Załącznik nr 1 do Zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: rozbudowa systemu do automatycznych testów podatności oraz monitorowania i ochrony Active Directory/Entra ID, poprzez dostawę nowych licencji wraz z instalacją, konfiguracją, gwarancją, wsparciem serwisowym i rozwojowym Wykonawcy.

1. **Przedmiot zamówienia obejmuje:**

a) Zamówienie gwarantowane - rozbudowa Systemu, poprzez zakup dodatkowych licencji Tenable lub instalacja i konfiguracja zaproponowanego rozwiązania oraz dostarczenie licencji równoważnych z instruktażem, spełniających wymagania wskazane w Załączniku nr 1 do OPZ, wraz z gwarancją i wsparciem świadczonym przez okres 24 miesięcy, wsparciem serwisowym i rozwojowym Wykonawcy (w przypadku dostarczenia licencji innych niż posiadane przez Zamawiającego równoważność jest opisana w Załączniku nr 1)

Lp.	Nazwa licencji	Liczba licencji	Gwarancja	Wsparcie serwisowe i rozwojowe Wykonawcy
1.	Tenable.sc+ - Perpetual License (TSCCV-P)	10000 szt.	24 miesiące	24 miesiące (on-premise)
2.	Tenable.sc+ - Maintenance Annual (TSCCV-M)	10000 szt.	24 miesiące	24 miesiące (on-premise)
3.	Tenable Identity Exposure (TAD-OP)	7000 szt.	24 miesiące	24 miesiące (on-premise)
4.	Wsparcie serwisowe i rozwojowe Wykonawcy – do wykorzystania w okresie obowiązywania umowy	280 roboczogodzin	Nie dotyczy	Tak

b) Zamówienie opcjonalne - dostawa licencji lub równoważne oraz wsparcia:

Lp.	Nazwa licencji	Liczba licencji	Gwarancja	Wsparcie serwisowe i techniczne Wykonawcy
1.	Tenable.sc+ - Perpetual License (TSCCV-P)	4000 szt.	24 miesiące	24 miesiące (on-premise)
2.	Tenable.sc+ - Maintenance Annual (TSCCV-M)	4000 szt.	24 miesiące	24 miesiące (on-premise)

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

Lp.	Nazwa licencji	Liczba licencji	Gwarancja	Wsparcie serwisowe i techniczne Wykonawcy
3.	Tenable Identity Exposure (TAD-OP)	4000 szt.	24 miesiące	24 miesiące (on-premise)
4.	Wsparcie serwisowe i rozwojowe Wykonawcy – – do wykorzystania w okresie obowiązywania umowy w ramach prawa opcji	140 roboczogodzin	Nie dotyczy	Nie dotyczy

2. Termin realizacji:

1. Dostawa zamówienia gwarantowanego, o którym mowa w pkt 1 lit. a) musi nastąpić w terminie do 10 dni licząc od daty podpisania umowy, jednak nie wcześniej niż w terminie 30.11.2026 r.
2. W przypadku zamówienia opcjonalnego, którego zakres opisano w pkt 1 lit. b) dostawa musi nastąpić w terminie do 10 dni od dnia dostarczenia Wykonawcy Zlecenia Opcji, o którym mowa w Umowie.
3. Zamawiający jest uprawniony do skorzystania z prawa opcji w całości lub w części, według bieżących potrzeb, w kilku odrębnych etapach, bez obowiązku wykorzystania pełnego zakresu opcji.
4. Prawo opcji może być realizowane w okresie 24 miesięcy od dnia podpisania protokołu odbioru licencji, przy czym Zamawiający przewiduje możliwość skorzystania z opcji:

4.1. przez pierwsze 12 miesięcy obowiązywania umowy– do 2000 licencji,

4.2. w kolejnych miesiącach obowiązywania umowy– do 2000 licencji,

5. Wykonawca udostępni lub przekaże Zamawiającemu klucze licencyjne (aktywacyjne) na nośniku CD/DVD lub udostępni drogą elektroniczną, np. mailem lub poprzez dostęp do strony internetowej zawierającej dane Oprogramowanie.
6. Gwarancja będzie świadczona przez okres 24 miesięcy od dnia podpisania Protokołu odbioru.
7. Wsparcie serwisowe i rozwojowe Wykonawcy będzie świadczone:

7.1. W ramach zamówienia podstawowego: od dnia podpisania Protokołu odbioru;

7.2. W ramach realizacji prawa opcji: przez okres 24 miesięcy od dnia podpisania Protokołu odbioru;

8. Po dostarczeniu licencji, o których mowa w pkt 1 lit. a) lub równoważnych, Wykonawca zainstaluje i skonfiguruje oprogramowanie w środowisku Zamawiającego.
9. W przypadku zaproponowania rozwiązania równoważnego, w momencie składania oferty Wykonawca przekaże Zamawiającemu szczegółowe informacje, w których znajdą się wymagania niezbędne do przygotowania instalacji i wdrożenia systemów u Zamawiającego, o których mowa w punkcie powyżej.
10. Ponadto w przypadku zaproponowania rozwiązania równoważnego, Wykonawca dostarczy i kompleksowo skonfiguruje środowisko do skanowania i zarządzania podatnościami oraz ochrony AD

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

mając na uwadze Przedmiot zamówienia wskazany w pkt. 1 a), zamówienia opcjonalne (pkt 1 b) oraz uwzględni obecnie użytkowane licencje i obecne środowisko wskazane w pkt. 3 OPZ.

3. Skanery Tenable wykorzystywane obecnie przez Zamawiającego:

1. W kontekście rozbudowy obecnego przedmiotu zamówienia Zamawiający użytkuje licencje **Tenable** wymienione poniżej:

Lp.	Nazwa licencji	Liczba licencji	Data wygaśnięcia posiadanej obecnie gwarancji producenta /licencji
1.	Tenable.sc+ - Maintenance Annual (TSCCV-M)	4400 szt.	2028-11-30
2.	Tenable.sc+ - Perpetual License (TSCCV-P)	4400 szt.	2028-11-30
3.	Tenable Identity Exposure TIE (TAD-OP)	5000 szt.	2028-11-30
4.	Standard Tenable.sc+ Console (TSCCV-STNDC-M)	1 szt.	2028-11-30

2. W ramach ww. licencji Zamawiający posiada rozbudowaną infrastrukturę skanerów podatności (16 skanerów Tenable/Nessus połączonych do jednej konsoli zarządzania Tenable sc+ oraz 7 sensorów TIE Secure Relays obejmujących 12 domen AD – również połączonych z jedną konsolą zarządzającą TIE) umiejscowionych i skonfigurowanych w poszczególnych obszarach sieci Zamawiającego. W kontekście planowanej rozbudowy rozwiązania Zamawiający planuje objęcie skanami dodatkowe obszary i systemy oraz domeny (w tym Entra ID).

4. Gwarancja oraz wsparcie serwisowe i techniczne Wykonawcy dla zakresu opisanego w pkt 1 lit. a) i b):

4.1. W ramach 24 miesięcznej gwarancji wymagany jest:

4.1.1. dostęp do aktualizacji oprogramowania;

4.1.2. dostęp do nowych wersji oprogramowania oraz poprawek;

4.1.3. dostęp do nowych sygnatur bezpieczeństwa, baz podatności i pluginów;

4.1.4. dostęp do bazy wiedzy producenta;

4.1.5. wsparcie świadczone w trybie: 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, bez ograniczenia liczby zgłoszeń;

4.1.6. dostęp do portalu pomocy technicznej producenta oprogramowania przez 24 godziny na dobę w celu:

4.1.6.1. przeglądania i składania informacji o problemach dotyczących przedmiotu zamówienia;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.1.6.2. informacji o nowych produktach;

4.1.6.3. dostępu do bazy wiedzy do oprogramowania będącego przedmiotem zamówienia;

4.1.6.4. informacji o dostępnych poprawkach do oprogramowania.

4.1.6.5. wysyłanie zgłoszeń serwisowych do producenta oprogramowania z poziomu portalu użytkownika, służącego również do zarządzania kluczami licencyjnymi oraz potwierdzenia poziomu posiadanego wsparcia u przez Zamawiającego w ramach niniejszego zamówienia.

4.2. Zamawiający będzie mógł dokonywać aktualizacji oprogramowania do najnowszej zalecanej przez producenta wersji przez cały okres obowiązywania gwarancji.

4.3. W trakcie 24 miesięcznej gwarancji Wykonawca będzie świadczył wsparcie serwisowe oraz usługi rozwojowe w następujących zakresie:

4.3.1. Stałą telefoniczną i mailową pomoc dla Administratorów i operatorów Systemu.

4.3.2. Usuwanie Błędów w oprogramowaniu, w tym wsparcie w procesie debugowania.

4.3.3. Aktualizację Systemu lub wsparcie w procesie aktualizacji.

4.3.4. Okresowe przeglądy Systemu (raz na 12 miesięcy) na życzenie Zamawiającego.

4.3.5. Proponowanie zmian w konfiguracji Systemów w zakresie dobrych praktyk i ciągłego doskonalenia rozwiązania w środowisku Zamawiającego.

4.3.6. Konfigurację i rozbudowę Systemów w środowisku Zamawiającego zgodnie z jego potrzebami w oparciu o licencje wskazane w pkt 1 lit. a) i b) w ramach zakontraktowanych godzin rozwojowych. Zamawiający przewiduje wykorzystanie części godzin rozwojowych na integrację Tenable sc+ i Tenable Identity Exposure z użytkowanymi systemami Jira Service Management i Jira Software (użytkowanych on-premise licencja Data Center).

4.4. W trakcie 24 miesięcznej umowy Zamawiający przewiduje możliwość skorzystania z godzin rozwojowych pracy inżyniera Wykonawcy w liczbie do 280 godzin zegarowych w ramach zamówienia podstawowego oraz w ramach prawa opcji do 140 godzin.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Załącznik nr 1 do OPZ

Opis wymagań dla oprogramowania równoważnego do Tenable sc+

Zamawiający posiada licencje na oprogramowanie Tenable sc+.
Jeżeli Zamawiający określił w Opisie przedmiotu zamówienia wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

I. Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego do oprogramowania Tenable:

1. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Opisie przedmiotu zamówienia, w szczególności w zakresie:
   a) warunków licencji/sublicencji w każdym aspekcie licencjonowania/sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania Tenable,
   b) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania Tenable”,
   c) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Tenable funkcjonującym u Zamawiającego,
   d) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
   e) poszczególne składowe oprogramowania równoważnego współpracują ze sobą w sposób nie gorszy niż oprogramowania wskazanego w zamówieniu,
   f) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
   g) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem.
2. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.

4. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
5. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

II. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

1. Zbudować środowisko równoważne w stosunku do obecnie funkcjonującego systemu po stronie Zamawiającego. Wymaganiem koniecznym jest zapewnienie wysokiego poziomu bezpieczeństwa systemów objętych skanami/testami realizowanymi z wykorzystaniem rozwiązania równoważnego.
2. Zainstalować i kompleksowo skonfigurować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu typu skaner podatności (Vulnerability Scanner) oraz zintegrować się z systemami/aplikacjami wytwarzanymi w ramach działalności Zamawiającego w terminie do 10 dni roboczych od dnia podpisania umowy. W ramach potwierdzenia poprawnego wykonania konfiguracji, Wykonawca wykona próbny skan i wygeneruje raport ze skanów.
3. Dostarczyć wszystkie niezbędne licencje na oprogramowanie równoważne (ze wsparciem na 24 miesiące na oprogramowanie - również firm trzecich) wymagane do wdrożenia i uruchomienia systemu.

4. Przeprowadzić Instruktaż stanowiskowy. Wykonawca przeprowadzi Instruktaż stanowiskowy dla minimum 4 osób wskazanych przez Zamawiającego.

    4.1. W instruktażu mogą uczestniczyć dodatkowe osoby wskazane przez Zamawiającego, lecz nie więcej niż 8 osób.

    4.2. Instruktaż będzie przeprowadzony przez certyfikowanego przez producenta instruktora.

    4.3. W przypadku zaproponowania rozwiązania równoważnego do opisywanego Systemu, Wykonawca przeprowadzi kompleksowy instruktaż równoważnego systemu.

    4.4. Instruktaż będzie realizowany w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej.

    4.5. Instruktaż będzie trwał minimum 2 Dni Robocze każdy (minimum 14 godzin zegarowych każdy).

    4.6. Jeśli Wykonawca wykaże, że zakres instruktażu wykracza poza liczbę dni wskazaną w pkt. 4.5 (np. z uwagi na złożoność zaproponowanego Systemu) określi on liczbę oraz zakres

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

instruktaży niezbędnych do pozyskania wiedzy niezbędnej do administrowania Systemem i w zakresie operatorskim. Wymagana jest wtedy akceptacja zakresu oraz liczby zaproponowanych przez Wykonawcę instruktaży przez upoważnionego przedstawiciela Zamawiającego.

4.7. Instruktaż dla administratorów i operatorów będzie obejmować wszelkie możliwe zagadnienia przydatne w codziennej pracy, a w szczególności:

4.7.1. Szczegółowe omówienie Systemu i jego funkcjonalności, w tym omówienie architektury Systemu i procesu przetwarzania danych w Systemie.

4.7.2. Tworzenie polityk, skanów, reguł wbudowanych w System oraz zdefiniowanych przez użytkownika.

4.7.3. Ćwiczenia praktyczne z budowania reguł, polityk, skanów, raportów, dashboardów.

4.7.4. Zarządzanie konfiguracją i bezpieczeństwem w Systemie.

4.7.5. Omówienie procesów instalacji, konfiguracji, aktualizacji Systemu, tworzenia kopii bezpieczeństwa oraz przywracania w przypadku awarii.

4.7.6. Omówienie procedur eksploatacyjnych.

4.7.7. Omówienie dobrych praktyk oraz możliwości integracji z innymi rozwiązaniami.

4.8. Zamawiający dopuszcza przeprowadzenie Instruktażu online lub w siedzibie Zamawiającego i decyzję przekaże Wykonawcy na etapie realizacji zamówienia. Na potrzeby Instruktażu Zamawiający zapewni sale, stacje robocze oraz pozostałą infrastrukturę (rzutnik, sieć, itp.).

4.9. Ponadto w ramach /instruktażu Wykonawca dostarczy:

4.9.1. szczegółową dokumentację producenta Systemu.

4.9.2. Inne materiały (instrukcje, video) niezbędne do pracy w Systemie dla Użytkowników.

4.9.3. wszystkie ww. materiały do przeprowadzenia instruktaży stanowiskowych i niezbędne w bieżącej pracy z Systemem będą przygotowane w języku polskim lub angielskim.

5. **Plan przeprowadzenia Instruktaży stanowiskowych**. Wykonawca przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu, w szczególności:

5.1. zakres Instruktażu (w szczególności: zajęcia praktyczne dla administratorów, operatorów).

5.2. szczegółowe określenie tematów Instruktażu,

5.3. proponowany harmonogram.

5.4. Dokument opisujący aspekty związane z Instruktażem stanowiskowym zostanie przekazany w terminie 2 dni roboczych od dnia zawarcia umowy.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

6. Wykonać analizę przedwdrożeniową środowiska Zamawiającego oraz dostarczyć projekt techniczny systemu równoważonego, obejmującego specyfikację techniczną określającą wymogi na infrastrukturę teleinformatyczną / środowisko wirtualne dla systemu, m.in:
    a) szczegółową specyfikację sprzętową serwerów/urządzeń sieciowych,
    b) ilość maszyn wirtualnych, procesorów wirtualnych, pamięci RAM, przestrzeni dyskowej,
    c) wymagane parametry łącza i przepływy sieciowe niezbędne do prawidłowej komunikacji systemu równoważnego zgodnie z wymaganiami Systemu,
    d) wymagane parametry systemu operacyjnego,
    e) wymagania wirtualizacji (platforma VMware).

    oraz szczegółowy opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do wdrożenia i konfiguracji Systemu równoważnego.
7. Przeprowadzić proces konfiguracji oprogramowania równoważnego z uwzględnieniem wskazanych przez Zamawiającego zasobów oraz podsieci, dokonać poprawnej konfiguracji mechanizmów komunikacji skanerów, sensorów, konsoli i innych komponentów systemu niezbędnych do prawidłowego i kompleksowego działania zaproponowanego rozwiązania równoważnego.
8. Wykonać dokumentację powykonawczą systemu równoważnego zgodnie z wymogami Zamawiającego, zawierającą m. in. informacje o szczegółach wykonanych prac wdrożeniowych, instrukcje instalacji, konfiguracji i użytkowania wdrożonego oprogramowania równoważnego, w tym dostarczy instrukcje stanowiskowe dla administratorów i operatorów.

III. Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania Tenable:

1. Rozwiązania równoważne dla skanera podatności (Vulnerability Scanner) (zwanego dalej „System") wraz z niezbędnymi licencjami:
    1.1. Dostarczenie i pełne skonfigurowanie Systemu w modelu „on premise" (czyli zainstalowanie na infrastrukturze Zamawiającego), funkcjonalność zarządzania wykrytymi podatnościami może być realizowana z pomocą dodatkowego panelu zarządzania.
2. W szczególności System równoważny dla skanera podatności obejmuje:
    2.1. Dostarczenie niezbędnych licencji wieczystych typu virtual appliance lub software appliance dla skanera podatności infrastruktury. Licencje z minimum 24 miesięcznym wsparciem zapewniającym aktualizacje dla Systemu.
    2.2. Dostarczenie najnowszej wersji Systemu na dzień składania oferty.
    2.3. Świadczenie usług gwarancyjnych oraz wsparcia serwisowego i rozwojowego Wykonawcy przez okres, o którym mowa w rozdz. I pkt 1 lit. a) i b).
    2.4. Środowisko Zamawiającego składa się z następujących stacji końcowych i aplikacji:

    2.4.1 Liczba hostów o unikalnych adresach IP wymagająca skanów podatności – ok. 14400 sztuk (oraz zgodnie z OPZ może być rozbudowane o dodatkowe 4000 szt. w trakcie trwania umowy), w tym:
        a) stacje robocze oparte o system operacyjny z rodziny MS Windows oraz Mac OS,
        b) serwery rodziny Windows Server oraz Linux w tym m.in. dystrybucji RHEL, CentOS,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

2.4.2 Zamawiający posiada rozbudowaną infrastrukturę skanerów podatności i umiejscowionych w poszczególnych obszarach sieci Zamawiającego. W przypadku zaoferowania rozwiązania równoważnego Wykonawca również dostosuje i skonfiguruje środowisko skanerów w poszczególnych obszarach sieci.

3. Wymagania minimalne dla Systemu typu skaner podatności:

3.1 Architektura Systemu.

3.1.1 W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.

3.1.2 Jeżeli System będzie instalowany jako System na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2012+, CentOS, RHEL.

3.1.3 Jeżeli System będzie dostępny przez interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersjach na dzień składania oferty.

3.1.4 Agent Systemu dla stacji końcowej powinien działać na systemach operacyjnych obsługiwanych przez Zamawiającego (Windows 10, 11, Microsoft Server 2012 i nowszych, macOS oraz Linux (RHEL/CentOS/Debian).

3.1.5 System musi dawać możliwość skanowania urządzeń końcowych działających na różnych systemach operacyjnych oraz znajdujących się w różnych podsieciach również bezagentowo.

3.1.6 System (zarówno silnik, jak i konsola) powinien dawać możliwość wdrożenia, jako:

3.1.7 Aplikacja, tj. System instalowany na systemie operacyjnym skanowanego hosta – agent; maszyna wirtualna.

3.1.8 System musi opcjonalnie, w określonych okolicznościach, dawać możliwość zainicjowania skanowania z poziomu: serwera (instalacja stand – alone), aplikacji dowolnego silnika skanującego (skanera), linii poleceń systemu, w którym jest zainstalowany skaner.

3.1.9 System powinien obsługiwać automatyczny/zaplanowany transfer logów z konsoli w celu archiwizacji.

3.1.10 Elementy zarządzające i analityczne Systemu nie mogą być ograniczone liczbą skanerów sieciowych w różnych podsieciach, liczbą hostów w podsieci czy liczbą możliwych do skanowania podsieci.

3.1.11 Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Internetem.

3.1.12 W przypadku braku dostępu do Internetu System zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.

3.1.13 W przypadku dostępu do Internetu System ma umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania Systemem.

3.1.14 System musi oferować możliwość skonfigurowania w trybie wysokiej dostępności (dostępność 24x7x365) chroniąc rozwiązanie przed awarią sprzętową, awariami pojedynczych komponentów Systemu lub błędami aplikacji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.1.15 W przypadku użycia w Systemie rozwiązań licencyjnych Zamawiający oczekuje, aby Wykonawca zadeklarował możliwość dostarczenia licencji tymczasowej na czas przesunięć w procesie zakupowym.

3.2 Zarządzanie Systemem.

3.2.1 System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.

3.2.2 Dostęp do systemu możliwy jedynie po uwierzytelnieniu użytkownika w systemie.

3.2.3 Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej.

3.2.4 System musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.

3.2.5 System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator systemu itp.) lub poprzez możliwość przypisania określonych operacji do zdefiniowanych ról.

3.2.6 System musi zapewniać segregację obowiązków poprzez umożliwianie dostępu danemu użytkownikowi tylko do wybranych zasobów.

3.2.7 System powinien się integrować z Active Directory w zakresie uwierzytelnienia do Systemu oraz kontroli dostępu na bazie zdefiniowanych ról. Dopuszcza się rozwiązanie używające wewnętrznego mechanizmu uwierzytelniania do Systemu.

3.2.8 System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.

3.2.9 System musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli. Dashboard powinien umożliwiać schodzenie do szczegółów w poszczególnych elementów z poziomu informacji podstawowych.

3.3 System centralnego zarządzania musi zapewnić możliwość:

3.3.1 przechowywania wszystkich danych pochodzących z dowolnego silnika skanującego i testującego,

3.3.2 przeglądanie tych danych w sposób przejrzysty dla użytkownika, co najmniej w postaci Top 10 podatności, Top 10 systemów zainfekowanych, możliwość filtrowania wykrytych podatności, m.in. po CVE, hostach,

3.3.3 tworzenie raportów dostępnych w systemie centralnego zarządzania oraz wysyłanych na wskazane adresy email,

3.3.4 monitorowania stanu pracy skanerów, co najmniej przez: okresową weryfikację czy skanery są uruchomione, stan pracy skanera,

3.3.5 prezentacji informacji o podatnościach wykrytych przez skanery pasywne,

3.3.6 prezentacji wyników skanowania otrzymanych ze skanerów aktywnych,

3.3.7 prezentacji informacji o podatnościach w połączeniu z wynikami skanowania ze skanerów aktywnych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.3.8 Szyfrowaną komunikację między serwerem zarządzającym a agentem zainstalowanym na stacji roboczej/serwerem.

3.4 Funkcjonalności Systemu.

3.4.1 Intuicyjny interfejs graficzny (GUI): Oprogramowanie musi zapewniać graficzny interfejs użytkownika umożliwiający łatwą obsługę narzędzi i funkcji. GUI powinno wspierać zarządzanie projektami, przeprowadzanie testów, analizę wyników oraz generowanie raportów w sposób przejrzysty i intuicyjny.

3.4.2 System musi zapewniać możliwość harmonogramowania (planowania w czasie) oraz jednoczesnego uruchomienia na wybranych lub wszystkich skanerach zainstalowanych na stacjach roboczych i serwerach podłączonych do systemu centralnego zarządzania. W tym również w sytuacji, gdy stacja robocza/serwer/skaner na stacji lub serwerze nie jest uruchomiony/-a (uruchomienie jest inicjowane przez system centralnego zarządzania).

3.4.3 Rozwiązanie musi zapewnić silne uwierzytelnianie tak aby bezpiecznie przesyłać poświadczenia w skanowaniu z uwierzytelnianiem.

3.4.4 System musi mieć możliwość wykonywania ręcznego i zaplanowanego skanowania określonych hostów lub podsieci.

3.4.5 Wszystkie dane zebrane przez zewnętrzne silniki skanujące i testujące muszą być przesyłane niezwłocznie do centralnej bazy i nie mogą być przechowywane przez skaner lokalnie.

3.4.6 Skanery aktywne podłączone do systemu centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz za pomocą uwierzytelnienia do systemu skanowanego,

3.4.7 Rozwiązanie powinno zapewnić możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod podczas skanowania z serwera:

3.4.7.1 Hasło;

3.4.7.2 Klucz SSH;

3.4.7.3 Kerberos, w tym integracja z Microsoft AD oraz Azure AD opcjonalnie możliwość zapewnienia użycia logowania wieloskładnikowego (MFA).

3.4.8 Skaner pasywny musi posiadać również swój własny interfejs webowy, w którym prezentuje aktualny stan pracy, między innymi informacje o połączeniach między systemami klienckimi a serwerami, IP stacji roboczych/serwerów, stan połączenia z centralnym systemem zarządzania, podgląd logu pracy.

3.4.9 Skaner pasywny musi umożliwiać zdefiniowanie adresów IP stacji roboczych/serwerów/sieci, które będą podlegać monitorowaniu.

3.4.10 Skaner pasywny musi wykrywać nowo pojawiające się stacje robocze/serwery w monitorowanej sieci i informować o tym system centralnego zarządzania.

3.4.11 Skaner pasywny musi zapewnić monitorowanie sieci lokalnej przez 24 godziny i 7 dni w tygodniu, z minimalnym czasem pracy 95% w skali roku, co najmniej w zakresie wykrywania zagrożeń, anomalii w sieci.

3.5 Automatyzacja procesów, powinna obejmować co najmniej:

3.5.1 skanowanie o zaplanowanym czasie;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.5.2 powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. syslog, SMTP, uruchom skan, wygeneruj raport);

3.5.3 możliwość tworzenia okien czasowych, w których skanowanie aktywne nie może rozpocząć się dla określonych przez administratora systemów;

3.5.4 Wszystkie testy i skany, które mogą wpłynąć na stabilność działania sprawdzanego hosta, powinny być oznaczone w jasny sposób dla administratora.

3.5.5 System musi umożliwiać automatyczne przeprowadzanie retestów luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.

3.5.6 Wykryte podatności powinny posiadać odnośniki do otwartych baz podatności, takich jak:

3.5.6.1 Bugtraq.

3.5.6.2 MSFT.

3.5.6.3 CVE.

3.5.6.4 BID.

3.5.6.5 OSVDB ID.

3.5.7 System musi mieć możliwość tworzenia grup dla danych wynikowych.

3.5.8 System centralnego zarządzania musi dostarczać wzorce polityk skanowania jak również możliwość zbudowania polityki skanowania od podstaw.

3.5.9 W ramach budowy polityki skanowania system musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE.

3.5.10 Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak:

3.5.10.1 Adres IP.

3.5.10.2 Poziom niebezpieczeństwa.

3.5.10.3 CVE ID.

3.5.10.4 CVSS Score w wersji 2 i nowszych.

3.5.10.5 CVSS Vector w wersji 2 i nowszych.

3.5.10.6 Dostępny exploit.

3.5.10.7 Narzędzi do wykonania ataku (w systemie musi być wskazana informacja o dostępnych exploitach przynajmniej z trzech narzędzi, np. Metasploit, Core Impact, Canvas).

3.5.10.8 Data opublikowania patchy dla danej podatności.

3.5.10.9 Port/Protokół.

3.5.10.10 Data opublikowania podatności.

3.5.10.11 Data zauważenia po raz pierwszy podatności dla systemu.

3.5.10.12 Data, kiedy ostatni raz widziana była podatność dla systemu.

3.5.10.13 Przydział do określonej grupy systemów.

3.5.10.14 CCE ID.

3.5.10.15 MS Bulletin ID.

3.5.11 System musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności (np. od 0 do 10) na podstawie własnego modelu uczenia maszynowego.

3.5.12 Administrator musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością dla konkretnego systemu, portu, protokołu.

3.5.13 System musi prezentować wyniki skanowania co najmniej za pomocą widoków:

3.5.13.1 Sumarycznie po IP.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.5.13.2 Sumarycznie po portach.
3.5.13.3 Sumarycznie po grupach systemów.
3.5.13.4 Sumarycznie po CCE.
3.5.13.5 Sumarycznie po CVE.
3.5.13.6 Sumarycznie po MS Bulletin ID.
3.5.13.7 Sumarycznie po protokołach.
3.5.13.8 Sumarycznie po systemach operacyjnych.

3.5.14 System musi umożliwiać tworzenie grup systemów spełniających określone warunki. Grupy systemów mogą być tworzone dynamicznie i/lub statycznie. Tworzenie grup powinno być możliwe w oparciu o co najmniej następujące parametry:
3.5.14.1 System operacyjny.
3.5.14.2 MAC adres.
3.5.14.3 IP adres.
3.5.14.4 Porty TCP i UDP.
3.5.14.5 Ilość dni od wykrycia konkretnej podatności.
3.5.14.6 Czy exploit jest dostępny.
3.5.14.7 Czy istnieje exploit w systemach między innymi Metasploit, Core Impact, Canvas.

3.5.15 Tworzenie nowych grup systemów musi odbywać się również na podstawie wyrażeń logicznych takich jak AND, OR, NOT pomiędzy istniejącymi grupami systemów.

3.5.16 Raportowanie musi być integralną częścią systemu centralnego zarządzania.

3.5.17 System musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować.

3.5.18 System musi pozwalać na budowanie raportu od podstaw używając do tego co najmniej elementów takich jak: rozdziały, iteracja wyników, linie trendów, wykresy kołowe, wykresy słupkowe, tabele, macierze, sekcje tekstów.

3.5.19 System musi umożliwiać generowane raportów co najmniej w następujących formatach: PDF, CSV.

3.5.20 System musi pozwalać na dodanie znaku wodnego podczas generowania raportu.

3.5.21 System musi mieć możliwość generowana raportów według harmonogramu oraz na żądanie.

3.5.22 System musi mieć możliwość automatycznego wysyłania raportów do wskazanych osób na maila.

3.5.23 System musi mieć możliwość wyboru systemów do skanowania w oparciu o przynajmniej następujące możliwości:
3.5.23.1 Podanie listy adresów IP.
3.5.23.2 Wskazanie zakresu adresów IP.
3.5.23.3 Podanie listy adresów IP podsieci.
3.5.23.4 Tworzenie dynamicznie lub statycznie grup systemów.
3.5.23.5 Wskazanie nazw domenowych systemów.

3.5.24 System musi posiadać gotowe wzorce widoków (ang. Dashboard) do systemu centralnego zarządzania podatnościami, które mogą być edytowane przez administratora systemu.

3.5.25 Administrator musi mieć możliwość tworzenia widoków od podstaw używając co najmniej takich elementów jak:
3.5.25.1 Tabela.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.5.25.2 Wykres kołowy.

3.5.25.3 Wykres liniowy.

3.5.25.4 Wykres słupkowy.

3.5.26 Administrator do tworzenia widoków musi mieć możliwość używania co najmniej wymienionych filtrów:

3.5.26.1 adres IP.

3.5.26.2 Poziom ryzyka/niebezpieczeństwa.

3.5.26.3 CVE ID.

3.5.26.4 CVSS Score w wersji 3 i nowsze.

3.5.26.5 CVSS Vector w wersji 3 i nowsze.

3.5.26.6 Dostępny exploit.

3.5.26.7 Narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas).

3.5.26.8 Data opublikowania patch'a dla danej podatności.

3.5.26.9 Port, protokół.

3.5.26.10 Data opublikowania podatności.

3.5.26.11 Data pierwszy raz zauważenia podatności dla systemu.

3.5.26.12 Data, kiedy ostatni raz widziana była podatność dla systemu.

3.5.26.13 Przydział do określonej grupy systemów.

3.5.26.14 CCE ID.

3.5.26.15 MS Bulletin ID.

3.5.27 System musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA.

3.5.28 System musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności bez konieczności kontaktu z suportem producenta. Producent musi udostępniać informację w jaki sposób można budować swoje własne wzorca sprawdzania zgodności ze standardami przyjętymi w firmie.

3.5.29 System musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów:

3.5.29.1 Windows.

3.5.29.2 Unix.

3.5.29.3 Vmware.

3.5.29.4 Cisco.

3.5.29.5 Fortigate.

3.5.29.6 Oracle.

3.5.29.7 MySQL.

3.5.29.8 SQL Server.

3.5.29.9 PostgreSQL.

3.5.29.10 Juniper.

3.6 Funkcjonalność kontroli aplikacji powinna być standardową częścią rozwiązania, a skanowanie powinno zawierać testy sprawdzające (co najmniej OWASP). Dopuszczalne jest, aby funkcjonalność ta realizowana była z pomocą dodatkowego panelu zarządzania

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

lub dodatkowego systemu, w tym umiejscowionego w chmurze oraz dostępnego w modelu licencyjnym z 24 miesięcznym wsparciem producenta.

3.7 Funkcjonalności dodatkowe Systemu.

3.7.1 System powinien integrować się z systemami zarządzania aktualizacjami w celu np. sprawdzenia czy wynik ze skanowania pokrywa się z informacjami z tych systemów co najmniej z takimi systemami jak:

3.7.1.1 Microsoft SCCM.

3.7.1.2 Microsoft WSUS.

3.7.1.3 Red Hat Satellite Server.

3.7.2 System powinien umożliwiać ciągłe monitorowanie ruchu w sieci w celu wykrycia podejrzanych przepływów sieciowych z lub do podatnych usług, nieznanych urządzeń, botnetów lub serwerów Command and Control (tzw. C&C).

3.7.3 System powinien używać analizy statystycznej oraz monitorowania anomalii w zachowaniu na zewnętrznych źródłach logów w celu automatycznego wykrywania podejrzanych aktywności.

3.7.4 System powinien oferować poza wymienionymi w pkt. 3.5.27 wzorce zgodności z regulacjami takimi jak: CERT, STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH.

Opis wymagań dla oprogramowania równoważnego do Tenable Identity Exposure.

Jeżeli Zamawiający określił w Opisie przedmiotu zamówienia wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

Oprogramowanie Tenable Identity Exposure służy do zabezpieczania infrastruktury IT poprzez monitorowanie i analizę środowisk Active Directory (AD) oraz Microsoft Entra ID (dawniej Azure Active Directory). Celem jest identyfikacja i eliminacja podatności, słabości w konfiguracji kont oraz wykrywaniem potencjalnych ścieżek ataku związanych z tożsamościami w organizacji.

I. Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego do oprogramowania Tenable Identity Exposure:

1. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Opisie przedmiotu zamówienia, w szczególności w zakresie:

a) warunków licencji/sublicencji w każdym aspekcie licencjonowania/sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

również wszystkie elementy licencjonowania jak dla oprogramowania Tenable Identity Exposure,

b) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania Tenable Identity Exposure”,

c) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Tenable funkcjonującym u Zamawiającego,

d) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,

e) poszczególne składowe oprogramowania równoważnego współpracują ze sobą w sposób nie gorszy niż oprogramowania wskazanego w zamówieniu,

f) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,

g) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem.

2. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.

3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.

4. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.

5. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

II. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

1. Zbudować środowisko równoważne w stosunku do obecnie funkcjonującego systemu po stronie Zamawiającego. Wymaganiem koniecznym jest zapewnienie wysokiego poziomu bezpieczeństwa systemów objętych skanami/testami realizowanymi z wykorzystaniem rozwiązania równoważnego.
2. Zainstalować i kompleksowo skonfigurować oprogramowanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji systemu oraz zintegrować się z systemami AD

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

użytkowanych przez Zamawiającego w terminie do 10 dni roboczych od dnia podpisania umowy. W ramach potwierdzenia poprawnego wykonania konfiguracji. Wykonawca wykona próbny skan i wygeneruje raport ze skanów.

3. Dostarczyć wszystkie niezbędne licencje na oprogramowanie równoważne (ze wsparciem producenta na 24 miesięcy na oprogramowanie - również firm trzecich) wymagane do wdrożenia i uruchomienia systemu.
4. Przeprowadzić Instruktaż. Wykonawca przeprowadzi Instruktaż stanowiskowy dla minimum 4 osób wskazanych przez Zamawiającego.

   4.1. W instruktażu mogą uczestniczyć dodatkowe osoby wskazane przez Zamawiającego, lecz nie więcej niż 8 osób.

   4.2. W instruktażu mogą uczestniczyć dodatkowe osoby wskazane przez Zamawiającego, lecz nie więcej niż 8 osób.

   4.3. Instruktaż będzie przeprowadzony przez certyfikowanego przez producenta instruktora.

   4.4. W przypadku zaproponowania rozwiązania równoważnego do opisywanego Systemu, Wykonawca przeprowadzi kompleksowy instruktaż równoważnego systemu.

   4.5. Instruktaż będzie realizowany w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej.

   4.6. Instruktaż będzie trwał minimum 2 Dni Robocze każdy (minimum 14 godzin zegarowych każdy).

   4.7. Jeśli Wykonawca wykaże, że zakres instruktażu wykracza poza liczbę dni wskazaną w pkt. 4.5 (np. z uwagi na złożoność zaproponowanego Systemu) określi on liczbę oraz zakres instruktaży niezbędnych do pozyskania wiedzy niezbędnej do administrowania Systemem i w zakresie operatorskim. Wymagana jest wtedy akceptacja zakresu oraz liczby zaproponowanych przez Wykonawcę instruktaży przez upoważnionego przedstawiciela Zamawiającego.

5. Instruktaż dla administratorów i operatorów będzie obejmować wszelkie możliwe zagadnienia przydatne w codziennej pracy, a w szczególności:

   5.1. Szczegółowe omówienie Systemu i jego funkcjonalności, w tym omówienie architektury Systemu i procesu przetwarzania danych w Systemie.

   5.2. Tworzenie polityk, skanów, reguł wbudowanych w System oraz zdefiniowanych przez użytkownika.

   5.3. Ćwiczenia praktyczne z budowania reguł, polityk, skanów, raportów, dashboardów.

   5.4. Zarządzanie konfiguracją i bezpieczeństwem w Systemie.

   5.5. Omówienie procesów instalacji, konfiguracji, aktualizacji Systemu, tworzenia kopii bezpieczeństwa oraz przywracania w przypadku awarii.

   5.6. Omówienie procedur eksploatacyjnych.

   5.7. Omówienie dobrych praktyk oraz możliwości integracji z innymi rozwiązaniami.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

5.8. Zamawiający dopuszcza przeprowadzenie Instruktażu online lub w siedzibie Zamawiającego i decyzję przekaże Wykonawcy na etapie realizacji zamówienia. Na potrzeby Instruktażu Zamawiający zapewni sale, stacje robocze oraz pozostałą infrastrukturę (rzutnik, sieć, itp.).

5.9. Ponadto w ramach /instruktażu Wykonawca dostarczy:

5.9.1. szczegółową dokumentację producenta Systemu.

5.9.2. Inne materiały (instrukcje, video) niezbędne do pracy w Systemie dla Użytkowników.

5.9.3. wszystkie ww. materiały do przeprowadzenia instruktaży stanowiskowych i niezbędne w bieżącej pracy z Systemem będą przygotowane w języku polskim lub angielskim.

5.10. Plan przeprowadzenia Instruktaży stanowiskowych

5.10.1. Wykonawca przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu, w szczególności:

5.10.1.1. zakres Instruktażu (w szczególności: zajęcia praktyczne dla administratorów, operatorów).

5.10.1.2. szczegółowe określenie tematów Instruktażu,

5.10.1.3. proponowany harmonogram.

5.10.1.4. Dokument opisujący aspekty związane z Instruktażem stanowiskowym zostanie przekazany w terminie 2 dni roboczych od dnia zawarcia umowy.

6. Wykonać analizę przedwdrożeniową środowiska Zamawiającego oraz dostarczyć projekt techniczny systemu równoważonego, obejmującego specyfikację techniczną określającą wymogi na infrastrukturę teleinformatyczną / środowisko wirtualne dla systemu (w przypadku zaproponowania rozwiązanie on-prem), m.in:
   a) szczegółową specyfikację sprzętową serwerów/urządzeń sieciowych,
   b) ilość maszyn wirtualnych, procesorów wirtualnych, pamięci RAM, przestrzeni dyskowej,
   c) wymagane parametry łącza i przepływy sieciowe niezbędne do prawidłowej komunikacji systemu równoważnego zgodnie z wymaganiami Systemu,
   d) wymagane parametry systemu operacyjnego,
   e) wymagania wirtualizacji (platforma VMware).

   oraz szczegółowy opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do wdrożenia i konfiguracji Systemu równoważnego.
7. Przeprowadzić proces konfiguracji oprogramowania równoważnego z uwzględnieniem wskazanych przez Zamawiającego zasobów oraz podsieci, dokonać poprawnej konfiguracji mechanizmów komunikacji skanerów, sensorów, konsoli i innych komponentów systemu niezbędnych do prawidłowego i kompleksowego działania zaproponowanego rozwiązania równoważnego.
8. Wykonać dokumentację powykonawczą systemu równoważnego zgodnie z wymogami Zamawiającego, zawierającą m. in. informacje o szczegółach wykonanych prac wdrożeniowych, instrukcje instalacji, konfiguracji i użytkowania wdrożonego oprogramowania równoważnego, w tym dostarczy instrukcje stanowiskowe dla administratorów i operatorów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

III. Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania Tenable Identity Exposure:

Rozwiązania równoważne dla automatycznego systemu do skanowania i zarządzania tożsamościami w środowiskach AD i Entra ID (zwanego dalej „System") wraz z niezbędnymi licencjami:

1. Dostarczenie i pełne skonfigurowanie Systemu w modelu „on premise" (czyli zainstalowanie na infrastrukturze Zamawiającego).
2. Dostarczenie najnowszej wersji Systemu na dzień składania oferty oraz niezbędnych licencji typu virtual appliance lub software appliance. Licencje wskazane w pkt 1 lit. b) z minimum 24 miesięcznym wsparciem producenta zapewniającym aktualizacje dla Systemu.
3. Świadczenie usług gwarancyjnych producenta oprogramowania oraz wsparcia serwisowego i rozwojowego Wykonawcy przez okres, o którym mowa w pkt 1 lit. b) niniejszego OPZ.
4. **Architektura Systemu.**
   - 4.1 W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.
   - 4.2 Jeżeli System będzie instalowany jako System na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2019 i nowsze
   - 4.3 Jeżeli System będzie dostępny przez interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersjach na dzień składania oferty.
   - 4.4 Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Internetem.
   - 4.5 W przypadku braku dostępu do Internetu System ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.
   - 4.6 W przypadku dostępu do Internetu System ma umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania Systemem.
5. **Zarządzanie Systemem.**
   - 5.1 System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.
   - 5.2 Dostęp do systemu możliwy jedynie po uwierzytelnieniu użytkownika w systemie.
   - 5.3 Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej.
   - 5.4 System musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.
   - 5.5 System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych lub poprzez możliwość przypisania określonych operacji do zdefiniowanych ról.
   - 5.6 System powinien się integrować z Active Directory i Entra ID w zakresie uwierzytelnienia do Systemu oraz kontroli dostępu na bazie zdefiniowanych ról. Dopuszcza się rozwiązanie używające wewnętrznego mechanizmu uwierzytelniania do Systemu.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.7 System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.

5.8 System musi mieć wbudowany panel sterowania z predefiniowaną zawartością dostosowaną do potrzeb określonej roli. Dashboard powinien umożliwiać schodzenie do szczegółów w poszczególnych elementów z poziomu informacji podstawowych.

6. **System zarządzania i prezentacji wyników musi zapewnić możliwość:**
   6.1 przechowywania wszystkich danych pochodzących z wykonanych skanów i wykrytych problemów,
   6.2 przeglądanie tych danych w sposób przejrzysty dla użytkownika, co najmniej w postaci prezentacji krytycznych znalezisk, możliwość filtrowania wykrytych problemów, kategorii, zasobów,
   6.3 tworzenie raportów dostępnych w systemie centralnego zarządzania oraz wysyłanych na wskazane adresy email,
   6.4 prezentacji informacji o wykrytych problemach wraz z zaleceniami
7. **Funkcjonalności Systemu.**
   7.1 Intuicyjny interfejs graficzny (GUI): Oprogramowanie musi zapewniać graficzny interfejs użytkownika umożliwiający łatwą obsługę narzędzi i funkcji. GUI powinno wspierać zarządzanie projektami, przeprowadzanie testów, analizę wyników oraz generowanie raportów w sposób przejrzysty i intuicyjny.

   7.2 Wszystkie dane zebrane przez zewnętrzne silniki/sensory skanujące, monitorujące i testujące muszą być przesyłane niezwłocznie do centralnej bazy.
   Wszystkie testy i skany, które mogą wpłynąć na stabilność działania AD powinny być oznaczone w jasny sposób dla administratora.
8. **Monitorowanie i analiza Active Directory (AD)**
   8.1 Ciągłe monitorowanie AD: Stała analiza konfiguracji i zmian w Active Directory w celu identyfikacji słabych punktów i nieprawidłowości.
   8.2 Wskaźniki Ataków: Wykrywanie prób ataków na AD, takich jak eskalacja uprawnień (privilege escalation) czy lateral movement, w szczególności:
      8.2.1. Zrzut poświadczeń systemu operacyjnego: Pamięć LSASS (OS Credential Dumping: LSASS Memory)
      8.2.2. Podejrzana zmiana hasła kontrolera domeny (Suspicious DC Password Change)
      8.2.3. DCShadow
      8.2.4. DCSync
      8.2.5. Wykorzystanie DNSAdmins (DNSAdmins Exploitation)
      8.2.6. Ekstrakcja klucza kopii zapasowej domeny (Domain Backup Key Extraction)
      8.2.7. Enumeracja lokalnych administratorów (Enumeration of Local Administrators)
      8.2.8. Golden Ticket
      8.2.9. Kerberoasting
      8.2.10. Masowy rekonesans (Massive Computers Reconnaissance)
      8.2.11. Ekstrakcja NTDS (NTDS Extraction)
      8.2.12. Próby zgadywania haseł (Password Guessing)
      8.2.13. Próby wykonywania password spraying (Password Spraying)
      8.2.14. Podszywanie się pod nazwę SAM (SAM Name Impersonation)
      8.2.15. Kerberoasting (Unauthenticated Kerberoasting)

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

8.2.16. Wykorzystanie Zerologon (Zerologon Exploitation)

8.3 Wskaźniki Ekspozycji: Identyfikacja potencjalnych podatności i błędnych konfiguracji w AD, które mogą być wykorzystane przez atakujących.

8.4 Analiza ścieżek ataku: Mapowanie potencjalnych technik i ścieżek ataku, którymi atakujący mogą poruszać się w sieci po kompromitacji konta.

9. **Integracja z Microsoft Entra ID**

9.1 Obsługa środowisk hybrydowych: Możliwość monitorowania i analizy zarówno lokalnych, jak i chmurowych środowisk tożsamościowych.

9.1. Unifikacja tożsamości: Konsolidacja informacji o tożsamościach z AD i Entra ID w celu kompleksowej analizy ryzyka.

10. **Ocena ryzyka tożsamości**

10.1. Scoring ryzyka: Przypisywanie ocen ryzyka poszczególnym tożsamościom na podstawie ich konfiguracji, uprawnień i aktywności.

10.2. Identyfikacja ryzykownych kont: Wykrywanie kont z nadmiernymi uprawnieniami lub słabymi hasłami, stanowiących potencjalne cele ataków.

11. **Raportowanie i alertowanie**

11.1. Intuicyjny pulpit nawigacyjny: Dostęp do interaktywnego interfejsu prezentującego aktualny stan bezpieczeństwa AD i Entra ID.

11.2. Generowanie raportów: Tworzenie szczegółowych raportów dotyczących wykrytych podatności, incydentów i rekomendacji naprawczych.

11.3. Alerty w czasie rzeczywistym: Powiadamianie o wykrytych incydentach bezpieczeństwa za pośrednictwem e-maila lub systemów SIEM i w Systemie.

12. **Wymagania dotyczące wdrożenia**

12.1. System powinien działać bez konieczności instalacji agentów na monitorowanych systemach oraz bez potrzeby nadawania specjalnych uprawnień.

12.2. System musi umożliwiać wdrożenie w wersji on-premise z pełną funkcjonalnością zgodnie z dokumentacją producenta.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706