tenable network security

SecurityCenter™ CV
continuous view

Zaprojektowana z myślą o potrzebach rynku platforma do ciągłego monitorowania

Zmieniający się sektor IT (wirtualne, mobilne i usługi 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.

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

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.

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.

"To wszechstronny as wśród rozwiązań Tenable, pozwala w każdej chwili spriorytetyzować ryzyka i ocenić ogólny stan bezpieczeństwa mego przedsiębiorstwa w oparciu o cele biznesowe"
— Dostawca usług z sektora opieki zdrowotnej

Istotne korzyści

- Wykrywa, co się dzieje 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

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 C&C serwerów.
- **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.

Więcej szczegółów na stronach tenable.com oraz openbiz.pl