EVENTSENTRY

Dobrze jest wiedzieć kiedy należy szybko działać.

Dlatego stworzyliśmy narzędzie pozwalające szczegółowo i w czasie rzeczywistym analizować dane.

EventSentry to idealne rozwiązanie do monitorowania incydentów bezpieczeństwa, pomagające zespołom IT w czasie rzeczywistym podejmować skuteczne decyzje w ochronie zasobów i danych. Niezawodne, wydajne, rozbudowane, łatwe we wdrożeniu i obsłudze narzędzie znacząco zwiększa skuteczność pracy zespołów odpowiedzialnych za utrzymanie bezpieczeństwa. EventSentry pozwala zaoszczędzić czas na analizach dużej ilości danych, pozwala znacznie zmniejszyć koszt utrzymania bezpieczeństwa (TCO) w stosunku do pozostałych narzędzi dostępnych na polskim rynku. Narzędzie otrzymało nagrodę „award-winning" za doskonałą obsługę i oferowane wsparcie klientom

KLUCZOWE CECHY:

- Zbieranie i analiza w czasie rzeczywistym dzienników zdarzeń, logów i alertów, w tym również między innymi informacji o wydajności, dostępnej przestrzeni dyskowej, kondycji działających usług i procesów dostarczanych zarówno przez systemy fizyczne, systemy wirtualne, stacje robocze, serwery jak i pozostałe urządzenia sieciowe.
- Monitorowanie procesów systemowych, logowania sieciowego, dostępu do plików, zdarzeń wynikających z zarządzania kontami użytkowników, w tym również monitorowanie zgodności z wymaganiami PCI, SOX, HIPAA, CJIS i innych.
- Szeroko konfigurowalny moduł prezentowania zdarzeń, posiadający wiele różnych szablonów wizualizacyjnych, indywidualnie dopasowany do każdego użytkownika. Rodzaj przedstawianych zdarzeń zależy od posiadanych przez użytkownika uprawnień.
- Bezpieczna, szyfrowana komunikacja między systemem zarządzającym a monitorowanym komponentami.
- Możliwe rozbudowanie podstawowej funkcjonalności narzędzia o wbudowane bądź stworzone własnoręcznie skrypty monitorujące.

OPINIE KLIENTÓW:

"EventSentry bardzo szybko stał się podstawowym narzędziem monitorowania bezpieczeństwa krytycznych komponentów teleinformatycznych naszej infrastruktury"

„Szwajcarski scyzoryk w rozwiązaniach monitorujących sieci teleinformatyczne"

"Skalowalność narzędzia wyprzedza konkurencję"

„Obsługa klienta jest na bardzo wysokim poziomie"

"Wdrożyliśmy narzędzie do monitorowania infrastruktury w ciągu kilka minut"

„Aplikacja znacząco wykracza poza zwykłe logowanie dziennika zdarzeń"

„Działa zgodnie z założeniami"

"Dzięki temu narzędziu poznaliśmy naszą infrastrukturę z zupełnie innej strony"

Version 3.2

www.eventsentry.com

Opis właściwości

EVENTSENTRY

Monitorowanie i zbieranie zdarzeń
Zbieranie i monitorowanie zdarzeń w czasie rzeczywistym z wykorzystaniem zaawansowanych funkcji takich jak np. zdefiniowane progi, powtarzające się zdarzenia, czasy występowania, występowanie spersonalizowanych znaków.

Zgodność z wymaganiami
Monitorowanie aktywności dostępu do plików, procesów i konsoli terminalowych, monitorowanie udanego i nieudanego logowania, monitorowanie zmian w procesie zarządzania użytkownikami, zgodności z wymaganiami PCI, HIPAA, SOX, CJIS, itd.

Zbieranie i analizowanie plików logów
Monitorowanie i zbieranie informacji z dowolnych plików logów takich usług jak np. IIS, DHCP, Backup, Firewall, w czasie rzeczywistym. Tworzenie dopasowanych do potrzeb raportów.

Monitorowanie wydajności
Monitorowanie i zbieranie danych o wydajności systemów operacyjnych Windows z wykorzystaniem usługi SNMP. Wbudowana inteligencja wykrywania problemów i samodoskonalenia procesu monitorowania.

Rozszerzona inwentaryzacja
EventSentry monitoruje aktualność zainstalowanych aktualizacji systemowych, przedstawia informacje techniczne o działającym sprzęcie, a nawet o gwarancji jakiej podlegają komponenty sprzętowe, takich firm jak Dell©, HP©, IBM©

Monitorowanie przestrzeni dyskowej
Przesyłanie alertów bazujących na ustawionych limitach dostępnego miejsca dla dysku bądź folderu. Przedstawianie statystyk najbliższego wykorzystania miejsca. Wskazywanie 250 plików zajmujących najwięcej przestrzeni dyskowej.

Synchronizacja czasu
Sprawdzanie i opcjonalna synchronizacja lokalnego czas monitorowanych komponentów zgodnie ze standardami RFC 1769 i RFC 1305.

Procesy, Usługi i Harmonogramy
Aktywne monitorowanie usług, zaplanowanych zadań i samodzielnie działających procesów. Ponowne uruchomienie źle działających procesów lub usług.

Bezpieczeństwo
Podniesienie poziomu bezpieczeństwa poprzez monitorowanie w czasie rzeczywistym plików zdarzeń, monitorowanie naruszenia integralności plików, dostępności działania usług. Wykrywanie za pomocą protokołu ARP nowych urządzeń podłączonych do sieci.

Powiadomienia
EventSentry zawiera 16 różnych sposobów powiadomień, pozwalających przesłać alerty do użytkownika za pomocą protokołów: SMTP email, Syslog, SNMP Traps, http(s), komunikator Jabber (IM), wpisu do bazy danych, SNPP, RSS, utworzeniu pliku tekstowego, uruchomieniu procesu lub usługi sieciowej, wyświetlając komunikat na monitorze, itp.

Wykorzystanie zasobów
Agenci monitorujący komponenty teleinformatyczne nie wpływają negatywnie na wydajność monitorowanych komponentów. Wdrożenie EventSentry nie wymaga zwiększania wydajności infrastruktury sieciowej co powoduje, że jest rozwiązaniem ekonomicznym finansowo.

Komunikacja z centralny systemem zarządzania
Komunikacja między systemem zarządzającym a monitorowanymi systemami jest szyfrowana. Zastosowana kompresji danych nie wpływa negatywnie na wydajność.

Dostęp do raportów przez portal webowy
Najnowszej generacji moduł raportowania pozwala dopasować ekran do przedstawiania wybranych przez użytkownika zdarzeń. Rozszerzony interfejs API umożliwia dostęp do danych aplikacjom firm trzecich.. Portal obsługiwany jest przez większość dostępnych przeglądarek, również na urządzeniach mobilnych.

Monitorowanie dostępności
EventSentry monitoruje czas działania usług TCP oraz komponentów teleinformatycznych monitorując w ten sposób ich aktualną dostępność.

Monitorowanie usługą Syslog/SNMP/ARP
EventSentry zbiera wiadomości wysyłane protokołami Syslog messages, SNMP traps (v1-v3) z dowolnych urządzeń i systemów. Zdefiniowane zdarzenia przesyłane są do systemu centralnego w czasie rzeczywistym.

Monitorowanie czasu działania
Rejestrowanie całkowitego czasu działania komponentów środowiska w trybie ciągłym umożliwia zidentyfikowanie problemów związanych np. z nieplanowanym uruchomieniem ponownym systemu.