ManageEngine
Log360

CASO DE USO

Usando o Log360 para detectar escalonamentos de privilégios

Usando o Log360 para detectar escalonamentos de privilégios

Os ataques de escalonamento de privilégios têm como objetivo obter acesso aos recursos mais confidenciais da rede. Os invasores exploram vulnerabilidades como bugs, erros de configuração de aplicações e sistemas operacionais sem patches para comprometer uma conta de usuário e elevar seus privilégios. Eles podem fazer isso várias vezes, até que tenham privilégios suficientes para realizar um ataque, roubar dados confidenciais, implantar malware, criar back doors ou realizar qualquer outro objetivo que tenham.

A detecção de uma tentativa ou mesmo de um escalonamento de privilégios bem-sucedido oferece uma chance melhor de impedir que os invasores obtenham o poder necessário para realizar o ataque principal. Então, como garantir que sua organização possa detectar com êxito o aumento de privilégios?

Como o Log360 ajuda

O Log360 da ManageEngine, uma solução SIEM simples de usar, tem uma abordagem multifacetada para detectar o aumento de privilégios. Com recursos como auditoria extensiva, geração de relatórios e alertas, inteligência contra ameaças, correlação e análise de comportamento, veja como você pode aproveitar o Log360 para detectar e impedir o aumento de privilégios.

Monitore as mudanças na conta do usuário em tempo real:

Para detectar com êxito os escalonamentos de privilégios, é preciso garantir a visibilidade das ações dos usuários na rede. O Log360 oferece vários painéis de segurança para rastrear a atividade do usuário em tempo real. Com trilhas completas de auditoria de usuários e um console de alertas, você pode ser notificado sobre qualquer coisa, desde logons e logoffs até mudanças de grupos e contas de usuários.

Detecte e corrija instalações suspeitas:

O Log360 possui um mecanismo de correlação robusto e baseado em regras que pode detectar padrões nos dados de registro recebidos. Com uma série de regras incorporadas e um criador para personalizados, você pode detectar instalações suspeitas de software, serviços, malware e muito mais em seus dispositivos da estação de trabalho.

Identifique a atividade maliciosa do servidor de comando e controle (C&C) em tempo real:

O processador de feeds STIX/TAXII incorporado e auto atualizado do Log360 garante que você tenha uma ampla inteligência sobre ameaças para detectar invasores em sua rede. Ele correlaciona os feeds de ameaças com os dados de registro da rede e o notifica sobre tentativas de acesso de domínios, URLs e endereços IP maliciosos, que podem ocorrer durante ataques de escalonamento de privilégios.

Detecte ataques de escalonamento de privilégios com análise comportamental:

Os invasores garantem que permaneçam discretos ao realizar ataques de escalonamento de privilégios, dificultando sua detecção. O complemento User Entity Behavior Analytics (UEBA) do Log360 identifica todas as ações incomuns de um usuário específico, como logons remotos em horários estranhos e acesso a vários arquivos confidenciais. Em seguida,a solução aumenta a pontuação de risco do usuário e notifica o administrador de segurança em tempo real.

Automatize os fluxos de trabalho para reduzir o tempo de resposta:

O sistema automatizado de resposta a incidentes do Log360 tem fluxos de trabalho para executar ações específicas, como eliminar um processo, bloquear um USB e muito mais, assim que os alertas de correlação são acionados. Essa é uma das maneiras mais rápidas de interromper atividades mal-intencionadas, como instalações ilícitas de software, no momento em que elas ocorrem em sua rede. Você pode realizar uma investigação mais aprofundada com relatórios de correlação detalhados e prontos para uso.

Equipe sua organização com o Log360 para detectar e evitar o aumento de privilégios.

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.

Obtenha o 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 orçamento

Download