Skaner podatności Nessus Professional

Nessus jest najpowszechniej stosowanym w branży skanerem podatności, który pomaga zmniejszyć obszar ataku i zapewnia zgodność w środowiskach fizycznym, wirtualnym, mobilnym i chmur. Nessus zapewnia szybkie badanie zasobów, audytowanie konfiguracji, profilowanie celów, wykrywanie złośliwego oprogramowania, danych wrażliwych i wiele innych.

Nessus wspiera więcej technologii niż konkurencyjne rozwiązania, skanuje systemy operacyjne, urządzenia sieciowe, hipernadzorców, bazy danych, serwery webowe i wrażliwą infrastrukturę pod kątem podatności, zagrożeń i naruszeń zasad zgodności.

Dzięki największej na świecie, ciągle uaktualnianej bibliotece podatności i testów konfiguracji oraz wsparciu przez zespół ekspertów firmy Tenable ds. badania podatności, Nessus stanowi standard szybkości i precyzji w skanowaniu podatności.

Nessus umożliwia użytkownikowi sortowanie i filtrowanie wyników za pomocą ponad 20 różnych kryteriów. Rankingi dotkliwości podatności mogą być dostosowywane wg potrzeb, podsumowanie zalecanych działań zapobiegawczych może posłużyć jako materiał dowodowy przy różnego rodzaju sporach.

Pełne pokrycie podatności:

• wirtualizacja i chmury

• szkodliwe oprogramowanie i botnety

• audyty konfiguracji

• aplikacje webowe

Kluczowe korzyści:

• **Zmniejsza liczbę miejsc potencjalnego ataku**: zapobiega atakom identyfikując podatności, które powinny zostać zlikwidowane

• **Wszechstronny**: odpowiada standardom regulatorów i wymogom zgodności w najszerszym zakresie

• **Skalowalny**: począwszy od pojedynczej licencji dla użytkownika Nessus Professional do Nessus Manager albo Nessus Cloud, jeśli tego wymagają zwiększające się potrzeby zarządzania podatnościami

• **Niski całkowity koszt posiadania (TCO)**: kompletne rozwiązanie do skanowania podatności przy niskich kosztach

• **Stale uaktualnianie**: zespół badawczy Tenable ciągle udostępnia aktualizacje

• **Łatwy dostęp**: dostęp przez przeglądarkę o dowolnej porze i w dowolnym miejscu

Zalety Nessus

Raportowanie i monitorowanie

• Elastyczność raportowania: dostosowanie raportów wg podatności lub urządzenia, możliwość wygenerowania streszczenia dla zarządu lub porównania wyników różnych skanów w celu wyróżnienia zmian.
– Standardowy (XML), PDF (wymagana jest instalacja Java na serwerze Nessus), formaty HTML i CSV.

• Celowane powiadomienia o wynikach skanowania wysyłane e-mailem, zalecenia działań naprawczych i usprawnień dot. konfiguracji skanów.

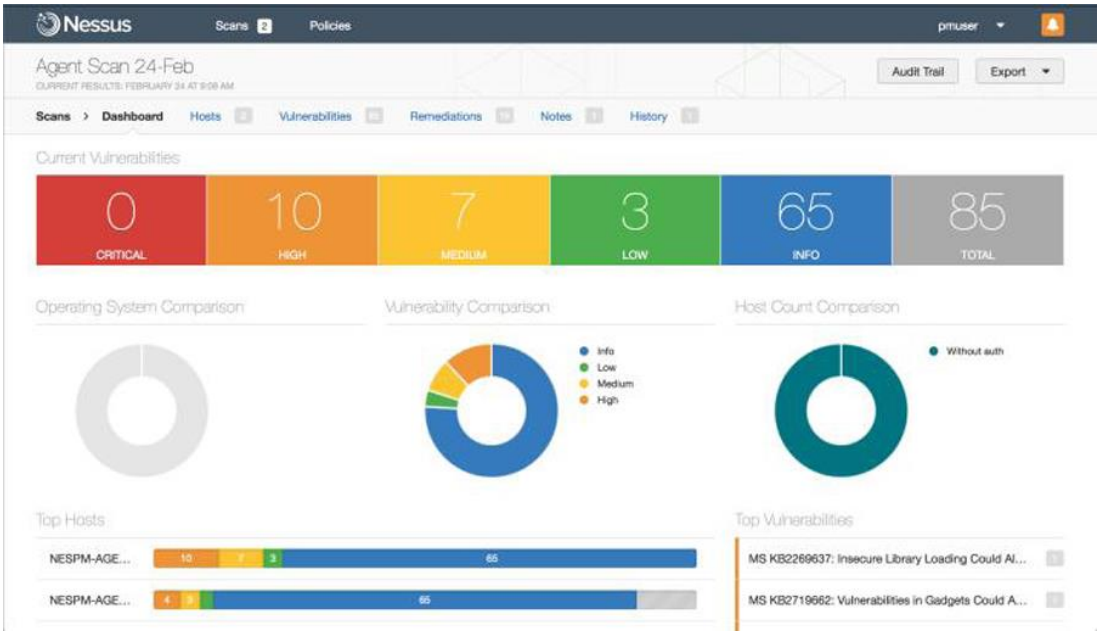
Zarządzanie podatnościami w zespole

Nessus® Manager łączy w sobie skuteczne wykrywanie, skanowane i zalety audytowania Nessusa, najpowszechniej stosowanego na świecie skanera podatności, z obszernymi możliwościami zarządzania i współpracy, co redukuje obszar ataku.

Nessus Manager umożliwia udostępnianie zasobów, w tym skanerów Nessus, harmonogramów i polityk skanowania i wyników skanów wśród wielu użytkowników lub grup. Nessus Manager pozwala członkom wieloosobowych zespołów udostępniać źródła zarządzania podatnościami w celu zwiększenia efektywności i skuteczności. Użytkownicy mogą by zaangażowani i udostępniać zasoby oraz dzielić odpowiedzialność ze współpracownikami: właścicielami systemów, wewnętrznymi audytorami, audytorami ryzyk i zgodności, administratorami IT i sieci oraz analitykami bezpieczeństwa. Takie funkcje pracy grupowej pozwalają zredukować czas i koszty skanowania bezpieczeństwa i audytu

zgodności poprzez usprawnienie skanów i wykrywanie złośliwego oprogramowania, błędów w konfiguracjach oraz przyspieszenie działań naprawczych.

Nessus Manager zabezpiecza środowiska fizyczne, wirtualne, mobilne i środowiska w chmurze. Nessus Manager jest dostępny do wdrożenia wewnętrznego lub z chmury w postaci usługi Nessus® Cloud utrzymywanej przez Tenable.
Nessus Manager wspiera najszerszy zakres systemów, urządzeń i zasobów, a za pomocą opcji wdrażania z uwierzytelnieniem i bez (Nessus Agent) łatwo rozszerza się na środowiska mobilne, które nie mają stałego dostępu do sieci i inne trudne do skanowania.



Kluczowe korzyści:

• Dokładne, sprawdzone i w pełni wspierane skanowanie: oparte o skaner podatności Nessus

• Udostępnianie zasobów: przydzielaj skanery, polityki i harmonogramy oraz dostęp do raportów wielu użytkownikom lub grupom

• Rozszerzony zakres działania skanów: Nessus Agent pozwalają skanować bez uwierzytelnienia urządzenia albo zasoby, które nie mają stałego dostępu do sieci

• Ulepszona analiza ryzyka poprzez uwzględnienie istniejącej infrastruktury i partnerskich frameworków.

• Łatwe wdrożenie i zarządzanie: Nessus Manager pozwala na szybkie rozpoczęcie pracy, a wsparcie wielu skanerów ułatwia rozszerzenie zakresu skanera

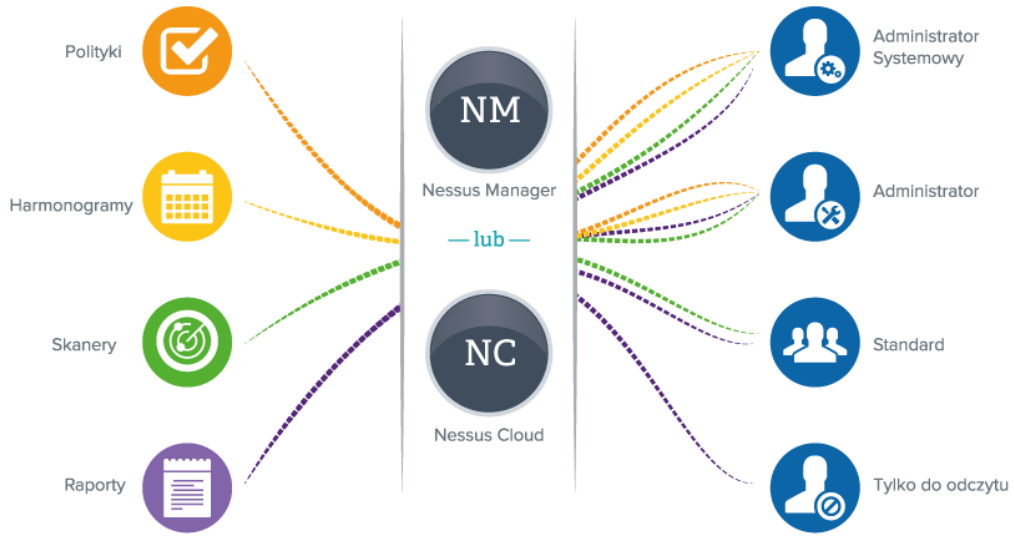
Wsparcie wielu skanerów

Możliwość zarządzania wieloma skanerami za pomocą Nessus Manager pozwala na łatwe rozszerzenie pokrycia skanami bardziej złożonych sieci, wdrożeń w infrastrukturach w

chmurze i geograficznie rozproszonych lokalizacjach. Użytkownicy mogą zarządzać harmonogramami skanów, dodawać polityki, przeglądać wyniki skanów wielu skanerów z jednej centralnej konsoli.

Integracja z systemem zarządzania poprawkami i MDM

Nessus Manager integruje się z innymi kluczowymi technologiami przez co wzmacnia się program zarządzania podatnościami organizacji. Nessus Manager integruje się z rozwiązaniami do zarządzania poprawkami z IBM, Microsoft, Red Hat i Dell, co pozwala upewnić się, że aktualizacje systemów i urządzeń są w stanie odpowiednim do wewnętrznych wymogów bezpieczeństwa. Ponadto Nessus Manager integruje się z głównymi rozwiązaniami Mobile Device Management (MDM) z Microsoft, Apple, Good, MobileIron i AirWatch, przez co urządzenia mobilne stają się częścią zidentyfikowanych zasobów i mogą być zarządzane w ramach programu zarządzania podatnościami w organizacji.



Role użytkowników

Nessus Manager pozwala na dodawanie wielu użytkowników i przedstawia cztery role użytkowników: Administrator Systemowy, Administrator, Standard i Tylko do odczytu. Każdy użytkownik może być przydzielony do różnych poziomów dostępu do zasobów bazującym na przydziale indywidualnym lub grupowym. Administrator Systemowy i Administrator mają uprawnienia do zarządzania użytkownikami i grupami. Grupy mogą być ustalane wg podziału departamentów, kompetencji, obowiązków lub odpowiedzialności, położenia – w taki sposób, aby najlepiej odpowiadać najbardziej specyficznym potrzebom.

Zespół badawczy

Podatności i nowe zagrożenia pojawiają się nieustannie, więc zespół badawczy Tenable zapewnia częste aktualizacje Nessus Manager, aby pomóc organizacjom zwalczyć zaawansowane zagrożenia i podatności natychmiast po ich pojawieniu się oraz sprostać nowym wymogom regulatorów. Te aktualizacje stanowią część subskrypcji Nessus Manager.

Nessus Agent

Nessus Agent dostępne wraz z Nessus Cloud i Nessus Manager usprawniają tradycyjny przebieg skanowania sieci, który zwykle jest związany z uwierzytelnieniem, tym samym ułatwiając skanowanie większego zakresu zasobów, w tym takich, które są offline.

Nessus Agent będzie atrakcyjnym rozwiązaniem w następujących przypadkach:

• Urządzenia, które nie są stale podłączone do sieci: Skanowanie laptopów i innych urządzeń, które nie mają stałego dostępu do sieci lokalnej.

• Skanowanie bez uwierzytelnienia: Chęć albo potrzeba skanowania zasobów bez uwierzytelnienia.

• Szybkie skanowanie: Nessus Agent dla skanowania wykorzystuje lokalne zasoby, a sieć jest wykorzystywana tylko w celu przesłania wyników do Nessus Cloud, co pozwala w łatwy sposób szybko przeskanować dużą liczbę urządzeń.

Tenable Passive Vulnerability Scanner

Tenable Passive Vulnerability Scanner pozwala na monitorowanie sieci w czasie rzeczywistym i jest przeznaczony do ciągłego skanowania i oceny poziomu bezpieczeństwa w organizacji w sposób nieinwazyjny. PVS badając wszystkie urządzenia śledzi ruch sieciowy na niskim poziomie, co gwarantuje wykrycie podatności serwerów i urządzeń.

PVS łatwo integruje się z siecią i wykrywa pasywnie aktywne urządzenia, w tym urządzenia wirtualne i znajdujące się w chmurze, urządzenia BYOD/mobilne, a nawet złamane (jailbroken) urządzenia z systemem iOS. PVS jest dostosowany do przyszłego zapotrzebowania na monitorowanie systemów wirtualnych, serwisów w chmurze i zwiększającej się liczby urządzeń.

Przegląd istotnych cech produktu

Tenable Passive Vulnerability Scanner™ (PVS™) to opatentowana technologia badania oraz analizy podatności, która pozwala na ciągłe, nieinwazyjne analizowanie sieci. PVS monitoruje protokoły IPv4, IPv6 oraz sieci mieszane na niskim poziomie, dzięki czemu jest w stanie określić ich topologię oraz wykryć aktywne serwisy i ich podatności. PVS może być wykorzystywany jako samodzielne narzędzie do efektywnego badania segmentów lub

małych sieci lub jako integralna część rozwiązania Tenable SecurityCenter Continuous View™. PVS w czasie rzeczywistym wykrywa i śledzi użytkowników, aplikacje, infrastrukturę w chmurze, zaufane połączenia oraz podatności. Ponadto automatycznie wykrywa użytkowników, infrastrukturę oraz podatności systemów operacyjnych, urządzeń sieciowych, maszyn wirtualnych, baz danych, tabletów, telefonów, serwerów webowych, aplikacji w chmurze i infrastruktury o znaczeniu krytycznym.

Korzyści z używania PVS

Najważniejszymi korzyściami ze skanowania ruchu w sieci za pomocą PVS jest identyfikacja wszystkich urządzeń i aplikacji, rozpoznanie ich podatności i wykrycie urządzeń mobilnych:

• Zawsze wiadomo jakie urządzenia, aplikacje, serwisy i połączenia są lub były aktywne w sieci

• Ochrona systemów wrażliwych, czyli takich, które nie mogą być skanowane aktywnie. Efektywne skanowanie bez konieczności logowania się do systemów wrażliwych, a co za tym idzie bez ryzyka spowodowania przerw w świadczeniu usług.

• Automatyczne wykrywanie zagrożeń stwarzanych przez podatności w znanych zasobach, nowych systemach lub systemach niezaufanych.

• Badanie zgodności zarówno z politykami wewnętrznymi, jak i z kluczowymi wymogami prawa poprzez weryfikację poprawności konfiguracji systemów.

• Wykrywanie nadużyć i określanie wewnętrznych zagrożeń, które nie są wykrywalne na urządzeniach strzegących obrzeża sieci.

• Skoncentrowanie na odpowiedziach na incydenty dzięki wzbudzaniu alarmów w wypadku wykrycia rzeczywistych zagrożeń.

• Przyśpieszenie usuwania zagrożeń i eliminacja “martwych obszarów” pomiędzy skanami aktywnymi.

• Wypełnienie luk w zaplanowanym aktywnym skanowaniu dzięki ciągłej analizie pasywnej.

Kluczowe funkcjonalności

Monitorowanie i wykrywanie podatności w czasie rzeczywistym

Tenable PVS w sposób ciągły monitoruje ruch sieciowy w celu uzyskania następujących informacji związanych z bezpieczeństwem:

• Śledzenie wszystkich podatności na aplikacjach klienckich i serwerowych

• Wykrywanie zmodyfikowanych lub skompromitowanych aplikacji

• Wykrywanie i zapamiętywanie nowych urządzeń w sieci

• Wykrywanie sytuacji wykonywania nieautoryzowanych skanów sieci przez maszyny znajdujące się wewnątrz niej

• Wychwytywanie interaktywnych oraz zaszyfrowanych sesji sieciowych

• Inwentaryzacja otwartych portów sieciowych w systemach oraz detekcja ruchu pomiędzy nimi

• Pasywnie wykrywanie systemu operacyjnego dla każdego aktywnego w sieci urządzenia

• Wykrywanie podatności w systemach wraz z określeniem, które protokoły i aplikacje były wykorzystane

• Rangowanie urządzeń według odnalezionych podatności systemów operacyjnych i aplikacji oraz generowanych przez nie połączeń

• Wsparcie dla sieci o przepustowości 10Gbps

PVS łączy się z siecią poprzez hub, span port, łącze ERSPAN albo network tap i w sposób ciągły monitoruje potoki danych, generując ostrzeżenia w czasie rzeczywistym i sporządzając wszechstronne raporty dla działów bezpieczeństwa, IT i kadry zarządzającej.

Monitorowanie sieci, WWW i FTP

PVS oferuje kompleksowe monitorowanie połączeń do sieci WWW lub FTP poprzez bezpośrednią analizę transferu pakietów. Pasywnie monitorując każde przesłanie danych poprzez HTTP lub FTP, PVS może określić i przedstawić informację o każdym urządzeniu w sieci, w tym:

• Wszystkie podatności i aplikacje zarówno po stronie klienta, jak i po stronie serwera WWW

• Listę wszystkich agentów WWW wykorzystanych na każdym urządzeniu

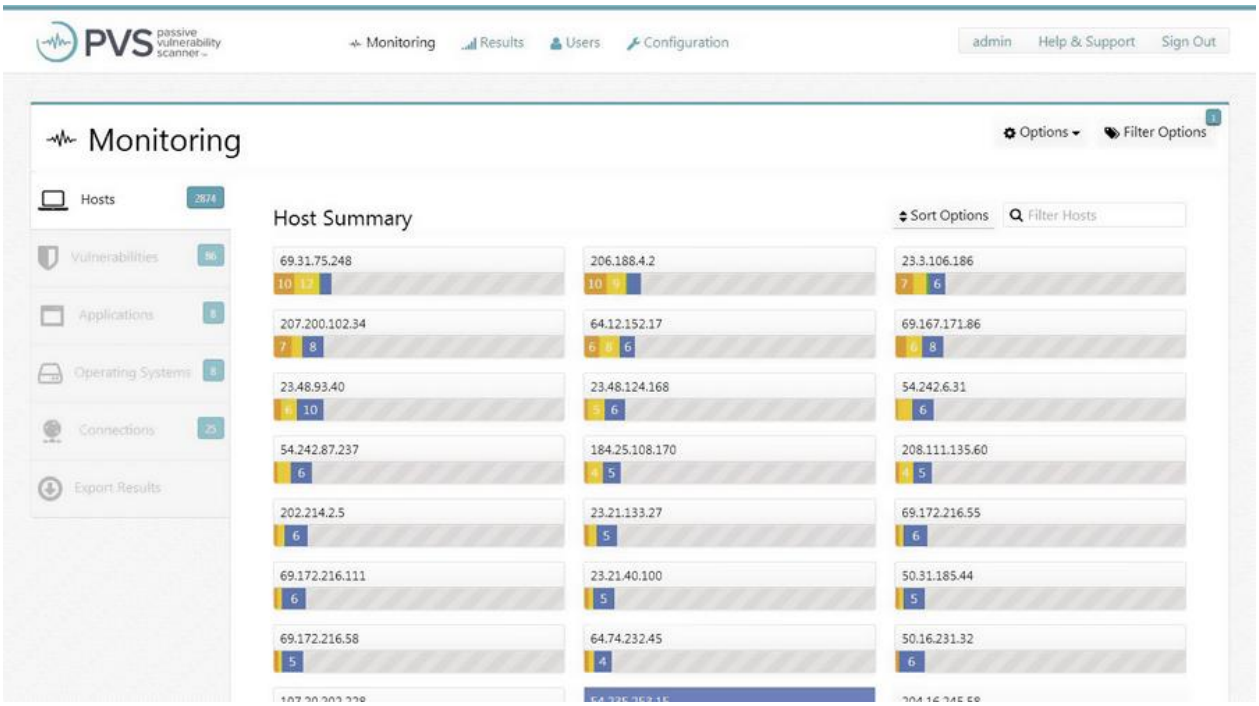
• Pasywne wyliczenie wszystkich plików udostępnianych przez FTP

• Zapisanie w czasie rzeczywistym logów wszystkich operacji GET, POST i pobranych plików

• Zapisanie w czasie rzeczywistym logów wszystkich plików przesyłanych przez GET, PUT lub protokołem FTP

• Zapisanie w czasie rzeczywistym logów zapytań do serwera DNS

Informacje takie są potrzebna do analizy aktywności wewnątrz sieci, aktywności pracowników, wykrywania infekcji złośliwym oprogramowaniem oraz zagrożeń zaawansowanych. Dzienniki detekcji mogą być wysłane do Tenable Log Correlation Engine™ w celu dalszej analizy, zbadania korelacji i archiwizacji.



Skanowanie bez konieczności instalacji agenta i dostęp bez instalacji klienta na urządzeniach końcowych

PVS oferuje zaawansowaną analizę protokołów SMB. Jeśli PVS jest wykorzystywany w sieci, w której funkcjonuje usługa Active Directory, to wówczas jest w stanie automatycznie uczyć się:

• Nazwy każdego urządzenia i każdej grupy roboczej

• Listy plików udostępnionych w dowolnym folderze

• Loginów i plików pobranych z sieci w czasie rzeczywistym

Możliwość pozyskania takiej informacji w czasie rzeczywistym pozwala na ocenę zaistniałej sytuacji i ma potężne znaczenie przy zbieraniu materiału dowodowego. W dużych sieciach pasywne określenie wszystkiego, co jest udostępniane w folderach, pozwala na o wiele łatwiejszą identyfikację ekspozycji potencjalnie wrażliwych danych. Stosowanie SecurityCenter Continuous View wraz z zintegrowanymi modulami PVS i Log Correlation Engine umożliwia analizę aktywności pracowników i złośliwego oprogramowania poprzez sprawdzenie informacji o udostępnionych przez sieć plikach.

Monitorowanie i zapisywanie logów baz danych SQL

PVS może przeglądać ruch sieciowy w celu identyfikacji baz danych SQL i ich podatności z jednoczesnym zapisywaniem logów tych działań w czasie rzeczywistym. Tak zapisywane logi zapytań SQL mogą być wysyłane do analizy do Log Correlation Engine, w celu archiwizacji oraz detekcji zagrożeń takich jak SQL injection ze strony serwerów WWW. Pełna obsługa środków kontrolowania wszystkich zdarzeń SQL może być osiągnięta zarówno poprzez

połączenie danych z PVS z konfiguracją bazy danych SQL dla Nessus® i danymi audytu podatności, jak i poprzez logi zapisywane z serwera bazy danych SQL przez agenta Log Correlation Engine.

Pasywne wykrycie topologii i analiza identyfikacji serwisów

Analiza danych dla poszczególnych podatności klientów lub serwerów odbywa się poprzez rekonstruowanie zachowania po obydwu stronach połączenia sieciowego. Protokoły, takie jak HTTP, SMTP i FTP, mają specyficzne ciągi znaków, które pozwalają zidentyfikować wersję serwisu. PVS wyznacza wersje i kojarzy je ze specyficznymi wtyczkami i testami podatności.

Zgodność PCI DSS

Standard PCI DSS wymaga dokładnej i wszechstronnej identyfikacji wszystkich systemów zaangażowanych w transmisję, przetwarzanie oraz przechowanie danych kart kredytowych. Systemy te wspólnie stanowią “cardholder data environment” (CDE), które musi być corocznie weryfikowane na zgodność z wymogami PCI DSS. Organizacje powinny dodatkowo zapewniać dokumentowanie wypełnionych procedur w celu zwiększenia spójności danych CDE. PVS nie tylko monitoruje znane przepływy danych przez CDE, ale również identyfikuje działania nieudokumentowane, w szczególności, informacje o niezaufanych płatnościach kartą.

Security Center & Security Center Continous View

Zaprojektowana z myślą o potrzebach rynku platforma do ciągłego monitorowania

Zmieniający się sektor IT (usługi wirtualne, mobilne i w chmurze) oraz ewoluujące zagrożenia cybernetyczne spowodowały, że cykliczne skany i audyty zgodności przestały skutecznie chronić biznes przed nowymi cyberatakami. Nowym podejściem do oceny ogólnego stanu bezpieczeństwa firm i ich działań jest ciągłe monitorowanie sieci dające pewność, że systemy i urządzenia z zakresu bezpieczeństwa są odpowiednio skonfigurowane i działają w sposób prawidłowy. Stały wgląd w ich konfigurację i działanie zapewnia podjęcie natychmiastowych działań w przypadku najbardziej istotnych ryzyk, mogących stać się zagrożeniem dla biznesu.

SecurityCenter™ Continuous View (CV) jest zaprojektowaną z myślą o potrzebach rynku platformą do ciągłego monitorowania, zapewniającą kompleksowe i całościowe spojrzenie na stan bezpieczeństwa w przedsiębiorstwie. To jedyna platforma łącząca unikalne detektory skanujące i wykrywające podatności z pasywnym monitorowaniem sieci i danych o zdarzeniach, poszerzając je o aktualne informacje o zagrożeniach i podatnościach. Zaawansowana analityka SecurityCenter™ CV pozwala zapewnić zgodność i szybko reagować na naruszenia bezpieczeństwa, dostarczając danych, które pozwalają w sposób ciągły w czasie rzeczywistym wykrywać wszystkie zasoby, identyfikować wszystkie podatności,

monitorować wszystkie sieci pod kątem zaawansowanych zagrożeń oraz gromadzić kontekstowe informacje o zdarzeniach.

SecurityCenter™ wprowadza innowacyjne rozwiązanie Assurance Report Card (ARC), które pozwala w sposób ciągły oceniać, analizować i obrazować skuteczność programu bezpieczeństwa. ARC oparte jest o ważne dla CISO i zarządu strategiczne cele biznesowe będące podstawą dostosowania polityk.

Szerokie możliwości dostosowania dashboardów, raportów, zarządzania incydentami w organizacji oraz realizacją polityk bezpieczeństwa pozwalają dostosować rozwiązanie do specyficznych potrzeb każdego biznesu

Istotne korzyści

• Wykrywa, co dzieje się w sieci, wliczając w to urządzenia fizyczne, zasoby wirtualne, mobilne i chmury

• Zmniejsza zakres ataku poprzez skanowanie wszystkich zasobów pod względem znanych podatności, błędów konfiguracji i szkodliwego oprogramowania

• Eliminuje martwe pola poprzez monitorowanie ruchu sieciowego pod kątem nieautoryzowanych urządzeń i podejrzanego ruchu

• Korelując logi z sieci i urządzeń, poprzez odpowiednią analitykę optymalizuje sposoby obrony

• Dzięki priorytetyzującym zdarzenia alarmom, powiadomieniom i ticketowaniu umożliwia błyskawiczną reakcję na incydenty

• Zapewnia bezpieczeństwo i zgodność w oparciu o polityki bezpieczeństwa dostosowane do strategicznych celów biznesowych

• Zaprojektowana z myślą o potrzebach rynku platforma do ciągłego monitorowania

Badania Tenable

Zespół badawczy Tenable dostarcza częstych aktualizacji informacji o zagrożeniach i podatnościach, zaawansowanych metod analityki, polityk bezpieczeństwa i zgodności, dashboardów i raportów oraz Assurance Report Card dla wszystkich użytkowników SecurityCenter™ CV. To nieszablonowe rozwiązanie oparte o najlepsze praktyki stosowane w poszczególnych branżach i zebrane przez Tenable jest teraz dostępne przy wsparciu zespołu badawczego Tenable i stanowi część subskrybcji SecurityCenter™ CV.

Istotne korzyści

• Assurance Report Card: w sposób ciągły mierzy skuteczność działań użytkownika, założoną w opartych o cele biznesowe politykach bezpieczeństwa, umożliwiając identyfikację i zamknięcie ewentualnych luk.

• Szerokie możliwości dostosowania dashboardów i raportów: nowy interfejs użytkownika oparty o HTML5 spełnia wymagania pracowników CISO, kierownictwa bezpieczeństwa, analityków i praktyków/operatorów.

• Ciągłe wykrywanie zasobów: wykrywa urządzenia mobilne, fizyczne, wirtualne w sieci i w chmurze, włącznie z zasobami nieuprawnionymi, w sposób zautomatyzowany szacuje ryzyka bezpieczeństwa.

• Ocena stanu sieci: ciągłe monitorowanie ruchu sieciowego pod kątem podejrzanego ruchu do i z podatnych systemów i usług, nieznanych urządzeń, botnetów i serwerów C&C.

• Wykrywanie w czasie rzeczywistym złośliwego oprogramowania: wbudowane w rozwiązanie Tenable wykrywanie kanałów zagrożeń (wskaźniki złośliwego oprogramowania, czarne listy) pozwala zidentyfikować zaawansowane złośliwe oprogramowanie w punktach końcowych.

• Wykrywanie anomalii: wykorzystując analizę statystyczną i anomalii zachowań do badania zewnętrznych źródeł logów, wykrywa zdarzenia odbiegające od norm.

• Zaawansowana analityka/tendencje: umożliwia priorytetyzację zdarzeń związanych z ogólnym stanem bezpieczeństwa wszystkich zasobów firmy poprzez kontekstowy dostęp do informacji.

• Szybka reakcja na naruszenia bezpieczeństwa: konfigurowalne alerty dotyczące inicjowanych przez administratora wysyłek maili, powiadomień i ticketowania zadań lub zautomatyzowane działania poprzez API.

• Ujednolicone raportowanie: zapewnia różne perspektywy oglądu konfiguracji systemów, podatności, zagrożeń i danych o zdarzeniach, pozwalające ocenić ogólny poziom bezpieczeństwa firmy.

• Usprawniona zgodność: wstępnie zdefiniowane kontrole zgodności z wymogami przemysłowych standardów i regulatorów, takich jak CERT, DISA STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH i innych.

• Integracja z istniejącą infrastrukturą: włącznie z systemami zarządzania poprawkami WSUS, SCCM, Red Hat, IBM i VMware, systemy MDM (Microsoft, Apple i Good Technology), narzędzia do ticketowania i działań naprawczych.

Całkowicie zintegrowane rozwiązanie

SecurityCenter™ jest jedynym całościowym i zintegrowanym rozwiązaniem dot. bezpieczeństwa, które łączy dane z:

• Nessus®: najczęściej wdrażany skaner do wykrywania podatności, błędów konfiguracji i złośliwego oprogramowania na urządzeniach sieciowych, w systemach, bazach danych i aplikacjach.

• Passive Vulnerability Scanner™: stale monitoruje ruch sieciowy identyfikując nowe hosty, usługi, protokoły, wykrywając podatności i zagrożenia natychmiast po ich wystąpieniu.

• Log Correlation Engine™: gromadząc i korelując dane z logów urządzeń sieciowych, punktów końcowych i serwerów aplikacji z całego przedsiębiorstwa zapewnia analitykę, pozwalającą na podjęcie decyzji i działań.

Wersje SecurityCenter™

SecurityCenter™

SecurityCenter™ jest rozwiązaniem do analizy podatności nowej generacji, które zawiera wiele skanerów Nessus, powszechnie wdrażanego skanera podatności. Zapewnia najbardziej kompleksowy ogląd poziomu bezpieczeństwa rozproszonych i złożonych infrastruktur IT.

SecurityCenter™ Continuous View

SecurityCenter™ Continuous View jest zaprojektowaną z myślą o potrzebach rynku platformą do ciągłego monitorowania. Łączy ona SecurityCenter™ z wieloma czujkami sieciowymi Passive Vulnerability Scanner (PVS™) i Log Correlation Engine (LCE™) w celu zapewnienia ciągłego monitorowania sieci.