LogWatch

Gerenciamento Inteligente de Logs

by 3Elos Segurança em TI

Em virtude da heterogeneidade da infra-estrutura de TI das empresas, com servidores, estações e serviços disponibilizados de forma descentralizada e em plataformas diferentes, fica evidente a dificuldade de análise da massa de dados gerada por seus ativos. Com isso, grande parte das empresas não consegue avaliar os danos causados em sua infra-estrutura de TI.

Na pesquisa de 2003 do Computer Security Institute (CSI), em conjunto com o Federal Bureau of Investigation (FBI), de 530 gerentes de TI:

15% não sabem se algum recurso foi usado sem autorização

22% não sabem se seus sites Web foram usados/acessados indevidamente

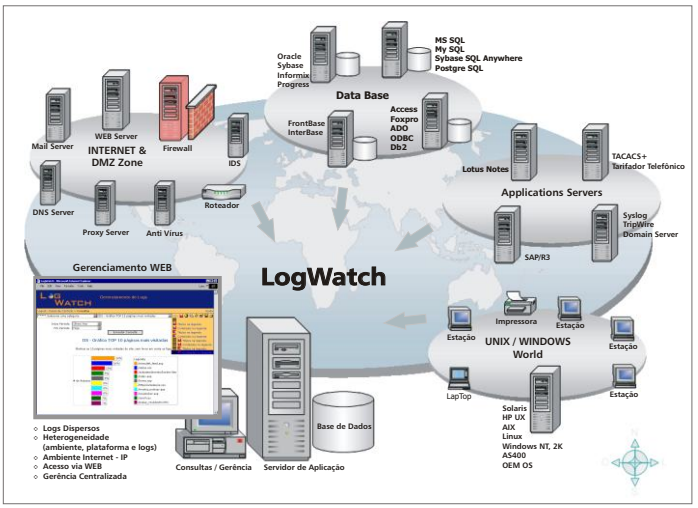
24% não sabem de onde os ataques foram originados (internos ou externos)

Os dados acima mostram que as empresas ainda não estão preparadas para detectar e prevenir as ameaças ao seu ambiente tecnológico.

Arquivos de log são a melhor forma de verificar a extensão de um incidente de segurança, identificando que ativo foi violado e que informação foi exposta. A maioria dos sistemas armazena seus eventos em arquivos de log no próprio equipamento e o processo de análise é feito de forma localizada e sem padronização, demandando um grande esforço. Sem ferramentas que possibilitem velocidade e precisão no levantamento das informações, a análise e correção de problemas torna-se uma tarefa muito custosa.

A gerência e a análise dos logs dos ativos torna-se, assim, uma atividade indispensável, gerando informações e conhecimento único para a empresa na correta aplicação de seus recursos.

O **LogWatch** é uma solução ágil, simples e eficaz para atender as necessidades de monitoramento e resposta aos eventos de segurança e da infra-estrutura de TI de sua empresa. Com ele é possível implementar, facilmente, vários agentes para consolidar os eventos do seu ambiente distribuído, incluindo sistemas operacionais, produtos de segurança, equipamentos de rede, bases de dados e aplicações de mercado.



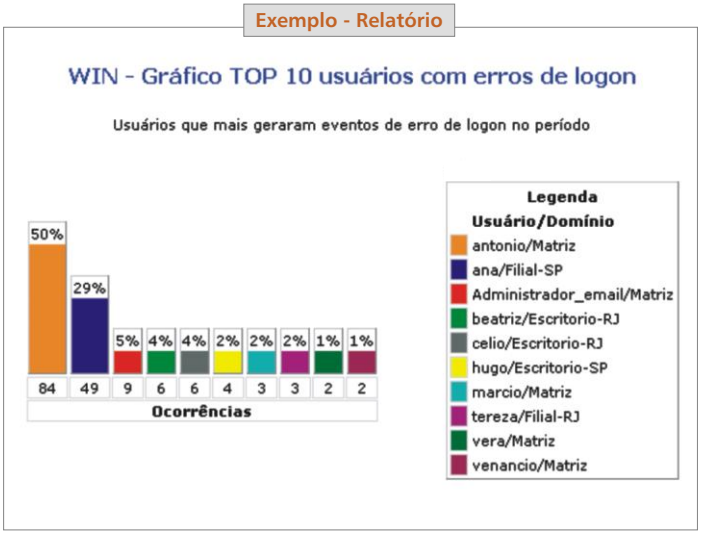
Principais benefícios

- Apoio na tomada de decisão
- Automatiza as tarefas manuais de análise de log, reduzindo a possibilidade de erros humanos
- Possibilita maior disponibilidade dos ativos críticos
- Reforça o cumprimento das políticas de segurança
- Possibilita a pronta resposta a incidentes internos e externos
- Permite mensurar a audiência dos eventos de Internet
- Adequação da empresa às leis regulatórias
- Possibilita mostrar os resultados e métricas de desempenho da infra-estrutura, aumentando a visibilidade da área de TI
- Agilidade no levantamento e análise de informações

Relatórios

Os relatórios do **LogWatch**, acessados via Web, concentram informações de forma organizada e detalhada para as áreas de segurança, auditoria ou tecnologia da informação. Podem, ainda, ser enviados por e-mail para qualquer usuário, na data e hora desejada.

Exemplo - Relatório



www.logwatch.com.br

Informações tratadas de forma inteligente.