ManageEngine
EventLog Analyzer

Automatizando a resposta a incidente com workflows no EventLog Analyzer

www.eventloganalyzer.com

Introdução

De acordo com o estudo de 2018 da Ponemon sobre os custos com a violação de dados, as empresas levam em média 69 dias para conterem uma violação. É alarmante considerar que, mesmo após a sua identificação, normalmente leva mais de dois meses para conter seus efeitos. Onde as organizações estão errando?

Simplificando, muitas organizações carecem de um planejamento de resposta ao incidente. Um plano abrangente define claramente as pessoas, os processos e a tecnologia envolvidos na resposta a uma violação para que as organizações possam evitar confusões e resolver incidentes mais rapidamente.

A tecnologia desempenha uma função crucial na otimização do ciclo de resolução de incidentes. Das várias ferramentas e técnicas que você pode usar, os workflows de incidentes automatizados são os mais úteis. Cada vez que um possível incidente é detectado, eles executam automaticamente uma série de medidas corretivas comuns com base no tipo de incidente, aliviando a carga de trabalho de sua equipe de segurança.

Este resumo das soluções destaca os benefícios do uso de workflows de incidentes e explica como você pode os configurar de forma automatizada para alertas de incidentes no EventLog Analyzer.

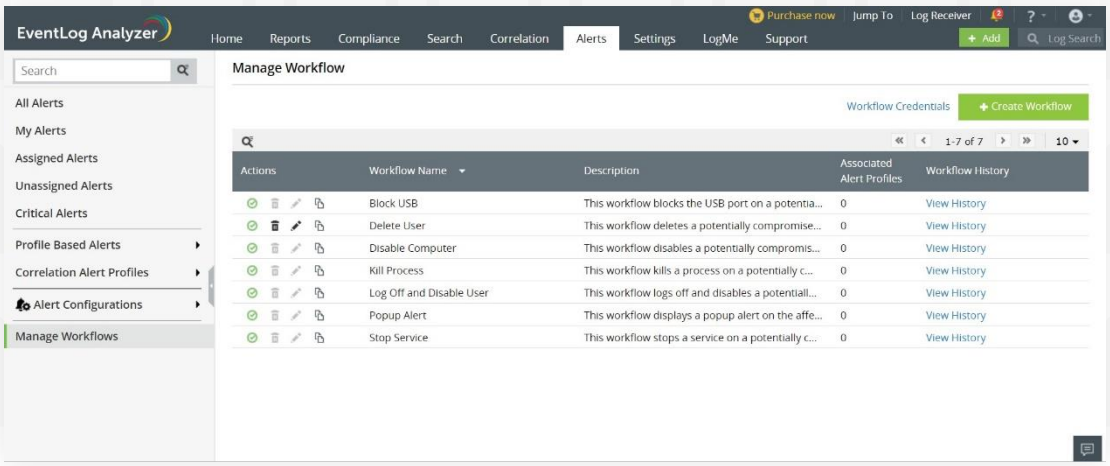
Benefícios de workflows de incidentes automatizados

- **Conter mais danos**. No mundo digital, alguns segundos é tudo que um invasor precisa para causar muitos problemas. As respostas automatizadas ajudam muito a conter possíveis danos à sua rede.

- **Fadiga de alerta reduzida.** Uma organização típica pode receber centenas de alertas de incidentes todos os dias. Workflos automatizados diminuem ou eliminam o tempo que você gasta respondendo a cada um, reduzindo assim a sua fadiga.

- **Uso otimizado do pessoal de segurança.** Como os colaboradores da equipe de segurança não precisam executar manualmente ações repetitivas banais em resposta a alertas de incidentes, eles estarão livres para investir seu tempo em incidentes mais complexos ou problemas de segurança que exijam sua atenção; ou eles podem ter tempo para se concentrar em projetos que impulsionam seus negócios, em vez de apenas mantê-los nos trilhos.

Usando workflows de incidentes no EventLog Analyzer



O EventLog Analyzer permite criar e gerenciar workflows de incidentes e automatizar etapas comuns de resposta. Os destaques incluem:

- **Construtor de workflow:** Use uma interface flexível de arrastar e soltar para criar workflows do zero. Escolha entre uma variedade de ações que gostaria de incluir, forneça os detalhes necessários e organize-os na ordem desejada.

- **Workflows integrados:** Utilize modelos de fluxo de trabalho predefinidos incluídos no produto.

- **Gerenciamento de workflows:** Visualize todos os workflows criados, habilite-os ou desabilite-os e visualize o número de perfis de alerta associados para cada um deles.

- **Rastreamento de workflow:** Exiba o histórico de cada workflow, visualize o status de todas as suas ocorrências e rastreie os detalhes de cada ação dentro dele.

- **Atribuição automática de incidentes:** Atribua incidentes automaticamente ao pessoal relevante que os pode rastrear e os gerenciar durante e depois da execução do workflow.

Exemplos de workflows de incidentes do EventLog Analyzer

Proteja os dados de insiders maliciosos

Embora as organizações configurem várias verificações contra ataques externos, elas tendem a negligenciar a ameaça representada por usuários internos mal-intencionadas. Os funcionários têm acesso fácil a dados confidenciais. Por exemplo, eles podem acessar fisicamente um servidor crítico e extrair arquivos em um dispositivo removível.

Para atenuar isso, você pode configurar um alerta para notificá-lo quando um dispositivo USB for conectado a este servidor fora do horário de trabalho. No entanto, apenas um alerta pode não ser suficiente. Você pode não ser capaz de impedir manualmente o roubo de dados, pois leva apenas alguns minutos para copiar arquivos.

Felizmente, o EventLog Analyzer fornece um workflow integrado, que pode bloquear a porta USB em um dispositivo e notificá-lo sobre o status. Com ele implantado, os funcionários não poderão obter informações confidenciais e você poderá investigar o incidente conforme sua conveniência.

Desabilite sistemas comprometidos em sua rede

Quando ocorre um incidente, a primeira etapa da investigação é revisar os logs do dispositivo, pois toda atividade de rede deixa um rastro. Às vezes, os invasores conseguem entrar em uma rede comprometendo uma conta de usuário legítimo. Eles podem então excluir logs das máquinas que violam para escapar da detecção ou ocultar sua presença contínua.

Felizmente, você pode configurar alertas para identificar quando os logs de segurança são apagados de uma máquina. Nestes casos, pode ser tarde demais para desfazer qualquer dano já causado, mas você pode impedir qualquer outra atividade mal-intencionada. O EventLog Analyzer fornece um workflow integrado para fazer logoff e desabilitar a conta de usuário comprometida, isolando com eficácia o invasor de sua rede.

Conclusão

Ao elaborar seu plano de resposta ao incidente, você deve identificar como impedir os vários tipos de incidentes que ocorrem e, em seguida, desenvolver as respostas apropriadas para eles, por meio de workflows automatizados. As respostas automatizadas fornecem vários benefícios empresariais, incluindo economia de custos e otimização do tempo da equipe, ao mesmo tempo em que mantém sua rede protegida contra ataques.