



GFI EventsManager

Zcentralizowane zarządzanie ochroną i monitoring rejestru zdarzeń

Rejestry zdarzeń to wartościowe narzędzia monitorujące bezpieczeństwo sieci i wydajność. Ze względu na swoją zawartość i objętość są często nie w pełni wykorzystywane. Wraz ze swoim rozwojem, firmy potrzebują coraz bardziej zorganizowanego podejścia do zarządzania i utrzymania rejestru zdarzeń. Ostatnie badania przeprowadzone przez SANS Institute pokazują, że 44% administratorów nie przechowuje rejestrów zdarzeń dłużej niż miesiąc.

Właściwe zarządzanie rejestrem zdarzeń pomaga osiągnąć następujące cele:

- Zapewnienie bezpieczeństwa systemu informatycznego i sieci
- Monitoring stanu systemu
- Spełnianie wymogów prawa (SOX, PCI DSS, HIPAA)
- Zapewnienie materiału dowodowego w przypadku postępowania sądowego

GFI EventsManager zbiera informacje ze wszystkich urządzeń, które są odnotowane w rejestrze zdarzeń systemu Windows, W3C i Syslog oraz dostosowuje reguły filtrowania odpowiednie do zidentyfikowania kluczowych danych. Umożliwia to ocenienie jak pracownicy wykorzystują swój czas pracy, czy dzwonią do domu, kiedy włączają swoje komputery i z jakich plików korzystają w godzinach pracy. GFI EventsManager alarmuje także w czasie rzeczywistym o zagrożeniach dla systemu i bezpieczeństwa, które mogą wymagać natychmiastowej interwencji.

■ Niewiarygodnie proste analizowanie rejestrów zdarzeń całej sieci

Jako administrator sieci z pewnością doświadczyłeś smaku nużącego procesu analizowania enigmatycznych i obszernych rejestrów. GFI EventsManager jest rozwiązaniem analizującym rejestry, które zapewnia kontrolę nad rejestrami zdarzeń systemu Windows, W3C i Syslog w obrębie całej sieci firmowej. GFI EventsManager posiada inteligentny procesor zdarzeń, który analizuje i prezentuje zebrane dane w scentralizowany, przyjazny dla użytkownika sposób.

Korzyści

Po co korzystać z GFI EventsManager?

Zbiera zdarzenia syslog, W3C i Windows wygenerowane przez firewalle, serwery, routery, switch-e, systemy telefonii, komputery PC i inne

Kreator konfiguracji upraszcza działanie i utrzymanie

Niezrównana wydajność skanowania sprawdza ponad 6 milionów zdarzeń na godzinę.

Predefiniowane procedury przetwarzania zdarzeń zaplanowane na klasyfikowanie i zarządzanie nieprzewidywanymi zdarzeniami.

Automatyczny całodobowy monitoring i informowanie o zagrożeniach
Potężne i efektywne narzędzie do monitorowania aktywności w sieci, gwarantujące natychmiastowy zwrot kosztów inwestycji

■ „Tłumaczenie” zawitych rejestrów

Analiza zawitych zapisów rejestrów jest długotrwałym procesem. GFI EventsManager zmienia niejasne, enigmatyczne opisy na zwarte i jasne wyjaśnienia oraz sugeruje możliwe rozwiązania.

■ Centralny rejestr zdarzeń

Rejestry zdarzeń są ciągle automatycznie generowane przez użytkownika lub proces działający w tle i przechowywane w rozproszonych lokalizacjach. GFI EventsManager zbiera wszystkie rejestry w jedną bazę SQL. Można również skonfigurować tworzenie zaplanowanych kopii zapasowych rejestrów zdarzeń.

■ Wysoce wydajny skaner

GFI EventsManager ma wbudowany zupełnie przeprojektowany skaner rejestru ustawiony na maksymalną wydajność skanowania. Testy wykazały, że jest on w stanie przeskanować i zebrać do 6 milionów zdarzeń na godzinę. Co więcej, jego metodologia oparta na wtyczkach pozwala dołączyć dodatkowe funkcje i moduły bez ingerowania w istniejący kod.

■ Ostrzeżenia w czasie rzeczywistym

GFI EventsManager potrafi wysyłać ostrzeżenia o wtargnięciach lub kluczowych zdarzeniach. Na takie sytuacje można szybko zareagować za pomocą skryptu lub wysłać zawiadomienie o nich do jednej lub wielu osób za pomocą e-maila, wiadomości sieciowej lub za pomocą SMS-a z bramki SMS-owej.

■ Rozbudowane wsparcie rejestru zdarzeń

GFI EventsManager przetwarza różne rejestry zdarzeń: systemu Windows, syslog czy W3C. Pozwala to zbierać więcej danych z komputerów i systemów komputerowych, najchętniej wykorzystywanych w firmowych sieciach komputerowych.

■ Inne cechy:

Usuwanie "szumu" oraz nieistotnych zdarzeń stanowiących większość zdarzeń związanych z bezpieczeństwem.

- Monitoring i ostrzeżenia w czasie rzeczywistym przez cały rok 24 godziny na dobę.
- Graficzny monitoring statusu GFI EventsManagera i ruchu w sieci dzięki wbudowanemu monitorowi statusu.
- Planowanie raportów i automatyczne wysyłanie za pomocą e-maila.

■ Jesteś w dobrym towarzystwie...

Wiele wiodących firm wybrało GFI EventsManager. Oto tylko niektóre z nich: Primerica, Pepsico France, Royal & Sunalliance USA Inc., ATP, Ceridian Canada. i wiele innych.

Wymagania systemowe

- System operacyjny Windows 2000 Pro lub Server, Windows XP lub Windows 2003
- Serwer i klient musi pracować na Windows NT, 2000, XP lub 2003

Nagrody



Pobierz wersję testową z <http://www.gfi.com/eventsmanager/>

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

ed&r Polska Sp. z o.o.
Biuro Handlowe
ul. Nowy Świat 32/106
Lublin 20 - 418
PL
Tel. +48/ 81/ 534-83-25
Fax. +48/ 81/ 534-83-26
gfi@edr.pl



ed&r
IT Experts Group
GFI
Authorised distributor
SECURITY SPECIALIST