SIEM: cinco requisitos que resolvem os maiores problemas corporativos

Após mais de uma década atuando em ambientes de produção, as soluções de gerenciamento de eventos e informações de segurança (SIEM) agora são consideradas amadurecidas. Capacidades como coleta de eventos, correlação, alertas e demonstração de conformidade com regulamentações são o mínimo exigido e a maioria das soluções de SIEM atende a essas necessidades. Contudo, o cenário de ameaças está mudando. As organizações enfrentam novas ameaças, como os ataques direcionados e persistentes; novas tendências, como mobilidade, nuvem e virtualização; e mudança de prioridades de negócios em termos de aquisição de clientes, eficiências operacionais e redução de custos. Como resultado, os casos de uso do SIEM exigem capacidades mais avançadas para resolver questões corporativas críticas.

A McAfee conversou com usuários de SIEM e pediu que falassem sobre seus principais problemas com o SIEM. Os cinco principais problemas mencionados foram:

- Segurança de grandes volumes de dados
- Percepção situacional
- Contexto em tempo real
- Facilidade de gerenciamento
- Segurança integrada

Para que o SIEM ajude na obtenção de estratégias de gerenciamento de risco e segurança mais eficazes — particularmente no que se refere a eliminação de ameaças, adoção de tendências e alinhamento com as prioridades da empresa — essas cinco questões precisam ser resolvidas. Cada questão é descrita aqui juntamente com seus respectivos estudos de casos de clientes e casos de uso.

Caso de uso: segurança de grandes volumes de dados

- Expanda a captura de dados com mais canais de mais fontes
- Realize análises e perícias em conjuntos de dados muito grandes
- Otimize de acordo com os requisitos de velocidade e volume da segurança dos grandes volumes de dados
- Aumente as eficiências dos processos e dos funcionários

1. Segurança de grandes volumes de dados

A segurança de grandes volumes de dados pode ser extremamente valiosa — se você consegue utilizá-la. As soluções SIEM legadas não foram projetadas para se integrar com um número tão grande de terminais, redes e fontes de dados, não sendo indicadas para processar taxas de eventos tão altas ou manter políticas de retenção tão duradoura. Como resultado, bancos de dados relacionais e sistemas de SIEM legados semelhantes, desenvolvidos basicamente levando em consideração eventos centrados na rede, simplesmente não satisfazem as necessidades de segurança das infraestruturas dinâmicas de TI de hoje em dia. Eles não têm a velocidade, a extensibilidade e a expansibilidade para serem eficazes e usáveis.

Estudo de caso: governo federal

Uma grande agência governamental estava interessada em aplicar análises avançadas ao grande volume de dados de segurança armazenados no banco de dados relacional de múltiplos petabytes de seu SIEM. No entanto, até mesmo relatórios simples levavam horas para serem gerados e alguns levavam mais de um dia, tornando o SIEM da agência impossível de ser utilizado para fins forenses.

Ao adotar o McAfee® Enterprise Security Manager como solução de SIEM, a agência pôde expandir o número e os tipos de dispositivos integrados — acrescentando a suas análises mais contexto centrado nos dados e nos usuários. A agência também aumentou as taxas de eventos e os dados armazenados. Agora os relatórios são gerados em minutos, aprimorando toda a abordagem à análise forense.

Caso de uso: percepção situacional

- Enriqueça a percepção situacional com mais soluções de identidade
- Resolva quem, quando, como, onde e o que
- Compreenda por quanto tempo, quem mais e o que mais
- Inclua ativos BYOD, como laptops e smartphones

2. Percepção situacional

Houve um tempo em que o SIEM era simplesmente uma ferramenta para correlacionar eventos entre firewalls e sistemas de detecção de intrusões e, talvez, aplicar alguns dados de avaliação de vulnerabilidades. Mesmo hoje, existem alguns SIEMs que dependem principalmente de dados de fluxo de rede. Embora todas essas fontes sejam importantes, elas precisam ser enriquecidas com informações sobre identidade, contexto e aplicativos. Sem isso, exige-se mais tempo e recursos para compreender e priorizar eventos com uma inteligência situacional suficiente para servir como base para decisões em tempo hábil.

Estudo de caso: empresa de assistência médica

Uma empresa regional de assistência médica adotou a ideia BYOD ("bring your own device", traga seu próprio dispositivo) para aumentar a agilidade da equipe ao permitir tablets pessoais. Contudo, devido a incidentes passados, a empresa estava preocupada com o abuso por parte dos funcionários. A antiga solução de SIEM da empresa de assistência médica não tinha a capacidade de compreender quais usuários estavam interagindo com dados confidenciais independentemente do dispositivo — laptop, desktop, tablet ou desktop virtual.

Com o McAfee Enterprise Security Manager, a empresa de assistência médica conectou-se com produtos de gerenciamento de identidade e mobilidade, Active Directory e LDAP para obter percepção de usuários e dispositivos. Devido à integração com armazenamentos de dados estruturados e não estruturados, como o suporte nativo a banco de dados, bem como integração com prevenção de perda de dados (LDP) e monitoramento de atividade de banco de dados (DAM), houve uma percepção situacional mais completa e melhor eliminação de ameaças internas.

Caso de uso: contexto em tempo real

- Compreenda as ameaças dentro e fora do ambiente
- Aprimore a inteligência do SIEM com contexto em tempo real
- Reduza a identificação de incidentes e os tempos de resposta
- Identifique e priorize as ameaças com canais adicionais para entrada de informações sobre segurança

3. Contexto em tempo real

Um dos primeiros casos de uso de SIEM foi o gerenciamento de logs — coletar, armazenar, consultar e mais algumas funcionalidades extras. Os logs ainda são um componente de base do SIEM, mas os SIEMs de hoje também precisam de contexto em tempo real.

Exemplos de tal contexto são o McAfee Global Threat Intelligence (McAfee GTI) e o McAfee Vulnerability Manager. O McAfee GTI oferece um serviço de reputação em tempo real com base em nuvem, e o McAfee Vulnerability Manager coleta informações organizacionais sobre vulnerabilidades em ativos.

Estudo de caso: varejista

Um varejista da Fortune 100, sem um SIEM de produção e sem soluções da McAfee, realizou uma prova de conceito. Na primeira semana, o varejista descobriu que mais de 30% do tráfego que tentava entrar em sua rede era de fontes maliciosas e/ou continha cargas maliciosas.

Utilizando o McAfee Enterprise Security Manager para correlacionar informações de eventos com o McAfee GTI, o varejista rapidamente identificou quais ativos estavam sendo visados dentre todos os data centers e localizações de lojas, compreendendo melhor os tipos de ataque que estavam ocorrendo contra a organização. A solução McAfee SIEM determinou o mais alto nível de gravidade e, em seguida, priorizou uma resposta. O SIEM, combinado com contexto em tempo real, permitiu maior rapidez na detecção, priorização e correção das ameaças.

Caso de uso: facilidade de gerenciamento

- Distribua o SIEM com listas brancas dinâmicas e segurança assistida por hardware para proteger dispositivos de função fixa
- Simplifique a análise forense com detalhamentos personalizáveis
- Integre o SIEM com firewall e sistemas de prevenção de intrusões (IPS) para uma resposta rápida a incidentes
- Aumente a vida útil dos ativos legados com uma segurança aprimorada

4. Facilidade de gerenciamento

Os SIEMs legados têm arquiteturas muito rígidas e carência de algumas capacidades essenciais. Por exemplo, eles não se integram facilmente com dispositivos previamente não suportados para tornar as informações usáveis. Por outro lado, um SIEM de próxima geração é fácil de personalizar e suficientemente flexível para se adaptar a qualquer ambiente. É exatamente isso que torna um SIEM de próxima geração estratégico para tantas organizações.

Estudo de caso: empresa de serviços públicos

Uma grande empresa de serviços públicos precisava empregar controles de segurança para impedir que ataques do tipo Stuxnet afetassem a infraestrutura e causassem interrupções para milhões de consumidores. Com o McAfee Enterprise Security Manager, a empresa obteve percepção situacional em todas as zonas de sistemas de controle industrial (ICS), SCADA e TI corporativa, com suporte nativo de protocolos, aplicativos e dispositivos.

O McAfee SIEM proporcionou ao cliente as ferramentas necessárias para sua própria integração personalizada com os dispositivos ICS e SCADA. Isso, por sua vez, permitiu a correlação, a detecção de anomalias e a análise de tendências em todas as três zonas. Além de uma coleta de eventos personalizada, o cliente constroi, com rapidez e facilidade, dashboards, relatórios, regras de correlação e alertas exclusivos.

Isso tornou o SIEM uma ferramenta imprescindível para segurança, demonstração de conformidade com regulamentações e disponibilidade de ativos — em outras palavras, manteve as luzes acesas.

Caso de uso: segurança integrada

- Simplifique o fluxo de trabalho de segurança e operações
- Reduza a complexidade com automação e fácil personalização
- Melhore a visibilidade e a percepção situacional com soluções de segurança que funcionem juntas
- Ofereça uma segurança melhor com inteligência e integração

5. Segurança integrada

O SIEM é um componente importante de qualquer iniciativa estratégica de segurança, mas ainda é apenas um dentre muitos. A integração entre soluções de segurança e conformidade proporciona mais do que apenas a soma das soluções individuais separadas, enquanto uma arquitetura não integrada cria complexidade. A complexidade é o motivo pelo qual a segurança costuma permanecer principalmente tática, em vez de se tornar mais estratégica e alinhada com as prioridades dos negócios.

Estudo de caso: serviços financeiros

Um cliente multinacional do ramo bancário tinha uma grande quantidade de produtos diferentes de vários fornecedores. Alguns produtos estavam em produção, mas muitos não tinham uso ou manutenção regular por limitação de recursos. O banco determinou que, aproveitando o SIEM em conjunto com controles de dados, rede e terminais integrados, poderia amenizar mais efetivamente o risco e reduzir os custos, ao mesmo tempo que também tornaria a segurança mais relevante para os negócios.

O banco reduziu o número de fornecedores e fez economias de escala. Ele pôde reduzir os custos de treinamento e o número de agentes, consoles, servidores e mais. Isso também reduziu os custos contratuais e uma variedade de despesas associadas. Além das reduções de custos, o banco assegurou que todas as soluções existentes e futuras fossem completamente integradas com o McAfee Enterprise Security Manager para garantir melhores controles e visibilidade sobre sua postura de segurança.

Considerações fundamentais

- Quão importante é a capacidade de administrar facilmente os desafios de coleta, armazenamento, acesso, processamento e análise apresentados pela segurança dos grandes volumes de dados?
- As partes interessadas na segurança estão obtendo as informações de que necessitam e quando delas necessitam para tomar decisões informadas e ações imediatas?
- A equipe de segurança tem o contexto em tempo real de que necessita para identificar riscos e ataques antes que estes causem algum dano?
- Qual seria o impacto sobre a segurança e os recursos se você utilizasse um SIEM com detalhamento intuitivo e visualizações facilmente personalizáveis?
- Como a integração por sua infraestrutura melhoraria a segurança, a visibilidade, os processos e a agilidade nas respostas?

Os SIEMs legados que funcionavam bem na década anterior simplesmente não atendem os requisitos de hoje. Com novas exigências em torno de grandes volumes de dados, inteligência de segurança, percepção situacional, desempenho, usabilidade e integração, os casos de uso do SIEM expandiram-se. As soluções de SIEM devem reduzir a complexidade, e não criá-la. Espere mais do seu SIEM.

Atualmente, os SIEMs precisam operar como parte de uma estrutura de segurança maior e conectada, na qual as prioridades de negócios e de segurança estejam alinhadas. O SIEM desempenha um papel importante em tornar a segurança mais estratégica e em oferecer um valor de negócios autêntico.

Para saber mais sobre soluções de SIEM da McAfee, visite: www.mcafee.com/br/products/siem/index.aspx.

Security Connected

A plataforma Security Connected da McAfee oferece uma arquitetura unificada para centenas de produtos, serviços e parceiros aprenderem uns com os outros, compartilharem dados contextualizados em tempo real e atuarem como uma equipe para manter as informações e as redes seguras. Qualquer organização pode aprimorar sua postura de segurança e minimizar os custos operacionais através dos conceitos inovadores, dos processos otimizados e das economias práticas da plataforma.

McAfee
An Intel Company

McAfee do Brasil Comércio de Software Ltda.
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.mcafee.com/br