

NESSUS EXPERT

ZABEZPIECZENIE WSPÓŁCZESNEJ POWIERZCHNI ATAKU

Współczesny sposób myślenia o powierzchni ataku znacznie odbiega od tego z 1998 r., kiedy to platforma Nessus po raz pierwszy pojawiła się na rynku. Specjaliści muszą teraz przyjmować szerszą perspektywę w zakresie ochrony organizacji, ponieważ strony atakujące znajdują się w świecie nieograniczonych podatności, które mogą chcieć wykorzystać.

Specjaliści ds. zabezpieczeń, konsultanci, deweloperzy i pentesterzy potrzebują rozwiązania do oceny podatności, które będzie uwzględniało zagrożenia wpływające na coraz szerszą powierzchnię ataku. Nowe wektory ataków wykraczają poza tradycyjne zasoby IT – np. infrastruktura chmurowa i rozproszone zasoby skierowane na zewnątrz, nieznane dla organizacji.

WZBOGACENIE PORTFOLIO NARZĘDZI DO DOKONYWANIA OCENY

Nessus to najlepiej rozpoznawalny w branży skaner podatności. Nessus Expert wykorzystuje to dziedzictwo, stając się pierwszym rozwiązaniem z zakresu oceny podatności, które zapewnia widoczność w obrębie współczesnej powierzchni ataku. Nessus Expert rozwija możliwości Nessus Professional, aby zapewniać zrozumienie zagrożeń wykraczających poza zasoby IT – gwarantując oceny wdrożeń infrastruktury jako kodu (IaC) i odkrywając zasoby narażone ze strony Internetu – wszystko to w jednym rozwiązaniu.

DOKŁADNOŚĆ I ZAKRES DZIAŁANIA

Zespół Tenable Research ściśle współpracuje ze społecznością zajmującą się zabezpieczeniami, aby odkrywać nowe podatności i zapewniać analitykę, dzięki której organizacje mogą rozwijać swoje praktyki z zakresu oceny podatności. Zespół Tenable Zero Day odkrył ponad 100 obszarów podatności dnia zerowego w ciągu ostatnich trzech lat.

NESSUS TO NR 1 W BRANŻY OCENY PODATNOŚCI

Nr 1 w zakresie dokładności

Nessus ma najniższy w branży współczynnik fałszywych potwierżeń w kontekście dokładności sixsigma (pomiar: 0,32 defektu na 1 milion skanowań).

Nr 1 w zakresie skuteczności działania

Nessus zapewnia największą dokładność i najszerszy zakres działania spośród ponad 62 000 CVE i ponad 100 nowych wtyczek wydawanych cotygodniowo, w ciągu 24 godzin od ujawnienia podatności.

Nr 1 w zakresie wdrażania

Platformie Nessus zaufało ponad 30 000 organizacji z całego świata, a aplikację pobrano 2 miliony razy. 50% firm z listy Fortune 500 i ponad 30% firm z listy Global 2000 polega na technologii Nessus.

ODKRYJ I OCEN
ZASOBY IT

ZABEZPIECZ
INFRASTRUKTURĘ CHMUROWĄ
PRZED WDROŻENIEM

ZYSKAJ WGLĄD
W POWIERZCHNIĘ ATAKU
SKIEROWANĄ NA INTERNET

WDRAŻAJ ZABEZPIECZENIA OD SAMEGO POCZĄTKU I CHROŃ INFRASTRUKTURĘ CHMUROWĄ

W środowisku usług i infrastruktury chmurowej wdrażanie nowych aplikacji i obciążeń roboczych może być bardzo proste. Jednak prędkość i elastyczność mają swój koszt – dodatkowe, nieznane zagrożenia cybernetyczne w tych środowiskach. Dostępne są istniejące rozwiązania do zabezpieczania chmury, ale są stosowane zbyt późno. Nessus Expert umożliwia skanowanie repozytoriów kodu IaC przed przejściem do środowiska produkcyjnego, aby zapewniać ochronę przed nieznanymi zagrożeniami.

KLUCZOWE KORZYŚCI:

- Korzystanie z proaktywnego podejścia do oceny podatności obciążeń roboczych w chmurze.
- Odkrywanie nieznanymi problemami z bezpieczeństwem w ramach cyklu rozwoju oprogramowania (SDLC).
- Skanowanie w celu wykrywania kosztownych i siejących spustoszenie podatności, zanim kod zostanie wdrożony.

ZYSKAJ WGLĄD W POWIERZCHNIĘ ATAKU SKIEROWANĄ NA INTERNET

Współczesna powierzchnia ataku składa się z zasobów skierowanych na Internet, które często są nieznanymi ze względu na brak środków do kontrolowania zasobów oraz możliwości deweloperów do wdrażania wystąpień chmurowych w ciągu kilku minut. Z perspektywy atakującego zasoby skierowane na Internet umożliwiają proste sondowanie podatności z ukrycia i infiltrowanie sieci, zwłaszcza gdy właściciel zasobów nie wie, komu zostały ujawnione... lub nie wie w ogóle, że takie zasoby istnieją. Nessus Expert umożliwia odkrywanie i ocenianie tych nieznanymi zasobów.

KLUCZOWE KORZYŚCI:

- Odkrywanie połączonych z Internetem zasobów, które wcześniej nie były znane w organizacji.
- Uruchamianie skanowania z oceną dla nowo zidentyfikowanych zasobów.
- Lepsze rozumienie ryzyka i niwelowanie luk dla zasobów wykraczających poza perymetr.

WYKORZYSTAJ MOC PREDYKCYJNEGO USTALANIA PRIORYTETÓW

Wykorzystaj ocenę priorytetu podatności Vulnerability Priority Rating (VPR) od Tenable, aby określać podatności, które stwarzają największe zagrożenie dla danego środowiska. Funkcja VPR łączy dane dotyczące podatności gromadzone przez Tenable z danymi zewnętrznymi i danymi dotyczącymi zagrożeń, a następnie analizuje je przy użyciu zaawansowanego algorytmu nauki o danych, opracowanego przez zespół Tenable Research.

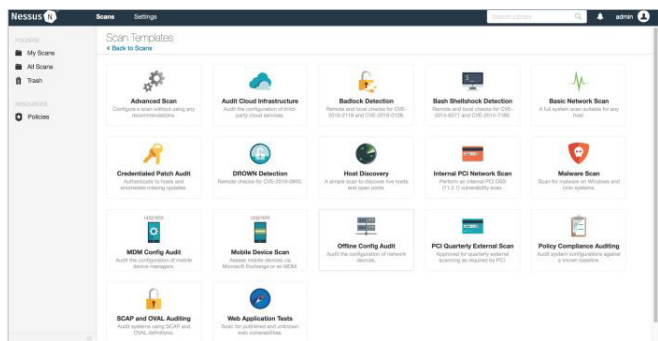
PROSTOTA OBSŁUGI

Rozwiązanie opracowane z myślą o specjalistach od zabezpieczeń, przez specjalistów od zabezpieczeń – platforma Nessus została stworzona jako pojedynczy punkt kontaktowy zapewniający intuicyjne środowisko dla profesjonalistów zajmujących się bezpieczeństwem na linii frontu. Dzięki tej platformie można szybciej i z większą pewnością wykrywać oraz naprawiać luki w zabezpieczeniach.

Aktualizacje środowiska użytkownika zwiększyły prostotę i intuicyjność nawigacji oraz obsługi. Nowe centrum zasobów Nessus udostępnia użytkownikom niezbędne informacje na wyciągnięcie ręki. Przewodniki dla użytkownika zawierają cenne informacje oraz wytyczne oparte na wykonywanych operacjach i funkcjach.

Szybkie wyświetlanie podatności z wstępnie opracowanymi politykami i szablonami

Gotowe do użytku, wstępnie skonfigurowane szablony dla zespołów IT i zasobów mobilnych, z uwzględnieniem audytów konfiguracji, pomagają w szybkim lokalizowaniu podatności.



Ponad 450 szablonów zgodności i konfiguracji umożliwia przeprowadzanie audytów zgodności konfiguracji względem wartości CIS i innych najlepszych praktyk.

Inteligentna ocena podatności z funkcją Wyniki na żywo

Funkcja Wyniki na żywo wykonuje inteligentną ocenę podatności w trybie offline przy każdej aktualizacji wtyczki – bez potrzeby uruchamiania skanowania. Wystarczy zalogować się i sprawdzić rezultaty oceny potencjalnych podatności w oparciu o historię skanowania. Wystarczy kliknąć przycisk, aby uruchomić skanowanie i potwierdzić obecność podatności – w ten sposób tworzy się szybsze, bardziej wydajne procesy oceny, ustalania priorytetów i rozwiązywania problemów.

Proste konfigurowanie raportów

Twórz raporty w oparciu o niestandardowe widoki (np. konkretne typy podatności, podatności wg hosta/wtyczki, wg zespołu/klienta) – w różnych formatach (HTML, CSV i Nessus XML).

Szczegółowe badanie i rozwiązywanie problemów

Sieci stają się coraz bardziej złożone i skomplikowane, przez co dokładne namierzenie potencjalnych problemów staje się bardzo czasochłonne. Funkcja przechwytywania pakietów Nessus zapewnia zaawansowane możliwości w zakresie debugowania, co umożliwia rozwiązywanie problemów ze skanowaniem.

Skupienie na najważniejszych kwestiach w grupowanym widoku

Podobne problemy lub kategorie podatności są grupowane razem i reprezentowane w jednym wątku. Opcja drzemki umożliwia użytkownikom wybranie problemów, które powinny zniknąć z widoku na określony czas. Ułatwia to ustalanie priorytetów – możesz skupić się tylko na tych problemach, które wymagają pracy w danym momencie.

Przenośne i elastyczne rozwiązanie

Platforma Nessus jest teraz dostępna na Raspberry Pi, co zapewnia większą mobilność i prostotę obsługi. Jest to szczególnie przydatne dla pentesterów, konsultantów i innych pracowników, których zadania wymagają przemieszczania się pomiędzy różnymi lokalizacjami.

DOSTĘPNE ZAAWANSOWANE WSPARCIE

Klienci Nessus Professional mogą uzyskać dostęp do pomocy technicznej za pośrednictwem poczty e-mail, portalu, czatu i telefonu – 24 godziny na dobę, 365 dni w roku – z subskrypcją zaawansowanego poziomu wsparcia technicznego. W ten sposób można również cieszyć się szybszymi reakcjami i rozwiązywaniem problemów. Wszystkie informacje dotyczące planów pomocy technicznej można znaleźć [tutaj](#).

INFORMACJE O TENABLE

Tenable®, Inc. to firma Cyber Exposure. Pomaga ponad 30 000 organizacjom na całym świecie zrozumieć i ograniczyć cyberzagrożenia. Jako twórca technologii Nessus® firma Tenable rozszerzyła swoją wiedzę ekspercką w dziedzinie podatności, by zaoferować najlepszą na świecie platformę do przeglądania i zabezpieczania wszelkich zasobów cyfrowych – na dowolnej platformie obliczeniowej. Wśród klientów Tenable jest ponad 50% firm z listy Fortune 500, ponad 30% firm z listy Global 2000 oraz wiele dużych agencji rządowych. Dowiedz się więcej na stronie www.tenable.com.

Więcej informacji: odwiedź stronę tenable.com

Kontakt: wyślij wiadomość e-mail na adres sales@tenable.com lub odwiedź stronę tenable.com/contact

