tenable.io

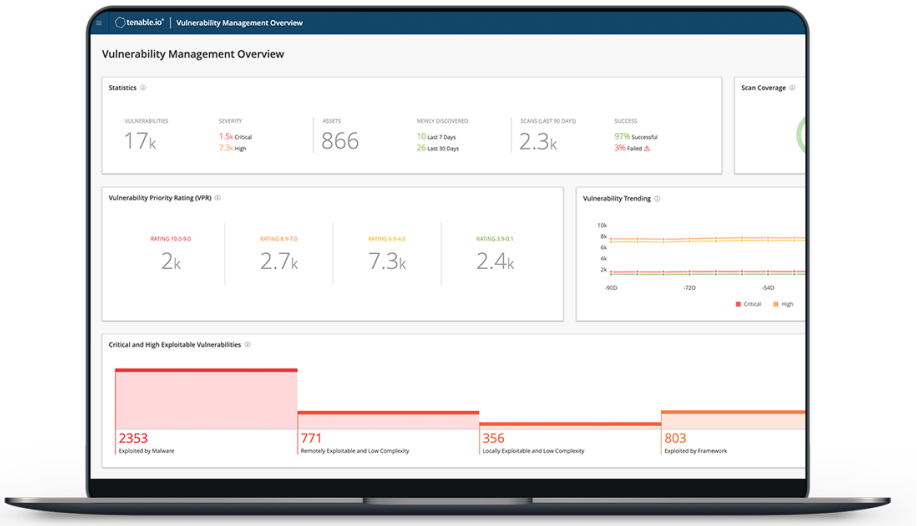
SPECYFIKACJA

ZARZĄDZANIE WSPÓŁCZESNYMI PODATNOŚCIAMI

ZOBACZ WSZYSTKO. PRZEWIDUJ TO, CO MA ZNACZENIE

Niezależnie od tego, czy rozwiązanie Tenable.io kupujesz jako samodzielny produkt, czy kluczowy komponent platformy Tenable Exposure (Tenable.ep), rozwiązanie to zapewnia oparty na ryzyku wgląd w całą powierzchnię ataku – od zasobów IT po chmurę, OT i kontenery – dzięki czemu możesz szybko identyfikować, badać i ustalać priorytety dla podatności. Zyskujesz natychmiastową widoczność, więc możesz zrozumieć zagrożenia i poznać podatności, które należy naprawić jako pierwsze.

Platforma Tenable.io, zarządzana w chmurze i oparta na technologii Nessus, zapewnia najbardziej kompleksowe w branży pokrycie podatności, z możliwością przewidywania najpilniejszych problemów związanych z bezpieczeństwem. Używając zaawansowanego algorytmu do identyfikacji zasobów, platforma Tenable.io zapewnia najbardziej dokładne informacje o dynamicznych zasobach i podatnościach w ciągle zmieniających się środowiskach. Jest to rozwiązanie chmurowe, a jego intuicyjne wizualizacje pulpitów nawigacyjnych, kompleksowe ustalanie priorytetów w oparciu o zagrożenia i bezproblemowa integracja z rozwiązaniami firm trzecich pomagają zespołom ds. bezpieczeństwa w maksymalizowaniu wydajności i skalowaniu pod kątem większej produktywności.



Ilustracja 1.

Tenable.io zapewnia dokładny wgląd w zasoby i podatności w środowisku, aby pomagać w ustalaniu priorytetów dla działań naprawczych w oparciu o faktyczne zagrożenia cybernetyczne.

KLUCZOWE KORZYŚCI

- **Ciągła widoczność**
  Śledź na bieżąco znane i nieznane zasoby i podatności. Identyfikuj zagrożenia i nieoczekiwane zmiany sieciowe, zanim przerodzą się one w naruszenia zabezpieczeń.
- **Większa produktywność**
  Wykorzystaj rozwiązanie oparte na SaaS, aby przeprowadzać wstępne oceny w mniej niż 5 minut, bez nakładów związanych ze sprzętem IT i konserwacją.
- **Priorytetyzacja podatności**
  Połącz dane o podatnościach, analitykę zagrożeń i naukę o danych, aby łatwiej zrozumieć oceny zagrożeń oraz szybko identyfikować największe zagrożenia biznesowe.
- **Automatyzacja procesów**
  Wykorzystaj w pełni udokumentowane interfejsy API i wstępnie skompilowane integracje, aby importować dane stron trzecich, automatyzować skanowanie i udostępniać dane swoim zespołom IT.
- **Maksymalizacja zwrotu z inwestycji**
  Wyeliminuj podwójne lub potrójne liczenie zasobów, które mają wiele adresów IP, korzystając z pierwszego w branży modelu licencjonowania opartego na zasobach.

KLUCZOWE MOŻLIWOŚCI

Przyjazne dla klientów, elastyczne licencjonowanie zasobów

Platforma Tenable.io oferuje pierwszy na rynku model licencjonowania oparty na zasobach, który zużywa jedną licencję na zasób, nawet jeśli zasób ma wiele adresów IP. Elastyczny model rozwiązania umożliwia również skanowanie w przypadku tymczasowego przekroczenia limitu licencji, a także automatycznie odzyskuje licencje z rzadko skanowanych zasobów lub jednorazowych wystąpień.

Kompleksowe opcje oceny

Tenable.io zapewnia ujednolicony wgląd w całą powierzchnię ataku. Platforma wykorzystuje czujniki Nessus, połączenie aktywnych skanerów, agentów, pasywnego monitorowania sieciowego, łączników chmurowych i integracji CMDB w celu maksymalizacji zakresu skanowania w infrastrukturze i zredukowania martwych pól podatności. Takie połączenie różnych typów czujników danych pomaga śledzić i oceniać znane i nieznane zasoby oraz ich podatności, z uwzględnieniem zasobów trudnych do przeskanowania, takich jak przejściowe urządzenia analizowane przez agentów i czułe systemy (np. przemysłowe systemy sterowania).

Dokładne śledzenie podatności oparte na zasobach

Platforma Tenable.io zapewnia możliwość śledzenia zasobów i ich podatności w sposób dokładniejszy niż jakiekolwiek inne rozwiązanie w branży. Zaawansowany algorytm identyfikacji zasobów korzysta z szerokiego zestawu atrybutów (np. Tenable ID, nazwy NetBIOS, adresu MAC i wielu innych), aby dokładnie identyfikować i śledzić zmiany w zasobach, niezależnie od tego, jak się zmieniają i jak długo trwają.

Ustalanie priorytetów podatności w oparciu o faktyczne zagrożenie

Tenable.io łączy dane dotyczące podatności, analitykę zagrożeń i naukę o danych, aby zapewniać łatwe do zrozumienia oceny ryzyka i umożliwiać ustalanie podatności wymagających naprawy w pierwszej kolejności. Szybko ocenisz ryzyko i zidentyfikujesz podatności o najwyższym wpływie na organizację.

Uproszczone zarządzanie podatnościami

Dzięki nowoczesnemu interfejsowi z intuicyjnymi wizualizacjami pulpitu nawigacyjnego platforma Tenable.io sprawia, że typowe zadania, takie jak konfiguracja skanowania, ocena i analiza rezultatów, są prostsze niż kiedykolwiek. Wstępnie zdefiniowane szablony skanowania i kontrolne audyty konfiguracji zgodne z najlepszymi normami, np. CIS i DISA STIG, pomagają Ci chronić organizację przy ułamku wysiłku, który byłby konieczny bez tego rozwiązania. Dostosuj raporty i analizy, korzystając ze wstępnie skonfigurowanych i gotowych do użycia pulpitów nawigacyjnych, lub szybko zbuduj własny pulpit od zera, aby sprostać potrzebom organizacji.

Zautomatyzowana widoczność chmury

Platforma Tenable.io zapewnia ciągłą widoczność i oceny środowisk w chmurach publicznych. Łączniki chmurowe automatycznie identyfikują zasoby w chmurach Amazon Web Services, Microsoft Azure i Google, a także monitorują ich stan w czasie rzeczywistym. Oceniaj środowiska w chmurze przy pomocy czujników Nessus, aby wykrywać podatności, złośliwe oprogramowanie i problemy z konfiguracją i zgodnością.

Widoczność technologii operacyjnej (OT)

Platforma Tenable.io integruje się z rozwiązaniem Tenable.ot, zapewniając korzyści zunifikowanego, opartego na ryzyku wglądu w infrastrukturę konwergentną. Zyskujesz ciągłą widoczność, możliwość wykrywania i minimalizowania zagrożeń, adaptacyjne oceny, zarządzanie podatnościami i kontrolę konfiguracji, dzięki czemu możesz chronić organizację przed zagrożeniami OT i IT.

Wstępnie skompilowane integracje i udokumentowane interfejsy API oraz zintegrowane zestawy SDK

Tenable.io zapewnia wstępnie skompilowane integracje – zwane „wtyczkami" – dostępne dla popularnych systemów zarządzania poświadczeniami, SIEM i zarządzania zgłoszeniami, a także innych rozwiązań uzupełniających. Dzięki temu można z łatwością opracować wydajny proces zarządzania podatnościami. Kompletną listę można znaleźć tutaj: https://www.tenable.com/partners/technology. Ponadto można z łatwością utworzyć własne integracje z Tenable.io, korzystając z w pełni udokumentowanych interfejsów API i zestawów SDK. Zastosowanie tych narzędzi do maksymalizacji wartości danych dotyczących podatności nie wiąże się z żadnymi dodatkowymi kosztami.

Umowy SLA z gwarancją dostępności

Tenable zapewnia pierwszą i jedyną w branży zarządzania podatnościami gwarancję dostępności usługi w postaci kompleksowej umowy o poziomie świadczenia usług (SLA) dla platformy Tenable.io. W przypadku braku realizacji postanowień umowy SLA oferowane są środki na usługi, tak jak w przypadku czołowych dostawców rozwiązań chmurowych, np. Amazon Web Services.

Zatwierdzony dostawca skanowania z certyfikacją PCI

Tenable.io to rozwiązanie zatwierdzonego dostawcy skanowania (ASV) z certyfikacją PCI umożliwiające sprzedawcom i dostawcom usług demonstrowanie bezpieczeństwa systemów połączonych z Internetem, zgodnie z wymaganiami dla skanowania zewnętrznego podatności sieciowych PCI Data Security Standard (PCI DSS).

Rozwiązanie wspierane przez Tenable Research

Platforma Tenable.io jest wspierana przez zespół badawczy Tenable Research, który zapewnia światowej klasy dane dotyczące narażenia cybernetycznego, analitykę z zakresu nauki o danych, alerty i porady dotyczące zabezpieczeń. Częste aktualizacje od Tenable Research gwarantują dostępność najnowszych kontroli podatności, badań dotyczących luk dnia zerowego oraz testów porównawczych konfiguracji, by wspierać i chronić organizację.

Więcej informacji: odwiedź stronę tenable.com
Kontakt: wyślij wiadomość e-mail na adres sales@tenable.com