



Fundusze Europejskie
dla Podkarpacia



Rzeczpospolita
Polska

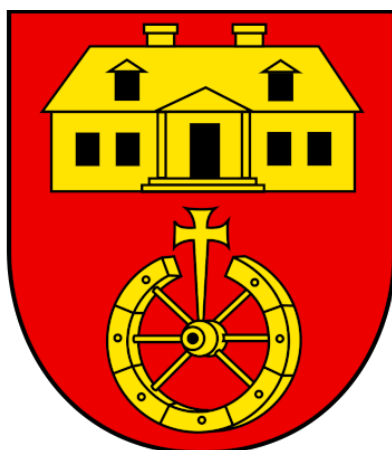
Dofinansowane przez
Unię Europejską



PODKARPACKIE
przestrzeń otwarta

Załącznik nr 1 do SWZ

Szczegółowy Opis przedmiotu zamówienia



Nozdrzec, 22 listopad 2025 r.



SPIS TREŚCI

Wprowadzenie	3
Metodyka projektu.....	3
Dokumentacja techniczna wymagana.....	5
Etapy wdrożenia	6
Termin realizacji Przedmiotu umowy.....	7
I. SPRZĘT i INFRASTRUKTURA.....	7
Zestawienie zakresu dostaw i usług	7
Wymagania ogólne dla urządzeń i oprogramowania infrastruktury.....	8
Wymagania gwarancyjne	9
2.1 Licencja na system Backupu – szt. 1 lic.	10
2.2 Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa – szt.1 lic.	16
2.3 Serwer – szt.1.....	36
2.4 Firewall – klaster (2 urządzenia w HA).....	40
2.5 Centralny system logów – szt.1	47
2.6 Zestaw komputerowy z oprogramowaniem – szt.15.....	50
2.7 Laptop – szt.20.....	66
2.8 Centralny UPS – szt.1	82
2.9 Agregat – szt.1.....	84
2.10 System do transmisji obrad Rady Gminy – sprzęt – 1 kpl.	85
2.11 Szkolenia TiK typ I – 120 godzin	87
2.12 Opracowanie procedur bezpieczeństwa informacji i przetwarzania danych	88
2.13 Instalacja i konfiguracja (Platforma sprzętowa) – 250 RBH	90
2.14 Wodomierze – szt. 296	104
5.6 Wodomierze – szt. 296	104
5.12 Przepływomierz – szt. 2.....	106
5.12.1 Model – 6 DN 65.....	106
5.12.2 Model – 6 DN 100.....	106



Wprowadzenie

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (SOPZ) w zakresie dostawy i wdrożenia oprogramowania i sprzętu służącego realizacji projektu pn. „Platforma e-usług publicznych w Gminie Nozdrzec”. Wszystkie parametry techniczne określone w niniejszym SOPZ określają minimalne wymagania stawiane oferowanym urządzeniom i oprogramowaniu. Wykonawca nie ma prawa żądać dodatkowego wynagrodzenia, jeśli dostarczone elementy systemów posiadały będą większą funkcjonalność niż wymagana niniejszym SOPZ.

Projekt pn. „Platforma e-usług publicznych w Gminie Nozdrzec” realizowany jest przez Gminę Nozdrzec. Głównym miejscem realizacji Projektu jest:

- **Urząd Gminy Nozdrzec, Nozdrzec 224, 36-245 Nozdrzec.**

Projekt realizowany przez Gminę Nozdrzec ma na celu jest rozwój społeczeństwa informacyjnego w Gminie Nozdrzec poprzez dostarczenie mieszkańcom i podmiotom gospodarczym nowoczesnych i bezpiecznych e-usług administracji lokalnej.

Metodyka projektu

W celu efektywnej realizacji projektu wdrożeniowego rozwiązania, projekt powinien być realizowany zgodnie z zaproponowaną przez wykonawcę i zaakceptowaną przez Zamawiającego metodyką projektową zgodą ze standardami branżowymi dostępnymi powszechnie, tj. PRINCE2®, M_o_R®, IPMA lub innymi równoważnymi standardami, w tym metodyki zwinne AGILE takie jak SCRUM.

Wykonawca jest zobowiązany wraz z zaproponowaną metodyką dostarczyć jej szczegółowy opis zawierający minimalnie strukturę zadań, podział obowiązków, ról w projekcie, zidentyfikowane ryzyka, harmonogram, opisy podstawowych procesów projektowych. W razie zaproponowania równoważnej metodyki opartej o równoważne standardy Wykonawca musi wykazać ich równoważność w zakresie wskazanym w powyższym zapisie.

Ogólne zasady równoważności rozwiązań

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może proponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na



całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp.

Zapisy dotyczące wymogów dostępności w dokumentacji zamówienia

Poniższe postanowienia należy włączyć do Specyfikacji Warunków Zamówienia (SWZ) / Opisu Przedmiotu Zamówienia (OPZ) / projektu umowy, celem zapewnienia zgodności zamówienia z ustawą z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze (Dz. U. 2024, poz. 731).

Postanowienia ogólne

1. Zamawiający informuje, że niniejsze zamówienie podlega przepisom ustawy z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze (Dz. U. 2024, poz. 731), zwanej dalej „Ustawą”.
2. Wykonawca zobowiązuje się do realizacji zamówienia w sposób zapewniający zgodność z wymogami dostępności wynikającymi z Ustawy oraz przepisów wykonawczych.
3. Wszelkie oferowane produkty i świadczone usługi muszą umożliwiać korzystanie z nich przez osoby ze szczególnymi potrzebami na zasadzie równości z innymi użytkownikami.

Wymagania szczegółowe dotyczące dostępności

1. Wykonawca jest zobowiązany zapewnić, aby wszystkie produkty, urządzenia, oprogramowanie oraz usługi objęte zamówieniem spełniały wymagania dostępności określone w Ustawie, w tym w szczególności w zakresie projektowania uniwersalnego oraz stosowania racjonalnych usprawnień.
2. W zależności od przedmiotu zamówienia, wymogi dostępności dotyczą w szczególności m.in.:
 - a) konsumenckich systemów sprzętu komputerowego ogólnego przeznaczenia i ich systemów operacyjnych,
 - b) terminali płatniczych lub samoobsługowych urządzeń elektronicznych,
 - c) urządzeń końcowych wykorzystywanych do świadczenia usług telekomunikacyjnych lub audiowizualnych,
 - d) usług e-handlu, usług telekomunikacyjnych, bankowości detalicznej oraz pozostałych usług wskazanych w Ustawie.
3. W przypadku gdy oferowany produkt lub usługa nie spełnia wymogów dostępności, Wykonawca zobowiązany jest zaproponować rozwiązanie równoważne zapewniające dostępność zgodnie z Ustawą.



Dokumenty potwierdzające zgodność z wymaganiami dostępności

1. Wykonawca zobowiązany jest dołączyć do oferty pisemne oświadczenie o spełnianiu wymagań dostępności przez oferowane produkty i/lub usługi.
2. Na żądanie Zamawiającego, Wykonawca zobowiąże się dostarczyć dokumentację techniczną, instrukcje użytkowania, deklaracje zgodności, certyfikaty lub inne dowody potwierdzające spełnienie wymogów dostępności.
3. Dokumentacja, o której mowa powyżej, musi być sporządzona w języku polskim.

Kontrola spełniania wymagań dostępności

1. Zamawiający zastrzega sobie prawo do kontroli spełnienia wymagań dostępności na każdym etapie realizacji umowy, w tym podczas odbioru przedmiotu zamówienia oraz w okresie gwarancyjnym.
2. W przypadku stwierdzenia niezgodności, Zamawiający może:
 - a) wezwać Wykonawcę do usunięcia niezgodności w wyznaczonym terminie,
 - b) odmówić odbioru przedmiotu zamówienia do czasu spełnienia wymogów dostępności,
 - c) naliczyć kary umowne przewidziane w umowie,
 - d) odstąpić od umowy z winy Wykonawcy, jeżeli brak spełnienia wymogów dostępności ma charakter istotny.

Odpowiedzialność Wykonawcy

1. Wykonawca ponosi pełną odpowiedzialność za zapewnienie zgodności produktów i usług z wymogami Ustawy.
2. Wykonawca zobowiązuje się do niezwłocznego informowania Zamawiającego o wszelkich zmianach wpływających na spełnianie wymagań dostępności.
3. W przypadku nałożenia przez organy nadzoru rynku kar, sankcji lub obowiązków związanych z brakiem spełnienia wymogów dostępności, odpowiedzialność ponosi Wykonawca.

Dokumentacja techniczna wymagana

Całość pracy w niniejszym opisie przedmiotu zamówienia musi znaleźć się w dokumentacji technicznej i powykonawczej. Dokumentacja powykonawcza w zakresie czynności IT odnosi się do zestawu dokumentów i raportów, które są przygotowywane po zakończeniu wdrożenia systemu informatycznego, projektu IT lub innego rodzaju prac technicznych. Jest ona kluczowa dla zapewnienia przejrzystości, utrzymania i dalszego rozwoju systemu.

Zamawiający będzie wymagał następujących opisów:

1. Opis systemu i architektury

- Szczegółowy opis infrastruktury IT, w tym serwerów, sieci, urządzeń, baz danych, aplikacji i ich wzajemnych powiązań.
- Architektura systemu z przedstawieniem wszystkich komponentów, ich wersji oraz ról.

2. Instrukcje instalacji i konfiguracji

- Kroki związane z instalacją i konfiguracją oprogramowania oraz sprzętu.
- Wersje używanych narzędzi, frameworków oraz systemów operacyjnych.

3. Instrukcje użytkownika i administracyjne

- Instrukcje obsługi systemu dla użytkowników końcowych.



- Dokumentacja dla administratorów dotycząca utrzymania systemu, wykonywania kopii zapasowych, monitorowania wydajności oraz zarządzania użytkownikami.

4. Raporty z testów

- Wyniki testów akceptacyjnych, testów wydajnościowych i innych rodzajów testów przeprowadzanych w trakcie wdrożenia.
- Zgłoszone błędy i sposoby ich naprawienia.

5. Zmiany wprowadzone podczas realizacji

- Opis modyfikacji w stosunku do pierwotnego planu, w tym zmiany w zakresie funkcjonalności, konfiguracji lub architektury systemu.

6. Plany awaryjne i odzyskiwanie po awarii

- Procedury dotyczące radzenia sobie z krytycznymi awariami i przywracania systemu do działania.
- Sposób wykonywania i przechowywania kopii zapasowych oraz procedury odzyskiwania danych.

7. Zasady bezpieczeństwa

- Polityki bezpieczeństwa, w tym konfiguracja zapór sieciowych, zabezpieczenia dostępu, monitorowanie logów oraz zarządzanie hasłami.

8. Lista komponentów i licencje

- Szczegółowy spis wszystkich komponentów sprzętowych i programowych użytych w projekcie, wraz z informacjami o licencjach i ich okresie ważności.

9. Kontakt do wsparcia technicznego

- Informacje kontaktowe do osób lub firm odpowiedzialnych za utrzymanie systemu lub jego poszczególnych części.

Dokumentacja powykonawcza w IT jest niezbędna do dalszej eksploatacji i wsparcia systemu, umożliwiając nowym zespołom szybkie zapoznanie się z wdrożeniem oraz umożliwiając efektywne zarządzanie systemem w przyszłości

Etapy wdrożenia

Zamawiający oczekuje, że Wykonawca lub Wykonawcy przedstawią Szczegółowy Harmonogram realizacji projektu wg złożonych ofert opracowany zgodnie ze swoją metodyką wdrożeniową, wraz ze szczegółową strukturą zadań oraz produktów poszczególnych etapów projektu z uwzględnieniem spodziewanych przez Zamawiającego dat uruchomienia poszczególnych elementów systemu, jednak nie mniej niż w podziale na:

- prace przygotowawcze, analiza przedwdrożeniowa,
- dostawa sprzętu, licencji, instalacja oprogramowania na dostarczonej infrastrukturze,
- wdrożenie poszczególnych modułów systemów w kolejności pozwalającej na optymalne obciążenie pracą zespołu Zamawiającego i Wykonawcy, obejmujące podział



na: prace konfiguracyjne, szkolenia personelu, uruchomienie modułu, oddanie modułu,

Termin realizacji Przedmiotu umowy

Nie dłuższy niż 6 miesięcy od podpisania Umowy.

Szczegółowy harmonogram zostanie przygotowany przez Wykonawcę lub Wykonawców w zakresie, którym złożył ofertę i zaakceptowany przez Zamawiającego.

Wymagania ogólne dotyczącą Instalacji i konfiguracji Platformy sprzętowej.

I. SPRZĘT I INFRASTRUKTURA

Zestawienie zakresu dostaw i usług

LP	NAZWA	Min. Gwarancja (m-ce)	Typ/ Rodzaj gwarancji	Ilość	JM
1.	Oprogramowanie do backupu	24	Producenta	1	lic.
2.	Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa	24	Producenta	1	lic.
3.	Serwer	36	Producenta	1	szt.
4.	Firewall – klaster (2 urządzenia w HA)	36	Producenta	1	kpl.
5.	Centralny system logów	36	Producenta	1	szt.
6.	Zestaw komputerowy z oprogramowaniem	36	Producenta	15	szt.
7.	Laptopy	36	Producenta	20	szt.
8.	Centralny UPS	36	Producenta	1	szt.
9.	Agregat	36	Producenta	1	szt.
10	System do transmisji obrad Rady Gminy - sprzęt	36	Wykonawcy/ producenta	1	kpl.
11	Wodomierze	36	Wykonawcy/ producenta	296	szt.
12	Przepływomierz	36	Wykonawcy/ producenta	2	szt.
13	Instalacja i konfiguracja (Platforma sprzętowa)	12	Wykonawcy	250	RBH
14	Dokumentacja techniczna	Nd.	Nd.	20	RBH
15	Szkolenia TiK typ I	Nd.	Nd.	120	RBH
16	Opracowanie procedur bezpieczeństwa informacji i przetwarzania danych	Nd.	Nd.	120	RBH

Zakres obejmuje:



1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
2. Urządzenia, które nie są montowane w szafach teleinformatycznych np.: komputery powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego.
3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
4. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
5. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
6. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchcordsy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
7. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
8. Instalacja, konfiguracja i wdrożenie dostarczonego oprogramowania
 - a) systemu wykonywania backupu i archiwizacji danych.
 - b) systemu serwerowego wraz z niezbędnymi usługami opisanymi
 - c) oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn.
 - d) monitorowania i analizy cyberbezpieczeństwa - SOC (SIEM/SOAR).
 - e) zarządzania infrastrukturą IT.
9. Rejestracja oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Wnioskodawcy)
10. Opracowanie dokumentacji powykonawczej
11. Asysta stanowiskowa.

Wymagania ogólne dla urządzeń i oprogramowania infrastruktury

- 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;
- ogólne zasady równoważności rozwiązań:

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może proponować



rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym, jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp. Portale, które zostaną uruchomione dzięki realizacji tego projektu, na których znajdować się będą oferowane e-usługi, będą spełniały wszystkie obowiązkowe wytyczne określone w dokumencie WCAG 2.1.

Wymagania gwarancyjne

- O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązania; 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.



2.1 Licencja na system Backupu – szt. 1 lic.

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 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. 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 jakiegokolwiek 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 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 predefiniowanymi alarmami
- 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 rozwiązywania 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 nadanych 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.



2.2 Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa – szt.1 lic.

System przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.

1. System musi umożliwić odbieranie logów z urządzeń sieciowych oraz wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
2. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
3. System powinien pozwalać na pracę z logami zdarzeń jednoliniowych oraz wieloliniowych.
4. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiające ich podział na poszczególne pola, na podstawie, których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
5. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmując zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
6. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
7. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
8. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
9. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji.
10. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
11. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze



odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.

12. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
13. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zawartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo, jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku, gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.
14. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego wypełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.
15. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.
16. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.
17. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
18. System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
19. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
20. System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.
21. Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent_bytes), rozmiar pliku (file_size) i czas trwania sesji (session_duration).
22. Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.



23. Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
24. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
25. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
26. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
27. Mechanizm archiwizacji musi umożliwiać pozwalając na przywracanie danych do systemu celem analizy online.
28. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
29. System musi umożliwiać integrację z zewnętrznymi modelami językowymi takimi jak OpenAI, Fireworks, lub modelem językowym (LLM) zgodnym ze standardem Ollama, z zachowaniem pełnej zgodności z zasadami bezpieczeństwa i ochrony danych obowiązującymi u Zamawiającego.
30. Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
31. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
32. Oferowany system musi być wyposażony we wbudowany model językowy (LLM/GPT), dostarczony przez Producenta i stanowiący integralną część oferowanej platformy. Model językowy musi działać lokalnie w infrastrukturze Zamawiającego lub w środowisku chmurowym należącym do Producenta, z zapewnieniem zgodności z wymaganiami w zakresie bezpieczeństwa i ochrony danych obowiązującymi u Zamawiającego.
33. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
34. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.
35. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z



możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.

36. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
37. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:
 - a. nowe zasoby wykryte w sieci,
 - b. typy wykrytych zasobów (np.: serwer lub stacja robocza),
 - c. zastosowane na nich zabezpieczenia,
 - d. usługi, z którymi się komunikują,
 - e. nowe usługi wykryte na zasobie,
 - f. komunikację do usług wykrytych na zasobie.
38. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
39. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:
 - a. fqdn,
 - b. e-mail,
 - c. nazwa pliku,
 - d. ścieżka do pliku,
 - e. hash,
 - f. adres IP,
 - g. klucz rejestru,
 - h. cmd.
40. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest, aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>).
41. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).



42. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).
43. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.
44. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
45. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwany wynik analizy jest lista niezgodności (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).
46. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
47. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
48. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.
49. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:
 - a. id techniki,
 - b. taktykę,
 - c. platformy których dotyczy,
 - d. potencjalne źródła,
 - e. opis zagrożenia,
 - f. mityzację,
 - g. sposób detekcji,
 - h. referencje.
50. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia



maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.

51. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).
52. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:
 - a. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
 - b. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
 - c. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
 - d. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.
53. System uczenia maszynowego musi posiadać wbudowane mechanizmy niewymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).
54. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP, na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.
55. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np.: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).
56. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
57. System musi umożliwiać definiowanie kontekstu organizacyjnego Zamawiającego, w tym: wykorzystywanych technologii, struktury organizacyjnej oraz obowiązujących wymagań prawnych. Na podstawie wprowadzonych danych wbudowany model językowy (LLM) ma zapewniać generowanie wyników analizy dostosowanych do specyfiki działalności Zamawiającego.
58. Wbudowany model językowy (LLM), stanowiący integralną część oferowanego systemu, musi umożliwiać dynamiczną analizę gromadzonych danych, w szczególności w zakresie:
 - a. automatycznego wyjaśnienia analizowanego zdarzenia,



- b. weryfikacji potencjalnego naruszenia bezpieczeństwa wraz z rekomendacją działań naprawczych,
 - c. klasyfikacji wykrytego zagrożenia z wykorzystaniem matrycy MITRE ATT&CK,
 - d. opisu wektora ataku,
 - e. wykrycia naruszenia danych wrażliwych."
55. Oprogramowanie musi udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.
56. System musi umożliwiać rozbudowywanie funkcji Asystenta AI o nowe zapytania/prompty w kontekście analizy logów. Utworzone zapytania muszą być dostępne dla wszystkich użytkowników systemu za pomocą nowych przycisków lub pozycji list rozwijalnych.
57. Oprogramowanie powinno udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.
58. Oprogramowanie powinno udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.
59. Asystent AI musi pozwalać na budowanie odpowiedzi w dowolnym języku.
60. Asystent AI musi automatycznie dopasowywać zdarzenie do technik i taktyk matrycy MITRE.
61. Asystent AI musi dokonywać automatycznej izolacji obiektów IoC ze wskazanego rekordu logów.
62. Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostępnej stronie internetowej producenta.
63. Oferowany system musi zapewniać dostęp do pełnej dokumentacji technicznej bezpośrednio z poziomu interfejsu użytkownika. Dokumentacja ta musi być możliwa do przeszukiwania z wykorzystaniem wbudowanego Asystenta Sztucznej Inteligencji modelu językowego (LLM), umożliwiającego formułowanie i wykonywanie zapytań w języku naturalnym.
64. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.
65. System musi posiadać interfejs graficzny do tworzenia własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie.



Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:

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

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

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

67. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

- a. wykrycie wystąpienia wartości pola na wybranej liście,



- b. wykrycie niewystępowania wartości pola na wybranej liście,
 - c. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony),
 - d. wykrycie niewystąpienia pary wartości na wybranej liście
 - e. (np.: nazwa użytkownika wraz aplikacją, z którą się wcześniej nie łączył).
68. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:
- a. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
 - b. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
 - c. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
 - d. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),
 - e. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.
69. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:
- a. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
 - b. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
 - c. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.
70. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:
- a. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie, jako wskaźnik kompromitacji;
 - b. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie, jako wskaźnik kompromitacji;
 - c. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie, jako wskaźnik kompromitacji;
71. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:
- a. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
 - b. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,



- c. wykrycie nieautoryzowanej usługi na serwerze,
 - d. wykrycie nieautoryzowanego połączenia do usługi na serwerze,
 - e. wykrycie nieautoryzowanego połączenia z serwera usług,
 - f. wykrycie nieautoryzowanego połączenia do sieci Internet.
72. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:
- a. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
 - b. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
 - c. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
 - d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
73. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:
- a. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
 - b. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
 - c. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
 - d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.
74. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:
- a. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
 - b. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
 - c. wykrycie zdarzeń o wysokim „severity” na zasobach posiadających krytyczne podatności,
 - d. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.
75. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:
- a. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,
 - b. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.



76. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:
- wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
 - wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
 - wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.
77. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:
- wykrycie anomalii na koncie uprzywilejowanym użytkownika,
 - wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
 - wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
 - wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
 - wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
78. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:
- sparsowane pola oraz ich wartości,
 - atrybuty użytkowników z Active Directory,
 - atrybuty komputerów z Active Directory,
 - informacje z elektronicznej dokumentacji.
79. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:
- adresie IP,
 - koncie domenowym użytkownika,
 - strefie bezpieczeństwa,



- d. zakresie adresów IP.
80. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.
- a. wszystkie skorelowane zdarzenia,
 - b. korespondencja pocztowa,
 - c. załączniki z próbkami lub dowodami,
 - d. wskaźniki kompromitacji (IoC),
 - e. informacje pozyskane z innych systemów.
81. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:
- a. identyfikację celu i źródła zagrożenia,
 - b. nazwę oraz adres IP źródła zagrożenia,
 - c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
 - d. lokalizację z której pochodzi zagrożenie np.: Internet,
 - e. strefę bezpieczeństwa, z której pochodzi zagrożenie,
 - f. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
 - g. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
 - h. nazwę oraz adres IP celu zagrożenia,
 - i. zabezpieczenia lokalne chroniące cel zagrożenia,
 - j. strefę bezpieczeństwa, w której znajduje się cel zagrożenia.
82. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:
- a. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
 - b. segregacja – segregacja i kwalifikacja zdarzeń,
 - c. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
 - d. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
 - e. zdarzenie obsłużone – zdarzenie, które zostało obsłużone w systemie.
83. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.



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

- a. gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o:
 - listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
 - listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
- b. gotowe i proste w użyciu filtry rozszerzające analizę logów o:
 - listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
 - listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

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

- a. warunki powiadomień,
 - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
 - zdarzeń o przekroczonych czasach SLA o definiowalny okres,
 - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
 - zdarzeń, których priorytet osiągnął określoną wartość,
 - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
 - zdarzeń na których doszło do naruszenia bezpieczeństwa,
 - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
 - zdarzeń realizujących zdefiniowaną usługę,
 - zdarzeń przetwarzających sklasyfikowane informacje,
 - zdarzeń przetwarzanych na krytycznych zasobach,
- b. odbiorców powiadomień, w tym:
 - operatora, któremu zostało przydzielone zdarzenie,
 - właściciela zasobu na którym wystąpiło zdarzenie,
 - zespół obsługi, który odpowiada za obsługę zdarzeń,
 - właściciela usługi, która jest realizowana na zasobie, na którym wystąpiło zdarzenie,
 - podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.



- c. kanały powiadomień, m.in. e-mail, sms, komunikator,
 - d. zastosowanie mechanizmów grupowania:
 - grupowanie wielu powiadomień w jednej wiadomości,
 - ograniczenie liczby wierszy powiadomienia do określonej wartości.
86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:
- a. utworzenia nowego zdarzenia z określonym priorytetem,
 - b. utworzenia nowego zdarzenia na zasobie krytycznym,
 - c. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
 - d. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
 - e. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
 - f. modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,
 - g. zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,
 - h. przejęcia przydzielonego operatorowi zdarzenia przez innego operatora.
87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:
- a. wybór raportu, który ma zostać wysłany,
 - b. zdefiniowanie jego tytułu,
 - c. zdefiniowanie cyklu, w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
 - d. możliwość ograniczenia cyklu do dni powszednich,
 - e. określenie daty przesłania pierwszego raportu,
 - f. możliwości ograniczenia okresu, przez jaki raport będzie przesyłany, do:
 - zdefiniowanej daty końcowej,
 - określonej liczby raportów,
 - g. określenie odbiorców raportu.
88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).
89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka, jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:
- a. strefę bezpieczeństwa, w której została wykryta podatność,
 - b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,



- c. rodzaj zasobu, którego dotyczy ta podatność,
 - d. ważność tego zasobu dla organizacji,
 - e. przetwarzane na tym zasobie informacje, np.: dane osobowe,
 - f. usługi realizowane przez ten zasób, np.: DNS,
 - g. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
 - h. poprawność konfiguracji zasobu, na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
 - i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.
90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi, jak i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:
- a. wyliczonym priorytecie podatności,
 - b. aktualnym statusie obsługi,
 - c. ważności zasobu na którym została wykryta,
 - d. adresie IP tego systemu,
 - e. parametrów SLA związanych z tym statusem,
 - f. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
 - g. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV)” = „Network”.
92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:
- a. przekroczenia czasu reakcji o określony czas np.: o godzinę,
 - b. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
 - c. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
 - d. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
 - e. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,



- f. przekroczenia czasu obsługi zdarzeń zakwalifikowanych, jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
 - g. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
 - h. przekroczenia czasu obsługi zdarzeń zakwalifikowanych, jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
 - i. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
 - j. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
 - k. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,
93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
- a. warunki powiadomień,
 - podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
 - podatności o przekroczonych czasach SLA o definiowalny okres,
 - podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
 - podatności, których priorytet osiągnął określoną wartość,
 - zdarzeń realizujących zdefiniowaną usługę,
 - zdarzeń przetwarzających sklasyfikowane informacje,
 - zdarzeń przetwarzanych na krytycznych zasobach,
 - b. odbiorców powiadomień, w tym:
 - operatora, któremu została przydzielona podatność,
 - właściciela zasobu, na którym wystąpiła podatność,
 - zespół obsługi, który odpowiada za obsługę podatności,
 - właściciela usługi, na która jest realizowana na zasobie, na którym wystąpiła podatność,
 - podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwany przez firmę zewnętrzną.
 - c. kanały powiadomień, m.in. e-mail, sms, komunikator,
 - d. zastosowanie mechanizmów grupowania:
 - grupowanie wielu powiadomień w jednej wiadomości,
 - ograniczenie liczby wierszy powiadomienia do określonej wartości.
94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im podatności do



obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

- a. przydzielenia nowej podatności do obsługi z określonym priorytetem,
 - b. przydzielenia nowej podatności do obsługi na zasobie krytycznym,
 - c. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
 - d. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
 - e. modyfikacji przydzielonej operatorowi podatności przez innego operatora,
 - f. zamknięcia przydzielonej operatorowi podatności przez innego operatora,
 - g. przejęcia przydzielonej operatorowi podatności przez innego operatora.
95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:
- a. wybór raportu, który ma zostać wysłany,
 - b. zdefiniowanie jego tytułu,
 - c. zdefiniowanie cyklu, w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
 - d. możliwość ograniczenia cyklu do dni powszednich,
 - e. określenie daty przesłania pierwszego raportu,
 - f. określenie okresu, przez jaki będą one przesyłane, poprzez:
 - zdefiniowanie daty końcowej,
 - bez daty końcowej,
 - określenie liczby raportów,
 - g. określenie odbiorców raportu.
96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentację danych do potrzeb zalogowanego użytkownika.
97. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących:
- a. zestaw wykresów dla bieżącego użytkownika,
 - b. zestaw wykresów dla wybranego użytkownika,
 - c. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
 - d. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).
98. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy:



- a. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
 - ilość zdarzeń nowych i niesklasyfikowanych,
 - ilość zdarzeń sklasyfikowanych, jako incydenty bezpieczeństwa,
 - ilość zdarzeń sklasyfikowanych, jako fałszywe alarmy,
- b. wykres przedstawiający skale zagrożeń, który uwzględnia:
 - ilość zasobów krytycznych, na których są obsługiwane zdarzenia,
 - ilość zasobów niekrytycznych, na których są obsługiwane zdarzenia,
- c. wykres przedstawiający źródła zagrożeń, który uwzględnia:
 - ilość nowych zdarzeń dotyczących użytkowników,
 - ilość podjętych zdarzeń dotyczących użytkowników,
 - ilość nowych zdarzeń dotyczących zasobów,
 - ilość podjętych zdarzeń dotyczących zasobów,
- d. wykres przedstawiający poziom zagrożeń, który uwzględnia:
 - ilość nowych zdarzeń w podziale na priorytety,
 - ilość podjętych zdarzeń w podziale na priorytety,
- e. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
 - ilość zdarzeń zarejestrowanych w bieżącym dniu,
 - ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
 - ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
 - ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
- f. wykres przedstawiający zagrożone usługi, który uwzględnia:
 - ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
 - ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
 - wykres przedstawiający zagrożone dane, który uwzględnia:
 - ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
- g. wykres przedstawiający skale podatności, który uwzględnia:



- ilość zasobów krytycznych, na których są obsługiwane podatności,
 - ilość zasobów niekrytycznych, na których są obsługiwane podatności,
- h. wykres przedstawiający czas obsługi podatności, który uwzględnia:
- ilość podatności zarejestrowanych w bieżącym dniu,
 - ilość podatności zarejestrowanych w ostatnim tygodniu,
 - ilość podatności zarejestrowanych w ostatnim miesiącu,
 - ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,
- i. wykres przedstawiający wagę podatności, który uwzględnia:
- ilość nowych podatności w podziale na priorytety,
 - ilość podjętych podatności w podziale na priorytety,
99. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
100. System musi być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
101. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.3.
102. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.
103. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencja nie może nakładać limitów w tym zakresie.
104. Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia.
105. Produkt musi umożliwiać równoczesną pracę, co najmniej 5 operatorów oraz obsługiwać 200 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.
106. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
107. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w



infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

108. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
109. Dostarczone rozwiązanie musi być objęte 24 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia niestanowiące błędu krytycznego lub poważnego).

Wykonawca udzieli Zamawiającemu wieczystej (perpetual), nieograniczonej czasowo licencji na zakupiony System.



2.3 Serwer – szt.1

Wymagania minimalne:

Obudowa

- Typu RACK, wysokość 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Możliwość zainstalowania 12 dysków twardych hot plug 3,5”;
- Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Zainstalowane 10 szt. dysków SSD 1,92TB Hot-Plug

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Zainstalowany moduł TPM 2.0;
- 6 złącz PCI Express w tym:
 - 2 fizyczne złącza o prędkości x16, generacji 5;
 - 2 fizyczne złącza o prędkości x8;
- 32 gniazda pamięci RAM;
- Obsługa minimum 8 TB pamięci RAM DDR5;
- Wsparcie dla technologii:
 - Memory Scrubbing;
 - ECC;
- Zainstalowana karta producenta dla dwóch dysków M.2. NVMe Dyski nie mogą zajmować klatek dla dysków hot-plug. Zainstalowane 2 dyski o pojemności minimum 960GB skonfigurowane w RAID1

Procesory

- Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64;
- Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 246 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany w konfiguracji dwuprocesorowej dla dowolnego producenta serwera na stronie <http://spec.org/cpu2017/results/cpu2017.html>.

Pamięć RAM

- 256 GB pamięci RAM;
- DDR5 minimum 5600MT/s;

Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

- 2x 1Gbit Base-T;
- 2x 10/25Gbit SFP28, wszystkie porty obsadzone modułami MMF LC;

Możliwość dołożenia karty PCI Express, aby osiągnąć dwa interfejsy 100Gbit QSFP28

Kontrolery I/O

- Kontroler RAID dla dysków wewnętrznych posiadający 8GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

Porty



- Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- 1 porty USB 3.0 wewnętrzne;
- 2 porty USB dostępne z tyłu serwera;
- 2 porty USB na panelu przednim;
- Opcjonalny port serial
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimum 1100W;
- Redundantne wentylatory hotplug.

Zarządzanie

- Wbudowany wyświetlacz informujący o stanie serwera - system przewidywania, rozpoznawania awarii;
 - informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
 - karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express;
 - procesory CPU;
 - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
 - status karty zarządzającej serwerem;
 - wentylatory;
 - bateria podtrzymująca ustawienia BIOS płyty głównej;
 - zasilacze;
- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
 - Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
 - Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
 - Dostęp poprzez przeglądarkę Web, SSH;
 - Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
 - Zarządzanie alarmami (zdarzenia poprzez SNMP);
 - Możliwość przejęcia konsoli tekstowej;
 - Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
 - Obsługa serwerów proxy (autentykacja);
 - Obsługa VLAN;
 - Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
 - Obsługa protokołów TLS 1.2, SSL v3;
 - Obsługa protokołu LDAP;
 - Synchronizacja czasu poprzez protokół NTP;



- Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

- Microsoft Windows Server 2025, 2022, 2019;
- VMWare vSphere 8.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9, 8;
- Microsoft Hyper-V Server 2025, 2022, 2019.

Gwarancja

- 3 lata gwarancji producenta serwera w trybie on-site. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
- Funkcja zgłaszania usterek i awarii sprzętowych poprzez założenie zgłoszenia w systemie helpdesk/servicedesk lub poprzez infolinie producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 lub równoważna na świadczenie usług serwisowych;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite

Dokumentacja, inne

- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Zgodność z normami:RoHS, WEEE oraz CE lub równoważnymi.



Fundusze Europejskie
dla Podkarpacia



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



PODKARPACKIE
przestrzeń otwarta

- Serwer będzie przeznaczony nie tylko dla Urzędu Gminy Nozdrzec, ale również będzie służył podniesieniu bezpieczeństwa w Gminnym Ośrodku Pomocy Społecznej.



2.4 Firewall – klaster (2 urządzenia w HA)

Wymagania minimalne

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 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 16 portami Gigabit Ethernet RJ-45.
 - 8 gniazdami SFP 1 Gbps.
 - 4 gniazdami SFP+ 10 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować, co najmniej 200 interfejsów wirtualnych, definiowanych, jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.



5. System jest wyposażony w zasilanie AC.
6. Parametry wydajnościowe:
 1. W zakresie Firewall'a obsługa nie mniej niż 2.8 mln. jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.
 2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.
 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 30 Gbps.
 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.
 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 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 - zaporę ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do 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. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.



- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
- 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
- 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
- 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
- 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - 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. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.



- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa 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, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do 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 21).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).



6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).



Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorii 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 dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego 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 oraz wykonane testy.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

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

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego



serwisu wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

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

2.5 Centralny system logów – szt.1

Wymagania minimalne

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:

VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

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

Parametry wydajnościowe:

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

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



Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować, co najmniej:
 - a. Listę najczęściej wykrywanych ataków.
 - b. Listę najbardziej aktywnych użytkowników.
 - c. Listę najczęściej wykorzystywanych aplikacji.
 - d. Listę najczęściej odwiedzanych stron www.
 - e. Listę krajów, do których nawiązywane są połączenia.
 - f. Listę najczęściej wykorzystywanych polityk Firewall.
 - g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa, (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa, co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich 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.

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

Wsparcie: System musi być objęty serwisem przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

2.6 Zestaw komputerowy z oprogramowaniem – szt.15

Wymagania minimalne

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Komputer	<p>Komputer fabrycznie wbudowany w obudowę monitora.</p> <p>Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.</p>
2.	Obudowa	<p>Obudowa typu All-in-One z możliwością zabezpieczenia fizycznego przez metalową linkę typu Kensington Lock oraz umożliwiającą beznarzędziową wymianę pamięci RAM.</p> <p>Wyposażona w listwę montażową w standardzie VESA 100x100.</p> <p>Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym</p>
3.	Podstawa	<p>Podstawa umożliwiająca regulację jednostki w zakresie co najmniej:</p> <ul style="list-style-type: none"> • pochylenie przód tył od -5 do 20 stopni • swivel w zakresie 45 stopni w każdą stronę • pivot w zakresie 90 stopni • regulację wysokości w do 110 mm
4.	Chipset	Dostosowany do zaoferowanego procesora
5.	Płyta główna	<p>Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 3 złącza M.2 z czego 2 dedykowane dla dysku SSD PCIe. Płyta główna wyposażona w min. 2 sloty pamięci RAM DDR5.</p>
6.	Procesor	<p>Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark - Multithread Rating wynik co najmniej 25000 pkt. według wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php</p> <p>Wynik nie starszy niż 90 dni od daty złożenia oferty. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.</p>



7.	Pamięć operacyjna	Min. 16GB RAM, Możliwość rozbudowy do min. 64GB Jeden slot pozostawiony wolny
8.	Dysk twardy	Min 512GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku OPAL, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość instalacji drugiego dysku SSD M.2
9.	Karta graficzna	Zintegrowana karta graficzna z procesorem.
10.	Matryca	Min. 23,8" IPS o rozdzielczości min. FHD 1920x1080 Jasność typowa min. 250 cd/m ² Kontrast typowy min. 1300:1 Typowy czas reakcji matrycy maksymalnie 14ms Odświeżanie min. 60Hz Gamut min. 99% sRGB Sprzętowa funkcja redukująca emisję światła niebieskiego Kąty widzenia poziomo/pionowo min. 178/178 stopni
11.	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane dwa głośniki o mocy min. 3W każdy Wbudowane dwa mikrofony. Kamera min. 5MP zintegrowana z obudową komputera, z mechaniczną zasłoną obiektywu, funkcją logowania za pomocą rozpoznawania twarzy oraz możliwością regulacji pochylenia w zakresie od -20 do 20 stopni.
12.	Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000 Wbudowana karta sieci bezprzewodowej, pracująca w standardzie AX Bluetooth min. 5.1
13.	Porty/złącza	Z tyłu obudowy: <ul style="list-style-type: none"> • 1 x USB 3.2 typu C Generacji 2; • 3 x USB 3.2 typu A Generacji 1; • 1 x HDMI combo; • 1x DisplayPort 1.4;

		<ul style="list-style-type: none"> • 1x RJ-45; <p>Z boku obudowy:</p> <ul style="list-style-type: none"> • 3x USB 3.2 typu A Generacji 2; • 1x złącze audio combo; <p>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.</p>
14.	Klawiatura/mysz	Przewodowa USB: klawiatura w układzie US + mysz z rolką
15.	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 180W oraz sprawności na poziomie min. 90%.
16.	Ergonomia	Głośność jednostki w konfiguracji oferowanej lub wyższej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w trybie jałowym (IDLE) ma wynosić maksymalnie 22dB
17.	System operacyjny	<p>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.



	<p>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.</p> <p>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.</p> <p>9. Wbudowany system pomocy w języku polskim.</p> <p>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</p> <p>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.</p> <p>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.</p> <p>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.</p> <p>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</p> <p>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.</p> <p>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</p> <p>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.</p> <p>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</p> <p>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p>
--	---



		<p>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</p> <p>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."</p> <p>24. Wbudowany mechanizm wirtualizacji typu hypervisor."</p> <p>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</p> <p>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>27. Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p>
--	--	--



		<p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ol style="list-style-type: none"> Login i hasło, Karty inteligentne i certyfikaty (smartcard), Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), Certyfikat/Klucz i PIN, Certyfikat/Klucz i uwierzytelnienie biometryczne. <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń.</p>
18.	BIOS	<p>Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznymi i podłączonymi do niego urządzeniami zewnętrznymi odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> • modelu komputera, • numerze seryjnym, • numerze inwentarzowym (AssetTag), • MAC Adres karty sieciowej, • wersji BIOS, • dacie produkcji BIOS, • zainstalowanym procesorze, • zainstalowanej pamięci RAM, • urządzeniach podłączonych do portów M.2. <p>Możliwość z poziomu Bios:</p> <ul style="list-style-type: none"> • wyłączenia/włączenia selektywnego (pojedynczo) portów USB, • wyłączenia karty sieciowej,



		<ul style="list-style-type: none"> • wyłączenia karty audio, • wyłączenia funkcji Wake on LAN, • wyłączenia wirtualizacji, • wyłączenia modułu TPM. <p>- możliwość ustawienia portów USB w jednym z dwóch trybów:</p> <ol style="list-style-type: none"> 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB, 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej. <p>- ustawienia hasła: administratora, Power-On, dysku twardego,</p> <p>- wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan),</p> <p>- ustawienia trybu wyłączenia komputera w stan niskiego poboru energii,</p> <p>- zdefiniowania sekwencji bootowania, z uwzględnieniem PXE, zewnętrznych nośników, dysku twardego,</p> <p>- załadowania optymalnych ustawień Bios,</p> <p>bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.</p>
19.	Zintegrowany System Diagnostyczny	<p>Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający wykonanie diagnostyki następujących podzespołów:</p> <ul style="list-style-type: none"> • test pamięci RAM, • test dysku twardego, • test portów USB, • test płyty głównej, • test procesora. <p>Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregośkolwiek z powyższych podzespołów komputera.</p> <p>Ponadto system powinien umożliwiać identyfikację testowanej jednostki i jej komponentów w następującym zakresie:</p> <ul style="list-style-type: none"> • PC: Producent, model,



		<ul style="list-style-type: none"> • BIOS: Wersja, data wydania, producent, • Procesor : Nazwa, taktowanie, liczba rdzeni, liczba wątków, pamięć cache L1, L2, L3, • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny, taktowanie, • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy, producent. <p>System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.</p>
20.	Certyfikaty i standardy	<p>Dla producenta sprzętu:</p> <ul style="list-style-type: none"> • ISO 9001 lub równoważny; • ISO 14001 lub równoważny; • ISO 50001 lub równoważny; <p>Dla komputera:</p> <ul style="list-style-type: none"> • Deklaracja zgodności CE lub równoważna; • TUV Rheinland Low Blue Light lub równoważna; • TUV Rheinland Flicker Free lub równoważna; • MIL-STD-810H lub równoważna;
21.	Bezpieczeństwo	<ul style="list-style-type: none"> - Złącze typu Kensington Lock; - Moduł TPM 2.0 z certyfikacją TCG; - Czujnik otwarcia obudowy;
22.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
23.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie.



24.	Gwarancja i wsparcie techniczne	<p>Świadczona w miejscu użytkowania sprzętu (on-site). Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:</p> <ul style="list-style-type: none"> • fabrycznej konfiguracji urządzenia, • rodzaju gwarancji, • dacie wygaśnięcia gwarancji, • aktualizacjach. <p>Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.</p>
25.	Pakiet biurowy	<p>Pakiet biurowy spełniający następujące wymagania techniczne:</p> <p>Licencja wieczysta</p> <p>Wymagania odnośnie interfejsu użytkownika:</p> <ul style="list-style-type: none"> • pełna polska wersja językowa interfejsu użytkownika, • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; • oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: • posiada kompletny i publicznie dostępny opis formatu, • w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleczeń, język skryptowy); • do aplikacji musi być dostępna pełna dokumentacja w języku polskim; <p>Pakiet zintegrowanych aplikacji biurowych musi zawierać:</p> <ul style="list-style-type: none"> • edytor tekstów, • arkusz kalkulacyjny, • narzędzie do przygotowywania i prowadzenia prezentacji, • narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami), <p>1. Edytor tekstów musi umożliwiać:</p> <ul style="list-style-type: none"> • edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, • wstawianie oraz formatowanie tabel, • wstawianie oraz formatowanie obiektów graficznych,



- wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
- automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
- automatyczne tworzenie spisów treści,
- formatowanie nagłówków i stopek stron,
- śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
- nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
- określenie układu strony (pionowa/pozioma),
- wydruk dokumentów,
- wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,
- zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
- wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,

2. Arkusz kalkulacyjny musi umożliwiać:

- tworzenie raportów tabelarycznych,
- tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
- tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
- tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, Webservice),
- obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,
- tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
- wyszukiwanie i zamianę danych,
- wykonywanie analiz danych przy użyciu formatowania warunkowego,
- nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,



		<ul style="list-style-type: none"> • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • formatowanie czasu, daty i wartości finansowych z polskim formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; <p>3. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <ul style="list-style-type: none"> • przygotowywanie prezentacji multimedialnych, • prezentowanie przy użyciu projektora multimedialnego, • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016; <p>4. Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none"> • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, • filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
--	--	--



		<ul style="list-style-type: none"> • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
26.	Program antywirusowy	<p>Administracja zdalna w chmurze</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po



	<p>wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.</p> <p>Ochrona stacji roboczych</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci
--	--



masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

15. 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.

16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

17. 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.

18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.



19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).

20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na gości (HIPS).

11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.



	<p>12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.</p> <p>21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.</p> <p>Ochrona urządzeń mobilnych opartych o system Android</p> <p>1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.</p> <p>2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.</p>
--	--



		<p>3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).</p> <p>4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.</p> <p>5. Rozwiązanie musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:</p> <ul style="list-style-type: none"> • usunięcie zawartości urządzenia, • przywrócenie urządzenie do ustawień fabrycznych, • zablokowania urządzenia, • uruchomienie sygnału dźwiękowego, • lokalizację GPS. <p>6. Rozwiązanie musi zapewniać administratorowi podejrzanie listy zainstalowanych aplikacji.</p> <p>7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:</p> <ul style="list-style-type: none"> • nazwę aplikacji, • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła.
--	--	--

2.7 Laptop – szt.20

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Typ	Komputer przenośny.
2.	Procesor	Procesor ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej minimum 17000 na podstawie wyników Passmark CPU Mark opublikowanych na stronie http://www.cpubenchmark.net/ . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
3.	Pamięć operacyjna RAM	Min. 16GB DDR5 pracującej w trybie dual channel. Możliwość rozbudowy pamięci do min. 64GB.



4.	Parametry pamięci masowej	M.2 512 GB SSD PCIe 4.0 x4 NVMe. Przygotowana, wolna zatoka do rozbudowy komputera o dodatkowy dysk SSD.
5.	Karta graficzna	Zintegrowana karta graficzna z procesorem.
6.	Wposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo 2x2W, port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu oraz obsługująca logowanie za pomocą danych biometrycznych, dwa mikrofony z funkcją wygłuszania niechcianych odgłosów tła, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
7.	Obudowa	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane, PC-ABS) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H lub równoważne.
8.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny urządzenia.
9.	Bezpieczeństwo	Moduł fTPM 2.0 lub dTPM 2.0. Slot typu Kensington. Komputery wyposażone w złącze Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington. Dysk systemowy zawierający partycję recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
10.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
11.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera



		<p>lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> • wersji BIOS, • nr seryjnym komputera, • typie procesora, • ilości pamięci RAM. <p>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:</p> <ul style="list-style-type: none"> • Możliwość ustawienia hasła administratora; • Możliwość ustawienia hasła dysku twardego; • Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS; • Możliwość włączenia/wyłączenia bootowania z USB oraz PXE; • Możliwość Wyłączania/Włączania: karty sieciowej, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, USB;
12.	Bezpieczeństwo – System Diagnostyczny	<p>Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednocześnie przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych:</p> <p>1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów:</p> <ul style="list-style-type: none"> • pamięci ram, • procesora, • pamięci masowej, • płyty głównej. <p>2. Identyfikację jednostki i jej komponentów w następującym zakresie:</p>



		<ul style="list-style-type: none"> • urządzenie (producent, model, numer seryjny), • bios (producent, wersja oraz data wydania), • procesor (nazwa, taktowanie, ilości pamięci cache), • pamięć ram (ilość zainstalowanej pamięci ram, producent), • dysk twardy (producent, model, numer seryjny, pojemność).
13.	Ekran	Matowy, matryca IPS 16" 16:10 z podświetleniem w technologii LED, rozdzielczość min. WUXGA 1920x1200, jasność min. 300 nits, kąt otwarcia pokrywy ekranu min. 180 stopni.
14.	Interfejsy Komunikacja /	<ul style="list-style-type: none"> - 2x USB 3.2 typu A; - 1x ThunderBolt 4; - 1x USB 3.2 typu C z obsługą power delivery oraz displayPort; - 1x HDMI; - 1x złącze audio combo; - 1x RJ-45; - 1x czytnik kart SD <p>Nie dopuszcza się osiągnięcia wymaganych portów poprzez zastosowanie przejściówek.</p>
15.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie min. Wi-Fi 6E 11ax. Bluetooth min. 5.3.
16.	Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, wyposażona w min. 2 tryby podświetlania przycisków (włączone, wyłączone).
17.	Czytnik papilarnych linii	Czytnik linii papilarnych wbudowany w klawiaturę lub przycisk zasilania. Przycisk zasilania znajdujący się poza obrysem klawiatury, celem uniknięcia przypadkowego naciśnięcia. Nie dopuszcza się umiejscowienia przycisku włączania np. w górnym rzędzie klawiatury.
18.	Akumulator	O pojemności min. 45Wh.
19.	Zasilacz	Zasilacz zewnętrzny USB-C min. 65W.
20.	Certyfikaty, oświadczenia i standardy	<p>Dla producenta sprzętu należy dostarczyć certyfikat:</p> <ul style="list-style-type: none"> - ISO 9001 lub równoważny; - ISO 14001 lub równoważny;



		<p>- ISO 50001 lub równoważny;</p> <p>Dla komputera: - Deklaracja zgodności CE lub równoważna;</p>
21.	Waga	Waga startowa urządzenia nie większa niż 1.75kg według karty katalogowej producenta.
22.	System operacyjny	<p>System operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).



	<p>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.</p> <p>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.</p> <p>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.</p> <p>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</p> <p>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.</p> <p>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</p> <p>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.</p> <p>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</p> <p>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</p> <p>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."</p> <p>24. Wbudowany mechanizm wirtualizacji typu hypervisor."</p> <p>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</p>
--	---



	<p>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>27. Wbudowana zaporą internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none"> a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN,
--	--



		<p>e. Certyfikat/Klucz i uwierzytelnienie biometryczne.</p> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń.</p>
23.	Oprogramowanie do aktualizacji sterowników	<p>Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.</p>
24.	Gwarancja i wsparcie techniczne	<p>Gwarancji świadczonej w miejscu użytkowania (on-site).</p> <p>Bezpłatna infolinia w języku polskim, funkcjonująca minimum w godzinach 9:00 – 16:00 oraz obsługująca zgłoszenia serwisowe i oferująca wsparcie techniczne w zakresie co najmniej:</p> <ul style="list-style-type: none"> - wsparcia technicznego dla zakupionego sprzętu, - weryfikacji konfiguracji fabrycznej zakupionego sprzętu, - weryfikacji statusu gwarancji zakupionego sprzętu. <p>i Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:</p> <ul style="list-style-type: none"> - fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji, - aktualizacjach. <p>Diagnostyka sprzętowa dostępna na stronie internetowej producenta</p>
25.	Pakiet biurowy	<p>Pakiet biurowy spełniający następujące wymagania techniczne:</p> <ul style="list-style-type: none"> • Licencja wieczysta;



- Wymagania odnośnie interfejsu użytkownika:
- pełna polska wersja językowa interfejsu użytkownika,
- prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;
- oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
- posiada kompletny i publicznie dostępny opis formatu,
- w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropolecień, język skryptowy);
- do aplikacji musi być dostępna pełna dokumentacja w języku polskim;

Pakiet zintegrowanych aplikacji biurowych musi zawierać:

- edytor tekstów,
- arkusz kalkulacyjny,
- narzędzie do przygotowywania i prowadzenia prezentacji,
- narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami),

1. Edytor tekstów musi umożliwiać:

- edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
- wstawianie oraz formatowanie tabel,
- wstawianie oraz formatowanie obiektów graficznych,
- wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
- automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
- automatyczne tworzenie spisów treści,
- formatowanie nagłówków i stopek stron,
- śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
- nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
- określenie układu strony (pionowa/pozioma),
- wydruk dokumentów,
- wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,
- zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,



		<ul style="list-style-type: none"> wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, <p>2. Arkusz kalkulacyjny musi umożliwiać:</p> <ul style="list-style-type: none"> tworzenie raportów tabelarycznych, tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, Webservice), obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, wyszukiwanie i zamianę danych, wykonywanie analiz danych przy użyciu formatowania warunkowego, nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, formatowanie czasu, daty i wartości finansowych z polskim formatem, zapis wielu arkuszy kalkulacyjnych w jednym pliku, zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; <p>3. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <ul style="list-style-type: none"> przygotowywanie prezentacji multimedialnych, prezentowanie przy użyciu projektora multimedialnego,
--	--	--



		<ul style="list-style-type: none"> • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016; <p>4. Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none"> • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, • filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
26.	Program antywirusowy	<p>Administracja zdalna w chmurze</p> <p>1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.</p> <p>2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.</p> <p>3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.</p>



	<p>4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.</p> <p>5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.</p> <p>6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.</p> <p>7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.</p> <p>8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.</p> <p>9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.</p> <p>10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.</p> <p>11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.</p> <p>12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.</p> <p>Ochrona stacji roboczych</p> <p>1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).</p> <p>2. Rozwiązanie musi wspierać architekturę ARM64.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.</p>
--	---



		<p>5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.</p> <p>6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p> <p>7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.</p> <p>9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.</p> <p>10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).</p> <p>11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.</p> <p>15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none"> • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z
--	--	--



		<p>możliwością wykorzystania reguł utworzonych przez użytkownika,</p> <ul style="list-style-type: none"> • 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. <p>16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.</p> <p>17. 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.</p> <p>18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).</p> <p>20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>Ochrona serwera</p> <p>1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.</p> <p>2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p>
--	--	---



	<p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.</p> <p>8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.</p> <p>10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na gości (HIPS).</p> <p>11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.</p> <p>12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p>
--	--



	<p>16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.</p> <p>21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.</p> <p>Ochrona urządzeń mobilnych opartych o system Android</p> <p>1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.</p> <p>2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.</p> <p>3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).</p> <p>4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.</p> <p>5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:</p> <ul style="list-style-type: none"> • usunięcie zawartości urządzenia, • przywrócenie urządzenie do ustawień fabrycznych, • zablokowania urządzenia, • uruchomienie sygnału dźwiękowego, • lokalizację GPS. <p>6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.</p> <p>7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:</p> <ul style="list-style-type: none"> • nazwę aplikacji,
--	--



		<ul style="list-style-type: none"> • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła.
--	--	---

2.8 Centralny UPS – szt.1

Lp.	Opis wymagań funkcjonalnych	techniczno-	Wartość minimalna
1.	Technologia		online double-conversion
2.	Budowa		beztransfatorowa, prostownik IGBT. UPS musi być wyposażony w podwójny tor zasilający niezależny dla prostownika i bypassu.
3.	Moc znamionowa		30 kVA / 30kW
4.	Wyściowy współczynnik mocy (PF)		1,0
5.	Współczynnik mocy wejściowej		>0,99
6.	Napięcie wejściowe trójfazowe		400 VAC 3F + N
7.	Zakres napięcia wejściowego (przy obciążeniu 100%)		min. 310 - 460 VAC
8.	Zakres częstotliwości wejściowej		wymagana 40-70 Hz
9.	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%		nie mniejsza niż 96%
10.	THDi (dla zakłóceń harmonicznnych na wejściu poniżej 1%)		≤ 2%
11.	Tryb pracy ECO mode, zapewniający podwyższoną sprawność zasilacza		wymagany (sprawność nie mniejsza niż 99%)
12.	Możliwość rozbudowy mocy w okresie eksploatacji		do minimum 4 sztuk w układzie pracy równoległej
13.	Napięcie wyjściowe trójfazowe		400 VAC 3F + N
14.	Częstotliwość wyjściowa		50/60Hz
15.	Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass)		statyczny przełącznik oraz ręczny rozłącznik serwisowy
16.	Zewnętrzny bezprzerwowy Bypass serwisowy		wymagany bypass bezprzerwowy, z informacją o położeniu dla zabezpieczenia falownika UPS przed uszkodzeniem w przypadku nieprawidłowego użycia.
17.	Wejście komunikacyjne na UPS do podłączenia sygnalizacji położenia przełącznika zewnętrznego Bypassu serwisowego, dla ochrony falownika UPS przed przypadkowym przełączeniem		wymagane
18.	Maksymalny prąd ładowania wbudowanej ładowarki		15A



19.	Czas podtrzymania (z wewnętrznymi łańcuchami baterijnymi)	minimum 13 minut przy obciążeniu 70%
20.	Moduł baterii	baterie muszą być umieszczone w obudowie UPS
21.	Możliwość uruchamiania z baterii	wymagane
22.	Napięcie ładowania baterii (DC)	regulowane (minimalny zakres regulacji od 220V do 300V)
23.	Minimalne przeciążenie falownika w trybie pracy normalnej	do 105% prac ciągła od 105% do 110% przez 60 minut od 110% do 125% przez 10 minut od 125% do 150% przez 1 minutę powyżej 150% - 1 sekunda
24.	Wyświetlacz	5-calowy, kolorowy, dotykowy
25.	Złącze interfejsów	złącze pomiaru temperatury baterii, cyfrowe wyjścia sygnałowe – 4 szt., cyfrowe wejścia sygnałowe – 2 szt., port równoległy – 2 szt., port USB, port RS232, port REPO, złącze Mini – 2 szt
26.	Karta sieciowa SNMP	wymagana
27.	Interfejs EPO (do wyłącznika ppoż.)	wymagana – zestaw NO oraz NC
28.	Poziom hałasu w odległości 1m	< 56 dBA
29.	UPS wyposażony w zdalny wyłącznik REPO	wymagane – dostawa po stronie dostawcy UPS.
30.	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	wymagane zarówno dla zasilacza UPS jak i baterii
31.	Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	wymagane
32.	Rozłączniki manewrowe	zasilacz UPS powinien być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPS-a.
33.	Podłączenie zasilania i odbiorów	podłączenie okablowania z tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych torów do zasilania prostownika i bypassu wewnętrznego.
34.	Zasilacz wyposażony w kółka transportowe pozwalające na łatwe przemieszczanie w czasie konserwacji	wymagane



35.	Wymiary UPS nie większe niż (S x G x W)	500 x 800 x 1250 mm
36.	Instrukcja w języku polskim	wymagane

2.9 Agregat – szt.1

1. Moc wg PN-ISO 8528 lub równoważnej (+/-5%):
PRP min. 60 kVA / 48 kW
LPT (SB) min. 70 kVA / 56 kW
2. Napięcie nominalne: 3x 400 VAC / 50 Hz
3. Prędkość obrotowa: 1500 obr/min
4. Klasa regulacji (ISO 8528-5) lub równoważna: G2
5. Regulator silnika: elektroniczny
6. Agregat obudowany i wyciszony o głośności nie większej niż 70 dB z 7 metrów
7. Obudowa wykonana z profili stalowych, ocynkowanych, malowanych proszkowo
8. Maksymalne wymiary obudowy nie większe niż 2700 x 1200 x 1800 mm (D x S x W)
9. Zbiornik paliwa – min. 100l.
10. Drzwi serwisowe po obu stronach obudowy + 1 drzwi do panelu sterowania
11. Dostęp do chłodnicy poprzez przy pomocy zdejmowanego panelu
12. Spawana, stalowa rama agregatu wyposażona w zbiornik paliwa na 8 godzin pracy z pełnym obciążeniem 100% PRP
13. Dwa wskaźniki poziomu paliwa:
- cyfrowy na panelu sterowania z możliwością wyprowadzenia zdalnego odczytu
14. Wlew paliwa na obudowie, zabezpieczony na klucz
15. Możliwość dotankowania podczas pracy agregatu
16. Agregat wyposażony w układ podgrzewania cieczy chłodzącej umożliwiający start zespołu w niskich temperaturach. Układ podgrzewania musi posiadać termostat umożliwiający regulację zadanej temperatury
17. Tłumiki wibroizolacyjne pomiędzy ramą, a zespołem silnikiem i prądnicą
18. Tłumik wydechu
19. Agregat z bieżącej produkcji, nowy
20. Pompa do spuszczenia oleju silnikowego
21. Spalanie silnika Diesla nieprzekraczające 17 l/h przy 100% obciążenia PRP
22. Zalecane przez producenta silnika przeglądy nie częściej niż co 500 motogodzin.
23. Konstrukcja prądnicy: synchroniczna, samowzbudna, samoregulująca, bez-szczotkowa, jednołożyskowa
24. Sprawność prądnicy przy 100% PRP min 88,5 %
25. Panelu automatyki wyposażony w sterownik mikroprocesorowy z cyfrowym wyświetlacz LCD oraz diody sygnalizujące tryb pracy agregatu oraz sieci
26. Panel automatyki posiadający minimum 7 wejść binarnych, 7 wyjść binarnych, 3 wejścia analogowe
27. Panel sterowania przygotowany do pracy w trybach: ręcznym, automatycznym i testowym.
28. Możliwość zastosowania komunikacji zdalnej SNMP oraz MODBUS RTU
29. Wejście do podania sygnału startu i stopu z zewnętrznego układu SZR
30. Możliwość sterowania zewnętrznym układem SZR
31. Menu sterownika w języku polskim



- 32. Historia zdarzeń sterownika min. 115wpisów
- 33. Agregat wyposażony w wyłącznik 3-biegunowy

2.10 System do transmisji obrad Rady Gminy – sprzęt – 1 kpl.

Zestaw sprzętowy dla 19 osób (15 radnych w tym Przewodniczący, Wójt, Sekretarz, Skarbnik, pracownik obsługi)

System transmisji z obrad (2 kamery, komputer do transmisji, monitor, montaż po stronie Wykonawcy)

1. Kamera do transmisji IP – 2 sztuki
 - 1.1. Praca w standardzie TCP/IP,
 - 1.2. przetwornik 1/2.8" STARVIS,
 - 1.3. obiektyw w zakresie 5-80 mm,
 - 1.4. zoom optyczny 16x,
 - 1.5. protokoły sieciowe: IPv4, SSL, RTSP, DHCP, UPnP,
 - 1.6. zasilanie PoE
 - 1.7. ONVIF.
2. Centrala system konferencyjnego – 1 szt.
 - 2.1. Jednostka sterująca systemu konferencyjnego.
 - 2.1.1. Funkcjonalność i parametry techniczne:
 - 2.1.1.1. Kontrola otwartych mikrofonów pozwalająca wybrać minimum 4 otwarte mikrofony
 - 2.1.1.2. Wbudowany rejestrator dźwięku może nagrywać dyskusję w formacie MP3 do pamięci wewnętrznej lub pamięci USB
 - 2.1.1.3. Napięcie zasilania sieciowego od 100 do 240 VAC \pm 10%
 - 2.1.1.4. Maks. od 1,6 A (100 VAC) do 0,7 A (240 VAC)
 - 2.1.1.5. Liczba pulpitów dyskusyjnych na jednostkę sterującą minimum 40
 - 2.1.1.6. Minimalna częstotliwość próbkowania 44,1 kHz
 - 2.1.1.7. Maksymalna waga 3.4 kg
 - 2.1.1.8. Materiał metal lakierowany
 - 2.1.1.9. Metoda montażu stołowy lub w szafie typu Rack 19"
 - 2.1.1.10. Wymiary maksymalne (wys. X szer. X gł.) 45 x 483 x 300
 - 2.1.1.11. Temperatura pracy od 5 do 45°C
 - 2.1.1.12. Złącza umieszczone na obudowie:
 - 2.1.1.12.1. Z przodu jednostki:
 - 2.1.1.12.1.1. Minimum 1 x złącze USB
 - 2.1.1.13. Z tyłu jednostki:
 - 2.1.1.13.1. Minimum 1 x wyjście analogowe
 - 2.1.1.13.2. Minimum 1 x wejście analogowe
 - 2.1.1.13.3. Minimum 1 x złącze Ethernet RJ45 do komunikacji
 - 2.1.1.14. Kontrola dyskusji odbywa się poprzez wybór jednego z dostępnych trybów dyskusji:
 - 2.1.1.14.1. Tryb otwarty - uczestnicy mogą mówić, naciskając przycisk na swoim mikrofonie. Gdy maksymalna liczba otwartych mikrofonów



zostanie osiągnięta, następny uczestnik, który naciśnie przycisk swojego mikrofonu, zostanie dodany do listy oczekujących. Pierwszy uczestnik z listy oczekujących będzie mógł mówić, gdy zostanie wyłączony któryś z aktywnych mikrofonów

2.1.1.14.2. Tryb z wyciszaniem - uczestnicy mogą wyciszać się wzajemnie przez włączanie swojego mikrofonu. Gdy maksymalna liczba otwartych mikrofonów zostanie osiągnięta, następny uczestnik, który naciśnie przycisk na swoim mikrofonie, zdezaktywuje mikrofon, który był najdłużej aktywny (mikrofon, który posiada przewodniczący nie jest uwzględniany w liczbie otwartych mikrofonów i dlatego nie może go wyciszyć żaden inny uczestnik).

2.1.1.14.3. Tryb aktywacji głosowej - uczestnicy mogą aktywować swoje mikrofony, mówiąc do nich. Mikrofon może być czasowo wyciszony poprzez naciśnięcie i przytrzymanie przycisku mikrofonu.

3. Zestaw mikrofonowy – 1 szt.

Minimalne parametry techniczne

Nazwa	Parametr
Typ urządzenia	zestaw mikrofonu bezprzewodowego
Częstotliwość nośna	672- 692 MHz
Pasmo przenoszenia	50- 18 000 Hz
Kanały wejściowe	1
THD	< 0.5 %
Dynamika	120 dB
Stosunek S/ N RF	105 dB
Dopuszcz. temp. Otoczenia	0- 40 °C
Moc nadajnika	< 25 mW/ 2.5 mW (EIRP)
Zasięg	≈ 50 m
Nadajnik, zasilanie	2 x 1.5 V bateria AA
Nadajnik, głębokość	52 mm
Nadajnik, wysokość	52 mm
Nadajnik, głębokość	275 mm
Nadajnik, waga	235 g
Odbiornik, wyjścia audio	350 mV/ 10 kΩ (6.3 mm) 25 mV/ 10 kΩ (XLR, sym.)
Odbiornik, zasilanie	z doł. zasilacza
Odbiornik, szerokość	152 mm
Odbiornik, wysokość	38 mm
Odbiornik, głębokość	120 mm
Odbiornik, waga	482 g
Odbiornik, złącza	1 x 6.3 mm, niesym. 1 x XLR, sym.

4. Mikrofon konferencyjny bezprzewodowy – 19 szt./Jednostki konferencyjne (pulpity dyskusyjne) –

4.1. Szyjka mikrofonu o długości minimum 480 mm oraz minimum jednym przegubie.

4.2. Przycisk aktywacji mikrofonu musi umożliwiać uczestnikowi włączanie/wyłączanie mikrofonu lub (w zależności od trybu aktywacji mikrofonu) zgłoszenie chęci



- wypowiedzi. Wokół, nad lub od spodu przycisku musi znajdować się podświetlany wskaźnik LED informujący o aktywnym mikrofonie (preferowany kolor czerwony).
- 4.3. Wbudowane 3,5 mm stereofoniczne gniazdo słuchawkowe
 - 4.4. Odporność na zakłócenia z sieci GSM
 - 4.5. Sygnalizacja świetlna umieszczona na szyjce mikrofonowej wskazująca włączenie i żądanie zabrania głosu (np. pierścień lub wskaźniki LED w dwóch kolorach – preferowany zielony oraz czerwony)
 - 4.6. Szeregowa topologia połączeń, każdy z pulpitów musi posiadać gniazdo przelotowe.
 - 4.7. Wbudowany wysokiej jakości głośnik
 - 4.8. Możliwość konfiguracji dowolnego pulpitu jako jednostki przewodniczącego lub dostarczenie pulpitu dedykowanego dla przewodniczącego.
 - 4.9. Pasma przenoszenia urządzenia obejmuje zakres częstotliwości od 200 Hz do 12,5 kHz
 - 4.10. Impedancja obciążenia słuchawek $> 8 \Omega < 1 \text{ k} \Omega$
 - 4.11. Maksymalne wymiary urządzenia bez mikrofonu (wys. X szer. X gł.) 65 x 210 x 150 mm
 - 4.12. Ciężar ok. 1 kg
 - 4.13. Materiał plastik, metal
 - 4.14. Temperatura pracy od 0 do 35°C

2.11 Szkolenia TiK typ I – 120 godzin

1. Wymagania minimalne dla szkoleń TIK typ I

Szkolenia/Asysta stanowiskowa ma obejmować 120 godzin szkoleniowych w ujęciu max. 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 15 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.

Asysta musi zostać podzielona na bloki dziedzinowe:

- Blok pierwszy (10 dni – 80 godzin) musi zostać przeprowadzony w centrum kompetencyjnym (poza terenem Zamawiającego) i mieć na celu zapoznanie uczestników z elementami technologicznymi, które składają się na całość autorskiego rozwiązania.
- Blok drugi (5 dni – 40 godzin) musi zostać przeprowadzony w miejscu instalacji (Urządzie Gminy) i musi ściśle dotyczyć podstawowych procedur administracyjnych, które są typowe dla codziennej pracy administratora celem zapewnienia poprawnej pracy rozwiązania sprzętowego jako platformy teleinformatycznej na potrzeby rozwiązania związanego z oprogramowaniem systemu.

Zakres asysty stanowiskowej:

- Architektura serwerowa;
- Architektura macierzowa;
- Architektura sieci LAN;
- System wirtualizacji danych;
- System backupu i replikacji danych;
- Administrowania i obsługi systemu operacyjnego (domena, usługa katalogowa) z zakresu zaoferowanego rozwiązania – oprogramowanie domenowe.



- Punkt styku z Internetem – firewall.

Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego.

Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego.

2.12 Opracowanie procedur bezpieczeństwa informacji i przetwarzania danych

W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy oraz wdroży Kompleksowy System Zarządzania Bezpieczeństwem Informacji (KSZBI). Usługa obejmuje analizę, projektowanie, implementację i szkolenie związane z wdrożeniem SZBI w jednostce. Celem usługi jest zwiększenie ochrony danych i informacji w organizacji na poziomie technicznym oraz organizacyjnym, zapewnienie zgodności z obowiązującymi przepisami prawnymi, poprawa ogólnego poziomu bezpieczeństwa informacji zgodnie z normami wyrażonymi w PN ISO/IEC 27001 lub równoważnymi w załączeniu KSZBI zawierać będzie co najmniej:

Dokumentacja zarządzania systemem zarządzania bezpieczeństwem informacji (uwzględniająca poniższe zagadnienia):

- Zasady dotyczące korzystania z systemu zakres, zasoby, ciągłe doskonalenie;
- Procedury przeprowadzania audytów, zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników.
- Procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania.
- Procedury wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania.

Dokumentacja dotycząca zabezpieczeń systemu zarządzania bezpieczeństwem informacji w obszarach (uwzględniająca poniższe zagadnienia):

- Zasady bezpiecznego przetwarzania informacji przez pracowników
- Zabezpieczenie stacji roboczych
- Zasady klasyfikacji informacji i postępowania z informacjami klasyfikowanymi
- Zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień
- Zasady zarządzania dostępem do usług informatycznych, w tym usług sieciowych
- Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami
- Zasady publikacji informacji
- Zasady wymiany danych z podmiotami zewnętrznymi
- Zasady wewnętrznej wymiany danych
- Zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach



- Zasady wprowadzania zmian w przetwarzaniu informacji, w szczególności z wykorzystaniem systemów informatycznych, z uwzględnieniem testowania bezpieczeństwa wprowadzanych rozwiązań
- Wytyczne w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych
- Zasady zgłaszania podatności w mechanizmach przetwarzających informacje
- Zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji
- Zasady kontroli bezpieczeństwa informacji.

Zamawiający wymaga by KSZBI zawierał:

- 1) Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzi następujące dokumenty:
 - a) Polityka Bezpieczeństwa Informacji;
 - b) Polityka ochrony danych osobowych;
 - c) Instrukcja zarządzania systemem informatycznym;
 - d) Polityka zarządzania ciągłością działania;
 - e) Procedura zarządzania incydentami cyberbezpieczeństwa
 - f) Analiza ryzyka w zakresie Bezpieczeństwa Informacji;
- 2) W ramach dokumentacji SZBI ujęte zostaną następujące procedury:
 - a) procedury korzystania z urządzeń mobilnych
 - b) procedury pracy zdalnej
 - c) postępowanie z nośnikami
 - d) procedury kontroli dostępu
 - e) zabezpieczenie pomieszczeń i obiektów
 - f) procedury czystego biurka
 - g) procedury czystego ekranu
 - h) procedury kopii zapasowych
 - i) procedury ochrony logów
 - j) bezpieczeństwo komunikacji
 - k) zarządzanie bezpieczeństwem sieci
 - l) przesyłanie informacji
 - m) plany ciągłości działania
 - n) procedury zarządzania incydentami
 - o) prywatność i ochrona danych osobowych
 - p) szacowanie ryzyka w obszarze bezpieczeństwa informacji.

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zleceniodawcy w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami oraz wszelkich innych informacji uzyskanych w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji. Doradztwo dotyczące czynności wdrażających dokumentację nastąpi po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji KSZBI.

2.13 Instalacja i konfiguracja (Platforma sprzętowa) – 250 RBH

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.		
1.	Usługi	<p>Celem prac jest przygotowanie środowiska teleinformatycznego – platformy sprzętowej, na potrzeby realizacji elementów Zintegrowanego Systemu Informatycznego i cyberbezpieczeństwa, dla świadczonych e-usług. Zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.</p> <p>Część sprzętowa powinna zostać oparta na rozbudowie istniejącego systemu wirtualizacji i backupu zasobów IT.</p> <p>Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania wdrożenia, migracji do nowego środowiska itp. Dostęp do infrastruktury będzie możliwy pod nadzorem 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>
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"> 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach RACK w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 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.



		<p>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).</p> <p>9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).</p> <p>10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem:</p> <ol style="list-style-type: none"> Stworzenia połączeń sieci LAN pomiędzy przełącznikami. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie, co najmniej n+1. Połączenia muszą wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	Instalacja i konfiguracja oprogramowania	<ol style="list-style-type: none"> Instalacja i konfiguracja istniejącego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. Zamawiający posiada licencje jedną wolną licencję na wirtualizator firmy Vmware. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu. Instalacja 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). Instalacja i konfiguracja systemów operacyjnych dla serwerów wirtualnych. Zarządzania infrastrukturą IT Instalacja i konfiguracja oprogramowania do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR).
4.	Konfiguracja przełączników/ sieci LAN:	<p>Re/Konfiguracja przełączników w zakresie:</p> <ol style="list-style-type: none"> Przeprowadzenie audytu obecnej topologii oraz konfiguracji. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych, aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).



		<ul style="list-style-type: none"> c. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy) d. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na dostarczonych urządzeniach firewall - klaster. e. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. f. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; g. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). h. Testowanie obsługi ruchu sieciowego. i. Testowanie skuteczności zabezpieczeń.
5.	Konfiguracja elementów bezpieczeństwa sieciowego.	<p>Konfiguracja/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. 3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Włączenie dostarczonego urządzenia do sieci LAN urzędu – stworzenie klastera HA. 5. Konfiguracja dostarczonych systemów Firewall: <ul 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: <ul style="list-style-type: none"> a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;



		<ul style="list-style-type: none"> 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 <p>7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.</p> <ul 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. <p>8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej.</p> <p>9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia.</p> <p>10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.</p> <p>11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC</p> <p>12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaze Zamawiający) dla każdej z poniższych funkcjonalności:</p> <ul style="list-style-type: none"> a. kontrola dostępu - zaporę 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] 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)
--	--	--



		<ul style="list-style-type: none"> 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.	Serwer	Zamawiający wymaga instalacji i konfiguracji dostarczonego serwera celem stworzenia bazy sprzętowej repliki dla istniejącego klastra niezawodnościowego i wydajnościowego stworzonego na bazie istniejących serwerów i oprogramowania do wirtualizacji.
7.	Backup	<p>W ramach projektu przewiduje się wykorzystanie istniejącego serwera backupu (Fujitsu PY RX2540 M7) oraz NAS na miejsce przechowywanie backupu.</p> <p>Na serwerze backupu należy zainstalować oprogramowanie do trzymania kopi zapasowych (Hardened repository), które jest wspierane przez zaoferowany system backupu. Zarządzanie środowiskiem backupem ma mieć miejsce z poziomu maszyny wirtualnej z jednego centralnego miejsca, tego samego jak dla serwerów wirtualizacyjnych.</p> <p>System musi zostać podłączony do macierzy produkcyjnej, musie posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego.</p> <p>Dostarczony serwer ma zostać użyty do przechowywania repliki on-line maszyn wirtualnych na lokalną platformę wirtualizacyjną – odmiejscowiona lokalizacja.</p> <p>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 system NAS i chmurę, gdzie będzie można skorzystać z replikacji danych – przesłania backupu dyskowego na zasób zdalny.</p> <p>Mechanizm podłączenia</p> <ol style="list-style-type: none"> 1. Konfiguracja i podłączenie serwera backupu 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

		<p>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.</p> <p>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> <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>Schemat przedstawia infrastrukturę IT z serwerami wirtualnymi, systemem wirtualizacji, macierzą dyskową, serwerem backupu, centralnym systemem logów, przełącznikami LAN, klasterem firewall, NAS, internetem i chmurą backupu. Wskazano również elementy do zakupu: Serwer #3, Centralny system logów, Firewall #1 i #2, oraz UPS i AGREGAT.</p>
<p>8.</p>	<p>Macierz dyskowa</p>	<p>Istniejąca macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dostarczone w projekcie jak i już istniejące w tym oprogramowanie dziedzinowe.</p> <p>Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów np.: wirtualizacyjnych zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. Macierz</p>



		należy zintegrować z istniejącym rozwiązaniem firmy Fujitsu – model DX60S5.
9.	UPS, Agregat.	W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanych urządzeń UPS i Agregat do sieci elektrycznej Urzędu celem zabezpieczenia pomieszczenia serwerowni. Wszystkie koszty z tym związane np.: modernizacji istniejącej instalacji elektrycznej muszą zostać przewidziane i uwzględnione w ofercie Wykonawcy.
10.	Migracja danych	Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Dane (systemy dziedziczne) muszą zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzicznych.
11.	Rekonfiguracja środowiska wirtualizacyjnego.	Zamawiający wymaga rekonfiguracji środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta – jeżeli jest taka potrzeba. 2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 4. Instalacja oprogramowania wirtualizacyjnego na dostarczonym serwerze. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracja i podłączenie serwera wirtualizacyjnego do zasobu dyskowego. Zamawiający wymaga (jeżeli to możliwe) takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu



	<p>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.</p> <ol style="list-style-type: none"> 7. Konfiguracja i podłączenie serwera wirtualizacyjnego do sieci LAN. Zamawiający wymaga, aby serwer wirtualizacyjny 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. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie replikacji wirtualnych maszyn ze środowiska produkcyjnego do zapasowego. 10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym – jeżeli jest wymagane.. 11. Konfiguracja klastra wysokiej dostępności: <ol style="list-style-type: none"> a. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika. b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn. c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera. 12. Weryfikacja działania klastra wysokiej dostępności. 13. Migracja istniejącej infrastruktury do środowiska wirtualnego. 14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
--	---



12.	Rekonfiguracja systemu zarządzania kopiami zapasowymi.	<ol style="list-style-type: none"> 1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na serwerze backupu (wgranie licencji). 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;
-----	--	--



		<ul style="list-style-type: none"> 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. Zapełnienia mail-slotu. <p>8. Uruchomienie testowych zadań backupu.</p> <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> <ul style="list-style-type: none"> a. serwer backupu., b. 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 istniejącą 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.	Oprogramowa nie do monitorowani a i analizy cyberbezpiecz eństwa (SIEM/SOAR)	<p>1. Proces wdrożenia systemu określony powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne wdrożenie rozwiązania w okresie 3 miesięcy.</p> <p>2. Proces wdrożeniowy podzielony zostanie na obszary:</p> <ul style="list-style-type: none"> a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji). b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM. c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i



		<p>podatności w ramach zainstalowania modułu SOAR.</p> <p>3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji, na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:</p> <ol style="list-style-type: none"> Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac). Uruchomienie systemu w infrastrukturze zamawiającego, w tym: <ul style="list-style-type: none"> konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu, przygotowanie przez Zamawiającego połączenia zdalnego, instalację lub import maszyny wirtualnej typu „software appliance”, aktywację licencji, wstępną konfigurację, import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN). Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym: <ul style="list-style-type: none"> przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu, uruchomienie reguł wykrywania. Prace audytowe, w tym: <ul style="list-style-type: none"> pasywną analizę transmisji sieciowej: <ul style="list-style-type: none"> o ruch z/do serwerów webowych i aplikacyjnych, o ruch z/do serwerów baz danych, o ruch z/do serwerów pocztowych, o ruch z/do kontrolerów domenowych, o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP), o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji. konsultacje w ramach otrzymanych wyników, zebranie danych audytowych wymaganych do sporządzenia raportu. Analizę podatności, w zakresie: <ul style="list-style-type: none"> integracji po API ze wskazanym przez zamawiającego
--	--	---



	<p>komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source,</p> <ul style="list-style-type: none"> • przygotowanie reguł priorytetów i importu krytycznych podatności. <p>f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:</p> <ul style="list-style-type: none"> • zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia, • potencjalne wektory ataków dla wykrytych zagrożeń, • wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków, • rekomendacja zabezpieczeń, • zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń. <p>4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:</p> <p>a. Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują:</p> <ul style="list-style-type: none"> • zapory sieciowe w punktach styku z siecią Internet (Firewall brzegowy), • sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam), • centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR), • kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym, • systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA), • system SIEM, • źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji. <p>b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą.</p>
--	--



	<p>c. Podłączenie reguł detekcji.</p> <p>d. Podłączenie i konfiguracja mechanizmów UEBA:</p> <ul style="list-style-type: none"> • integracja z Active Directory, • adaptacja profili użytkowników UBA, • adaptacja profili hostów EBA, • import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia. <p>5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać:</p> <ul style="list-style-type: none"> a. Import gotowych scenariuszy obsługi. b. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi. c. Konfigurację mechanizmów powiadamiania. <p>6. Usługa konsultacji powdrożeniowej, świadczona przez dedykowanego inżyniera w ramach okresu wsparcia musi w szczególności uwzględniać:</p> <ul style="list-style-type: none"> a. przygotowanie i modyfikację formularzy raportów; b. tworzenie i edycję parserów; c. przygotowywanie nowych reguł bezpieczeństwa; d. modyfikację dostępnych reguł i ich dostrojenie; e. wsparcie w procesie aktualizacji systemu; f. tworzenie i edycję nowych scenariuszy reakcji; g. tworzenie i dostosowanie dashboardów danych. <p>7. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.</p> <p>Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 5 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego</p>
--	---

		wspomniane umiejętności wydany przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.
14.	Testowanie i modyfikacja parametrów infrastruktury sieciowej.	<ol style="list-style-type: none"> 1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. 2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie mechanizmów replikacji danych. 4. Testowanie dostępu publicznego do zasobów. 5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach.
15.	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>
16.	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"> a. zastosowanej technologii serwerów

		<ul style="list-style-type: none">b. zastosowanej technologii pamięci masowejc. wirtualizacjid. systemu backupue. zastosowanych rozwiązań aplikacyjnych <p>Wykonawca zapewni również wsparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.</p>
17.	Opracowanie dokumentacji powykonawczej	<p>Zamawiający wymaga opracowania dokumentacji technicznej powykonawczej.</p> <ul style="list-style-type: none">1. Konfiguracja urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).2. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.3. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.4. Hasła dostępowe do dostarczonych i zainstalowanych systemów.

2.14 Wodomierze – szt. 296

5.6 Wodomierze – szt. 296

Przedmiotem zamówienia jest dostawa i montaż 296 szt. wodomierzy z wybudowanym modułem radiowym z systemem odczytu zdalnego, zgodnych z określonymi wymaganiami technicznymi i eksploatacyjnymi o minimalnym progu rozruchu dla pomiaru zużycia wody – 0,75 l/h.

Celem wdrożenia jest zapewnienie nowoczesnej, zdalnej obsługi pomiaru zużycia wody oraz integracja systemu z istniejącymi infrastrukturami informatycznymi zamawiającego.

1. Zakres dostawy

W ramach realizacji zamówienia przewidziana jest dostawa wodomierzy statycznych DN20 R \geq 250, Q₃₋₄ L-130/DN 15 R \geq 250 Q₃ – 2,5 L-110, według zapotrzebowania Zamawiającego, wyposażonych w moduł radiowy WMBus oraz LoRaWAN, Dodatkowo każdy wodomierz zostanie zaopatrzony w plombę wodomierzową zatrzaskową z indywidualną numeracją. Dostawca dostarczy dokumentację obejmującą dokumentację techniczną, karty katalogowe, certyfikaty oraz dokumentację oprogramowania.

2. Wymagania techniczne wodomierzy

Wodomierze muszą posiadać statyczny układ pomiarowy, pozbawiony części ruchomych, co zapewni długotrwałą i bezawaryjną pracę. Konstrukcja wodomierza powinna być niezależna



od przewodności elektrycznej wody, a jego obudowa wykonana z mosiądzu, posiadającego stosowne atesty higieniczne do kontaktu z wodą pitną. Wodomierze powinny być odporne na temperatury w zakresie od +5°C do +55°C, a ich liczydła powinny być wyposażone w elektroniczny wyświetlacz o minimalnym zakresie wskazań 999999,999 m³.

3. Integracja i funkcjonalność systemu

System odczytu zdalnego musi umożliwiać bieżące monitorowanie zużycia wody, identyfikację przepływów wstecznych, wykrywanie ingerencji oraz przekroczeń parametrów granicznych. Moduły radiowe powinny obsługiwać komunikację dwukierunkową zgodną z LoRaWAN oraz Wireless M-Bus, zapewniając wysoką jakość przesyłu danych oraz ich szyfrowanie. Wodomierze muszą być kompatybilne z systemem inkasenckim oraz umożliwiać integrację z platformą zarządzającą SPIDAP Cloud.

4. Wymagania dotyczące szczelności i trwałości

Korpus wodomierza powinien posiadać oznaczenia materiałowe oraz numer seryjny, umożliwiające jednoznaczną identyfikację. Klasa szczelności obudowy powinna odpowiadać IP68, a liczydło być odporne na zaparowanie i zanieczyszczenia. System pomiarowy nie może być wypełniony żywicą, lecz umożliwiać rozłożenie na elementy poddawane recyklingowi.

5. Wymagania normatywne Wodomierze muszą spełniać wymagania norm:

- EN-ISO 4064-1÷5:2014(E) lub równoważna – wodomierze do wody zimnej pitnej i wody gorącej,
- OIML R49:2013 – wodomierze przeznaczone do pomiaru zimnej wody pitnej i wody ciepłej,
- Dyrektywa 2014/32/EC Parlamentu Europejskiego dotycząca przyrządów pomiarowych,
- EN 13757-4:2019 – komunikacja bezprzewodowa M-Bus,
- WELMEC 7.2 – zasady metrologiczne dla urządzeń pomiarowych lub równoważne.

6. Wymagania dotyczące systemu odczytu radiowego S

System powinien umożliwiać odczyt danych w trybach wM-Bus i LoRaWAN, zapewniając pełną rejestrację danych pomiarowych i diagnostycznych. Wodomierze powinny obsługiwać mechanizm adaptacyjnej regulacji transmisji danych (ADR), a dane powinny być szyfrowane zgodnie z OMS3 encryption 5.

7. Oprogramowanie i wsparcie techniczne

Dostawca zobowiązany jest do dostarczenia oprogramowania inkasenckiego SPIDAP Mobile oraz jego integracji z platformą SPIDAP Cloud. System powinien zapewniać harmonogramowanie zadań, analizę zużycia oraz eksport danych do plików CSV. Oprogramowanie powinno być zgodne z systemami operacyjnymi Android oraz posiadać wsparcie dla komunikacji NFC i Bluetooth.

Dostawca zapewni wsparcie techniczne, szkolenie użytkowników oraz bieżące aktualizacje systemu. Wszystkie urządzenia muszą być fabrycznie nowe, posiadać aktualne certyfikaty legalizacyjne oraz gwarancję na co najmniej 5 lat.



5.12 Przepływomierz – szt. 2

Zamawiający zamierza dokonać opomiarowania zrzutu ścieków na oczyszczalniach ścieków w Nozdrzcu i Siedliskach za pomocą przepływomierzy elektromagnetycznych do pomiaru przepływu cieczy w zamkniętych instalacjach rurociągowych bezciśnieniowych. Zamawiający zamierza również dokonać opomiarowanie wody przeznaczonej do płukania filtrów na Stacji Uzdatniania Wody w Wesolej. Zakres pomiarowy przepływomierzy: 60-2 000 l/min. Dokładność pomiaru: $\pm 0,5\%$. Zakres ciśnienia procesowego: maks. 16 bar Zakres temperatury procesowej: 0-60 °C

Pomiar przepływ cieczy przewodzących czystych i zanieczyszczonych, agresywnych i obojętnych chemicznie oraz przewodzących mieszanin i pulp.

Przedmiotem zamówienia jest dostawa i montaż przepływomierza elektromagnetycznego DN 65 (urządzenie pomiarowe służące do mierzenia przepływu objętościowego cieczy przewodzących (np. wody, ścieków, cieczy technologicznych) w rurociągach o nominalnej średnicy DN 65 (czyli 65 mm). Urządzenie musi zapewniać precyzyjny pomiar objętościowy przepływu wody czystej i uzdatnionej.

5.12.1 Model – 6 DN 65

Wymagania techniczne obejmują:

- Średnica nominalna DN 65,
- Zakres pomiarowy Q_{min} - Q_{max} dostosowany do warunków eksploatacyjnych zamawiającego,
- Dokładność pomiaru zgodna z normami EN ISO 4064 lub równoważnymi,
- Obudowa i elementy pomiarowe odporne na korozję,
- Interfejs komunikacyjny kompatybilny z systemem LoRaWAN lub M-Bus,
- Certyfikaty i atesty do stosowania w instalacjach wodociągowych.

5.12.2 Model – 6 DN 100

Wymagania techniczne obejmują:

- Średnica nominalna DN 100,
- Zakres pomiarowy Q_{min} - Q_{max} dostosowany do warunków eksploatacyjnych zamawiającego,
- Dokładność pomiaru zgodna z normami EN ISO 4064 lub równoważnymi,
- Obudowa i elementy pomiarowe odporne na korozję,
- Interfejs komunikacyjny kompatybilny z systemem LoRaWAN lub M-Bus,
- Certyfikaty i atesty do stosowania w instalacjach wodociągowych.

Przez równoważne rozwiązanie uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować



Fundusze Europejskie
dla Podkarpacia



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



PODKARPACKIE
przestrzeń otwarta

rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową

UWAGA:

Dostawca zobowiązuje się do dostarczenia urządzenia wraz z dokumentacją techniczną, atestami oraz instrukcją eksploatacyjną.