Załącznik Nr 2 do SWZ

**POWIAT WŁODAWSKI**

**Al. Józefa Piłsudskiego 24**

**22-200 Włodawa**

**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

**Przedmiot zamówienia:**

**Dostawa rozwiązań podnoszących poziom cyberbezpieczeństwa systemów teleinformatycznych oraz usługa audytu bezpieczeństwa systemów IT w Starostwie Powiatowym we Włodawie.**

**dotyczy postępowania o udzielenie zamówienia publicznego klasycznego w trybie podstawowym bez negocjacji**

o wartości nie przekraczającej kwoty wartości zamówienia określonej w przepisach, o których mowa w art. 3 ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych (tekst jedn.: Dz. U. z 2023 r. poz. 1605 z późn. zm.)

Znak postępowania: WO.272.2.4.2024

Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0387/ FERC.02.02-CS.01-001/23/2024

Umowa finansowana z Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)

Spis treści

[**Rozdział I: Założenia początkowe oraz wymagania ogólne** 4](#_Toc166672473)

[1. Wprowadzenie 4](#_Toc166672474)

[2. Ogólny opis przedmiotu zamówienia 4](#_Toc166672475)

[3. Termin realizacji Przedmiotu Zamówienia 5](#_Toc166672476)

[**Rozdział II. Szczegółowy opis przedmiotu zamówienia 9**](#_Toc166672477)

[1. Wznowienie subskrypcji zabezpieczeń do posiadanego systemu Unified Threat Management firmy Fortigate. 9](#_Toc166672478)

[2. Rozbudowa posiadanych systemów Unified Threat Management firmy Fortigate oraz wznowienie subskrypcji zabezpieczeń UTP. 9](#_Toc166672479)

[2.1 Urządzenie klasy UTM z gwarancją i wsparciem na okres min. 24 miesięcy – 2 sztuki 9](#_Toc166672480)

[2.2 Zakres wdrożenia 15](#_Toc166672481)

[2.3 Instruktaże 15](#_Toc166672482)

[2.4 Dokumentacja powykonawcza. 16](#_Toc166672483)

[2.5 Rozszerzone wsparcie serwisowe świadczone przez okres min. 24 miesięcy 16](#_Toc166672484)

[3. Oprogramowanie antywirusowe - wznowienie subskrypcji na kolejne 2 lata + rozszerzenie o funkcję sandboxing. 17](#_Toc166672485)

[4. Oprogramowanie przeciwdziałające wyciekowi danych DLP - Data Leak Prevention 22](#_Toc166672486)

[5. Oprogramowanie do wykonywania kopii zapasowych – nowe licencje 26](#_Toc166672487)

[6. Oprogramowanie do wykonywania kopii zapasowych - wznowienie lub nowe licencje 31](#_Toc166672488)

[7. Oprogramowanie do monitorowania infrastruktury informatycznej 36](#_Toc166672489)

[8. Dostawa, wdrożenie systemu SIEM (Security Information and Event Management) z usługą zewnętrznego SOC - Centrum Operacji Bezpieczeństwa (Security Operations Center). 39](#_Toc166672490)

[8.1 Słownik pojęć: 39](#_Toc166672497)

[8.2 Termin realizacji usługi SOC 41](#_Toc166672498)

[8.3 Wymagania dla Usługi SOC (Security Operations Center) 42](#_Toc166672499)

[8.4 Pierwsza i Druga Linia Wsparcia 42](#_Toc166672500)

[8.5 Scenariusze 42](#_Toc166672505)

[8.6 Raport Poincydentalny 43](#_Toc166672508)

[8.7 Systemy Zamawiającego wymagające monitorowania 43](#_Toc166672509)

[8.8 Wymagania dla Systemu Zbierania i Analizy Logów oraz Systemu SIEM. 44](#_Toc166672510)

[8.9 Wymagania dla Systemu SIEM. 45](#_Toc166672539)

[8.10 Administracja Systemem Analizy Logów: 45](#_Toc166672555)

[8.11 Testowanie Systemu Analizy Logów: 46](#_Toc166672562)

[8.12 Analiza złośliwego oprogramowania: 46](#_Toc166672563)

[8.13 Ogólne warunki SLA 47](#_Toc166672564)

[8.14 Transfer wiedzy. 49](#_Toc166672565)

[8.15 Zespół SOC 50](#_Toc166672570)

[8.16 Wymagania dodatkowe 50](#_Toc166672571)

[8.17 Opcjonalny moduł EDR (Endpoint Detection and Response - moduł punktowany dodatkowo). 50](#_Toc166672572)

[8.18 Opcjonalny moduł NDR (Network Detection and Response - moduł punktowany dodatkowo). 51](#_Toc166672573)

[9. Zakup bibliotek taśmowych do przechowywania kopii zapasowych 52](#_Toc166672574)

[10. Zakup certyfikatu SSL do zabezpieczenia serwera poczty elektronicznej 54](#_Toc166672575)

[*11.* System do inwentaryzacji zasobów infrastruktury informatycznej, zarządzania zgłoszeniami *- moduł punktowany dodatkowo* 54](#_Toc166672576)

[12. Zakup gwarancji producenta dla posiadanych serwerów i macierzy 56](#_Toc166672578)

[13. Szkolenia z zakresu Cyberbezpieczeństwa dla administratora 56](#_Toc166672579)

[14. Szkolenie z zakresu cyberbezpieczeństwa dla pracowników – platforma szkoleniowa 61](#_Toc166672580)

[15. Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji 62](#_Toc166672581)

[16. Audyt bezpieczeństwa - wstępny („zerowy”). Analiza stanu bezpieczeństwa użytkowanych systemów oraz wskazanie koniecznych działań, które zwiększą poziom bezpieczeństwa IT 64](#_Toc166672582)

[17. Audyt bezpieczeństwa – końcowy. Analiza poziomu bezpieczeństwa po zakończeniu projektu. Weryfikacja osiągnięcia założonych celów projektu - Część II zamówienia 65](#_Toc166672588)

# Rozdział I: Założenia początkowe oraz wymagania ogólne

# Wprowadzenie

* 1. Przedmiot zamówienia jest realizowany w ramach grantu pn. „Cyberbezpieczny Samorząd” współfinansowanego ze środków Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.
  2. Realizacja grantu ma na celu zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego (JST) oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie. Program jest odpowiedzią na wzrastającą liczbę ataków na podmioty administracji publicznej w Powiecie Włodawskim.

# Ogólny opis przedmiotu zamówienia

* 1. Przedmiot zamówienia obejmuje systemy cyberbezpieczeństwa w zakresie:

|  |  |
| --- | --- |
| **Lp.** | **Opis** |
| 1 | Wznowienie subskrypcji zabezpieczeń UTP do posiadanego systemu Unified Threat Management firmy Fortigate. |
| 2 | Rozbudowa posiadanych systemów Unified Threat Management firmy Fortigate oraz wznowienie subskrypcji zabezpieczeń UTP. |
| 3 | Oprogramowanie antywirusowe - wznowienie subskrypcji na kolejne 2 lata + rozszerzenie o funkcję sandboxing. |
| 4 | Oprogramowanie przeciwdziałające wyciekowi danych DLP - Data Leak Prevention |
| 5 | Oprogramowanie do wykonywania kopii zapasowych – nowe licencje |
| 6 | Oprogramowanie do wykonywania kopii zapasowych – wznowienie lub nowe licencje |
| 7 | Oprogramowanie do monitorowania infrastruktury informatycznej |
| 8 | Dostawa, wdrożenie systemu SIEM (Security Information and Event Management) z usługą zewnętrznego SOC - Centrum Operacji Bezpieczeństwa (Security Operations Center) |
| 9 | Zakup bibliotek taśmowych do przechowywania kopii zapasowych |
| 10 | Zakup certyfikatu do zabezpieczenia poczty elektronicznej |
| 11 | System do inwentaryzacji zasobów infrastruktury informatycznej, zarządzania zgłoszeniami |
| 12 | Zakup gwarancji producenta dla posiadanych serwerów i macierzy |
| 13 | Szkolenia z zakresu Cyberbezpieczeństwa dla administratora |
| 14 | Szkolenie z zakresu cyberbezpieczeństwa dla pracowników – platforma szkoleniowa |
| 15 | Aktualizacja dokumentacji System Zarządzania Bezpieczeństwem Informacji |
| 16 | Audyt bezpieczeństwa - wstępny („zerowy”). Analiza stanu bezpieczeństwa użytkowanych systemów oraz wskazanie koniecznych działań, które zwiększą poziom bezpieczeństwa IT |
| 17 | Audyt bezpieczeństwa – końcowy. Analiza poziomu bezpieczeństwa po zakończeniu projektu. Weryfikacja osiągnięcia założonych celów projektu – część II zamówienia |

* 1. Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego we wskazanym miejscu.
  2. Wszystkie dostarczane Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem przedmiotu zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach) oraz Komponenty (rozumiane jako integralna część dostawy i wdrożenia przedmiotu zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
  3. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca musi przeprowadzić zgodnie z postanowieniami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
  4. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Wzoru Umowy.
  5. Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy PZP należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 101 ust. 4 ustawy PZP dopuszcza rozwiązanie równoważne opisywanym w treści OPZ. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 101 ust. 4 ustawy PZP dopuszcza składanie ofert na rozwiązania równoważne. Wszelkie „produkty” pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego, stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dotyczący minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.

# Termin realizacji Przedmiotu Zamówienia

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie:

* do 31.12.2025 r.
* Audyt bezpieczeństwa – końcowy: po zakończeniu prac objętych projektem w terminie do 31.01.2026 r.
  1. **Organizacja wdrożenia**

1. Założenia podstawowe:
2. Przedmiot Zamówienia będzie realizowany w oparciu o przygotowany uprzednio przez Wykonawcę Harmonogram Ramowy (rzeczowo-finansowy), który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram Ramowy w terminie 7 dni od daty podpisania umowy.
3. Wykonawca w Harmonogramie Ramowym musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
4. Harmonogram musi zawierać w szczególności:
5. trzy (3) etapy rozliczeniowe realizacji przedmiotu Umowy (2 etapy częściowe i etap końcowy) oraz odpowiadające im koszty i terminy ich wykonania, z uwzględnieniem wymagania, że etap pierwszy zostanie zrealizowany w terminie do 30 dni od dnia zawarcia Umowy;
6. zadania obejmujące zakresy dostaw i prac składających się na poszczególne etapy realizacji przedmiotu umowy oraz odpowiadające im koszty i terminy ich wykonania przy założeniu, że:

* w pierwszym etapie rozliczeniowym zakres dostaw/usług obejmować będzie pozycje nr 1, nr 3, nr 5 nr 6, nr 10, nr 12 oraz nr 16 według Ogólnego opisu przedmiotu zamówienia (pkt 2 ppkt 2.1 niniejszego dokumentu) a łączna wartość zadań realizowanych nie przekroczy 30 % kwoty wynagrodzenia Wykonawcy;
* w drugim etapie rozliczeniowym zakres dostaw/usług obejmować będzie pozycje nr 2, nr 4, oraz nr 9 według Ogólnego opisu przedmiotu zamówienia (pkt 2 ppkt 2.1 niniejszego dokumentu) a wartość dostaw/usług nie przekroczy 30 % kwoty wynagrodzenia Wykonawcy;
* w trzecim etapie rozliczeniowym zakres dostaw/usług obejmować będzie pozycje nr 7, nr 8, nr 11, nr 13, nr 14 oraz nr 15 według Ogólnego opisu przedmiotu zamówienia (pkt 2 ppkt 2.1 niniejszego dokumentu) a wartość dostaw/usług nie przekroczy 40 % kwoty wynagrodzenia Wykonawcy.

1. Wykonawca umożliwi Zamawiającemu udział we wszystkich realizowanych przez niego pracach w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji, wdrożeniu i testowaniu).
2. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Dopuszcza się narady prowadzone w trybie zdalnym z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca. Zamawiający przewiduje częstotliwość narad nie częściej niż jeden raz w miesiącu, narad zdalnych maksymalnie 3 razy w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań w siedzibie lub odbywanych zdalnie.
3. Wykonawca zobowiązany jest przeprowadzić prace wdrożeniowe przedmiotu zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
4. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie przedmiotu zamówienia.
5. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
6. W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:
7. Kierownik Projektu ze strony Wykonawcy,
8. Zespół Wdrożeniowy ze strony Wykonawcy.
9. Wdrożenie, z zastrzeżeniami wskazanymi poniżej muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
10. Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
11. Wykonawca musi przekazać Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.
    1. **Przygotowanie Dokumentacji**
12. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia(zwaną dalej Dokumentacją), która składa się z nw. zakresów:
13. Dokumentacja powyższa musi zawierać bazowe zapisy opisujące budowane rozwiązania oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach przedmiotu zamówienia. Dokumenty te wraz ze SWZ z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
14. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
15. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia muszą być opracowane w oparciu o wymagania określone w niniejszym OPZ.
    1. **Analiza Przedwdrożeniowa**

Analiza Przedwdrożeniowa obejmuje wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie środowiska informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwana dalej DAP) oraz harmonogram wdrożenia, na podstawie którego organizacyjnie i technicznie będzie realizowany przedmiot zamówienia. DAP będzie podlegał uzgodnieniu i akceptacji Zamawiającego. Termin wykonania analizy został określony w umowie. DAP musi zawierać w szczególności:

|  |
| --- |
| **ZawarTość Dokumentacji Analizy Przedwdrożeniowej (DAP)** |
| 1. **Wymagane dane ZARZĄDCZE:** |
| 1. plan i sposób komunikacji Stron. |
| 1. harmonogram wdrożenia |
| 1. **Audyt bezpieczeństwa systemów IT (‘zerowy”):** |
| 1. Analiza stanu bezpieczeństwa użytkowanych systemów przed rozpoczęciem realizacji projektu |
| 1. Opis koniecznych działań dla osiągnięcia wymaganego stanu cyberbezpieczeństwa |
| 1. **Wymagane dane dotyczące systemów cyberbezpieczeństwa:** |
| 1. podział przedmiotu zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty, |
| 1. analiza wymagań przedmiotu zamówienia zawierająca opis sposobu realizacji wymagań, sposób testowania i odbioru, |
| 1. Wykonawca określi w Analizie przedwdrożeniowej zalecaną specyfikację i optymalną konfigurację środowiska dla Systemu SIEM, migrowanych systemów Zamawiającego m.in. pamięć, liczbę procesorów, wymagana powierzchnia dyskowa. |
| 1. Dla każdego systemu cyberbezpieczeństwa Wykonawca opracuje:  * Architekturę rozwiązania * Wersję oprogramowania wchodzące w skład Systemu * Konfigurację Systemu * Zastosowane licencje/subskrypcje. |
| 1. Procedura testowania – scenariusze testowe dla wdrażanych systemów |
| 1. Harmonogram wdrożenia |
| 1. Opis instalacji i wdrożenia oprogramowania |
| 1. Szczegółowy zakres i zawartość pozostałej Dokumentacji. |

* 1. **Dokumentacja Powykonawcza**

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową i techniczną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej oraz w wersji elektronicznej w formacie edytowalnym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta musi zawierać:
   1. Schemat infrastruktury i architekturę rozwiązania wraz z opisem.
   2. Zasady licencjonowania dostarczonych elementów.
   3. Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.
   4. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.
   5. Procedury konfiguracji kont w dostarczonych systemach.
   6. Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii.
   7. Procedury wykonywania odtworzenia wdrożonych systemów z kopii zapasowej.
   8. Procedury opisujące standardowe działania administracyjne.
   9. Procedury odzyskania wdrożonych systemów po awarii.
   10. Wytyczne (dobre praktyki) dla administratorów.
   11. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.
   12. **Odbiór Etapu/Dokumentacji/Końcowy**
4. Odbiory Etapów/Dokumentacji będą się odbywać po zakończeniu określonych prac danego Etapu/Dokumentacji.
5. Odbiór końcowy przedmiotu zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
6. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej załącznik **nr 5 do SWZ.**
   1. **Testy**
7. W ramach odbioru przedmiotu zamówienia muszą zostać przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale.
8. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego przedmiotu zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru Końcowego.
9. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
10. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym przedmiotu zamówienia.
11. Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze z zakresu:
12. Uruchamianie i zatrzymywanie wdrożonych systemów
13. Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w dokumentacji.
14. Weryfikacja poprawności działania procedur.
15. Symulację awarii wdrożonych systemów.
    1. **Dodatkowe zobowiązania Wykonawcy**
16. Wykonanie przedmiotu zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
17. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres   
    i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
18. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
19. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
20. Współdziałanie z osobami wskazanymi przez Zamawiającego.

# Rozdział II. Szczegółowy opis przedmiotu zamówienia

# Wznowienie subskrypcji zabezpieczeń do posiadanego systemu Unified Threat Management firmy Fortigate.

Zamawiający posiada dwa urządzenia klasy UTM Fortigate 101E pracujące w klastrze niezawodnościowym. Należy przedłużyć komplet posiadanych serwisów: Unified Threat Protection (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) dla dwóch urządzeń FortiGate 101E o numerach seryjnych: FG101ETK18006531, FG101ETK18006764 na kolejne 24 miesiące.

# Rozbudowa posiadanych systemów Unified Threat Management firmy Fortigate oraz wznowienie subskrypcji zabezpieczeń UTP.

Zamawiający użytkuje obecnie klaster 2 urządzeń UTM firmy Fortigate model 60E z serwisami UTP (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium). W związku z zbliżającą się datą zakończenia trwającego wsparcia technicznego oraz niską wydajnością w stosunku do urządzeń najnowszej generacji Zamawiający zamierza wymienić stare urządzenia na najnowsze dostępne modele. Wykonawca dostarczy nowe urządzenia z serwisami nie gorszymi niż obecnie użytkowane na okres min. 24 miesięcy. Wykonawca musi opracować: projekt wymiany obecnych urządzeń brzegowych (tj. urządzeń pracujących na styku sieci LAN oraz WAN), projekt podziału sieci LAN na wirtualne podsieci, harmonogram wdrożenia oraz zakres wdrożenia, który przedstawi Zamawiającemu do akceptacji. Wykonawca musi wdrożyć dostarczane urządzenia, w tym min. skonfigurować je do pracy w klastrze wysokiej dostępności; wykonać instruktaż z zakresu administracji dostarczonych urządzeń UTM; opracować dokumentację powykonawczą; świadczyć rozszerzone wsparcie serwisowe przez okres min. 24 miesięcy. Wymagany klaster dwóch urządzeń UTM musi spełniać wszystkie wymienione poniżej funkcje sieciowe oraz 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. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzający gotowość świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.



## **Urządzenie klasy UTM z gwarancją i wsparciem na okres min. 24 miesięcy – 2 sztuki**

System UTM realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Musi być możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

**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.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 10 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 34 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 1750 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 620 Mbps.

**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 oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. 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).

**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.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. 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.

**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.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

**Routing i obsługa łącz 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, oznaczeń Type of Service w nagłówkach IP).
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.

**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).

**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.

**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. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
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 chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

**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 5 000 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. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

**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 2 000 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.

**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.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. 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.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**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 dwuskładnikowego 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.

**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.

**Testy wydajnościowe oraz funkcjonalne**

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

**Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagany jest pakiet licencji zawierający funkcjonalności minimalne: 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 min. 24 miesięcy.

**Gwarancja oraz wsparcie**

1. Urządzenia muszą być objęte standardowym serwisem gwarancyjnym producenta przez okres min. 24 miesięcy.
2. Dodatkowo wymagana jest rozszerzona gwarancja na urządzenia, polegająca na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement) w czasie nie dłuższym niż 24 godziny w dni robocze, dla zgłoszeń utworzonych do godz. 14:00 w dni robocze.
3. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie Zamawiającego, realizowana przez producenta lub autoryzowanego partnera w języku polskim.

## **Zakres wdrożenia**

Wykonawca dostarczy system UTM, zainstaluje, skonfiguruje oraz dokona przeniesienia całej obecnej konfiguracji z obecnie używanego systemu firewall. Wdrożenie będzie obejmować co najmniej:

1. konfigurację ogólną systemu - adresy IP, DNS, DHCP, routing, NTP,
2. konfiguracja interfejsów sieciowych - WAN, LAN, DMZ. Konfiguracja dodatkowego łącza zapasowego,  
   łącznie z ustawieniem routingu oraz przygotowanie odpowiednich polityk
3. integracja nowego systemu UTM z Active Directory,
4. przeniesienie całej konfiguracji z istniejącego urządzenia Firewall na nowy system UTM z najnowszą stabilną wersją oprogramowania
5. audyt reguł i ustawień, weryfikacja i poprawienie reguł oraz ustawień, optymalizacja używanych dotychczas reguł, zgodnie z dobrymi praktykami,
6. konfiguracja loadbalancingu dla min. dwóch łączy WAN,
7. konfiguracja QoS oraz kształtowania pasma dla co najmniej 5 profili,
8. przeniesienie istniejących obiektów sieciowych – około 70 obiektów,
9. przeniesienie istniejących reguł firewall oraz NAT – około 30 reguł,
10. przeniesienie konfiguracji IPSec VPN,
11. przeniesienie filtrów URL oraz SSL, konfiguracja inspekcji SSL – około 60 obiektów URL oraz około 30 obiektów SSL,
12. opracowanie polityki deszyfracji danych szyfrowanych SSL (Secure Sockets Layer), opracowanie reguł działania w zależności od rodzaju ruchu, opracowanie polityki ponownego szyfrowania danych, konfiguracja urządzeń UTM
13. konfiguracja przesyłania logów do posiadanych przez Zamawiającego instancji zbierających i przechowujących logi,
14. wykonanie projektu podziału sieci LAN Zamawiającego
15. utworzenie wirtualnych sieci LAN, konfiguracja przełączników, urządzeń UTM, konfiguracja polityk

Zamawiający może wymagać skonfigurowania dodatkowych parametrów systemu UTM, jeśli podczas wdrożenia zajdzie taka potrzeba.

Zamawiający wymaga, aby wdrożenie przeprowadził inżynier posiadający ważny certyfikat techniczny producenta oferowanego rozwiązania, potwierdzający kompetencje z zakresu wdrażania systemów UTM. Wykonawca przed przystąpieniem do wdrożenia przygotuje harmonogram wdrożenia.

## **Instruktaże**

Zamawiający wymaga przeprowadzenia instruktaży dla swoich administratorów zgodnie z poniższym opisem:

1. Instruktaż podstawowy (wdrożeniowy) – odbędzie się przy okazji wdrożenia i konfiguracji systemu UTM w siedzibie Zamawiającego, jego przedstawiciele będą uczestniczyć w wykonywanych pracach.
2. Instruktaż z zakresu wdrożonego systemu UTM (powdrożeniowy), dla grupy do 3 osób, średniozaawansowanych (wcześniej pracujących na systemach UTM), minimum 3 maksimum 5 dniowy, obejmujący cały niżej wymieniony zakres materiału szkoleniowego:

* rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego; ustawienia systemowe i uprawnienia administratorów;
* instalacja licencji i aktualizacja systemu; tworzenie kopii zapasowej i przywracanie konfiguracji;
* zbieranie logów i monitorowanie; przedstawienie kategorii zbieranych logów;
* wykresy historyczne i monitorowanie; obiekty: typy obiektów oraz ich wykorzystanie;
* obiekty sieciowe i obiekt typu „router”;
* konfiguracja sieci: tryby pracy urządzenia; typy interfejsów (ethernet, modem, bridge, vlan, gretap)
* typy routingu oraz ich priorytety; translacja adresów sieciowych (nat); translacja połączeń wychodzących (maskarada); translacja połączeń przychodzących (przekierowanie); translacja dwukierunkowa (jeden do jeden);
* filtrowanie ruchu sieciowego (firewall); ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (stateful inspection); szczegółowy opis parametrów reguły firewall; kolejność przetwarzania reguł firewall i nat;
* ochrona aplikacji: implementacja filtrowania url dla ruchu http i https; konfigurowanie skanowania antywirusowego i modułu breach fighter;
* moduł ips i stosowanie profili inspekcji; użytkownicy i uwierzytelnianie
* konfiguracja usługi katalogowej: wprowadzenie do różnych metod uwierzytelniania (ldap, kerberos, radius, certyfikat ssl, spnego, sso);
* rejestracja użytkowników; uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania; wirtualne sieci prywatne (vpn);
* koncepcje i ogólne informacje dotyczące protokołu ipsec vpn (ikev1 i ikev2);
* tunele site-to-site z wykorzystaniem klucza współdzielonego (psk);
* tunele vti; ssl vpn - zasada działania, konfiguracja

1. Instruktaż powdrożeniowy musi zawierać elementy warsztatowe i opierać się na zadaniach praktycznych realizowanych w przygotowanym laboratorium (LAB) z oferowanymi systemami UTM. LAB musi być przygotowany w wersji oprogramowania zastosowanej podczas wdrożenia na systemie UTM Zamawiającego.
2. Instruktaże muszą być prowadzone przez praktyka posiadającego co najmniej 3-letnie doświadczenie w zakresie wdrażania systemów UTM oraz posiadającego ważny certyfikat inżynierski w zakresie administracji UTM.

W przypadku wykonania instruktażu powdrożeniowego w miejscu, gdzie łączny czas dojazdu transportem publicznym pracowników Zamawiającego jest dłuższy niż 1 godzina (od siedziby Zamawiającego), Wykonawca zapewni:

* zakwaterowanie w hotelu (co najmniej trzygwiazdkowym) począwszy od dnia poprzedzającego instruktaże
* pełne wyżywienia (śniadanie, obiad, kolacja). Zakwaterowanie w hotelu nie może być oddalone od miejsca szkolenia więcej niż 10 minut pieszo.

Instruktaż musi zakończyć się w ciągu maksymalnie 3 miesięcy licząc od dnia zakończenia wdrożenia. Instruktaż musi zostać zrealizowany w jednym terminie dla wszystkich osób, a termin Instruktażu Wykonawca musi ustalić z Zamawiającym.

## **Dokumentacja powykonawcza.**

Wykonawca dostarczy co najmniej w formie elektronicznej dokumentację powykonawczą. Dokumentacja powinna zawierać wszystkie dane dostępowe do konfigurowanych urządzeń, systemów, schematy podłączenia urządzeń do sieci LAN, opis konfiguracji dostarczonego i wdrożonego systemu UTM, opis wdrożonych polityk.

## **Rozszerzone wsparcie serwisowe świadczone przez okres min. 24 miesięcy**

System UTM będzie objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego partnera przez okres min. 24 miesięcy.

System będzie objęty rozszerzonym wsparciem technicznym w zakresie:

* Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
* Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
* Doradztwo w zakresie konfiguracji.
* Doradztwo w zakresie podnoszenia poziomu bezpieczeństwa.
* Zdalne wsparcie techniczne.
* Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
* Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
* Przygotowanie systemu UTM do zdalnej konfiguracji.
* Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
* Nielimitowana rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
* Nielimitowana usługa zdalnego przeglądu konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
* Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług serwisowych, podmiot świadczący wsparcie musi posiadać certyfikat ISO 27001. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wymagany jest czas reakcji nie dłuższy niż 4 godziny dla połączeń telefonicznych lub nie dłuższy niż 6 godzin dla odpowiedzi w portalu serwisowym. Zamawiający wymaga, aby wsparcie serwisowe świadczył zespół certyfikowanych inżynierów w zakresie administracji systemami UTM, legitymujący się ważnymi certyfikatami.

Na żądanie Zamawiającego Wykonawca przedstawi oświadczanie o gotowości świadczenia wymaganego serwisu zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej oraz ważne certyfikat techniczny inżyniera/ów wystawione przez Producentów systemów UTM oraz certyfikat ISO 27001 Wykonawcy.

Podmiot świadczący wsparcie posiada certyfikat ISO 27001 – **dodatkowo punktowane – Załącznik nr 6.**

# Oprogramowanie antywirusowe - wznowienie subskrypcji na kolejne 2 lata + rozszerzenie o funkcję sandboxing.

Zamawiający posiada 110 licencji oprogramowania antywirusowego ESET PROTECT Essential ON-PREM z wsparciem technicznym ważnym do dnia 30.06.2024. Należy dostarczyć 110 licencji z wsparciem na 24 miesiące na oprogramowanie o poniższej funkcjonalności minimalnej:

**Administracja zdalna w chmurze**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać 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. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. 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 funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. 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**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
17. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
18. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
19. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
20. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
21. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
22. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
23. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
24. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
25. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
26. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
27. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
28. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
29. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
30. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
31. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
32. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
33. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
34. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
35. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
36. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
37. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
38. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
39. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

**Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

**Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
6. usunięcie zawartości urządzenia,
7. przywrócenie urządzenie do ustawień fabrycznych,
8. zablokowania urządzenia,
9. uruchomienie sygnału dźwiękowego,
10. lokalizację GPS.
11. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
12. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
13. nazwę aplikacji,
14. nazwę pakietu,
15. kategorię sklepu Google Play,
16. uprawnienia aplikacji,
17. pochodzenie aplikacji z nieznanego źródła.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
13. Czysty,
14. Podejrzany,
15. Bardzo podejrzany,
16. Szkodliwy.
17. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
18. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
19. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Należy skonfigurować konsolę w chmurze, podłączyć do konsoli wszystkie stacje robocze, skonfigurować konsolę wg zaleceń producenta, dobrych praktyk oraz zaleceń Zamawiającego. Należy wykonać instruktaż dla administratora wg poniższych zagadnień minimalnych oferowanego oprogramowania:

* architektura i omówienie komponentów,
* Instalacja i aktualizacja serwera
* omówienie funkcji serwera,
* zarządzanie administratorami i ich uprawnieniami
* zdalna instalacja i omówienie możliwości,
* grupy statyczne i dynamiczne,
* zadania klienta, serwera oraz wyzwalacze,
* zdalna instalacja klienta na stacji roboczej,
* omówienie funkcji podstawowych i zaawansowanych klienta,
* ochrona antywirusowa,
* zarządzanie aktualizacją,
* polityki i dziedziczenie
* bridge,
* zapora osobista
* moduł antyspamowy,
* powiadomienia,
* raportowanie
* kontrola dostępu do stron internetowych
* kontrola dostępu do urządzeń
* wdrożenie klienta na telefonie z Android

# Oprogramowanie przeciwdziałające wyciekowi danych DLP - Data Leak Prevention

System klasy DLP czyli system monitorowania i ochrony poufnych informacji, zapobiegania utracie danych, wyciekom danych. Wymagane jest dostarczenie licencji bezterminowej dla 100 urządzeń z wsparciem technicznym na min. 24 miesiące. Minimalne wymagania dla systemu DLP:

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL oraz AzureSQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania:

kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.

1. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
2. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania oraz edycji wyżej wymienionych kategorii.
3. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
4. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
   1. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
   2. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
5. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
6. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
   1. logowanie oraz wylogowanie użytkownika,
   2. włączenie oraz wyłączenie stacji roboczej,
   3. blokada oraz odblokowanie stacji roboczej,
   4. przejście w stan bezczynności stacji roboczej.
7. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
8. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
9. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
10. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
11. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF oraz XLS.
12. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
13. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
14. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
15. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
16. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
17. Serwer administracyjny musi posiadać domyślnie skonfigurowany serwer SMTP udostępniony przez producenta oprogramowania.
18. 30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
19. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
20. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
    1. aplikacje, z której zostały utworzone,
    2. lokalizację,
    3. adres URL,
    4. format pliku,
    5. zawartość pliku.
21. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
22. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
23. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
24. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
25. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
26. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
27. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
28. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
29. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
    * + Dropbox,
      + Google Drive,
      + SharePoint,
      + OneDrive Business,
      + OneDrive Personal.
30. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
31. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
32. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
33. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,
34. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
35. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
36. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
37. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
38. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
39. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
40. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
41. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
42. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
43. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
44. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
    1. numery kart kredytowych,
    2. numer PESEL,
    3. numer polskiego dowodu osobistego,
    4. polski numer paszportu,
    5. wyrażenia regularne,
    6. określone ciągi znaków,
    7. numer IBAN.
45. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
46. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition) z wsparciem języka polskiego.
47. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
48. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e-mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).
49. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
50. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
51. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania klasy SIEM.
52. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do systemu umożliwiającego ochrony poczty, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
53. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
    1. audyt i logowanie wiadomości e-mail,
    2. audyt operacji na plikach Sharepoint Online.
54. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
55. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi.
56. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
    1. Bezpieczeństwo danych:
       * Przegląd informacji o incydentach bezpieczeństwa.
       * Przegląd danych przychodzących.
       * Przegląd danych wychodzących.
       * Podłączane/odłączane urządzenia przenośne.
    2. Produktywność:
       * Przegląd informacji na temat produktywności użytkowników.
       * Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
       * Trendy.
    3. Eksploatacja sprzętu:
       * Przegląd informacji na temat eksploatacji sprzętu komputerowego.
       * Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
       * Eksploatacja drukarek.
       * Eksploatacji sieci.
57. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
58. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
59. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt.:
    * + plików przenoszonych na nośniki USB i inne urządzenia przenośne,
      + plików przesłanych za pomocą wiadomości e-mail,
      + plików przesłanych za pomocą poczty webowej,
      + plików przesłanych do Internetu,
      + plików wysłanych za pomocą komunikatorów,
      + plików przesłanych na dyski chmurowe,
      + analiza sposobu korzystania z aplikacji,
      + analiza korzystania z Internetu,
      + analiza wykorzystania portali do poszukiwania pracy.
60. Konsola aplikacyjna musi umożliwiać możliwość konfiguracji podwójnej autoryzacji
61. Konsola aplikacyjna musi umożliwiać konfigurację dwóch języków dla mechanizmu OCR

# Oprogramowanie do wykonywania kopii zapasowych – nowe licencje

Należy dostarczyć licencje bezterminowe obejmujące 10 maszyn wirtualnych wraz z wsparciem technicznym producenta na okres min. 24 miesięcy.

|  |  |
| --- | --- |
| **Wymagane parametry techniczne, minimalne** | **Oferowane parametry techniczne zgodnie z wymaganiami technicznymi**  **Wpisać: TAK lub NIE** |
| **1. Wymagania ogólne**:   1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner:   https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions  i spełniać minimalne wymaganie:  - minimalna liczba referencji 150,  - minimalna ocena z referencji 4,5,   1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych 2. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |  |
| **2. Całkowite koszty posiadania**   1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej 2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków 3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji 4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. 5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. 6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. 7. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie. 8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania 9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) 10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu 11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API 12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji 13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji 14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania 15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. 16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |  |
| **3. Wymagania RPO (Recovery Point Objective) – określające dopuszczalną ilość utraconych danych i maksymalny akceptowalny czas pomiędzy wystąpieniem awarii, a backupem danych**   1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej 2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru 4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. 5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. 6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. 7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. 9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. 10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. 11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. 12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik 14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) 15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |  |
| 1. **Wymagania RTO (Recovery Time Objective), czas przywrócenia do działania po awarii z kopii zapasowej** 2. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. 3. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 4. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami 5. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre 6. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. 7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków 8. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. 9. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików 10. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. 11. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell 12. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. 13. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 14. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. 15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. 16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. 17. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. 18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. 19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. 20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN 21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle 22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI 23. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |  |
| 1. **Ograniczenie ryzyka** 2. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 3. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. 4. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem 5. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. 6. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |  |
| 1. **Środowiska fizyczne** 2. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego 3. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych 4. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE 5. Rozwiązanie musi wspierać system operacyjny macOS 6. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix 7. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) 8. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster 9. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów 10. Rozwiązanie musi wspierać backup podłączonych dysków USB 11. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym 12. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) 13. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone 14. Rozwiązanie musi wspierać kontrolę pasma sieciowego 15. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych 16. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN 17. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft 18. Rozwiązanie musi wspierać technologię BitLocker 19. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania 20. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych 21. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych 22. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. 23. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform 24. Rozwiązanie musi wspierać szyfrowanie 25. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne 26. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego 27. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej 28. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |  |

System zostanie wdrożony zostanie w taki sposób, aby był zgodny z zasadą Backup 3-2-1. Jest to to strategia tworzenia kopii zapasowych danych zaprojektowana w celu zapewnienia możliwości szybkiego odzyskania i przywrócenia danych w przypadku incydentu utraty danych. W szczególności strategia tworzenia kopii zapasowych musi zapewniać posiadanie trzech niezależnych kopii danych:

* Pierwsza kopia będzie przechowywana lokalnie na wewnętrznych dyskach twardych np. urządzenia NAS
* Druga kopia będzie przechowywana na taśmach LTO umieszczonych w bibliotece LTO,
* Trzecia kopia danych będzie przechowywana na taśmach LTO (zarówno wielokrotnego zapisu RW jak jednokrotnego zapisu WORM), przy czym taśmy będą umieszczane w bezpiecznym miejscu poza budynkiem Gminy (kopia wyniesiona)

Wdrożony system tworzenia kopii zapasowych musi umożliwiać wysyłanie zaszyfrowanych kopi zapasowych do zasobów chmurowych.

Celem wdrożenia strategii tworzenia kopii zapasowych 3-2-1 jest zmniejszenie potencjalnego wpływu „pojedynczego punktu podatności na awarię”. Oznacza to, że jeśli jedno z urządzeń ulegnie awarii i znajdująca się na nim kopia danych zostanie utracona, do dyspozycji są jeszcze pozostałe dwie kopie danych. Wyniesienie taśm z kompletną kopia zapasową poza budynek Gminy umożliwia natomiast odzyskanie kluczowych danych Zamawiającego w przypadku awarii dużych rozmiarów bądź fizycznego zniszczenia siedziby Zamawiającego (pożar, wybuch, działania terrorystyczne, klęski żywiołowe).

Kluczowym elementem wdrożenia jest opracowanie polityki backupowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.

Polityka backup oraz uruchomione środowisko backup misi być również zgodne z rekomendacją dotycząca wykonywania kopii zapasowych opublikowaną przez Ministerstwo Zdrowia, która dostępna jest pod adresem:

https://www.gov.pl/web/baza-wiedzy/tworzenie-zapasowych-kopii-danych

# Oprogramowanie do wykonywania kopii zapasowych - wznowienie lub nowe licencje

Należy przedłużyć wsparcie dla posiadanego/użytkowanego oprogramowania firmy Veem na okres min. 24 miesięcy lub dostarczyć nowe licencje bezterminowe obejmujące 20 maszyn wirtualnych wraz z wsparciem technicznym producenta na okres min. 24 miesięcy. Minimalne parametry techniczne dla nowych licencji:

1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner:

https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie:

- minimalna liczba referencji 150,

- minimalna ocena z referencji 4,5

1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych
2. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
3. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
4. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
5. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
6. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
7. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
8. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
9. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie.
10. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
11. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
12. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
13. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
14. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
15. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
16. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
18. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
19. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
20. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
21. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru
22. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
23. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
24. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
25. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
26. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
27. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
28. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
29. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
30. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
31. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
32. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
33. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
34. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
35. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
36. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
37. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
38. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
39. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
40. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
41. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
42. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
43. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
44. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
45. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
46. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
47. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
48. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
49. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
50. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
51. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
52. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
53. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
54. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
55. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
56. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
57. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
58. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
59. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
60. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
61. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
62. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
63. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
64. Rozwiązanie musi wspierać system operacyjny macOS
65. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
66. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
67. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
68. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
69. Rozwiązanie musi wspierać backup podłączonych dysków USB
70. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
71. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
72. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
73. Rozwiązanie musi wspierać kontrolę pasma sieciowego
74. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
75. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
76. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
77. Rozwiązanie musi wspierać technologię BitLocker
78. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
79. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
80. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
81. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
82. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
83. Rozwiązanie musi wspierać szyfrowanie
84. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
85. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
86. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
87. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

System tworzenia kopii zostanie wdrożony zostanie w taki sposób, aby był zgodny z zasadą Backup 3-2-1. Jest to to strategia tworzenia kopii zapasowych danych zaprojektowana w celu zapewnienia możliwości szybkiego odzyskania i przywrócenia danych w przypadku incydentu utraty danych. W szczególności strategia tworzenia kopii zapasowych musi zapewniać posiadanie trzech niezależnych kopii danych:

* Pierwsza kopia będzie przechowywana lokalnie na wewnętrznych dyskach twardych np. urządzenia NAS
* Druga kopia będzie przechowywana na taśmach LTO umieszczonych w bibliotece LTO,
* Trzecia kopia danych będzie przechowywana na taśmach LTO (zarówno wielokrotnego zapisu RW jak jednokrotnego zapisu WORM), przy czym taśmy będą umieszczane w bezpiecznym miejscu poza budynkiem Starostwa (kopia wyniesiona)

Wdrożony system tworzenia kopii zapasowych musi umożliwiać wysyłanie zaszyfrowanych kopi zapasowych do zasobów chmurowych.

Celem wdrożenia strategii tworzenia kopii zapasowych 3-2-1 jest zmniejszenie potencjalnego wpływu „pojedynczego punktu podatności na awarię”. Oznacza to, że jeśli jedno z urządzeń ulegnie awarii i znajdująca się na nim kopia danych zostanie utracona, do dyspozycji są jeszcze pozostałe dwie kopie danych. Wyniesienie taśm z kompletną kopia zapasową poza budynek Gminy umożliwia natomiast odzyskanie kluczowych danych Zamawiającego w przypadku awarii dużych rozmiarów bądź fizycznego zniszczenia siedziby Zamawiającego (pożar, wybuch, działania terrorystyczne, klęski żywiołowe).

Kluczowym elementem wdrożenia jest opracowanie polityki backupowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.

Polityka backup oraz uruchomione środowisko backup misi być również zgodne z rekomendacją dotycząca wykonywania kopii zapasowych opublikowaną przez Ministerstwo Zdrowia, która dostępna jest pod adresem:

https://www.gov.pl/web/baza-wiedzy/tworzenie-zapasowych-kopii-danych

# Oprogramowanie do monitorowania infrastruktury informatycznej

W ramach realizacji zadania Wykonawca dostarczy licencje bezterminowe z wsparciem technicznym na okres min. 24 miesięcy, dokona instalacji, konfiguracji oraz podłączenia wszystkich wymaganych systemów będących celem monitorowania. System musi spełniać poniższe wymagania minimalne:

|  |  |
| --- | --- |
| Użytkownicy | |
| 1 | * Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. * Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. * Ograniczania użytkownikom dostępu do wybranych grup hostów. |
| Monitorowanie | |
| 2 | * Monitorowania serwerów fizycznych. * Monitorowania urządzeń sieciowych. * Monitorowania stanu połączeń. * Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów * Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux. * Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych. * Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń. * Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu. * Grupowanie hostów. * Definiowanie planowanych przerw serwisowych dla hostów i usług. * Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK). * Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych). * Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www). * Monitorowanie serwerów za pomocą agentów * Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server. * Monitorowanie Active Directory. * Monitorowanie serwerów plików, udziałów sieciowych. * Monitorowanie statusu serwerów Apache. * Monitorowanie baz danych: * ORACLE, * MySQL, * Postgress. * MSSQL Server * DB2 * Monitorowanie urządzeń przez następujące protokoły: * SNMP, * WMI, * IPMI. * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW. * Monitorowanie poprawności działania DNS. * Monitorowanie środowiska VMware. * Monitorowanie środowiska Hyper-V. * Monitorowanie środowisk Proxmox * Monitorowanie działania serwera czasu NTP. * Monitorowanie offsetu czasu na serwerach. * Monitorowanie ping - czasy odpowiedzi, straty pakietów. * Monitorowanie zajętości miejsca na poszczególnych partycjach. * Monitorowanie obciążenia dysków. * Monitorowanie wykorzystania pamięci RAM. * Monitorowanie obciążenia CPU. * Monitorowanie logów systemowych Windows. * Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia. * Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane. * Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix. * Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence) * Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe * Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów). * Wykrywanie niestabilnie działających usług. * Monitorowanie dostępności stron internetowych. * Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń). |
| Prezentacja | |
| 3 | * Prezentację stanu urządzeń na mapie. * Prezentację danych na dashboardach. * Elastyczną konfigurację dashboardów, wybór elementów. * Wizualizację stanu działania całej infrastruktury na jednym dashboardzie. * Tworzenie indywidualnych dashboardów przez użytkowników |
| Powiadomienia | |
| 4 | * Globalne wyłączanie powiadomień. * Powiadamianie użytkownika o problemach przez e-mail. * Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie. * Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników. * Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług |
| Konfiguracja | |
| 5 | * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW * Automatyczna konfiguracja i działanie z REST-API * Centralne zarządzanie agentami * Integracja danych z różnych źródeł danych (JSON, XML, SNMP) |
| Monitoring bazy danych systemu HIS | |
| 6 | Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:   * Instance state * Version * Jobs * Locks * Processes * Number of active sessions * Recovery area * Log switch activity * General tablespace information * Tablespaces performance * Long active sessions * Undo retention * Checkpoint and online backup state * Custom SQLs * RMAN backup status * RMAN backups * ASM disk groups * Apply and transport lag of Oracle Data-Guard * Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości |
| Kolektor logów | |
| 7 | * System posiada własny kolektor logów syslog * Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps * Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event * Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe. |
| Cyberbezpieczeństwo | |
| 8 | * System monitoruje urządzenia klasy UTM minimum w zakresie: * wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika * monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT. * monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1). * monitoruje aktualną liczbę sesji na urządzeniu * monitoruje liczbę dostępnych tuneli IPSec VPN * monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika. * monitoruje poziom wykorzystania procesora * Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne. * System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog * System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog. |
| Monitoring | |
| 9 | W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:   * Serwer fizyczny – do 5 sztuk * maszyna wirtualna Windows / Linux – do 30 sztuk * serwer AD - 3 sztuki * Macierze / NASy – do 6 sztuk * Przełącznik rdzeniowy – 4 sztuki * Przełącznik dostępowy (LAN) – do 10 sztuk * Zasilacz awaryjny (UPS) - 3 sztuki * Serwer bazodanowy - 4 sztuki * Serwer wirtualizacji (Host, hypervizor) - 4 sztuki * Serwer Backupu - 2 sztuki * W ramach usługi wykonawca monitoruje krytyczne systemy Zamawiającego: * Baza danych systemu księgowego, geodezyjnego, obiegu dokumentów. * Systemów AD, File Serwer, (użytkowany przez Zamawiającego) |

# Dostawa, wdrożenie systemu SIEM (Security Information and Event Management) z usługą zewnętrznego SOC - Centrum Operacji Bezpieczeństwa (Security Operations Center).

Zamawiający wymaga dostarczenia licencji bezterminowych i wdrożenia systemu SIEM z gwarancją oraz wsparciem technicznym na okres min. 12 miesięcy (parametr punktowany dodatkowo) oraz świadczenie usługi SOC (Security Operations Center) przez okres min. 12 miesięcy (**parametr punktowany dodatkowo)  
– Załącznik nr 6 do SWZ.**



## **Słownik pojęć:**

|  |  |
| --- | --- |
| **Skrót lub Pojęcie** | **Opis** |
| **Best Effort** | Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji. |
| **Cyberbezpieczeństwo** | Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego. |
| **Cyberprzestrzeń** | Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem  i komputerem. |
| **Czas** | Wszystkie wskazania w dokumencie w zakresie czasu dotyczą czasu w aktualnej strefie czasowej przyjętej jako czas urzędowy obowiązujący w Polsce. |
| **Departament**  **Bezpieczeństwa** | Komórka organizacyjna w strukturach Zamawiającego, odpowiedzialna za bezpieczeństwo informacji. |
| **Dzień roboczy** | Od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego. |
| **Incydent Bezpieczeństwa**  **Informacji (Incydent)** | Pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. |
| **Koordynator Wykonawcy** | Osoba z ramienia Wykonawcy odpowiedzialna za podejmowanie decyzji w zakresie realizacji spełniania warunków SLA usługi oraz za kontakt  z Zamawiającym. Koordynator może mieć jednego lub wielu zastępców. |
| **Okres przejściowy** | Czas, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie przejęcie wiedzy od Zamawiającego o jego systemie monitoringu, uzgodnienia z Zamawiającym wzoru Miesięcznego Raportu Rozliczenia Usług, ustalenia z Zmawiającym harmonogramu wdrożenia dla pierwszych scenariuszy użycia oraz dopasowanie i uzgodnienie zasad współpracy Zamawiającego  z systemami Wykonawcy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru. |
| **Koordynator**  **Zamawiającego** | Osoba z ramienia Zamawiającego odpowiedzialna za podejmowanie decyzji  w zakresie realizacji usługi. Koordynator może mieć jednego lub wielu zastępców. |
| **Miejsce świadczenia usługi monitorowania cyberbezpieczeństwa** | Miejsce świadczenia usługi Monitorowania Cyberbezpieczeństwa przez zespół Wykonawcy spełniające wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560). |
| **Pierwsza Linia Wsparcia** | Pierwsza Linia Wsparcia SOC – usługa realizująca w szczególności zadania:   * Identyfikacji zdarzeń; * Analizy i eliminacji najprostszych znanych zdarzeń |
| **Druga Linia Wsparcia** | Druga Linia Wsparcia SOC – usługa realizująca w szczególności zadania:   * Współpracy w reakcji na zdarzenia skomplikowane i nieznane; * Tworzenie Scenariuszy Reakcji na powtarzalne zdarzenia; * Nadzór nad poprawnością działania konfiguracji scenariuszy użycia; |
| **On-call** | Dyżur pod telefonem, czekanie w gotowości na zgłoszenie Drugiej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Poważnym. |
| **CTI/OSINT** | Ang. Cyber Threat Inelligence/OpenSource Inteligence - narzędzia dostarczające szczegółowe informacje o technikach hakerskich, zagrożeniach, podatnościach, artefaktach lub umiejętności ich interpretowania i dekodowania oraz czynności pozwalające na pozyskanie informacji z powszechnie dostępnych źródeł umożliwiających powiększenie zakresu wiedzy na temat potencjalnych zagrożeń. |
| **Praca ciągła** | Praca systemu w trybie 24/7/365 dni. |
| **PUODO** | Prezes Urzędu Ochrony Danych Osobowych – organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10 maja 2018 roku o ochronie danych osobowych. Jest również organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych. |
| **RODO** | Ustawa o ochronie danych osobowych z dnia 28 maja 2018 roku uszczegółowiające wymagania Rozporządzenia 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) jest odpowiedzią na wyzwania związane ze zmieniającą się gospodarką dupa osobowymi. |
| **SOC** | Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na cyber zagrożenia. |
| **Scenariusz Reakcji** | Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia nieporządnego, składający się z:   * Zestawu możliwości technicznych wykrycia zdarzenia; * Zdefiniowanych warunków wywołania zdarzenia niepożądanego; * Opisu identyfikacji zdarzeń zależnych; * Instrukcji reakcji na zdarzenie; * Instrukcji uruchomienia działań korekcyjnych; * Instrukcji wykonywania działań informacyjnych; * Ogólnych i szczegółowych ścieżek eskalacyjnych. |
| **Scenariusz użycia systemu bezpieczeństwa** | Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Drugiej Linii Wsparcia, w skład którego wchodzą między innymi:   * Skonfigurowanie jednego lub kilku źródeł zdarzeń; * Przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia. |
| **SLA** | Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagany w zakresie jakościowym. |
| **System analizy logów** | System umożliwiający zbieranie i analizę logów z urządzeń, sieci i systemów informatycznych |
| **Transfer Wiedzy** | Usługa przekazywania kompetencji w zakresie realizacji usług Pierwszej i Drugiej Linii Wsparcia. |
| **Usługa monitorowania**  **Cyberbezpieczeństwa** | Zestaw czynności wykonywanych przez Wykonawcę w ramach umowy w celu identyfikacji Incydentów Bezpieczeństwa Informacji. |
| **Zdarzenia niepożądane** | Zdarzenie mogące wskazywać na wystąpienie incydentu bezpieczeństwa w środowisku chronionym. |
| **Zdarzenie False-Negative** | Wykrycie przez Drugą Linię Wsparcia, zdarzenia nie poprawnie rozpoznanego przy zastosowaniu ustalonych i zaakceptowanych procedur bezpieczeństwa. Realizacja i rozpoznawanie zdarzeń „False-Negative”. |
| **Zdarzenie False-Positive** | Wykrycie przez automatyczne systemy zdarzenia, które po analizie zostało uznane jako zdarzenie poprawne. W przypadku notorycznego występowania, statystycznie rozumianego jako więcej niż 100 zdarzeń „False - Positive” na 1 incydent bezpieczeństwa w miesiącu, należy uznać regułę automatyczną tworzącą takie zdarzenia jako błędną konfigurację systemu bezpieczeństwa. |
| **Przypadek testowy** | Celowe wykonanie pełnego przebiegu zdarzenia od momentu wystąpienia sytuacji niepożądanej do momentu zakończenia przetwarzania fazy analizy incydentu. Gdy jest to możliwe, obejmuje wykonanie odwracalnych kroków reakcji na incydent, sprawdzenie scenariusza end-to-end łącznie z zablokowaniem wskaźników kompromitacji w narzędziach prewencyjnych. |

## **Termin realizacji usługi SOC**

1. Świadczenie Usługi SOC rozpoczęte zostanie w terminie określonym na etapie tworzenia planu wdrożenia.
2. Termin, o którym mowa w punkcie 8.2 podpunkt 1 licząc od dnia podpisania umowy do rozpoczęcia świadczenia usługi, traktuje się jako okres przejściowy, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie dopasowanie i uzgodnienie zasad współpracy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.
3. Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia dostarczone w niniejszym postępowaniu oraz udostępnione przez Zamawiającego. Dostęp do narzędzi i systemów Zamawiającego musi być zrealizowany za pomocą bezpiecznego połączenia szyfrowanego.

## **Wymagania dla Usługi SOC (Security Operations Center)**

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

## **Pierwsza i Druga Linia Wsparcia**

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

### Pierwsza Linia Wsparcia

### W ramach realizacji zadań Pierwszej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

* 1. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa zgodnie warunkami określonymi w punkcie 8 (Ogólne warunki SLA).
  2. Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
  3. Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.
  4. Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.
  5. Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszy Reakcji.
  6. Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
  7. Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).
  8. Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.
  9. Przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa.

### Druga Linia Wsparcia

### W ramach realizacji zadań Drugiej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

* + - 1. Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA (Ogólne warunki SLA).
      2. Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.
      3. Przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami przedstawionymi przez Zamawiającego.
      4. Przygotowanie Scenariuszy Reakcji.
      5. Przygotowanie Miesięcznych raportów z realizacji prac.

## **Scenariusze**

### **Scenariusz użycia systemu bezpieczeństwa**

Zamawiający wymaga przygotowania i wdrożenia możliwych scenariuszy użycia dla zidentyfikowanych przez Zamawiającego ryzyk. Harmonogram wdrożenia zostanie ustalony w okresie przejściowym dla pierwszych scenariuszy użycia, pozostałe scenariusze zostaną przygotowane w uzgodnionym terminie. Każdorazowo Scenariusz użycia musi zostać zaakceptowany przez Zamawiającego. Zamawiający posiada listę przykładowych scenariuszy użycia, które należy przygotować i wdrożyć. Przykładowe scenariusz użycia:

* + - * + Wykrywanie logowania z pominięciem systemu klasy PAM
        + Wykrywanie utworzenia użytkownika (lokalnego i domenowego)
        + Wykrycie złośliwego oprogramowania na chronionym obiekcie

#### Minimalny zakres zadań, z których ma być zbudowany Scenariusz użycia systemu bezpieczeństwa zawiera:

* + - * + Skonfigurowanie jednego lub kilku źródeł zdarzeń,
        + Stworzenie Scenariusza Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia,
        + Opisanie szczegółowej ścieżki eskalacji,

#### Opracowanie scenariusza manualnego lub automatycznego sprawdzania poprawności działania. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek zaktualizować w porozumieniu z Zamawiającym istniejące Scenariusze użycia systemu bezpieczeństwa.

### **Scenariusz Reakcji**

Przygotowany przez Wykonawcę oraz zatwierdzony przez Zamawiającego Scenariusz Reakcji określa minimalny zestaw czynności konieczny do udokumentowania oraz wyciągnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji składa się z podzadań realizujących funkcje:

* + - * **Wzbogacenia** wiedzy o artefaktach tj. adresy IP, domeny, hash’e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez udostępnione narzędzia klasy CTI / OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji,
      * **Analizy** zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia,
      * **Reakcji** rozumianej jako ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym,
      * **Informowania i raportowania** obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.

## **Raport Poincydentalny**

Zamawiający wymaga przygotowania Raportu Poincydentalnego dla incydentów o priorytecie Poważnym i Wysokim nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje:

* + - * Unikalny identyfikator zdarzenia
      * Kiedy incydent wystąpił?
      * Kiedy incydent został zauważony / wykryty?
      * Kto lub jaki proces był sprawcą incydentu?
      * Co się wydarzyło?
      * Gdzie wydarzenie miało miejsce?
      * Dlaczego zdarzenie mogło wystąpić?
      * Jakie czynności zostały przeprowadzone w celu powstrzymania incydentu?
      * Zalecenia Poincydentalne zawierające informację jakie zabezpieczenia zostały ustanowione lub powinny zostać ustanowione w celu zapobieżenia ponownemu wystąpieniu incydentu.

W przypadku przygotowania zaleceń, dla których konieczne jest wprowadzenie istotnych zmian do systemów bezpieczeństwa lub jakiejkolwiek rekonfiguracji systemów Zamawiającego Koordynator Wykonawcy przedstawi do akceptacji Koordynatorowi Zamawiającego zakres i szczegółową listę zmian. Zwolnione z takiej czynności są Zalecenia Poincydentalne konieczne do powstrzymania zidentyfikowanego Incydentu zagrażającego cyberbezpieczeństwu infrastruktury lub danych Zamawiającego.

## **Systemy Zamawiającego wymagające monitorowania**

Usługa monitorowania, będąca przedmiotem zamówienia, może być oparta o logi/dane z poniższych systemów Zamawiającego (źródła logów) udostępnionych przez Zamawiającego:

|  |  |
| --- | --- |
| Rodzaj usługi lub urządzenia | Liczba urządzeń / nodów będących źródłami logów |
| Active Directory (liczba serwerów) | 3 |
| Windows Server | 20 |
| Linux Server | 4 |
| DNS, DHCP | 2 |
| Systemy bezpieczeństwa np.: serwer systemu antywirusowego, web application firewall, inne | 1 |
| Centralny Firewall / UTM | 2 |
| Pomocniczy Firewall / UTM | 2 |
| IPS / IDS | 2 |
| VPN | 1 |
| Przełączniki sieci LAN, punkty dostępowe WiFi | 4 |

Zamawiający na bieżąco będzie aktualizował listę źródeł logów wysyłających nowe dane do Wykonawcy.

## **Wymagania dla Systemu Zbierania i Analizy Logów oraz Systemu SIEM.**

## Wymagania dla Systemu Analizy Logów

### W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.

### Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku Vmware lub Windows Hyper-V

### Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.

### Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.

### Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.

### Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.

### Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.

### Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.

### Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).

### Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.

### Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. –

### Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).

### Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.

### Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).

### Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)

### Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.

### Rozwiązanie musi umożliwiać tworzenie statycznych raportów.

### Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.

### Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.

### Rozwiązanie musi umożliwiać tworzenie własnych raportów.

### Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.

### Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.

**Wymagania systemowe**

### Liczba zdarzeń na sekundę (EPS): min. 9 500

### Zarządzanie logami: min. 2 lata

### Liczba obsługiwanych urządzeń min. 600

### Liczba zapisu zdarzeń na dobę: min 12000 MB

### System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV

## **Wymagania dla Systemu SIEM.**

### W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego

### Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)

### Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.

### Architektura rozwiązania musi być oparta także o fizyczne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich

### Platformy muszą obsługiwać szyfrowanie dysków w standardzie LUKS.

### Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.

### Serwer dedykowany musi posiadać redundantne zasilanie oraz musi być objęty 3 letnim okresem gwarancyjnym w miejscu instalacji.

### Sonda musi posiadać co najmniej 4 porty monitorujące i muszą być w stanie przetworzyć dane dla maksymalnego odbieranego ruchu sieciowego na poziomie 4Gb/s.

### Serwer dedykowany musi obsługiwać do 3 900 zdarzeń na sekundę, musi przechowywać do 9 milionów zdarzeń, musi mieć możliwość detekcji malware, a także musi analizować przy pomocy silnika detekcji shellcode/powershell do 3 na sekundę.

### Licencja na zakup i serwis oprogramowania musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem: 250.

### Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce

### Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.

### Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).

### Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.

### Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

## **Administracja Systemem Analizy Logów:**

W ramach realizacji zadań administracji Systemem Analizy Logów Wykonawca będzie odpowiedzialny za:

### Informowanie Zamawiającego o awariach Systemu Analizy Logów, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie,

### Rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa.

### Optymalizowanie konfiguracji Systemu Analizy Logów w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji.

### Konfigurację Systemu Analizy Logów w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego zgodnie z punktem 86.7

### Weryfikację czy System Analizy Logów prawidłowo analizuje logi

### Tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.

## **Testowanie Systemu Analizy Logów:**

W ramach realizacji zadań testowania Systemu Analizy Logów Wykonawca będzie odpowiedzialny za:

1. Przygotowanie i uzyskanie aprobaty Zamawiającego dla scenariuszy testów Systemu Analizy Logów,
2. Weryfikację wdrożonych scenariuszy użycia oraz implementacji nowych przypadków zgłoszonych przez Zamawiającego,
3. Weryfikację możliwości wdrożenia przypadków użycia w środowisku Zamawiającego,

## **Analiza złośliwego oprogramowania:**

1. W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, nie więcej niż 6 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy.
2. Zakres analizy złośliwego oprogramowania będzie nie mniejszy niż:
3. Analiza statyczna wskazanej próbki złośliwego oprogramowania,
4. Analizy dynamiczna w kontrolowanym środowisku pozwalającym na wyłączenie funkcji ukrywania lub wykrywania analizy,
5. W przypadku wykorzystywania rodziny malware określenia wersji
6. Każdorazowo po wykonanej analizie złośliwego oprogramowania Wykonawca przekaże drogą mailową raport z wykonanej analizy. Zakres raportu zostanie ustalony po podpisaniu umowy.

## **Ogólne warunki SLA**

Wykonawca zapewni świadczenie Usługi monitorowania zgodnie z określonym poziomem SLA.

|  |  |  |
| --- | --- | --- |
| **Nazwa usługi** | **Poziom świadczonej usługi** | |
| **Pierwsza Linia Wsparcia**  Czasy dla pierwszych zdarzeń każdego dnia w wymiarze 30 zdarzeń, pozostałe zadania realizowane będą w trybie ***„Best Effort”*** | Dostępność usługi w dni robocze pomiędzy godzinami  8:00 a 17:00.   |  |  |  | | --- | --- | --- | | Priorytet zdarzenia | Czas od wykrycia przez L1 do | | | Podjęcia | Realizacji | | Poważny | 30 min | 2 h | | Wysoki | 60 min | 6 h | | Średni | 2 h | 12 h | | Niski | 4 h | 24 h | | |
| **Druga Linia Wsparcia**  Czasy dla pierwszych Incydentów każdego dnia w wymiarze 5 incydentów, pozostałe zadania realizowane w trybie ***„Best Effort”*** |  | Dostępność usługi w dni robocze pomiędzy godzinami  8:00 a 17:00.   |  |  |  | | --- | --- | --- | | Priorytet incydentu | Czas od eskalacji pierwszej linii wsparcia do | | | Podjęcia | Realizacji | | Poważny | 30 min | 24 h | | Wysoki | 60 min | 2 dni | | Średni | 2 h | 4 dni | |
| **Analiza złośliwego oprogramowania** | Rozpoczęcie analizy w terminie do 2 dni roboczych od przekazania podejrzanej próbki oprogramowania przez Koordynatora Zamawiającego do Koordynatora Wykonawcy oraz potwierdzenia otrzymania próbki przez Koordynatora Wykonawcy. | |
| **Scenariusz użycia systemu bezpieczeństwa** | Przygotowanie i wdrożenie scenariusza użycia systemu wraz ze scenariuszami reakcji w terminie do 5 dni roboczych od przekazania informacji od Koordynatora Zamawiającego do Koordynatora Wykonawcy z wyjątkiem scenariuszy ujętych w harmonogramie przygotowanym w okresie przejściowym. | |

1. W uzasadnionych przypadkach Wykonawca ma prawo zwrócenia się do Zamawiającego o zgodę na zawieszenie SLA na usługę Pierwszej i Drugiej Linii Wsparcia na uzgodniony z Zamawiającym okres jednak nie dłuższy niż 14 dni. Wniosek o zawieszenie SLA musi zawierać uzasadnienie. Zamawiający w takim przypadku zobowiązany jest do rozpatrzenia prośby w ciągu 1 dnia roboczego od chwili uzyskania informacji o tym fakcie. W przypadku odmowy Zamawiający jest zobowiązany w ciągu 3 Dni Roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.
2. Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia przez pierwsza linię wsparcia a czasem nadania priorytetu.
3. Czas realizacji Incydentu będzie liczony jako delta czasu pomiędzy podjęciem incydentu a zakończeniem obsługi podsumowanym wydanymi wstępnymi rekomendacjami i/lub raportem, w zależności od przypisanego scenariusza reakcji.
4. Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski. Domyślnie każdy incydent zarejestrowany, jeżeli nie zostanie to uszczegółowione inaczej ma priorytet Średni.
5. Minimalny miesięczny czas świadczenia usług analizy zdarzeń to 8 godzin miesięcznie.

|  |  |
| --- | --- |
| **Priorytet** | **Opis** |
| **Poważny** | 1. Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; 2. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika; 3. Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); 4. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; 5. Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; 6. Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; 7. Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; 8. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 9. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; 10. Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; 11. Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej; 12. Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u 13. Zamawiającego procesu eskalacyjnego KSC lub RODO; |
| **Wysoki** | 1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące  o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; 2. Ujawnienie zestawionej sesji zwrotnej z C&C, trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min); 3. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych  w strefie chronionej; 4. Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers; 5. Potwierdzona Informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; 6. Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; 7. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 8. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; 9. Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, upload na dyski webowe lub przenoszenie przez nieautoryzowane pendrive; 10. Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); 11. Ujawnienie nieznanego przez VirusTotal lub inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu; 12. Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; |
| **Średni** | 1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; 2. Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; 3. Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; 4. Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa; 5. Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie; |
| **Niski** | 1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa. |

## **Transfer wiedzy.**

1. Zamawiający wymaga, aby w każdym półroczu trwania umowy, Wykonawca przeprowadził dla grupy nie większej niż 3 osób wskazanych przez Koordynatora Zamawiającego warsztaty. Łączny wymiar godzin w półroczu wynosi nie więcej niż 4. Spotkanie ma formę Warsztatów prowadzonych w formie zdalnej. Niewykorzystane godziny nie kumulują się i nie przechodzą na kolejne okresy.
2. Warsztaty swoim zakresem będą obejmować:

* Wyjaśnianie zagrożeń płynących z wykrytych i opisanych incydentów
* Wyjaśnianie sposobów implementacji zaleceń opisanych w Raportach Miesięcznych
* Szczegółowy harmonogram warsztatów oraz lista uczestników zostaną uzgodnione przez Koordynatorów stron.

1. Raportowanie i rozliczanie pracy
2. Miesięczny Raport Rozliczenia Usług

### Każdy miesiąc świadczenia Usług podsumowany zostanie Raportem Miesięcznym wg według wzoru przedstawionego przez Wykonawcę. Wykonawca zobowiązany jest przedstawić Raport wraz z listą zaleceń do wykonania przez personel Zamawiającego w terminie 5 Dni Roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa.

### Zamawiający zastrzega sobie prawo zgłoszenia zastrzeżeń do Raportu, w terminie do 5 Dni roboczych od dnia jego otrzymania i zażądać uzupełnienia lub poprawy Raportu w terminie do 3 dni roboczych. Po uwzględnieniu przez Wykonawcę uwag do Raportu, Zamawiający w terminie kolejnych 3 Dni roboczych zweryfikuje ostateczną treść Raportu.

### Dostarczony Raport Miesięczny bez uwag jest potwierdzeniem prawidłowego wykonania Usługi w miesiącu, którego dotyczy.

### Raport składa się z sekcji:

#### Monitorowanie cyberbezpieczeństwa

* Data świadczenia usług
* Zestawienie obsłużonych incydentów
  + - * Identyfikator incydentu
      * Nazwa
      * Klasyfikacja priorytetu Incydentu
      * Dokładna data i godzina ujawienia incydentu
      * Statusy końcowe
* Ogólne rekomendacje i zalecenia Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsłużonych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości.

#### Analiza złośliwego oprogramowania

* Data świadczenia usług
* Lista zgłoszonych analiz złośliwego oprogramowania
* Liczba analiz przeprowadzonych zgodnie z SLA

## **Zespół SOC**

Dla zapewnia prawidłowej realizacji usługi SOC Zamawiający stawia minimalny wymóg dla składu zespołu SOC:

1. Operatorzy I linii SOC – 2 osoby
2. Operatorzy II linii SOC – 1 osoba
3. SOC manager – 1 osoba
4. Zarządzania podatnościami – 1 osoba
5. Eksperci od bezpieczeństwa urządzeń – 1 osoba
6. Eksperci od ochrony danych osobowych – 1 osoba
7. Eksperci od zgodności z NIS2 i KSC – 1 osoba

## **Wymagania dodatkowe**

1. Cała dokumentacja powinna być dostarczana w edytowalnej postaci elektronicznej, w formacie przetwarzanym przez MS Word, Excel (od wersji 2007) lub PDF.
2. Zamawiający wymaga zatrudnienia przez Wykonawcę na podstawie umowy o pracę przez cały okres realizacji zamówienia 2 (dwóch) osób, wykonujących usługi w zakresie czynności Pierwszej oraz Drugiej Linii Wsparcia związanych z obsługą realizacji przedmiotu zamówienia, jeżeli wykonywane przez nich czynności polegają na wykonywaniu pracy w rozumieniu przepisu art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 2018 r., poz. 917, z późn. zm.). Zamawiający nie będzie ingerować w sposób prowadzenia działalności oraz organizację pracy administracyjno-biurowej Wykonawcy.
3. Wykonawca zobowiązany zostanie do przestrzegania polityki bezpieczeństwa opisanej w Polityce Bezpieczeństwa Informacji dla dostawców, która stanowi załącznik do umowy. O zmianach polityki mogących mieć wpływ na realizację umowy Wykonawca zostanie bezzwłocznie poinformowany.

## **Opcjonalny moduł EDR (Endpoint Detection and Response - moduł punktowany dodatkowo).**

(Punktowane dodatkowo)- **– Załącznik nr 6 do SWZ.**

Wykonawca wraz z system SIEM może dostarczyć system klasy Endpoint Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla 150 urządzeń wraz z wsparciem technicznym na okres min. 12 miesięcy.

(Uwaga: Oferowany okres wsparcia dodatkowo punktowany)- Załącznik nr 6 do SWZ.

Minimalne wymagania dla systemu EDR:

1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS umożliwiające bezproblemową współpracę z systemem antywirusowym do ochrony stacji roboczych, użytkowanym przez Zamawiającego.
2. Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
6. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
7. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
8. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
11. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
12. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
13. Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14. Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
15. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe.
16. Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
17. Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
18. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
19. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
20. Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.

## **Opcjonalny moduł NDR (Network Detection and Response - moduł punktowany dodatkowo).**

(Punktowane dodatkowo)– Załącznik nr 6 do SWZ.

Wykonawca wraz z system SIEM może dostarczyć system klasy Network Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla 200 adresów IP wraz z wsparciem technicznym na okres min. 12 miesięcy.

(Uwaga: Oferowany okres wsparcia dodatkowo punktowany) – Załącznik nr 6 do SWZ.

Minimalne wymagania dla systemu NDR:

1. Wielowątkowy silnik detekcji umożliwiający obsługę ruchu liczonego w dziesiątkach Gigabitów

* Możliwość obsługi wielu podsieci VLAN
* Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
* Obsługa biblioteki wyrażeń regularnych HyperScan
* Możliwość aktualizacji reguł bez wyłączania/ponownego uruchamiania silnika detekcji

1. Obsługa wielowątkowości procesora
2. Możliwość analizy kopii ruchu w sieci LAN w czasie rzeczywistym bez ingerencji w ruch sieciowy
3. Rejestracja żądań HTTP
4. Rejestracja i przechowywanie certyfikatów TLS
5. Możliwość wyodrębnienia plików z analizowanego ruchu sieciowego i zapisania ich na dysku do późniejszej analizy
6. Możliwość przechwytywania pakietów danych przesyłanych w sieci LAN i zapisywanie ich dla późniejszej analizy offline
7. Tworzenie raportów w przypadku wykrycia ruchu opisanego regułami jako ruch niebezpieczny
8. Rejestrowanie i dogłębna analiza ruchu szyfrowanego TLS/SSL
9. Rejestrowanie wszystkich kluczy wymiany do analizy oraz w celu zapobiegania podmianie
10. Rejestrowanie, zapisywanie ruchu HTTP z dowolnego portu do pliku w celu późniejszej analizy
11. Możliwość identyfikacji, wyodrębniania i rejestrowania plików w ruchu HTTP
12. Rejestracja wszystkich zapytań i odpowiedzi DNS
13. Funkcja wykrywania włamań sieciowych
14. Funkcja zapobiegania włamaniom sieciowym
15. funkcja monitorowania bezpieczeństwa sieci LAN
16. Pełne wsparcie dla protokołu IPv6
17. Możliwość dekodowania tuneli: IP-IP, IP6-IP4, IP4-IP6, GRE, VXLAN, Geneve, Teredo
18. Silnik analizy strumienia danych TCP
19. Defragmentacja pakietów w celu poddania ich analizie IPS
20. Możliwość obsługi wielu podsieci VLAN
21. Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
22. Możliwość modyfikacji reguł
23. Możliwość zdefiniowania niebezpiecznych plików przez parametry: wielkość, nazwa, rozszerzenie
24. Możliwość wykrywania złośliwego oprogramowania w oparciu o odcisk palca JA3, JA3S
25. Możliwość wykrywania złośliwego oprogramowania w oparciu o metodę HASSH
26. Obsługa dekodowania pakietów: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN
27. Dekodowanie warstwy aplikacji: HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP, RFB
28. Możliwość tworzenia raportów zgodnych z standardem JSON, SYSLOG,
29. Możliwość filtrowania alertów z podziałem na wagę/priorytet
30. Możliwość filtrowania alertów dla wybranej reguły z podziałem na wagę/priorytet
31. Wspierane systemy operacyjne: Windows, Linux, FreeBSD, OpenBSD, MacOS, Mac OS X
32. Obsługa przekazywania alertów „dalej” do systemów takich jak: syslog, eve.log, JSON, Unified 2
33. Filtrowanie alertów na poziomie: reguł, hostów, sieci

# Zakup bibliotek taśmowych do przechowywania kopii zapasowych

Zamawiający posiada dwa niezależne środowiska informatyczne, dla których tworzone będą dedykowane kopie zapasowe. Obecnie dla jednego środowiska Zamawiający posiada licencje do tworzenia kopii zapasowych, a dla drugiego zostaną zakupione w niniejszym postępowaniu – punkt 5.

Każde z środowisk zostanie rozbudowane o bibliotekę taśmową LTO wraz z kompletem taśm. Dostarczone dwa urządzenia muszą współpracować z posiadanym systemem tworzenia kopii zapasowych z punktu 6 (lub nowym, oferowanym oprogramowaniem) oraz nowym oprogramowaniem opisanym w punkcie 5. Biblioteki musza spełniać poniższe wymagania minimalne:

|  |  |
| --- | --- |
| **Właściwość** | **Parametry minimalne** |
| Obudowa | Obudowa typu Rack o wysokości max 2U |
| Typ napędu LTO | Min. LTO8 |
| Ilość napędów | Min. 1, możliwość rozbudowy do min. 2 napędów LTO |
| Technologie obsługiwanych napędów | Min. LTO 6,7,8,9 |
| Interfejs komunikacyjny | Fibre Channel min. 8Gbps |
| Maksymalna, możliwa pojemność danych | Min. 270 TB natywnie oraz 710 TB z użyciem kompresji danych |
| Maksymalny transfer danych w oferowanej konfiguracji | Min. 270 mb/s |
| Ilość slotów na taśmy | Min. 24 |
| Panel diagnostyczny | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie  informacji o stanie urządzenia |
| Możliwość szyfrowania danych | Min. Kluczem AES256 |
| Złącza | Min. 1 x LC optyczne, min 1 x RJ45 oraz min. 1x USB |
| Zarządzanie | - komunikacja poprzez interfejs RJ45  - wbudowana diagnostyka  - wsparcie dla IPv4 i Ipv6  - sterowniki do Windows Serwer 2008/2012 R2/2016/2019 /2022 |
| Wyposażenie | Wraz z urządzeniem należy dostarczyć 15 taśm LT08 RW, 7 taśm LTO8 WORM z zestawem etykiet oraz 1 taśmę czyszczącą, kable połączeniowe zasilające oraz 2 kable LC-LC min. OM4 o długości min. 3mb do połączenia z siecią SAN. |
| Wsparcie techniczne | 3-letnia gwarancja producenta w miejscu instalacji w następny dzień roboczy. Wsparcie techniczne realizowane przez serwis producenta oferowanego urządzenia. |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. Oferowany napęd LTO musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Windows Server 2008 R2. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

Wykonawca wraz z bibliotekami taśmowymi dostarczy wszystkie niezbędne materiały (kable, listwy zasilające itp.) niezbędne do uruchomienia bibliotek. Zamawiający wymaga instalacji bibliotek w wskazanych szafach rack, podłączenia do serwerów backupu, konfiguracji do pracy w infrastrukturze Zamawiającego. Aktualizacji firmware do najnowszej dostępnej, stabilnej wersji. Usługi muszą zostać wykonane w taki sposób, aby nie zakłócać ciągłości pracy kluczowych systemów Zamawiającego. Biblioteki musza zostać skonfigurowane przez Wykonawcę zgodnie z wymaganiami Zamawiającego z wykorzystaniem dostarczonego przez Wykonawcę systemu kopii zapasowych (punkty 5,6).

# Zakup certyfikatu SSL do zabezpieczenia domeny i certyfikatów poczty elektronicznej

Przedmiotem zadania jest dostawa certyfikatu SSL „wild card” dla domeny oraz certyfikatów S/MIME – 70 szt. które będą zabezpieczały pocztę Zamawiającego.

Minimalne wymagania dla certyfikatu:

* zabezpieczenie dla min. 4 domen
* automatyczna walidacja domeny
* obsługa krzywych eliptycznych
* zabezpieczenie gwarancyjne min. 200 000 Euro

Wykonawca dostarczy, zainstaluje certyfikat SSL na serwerze, dokona implementacji na stronie WWW.

Wykonawca skonfiguruje rekordy SPF (Sender Policy Framework) zgodnie z wymagania Zamawiającego.

Wykonawca skonfiguruje mechanizm DKIM (DomainKeys Identified Mail) na serwerze pocztowym Zamawiającego.

Wykonawca skonfiguruje mechanizm potwierdzenia domeny nadawcy DMARC (Domain-based Message Authentication, Reporting and Conformance) w oparciu o zabezpieczenia SPF lub DKIM.

# System do inwentaryzacji zasobów infrastruktury informatycznej, zarządzania zgłoszeniami *- moduł punktowany dodatkowo*

Wykonawca dostarczy, zainstaluje oprogramowanie na zasobach Zamawiającego. Skonfiguruje do używania w pełnym wymaganym przez Zamawiającego zakresie.

(Uwaga: parametr nr 25 dodatkowo punktowany)– Załącznik nr 6 do SWZ.

Minimalne wymagania dla systemu:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ |
|  | Licencja bezterminowa | TAK |  |
|  | Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej. | TAK |  |
|  | Składowe systemu (min. wymagany zakres):   * inwentaryzacja komputerów i serwerów, * inwentaryzacja serwerów wirtualizacji i maszyn wirtualnych, * inwentaryzacja systemów operacyjnych, * inwentaryzacja aplikacji i pakietów, * inwentaryzacja plików, * inwentaryzacja drukarek, * inwentaryzacja wszystkich typów urządzeń, * inwentaryzacja materiałów eksploatacyjnych, |  |  |
|  | Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników. | TAK |  |
|  | Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control). | TAK |  |
|  | Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu). | TAK |  |
|  | Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról. | TAK |  |
|  | Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java. | TAK |  |
|  | Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych. | TAK |  |
|  | Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty. | TAK |  |
|  | Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego. | TAK |  |
|  | Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, predefiniowane atrybuty komputera. | TAK |  |
|  | Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, | TAK |  |
|  | Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów. | TAK |  |
|  | Szkolenie personelu w zakresie eksploatacji i obsługi w miejscu instalacji. | TAK |  |
|  | Oprogramowanie musi posiadać wbudowany moduł HelpDesk z dedykowanym portalem WWW dla użytkowników, umożliwiającym przesyłanie zgłoszeń dotyczących awarii sprzętu. | TAK |  |
|  | Moduł HelpDesk musi umożliwiać zarządzanie zmianą operatorów. | TAK |  |
|  | Moduł HelpDesk musi posiadać wbudowany moduł planowania zadań na podstawie ich priorytetu. Zaplanowane zadania zostaną umieszczone na widoku kalendarzu, harmonogramu. | TAK |  |
|  | Oprogramowanie musi umożliwiać inwentaryzację innych pasywnych elementów takich jak: Szafy RACK, Kable, Listwy zasilające, Karty SIM, Telefony, Urządzenia USB, Kartridże | TAK |  |
|  | Oprogramowanie musi umożliwiać inwentaryzowanie zakupionych licencji oraz powiadamiać o czasie ich wygaśnięcia. Licencje muszą mieć możliwość przypisywania do jednostek, grupy, użytkowników, którzy je wykorzystują. | TAK |  |
|  | Oprogramowanie musi umożliwiać tworzenie bazy danych kontaktów, dostawców. | TAK |  |
|  | Oprogramowanie musi umożliwiać tworzenie kontraktów, zapisów dotyczących umów serwisowych zawartych z zewnętrznymi organami. | TAK |  |
|  | Oprogramowanie musi posiadać moduł Baza Wiedzy, gdzie Administratorzy mogą prowadzić notatki, tworzyć wpisy i udostępniać je dla wybranych użytkowników. | TAK |  |
|  | Oprogramowanie musi posiadać możliwość tworzenia akcji automatycznych, definiowanych przez administratora, które umożliwią aktualizację rekordów w bazie i wysyłanie powiadomień. | TAK |  |
|  | System do zarządzania zgłoszeniami posiadający funkcjonalność zarządzania projektami w tym: tworzenie raportów, tablic Kanban, wykresów GANTTA, tworzenie i przydzielanie zadań współpracownikom | NIE: 0 pkt  TAK: 5 pkt |  |
|  | Okres gwarancji | min. 24 miesiące |  |

# Zakup gwarancji producenta dla posiadanych serwerów i macierzy

Przedmiotem zadania jest przedłużenie gwarancji producenta dla użytkowanych dwóch serwerów oraz macierzy firmy HPE, na kolejne 2 lata:

* serwery HPE Proliant DL380 Gen10 o numerach seryjnych: CZ284907DF, CZ284907DG
* macierzy dyskowej HPE MSA 2050 o numerze seryjnym: 2S6842B308, 2S6838B530

# Szkolenia z zakresu Cyberbezpieczeństwa dla administratora

Zamawiający wymaga dostarczenia voucherów na szkolenia z zakresu Cyberbezpieczeństwa dla administratora. Dla każdego szkolenia należy dostarczyć jeden voucher, każdy musi być ważny przez okres min. 6 miesięcy. Szkolenia muszą być prowadzone przez profesjonalnego instruktora w formie zdalnej, w dni robocze. Lista wymaganych szkoleń poniżej. Minimalny zakres szkoleń w linkach poniżej:

* + - 1. Szkolenie – Wprowadzenie do technik analizy pakietów sieciowych - technika używana do przeglądania w czasie rzeczywistym nieprzetworzonych danych wysyłanych i odbieranych przez interfejs sieciowy. Analiza z wykorzystaniem produktu Wireshark - darmowego analizatora pakietów typu open source.

Zakres szkolenia:

* Przegląd Koncepcji Rozwiązywania Problemów z Siecią
* Przegląd Funkcji Wireshark
* Nawigacja po interfejsie użytkownika
* Przechwytywanie ruchu w środowisku testowym
* Wybór interfejsu sieciowego
* Przechwytywanie pakietów w sieciach przewodowych i bezprzewodowych
* Analiza logów
* Inspekcja pakietów HTTP
* Przeglądanie strumieni TCP
* Zapisywanie logów do analizy offline
* Analiza problemów z szybkością połączenia podczas łączenia się z konkretną stroną internetową
* Korzystanie z filtrów
* Przeglądanie statystyk
* Analiza według typu ruchu
* DNS, ARP, IPv4, IPv6, ICMP, UDP, TCP oraz HTTP/HTTPS
* Systematycznie wolne połączenia przez dłuższy czas
* Sprawdzanie czasów odpowiedzi
* Ustawianie kolumn czasu delta
* Sprawdzanie komputerów zainfekowanych wirusem
* Inspekcja ruchu ARP
* Inspekcja źródeł ruchu sieciowego
* Sonda Intel ANS
* Uszkodzone/nieprawidłowo skonfigurowane oprogramowanie (zalewanie sieci)
* Wskazywanie problemów z wydajnością
* Tworzenie statystycznych wykresów i diagramów
* Ustawianie kolorów w Wireshark
* Filtrowanie ruchu
* Korzystanie z systemu eksperckiego Wireshark i schematu rozwiązywania problemów TCP/IP
* Rozwiązywanie problemów z połączeniami w zabezpieczonym środowisku sieciowym
* Proksy, zapory i klienci
* Konfiguracja Wireshark dla optymalnej wydajności
* Analiza nieinwazyjna
* Rozwiązywanie problemów
  + - 1. Szkolenie – Zaawansowane techniki analizy i rozwiązywania problemów siecią z wykorzystaniem narzędzia Wireshark. Zakres szkolenia:
* Narzędzia analizy z poziomu wiersza poleceń
* Zaawansowane korzystanie z filtrów przechwytywania i wyświetlania
* Pisanie zaawansowanych skryptów filtrów Capture
* Pisanie zaawansowanych filtrów wyświetlania
* Podstawowa komunikacja sieciowa
* Luki w procesie rozpoznawania protokołu TCP/IP
* Skanowanie portów
* Skany mutantów
* Skanowanie IP
* Mapowanie aplikacji
* Analiza VoIP
* Analiza SIP i rozwiązywanie problemów
* RTP, RTCP i analiza mediów
* Tworzenie filtrów VoIP i profili analitycznych
* Analiza aplikacji i rozwiązywanie problemów
* Analiza protokołu HTTP i rozwiązywanie problemów
* Analiza FTP i rozwiązywanie problemów
* Obsługa DNS i rozwiązywanie problemów
* Analiza transmisji wideo
* Problemy związane z siecią baz danych
* Podstawy bezpieczeństwa sieci i kryminalistyki
* Wykrywanie podejrzanych wzorców bezpieczeństwa
* Podszywanie się pod adresy MAC i IP
* Atakuje sygnatury i lokalizacje sygnatur
* Zatrucie ARP
* Nagłówek i podpisy sekwencyjne
* Ataki i exploity
* Splicing TCP i nietypowy ruch
* Ataki DoS i DDoS
* Skanowanie protokołu
  + - 1. Szkolenie – Certyfikowany administrator systemu LINUX – poziom podstawowy. Celem szkolenia jest zapoznanie z zasadami działania systemu operacyjnego Linux. Zakres szkolenia:
* praca w linii komend Linuxa, korzystając ze strumieni, potoków i przekserowań;
* tworzenie i zarządzanie dostępem do plików i katalogów;
* edytowanie plików tekstowych edytorem vi;
* zarządzanie procesami w systemie;
* tworzenie i zarządzanie partycjami i systemami plików;
* jak instalować, aktualizować i odinstalowywać oprogramowanie przy użyciu managerów oprogramowania debiana, rpm, yum;
* sposób obsługi urządzeń w systemie Linux;
* proces uruchamiania systemu, oraz modyfikować opcje boot leadera;
  + - 1. Szkolenie – Certyfikowany administrator systemu LINUX – poziom zaawansowany. Celem szkolenia jest zapoznanie z zasadami działania systemu operacyjnego Linux. Zakres szkolenia:
* konfigurowanie środowisko pracy;
* jak pisać i modyfikować proste skrypty;
* jak używać podstawowych komend SQL;
* instalowanie i konfigurowanie środowiska graficznego;
* zarządzanie użytkownikami i grupami;
* automatyzowanie zadania;
* konfigurowanie drukarki;
* jak konfigurować logi systemowe;
* podstawy protokołu TCP/IP;
* konfigurowanie sieci;
* bezpieczeństwo systemu.
  + - 1. Szkolenie – Linux Administracja poziom zaawansowany. Zakres szkolenia:
* instalować i konfigurować serwery: www, proxy, samba, dhcp, poczty, ftp, ssh;
* diagnozować i rozwiązywać problemy występujące w systemie;
* korzystać z klienta LDAP;
* konfigurować ustawienia związane z bezpieczeństwem systemu;
* konfigurować routing statyczny;
* konfigurować firewall systemowy.
  + - 1. Szkolenie – Programowanie w powłoce BASH. Zakres szkolenia:
* Wstęp do pisania skryptów
* Wybór powłoki (magic number #!, sha-bang)
* Wywoływanie skryptu
* Zmienne i parametry
* Niszczenie zmiennych (unset)
* Zmienna o wartości null
* Zmienne lokalne, zmienne środowiskowe (export)
* Parametry wywołania skryptu ($0, $#, $1, $2, $3....)
* Symbole wieloznaczne (wildcards)
* Znaki ucieczkie (escaped characters)
* Kończenie skryptu
* Instrukcja exit
* Wykorszystanie statusu zakończenie programu w skryptach ($?)
* Konstrukcja testu
* Operatory porównania
* Stałe numeryczne
* Pętle
* Instrukcja case
* Automatyzacja przy użyciu języka AWK
  + - 1. Szkolenie – Linux – bezpieczeństwo systemu. Zakres szkolenia:
* Analiza ryzyka, kosztów i zysków związanych z bezpieczeństwem
* Role administratorów i użytkowników
* Bezpieczeństwo konsoli: bezpieczeństwo konsoli fizycznej, bezpieczeństwo konsoli zdalnej
* Bezpieczeństwo systemów plików
* backup system
* Techniki i infrastruktury uwierzytelniania
* Dzienniki systemowe
* Zabezpieczanie sieci
* Główne założenia konfiguracyjne firewall'a
* Konfiguracja firewalld
* Omówienie filtrów pakietowych
* usługa NAT w systemie Linux.
* Wirtualne Sieci Prywatne
* Wykrywanie włamań do sieci i metody reakcji na incydenty
  + - 1. Szkolenie – Open Source Virtualization. Zakres szkolenia:
* Przegląd wirtualizacji
* Architektura KVM I jej związek z Linuxem
* KVM z użyciem QEMU
* Obsługa sprzętu
* Optymalizacja wydajności
* Bezpieczeństwo w KVM
* Architektura hipernadzorcy XEN
* Instalacja i konfiguracja Xen
* Administracja domenami XEN
* Wydajność i optymalizacja XEN
* Bezpieczeństwo w XEN
* Praca z kontenerami w Linuxie
  + - 1. Szkolenie – Bezpieczeństwo Windows. Zakres szkolenia:
* model “Cyber Kill Chain” w kontekście bezpieczeństwa infrastruktury Windows,
* obszary ataku na systemy Microsoft Windows,
* jak identyfikować systemy Windows w sieci komputerowej, oraz określać oferowane przez nie usługi za pomocą narzędzi do skanowania sieci komputerowych,
* jak prawidłowo przeprowadzać skanowanie podatności w sieci LAN,
* słabe punkty - podatności poprzez sieć komputerową przy dostępie lokalnym oraz zdalnym,
* jak przejąć kontrolę nad systemem operacyjnym Windows,
* eskalowanie uprawnień w środowisku Active Directory w celu przejęcia kontroli nad usługą,
* jak poprawnie zabezpieczać środowisko stacji roboczych przed omawianymi zagrożeniami,
* wdrażanie zabezpieczeń Active Directory w celu utrudnienia skompromitowania usługi.
  + - 1. Szkolenie – Administrowanie z PowerShell cz. I. Zakres szkolenia:
* Jak wyszukiwać i identyfikować polecenia PowerShell do wykonania wybranych czynności administracyjnych.
* praca z PowerShell pipeline,
* Praca ze zmiennymi, tablicami i listami,
* podstawowe skrypty przy użyciu PowerShell,
* import i eksport danych do PowerShell,
* podstawowy sposób obsługi błędów,
* jak używać PSProviders i PSDrives.
* przeszukiwanie informacji w systemie za pomocą WMI i CIM.
* administrowanie zdalnymi komputerami przy użyciu PowerShell
* zarządzanie usługami w chmurze publicznej Microsoft Azure
  + - 1. Szkolenie – Administrowanie z PowerShell cz. II. Zakres szkolenia:
* zaawansowane funkcje z obsługą parametrów -whatif i -confirm
* walidacja przekazywanych do funkcji danych,
* błędy oraz dokumentacja skryptów,
* dane wyjściowe ze skryptu m.in. w formacie XML, JSON i inne
* skrypty współpracujące z użytkownikiem
  + - 1. Szkolenie – Certified Ethical Hacker. Zakres szkolenia:
* Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking)
* Zbieranie informacji o ataku (Footprinting and Reconnaissance)
* Skanowanie sieci (Scanning Networks)
* Enumeracja (Enumeration)
* Analiza podatności (Vulnerability Analysis)
* Hackowanie systemu (System Hacking)
* Złośliwe oprogramowanie (Malware Threats)
* Monitorowanie i przechwytywanie danych (Sniffing)
* Inżynieria społeczna – socjotechniki (Social Engineering)
* Ataki DDoS (Denial-of-Service)
* Przejęcie/przechwytywanie sesji (Session Hijacking)
* Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots)
* Hakowanie serwerów sieciowych (Hacking Web Servers)
* Hakowanie aplikacji internetowych (Hacking Web Applications)
* Ataki przez zapytania w SQL (SQL Injection)
* Hakowanie sieci bezprzewodowych (Hacking Wireless Networks)
* Hakowanie mobilnych platform (Hacking Mobile Platforms)
* Hakowanie Internetu Rzeczy (IoT Hacking)
* Bezpieczeństwo chmury (Cloud Computing)
* Kryptografia (Cryptography)
  + - 1. Szkolenie – Testy penetracyjne. Zakres szkolenia:
* Etapy prowadzenia testów penetracyjnych
* Przykładowy harmonogram testów penetracyjnych
* Modyfikacja komunikacji sieciowej
* Bezpieczeństwo sieci – Ethernet
* Podsłuchiwanie rozmów VoIP – LAB zawierający realne telefony IP
* Podsłuch transmisji w środowisku switchowanym – atak klasy MAC flooding (port stealing)
* Podsłuch transmisji w środowisku switchowanym – atak klasy ARP Poison Routing
* Atak man-in-the-middle w środowisku switchowanym – na serwis chroniony protokołem HTTPS
* Ustawienie wrogiego serwera DHCP oraz wykonanie ataku klasy man-in-the middle na serwis www chroniony protokołem HTTPS
* Wybrane zagadnienia bezpieczeństwa protokołów działających pomiędzy switchami.
* Bezpieczeństwo warstwy 3 modelu OSI
* Skanowanie portów TCP/UDP na wybranym serwerze
* Skanowanie wybranego urządzenia a skanowanie wybranej podsieci.
* Wykorzystanie ndiff jako narzędzia wspierającego mapowanie zmian w aktywnych usługach działających w sieci.
* Określenie oprogramowania działającego na docelowym serwerze (oprogramowanie usługowe oraz wersja systemu operacyjnego)
* Wykrywanie firewalla bezstanowego oraz omijanie oferowanych przez niego zabezpieczeń
* Wykorzystanie oprogramowania nmap do skanowania urządzenia sieciowego
* Wykorzystanie oprogramowania hping do badania szczelności firewalla
* Bezpieczeństwo IPsec
* Skanowanie VPN (na podstawie IPsec)
* Brute force hasła dostępowego dla IPsec
* Bezpieczeństwo protokołów routingu
* Wstęp do bezpieczeństwa systemów webowych (WWW)
* Systemy klasy IPS (Intrusion Prevention System) oraz firewalle aplikacyjne
* Metody testowania bezpieczeństwa systemu IDS
* Omijanie systemów IPS / Application Firewall (na przykładzie infrastruktury web)
  + - 1. Szkolenie – Bezpieczeństwo Windows. Zakres szkolenia:
* popularne ataki na Windows
* monitorowanie wydarzeń w Windows
* architektura systemu
* jak reagować na incydenty
* mechanizmy obronne
* sposoby automatyzacji zabezpieczeń
* rola domeny i kontrolerów domeny
* pliki POL
* szablony
* klient GPO
* rozszerzenia GPO
* zarządzanie GPO

# Szkolenie z zakresu cyberbezpieczeństwa dla pracowników – platforma szkoleniowa

Wykonawca udostępni Zamawiającemu platformę szkoleniową umożliwiającą przeprowadzenie szkoleń z zakresu podstaw Cyberbezpieczeństwa dla pracowników Gminy. Minimalny zakres szkolenia dostępnego na platformie:

**Moduł 1: Wprowadzenie**

Czy w cyfrowym świecie naprawdę jest niebezpiecznie?

Czym ryzykujemy zaniedbując bezpieczeństwo?

Co zrobić, gdy popełniliśmy błąd w security?

Co można stracić

**Moduł 2: Wiedza podstawowa**

Jak dbać o swoje stanowisko pracy

Unikanie ryzykownego sprzętu elektronicznego

Podstawowe oprogramowanie zabezpieczające

Wewnętrzne szkolenia z bezpieczeństwa

**Moduł 3: Jak nas podejść, popularne techniki ataków**  
Socjotechnika  
Phishing  
Ransomware

**Moduł 4: Jak się bronić**- hasła  
- jako korzystać i chronić  
- zabezpieczenie wieloczynnikowe  
- antywirus  
- kopie zapasowe  
- aktualizacja oprogramowania  
- zaufanie, a właściwie jego brak  
- szyfrowanie danych

**Moduł 5: Co chronimy**Twoje dane  
Email -dlaczego należy chronić  
Przeglądarka, telefon, karty, komputer

**Moduł 6: użyteczne oprogramowanie**

Samodzielne rozwijanie wiedzy o bezpieczeństwie

Jeśli wyjdziesz z zamku, jego mury Cię nie obronią - dyscyplina

Polityka prywatności, RODO i prawidłowe przetwarzanie danych wrażliwych

**Moduł 7: Bezpieczne hasła**

Jakie hasła są naprawdę bezpieczne?

Korzyści ze sprawdzonego narzędzia - KeePass

Instalacja i konfiguracja KeePass

Dodawanie i używanie własnych haseł w KeePass

Jak współdzielić hasła firmowe za pomocą KeePass

**Moduł 8: Uwierzytelnianie dwuskładnikowe**

Obrona przed wyciekiem haseł

Czym jest uwierzytelnianie dwuskładnikowe?

Jakie rodzaje dodatkowych poświadczeń możemy wykorzystać?

Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Google

Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Facebook

Do jakich usług zaleca się koniecznie korzystać z uwierzytelnienia dwuskładnikowego?

**Moduł 9: Email oraz przeglądarka internetowa**

Co robimy, a co nie w przeglądarce

Jak bezpiecznie używać poczty elektronicznej

**Moduł 10: Smartfony i tablety**

Może lepiej nie korzystać ze wzoru bezpieczeństwa?

Ile zajmuje włamywaczowi zainstalowanie szkodliwego programu na smartfonie?

Czy można instalować aplikacje spoza sklepu google play?

Ogranicz zaufanie do osób kontaktujących się telefonicznie

**Moduł 11: Zagrożenia w pracy zdalnej**

Domownicy i własne dzieci mogą niecelowo Ci zaszkodzić

Jak nie dać sobie ukraść danych osobowych

Przechwycenie tożsamości i oszuści na portalach społecznościowych

Okazje, zaskakująco dobre oferty i wygrane w konkursach

**Moduł 12: Szkodliwe oprogramowanie, "robaki"**

Czym jest Bloatware i jak można się go pozbyć

Jak sprawdzić czy jakiś plik jest bezpieczny

Jak poznać się, że program spowalnia komputer

# Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

**Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001:2022 z 25 października 2022 roku.**

ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie „Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych” w §20 „System zarządzania bezpieczeństwem informacji” (SZBI) zobowiązuje instytucje publiczne do opracowania strategii działania SZBI rozumianej jako zespół dobrych praktyk, mających na celu dbałość o bezpieczeństwo informacji w Gminie. Podejście bazuje na szacowaniu ryzyka   
i poziomach akceptacji ryzyka dla organizacji zaprojektowanych, tak aby skutecznie postępować i zarządzać ryzykiem. Na SZBI składają się: polityka, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. Wymagane jest zapewnienie poufności, integralności i dostępności informacji.

Wymagania minimalne dla dokumentacji SZBI:

1. Procedury operacyjne
   1. Procedura identyfikacji zagrożeń i oceny ryzyka
   2. Procedura zarządzania ryzykiem
   3. Procedura nadzorowania systemu informacji
   4. Procedura zarządzania dostępem
   5. Procedura zarządzania incydentami bezpieczeństwa informacji
   6. Procedura monitorowania i audytu
   7. Procedura zarządzania zmianami
   8. Procedura zarządzania dostawcami
   9. Procedura zarządzania ciągłością działania
   10. Procedura zarządzania szkoleniami i świadomością
2. Instrukcje operacyjne
   1. Instrukcja tworzenia haseł
   2. Instrukcja obsługi systemów bezpieczeństwa
   3. Instrukcja obsługi narzędzi monitorujących
   4. Instrukcja obsługi procedury audytu
   5. Instrukcja obsługi systemu raportowania incydentów
   6. Instrukcja obsługi narzędzi zarządzania ryzykiem
   7. Instrukcja obsługi systemu zarządzania dokumentacją
3. Instrukcje techniczne
   1. Instrukcja konfiguracji oprogramowania antywirusowego
   2. Instrukcja konfiguracji zapór sieciowych
   3. Instrukcja konfiguracji systemów monitorowania
   4. Instrukcja konfiguracji narzędzi szyfrowania danych
   5. Instrukcja konfiguracji systemów uwierzytelniania
4. Plany i strategie
   1. Plan zarządzania incydentami
   2. Plan ciągłości działania
   3. Strategia zapewnienia bezpieczeństwa fizycznego
   4. Strategia monitorowania i audytu
   5. Strategia zarządzania zmianami
   6. Strategia zarządzania dostawcami
   7. Strategia zarządzania ryzykiem
   8. Strategia zarządzania dostępem
   9. Strategia zarządzania szkoleniami i świadomością
5. Rejestr dokumentów i rejestr zabezpieczeń
6. Raporty i dokumentacja audytowa
7. Procesy certyfikacji i dokumentacja związana z audytem certyfikującym
8. Schemat organizacyjny i uprawnienia w zakresie zarządzania SZBI
9. Plan komunikacji wewnętrznej w zakresie SZBI
10. Dokumentacja związana z wdrożeniem systemu zarządzania SZBI
11. Procesy kontrolne i monitorujące związane z dokumentacją SZBI
12. Dokumentacja szkoleń pracowników w zakresie SZBI
13. Ewidencja incydentów bezpieczeństwa informacji
14. Zasoby związane z audytem wewnętrznym i zewnętrznym
15. Procedury dokumentacji zmian w systemie zarządzania SZBI
16. Mapy procesów w zakresie zarządzania bezpieczeństwem informacji
17. Procedury oceny zgodności z wymaganiami normy ISO 27001
18. Dokumentacja dotycząca ewaluacji efektywności systemu zarządzania SZBI
19. Dokumentacja dotycząca audytu wewnętrznego
20. Raporty dotyczące wyników audytów i przeglądów SZBI
21. Dokumentacja dotycząca działań korygujących i zapobiegawczych
22. Procedury dokumentacji usuwania danych i aktywów
23. Instrukcje dotyczące kierowania wypadkami i awariami
24. Procedury dokumentacji zarządzania systemami monitoringu i wykrywania zagrożeń
25. Procedury dokumentacji zarządzania zasobami ludzkimi w kontekście bezpieczeństwa informacji
26. Dokumentacja dotycząca zarządzania incydentami związanymi z ochroną danych osobowych (RODO/GDPR)
27. Instrukcje dotyczące dokumentacji zarządzania systemami kontroli dostępu fizycznego
28. Procedury dokumentacji zarządzania uprawnieniami i kontrolą dostępu do systemów informatycznych
29. Dokumentacja dotycząca planowania i wdrażania systemów monitorowania i reagowania na incydenty cybernetyczne
30. Instrukcje dotyczące dokumentacji zarządzania zgodnością z wymaganiami regulacji branżowych i prawnych
31. Procedury dokumentacji zarządzania zewnętrznymi dostawcami usług IT i infrastruktury
32. Dokumentacja dotycząca zarządzania ryzykiem dla projektów IT i procesów biznesowych
33. Instrukcje dotyczące dokumentacji przeglądów i ocen skuteczności systemu zarządzania bezpieczeństwem informacji
34. Procedury dokumentacji zarządzania konfiguracją systemów informatycznych i aplikacji
35. Dokumentacja dotycząca zarządzania reputacją i wizerunkiem firmy w kontekście bezpieczeństwa informacji
36. Instrukcje dotyczące dokumentacji zarządzania monitorowaniem i analizą zagrożeń informacyjnych
37. Procedury dokumentacji zarządzania testami penetracyjnymi i oceną podatności systemów informatycznych.

# Audyt bezpieczeństwa - wstępny („zerowy”). Analiza stanu bezpieczeństwa użytkowanych systemów oraz wskazanie koniecznych działań, które zwiększą poziom bezpieczeństwa IT

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** |  |
| **Zakres prac** | | |
|  | Przeprowadzenie audytu bezpieczeństwa, którego celem jest ocena aktualnego – przed przystąpieniem do realizacji projektu - poziomu bezpieczeństwa teleinformatycznego. | |
| **Cel audytu** | | |
|  | Celem audytu jest przedstawienie szczegółowego obrazu obecnego stanu bezpieczeństwa organizacji, identyfikacja obszarów wymagających usprawnień. | |
| **Obszary Audytu** | | |
| **Wymagania dla jednostki przeprowadzającej audyt:** | | |
| Zamawiający wymaga, aby jednostka przeprowadzająca audyt spełniała wymagania określone w Ustawie z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560). | | |
| **Raport z Audytu Bezpieczeństwa** | | |
| Raport z audytu bezpieczeństwa zawiera szczegółowe wyniki analizy, identyfikację potencjalnych zagrożeń, rekomendacje dotyczące poprawy bezpieczeństwa, a także plan działania.  Raport stanowi część Dokumentacji Analizy Przedwdrożeniowej (DAP) opracowanej przez wykonawcę zakresu rzeczowego projektu i zatwierdzonej przez Zamawiającego. | | |

# Audyt bezpieczeństwa – końcowy. Analiza poziomu bezpieczeństwa po zakończeniu projektu. Weryfikacja osiągnięcia założonych celów projektu – Część II zamówienia.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** |  |
| **Zakres prac** | | |
|  | Przeprowadzenie audytu bezpieczeństwa, którego celem jest ocena poziomu bezpieczeństwa teleinformatycznego. | |
| **Cel audytu** | | |
|  | Celem audytu jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności zgodnie z projektem w obszarach wskazanych w poniższej tabeli w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa w formie ankiety.  Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z wyników Audytu wstępnego (audyt „zerowy”) lub jego brak. | |
| **Obszary Audytu** | | |
|  | 1. Ocena skuteczności działania infrastruktury w zakresie:  * urządzenia i konfiguracja w zakresie ochrony poczty, * urządzenia i konfiguracja w zakresie ochrony sieci, * urządzenia i konfiguracja w zakresie systemów serwerowych, * urządzenia i konfiguracja w zakresie stacji roboczych, * urządzenia i konfiguracja w zakresie systemów bezpieczeństwa.  1. Procesy zarządzania bezpieczeństwem informacji:  * nośniki wymienne - udokumentowany sposób postępowania, * zarządzanie tożsamością/dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu, * pomieszczenie/pomieszczenia w dyspozycji Zespołu IT  1. Monitorowanie i reagowanie na incydenty bezpieczeństwa:  * procedury zarządzania incydentami, * raportowanie poziomów pokrycia scenariuszami znanych incydentów, * dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa, * monitorowanie i wykrycie incydentów bezpieczeństwa, * Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.  1. Zarządzanie ciągłością działania:  * konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa, * raport z przeglądów i testów odtwarzania kopii bezpieczeństwa, * procedury wykonywania i przechowywania kopii zapasowych, * strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP), * procedury utrzymaniowe.  1. Utrzymanie systemów informacyjnych:  * harmonogramy skanowania podatności, * aktualny status realizacji postępowania z podatnościami, * procedury związane ze z identyfikowaniem (wykryciem) podatności, * współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.  1. Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:  * polityka bezpieczeństwa w relacjach z dostawcami, * standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa, * dostęp zdalny, * metody uwierzytelnienia. | |
| **Wymagania dla jednostki przeprowadzającej audyt:** | | |
| Zamawiający wymaga, aby jednostka przeprowadzająca audyt spełniała wymagania określone w Ustawie z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560).  Audyt bezpieczeństwa może być przeprowadzony przez:  1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r.  o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;  2) co najmniej dwóch audytorów posiadających:  a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu;  b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych,  lub  c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.  Wykaz certyfikatów uprawniających do przeprowadzenia audytu:   1. Certified Internal Auditor (CIA); 2. Certified Information System Auditor (CISA); 3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-ENISO/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, w zakresie certyfikacji osób; 4. 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; 5. Certified Information Security Manager (CISM); 6. Certified in Risk and Information Systems Control (CRISC); 7. Certified in the Governance of Enterprise IT (CGEIT); 8. Certified Information Systems Security Professional (CISSP); 9. Systems Security Certified Practitioner (SSCP); 10. Certified Reliability Professional; 11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert. | | |
| **Kryteria Audytu Bezpieczeństwa** | | |
| Kryteria Audytu Bezpieczeństwa oparte będą o:   * Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa. * Wymagania normatywne PN-EN ISO/IEC 27001:2017-06. * Wymagania normatywne PN-EN ISO 22301:2020-04. * Wewnętrzną dokumentację Zamawiającego. * Przepisy o Krajowym Systemie Cyberbezpieczeństwa. * Standardy Krajowych Ram Interoperacyjności (KRI).   Audytowi poddany zostanie wpływ przeprowadzonych inwestycji na podniesienie poziomu cyberbezpieczeństwa Zamawiającego. | | |