

# WZMOCNIJ PROGRAM ZABEZPIECZEŃ DZIĘKI LOKALNEMU ZARZĄDZANIU PODATNOŚCIAMI OPARTEMU NA RYZYKU

Zobacz wszystko. Przewiduj, co będzie ważne w kontekście zasobów zarządzanych lokalnie dzięki Tenable Security Center Plus.

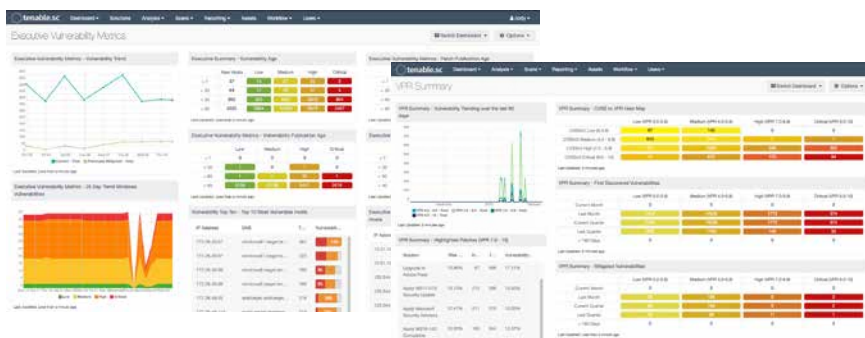
„Kompleksowe rozwiązanie Tenable umożliwia ustalanie priorytetów zagrożeń i ocenę poziomu zabezpieczeń przedsiębiorstwa na podstawie celów biznesowych w dowolnym momencie”.

– Dostawca usług z zakresu opieki zdrowotnej

Zmiana krajobrazu IT i ewolucja zagrożeń cybernetycznych sprawiły, że okresowe skanowanie i audyty zgodności są nieefektywne w kontekście ochrony przed współczesnymi cyberatakami. Aby zapewnić bezpieczeństwo organizacji, potrzebujesz rozwiązania do zarządzania podatnościami, które zapewnia kompletny przegląd powierzchni ataku, umożliwiając zarządzanie cyberzagrożeniami i ich pomiar.

Oparte na czołowej technologii Nessus rozwiązanie Tenable Security Center Plus to wiodąca na rynku platforma nowej generacji do lokalnego zarządzania podatnościami. Poprzez zaawansowaną analitykę, konfigurowalne pulpity nawigacyjne, raporty i przepływy pracy Tenable Security Center Plus pomaga doskonalić zarządzanie podatnościami i zmniejszać ryzyko organizacyjne.

Wykorzystaj predykcyjne ustalanie priorytetów łączące dane i analitykę zagrożeń z wielu źródeł, aby przewidzieć prawdopodobieństwo wykorzystania podatności, z uwzględnieniem krytycznego znaczenia dynamicznych zasobów w ciągle zmieniającym się środowisku. Rezultat? Dokładny wgląd i ustalenie priorytetów dla podatności powiązanych z najważniejszymi zasobami, by zyskać dane do podjęcia działań w celu zabezpieczenia organizacji przed naruszeniami wpływającymi na działalność biznesową.



Rysunek 1: Pulpity nawigacyjne, raporty, przepływy pracy i zasady zabezpieczeń z możliwością szczegółowej konfiguracji, dopasowane do konkretnych potrzeb biznesowych.

Tenable Security Center Plus obejmuje ponad 350 wstępnie zbudowanych, wysoce konfigurowalnych pulpity nawigacyjnych i raportów, dzięki którym zyskasz natychmiastowy wgląd w zgodność ze standardami zabezpieczeń, efektywność i zagrożenia. Możesz na bieżąco mierzyć, analizować i wizualizować efektywność programu bezpieczeństwa w oparciu o cele biznesowe wysokiego poziomu oraz fundamentalne polityki, o które dbają kadry kierownicze.

## Kluczowe korzyści

- Ciągła widoczność**  
 Śledź na bieżąco znane i odkrywaj nieznanne zasoby oraz podatności. Identyfikuj zagrożenia i nieoczekiwane zmiany sieciowe, zanim przerodzą się one w naruszenia zabezpieczeń.
- Pasywne wykrywanie podatności**  
 Wyjdź poza skanowanie punktów w czasie i wyeliminuj martwe punkty, korzystając z pasywnego wykrywania podatności zasobów, rejestrując odkrycia i dalej analizując zasoby pod kątem wykrywania zmian.
- Nadawanie priorytetów zasobom i podatnościom**  
 Połącz dane o zasobach i podatnościach, analitykę zagrożeń i naukę o danych, aby łatwiej zrozumieć oceny zagrożeń oraz szybko identyfikować podatności i najważniejsze zasoby, które stwarzają największe ryzyko dla działalności biznesowej.
- Dokładność i zakres działania**  
 Zespół Tenable Research ściśle współpracuje ze społecznością zajmującą się zabezpieczeniami, aby odkrywać nowe podatności i zapewniać analitykę, dzięki której organizacje mogą rozwijać swoje praktyki z zakresu oceny podatności. Z ponad 67 000 podatności Tenable ma najszersze w branży pokrycie CVE oraz wsparcie w konfiguracji zabezpieczeń, dzięki którym możesz lepiej zrozumieć wszystkie przypadki narażenia.
- Automatyzacja procesów**  
 Wykorzystaj w pełni udokumentowane interfejsy API i wstępnie skompilowane integracje, aby importować zewnętrzne dane, automatyzować skanowanie i udostępniać dane swoim zespołom IT.

# Kluczowe możliwości

## Zarządzanie danymi we własny sposób

Tenable Security Center Plus to czołowe rozwiązanie do lokalnego zarządzania podatnościami. Zarządzaj danymi w wybrany sposób, korzystając z wdrożenia lokalnego lub hybrydowego, zgodnego z Twoimi najbardziej złożonymi wymaganiami – a wszystko to przy jednoczesnej redukcji zagrożeń dla organizacji.

## Kompleksowe opcje oceny

Tenable Security Center Plus zapewnia ujednoczony wgląd w całą powierzchnię ataku. Platforma wykorzystuje czujniki Nessus, połączenie aktywnych skanerów, agentów, pasywnego monitorowania sieciowego i integracji CMDB, w celu maksymalizacji pokrycia skanowania w infrastrukturze, aby zredukować martwe pola podatności. Takie połączenie typów czujników danych pomaga śledzić i oceniać znane i nieznanne zasoby i podatności.

## Pasywne wykrywanie podatności

Wyjdź poza skanowanie punktów w czasie i wyeliminuj martwe punkty, korzystając z pasywnego wykrywania podatności zasobów, rejestrując odkrycia i dalej analizując zasoby pod kątem wykrywania zmian.

## Ustalanie priorytetów podatności w oparciu o faktyczne zagrożenie

Tenable Security Center Plus łączy dane dotyczące podatności, analitykę zagrożeń i naukę o danych, aby zapewniać proste zrozumienie 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 intuicyjnym raportom, wizualizacjom pulpitów nawigacyjnych i prostemu w obsłudze interfejsowi platforma Tenable Security Center Plus sprawia, że typowe zadania, takie jak konfiguracja skanowania, ocena i analiza rezultatów, są prostsze niż kiedykolwiek. Wstępnie zdefiniowane szablony skanowania, konfiguracja i kontrolne audyty zgodności zgodne z najlepszymi praktykami 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.

## Zrozumienie krytycznego znaczenia zasobów

Użyj rozwiązania do oceny znaczenia zasobów Tenable Asset Criticality Rating (ACR) w ramach platformy Tenable Security Center Plus, aby przewidywać priorytety dla zasobów w oparciu o wskaźniki znaczenia krytycznego i wartości biznesowej. Połączenie oceny znaczenia krytycznego zasobów i predykcyjnego ustalania priorytetów tworzy dostosowane podejście do zarządzania podatnościami, dzięki czemu można wykazać, które podatności i powiązane zasoby muszą uzyskać najwyższy priorytet.

**Więcej informacji:** wyślij wiadomość e-mail na adres [sales@tenable.com](mailto:sales@tenable.com) lub odwiedź [tenable.com/contact](https://tenable.com/contact)

## Integracja Tenable One

Łatwo zintegruj dane Tenable Security Center z Tenable One i rozpocznij zarządzanie narażeniem zabezpieczeń. W pełni wykorzystaj zaawansowane funkcje takie jak Lumin Exposure View, Attack Path Analysis oraz Asset Inventory, aby uzyskać ujednoczoną widoczność na całej współczesnej powierzchni ataku i proaktywnie zarządzać zagrożeniami cybernetycznymi.

## Uproszczona zgodność

Zrozumienie zasad dotyczących zgodności i składanie raportów jest łatwiejsze dzięki wstępnie zdefiniowanym kontrolom, wskaźnikom i proaktywnym alertom dotyczącym standardów branżowych i obowiązków prawnych. Normy branżowe obejmują CERT, NIST, DISA STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH i wiele więcej.

## Tenable Research

Platforma Tenable Security Center Plus 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.

## Wykorzystaj dodatek Tenable Security Center Director

Tenable Security Center Director to dodatek zapewniający centralne zarządzanie i wgląd w poziom ryzyka, którego celem jest obniżenie stopnia złożoności i uzyskanie kompletnego wglądu we wszystkie konsole w całym wdrożeniu.

## Wstępnie skompilowane integracje i udokumentowane interfejsy API oraz zintegrowane zestawy SDK

Zarządzanie podatnościami Tenable zapewnia gotowe do użycia integracje do skanowania z poświadczeniami, SIEM, SOAR, systemami zgłoszeń i dystrybucji łatek, a także inne rozwiązania uzupełniające, dzięki którym możesz uprościć proces zarządzania podatnościami. Kompletną listę można znaleźć tutaj. Ponadto możesz z łatwością utworzyć własne integracje z Tenable Security Center Plus, korzystając z w pełni udokumentowanych interfejsów API. Nie ma dodatkowego kosztu zastosowania tych narzędzi do maksymalizacji wartości konkretnych przypadków użycia zarządzania podatnościami.

## Informacje o Tenable

Tenable® to firma zajmująca się zarządzaniem narażeniem na niebezpieczeństwo. Pomaga ponad 40 000 organizacji na całym świecie zrozumieć 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 stronie [www.tenable.com](https://www.tenable.com).

