DLACZEGO WARTO DOKONAĆ UAKTUALNIENIA – 5 NAJWAŻNIEJSZYCH POWODÓW

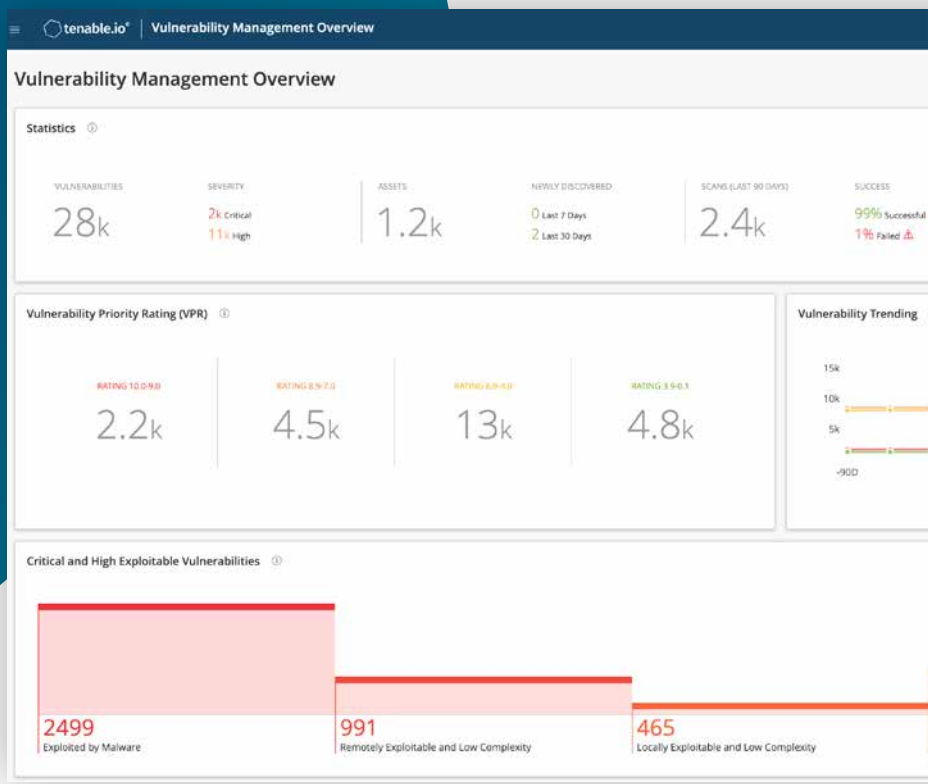
PRZEJŚCIE Z NESSUS PRO NA PLATFORMĘ TENABLE W CELU ZARZĄDZANIA PODATNOŚCIAMI NA PODSTAWIE RYZYKA

Użytkownicy Nessus® Professional korzystają już z najbardziej kompleksowych narzędzi do oceny podatności (VA) na rynku. Jednak nawet najlepsze narzędzia VA nie zostały zaprojektowane z myślą o dzisiejszych płaszczyznach ataków oraz rosnącej liczbie zagrożeń. Widoczność tych narzędzi jest ograniczona do tradycyjnych środowisk IT, przez co całkowicie pomijają one wszelkie podatności występujące w najbardziej dynamicznych aspektach dzisiejszych płaszczyzn ataków, takich jak środowiska chmurowe, kontenerowe i związane z technologiami operacyjnymi.

Ponadto do określania podatności, które należy usunąć, wykorzystuje się oceny oparte na systemie CVSS (Common Vulnerability Scoring System), co stanowi duże ograniczenie. CVSS jest systemem dalekim od doskonałości. Może on zasypać Twój zespół tysiącami podatności w miesiącu, co z kolei może prowadzić do tracenia czasu na takie, które nie niosą ze sobą poważnego ryzyka biznesowego.

Aby sprostać tym wyzwaniom, należy w taki sposób rozwijać program VA, aby przy zarządzaniu podatnościami uwzględniać stopień ryzyka (VM).

Dzięki uaktualnieniu programu Nessus Professional do pełnej wersji platformy Tenable zyskasz następujące możliwości:



1. Modernizacja programu bezpieczeństwa

Potrzebujesz czegoś więcej niż samej listy podatności, wydłużającej się z miesiąca na miesiąc. Platforma Tenable umożliwi Ci aktywne zarządzanie podatnościami, co z kolei przełoży się na zmniejszenie liczby zagrożeń przy możliwie najmniejszym nakładzie pracy. Nadaj odpowiedni priorytet zasobom i podatnościom o znaczeniu krytycznym, skutecznie zarządzaj ryzykiem, podejmując właściwe działania, oraz monitoruj kluczowe wskaźniki wydajności (KPI), aby lepiej zrozumieć wartość programu VM opartego na ryzyku i podzielić się swoją wiedzą z innymi.

2. Obserwacja całej powierzchni ataku

Pomyślne przejście audytu nie oznacza gwarancji bezpieczeństwa. Okazjonalne skanowanie wyłącznie zasobów, które wchodzą w zakres audytu, należy zastąpić nieustanną oceną wszystkich znanych zasobów. Dodatkowo należy każdorazowo odnotować fakt dodania nowych zasobów do sieci, a następnie je ocenić. Dzięki nieustannemu monitorowaniu całej powierzchni narażonej na ataki platforma Tenable eliminuje martwe punkty, które były plagą starszych narzędzi, i pozwala zespołom ds. bezpieczeństwa wspólnie odkrywać podatności i poddawać je ocenie.

3. Przewidywanie ryzyka podatności z pełnymi danymi kontekstowymi

Same wyniki bazowe z systemu CVSS nie wystarczą, aby określić, co wymaga naprawy. Platforma Tenable dodaje do wyników z systemu CVSS rozbudowane dane kontekstowe, w tym te dotyczące poziomu krytyczności danego zasobu i zagrożenia, a także wykorzystuje informacje o exploitach i przewiduje, które podatności mogą zostać wykorzystane w ciągu kolejnych 30 dni. Gdy zrozumiesz realne ryzyko biznesowe stojące za każdą podatnością, zyskasz czas, aby skoncentrować uwagę na podatnościach, którymi należy się zająć najpilniej.

4. Szybkie i pewne działanie

Zaoszczędź czas i zyskaj pewność dzięki zautomatyzowanym analizom. Platforma Tenable wykorzystuje automatyzację uczenia maszynowego do nieustannego poszukiwania korelacji, przetwarzania i analizowania petabajtów danych zabezpieczeń, aby zawsze dostarczać najnowszą analizę ewoluującego krajobrazu zagrożeń. Dzięki temu zespoły ds. bezpieczeństwa wiedzą, że zajmują się właściwymi sprawami i nie marnują cennego czasu na ręczną analizę podatności w celu określenia ich stopnia ryzyka.

5. Jasne wskaźniki sukcesu

Liczba wdrażanych poprawek nie ma znaczenia, jeśli usuwasz niewłaściwe podatności. Z platformą Tenable mierzysz sukces zespołu ds. bezpieczeństwa, monitorując ryzyko, na jakie narażone są zasoby o znaczeniu krytycznym. Krótko mówiąc, wiesz, że Twoja praca ma znaczenie. Dzięki potężnym i konfigurowanym narzędziom raportowania możesz skutecznie informować o wydajności zespołu liczne grono interesariuszy i zyskać, a potem utrzymać, zaufanie kierownictwa do Twoich umiejętności.

tenable

Przechodząc z rozwiązania Nessus Professional na pełną platformę Tenable, możesz wykorzystać pełny potencjał programu VM opartego na ryzyku, który maksymalizuje wydajność i efektywność działań naprawczych. Dzięki temu możesz zrobić możliwie najlepszy użytek z ograniczonych zasobów bezpieczeństwa.

DOWIEDZ SIĘ WIĘCEJ