

PAKIET I - Zakup usługi opracowania dokumentacji SZBI, przeprowadzenia szkoleń, audytów oraz testów penetracyjnych, zakup oprogramowania do monitorowania infrastruktury IT

1. Opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji:

Minimalny zakres prac:

ETAP I. Audyt zerowy

- diagnoza przedwdrożeniowa - prace wykonane w siedzibie urzędu,
- analiza dokumentacji urzędu, zapoznanie się z dostępnymi regulacjami wewnętrznymi mającymi wpływ na bezpieczeństwo informacji,
- przeprowadzenie przez wykonawcę audytu w organizacji, w tym:
 - a. wywiady z kluczowymi pracownikami, piastującymi funkcje istotne z perspektywy bezpieczeństwa informacji ,
 - b. weryfikacja zgodności dokumentacji oraz procedur z normą ISO 27001,
 - c. identyfikacja i analiza luk w organizacji pod kątem zapewnienia bezpieczeństwa informacji oraz spełniania wymagań normy ISO 27001.
- opracowanie wyników audytu,
- opracowanie raportu wraz propozycją planu realizacji kolejnych etapów.

ETAP II. Analiza ryzyka

- przedstawienie propozycji metodyki analizy ryzyka w ramach Systemu Zarządzania Bezpieczeństwem Informacji,
- przeprowadzenie inwentaryzacji aktywów związanych z przetwarzaniem informacji oraz ich klasyfikacja uwzględniając specyfikę organizacji,
- przeprowadzenie analizy ryzyka w ramach SZBI, przy wsparciu wykonawcy w narzędziu wspierającym analizę ryzyka,
- opracowanie raportu zbiorczego, tj podsumowania zrealizowanych prac i wynikających z tego wniosków,

ETAP III. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji:

- Polityka bezpieczeństwa informacji
- Polityka ochrony danych osobowych
- Zasady bezpieczeństwa teleinformatycznego
- Zasady bezpieczeństwa osobowego
- Zasady bezpieczeństwa prawno-organizacyjnego
- Zasady bezpieczeństwa fizycznego
- Inne niezbędne i wymagane dokumenty (instrukcje, regulaminy)

W/w dokumenty powinny zostać stworzone w narzędziu wspierającym zarządzanie SZBI, o którym mowa w pkt. 10.

ETAP IV. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

- przygotowanie materiałów szkoleniowych dla pracowników.
- wsparcie przy przeprowadzeniu audytu wewnętrznego w ramach SZBI.
- wsparcie przy przeprowadzeniu przeglądu zarządzania w organizacji.

Dokumentacja SZBI musi zawierać wszystkie elementy określone w obowiązującej wersji norm ISO/IEC 27001 i ISO/IEC 27005, oraz zawierać politykę ochrony danych osobowych zgodną z RODO. Całość dokumentacji musi być zaimplementowana w narzędziu wspierającym zarządzanie SZBI.

Opracowanie dokumentacji SZBI ma być zgodne z:

- normami ISO/IEC 27001, ISO 22301,
- Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773),
- Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn.zm.),
- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.),
- Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80)

Przeprowadzenie audytu wdrożonego SZBI według normy ISO/IEC 27001.

- Audyt musi zostać przeprowadzony w okresie do 3 miesięcy od opracowania dokumentacji SZBI.
- Audyt musi zostać przeprowadzony w siedzibie zamawiającego oraz we wszystkich jednostkach podległych tj.:
 - Ośrodek Kultury Fizycznej i Rekreacji w Śmiglu,
 - Ośrodek Pomocy Społecznej w Śmiglu,
 - Szkoła Podstawowa w Bronikowie,
 - Szkoła Podstawowa w Starym Bojanowie,
 - Szkoła Podstawowa w Starej Przysiece Drugiej,
 - Szkoła Podstawowa w Śmiglu,
 - Zespół Szkół w Czaczu,
 - Zespół Przedszkoli w Śmiglu.
- Audyty muszą być wykonane zgodnie z KRI z elementami KSC w kontekście SZBI oraz muszą być zgodne z wytycznymi organów kontroli.
- Audyt musi być wykonany przez audytorów posiadających uprawnienia i doświadczenie opisane szczegółowo w pkt V. przedmiotowego Zapytania –

Zespół audytorski jest zobowiązany także do weryfikacji zgodności z innymi przepisami, m.in. w zakresie:

- oceny zgodności z przepisami o ochronie danych osobowych (np. RODO), w kontekście zarządzania danymi i bezpieczeństwa informacji i cyberbezpieczeństwem;
- weryfikacji zgodności z krajowymi i międzynarodowymi normami i standardami w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa.

2.Przeprowadzenie szkoleń pracowników i kierownictwa urzędu oraz jednostek podległych w zakresie wymagań SZBI i cyberbezpieczeństwa.

1. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu Miasta Śmigła. Szkolenie dla urzędu musi zostać przeprowadzone stacjonarnie z podziałem na minimum dwie grupy dla wszystkich pracowników i minimum jedną grupę dla kierownictwa urzędu. Czas trwania szkolenia minimum 4h na jedną grupę uczestników. Szkolenie musi omówić cały zakres opracowanej w zadaniu nr 1 dokumentacji SZBI.
2. Przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników jednostek podległych tj.:
 - Ośrodek Kultury Fizycznej i Rekreacji w Śmiglu,
 - Ośrodek Pomocy Społecznej w Śmiglu,
 - Szkoła Podstawowa w Bronikowie,
 - Szkoła Podstawowa w Starym Bojanowie,
 - Szkoła Podstawowa w Starej Przysiece Drugiej,
 - Szkoła Podstawowa w Śmiglu,
 - Zespół Szkół w Czaczu,
 - Zespół Przedszkoli w Śmiglu.

w wymiarze minimum 4h. Szkolenie musi omówić cały zakres opracowanej w zadaniu nr 1 dokumentacji SZBI.

3. Przeprowadzenie czterech szkoleń socjotechnicznych w wymiarze 3h każde dla wskazanych przez zamawiającego grup użytkowników. Wymaga się, aby tematyka szkoleń zawierała co najmniej:
 - omówienie poprawnych zasad związanych z cyberbezpieczeństwem;
 - wyjaśnienie pojęcia „cyberbezpieczeństwo”;
 - informacje na temat zagrożeń w sieci takie jak phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, wyłudzenia i inne zagrożenia - przykłady i omówienie sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami;
 - metody nieautoryzowanego pozyskania danych wraz z przykładami;
 - bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja;
 - stosowanie bezpiecznych haseł, autoryzacja dwuetapowa, klucze sprzętowe;
 - metody obrony oraz przeciwdziałania (w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, oprogramowaniem mogącym zablokować dostęp do urządzeń w urzędzie, szkodliwymi programami mogącymi pozyskać dane osobowe).
4. Przeprowadzenie szkoleń specjalistycznych dla pracowników technicznych urzędu – minimum 2 grupy po 6 h.

5. Przeprowadzenie szkolenia specjalistycznego dla audytorów SZBI – minimum 1 grupa w wymiarze 6h.

3.Przeprowadzenie testów penetracyjnych dla Urzędu Miejskiego Śmigła

Minimalny zakres testów penetracyjnych (przy czym przez testy penetracyjne należy rozumieć przeprowadzenie testów mających na celu wykrycie nieznanych podatności - skanowanie pod kątem znanych podatności narzędziami typu Nessus, BurpSuite, Rapid7 i inne podobne (komercyjne) wykonanych przez pentestera obejmuje przynajmniej:

- Zewnętrzne testy penetracyjne infrastruktury informatycznej:
 - Analiza topologii brzegu sieci: Ocena struktury i zabezpieczeń brzegów sieci oddzielających wewnętrzne zasoby od Internetu.
 - Weryfikacja mechanizmów ochronnych: Przegląd i testowanie zabezpieczeń zastosowanych na granicy sieci, w tym firewalli, systemów wykrywania i zapobiegania intruzom (IDS/IPS) oraz innych mechanizmów ochronnych.
 - Wykrywanie usług sieciowych udostępnianych do Internetu: Skanowanie portów i usług dostępnych publicznie w celu identyfikacji potencjalnych wejść dla atakujących.
 - Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet: Identyfikacja wersji oprogramowania serwerowego dostępnego publicznie, co może pomóc w wykryciu znanych podatności.
 - Eksploatacja dostępnych urządzeń oraz usług wystawionych do sieci Internet: Próby eksploatacji zidentyfikowanych podatności w celu oceny ryzyka.
 - Przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią Internet: Rekomendacje dotyczące wzmocnienia zabezpieczeń brzegu sieci.
- Wewnętrzne testy penetracyjne infrastruktury informatycznej:
 - Analiza topologii sieci LAN: Ocena struktury i zabezpieczeń wewnętrznej sieci LAN.
 - Weryfikacja mechanizmów ochronnych w sieci: Analiza i testowanie wewnętrznych zabezpieczeń sieciowych, w tym segregacji sieci i izolacji urządzeń.
 - Analiza komunikacji sieciowej: Monitoring i analiza ruchu sieciowego w poszukiwaniu nietypowych wzorców mogących wskazywać na naruszenia bezpieczeństwa.
 - Skanowanie portów TCP/UDP i wykrywanie usług sieciowych: Identyfikacja usług i aplikacji działających w sieci wewnętrznej.
 - Skanowanie hostów aktywnych w sieci: Lokalizacja i analiza aktywnych urządzeń w sieci wewnętrznej.
 - Eksploatacja dostępnych urządzeń oraz usług w sieci LAN: Próby eksploatacji znalezionych podatności w celu oceny wewnętrznych ryzyk bezpieczeństwa.
 - Proces tworzenia i odtwarzania kopii zapasowych: Ocena procedur backupu i możliwości odzyskania danych.
 - Monitorowanie ruchu sieciowego: Sprawdzenie systemów monitorowania w celu wykrywania podejrzanych aktywności i naruszeń bezpieczeństwa.
 - Przedstawienie rozwiązań zwiększających bezpieczeństwo sieci LAN: Rekomendacje dotyczące poprawy zabezpieczeń wewnętrznej sieci LAN.
- Audyt serwisów WWW, obejmujący:

- Wersje serwera HTTP i systemu CMS: Sprawdzenie aktualności i bezpieczeństwa zainstalowanych wersji, z naciskiem na znane podatności.
- Bezpieczeństwo komunikacji: Ocena aktualności certyfikatów X.509, wersji protokołu TLS i stosowanych algorytmów kryptograficznych, zapewniająca poufność i integralność przesyłanych danych.
- Raport z testów i audytu:
 - Opis zakresu przeprowadzonych prac audytowych: Szczegółowe przedstawienie metodologii, narzędzi i zakresu wykonanych testów i analiz.
 - Analiza informacji zebranych podczas audytów: Przedstawienie i omówienie wyników testów, w tym zidentyfikowanych podatności i potencjalnych ryzyk.
 - Wnioski i zalecenia dotyczące rozwiązań występujących problemów: Opracowanie propozycji działań naprawczych, zaleceń dotyczących poprawy bezpieczeństwa oraz strategii minimalizacji ryzyka.
 - Weryfikacja aspektów technicznych: Szczegółowa analiza zabezpieczeń serwisów WWW, lokalnych sieci teleinformatycznych oraz połączenia z siecią Internet, wraz z zaleceniami dotyczącymi poprawy i utrzymania wysokiego poziomu bezpieczeństwa.

Audyt ma zostać przeprowadzony w siedzibie Urzędu Miejskiego Śmigła.

Inne istotne warunki zamówienia:

| Informacje: | Ilość/szt.: Urząd |
|---|---|
| Ilość lokalizacji działalności organizacji | 1 |
| Ilość serwerów fizycznych | 1 |
| Ilość serwerów wirtualnych | 9 |
| Ilość zewnętrznych adresów IP | 5 |
| 1. stacji roboczych 2. drukarki sieciowe 3. routery 4. switch-e 5. access point 6. UTM | 1. 67 2. 18 3. 1 - INEA 4. 15 5. 6 6. 1 - FG |

4. Zakup oprogramowania do monitorowania infrastruktury IT: badania podatności, analizy ryzyka oraz wspierającego zarządzanie SZBI dla Urzędu Miejskiego Śmigła

Wymagania Ogólne systemu do monitorowania infrastruktury IT

1. Oprogramowanie musi być dostępne w wersji komercyjnej gotowej do instalacji i konfiguracji w środowisku Zamawiającego.
2. Oprogramowanie musi być dostępne w oficjalnej dystrybucji na terenie Polski.
3. Oprogramowanie musi być opatrzone licencją i ścieżką rozwoju producenta.
4. Licencjonowanie musi być oparte o ilość unikatowych monitorowanych adresów IP.
5. Licencjonowanie nie może ograniczać ilości monitorowanych metryk w ramach monitorowanego adresu IP.
6. system musi być dostarczony w najnowszej dostępnej wersji oprogramowania.
7. System musi być dostarczony z licencją bezterminową dla 5 szt. IP.
8. System musi być dostarczony wraz ze wsparciem produktowym producenta przez okres minimum 12 miesięcy (upgrade do najnowszej wersji, pomoc techniczna). Oferowane oprogramowanie musi posiadać wsparcie, którego co najmniej pierwsza linia jest świadczona w języku polskim.
9. Oprogramowanie posiadające oficjalne, Nielimitowane wsparcie producenta. Nie jest akceptowalne wsparcie typu „community support”, oferowane przez społeczność jego użytkowników.
10. Asysta/wsparcie przy wdrożeniu/konfiguracji oprogramowania w środowisku Zamawiającego.
11. Dołączona dokumentacja, instrukcje/prezentacje konfiguracji i obsługi oprogramowania.

Wymagania Funkcjonalne

1. Monitorowanie Serwerów i Urządzeń Sieciowych

- Możliwość monitorowania różnorodnych systemów operacyjnych (Windows, Linux, Unix).
- Obsługa monitorowania urządzeń sieciowych (routery, switchy, firewalle).
- Monitorowanie zasobów fizycznych (CPU, pamięć, dyski twarde).

2. Monitorowanie Aplikacji i Usług

- Monitorowanie dostępności i wydajności aplikacji webowych oraz baz danych.
- Wsparcie dla monitorowania aplikacji chmurowych (AWS, Azure, Google Cloud).
- Możliwość monitorowania usług takich jak HTTP, HTTPS, FTP, SMTP, DNS itp.

3. Monitorowanie Użytkowników i aplikacji www

- Realizacja automatycznych testów pracy użytkownika w aplikacji www
- Monitorowanie wydajności aplikacji z perspektywy użytkownika końcowego.
- Kontrola międzyczasów podstron/kroków scenariusza pracy użytkownika aplikacji www.

4. Alertowanie i Powiadomienia

- Definiowanie progów alarmowych i automatyczne powiadamianie (e-mail, SMS, powiadomienia PUSH).

- Możliwość konfiguracji alertów w zależności od krytyczności incydentu.
- Integracja z systemami zarządzania incydentami (ITSM).
- Eskalacja powiadomień

5. Raportowanie i Analiza Danych

- Generowanie raportów dotyczących dostępności, wydajności oraz wykorzystania zasobów.
- Wizualizacja danych w postaci wykresów i dashboardów.
- Możliwość eksportu raportów do formatów takich jak PDF, CSV.
- Tworzenie i modyfikacja raportów za pośrednictwem interfejsu WWW bez konieczności instalacji dodatkowego oprogramowania (poza przeglądarką i ew. technologiami Java, Flash itp.).
- Narzędzie raportujące musi umożliwiać automatyczną generację dowolnych raportów według zdefiniowanego harmonogramu, możliwość generowania raportów dostępności (wg hostów lub usług), raportów SLA (wg hostów lub usług), raportowanie incydentów, awarii itp., raportowanie wydajności sieci, zapis raportów do plików PDF, okresowe wysyłanie raportów e-mailem do wskazanych użytkowników, powiadomienia e-mail o incydencie, zapis zdefiniowanych parametrów raportów celem późniejszego wywołania.

6. Automatyzacja i Orkiestracja

- Automatyczna konfiguracja nowych urządzeń
- Automatyczne wykonywanie skryptów w odpowiedzi na zdarzenia.
- Integracja z narzędziami do zarządzania konfiguracją (Ansible, Puppet, Chef).
- Możliwość definiowania i uruchamiania zadań uwzględniając harmonogram dni i godzin.

7. Bezpieczeństwo i Audyt

- Zapewnienie szyfrowanej komunikacji między komponentami systemu.
- Monitorowanie i audytowanie zdarzeń związanych z bezpieczeństwem.
- Wbudowany mechanizm tworzenia kopii zapasowych ustawień systemu (monitorowane hosty i usługi).
- Wbudowany mechanizm zarządzania użytkownikami systemu.
- Możliwość tworzenia grup użytkowników.
- Historia danych statystycznych.
- Mechanizm przydzielania uprawnień użytkowników (dostęp do danych nt. hostów lub usług, możliwość konfiguracji obiektów, powiadomienia).
- Audyt pracy użytkownika w systemie

8. Integracje i API

- Otwarte API umożliwiające integrację z innymi systemami.
- Wsparcie dla integracji z popularnymi narzędziami do zarządzania IT (np. ServiceNow, Jira).
- Natywna integracja z systemami do centralnego gromadzenia logów i analizy zdarzeń opartymi o architekturę Elasticsearch, Opensearch
- Natywna integracja z systemami klasy SOAR
- Możliwość korzystania z webhooków do przesyłania danych w czasie rzeczywistym.
- Możliwość konfiguracji oprogramowania poprzez stronę www oraz programistyczne, udokumentowane API.

9. Interfejs Użytkownika

- Interfejs graficzny do wizualizacji struktury sieci.
- Interfejs graficzny do wizualizacji poszczególnych wybranych parametrów urządzeń.
- Przyjazny i intuicyjny interfejs webowy dostępny z poziomu przeglądarki.
- Możliwość personalizacji podstawowego ekranu aplikacji w powiązaniu z użytkownikiem systemu oraz dowolnej konfiguracji składników wyświetlanych na podstawowym ekranie aplikacji poprzez wybór odpowiednich widget'ów.
- Możliwość tworzenia wielu dashboardów
- Możliwość tworzenia dashboardów prywatnych jak i współdzielnych pomiędzy innymi użytkownikami aplikacji
- Możliwość tworzenia dashboardów typu iFrame - będącymi oknem aplikacji zewnętrznym
- Możliwość tworzenia własnych dodatków do dashboardów w formie obieteków programistycznych typu Widget. Aplikacja musi wspierać dodawanie własnych rozszerzeń do dashboardów.
- Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień push.
- Możliwość tworzenia i zapisywania filtrów dla monitorowanych urządzeń i ich parametrów
- Możliwość wykorzystania filtrów podczas tworzenia dashboardów

10. Monitorowanie Specyficznych Parametrów i Elementów Infrastruktury

- Monitorowanie podstawowych parametrów sprzętowych bez użycia dodatkowych agentów oraz pozostałych parametrów działania systemu operacyjnego i usług za pomocą dedykowanych agentów (w zależności od konfiguracji monitorowanego hosta).
- Możliwość monitorowania aplikacji i procesów o dynamicznym zachowaniu.
- Możliwość monitorowania min. krytycznych elementów infrastruktury, aplikacji, usług sieciowych, protokołów sieciowych, wskaźników systemowych, infrastruktury sieciowej, portów.
- Możliwość śledzenia parametrów takich jak:
 - Telnet na wybrany port - nasłuch na porcie,
 - Ping dostępność urządzenia,
 - Odczyt, przetwarzanie i generowanie alertów z pułapek SNMP,
 - Poprawne działanie serwera DHCP,
 - Poprawne działanie serwera czasu NTP,
 - Zajętość danych na poszczególnych partycjach,
 - Zajętość RAM,
 - Obciążenie systemu,
 - Obciążenie dysków,
 - Ilość zalogowanych użytkowników,
 - Ilość procesów,
 - Obecność procesów w systemie,
 - Synchronizacja dysków programowego RAID,
 - Synchronizacja dysków sprzętowego RAID,
 - Kontrola parametrów polecenia VMSTAT,
 - Obecność SSH.
- Możliwość śledzenia parametrów monitoringu systemu poczty:
 - Poprawne działanie serwera SMTP,
 - Poprawne działanie serwera POP3,
 - Poprawne działanie serwera IMAP,
 - Ilość listów w kolejkach serwera Postfix.

- Możliwość śledzenia parametrów monitoringu DNS:
- Poprawne działanie DNS,
- Rozwiązywanie zadanych domen na adresy IP,
- Parametry serwerów WWW,
- Poprawne działanie serwera WWW,
- Kontrola występowania oczekiwanych treści na stronie,
- Czas odpowiedzi serwera WWW.
- Możliwość śledzenia parametrów monitoringu bazy danych:
- Poprawna praca bazy,
- Kontrola stanu synchronizacji baz,
- Zajętość przestrzeni danych.
- Możliwość śledzenia parametrów DRBD i HEARTBEAT:
 - Poprawne działanie klastra,
 - Poprawne działanie replikacji danych.
- Możliwość śledzenia parametrów macierzy dyskowych:\ul>- Analiza statusów ogólnych urządzenia,
- Analiza dysków urządzenia.

11. Dodatkowe Elementy Infrastruktury Informatycznej do Monitorowania

- Monitorowanie zasobów wirtualnych (maszyny wirtualne, hypervisory).
- Monitorowanie infrastruktury kontenerowej (Docker, Kubernetes).
- Monitorowanie systemów backupowych i urządzeń magazynujących.
- Monitorowanie systemów IoT i urządzeń edge computing.
- Monitorowanie systemów SCADA i przemysłowych systemów sterowania.
- Monitorowanie infrastruktury zasilania (UPS, generatory).
- Monitorowanie systemów HVAC (Heating, Ventilation, and Air Conditioning).

Wymagania Techniczne

1. Architektura Systemu

- System musi działać w modelu klient-serwer.
- System pracuje pod kontrolą środowiska OS w licencji open source.
- Możliwość wdrożenia systemu zarówno on-premises, jak i w chmurze.
- Wsparcie dla skalowalności poziomej i pionowej.
- System musi wspierać architekturę wysokiej dostępności dla każdej warstwy systemu.

2. Wymagania dotyczące Wydajności

- System musi umożliwić rozbudowę, pozwalającą na monitorowanie nieograniczonej wydajnością liczby urządzeń w sieci. Architektura musi umożliwiać rozkładanie obciążenia pomiędzy elementy systemu.

3. Wymagania dotyczące składowania danych

- Możliwość replikacji i backupu danych.
- Gromadzone dane muszą być składowane w nierelacyjnej bazie danych. W przypadku architektury Monitoringu HA baza dostarczana jest również w trybie HA,

pozwalając na klastrowanie danych. Nie jest dopuszczane składowanie metryk w osobnych bazach węzłów HA.

Wymagania dot. montażu, instalacji i konfiguracji sprzętu

Dostarczone urządzenie zostanie podłączone i skonfigurowane z najlepszą wiedzą techniczną i zaleceniami producenta.

Wymagania dla oprogramowania do badania podatności, analizy ryzyka oraz wspierającego zarządzanie SZBI:

1. System powinien być dostępny przez przeglądarkę internetową bez konieczności instalowania oprogramowania na komputerach użytkowników końcowych.
2. System powinien umożliwiać logowanie użytkownikom poprzez Active Directory.
3. System powinien posiadać intuicyjny interfejs użytkownika oparty na stronach WWW zgodnych ze specyfikacją języka HTML i działać poprawnie w aktualnych wersjach przeglądarek internetowych bez konieczności instalowania dodatków/wtyczek do przeglądarki.
4. System powinien zapewniać możliwość dostosowania wyglądu (logo, kolorystyka) do potrzeb Zamawiającego.
5. Interfejs użytkownika musi być dostępny w języku polskim. Administrator powinien mieć możliwość samodzielnej modyfikacji nazw pozycji menu, etykiet pól formularzy, podpowiedzi oraz innych elementów interfejsu bez konieczności angażowania dostawcy oprogramowania.
6. System powinien oferować konfigurowalne widoki danych możliwe do dostosowania przez użytkownika w zależności od potrzeb (co najmniej w zakresie widoczności/kolejności kolumn, filtrów i porządku sortowania).
7. System powinien oferować kokpity menedżerskie prezentujące syntetyczne informacje w postaci wykresów i rankingów co najmniej w zakresie zidentyfikowanych podatności, najwyższych ryzyk, statusu realizacji działań (usuwanie podatności, postępowania z ryzykiem/incydemem), zmian poziomu ryzyka. Kokpity powinny być konfigurowalne (każdy użytkownik tworzy swój kokpit) i prezentować tylko te dane, do których użytkownik ma dostęp w systemie (nawet statystyczne/sumaryczne).
8. System powinien umożliwiać zarządzanie uprawnieniami użytkowników do poszczególnych funkcji i zasobów systemu.
9. System powinien posiadać mechanizm historii zmian, który rejestruje wszystkie modyfikacje danych dokonywane w systemie przez użytkowników.
10. System powinien umożliwiać wyszukiwanie informacji w bazie danych na podstawie różnych kryteriów.
11. System powinien umożliwiać tworzenie raportów operacyjnych przez użytkowników (nałożone filtry, porządek sortowania, widoczne pola) z opcją zapisania/wczytania oraz eksportu odfiltrowanych danych (format XLSX lub CSV).
12. System powinien generować raporty z dostępu do danych (kto czytał/modyfikował dany wpis, pobierał pliki itd.).
13. System powinien zawierać zestaw niezbędnych procesów biznesowych związanych z badaniem podatności i zarządzaniem nimi, analizą ryzyka, obsługą incydentów i postępowania w wyniku incydemu, podatności, wysokiego ryzyka.
14. System powinien posiadać mechanizm powiadamiania użytkowników o zadaniach a także generować przypomnienia o zadaniach, dla których określono termin realizacji.
15. System powinien umożliwiać tworzenie i zarządzanie strukturami organizacyjnymi (jednostki/komórki organizacyjne, stanowiska, osoby) zapewniając intuicyjną prezentację

(np. diagram / drzewo struktury) i łatwe zmiany (np. przenoszenie obiektów poprzez drag&drop).

16. System powinien pozwalać na definiowanie ról (poprzez powiązanie komórek/stanowisk/osób z daną rolą) i uprawnień użytkowników, a także kontrolować dostęp do danych i funkcjonalności systemu.

17. System powinien zapisywać historię zmian w strukturze organizacyjnej i rolach w kontekście poszczególnych użytkowników i prezentować ją w przyjaznej, łatwej do analizy formie z opcją wyszukiwania co najmniej po nazwisku poszczególnych osób.

18. System powinien zapewniać automatyczne uprawnienia dla przełożonych poszczególnych osób w taki sposób, aby miały dostęp do danych przez nie przetwarzanych (wyniki analizy ryzyka, postępowania, dokumenty itd.).

19. System powinien oferować mechanizm zastępstw. Osoba zastępowana powinna na czas zastępstwa otrzymywać zadania osoby niedostępnej i mieć dostęp do jej danych w systemie.

20. System powinien zapewniać możliwość generowania raportów i analiz na podstawie danych zgromadzonych w systemie.

21. System powinien być bezpieczny i chronić dane przed nieautoryzowanym dostępem.

22. System powinien umożliwiać tworzenie, edycję i zarządzanie dokumentami publikowanymi w organizacji, w tym ich wersjonowanie i opisywanie zmian.

23. System powinien rejestrować dostępy do dokumentów (dokumentacja, zasoby, ryzyka, etc.) a także posiadać mechanizm informowania o nowościach (nowe dokumenty) wybranych użytkowników w postaci widoku w systemie i wysyłanego newsletter'a.

24. Dla wybranych dokumentów (procedury, instrukcje itd.) system powinien zapewniać możliwość wymuszenia potwierdzenia przeczytania dokumentu i możliwość raportowania, kto już potwierdził przeczytanie.

25. System powinien zapewniać mechanizmy do śledzenia zmian w dokumentach i procesach, a także przeglądania tej historii.

26. System musi prowadzić szczegółowe logi audytowe wszystkich wykonywanych operacji, obejmujące:

- Rejestrację podstawowych zdarzeń systemowych, takich jak: udane i nieudane logowania użytkowników, dostęp do danych (tworzenie, odczyt, zapis, pobieranie plików), zmiany konfiguracyjne.
- Rejestrację zdarzeń w ramach procesów, takich jak: data wygenerowania zadania, data przyjęcia zadania, data zakończenia zadania, osoby przypisane do zadania, osoba faktycznie wykonująca zadanie, akcja kończąca zadanie.
- Rejestrację modyfikacji danych z precyzją do poziomu pola formularza, obejmującą datę zmiany, wartość przed i po zmianie, osobę dokonującą zmiany oraz etap procesu, na którym zmiana została wprowadzona.

27. System powinien zapewniać możliwość generowania raportów o różnych aspektach działania systemu, takich jak lista dokumentów, status procesów, aktywność użytkowników.

28. System powinien umożliwiać eksport raportów w formacie co najmniej PDF, DOCX, XLS/XLSX.

29. System powinien zakładać rozproszoną realizację zadań przez wielu pracowników z organizacji i opierać się na mechanizmach przepływu pracy (workflow) zlecając zadania (np. klasyfikacja informacji, analiza ryzyka, itd.) wielu użytkownikom a następnie przetwarzając/agregując dane przez nich wprowadzone.

30. System musi umożliwiać późniejszą modyfikację/rozbudowę o kolejne moduły / zmiany w istniejących modułach i procesach bez naruszania spójności i przebiegu już rozpoczętych działań.

31. System powinien umożliwiać kompleksowe zarządzanie aktywami, w tym ich klasyfikację, opis cech oraz rejestrację działań na nich wykonywanych.

32. System powinien udostępniać funkcjonalność do identyfikacji podatności w systemach IT poprzez integrację z narzędziami skanującymi sieci i systemy.

33. System powinien umożliwiać ocenę ryzyka dla poszczególnych zasobów przez pryzmat klasyfikacji informacji, które przetwarzają, incydentów oraz zidentyfikowanych podatności dla danego zasobu/usługi.
34. System powinien wspierać proces oceny ryzyka, w tym automatyczne obliczanie istotności ryzyka na podstawie zdefiniowanego modelu.
35. System powinien umożliwiać definiowanie i zarządzanie planami postępowania z ryzykiem, w tym przypisywanie odpowiedzialnych za realizację działań oraz monitorowanie ich postępu.
36. System powinien udostępniać funkcjonalność do zgłaszania, analizy i zarządzania incydentami, w tym powiązanie ich z zasobami i ryzykami.
37. System powinien zapewniać możliwość generowania raportów i zestawień dotyczących aktywów, ryzyk, incydentów oraz innych aspektów bezpieczeństwa.
38. System powinien umożliwiać przeprowadzenie inwentaryzacji systemów informatycznych (zasobów i usług). Inwentaryzacja powinna być wspierana skanowaniem aktywnych hostów i usług w sieci (discovery).
39. System powinien umożliwiać przeprowadzenie klasyfikacji grup informacji w oparciu o Poufność, Integralność i Dostępność a także wskazanie zasobów (serwerów, usług, pomieszczeń), w których dana grupa informacji jest przetwarzana.
40. Klasyfikacja informacji powinna być realizowana w sposób rozproszony (przez właścicieli grup informacji) a następnie agregowana.
41. Na podstawie wyników klasyfikacji informacji system powinien określić istotność danego aktywa dla organizacji przez pryzmat informacji, które ono przetwarza (agregacja wyników klasyfikacji informacji).
42. System powinien pozwalać na analizę ryzyka związanego z bezpieczeństwem informacji, uwzględniając skutki utraty poufności, integralności i dostępności.
43. System powinien umożliwiać zaplanowanie działań mających na celu zmniejszenie ryzyka oraz monitorowanie realizacji tych działań.
44. System powinien wspierać zarządzanie zdarzeniami (incydentami) bezpieczeństwa, w tym gromadzenie informacji o incydentach, wiązanie ich z zasobami i ryzykami, ich analizę, planowanie i realizację planowania działań naprawczych.
45. System powinien umożliwiać definiowanie i zarządzanie aktywami, takimi jak systemy teleinformatyczne, urządzenia, obiekty i inne zasoby.
46. System powinien pozwalać na przypisanie informacji przetwarzanych do konkretnych aktywów oraz identyfikację ryzyk związanych z tymi aktywami a także prezentować raport z dotyczący ryzyka utraty bezpieczeństwa informacji w kontekście danej grupy informacji (na podstawie ryzyk dotyczących poszczególnych aktywów przetwarzających).
47. System powinien zapewniać mechanizmy audytu i śledzenia działań użytkowników.
48. System powinien umożliwiać integrację z narzędziami klasy SIEM, w tym bieżące przekazywanie logów przeznaczonych dla SIEM do serwera Syslog.
49. System powinien umożliwiać definiowanie własnych raportów.
50. System powinien wspierać skanowanie i analizę aktywnych hostów i usług w sieci / sieciach i generować zestawienie hostów (adres IP) oraz usług (adres IP i port).
51. System powinien umożliwiać centralne zarządzanie zlecanymi skanami discovery oraz skanami podatności wybranych hostów/portów/usług i zbierać wyniki skanów w sposób ujednolicony i scentralizowany.
52. System powinien zawierać własne lub integrować się z dostępnymi na rynku narzędziami do skanowania sieci (np. NMAP) oraz narzędziami do wykrywania podatności usług dostępnych w sieci (skanery podatności).
53. Skany podatności powinny być realizowane automatycznie z poziomu systemu głównego (bez konieczności przechodzenia do innego programu/narzędzia, wprowadzania tam danych i uruchamiania skanu).

54. System musi umożliwiać uruchamianie skanów usług w różnych podsieciach, do których nie ma on bezpośredniego dostępu (dopuszczony jedynie ruch ze skanowanej podsieci do serwera na wybranym porcie).
55. Na podstawie zidentyfikowanych aktywów w wyniku skanu (discovery) powinno być możliwe ich dodatkowe opisanie w tym łącznie wielu elementów w jedną usługę (np. ta sama usługa działająca na wielu portach) w sposób przyjazny dla użytkownika (np. zaznaczenie jednego lub więcej elementów i utworzenie paszportu usługi).
56. System musi zapewniać wprowadzanie i utrzymywanie kompletnego, spójnego i aktualnego rejestru aktywów.
57. System musi umożliwiać wypełnianie i generowanie metryk / paszportów zasobu zawierającego minimum: nazwę, typ, właściciela, osobę odpowiedzialną za ocenę ryzyka (może być inna niż formalny właściciel), zasoby podrzędne i nadrzędne (z wyraźnym rozgraniczeniem), adresy IP i porty (jeśli dotyczy), umiejscowienie fizyczne.
58. System musi umożliwiać wskazanie działań związanych z danym aktywem w podziale na planowane (termin, przypomnienie przed, odpowiedzialność) i wykonane (wynik działania, np. czasowe wyłączenie, serwis, audyt) oraz zapewnić komunikację zdarzeń, przypomnienia i raportowanie.
59. System powinien umożliwiać zbiorcze zarejestrowanie działań na wielu zasobach przez kontrahentów zewnętrznych (np. poprzez wygenerowanie dla nich arkusza z miejscem do wprowadzenia wyników) i import ich jako działań powiązanych z konkretnymi zasobami.
60. Wyniki skanowania podatności powinny być wstępnie filtrowane na podstawie atrybutu CVSS aby uniknąć konieczności analizowania wpisów informacyjnych i mało istotnych podatności (definiowalny próg odcięcia). W systemie (w widoku do analizy) powinny się znaleźć tylko te wpisy, które przekraczają zadany próg CVSS, ale powinna być możliwość dotarcia do „surowych” danych (np. plików CSV, XLS lub innych) zawierających kompletne wyniki skanu.
61. System musi umożliwiać import wyników skanowania podatności z pliku (import skanów zrealizowanych niezależnie od systemu) wyeksportowanego ze skanera podatności (np. oprogramowania Nessus).
62. System powinien zapewniać mapowanie wyników skanów w zakresie pól (danych) generowanych przez skaner podatności na pola dostępne w systemie. W przypadku zastosowania integracji z wieloma skanerami podatności, wyniki skanu powinny być prezentowane w zunifikowanej formie (wspólne kolumny), w jednym wspólnym rejestrze możliwym do filtrowania i sortowania po wszystkich kolumnach.
63. System powinien wiązać wyniki skanu z zasobami (hostami i usługami) na podstawie adresu IP oraz portu, na którym wykryto podatność. Wyniki skanów powinny być prezentowane osobom oceniającym ryzyko dla danego zasobu.
64. Dla wyników skanu powinna istnieć możliwość uruchomienia postępowania grupującego wyniki (np. kilkadziesiąt wpisów dotyczących podatności nieaktualnej wersji SZBD czy serwera WWW, identyczne podatności na wielu hostach) po wskazaniu jednego lub więcej wyników skanu.
65. W ramach postępowania system powinien wskazać zasoby, których ono dotyczy, a także pozwolić na powiązanie jej z ryzykiem dotyczącym tych zasobów.
66. Postępowania z podatnościami (wraz ze statusem) powinny być widoczne dla osoby oceniającej ryzyko dla danego zasobu.
67. W ramach postępowania z podatnością wymagane jest wskazanie osoby prowadzącej postępowanie a także możliwość zdefiniowania szczegółowych działań (zadań) z określeniem co najmniej osoby odpowiedzialnej, terminu realizacji, częstotliwości cyklicznego raportowania postępów.
68. System powinien monitorować postępy w usuwaniu podatności poprzez wymuszanie wprowadzenia raportu z postępów na użytkownikach odpowiedzialnych za działania zgodnie z zadaniem czasokresem raportowania (np. co tydzień, co miesiąc, co kwartał).

69. Po zakończeniu postępowania uprawniona osoba powinna określać deklaratywnie, czy podatność została wyeliminowana (zgodnie z przedstawionymi informacjami z przebiegu postępowania).

70. System powinien umożliwiać ponowienie skanu (dla tych samych kryteriów, hosta, portów) w celu weryfikacji czy podatności faktycznie wyeliminowano i oznaczyć poprzednio zaimportowane wyniki skanów odpowiednim statusem mówiącym o tym, czy podatność nadal występuje (co najmniej: nowa – nie było wcześniej/nie badano ponownie, nadal występuje – po ponownym badaniu, wyeliminowana – nie wystąpiła w ostatnim skanie).

71. System musi być zgodny z aktualnymi normą PN-EN ISO/IEC 27001.

72. System musi posiadać mechanizmy umożliwiające zarządzanie ryzykiem w bezpieczeństwie informacji.

73. Administrator systemu/modułu powinien mieć możliwość zbiorczego zlecania zadań związanych z oceną / aktualizacją oceny ryzyka bezpieczeństwa informacji.

74. Podczas realizacji powtarzalnych zadań (np. cykliczna ocena ryzyka) system powinien podpowiadać wartości wprowadzone wcześniej z opcją ich zmiany.

75. System musi zapewniać realizację wszystkich zadań wynikających z procesu zarządzania ryzykiem w bezpieczeństwie informacji (identyfikacja, analiza, ocena, postępowanie z ryzykiem, monitorowanie, komunikacja) i generować stosowne dokumenty i raporty.

76. System musi umożliwiać samodzielne dostosowanie i określenie skali ocen oraz progów prawdopodobieństwa i wpływu ryzyka na organizację.

77. System musi oferować predefiniowany katalog zagrożeń z możliwością jego modyfikacji.

78. System musi wersjonować wyniki analizy ryzyka i rejestrować liczbową zmianę poziomu ryzyka pomiędzy kolejnymi wersjami (ocenami ryzyka).

79. System musi pozwalać na określenie planowanej reakcji na ryzyko (akceptacja / monitorowanie / działanie) zależnie od poziomu ryzyka.

80. System musi wspierać realizację działań związanych z minimalizacją ryzyka.

81. W ramach postępowania z ryzykiem wymagane jest wskazanie osoby prowadzącej postępowania a także możliwość zdefiniowania szczegółowych działań (zadań) z określeniem co najmniej osoby odpowiedzialnej, terminu realizacji, częstotliwości cyklicznego raportowania postępów. System powinien kierować zadania do osób wskazanych i przypominać im o terminach a także wymagać od nich cyklicznego składania raportów z postępów (z opcją odstąpienia od raportowania przy planowaniu działań).

82. System musi zapewniać generowanie raportów z oceny ryzyka w kontekście: zagrożeń, zasobów, grup informacji.

83. System powinien działać poprawnie w środowiskach wirtualnych (jako maszyna wirtualna lub kontener).

84. W ramach wdrożenia Zamawiający oczekuje licencji dla dwóch środowisk: testowego i produkcyjnego.

85. System powinien działać w środowisku Zamawiającego. Dostępne zasoby / oprogramowanie:

- System operacyjny: Widnows Serwer 2022 Standard i Windows Serwer 2012 Standard
- Bazy danych: SQL Server 2014
- Dostępne vCPU: 48 .
- Dostępna pamięć vRAM: 64.
- Skaner podatności: Brak .

Wszystkie licencje wymagane do uruchomienia systemu (za wyjątkiem komercyjnych skanerów podatności, które zakupi Zamawiający) powinny być dostarczone przez Wykonawcę i wliczone w koszt wdrożenia. Dotyczy to systemu operacyjnego (jeśli inny niż posiadany przez Zamawiającego), oprogramowania firm trzecich,

stosowanych bibliotek komercyjnych osób trzecich, systemu zarządzania bazą danych (jeśli inny niż posiadany przez Zamawiającego), itd.

86. Z uwagi na fakt, iż Zamawiający zamierza aktywnie angażować wszystkich pracowników organizacji w procesy związane z bezpieczeństwem informacji, licencja na system powinna być udzielona organizacji, bez limitu użytkowników lub zapewniać jednoczesną pracę 70 użytkowników. W przypadku licencji udzielanej na użytkownika należy podać koszt dokupienia dodatkowych licencji.

Parametry SLA (godziny robocze):

- Awaria – reakcja 4h, rozwiązanie 16h
- Błąd – reakcja 8h, rozwiązanie 40h
- Usterka – reakcja 16h, rozwiązanie 14 dni roboczych

Producent zapewni minimum 12 miesięcy asysty technicznej.

Wymagania dla skanera podatności:

- musi być zarządzany przez przeglądarkę, zabrania się używania jakiegokolwiek grubego agenta/klienta,
- musi mieć opcję dostarczenia jako oprogramowanie i maszyna wirtualna. W przypadku dostarczenia jako maszyna wirtualna muszą być wspierane środowiska Hyper-V oraz Vmware. W przypadku systemu operacyjnego na którym będzie instalowany produkt jako oprogramowanie, muszą być wspierane co najmniej systemy operacyjne: Ubuntu 18.04/20.04/22.04, SUSE Enterprise 12, Windows Server 2012/2012 R2/2016/2019/2022, Windows 10,11, CentOS 9, Oracle Linux 7/8/9, macOS 12/13/14
- licencja nie może być ograniczona ilością skanowanych adresów IP,
- system musi mieć możliwość pracy bez dostępu do Internetu, a dostarczanie nowych reguł skanowania musi odbywać się za pomocą ręcznej aktualizacji z poziomu interfejsu,
- interfejs systemu musi przedstawiać informacje o systemie takie jak użycie CPU, pamięci, ilość skanowanych systemów, ilość sesji TCP, ruch przesyłany i odbierany do/z skanera,
- możliwość wymuszenia polityki haseł dla administratorów logujących się do systemu.
- musi być dostarczony z predefiniowanymi politykami skanowania minimum polityka dotycząca wykrycia hostów w sieci, WannaCry, Log4Shell, SoloriGate,
- musi być możliwość skanowania systemów pod kontem zgodności z regulacjami takimi jak CIS, DISA. W przypadku zgodności z regulacjami, producent musi dostarczać gotowe wzorce polityk zgodności z CIS, DISA jak również musi być możliwość zbudowania własnej polityki sprawdzania pod kontem zgodności z przyjętymi regulacjami w firmie w oparciu o dokumentację dostarczoną przez producenta. Wzorce zgodności z regulacjami dostarczone przez producenta muszą być możliwe do edycji. Sprawdzanie systemu pod kontem zgodności z regulacjami oraz dostęp do wzorców regulacji na stronie producenta nie wymaga żadnej dodatkowej licencji,
- musi być możliwość tworzenia własnej polityki skanowania w której administrator wybiera jakie podatności będą sprawdzane,
- system musi umożliwiać skanowanie z uwierzytelnieniem i bez uwierzytelnienia. W przypadku skanowania z uwierzytelnieniem muszą być wspierane następujące metody:

- Windows – Kerberos, LM Hash, NTLM Hash, hasło
- SSH – kluczy publiczny, Kerberos, hasło, certyfikat,
- SNMP3
- w przypadku skanowania systemów opartych o system linux/unix musi być możliwość podniesienia uprawnień przynajmniej za pomocą poniższych technik: .k5login, Cisco (enable), dzdo, pbrun, su, sudo,
- system pozwala na tworzenie jak również używanie dostarczonych przez producenta wzorców skanowania pod kontem konfiguracji systemów bezpieczeństwa i sieciowych. Muszą być wspierane przynajmniej wymienione systemy: FireEye, SonicWall, Fortinet FortiGate, BlueCoat ProxySG, Amazon AWS, Microsoft Azure,
- system zezwala na tworzenie harmonogramu skanowania podatności jak również uruchomienia na żądanie,
- -system musi pozwalać na porównanie wyników dwóch wykonanych skanów,
- system musi umożliwiać sprawdzenie konfiguracji systemu bez dostępu do niego. Sprawdzenie ma być dokonane na podstawie pliku konfiguracyjnego. Muszą być wspierane przynajmniej systemy jak: FireEye, SonicWall, Fortinet FortiGate, BlueCoat ProxySG,
- system musi umożliwiać filtrowanie wyników przynajmniej po takich parametrach jak: CVE, CVSS, CVSS v4/v3/v2, Czy jest dostępny exploit, hostname, kiedy była upubliczniona aktualizacja na dana podatność, port, protokół, wrażliwość w oparciu o punktację CVSS, zawartość opisu podatności, Bugtraq ID, CERT Vulnerability ID, CPE, IAVB ID,
- system musi być wspierany przez dodatkowy system punktowania podatności prezentowany w GUI oparty min. o uczenie maszynowe i aktualizowany codziennie. Mechanizm ten wspierany musi być również przez zespół ludzi producenta skanera, którzy analizują wyniki z modelu uczenia maszynowego jak również monitorują źródła takie jak min. Darknet,
- system musi mieć możliwość przetrzymywania historii wykonanych skanów,
- możliwość wyeksportowania wyników skanowania przynajmniej do formatów HTML, CSV, PDF,
- możliwość wygenerowania przynajmniej raportu Top 10 Podatności, Wykryty system operacyjny, nie wspierane oprogramowanie, Podatności na które są znane exploity,
- możliwość dodania nazwy oraz własnego logo do raportu,
- system musi prezentować wynik skanowania wraz z rekomendacją od jakich aktualizacji zacząć, aby wyeliminować największe ryzyko przez daną aktualizację,
- system musi umożliwiać zmianę wrażliwości wykrytej podatności w wyniku wykonanego skanu, musi być możliwość ukrycia w wynikach danej podatności,
- system musi umożliwiać zmianę elementu wykrywającego daną podatność zawiązując regułę do konkretnego systemu skanowanego oraz czas jak długo dana reguła ma obowiązywać,
- aktualizacja reguł wykrywania podatności musi być wykonywana automatycznie w przypadku dostępu systemu do Internetu,
- system musi umożliwiać automatyczną instalację Terrascan z poziomu GUI skanera,
- system musi umożliwiać nagrywanie ruchu pomiędzy skanerem, a skanowanym hostem w przypadku rozwiązywania problemów,
- system musi pozwalać na ustawienie skanowania adresów IP w przypadkowej kolejności,
- system musi umożliwiać ustawienia dotyczące wydajności skanowania tzn. liczba jednocześnie skanowanych systemów, liczba jednoczesnych elementów sprawdzanych na skanowanym systemie, maksymalna liczba jednoczesnych sesji TCP na skanowany system oraz maksymalna liczba jednoczesnych sesji na skan,
- system musi umożliwiać wykonanie w ramach jednego skanu skanowania pod kontem podatności oraz zgodności z regulacjami.

Wykonawca zapewni minimum 12 miesięcy asysty technicznej.

Wymagania dot. montażu, instalacji i konfiguracji oprogramowania

Dostarczone oprogramowanie zostanie podłączone i skonfigurowane z najlepszą wiedzą techniczną i zaleceniami producenta.