|  |  |
| --- | --- |
| Numer sprawy: Or.271.2.2025 | Działoszyce, dnia 30.04.2025 r. |
| Szczegółowy Opis Przedmiotu Zamówienia na dostawy związane z realizacją projektu„Cyberbezpieczny Samorząd” |

Spis treści

[1. Zestawienie ilościowe. 3](#_Toc196644974)

[2. Zasada równoważności rozwiązań i neutralności technologicznej. 4](#_Toc196644975)

[3. Przedmiot zamówienia dla części nr 1. 7](#_Toc196644976)

[3.1. Wymagania ogólne. 7](#_Toc196644977)

[3.2. Zakup serwera (1 szt.). 10](#_Toc196644978)

[3.3. Zakup access point (4 szt.). 13](#_Toc196644979)

[3.4. Zakup przełączników sieciowych (2 szt.) 14](#_Toc196644980)

[3.5. Rozbudowa infrastruktury UTM (1 szt.). 14](#_Toc196644981)

[4. Przedmiot przedmiotu zamówienia części nr 2. 18](#_Toc196644982)

[4.1. Wymagania ogólne. 18](#_Toc196644983)

[4.2. Zakup oprogramowania do agregowania logów (1 szt.). 22](#_Toc196644984)

[4.3. Zakup oprogramowania backup (1 szt.). 23](#_Toc196644985)

[4.4. Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami (1 szt.). 26](#_Toc196644986)

[4.5. Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem) (1 szt.). 35](#_Toc196644987)

# Zestawienie ilościowe.

Część nr 1 – Dostawa sprzętu i oprogramowania informatycznego.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Zakup serwera | 1 szt. |
| 2. | Zakup access point | 4 szt. |
| 3. | Zakup przełączników sieciowych | 2 szt. |
| 4. | Rozbudowa infrastruktury UTM | 1 szt. |

Część nr 2 – Dostawa oprogramowania informatycznego.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Zakup oprogramowania do agregowania logów | 1 szt. |
| 2. | Zakup oprogramowania backup | 1 szt. |
| 3. | Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami | 1 szt. |
| 4. | Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem) | 1 szt. |

# Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. 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 lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. 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 rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających 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.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

# Przedmiot zamówienia dla części nr 1.

# Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
12. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia sprzętu i oprogramowania – wymagania minimalne:
13. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego sprzętu i oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
14. scenariusze testowe, procedury oraz wzory raportów testów,
15. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
16. opis koncepcji realizacji prac,
17. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
18. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
19. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 15 dni kalendarzowych od dnia zawarcia umowy,
20. Zamawiający w terminie nie dłuższym niż 5 dni kalendarzowych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
21. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni kalendarzowych od dnia ich otrzymania,
22. Zamawiający w terminie 5 dni kalendarzowych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
23. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
24. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
25. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
26. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
27. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
28. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
29. Instruktaże w zakresie dostarczonego sprzętu i oprogramowania – wymagania minimalne.
30. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
31. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
32. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 2 osoby).
33. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
34. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.
35. Wymagania licencyjne dla dostarczonego oprogramowania:
36. Licencjobiorcą wszystkich licencji będzie Gmina Działoszyce.
37. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
38. Licencje muszą obowiązywać do dnia 14.03.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania (pod warunkiem, że w dalszej części dokumentu Zamawiający nie określił innego okresu ważności licencji).
39. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
40. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
41. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
42. Wymagania gwarancyjne i serwisowe dla dostarczonego sprzętu i oprogramowania w formie licencji czasowych lub subskrypcyjnych:
	1. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 14.03.2026 r. (pod warunkiem, że w dalszej części dokumentu Zamawiający nie określił innego okresu ważności licencji).
	2. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
	3. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 14.03.2026 r.
	4. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta lub Wykonawcę w języku polskim i objąć musi minimum:
		1. dostęp do najnowszych wersji oprogramowania,
		2. wsparcie telefoniczne w zakresie oferowanego sprzętu i oprogramowania zespołu inżynierów technicznych,
		3. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu sprzętu i oprogramowania,
		4. przyjmowanie i realizacja zgłoszeń serwisowych,
		5. doradztwo techniczne w zakresie konfiguracji i optymalizacji sprzętu i oprogramowania,

w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.

1. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

# Zakup serwera (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowany jeden procesor wielordzeniowy klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiający osiągnięcie przez serwer wyniku co najmniej 195 punktów w teście SPECrate2017\_fp\_base według wyników publikowanych na stronie [www.spec.org](http://www.spec.org). Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 128 GB, płyta główna musi obsługiwać do min. 1 TB pamięci RAM, co najmniej 10 slotów na pamięć wolnych.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Gniazda PCIe: co najmniej jeden wolny slot w celu możliwości rozbudowy serwera.
7. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024.
8. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 - porty nie mogą być osiągnięte poprzez karty w slotach PCIe.
9. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 3 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 1,9 TB każdy. Zainstalowane dwa dyski SSD SATA o pojemności min. 960 GB Hot-Plug. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
10. Kontroler RAID: Sprzętowy kontroler dyskowy, umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
11. Wsparcie dla dysków samoszyfrujących.
12. Wbudowane porty: min. 1 zewnętrzny port VGA, min. 3 zewnętrzne porty USB, w tym co najmniej 1 port USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy. Dodatkowo min. jeden port dedykowany dla karty zarządzającej. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
13. Wentylatory: Redundantne typu Hot Plug.
14. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 700 W każdy.
15. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
	1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
	2. zdalne monitorowanie i informowanie o statusie serwera,
	3. szyfrowane połączenie oraz autentykacje i autoryzację użytkownika,
	4. możliwość podmontowania zdalnych wirtualnych napędów,
	5. wirtualną konsolę z dostępem do myszy, klawiatury,
	6. wsparcie dla IPv6,
	7. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
	8. integracja z Active Directory,
	9. wsparcie dla dynamic DNS.
16. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
	1. wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
	2. blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
	3. moduł TPM 2.0;
	4. możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera;
17. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard w najnowszej wersji oferowanej przez producenta na dzień składania ofert wraz z 30 licencjami dostępowymi umożliwiającymi korzystanie przez 30 użytkowników oraz 10 licencji umożliwiających zdalny dostęp lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania klasy Microsoft Windows Serwer Standard:

* 1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
	2. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
	3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny.
	4. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
	5. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
	6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
	7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
	8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
	9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
	10. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
	11. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
	12. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
	13. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
	14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
	15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
	16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
	17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
	18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
	19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
	20. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
	21. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
	22. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
	23. O ile to konieczne ze względu na licencjonowanie producenta oferowanego serwerowego systemu operacyjnego Zamawiający wymaga dostarczenia licencji dostępowych dla 30 użytkowników oraz 10 licencji umożliwiających zdalny dostęp.
1. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
2. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań w zakresie określonym powyżej.
3. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera.

# Zakup access point (4 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa umożliwiająca montaż na ścianie.
2. Co najmniej dwie anteny dookólne, Zamawiający dopuszcza anteny wewnętrzne.
3. Standard komunikacji: Wi-Fi 6 802.11a/b/g/n/ac/ax.
4. Pracujący na dwóch częstotliwościach 2,4 GHz i 5 GHz.
5. Min. przepustowość na częstotliwości 2,4 GHZ: min. 500 Mb/s.
6. Min. przepustowość na częstotliwości 5 GHZ: min. 4 Gbps.
7. Inne: obsługa RADIUS, obsługa PoE, w zestawie adapter umożliwiający podłączenie bez przełącznika PoE.
8. Standardy komunikacyjne: IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n.
9. Funkcje: technologia 2x2 MIMO, obsługa TWT, technologia MU-MIMO, agregacja pakietów A-MPDU, agregacja pakietów A-MSDU, technologia SU-MIMO.
10. Liczba klientów bezprzewodowych: min. 200.
11. Interfejsy urządzenia: min. 4 x GbE RJ45 wyjściowe, 1 x GbE RJ45 wejściowe.
12. Obsługiwane algorytmy szyfrujące: WPA2, WPA3.
13. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany Access Point spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta Access Point lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany access point wymagań w zakresie określonym powyżej.
14. Co najmniej 24 miesiące gwarancji producenta.

# Zakup przełączników sieciowych (2 szt.)

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzany przełącznik L3.
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 170 Gbps.
4. Prędkość przekazywania: min. 100 Mpps.
5. Rozmiar tablicy MAC: min. 32 000 wpisów.
6. Dostępne interfejsy: min. 48 x RJ45 10/100/1000 Mbps; 4 x sloty SFP+ 10G.
7. Obsługa PoE+ na wszystkich 48 portach RJ-45.
8. Obsługiwane standardy komunikacyjne: IEEE 802.1AX, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1v, IEEE 802.1w, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az, IEEE 802.3u, IEEE 802.3x
9. Dodatkowo obsługa: QoS, VLAN, ACL, DHCP, IPv4, IPv6, Telnet, SNMP v1/v2c, Http/Https, SSL, SSHv1/SSHv2, RADIUS/TACACS+.
10. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik i jego producenta w zakresie określonym powyżej.
11. Co najmniej 24 miesiące gwarancji producenta.

# Rozbudowa infrastruktury UTM (1 szt.).

W ramach działania przewiduje się zakup usług subskrypcji na istniejące urządzenie producenta Stormshield model: SN310. Subskrypcja musi umożliwić Zamawiającemu korzystanie z aktualnych baz funkcji ochronnych producenta i serwisów oraz obejmować firewall, IPS, kształtowanie pasma, antywirus, antyspam, VPN, filtry URL. W ramach przedmiotu zamówienia Wykonawca musi zapewnić także wsparcie techniczne, które może być tylko realizowane przez producenta, dystrybutora, bądź oficjalnego partnera dystrybutora. Subskrypcja dla urządzenia UTM obejmująca wszystkie wymagania wskazane powyżej musi być dostarczona na okres do dnia 14.03.2026 r. niezależnie od oferowanych modeli licencjonowania producenta.

Zamawiający dopuszcza rozwiązanie równoważne w postaci dostawy innego urządzenia lub platformy bezpieczeństwa spełniających poniższe kryteria równoważności funkcjonalnej.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. System detekcji i prewencji włamań (IPS).
3. Kształtowanie pasma.
4. Ochrona antywirusowa.
5. Ochrona antyspam.
6. VPN.
7. Flitry URL.

Minimalne parametry techniczne urządzenia:

1. Przepustowość Firewall: min. 4 Gbps.
2. Musi obsługiwać min. 300 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 20 jednoczesnych połączeń SSL VPN.
4. Przepustowość IPS: min. 2,4 Gbps.
5. Wydajność SSL VPN: min. 600 Mbps.
6. Ilość interfejsów sieciowych: minimum 8 portów Gigabit Ethernet RJ-45.

Minimalne parametry funkcjonalne urządzenia:

1. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
	1. Firewall.
	2. System detekcji i prewencji włamań (IPS).
	3. Kształtowanie pasma.
	4. Ochrona antywirusowa.
	5. Ochrona antyspam.
	6. VPN.
	7. Flitry URL.
2. W ramach funkcji firewall system musi:
	1. posiadać Firewall klasy Stateful Inspection,
	2. umożliwiać budowanie reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, usług internetowych (web services), przypisania kolejki QoS,
	3. umożliwiać wskazanie trasy routingu dla wybranej reguły,
	4. umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP,
	5. umożliwiać filtrowanie na podstawie adresów MAC,
	6. umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
3. W ramach funkcji systemu detekcji i prewencji włamań IPS system musi:
	1. wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe,
	2. umożliwiać tworzenie własnych sygnatur dla systemu IPS przez administratora,
	3. usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej,
	4. umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL,
	5. umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0,
	6. zapewniać automatyczną aktualizację sygnatur kontekstowych.
4. W ramach funkcji kształtowania pasma system musi:
	1. umożliwiać kształtowanie pasma w oparciu o priorytety ruchu,
	2. umożliwiać ograniczenie pasma lub priorytetu reguły firewall pod względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika,
	3. umożliwiać śledzenie konkretnego typu ruchu,
	4. umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
5. W ramach funkcji ochrony antywirusowej system musi:
	1. posiadać skaner antywirusowy w ramach podstawowej subskrypcji w okresie udzielonej gwarancji na system,
	2. mieć możliwość skanowania plików,
	3. powiadamiać użytkownika o wykryciu infekcji,
	4. wykrywać infekcje wewnątrz protokołów, min. POP3, SMTP i FTP.
6. W ramach funkcji ochrony antyspam system musi:
	1. posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM),
	2. działać w oparciu o minimum białe/czarne listy, DNS RBL, skaner heurystyczny,
	3. umożliwiać modyfikację listy serwerów RBL,
7. W ramach funkcji VPN system musi:
	1. umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja),
	2. wspierać co najmniej następujące typy sieci VPN: IPSec VPN, SSL VPN,
	3. umożliwiać działanie SSL VPN co najmniej w trybie tunelu,
	4. umożliwiać pobranie klienta VPN współpracującego z oferowanym systemem,
	5. umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe,
	6. umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
8. W ramach funkcji filtrowania URL system musi:
	1. posiadać wbudowany filtr URL,
	2. działać w oparciu o klasyfikację URL kategorii tematycznych stron internetowych,
	3. umożliwiać dodawanie własnych kategorii URL,
	4. umożliwiać blokowanie dostępu do adresu URL,
	5. umożliwiać zezwolenie na dostęp do adresu URL,
	6. umożliwiać blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora,
	7. uwzględniać komunikację po protokole HTTPS.
9. Inne funkcje systemu:
	1. system musi umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory,
	2. system musi umożliwiać dwuskładnikową autoryzację użytkowników,
	3. system musi umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet,
	4. system musi umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego,
	5. system musi umożliwiać statyczne trasowanie pakietów,
	6. system musi umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall,
	7. system musi umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP,
	8. system musi umożliwiać konfigurację z wykorzystaniem polskiego interfejsu graficznego,
	9. system musi umożliwiać dostęp poprzez przeglądarkę internetową,
	10. system musi umożliwiać zarządzenie z poziomu konsoli (SSH),
	11. system musi umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania,
	12. system musi posiadać graficzny interfejs administracyjny obejmujący narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup,
	13. system musi posiadać graficzny interfejs administracyjny obejmujący narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych,
	14. system musi posiadać graficzny interfejs administracyjny obejmujący możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła,
	15. system musi posiadać graficzny interfejs administracyjny obejmujący możliwość generowania skryptów z czynności wykonywanych przez administratora,
	16. system musi umożliwiać zapisywanie logów,
	17. system musi umożliwiać eksportowanie logów na zewnętrzny serwer (syslog),
	18. system musi umożliwiać eksportowanie backupu konfiguracji,
	19. system musi umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika,
	20. system musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów,
	21. system musi umożliwiać eksport wyników raportu do formatu CSV,
	22. system musi posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej,
	23. system musi umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny.
10. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące funkcje: Firewall, System detekcji i prewencji włamań (IPS), Kształtowanie pasma, Ochrona antywirusowa, Ochrona antyspam, VPN, Flitry URL na okres do dnia 14.03.2026 r.
11. Gwarancja producenta do dnia 14.03.2026 r. Gwarancja powinna obejmować również możliwość wymiany urządzenia na nowe w przypadku wady urządzenia UTM.
12. W przypadku zaoferowania rozwiązania równoważnego Wykonawca jest zobligowany do instalacji, wdrożenia oraz migracji konfiguracji istniejącego urządzenia UTM oraz przeprowadzenia szkolenia dla administratora w zakresie konfiguracji i eksploatacji na podstawie wcześniej zaakceptowanego przez Zamawiającego zakresu merytorycznego szkolenia.

# Przedmiot przedmiotu zamówienia części nr 2.

# Wymagania ogólne.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe, oprogramowanie nie może znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
6. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
7. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
8. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
9. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
10. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
11. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
12. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
13. Usługa wsparcia wdrożenia obejmuje:
14. przeprowadzenie analizy przedwdrożeniowej,
15. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
16. rejestracja produktu – jeżeli wymagana,
17. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
18. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
19. konfigurację oprogramowania,
20. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
21. szkolenie administratorów z zakresu pracy z programem,
22. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
23. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
24. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
25. scenariusze testowe, procedury oraz wzory raportów testów,
26. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
27. opis koncepcji realizacji prac,
28. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
29. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
30. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 15 dni kalendarzowych od dnia zawarcia umowy,
31. Zamawiający w terminie nie dłuższym niż 5 dni kalendarzowych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
32. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni kalendarzowych od dnia ich otrzymania,
33. Zamawiający w terminie 5 dni kalendarzowych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
34. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
35. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
36. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
37. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
38. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
39. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
40. Instruktaże w zakresie dostarczonego oprogramowania – wymagania minimalne.
41. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
42. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
43. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 2 osoby).
44. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
45. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.
46. Wymagania licencyjne dla dostarczonego oprogramowania:
47. Licencjobiorcą wszystkich licencji będzie Gmina Działoszyce.
48. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
49. Licencje muszą obowiązywać do dnia 14.03.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania (pod warunkiem, że w dalszej części dokumentu Zamawiający nie określił innego okresu ważności licencji).
50. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
51. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
52. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
53. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
54. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
55. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
56. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
57. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
58. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania w formie licencji czasowych lub subskrypcyjnych:
59. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 14.03.2026 r.
60. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
61. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 14.03.2026 r.
62. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
63. dostęp do najnowszych wersji oprogramowania,
64. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
65. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
66. przyjmowanie i realizacja zgłoszeń serwisowych,
67. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,

w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.

1. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

# Zakup oprogramowania do agregowania logów (1 szt.).

Minimalne wymagania funkcjonalne oprogramowania:

* 1. Oprogramowanie musi umożliwiać scentralizowane zarządzanie komunikatami dzienników logów na urządzeniach sieciowych i serwerach wyposażonych w systemy operacyjne i firmware Linux/Unix/Windows.
	2. Oprogramowanie musi umożliwiać przeglądanie wszystkich logów ze wskazanych urządzeń w jednej konsoli w oparciu o syslog i protokół SNMP.
	3. Oprogramowanie nie może ograniczać liczby urządzeń, z których zbiera logi.
	4. Oprogramowanie powinno zbierać logi z urządzeń obsługujących IPv4 i IPv6.
	5. Oprogramowanie musi umożliwiać powiadamianie w czasie rzeczywistym w ramach wcześniej zdefiniowanych kryteriów.
	6. Konsola oprogramowania powinna być dostępna przez przeglądarkę.
	7. Oprogramowanie powinno posiadać bufor na minimum 1 000 000 wiadomości syslog.
	8. Oprogramowanie powinno umożliwiać zapisywanie zebranych dysków do wskazanej lokalizacji.
	9. Oprogramowanie powinno dzielić logi według: priorytetu, czasu, adresu IP lub nazwy hosta, sieci, zawartości treści, ze względu na źródło (UDP, TCP, SNMP).
	10. Oprogramowanie powinno umożliwiać wysyłanie powiadomień e-mail w oparciu o zdefiniowanie wcześniej reguły.
	11. Oprogramowanie powinno umożliwiać uruchamianie skryptów w oparciu o zdefiniowanie wcześniej reguły.
	12. Oprogramowanie powinno umożliwiać logowanie do plików oraz baz danych ODBC.
	13. Oprogramowanie powinno umożliwiać przesyłanie dalej wygenerowanej wiadomości w oparciu o zdefiniowanie wcześniej reguły.
	14. Oprogramowanie powinno umożliwiać generowanie wykresów dla statystyk syslog dla określonych przedziałów czasowych.
	15. Oprogramowanie powinno umożliwiać przeglądanie i filtrowanie widomości na podstawie priorytetu, czasu, adresu IP lub nazwy hosta, sieci, zawartości treści, ze względu na źródło (UDP, TCP, SNMP).

Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:

1. Oprogramowanie ma umożliwiać instalację na serwerach fizycznych (2 serwerów) jako oddzielne instancje oraz maszynach wirtualnych (maksymalnie 4 maszyny wirtualne) oraz umożliwiać podłączenie nielimitowanej liczby urządzeń końcowych do jednego zainstalowanego serwera.
2. Zamawiający dopuszcza instalację i wdrożenie zdalne.
3. Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej posiadanym i wskazanym przez Zamawiającego.
4. Wykonawca będzie udzielał pomocy technicznej dla Zamawiającego przez okres gwarancji.
5. Usługa wsparcia wdrożenia obejmuje:
6. analizę przedwdrożeniowa,
7. pomoc przy instalacji silnika bazy danych - jeżeli będzie wymagana instalacja,
8. instalację oprogramowania: na serwerach fizycznych i maszynach wirtualnych,
9. konfigurację oprogramowania,
10. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego.

# Zakup oprogramowania backup (1 szt.).

Minimalne parametry funkcjonalne oprogramowania:

1. System powinien umożliwiać tworzenie kopii zapasowych dla 50 komputerów oraz 2 hostów wirtualizacji.
2. System musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych.
3. System musi mieć mechanizmy kompresji w celu zmniejszenia wielkości archiwów.
4. System musi zapewniać backup jednoprzebiegowy.
5. System musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania.
6. System musi mieć możliwość uruchamiania skryptów przed i po zadaniu backupowym.
7. System musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
8. System musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.
9. System musi wspierać backup maszyn wirtualnych.
10. System powinien zapewniać wykonywanie kopii zapasowych plików przechowywanych na urządzeniach pracujących pod kontrolą systemów Windows, NetWare i Linux.
11. Pliki kopii .zip powinno być można w przypadku awarii systemu przeglądać i rozpakowywać różnymi programami obsługującymi format PKZIP ZIP64.
12. System powinien posiadać konsolę sterowania, obsługiwaną przez „thin client” przeglądarką internetową, dostęp do konsoli zarządzającej systemu backupu nie powinien wymagać konieczności instalacji dodatkowego oprogramowania. Powinien działać w oparciu o stronę internetową. Serwer www powinien być wbudowany bezpośrednio do modułu serwera backupu, bez potrzeby instalowania na serwerze backupu zewnętrznego serwera www, np. IIS lub Apache.
13. System powinien obsługiwać kodowanie znaków Unicode, przez co możliwy powinien być backup plików zawierających w nazwie dowolne znaki narodowe.
14. System powinien mieć możliwość pracy w programie z dowolnego miejsca bez potrzeby korzystania z Pulpitu zdalnego, jednoczesnej pracy z danym serwerem przez kliku administratorów.
15. System powinien mieć wbudowane następujące funkcje:
	1. Możliwość wykonania backupu całego systemu operacyjnego, łącznie z zainstalowanymi programami, sterownikami i danymi użytkownika, tak aby w przypadku awarii możliwe było odzyskanie działającego systemu operacyjnego i wszystkich zainstalowanych komponentów.
	2. Zautomatyzowane przywracanie systemu operacyjnego z serwerów (prosty sposób przywracania systemu operacyjnego z serwera kopii zapasowych poprzez sieć do uszkodzonego komputera). Możliwość przywrócenia po awarii systemu operacyjnego wraz z wszystkimi zainstalowanymi programami (ang. bare-metal restore), tak aby uruchomić system operacyjny bez potrzeby ponownej instalacji i konfiguracji.
	3. Ochrona przed programami ransomware szyfrującymi pliki.
	4. Backup i odzyskiwanie maszyn wirtualnych Hyper-V oraz VMWare ESX, ESXi. Program powinien wykonywać kopie zapasowe zarówno zatrzymanych jak i uruchomionych maszyn wirtualnych.
	5. Certyfikaty SSL dla połączeń HTTPS – możliwość obsługi samopodpisanych certyfikatów oraz stosowania własnych certyfikatów SSL.
	6. Zabezpieczanie połączeń sieciowych w systemach archiwizacji danych - typu klient-serwer za pomocą reguł IPSec.
	7. Możliwość archiwizacja danych w chmurze.
	8. Backup plików PST (MS Outlook) - backup plików PST bez zamykania programu Outlook.
	9. Możliwość automatycznego backupu urządzenia przy zamykaniu systemu.
	10. Archiwizacja danych także na napędy taśmowe – możliwość replikacji na napędy taśmowe.
	11. Możliwość backupu na dysk sieciowy - składowanie kopii na urządzeniach typu NAS szybkim i wydajnym protokołem iSCSI.
	12. Możliwość instalacji serwera backupu pod systemem Linux i Mac OS.
	13. Możliwość wydajnego i pewnego backupu baz danych i plików poczty (Microsoft SQL Server, Microsoft Exchange Server, Oracle, MySQL, InterBase, Firebird, Microsoft Access, dBase, Paradox oraz plików programów pocztowych: Microsoft Outlook, Outlook Express, Mozilla Thunderbird).
	14. Możliwość archiwizacji otwartych i zablokowanych plików.
	15. Możliwość szyfrowania archiwów (w tym AES 256).
	16. Możliwość wykonywania archiwizacji pełnej i różnicowej, także różnicowej na poziomie fragmentów plików (archiwizowane są tylko te części plików, które zostały zmodyfikowane od czasu poprzednich archiwizacji a pozostałe są pomijane).
	17. Możliwość generowania raportów i statystyk, które pomagają w analizie działania aplikacji (Raporty informujące o niewykonanych i opóźnionych zadaniach archiwizacji i statystyki zawierające informacje na temat szybkości i rozmiaru backupu z poszczególnych komputerów).
	18. Możliwość wykonywania zadań archiwizacji w/g harmonogramu następującego typu: Na żądanie - zadanie archiwizacji będzie wykonywane tylko przez manualne uruchomienie zadania; Codziennie - zadanie archiwizacji będzie uruchamiane codziennie o wskazanej godzinie; Co określoną liczbę dni - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę dni; Co określoną liczbę godzin - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę godzin; Co określoną liczbę minut - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę minut; W dni tygodnia - zadanie archiwizacji będzie wykonywane automatycznie w wybrane dni tygodnia; Czas rozpoczęcia - umożliwia ustalenie terminu rozpoczęcia zadania archiwizacji z dokładnością do jednej minuty; Następny termin - umożliwia ustalenie daty kolejnej archiwizacji; Zadania opóźnione mogą być pominięte i wykonane w następnym terminie, wykonane natychmiast po podłączeniu serwera; Przy zamykaniu systemu.
	19. Dziennik zdarzeń służący do sprawdzania poprawności działania systemu i wyszukiwania przyczyn ewentualnych problemów – możliwość na bieżąco śledzenia generowanych zdarzeń, dotyczących działania całego systemu, takie jak: błędy, ostrzeżenia i informacje. Wszystkie zapisane zdarzenia można filtrować co najmniej według typu zdarzenia oraz nazwy komputera, którego dana informacja dotyczy.
	20. Podczas wyboru plików i katalogów do archiwizacji pozwalać określić woluminy, maski lub pełne ścieżki do plików i katalogów, które mają być archiwizowane i te, które mają być wykluczone z archiwizacji.
	21. Obsługę co najmniej następujących rodzajów archiwizacji: archiwizacja pełna; archiwizacja różnicowa; archiwizacja różnicowa na poziomie fragmentów plików.
	22. Obsługę kopii rotacyjnych (wersjonowanie, retencja danych - pozwala określić, ile maksymalnie przechowywać archiwów na dysku, ile przechowywać kopii wstecz).
	23. Obsługę replikacji archiwów - archiwa należące do wybranego zadania backupu mogą być powielane w inne miejsce, replikacja może być wykonywana na napędy dyskowe, optyczne i taśmowe.
	24. Monitoring i kontrola pracy serwera backupu, powinna w łatwy i intuicyjny sposób umożliwić zatrzymanie i uruchomienie serwera backupu, możliwość wywołania wirtualnego wiersz poleceń na serwerze backupu i podłączonych stacjach roboczych.
	25. Dziennik zdarzeń służy do sprawdzania poprawności działania Systemu i wyszukiwania przyczyn ewentualnych problemów. W zakładce Dziennik zdarzeń można na bieżąco śledzić wszystkie generowane zdarzenia dotyczące działania całego Systemu (serwera jak i stacji roboczych), takie jak: błędy, ostrzeżenia i informacje.
	26. Wszystkie zapisane zdarzenia można filtrować według typu zdarzenia oraz nazwy urządzenia, którego dana informacja dotyczy.
	27. Wysyłanie alertów administracyjnych, zawierających raporty lub wybrane komunikaty z dziennika zdarzeń, wg ustalonego harmonogramu na wskazany adres e-mail lub np. do serwera syslog.
	28. Możliwy dostęp do zasobów sieciowych przez np. definiowanie ścieżki UNC, dyski sieciowe i dyski serwerów FTP, które mogą być wykorzystywane przez system jako: miejsce przechowywania archiwów, katalog docelowy replikacji, ścieżka zapisu alertów administracyjnych.
	29. Możliwe używania poleceń lokalnych, służących do rozszerzania funkcjonalności programu. Dzięki nim można automatycznie uruchamiać na serwerze backupu zewnętrzne programy, skrypty lub pliki wsadowe, wykonywać operacje na plikach, wykorzystywać komponenty ActiveX, sterować usługami Active Directory, itp.
	30. Program może być uruchamiany w trybie Usługi systemowej lub awaryjnie, także w trybie aplikacji użytkownika.
	31. Możliwe uruchomienie programu w trybie diagnostycznym oraz w trybie naprawy bazy danych.

# Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami (1 szt.).

Aktualnie Zamawiający posiada 30 licencji oprogramowania antywirusowego ESET Endpoint Security. Przedmiotem zamówienia jest rozbudowa istniejącego oprogramowania antywirusowego poprzez podniesienie wersji istniejącego oprogramowania dla Gminy Działoszyce do wersji ESET PROTECT Elite ważnej w okresie do dnia 14.03.2026 r. dla 40 użytkowników/urządzeń oraz umożliwienie zarządzania wszystkimi użytkownikami/urządzeń końcowych z jednej konsoli chmurowej wraz z wdrożeniem oprogramowania zgodnie z wytycznymi wynikającymi z rozdziału nr 4.1. Wymagania ogólne niniejszego dokumentu w zakresie modułów XDR, zarządzania podatnościami i szyfrowania dysków

lub dostawa równoważnej platformy bezpieczeństwa zgodnie z określonymi poniżej kryteriami równoważności.

Minimalne wymagania (kryteria równoważności) określone dla równoważnej platformy bezpieczeństwa:

Administracja zdalna w chmurze.

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

Ochrona stacji roboczych.

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

Ochrona serwera.

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

Dodatkowe wymagania dla ochrony serwerów Windows:

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

Dodatkowe wymagania dla ochrony serwerów Linux:

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

Szyfrowanie.

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10/11 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android.

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

Ochrona serwera pocztowego MS Exchange.

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze.

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

Ochrona usługi Microsoft 365.

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępne w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
	1. użytkowników, otrzymujących najwięcej spamu,
	2. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
	3. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
	4. kont użytkowników, które mogę być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
	1. jaka ilość wiadomości została przeskanowania,
	2. wynik skanowania poszczególnej wiadomości,
	3. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte,
	1. na jakim koncie zostały wykryte,
	2. jakie zagrożenie zostało wykryte,
	3. podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
	1. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
	2. wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,
	3. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Moduł zarządzania podatnościami i aktualizacjami.

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
	1. nazwę aplikacji lub systemu operacyjnego;
	2. punktacje CVSS;
	3. opis wykrytej podatności;
	4. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.
6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Moduł XDR.

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać minimum 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Ochrona poprzez dwuskładnikowe uwierzytelnianie.

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.

Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy i musi odbywać się zgodnie z wytycznymi wynikającymi z rozdziału nr 4.1. Wymagania ogólne niniejszego dokumentu.

# Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem) (1 szt.).

Minimalne wymagania funkcjonalne dla oprogramowania:

1. Oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.
3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:
	1. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
	2. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
	3. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
	4. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
	5. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,
	6. monitorowania serwerów WWW i adresów URL,
	7. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
	8. obsługi komunikatów syslog i pułapek SNMP.
	9. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
	10. kontroli nad monitorem usług Windows,
	11. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:
	1. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;
	2. zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
	3. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkowania licencji w organizacji;
	4. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
	5. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera;
	6. możliwość odczytania numeru seryjnego (klucze licencyjne);
	7. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
	8. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie:
	1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
	2. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
	3. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
	4. archiwizacji i porównywania audytów środków trwałych;
	5. tworzenia kodów kreskowych w Środkach Trwałych;
	6. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy;
	7. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android;
	8. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).
8. Oprogramowanie musi zapewniać funkcjonalność w zakresie monitorowania aktywności użytkowników na stacjach roboczych w zakresie:
	1. faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);
	2. monitorowania procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika);
	3. użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona);
	4. informacji o edytowanych przez użytkownika dokumentach;
	5. historii pracy (cykliczne zrzuty ekranowe);
	6. listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
	7. transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
	8. wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.
9. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
	1. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
	2. zarządzanie posiadanymi licencjami;
	3. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
	4. zarządzanie posiadanymi licencjami: raport zgodności licencji;
	5. możliwość przypisania do programów numerów seryjnych, wartości itp.
10. Oprogramowanie musi zapewniać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
11. W zakresie pomocy technicznej system musi umożliwiać:
	1. tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów);
	2. załączanie komentarzy, zrzutów ekranów i załączników w zgłoszeniach;
	3. konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia;
	4. przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach”);
	5. dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;
	6. planowanie zastępstw w przydzielaniu zgłoszeń;
	7. funkcję rozbudowanych raportów;
	8. powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;
	9. baza zgłoszeń z rozbudowaną wyszukiwarką;
	10. przejrzysty i intuicyjny interfejs webowy;
	11. wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;
	12. komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;
	13. zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;
	14. dwukierunkowa wymiana plików;
	15. zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;
	16. zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);
	17. procesowanie zgłoszeń z wiadomości e-mail;
	18. integracja bazy użytkowników z Active Directory;
	19. zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).
12. W zakresie kontroli dostępu do danych system musi umożliwiać:
	1. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
	2. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
	3. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
	4. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;
	5. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
	6. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
	7. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
	8. integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów
	9. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
	10. informacje o urządzeniach podłączonych do danego komputera;
	11. lista wszystkich urządzeń podłączonych do komputerów w sieci;
	12. audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
	13. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników;
	14. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:

1. Instalacja ma odbyć się na wszystkich komputerach oraz serwerach posiadanych przez Zamawiającego – 40 użytkowników/urządzeń.
2. Zamawiający dopuszcza instalację i wdrożenie zdalne.
3. Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
4. Wykonawca będzie udzielał pomocy technicznej Zamawiającemu przez okres gwarancji.
5. Usługa wsparcia wdrożenia obejmuje:
6. analizę przedwdrożeniowa,
7. pomoc przy instalacji silnika bazy danych - jeżeli będzie wymagana instalacja,
8. instalację oprogramowania: na stacji roboczej,
9. dystrybucję oprogramowania na wybranych stacjach roboczych,
10. konfigurację oprogramowania,
11. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
12. szkolenie administratorów z zakresu pracy z programem:
13. przykładowy audyt oprogramowania i plików na wybranej stacji roboczej,
14. generowanie raportów i zestawień dotyczących sprzętu, oprogramowania i użytkowników,
15. użytkowanie zdalnego pulpitu.
16. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.