

Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia

na wykonanie zadania pn. **„Dostawa sprzętu IT i oprogramowania w ramach projektu „Cyberbezpieczne Wodociągi” realizowanego przez Zakład Usług Komunalnych w Piekoszowie Sp. z o. o. w ramach inwestycji C3.1.1 Krajowego Programu Odbudowy i Zwiększania Odporności”**



**Rzeczpospolita
Polska**



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Spis treści

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.....	4
2. Wymagania gwarancyjne.	4
3. Miejsce instalacji sprzętu i oprogramowania/systemu.....	4
4. Zestawienie zakresu dostaw i usług.	5
5. Szczegółów opis pozycji.....	9
5.1. Oprogramowanie antywirusowe – 20 licencji.....	9
5.2. Serwer z oprogramowaniem – szt.1 – wymagania minimalne	19
5.3. Macierz dyskowa TYP A – szt. 1 – wymagania minimalne	22
5.4 Oprogramowanie do backupu – szt. 1 – wymagania minimalne	24
5.5 Macierz dyskowa TYP B – szt. 1 – wymagania minimalne.....	28
5.6 Biblioteka taśmowa LTO-9 – szt.1	30
5.7 Przetłacznik sieci LAN CORE – szt.1 - wymagania minimalne	31
5.8 Urządzenia Access Point Wifi – szt.2	33
5.9 Urządzenie UTM – TYP A – szt. 1.....	35
5.10 Urządzenie UTM – TYP B – szt.1	40
5.10.1 Urządzenia Access Point dla sieci OT – TYP A – 4 szt.	46
5.10.2 Urządzenia Access Point dla sieci OT – TYP B – 6 szt.....	47
5.11 Oprogramowanie do analizy logów.....	48
5.12 Oprogramowanie serwerowe	49
5.13 System monitorujący prace urządzeń sieciowych i serwerowych	49
5.14 Instalacja, konfiguracja, wdrożenie – szt.1 – wymagania minimalne	51
5.15 Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	60
5.16 Audyt Informatyczny SZBI, audyt zgodności KRI.uoKSC.....	62
5.17 Testy bezpieczeństwa infrastruktury sieciowej IT/OT.....	63
5.18 Szkolenia z zakresu cyberbezpieczeństwa dla pracowników i kadry Zarządzającej.....	66
5.19 Szkolenie pracowników z zakresu cyberbezpieczeństwa z uwzględnieniem wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Zakładzie	66
5.20 Szkolenia specjalistyczne dla administratorów IT	67

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

2. Wymagania gwarancyjne.

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

Oprogramowanie

- oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

3. Miejsce instalacji sprzętu i oprogramowania/systemu.

- Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w siedzibie głównej Zakładu oraz w innych budynkach Zakładu, w miejscach wskazanych przez Zamawiającego.

4. Zestawienie zakresu dostaw i usług.

Lp.	Nazwa	Wymagana minimalna długość gwarancji (m-ce)	Ilość	Jednostka miary	Uwagi
1.	Oprogramowanie antywirusowe	24	20	Szt.	Oprogramowanie antywirusowe dla stacji roboczych i serwerów
2.	Serwer z oprogramowaniem	36	1	Szt.	Pozycja dotyczy rozbudowy klastra niezawodnościowego HA, chmury prywatnej z dwóch fizycznych serwerów.
3.	Macierz dyskowa TYP A	36	1	Szt.	Pozycja dotyczy zakupu macierzy dyskowej w celu zapewnienia przestrzeni dyskowej dla klastra serwerów HA, który zostanie do niej podłączony.
4.	Oprogramowanie do backupu	24	1	Szt.	Pozycja dotyczy elementu systemu kopii zapasowych. Obecny system nie pozwala na łatwe odzyskanie środowiska produkcyjnego oraz na utrzymanie ciągłości pracy. Konieczne jest zatem stworzenie dedykowanego systemu kopii zapasowej pozwalającego na odtworzenie kompletnego systemu. Na maszynie wirtualnej zostanie zainstalowane oprogramowanie do backupu i archiwizacji danych. System zostanie podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych. Miejscem przechowywania danych backupu będą udziały stworzone na macierzy NAS znajdującej się w siedzibie Głównej, kopiowane będą do biblioteki taśmowej oraz będą kopiowane do macierzy zapasowej odmiejscowionej od siedziby głównej.
5.	Macierz dyskowa – TYP B dla backup`u	36	1	Szt.	Pozycja dotyczy zakupu macierzy dyskowej w celu zapewnienia przestrzeni dyskowej dla kopii zapasowych odmiejscowionych od siedziby głównej Zakładu.

6.	Biblioteka taśmowa LTO 9	36	1	Szt.	Pozycja dotyczy dostarczenia biblioteki taśmowej LTO Ultrium-9 SAS, która przechowywać będzie kopie zapasowe systemów, danych, maszyn wirtualnych
7.	Przełącznik sieci LAN CORE	24	1	Szt.	Urządzenie pozwoli na stworzenie rozległej sieci szkieletowej 10G. Będzie stanowił centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI–L2 (warstwa łącza danych) oraz zapewni wsparcie dla protokoły STP (protokół drzewa rozpinającego). Na przełączniku zostanie zrealizowany mechanizm sieci wirtualnych VLAN (separacji ruchu sieciowego na warstwie L2 modelu ISO/OSI)..
8.	Urządzenia Access Point – TYP A - Wifi	24	2	Szt.	Pozycja dostarczenia urządzeń sieci WiFi Access Point dla siedziby Głównej Zakładu, która umożliwi zbudowanie sieci dostępowej dla urządzeń bezprzewodowych wykorzystywanych w Zakładzie oraz sieci Guest WiFi
9.	Urządzenie UTM – TYP A dla serwerowni głównej	24	1	Szt.	Pozycja dotyczy dostarczenia urządzenia UTM Firewall, w celu zabezpieczenia sieci IT Zakładu na styku z siecią Internet
10.	Urządzenie UTM – TYP B – oczyszczalnia	24	1	Szt.	Pozycja dotyczy dostarczenia urządzenia UTM Firewall, w celu zabezpieczenia sieci OT Zakładu oraz utworzenia szyfrowanego tunelu VPN z serwerownią w siedzibie głównej Zakładu
11.	Urządzenia Access Point dla sieci OT	24	10	Szt.	Pozycja dostarczenia urządzeń sieci Access Point dla siedziby Głównej Zakładu oraz oczyszczalni ścieków i ujęć wody, która umożliwi zbudowanie sieci intranet dla urządzeń OT
12.	Oprogramowanie do analizy logów	24	1	Szt.	W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych,

					systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
13.	Oprogramowanie serwerowe	24	1	Szt.	W ramach postępowania należy dostarczyć oprogramowanie systemów operacyjnych dla dostarczanych serwerów.
14.	System monitorujący prace urządzeń sieciowych i serwerowych	12	1	Szt.	W ramach postępowania należy dostarczyć oprogramowanie do monitorowania pracy urządzeń sieciowych oraz serwerów
15.	Instalacja, konfiguracja, wdrożenie.	24	1	Szt.	Pozycja dotyczy pełnej instalacji i konfiguracji dostarczonych elementów projektu (sprzętowo-programowych) wraz z migracją danych, przeszkoleniem administratorów urzędu oraz zapewnieniem wsparcia powdrożeniowego na okres trwania projektu. Wdrożenie obejmować będzie również wdrożenie usługi Active Directory dla całej sieci Zakładu oraz stworzenie dedykowanych polis GPO.
16.	Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	12	1	Szt.	Pozycja dotyczy opracowania, wdrożenia, przeglądu wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Zakładzie.
17.	Audyt Informatyczny SZBI, audyt zgodności KRI.uoKSC	12	1	Szt.	W ramach zadania Wykonawca przeprowadzi audyt Systemu Zarządzania Bezpieczeństwem Informacji oraz zgodności z Krajowymi Ramami Interoperacyjności.
18.	Testy bezpieczeństwa infrastruktury sieciowej IT/OT	12	1	Szt.	Pozycja dotyczy przeprowadzenia testów bezpieczeństwa w tym testów penetracyjnych infrastruktury sieciowej IT/OT
19.	Szkolenia z zakresu cyberbezpieczeństwa dla pracowników i kadry Zarządzającej	12	2	Szt.	Pozycja dotyczy przeprowadzenia szkolenia podstawowego dla pracowników Zakładu oraz kadry Zarządzającej
20.	Szkolenie pracowników z zakresu cyberbezpieczeństwa z	12	1	Szt.	Pozycja dotyczy przeprowadzenia szkolenia z cyberbezpieczeństwa dla

	uwzględnieniem wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Zakładzie				pracowników i kadry Zarządzającej Zakładu z uwzględnieniem wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji
21.	Szkolenia specjalistyczne dla administratorów IT	12	3	Szt.	Szkolenia specjalistyczne dla administratorów IT Zakładu z zakresu zastosowanych środków bezpieczeństwa i wdrożonych urządzeń

5. Szczegółów opis pozycji.

5.1. Oprogramowanie antywirusowe – 20 licencji

Rozwiązanie do ochrony stacji roboczych i serwerów przed szkodliwym oprogramowaniem.

Centralne zarządzanie

1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).
2. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim.
3. Rozwiązanie musi udostępniać możliwość zmiany języka bez przeinstalowania ani ponownego uruchamiania usług centralnego zarządzania.
4. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS.
5. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID.
6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.
7. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.
8. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
 - Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania.
 - Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
 - Buforowanie ruchu HTTPS.
9. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
10. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania.
11. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - Google Authenticator,
 - Microsoft Authenticator,
 - Authy,
 - Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
12. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
13. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
14. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
 - Adresy sieciowe IP.
 - Aktywne zagrożenia.
 - Stan funkcjonowania oraz ochrony.
 - Wersja systemu operacyjnego.
 - Podzespoły komputera.
15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
 - Wyrażenie CRON.
 - Codziennie / Cotygodniowo / co miesiąc / Co rok.
 - Po wystąpieniu nowego zdarzenia.

- Po automatycznym umieszczeniu hosta w grupie dynamicznej.
16. Rozwiązanie musi udostępniać możliwość tagowania obiektów.
 17. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
 18. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
 - JSON / LEEF / CEF.

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu: Wirus.
 - Trojan.
 - Robak.
 - Adware.
 - Spyware.
 - Dialer.
 - Phishing.
 - Backdoor.
4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
 - Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
 - Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
 - Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - Całego dysku.
 - Wybranych katalogów.
 - Pojedynczych plików.
 - Plików spakowanych oraz skompresowanych.
 - Dysków sieciowych.
 - Dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - Wybranych plików.
 - Wybranych procesów
 - Wybranych lokalizacji.
 - Wybranych rozszerzeń.

- Nazwy wykrycia.
 - Sumy kontrolnej (SHA1).
12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
13. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
- Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. Rozwiązanie musi udostępniać 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).
15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi udostępniać 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- Typ urządzenia:
 - Pamięci masowe.
 - Optyczne pamięci masowe / Pamięci masowe Firewire.,
 - Urządzenia do tworzenia obrazów,
 - Drukarki USB,
 - Urządzenia Bluetooth,
 - Czytniki kart inteligentnych.
 - Modemy.
 - Porty LPT/COM.
 - Urządzenia przenośne.
 - parametry urządzenia:
 - Numer seryjny.
 - Producent.
 - Model.
 - typ dostępu:
 - Brak możliwości zapisu.
 - Pełen dostęp.
 - Ostrzeżenie użytkownika.
 - Brak dostępu.
18. Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów:
- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji
- Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
 - Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
 - Raport musi posiadać co najmniej:
 - Listę zainstalowanych aplikacji.
 - Listę usług systemowych.
 - Informacje o systemie operacyjnym i sprzęcie.
 - Listę aktywnych procesów i połączeń sieciowych.
 - Harmonogram systemu operacyjnego. ➤ Szczegóły pliku hosts.
 - informacje o sterownikach.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
- Antywirus.
 - Zapora osobista.
 - Sandbox,
 - Antyspyware.
 - Metody heurystyczne.
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
 - Ochrona musi być realizowana w oparciu o co najmniej:
 - globalna czarna lista RBL,
 - czarna lista użytkownika,
 - biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - Skanowanie portów TCP oraz UDP,
 - Wykrywanie duplikacji adresu IP,
 - Atak zatrutowania ARP,
 - Nieprawidłowa długość pakietu TCP oraz UDP.
 - Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
 - RDP,
 - SMB,
 - My SQL,
 - Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.

24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

- Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
- Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.

- Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.

- Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
- Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:
 - Treść komunikatu.
 - Obraz.

Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
 - Microsoft Windows Server 2012 R2 / 2016 / 2019 / 2022 / 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - Wirus.
 - Trojan.
 - Robak.
 - Adware.
 - Spyware.
 - Dialer.
 - Phishing.
 - Backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
 - Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.

- Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
 - Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
6. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
 7. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
 8. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
 9. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
 10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - całego dysku,
 - wybranych katalogów,
 - pojedynczych plików,
 - plików spakowanych oraz skompresowanych,
 - dysków sieciowych,
 - dysków przenośnych.
 11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - wybranych plików,
 - wybranych procesów,
 - wybranych lokalizacji,
 - wybranych rozszerzeń,
 - nazwy wykrycia,
 - sumy kontrolnej (SHA1).
 12. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
 13. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
 14. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
 - Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

- Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
 - Raport musi posiadać co najmniej:
 - Listę zainstalowanych aplikacji,
 - Listę usług systemowych,
 - informacje o systemie operacyjnym i sprzęcie,
 - Listę aktywnych procesów i połączeń sieciowych,
 - harmonogram systemu operacyjnego,
 - Szczegóły pliku hosts,
 - Informacje o sterownikach.
15. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
- antywirus,
 - zapora osobista
 - sandbox,
 - antyspyware,
 - metody heurystyczne.
16. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper
17. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
18. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- typ urządzenia:
 - Pamięci masowe.
 - Optyczne pamięci masowe.
 - Pamięci masowe Firewire.
 - Urządzenia do tworzenia obrazów.
 - Drukarki USB.
 - Urządzenia Bluetooth.
 - Czytniki kart inteligentnych.
 - Modemy.
 - Porty LPT/COM.
 - Urządzenia przenośne.
 - parametry urządzenia:
 - Numer seryjny,
 - Producent,
 - Model.
 - typ dostępu:
 - Brak możliwości zapisu,
 - Pełen dostęp,
 - Ostrzeżenie użytkownika,
 - Brak dostępu.
19. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
- MS SQL.
 - Active Directory.
 - IIS.

- Sysvol.
 - DNS.
 - DHCP.
 - Hyper-V.
 - Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
20. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - Skanowanie portów TCP oraz UDP,
 - Wykrywanie duplikacji adresu IP,
 - Atak zatrutowania ARP,
 - Nieprawidłowa długość pakietu TCP oraz UDP.
 - Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
 - RDP,
 - SMB,
 - My SQL,
 - Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
21. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
22. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
- Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Mobile Device Management

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
 - MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
 - Android / iOS / iPadOS.
 - MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
 - Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - Apple Business Manager (ABM),
 - Android Enterprise (co najmniej w zakresie Device Owner).
3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - usunięcie zawartości urządzenia,
 - przywrócenie urządzenia do ustawień fabrycznych,

- zablokowanie urządzenia,
 - uruchomienie sygnału dźwiękowego,
 - lokalizację GPS,
 - Resetowanie hasła blokady ekranu.
4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
 5. MDM musi umożliwiać co najmniej:
 - Dla systemów iOS oraz iPadOS
 - konfigurację kont e-mail,
 - konfigurację połączeń VPN,
 - Konfigurację połączeń Wi-Fi,
 - Konfigurację listy certyfikatów,
 - możliwość uruchomienia trybu jednej aplikacji.
 - Dla systemu Android:
 - blokadę wykonywania połączeń,
 - blokadę konfiguracji sieci Wi-Fi,
 - blokadę konfiguracji tuneli VPN,
 - zarządzanie aktualizacjami systemu operacyjnego,
 - blokadę zmiany tapety urządzenia.

Mobile Threat Defense (MTD) dla systemu Android

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
 - Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
 - Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
 - Złożoność kodu blokady ekranu:
 - Wzór / PIN / Hasło.
 - Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,
 - Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - nazwę aplikacji,
 - nazwę pakietu,
 - kategorię sklepu Google Play,
 - uprawnienia aplikacji,
 - pochodzenie aplikacji z nieznanego źródła.
6. Rozwiązanie musi posiadać ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.

3. Rozwiązanie musi wspierać systemy w tym co najmniej:
 - Microsoft Windows 10 oraz 11,
 - Microsoft Windows Server,
 - macOS 11 (Big Sur) oraz nowszych
 - RedHat Enterprise Linux (RHEL),
 - Rocky Linux,
 - Ubuntu,
 - Debian,
 - SUSE Linux Enterprise Server (SLES),
 - Oracle Linux,
 - Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
 - archiwa,
 - skrypty,
 - pliki wykonywalne,
 - pliki rejestru systemowego (.reg),
 - możliwy spam,
 - dokumenty.
7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
 - natychmiast po ich przeanalizowaniu,
 - po upływie 30 dni,
 - nigdy.
8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej.
W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
 - Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
 - czysty,
 - podejrzany,
 - bardzo podejrzany,
 - szkodliwy.
14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
 - wstrzymania uruchamiania pobieranych plików z następujących źródeł:
 - przeglądarki internetowej,
 - programy poczty e-mail,
 - nośniki wymienne,

- pliki wyodrębnione z archiwum.

15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

Szyfrowanie

1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
5. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
 - Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
 - Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
 - Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
 - Hasło odzyskiwania nie może być krótsze niż 8 znaków.
 - Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
10. Rozwiązanie musi wspierać dyski wykorzystujące funkcji OPAL w wersji co najmniej 2.0.
11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.
12. Rozwiązanie musi umożliwiać automatyczne wstrzymanie uwierzytelnienia w przypadku aktualizacji systemu operacyjnego.

Wsparcie techniczne.

1. Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji.

5.2. Serwer z oprogramowaniem – szt.1 – wymagania minimalne

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi.
Procesor	Jeden procesor szesnasto-rdzeniowy 4514Y, x86 - 64 bity, pracujące z częstotliwością bazową min. 2.0 GHz lub równoważny procesor szesnasto-rdzeniowy osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 267 punktów dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Płyta główna wspierająca zastosowanie dwóch procesorów do 64 rdzeni, mocy do min. 385W
Pamięć operacyjna	Min. 64 GB RDIMM DDR5 5600 MT/s w modułach pamięci o pojemności min. 32 GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiającą instalację do minimum 8TB.

Sloty rozszerzeń	Min. 3 aktywne gniazda PCI-Express generacji 5, gniazda pełnej wysokości (full height) i pełnej długości (full Length) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 1 slot x16 (szybkość slotu – bus width). Serwer z możliwością rozbudowy do 8 gniazd PCI-Express generacji 5, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi. Dwa sloty OCP 3.0 możliwe do obsadzenia poprzez kontrolery sprzętowe dla dysków lub karty sieciowe w dowolnej konfiguracji.
Dysk twardy	Zatoki (wnęki) dyskowe gotowe do zainstalowania min. 8 dysków SFF typu Hot Swap, SAS/SATA/SSD/ NVMe. Serwer z możliwością rozbudowy do obsługi min. 24 dysków SFF typu Hot Swap, SAS/SATA/SSD/ NVMe. Zainstalowane min. 2 szt. dysków HDD 2.4 TB SAS typu Hot-swap. Zainstalowane min. 2szt. dysków HotPlug SSD 960GB Read Intensive.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 8 napędów dyskowych SSD/SATA/SAS/NVMe. Kontroler nie zajmujący gniazd opisanych w sekcji „Sloty rozszerzeń”. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. Możliwość rozbudowy o kontroler z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, min. 32 portowy obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 24 napędów dyskowych SSD/SATA/SAS/NVMe.
Interfejsy sieciowe	Zainstalowana karta 2 portowa 10Gb Base-T oparta o chipset BCM57416 nie zajmująca gniazd opisanych w sekcji „sloty rozszerzeń”.
Karta graficzna	Zintegrowana karta graficzna
Porty	4 x USB 3.2 (w tym 2 porty wewnętrzne) 1x VGA Możliwość rozbudowy/rekonfiguracji o: 1x cyfrowy port video (Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB 1x 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.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W klasy Titanium.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Diagnostyka	Możliwość instalacji w przyszłości elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0
Karta/moduł zarządzający	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: <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 dostęp do karty możliwy

	<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 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) • uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu • 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 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	Oferowany serwer zapewnia wsparcie dla: Microsoft Windows Server 2022, 2025 Ubuntu 20.04 LTS, 22.04 LTS Red Hat Enterprise Linux (RHEL) 8.6, 9.0 VMware ESXi 8.0 U2/U3, 9.0
Wsparcie techniczne	Minimum 3-letnia gwarancja producenta obejmująca: - części, robociznę i naprawę w miejscu instalacji z 4-godzinny czas reakcji przez całą dobę (przybycie na miejsce); - uszkodzone dyski pozostają własnością zamawiającego; - w okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania pokładowego dostarczonego wraz z serwerem i jego wszystkich komponentów. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.
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.

5.3. Macierz dyskowa TYP A – szt. 1 – wymagania minimalne

Typ urządzenia	Serwer NAS
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 2,4 GHz, maksymalnie 2,7 GHz z technologią Turbo Boost osiągający w teście PassMark na sierpień 2022 co najmniej 5870 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 8 GB pamięci DDR4 ECC UDIMM z możliwością rozszerzenia do min. 64GB
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 gniazd rozszerzeń Infiniband
Ilość zainstalowanych dysków HDD	6 dysków 8 TB SATA 3,5"
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 2 gniazda rozszerzenia (półki dyskowe)
Porty sieciowe	Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • Możliwość podłączenia dodatkowych kart sieciowych 10G/25G poprzez gniazdo rozszerzeń PCIe x8
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 2x 8-liniowe gniazdo x8

Wentylator obudowy	Min. 4 wentylatory 80 x 80 mm
Obsługiwane protokoły sieciowe	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: <ul style="list-style-type: none"> 1 PB (wymagana pamięć 64 GB, tylko grupy RAID 6) 200 TB (wymagana pamięć 32 GB) o 108 TB Minimalna liczba wewnętrznych wolumenów: 128 Minimalna liczba obiektów iSCSI Target: 64 Minimalna liczba jednostek iSCSI LUN: 512 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Podstawowy (basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID F1
Funkcja udostępniania plików	<ul style="list-style-type: none"> Minimalna liczba kont użytkowników: 16 000 Minimalna liczba grup użytkowników: 512 Minimalna liczba folderów współdzielonych: 512 Minimalna liczba jednoczesnych połączeń CIFS/AFP/FTP: 2 000
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 lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Chrome®, Firefox®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze; Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze)

Oprogramowanie	<ul style="list-style-type: none"> • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzeniach PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.
Konserwacja	<ul style="list-style-type: none"> • Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack
	<ul style="list-style-type: none"> • Wymiana wentylatora systemowego ma przebiegać w szybki i bezpieczny sposób bez użycia narzędzi
Gwarancja	<p>Wykonawca udzieli gwarancji:</p> <ul style="list-style-type: none"> • 5 lat na urządzenia główne • 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack

5.4 Oprogramowanie do backupu – szt. 1 – wymagania minimalne

Wymagania ogólne

- Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 20 VM oraz 3 serwerach fizycznych.
- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 i 9.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.

- Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
- Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental)
- 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
- 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.
- Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- 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
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
- Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- 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
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
- Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

- Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- Repozytoria oparte o XFS muszą pozwalać na niezmienną ilość danych przez określoną ilość czasu (tzw Immutability)
- 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.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

- 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 oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- 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
- Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
- Oprogramowanie musi umożliwić odtworzenie plików 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
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
 - Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
 - BSD: UFS, UFS2
 - Solaris: ZFS, UFS
 - Mac: HFS, HFS+
 - Windows: NTFS, FAT, FAT32, ReFS
 - Novell OES: NSS
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
- Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych

- Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
- Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
- 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.
- Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
- 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
- Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
- 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.
- Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Monitoring

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
- System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
- System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

- 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.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x

Raportowanie

- System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

5.5 Macierz dyskowa TYP B – szt. 1 – wymagania minimalne

Typ urządzenia	Serwer NAS
Obudowa	Tower
Procesor	Czterordzeniowy procesor o taktowaniu 2.2 GHz.
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB

Możliwości rozbudowy	<ul style="list-style-type: none"> Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 9 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu USB type-C. Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej
Ilość zainstalowanych dysków HDD	2 dyski 12 TB SATA 3,5"
Porty zewnętrzne	<p>Minimum:</p> <ul style="list-style-type: none"> 2 porty USB 3.2.1 1 port USB Typ-C (podłączenie jednostki rozszerzającej)
Porty sieciowe	<p>Minimum:</p> <ul style="list-style-type: none"> 2x port 2.5GbE RJ45
Funkcja Wake on LAN/WAN	Tak
Wentylator obudowy	Min. 2 wentylatory 92 mm x 92 mm
System plików	<p>Min.:</p> <ul style="list-style-type: none"> Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Zarządzanie pamięcią masową	<ul style="list-style-type: none"> Maksymalny rozmiar pojedynczego wolumenu: <ul style="list-style-type: none"> 108 TB 200 TB (wymagana pamięć RAM 32 GB) Minimalna liczba wewnętrznych wolumenów: 32 Minimalna liczba obiektów iSCSI Target: 32 Minimalna liczba jednostek iSCSI LUN: 64 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane protokoły	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, sesje Kerberized NFS, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Konto i folder współdzielony	<ul style="list-style-type: none"> Minimalna liczba kont użytkowników: 512 Minimalna liczba grup użytkowników: 128 Minimalna liczba folderów współdzielonych: 128
Usługi plików	<ul style="list-style-type: none"> Protokół plików: SMB, AFP, NFS, FTP, WebDAV, Rsync Minimalna liczba jednoczesnych połączeń SMB: 40 Integracja z listą kontroli dostępu Windows (ACL) Uwierzytelnianie Kerberos NFS
Wirtualizacja	Obsługa VMware vSphere with VAAI, Windows Server 2022, Citrix Ready, OpenStack
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywany pakiet szyfrowania)
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 120 W
Oprogramowanie	<ul style="list-style-type: none"> Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą

	<p>integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych</p> <ul style="list-style-type: none"> • Urządzenie musi wspierać funkcję WORM (Write Once, Read Many) oraz migawki niezmiennie • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioneing. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Gwarancja	<p>Wykonawca udzieli gwarancji:</p> <ul style="list-style-type: none"> • 3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dodatkowego pakietu gwarancyjnego

5.6 Biblioteka taśmowa LTO-9 – szt.1

Wykorzystana technologia	LTO Ultrium wspierająca technologię partycjonowania nośników.
Obudowa	<p>Typu rack 19". Wysokość maksymalnie 1U - wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem.</p> <p>Urządzenie musi mieć możliwość instalowania w tej samej obudowie różnych generacji napędów LTO (minimum od LTO-6 wzwyż).</p>

Wbudowany napęd	LTO-9 wyposażony w złącze mSAS SFF-8644. Urządzenie musi mieć możliwość instalowania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania kasety oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2
Ilość slotów i magazynki	Minimum 8 kieszeni na taśmy podzielone na dwa magazynki (urządzenie musi być dostarczone z kompletem magazynków). Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot musi odbywać się bez konieczności wysuwania całego magazynka.
Pojemność	Pojemność bez kompresji – minimum 144TB przy obsadzeniu wszystkich slotów na taśmy wyłącznie nośnikami LTO-9
Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNMP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówno poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
Dodatkowe interfejsy	Biblioteka musi być wyposażona w interfejs sieciowy min. FastEthernet, interfejs USB oraz interfejs ADI
Obsługa urządzenia	Wymagana możliwość wymiany napędu, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lampki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki. Wsparcie funkcjonalności Air Gap (izolacji powietrznej)
Wypożyczenie	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli: 1x zasilając, 1x kabel sieciowy, 1x komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera i umożliwiającego komunikację z urządzeniem – długość kabla min. 2m. Wraz z urządzeniem należy dostarczyć także zestaw 20-tu identycznych nośników na dane o pojemności natywnej pojedynczego nośnika min. 18TB oraz jeden nośnik czyszczący wyposażonych w unikalne naklejki z kodem kreskowym. Wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy potwierdzić odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty.
Gwarancja	60 miesięcy gwarancji producenta wraz z szybką wymianą komponentów lub całego urządzenia w czasie do 72 godz. (dni robocze) od momentu zgłoszenia uszkodzenia. Czas przyjmowania zgłoszeń serwisowych w trybie 5x9 z czasem reakcji do 12 godzin od zgłoszenia. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Do oferty należy dołączyć pisemne oświadczenia wystawione przez producenta o gwarancji świadczonej w rygorze 5x9x12 realizowanej przez producenta wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy.

5.7 Przełącznik sieci LAN CORE – szt.1 - wymagania minimalne

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa (Urządzenie UTM opisane w pkt 5.9 w specyfikacji) o następujących parametrach.

Parametry fizyczne platformy:

- Wymiary urządzenia muszą pozwalać na montaż w szafie RACK 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe – wymagania minimalne:

Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

- a) 48 porty GE RJ-45.
- b) 4 porty 10 GE SFP+.

Zarządzanie:

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3.
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe:

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje:

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia.
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie:

System jest objęty serwisem gwarancyjnym producenta przez okres do 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Certyfikat ISO 9001 podmiotu serwisującego

5.8 Urządzenia Access Point Wifi – szt.2

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

- Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
 - a. Temperatura 0–50°C,
 - b. Wilgotność 5–90%.

- Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
- Urządzenie musi być wyposażone w cztery niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
 - c. 2.4 GHz 802.11b/g/n,
 - d. 5 GHz 802.11a/n/ac/ax,
 - e. 6 GHz 802.11ax/be
 - f. Skaner 2.4/5/6GHz
- Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
- Urządzenie musi być wyposażone w moduł BLE.
- Urządzenie musi być wyposażone w dwa interfejsy Ethernet (RJ45), w tym co najmniej jeden wspierający szybkości 100M/1000M/2.5G/5.0G/10G
- Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3bt lub zewnętrzny zasilacz.
- Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - g. Tunnel,
 - h. Bridge,
 - i. Mesh.
- Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
- Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
- Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - j. MIMO – 2x2,
 - k. Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych:
 - i. 688 Mbps;
 - ii. 4324 Mbps;
 - iii. 5765 Mbps;
 - iv. Dedykowany skaner
 - l. Wymagana moc nadawania:
 - i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - ii. min. 26 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - iii. min. 23 dBm dla pasma 6GHz z możliwością zmiany co 1dBm
 - m. Wsparcie dla kanałów 20/40/80/160/320MHz,
 - n. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.
 - o. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
- Maksymalna deklarowana liczba klientów na każdy moduł radiowy 1, 2 lub 3 – 512
- Funkcje dodatkowe:
 - p. OFDMA UL i DL
 - q. Spatial Reuse (BSS Coloring)
 - r. UL-MU-MIMO
 - s. DL-MU-MIMO
 - t. Enhanced Target Wake Time (TWT)
 - u. Wbudowany analizator widma
 - v. Wbudowane mechanizmy WIPS/WIDS

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

5.9 Urządzenie UTM – TYP A – szt. 1

Wymagania Ogólne

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

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

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

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

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 90 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.4 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.3 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.
7. 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.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. 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 dwu-składnikowego 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. Możliwość filtrowania zapytań DNS 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: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.
 - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).

- Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec 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).
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).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.

4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. System wstrzymuje dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox.
9. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
11. 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. System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.
7. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
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. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

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 lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

Serwisy i licencje

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

- a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. Ochrona systemów przemysłowych SCADA na okres 24 miesięcy.
- b) Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum 1 rok, na okres 12 miesięcy
- c) Logowanie, korelowanie zdarzeń, raportowanie oraz generowanie powiadomień w oparciu o usługę realizowaną w chmurze, na okres 12 miesięcy

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

5.10 Urządzenie UTM – TYP B – szt.1

Wymagania Ogólne

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

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

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

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

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

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:
 - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 50 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 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.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.

12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.
 - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym 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 łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPsec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

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. System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA
7. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
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. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.

3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

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 lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

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 12 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do

aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

5.10.1 Urządzenia Access Point dla sieci OT – TYP A – 4 szt.

Częstotliwość pracy	5150 - 5875 MHz (2412 - 2472 MHz do konfiguracji)
Zysk energetyczny	19 dBi
Interfejs sieciowy	2 gigabitowe porty Ethernet 10/100/1000 Mb/s
Procesor	Atheros Taktowanie: 720 MHz
Pamięć RAM	128 MB DDR2
Pamięć wbudowana	8 MB Flash
VSWR	Maks. 1,5:1
Szerokość kanału	Tryb PtP: 10/20/30/40/50/60/80 MHz Tryb PtMP: 10/20/30/40 MHz
Polaryzacja	Podwójna, liniowa (pionowa i pozioma)
Dołączony zasilacz	24 V. 0.5 A PoE Gigabitowy port
Maksymalny pobór mocy	8,5 W
Obudowa	Wykonana z tworzywa sztucznego odpornego na promieniowanie UV
Montaż	Na słupie
Odporność na wiatr	Do 200 km/h
Opór wiatru	45,5 N przy 200 km/h
Wymiary	189x189x125 mm (wliczając uchwyt)
Waga	0,53 kg (wliczając uchwyt)
Ochrona ESD/EMP	24 kV
Dopuszczalna temperatura pracy	Od -40 do 80 st. C
Dopuszczalna wilgotność powietrza	5%-95% niekondensująca
Certyfikaty	CE, FCC, IC
Zgodność z RoHS	Tak

Testy	IEC 68-2-11 (ASTM B117) MIL-STD-810G Method 509.5 IEC 68-2-6 IEC 68-2-14 IEC 68-2-5 przy 40 st. C ETS 300 019-1-MIL-STD-810G Method 506.6
-------	--

5.10.2 Urządzenia Access Point dla sieci OT – TYP B – 6 szt.

Typ	GSM 3G/4G
Transmisja danych:	EDGE UMTS LTE
Sieć GSM:	900 MHz 1900 MHz
Sieć UMTS:	850 MHz 900 MHz 2100 MHz
Sieć LTE:	800 MHz 850 MHz 900 MHz 1800 MHz 2100 MHz 2300 MHz 2500 MHz
Obsługiwane standardy:	802.11b 802.11g 802.11n IPv4 IPv6
Liczba anten:	3-złącza na anteny
Antena:	Zewnętrzna odłączana
Złącza do anten:	2x złącze komórkowe SMA, złącze żeńskie anteny do WIFI (1xRP-SMA)
Szybkość zainstalowanego procesora:	580 MHz
Pamięć RAM:	128 MB
Pamięć Flash:	16 MB
Porty we/wy:	1 x 10/100 Mbit/s 1 x 10/100 Mbit/s WAN 1 x Slot karty SIM
Protokoły sieciowe:	TCP, UDP, IPv4, IPv6, ICMP, NTP, DNS, HTTP, HTTPS, FTP, SMTP, SSLv3, TLS 1.3, ARP, PPP, PPPoE, DHCP, Telnet
Zasilanie:	Złącze 4 pinowe, 9-30 VDC, zasilacz 9W
Bezpieczeństwo:	DDOS prevention (SYN flood protection, SSH attack prevention, HTTP/HTTPS attack prevention) Port scan prevention (SYN-FIN, SYN-RST, X-mas, NULL flags, FIN scan attacks) VPN: OpenVPN, IPsec, GRE, PPTP, L2TP, Stunnel, DMVPN, SSTP, ZeroTier, WireGuard WiFi security: WPA2-Enterprise - PEAP, WPA2-PSK, WEP, WPA-EAP, WPA-PSK; AES-CCMP, TKIP, Auto Cipher modes, client separation
Zarządzanie, monitorowanie, konfiguracja:	Funkcje komórkowe: Auto APN, Band lock Network: Failover (Network backup), VLAN, QoS, Load Balancing Monitoring i zarządzanie: WEB UI, CLI, SSH, CALL, SMS, TR-069, SNMP, JSON-RPC, MQTT, MODBUS, RMS, Ping Reboot, Wget reboot, Periodic Reboot, LCP and ICMP for link inspection Rozwiązania chmurowe: RMS, FOTA, Telenor, Azure IoT Hub, Cloud of Things, Cumulocity, ThingWorx

	SMS: SMS status, SMS configuration, Send/Read SMS via HTTP POST/GET, EMAIL to SMS, SMS to Email, SMS to HTTP, SMS to SMS, scheduled SMS, SMS autoreply, SMPP Serwisy: DDNS, VRRP, Wake On Lan (WOL), WEB filter, UPNP, Traffic Logging, Ipsec VPN
Obudowa:	Aluminium z możliwością montażu na szynie DIN
Stopień ochrony:	IP30

5.11 Oprogramowanie do analizy logów

Wymagania Ogólne

W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz 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 w aktualnie wspieranych wersjach: VMware ESX/ESXi; Microsoft Hyper-V; Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 1 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 długo czasowego 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 korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - Malware.
 - Aplikacje sieciowe.
 - Email.
 - IPS.
 - Traffic.
 - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

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.
 - a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. 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 modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. Wsparcie: System musi być objęty serwisem producenta przez okres do 30 czerwca 2026 roku od daty wdrożenia, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7

5.12 Oprogramowanie serwerowe

Dostawa oprogramowania Microsoft Server Standard 2025 – 2 szt. szczegółowe minimalne parametry:
Zamawiający wymaga dostarczenia do posiadanego serwera oraz nowo kupowanego serwera licencji na Windows Server Standard 2025 w ilości zapewniającej pokrycie na sumaryczną liczbę rdzeni w posiadanych serwerach: 2 serwery jednoprocessorowe po 16 rdzeni w każdym serwerze lub równoważne, tj. obsługujące technologię COM, .NET posiadające możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory opartej na Windows Server i w pełni wspierające MS Exchange, MS System Center Configuration Manager, MS Lync oraz umożliwiający implementację nieograniczonej licencji na liczbę maszyn wirtualnych opartych o usługę Hyper-V.
Licencje na oprogramowanie Microsoft Server Standard 2025 Device CAL – 20 szt.

5.13 System monitorujący prace urządzeń sieciowych i serwerowych

1. Wymagania dla systemu

- System operacyjny powinien być na licencji Open Source (Ubuntu 18.04 lub 20.04, Debian Linux 10, CentOS 8).
- Platformą sprzętową dla rozwiązania jest w sieci Zamawiającego fizyczny serwer będący na wyposażeniu Zamawiającego -wirtualna maszyna w środowisku Vmware lub wirtualna maszyna w środowisku Hyper-V.
- Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source czyli MongoDB oraz Elasticsearch.
- Zamawiający na wyżej wymieniony cel planuje przeznaczyć rozwiązanie sprzętowe - maszynę wirtualną o parametrach procesora (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 1TB.
- Tworzenie użytkowników w systemie centralnego składowania logów powinno odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
- Konta użytkowników w systemie powinny podlegać regulacją pozwalającym na przypisanie ról dla poszczególnych pracowników departamentu IT. Wymagane jest minimalnie, aby system pozwalał na kreowanie ról dostępowych do systemu, które pozwalają na przyznawanie m.in. pełnych uprawnień do systemu, roli menadżera alarmów, operatora widoków nawigacyjnych (dashboardów), dostępu tylko do odczytu do wybranych zestawów danych.
- System powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
- Oprogramowanie powinno mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów.
- System powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.
- System powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
- System powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
- System powinien mieć możliwość tworzenia lub importowania list z pliku do użycia w źródłach wejściowych.

2. W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfiguracją rozwiązania jak i szkolenie z codziennego wykorzystania systemu:

- Instalacja systemu operacyjnego na wybranym przez Zamawiającego serwerze fizycznym-maszynie wirtualnej .
- Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających loga do systemu. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspoźnienie zegarów czasów sieci Zamawiającego.
- Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
- Konfiguracja retencji przechowywania danych z uwzględnieniem zapisów aktów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.

- Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:
 - Urządzenie klasy UTM
 - Przełączniki zarządzalne opisane w niniejszym opisie przedmiotu zamówienia
 - Serwery Windows
 - Serwery Linux
 - (15x) Stacji roboczych Windows 10 i 11
 - Aplikację centralnego zarządzania oprogramowaniem antywirusowego
 - (2x) Serwer wirtualizacji Hyper-V
- Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
- Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
- Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
- Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
- Konfiguracja wysyłania powiadomień poprzez e-maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
- Szkolenie pracowników z obsługi wdrożonego systemu.

3. Gwarancja i asysta techniczne:

- Zamawiający wymaga aby Wykonawca w czasie do 12 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
- Zamawiający wymaga aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów
- Zamawiający wymaga aby w/w usługi były świadczone w poniedziałek, wtorek, czwartek, piątek w godzinach 7.30-15.00 lub w środę w godzinach 7.30-17.30
- Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę i może to być system zgłoszeń elektronicznych lub komunikacja mailowa

5.14 Instalacja, konfiguracja, wdrożenie – szt.1 – wymagania minimalne

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.

1.	Usługi	<p>Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji elementów cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.</p> <p>Część sprzętowa powinna zostać oparta na rozbudowie systemie wirtualizacji zasobów IT.</p> <p>Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem</p>
----	---------------	---

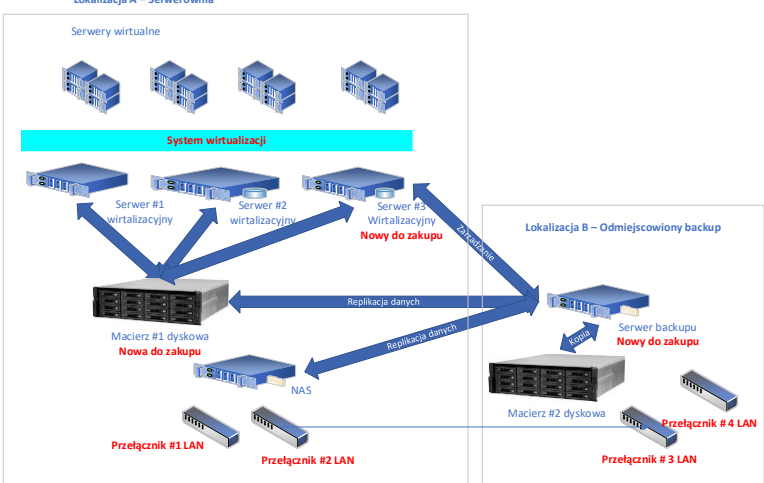
		<p>Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.</p> <p>Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.</p> <p>W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową.</p> <p>Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:</p> <ol style="list-style-type: none"> Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązanie dla sytuacji kryzysowych wdrożenia. Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności: <ol style="list-style-type: none"> koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych. schematy połączeń mechanizmy działania głównych elementów sprzętowych: <ul style="list-style-type: none"> sieć LAN - przełączniki sieciowe system backupu i archiwizacji danych system serwerowy system macierzowy sieć WIFI testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności sposób odbioru uzgodniony z Zamawiającym listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu opis przypadków, w których projekt dopuszcza niedziałanie systemu realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą <p>Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia.</p>
2.	Montaż i fizyczne uruchomienie systemu	<p>Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:</p> <ol style="list-style-type: none"> Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. Rozbudowa istniejących zasobów sprzętowych. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.

		<ol style="list-style-type: none"> 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem: <ol style="list-style-type: none"> a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami. b. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN. c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1. d. Połączenia muszą wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	Instalacja i konfiguracja oprogramowania	<ol style="list-style-type: none"> 1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych. 3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). 4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych. 5. Wdrożenie usług Active Directory dla całej organizacji 6. Stworzenie zasad GPO dla zasobów organizacji
4.	Konfiguracja przełączników/sieci LAN:	<p>Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami występującymi w projekcie według topologii gwiazdy. Centralnym punktem będzie serwerownia zlokalizowana w Zakładzie.</p> <p>Dostarczony przełącznik i urządzenia będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łączy danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego).</p> <p>Konfiguracja przełączników w zakresie:</p> <ol style="list-style-type: none"> a. Przeprowadzenie audytu obecnej topologii oraz konfiguracji. b. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.

		<p>c. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).</p> <p>d. Wymagane jest wydzielenie i skonfigurowanie co najmniej stref:</p> <ul style="list-style-type: none"> • SERWERY • UŻYTKOWNICY WEWNĘTRZNI • UŻYTKOWNICY ZEWNĘTRZNI • MANAGEMENT • URZĄDZENIA OT <p>e. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy)</p> <p>f. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall.</p> <p>g. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN.</p> <p>i. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink.</p> <p>ii. Z wykorzystaniem połączeń światłowodowych oraz miedzianych.</p> <p>iii. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu.</p> <p>iv. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbps (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps.</p> <p>h. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN.</p> <p>i. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster;</p> <p>j. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK).</p> <p>k. Zamawiający wymaga skonfigurowania mechanizmów bezpieczeństwa na dostarczonych przełącznikach LAN co najmniej w zakresie:</p> <ul style="list-style-type: none"> • Konfiguracja mechanizmów DHCP Snooping • Konfiguracja mechanizmów Dynamic ARP Inspection • Konfiguracja mechanizmów Port Security na wskazanych portach przełączników <p>l. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall.</p> <p>m. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source..</p> <p>n. Wykonawca skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów.</p> <p>o. Testowanie obsługi ruchu sieciowego.</p> <p>p. Testowanie skuteczności zabezpieczeń.</p>
5.	Konfiguracja elementów bezpieczeństwa sieciowego.	<p>Modernizacja konfiguracji UTM dla nowych urządzeń w zakresie.</p> <ol style="list-style-type: none"> 1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.

		<ol style="list-style-type: none"> 3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Przygotowanie projektu włączenia urządzenia do sieci LAN zakładu. 5. Konfiguracja dostarczonych systemów Firewall: <ol style="list-style-type: none"> a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp. d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: <ol style="list-style-type: none"> a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. <ol style="list-style-type: none"> a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny. 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN. 11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaze Zamawiający) dla każdej z poniższych funkcjonalności: <ol style="list-style-type: none"> a. kontrola dostępu - zaporą ogniową klasy Stateful Inspection b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
--	--	--

		<ul style="list-style-type: none"> d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Ochrona przed wyciekiem poufnej informacji (DLP) i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) j. Inspekcja ruchu SSL k. Ochrony przez atakami na stacje klienckie l. Kontrola pasma <p>13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi.</p> <p>14. Konfiguracja logowania i raportowania.</p>
6.	System backupu	<p>W ramach projektu przewiduje się stworzenie maszyny wirtualnej do zarządzania i tworzenia backupu..</p> <p>Na serwerze należy zainstalować maszynę wirtualną dostarczoną w ramach niniejszego zamówienia. Serwer musi zostać podłączony do macierzy produkcyjnej, musi posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego. Natomiast druga część zasobu musi zostać wykorzystana do wykonywania replikacji on-line maszyn wirtualnych na lokalną platformę wirtualizacyjną. Takie podejście ma gwarantować zabezpieczenie kluczowych węzłów sieciowych (serwerów wirtualnych) na dwa sposoby tj. plik off-line maszyny wirtualnej oraz kopia on-line replikowania asynchronicznie według harmonogramu.</p> <p>Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej.</p> <p>Oprogramowanie backupu musi obsługiwać również bibliotekę taśmową i system NAS, gdzie będzie można skorzystać z replikacji danych – przesłania backupu dyskowego np.: na zasób taśmowy.</p> <p>Mechanizm podłączenia</p> <ol style="list-style-type: none"> 1. Konfiguracja i podłączenie serwera do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) $n-(n-1)$ ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) $n-(n-1)$ ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.

		<p>3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.</p> <p>Logiczny schemat rozbudowywanego systemu backup – stan docelowy.</p> <p>Lokalizacja A – Serwerownia</p> 
8.	Macierz dyskowa	<p>Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klastery serwerów).</p> <p>Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej.</p>
9.	Migracja danych	<p>Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów.</p> <p>Dane (systemy dziedzinowe) muszą zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalony z Zamawiającym na etapie analizy przedwdrożeniowej.</p> <p>Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych.</p>
10.	Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych.	<ol style="list-style-type: none"> 1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy. 2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego). 3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie. 4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
11.	Instalacja i konfiguracja sieci radiowej i LTE	<p>Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania sieci radiowej i LTE co najmniej w zakresie:</p>

		<ol style="list-style-type: none"> 1. Montaż urządzeń w lokalizacjach wskazanych przez Zamawiającego 2. Konfigurację mostu radiowego na urządzeniach radiowych z urządzeniami sieciowymi zainstalowanymi w serwerowni głównej Zakładu 3. Konfigurację urządzeń LTE w zakresie polityk bezpieczeństwa oraz wykreowanie tunelu ipsec do podstawowej bramy sieciowej Zakładu 4. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 5. Konfiguracja powiadomień o krytycznych zdarzeniach (email) lub SMS jeżeli urządzenie umożliwiać będą takie powiadomienia 6. Podłączenie urządzeń OT
12.	Rekonfiguracja systemu zarządzania kopiami zapasowymi.	<ol style="list-style-type: none"> 1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na dostarczonym serwerze. 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system backupu. 5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania: <ol style="list-style-type: none"> a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; e. musi istnieć możliwość odtworzenia: <ol style="list-style-type: none"> i. całej wirtualnej maszyny; ii. dysku wirtualnej maszyny; iii. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); 6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej: <ol style="list-style-type: none"> a. Nazwę zadania backupu b. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/ c. Długość trwania zadania backupu d. Ilość zapisanych na taśmie danych 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach: <ol style="list-style-type: none"> a. Błąd urządzenia b. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi c. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi d. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi e. Zdarzenia dotyczące licencji f. Zapętnienia mail-słotu 8. Uruchomienie testowych zadań backupu

		<p>9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email</p> <p>10. Uruchomienie testowych zadań odtworzenia danych</p> <p>11. Miejscem przechowywania kopii zapasowych jest:</p> <ol style="list-style-type: none"> serwer backupu. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym <p>12. Do serwera backupu należy podłączyć istniejąca macierz, oraz system NAS.</p> <p>System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.</p>
13.	Testowanie i modyfikacja parametrów infrastruktury sieciowej.	<ol style="list-style-type: none"> Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. Testowanie mechanizmów replikacji danych. Testowanie dostępu publicznego do zasobów. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu Testowanie autoryzowanego dostępu do wewnętrznych zasobów. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
14.	Asysty stanowiskowe	<p>Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.</p> <p>Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego.</p> <p>Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego.</p>
15.	Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.	<p>Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.</p> <p>Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.</p> <p>W tym czasie przedstawiciel Wykonawcy:</p> <ul style="list-style-type: none"> zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. dokona prezentacji działania systemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: <ol style="list-style-type: none"> zastosowanej technologii serwerów zastosowanej technologii pamięci masowej

		c) wirtualizacji d) systemu backupu e) zastosowanych rozwiązań aplikacyjnych Wykonawca zapewni również wsparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązywaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.
16.	Opracowanie dokumentacji powykonawczej	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. <ol style="list-style-type: none"> 1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.
17.	Opieka serwisowa	Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.

5.15 Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Typ	Wykonanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji [SZBI] zgodnie z wymogami Krajowych Ram Interoperacyjności, wytycznymi normy PN-EN ISO/IEC 27001 i dobrych praktyk.
Zakres dokumentacji	<p>W ramach zamówienia wymagane jest analiza posiadanej dokumentacji przez zamawiającego, a w przypadku braku przygotowanie dokumentacji w zakresie minimalnym:</p> <ul style="list-style-type: none"> • Polityka Bezpieczeństwa Informacji • Polityka ochrony danych osobowych – dostosowanie obowiązującego dokumentu do potrzeb wdrażanej dokumentacji SZBI. • Polityka zarządzania systemem informatycznym • Polityka zarządzania ciągłością działania • Procedura zarządzania incydentami cyberbezpieczeństwa lub jej aktualizacja • Analiza ryzyka w zakresie Bezpieczeństwa Informacji • Harmonogram weryfikacji, aktualizacji, wykonania przygotowanej dokumentacji i procedur

Wymagane procedury	<p>W ramach poszczególnych elementów SZBI wymagane jest przygotowanie niezbędnych procedur w zakresie minimalnym, zgodnych z przepisami prawa, które są powszechnie obowiązujące:</p> <ul style="list-style-type: none"> • Procedury korzystania z urządzeń mobilnych • Postępowanie z nośnikami • Procedury kontroli dostępu • Procedury czystego biurka • Procedury czystego ekranu • Procedury kopii zapasowych • Procedury ochrony logów • Bezpieczeństwo komunikacji • Zarządzanie bezpieczeństwem sieci • Przesyłanie informacji • Plany ciągłości działania • Procedury zarządzania incydentami • Prywatność i ochrona danych osobowych • Szacowanie ryzyka w obszarze bezpieczeństwa informacji • Szkolenia personelu • Plan zarządzania podatnościami • Plan reagowania na incydenty • Plan przywracania <p>Zamawiający zastrzega sobie prawo wnoszenia uwag do zaproponowanego SZBI, w tym do rodzaju dokumentów, zakresu merytorycznego itp.</p> <p>Wykonawca gwarantuje, że opracowana przez niego dokumentacja systemu zarządzania bezpieczeństwem informacji będzie zgodna z obowiązującymi przepisami prawa.</p>
Wymagania dodatkowe	<p>Wymaga się aby wykonawca dysponował:</p> <ol style="list-style-type: none"> 1. Co najmniej jedną osobą posiadającymi uprawnienia Audytora wiodącego na podstawie certyfikatów wskazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020 poz. 1369 ze zm.). <p>Wykaz certyfikatów wskazanych w w/w rozporządzeniu:</p> <ul style="list-style-type: none"> • Certified Internal Auditor (CIA); • Certified Information System Auditor (CISA); • Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób; • Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku, w

	<p>zakresie certyfikacji osób;</p> <ul style="list-style-type: none"> • Certified Information Security Manager (CISM); • Certified in Risk and Information Systems Control (CRISC); • Certified in the Governance of Enterprise IT (CGEIT); • Certified Information Systems Security Professional (CISSP); • Systems Security Certified Practitioner (SSCP); • Certified Reliability Professional; • Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert. <p>2. Przynajmniej jeden z audytorów musi posiadać wyższe wykształcenie II stopnia z zakresu cyberbezpieczeństwa, posiadać doświadczenie w realizacji zadań na rzecz samorządu - starostwa powiatowego, urzędu miasta, urzędu gminy.</p> <p>3. Wykonawcy ubiegający się o realizację zamówienia powinni posiadać niezbędną wiedzę i doświadczenie oraz dysponować odpowiednimi zasobami osobowymi umożliwiającymi wykonanie przedmiotu zamówienia, a o udział w zamówieniu mogą ubiegać się Wykonawcy, którzy spełniają następujące warunki w zakresie doświadczenia</p> <p>a) w okresie od 01.01.2022 r. wykonali (tj. świadczyli, zrealizowali, zakończyli) co najmniej 3 usługi opracowania dokumentacji SZBI</p> <p>b) <u>Na potwierdzenie spełniania warunku wymagane jest dołączenie dokumentów potwierdzających posiadane certyfikaty oraz referencje z wykonanych dokumentacji.</u></p>
--	--

5.16 Audyt Informatyczny SZBI, audyt zgodności KRI.uoKSC

Wymagania	Należy przeprowadzić audyt informatyczny Systemu Zarządzania Bezpieczeństwem Informacji na podstawie wdrożonych procedur SZBI zgodnie z wymogami Krajowych Ram Interoperacyjności oraz wytycznymi normy PN-EN ISO/IEC 27001
Wymagania dodatkowe	<p>Wymaga się aby wykonawca dysponował:</p> <p>1. Co najmniej jedną osobą posiadającymi uprawnienia Audytora wiodącego na podstawie certyfikatów wskazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020 poz. 1369 ze zm.).</p> <p>Wykaz certyfikatów wskazanych w w/w rozporządzeniu:</p> <ul style="list-style-type: none"> • Certified Internal Auditor (CIA); • Certified Information System Auditor (CISA); • Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o

	<p>systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;</p> <ul style="list-style-type: none"> • Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób; • Certified Information Security Manager (CISM); • Certified in Risk and Information Systems Control (CRISC); • Certified in the Governance of Enterprise IT (CGEIT); • Certified Information Systems Security Professional (CISSP); • Systems Security Certified Practitioner (SSCP); • Certified Reliability Professional; • Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert. <p>2. Przynajmniej jeden z audytorów musi posiadać wyższe wykształcenie II stopnia z zakresu cyberbezpieczeństwa, posiadać doświadczenie w realizacji zadań na rzecz samorządu - starostwa powiatowego, urzędu miasta, urzędu gminy.</p> <p>3. Wykonawcy ubiegający się o realizację zamówienia powinni posiadać niezbędną wiedzę i doświadczenie oraz dysponować odpowiednimi zasobami osobowymi umożliwiającymi wykonanie przedmiotu zamówienia, a o udział w zamówieniu mogą ubiegać się Wykonawcy, którzy spełniają następujące warunki w zakresie doświadczenia</p> <ol style="list-style-type: none"> a. w okresie od 01.01.2025 r. wykonali (tj. świadczyli, zrealizowali, zakończyli) co najmniej 3 usługi audytu SZBI b. <u>Na potwierdzenie spełniania warunku wymagane jest dołączenie dokumentów potwierdzających posiadane certyfikaty oraz referencje z wykonanych dokumentacji.</u>
--	--

5.17 Testy bezpieczeństwa infrastruktury sieciowej IT/OT

Wymagania	<p>Zakres Prac</p> <p>1. Infrastruktura Sieciowa</p> <p>Testy penetracyjne infrastruktury sieciowej obejmujące:</p> <ul style="list-style-type: none"> • Skanowanie i analiza portów. • Identyfikację i eksploatację luk bezpieczeństwa w sieci. • Testy odporności na ataki DoS/DDoS wolumetryczne oraz aplikacyjne • Testy zabezpieczeń urządzeń sieciowych (routery, firewalle, przełączniki, punkty dostępowe), wewnętrzne i zewnętrzne. • Sprawdzenie polityk zabezpieczeń sieci. (w zakresie podłączania obcych urządzeń, przechodzenia między podsieciami, separacji logicznej sieci itp.) • Analiza i testy VPN oraz innych połączeń zdalnych. • Testy systemów wykrywania i zapobiegania włamaniom (IDS/IPS).
------------------	---

2. Infrastruktura Serwerowa

Testy penetracyjne infrastruktury serwerowej obejmujące:

- Analizę konfiguracji serwerów pod kątem bezpieczeństwa
- Analiza bezpieczeństwa Active Directory
- Identyfikację i eksploatację luk w systemach operacyjnych (Windows, Linux, Unix).
- Testy podatności na ataki typu privilege escalation.
- Sprawdzenie polityk zarządzania użytkownikami i kontrolą dostępu.
- Weryfikacja kont z dostępem administracyjnym i zakresu dostępów.
- Testy zabezpieczeń usług serwerowych (np. FTP, SSH, HTTP/HTTPS, DNS,DHCP).
- Analiza i testy zabezpieczeń baz danych.
- Weryfikacja poprawności stosowania aktualizacji i łat bezpieczeństwa.
- Testy systemów kopii zapasowych i odzyskiwania danych.

Metodologia Przeprowadzania Testów

Istotne założenia:

- Czas na realizację testów to 14 dni kalendarzowych.
- Czas na wytworzenie raportu po zakończeniu prac to 14 dni kalendarzowych.
- W ramach testów nie jest przewidziana próba przełamania zabezpieczeń fizycznych.
- Zespół testerów dołoży wszelkich starań w trakcie pozyskiwania informacji i testowania w celu zminimalizowania ingerencji w sieć produkcyjną. Jednak działania testerów mogą być obarczone pewnym prawdopodobieństwem destabilizacji niektórych usług, o czym wykonawca powiadomi zamawiającego przed wykonaniem danego testu.
- Działania audytowe mogą być prowadzone o dowolnej porze dnia i nocy.
- Tester użyje komputera niepowiązanego z podmiotem audytowanym przy próbach dostępu do zasobów
- Testy penetracyjne danej jednostki zostaje zakończony w momencie przekazania raportu zamawiającemu jako zaszyfrowany załącznik w wiadomości email.
- Przed rozpoczęciem prac audytowych niezbędne będzie wypełnienie stosownej deklaracji osób decyzyjnych zamawiającego oraz jednostki audytowanej świadczącej o zgodzie na działania i wiedzy nt. potencjalnych skutków działań testerów.
- Wykonawca, z dniem podpisania protokołu odbioru raportu, przenosi na Zamawiającego autorskie prawa majątkowe do raportu

3. Przeprowadzenie testów

Raportowanie

- Zebranie wyników testów bezpieczeństwa
- Analiza wyników audytu
- Opisanie podatności wraz z kategoryzacją CVE i CVSS
- Opisanie rekomendacji

	<ul style="list-style-type: none"> Przekazanie raportu <p>Zawartość raportu:</p> <ul style="list-style-type: none"> Executive Summary – główne konkluzje Główne rekomendacje Przedmiot testów Ranking ryzyk Metodologia i kryteria testowania Wykorzystane narzędzia w trakcie prowadzenia skanów Wykaz zidentyfikowanych podatności wraz z odpowiadającym im kodem CVE (Common Vulnerability Enumeration) oraz odnośnikiem do opisu luki. Podatności będą pogrupowane według ryzyka, zgodnie ze standardem CVSS (Common Vulnerability Scoring System). Rekomendacje związane z możliwym usunięciem wykrytych podatności
<p>Wymagania dodatkowe</p>	<p>Wymaga się aby wykonawca dysponował:</p> <ol style="list-style-type: none"> Co najmniej jedną osobą posiadającymi uprawnienia Audytora wiodącego na podstawie certyfikatów wskazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020 poz. 1369 ze zm.). <p>Wykaz certyfikatów wskazanych w w/w rozporządzeniu:</p> <ul style="list-style-type: none"> Certified Internal Auditor (CIA); Certified Information System Auditor (CISA); Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób; Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób; Certified Information Security Manager (CISM); Certified in Risk and Information Systems Control (CRISC); Certified in the Governance of Enterprise IT (CGEIT); Certified Information Systems Security Professional (CISSP); Systems Security Certified Practitioner (SSCP); Certified Reliability Professional; Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert. <ol style="list-style-type: none"> Przynajmniej jeden z audytorów musi posiadać wyższe wykształcenie II stopnia z zakresu cyberbezpieczeństwa, posiadać doświadczenie w

	<p>realizacji zadań na rzecz samorządu - starostwa powiatowego, urzędu miasta, urzędu gminy.</p> <p>3. Wykonawcy ubiegający się o realizację zamówienia powinni posiadać niezbędną wiedzę i doświadczenie oraz dysponować odpowiednimi zasobami osobowymi umożliwiającymi wykonanie przedmiotu zamówienia, a o udział w zamówieniu mogą ubiegać się Wykonawcy, którzy spełniają następujące warunki w zakresie doświadczenia</p> <p>a. w okresie od 01.01.2025 r. wykonali (tj. świadczyli, zrealizowali, zakończyli) co najmniej 3 usługi audytu SZBI</p> <p>b. <u>Na potwierdzenie spełniania warunku wymagane jest dołączenie dokumentów potwierdzających posiadane certyfikaty oraz referencje z wykonanych dokumentacji.</u></p>
--	--

5.18 Szkolenia z zakresu cyberbezpieczeństwa dla pracowników i kadry Zarządzającej

Wykonawca przeprowadzi szkolenia z zakresu cyberbezpieczeństwa dla pracowników i kadry Zarządzającej Zamawiającego dla dwóch grup po maksymalnie 20 osób.

Czas szkolenia do 1,5 ha plus 30 min (ewentualna dyskusja i zadawanie pytań) .

Tematyka będzie dotyczyła między innymi:

- Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2),
- Ochrony danych osobowych pod kątem RODO,
- Socjotechniczne mechanizmy działania cyberprzestępców,
- Zagrożenia dla użytkownika i zasobów organizacji,
- Konsekwencje lekceważenia zasad cyberbezpieczeństwa
- Zabezpieczenia informatyczne środowiska pracy

Do dyspozycji Zamawiającego zostaną przekazane w formie elektronicznej materiały tematykę szkolenia. Wykonawca wystawi zaświadczenia dla osób z odbycia szkolenia i dostarczy do Zamawiającego w formie papierowej.

5.19 Szkolenie pracowników z zakresu cyberbezpieczeństwa z uwzględnieniem wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Zakładzie

Wykonawca przeprowadzi szkolenia z zakresu wdrożonego przez Wykonawcę Systemu Zarządzania Bezpieczeństwem Informacji dla pracowników i kadry Zarządzającej Zamawiającego dla dwóch grup po maksymalnie 20 osób.

Czas szkolenia do 1,5 ha plus 30 min (ewentualna dyskusja i zadawanie pytań) .

Do dyspozycji Zamawiającego zostaną przekazane w formie elektronicznej materiały tematykę szkolenia. Wykonawca wystawi zaświadczenia dla osób z odbycia szkolenia i dostarczy do Zamawiającego w formie papierowej.

5.20 Szkolenia specjalistyczne dla administratorów IT

1. Szkolenie dla Administratorów z zakupionego urządzenia UTM – dla 2 (dwóch) osób do końca czerwca 2026r.
Szkolenie stacjonarne w siedzibie Zamawiającego, w obecności trenera na sali szkoleniowej
2. Szkolenie Administratora: Windows Server, AD, 1 osoba do końca czerwca 2026.
Szkolenie stacjonarne w siedzibie Zamawiającego, w obecności trenera na sali szkoleniowej.