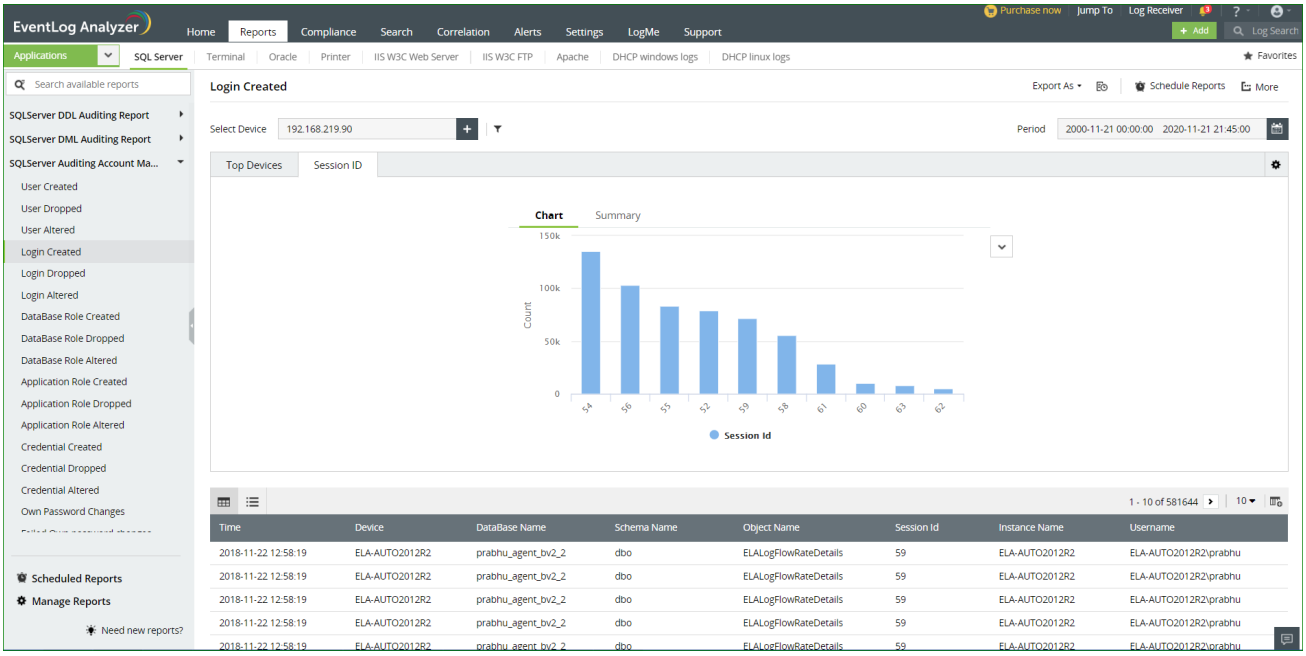
pinpoint GESTÃO DE TI | ManageEngine

EventLog Analyzer

Software para gerenciamento de log, auditorias e gerenciamento da conformidade de TI para SIEM. Saiba o que está acontecendo na sua rede, obtenha insights sobre as potenciais ameaças e as detenha antes que se transformem em um ataque bem sucedido.

Cada negócio gera diferentes logs dentro da rede que geram um enorme volume de dados, peneirar manualmente para encontrar eventos de segurança de interesse se torna inviável.



Recursos Disponíveis

Análise de Logs

Analisador personalizado, que extrai campos a partir de qualquer formato de log legível. Ao gerenciar os logs com o scanner de vulnerabilidades, a camada de inteligência contra ameaças e aplicações de prevenção contra perda, em um único console, equipes visualizarão todos os dados de log.

Auditoria de dispositivos na rede

O EventLog Analyzer faz a auditoria de dados de logs a partir de dispositivos de perímetro, incluindo roteadores, switches, firewalls e IDS/IPS para fornecer insights valiosos sobre altera em política ou regra de segurança do firewall, logons e logoffs dos usuários (incluindo os com falha) e tráfego de entrada e saída. Além disso, você pode configurar alertas com modelos pré-definidos para capturar eventos anômalos da rede.

Auditoria em aplicativos
Audite alterações críticas, detecte roubos de dados, identifique ataques e rastreie o tempo de inatividade nos aplicativos essenciais como bancos de dados e servidores de web.

Correlação de logs em tempo real
Detecte instantaneamente as tentativas de ataques e rastreie potenciais ameaças de segurança correlacionando os dados de log com mais de 20 regras pré-definidas em um construtor drag and drop. De forma automática, abra um ticket para o help desk e garanta uma rápida resolução do incidente. Além disso, o EventLog Analyzer reúne todos os eventos de segurança relativos a uma regra específica dentro de um relatório único, com visualização na forma de linha do tempo para auditoria de segurança eficaz.

Gerenciamento de conformidade integrado
Simplifique a auditoria de conformidade de TI com modelos de relatórios pré-definidos para diferentes órgãos regulatórios como PCI DSS, HIPAA, FISMA, GDPR, SOX, e ISO 27001. Arquive dados de logs por períodos personalizados para atender aos requisitos de arquivamento. Exporte relatórios em diferentes formatos, utilizando os modelos existentes ou criando novos.

Maior inteligência contra ameaças
Detecte ameaças a partir de endereços IP maliciosos através do EventLog Analyzer, que possui um banco de dados de ameaças de IP gerais e processador de feed STIX/TAXII. Identifique em tempo real qualquer interação maliciosa de endereço IP, URL ou domínio com sua rede. O sistema de inteligência contra ameaças do EventLog Analyzer é atualizado automaticamente todos os dias para ajudá-lo a se manter atualizado sobre as mais recentes ameaças. Integrado à ferramenta existe o recurso de gerenciamento de incidentes, apoiando a resolver incidentes rapidamente.

Sobre nós

A Pinpoint impulsiona empresas ao fortalecer as tecnologias que sustentam sua operação, com soluções integradas para redes, monitoração e gestão ágil de TI preparadas para ambientes complexos e redes distribuídas.

Desde 2009, garantimos a estabilidade e a eficiência de operações críticas, apoiando gestores de tecnologia e operações a superarem os desafios de um cenário dinâmico e exigente. Porque cada minuto importa, e a visibilidade e o uso inteligente dos recursos fazem toda a diferença.

Como parceiros estratégicos da ManageEngine no Brasil, trazemos um conjunto abrangente de soluções focadas em simplificar a gestão de TI e segurança. Sua força está na capacidade de integrar funções essenciais (endpoints, identidade, ITSM, ITOM) em plataformas coesas, oferecendo eficiência e controle.

Transforme sua TI em motor de crescimento

Fale com nossos especialistas e veja como simplificar processos, ganhar controle e liberar sua equipe para o que realmente importa.

11 3900-1391 | comercial@pinpoint.com.br | pinpoint.com.br