlação simultaneamente para detectar riscos e ameaças antes que estes ocorram. As pontuações de risco podem ser utilizadas na lógica de correlação convencional. Por exemplo, uma assinatura de detecção de ameaça convencional com base em regras pode ser "um evento de malware que está ocorrendo após um evento de login de força bruta". Normalmente, quando essa assinatura é disparada, o evento

já ocorreu. Já a solução McAfee Advanced Correlation Engine possibilita incorporar um fator de risco, como um aumento de 20% na pontuação de risco após um evento de login de força bruta. Assim que esse evento é percebido, a solução McAfee Advanced Correlation Engine pode proporcionar um alerta proativo de um incidente iminente, possibilitando a intervenção antes que os danos sejam causados.

Avaliação recursiva de ameaças

Não raro, uma ameaça é identificada ou uma violação é revelada somente para saber se ela realmente esteve lá o tempo todo. Distribuindo a solução McAfee Advanced Correlation Engine no modo de histórico, é possível reproduzir qualquer conjunto de dados de histórico contido por meio dos mecanismos de correlação convencional ou sem regras.

Ao determinar quando uma ameaça recém-descoberta se concretizou pela primeira vez, há uma probabilidade muito maior de se identificar a causa raiz dessa condição.

Modos operacionais

Modo de correlação em tempo real

- Correlação com base em regras dos dados de evento em tempo real para detectar as ameaças à medida que ocorrem.
- Correlação sem regras dos dados de evento em tempo real para detectar as ameaças à medida que se desenvolvem.

Modo de correlação de histórico

- Correlação com base em regras dos dados de evento de histórico para proporcionar detecção recursiva das ameaças.
- Correlação sem regras dos dados de evento de histórico para proporcionar avaliação recursiva das ameaças.

Capacidade de correlação

- Correlação simultânea com base em regras ou sem regras.
- Correlaciona dados de qualquer fonte de dados compatível.
- Correlaciona dados em redes distribuídas e coletores.
- Inclui centenas de regras de correlação de eventos predefinidas.
- Inclui um editor de configurações para correlação sem regras.
- Inclui um editor de regras de correlação de eventos com uma GUI fácil de usar, para criar novas regras ou personalizar as existentes.

Para obter mais informações, visite **http://www.mcafee.com/br/products/siem/index.aspx**.

Figura 1. A correlação com base em riscos ajuda a detectar ameaças que visam os seus ativos mais importantes.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com