tenable.io
web app scanning

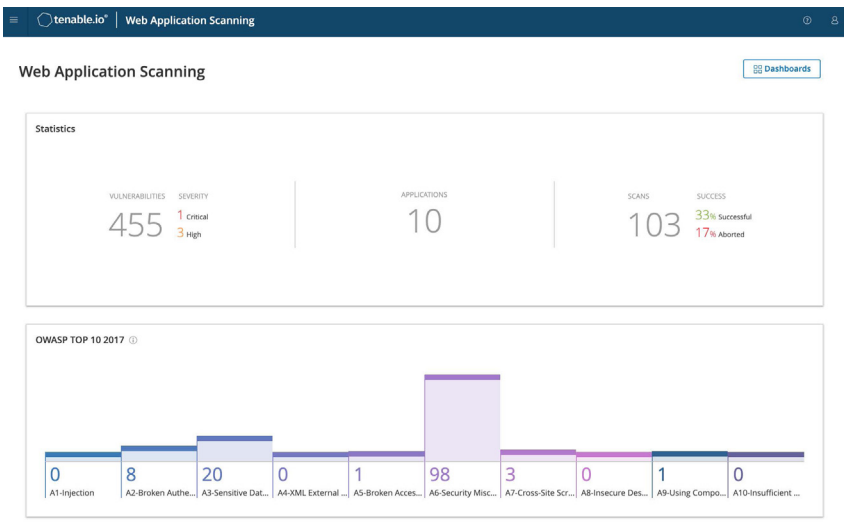
SPECYFIKACJA

PROSTE, SKALOWALNE PODEJŚCIE DO DYNAMICZNEGO TESTOWANIA ZABEZPIECZEŃ APLIKACJI

Nowoczesne aplikacje webowe nadal są wyzwaniem dla organizacji, które chcą je zabezpieczyć, ponieważ deweloperzy opracowują coraz bardziej złożone aplikacje biznesowe – szybciej niż kiedykolwiek wcześniej. Wiele organizacji wydaje nowe lub zaktualizowane aplikacje webowe wiele razy w ciągu dnia, a średnio każda z nich zawiera kilka podatności. Zespoły ds. bezpieczeństwa, które są często 100 razy mniej liczne od zespołów deweloperskich, nie nadążają za zmianami. Wiele aplikacji webowych nie jest ocenianych pod kątem bezpieczeństwa do momentu, gdy jest już za późno. Brak umiejętności i zasobów w zakresie bezpieczeństwa aplikacji uniemożliwia wielu organizacjom wdrażanie adekwatnych zabezpieczeń przed zagrożeniami cybernetycznymi.

Jednak wdrożenie kolejnego, samodzielnego produktu związanego z bezpieczeństwem nie jest właściwym rozwiązaniem. Liderzy ds. bezpieczeństwa muszą mieć wgląd w zabezpieczenia wszystkich aplikacji webowych w ramach kompleksowego rozwiązania do oceny narażenia cybernetycznego, aby zyskać widoczność w kontekście bezpieczeństwa i zgodności.

Niezależnie od tego, czy rozwiązanie Tenable.io Web Application Scanning jest zakupione jako moduł platformy Tenable.io, czy jako kluczowy komponent platformy Tenable Exposure (Tenable.ep), będzie zapewniać tę widoczność w ramach kompleksowego rozwiązania do monitorowania narażenia cybernetycznego. Produkt zapewnia bezpieczne, zautomatyzowane skanowanie podatności, które można z łatwością skalować, aby pokryć całe portfolio produktów online. W ten sposób eksperci ds. zabezpieczeń mogą szybko oceniać swoje aplikacje webowe bez wysiłku związanego z działaniami ręcznymi. Funkcja skanowania aplikacji webowych Tenable.io Web Application Scanning zapewnia szybkie wykrywanie przy minimalnej liczbie wykryć pozornych, dzięki czemu użytkownik może cieszyć się dogłębnym zrozumieniem prawdziwego ryzyka cybernetycznego w kontekście aplikacji webowych.



Funkcja skanowania aplikacji webowych Tenable.io Web Application Scanning umożliwia zespołom ds. bezpieczeństwa wyświetlanie zidentyfikowanych podatności, gwarantując wgląd i ułatwiając ustalanie priorytetów dla działań naprawczych.

KLUCZOWE KORZYŚCI

- **Większa pewność podczas skanowania**
  Dostarczaj wysoce dokładne wyniki przy minimalnej liczbie wykryć pozornych i błędów, zapewniając sobie i deweloperom pewność co do trafności raportów.

- **Mniej pracy wykonywanej ręcznie**
  Zautomatyzowane skanowanie wymagające minimalnego nakładu pracy umożliwia poznanie zagrożeń dla bezpieczeństwa aplikacji webowych w ewoluującym środowisku i pozwala oszczędzić czas.

- **Usuwanie martwych punktów w zabezpieczeniach**
  Skanuj wszystkie aplikacje, w tym aplikacje kompilowane przy użyciu nowoczesnych struktur internetowych, np. środowisk JavaScript, AJAX, HTML5, z uwzględnieniem aplikacji jednostronicowych.

- **Natychmiastowa ocena zabezpieczeń**
  Ciesz się natychmiastową wartością dostarczaną przy użyciu szybkich skanów aplikacji webowych, aby odkrywać typowe problemy związane z bezpieczeństwem – skanowanie w ciągu niespełna dwóch minut.

- **Redukcja niekontrolowanego rozrostu bazy produktów**
  Zyskaj wgląd w realne zagrożenia cybernetyczne obejmujące współczesną powierzchnię ataku w ramach platformy Tenable Cyber Exposure, aby zredukować złożoność i niekontrolowany wzrost liczby produktów.

KLUCZOWE MOŻLIWOŚCI

Zrozumienie aplikacji webowych

Skanowanie Tenable.io Web Application Scanning umożliwia zrozumienie struktury i układu stron aplikacji webowych. Skanowanie przeglądowe zapewnia kluczowe, podstawowe informacje w krótkim czasie, dzięki czemu możesz lepiej zaplanować pełną ocenę.

Zaawansowane możliwości pulpitów nawigacyjnych

Pulpity nawigacyjne w funkcji Tenable.io Web Application Scanning zapewniają widoczność „na pierwszy rzut oka" w kontekście skanowanych aplikacji webowych. Wyświetlaj podatności w czasie w oparciu o poziom ryzyka, najważniejsze 10 problemów z bezpieczeństwem OWASP, a także opisy dla wszystkich podatności ze szczegółowymi instrukcjami dotyczącymi działań naprawczych dla deweloperów. Wstępnie skonfigurowane pulpity nawigacyjne z podsumowaniem dla kadry kierowniczej umożliwiają udostępnianie menedżerom szczegółów o krytycznym znaczeniu biznesowym. Pulpity nawigacyjne z możliwością dostosowania pomagają w jasnym przekazywaniu wskaźników dotyczących bezpieczeństwa aplikacji o największym znaczeniu dla zespołu.

Bezpieczne skanowanie aplikacji webowych

W celu zapobiegania opóźnieniom i zakłóceniom wpływającym na wydajność bardzo ważne jest określenie części aplikacji webowych o krytycznym znaczeniu, które można bezpiecznie skanować, oraz określenie innych części, których nigdy nie należy skanować. Z funkcją skanowania Tenable.io Web Application Scanning można wykluczać części aplikacji webowych ze skanowania poprzez podanie adresów URL lub rozszerzeń plików, aby zapewnić, że skanowanie nie będzie inwazyjne.

Zautomatyzowane skanowanie aplikacji webowych

W obliczu niedoboru profesjonalistów (i kosztów) w branży zabezpieczeń bardzo ważne jest korzystanie z rozwiązań oferujących automatyzację, co pomaga łagodzić skutki niewystarczającej ilości zasobów w zakresie bezpieczeństwa. Rozwiązanie Tenable.io Web Application Scanning umożliwia proste i szybkie ocenianie wszystkich aplikacji webowych za pomocą wysoce zautomatyzowanego rozwiązania, które redukuje konieczność pracy ręcznej.

Pokrycie nowoczesnych struktur aplikacji webowych

Starsze skanery aplikacji internetowych nie nadążają za nowoczesnymi aplikacjami, które są dziś opracowywane coraz szybciej. Skanowanie Tenable.io Web Application Scanning nie tylko może skanować tradycyjne aplikacje webowe HTML, ale też obsługuje dynamiczne aplikacje webowe tworzone na platformach HTML5, JavaScript i AJAX, z uwzględnieniem aplikacji jednostronicowych.

Natychmiastowe wykrywanie problemów z higieną cybernetyczną

Skanowanie Tenable.io Web Application Scanning zapewnia dwa wstępnie skonfigurowane szablony skanowania wykrywające typowe i potencjalnie kosztowne błędy konfiguracji aplikacji webowych. Skanowanie SSL/TLS kontroluje nieprawidłowe, wygasające lub nieprawidłowo wydane certyfikaty, które wyzwalają ostrzeżenia w przeglądarkach i wpływają na współczynnik odrzucania użytkowników. Skanowanie audytu konfiguracji kontroluje nadmiernie opisowe odpowiedzi na wywołania HTTP, które zapewniają cenne informacje dla potencjalnych hakerów. Oba skanowania są przeprowadzane w ciągu kilku minut, aby zapewniać niemal natychmiastowe rezultaty.

Skanowanie komponentów firm trzecich

Aplikacje webowe składają się w 85% z komponentów firm trzecich i komponentów open source, w tym systemów zarządzania zawartością, serwerów internetowych i silników do obsługi języka, które często zawierają niebezpieczne podatności. Skanowanie Tenable.io Web Application Scanning może identyfikować komponenty zewnętrzne w aplikacji i oceniać je pod kątem podatności, w ramach kompleksowego skanowania aplikacji webowej.

Zaawansowane wsparcie uwierzytelniania

Wiele aplikacji internetowych wdraża uwierzytelnianie, aby kontrolować dostęp do poufnych danych użytkowników, co może ograniczać możliwość oceny aplikacji przez skanery podatności. Rozwiązanie Tenable.io Web Application Scanning obsługuje szeroką gamę metod uwierzytelniania, np. uwierzytelniania opartego na formularzach, uwierzytelniania opartego na plikach cookie, obsługi NTLM, uwierzytelniania Selenium, aby spełniać większość wymagań dotyczących aplikacji webowych.

Ujednolicone skanowanie aplikacji webowych i zarządzanie podatnościami

Tenable.io Web Application Scanning zapewnia kompleksowe i dokładne skanowanie aplikacji webowych w ramach płynnego środowiska platformy Tenable Cyber Exposure, dzięki czemu zyskujesz kompleksowy wgląd w zabezpieczenia i narażenie w zakresie zgodności. Pomaga to wyeliminować silosy danych i zminimalizować niekontrolowany rozrost bazy produktów, dzięki czemu poznasz zagrożenia cybernetyczne i ochronisz organizację przy użyciu jednego rozwiązania.

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