

Znak sprawy: IR.271.9.2025

ZAŁĄCZNIK NR 1 DO SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

na dostawę i wdrożenie infrastruktury sprzętowej
oraz oprogramowania dla Gminy Zebrzydowice
w ramach projektu Cyberbezpieczny Samorząd

Zebrzydowice 2025

Spis treści

ROZDZIAŁ I. ZAŁOŻENIA POCZĄTKOWE ORAZ WYMAGANIA OGÓLNE	3
I.1 WPROWADZENIE I CEL PROJEKTU	3
I.2 AKTY PRAWNE.....	3
I.3 OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA.....	3
I.4 TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA.....	7
I.5 ORGANIZACJA WDROŻENIA	7
I.6 PRZYGOTOWANIE DOKUMENTACJI.....	8
I.7 HARMONOGRAM WDROŻENIA	8
I.8 ANALIZA PRZEDWDROŻENIOWA.....	8
I.9 DOKUMENTACJA POWYKONAWCZA	9
I.10 ODBIÓR DOKUMENTACJI/KOŃCOWY	10
I.11 TESTY.....	10
I.12 DODATKOWE ZOBOWIĄZANIA WYKONAWCY	11
ROZDZIAŁ II. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA.....	11
II.1 DOSTAWA I WDROŻENIE INFRASTRUKTURY SPRZĘTOWEJ I OPROGRAMOWANIA	11
II.2 ZAKUP I WDROŻENIE KLASTRA UTM	12
II.3 ROZBUDOWA INFRASTRUKTURY AKTYWNEJ – ZAKUP PRZELĄCZNIKÓW 6 SZT.	25
II.4 ROZBUDOWA ROZWIĄZANIA DO OCHRONY DANYCH DO ROZWIĄZANIA KLASY EDR XDR – ROZSZERZENIE LICENCJI.....	30
II.5 USŁUGA ANALIZY KONFIGURACJI W OBECNIE POSIADANYCH ROZWIĄZANIACH	38
II.6 ZAKUP I WDROŻENIE ROZWIĄZANIA KLASY NAC	39
II.7 DOSTAWA I KOMPLEKSOWE WDROŻENIE SYSTEMU DO WYKRYWANIA I ZARZĄDZANIA INCYDENTAMI, PODATNOŚCIAMI I RYZYKIEM SIEM, SOAR	49
II.8 SERWER TWORZĄCY PLATFORMĘ SPRZĘTOWĄ DLA SOC – 1 SZT.	79
II.9 ROZBUDOWA INFRASTRUKTURY O MACIERZ DYSKOWĄ – 1 SZT.	88
II.10 ZAKUP NIEZBĘDNYCH LICENCJI DO FUNKCJONOWANIA ŚRODOWISKA BAZODANOWEGO	90
II.11 PRZEDŁUŻENIE LICENCJI I WSPARCIA NA POSIADANE ROZWIĄZANIE DO ZARZĄDZANIA INFRASTRUKTURĄ, STACJAMI ROBOCZYMI I SERWERAMI	97
II.12 PRZEDŁUŻENIE WSPARCIA NA POSIADANE ROZWIĄZANIE DO KOPII ZAPASOWYCH	98
II.13 ROZBUDOWA INFRASTRUKTURY BACKUPOWEJ – ZAKUP SYSTEMU POZWALAJĄCEGO NA TWORZENIE KOPII ZAPASOWYCH WSZYSTKICH DANYCH.....	104
II.14 ZAKUP UPS DLA STACJI KOŃCOWYCH – 20 SZTUK.	133
II.15 ZAKUP UPS DO SERWEROWNI – 2 SZT.	134
II.16 USŁUGA WYKONANIA SEGMENTACJI SIECI	138
II.17 USŁUGA PRZEPROWADZENIA TESTÓW PENETRACYJNYCH	139
II.18 SZKOLENIE DLA PRACOWNIKÓW IT Z ZAKRESU ZABEZPIECZANIA ŚRODOWISKA DOMENOWEGO.....	142
II.19 SZKOLENIE DLA PRACOWNIKÓW IT Z ZAKRESU CYBERBEZPIECZEŃSTWA	147
II.20 INSTRUKTARZE STANOWISKOWE	148
ROZDZIAŁ III. GWARANCJA	150
III.1 WARUNKI GWARANCJI	150
III.2 WADY PRZEDMIOTU ZAMÓWIENIA	151

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie i cel projektu

Gmina bierze udział w projekcie „Cyberbezpieczny Samorząd”, którego celem jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych.

Realizacja projektu poprzez wsparcie grantowe jednostek samorządowych, przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI),
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

I.2 Akty prawne

Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Rozwiązania muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem.

I.3 Ogólny opis przedmiotu zamówienia

Dostawa i wdrożenie infrastruktury sprzętowej oraz oprogramowania dla Gminy Zebrzydowice.

Przedmiot zamówienia niniejszego postępowania przetargowego obejmuje:

Poz. OPZ	Opis	Ilość sztuk/kpl.
Rozdział	Rodzaj zamawianego asortymentu	
II.2	Zakup i wdrożenie klastra UTM	1 szt.
II.3	Rozbudowa infrastruktury aktywnej – zakup przełączników	6 szt.
II.4	Rozbudowa rozwiązania do ochrony danych do rozwiązania klasy EDR XDR – rozszerzenie licencji	1 szt.
II.5	Usługa analizy konfiguracji w obecnie posiadanych rozwiązaniach	1 szt.
II.6	Zakup i wdrożenie rozwiązania klasy NAC	1 szt.
II.7	Dostawa i kompleksowe wdrożenie systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM, SOAR	1 szt.
II.8	Serwer tworzący platformę sprzętową dla SOC	1szt.
II.9	Rozbudowa infrastruktury o macierz dyskową	1 szt.
II.10	Zakup niezbędnych licencji do funkcjonowania środowiska bazodanowego	1szt.
II.11	Przedłużenie licencji i wsparcia na posiadane rozwiązanie do zarządzania infrastrukturą, stacjami roboczymi i serwerami	1 szt.

II.12	Przedłużenie wsparcia na posiadane rozwiązanie do kopii zapasowych	1 szt.
II.13	Rozbudowa infrastruktury backupowej – zakup systemu pozwalającego na tworzenie kopii zapasowych wszystkich danych	1 szt.
II.14	Zakup UPS dla stacji końcowych	20 szt.
II.15	Zakup UPS do serwerowni	2 szt.
II.16	Usługa wykonania segmentacji sieci	1 szt.
II.17	Usługa przeprowadzenia testów penetracyjnych	1 szt.
II.18	Szkolenie dla pracowników IT z zakresu zabezpieczania środowiska domenowego	3 szt.
II.19	Szkolenie dla pracowników IT z zakresu cyberbezpieczeństwa	3 szt.

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
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).
 - 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 przeprowadzi zgodnie z zapisami niniejszego SOPZ 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 SOPZ oraz Umowy.
5. Tam, gdzie w opisie przedmiotu zamówienia został wskazany znak towarowy (marka), producent, dostawca, patent, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczone przez konkretnego Wykonawcę lub nastąpiło wskazanie norm, europejskich ocen technicznych, wspólnych specyfikacji technicznych lub innych odniesień, o których mowa w art. 101 ust. 1 pkt 2 lub ust. 3 ustawy, Zamawiający zgodnie z art. 99 ust. 5 ustawy dopuszcza złożenie oferty równoważnej lub zgodnie z art. 101 ust. 4 ustawy zaoferowanie rozwiązań „równoważnych” w stosunku do wskazanych w opisie przedmiotu zamówienia pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych od założonych w SWZ.
6. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia, elementu i/lub licencji, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
7. Wszelkie dostarczane urządzenia:
 - Muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych. Wszelkie dostarczane urządzenia muszą być wyprodukowane po dniu 30 czerwca 2024r.
 - Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
 - Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
 - Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
 - Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
 - Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.

I.4 Termin realizacji Przedmiotu Zamówienia

Termin realizacji całości Przedmiotu zamówienia wynosi nie więcej niż **120 dni** kalendarzowych od dnia zawarcia Umowy.

I.5 Organizacja wdrożenia

Założenia podstawowe:

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram Wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
2. Wykonawca w Harmonogramie Wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji, wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac przez Zamawiającego. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, chyba że, nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań.
5. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
6. W przypadku dostarczania Infrastruktury Serwerowej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczona w oryginalnych opakowaniach fabrycznych.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
9. W ramach wdrożenia Wykonawca przygotuje informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującą się realizacją Przedmiotu Zamówienia, w ramach której muszą zostać powołane minimum następujące role:
 - a. Kierownik Projektu ze strony Wykonawcy,
 - b. Zespół Wdrożeniowy ze strony Wykonawcy

10. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
11. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i interesantów urzędu.

I.6 Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
 - a) Harmonogram Wdrożenia.
 - b) Dokumentacja Analizy Przedwdrożeniowej (DAP).
 - c) Dokumentacja Powykonawcza.
2. Dokumentacja powyższa będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy 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 Specyfikacją Warunków Zamówienia wraz z załącznikami (dalej zwanych SWZ) będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu Wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem Wdrożenia zostaną opracowane w oparciu o wymagania określone w niniejszym SOPZ.

I.7 Harmonogram Wdrożenia

Wykonawca zobowiązany jest opracować na podstawie SWZ oraz SOPZ szczegółowy Harmonogram Wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 14 dni od podpisania Umowy.

I.8 Analiza Przedwdrożeniowa

1. Analiza Przedwdrożeniowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwaną dalej DAP), na podstawie, której będzie realizowany

organizacyjnie i technicznie Przedmiot Zamówienia. Dokumentacja Analizy Przedwdrożeńowej będzie podlegała uzgodnieniu i akceptacji Zamawiającego.

2. Dokumentacja Analizy Przedwdrożeńowej DAP powinna zawierać w szczególności:

SKŁAD DAP
ZARZĄDCZE
– plan i sposób komunikacji Stron
INFRASTRUKTURA SERWEROWA I SIECIOWA
– podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty
– analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru
– karty katalogowe urządzeń potwierdzające spełnienie wymagań
– plan dostaw
– opis instalacji i wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą
– Procedura testowania – scenariusze testowe dla wdrażanych systemów
– harmonogram instruktażu personelu oraz administratorów

I.9 Dokumentacja Powykonawcza

- Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
- W Dokumentacji Powykonawczej muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
- Wykonawca wraz z Dokumentacją Powykonawczą dostarczy propozycję scenariuszy testowych, które będą podlegały akceptacji Zamawiającego.
- W szczególności dokumentacja ta powinna zawierać następujące elementy:
 - Schemat infrastruktury i architekturę rozwiązania wraz z opisem.
 - Zasady licencjonowania dostarczonych elementów.
 - Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.

- d. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.
- e. Procedury konfiguracji kont w dostarczonych systemach.
- f. Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii.
- g. Procedury opisujące standardowe działania administracyjne.
- h. Procedury odzyskania wdrożonych systemów po awarii.
- i. Wytyczne (dobre praktyki) dla administratorów.
- j. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.

I.10 Odbiór Dokumentacji/Końcowy

1. Odbiór Końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej Załącznik nr 4 do SWZ.

I.11 Testy

1. W ramach postępowania zostaną 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 Zamawiającego jak i wskazanych przez Zamawiającego osób lub podmiotów zewnętrznych.
2. 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.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. Koszt zewnętrznego audytora będzie kosztem Zamawiającego. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. Zamawiający w końcowej fazie wdrożenia oczekuje realizacji przez Wykonawcę testów bezpieczeństwa.
5. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym Przedmiotu Zamówienia.

6. Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze co najmniej z zakresu:
 - a) Uruchamianie i zatrzymywanie wdrożonych systemów
 - b) Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w Dokumentacji.
 - c) Weryfikacja poprawności działania procedur.
 - d) Symulację awarii wdrożonych systemów.

I.12 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie będącej Załącznikiem nr 4 do SWZ.
3. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
4. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
5. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
6. Współdziałanie z osobami wskazanymi przez Zamawiającego.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II.1 Dostawa i wdrożenie infrastruktury sprzętowej i oprogramowania

1. Jeżeli zajdzie potrzeba, wraz z dostarczaną Infrastrukturą, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie dostarczanej infrastruktury. Dostarczona Infrastruktura musi zapewniać bezproblemową pracę po podłączeniu do sieci informatycznej Zamawiającego.
2. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
3. Wszystkie elementy Infrastruktury Serwerowej powinny zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację.

4. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury zostaną ustalone w trakcie prac nad harmonogramem wdrożenia.

Po zakończonym montażu Wykonawca przekaze Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, bazodanowego, wirtualizacyjnego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycia dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie (o ile dostarcza je producent). Wykonawca wykona również instruktaże użytkowe dla wskazanych przez Zamawiającego administratorów, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu.

II.2 Zakup i wdrożenie klastra UTM

Zamawiający wymaga dostarczenia dwóch nowych, identycznych urządzeń klasy UTM wraz z gwarancją oraz dostępem do aktualizacji oprogramowania zabezpieczającego przez okres min. 36 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; opracować politykę deszyfracji danych szyfrowanych SSL (Secure Sockets Layer), opracować reguły działania w zależności od rodzaju ruchu, opracować polityki ponownego szyfrowania danych, skonfigurować urządzenia UTM do analizy ruchu SSL, opracować koncepcję segmentacji sieci, a w szczególności: skonfigurować wirtualne sieci LAN, strefy, skonfigurować urządzenia UTM oraz wszystkie przełączniki sieciowe. Ponadto Wykonawca wykona instruktaż z zakresu administracji dostarczonych urządzeń UTM; opracuje dokumentację powykonawczą oraz będzie świadczyć rozszerzone wsparcie serwisowe przez okres min. 36 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. Wymaga się dostarczenia dokumentu potwierdzonego przez producenta lub autoryzowanego partnera o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

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

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 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:
 - Min. 10 portów Gigabit Ethernet RJ-45
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 95 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 9.6 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 9.4 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.4 Gbps.
5. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6.9 Gbps.
6. 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 2.4 Gbps.

7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 950 Mbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.2 Gbps.

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 - zaporą ogniową 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.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - Nuage Networks VSP.
 - OpenStack.
 - VMware vCenter (ESXi).
 - VMware NSX.
 - VMware NSX.Nutanix.
 - VMware NSX.IBM Cloud.
 - 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 oraz 21.
 - Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh.
 - Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. 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 RIPv2), 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 łącz WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
3. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu.
4. Rozwiązanie powinno wspierać funkcję Forward Error Correction na tunelach IPSec.
5. Funkcja monitorowania łączy w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.

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, 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 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injection, 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 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).
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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
9. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
10. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
11. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo.
12. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

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

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

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym, przez okres min. 36 miesięcy, gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów dla Zamawiającego, realizowanym przez producenta rozwiązania lub autoryzowanego partnera przez okres wymaganej gwarancji.

Opcjonalne rozszerzone wsparcie techniczne (opcja punktowana dodatkowo)

Do zamawianego sprzętu Wykonawca zapewni usługę rozszerzonego wsparcia technicznego świadczonego przez producenta lub autoryzowanego partnera w języku polskim, przez okres 36 miesięcy w zakresie minimalnym:

- obsługa procesu RMA u producenta,
- pomoc w zakładaniu zgłoszeń serwisowych u producenta,
- pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą),
- doradztwo w zakresie konfiguracji, zdalne wsparcie techniczne, zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta – do 6 godzin na rok,
- jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym poziomem certyfikacji technicznej producenta,
- minimum raz w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich,
- dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.

Dostęp do usługi powinien być świadczony przez dedykowaną infolinię czynną od 7:00-19:00 (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).

Usługa ma być świadczona przez podmiot posiadający ważne certyfikaty: ISO 9001, ISO 27001.

Usługa ma być świadczona przez zespół certyfikowanych inżynierów, legitymujących się ważnymi certyfikatami wystawionymi przez producenta oferowanego urządzenia UTM.

Do oferty należy załączyć oświadczenie o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001, ISO 27001 oraz dokument potwierdzający status partnerski u producenta oferowanego urządzenia UTM.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa

państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Funkcja zbierania, przechowywania oraz analizy logów.

W ramach postępowania należy dostarczyć wraz klastrem urządzeń UTM centralny system logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz zagrożenia bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 6.7, 7.x, 8.x; Microsoft Hyper-V wersje: 2012 R2, 2016, 2019, 2022, 2025; KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności min. 3 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
 - a) Listę najczęściej wykrywanych ataków.
 - b) Listę najbardziej aktywnych użytkowników.
 - c) Listę najczęściej wykorzystywanych aplikacji.

- d) Listę najczęściej odwiedzanych stron www.
 - e) Listę krajów, do których nawiązywane są połączenia.
 - f) Listę najczęściej wykorzystywanych polityk Firewall.
 - g) Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długoczasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System ma korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - a) Malware.
 - b) Aplikacje sieciowe.
 - c) Email.
 - d) IPS.
 - e) Traffic.
 - f) Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. System musi być dostarczony w postaci licencji bezterminowej tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. System musi być objęty wsparciem technicznym producenta przez okres min. 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami,

technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Token sprzętowy do uwierzytelniania wieloskładnikowego (MFA) – 10 sztuk

Wraz z klastrem urządzeń UTM należy dostarczyć tokeny sprzętowe, które umożliwiają wymuszenie uwierzytelnienia wieloskładnikowego. Tokeny muszą się integrować z dostarczającymi systemami UTM. Dostarczone rozwiązanie musi umożliwiać Zamawiającemu wdrażanie różnych metod tokenów, w tym: jednorazowych haseł, tokenów SMS i adaptacyjnego uwierzytelniania.

Aby zapewnić jeszcze większe bezpieczeństwo, sprzętowy token musi umożliwiać użytkownikom uwierzytelnianie bez hasła na podstawie specyfikacji FIDO i FIDO2.

II.3 Rozbudowa infrastruktury aktywnej – zakup przełączników 6 szt.

Zarządzalne przełączniki sieciowe – 6 sztuk

Obecnie używane przez Zamawiającego przełączniki tworzące sieć LAN są przestarzałe, nie ma wydzielonych przełączników do rdzenia sieci, brak możliwości instalacji nowego oprogramowania wewnętrznego. Przedmiotem zadania jest dostawa nowych przełączników umożliwiających utworzenie sieci LAN o wysokiej przepustowości. Wraz z przełącznikami należy dostarczyć wszystkie niezbędne moduły SFP+, przewody połączeniowe umożliwiające uruchomienie nowej sieci LAN oraz podłączenie urządzeń do nowych przełączników.

Przełącznik zarządzalny Typ 1 – 5 sztuk

Przełączniki dostępne muszą spełniać opisane niżej parametry minimalne:

- wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
- Zasilanie 230V
- MTBF > 10lat

Interfejsy sieciowe

- 48 portów GE, RJ-45
- 4 porty 10GE SFP+

Zarządzanie

- port konsoli szeregowej RJ45 lub USB lub USB-C
- Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę.
- Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Wsparcie dla Syslog UDP/TCP
- Wsparcie dla Link Monitor, SPAN, RSPAN

Parametry wydajnościowe

- przepustowość urządzenia - min. 170 Gbps,
- pakiety na sekundę: min. 250 Mpps
- możliwość zapamiętania co najmniej 30 000 adresów MAC
- Opóźnienie - poniżej 1 mikrosekundy
- Bufor pakietów: min. 2 MB
- Pamięć DRAM: min. 500 MB
- Pamięć FLASH: min. 60 MB

Wymagane funkcje

- możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
- obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
- możliwość agregacji portów zgodna z 802.3ad oraz 802.3ax
- obsługa funkcji: IEEE 802.1ab Link Layer Discovery Protocol, IEEE 802.1ab LLDP-MED, IEEE 802.1ae MAC Security
- obsługa funkcji: IEEE 802.3az Energy Efficient Ethernet, IEEE 802.3x Flow Control
- obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
- port-mirroring
- Kontrola dostępu w oparciu o standard 802.1x, możliwość uwierzytelniania według: MAC adres, Port, przypisany VLAN
- zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTTP, LLDP (w trybie odbioru)
- możliwość zarządzania przez interfejs graficzny i tekstowy

- możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
- możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
 - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
 - obsługa białych i czarnych list MAC
 - stateful firewall, umożliwiającą kontrolę dostępu do sieci
 - routing statyczny i dynamiczny, co najmniej OSPF

Wymagania ogólne

- W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
- Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Gwarancja

- Dożywotnia Gwarancja: urządzenia muszą być objęte dożywotnią gwarancją producenta, gwarantującą wymianę wadliwego sprzętu (okres min. 5 lat od ogłoszenia zakończenia produkcji).
- Wsparcie techniczne producenta: system musi być objęty serwisem gwarancyjnym producenta przez okres min. 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej.

Przełącznik zarządalny Typ 2 – 1 sztuka

Przełączniki dostępne muszą spełniać opisane niżej parametry minimalne:

- wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
- Zasilanie 230V
- MTBF > 10lat

Interfejsy sieciowe

- 48 portów GE, RJ-45
- 4 porty 10GE SFP+

Zarządzanie

- port konsoli szeregowej RJ45 lub USB lub USB-C
- Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę.
- Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Wsparcie dla Syslog UDP/TCP
- Wsparcie dla Link Monitor, SPAN, RSPAN

Parametry wydajnościowe

- przepustowość urządzenia - min. 170 Gbps,
- pakiety na sekundę: min. 250 Mpps
- możliwość zapamiętania co najmniej 30 000 adresów MAC
- Opóźnienie - poniżej 1 mikrosekundy
- Bufor pakietów: min. 2 MB
- Pamięć DRAM: min. 500 MB
- Pamięć FLASH: min. 60 MB

Wymagane funkcje

- możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
- obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
- możliwość agregacji portów zgodna z 802.3ad oraz 802.3ax
- obsługa funkcji: IEEE 802.1ab Link Layer Discovery Protocol, IEEE 802.1ab LLDP-MED, IEEE 802.1ae MAC Security

- obsługa funkcji: IEEE 802.3az Energy Efficient Ethernet, IEEE 802.3x Flow Control
- obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
- port-mirroring
- Kontrola dostępu w oparciu o standard 802.1x, możliwość uwierzytelniania według: MAC adres, Port, przypisany VLAN
- zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTTP, LLDP (w trybie odbioru)
- możliwość zarządzania przez interfejs graficzny i tekstowy
- możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
- możliwość zasilania podłączonych urządzeń, budżet mocy min. 700W
- możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
 - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
 - obsługa białych i czarnych list MAC
 - stateful firewall, umożliwiający kontrolę dostępu do sieci
 - routing statyczny i dynamiczny, co najmniej OSPF

Wymagania ogólne

- W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
- Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Gwarancja

- Dożywotnia Gwarancja: urządzenia muszą być objęte dożywotnią gwarancją producenta, gwarantującą wymianę wadliwego sprzętu (okres min. 5 lat od ogłoszenia zakończenia produkcji).

- Wsparcie techniczne producenta: system musi być objęty serwisem gwarancyjnym producenta przez okres min. 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej.

Centralny, sprzętowy kontroler przełączników (opcja punktowana dodatkowo).

Sprzętowy kontroler centralnego zarządzania przełącznikami Typ-1, Typ-2 musi oferować minimum 4 poniższe funkcje:

- musi umożliwiać wykonywanie akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – min. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
- musi umożliwiać aktualizację oprogramowania podłączonych, zarządzanych przełączników.
- musi być możliwość podejrzenia z poziomu kontrolera informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
- musi umożliwiać automatyczną instalację wskazanej wersji oprogramowania układowego firmware, po podłączeniu przełącznika. Oprogramowanie przełącznika, musi być przechowywane na kontrolerze.

II.4 Rozbudowa rozwiązania do ochrony danych do rozwiązania klasy EDR XDR – rozszerzenie licencji

Zamawiający użytkuje oprogramowanie antywirusowe ESET PROTECT Enterprise ON-PREM, klucz publiczny: 3AJ-XND-GTP, liczba chronionych urządzeń: 100. Należy dostarczyć nowe funkcjonalności EDR, XDR, szyfrowanie dysków twardych. Licencje muszą być objęte gwarancją i wsparciem producenta oraz umożliwiać aktualizację programu oraz definicji zagrożeń na okres do 30.06.2026r. .

Dostarczone licencje należy zainstalować na wskazanych przez Zamawiającego serwerach w czasie wyznaczonym przez Zamawiającego (poza godzinami pracy). Wykonawca może dostarczyć rozbudowane oprogramowanie firmy ESET lub oprogramowanie równoważne. W przypadku dostarczenia oprogramowania równoważnego, Wykonawca dokona instalacji oprogramowania na wszystkich obecnie chronionych urządzeniach oraz konfiguracji konsoli zarządzającej. Oferowane oprogramowanie musi spełniać poniższe wymagania minimalne:

I. Rozbudowa systemu ochrony stacji w zakresie szyfrowania, funkcji XDR

1)	Istniejący system ochrony urządzeń ESET należy rozbudować w zakresie modułu posiadającego narzędzia wykrywania incydentów i automatycznego reagowania umożliwiającego korelację zdarzeń (XDR), mechanizmy uwierzytelniania wieloskładnikowego (MFA) oraz w zakresie proaktywnej ochrony przed zagrożeniami zero-day z analizą w odizolowanym chmurowym środowisku. Nr licencji obecnie posiadanego systemu 3AJ-XND-GTP
2)	W wyniku rozbudowy systemu o nowe moduły funkcjonalne przy zachowaniu dotychczasowej funkcjonalności w zakresie ochrony stacji roboczych, ochrony serwerów, ochrony urządzeń mobilnych. Nowe moduły muszą być kompatybilne z istniejącym systemem, a całe rozwiązanie musi zapewniać minimum funkcjonalność określoną w pkt. 2 - 8
3)	Zamawiający dopuszcza wymianę istniejącego rozwiązania na rozwiązanie równoważne do istniejącego systemu ochrony urządzeń, realizującego minimum funkcjonalności opisane w pkt.2-8, Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana systemu na równoważne nie zakłóciła bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania Oprogramowania w środowisku produkcyjnym itp.
4)	Rozwiązanie musi zapewniać ochronę 100 stacji komputerowych w poniższym zakresie.
II. WYMAGANIA OGÓLNE	
1)	Rozwiązanie musi być zarządzane z jednej centralnej konsoli administracyjnej dostępnej z poziomu interfejsu WWW zabezpieczonego protokołem SSL. Wymagana jest autoryzacja dwuetapowa do konsoli administracyjnej.
2)	Serwer administracyjny dostępny w chmurze musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zaporę osobistą, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci oraz musi umożliwiać tworzenie polityk dla programów zabezpieczających i komponentów środowiska

	serwera centralnego zarządzania.
3)	Konsola administracyjna musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
4)	Moduł XDR musi być oparty o motor baz danych SQL celem zapewnienia maksymalnej wydajności pracy i maksymalnej ochrony danych. Motor bazy SQL należy dostarczyć wraz z modulem XDR.
5)	Rozwiązanie musi zapewnić uwierzytelnianie użytkownika zanim zostanie uruchomiony system operacyjny.
III. XDR	
1)	Automatyczna wizualizacja zdarzeń, incydentów i ataków ukierunkowanych
2)	Możliwość wyszukiwania zagrożeń na podstawie definiowanych filtrów
3)	Wbudowany zestaw reguł zapewniający reagowanie na wykryte incydenty z możliwością budowania własnych reguł oraz edycji istniejących.
4)	Możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
5)	Możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa
6)	Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7)	Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8)	Możliwość uruchomienia reguł w oparciu o dane historyczne.

9)	Możliwość blokowania plików po sumach kontrolnych.
10)	Możliwość ustawiania priorytetu zdarzeń.
11)	Możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
12)	Możliwość oznaczenia plików DLL jako bezpieczne, pobrania do analizy oraz ich zablokowania.
13)	Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.
14)	Dla wykonanego skryptu lub pliku exe, weryfikacja powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15)	Możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
16)	Możliwość włączenia izolacji komputera od sieci.
IV. UWIERZYTELNIANIE WIELOSKŁADNIKOWE (MFA)	
1)	Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
2)	Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemem operacyjnego.
3)	Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modulem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.
4)	Możliwość określenia metody uwierzytelniania dwuskładnikowego użytkowników, minimum wiadomość SMS, aplikacja mobilna

5)	Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.
6)	Możliwość wysyłania wiadomości na telefony pracujące w roamingu.
7)	Możliwość wyboru użytkowników uwierzytelniania dwuskładnikowego.
8)	Możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji.
9)	Rozwiązanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika.
10)	W ramach modułu musi być zapewniony dostęp do dedykowanej aplikacji mobilnej działającej pod kontrolą Android i iOS
11)	Dostępne API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu minimum o usługę Active Directory. Dla środowisk nie wykorzystujących usług Active Directory musi być dostępny pakiet SDK umożliwiający implementację w tych środowiskach, dwuskładnikowego uwierzytelniania do autoryzacji użytkowników.
V. SANDBOXING W CHMURZE	
1)	Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
2)	Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemem operacyjnego.
3)	Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modulem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.

4)	Ochrona przed zagrożeniami 0-day.
5)	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.
6)	Możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
7)	Możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
8)	Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
9)	Możliwość wyświetlenia listy plików, które zostały przesłane do analizy.
10)	Możliwość analizowania plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
VI. OCHRONA STACJI ROBOCZYCH	
1)	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
2)	Ochrona przed rootkitami oraz podłączeniem komputera do sieci botnet.
3)	Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
4)	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5)	Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
6)	Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
7)	Umieszczenia na liście wykluczeń wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

8)	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).
9)	Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
10)	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.
11)	Blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych firewall, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
12)	Blokowanie nośników wymiennych, bądź grup urządzeń wraz z możliwością tworzenia reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
13)	Możliwość generowania raportu dotyczącego stacji, zawierającego informacje dotyczące, minimum: zainstalowanych aplikacji, usług systemowych, systemu operacyjnego, aktywnych procesów, połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
14)	Automatyczna, inkrementalna aktualizacja silnika detekcji.
15)	Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
16)	Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17)	Zintegrowany moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika.
18)	Zintegrowany moduł kontroli dostępu do stron internetowych.

19)	Możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
20)	Ochrona przed zagrożeniami 0-day.
VII OCHRONA SERWERÓW	
1)	Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2)	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3)	Skanowania dysków sieciowych typu NAS.
4)	Wbudowane minimum 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.
5)	Automatyczna, inkrementalna aktualizacja silnika detekcji.
6)	Możliwość wykluczania ze skanowania procesów.
7)	Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
8)	System zapobiegania włamaniom działający na hoście (HIPS).
9)	Skanowanie magazynu Hyper-V.
10)	Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
11)	Możliwość blokowania zewnętrznych nośników danych na serwerze 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.
12)	Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

13)	Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
14)	Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
15)	Możliwość uruchomienia lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
VII OCHRONA URZĄDZEŃ MOBILNYCH	
1)	Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2)	Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
3)	Możliwość skonfigurowania zaufanej karty SIM.
4)	Wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS.
5)	Wyświetlenie listy zainstalowanych aplikacji.
6)	Blokowanie aplikacji w oparciu o nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.
7)	Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

II.5 Usługa analizy konfiguracji w obecnie posiadanych rozwiązaniach

Wykonawca przeprowadzi dokładną analizę konfiguracji posiadanych systemów i urządzeń w celu prawidłowego dostrojenia parametrów niezbędnych do działania całości dostarczanego oprogramowania. W trakcie wykonywania prac Wykonawca powinien brać pod uwagę ustalenia z Zamawiającym na etapie Analizy Przedwdrożeńowej. Efektem analizy powinny być:

- Analiza wydajności systemów
- Sprawdzenie poprawności działania cyklicznych zadań utrzymania na platformie sprzętowej
- Ustalenie zagrożeń i określenie ich wpływu na wdrożenie
- Zdefiniowanie zakresu odpowiedzialności uczestników wdrożenia
- Koncepcja rozwiązań i ich implementacja

II.6 Zakup i wdrożenie rozwiązania klasy NAC

Wykonawca dostarczy oraz wdroży system klasy NAC (Network Access Control) zgodnie z zaakceptowanym przez Zamawiającego projektem wdrożenia. Zamawiający wymaga dostarczenia systemu wraz z wsparciem technicznym gwarantującym dostępem do najnowszych wersji i poprawek przez okres min. 24 miesięcy. Zamawiający wymaga wdrożenia oferowanego systemu w taki sposób, aby możliwe było używanie systemu z wymaganą poniżej funkcjonalnością. W ramach wdrożenia Wykonawca musi skonfigurować wszystkie urządzenia Zamawiającego do prawidłowej współpracy z wdrażanym systemem. System kontroli dostępu musi charakteryzować się następującymi cechami:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja zajęta przez dane urządzenie musi być natychmiast zwalniana po rozłączeniu urządzenia z siecią.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own

- Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
- VM – min. VMWare ESXi co najmniej w wersji 7.x, Hyper-V w wersji min. 2016, Proxmox w wersji min 5.x, KVM w wersji min 7.x.
 - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
- RADIUS dla infrastruktury sieciowej,
 - OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
 - SYSLOG,
 - TACACS+,
 - Monitoringu,
 - DHCP,
 - polityk uwierzytelniania i kontroli dostępu 802.1X,
 - WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min. MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.

17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.

33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.

52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min. dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
 - Czy włączony jest firewall
 - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
 - Czy jest włączone szyfrowanie dysku systemowego
 - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
 - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
 - Czy w systemie są uruchomione procesy wskazane przez administratora
 - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
 - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
 - Wartości klucza rejestru
 - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min. za pomocą agenta i Captive Portal.

61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (auto konfiguratorzy sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
 - Microsoft Windows,
 - Mac OS,
 - iOS,
 - Android.
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (auto konfiguratorzy sieci).
64. System musi wspierać protokół IPv6 min. dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
 - MAC,
 - PAP/ASCII,
 - SNMP,
 - CHAP,
 - 802.1X.

wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.

3. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
4. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
5. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Suppliment, Apple iOS Suppliment, Google Android Suppliment, Ubuntu Suppliment).
6. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
 - Tożsamość/Urządzenie końcowe,
 - Grupa tożsamości/urządzeń końcowych,
 - Parametry urządzeń końcowych, min: system operacyjny, wersja,
 - Atrybuty Active Directory,

- Jednostka organizacyjna tożsamości/urządzeń końcowych,
 - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
 - Grupy urządzeń sieciowych,
 - Porty urządzeń sieciowych,
 - Grupy portów urządzeń sieciowych,
 - Jednostka organizacyjna portów,
 - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
 - Data, czas ważności polityki,
 - Wewnętrzny Captive Portal,
 - Metoda autoryzacji.
7. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
 8. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
 9. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
 10. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
 11. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
 12. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
 13. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
 14. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
 15. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
 16. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
 17. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu

Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.

18. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
19. System musi umożliwiać przysyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
 - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych,
 - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych,
 - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol),
 - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
 - Uruchamianie usługi dla wybranych podsieci,
 - Przypisanie ustalonego adresu IP dla adresu MAC,
 - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
 - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
 - Możliwość określania braku dostępu dla wybranych adresów MAC,
 - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
 - Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
 - Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,

- Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
- Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów.
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostatek aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
2. Raport ze zdarzeń logowania z informacją o danym adresie IP.
3. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
4. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
5. System musi umożliwiać co najmniej monitoring poniższych funkcjonalności:
 - Status autoryzacji,
 - zdarzeń systemowych,
 - zdarzeń serwera DHCP,
 - tożsamości,
 - urządzeń końcowych,
 - urządzeń sieciowych,

6. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
7. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
8. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
9. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
10. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych, musi prezentować minimum poniższe dane:
 - ostatnia autoryzacja do sieci,
 - wykorzystanie urządzeń końcowych wg tożsamości na dzień,
 - parametry urządzeń końcowych, min: system operacyjny i jego wersja.
11. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
12. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
13. Raport zdarzeń Microsoft Active Directory, minimum:
 - Logowania, wylogowania z systemu,
 - Informacje o błędnych logowaniach,
 - Logowania do sieci 802.1X.

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
 - wiadomości e-mail,
 - protokół Syslog,
 - notyfikacji systemowych.
2. Alarmy mogą być generowane w minimum poniższych sytuacjach:
 - Liczba obsługiwanych transakcji RADIUS,
 - Opóźnienie obsługi transakcji RADIUS,
 - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
 - badanie łączności IP za pomocą ping, traceroute,
 - tcpdump protokołów RADIUS, TACACS+,
 - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
 - unikatowej nazwy użytkownika,

- adresu MAC,
- statusu uwierzytelnienia (udana lub nieudana),
- powodu niedanego uwierzytelnienia,
- zakresu czasowego z dokładnością do min. pełnych minut,
- wykonanie zdalnego polecenia na urządzeniu sieciowym.

II.7 Dostawa i kompleksowe wdrożenie systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM, SOAR

1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającego cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.
2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.
4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
5. System powinien pozwalać na pracę z logami zdarzeń jednoliniowych oraz wieloliniowych.
6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiające ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianę wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól

o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.

11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji.

12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.

13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.

14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.

15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zawartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.

16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.

17. System musi umożliwiać fizyczne rozdzielanie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.

18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielania ich składowania na osobny serwer i dedykowane zasoby dyskowe.

19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralności danych.
21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.
22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.
25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.

26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.

27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.

28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.

29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:

- a. nowe zasoby wykryte w sieci,
- b. typy wykrytych zasobów (np.: serwer lub stacja robocza),
- c. zastosowane na nich zabezpieczenia,
- d. usługi z którymi się komunikują,
- e. nowe usługi wykryte na zasobie
- f. komunikację do usług wykrytych na zasobie.

30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.

31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.

32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy.

33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:

- a. fqdn,
- b. e-mail,
- c. nazwa pliku,
- d. ścieżka do pliku,
- e. hash,
- f. adres IP,
- g. klucz rejestru,
- h. cmd.

34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>).

35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np.: obraz pliku, hash, nazwa procesu).

36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).

37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.

39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwany wynik analizy jest lista niezgodności (np.: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).

40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.
43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:
- id techniki,
 - taktykę,
 - platformy których dotyczy,
 - potencjalne źródła,
 - opis zagrożenia,
 - mityzację,
 - sposób detekcji,
 - referencje.
44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).

46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:

- a. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
- b. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
- c. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
- d. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.

47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).

48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.

49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np.: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.

52. System musi posiadać interfejs graficzny do tworzenia własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenia reguł musi uwzględniać:

- a. sparsowane pola oraz ich wartości,

- b. listy referencyjne,
- c. atrybuty użytkowników z Active Directory,
- d. atrybuty komputerów z Active Directory,
- e. bazę wskaźników kompromitacji (IOC),
- f. informacje z elektronicznej dokumentacji,
- g. anomalie w zachowaniu użytkowników (UBA),
- h. anomalie w zachowaniu zasobów (EBA),
- i. podatności na zasobach,
- j. wyniki analizy konfiguracji,
- k. techniki MITRE ATT&CK®,

53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:

- a. wykrycie dowolnej treści w logach,
- b. wykrycie zmiany jednego z kilku pól,
- c. wykrycie zaniku wiadomości,
- d. wykrycie nowej wartości pola w zadanym okresie czasu,
- e. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
- f. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
- g. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
- h. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
- i. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
- j. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,
- k. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
- l. wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
- m. wykrycie skanowania portów.

54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

- a. wykrycie wystąpienia wartości pola na wybranej liście,
- b. wykrycie niewystępowania wartości pola na wybranej liście,
- c. wykrycie wystąpienia pary wartości na wybranej liście^[1] (np.: proces i obraz pliku z którego został uruchomiony),

- d. wykrycie niewystąpienia pary wartości na wybranej liście
- e. (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).

55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:

- a. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
- b. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
- c. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
- d. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),
- e. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.

56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:

- a. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
- b. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
- c. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:

- a. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;
- b. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;
- c. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;

58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:

- a. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
- b. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
- c. wykrycie nieautoryzowanej usługi na serwerze,
- d. wykrycie nieautoryzowanego połączenia do usługi na serwerze,

- e. wykrycie nieautoryzowanego połączenia z serwera usług,
- f. wykrycie nieautoryzowanego połączenia do sieci Internet.

59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:

- a. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
- b. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
- c. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
- d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.

60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:

- a. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
- b. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
- c. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
- d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:

- a. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
- b. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
- c. wykrycie zdarzeń o wysokim „severity” na zasobach posiadających krytyczne podatności,
- d. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.

62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:

- a. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,
- b. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:

- a. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
- b. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
- c. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.

64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:

- a. wykrycie anomalii na koncie uprzywilejowanym użytkownika,
- b. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
- c. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
- d. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
- e. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:

- a. sparsowane pola oraz ich wartości,
- b. atrybuty użytkowników z Active Directory,
- c. atrybuty komputerów z Active Directory,
- d. informacje z elektronicznej dokumentacji.

66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:

- a. adresie IP,
- b. koncie domenowym użytkownika,

- c. strefie bezpieczeństwa,
- d. zakresie adresów IP.

67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.

68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.

69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.:

- a. wszystkie skorelowane zdarzenia,
- b. korespondencja pocztowa,
- c. załączniki z próbkami lub dowodami,
- d. wskaźniki kompromitacji (IoC),
- e. informacje pozyskane z innych systemów.

70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.

71. Dla obsługiwanego zdarzenia system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.

72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:

- a. identyfikację celu i źródła zagrożenia,
- b. nazwę oraz adres IP źródła zagrożenia,

- c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
- d. lokalizację z której pochodzi zagrożenie np.: Internet,
- e. strefę bezpieczeństwa z której pochodzi zagrożenie,
- f. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
- g. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
- h. nazwę oraz adres IP celu zagrożenia,
- i. zabezpieczenia lokalne chroniące cel zagrożenia,
- j. strefę bezpieczeństwa w której znajduje się cel zagrożenia.

73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).

74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.

75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:

- a. nazwy zasobu,
- b. rodzaju zasobu,
- c. ważności zasobu dla organizacji,
- d. rodzaj przetwarzanych informacji,
- e. usług, które ten zasób świadczy,
- f. lokalizację użytkowników, którzy z niego korzystają,
- g. usługi z których zasób korzysta.

76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi

uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.

77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:

- a. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
- b. segregacja – segregacja i kwalifikacja zdarzeń,
- c. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
- d. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
- e. zdarzenie obsłużone – zdarzenie, które zostało obsłużone w systemie.

System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.

78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.

79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.

81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.

82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.

83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.

84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:

- a. podgląd aktywności zagrożonego zasobu na linii czasu,
- b. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
- c. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
- d. podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
- e. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
- f. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
- g. gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o:
 - listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
 - listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
 - gotowe i proste w użyciu filtry rozszerzające analizę logów o:
 - listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
 - listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

- a. warunki powiadomień,

- zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
- zdarzeń o przekroczonych czasach SLA o definiowalny okres,
- zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
- zdarzeń, których priorytet osiągnął określoną wartość,
- zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
- zdarzeń, na których doszło do naruszenia bezpieczeństwa,
- zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
- zdarzeń realizujących zdefiniowaną usługę,
- zdarzeń przetwarzających sklasyfikowane informacje,
- zdarzeń przetwarzanych na krytycznych zasobach,

b. odbiorców powiadomień, w tym:

- operatora, któremu zostało przydzielone zdarzenie,
- właściciela zasobu na którym wystąpiło zdarzenie,
- zespół obsługi, który odpowiada za obsługę zdarzeń,
- właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
- podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.

c. kanały powiadomień, m.in. e-mail, sms, komunikator,

d. zastosowanie mechanizmów grupowania:

- grupowanie wielu powiadomień w jednej wiadomości,
- ograniczenie liczby wierszy powiadomienia do określonej wartości.

86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

- a. utworzenia nowego zdarzenia z określonym priorytetem,
- b. utworzenia nowego zdarzenia na zasobie krytycznym,
- c. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
- d. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
- e. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
- f. modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,
- g. zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,
- h. przejścia przydzielonego operatorowi zdarzenia przez innego operatora.

87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę

elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:

- a. wybór raportu, który ma zostać wysłany,
- b. zdefiniowanie jego tytułu,
- c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
- d. możliwość ograniczenia cyklu do dni powszednich,
- e. określenie daty przesłania pierwszego raportu,
- f. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
 - zdefiniowanej daty końcowej,
 - określonej liczby raportów,
- g. określenie odbiorców raportu.

88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).

89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczają dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:

- a. strefę bezpieczeństwa w której została wykryta podatność,
- b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
- c. rodzaj zasobu którego dotyczy ta podatność,
- d. ważność tego zasobu dla organizacji,
- e. przetwarzane na tym zasobie informacje, np.: dane osobowe,
- f. usługi realizowane przez ten zasób, np.: DNS,
- g. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
- h. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
- i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.

90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jak i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.

91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:

- a. wyliczonym priorytecie podatności,
- b. aktualnym statusie obsługi,
- c. ważności zasobu na którym została wykryta,
- d. adresie IP tego systemu,
- e. parametrów SLA związanych z tym statusem,
- f. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
- g. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”.

92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:

- a. przekroczenia czasu reakcji o określony czas np.: o godzinę,
- b. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
- c. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
- d. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
- e. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
- f. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
- g. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
- h. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
- i. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
- j. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
- k. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,

93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

a. warunki powiadomień,

- podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
- podatności o przekroczonych czasach SLA o definiowalny okres,
- podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
- podatności, których priorytet osiągnął określoną wartość,
- zdarzeń realizujących zdefiniowaną usługę,
- zdarzeń przetwarzających sklasyfikowane informacje,
- zdarzeń przetwarzanych na krytycznych zasobach,

b. odbiorców powiadomień, w tym:

- operatora, któremu została przydzielona podatność,
- właściciela zasobu na którym wystąpiła podatność,
- zespół obsługi, który odpowiada za obsługę podatności,
- właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,
- podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.

c. kanały powiadomień, m.in. e-mail, sms, komunikator,

d. zastosowanie mechanizmów grupowania:

- grupowanie wielu powiadomień w jednej wiadomości,
- ograniczenie liczby wierszy powiadomienia do określonej wartości.

94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

- przydzielenia nowej podatności do obsługi z określonym priorytetem,
- przydzielenia nowej podatności do obsługi na zasobie krytycznym,
- przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
- przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
- modyfikacji przydzielonej operatorowi podatności przez innego operatora,
- zamknięcia przydzielonej operatorowi podatności przez innego operatora,
- przejęcia przydzielonej operatorowi podatności przez innego operatora.

95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:

- wybór raportu który ma zostać wysłany,

- b. zdefiniowanie jego tytułu,
- c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
- d. możliwość ograniczenia cyklu do dni powszednich,
- e. określenie daty przesłania pierwszego raportu,
- f. określenie okresu przez jaki będą one przesyłane, poprzez:
 - zdefiniowanie daty końcowej,
 - bez daty końcowej,
 - określenie liczby raportów,
- g. określenie odbiorców raportu.

96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentację danych do potrzeb zalogowanego użytkownika.

97. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących:

- a. zestaw wykresów dla bieżącego użytkownika,
- b. zestaw wykresów dla wybranego użytkownika,
- c. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
- d. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

98. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy:

a. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:

- ilość zdarzeń nowych i niesklasyfikowanych,
- ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
- ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,

b. wykres przedstawiający skalę zagrożeń, który uwzględnia:

- ilość zasobów krytycznych na których są obsługiwane zdarzenia,
- ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,

c. wykres przedstawiający źródła zagrożeń, który uwzględnia:

- ilość nowych zdarzeń dotyczących użytkowników,
- ilość podjętych zdarzeń dotyczących użytkowników,
- ilość nowych zdarzeń dotyczących zasobów,
- ilość podjętych zdarzeń dotyczących zasobów,

d. wykres przedstawiający poziom zagrożeń, który uwzględnia:

- ilość nowych zdarzeń w podziale na priorytety,
 - ilość podjętych zdarzeń w podziale na priorytety,
- e. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
- ilość zdarzeń zarejestrowanych w bieżącym dniu,
 - ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
 - ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
 - ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
- f. wykres przedstawiający zagrożone usługi, który uwzględnia:
- ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
 - ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
- g. wykres przedstawiający zagrożone dane, który uwzględnia:
- ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
- h. wykres przedstawiający skalę podatności, który uwzględnia:
- ilość zasobów krytycznych na których są obsługiwane podatności,
 - ilość zasobów niekrytycznych na których są obsługiwane podatności,
- i. wykres przedstawiający czas obsługi podatności, który uwzględnia:
- ilość podatności zarejestrowanych w bieżącym dniu,
 - ilość podatności zarejestrowanych w ostatnim tygodniu,
 - ilość podatności zarejestrowanych w ostatnim miesiącu,
 - ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,
- j. wykres przedstawiający wagę podatności, który uwzględnia:
- ilość nowych podatności w podziale na priorytety,
 - ilość podjętych podatności w podziale na priorytety,

99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:

- a. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać

te same wartości których dotyczy wykres,

- b. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- c. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- d. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- e. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- f. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.

100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.

101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:

- a. kolektor parsujący;
- b. kolektor logów;
- c. kolektor korelacyjny;
- d. kolektor zdarzeń;
- e. kolektor sztucznej inteligencji;
- f. kolektor reakcyjny;
- g. kolektor kontrolujący.

102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie

z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tys zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.

105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).

106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.

107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.

108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.

109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszą być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.

110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.

111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jak i przywracanie poprzednich wersji reguł i parserów.

112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tys zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.

114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)

115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.

116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.

117. Rozwiązanie nie może przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, PostgreSQL, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.

118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.

119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.

120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).

121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.

122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów

123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).

125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:

- a. zdolność do definiowania wzorców które powtarzają się jako zmienne;
- b. zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;
- c. zdolność do testowania poszczególnych funkcji;
- d. zdolność do przekształcania danych w trakcie ich parsowania.

126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:

- a. centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;
- b. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;
- c. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;
- d. zdolność do monitorowania integralności plików;
- e. zdolność do monitorowania rejestru systemowego;
- f. zdolność do monitorowania urządzeń zewnętrznych (removable devices);
- g. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;
- h. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemem;
- i. musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;
- j. musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.

127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.

128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI

129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Intelligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.

130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).

131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi
132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal.
133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.
134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.
135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.
136. System musi wspierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyłeń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.
137. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang.: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.
138. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalnościami będzie mógł je potwierdzić lub im zaprzeczyć.

139. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.

140. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencja nie może nakładać limitów w tym zakresie.

141. Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz obsługiwać 100 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.

142. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.

143. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

144. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).

145. Dostarczone rozwiązanie musi być objęte minimum 24 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędów krytycznych lub poważnych).

146. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji).

Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.

147. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 10 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.

148. Zamawiający wymaga by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający maksymalnie w ciągu dwóch dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ. W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona.

149. Wykonawca musi dostarczyć oferowane rozwiązanie w formie demonstracyjnej aby umożliwić weryfikację przez Zamawiającego wybranych wymagań OPZ, co do których Zamawiający nie uzyskał wystarczających informacji potwierdzających ich zgodność. Rozwiązanie musi być skonfigurowane w sposób umożliwiający jego weryfikację z wymaganiami OPZ oraz pozwalać na zdalny dostęp. W ramach dostępu do rozwiązania, Wykonawca musi przygotować odpowiednią instrukcję oraz zapewnić wsparcie konsultanta technicznego. Procedura weryfikacji spełnienia wymagań OPZ będzie przebiegać następująco:

- a. Zamawiający dokona wyboru min. 10 wymagań OPZ, które zostaną zaprezentowane przez Wykonawcę na systemie demonstracyjnym;
- b. Wykonawca w terminie 2 dni od wyboru wymagań OPZ (ppkt a) dostarczy zwięzły opis do każdego z wybranych wymagań, określający zakres planowanych testów demonstracyjnych;
- c. Wykonawca w terminie 3 dni od dostarczenia opisu (ppkt b) dokona przygotowania systemu demonstracyjnego, w tym: dokona odpowiedniej konfiguracji systemu (umożliwiającego weryfikację wskazanych wymagań OPZ), przygotuje instrukcję dostępową do systemu demonstracyjnego; opracuje instrukcję realizacji zaproponowanych scenariuszy testowania;

- d. Wykonawca przekaże Zamawiającemu dostęp do systemu demonstracyjnego na okres 3 dni w celu analizy zgodności z OPZ oraz weryfikacji intuicyjności obsługi.
- e. Zamawiający oceni każde z 10 wybranych wymagań, uwzględniając:
 - Intuicyjność (25%)
 - Zgodność (75%)
- f. Każde z wymagań może uzyskać maksymalną ocenę 100%. Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%. Procentowa suma wszystkich wymagań nie może być niższa niż 90%.
- g. Wykonawca w okresie 3 dni od otrzymania oceny ze strony Zamawiającego (ppkt. f) ma możliwość wyznaczenia spotkania w formie zdalnej (np. za pomocą platformy: Teams, Zoom lub Webex), podczas którego odniesie się on do wyników oceny zgodności i intuicyjności systemu, opracowanych przez Zamawiającego. Jeśli w wyznaczonym terminie Wykonawca nie zorganizuje spotkania i/lub nie przedstawi odpowiedzi na ocenę Zamawiającego zostanie uznane, że oferowane rozwiązanie spełnia wymagań OPZ.

150. System XDR powinien posiadać następujące cechy i funkcjonalności

- a. Powinien posiadać możliwość instalacji agenta XDR na systemach: ~~Windows~~ Windows 10 i nowsze,
- b. Windows Server 2016 i nowsze. Agent umożliwia: zbieranie logów ze stacji końcowej/serwera do modułu SIEM, dodawania i wyłączanie reguł zapory sieciowej na stacji końcowej/serwerze, zawieszanie i odwieszanie procesu na stacji końcowej/serwerze. Dodatkowo zapewnia mechanizm do instalacji oraz zarządzania konfiguracją narzędzia Microsoft Sysmon na stacjach końcowych/serwerach, w celu rozszerzenia logów systemowych o aktywność procesów, plików oraz rejestrów.
- c. System powinien być wyposażony w serwer aplikacji udostępniający konsolę graficzną dla operatorów oraz sterujący działaniem orkiestratora oraz kontrolera
- d. System powinien posiadać Orkiestrator służący do wykonania akcji na innych systemach niż komputery, na których zainstalowany jest agent XDR, np.: zablokowanie ruchu wychodzącego na Firewall dla hosta na którym zainstalowany jest agent służy do zarządzania agentami XDR i jest odpowiedzialny zarówno za ich monitorowanie, aktualizację oraz zlecanie im zadań, np.: izolacja procesu czy izolacja sieciowa
- e. Agent XDR powinien wzbogacać analizę zdarzeń na nim występujących o pełne dane telemetryczne.
- f. System powinien posiadać centralny kontroler zarządzający agentami XDR oraz monitorujący ich pracę
- g. System powinien posiadać mechanizm wykrywania zagrożeń zgodny z taktykami i technikami Mitre

Att&ck™

- h. System powinien umożliwiać wykrywanie zagrożeń na komputerze na bazie wielu wskaźników naruszeń bezpieczeństwa (IoC)
- i. System powinien umożliwiać centralną korelację zdarzeń z komputera względem innych zdarzeń (sieć, chmura, Threat Intel)
- j. System powinien być wyposażony w mechanizmy uczenia maszynowego obejmujące analizę behawioralną komputera oraz jego użytkownika
- k. System powinien posiadać wiele algorytmów wykrywania anomalii oraz profilowania komputera i jego użytkownika
- l. System powinien umożliwiać rozszerzoną analizę behawioralną użytkownika komputera względem pracy innych użytkowników
- m. System powinien umożliwiać kontrolę aplikacji zainstalowanych na stacjach roboczych i serwerach
- n. System powinien umożliwiać kontrolę podatności, zgodności oraz zainstalowanych poprawek
- o. System powinien mieć możliwość zaawansowanej analizy zdalnej np.: uruchomione procesy czy połączenia sieciowe
- p. System powinien posiadać mechanizmy automatyzujące reakcję na komputerze z poziomu agenta, np.: wstrzymanie procesu, blokada portu
- q. System powinien posiadać funkcjonalność dostosowania reakcji na zagrożenia w zależności od rodzajów zagrożeń (konfigurowalne playbooki)
- r. System musi być wyposażony w autonomiczny mechanizm oceny ryzyka dla wykrytych zagrożeń
- s. System powinien umożliwiać zarządzanie zgodnością (Compliance): KSC/KRI/GDRP
- t. System powinien posiadać panel do zarządzania incydentami oraz podatnościami wsparty playbookami
- u. System powinien posiadać przejrzyste dashbordy z możliwości drążenia danych oraz wizualizacji zagrożeń
- v. System powinien posiadać możliwości powiadamiania o zagrożeniach poprzez e-mail, sms

II.8 Serwer tworzący platformę sprzętową dla SOC – 1 szt.

Należy dostarczyć serwer o wysokiej wydajności, umożliwiający instalację wszystkich niezbędnych maszyn wirtualnych wchodzących w skład platformy SIEM z modułem SOAR. Parametry minimalne dla serwera:

Element konfiguracji	Wymagania minimalne
----------------------	---------------------

Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie). Obudowa wyposażona w zamykany panel chroniący dyski twarde przed nieuprawnionym wyjęciem.
Procesor	Procesor min. 16 rdzeniowy, osiągający w teście SPECrate®2017_int_base wynik co najmniej 217 punktów. Płyta główna obsługująca procesory od 16 do 128 rdzeni, wymagające mocy do 400W.
Liczba procesorów	1
Pamięć operacyjna	Zainstalowanych min. osiem modułów 64 GB DDR5 6400MT/s każdy. Płyta główna z minimum 12 slotami na pamięć, umożliwiającą instalację do minimum 3TB pamięci RAM, obsługująca moduły 6400 MT/s Obsługa zabezpieczeń: Advanced ECC.
Sloty rozszerzeń	Możliwość instalacji 6 kart PCI-Express generacji 5 pełnej wysokości, x16 (szybkość slotu – bus width).
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę min. 8 dysków oraz obsługujący poziomy: RAID 0,1,10,5,50,6,60, nie zajmujący gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
Dysk twardy	Możliwość instalacji do 20 dysków 3,5”. Zainstalowane 3 dyski 7.2k RPM o pojemności min. 24 TB każdy. Zainstalowane min. 3 dyski SSD o pojemności 3.84TB każdy.
Interfejsy sieciowe	Zainstalowana karta sieciowa z dwoma portami 10Gb SFP+ nie zajmująca slotów PCIe opisanych w sekcji „Sloty rozszerzeń”. Zainstalowana karta sieciowa z dwoma portami 10Gb SFP+. Zainstalowana karta z 4 portami 1Gbit nie zajmująca slotów PCIe opisanych w sekcji „Sloty rozszerzeń”.
Karta graficzna	Zintegrowana karta graficzna z pamięcią min. 16 MB, umożliwiającą wyświetlenie obrazu min. 1920 x 1200@60Hz
Porty	Min. 4 porty USB 3.2 wbudowane (w tym min. 1 port wewnętrzny i 1 z przodu obudowy) 1 port VGA Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express

	1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy maximum 1000W, efektywność zasilaczy 94%
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	<p>Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.</p>
Karta/moduł zarządzający i system zarządzania	<p>Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:</p> <ul style="list-style-type: none"> • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez <ul style="list-style-type: none"> - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera <p>dostęp do karty możliwy</p> <ul style="list-style-type: none"> - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)

- wbudowane narzędzia diagnostyczne
- zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
- obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
- wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
- przysyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
- obsługa zdalnego serwera logowania (remote syslog)
- wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
- funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
- zdalna aktualizacja oprogramowania (firmware)
- zarządzanie grupami serwerów, w tym:
 - tworzenie i konfiguracja grup serwerów
 - sterowanie zasilaniem (wł./wył.)
 - ograniczenie poboru mocy dla grupy (power capping)
 - aktualizacja oprogramowania (firmware)
 - wspólne wirtualne media dla grupy
- możliwość równoczesnej obsługi przez 6 administratorów
- autentykacja dwuskładnikowa (Kerberos)

	<ul style="list-style-type: none"> wsparcie dla Microsoft Active Directory obsługa SSL i SSH enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API wsparcie dla Integrated Remote Console for Windows clients możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	<p>Min. Microsoft Windows Server 2019, 2022, 2025</p> <p>Min. Red Hat Enterprise Linux (RHEL): 8.6, 9.0</p> <p>Min. SUSE Linux Enterprise Server (SLES) 15</p> <p>Min. VMware ESXi 7.0 U3, 8.0</p>
System operacyjny	<p>Serwerowy System Operacyjny musi posiadać następujące, wbudowane cechy minimalne:</p> <ol style="list-style-type: none"> Współpraca z procesorami o architekturze x86-64 bit Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. Pojedyncza licencja musi obsługiwać serwer fizyczny wyposażony w 1 procesor 16 rdzeniowy. Dostarczona licencja musi umożliwiać na instalację min. 2 wystąpień wirtualnych (min. 2 maszyn wirtualnych) Praca w roli klienta domeny Microsoft Active Directory. System musi być wspierany przez producenta oprogramowania do 2030 r. (wsparcie techniczne, aktualizacje bezpieczeństwa) Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2022. Możliwość uruchomienia roli klienta i serwera czasu (NTP). Możliwość uruchomienia roli serwera plików w z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. Możliwość uruchomienia roli serwera stron WWW. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania.
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18. Wbudowany mechanizm klasyfikowania i indeksowania plików w (dokumentów) w oparciu o ich zawartość
19. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
20. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilkoma serwerami.
21. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
22. Zlokalizowane w języku polskim lub angielskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
24. Mechanizmy logowania w oparciu o:
 - a. login i hasło,
 - b. karty z certyfikatami (smartcard),
 - c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
25. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
 - a. określonych grup użytkowników.

- b. zastosowanej klasyfikacji danych,
 - c. centralnych polityk dostępu w sieci,
 - d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
26. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
27. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
28. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
29. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
30. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
31. Możliwość implementacji usług sieciowych: DHCP oraz DNS wspierający DNSSEC.
32. Możliwość implementacji usług katalogowej oparte o LDAP i pozwalającej na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
- a. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - b. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
 - c. zdalna dystrybucja oprogramowania na stacje robocze,
33. Możliwość implementacji Centrum Certyfikatów (CA) z obsługą klucza publicznego i prywatnego) umożliwiające:
- a. Dystrybucję certyfikatów poprzez http,
 - b. Konsolidację CA dla wielu lasów domeny

- c. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- d. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- e. szyfrowanie plików i folderów,
- f. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
- g. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
- h. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail - over) oraz rozłożenia obciążenia serwerów,
- i. serwis udostępniania stron WWW,
- j. wsparcie dla protokołu IP w wersji 6 (IPv6),
- k. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- l. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
- m. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- n. mechanizmy wirtualizacji mające wsparcie dla:
 - a. dynamicznego podłączania zasobów dyskowych typu hot plug do maszyn wirtualnych,
 - b. obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - c. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
 - d. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego

	<p>umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p> <ul style="list-style-type: none"> e. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). f. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. g. mechanizm konfiguracji połączenia VPN do platformy Azure. h. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. i. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów. j. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard) <p>Wraz z licencjami na Serwerowy Systemem Operacyjnym SSO należy dostarczyć licencje dostępowe dla 70 użytkowników, które umożliwią konkretnemu użytkownikowi dostęp do serwerów z SSO z dowolnego urządzenia. Licencje dostępowe muszą umożliwiać dostęp do: usługi katalogowej, plików na dyskach sieciowych serwerów oraz usługi drukowania sieciowego.</p>
Gwarancja	<p>Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2 godzinnym czasem reakcji na zgłoszenie. Rozpoczęcie naprawy w miejscu instalacji w następnym dniu roboczym. Usługi gwarancji oraz wsparcia technicznego muszą być świadczone przez autoryzowany serwis producenta oferowanego serwera lub autoryzowanego partnera.</p> <p>Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji oraz opcją pozostawieniem uszkodzonych dysków u Zamawiającego.</p>
Inne	<p>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.</p>

	Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
--	--

II.9 Rozbudowa infrastruktury o macierz dyskową – 1 szt.

Należy dostarczyć macierz dyskową typu NAS, wyposażoną w dyski dużej pojemności. Macierz będzie przechowywać drugą kopię danych systemów kluczowych. Macierz musi spełniać poniższe wymagania minimalne:

Typ urządzenia	Serwer NAS
Obudowa	Rack max 2U
Procesor	Min. czterordzeniowy procesor o taktowaniu min. 2,4 GHz, 64 bitowy
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć operacyjna (RAM)	min. 8 GB pamięci ECC UDIMM
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu Hot-Swap z możliwością rozszerzenia do 36 dysków łącznie, przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń
Porty zewnętrzne	Minimum: <ul style="list-style-type: none"> 2 porty USB 3.2.1 2 gniazda rozszerzeń
Porty sieciowe	Minimum: <ul style="list-style-type: none"> 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) 2 porty 10Gb SFP+ wraz z modułami
Zainstalowane dyski	Min. 8 dysków SATA3 przeznaczonych do pracy w trybie 24x7 o pojemności min. 20TB każdy, prędkość obrotowa min. 7200, pamięć podręczna min. 250MB, średni czas do wystąpienia awarii (MTTF) min. 1 mln godzin. Min 4 dyski SSD SATA 6G o pojemności min. 3.84TB każdy przeznaczone do pracy w trybie 24/7, z funkcjami: ochrona danych w przypadku nieoczekiwanej awarii zasilania, 256-bitowego szyfrowania AES.
Funkcja Wake on LAN/WAN	Tak

Gniazdo rozszerzeń PCIe 3.0	Min. 2 gniazda x8 (Gen.3)
Wentylator obudowy	Min. 4 wentylatory 80 mm x 80 mm
Obsługiwane protokoły	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: <ul style="list-style-type: none"> Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	<ul style="list-style-type: none"> Maksymalny rozmiar pojedynczego wolumenu: min. 200 TB Minimalna liczba wewnętrznych wolumenów: 120 Minimalna liczba obiektów iSCSI Target: 250 Minimalna liczba jednostek iSCSI LUN: 500 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	<ul style="list-style-type: none"> Minimalna liczba kont użytkowników: 16 000 Minimalna liczba grup użytkowników: 500 Minimalna liczba folderów współdzielonych: 500 Maksymalna liczba jednoczesnych połączeń SMB/AFP/FTP min. 2000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP, integracja z LDAP
System logów	Liczba rejestrowanych zdarzeń Syslog na sekundę min. 3000
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Safari®
Oprogramowanie	<ul style="list-style-type: none"> Urządzenie musi umożliwiać obsługę migawek w zakresie min.: <ul style="list-style-type: none"> Możliwość planowania i niemal natychmiastowa ochrona danych Obsługa różnych topologii replikacji dla różnych scenariuszy, w tym architektury active-active, rozszerzonej replikacji, replikacji typu jeden do wielu i typu hub-to-spoke

	<ul style="list-style-type: none"> – Szybkie odzyskiwanie danych w lokalizacji odzyskiwania po awarii – Obsługa funkcji migawek folderów współdzielonych w wolumenie i jednostkach LUN z systemem plików Btrfs, w tym harmonogramowanie, zarządzanie, przeglądanie, odzyskiwanie – Obsługa podglądu migawek i kopiowania plików w dedykowanej aplikacji – Obsługa podglądu migawek, kopiowania plików i odzyskiwania w Eksploratorze plików systemu Windows • Możliwość uruchomienia replikacji danych w czasie rzeczywistym między serwerem aktywnym a pasywnym w celu zachowania spójności danych i maksymalizacji dostępności usług • Wymaga się zapewnienia darmowej aplikacji do realizacji synchronizacji i udostępniania pomiędzy serwerem, a różnymi chmurami publicznymi, takimi jak Dropbox, Baidu Cloud i Dysk Google. • Wymaga się dostarczenia licencji na 5 kont e-mail oraz możliwości rozbudowy licencji do 750 kont e-mail
Montaż w szafie	<ul style="list-style-type: none"> • szyny rack, wysuwane
Zasilanie	<ul style="list-style-type: none"> • Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz o mocy max. 550W
Gwarancja	<p>Wykonawca udzieli gwarancji:</p> <ul style="list-style-type: none"> • 3 lata na urządzenia główne • 3 lata na dyski twarde <p>Wymagana jest możliwość rozszerzenia gwarancji do 5 lat</p>

II.10 Zakup niezbędnych licencji do funkcjonowania środowiska bazodanowego

W przypadku zaoferowania systemu SIEM z modulem SOAR wymagającego dodatkowej licencji na bazę danych firmy trzeciej, należy ją dostarczyć, zainstalować i skonfigurować w wymaganej przez producenta systemu SIEM/SOAR wersji. Licencja musi być dostarczona w postaci licencji bezterminowej. Jeżeli do

prawidłowego działania lub dostępu do aktualizacji wersji, poprawek niezbędne jest wsparcie techniczne producenta je dostarczyć wraz z licencją na okres min. 12 miesięcy.

Wymagania minimalne dla licencji środowiska bazodanowego:

Na potrzeby uruchomienia systemu SIEM i kolekcjonowania logów z urządzeń Zamawiającego, niezbędna jest licencja dla serwera bazy danych. Należy dostarczyć licencję bezterminową na serwer bazy danych w najnowszej dostępnej wersji wraz z licencją dla 2 użytkowników. System bazodanowy (SBD) musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

1. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych.
7. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
 - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
 - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
 - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,

8. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.

9. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128, AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.

10. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.

11. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.

12. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń.

Wymagana jest rejestracja zdarzeń:

- odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
- wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
- para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).

13. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.

14. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficzną dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania

danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.

15. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:

- udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
- udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
- udostępniać język zapytań do struktur XML,
- udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
- udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.

16. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:

- zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
- oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
- obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
- typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.)

17. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania.

18. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.

19. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.

20. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.

21. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.

22. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:

- mechanizm debuggowania tworzonego rozwiązania,
- mechanizm stawiania „pułapek” (breakpoints),
- mechanizm logowania do pliku wykonywanych przez transformację operacji,
- możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
- możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
- mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
- mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),

- mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
- mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przepamiętania kolumn w sytuacji podmiiany źródła danych.

23. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.

24. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).

25. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądaniem obszarem kostki).

26. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.

27. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).

28. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytowywania tych modeli.

29. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności

powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.

30. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępniane przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:

- raporty parametryzowane,
- cache raportów (generacja raportów bez dostępu do źródła danych),
- cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
- współdzielenie predefiniowanych zapytań do źródeł danych,
- wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
- możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
- możliwość wizualizacji wskaźników KPI,
- możliwość wizualizacji danych w postaci obiektów sparkline.

31. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).

32. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.

33. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.

34. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).

35. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.

36. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache'u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.

37. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.

38. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).

II.11 Przedłużenie licencji i wsparcia na posiadane rozwiązanie do zarządzania infrastrukturą, stacjami roboczymi i serwerami

Oferowane oprogramowanie musi być dostarczone jako licencja bezterminowa umożliwiająca zarządzanie min. 70 stacjami roboczymi. Licencja powinna obejmować następujące możliwości oraz funkcjonalności w odniesieniu do infrastruktury Zamawiającego:

1. Skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP, tworzenie interaktywnych map sieci, map użytkownika, oddziałów, map inteligentnych.
2. Serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/ utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.).
3. Liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
4. Działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń.
5. Liczniki SNMP v1/2/3 (np. Transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne).
6. Zarządzanie wszelkimi zasobami, za które odpowiada dział IT.
7. Szczegółowe informacje i ewidencja czynności wykonywanych na zasobach w trakcie całego cyklu życia, możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu.
8. Widok zasobów, aplikacji, dokumentów, licencji dla poszczególnych użytkowników lub osobny widok według zasobów przypisanych do urządzeń.
9. Jednoczesne przypisywanie dokumentu do wielu zasobów.
10. Uprawnienia dostępu administratorów do typów zasobów, licencji i dokumentów w ramach oddziałów.
11. Masowa edycja atrybutów zasobów, np. Statusu.
12. Rozbudowany system zarządzania aplikacjami i licencjami, identyfikacja realnego zużycia licencji.
13. Rozliczanie dowolnego typu licencji, w tym modelowanie licencji chmurowych.

14. Rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji.
15. Audyt inwentaryzacji sprzętu i oprogramowania.
16. Wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach.
17. Zdalny dostęp do menedżera plików z możliwością usuwania plików użytkownika.
18. Pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa, w tym:
 - a. blokowanie uruchamianych aplikacji,
 - b. monitorowanie wiadomości e-mail (nagłówki) – antyphishing,
 - c. szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy),
 - d. używane aplikacje (aktywnie i nieaktywnie),
 - e. odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt),
 - f. audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków,
 - g. statyczny zdalny podgląd pulpitu użytkownika (bez dostępu),
 - h. zrzuty ekranowe (historia pracy użytkownika ekran po ekranie),
 - i. blokowanie stron WWW,
 - j. rejestr naruszeń blokad agregujący informacje o próbie dostępu do blokowanych stron WWW, uruchamianiu zakazanych aplikacji oraz pobieraniu plików z niedozwolonymi rozszerzeniami.
19. Informacje o urządzeniach podłączonych do danego komputera.
20. Lista wszystkich urządzeń podłączonych do komputerów w sieci.
21. Audyt (historia) połączeń i operacji na urządzeniach przenośnych oraz udziałach sieciowych i dyskach lokalnych.
22. Monitorowanie operacji na plikach w katalogach na dysku systemowym.
23. Monitorowanie operacji na plikach z zasobów sieciowych udostępnianych przez urządzenia nieobsługiwane przez agenta.
24. Zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników.
25. Centralna konfiguracja: ustawienie reguł dla całej sieci oraz grup i użytkowników Active Directory.
26. Integracja bazy użytkowników i grup z Active Directory.
27. Alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym oraz na dyskach lokalnych.
28. Oprogramowanie musi być objęte wsparciem technicznym producenta przez okres min. 24 miesięcy.

II.12 Przedłużenie wsparcia na posiadane rozwiązanie do kopii zapasowych

Przedłużenie wsparcia na posiadane rozwiązanie do tworzenia kopii zapasowych stacji roboczych

Zamawiający posiada licencję programu Ferro Backup, który jest wykorzystywanych do tworzenia kopii zapasowych systemów operacyjnych stacji roboczych. Należy przedłużyć wsparcie techniczne dla posiadanych licencji na kolejne 12 miesięcy lub dostarczyć oprogramowanie spełniające poniższe wymagania minimalne:

1. Zintegrowane rozwiązanie do tworzenia kopii zapasowych musi współpracować z serwerami fizycznymi z systemem Windows oraz Linux, komputerami z systemem Windows, Mac, serwerami plików RSync i SMB oraz maszyn wirtualnych min. VMware vSphere, Microsoft Hyper-V.
2. Centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych.
3. Różne metody przywracania, w tym przywracanie całego urządzenia, natychmiastowe przywracanie, szczegółowe odzyskiwanie plików.
4. Maksymalna wydajność tworzenia kopii zapasowych i pamięci masowej dzięki zastosowaniu funkcji deduplikacji globalnej.
5. Możliwość tworzenia szczegółowe logów i raportów umożliwiających śledzenie stanów kopii zapasowych i diagnostykę problemów.
6. Możliwość generowania raportów według dostosowanego harmonogramu w celu śledzenia ogólnego stanu kopii zapasowej.
7. Możliwość przeglądania szczegółowe dzienników i historii zadań dotyczących stanu kopii zapasowej, anulowanych zadań, niepowodzeń tworzenia kopii zapasowej, migracji przywracania i przywracania urządzeń.
8. Możliwość włączenia kompresja lub szyfrowanie w miejscu docelowym kopii zapasowej.
9. Po włączeniu kompresji lub szyfrowania w miejscu docelowym kopii zapasowej funkcja natychmiastowego przywracania w programie Microsoft Hyper-V lub Virtual Machine Manager nie jest dostępna w niektórych modelach.
10. Obsługiwane platformy Windows: 11 (wszystkie wersje), Windows 10 (wszystkie wersje), Windows 8.1 (wszystkie wersje) i Windows 7 SP1 (wszystkie wersje) w zakresie minimum:
 - a) Obsługa systemu plików NTFS,
 - b) Tryby tworzenia kopii zapasowej: kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu,
 - c) Metody przywracania: przywracanie całego urządzenia, przywracanie na poziomie plików/folderów oraz przywracanie na poziomie woluminów,
 - d) Kopia zapasowa oparta na obrazie musi tworzyć kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu,

- e) Kopia zapasowa oparta na agencie musi tworzyć kopie zapasowe i przywracać zmienione bloki znalezione między migawkami,
 - f) Oprogramowanie musi umożliwiać tworzenie przyrostowych kopii zapasowych,
 - g) Zdarzenie tworzenia kopii zapasowych może być wyzwalane zdarzeniami: blokada ekranu urządzenia, wylogowanie użytkownika i uruchamianie urządzenia,
 - h) Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej,
 - i) Obsługa wstawiania argumentów (adres IP serwera NAS, nazwa użytkownika, hasło i tworzenie ikony kopii zapasowej) do instalatora .msi w celu masowego wdrażania agenta na urządzeniach w domenie Active Directory,
 - j) Maksymalna wielkość pojedynczej kopii zapasowej co najmniej 60 TB dla NAS z systemem BTRFS,
 - k) Możliwość tworzenia kopii zapasowych na zewnętrznych dyskach twardych,
 - l) Możliwość tworzenia kopii zapasowych dysków dynamicznych min. woluminy proste.
11. Obsługiwane platformy macOS min.: Catalina 10.15.7, Big Sur 11, Monterey 12, Ventura 13, Sonoma 14 w zakresie minimalnym:
- a) Obsługuje system plików APFS,
 - b) Tryby tworzenia kopii zapasowych: kopia zapasowa całego urządzenia, woluminu systemowego i niestandardowego woluminu,
 - c) Metody przywracania: przywracanie na poziomie plików/folderów,
 - d) Kopia zapasowa oparta na agencie tworzy kopie zapasowe i przywraca zmienione bloki znalezione między migawkami,
 - e) Wykorzystuje Apple Software Restore do wykonywania przyrostowych kopii zapasowych z funkcją śledzenia zmiany bloków,
 - f) Okno tworzenia kopii zapasowych umożliwia użytkownikom dostosowanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych,
 - g) Możliwość tworzenia kopii zapasowych zewnętrznych dysków twardych w formacie APFS,
 - m) Możliwość tworzenia kopii zapasowych dysków dynamicznych min. woluminy proste.
12. Obsługiwane platformy serwerowe min.: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 i Windows Server 2022, Windows Server 2025 w zakresie minimalnym:
- a) Obsługa systemu plików NTFS,
 - b) Tryby tworzenia kopii zapasowych: Kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu,

- c) Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów, przywracanie na poziomie woluminów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V,
 - d) Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu,
 - e) Kopia zapasowa oparta na agencie tworzy kopie zapasowe zmienionych bloków znalezionych między migawkami,
 - f) Oprogramowanie musi umożliwiać tworzenie przyrostowych kopii zapasowych,
 - g) Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej,
 - n) Obsługa wstawiania argumentów (adres IP serwera NAS, nazwa użytkownika, hasło i tworzenie ikony kopii zapasowej) do instalatora .msi w celu masowego wdrażania agenta na urządzeniach w domenie Active Directory,
 - o) Maksymalna wielkość pojedynczej kopii zapasowej co najmniej 60 TB dla NAS z systemem BTRFS,
 - h) Możliwość tworzenia kopii zapasowych na zewnętrznych dyskach twardych,
 - i) Możliwość tworzenia kopii zapasowych dysków dynamicznych min. woluminy proste.
13. Obsługiwane systemy operacyjne Linux z wersją jądra między 2.6 a 6.8, obsługiwane platformy: CentOS 7.8-8.5; RHEL 6.10-9.4; Ubuntu 20.04-24.04; Fedora 38-40; Debian 10-12 w zakresie minimalnym:
- a) Obsługa systemów plików min.: ext2, ext3, ext4, XFS,
 - b) Tryby tworzenia kopii zapasowych: Całe urządzenie, wolumen systemowy i dostosowane kopie zapasowe wolumenów,
 - c) Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów, przywracanie na podstawie wolumenów oraz natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V,
 - d) Kopia zapasowa oparta na obrazach musi tworzyć kopie całych urządzeń, w tym danych i konfiguracji systemu,
 - e) Kopia zapasowa oparta na agencie musi tworzyć kopie zapasowe i przywraca zmienione bloki znalezione między migawkami,
 - f) Oprogramowanie może wykorzystywać śledzenie zmienionych bloków oparte na sterowniku migawki Linux do wykonywania kopii zapasowych przyrostowych,
 - g) Okno tworzenia kopii zapasowych umożliwia użytkownikom dostosowanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych,
 - h) Oprogramowanie musi obsługiwać co najmniej następujące typy urządzeń: /dev/sdx, /dev/hdx, /dev/vdx, /dev/nvmex, /dev/mdx.

14. Obsługa serwerów plików SMB w zakresie minimalnym:

- a) Obsługiwane protokoły SMB min.: SMB1, SMB2 i SMB3,
- b) Tworzenie kopii zapasowych bez agentów,
- c) Tryby tworzenia kopii zapasowych min.: wiele wersji, kopia lustrzana i przyrostowe kopie zapasowe,
- d) Metoda przywracania min.: przywracanie na poziomie plików/folderów,
- e) Obsługa tworzenia kopii zapasowych listy ACL systemu Windows,
- f) Obsługa usługi Windows VSS w celu zapewnienia spójności danych kopii zapasowej,
- g) Jednoczesne wykonywanie zadań kopii zapasowej,
- h) Obsługa systemów plików w miejscu docelowym kopii zapasowej min.: Btrfs, ext4.

15. Serwer plików Rsync w zakresie minimalnym:

- a) Obsługa wersji RSync 3.0 lub nowszej,
- b) Kopia zapasowa bez agentów,
- c) Tryby kopii zapasowych min.: wiele wersji, kopia lustrzana i przyrostowe kopie zapasowe,
- d) Metoda przywracania min. Przywracanie na poziomie pliku/folderu,
- e) Obsługa tworzenia kopii zapasowej Linux POSIX ACL,
- f) Obsługa trybu RSync module, trybu RSync shell przez SSH oraz trybu RSync module przez SSH,
- g) Obsługa uwierzytelniania za pomocą hasła lub klucza SSH,
- h) Obsługa transferu na poziomie bloku, szyfrowania i kontroli przepustowości,
- i) Jednoczesne wykonywanie zadań tworzenia kopii zapasowych,
- j) Obsługa systemów plików w miejscu docelowym kopii zapasowej min.: Btrfs, ext4.

16. Obsługa maszyn wirtualnych w zakresie minimalnym:

- a) Obsługiwane platformy VMware vSphere min.: 5.0-8.0,
- b) Obsługiwane wersje VMware vSphere: VMware free ESXi, Essentials, Essentials Plus, Standard, Advanced, Enterprise oraz Enterprise Plus,
- c) Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62 TB VMDK,
- d) Obsługa monitorów maszyny wirtualnej Microsoft Hyper-V: Hyper-V 2016, Hyper-V 2019, Hyper-V 2022 i Hyper-V 2025,
- e) Obsługa oprogramowania Microsoft System Center Virtual Machine Manager (SCVMM): System Center Virtual Machine Manager 2016, System Center Virtual Machine Manager 2019,
- f) Obsługa klastrów przełączania awaryjnego Microsoft Hyper-V: Hyper-V 2016, Hyper-V 2019, Hyper-V 2022 i Hyper-V 2025,
- g) Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0,

- h) Kopia zapasowa bez agentów,
 - i) Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych,
 - j) Metody przywracania min.: przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V,
 - k) Możliwość przywracania na poziomie plików w systemie operacyjnym gościa dla systemów plików min.: NTFS, FAT32, ext3, ext4,
 - l) Możliwość tworzenia kopii zapasowej uwzględniającej aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V,
 - m) Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V.
17. System musi być wyposażony w konsolę do przywracania danych o funkcjonalności minimalnej:
- a) Możliwość przywracania pojedynczego pliku/folderu,
 - b) Możliwość wyszukiwania słów kluczowych użytkowników,
 - c) Zbiorcze przywracanie pliku/folderu w tym samym katalogu,
 - d) Możliwość przywracania plików/folderów do nowych urządzeń z tym samym systemem operacyjnym,
 - e) Możliwość przywracania danych kopii zapasowej fizycznych serwerów z systemem Windows/Linux, serwerów plików i maszyn wirtualnych należących do wersji kopii zapasowych zakończonych częściowym powodzeniem,
 - f) Metadane, które można przywracać, różnią się w zależności od przywracanych systemów:
 - g) Możliwość przywracania pliku/folderu Windows wg parametru: czas modyfikacji danych (mTime) i czas dostępu (aTime)
 - h) Możliwość przywracania pliku/folderu Mac wg parametru: czas modyfikacji danych (mTime), czas dostępu (aTime), właściciel pliku, uprawnienia pliku (uprawnienia ACL) i Atrybut rozszerzony.
 - i) Możliwość przywracania pliku/folderu Linux wg parametru: czas modyfikacji danych (mTime), czas dostępu (aTime), właściciel pliku i uprawnienia pliku (uprawnienia ACL)
 - j) Możliwość przywracania pliku/folderu z maszyny wirtualnej wg parametru: czas modyfikacji danych (mTime), czas dostępu (aTime), czas utworzenia (cTime) i uprawnienia pliku (uprawnienia ACL), UID i GID
 - k) Możliwość zbiorczego pobierania pliku/folderu w tym samym katalogu z kompresją do pojedynczego pliku

- l) Możliwość pobierania danych kopii zapasowej fizycznych serwerów z systemem Windows/Linux, serwerów plików i maszyn wirtualnych należących do wersji kopii zapasowych zakończonych częściowym powodzeniem.

II.13 Rozbudowa infrastruktury backupowej – zakup systemu pozwalającego na tworzenie kopii zapasowych wszystkich danych

W ramach realizacji zadania Wykonawca dostarczy nowe licencje oprogramowania do tworzenia kopii zapasowej wszystkich maszyn wirtualnych działających na hostach Zamawiającego, zainstaluje, skonfiguruje dostarczone oprogramowanie. Wykonawca opracuje politykę backupu 3-2-1 w oparciu o dostarczony sprzęt, oprogramowanie oraz sprzęt Zamawiającego, opracuje harmonogram oraz utworzy zadania backupowe. Wykonawca przeprowadzi testy odtworzeniowe, instruktaż z obsługi wdrożonego systemu tworzenia kopii, opracuje dokumentację powykonawczą.

Wymagane jest dostarczenie licencji bezterminowych ze wsparciem technicznym przez okres min. 24 miesięcy, spełniających poniższe wymagania minimalne:

1. Dostarczone oprogramowanie musi umożliwiać wykonywanie kopii zapasowych z minimum 20 maszyn wirtualnych pracujących w środowisku wirtualizacyjnym (składającym się z trzech serwerów wirtualizacyjnych) lub 10 serwerów fizycznych, każdy z własną instancją systemu operacyjnego.
2. Dostarczone oprogramowanie musi być objęte wsparciem technicznym producenta przez okres minimum 2 lat.
3. 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.
4. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Wymagania funkcjonalne

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 do 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 niezmiennosc 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.
17. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora).
18. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS).
19. Oprogramowanie musi posiadać integracje z systemami typu SIEM.
20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

Wymagania w zakresie docelowego punktu odzyskiwania

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 (LTO oraz IBM 3592).
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, 2022 lub 2025 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 VAAI, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu 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).

Wymagania w zakresie oczekiwanego czasu odzyskiwania

1. 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.
2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchamianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
3. 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.
4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.

5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
8. 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.
9. 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.
10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.
11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.
12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.

19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.
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 posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.
24. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.

Możliwości ograniczenia ryzyka

1. 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 uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3. 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.
4. 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.
5. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.
6. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.
7. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.
8. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Wsparcie dla serwerów fizycznych

1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.
3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE.
4. Rozwiązanie musi wspierać system operacyjny macOS.
5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.
6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).
7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.
8. 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.
9. Rozwiązanie musi wspierać backup podłączonych dysków USB.
10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.
11. 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).
12. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.
13. Rozwiązanie musi wspierać kontrolę pasma sieciowego.
14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci przewodowych.
15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.
16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.
17. Rozwiązanie musi wspierać technologię BitLocker.
18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.
19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorazowej 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.

20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
22. 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.
23. Rozwiązanie musi wspierać szyfrowanie.
24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.
25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.
26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.
27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

Monitorowanie systemu

1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.
2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4. System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.

7. System musi dawać możliwość połączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
12. System musi zapewnić możliwość połączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy Vmware.
17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4.

Raportowanie

1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
11. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.

15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy Vmware.
16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

1. Serwer backupowy – 1 sztuka

Wraz z licencjami na oprogramowanie do tworzenia kopii zapasowych wszystkich systemów kluczowych, należy dostarczyć serwer backupowy, na którym będzie:

- a) zainstalowane, działające oprogramowanie do backupu,
- b) przechowywana replika wszystkich kluczowym systemów Zamawiającego,
- c) przechowywana pierwsza kopia danych systemów kluczowych,
- d) odpowiednio duży zasób dyskowy umożliwiający wykonanie testów odtworzeniowych.

W przypadku awarii jednego z serwerów produkcyjnych będzie możliwe awaryjne uruchomienie systemu z dostępnej repliki lub z ostatniej kopii zapasowej na serwerze backupowym. Serwer backupowy musi spełniać poniższe wymagania minimalne:

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie). Obudowa wyposażona w zamykany panel chroniący dyski twarde przed nieuprawnionym wyjęciem.
Procesor	Procesor min. 16 rdzeniowy, osiągający w teście SPECrate®2017_int_base wynik co najmniej 217 punktów. Płyta główna obsługująca procesory od 16 do 128 rdzeni, wymagające mocy do 400W.
Liczba procesorów	1
Pamięć operacyjna	Zainstalowane min. cztery moduły 64 GB DDR5 6400MT/s każdy. Płyta główna z minimum 12 slotami na pamięć, umożliwiającą instalację do minimum 3TB pamięci RAM, obsługująca moduły 6400 MT/s Obsługa zabezpieczeń: Advanced ECC.
Sloty rozszerzeń	Możliwość instalacji 6 kart PCI-Express generacji 5 pełnej wysokości, x16 (szybkość slotu – bus width).

Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę min. 8 dysków oraz obsługujący poziomy: RAID 0,1,10,5,50,6,60, nie zajmujący gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
Dysk twardy	Możliwość instalacji do 20 dysków 3,5”. Zainstalowanych 8 dysków 7.2k RPM o pojemności min. 24 TB każdy.
Urządzenie rozruchowe	Zainstalowana karta rozruchowa, umożliwiającą start hypervizora VMware lub Hyper-V, zainstalowane 2 dyski NVMe o pojemności min. 480GB, zorganizowane w RAID 1.
Interfejsy sieciowe	Zainstalowana karta sieciowa z dwoma portami 10Gb SFP+ nie zajmująca slotów PCIe opisanych w sekcji „Sloty rozszerzeń”. Zainstalowana karta sieciowa z dwoma portami 10Gb SFP+.
Karta graficzna	Zintegrowana karta graficzna z pamięcią min. 16 MB, umożliwiającą wyświetlenie obrazu min. 1920 x 1200@60Hz
Porty	Min. 4 porty USB 3.2 wbudowane (w tym min. 1 port wewnętrzny i 1 z przodu obudowy) 1 port VGA Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express 1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy maximum 1000W, efektywność zasilaczy 94%
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.

Karta/moduł zarządzający i system zarządzania	<p>Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:</p> <ul style="list-style-type: none"> • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe, • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez <ul style="list-style-type: none"> - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera <p>dostęp do karty możliwy</p> <ul style="list-style-type: none"> - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) <ul style="list-style-type: none"> • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog)
---	--

	<ul style="list-style-type: none"> wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) zdalna aktualizacja oprogramowania (firmware) zarządzanie grupami serwerów, w tym: <ul style="list-style-type: none"> tworzenie i konfiguracja grup serwerów sterowanie zasilaniem (wł./wył.) ograniczenie poboru mocy dla grupy (power capping) aktualizacja oprogramowania (firmware) wspólne wirtualne media dla grupy możliwość równoczesnej obsługi przez 6 administratorów autentykacja dwuskładnikowa (Kerberos) wsparcie dla Microsoft Active Directory obsługa SSL i SSH enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API wsparcie dla Integrated Remote Console for Windows clients możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	<p>Min. Microsoft Windows Server 2019, 2022, 2025</p> <p>Min. Red Hat Enterprise Linux (RHEL): 8.6, 9.0</p> <p>Min. SUSE Linux Enterprise Server (SLES) 15</p> <p>Min. VMware ESXi 7.0 U3, 8.0</p>

System operacyjny

Serwerowy System Operacyjny musi posiadać następujące, wbudowane cechy minimalne:

1. Współpraca z procesorami o architekturze x86-64 bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Oferowana licencja musi obsługiwać serwer fizyczny wyposażony w oferowany procesor 16 rdzeniowy.
4. Dostarczona licencja musi umożliwiać na instalację min. 2 wystąpień wirtualnych (min. 2 maszyn wirtualnych).
5. Praca w roli klienta domeny Microsoft Active Directory.
6. System musi być wspierany przez producenta oprogramowania do 2030 r. (wsparcie techniczne, aktualizacje bezpieczeństwa).
7. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2022.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików w z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania.
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:

- a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
19. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
20. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
21. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
22. Zlokalizowane w języku polskim lub angielskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
24. Mechanizmy logowania w oparciu o:
- a. login i hasło,
 - b. karty z certyfikatami (smartcard),
 - c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
25. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
- a. określonych grup użytkowników,
 - b. zastosowanej klasyfikacji danych,
 - c. centralnych polityk dostępu w sieci,
 - d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
26. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
27. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
28. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

29. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
30. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
31. Możliwość implementacji usług sieciowych: DHCP oraz DNS wspierający DNSSEC.
32. Możliwość implementacji usługi katalogowej opartej o LDAP i pozwalającej na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - a. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - b. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
 - c. zdalna dystrybucja oprogramowania na stacje robocze.
33. Możliwość implementacji Centrum Certyfikatów (CA) z obsługą klucza publicznego i prywatnego) umożliwiające:
 - a. Dystrybucję certyfikatów poprzez http,
 - b. Konsolidację CA dla wielu lasów domeny,
 - c. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - d. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
 - e. szyfrowanie plików i folderów,
 - f. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
 - g. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
 - h. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail - over) oraz rozłożenia obciążenia serwerów,

- i. serwis udostępniania stron WWW,
 - j. wsparcie dla protokołu IP w wersji 6 (IPv6),
 - k. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 - l. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
 - m. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
34. Mechanizmy wirtualizacji mające wsparcie dla:
- a. dynamicznego podłączania zasobów dyskowych typu hot plug do maszyn wirtualnych,
 - b. obsługi ramek typu jumbo frames dla maszyn wirtualnych,
 - c. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego,
 - d. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,
 - e. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath),
 - f. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,
 - g. mechanizm konfiguracji połączenia VPN do platformy Azure,
 - h. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu,
 - i. mechanizmy pozwalające na blokadę dostępu nieznanym procesom do chronionych katalogów,

	j. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).
Gwarancja	Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2 godzinnym czasem reakcji na zgłoszenie. Rozpoczęcie naprawy w miejscu instalacji w następnym dniu roboczym. Uszkodzone w trakcie trwania gwarancji dyski twarde pozostają własnością Zamawiającego. Usługi gwarancji oraz wsparcia technicznego muszą być świadczone przez autoryzowany serwis producenta oferowanych urządzeń. Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji oraz opcją pozostawieniem uszkodzonych dysków u Zamawiającego.
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.

2. Instalacja, konfiguracja systemu do tworzenia kopii zapasowej

Wykonawca dokona konfiguracji dostarczonego systemu kopii bezpieczeństwa, która będzie obejmować:

1. instalację i konfigurację dostarczonego systemu kopii bezpieczeństwa na dostarczonym serwerze backupowym.
2. skonfigurowanie przestrzeni dla kopii bezpieczeństwa na dostarczonym serwerze backupowym.
3. konfigurację miejsc przechowywania, w tym macierzy NAS, w chmurze.
4. konfigurację polityki składowania oraz harmonogramów.
5. konfigurację zabezpieczeń wewnętrznych, w tym kopii ratunkowej (ang. disaster recovery) systemu kopii bezpieczeństwa.
6. instalację i konfigurację dodatkowych maszyn wirtualnych klientów, jeśli są wymagane, w środowisku Zamawiającego.
7. konfigurację kopii zapasowych maszyn wirtualnych Zamawiającego dla dwóch repozytoriów: serwera backupowego oraz serwera NAS.
8. instalację niezbędnych agentów dla środowiska bazodanowego Zamawiającego i konfigurację kopii zapasowych baz danych.

9. konfigurację automatycznej weryfikacji kopii bezpieczeństwa maszyn wirtualnych Zamawiającego.
10. konfigurację powiadomień i codziennych raportów.

Wykonawca opracuje i przedstawi Zamawiającemu dokumentację powykonawczą zawierającą:

1. podstawowe procedury obsługowe.
2. opis skonfigurowanych polityk i harmonogramów.
3. opis odtworzenia maszyn wirtualnych.
4. opis odtworzenia pojedynczego pliku.
5. opis odtworzenia bazy danych Zamawiającego.
6. opis sposobu aktualizacji systemu.

Wykonawca przeprowadzi jednodniowy instruktaż stacjonarny w siedzibie Zamawiającego w czasie do 21 dni kalendarzowych od daty zakończenia wdrożenia dla 3 pracowników Zamawiającego, który obejmie co najmniej:

1. podstawową wiedzę dotyczącą systemu.
2. dodawania i usuwanie z systemu maszyn wirtualnych.
3. dodawanie i usuwanie z systemu fizycznych urządzeń.
4. zagadnienia dotyczące zmian platform wirtualizacji.
5. możliwości dodawania, zmiany i usuwania kolejnych miejsc przechowywania kopii zapasowych.
6. procedurę aktualizacji systemu.
7. procedurę odtworzenia konfiguracji po awarii dysków głównego serwera backupu, np. po ponownej instalacji hypervizora, systemu operacyjnego serwera.

3. Powierzchnia dyskowa w chmurze

Wykonawca dostarczy licencję umożliwiającą korzystanie z przestrzeni chmurowej w wymiarze 25 TB na okres do 30.06.2026r. Wymagana powierzchnia będzie dostępna przez cały okres trwania licencji w pełnej wymaganej wielkości. Zamawiający nie dopuszcza dostarczenia licencji na sumaryczną powierzchnię 25TB rozłożoną na oferowany okres. Dostarczone rozwiązanie musi być zgodne z oferowanym oprogramowaniem do tworzenia kopii zapasowych, musi umożliwiać tworzenie kopii zapasowych do oferowanej chmury oraz odzyskiwanie danych po awarii z chmury bez ponoszenia dodatkowych opłat przez Zamawiającego. Opłata za licencję będzie jednorazowa, ryczałtowa bez jakichkolwiek dopłat. Zamawiający nie dopuszcza opcji płatności w ratach miesięcznych. Licencja zostanie dostarczona na okres 36 miesięcy. Minimalne parametry dla wymaganej powierzchni dyskowej w chmurze:

- dostępna pojemność min. 25TB,
- gwarantowany dodatkowy bufor min. 10TB na czas przesyłania nowej kopii,
- gwarantowane łącze internetowe do min. 500 Mbit/s,

- lokalizacja na terenie Polski.

Opcjonalne, dodatkowe wsparcie techniczne inżyniera (parametr punktowany dodatkowo):

Wsparcie techniczne inżyniera realizowane zdalnie, świadczone w języku polskim. W ramach realizacji usługi zostanie wyznaczony dedykowany inżynier legitymujący się certyfikatem z zakresu administracji, konfiguracji systemu kopii zapasowych. Wsparcie powdrożeniowe musi być świadczone 7 dni w tygodniu w godzinach 8:00 – 17:00 – kontakt z inżynierem poprzez dedykowaną tylko dla Zamawiającego infolinię – dostęp po podaniu hasła lub PIN-u.

4. Nośniki wymienne RDX – 3 sztuki

Zamawiający posiada napęd RDX, który zostanie wykorzystany do tworzenia kopii odmiejscowionej. Wykonawca dostarczy min. 3 nośniki o pojemności min. 4TB każdy.

5. Dedykowana sieć backupowa o przepustowości min. 10 Gbit

Należy utworzyć dedykowaną sieć ethernet, do której zostaną podłączone wszystkie serwery produkcyjne (źródła kopii zapasowych) oraz wszystkie zasoby backupowe (serwera backupowy, macierze NAS). Sieć należy zbudować na min. 2 przełącznikach, zapewniających ciągłość działania w przypadku awarii jednego z nich. Wszystkie urządzenia zostaną podłączone niezależnym połączeniem do każdego z przełączników. Przełączniki muszą spełniać poniższe wymagania minimalne:

Element konfiguracji	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 250mm, możliwość montażu w szafie rack
Techniczne	Minimum 1 port ethernet 10/000BaseT Minimum 24 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Minimum 2 porty SFP28, pozwalające na instalację wkładek 25Gbit. Minimum 1 port konsoli: RJ45
Wydajność	Pojemność matrycy przełączania: minimum 216 Gbps Wydajność: minimum 108 Gbps Tablica adresów MAC o wielkości minimum 32k pozycji
Procesor	Min. 1 procesor 650Mhz
Pamięć RAM	Min. 64 MB
Pamięć wbudowana	Min. 16 MB
Stackowanie / MLAG	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) lub możliwość wykonania MLAG (Multichassis Link Aggregation)
Funkcje minimalne	Obsługa ramek Jumbo minimum 9k

	<p>Routing IPv4 – minimum: statyczny, RIP, OSPF, BFD, VRF, VRRP</p> <p>Routing IPv6 – minimum: statyczny, RIPng, OSPF</p> <p>Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping</p> <p>Obsługa vxlan</p> <p>Obsługa Port isolation</p> <p>Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol</p> <p>Obsługa funkcji Loop Protect</p> <p>Obsługa funkcji Traffic Shaping</p> <p>Obsługa 4094 tagów IEEE 802.1Q oraz minimum 1000 jednoczesnych sieci VLAN z BPDU protection</p> <p>Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie lub MLAG</p> <p>Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping ze wsparciem opcji 82</p> <p>Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI</p> <p>Obsługa standardu 802.1p</p> <p>Funkcja mirroringu portów</p> <p>Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) lub CDP Cisco Discovery Protocol</p> <p>Funkcja autoryzacji użytkowników zgodna z 802.1x</p> <p>Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo RADIUS Accounting</p>
Zarządzanie	<p>Zarządzanie poprzez port konsoli (pełne),</p> <p>Musi wspierać możliwość zarządzania przez następujące protokoły:</p> <ul style="list-style-type: none"> • SNMP v.1, 2c i 3, • Telnet, SSH v.2, • http, • https, • Syslog, • NTP. <p>Musi być możliwość przechowywania co najmniej trzech plików</p>

	konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
Zasilanie	Urządzenie musi być wyposażone w dwa redundantne, dedykowane zasilacze Możliwość zasilania PoE
Wyposażenie	Wraz z przełącznikiem należy dostarczyć niezbędne wkładki SFP+ z przewodami do redundantnego podłączenia wszystkich wskazanych przez Zamawiającego urządzeń do tworzonej sieci backupowej lub przewody typu DAC. Zestaw do montażu w szafie rack
Gwarancja	Min. 24 miesiące gwarancji w miejscu instalacji

6. Opracowanie polityki tworzenia kopii zapasowej (Backup 3-2-1):

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

- Pierwsza kopia będzie przechowywana lokalnie na wewnętrznych dyskach twardych serwera backupowego,
- Druga kopia będzie przechowywana na serwerze NAS,
- Trzecia kopia danych będzie przechowywana na nośnikach wymiennych,
- Czwarta kopia będzie przechowywana w Chmurze na terenie Polski.

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 trzy kopie danych. Wyniesienie nośników wymiennych poza budynek Urzędu Gminy umożliwi 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 musi być również zgodne z rekomendacją dotyczącą wykonywania kopii zapasowych opublikowaną przez Ministerstwo, która dostępna jest pod adresem:

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

Wymagany zakres prac do wykonania w ramach zadania Backup 3-2-1:

1. Dostawa serwera backupowego-zapasowego przeznaczonego do przechowywania kopii zapasowych (serwer backupowy); macierzy NAS, niezbędnych licencji oprogramowania do tworzenia kopii zapasowych z wsparciem technicznym oraz dostępem do aktualizacji oraz powierzchni w chmurze.
2. Montaż serwerów, konfiguracja serwerów do pracy w infrastrukturze Zamawiającego, uruchomienie; aktualizacja firmware serwerów; instalacja hypervizora na serwerze backupowym na potrzeby dostarczonego oprogramowania; konfiguracja maszyny wirtualnej dla systemu backupu; instalacja serwera/konsoli zarządzającej kopiami zapasowymi.
3. Opracowanie polityki backupu 3-2-1 w oparciu o:
 - dostarczony sprzęt i oprogramowanie,
 - sprzęt Zamawiającego,
 - przeprowadzoną analizę środowiska Zamawiającego (liczba maszyn wirtualnych, krytyczność systemu, wielkość maszyny wirtualnych czy ilość danych na serwerach fizycznych).

Na podstawie zebranych danych oraz wymagań Zamawiającego, Wykonawca opracuje Harmonogram tworzenia kopii zapasowych z podziałem na maszyny fizyczne/wirtualne; określeniem: częstotliwości tworzenia kopii pełnych, częstotliwości tworzenia kopii przyrostowych, częstotliwości tworzenia kopii na nośnikach wymiennych, częstotliwości weryfikacji poprawności tworzonych kopii zapasowych, częstotliwości i zakresu przeprowadzania testów odtworzeniowych. Na podstawie Harmonogramu Wykonawca skonfiguruje zadania backupowe na dostarczonym oprogramowaniu. Uruchomi tworzenie kopii zapasowych na serwerze backupowym, macierzy NAS, nośnikach wymiennych. Wykonawca skonfiguruje dodatkowo tworzenie kopii zapasowych na wskazanych przez Zamawiającego zasobach chmurowych.

4. Począwszy od dnia uruchomienia tworzenia kopii zapasowych, Wykonawca będzie zobowiązany do monitorowania pracy systemu backupowego przez min. 7 dni. Nadzór będzie miał na celu potwierdzenie prawidłowości wykonywanych kopii na serwerze oraz nośnikach wymiennych; potwierdzenie tworzenia kopii zgodnie z Harmonogramem.
5. Po zakończeniu pełnego cyklu tygodniowego tworzenia kopii zapasowych zgodnie z Harmonogramem, Wykonawca odtworzy wszystkie serwery fizyczne/maszyny wirtualne z kopii zapasowych na serwerze backupowym. Testy odtworzeniowe będą przeprowadzone przy udziale administratora Zamawiającego.
6. Po okresie monitorowania, na podstawie potwierdzenia przez Zamawiającego zgodności wykonywanych kopii zgodnie z Harmonogramem oraz na podstawie zakończonych sukcesem testów

odtworzeniowych, Wykonawca przeprowadzi instruktaż z zakresu:

- bieżącej obsługi systemu, podstaw administracji,
- modyfikacji Harmonogramu i zadań backupowych,
- czynności sprawdzania prawidłowości wykonywanych kopii zapasowych na serwerze oraz nośnikach wymiennych,
- procedury i czynności przeprowadzania testów odtworzeniowych.

7. Wykonawca wykona instruktaż z uruchomienia maszyn wirtualnych z repliki tworzonej krzyżowo na obecnie eksploatowanym serwerze oraz nowym serwerze zapasowym na okoliczność awarii jednego z serwerów.
8. Ostatnim etapem wdrażania systemu backupu 3-2-1 jest opracowanie dokumentacji powykonawczej, która będzie zawierać opis wszystkich wykonanych prac, niezbędne dane konfiguracyjne, opis polityki backupowej wraz z harmonogramem oraz instrukcjami umożliwiającymi samodzielne użytkowanie, administrowanie wdrożonym środowiskiem przez Zamawiającego.

W ramach rozbudowy systemu backupowego konieczne jest zbudowanie szybkiej sieci LAN dedykowanej do połączenia systemów kluczowych oraz urządzeń backupowych.

7. Opcjonalne oprogramowanie do monitorowania infrastruktury informatycznej (backupowej) **(funkcjonalności punktowane dodatkowo)**

W ramach realizacji zadania Wykonawca dostarczy, zainstaluje, skonfiguruje do pracy w środowisku informatycznym Zamawiającego oprogramowanie, podłączy wszystkie wymagane systemy krytyczne Zamawiającego. System musi spełniać poniższe wymagania minimalne:

Użytkownicy	
1	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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.
- 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.

	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	
6	<p>Możliwość monitorowania bazy danych systemu w zakresie co najmniej:</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> ▪ System monitoruje urządzenia klasy UTM minimum w zakresie: <ul style="list-style-type: none"> – 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	<p>W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:</p> <ul style="list-style-type: none"> – Serwer fizyczny – do 8 sztuk – maszyna wirtualna Windows / Linux / hosty – do 30 sztuk – serwer AD - 2 sztuki – Macierze / NASy – do 6 sztuk – Przełącznik rdzeniowy – 2 sztuki – Przełącznik dostępowy (LAN) – do 8 sztuk – Zasilacz awaryjny (UPS) - 2 sztuki – Serwer bazodanowy - 1 sztuka – Serwer Backupu - 1 sztuka

II.14 Zakup UPS dla stacji końcowych – 20 sztuk.

W celu zapewnienia ciągłości działania, ciągłości pracy systemów oraz dostępności do nich, zostaną zakupione UPS dla stacji końcowych oraz do serwerowni (dla sprzętu serwerowego i sieciowego). Parametry minimalne dla zasilaczy awaryjnych (UPS), przeznaczonych dla stacji roboczych:

Zasilacz awaryjny	
Parametr	Wymagane minimalne parametry techniczne
Typ	Zasilacz awaryjny z automatyczną regulacją napięcia
Obudowa	Tower
Moc pozorna	Min. 1600 VA
Moc czynna	Min. 900 Watt
Podtrzymanie zasilania	Min. 21 minut przy obciążeniu 180W Min. 7 minut przy obciążeniu 360W
Technologia zasilacza	Liniowa interaktywna
Napięcie wejściowe	Min. 220/230/240 V
Złącza wyjściowe zasilania	Min. 4 gniazda zasilania urządzeń typu E (podtrzymanie i zabezpieczenie przepięciowe)
Liczba akumulatorów	Min.2
Technologia wykonania	Min. Kwasowo-ołowiowy
Interfejs do zdalnego zarządzania	Min. 1 x USB
Dołączone przewody	Kabel USB min. 1,8 m
Cechy dodatkowe	- ochrona przed głębokim rozładowaniem - funkcja zimny start

	- automatyczny test baterii
Zgodność z normami	Min. LVD; EMC; RoHS; WEEE
Certyfikaty	Min. EN/IEC: 62040-1; 62040-2; 62040-3; CE; EAC
Dołączone oprogramowanie o funkcjach umożliwiających co najmniej	bezpieczne zamknięcie systemu, pomiar zużycia energii, konfigurację ustawień zasilacza UPS, konfigurację parametrów wyłączania
Szerokość	Max. 14 cm
Głębokość (długość)	Max. 35 cm
Wysokość	Max. 19 cm
Waga	Max. 9,4 kg
Gwarancja	Min. 24 miesiące gwarancji producenta na urządzenie oraz baterie w miejscu instalacji

II.15 Zakup UPS do serwerowni – 2 szt.

Zakup, wdrożenie, uruchomienie zasilaczy awaryjnych do serwerowni.

Parametry minimalne dla zasilaczy awaryjnych (UPS), przeznaczonych do montażu w serwerowni, do utrzymania pracy serwerów, przełączników, macierzy NAS:

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych
1	Moc pozorna	5000 VA
2	Moc rzeczywista	4500 W

3	Topologia	On-line z podwójną konwersją
4	Współczynnik mocy	0,9
5	Liczba, typ gniazd wyjściowych	Min. 8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza), 2 x IEC C19 16A
6	Czas podtrzymania przy 1 600W obciążenia	Min. 75 min
7	Czas podtrzymania dla 2 200W obciążenia	Min. 47 min
8	Czas podtrzymania przy 3 300W obciążenia z dodatkowym modulem baterijnym	Min. 26 min
9	Napięcie znamionowe	200/208/220/230/240V
10	Częstotliwość znamionowa	50/60 Hz
11	Tolerancja częstotliwości	40– 70 Hz
12	Kształt napięcia	Sinusoidalny
13	Napięcie znamionowe wyjściowe	Min. 200/208/220/230/240V
14	Częstotliwość wyjściowa	50/60 Hz
15	Baterie wymieniane przez użytkownika "na gorąco"	Tak
16	Ochrona przed głębokim rozładowaniem	Tak
17	Automatyczny test baterii	Tak
18	Dodatkowe baterie	Możliwość podłączenia do 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania
19	Interfejsy komunikacyjne	• USB

		• RS232 DB-9 żeński (HID)
		• styki przekaźnikowe
		• mini port wyłącznik ON/OFF
		• SNMP/Ethernet
20	Panel sterowania z wyświetlaczem LCD	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS) dostarczający informacji o: stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
		Poziomy rząd przycisków sterowania
		Poziomy rząd wskaźników stanu: zasilanie z sieć(zielony), trybu bateryjnego (żółty), usterki (czerwony)
		Sygnalizator akustyczny
21	Sygnały akustyczne	• Awaria, brak baterii
		• Niski stan naładowania baterii
		• Przeciążenie
		• Serwis
22	Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
		• Przyciski funkcyjne (przewijanie w górę i w dół)
		• Przycisk Enter (potwierdzający)
		• Przycisk ON/OFF załączenia i wyłączenia
		• LED trybu zasilania z sieć i(kolor zielony)

		<ul style="list-style-type: none"> • LED trybu baterii (kolor pomarańczowy)
		<ul style="list-style-type: none"> • LED usterki (kolor czerwony)
23	Dane techniczne karty SNMP	<p>Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP</p> <p>Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.</p> <p>Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI</p> <p>Kompatybilność: SNMP v1/v3 i IP v4/v6</p> <p>Interfejs: HTML5</p> <p>Adresowanie IP: DHCP/BootP/Manualne</p> <p>Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256</p> <p>Dostępny port USB (microUSB - port serwisowy)</p>
24	Dołączone oprogramowanie	<p>Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych:</p> <ul style="list-style-type: none"> - Windows: 7 / 8 / 10 /11 - Microsoft Windows Server - Linux: Debian, SUSE, OpenSUSE, Redhat, Ubuntu - VMWare: vCenter / ESXi - Citrix XEN
25	Standard energetyczny	Min. Energy Star
26	Maksymalna wysokość całkowita zestawu w szafie rack	6U

27	Bypass	Wewnętrzny
28	Maksymalna głębokość	69 cm
29	Poziom hałasu z odległości 1m dla pracy normalnej	Max. 42 dBA z odległości 1 metra
30	Certyfikaty	Min. CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2, UL 1778, EAC
31	Gwarancja producenta	Min. 24 miesiące dla elektroniki oraz baterii.

Instalacja, konfiguracja:

Zamawiający wymaga: montażu dostarczanych zasilaczy w wskazanych szafach rack, podłączenia, uruchomienia, konfiguracji karty SNMP oraz parametrów pracy zasilaczy wg zaleceń Zamawiającego.

II.16 Usługa wykonania segmentacji sieci

Zamawiający wymaga, aby w ramach wykonania przedmiotu zamówienia, Wykonawca wykonał niezbędną konfigurację oraz segmentację sieci LAN zgodnie z zaleceniami Zamawiającego oraz wymaganiami z pkt. II.2 niniejszego dokumentu. Celem modernizacji jest poprawa bezpieczeństwa sieci LAN.

Usługa będąca przedmiotem zamówienia obejmuje w szczególności:

- Stworzenie koncepcji podziału sieci na co najmniej X podsieci z wykorzystaniem istniejącej infrastruktury sieciowej.
- Uruchomienie usługi i konfiguracja przełączników w celu filtracji MAC użytkowników (przypisanie adresu MAC urządzeń do konkretnych portów przełącznika), lub uruchomienie serwera DHCP w celu filtracji adresów MAC użytkowników sieci LAN.
- Opracowanie instrukcji / procedury konfiguracji stacji roboczych zgodnie z opracowaną koncepcją (Zamawiający na jej podstawie samodzielnie wykona konfigurację stacji roboczych zgodnie z opracowaną koncepcją).

Zamawiający zaleca, aby Wykonawca przed złożeniem oferty dokonał wizji lokalnej Infrastruktury sieciowej urzędu Zamawiającego. Zamawiający zakłada, że usługi będące przedmiotem zamówienia nie będą obejmować budowy nowych połączeń sieciowych, tras kablowych itp. Wykonawca musi oszacować wszelkie

koszty konieczne do osiągnięcia celu zamówienia. Wszelkie proponowane przez Wykonawcę rozwiązania muszą zostać uprzednio skonsultowane z Zamawiającym i uzyskać jego akceptację.

Po wykonaniu usługi, Wykonawca sporządzi dokumentację powykonawczą zawierającą opis przeprowadzonych prac, schemat wykonanych połączeń oraz konfiguracje wprowadzone do urządzeń sieciowych. Przedłożenie niniejszej dokumentacji Zamawiającego będzie wymagane przed podpisaniem protokołu odbioru wykonanego zadania.

II.17 Usługa przeprowadzenia testów penetracyjnych

Wykonanie testów penetracyjnych w środowisku Zamawiającego.

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia. Warunek potencjał techniczny jest spełniony, gdy posiada narzędzia takie jak automatyczny skaner podatności posiadający funkcje pozwalające na:

- wykonanie skanowań z wykorzystaniem wbudowanych szablonów,
- skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi),
- weryfikację domyślnych haseł według zadanego słownika,
- skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika,
- możliwość porównania wyników poszczególnych skanowań,
- możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (np. HTML, CVS i XML),
- możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową nawet gdy używany jest HTTPS,
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta,
- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia,
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w celu ułatwienia testowania,

- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy,
- precyzyjna konfiguracja reguł przechwytywania wiadomości,
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS,
- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL,
- żądania i odpowiedzi dostępne w edytorze http,
- narzędzie do ręcznej edycji i ponownego wstawiania żądań,
- narzędzie do analizy statystycznej tokenów sesji,
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca,
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami,
- możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach,
- skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań,
- możliwość analizy docelowej aplikacji internetowych,
- narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Warunek potencjał osobowy jest spełniony, gdy Wykonawca posiada inżynierów z kompetencjami umożliwiającymi wykonanie testów penetracyjnych zgodnie z wymaganiami Zamawiającego, przy użyciu narzędzia wymaganego przez Zamawiającego.

W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.

- a) Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł,
- b) Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi),
- c) zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych,
- d) Sprawdzenie występowania wyciekach znalezionych loginów.

2. Enumeracja zasobów.

- a) Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
 - b) Skanowanie publicznej infrastruktury.
 - c) Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
 - d) Sprawdzenie udostępnionych w sieci wewnętrznej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
 - e) Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
3. Eksploatacja.
- a) Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
 - b) Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
 - c) Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
4. Eskalacja uprawnień.
- a) Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
 - b) Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).
5. Raport z testu penetracyjnego. Wykonawca dostarczy raport zawierający:
- a) Podsumowanie dla kierownictwa.
 - b) Opis zakresu wykonanych prac.
 - c) Wyłączenia z testów jeżeli były.
 - d) Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
 - e) Listę znalezionych podatności wraz z określoną dla niej wagą zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
 - f) Szczegółowy opis znalezionych podatności.
 - g) Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

II.18 Szkolenie dla pracowników IT z zakresu zabezpieczania środowiska domenowego

1. Szkolenie specjalistyczne z administracji systemu operacyjnego Microsoft Windows Server – 3 vouchery

Zamawiający wymaga dostarczenia voucherów na szkolenie z zakresu administracji systemem Windows Server w wersji 2019 i nowszej. Vouchery muszą być ważne przez okres min. 6 miesięcy. Szkolenie musi być prowadzone przez profesjonalnego instruktora w formie zdalnej lub stacjonarnej, w dni robocze. Czas trwania pięć dni. Celem szkolenia jest zdobycie wiedzy z zakresu: zarządzania tożsamością, siecią, pamięcią masową i obliczeniami przy użyciu systemu Windows Server oraz wiedzy na temat: scenariuszy, wymagań oraz opcji dostępnych w systemie Windows Server. Minimalny, przykładowy zakres szkolenia przedstawiono poniżej:

Moduł 1: Wprowadzenie do administracji systemu Windows Server

- a. Wprowadzenie do systemu Windows Server
- b. Wprowadzenie do systemu Windows Server Core
- c. Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server
- d. **Ćwiczenie:** Wdrażanie i konfiguracja systemu Windows Server
 - Wdrażanie i konfiguracja systemu Server Core
 - Wdrażanie i stosowanie zdalnej administracji serwerami

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać system Windows Server, a także techniki wdrażania, serwisowania i aktywacji,
- Opisać system Windows Server Core, przedstawić jego specyfikę i sposoby administrowania nim.

Moduł 2: Usługi zarządzania tożsamością w systemie Windows Server

- a. Wprowadzenie do AD DS
- b. Wdrażanie kontrolerów domeny Windows Server
- c. Wprowadzenie do usługi Azure AD
- d. Wdrażanie zasad grupy
- e. Wprowadzenie do usług certyfikatów Active Directory
- f. **Ćwiczenie:** Wdrażanie usług zarządzania tożsamością i zasad grupy
 - Wdrażanie nowego kontrolera domeny w systemie Server Core
 - Konfigurowanie zasad grupy
 - Wdrażanie i korzystanie z usług certyfikatów
 - Wyjaśnienie podstaw zasad grupy i konfiguracja GPO w środowisku domenowym
 - Opis roli usług certyfikatów Active Directory i korzystanie z certyfikatów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać AD DS w środowisku systemu Windows Server,
- Wdrażać kontrolery domeny w AD DS,
- Opisać Azure AD i korzyści płynące z integracji Azure AD z AD DS.

Moduł 3: Usługi infrastruktury sieciowej w systemie Windows Server

- Wdrażanie i zarządzanie protokołem DHCP
- Wdrażanie i zarządzanie systemem DNS
- Wdrażanie i zarządzanie systemem IPAM
- Usługi dostępu zdalnego w systemie Windows Server
- Ćwiczenie:** Wdrażanie i konfiguracja usług infrastruktury sieciowej w systemie Windows Server
 - Wdrażanie i konfiguracja protokołu DHCP
 - Wdrażanie i konfiguracja systemu DNS
 - Wdrażanie serwera proxy aplikacji sieci WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać, wdrożyć i skonfigurować usługę DHCP,
- Wdrażać, konfigurować i zarządzać systemem DNS,
- Opisać, wdrożyć i zarządzać systemem IPAM.

Moduł 4: Serwery plików i zarządzanie pamięcią masową w systemie Windows Server

- Woluminy i systemy plików w systemie Windows Server
- Wdrażanie udostępniania w systemie Windows Server
- Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server
- Wdrażanie deduplikacji danych
- Wdrażanie interfejsu iSCSI
- Wdrażanie rozproszonego systemu plików
- Ćwiczenie:** Wdrażanie rozwiązań pamięci masowej w systemie Windows Server
 - Wdrażanie deduplikacji danych
 - Konfiguracja magazynu iSCSI
 - Konfiguracja nadmiarowych przestrzeni dyskowych
 - Wdrażanie Storage Spaces Direct

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Wdrażać udostępnianie w systemie Windows Server,
- Wdrożyć technologię Storage Spaces,
- Wdrażać funkcję deduplikacji danych,
- Wdrażać pamięć masową opartą na iSCSI,
- Wdrożyć i zarządzać rozproszonym systemem plików (DFS - Distributed File System).

Moduł 5: Wirtualizacja Hyper-V i kontenery w systemie Windows Server

- a. Hyper-V w systemie Windows Server
- b. Konfiguracja maszyn wirtualnych
- c. Zabezpieczanie wirtualizacji w systemie Windows Server
- d. Kontenery w systemie Windows Server
- e. Wprowadzenie do platformy Kubernetes
- f. **Ćwiczenie:** Wdrażanie i konfiguracja wirtualizacji w systemie Windows Server
 - Tworzenie i konfigurowanie maszyn wirtualnych
 - Instalacja i konfiguracja kontenerów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać kluczowe cechy Hyper-V w systemie Windows Server,
- Opisać ustawienia maszyn wirtualnych oraz wdrożyć i skonfigurować maszyny wirtualne w Hyper-V,
- Wyjaśnić zastosowanie technologii bezpieczeństwa w wirtualizacji,
- Opisać i wdrożyć kontenery w systemie Windows Server,
- Wyjaśnić zastosowanie platformy Kubernetes w systemie Windows.

Moduł 6: Wysoka dostępność w systemie Windows Server

- a. Planowanie wdrożenia klastra pracy awaryjnej
- b. Tworzenie i konfiguracja klastra pracy awaryjnej
- c. Wprowadzenie do rozciągniętych klastrów
- d. Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V
- e. **Ćwiczenie:** Wdrażanie klastra pracy awaryjnej
 - Konfiguracja pamięci masowej i tworzenie klastra
 - Wdrażanie i konfiguracja serwera plików o wysokiej dostępności
 - Sprawdzanie poprawności wdrożenia serwera plików o wysokiej dostępności

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać klastr pracy awaryjnej i warunki jego wdrożenia,
- Tworzyć i konfigurować klastry pracy awaryjnej,
- Opisać klastry rozciągnięte,
- Opisać opcje osiągnięcia wysokiej dostępności za pomocą maszyn wirtualnych Hyper-V.

Moduł 7: Odzyskiwanie danych po awarii w systemie Windows Server

- a. Funkcja Hyper-V Replica
- b. Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server

c. **Ćwiczenie:** Wdrażanie funkcji Hyper-V Replica i Windows Server Backup

- Wdrażanie funkcji Hyper-V Replica
- Wdrażanie tworzenia kopii zapasowych i przywracania za pomocą narzędzia Windows Server Backup

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać i wdrożyć funkcję Hyper-V Replica,
- Opisać usługę Azure Site Recovery,
- Opisać i wdrożyć narzędzie Windows Server Backup,
- Opisać usługę Azure Backup.

Moduł 8: Bezpieczeństwo systemu Windows Server

- a. Ochrona danych uwierzytelniających i dostępu uprzywilejowanego
- b. Hardening systemu Windows Server
- c. JEA w systemie Windows Server
- d. Zabezpieczanie i analiza ruchu w SMB
- e. Zarządzanie aktualizacjami w systemie Windows Server
- f. **Ćwiczenie:** Konfiguracja zabezpieczeń w systemie Windows Server
 - Konfiguracja funkcji Windows Defender Credential Guard
 - Lokalizowanie problematycznych kont
 - Wdrażanie rozwiązania LAPS

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać dane uwierzytelniające wykorzystywane w systemie Windows Server,
- Wyjaśnić, jak wdrożyć zabezpieczenia dostępu uprzywilejowanego,
- Opisać metody i technologie hardeningu zabezpieczeń w systemie Windows Server,
- Opisać i skonfigurować usługę Just Enough Administration (JEA),
- Zabezpieczyć ruch SMB w systemie Windows Server,
- Opisać usługę Windows Update oraz jej opcje wdrażania i zarządzania.

Moduł 9: RDS (usługi pulpitu zdalnego) w systemie Windows Server

- a. Wprowadzenie do RDS
- b. Konfiguracja wdrażania pulpitu opartego na sesji
- c. Wprowadzenie do osobistych i połączonych pulpituów wirtualnych
- d. **Ćwiczenie:** Wdrażanie RDS w systemie Windows Server
 - Wdrażanie RDS
 - Konfigurowanie ustawień kolekcji sesji i wykorzystywanie RDC
 - Konfiguracja szablonu pulpitu wirtualnego

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać usługi Remote Desktop Services (RDS - usługi pulpitu zdalnego) w systemie Windows Server,
- Opisać i wdrożyć pulpity oparte na sesji,
- Opisać osobiste i połączone pulpity wirtualne.

Moduł 10: Dostęp zdalny i usługi internetowe w systemie Windows Server

- a. Wdrażanie sieci VPN
- b. Wdrażanie usługi Always On VPN
- c. Wdrażanie systemu NPS
- d. Wdrażanie serwera WWW w systemie Windows Server
- e. **Ćwiczenie:** Wdrażanie obciążeń sieciowych
 - Wdrażanie sieci VPN w systemie Windows Server
 - Wdrażanie i konfiguracja serwera WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać opcje sieci VPN w systemie Windows Server,
- Opisać funkcję Always On VPN,
- Opisać i skonfigurować NPS,
- Opisać i skonfigurować serwer WWW (IIS).

Moduł 11: Monitorowanie serwera i wydajności w systemie Windows Server

- a. Wprowadzenie do narzędzi do monitorowania systemu Windows Server
- b. Korzystanie z monitora wydajności
- c. Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów
- d. **Ćwiczenie:** Monitorowanie i rozwiązywanie problemów z systemem Windows Server
 - Ustanowienie bazowego poziomu wydajności
 - Identyfikacja źródła problemu z wydajnością

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia monitorujące w systemie Windows Server,
- Opisać monitorowanie wydajności i wykorzystać je w systemie Windows Server,
- Opisać rejestrowanie zdarzeń i monitorować rejestrowanie zdarzeń dla celów rozwiązywania problemów.

Moduł 12: Aktualizacja i migracja w systemie Windows Server

- a. Migracja AD DS
- b. Usługa migracji pamięci masowej
- c. Narzędzia do migracji systemu Windows Server

d. **Ćwiczenie:** Migracja obciążeń serwera

- Wdrażanie usługi migracji pamięci masowej

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia, których należy użyć do migracji AD DS,
- Opisać usługę migracji pamięci masowej,
- Opisać narzędzia do migracji Windows Server i scenariusze ich użycia.

II.19 Szkolenie dla pracowników IT z zakresu cyberbezpieczeństwa

Szkolenie specjalistyczne z zakresu administrowania oraz konfigurowania urządzeń UTM – 3 vouchery

Zamawiający wymaga dostarczenia voucherów na szkolenie z zakresu administracji urządzeń UTM. Vouchery muszą być ważne przez okres min. 6 miesięcy. Szkolenie musi być prowadzone przez profesjonalnego inżyniera w formie zdalnej, w dni robocze. Czas trwania 3 dni. Celem szkolenia jest zdobycie wiedzy z zakresu: zasad działania zapory sieciowej, uwierzytelniania użytkowników, klastra wysokiej dostępności, SSL VPN, site-to-site IPsec VPN oraz sposobów ochrony sieci za pomocą profili bezpieczeństwa, takich jak IPS, antywirus, filtrowanie sieci, kontrola aplikacji. Minimalny, przykładowy zakres szkolenia przedstawiono poniżej:

1. Podstawowa konfiguracja urządzenia UTM
2. Konfiguracja, kontrola dostępu administratora do UTM
3. Używanie interfejsu GUI i CLI do administracji
4. Kontrola dostępu do skonfigurowanych sieci za pomocą polityk firewall
5. Stosowanie przekierowania portów, źródłowego NAT i docelowego NAT
6. Analizowanie tabeli tras urządzenia UTM
7. Trasowanie pakietów przy użyciu tras statycznych, opartych na zasadach dla wdrożeń wieloscieżkowych i z równoważeniem obciążenia
8. Uwierzytelnianie użytkowników przy użyciu polityk zapory
9. Monitorowanie użytkowników zapory sieciowej z poziomu graficznego interfejsu użytkownika UTM
10. Oferowanie dostępu Single Sign-On (SSO) do usług sieciowych, zintegrowanego z Microsoft Active Directory (AD)
11. Wyjaśnienie funkcji szyfrowania i certyfikatów
12. Sprawdzanie ruchu zabezpieczonego protokołem SSL/TLS w celu zapobiegania szyfrowaniu wykorzystywanemu do omijania zasad bezpieczeństwa
13. Konfigurowanie profili bezpieczeństwa w celu neutralizacji zagrożeń i nadużyć, w tym wirusów, torrentów i nieodpowiednich stron internetowych.
14. Stosować techniki kontroli aplikacji do monitorowania i kontrolowania aplikacji sieciowych, które

mogą korzystać ze standardowych lub niestandardowych protokołów i portów.

15. Oferowanie SSL VPN dla bezpiecznego dostępu do sieci prywatnej
16. Ustanowienie tunelu IPsec VPN między dwoma urządzeniami UTM
17. Konfiguracja routingu statycznego
18. Konfiguracja sieci SD-WAN typu underlay, overlay i local breakout
19. Wdrażanie urządzeń UTM jako klastra HA w celu zapewnienia odporności na awarie i wysokiej wydajności
20. Diagnozowanie i rozwiązywanie typowych problemów

II.20 Instruktarze stanowiskowe

1. Z uwagi na to, iż w ramach projektu planuje się wdrożenie specjalistycznego oprogramowania i aplikacji, konieczne jest przeszkolenie personelu Zamawiającego. W związku z tym w ramach tego zadania zostaną zrealizowane instruktaże stanowiskowe.
2. Wykonawca przeprowadzi instruktaże stanowiskowe w siedzibie Zamawiającego. Zamawiający udostępni pomieszczenie celem przeprowadzenia instruktaży stanowiskowych.
3. Na podstawie przekazanego przez Zamawiającego wykazu osób oraz przewidywanego terminu i czasu instruktażu stanowiskowego, Wykonawca zaproponuje harmonogram jak i ewentualny podział na grupy.
4. Szczegółowy harmonogram realizacji instruktaży zostanie uzgodniony na etapie Analizy Przedwdrożeniowej.
1. Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa użytkowników w instruktażach stanowiskowych.
2. Instruktaże stanowiskowe administratorów będą musiały spełniać minimum następujących wymagań:
 - zajęcia powinny odbywać się pomiędzy godzinami od godz. 8.00 do 15.00,
 - zajęcia nie będą mogły trwać dłużej niż 5 godzin dziennie,
5. Za skuteczne przeprowadzenie instruktażu stanowiskowego uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić instruktaż zgodnie z ustalonym harmonogramem.
6. Wykonawca w ramach instruktażu stanowiskowego przekaże instrukcje do wdrożonego Systemu oraz materiały szkoleniowe. Instruktaże stanowiskowe będą prowadzone w języku polskim.

7. Wykonawca zapewnia dodatkowo możliwość konsultacji (instruktaży) realizowanych on-line. Ilość godzin nie jest ograniczona, jednakże muszą one się odbywać w okresie wdrożenia i zakończyć do dnia podpisania protokołu odbioru końcowego.
8. W ramach przeprowadzonych instruktaży stanowiskowych wymaga się:
 - przekazania wiedzy niezbędnej do poprawnego użytkowania wdrożonego systemu, jego zakresu funkcjonalnego,
 - przekazania wiedzy w zakresie tworzenia i gromadzenia informacji, tworzenia i gromadzenia dokumentów, wykonywania analiz, sprawozdań i raportów.
9. Zakres instruktaży stanowiskowych musi objąć teorię i praktykę (musi być zapewniona odpowiednia liczba ćwiczeń – minimum w stosunku 50% / 50%) tak, aby personel Zamawiającego mógł podjąć samodzielnie działania użytkowania wdrożonych rozwiązań.
10. Szacowana liczba pracowników Zamawiającego planowanych do instruktaży stanowiskowych to 3 osoby.
11. Zamawiający dopuszcza przeprowadzenie instruktaży stanowiskowych on-line wyłącznie po wcześniejszym wyrażeniu zgody.
12. Instruktaże stanowiskowe on-line powinny być prowadzone w technologii transmisji audio-wideo w czasie rzeczywistym, tzn. technologią typu „Streaming” umożliwiającą przesyłanie takich danych jak fonii, wizja i tekst „na żywo” dzięki czemu uczestnik otrzymuje pełnowartościowe szkolenie:
 - a) fonii / głos – słyszy lektora prowadzącego szkolenie „na żywo”
 - b) wizja / wideo – widzi lektora prowadzącego szkolenie „na żywo”
 - c) pokaz slajdów, prezentacji, widoku ekranu – całą prezentację widzi u siebie na ekranie.

Instruktaże stanowiskowe on-line muszą umożliwiać pełną interakcję zarówno z prowadzącym jak i z innymi uczestnikami instruktażu, poprzez:

- a) dostęp do czatu z możliwością zadawania pytań oraz udzielania odpowiedzi,
- b) przeprowadzenia ankiet on-line.

Zakres instruktaży stanowiskowych on-line musi obejmować teorię, czyli prezentację oraz praktykę, tj. wykonywania ćwiczeń przez uczestników, zgodnie z pkt 9 niniejszego rozdziału.

Wykonawca jest odpowiedzialny za organizację instruktaży stanowiskowych on-line, w tym co najmniej: zapewnienie sprzętu, oprogramowania oraz transmisji do przeprowadzenia instruktaży, w miejscu wyznaczonym przez Zamawiającego.

Rozdział III. Gwarancja

III.1 Warunki gwarancji

Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na niniejszy przedmiot zamówienia:

1) Dostawa i wdrożenie Infrastruktury sprzętowej wraz z oprogramowaniem:

Poz. OPZ	Opis	Gwarancja
Rozdział	Rodzaj zamawianego asortymentu	
II.2	Zakup i wdrożenie klastra UTM*	36 miesięcy
II.3	Rozbudowa infrastruktury aktywnej – zakup przełączników	60 miesięcy
II.4	Rozbudowa rozwiązania do ochrony danych do rozwiązania klasy EDR XDR – rozszerzenie licencji	Do 30.06.2026
II.5	Usługa analizy konfiguracji w obecnie posiadanych rozwiązaniach	12 miesięcy
II.6	Zakup i wdrożenie rozwiązania klasy NAC	24 miesiące
II.7	Dostawa i kompleksowe wdrożenie systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM, SOAR	24 miesiące
II.8	Serwer tworzący platformę sprzętową dla SOC*,**	36 miesięcy
II.9	Rozbudowa infrastruktury o macierz dyskową*,**	36 miesięcy

II.10	Zakup niezbędnych licencji do funkcjonowania środowiska bazodanowego	12 miesięcy
II.11	Przedłużenie licencji i wsparcia na posiadane rozwiązanie do zarządzania infrastrukturą, stacjami roboczymi i serwerami	24 miesiące
II.12	Przedłużenie wsparcia na posiadane rozwiązanie do kopii zapasowych	12 miesięcy
II.13	Rozbudowa infrastruktury backupowej – zakup systemu pozwalającego na tworzenie kopii zapasowych wszystkich danych	24 miesiące
II.14	Zakup UPS dla stacji końcowych	24 miesiące
II.15	Zakup UPS do serwerowni	24 miesiące
II.16	Usługa wykonania segmentacji sieci	12 miesięcy
II.17	Usługa przeprowadzenia testów penetracyjnych	12 miesięcy

* W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

** W przypadku awarii dysków pozostają one własnością Zamawiającego.

1. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.

III.2 Wady Przedmiotu Zamówienia

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami jak poniżej:

- 1) **Awaria** - Kategoria Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiającego jego użytkowanie. Sytuacja, w której dane rozwiązanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia
 - 2) **Usterka** - Należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz OPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
2. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany SZ) przy czym:
- 1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
 - 2) za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady.
3. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
4. Z powodów organizacyjnych leżących po stronie Zamawiającego lub powodów technicznych, strony mogą uzgodnić dłuższy czas usuwania awarii.
5. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
- 1) Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

Tabela 1. Usługi gwarancji dla Infrastruktury sprzętowej i oprogramowania:

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE*	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
------------------------------	-----------------------------	------------------------	------------------------	--------------

AWARIA	24/7/365	niezwłocznie, nie później niż 36 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 14 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia

* nie dotyczy sprzętu zastępczego

- 2) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
- 3) czasy naprawy mogą być inne niż wskazane w powyższej tabeli, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),
- 4) w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,
- 5) Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy,

Uwaga:

W przypadku zapisu terminu jako:

- Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
- Godziny Robocze należy rozumieć godziny od 8.00 do 16.00 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.