# Tenable One

## Platforma zarządzania narażeniem

### Przewiduj prawdopodobne ataki. Zredukuj proaktywnie narażenie

W obliczu dramatycznego wzrostu liczby ataków ransomware, zagrożeń obejmujących cały kraj oraz nowych podatności zespoły ds. cyberbezpieczeństwa to nieustannie oblegane fortece. Aby walczyć z tymi zagrożeniami, powstało wiele nowych rozwiązań w zakresie wykrywania zagrożeń oraz reagowania na incydenty, dzięki którym zespoły ds. cyberbezpieczeństwa mogą stawiać czoła nowym wyzwaniom związanym z bezpieczeństwem. Jednak taka liczba różnych rozwiązań jest związana z wieloma wymogami dotyczącymi metryk, raportowania i szkolenia, co utrudnia ujednolicenie różnych analiz i zrozumiałe komunikowanie stanu zabezpieczeń organizacji.

Dzięki rozwiązaniu Tenable One organizacje mogą teraz przekładać techniczne dane dotyczące zasobów, podatności i zagrożeń na zrozumiałe informacje biznesowe oraz analizy umożliwiające podejmowanie działań kadrze kierowniczej i wszystkim osobom zajmującym się bezpieczeństwem. Platforma zapewnia najszersze pokrycie luk w zabezpieczeniach z różnymi zasobami IT, zasobami w chmurze, kontenerami, aplikacjami internetowymi i systemami tożsamości, wykorzystuje prędkość i głębię pokrycia podatności zapewnianego przez zespół Tenable Research, a także dodaje kompleksową analitykę i ustalanie priorytetów dla działań i komunikacji związanej z zagrożeniami cybernetycznymi. Dzięki Tenable One organizacje zyskują następujące korzyści:

- Kompleksowy wgląd we współczesną powierzchnię ataku
- Przewidywanie zagrożeń i nadawanie priorytetów działaniom, dzięki którym można zapobiegać atakom
- Komunikacja w zakresie zagrożenia cybernetycznego umożliwiająca podejmowanie lepszych decyzji


## KLUCZOWE KORZYŚCI

**Kompleksowa widoczność**
*Zyskaj ujednolicony wgląd* we wszystkie zasoby i powiązane podatności programowe, podatności związane z konfiguracją oraz uprawnieniami: niezależnie od tego, czy są to zasoby lokalne, czy działające w chmurze. Monitoruj stale Internet, aby natychmiastowo odkrywać i identyfikować wszystkie zasoby z łącznością zewnętrzną w celu wyeliminowania obszarów znanych i nieznanych zagrożeń. Zredukuj czas i wysiłki wymagane do zrozumienia całej powierzchni ataku, wyeliminowania martwych punktów i stworzenia fundamentów dla efektywnego zarządzania ryzykiem.

**Przewidywanie**
*Przewiduj konsekwencje* ataków cybernetycznych poprzez wykorzystanie największego w branży zestawu danych, aby zrozumieć relacje pomiędzy zasobami, narażeniami, uprawnieniami i zagrożeniami w ścieżce ataku.

**Ustalanie priorytetu dla działań**
*Popraw ustalanie priorytetów dla zagrożeń* poprzez ciągłą identyfikację i skupienie się na podatnościach możliwych do wykorzystania, ścieżkach ataku i lukach w zabezpieczeniach, które stanowią największe ryzyko. Zapewnia to bardziej dokładne i predykcyjne dane dotyczące rozwiązań, dzięki którym można wyeliminować ryzykowne ścieżki przy możliwie niewielkim wysiłku w celu zapobiegania atakom.

**Efektywna komunikacja w zakresie zagrożenia cybernetycznego**
Zyskaj *scentralizowany i zgodny z założeniami biznesowymi wgląd w zagrożenia* przy użyciu wyraźnych wskaźników KPI, aby wykazywać postępy w czasie i przedstawiać wyniki testów porównawczych realizowanych względem zewnętrznych konkurentów z branży. Informacje umożliwiające podejmowanie decyzji przekładają się na oceny ryzyka zgodne z założeniami biznesowymi, które poprawiają ogólną komunikację i współpracę pomiędzy różnymi interesariuszami.

**Elastyczne licencjonowanie**
Przydzielaj licencje produktów zgodnie z realnymi potrzebami związanymi z narażeniem na niebezpieczeństwo i modyfikuj przydział wedle potrzeb i uznania.

# KLUCZOWE MOŻLIWOŚCI

## Globalny wgląd w narażenia

Zapewnia rozwiązania w ramach skoncentrowanych wysiłków w zakresie bezpieczeństwa poprzez dostarczanie jasnych, zwięzłych danych dotyczących narażenia na niebezpieczeństwo organizacji, z odpowiedzią na pytania o krytycznym znaczeniu, np. „W jakim stopniu jesteśmy bezpieczni?" oraz „Jak wyglądają nasze działania w zakresie prewencji i łagodzenia skutków?". Odpowiedź na pytanie „Jak radzimy sobie w czasie i jakie są kluczowe zdarzenia?" umożliwia stosowanie ujednoliconego, globalnego wyniku w kontekście narażenia na niebezpieczeństwo w oparciu o różne źródła danych.

## Zarządzanie powierzchnią ataku zewnętrznego

Wgląd w zewnętrzną powierzchnię ataku, dzięki któremu organizacje mogą identyfikować i redukować zagrożenia z perspektywy atakującego.

## Ocena ścieżki ataku

Przykłady wizualizacji ścieżki ataku i ustalenia priorytetów umożliwiają skoncentrowane reagowanie przerywające wszelkie prawdopodobne ścieżki ataków. Funkcja jest realizowana poprzez mapowanie krytycznych zagrożeń w strukturze MITRE ATT&CK w celu ciągłej wizualizacji wszystkich użytecznych ścieżek ataku – lokalnie i w chmurze.

## Scentralizowany spis zasobów

Wyeliminuj martwe pola. Kompleksowy spis zasobów zapewnia pełną widoczność wszystkich zasobów, niezależnie od źródła danych (VM, WAS, Active Directory itp.). Ten scentralizowany wgląd w zasoby z różnych źródeł danych umożliwia tworzenie konkretnych znaczników zasobów obejmujących ich różne typy.

## Zarządzanie podatnościami oparte na ryzyku

Zredukuj podatności w całej powierzchni ataku poprzez dynamiczne ustalanie priorytetów w oparciu o zagrożenia z prawdziwego świata i uwzględnienie tych danych analitycznych dotyczących ryzyka w pomiarach narażenia organizacji na zagrożenia.

## Kompleksowa ocena

Wgląd w narażenie na niebezpieczeństwo cybernetyczne wszystkich zasobów, wraz z podatnościami, błędnymi konfiguracjami i innymi potencjalnymi zagrożeniami bezpieczeństwa.

## Bezpieczna usługa Active Directory

Zakłócanie ataków na usługę Active Directory – organizacje mogą zobaczyć wszystkie ważne dane, przewidywać istotne kwestie i reagować na zagrożenia dla usługi AD.

## Bezpieczna infrastruktura chmurowa

Kompletna i ciągła widoczność i działania naprawcze w przypadku narażenia we wszystkich zasobach chmurowych.

## Kubernetes i bezpieczeństwo kontenerów

Bezpieczne skanowanie obrazów kontenerów bez potrzeby przesyłania obrazów poza sieć organizacji.

## Zautomatyzowane skanowanie aplikacji webowych

Zapewnia kompleksowe i dokładne skanowanie podatności, z pełną widocznością narażenia zasobów IT, chmury i aplikacji webowych.

## Testy porównawcze względem konkurencji

Porównuj narażenie cybernetyczne wewnętrznie pomiędzy jednostkami biznesowymi i poszczególnymi lokalizacjami lub zewnętrznie względem konkurentów z branży, aby określić, kiedy i gdzie należy dokonać kluczowych inwestycji finansowych i w zakresie siły roboczej.

## Metryki efektywności programu

Pomiary dojrzałości rozwiązań zapewniają kontekst dla wysiłków związanych z łagodzeniem ryzyka. Odpowiada na pytania typu „Jak dobrze idzie nam realizacja wewnętrznie ustalonych umów SLA?"

## Nowości

Integracja z blogami Tenable Research umożliwia tworzenie niestandardowych kart narażenia na niebezpieczeństwo, które będą odzwierciedlać postępy w zakresie zabezpieczeń cybernetycznych.

## Rozwiązanie wspierane przez Tenable Research

Światowej klasy dane analityczne dotyczące narażenia cybernetycznego, analityka z zakresu nauki o danych, alerty i porady dotyczące zabezpieczeń.

## Nowość – elastyczne licencjonowanie

Nowe podejście do licencjonowania zasobów – tak elastyczne jak powierzchnia ataku. Licencjonowanie all-inclusive zapewnia elastyczność związaną z dynamiczną relokacją licencji pomiędzy infrastrukturą IT, chmurą, kontenerami, aplikacjami webowymi i użytkownikami usługi AD.

## Informacje o Tenable

Tenable® to firma zajmująca się zarządzaniem narażeniem na niebezpieczeństwo. Pomaga około 40 000 organizacji na całym świecie poznawać i ograniczać 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 około 60% firm z listy Fortune 500, około 40% firm z listy Global 2000 oraz wiele dużych agencji rządowych. Dowiedz się więcej na tenable.com.

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