

Sentinel™ firmy Novell: zarządzanie bezpieczeństwem i zgodnością z regulacjami

Novell.

Integracja i automatyzacja zarządzania bezpieczeństwem i zgodnością z regulacjami

W środowisku IT pozbawionym rozwiązania działającego w czasie rzeczywistym zgodność z regulacjami można utracić praktycznie w mgnieniu oka. Co na przykład zrobić, jeśli firewall informuje o istotnym problemie, zaś system wykrywania włamań nas nie alarmuje? Który system się myli? W jaki sposób należy zareagować? Jak następnie upewnić się, że problem związany z bezpieczeństwem został rozwiązany? Jak udowodnić audytorowi, że wprowadzone elementy kontrolne mające na celu wyeliminowanie potencjalnych zagrożeń działają prawidłowo? Odpowiedzią na te problemy jest wszechstronne rozwiązanie, które dostarcza niezbędne informacje w czasie rzeczywistym. Odpowiedzią jest oprogramowanie Sentinel™ firmy Novell.

Osoby odpowiedzialne za bezpieczeństwo informacji w firmie za pomocą oprogramowania Sentinel mogą utworzyć rygorystyczne programy utrzymania bezpieczeństwa i zgodności z regulacjami obowiązujące w całym przedsiębiorstwie, usprawnić pracochłonne i podatne na błędy procesy ręcznej sprawozdawczości, a dzięki wbudowanej w Sentinel automatyzacji — zmniejszyć koszty z tym związane.

Współczesne problemy biznesowe

Obecnie większość instytucji i przedsiębiorstw stoi przed podobnymi problemami związanymi z zabezpieczaniem systemów i uzyskaniem zgodności z regulacjami:

- **Nadmiarowe koszty i ryzyko.** *Wyzwania związane z osiągnięciem zgodności z regulacjami oraz z zarządzaniem ryzykiem stają się coraz bardziej rozległe i bardziej złożone. Jednocześnie dział IT zmaga się z rosnącymi kosztami oraz z koniecznością spełnienia potrzeb użytkowników — bez obniżania poziomu bezpieczeństwa. Dotychczas firmy i instytucje radziły z tym sobie opracowując wyspecjalizowane narzędzia i ręczne procesy — drogie, nieefektywne i zwracające niespójne wyniki.*
- **Braki w integracji.** *Opracowano jak dotąd niewiele sprawdzonych procedur, a także osiągnięto niewielki stopień centralizacji w zakresie monitorowania sieci oraz zarządzania zdarzeniami. Dane są rozproszone, przechowywane w różnych bazach danych, systemach plików i aplikacjach. Niektóre narzędzia skupiają się na urządzeniach, zaś inne na tożsamości użytkowników. Zadanie utworzenia skonsolidowanego widoku osób, procesów i technologii w dużym przedsiębiorstwie może okazać się ponad siły.*
- **Bezpieczeństwo to cel ruchomy.** *Intruzi stale wystawiają na próby zewnętrzne mechanizmy zabezpieczeń, zaś do zarządzania potencjalnymi zagrożeniami wewnętrznymi potrzeba ciągłego nadzoru. Bycie „krok do przodu” jest prawie niemożliwe, szczególnie wobec faktu, że sieć jest rozszerzana wciąż o nowych użytkowników i nowe zasoby.*
- **Pełna zgodność z regulacjami wydaje się niemożliwa do osiągnięcia.** *Bez rozwiązania działającego w czasie rzeczywistym można utracić zgodność z regulacjami praktycznie w mgnieniu oka. Często firmy i instytucje podlegają różnym nowym regulacjom, o różnych terminach obowiązywania, co powoduje nigdy niekończący się wyścig z czasem w celu utrzymania zgodności z regulacjami.*

Aby zaradzić tym problemom, wiele przedsiębiorstw i instytucji stosuje ręczne procesy, które okazują się zwykle niemożliwe do utrzymania. Sama logistyka stanowi duży problem. Przedsiębiorstwa muszą zatrudniać wiele osób do monitorowania dzienników zdarzeń z wielu różnych urzędzeń, systemów i aplikacji znajdujących się w bardzo rozproszonych sieciach. Osoby te muszą analizować i zinterpretować duże ilości danych, a następnie przygotować raporty dowodzące nie tylko, że firma lub instytucja wprowadziła wymagane elementy nadzoru informatycznego, ale także iż działają one tak, jak powinny. Proces zbierania tych danych, analizowania ich i tworzenia raportów może trwać miesiące — na tyle długo, że dane stają się archaiczne w momencie, w którym docierają do decydentów.

Bezpieczeństwo firmy a zgodność z regulacjami

Czym więcej zmian, tym bardziej obciążające stają się wymagania związane ze zgodnością z regulacjami. Firmy amerykańskie wydały w 2006 r. około 15 mld. USD na technologie i usługi pomagające spełnić wymagania związane z regulacjami federalnymi, by zminimalizować ryzyko i zagwarantować klientom oraz partnerom, że sieci i dane są dobrze zabezpieczone¹. Nie miały innego wyjścia, gdyż taka jest cena prowadzenia działalności. Aż do teraz, procesy ręczne wykorzystywane przez firmy i instytucje do przygotowania wymaganych raportów, były bardzo złożone, czasochłonne i podatne na błędy.

Zarządzanie rozproszonym, heterogenicznym środowiskiem zabezpieczeń informatycznych przy użyciu narzędzi konwencjonalnych to syzyfowa praca. Wszystkie elementy takie jak serwery, bazy danych, aplikacje, zapory, routery, przełączniki, a także systemy wykrywania włamań oraz zapobiegania włamaniom, dostarczają danych, które muszą być agregowane i przeanalizowane w celu uzyskania wyraźnego obrazu bezpieczeństwa firmy oraz jej zgodności z regulacjami. Jeśli zaś chodzi o bezpieczeństwo, to każdy proces, system czy też urządzenie w sieci stanowią potencjalnie słabe ogniwo. Odpowiedzią na te problemy jest właśnie oprogramowanie Sentinel firmy Novell.

Rozwiązanie Sentinel

Sentinel firmy Novell to wszechstronne rozwiązanie do zarządzania informacjami o zabezpieczeniach oraz zdarzeniami w sieci. Zapewnia ono pełny wgląd we wszystkie aspekty kontroli bezpieczeństwa oraz zgodności z regulacjami, w czasie rzeczywistym, w dowolnym środowisku informatycznym. Oprogramowanie Sentinel zapewnia zintegrowany widok zdarzeń w sieci mających wpływ na bezpieczeństwo oraz zgodność z regulacjami. Pozwala administratorom zidentyfikować zarówno zewnętrzne jak i wewnętrzne zagrożenia dla bezpieczeństwa oraz wszelkiego rodzaju naruszenia zgodności z regulacjami. Dzięki systemowi Sentinel, administratorzy mogą podejmować natychmiastowe działania w celu wyeliminowania słabych punktów — w oparciu o wymagania związane z regulacjami, strategię biznesową firmy, a przede wszystkim w oparciu o role użytkowników pełnione w organizacji.

Sentinel łączy zalety systemów kontroli tożsamości i zarządzania systemami z zaletami systemów do monitorowania zdarzeń związanych z bezpieczeństwem w czasie rzeczywistym. Na pojedynczej konsoli przedstawia wszechstronny widok zdarzeń powiązanych z użytkownikami, sieciami i aplikacjami. Dzięki temu można szybciej i skuteczniej reagować na potencjalne zagrożenia. Usprawnia ponadto procesy

¹ AMR Research, Boston, wg wersji online magazynu Sarbanes-Oxley Compliance Journal, Email Management and Sarbanes Oxley Compliance, 2006-06-08, Craig Rhinehart

ręcznej sprawozdawczości (czasochłonne i podatne na błędy) redukując związane z tym koszty. I co najważniejsze, Sentinel pomaga utworzyć rygorystyczne programy utrzymania bezpieczeństwa oraz zgodności z regulacjami w całym przedsiębiorstwie.

Inteligentna automatyzacja oparta na regułach

Sentinel automatyzuje identyfikację incydentów i rozwiązywanie problemów w oparciu o wbudowane reguły biznesowe. Reguły te można łatwo dopasować do strategii firmy lub instytucji oraz obowiązujących procedur, jednocześnie utrzymując zgodność z regulacjami. Dzięki systemowi Sentinel administratorzy systemów informatycznych mogą monitorować przypadki naruszenia bezpieczeństwa oraz śledzić status rozwiązywania problemów. Mogą też szybko identyfikować (przy użyciu praktycznie dowolnego źródła danych) nowe trendy występujące w całym przedsiębiorstwie czy też pojedyncze ataki. Informatycy mogą operować na informacjach graficznych zbieranych w czasie rzeczywistym lub też przeglądać informacje historyczne dotyczące konkretnego urządzenia, użytkownika lub zdarzenia, obejmujące czas sprzed kilku sekund czy godzin.

Sentinel wykorzystuje techniki korelacji wykonywane w pamięci, aby zmniejszyć obciążenie bazy danych i przyspieszyć proces dostarczenia ważnych danych o zdarzeniach do centralnej konsoli. Może połączyć się z dowolnym urządzeniem, które wykorzystuje protokoły SNMP, ODBC lub inne standardy. Sentinel nie wymusza też stosowania określonej platformy, gdyż działa i jest zgodny z wieloma systemami, jak Windows*, UNIX*, Solaris* i Linux*.

Natychmiastowe korzyści

Sentinel zaraz po wdrożeniu informuje o stanie elementów służących do nadzoru informatycznego oraz urządzeń wykorzystywanych do zabezpieczenia sieci. Jeśli zdarzy się problem, informuje jak go rozwiązać i uruchamia automatyczną procedurę przepływu pracy w celu śledzenia statusu działań związanych z rozwiązywaniem problemu. Dlatego Sentinel jest idealnym rozwiązaniem np. dla instytucji finansowych, czy centrów medycznych, gdyż mają one prawny obowiązek chronienia danych klientów lub pacjentów. System Novella dostarcza informacje niezbędne do tego, by udowodnić audytorom, akcjonariuszom oraz klientom, iż dane są odpowiednio zabezpieczone.

Zasadność stosowania oprogramowania Sentinel

Sentinel pomaga informatykom podejmować szybkie decyzje i skutecznie reagować na wszelkie zdarzenia — od ataku wirusów po nieuprawnione żądanie dostępu do aplikacji finansowej firmy. Tworzy też dziennik kontroli dotyczący wszystkiego, co dzieje się w sieci. Sentinel identyfikuje i dokumentuje zarówno znane jak i nowe zagrożenia, by można było szybko reagować i skutecznie rozwiązywać problemy, a w razie potrzeby — by udowodnić audytorom, że nadzór informatyczny działa prawidłowo.

Najważniejsze korzyści wynikające ze stosowania oprogramowania Sentinel

Sentinel zapewnia:

- *Zintegrowane, skalowalne i zautomatyzowane monitorowanie bezpieczeństwa i zgodności z regulacjami, w czasie rzeczywistym, obejmujące wszystkie systemy i sieci.*
- *Zautomatyzowane reakcje na zdarzenia związane z zarządzaniem użytkownikami i bezpieczeństwem. Na przykład próba dostępu do danych finansowych podjęta przez niepowołaną*

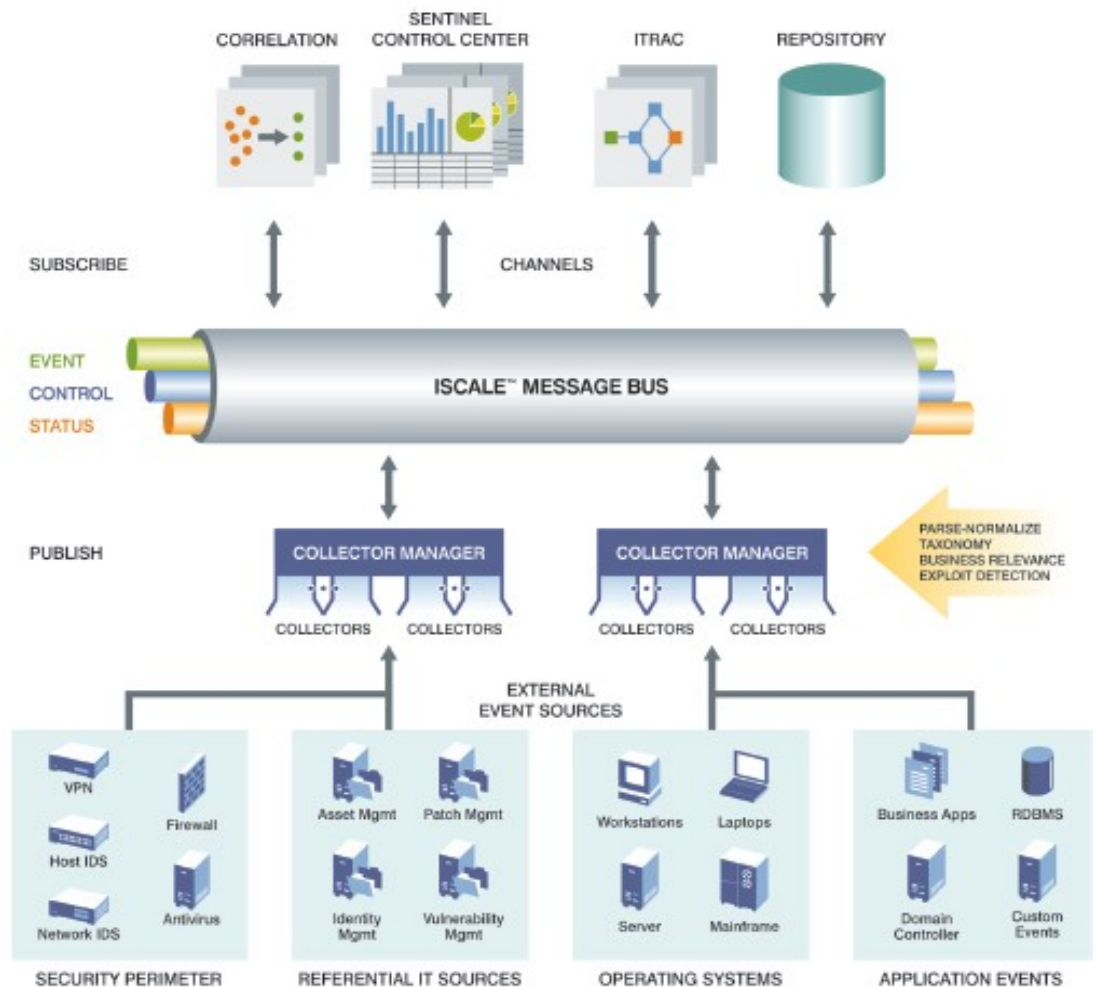
osobę może spowodować zapisanie szczegółowych informacji o zdarzeniu oraz przesłanie poczty elektronicznej do osoby odpowiedzialnej w firmie za bezpieczeństwo.

- *Możliwość analizowania zdarzeń związanych zarówno z użytkownikami, jak i urządzeniami, przy użyciu pojedynczego narzędzia.*
- *Środowisko, które umożliwia ustalenie strategii informatycznej i podejmowanie działań w oparciu o strategię biznesową. Możliwość samodzielnego ustalenia kryteriów alarmów, miar, a także poziomu szczegółowości danych w raportach.*
- *Zautomatyzowane zbieranie, analizowanie, korelowanie, rozwiązywanie i raportowanie zdarzeń związanych z bezpieczeństwem oraz zgodnością z regulacjami, obejmujące całość przedsiębiorstwa.*
 - Wstępnie skonfigurowane i łatwe do dostosowania Kolektory zbierają dane z dowolnych systemów, procesów lub urządzeń w sieci przedsiębiorstwa.
 - Reguły korelacji pozwalają przeanalizować dane w czasie rzeczywistym, zidentyfikować przypadki naruszenia bezpieczeństwa lub zgodności oraz zweryfikować zdarzenia w różnych narzędziach i systemach.
 - Działania podjęte w celu rozwiązania problemu mogą być wykonywane w oparciu o szablony procesów.
 - System dostarcza raporty dostosowane do przepisów lub ról pełnionych przez użytkowników w organizacji, co pozwala stale oceniać i potwierdzać zgodność z regulacjami.
- *Wykrywanie nowych zagrożeń, gdy tylko pojawią się gdziekolwiek na terenie przedsiębiorstwa.*
- *Możliwość monitorowania i udowodnienia zgodności ze strategią wewnętrzną firmy i regulacjami takimi jak Sarbanes-Oxley, HIPAA, GLBA i FISMA.*
- *Pełna sprawozdawczość w zakresie bezpieczeństwa i zgodności z regulacjami, która wykracza znacznie poza dostarczanie prostych plików dziennika.*
 - Konsole i raporty dla kierownictwa prezentują pojedynczy widok każdego zdarzenia.
 - Analiza z uszczegóławianiem oraz modelowanie pozwalają zaprojektować scenariusze „co by było, gdyby...” oraz umożliwiają aktywne zarządzanie, które jest niezbędne do wszechstronnego zarządzania bezpieczeństwem i zgodnością z regulacjami.

Jak działa Sentinel

Podstawowa funkcjonalność oprogramowania Sentinel koncentruje się na zarządzaniu bezpieczeństwem i zgodnością z regulacjami. W tym celu Sentinel:

- *Pobiera dane z wielu rodzajów urządzeń, źródeł odniesienia, systemów operacyjnych oraz aplikacji.*
- *Analizuje i koreluje dane o zdarzeniach, aby określić czy zdarzenie narusza wstępnie zdefiniowany warunek lub przekracza akceptowalne progi. Jeśli tak, system informuje o „incydencie”.*
- *Umożliwia tworzenie mechanizmów przepływu pracy w celu automatyzacji wykrywania incydentów i obsługi procesów naprawczych.*
- *Zapisuje powiązane z incydemtem dane do dalszej analizy.*
- *Dostarcza raport o zdarzeniu w kontekście określonych reguł biznesowych i wymagań stawianych przez przepisy. Gwarantuje to pełen widok zdarzeń w sieci, a także całościowego bezpieczeństwa i zgodności z regulacjami w przedsiębiorstwie.*



Rys. 1. Architektura systemu Sentinel

Siedem głównych elementów architektury systemu przedstawionych na powyższym diagramie opisano w dalszej części tego dokumentu. Natomiast dolna część diagramu przedstawia cztery obszary, z których system Sentinel może pobierać dane o zdarzeniach:

- *Urządzenia bezpieczeństwa na granicy sieci, takie jak systemy VPN, zapory, routery i przełączniki.*
- *Źródła odniesienia takie jak systemy zarządzania tożsamością, zarządzania zasobami oraz zarządzania poprawkami.*
- *Główne urządzenia do przetwarzania informacji, takie jak serwery łącznie z serwerami klasy mainframe, stacje robocze i laptopy.*
- *Aplikacje użytkownika, systemy zarządzania bazami danych, kontrolery domen i systemy pracy grupowej.*

Kolektory i Menedżery kolektorów

Kolektory systemu Sentinel (*Collector*) oraz Menedżery kolektorów (*Collector Manager*) to elastyczne narzędzia, które pozwalają monitorować praktycznie dowolne źródło danych związanych z bezpieczeństwem. Obejmuje to zarówno popularne systemy, aplikacje i urządzenia, a także własne, niestandardowe. Kolektory pozwalają zautomatyzować procesy, inteligentnie reagują na reguły i podejmują działania przy spełnieniu określonych warunków. Mogą zbierać i filtrować zdarzenia zdalnie

lub lokalnie, tam gdzie są wywoływane. Za wyjątkiem dosłownie kilku systemów (takich jak serwery klasy mainframe), Kolektory są pozbawione agentów. Zbierają więc dane zdalnie i nie wymagają instalowania dodatkowego oprogramowania na monitorowanym systemie lub urządzeniu.



Oprogramowanie zawiera też interfejsy API, które umożliwiają dwukierunkową komunikację z systemami rozwiązywania problemów (np. HP ServiceDesk*, BMC Software's Remedy*) lub urządzeniami, które nie tworzą czytelnych dzienników, np. serwery klasy mainframe.

Rys 2. Menedżer kolektorów

Kolektory automatyzują proces filtrowania zdarzeń. Informacje o większości zdarzeń przesyłają do Repozytorium (*Repository*, opis na str. 9) w celu przechowania i późniejszej analizy. Część informacji jest z kolei przesyłana do Mechanizmu korelacji (*Correlation engine*, opis poniżej) w celu oceny oraz odniesienia do zdefiniowanej uprzednio strategii oraz informacji o zdarzeniach napływających z innych źródeł w sieci. Kolektory rozszerzają zakres informacji o zdarzeniach, uzupełniając je o dane (taksonomię zdarzeń i odniesienia biznesowe), które pomagają w ich identyfikacji i klasyfikacji. Na końcu tej broszury zamieszczono listę Kolektorów przygotowanych przez firmę Novell.

Magistrala komunikatów iSCALE

Komunikacja między komponentami systemu Sentinel jest zrealizowana w oparciu o magistralę komunikatów opartą na architekturze magistrali Sonic JMS*. Pozwala ona łatwo zintegrować ten produkt z systemem do zarządzania tożsamością Novell Identity Manager oraz innymi systemami działającymi w oparciu o komunikację przez magistralę.



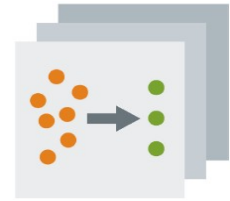
Rys. 3. Magistrala komunikatów iSCALE

Architektura systemu Sentinel oparta na magistrali komunikatów jest bardzo skalowalna, tak że nawet rozbudowane środowiska IT mogą korzystać z Sentinela bez utraty wydajności. Wynika to z faktu, że architektura systemu Sentinel nie opiera się o relacyjną bazę danych, która może stanowić ograniczenie wydajności i ekonomicznej skalowalności. Zamiast tego Sentinel wykorzystuje przetwarzanie w pamięci, aby szybko wychwytywać i odfiltrowywać istotne zdarzenia. Dzięki temu możliwa jest analiza tysięcy zdarzeń na sekundę w czasie rzeczywistym. Komponenty można skalować niezależnie od siebie, bez powielania całego systemu i bez dokupowania sprzętu czy licencji na bazy danych.

Mechanizm korelacji

Mechanizm korelacji określa, czy seria zdarzeń jest incydem wymagającym reakcji. Moduł ten otrzymuje informacje o zdarzeniach przekazywane z magistrali komunikatów, ocenia je i podejmuje decyzje w oparciu o uprzednio zdefiniowane kryteria.

Po zdecydowaniu o następnych krokach, mechanizm korelacji przesyła informacje przez magistralę komunikatów, umożliwiając modułowi iTRAC™ (patrz poniżej) i innym komponentom lub aplikacjom otrzymanie informacji o zdarzeniu i podjęcie stosownych działań. Automatyczna korelacja zdarzeń pozwala informatykom oszczędzić czas poświęcany na analizowanie plików dziennika.



Rys. 4. Korelacja

Zmniejsza to możliwość wystąpienia błędów w analizie i pozwala uniknąć sytuacji, w której incydent związany z bezpieczeństwem lub zgodnością z regulacjami zostaje pominięty.

Centrum sterowania

Centrum sterowania systemu Sentinel to główna konsola do wizualizacji i analizy zdarzeń oraz incydentów. Intuicyjne monitory pozwalają analitykom szybko identyfikować nowe trendy, ataki lub naruszenia obowiązujących zasad, a także operować na informacjach graficznych zbieranych w czasie rzeczywistym, w tym również na szczegółowych danych historycznych.



Centrum sterowania zawiera ponadto gotowe panele konsoli monitorowania bezpieczeństwa i zgodności z regulacjami, które zostały skonfigurowane według najlepszych procedur w branży. Łatwo można je dostosować do kontekstów biznesowych charakterystycznych dla danej firmy lub instytucji.

Rys. 5. Centrum sterowania systemu Sentinel

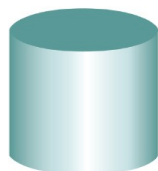
iTRAC

iTRAC to wbudowany, automatyczny system obsługi procesów przepływu pracy i naprawiania problemów. Zbudowano go w oparciu o szablony rozwiązywania incydentów organizacji SANS Institute. iTRAC określa działania, które należy podjąć w przypadku wystąpienia konkretnych zdarzeń. Wstępnie zdefiniowane procesy można dostosować tak, aby pasowały do procedur danej firmy lub instytucji, zaś po zakończeniu każdego działania dostępny jest dziennik kontroli, który dowodzi zgodności z regulacjami. Dodatkowo iTRAC pozwala administratorom automatycznie przekazywać zadania do systemów zewnętrznych, takich jak Remedy, HP ServiceDesk lub innych, jeśli jest to konieczne.



Rys. 6. iTRAC

Repozytorium



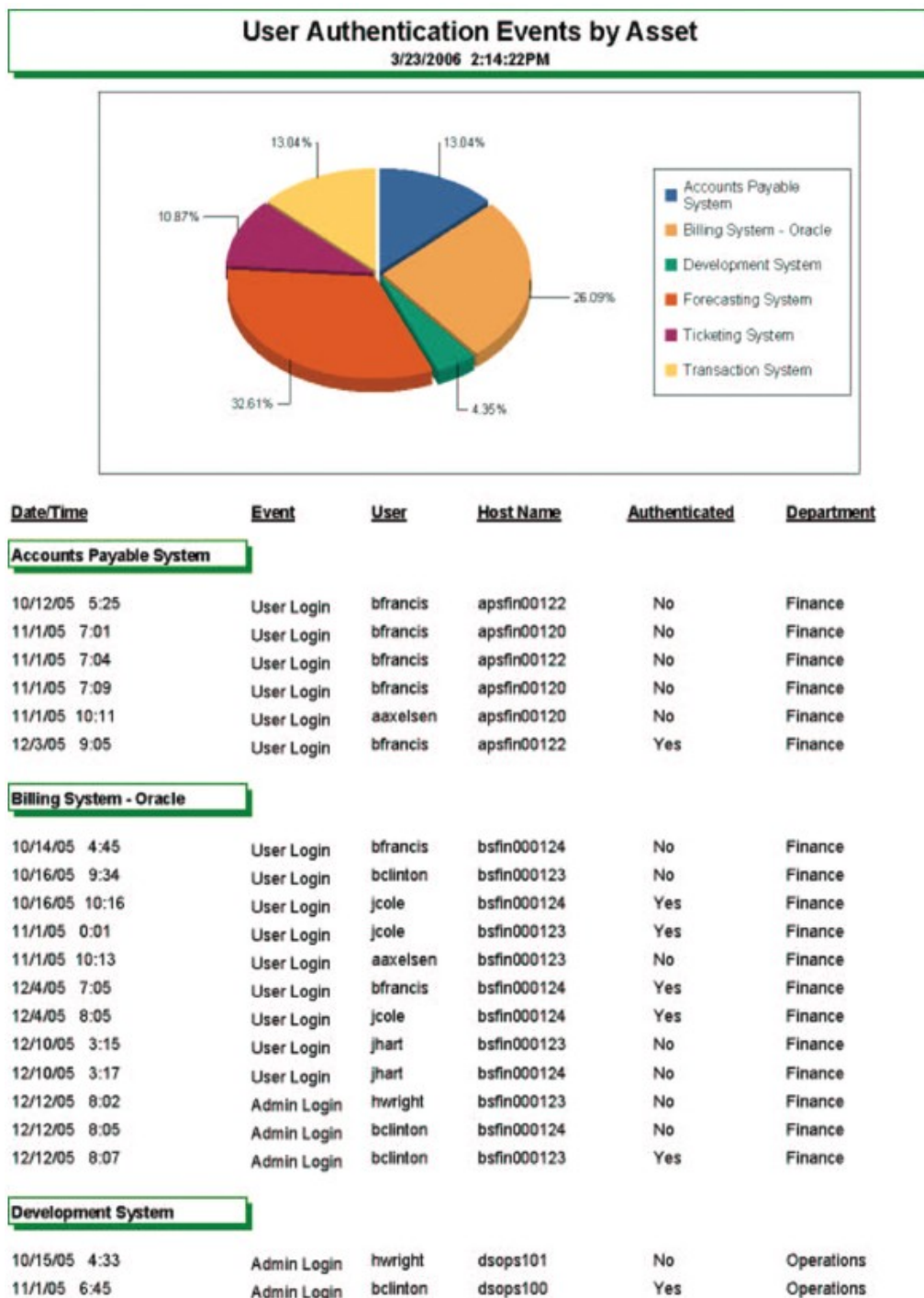
W zależności od potrzeb i preferencji przedsiębiorstwa jako repozytorium zdarzeń można wykorzystać bazę danych Oracle* lub SQL*. Ilość danych utrzymywanych w repozytorium zależy od ilości informacji o danym zdarzeniu oraz zasad filtrowania w Kolektorach.

Rys. 7. Repozytorium

Dodatkowe komponenty oprogramowania Sentinel

Sprawozdawczość

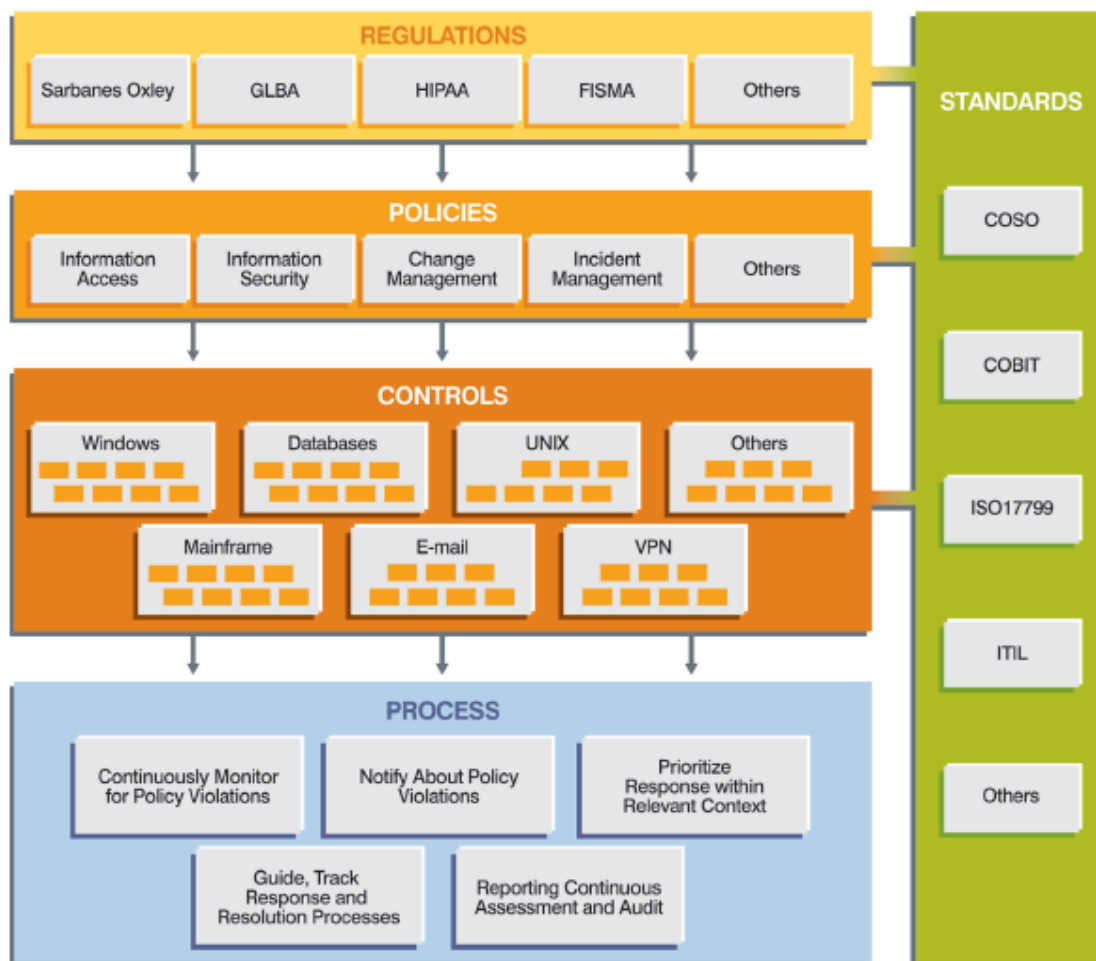
W skład oprogramowania Sentinel wchodzi aplikacja Sentinel Reports służąca do wizualizacji środowiska zabezpieczeń w przedsiębiorstwie, dokumentowania zgodności z regulacjami, a także efektywnego zarządzania ryzykiem operacyjnym. Sentinel Reports zawiera kilka wstępnie zdefiniowanych szablonów raportów. Administratorzy mogą też tworzyć własne raporty oraz generować zapytania do repozytorium przy użyciu narzędzia Crystal Reports* jako mechanizmu zaplecza.



Rys. 8. Przykład raportu

Pakiety sterujące

Pakiety sterujące to rozwiązania przeznaczone dla specyficznych grup nadzoru informatycznego, które zawierają agentów, reguły korelacji, szablony procesów iTRAC oraz raporty odnoszące się do ogólnych kategorii nadzoru. Kategorie te obejmują administrację bezpieczeństwem, zarządzanie zmianami w aplikacjach, zarządzanie danymi, odtwarzanie po awarii i zarządzanie incydentami. Część rozwiązania stanowią też gotowe do uruchomienia raporty dotyczące zgodności ze strategią przedsiębiorstwa, jej naruszeń, a także działań naprawczych. Pakiety sterujące powodują, że strategie opracowane na papierze stają się automatycznie monitorowanymi informatycznymi elementami nadzoru.



Rys. 9. Sentinel firmy Novell przekształca strategie opracowane na papierze w automatycznie monitorowane informatyczne elementy nadzoru

Integracja produktów firm Novell i e-Security

W wyniku bezpośredniego zakupu firmy e-Security Novell zintegrował system Sentinel ze swoją ofertą produktów i obecnie stosuje charakterystyczną dla tego produktu wizję wszechstronnego zarządzania bezpieczeństwem i tożsamością. Wypuszczając na rynek w sierpniu 2006 r. oprogramowanie Sentinel w wersji 5.1.3 firma Novell zrealizowała obietnicę, iż zaoferuje klientom jedyny produkt na rynku, który gwarantuje pojedynczy widok działań związanych z bezpieczeństwem oraz zgodnością z regulacjami, w czasie rzeczywistym, obejmujący całość przedsiębiorstwa.

Architektura oprogramowania Sentinel jest oparta na magistrali komunikatów, dlatego pozwala na łatwe zintegrowanie go z innymi produktami firmy Novell przeznaczonymi do zarządzania tożsamością, bezpieczeństwem oraz dostępem, w tym m.in.:

Novell Identity Manager

Novell Identity Manager to idealne rozwiązanie dla obciążonych działów informatyki. Automatyzuje zaopatrywanie użytkowników w dostęp do potrzebnych im zasobów oraz zarządzanie uprawnieniami, w tym hasłami, na każdym etapie cyklu życia konta pracownika. Za pomocą Novell Identity Manager można w całym środowisku IT zmieniać lub anulować dostęp do zasobów w zależności od potrzeb wynikających z roli pełnionej przez pracownika w organizacji. System automatyzuje zarządzanie hasłami oraz umożliwia synchronizację wielu haseł w jedno bezpieczne hasło. Novell Identity Manager stanowi jednocześnie wiarygodne źródło informacji o tożsamości, które pomagają kontrolować obejmujące całe przedsiębiorstwo zasady bezpieczeństwa oraz wyeliminować złożone, ręczne procesy świadczenia pomocy użytkownikom przez dział IT.

Novell Access Manager

W dzisiejszym świecie biznesu każdy korzysta z sieci. Pracownicy, partnerzy, klienci, a czasem również włamywacze. Dlatego też teraz, bardziej niż kiedykolwiek w przeszłości, przedsiębiorstwa potrzebują rozwiązania, które gwarantuje zaufanie w relacjach biznesowych, upraszczając współużytkowanie zasobów (również przez Internet) i gwarantując jednocześnie bezpieczeństwo. Novell Access Manager to nowoczesne rozwiązanie do zarządzania dostępem i federowania tożsamości, które pomaga sterować dostępem przez przeglądarkę internetową do treści umieszczonych w aplikacjach, zarówno starszych jak i nowoczesnych, webowych. Firma lub instytucja może z łatwością wdrożyć to rozwiązanie i zarządzać nim, niezależnie od tego czy ma setki, tysiące czy miliony użytkowników.

Novell Audit

Czy firma musi utrzymać zgodność ze strategią wewnętrzną i regulacjami zewnętrznymi? Czy musi dysponować dokumentami, które temu dowodzą? Novell Audit to bezpieczne rozwiązanie do rejestrowania działań w sieci oraz ich audytowania. Pobiera i zapisuje dane dotyczące zdarzeń związanych z bezpieczeństwem, systemami i aplikacjami, które występują w całej sieci. Novell Audit monitoruje w czasie rzeczywistym zdarzenia i informuje o problemach, jeśli naruszona zostanie strategia lub przepisy. Może zapisywać dane w różnych formatach, np. zwykłych plikach, bazach Microsoft SQL*, MySQL*, Oracle lub SYSLOG. Dzięki temu można łatwo wygenerować raporty dotyczące dowolnych zdarzeń w sieci. Umożliwia też stosowanie standardowych zapytań SQL i zawiera zbiór wstępnie zdefiniowanych raportów Crystal Reports.

Dlaczego Novell

Dzięki poszerzeniu serii produktów Novella do zarządzania tożsamością o oprogramowanie Sentinel powstało rozwiązanie działające w czasie rzeczywistym, obejmujące całe przedsiębiorstwo, pozwalające w inteligentny i automatyczny sposób reagować na wszelkiego rodzaju zdarzenia, od ataku wirusów po nieuprawnione żądanie dostępu do aplikacji finansowej. Novell to pierwsza firma, która zapewnia pojedynczy widok działań związanych z bezpieczeństwem i zgodnością z regulacjami, obejmujący całość przedsiębiorstwa. Inne produkty na rynku nadal koncentrują się na sieci z punktu widzenia platformy lub urządzenia, podczas gdy Novell oferuje pełne rozwiązanie w zakresie bezpieczeństwa i zgodności z regulacjami. Po zakupie przez Novella firmy e-Security, analitycy firmy

Gartner umieścili firmę Novell w kwadrancie liderów w rankingu Magic Quadrant* for Security Information and Event Management², co sugeruje, iż Novell jest uznawany za wiodącą firmę na rynku producentów tego rodzaju rozwiązań.

Oprócz najlepszego na rynku oprogramowania Sentinel, Novell oferuje całą gamę oprogramowania i usług pomagających uzyskać bezpieczną, niezawodną infrastrukturę przedsiębiorstwa. Rozpoczynając od wydania ponad dwadzieścia lat temu systemu NetWare, aż do wprowadzonego niedawno na rynek systemu SUSE Linux Enterprise 10, firma Novell nieprzerwanie tworzy stabilne, skalowalne i bezpieczne systemy operacyjne, narzędzia oraz aplikacje sieciowe. Są one tak niezawodne i bezpieczne, że na całym świecie tysiące agend rządowych oraz stawiających na bezpieczeństwo korporacji stosuje produkty firmy Novell do obsługi najważniejszych dla nich zadań. Dodatkowo Novell oferuje wysokiej jakości usługi pomocy technicznej, szkoleń i konsultacji, od planowania po wdrożenie technologii. Firmę Novell wspiera przy tym wielu globalnych partnerów, do których należą światowi dostawcy sprzętu i oprogramowania.

Wnioski

Sentinel to punkt zwrotny dla przedsiębiorstw. Kosztowne, czasochłonne i podatne na błędy ręczne procesy zapewniania bezpieczeństwa i zgodności z regulacjami można teraz zastąpić zautomatyzowanym, rygorystycznym i przewidywalnym programem monitorowania środowiska IT firmy czy instytucji. Wprowadzając automatyzację i pełen nadzór do zarządzania bezpieczeństwem i monitorowania zgodności z regulacjami, oprogramowanie Sentinel pozwala w pełni przygotować się na wewnętrzne i zewnętrzne zagrożenia, a także sprostać oczekiwaniom audytorów. Firmy i instytucje mają nareszcie dostęp do pełnych, dostępnych w czasie rzeczywistym informacji o zdarzeniach związanych z bezpieczeństwem. Mogą też zareagować na znane zagrożenia, identyfikując i eliminując nowe. Ponadto Sentinel umożliwia sporządzanie raportów obejmujących całość przedsiębiorstwa i dowodzących spełniania norm bezpieczeństwa oraz zgodności z regulacjami.

Więcej informacji na temat oprogramowania Novell Sentinel można uzyskać kontaktując się z bezpłatną infolinią firmy Novell w Polsce (nr tel. 0 800 22 66 85) oraz na stronach internetowych <http://www.novell.com/products/sentinel>

INFORMACJE O FIRMIE NOVELL

Novell, Inc. jest producentem oprogramowania tworzącego infrastrukturę Przedsiębiorstwa Otwartego. Firma jest czołowym dostawcą środowisk operacyjnych open source opartych na systemie Linux oraz najwyższej klasy narzędzi do zarządzania i bezpieczeństwa, przystosowanych do pracy w mieszanych środowiskach systemowo-sprzętowych. Novell pomaga klientom w koncentrowaniu się na rozwoju biznesu udzielając daleko idącej pomocy w zakresie zarządzania, upraszczania, integrowania i zabezpieczania środowiska informacyjnego przy jednoczesnym obniżaniu poziomu ryzyka i kosztów jego posiadania.

Więcej informacji: <http://www.novell.com>

² „Magic Quadrant for Security Information and Event Management, 1H06”, autorzy: Mark Nicolett, Amrit Williams and Paul Proctor, firma Gartner Group

Dodatek: Kolektory systemu Sentinel

Kolektory pobierają dane z urządzeń źródłowych za pomocą wielu metod połączenia, w tym SYSLOG, ODBC, JDBC, OPSEC, SSL, SNMP, HTTP, HTTPS itp. Elastyczna technologia Kolektorów systemu Sentinel pozwala utworzyć Kolektory do praktycznie dowolnego źródła danych związanych z bezpieczeństwem. Obejmuje to systemy, aplikacje i urządzenia firmowe oraz niestandardowe. Oto przykładowa lista urządzeń, systemów i aplikacji, z których system Sentinel może pobierać zdarzenia i informacje.

Aplikacje firmy Novell:

Novell Access Manager
Novell eDirectory
Novell Identity Manager
Novell NetWare
Novell SecureLogin
Novell ZENworks

Aplikacje firmowe

Oracle Financials
SAP

Bazy danych

IBM DB2
MS SQL Server 2000/2003
Oracle 8i/9i/10g

Programy antywirusowe

CA eTrust
McAfee ePolicy Orchestrator
Symantec AntiVirus Corporate Edition
Trend Micro InterScan VirusWall

Zapory (firewall)

Checkpoint Firewall-1 i Provider-1
Cisco Pix
Juniper NetScreen Firewall
Microsoft ISA Firewall
Secure Computing
Gauntlet/Sidewinder
Symantec Gateway Security Firewall

Systemy wykrywania włamań oparte na centralnym serwerze

Cisco Security Agent
Enterasys Dragon
InterSect Alliance SNARE
ISS RealSecure Server
McAfee Enterscept
Symantec Intruder Alert

Sieciowe systemy wykrywania włamań

Cisco Secure IDS
Enterasys Dragon
Gnu Snort
ISS RealSecure
ISS SiteProtector
Intrusion.com SecureNet
Juniper NetScreen IDP
McAfee IntruShield
NFR Sentivist
Sourcefire Defense Center
Symantec Network Security
Tipping Point Security Management System

Serwery mainframe oraz midrange

ACF2
HP NonStop/Tandem Himalaya
IBM iSeries/AS400
IBM z/OS RACF
IBM z/OS Top Secret
VAX VMS

Systemy operacyjne

IBM AIX
HP-UX
Microsoft Windows NT, 2000, 2003, XP
Microsoft MOM
Novell SUSE Linux Enterprise Server
Red Hat Enterprise Linux
Sun Solaris
Sun Trusted Solaris

Skanery wykrywania luk

eEye Retina
Gnu Nessus Scanner
ISS Internet Scanner
McAfee Foundstone Enterprise
nCircle IP360
Qualys QualysGuard

Aplikacje VPN

(Virtual Private Network)

Checkpoint VPN
Cisco VPN 3000/3030
Juniper Netscreen VPN-1
Nortel Contivity VPN

Serwery aplikacji oraz Web

Apache HTTP Server
IBM WebSphere
Microsoft IIS
SunOne/iPlanet

Copyright © 2006 Novell Inc. Wszelkie prawa zastrzeżone. Novell, logo Novell, logo N, NetWare, SUSE i ZENworks są zastrzeżonymi znakami towarowymi, zaś eDirectory i Sentinel są znakami towarowymi firmy Novell Inc. w Stanach Zjednoczonych oraz innych krajach.

* Linux jest zastrzeżonym znakiem towarowym Linusa Torvaldsa. Pozostałe znaki towarowe należą do odpowiednich właścicieli.