

PROBLEMY, KTÓRE ROZWIĄZUJEMY

Współczesna powierzchnia ataku rośnie, nieustannie zmienia się i jest bardziej połączona wewnętrznie niż kiedykolwiek wcześniej. W odpowiedzi na te wyzwania zespoły ds. bezpieczeństwa wdrożyły wiele technologii zabezpieczeń, z których każda stosuje własną analitykę i nie zapewnia spójnego raportowania. Rozproszone narzędzia mogą prowadzić do duplikowania wysiłków i tworzenia nieefektywnych programów, bez wyraźnej ścieżki działania umożliwiającej namacalną redukcję ryzyka lub wyraźne komunikowanie stanu zabezpieczeń organizacji. Co gorsza, podejście do cyberbezpieczeństwa oparte na reagowaniu i gaszeniu pożarów sprawia, że obrońcy są na dużo gorszej pozycji.

Zespoły ds. bezpieczeństwa cybernetycznego potrzebują ujednoczonego, predykcyjnego i proaktywnego sposobu na zarządzanie narażeniem na całej powierzchni ataku. Tenable One, platforma do zarządzania narażeniem, zapewnia kontekstową świadomość zagrożeń oraz możliwość przejścia z podejścia reaktywnego do prewencyjnego, dzięki czemu zespoły ds. bezpieczeństwa mogą przewidywać i blokować zagrożenia, zanim spowodują jakiegokolwiek szkody.

DANE O FIRMIE

ROK ZAŁOŻENIA

2002

SIEDZIBA

- Columbia, Maryland, USA
- Siedziba międzynarodowa w Dublinie w Irlandii
- Obecność w ponad 40 krajach

ZASIĘG RYNKOWY

- Ponad 40 000 klientów
- Ponad 60% z listy Fortune 500
- Ponad 40% z rankingu Global 2000

KIEROWNICTWO

Amit Yoran, Chairman and CEO
Steve Vintz, Chief Financial Officer
Mark Thurmond, Chief Operating Officer
Nico Popp, Chief Product Officer
Glen Pendley, Chief Technology Officer
Robert Huber, Chief Security Officer
Dave Feringa, Chief Revenue Officer
Brian Goldfarb, Chief Marketing Officer
Bridgett Paradise, Chief People and Culture Officer
Michelle VonderHaar, Chief Legal Officer and General Counsel
Patricia Grant, Chief Information Officer
Terry Dolce, EVP, Operations, Global Business Development and Channels
James Hayes, Senior Vice President, Global Government Affairs
Michela Stribling, Chief Communications Officer
Matt Olton, Senior Vice President of Corporate Development and Strategy

INFORMACJE O TENABLE

Tenable[®] to firma zajmująca się zarządzaniem zagrożeniami. Pomaga około 43 000 organizacji na całym świecie poznać 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 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.

TENABLE ONE, PLATFORMA DO ZARZĄDZANIA NARAŻENIEM

Tenable One ma za zadanie pomagać organizacjom uzyskać wgląd we współczesną powierzchnię ataku, skoncentrować wysiłki na zapobieganiu prawdopodobnym atakom i precyzyjnie informować o zagrożeniach cybernetycznych, aby wspierać optymalną wydajność biznesową. Platforma Tenable One oferuje różnorodny zakres działania i ochronę przed podatnościami obejmującą zasoby IT, zasoby w chmurze, kontenery, aplikacje webowe i systemy tożsamości.

TENABLE OFERUJE:

Bezpieczeństwo chmury

Tenable oferuje kompletną, wielochmurową widoczność i bezpieczeństwo, zapewniając ujednoczony wgląd w podatności, błędne konfiguracje i dryf – w jednym miejscu. Szybkie ustalanie priorytetów dla działań z ocenami opartymi na ryzyku, raportowanie w zakresie zgodności z przepisami oraz automatyczne działania naprawcze podnoszące średni czas reakcji (MTTR) nawet do 99%.

Skanowanie aplikacji webowych

Aplikacje webowe są wszechobecne, mają kluczowe znaczenie dla biznesu i podlegają ciągłym zmianom. Tenable zapewnia łatwe w obsłudze, kompleksowe i automatyczne skanowanie podatności dla nowoczesnych aplikacji webowych. Użytkownicy mogą konfigurować skanowanie aplikacji webowych i zarządzać nim, a także korzystać z wyników umożliwiających podejmowanie działań w ciągu kilku minut.

Narażenie tożsamości

Niemal za każdym włamaniem trafiającym do nagłówków serwisów informacyjnych stoi atak na usługę Active Directory (AD), który umożliwia atakującemu podniesienie uprawnień i wykorzystanie ruchu bocznego. Tenable zapewnia użytkownikom widoczność wszystkich działań w środowisku AD, przewidywania tego, co ma znaczenie, a także reagowania na zagrożenia w celu usuwania ścieżek ataku, zanim atakujący będą mogli je wykorzystać.

Zarządzanie podatnościami

Starsze narzędzia do zarządzania podatnościami (VM) nie nadają się do współczesnego krajobrazu IT. Zarządzanie podatnościami oparte na ryzyku to koniec ze zgadywaniem, które podatności wymagają priorytetowych działań.

Zarządzanie powierzchnią ataku

Widoczność to podstawa cyberbezpieczeństwa, jednak niewiele organizacji może się nią cieszyć. Zarządzanie powierzchnią ataku zewnętrznego (EASM) mapuje cały Internet i odkrywa wszystkie domeny organizacji. Możesz identyfikować i zabezpieczać wcześniej nieznaną dla organizacji zasoby połączone z Internetem, aby wyeliminować martwe punkty.

Bezpieczeństwo OT

Przemysłowa transformacja cyfrowa zwiększa kontrolę, wydajność, produktywność i bezpieczeństwo, ale wiąże się również z zagrożeniami. Tenable oferuje kompletną widoczność, ujednoczone zabezpieczenia oraz ustalanie priorytetów w kontekście zarządzania zagrożeniami, dzięki czemu można łagodzić ryzyko w całym krajobrazie zintegrowanych systemów IT i OT.

Platforma oparta na rozwiązaniu Nessus, złotym standardzie oceny podatności

Zrozumienie podatności ma fundamentalne znaczenie dla zarządzania narażeniem – Nessus jest rdzeniem platformy Tenable One. Pomagając użytkownikom w ocenie współczesnej powierzchni ataku, rozwiązanie Nessus zapewnia dokładny obraz, dzięki czemu użytkownicy mogą działać szybko i wydajnie.