Załącznik nr 2 do Ogłoszenia o zamówieniu (2025-01)

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**- Specyfikacja parametrów funkcjonalno - technicznych**

**Działania zwiększające poziom cyberbezpieczeństwa Szpitala poprzez wdrożenie   
lub modyfikację systemu zarządzania bezpieczeństwem informacji i opracowanie audytu końcowego, przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa oraz zakup oprogramowania EDR/XDR   
i zapór sieciowych w związku z realizacją projektu pn. „Transformacja cyfrowa   
w zakresie świadczonych usług medycznych Szpitala ARION Med Sp. z o.o. w Gorzewie” (KPOD.07.03-IP.10-0180/25) w ramach Programu: Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia”, Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” (nabór konkurencyjny nr KPOD.07.03-IP.10-001/25).**

**Zadanie nr 1 Wdrożenie lub modyfikacja Systemu Zarządzania Bezpieczeństwem Informacji oraz audyt końcowy (1 kpl)**

kod CPV 72222000-7 Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej   
oraz usługi w zakresie planowania

kod CPV 72224100-2 Usługi w zakresie planowania wdrażania systemu

kod CPV 72212781-7 Usługi opracowywania oprogramowania do zarządzania systemem

**Zakres wdrożenia Systemu zarządzania bezpieczeństwem informacji (SZBI):**

Wdrożenie SZBI będzie obejmowało kilka kluczowych etapów:

1. Audyt wstępny ISO/IEC 27001– ocena obecnego stanu bezpieczeństwa informacji

2. Analiza ryzyka – identyfikacja i ocena zagrożeń dla informacji oraz określenie odpowiednich środków zaradczych. W ramach analizy ryzyka weryfikacja obecnych oraz planowanie nowych środków zabezpieczenia technicznego – np. systemów klasy EDR/XDR, zapór NGFW, systemów zarządzania kopiami bezpieczeństwa systemów logowania zdarzeń oraz zarządzania podatnościami itp.

3. Opracowanie dokumentacji SZBI – stworzenie polityk, procedur i instrukcji dotyczących zarządzania bezpieczeństwem informacji, w tym:

a) Polityki/procedury/instrukcji zarządzania dostępem i uprawnieniami;

b) Polityki/procedury/instrukcji kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania;

c) Polityki/procedury/instrukcji zarządzania podatnościami;

d) Polityki/procedury/instrukcji zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa;

e) Polityki/procedury/instrukcji logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolera domeny;

f) Polityki/procedury/instrukcji kopii bezpieczeństwa;

g) Polityki/procedury/instrukcji zarządzania incydentami bezpieczeństwa;

h) Polityki/procedury/instrukcji zarządzania ciągłością działania;

i) Polityki/procedury/instrukcji ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych.

4. Szkolenia personelu – przeszkolenie pracowników w zakresie nowych procedur i zasad bezpieczeństwa informacji (2 szkolenia stacjonarne pracowników w siedzibie firmy).

5. Wdrożenie i monitorowanie – implementacja SZBI oraz zasad ciągłego monitorowanie jego skuteczności oraz wprowadzania niezbędnych usprawnień.

Wymagania do spełnienia przez oferenta:

Zamawiający uzna, że Wykonawca spełnia warunek w zakresie zdolności technicznej lub zawodowej, jeżeli Wykonawca wykaże, że: dysponuje audytorem posiadającym uprawnienia na podstawie certyfikatów wskazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077 ze zm.). Audytorem wykonującym zadania w ramach wdrożenia ZSBI musi być osoba wskazana przez Wykonawca w dokumentach w ramach postępowania.

Wykaz certyfikatów wskazanych w w/w rozporządzeniu:

\* Certified Internal Auditor (CIA);

\* Certified Information System Auditor (CISA);

\* Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy   
z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398   
oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;

\* Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r.   
o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

\* Certified Information Security Manager (CISM);

\* Certified in Risk and Information Systems Control (CRISC);

\* Certified in the Governance of Enterprise IT (CGEIT);

\* Certified Information Systems Security Professional (CISSP);

\* Systems Security Certified Practitioner (SSCP);

\* Certified Reliability Professional;

\* Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Termin realizacji zadania - do dnia 30.03.2026 r.

**Zadanie nr 2 Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny) - (1 kpl)**

kod CPV 80550000-4 Usługi szkolenia w dziedzinie bezpieczeństwa

kod CPV 80510000-2 Usługi szkolenia specjalistycznego

kod CPV 79632000-3 Szkolenie pracowników

Opis ogólny:

Przedmiotem zamówienia jest przeprowadzenie serii szkoleń dla pracowników Zamawiającego.

Celem szkolenia jest:

1. Poszerzenie praktycznej wiedzy z zakresu cyberbezpieczeństwa oraz podniesienie świadomości odnośnie bezpieczeństwa informatycznego.

2. Przybliżenie uczestnikom, zagrożeń bezpieczeństwa informacji jak i sposobów obrony przed nimi   
Zamawiający wymaga przeprowadzenia szkolenia dla wyznaczonych pracowników. Zamawiający   
nie dopuszcza szkolenia w formie e-learningu.

Szkolenie powinno trwać 2 godziny lekcyjne dla jednego bloku szkoleniowego.

Wymóg 4 szkoleń dla kadry kierowniczej:

- 2 terminy stacjonarne,

- 2 terminy zdalnie.

Dodatkowo 7 szkoleń dla biurowej i medycznej:

- 3 terminy stacjonarne,

- 4 terminy zdalne.

Ramowy program szkolenia dla kadry kierowniczej powinien obejmować (ostateczny zakres do akceptacji Zamawiającego):

* Cyberzagrożenia i cyberprzestępczość
* Podstawy prawne w obszarze cyberbezpieczeństwa
* Typów ataków
* Reagowanie na incydenty
* Wykonywania badań bezpieczeństwa
* Omówienie roli kadry zarządzającej w procesach bezpieczeństwa
* Obowiązki operatorów usług kluczowych
* Jak przygotować instytucję na ataki hakerskie czy kradzież środków pieniężnych
* Rozwiązania teleinformatyczne dla cyberbezpieczeństwa
* Rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestępczością
* Zagrożenia bezpieczeństwa i klasyfikacja
* Rodzaje złośliwego oprogramowania
* Najpopularniejsze zagrożenia w ostatnim czasie
* Co to jest Ransomware i jak chronić się przed Ransomware
* Bezpieczne korzystanie z www i e-mail
* Bankowość i Płatności Online
* Prywatność w Internecie
* Bezpieczeństwo na portalach społecznościowych
* Szyfrowanie
* Zagrożenia mobilne
* Zarządzanie hasłami dostępowymi
* Ciemne zakątki Internetu
* Backup danych i bezpieczne usuwanie danych
* Fake News i jak go rozpoznać
* Dobre praktyki i zasady bezpiecznego używania komputerów

Ramowy program szkolenia dla kadry biurowej i medycznej, powinien obejmować (ostateczny zakres   
do akceptacji Zamawiającego):

* Cyberzagrożenia i cyberprzestępczość
* Typów ataków wraz z przykładami
* Reagowanie na incydenty
* Jak przygotować instytucję na ataki hakerskie czy kradzież środków pieniężnych
* Rozwiązania teleinformatyczne dla cyberbezpieczeństwa
* Rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestępczością
* Zagrożenia bezpieczeństwa i klasyfikacja
* Rodzaje złośliwego oprogramowania
* Najpopularniejsze zagrożenia w ostatnim czasie
* Co to jest Ransomware i jak chronić się przed Ransomware
* Bezpieczne korzystanie z www i e-mail
* Bankowość i Płatności Online
* Prywatność w Internecie
* Bezpieczeństwo na portalach społecznościowych
* Szyfrowanie
* Zagrożenia mobilne
* Zarządzanie hasłami dostępowymi
* Ciemne zakątki Internetu
* Backup danych i bezpieczne usuwanie danych
* Fake News i jak go rozpoznać
* Dobre praktyki i zasady bezpiecznego używania komputerów

Wykonawca powinien:

* Zapewnić materiały dydaktyczne w formie elektronicznej dla każdego uczestnika.
* Zapewnić realizację szkolenia w formie wykładu połączonego z warsztatami wykorzystującymi ćwiczenia indywidualne i grupowe, burzę mózgów, case studies, z zastosowaniem technik multimedialnych oraz dyskusję.
* Zapewnić osobę trenera lub trenerów, którzy posiadają adekwatne do tematu szkolenia wiedzę   
  i doświadczenie.

Trener prowadzący szkolenie powinien posiadać jeden z certyfikatów:

* Certified Internal Auditor (CIA);
* Certified Information System Auditor (CISA);
* Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie   
  z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
* Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301   
  wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy   
  z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
* Certified Information Security Manager (CISM);
* Certified in Risk and Information Systems Control (CRISC);
* Certified in the Governance of Enterprise IT (CGEIT);
* Certified Information Systems Security Professional (CISSP);
* Systems Security Certified Practitioner (SSCP);
* Certified Reliability Professional;
* Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Zamawiający uzna, że warunek jest spełniony po przedstawieniu aktualnego minimum jednego   
z powyższych certyfikatów dla osoby/osób prowadzących szkolenie.

Termin realizacji zadania - do dnia 30.04.2026 r.

**Zadanie nr 3 EDR/XDR - Zakup oprogramowania zapewniającego pełną ochronę zgodną z zakresem (docelowa liczba stanowisk: 170) - (1 kpl)**

kod CPV [48730000-4](https://www.google.com/search?client=firefox-b-d&sca_esv=50bc830c1331a679&cs=0&q=48730000-4&sa=X&ved=2ahUKEwiLs6-yn8KQAxXhQvEDHdPlCIQQxccNegQIDhAB&mstk=AUtExfAMfId3OJkYlmIQR-rrvVmPip9odA3rcWOltyhFBlkEWBL6-ZrwzlIhD_MjLhWuQV66Q0tCwqSUAwcnpvuAWvilwxL0JckyRnMvTDoHlsEKcDjSAh3S9FTOXVqei0QUVkI&csui=3) Pakiety oprogramowania zabezpieczającego

kod CPV [48732000-8](https://www.google.com/search?client=firefox-b-d&sca_esv=50bc830c1331a679&cs=0&q=48732000-8&sa=X&ved=2ahUKEwiLs6-yn8KQAxXhQvEDHdPlCIQQxccNegQIDxAB&mstk=AUtExfAMfId3OJkYlmIQR-rrvVmPip9odA3rcWOltyhFBlkEWBL6-ZrwzlIhD_MjLhWuQV66Q0tCwqSUAwcnpvuAWvilwxL0JckyRnMvTDoHlsEKcDjSAh3S9FTOXVqei0QUVkI&csui=3) Pakiety oprogramowania do zabezpieczania danych

kod CPV [48219100-7](https://www.google.com/search?client=firefox-b-d&sca_esv=50bc830c1331a679&cs=0&q=48219100-7&sa=X&ved=2ahUKEwiLs6-yn8KQAxXhQvEDHdPlCIQQxccNegQIEBAB&mstk=AUtExfAMfId3OJkYlmIQR-rrvVmPip9odA3rcWOltyhFBlkEWBL6-ZrwzlIhD_MjLhWuQV66Q0tCwqSUAwcnpvuAWvilwxL0JckyRnMvTDoHlsEKcDjSAh3S9FTOXVqei0QUVkI&csui=3) Pakiety oprogramowania bramowego

kod CPV [72263000-6](https://www.google.com/search?client=firefox-b-d&sca_esv=50bc830c1331a679&cs=0&q=72263000-6&sa=X&ved=2ahUKEwiLs6-yn8KQAxXhQvEDHdPlCIQQxccNegQIEhAB&mstk=AUtExfAMfId3OJkYlmIQR-rrvVmPip9odA3rcWOltyhFBlkEWBL6-ZrwzlIhD_MjLhWuQV66Q0tCwqSUAwcnpvuAWvilwxL0JckyRnMvTDoHlsEKcDjSAh3S9FTOXVqei0QUVkI&csui=3) Usługi wdrażania oprogramowania

Opis ogólny:

Zakup rozbudowy/rozszerzenia subskrypcji oprogramowania do zarządzania bezpieczeństwem punktów końcowych wraz z narzędziem do wykrywania i reagowania na incydenty: oprogramowanie ESET Protect Enterprise.

Docelowa liczba stanowisk: 170

Licencja zostaje przedłużona o 36 miesięcy.

Opis modułu EDR:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Konsola zarządzania WWW | Dostęp do konsoli centralnego zarządzania realizowany jest przez interfejs WWW. |  |  |
| 2 | Integracja zdarzeń | Serwer administracyjny umożliwia wysyłanie zdarzeń do konsoli administracyjnej tego samego producenta. |  |  |
| 3 | Zabezpieczenie SSL | Interfejs do zarządzania zabezpieczony jest protokołem SSL. |  |  |
| 4 | Wykluczanie alarmów | Serwer administracyjny umożliwia wprowadzanie wykluczeń, które zapobiegają wyzwoleniu alarmu bezpieczeństwa. |  |  |
| 5 | Zakres wykluczeń | Wykluczenia obejmują proces lub proces „rodzica”. |  |  |
| 6 | Automatyczne rozwiązywanie alarmów | Utworzenie wykluczenia automatycznie rozwiązuje powiązane alarmy bezpieczeństwa. |  |  |
| 7 | Konfiguracja kryteriów wykluczeń | Kryteria wykluczeń konfigurowane min. po: nazwie procesu, ścieżce, wierszu polecenia, wydawcy, typie podpisu, SHA-1, nazwie komputera, grupie, użytkowniku. |  |  |
| 8 | Reguły bezpieczeństwa | Serwer zawiera ponad 900 wbudowanych reguł wyzwalających alarm i zapewnia możliwość tworzenia i edycji własnych reguł przez administratora. |  |  |
| 9 | Blokowanie po sumie kontrolnej | Możliwość blokowania plików na podstawie sumy kontrolnej (SHA-1) wraz z dodaniem komentarza i konfiguracją reakcji na zdarzenie. |  |  |
| 10 | Analiza procesów | Możliwość weryfikacji uruchomionych plików na stacji roboczej z podglądem: SHA-1, typ podpisu, wydawca, opis, wersje i nazwy, rozmiar, reputacja i popularność pliku. |  |  |
| 11 | Operacje na plikach i bibliotekach | Oznaczenie plików wykonywalnych i DLL jako bezpieczne, pobranie ich do analizy lub zablokowanie. |  |  |
| 12 | Weryfikacja i klasyfikacja skryptów | Możliwość weryfikacji uruchamianych skryptów z informacją o parametrach, oznaczenie jako bezpieczne/niebezpieczne. |  |  |
| 13 | Szczegóły wykonania skryptu | Szczegółowy podgląd czynności wykonanych przez skrypt dostępny w formie tekstowej. |  |  |
| 14 | Powiązane zdarzenia procesu | Możliwość weryfikacji powiązanych zdarzeń (modyfikacje plików, rejestru, połączenia sieciowe, pliki wykonywalne) dla skryptu  lub pliku exe. |  |  |
| 15 | Przekierowanie do konsoli AV | Przekierowanie do konsoli zarządzającej produktu antywirusowego tego samego producenta w celu analizy stacji roboczej oraz wglądu w sprzęt, podzespoły i zainstalowane oprogramowanie. |  |  |
| 16 | Tagowanie obiektów | Możliwość tagowania dowolnych obiektów  w konsoli administracyjnej. |  |  |
| 17 | Zdalne polecenia powershell | Możliwość zdalnego połączenia się do stacji roboczej i wykonywania poleceń powershell bezpośrednio z konsoli XDR. |  |  |

Wymagania szczegółowe:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Automatyczne tworzenie incydentów  z wizualizacją | System sam agreguje powiązane wykrycia, procesy i zasoby w logiczny "Incident", prezentując oś czasu i relacje między zdarzeniami. |  |  |
| 2 | Terminal Live Response | Wbudowana powłoka zdalna (PowerShell/Bash) umożliwia interaktywne polecenia na odizolowanym hoście, działa  w czasie zbliżonym do rzeczywistego. |  |  |
| 3 | Izolacja hosta | Możliwość natychmiastowego odcięcia zainfekowanego komputera od sieci  (z wyjątkiem komunikacji z produktami ESET). |  |  |
| 4 | Scoring incydentów  i priorytetyzacja | Każdemu alarmowi przypisywana jest liczba punktów (Severity Score 1-100), a komputery są rankowane według łącznej wagi incydentów. |  |  |
| 5 | Mapowanie do MITRE | Każda reguła i wykrycie zawiera odniesienie  do taktyk i technik. |  |  |
| 6 | Learning Mode (uczenie środowiska) | Tymczasowo uczy się typowych zachowań  w organizacji i proponuje automatyczne wykluczenia, aby zredukować fałszywe alarmy. |  |  |
| 7 | Anomalia użytkownika / polityki firmowej | Reguły wykrywające naruszenia polityk  (np. TOR, klienci P2P, nieszyfrowane dyski USB). |  |  |
| 8 | Monitorowanie API Win32 / Canary Files | Inspektor rejestruje wybrane wywołania API  i monitoruje pliki-wabiki (canary) do detekcji ransomware. |  |  |
| 9 | Integracja SIEM/SOAR przez REST API  i Syslog | Publiczne API (Swagger) oraz eksport Syslog umożliwiają streaming zdarzeń do Splunk, QRadar, Azure Sentinel itp. |  |  |
| 10 | Uczenie reguł i edycja XML | Ponad 900 reguł można modyfikować lub pisać własne w pełni transparentnym formacie XML. |  |  |
| 11 | IoC Search & Threat Hunting | Zaawansowane zapytania (hash, domena, IP, patterny czasowe) — z obsługą operatorów logicznych i wildcardów. |  |  |
| 12 | Blokowanie modułów DLL i bibliotek | Oprócz plików .exe można blokować pojedyncze moduły DLL w całej flocie. |  |  |
| 13 | Rozbudowane filtry i tagowanie | Setki pól (np. Reputation, Company Name, File Version, Rule Name) + globalne tagi współdzielone między użytkownikami. |  |  |
| 14 | Korelacja z LiveGrid® (reputacja 110 mln endpointów) | Każdy plik oceniany jest punktacją 1–9  na podstawie globalnej reputacji i popularności. |  |  |
| 15 | Publiczny feed zdarzeń do automatyzacji | Możliwość triggerowania zewnętrznych procesów (np. SOAR) po zdarzeniu poprzez web-hooki/API. |  |  |
| 16 | Submit to LiveGuard  z poziomu konsoli | Jednym kliknięciem można wysłać dowolny plik do chmurowej analizy sandboxingowej. |  |  |
| 17 | Obsługa 25 000 endpointów w jednym tenant'cie | Rozwiązanie skalowalne w modelu cloud, automatycznie zarządza certyfikatami i retencją danych. |  |  |
| 18 | Priorytetowe mutowanie reguł (auto-mute) | Przy nadmiernej liczbie alarmów dana reguła jest automatycznie wyciszana na 24 h  dla konkretnej maszyny. |  |  |

Sandbox

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Ochrona przed zagrożeniami 0-day | Rozwiązanie musi zapewniać ochronę przed zagrożeniami typu 0-day. |  |  |
| 2 | Wykorzystanie chmury producenta | Rozwiązanie musi wykorzystywać do działania chmurę producenta. |  |  |
| 3 | Automatyczne przesyłanie plików | Możliwość określenia, jakie pliki mają być przesyłane automatycznie do chmury, w tym: archiwa, skrypty, pliki wykonywalne, potencjalny spam, dokumenty, pliki .jar, .reg, .msi. |  |  |
| 4 | Czas przechowywania plików | Administrator definiuje, po jakim czasie przesłane pliki muszą zostać usunięte  z serwerów producenta. |  |  |
| 5 | Ograniczenie rozmiaru próbek | Administrator definiuje maksymalny rozmiar przesyłanych próbek. |  |  |
| 6 | Lista wykluczeń | Możliwość utworzenia listy wykluczeń plików lub folderów z przesyłania do chmury. |  |  |
| 7 | Przesyłanie wyników analizy | Po analizie pliku wynik jest przekazywany  do wszystkich wspieranych produktów. |  |  |
| 8 | Podgląd wysłanych plików | Administrator może podejrzeć listę plików przesłanych do analizy. |  |  |
| 9 | Analiza niezależna od lokalizacji | Możliwość analizy plików niezależnie od lokalizacji stacji roboczej, w razie wykrycia zagrożenia całe środowisko jest bezzwłocznie chronione. |  |  |
| 10 | Brak dodatkowego agenta | Rozwiązanie nie wymaga instalacji dodatkowego agenta na stacjach roboczych. |  |  |
| 11 | Wysyłka próbek przez użytkownika lub admina | Możliwość wysłania dowolnej próbki przez użytkownika lub administratora, możliwość podglądu, jakie pliki i przez kogo zostały wysłane do analizy. |  |  |
| 12 | Klasyfikacja przeanalizowanych plików | Przeanalizowane pliki muszą być oznaczone: czysty, podejrzany, bardzo podejrzany, szkodliwy. |  |  |
| 13 | Zatrzymywanie niepewnych plików | Dla stacji roboczych – możliwość wstrzymania uruchamiania pobieranych plików poprzez przeglądarkę, pocztę e-mail, nośniki wymienne lub wyodrębnione z archiwum. |  |  |
| 14 | Wstrzymanie poczty do końca analizy | Dla serwerów pocztowych – możliwość wstrzymania dostarczania wiadomości do czasu zakończenia analizy próbki. |  |  |
| 15 | Kwarantanna | Wszystkie wykryte zagrożenia muszą być przenoszone do bezpiecznego obszaru kwarantanny, z którego administrator może  je przywrócić i utworzyć wyłączenia dla kwarantanny. |  |  |

Panel administracyjny

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Dostępność w chmurze | Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. |  |  |
| 2 | Konsola zarządzania WWW | Rozwiązanie musi umożliwiać dostęp  do konsoli centralnego zarządzania z poziomu interfejsu WWW. |  |  |
| 3 | Bezpieczeństwo SSL | Rozwiązanie musi być zabezpieczone  za pośrednictwem protokołu SSL. |  |  |
| 4 | Wykrywanie klonów stacji | Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny  na podstawie unikatowego identyfikatora sprzętowego stacji. |  |  |
| 5 | HTTP Proxy | Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. |  |  |
| 6 | MDM | Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. |  |  |
| 7 | Dwufazowa autoryzacja | Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. |  |  |
| 8 | Uprawnienia użytkowników | Możliwość dodania zestawu uprawnień  dla użytkowników w oparciu co najmniej  o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. |  |  |
| 9 | Szablony raportów | Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. |  |  |
| 10 | Grupy komputerów | Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. |  |  |
| 11 | Szablony grup dynamicznych | Grupy dynamiczne muszą być tworzone  na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan ochrony, wersja systemu operacyjnego oraz podzespoły komputera. |  |  |
| 12 | Automatyzacja zadań | Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta  w grupie dynamicznej. |  |  |

Ochrona stacji roboczych

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Wsparcie dla Windows 10/11 | Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). |  |  |
| 2 | Wsparcie dla ARM64 | Rozwiązanie musi wspierać architekturę ARM64. |  |  |
| 3 | Detekcja zagrożeń | Rozwiązanie musi wykrywać i usuwać adware, spyware, dialer, phishing, narzędzia hakerskie, backdoor. |  |  |
| 4 | Ochrona przed rootkitami i botnetami | Rozwiązanie musi mieć wbudowaną technologię ochrony przed rootkitami i podłączeniem do sieci botnet. |  |  |
| 5 | Wykrywanie niepożądanych aplikacji | Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne i podejrzane aplikacje. |  |  |
| 6 | Ochrona on-access | Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. |  |  |
| 7 | Skanowanie na żądanie i wg harmonogramu | Skanowanie całego dysku, wybranych katalogów lub plików na żądanie lub zgodnie  z harmonogramem. |  |  |
| 8 | Skanowanie plików spakowanych i dysków zewnętrznych | Skanowanie plików spakowanych, skompresowanych, dysków sieciowych  i przenośnych. |  |  |
| 9 | Wykluczenia ze skanowania | Możliwość wykluczenia plików/katalogów  ze skanowania na podstawie rozszerzenia, nazwy, sumy SHA1 i lokalizacji. |  |  |
| 10 | Integracja z Intel TDT | Rozwiązanie musi integrować się z Intel Threat Detection Technology. |  |  |
| 11 | Skanowanie poczty POP3/IMAP | Skanowanie i oczyszczanie poczty przychodzącej POP3/IMAP „w locie”,  przed dostarczeniem do klienta pocztowego. |  |  |
| 12 | Skanowanie szyfrowanego ruchu sieciowego | Skanowanie ruchu sieciowego w protokołach HTTPS, POP3S, IMAPS. |  |  |
| 13 | Zaawansowana heurystyka i AI | Dwa moduły heurystyczne: pasywny  i aktywny, AI, możliwość wyboru trybu skanowania. |  |  |
| 14 | Blokowanie nośników/urządzeń | Blokowanie zewnętrznych nośników: pamięci masowe, optyczne, Firewire, urządzenia obrazujące, drukarki USB, Bluetooth, smartcard, modemów, LPT/COM, urządzeń przenośnych. |  |  |
| 15 | Reguły blokowania urządzeń | Funkcja umożliwiająca reguły blokowania nośników/urządzeń według typu, numeru seryjnego, dostawcy, modelu. |  |  |
| 16 | Moduł HIPS – tryby pracy | 5 trybów HIPS: automatyczny, interaktywny, oparty na regułach, uczenia się (z automatycznym przełączaniem), inteligentny (powiadamia o podejrzanych działaniach). |  |  |
| 17 | Raportowanie o stacji roboczej | Funkcja generująca szczegółowy raport (zainstalowane aplikacje, usługi, system, sprzęt, procesy, połączenia sieciowe, harmonogram, hosts, sterowniki). |  |  |
| 18 | Filtrowanie wyników raportu | Raportowanie z minimum 9 poziomami filtrowania pod kątem zagrożeń. |  |  |
| 19 | Automatyczna aktualizacja | Automatyczna, inkrementacyjna aktualizacja silnika detekcji. |  |  |
| 20 | Jeden proces w pamięci | Tylko jeden proces w pamięci obsługuje wszystkie funkcje (AV, antyspyware, heurystyka). |  |  |
| 21 | Skaner UEFI | Funkcjonalność skanera UEFI wykrywającego zagrożenia przed startem systemu operacyjnego. |  |  |
| 22 | Antyspam dla Outlooka | Ochrona antyspamowa dla programu pocztowego Microsoft Outlook. |  |  |
| 23 | Tryby zapory osobistej | 4 tryby zapory: automatyczny (blokuje ruch przychodzący), interaktywny (pyta o każde połączenie), oparty na regułach, uczenia się (admin konfiguruje czas). |  |  |
| 24 | Moduł bezpiecznej przeglądarki | Rozwiązanie musi mieć wbudowany moduł bezpiecznej przeglądarki. |  |  |
| 25 | Szyfrowanie danych w przeglądarce | Przeglądarka automatycznie szyfruje wszelkie dane wprowadzane przez użytkownika. |  |  |
| 26 | Wizualne wyróżnienie bezpiecznej przeglądarki | Praca w bezpiecznej przeglądarce ma być wyróżniona (kolor ramki, informacja  na ramce). |  |  |
| 27 | Kontrola WWW | Zintegrowany moduł kontroli dostępu do stron internetowych. |  |  |
| 28 | Filtrowanie stron WWW | Filtrowanie adresów URL na podstawie  co najmniej 140 kategorii/podkategorii. |  |  |
| 29 | Ochrona przed 0-day | Ochrona przed zagrożeniami typu zero-day. |  |  |
| 30 | Blokada uruchamiania podejrzanych plików | Wstrzymanie uruchamiania pobieranych plików (przeglądarki, klient poczty, nośniki, archiwa) na stacjach roboczych. |  |  |

Ochrona serwera

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Wieloplatformowość serwerów | Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux, w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. |  |  |
| 2 | Ochrona przed złośliwym oprogramowaniem | Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. |  |  |
| 3 | Detekcja niebezpiecznych aplikacji | Rozwiązanie musi zapewniać wykrywanie  i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich i backdoor. |  |  |
| 4 | Skanowanie NAS | Rozwiązanie musi umożliwiać skanowanie dysków sieciowych typu NAS. |  |  |
| 5 | Podwójna heurystyka  i AI | Musi posiadać dwa niezależne moduły heurystyczne: jeden oparty na metodach pasywnych, drugi na aktywnych oraz elementach sztucznej inteligencji. Administrator musi mieć możliwość wyboru, z jaką heurystyką będzie realizowane skanowanie (jedna lub obie naraz). |  |  |
| 6 | Automatyczna aktualizacja | Wspierana musi być automatyczna, inkrementacyjna aktualizacja silnika detekcji. |  |  |
| 7 | Wykluczanie procesów  z ochrony | Rozwiązanie musi zapewniać możliwość wykluczania procesów ze skanowania. |  |  |
| 8 | Przesyłanie podejrzanych plików | Możliwość określania typów podejrzanych plików kierowanych do producenta  (co najmniej wykonywalne, archiwa, skrypty, dokumenty). |  |  |
| 9 | Skanowanie chmury OneDrive (Windows) | Możliwość skanowania plików i folderów umieszczonych w usłudze chmurowej OneDrive. |  |  |
| 10 | Host-based Intrusion Prevention System (HIPS, Windows) | System zapobiegania włamaniom działający na hoście musi być zaimplementowany. |  |  |
| 11 | Skanowanie Hyper-V (Windows) | Wspierane musi być skanowanie magazynu Hyper-V. |  |  |
| 12 | Skaner UEFI (Windows) | Funkcja skanowania UEFI chroniąca przed zagrożeniami uruchamianymi przed startem systemu operacyjnego. |  |  |
| 13 | Blokada nośników zewnętrznych (Windows) | Możliwość blokowania zewnętrznych nośników danych: pamięci masowych, optycznych, Firewire, urządzeń do tworzenia obrazów, drukarek USB, Bluetooth, smartcard, modemów, portów LPT/COM, urządzeń przenośnych. |  |  |
| 14 | Auto-wyjątki dla usług serwera (Windows) | Automatyczne wykrywanie usług zainstalowanych na serwerze i generowanie dla nich odpowiednich wyjątków w regułach. |  |  |
| 15 | IDS – wykrywanie ataków/anomalii (Windows) | Wbudowany system IDS do detekcji prób ataków, anomalii sieciowych oraz aktywności wirusów sieciowych. |  |  |
| 16 | Wyjątki IDS (Windows) | Możliwość dodania wyjątków w systemie IDS na podstawie: alertu, kierunku, aplikacji, czynności oraz adresu IP. |  |  |
| 17 | Ochrona przed ransomware (Windows) | Dedykowany moduł ochrony przed oprogramowaniem wymuszającym okup. |  |  |
| 18 | Lokalna konsola administracyjna (Linux) | Możliwość uruchomienia lokalnej konsoli administracyjnej przez przeglądarkę internetową. |  |  |
| 19 | Brak wymogu zewnętrznego serwera WWW (Linux) | Konsola administracyjna nie wymaga uruchomienia/instalacji usługi serwera Web. |  |  |
| 20 | Skanowanie EMC Isilon (Linux) | Możliwość pełnego wsparcia dla Dell EMC Isilon przy skanowaniu macierzy NAS/SAN. |  |  |
| 21 | Architektura mikroserwisowa (Linux) | System musi działać w architekturze mikroserwisów – awaria jednego komponentu nie przerywa pracy całości, lecz powoduje restart tylko danego mikroserwisu. |  |  |

Szyfrowanie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Wsparcie dla Windows 10/11 | System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. |  |  |
| 2 | Wsparcie dla macOS FileVault | System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem  w systemach macOS (FileVault). |  |  |
| 3 | Autentykacja Pre-boot | Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny, z możliwością całkowitego  lub czasowego wyłączenia tego uwierzytelnienia. |  |  |
| 4 | Szyfrowanie na UEFI | Aplikacja musi umożliwiać szyfrowanie danych na komputerach wyposażonych  w UEFI. |  |  |

Ochrona urządzeń mobilnych opartych o system Android

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Skanowanie wszystkich typów plików | Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno  w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. |  |  |
| 2 | Poziomy skanowania | Rozwiązanie musi umożliwiać co najmniej  2 poziomy skanowania: inteligentne oraz dokładne. |  |  |
| 3 | Skanowanie w trybie bezczynności | Rozwiązanie musi automatycznie uruchamiać skanowanie, gdy urządzenie jest w trybie bezczynności (w pełni naładowane  i podłączone do ładowarki). |  |  |
| 4 | Konfiguracja zaufanej karty SIM | Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. |  |  |
| 5 | Komendy zdalne z konsoli | Rozwiązanie musi umożliwiać wysłanie  na urządzenie komend z konsoli centralnego zarządzania: usunięcie zawartości urządzenia, przywrócenie do ustawień fabrycznych, zablokowanie urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. |  |  |
| 6 | Podgląd zainstalowanych aplikacji | Rozwiązanie musi zapewniać administratorowi możliwość podejrzenia listy zainstalowanych aplikacji na urządzeniu. |  |  |
| 7 | Blokowanie aplikacji | Rozwiązanie musi umożliwiać blokowanie aplikacji na podstawie: nazwy aplikacji, nazwy pakietu, kategorii sklepu Google Play, uprawnień aplikacji oraz pochodzenia aplikacji z nieznanego źródła. |  |  |

Wymaganie dodatkowe (usługi wdrożenia oraz utrzymania):

W ramach oferty wykonawca zapewni 300 rbh pracy inżyniera w poniższym zakresie.

* Pełne udokumentowanie wdrożonego rozwiązania, potwierdzająca zastosowanie polityk bezpieczeństwa oraz wdrożenie agentów rozwiązania na stacjach roboczych oraz serwerach
* Dodawanie oraz zarządzanie licencjami na produkty ESET.
* Instalacja oraz konfiguracja agentów ESET Management na urządzeniach.
* Tworzenie, wdrażanie i egzekwowanie polityk bezpieczeństwa dla komputerów i serwerów.
* Uruchamianie zadań administracyjnych: instalacja, aktualizacja, dezinstalacja oprogramowania,   
  skanowania na żądanie.
* Monitorowanie stanu zabezpieczeń, generowanie raportów oraz analiza wykrytych zagrożeń.
* Zarządzanie użytkownikami i grupami – przypisywanie uprawnień, tworzenie kont, wdrażanie uwierzytelniania dwuskładnikowego.
* Reagowanie na incydenty, w tym zdalna blokada urządzeń i inicjowanie skanowania lub aktualizacji.
* Usuwanie aplikacji antywirusowych innych firm oraz zarządzanie produktami endpoint.
* Tworzenie i zarządzanie dynamicznymi grupami urządzeń dla efektywnej administracji środowiskiem.
* Automatyzacja czynności, planowanie raportów i powiadomień o statusie urządzeń.
* Analiza wykrytych zagrożeń i elementów znajdujących się w kwarantannie.
* Przegląd incydentów bezpieczeństwa. Zdalna blokada urządzeń oraz inicjowanie skanowania lub aktualizacji.
* Identyfikacja komputerów i użytkowników z największą liczbą incydentów.
* Skanowanie w poszukiwaniu luk w zabezpieczeniach systemu operacyjnego i aplikacji.
* Zarządzanie poprawkami bezpieczeństwa z automatycznymi aktualizacjami.
* Ustalanie priorytetów luk na podstawie ich ważności (informacyjne, ostrzegawcze, krytyczne).
* Harmonogramowanie regularnego skanowania w poszukiwaniu luk w zabezpieczeniach.
* Integracja z narzędziami systemami zgłaszania problemów.
* Konfiguracja i utrzymanie systemu dla dystrybucji aktualizacji i komunikacji z agentami.
* Zarządzanie szyfrowaniem ESET Full Disc Encryption.
* Obsługa rozwiązania ESET Inspect dla zaawansowanego wykrywania zagrożeń.
* Wykrywanie i reagowanie na zagrożenia zero-day oraz ransomware.

**Czas reakcji na podjęcie działań na zgłoszenie zapotrzebowania na prace 4h.**

**Wymagania na inżyniera:**

Posiada wiedzę oraz szkolenia dotyczące zagadnień prawnych, organizacyjnych i technicznych związanych   
z ochroną teleinformatyczną, w tym w szczególności aktualnego stanu cyberzagrożeń oraz wymagań związanych z najnowszymi aktami prawnymi i nakładanych na podmioty zobowiązane, problematyką wdrożenia zasad Zero Trust, ewakuacji danych do chmury obliczeniowej i ochrony rozwiązań sztucznej inteligencji.

Zamawiający jako potwierdzenie spełnienia wymagań wymaga certyfikatu wystawionego   
na dane inżyniera wykonującego prace wdrożeniowe oraz zadania planowane w ramach postępowania.

Termin realizacji zadania

Czas na dostarczenie licencji i pełne udokumentowanie wdrożonego rozwiązania, potwierdzająca zastosowanie polityk bezpieczeństwa oraz wdrożenie agentów rozwiązania na stacjach roboczych   
oraz serwerach - 21 dni od dnia zawarcia Umowy.

**Zadanie nr 4 Zapory sieciowe - Zakup odnowienia subskrypcji i wsparcia technicznego dla posiadanych przez Zamawiającego urządzeń WatchGuard Firebox M290**

kod CPV 32420000-3 Urządzenia sieciowe

Opis ogólny

Zakup przedłużenia wsparcia producenta dla dwóch posiadanych urządzeń WatchGuard M290   
na okres 36 miesięcy.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Przedmiot zamówienia | Zakup odnowienia subskrypcji i wsparcia technicznego producenta WatchGuard  dla dwóch urządzeń Firebox M290 |  |  |
| 2 | Producent | WatchGuard Technologies |  |  |
| 3 | Model urządzeń | Firebox M290 (2 sztuki) |  |  |
| 4 | Typ wsparcia 1 | WatchGuard Total Security Suite Renewal/Upgrade – 3 lata |  |  |
| 5 | Zakres Total Security Suite | - Intrusion Prevention Service (IPS)  - Application Control  - WebBlocker (filtrowanie treści WWW)  - spamBlocker  - Gateway AntiVirus  - Reputation Enabled Defense  - Network Discovery  - APT Blocker (zaawansowana ochrona przed zagrożeniami)  - ThreatSync  - Data Loss Prevention  - DNSWatch  - IntelligentAV  - WatchGuard Cloud Visibility (pełna analiza zagrożeń)  - Support Standard 24x7 |  |  |
| 6 | Typ wsparcia 2 | WatchGuard Standard Support Renewal  – 3 lata |  |  |
| 7 | Zakres Standard Support | - Dostęp do aktualizacji i poprawek systemowych  - Dostęp do wsparcia technicznego producenta w trybie 24x7  - Dostęp do portalu wsparcia technicznego WatchGuard  - Dostęp do baz wiedzy i dokumentacji technicznej |  |  |
| 8 | Liczba urządzeń | 2 sztuki (dla każdego urządzenia osobna subskrypcja) |  |  |
| 9 | Czas trwania subskrypcji | 36 miesięcy (3 lata) dla każdej usługi |  |  |
| 10 | Wymagania dodatkowe | - Wsparcie musi być przypisane  do istniejących numerów seryjnych urządzeń Firebox M290  - Subskrypcje muszą pochodzić  z autoryzowanego kanału sprzedaży WatchGuard  - Sprzedawca zobowiązany jest do dostarczenia kodów aktywacyjnych  i potwierdzenia przypisania ich do właściwych urządzeń |  |  |

Termin realizacji zadania - w ciągu 7 dni od dnia zawarcia umowy.

**Zadanie nr 5 Zapory sieciowe - Zakup i dostawę dwóch sztuk zapór sieciowych (Firewall) wraz z niezbędnymi licencjami i wsparciem na 36 miesięcy**

kod CPV 32420000-3 Urządzenia sieciowe

Opis ogólny

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów   
w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

\* Firewall.

\* Ochrony w warstwie aplikacji.

\* Protokołów routingu dynamicznego.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| 1 | Model/ producent | Podać: |  |  |
| 2 | Redundancja, monitoring  i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.  2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  3. Monitoring stanu realizowanych połączeń VPN.  4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |  |
| 3 | Interfejsy, Dysk, Zasilanie | 1, System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  \* 10 portami Gigabit Ethernet RJ-45.  2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.  3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu  o standard 802.1Q.  D4. Wbudowana pamięć dyskowa SSD  o pojemności nie mniej niż 60GB. |  |  |
| 4 | Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 100 tys. nowych połączeń na sekundę.  2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.  3, Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.5 Gbps.  4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej  niż 4 Gbps.  5. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum  1 Gbps.  6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. |  |  |
| 5 | Funkcje Systemu Bezpieczeństwa | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:  1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  2. Kontrola Aplikacji.  3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.  4. Ochrona przed malware.  5. Ochrona przed atakami - Intrusion Prevention System.  6. Kontrola stron WWW.  7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.  8. Zarządzanie pasmem (QoS, Traffic shaping).  9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.  11. Możliwość filtrowania zapytań DNS  w ruchu przechodzącym przez system.  12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |  |  |
| 6 | Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  \* Translację jeden do jeden oraz jeden  do wielu.  \* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.  5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  6. Możliwość ustawienia przedziału czasu,  w którym dana reguła w politykach firewall jest aktywna.  7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  \* Amazon Web Services (AWS).  \* Microsoft Azure.  \* Cisco ACI.  \* Google Cloud Platform (GCP).  \* OpenStack.  \* VMware NSX.  \* Kubernetes. |  |  |
| 7 | Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  \* Wsparcie dla IKE v1 oraz v2.  \* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).  \* Obsługa protokołu Diffie-Hellman grup 19, 20.  \* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.  \* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.  \* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.  \* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.  \* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.  \* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.  \* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.  \* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.  \* Mechanizm „Split tunneling” dla połączeń Client-to-Site.  2, Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń VPN z oferowanym systemem. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |  |  |
| 8 | Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę:  1. Routingu statycznego.  2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).  3. Protokołów dynamicznego routingu  w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.  4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.  5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.  6. BFD (Bidirectional Forwarding Detection).  7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |  |  |
| 9 | Funkcje SD-WAN | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |  |  |
| 10 | Zarządzanie pasmem | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej  i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  2. System daje możliwość określania pasma dla poszczególnych aplikacji.  3. System pozwala zdefiniować pasmo  dla wybranych użytkowników niezależnie  od ich adresu IP.  4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |  |  |
| 11 | Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji  dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.  3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.  4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.  5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz  z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.  8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |  |  |
| 12 | Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.  3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.  5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).  7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |  |  |
| 13 | Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |  |  |
|  | Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.  3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.  4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).  6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.  7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.  9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |  |  |
| 14 | Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:  \* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.  \* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych  z LDAP.  \* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  2. System daje możliwość zastosowania  w tym procesie uwierzytelniania wieloskładnikowego.  3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.  4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |  |
| 15 | Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.  2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.  4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.  8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  9. Możliwość zarządzania systemem tylko  z określonych adresów źródłowych IP. |  |  |
| 16 | Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  4. Możliwość włączenia logowania per reguła w polityce firewall.  5. System zapewnia możliwość logowania  do serwera SYSLOG.  6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |  |  |
| 17 | Testy wydajnościowe oraz funkcjonalne | 1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane  w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. |  |  |
| 18 | Serwisy i licencje | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  a) Kontrola Aplikacji, IPS, Antywirus  (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.  b) Kontrola Aplikacji, IPS, Antywirus  (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |  |  |
| 19 | Gwarancja oraz wsparcie | 1. System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.  W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię. |  |  |

Termin realizacji zadania - w ciągu 30 dni od dnia zawarcia umowy.

**Zadanie nr 6 Zapory sieciowe - Wdrożenie, montaż, konfiguracja   
i dokumentacja powykonawcza zapór sieciowych wraz z zabezpieczeniami**

kod CPV 72700000-7 Usługi w zakresie sieci komputerowej

Opis ogólny

Wdrożenie, montaż, konfiguracja, wykonanie dokumentacji obecnego środowiska zapór sieciowych, dołączenie zakupionych zapór do obecnej infrastruktury, wykonane polityk bezpieczeństwa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Element** | **Opis szczegółowy** | **Potwierdzenie spełnienia parametru (tak/nie)** | **Wartość/opis oferowanego parametru** |
| **I. Wdrożenie, montaż, konfiguracja i dokumentacja powykonawcza zapór sieciowych wraz z zabezpieczeniami (1 kpl.)** | | | | |
| 1 | I. Etap przygotowawczy | Analiza środowiska IT klienta (topologia, polityki bezpieczeństwa, role zapór). |  |  |
| 2 | I. Etap przygotowawczy | Weryfikacja wymagań sprzętowych i środowiskowych (moc, chłodzenie, miejsce  w szafie rack). |  |  |
| 3 | I. Etap przygotowawczy | Opracowanie planu wdrożenia (harmonogram, plan migracji, plan testów). |  |  |
| 4 | II. Montaż fizyczny | Instalacja urządzeń w szafach rack. |  |  |
| 5 | II. Montaż fizyczny | Podłączenie zasilania oraz interfejsów sieciowych. |  |  |
| 6 | II. Montaż fizyczny | Etykietowanie kabli i portów. |  |  |
| 7 | III. Konfiguracja zapór | Backup aktualnej konfiguracji (dla istniejących zapór). |  |  |
| 8 | III. Konfiguracja zapór | Aktualizacja firmware’u (jeśli wymagane). |  |  |
| 9 | III. Konfiguracja zapór | Wstępna konfiguracja dostępu (adresacja IP, dostęp administracyjny). |  |  |
| 10 | III. Konfiguracja zapór | Konfiguracja stref, VLAN, tras, NAT, reguł ACL, UTM, VPN, HA. |  |  |
| 11 | III. Konfiguracja zapór | Wdrożenie polityki logowania i centralnego zarządzania. |  |  |
| 12 | III. Konfiguracja zapór | Weryfikacja zgodności z polityką bezpieczeństwa.  Integracja zapory z istniejącą infrastrukturą sieciową, przełącznki.  Przełączenie ruchu na nową zaporę. |  |  |
| 13 | IV. Testy | Test połączeń WAN/LAN/DMZ. |  |  |
| 14 | IV. Testy | Test dostępu do kluczowych zasobów. |  |  |
| 15 | IV. Testy | Symulacja ataków/testy bezpieczeństwa |  |  |
| 16 | IV. Testy | Test odtwarzania konfiguracji z backupu. |  |  |
| 17 | IV. Testy | Testy redundancji (jeśli HA). |  |  |
| 18 | V. Dokumentacja | Dokumentacja topologii logicznej i fizycznej. |  |  |
| 19 | V. Dokumentacja | Opis konfiguracji zapór. |  |  |
| 20 | V. Dokumentacja | Bezpieczne przekazanie haseł administracyjnych. |  |  |
| 21 | V. Dokumentacja | Procedury odzyskiwania konfiguracji. |  |  |
| 22 | V. Dokumentacja | Plan awaryjny (disaster recovery). |  |  |
| 23 | V. Dokumentacja | Protokół uruchomienia systemu. |  |  |
| 24 | VI. Szkolenie i przekazanie | Szkolenie administratorów (opcjonalnie). |  |  |
| 25 | VI. Szkolenie i przekazanie | Przekazanie dokumentacji oraz dostępów. |  |  |
| 26 | VI. Szkolenie i przekazanie | Sporządzenie i podpisanie protokołu odbioru. |  |  |
| **II. Przeprowadzenie testu potwierdzającego skuteczność wprowadzonych zabezpieczeń  i potwierdzającego zgodność konfiguracji z dokumentacją (1 kpl.)** | | | | |
| 1 | Polityki dostępu | Sprawdzenie działania reguł firewall (dozwolone/blokowane połączenia) |  |  |
| 2 | Polityki dostępu | Test poprawności działania NAT i przekierowań portów |  |  |
| 3 | VPN | Test zestawiania tunelu VPN site-to-site  oraz client-to-site |  |  |
| 4 | VPN | Weryfikacja szyfrowania VPN (np. AES 128/256) i dostępność zasobów |  |  |
| 5 | UTM / NGFW | Weryfikacja działania IPS/IDS – symulacja ataków testowych |  |  |
| 6 | UTM / NGFW | Sprawdzenie wykrycia testowego wirusa  (np. EICAR) przez moduł AV |  |  |
| 7 | UTM / NGFW | Test filtrowania stron internetowych  (np. blokowanie social media) |  |  |
| 8 | UTM / NGFW | Test kontroli aplikacji – blokowanie określonych aplikacji |  |  |
| 9 | UTM / NGFW | Weryfikacja działania SSL inspection  dla HTTPS |  |  |
| 10 | Redundancja / HA | Test przełączenia urządzenia w trybie HA  – awaria zapory głównej |  |  |
| 11 | Redundancja / HA | Weryfikacja działania monitoringu zapory (syslog, SNMP, SIEM) |  |  |
| 12 | Zgodność z dokumentacją | Porównanie aktywnej konfiguracji z dokumentacją (adresacja, ACL, VPN itd.) |  |  |
| 13 | Zgodność z dokumentacją | Weryfikacja konfiguracji kont, certyfikatów, haseł |  |  |
| 14 | Logowanie zdarzeń | Test rejestracji logów ruchu, blokad i operacji administracyjnych |  |  |
| 15 | Logowanie zdarzeń | Sprawdzenie przesyłania logów do systemów zewnętrznych (syslog, SIEM) |  |  |
| 16 | Bezpieczeństwo | Skanowanie podatności firewall  (np. Nessus/OpenVAS) |  |  |
| 17 | Bezpieczeństwo | Weryfikacja braku otwartych portów zarządzających z Internetu |  |  |
| 18 | Odporność na awarie | Symulacja odłączenia interfejsu lub urządzenia – test failover |  |  |
| 19 | Odporność na awarie | Test przywrócenia konfiguracji z backupu |  |  |
| 20 | Protokół testów | Sporządzenie i podpisanie protokołu testów powdrożeniowych |  |  |
| **III. Usługi utrzymania infrastruktury zapór sieciowych oraz sieci: 36 miesięcy (1 kpl.)** | | | | |
| 1 | Administracja i utrzymanie zapór sieciowych | \* Zarządzanie konfiguracją zapór (tworzenie, modyfikacja, usuwanie reguł bezpieczeństwa).  \* Wdrożenie polityki bezpieczeństwa zgodnie z wytycznymi klienta.  \* Tworzenie i utrzymywanie kopii zapasowych konfiguracji zapór.  \* Regularne przeglądy i optymalizacja konfiguracji (minimum raz na kwartał).  \* Zarządzanie certyfikatami i kluczami szyfrującymi |  |  |
| 2 | Monitorowanie i reagowanie | \* Monitorowanie stanu zapór i interfejsów  \* Reakcja na incydenty bezpieczeństwa 4h  od zgłoszenia i awarie w czasie nie dłuższym niż 1h.  \* Powiadamianie klienta o wykrytych anomaliach, atakach, nieautoryzowanym ruchu. |  |  |
| 3 | Zarządzanie aktualizacjami | \* Planowanie i wdrażanie aktualizacji oprogramowania zapór (firmware/patching)  w uzgodnionych terminach.  \* Testowanie zmian przed wdrożeniem  w środowisku produkcyjnym.  \* Zapewnienie zgodności z polityką bezpieczeństwa i wymaganiami producenta. |  |  |
| 4 | Zabezpieczenia i audyt | \* Wdrażanie i egzekwowanie polityk zabezpieczeń (np. IPS, filtrowanie URL, DPI).  \* Przeprowadzanie regularnych testów skuteczności reguł zapory (kwartalnie).  \* Sporządzanie raportów audytowych z logów systemowych i działań administracyjnych. |  |  |
| 5 | Dokumentacja | \* Prowadzenie aktualnej dokumentacji konfiguracji zapór.  \* Raporty z wykonanych działań administracyjnych (miesięczne).  \* Dokumentacja incydentów i działań naprawczych. |  |  |
| 6 | Wsparcie techniczne | \* Udzielanie konsultacji dotyczących konfiguracji i zmian architektonicznych.  \* Obsługa zgłoszeń serwisowych zgodnie  z ustalonym SLA (4h)  \* Doradztwo przy integracji zapór z innymi systemami bezpieczeństwa. |  |  |
| 7 | Wymagania organizacyjne | \* Zapewnienie nadmiarowości i procedur przywracania po awarii (disaster recovery).  \* Praca zgodna z wymaganiami RODO  i innymi przepisami prawa. |  |  |

Wymagania do spełnienia przez oferenta (wspólne dla Zadania nr 6):

1. Oferent powinien dysponować minimum dwiema osobami (**inżynier sieci, expert bezpieczeństwa**)   
z minimum 5-letnim doświadczeniem każda. Osoby te powinny być delegowane do pracy na rzecz Zamawiającego w całym okresie trwania umowy.

Wymaganie dla inżyniera sieci:

a) Minimum 5-letnie doświadczenie w świadczeniu usług wdrożeniowych i administracyjnych dla rozwiązań klasy Next Generation Firewall, w zakresie: filtracja aplikacyjna (App Control), system zapobiegania włamaniom (IPS/IDS), inspekcja SSL/TLS (SSL inspection), kontrola użytkowników (User-ID, integracja   
z AD), filtrowanie URL, ochrona przed malware i sandboxing.

Potwierdzeniem spełnienia wymagań będzie stanowiło dostarczenie do Zamawiającego referencji obejmujących wymagany zakres i okres doświadczenia zawodowego.

b) Doświadczenie w integracji NGFW z systemami SIEM i/lub EDR .

Potwierdzeniem spełnienia wymagań będzie stanowiło dostarczenie do Zamawiającego referencji obejmujących wymagany zakres.

c) Dobra znajomość przynajmniej jednego z wiodących producentów NGFW (np. Palo Alto Networks, Fortinet, Check Point, Cisco Firepower, Juniper, WatchGuard), potwierdzona certyfikatem ze ścieżki Security dotyczące Next Generation Firewall.

Potwierdzeniem spełnienia wymogów będzie stanowiło dostarczenie do Zamawiającego certyfikatu producenta NGFW wystawionego na dane osoby delegowanej do pracy na rzecz Zamawiającego.

d) Minimum 5-letnie doświadczenie w administrowaniu, zarządzaniu i projektowaniu infrastruktury sieciowej potwierdzone certyfikatem na poziomie proffessional Wymagany certyfikat CCNP (Cisco Certified Network Professional) lub równoważny.

Potwierdzeniem spełnienia wymogów będzie stanowiło dostarczenie do Zamawiającego wymaganego certyfikatu wystawionego na dane osoby delegowanej do pracy na rzecz Zamawiającego i okres doświadczenia zawodowego.

e) Dobra znajomość w zakresie projektowania infrastruktury sieciowej potwierdzona certyfikatem. Wymagany certyfikat CCDP (Cisco Certified Design Professional) lub równoważny.

Potwierdzeniem spełnienia wymogów będzie stanowiło dostarczenie do Zamawiającego wymaganego certyfikatu wystawionego na dane osoby delegowanej do pracy na rzecz Zamawiającego.

f) W ciągu ostatnich 3 lat przed upływem terminu składania ofert przez okres minimum 1 roku brał udział   
w co najmniej 1 usłudze polegającej na wsparciu i administrowaniu infrastrukturą sieciową, obejmującą   
co najmniej 200 jednocześnie zalogowanych użytkowników, w której wykonywał czynności związane   
z zarządzaniem NG Firewall, w całym zakresie funkcjonalności.

Potwierdzeniem spełnienia wymogów będzie stanowiło dostarczenie do Zamawiającego wymaganego certyfikatu wystawionego na dane osoby delegowanej do pracy na rzecz Zamawiającego, w tym wskazującego wymagany okres doświadczenia zawodowego.

Wymaganie dla experta bezpieczeństwa:

a) Minimum 5 - letnie doświadczenie i znajomość praktycznych zagadnień dotyczących bezpieczeństwa informatycznego potwierdzonego certyfikatem CPEH (Certified Professional Ethical Hacker)

Potwierdzeniem spełnienia wymogów będzie stanowiło dostarczenie do Zamawiającego wymaganego certyfikatu wystawionego na dane osoby delegowanej do pracy na rzecz Zamawiającego.

b) Doświadczenie i znajomość praktycznych zagadnień dotyczących przeprowadzania audytów   
w jednostkach m.in. szpitalnych potwierdzona certyfikatem Audytora Wiodącego ISO 27001

Potwierdzeniem spełnienia wymogów będzie stanowiło dostarczenie do Zamawiającego wymaganego certyfikatu wystawionego na dane osoby delegowanej do pracy na rzecz Zamawiającego.

2. Doświadczenie oferenta: Wymagane wykazaniem się doświadczeniem obejmującym minimum 2 usługi,   
z których każda odpowiadała swoim rodzajem przedmiotowi zamówienia tj. polegała na wsparciu   
i administrowaniu infrastrukturą sieciową, obejmującą co najmniej 250 jednocześnie zalogowanych użytkowników, wraz z podaniem ich przedmiotu wraz z liczbą użytkowników, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane.

Potwierdzeniem spełnienia wymagań będzie stanowiło dostarczenie do Zamawiającego referencji obejmujących wymagany zakres.

Termin realizacji zadania - w ciągu 14 dni od dnia zawarcia umowy (część I, II), przy czym usługi utrzymania infrastruktury zapór sieciowych oraz sieci - 36 miesięcy od dnia zawarcia umowy (część III).

**UWAGA:**

1.W przypadku zastosowania przez Zamawiającego w opisie przedmiotu zamówienia odniesień lub nazw specyfikacji technicznych, aprobat, technologii, funkcjonalności lub norm, Zamawiający dopuszcza zaoferowanie rozwiązań co najmniej równoważnych   
z opisywanymi. Wykonawca, który w celu realizacji Zamówienia powołuje się na rozwiązania co najmniej równoważne z opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez Wykonawcę rozwiązania spełniają wymagania określone przez Zamawiającego.

2. Jeżeli w jakimkolwiek dokumencie postępowania znajduje się jakikolwiek znak towarowy, znak handlowy jakiegoś wyrobu, nazwa własna (handlowa), patent czy pochodzenie – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza zastosowanie materiałów, urządzeń, sprzętu i wyposażenia o co najmniej równoważnych parametrach technicznych w odniesieniu   
do parametrów podanych pod pojęciem typu. Wykonawca, który w celu realizacji Zamówienia powołuje się na rozwiązania co najmniej równoważne, jest obowiązany wykazać, że oferowane przez Wykonawcę rozwiązania spełniają wymagania określone   
przez Zamawiającego.

........................................ dnia ........................... ............................................................

(miejscowość) (podpis(y) *osoby ( osób) upoważnionej*

*do występowania w imieniu Oferenta*