Szczegółowy Opis Przedmiotu Zamówienia

1. Przedmiot zamówienia – opis ogólny

Przedmiotem zamówienia jest:

1) **przedłużenie** licencji na oprogramowanie do zarządzania podatnościami Tenable Security Center dla 1024 aktywnych adresów IP wraz z agentami Tenable Agent, na okres 24 miesięcy,
2) **rozbudowa** posiadanej licencji o Tenable Web App Scanning do skanowania aplikacji webowych (DAST), przy jednoczesnym zachowaniu wszystkich dotychczasowych funkcji systemu.

Zamówienie obejmuje przedłużenie prawa do korzystania z oprogramowania (licencja czasowa), dostęp do aktualizacji pluginów (plugin feed) oraz wsparcie techniczne producenta na okres 24 miesięcy od 28 września 2026 r. – zarówno dla komponentów przedłużanych, jak i rozbudowywanych.

Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego, spełniającego wymagania określone w pkt 3, 4 i 5.

2. Stan obecny

Zamawiający eksploatuje centralną konsolę zarządzania podatnościami Tenable Security Center (Customer ID: 940726, typ licencji: czasowa, 1024 IP, ważna do 28 września 2026 r.) wraz ze skanerem sieciowym Tenable Nessus w wersji Professional i agentami Tenable Agent zainstalowanymi na hostach w środowisku IT. System służy do:

1) skanowania podatności w sieci (skany uwierzytelnione i nieuwierzytelnione),
2) skanowania zgodności konfiguracji z politykami bezpieczeństwa (compliance),
3) skanowania agentowego na hostach końcowych,
4) centralnego raportowania i dashboardingu,
5) integracji API z systemami zewnętrznymi (np. SIEM, CMDB, automatyczne raportowanie podatności w Jira i przypisywanie ich do konkretnych osób/zespołów w Jira – rozwijany przez Tenable addon w Jira).

3. Wymagania licencyjne

Model licencjonowania: licencja czasowa (terminowa) na okres 24 miesięcy, obejmująca prawo do korzystania z oprogramowania, dostęp do aktualizacji pluginów (plugin feed) oraz wsparcie techniczne producenta.

Zakres licencji: do 1024 aktywnych adresów IP (lub UUID w repozytoriach uniwersalnych), gdzie każdy unikalny adres IP lub UUID liczony jest pojedynczo niezależnie od liczby metod skanowania oraz liczby repozytoriów.

Komponenty objęte licencją:

1) centralna konsola zarządzania – jedna instancja,
2) skaner sieciowy w wersji rozszerzonej (klasy Tenable Nessus Expert lub równoważny) – nieograniczona liczba instancji zarządzanych przez konsolę,
3) skaner aplikacji webowych – funkcjonalność DAST w ramach skanera Expert (5 aplikacji webowych na ruchome 90-dniowe okno, z możliwością dokupienia kolejnych FQDN),
4) menedżer agentów – funkcjonalność zarządzania agentami w ramach skanera,
5) agenci on-premises – do 1024 agentów instalowanych na hostach w środowisku Zamawiającego.

Okres obowiązywania licencji: 24 miesiące od dnia 28.09.2026 r.

Uprawnienia w okresie licencji:

1) dostęp do wszystkich aktualizacji pluginów podatności publikowanych przez producenta w cyklu dobowym,
2) dostęp do aktualizacji oprogramowania – nowych wersji w ramach posiadanej linii produktowej,
3) dostęp do wsparcia technicznego producenta w zakresie opisanym w sekcji 5,
4) dostęp do bazy wiedzy, dokumentacji technicznej oraz platformy szkoleniowej producenta.

4. Wsparcie techniczne i SLA

W okresie obowiązywania licencji Zamawiający otrzymuje dostęp do wsparcia technicznego świadczonego przez producenta, obejmującego możliwość zgłaszania incydentów technicznych przez portal wsparcia, telefon oraz email.

Producent zapewnia dostępność aktualizacji pluginów podatności w cyklu dobowym, z możliwością konfiguracji harmonogramu pobierania przez Zamawiającego.

Producent zapewnia dostępność aktualizacji oprogramowania w ramach posiadanej linii produktowej.

5. Minimalne wymagania dla rozwiązania równoważnego

W przypadku zaoferowania rozwiązania równoważnego, musi ono spełniać następujące wymagania minimalne. Wymagania pogrupowano tematycznie, odpowiadając kluczowym obszarom funkcjonalnym i technicznym rozwiązania.

5.1. Architektura i wdrożenie

Rozwiązanie w pełni on-premises – całość infrastruktury (konsola centralna, skanery, menedżer agentów) funkcjonuje w siedzibie Zamawiającego, bez zależności od chmury publicznej producenta. Dopuszczalne wdrożenie na serwerze fizycznym lub maszynie wirtualnej (VMware).

System może pracować w środowisku odseparowanym od internetu (air-gapped), z możliwością manualnej aktualizacji pluginów, licencji i plików audytu z przenośnego nośnika.

System wspiera zewnętrzną relacyjną bazę danych, umożliwiającą niezależne strategie backupu i wysokiej dostępności.

5.2. Centralne zarządzanie

Centralna konsola zapewnia:

1) zarządzanie nieograniczoną liczbą skanerów sieciowych z centralną dystrybucją polityk skanowania i kodów aktywacyjnych,
2) zarządzanie skanerami aplikacji webowych jako odrębnym typem skanerów (dedykowanych do testów DAST),
3) zarządzanie pasywnymi skanerami sieciowymi (typu Network Monitor) do pasywnego wykrywania podatności,
4) obsługę pośredników komunikacyjnych (Sensor Proxies) umożliwiających łączność ze skanerami w odseparowanych segmentach sieci,
5) definiowanie stref skanowania (scan zones) do grupowania skanerów według lokalizacji lub jednostki organizacyjnej,
6) okna zamrożenia skanów (freeze windows) – blokowanie uruchamiania i wstrzymywanie trwających skanów w zdefiniowanych przedziałach czasowych,
7) tworzenie repozytoriów danych o podatnościach (IPv4, IPv6, agentowych, mobilnych, uniwersalnych, zdalnych, offline) z konfigurowalną retencją (minimum 90 dni) i automatycznym oczyszczaniem,
8) skalowanie przez dodawanie kolejnych skanerów bez dodatkowych opłat licencyjnych,
9) konsolidację danych z wielu instancji konsoli (federated/consolidated reporting) umożliwiającą agregację wyników z odseparowanych środowisk (np. air-gapped).

5.3. Zarządzanie agentami

System zapewnia:

1) rejestrację agentów łączących się z menedżerem, tworzenie grup agentów (według OS, typu zasobu, lokalizacji) i przypisywanie polityk,

2) profile agentów zapobiegające duplikacji zasobów przy współistnieniu skanów sieciowych i agentowych,
3) agent działający w przestrzeni użytkownika – bez konieczności uprawnień administratora do skanu, odpowiedni dla systemów utwardzonych (kontrolery domeny, DMZ),
4) działanie agenta na hostach okresowo odłączonych od sieci (skan lokalny, wyniki przesyłane po przywróceniu łączności),
5) rozpraszanie skanów w czasie (Scan Staggering) – rozkładanie obciążenia przez przypisywanie różnych okien skanowania do grup agentów,
6) automatyczne aktualizacje przyrostowe pluginów (differential updates) i dostosowywanie wersji do planu menedżera,
7) mechanizm samonaprawy (auto-detection i self-remediation) przy wykryciu problemów,
8) kontrolę zużycia zasobów (priorytet procesów, wydajność skanowania i kompilacji pluginów, parametry konsolidacji wyników),
9) wsparcie dla proxy z mechanizmem fallbacku,
10) instalację na Linux, Windows, macOS.

5.4. Zarządzanie zasobami IT (Assets)

System wspiera:

1) statyczne listy zasobów (wg adresów IP, nazw DNS, hostów),
2) dynamiczne listy na podstawie zapytań LDAP,
3) listy kombinowane (łączące wiele źródeł),
4) listy obserwowane (watchlist) – automatycznie aktualizowane na podstawie wyników skanowania,
5) import i eksport definicji zasobów,
6) etykietowanie zasobów (labels) do grupowania i filtrowania według klas.

5.5. Zarządzanie poświadczeniami

System zapewnia scentralizowane zarządzanie poświadczeniami:

1) dla systemów operacyjnych (SSH, Windows, Kerberos, LAPS),
2) dla baz danych (co najmniej: MS SQL Server, PostgreSQL, MySQL, MongoDB),
3) integrację z zewnętrznymi dostawcami sekretów (co najmniej: HashiCorp Vault, CyberArk, Delinea),
4) dedykowaną rolę użytkownika do zarządzania poświadczeniami bez możliwości podglądu ich treści.

5.6. Skanowanie – tryby

Skaner sieciowy zapewnia co najmniej następujące tryby:

1) Host Discovery – wykrywanie aktywnych hostów w sieci wewnętrznej (w tym wariant lekki – Ping-Only Discovery),
2) skanowanie nieuwierzytelnione – enumeracja portów, protokołów, usług,
3) skanowanie uwierzytelnione – logowanie z poświadczeniami, identyfikacja łatek, błędów konfiguracji i podatności, w tym dla środowisk VMware (ESXi, vCenter, maszyny wirtualne),
4) Credential Validation – lekki skan weryfikujący poprawność poświadczeń bez pełnego skanowania,
5) profilowanie zasobów (Target Profiling) – identyfikacja systemów operacyjnych, zainstalowanego oprogramowania i usług,
6) Malware Scan – wykrywanie złośliwego oprogramowania na systemach Windows i Unix,
7) Patch Audit – audyt zainstalowanych i brakujących aktualizacji,
8) Web Application Scan (DAST) – skanowanie aplikacji webowych,
9) Configuration Audit – skanowanie zgodności konfiguracji,
10) Cryptographic Inventory – inwentaryzacja wersji SSL/TLS, szyfrów i certyfikatów cyfrowych w środowisku,
11) Find AI – wykrywanie zainstalowanych aplikacji sztucznej inteligencji, modeli LLM i frameworków uczenia maszynowego,
12) Agent Scan – skanowanie przez agentów.

Skaner umożliwia:

1) podgląd wyników skanowania w czasie rzeczywistym, przed zakończeniem skanu,
2) porównywanie wyników dwóch skanów,
3) czasowe ukrywanie wybranych podatności na zdefiniowany okres (bez usuwania ich z bazy),
4) szczegółową konfigurację parametrów skanów: wykrywanie hostów i usług, skanowanie portów, ocena podatności (bruteforce, SCADA, aplikacje webowe, Windows, malware, bazy danych), limity czasu i wydajności, harmonogramowanie,
5) skanowanie remediacyjne – skan kontrolny weryfikujący, czy podjęte działania naprawcze usunęły zidentyfikowane podatności,
6) zapisywanie i ponowne wykorzystanie filtrów wyszukiwania,
7) automatyczne generowanie raportu po zakończeniu skanu (post-scan report) z możliwością wskazania szablonu raportu.

5.7. Polityki skanowania, pliki audytu i pluginy

System zapewnia:

1) predefiniowane szablony polityk skanowania (co najmniej: Host Discovery, Ping-Only Discovery, Basic/Advanced Network Scan, Malware, Patch Audit, Web Application Tests, Configuration Audit, Active Directory Scan, Cryptographic Inventory, Find AI, Remote Monitoring and Management),
2) predefiniowane szablony agentowe (co najmniej: Basic Agent Scan, Advanced Agent Scan, Malware Agent Scan),
3) tworzenie niestandardowych polityk z możliwością importu i eksportu,
4) dynamiczne filtry pluginów (Dynamic Plugins) – automatyczny dobór pluginów na podstawie charakterystyki skanowanych zasobów, bez konieczności ręcznej selekcji,
5) reguły pluginów (Plugin Rules) – możliwość nadpisywania krytyczności (severity) dla wskazanych pluginów,
6) zarządzanie plikami audytu zgodności – szablony producenta i niestandardowe, import i eksport,
7) audytowanie zgodności w standardzie SCAP (Security Content Automation Protocol) obejmującym OVAL, CVE, CVSS, CPE,
8) możliwość tworzenia i wgrywania niestandardowych pakietów pluginów (w natywnym formacie skryptowym systemu),
9) harmonogram automatycznych aktualizacji pluginów z możliwością edycji.

5.8. Dashboardy, raporty i analityka

System zapewnia:

1) dashboardy szablonowe (co najmniej: Executive Summary, Compliance Summary, Health Overview) i niestandardowe z komponentami: macierze, tabele, wykresy,
2) raporty szablonowe i niestandardowe z rozdziałami (chapters), elementami grupowymi, tekstowymi, macierzowymi, tabelarycznymi i wykresami; dystrybucja email i publikacja,
3) publikację raportów i dashboardów do witryn umożliwiających dostęp dla interesariuszy bez konieczności posiadania konta w systemie,
4) karty raportowe zgodności – mierzalne wskaźniki poziomu zgodności z politykami i standardami, umożliwiające ocenę w skali punktowej/procentowej,
5) scoring podatności wg CVSS (v2, v3, v4) z możliwością wyboru wersji jako domyślnej dla systemu oraz indywidualnie dla skanu,

6) scoring ryzyka wykraczający poza CVSS – uwzględniający m.in. historię podatności, dostępność exploita, źródła threat intelligence oraz krytyczność zasobu, z możliwością prezentacji czynników, które miały największy wpływ na ocenę,
7) scoring EPSS (Exploit Prediction Scoring System) – prawdopodobieństwo wykorzystania podatności w ciągu najbliższych 30 dni,
8) wyszukiwanie podatności po CVE,
9) budowanie zapytań analitycznych z filtrami na danych o podatnościach i zasobach,
10) zapisywanie i ponowne wykorzystanie zapytań.

5.9. Użytkownicy, role i uwierzytelnianie

System zapewnia:

1) co najmniej następujące wbudowane role: Administrator, Security Manager, Auditor, Credential Manager, Executive, Security Analyst, Vulnerability Analyst,
2) możliwość tworzenia niestandardowych ról z granularnymi uprawnieniami (co najmniej w zakresie: skanowania, zasobów, analizy ryzyka, workflow, aktualizacji pluginów, zarządzania użytkownikami),
3) integrację z LDAP (w tym obsługa wielu OU i automatyczny provisioning użytkowników),
4) integrację z SAML (co najmniej: Keycloak, Microsoft ADFS) lub OIDC,
5) uwierzytelnianie certyfikatami SSL klienta,
6) uwierzytelnianie kluczami API z możliwością zarządzania (generowanie, usuwanie, włączanie/wyłączanie)

5.10. Organizacje i grupy

System wspiera architekturę wielodostępną:

1) wiele organizacji, każda z przypisanymi repozytoriami,
2) grupy w ramach organizacji z granularnymi uprawnieniami na poziomie obiektów – osobna kontrola uprawnień do: użytkowników, grup, raportów, wyników raportów, rezultatów skanów, polityk, zasobów, alertów, plików audytu, poświadczeń, zgłoszeń biletowych, reguł ryzyka, zapytań, dashboardów, kart zgodności,
3) udostępnianie obiektów między grupami z możliwością selektywnego nadawania uprawnień (np. podgląd dashboardów innej grupy bez prawa edycji).

5.11. Workflow i reagowanie

System zapewnia:

1) alerty konfigurowalne – wyzwalanie skanów, generowanie raportów, wysyłanie emaili,

2) reguły akceptacji ryzyka – ukrywanie określonych podatności z widoków,
3) reguły przeklasyfikowania ryzyka – zmiana poziomu krytyczności,
4) integrację z systemami biletowymi – tworzenie, edycja, zamykanie zgłoszeń.

5.12. API

System udostępnia API REST umożliwiające programowe zarządzanie co najmniej:

1) zasobami (tworzenie, odczyt, aktualizacja, eksport, import),
2) skanami (tworzenie, uruchamianie, odczyt wyników – skany aktywne i agentowe),
3) agentami (grupy, wyniki, synchronizacja),
4) workflow (alerty, reguły ryzyka, zgłoszenia),
5) analityką (zapytania, pobieranie i eksport wyników – typy: podatności, zdarzenia, użytkownicy, urządzenia mobilne),
6) użytkownikami, rolami, organizacjami, kluczami API,
7) konfiguracją systemu (ustawienia, licencje, pluginy, harmonogramy),
8) zadaniami i kolejką zadań (job queue),
9) operacjami zbiorczymi (bulk operations),
10) uwierzytelnianiem przez klucze API.

5.13. Backup, monitorowanie i bezpieczeństwo systemu

System zapewnia:

1) automatyczne i manualne kopie zapasowe konfiguracji oraz pełne kopie zapasowe (konfiguracja + dane), z możliwością przywracania,
2) dashboard stanu systemu (Health Overview) pokazujący kondycję i status licencji,
3) podgląd kolejki zadań i logów systemowych z możliwością pobierania,
4) generowanie plików diagnostycznych,
5) logi debugowania z możliwością włączania/wyłączania i pobierania,
6) integrację z zewnętrznym syslogiem,
7) powiadomienia email (SMTP),
8) konfigurowalne okresy przechowywania danych (data expiration) – osobno dla wyników skanów, zamkniętych zgłoszeń biletowych i danych o podatnościach,
9) konfigurowalne harmonogramy zewnętrzne (external schedules) – definiowanie interwałów pobierania danych z zewnętrznych źródeł,
10) wsparcie dla SELinux w trybie enforcing,
11) zgodność ze standardem FIPS 140-2 dla modułów kryptograficznych,
12) rejestrowanie ścieżki audytu skanów (audit trail).

5.14. Kompatybilność ze środowiskiem Zamawiającego

Rozwiązanie równoważne musi być kompatybilne z istniejącym środowiskiem:

1) możliwość importu historycznych danych skanów z obecnego rozwiązania lub zapewnienie mechanizmu zachowania ciągłości analizy trendów podatności,
2) integracja z systemami Zamawiającego: SIEM (przez syslog/api), system zgłoszeniowy Jira (przez API – dedykowana aplikacja do automatycznego zgłaszania podatności i przypisywania ich do konkretnych osób/zespołów).