

Umowa ramowa nr COI/U/PZP/262/13/2026 (COI-ZAK.262.71.2025)**na dostawę oprogramowania antywirusowego**

zawarta w Warszawie w dniu złożenia podpisu przez ostatnią ze Stron, zwana dalej „**Umową Ramową**”, pomiędzy:

Centralnym Ośrodkiem Informatyki z siedzibą w Warszawie, adres: Aleje Jerozolimskie 132-136, 02-305 Warszawa, wpisanym do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy, pod numerem KRS: 0000372110, NIP: 7252036863, REGON: 100999489, zwanym dalej „**Centralnym Zamawiającym**”, reprezentowanym przez:

[REDAKCE]

zgodnie z informacją odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców, pobraną na podstawie art. 4 ust. 4aa ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym stanowiącą Załącznik nr 6 do Umowy

a

- 1) **Servcomp sp. z o.o.** z siedzibą w Lublińcu, przy ul. Oleskiej 11 (42-700 Lubliniec) wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Częstochowie, XVII Wydział Gospodarczy pod numerem KRS 0000993464, NIP 5751906703, REGON 523191771, zwaną dalej „**Wykonawcą**”, reprezentowaną przez:

[REDAKCE]

zgodnie z informacją odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców, pobraną na podstawie art. 4 ust. 4aa ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym stanowiącą Załącznik nr 7 do Umowy

- 2) **Ikaria sp. z o.o. sp.k.** z siedzibą w Łodzi, przy ul. Gen. Lucjana Żeligowskiego 3/5 (90-752 Łódź) wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy pod numerem KRS 0000332204, NIP 7272746817, REGON 100703365, zwaną dalej „**Wykonawcą**”, reprezentowaną przez:

[REDAKTOWANE]
zgodnie z informacją odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców, pobraną na podstawie art. 4 ust. 4aa ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym stanowiącą Załącznik nr 8 do Umowy

- 3) **Perceptus sp. z o.o.** z siedzibą w Zielonej Górze, przy ul. Nowy Kisielin – Antoniego Wysockiego 10 (66-002 Zielona Góra), wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Zielonej Górze, VIII Wydział Gospodarczy pod numerem KRS 0000320099, NIP 9291808578, REGON 080307093, zwaną dalej „**Wykonawcą**”, reprezentowaną przez:

[REDAKTOWANE]
zgodnie z informacją odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców, pobraną na podstawie art. 4 ust. 4aa ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym stanowiącą Załącznik nr 9 do Umowy

- 4) [REDAKTOWANE]
wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod numerem NIP [REDAKTOWANE] REGON [REDAKTOWANE] zwaną dalej „Wykonawcą”

zgodnie z informacją odpowiadającą wydrukowi z systemu teleinformatycznego Centralnej Ewidencji i Informacji o Działalności Gospodarczej, stanowiącej Załącznik nr 10 do Umowy

- 5) **Seven sp. z o.o.** z siedzibą w Zielonej Górze, przy ul. Chopina 14A (65-001 Zielona Góra), wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Zielonej Górze, VIII Wydział Gospodarczy pod numerem KRS 0000249558, NIP 9730852602, REGON 080070691, zwaną dalej „Wykonawcą”, reprezentowaną przez:

[REDAKTOWANE]
zgodnie z informacją odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców, pobraną na podstawie art. 4 ust. 4aa ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym stanowiącą Załącznik nr 11 do Umowy

zwanymi także dalej wspólnie „**Stronami**” lub każda z osobna również „**Stroną**”.

Zamawiający i Wykonawcy zwani są łącznie w dalszej treści Umowy Ramowej „**Stronami**”, a indywidualnie również „**Stroną**”.

W związku z rozstrzygnięciem postępowania o udzielenie zamówienia publicznego dotyczącego dostawy chmurowego oprogramowania antywirusowego, przeprowadzonego na podstawie art. 311 ust. 1 pkt 1 w zw. z art. 132 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej: „**Ustawa PZP**”), w trybie przetargu nieograniczonego, w celu zawarcia umowy ramowej, Strony zgodnie postanowiły zawrzeć Umowę Ramową o następującej treści:

§ 1

DEFINICJE

Lp.	Termin	Definicja
1.	Dni Robocze	Dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.
2.	Jednostka lub Zamawiający	Podmioty udzielające Zamówień Wykonawczych będący: 1) podmiotem sektora finansów publicznych, o których mowa w art. 9 pkt 1–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych; 2) instytutem badawczym, instytutem działającym w ramach Sieci Badawczej Łukasiewicz; 3) inną państwową lub samorządową osobą prawną utworzoną na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem

		przedsiębiorstw, banków i spółek prawa handlowego; 4) inną, niż określoną w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, państwową jednostką organizacyjną nieposiadającą osobowości prawnej.
3.	Oferta Wykonawcza	Oferta złożona przez Wykonawcę w wyniku Zaproszenia do składania ofert, stanowiąca Załącznik nr 1 do Umowy Wykonawczej .
4.	Oferta Wykonawcy	Oferta Wykonawcy, złożona w Postępowaniu, której Formularz Ofertowy wraz z dokumentami wymaganymi przez przepisy prawa oraz wskazanymi w dokumentach Postępowania (z wyłączeniem informacji objętych tajemnicą przedsiębiorstwa), stanowią Załącznik nr 1 do Umowy Ramowej .
5.	Oprogramowanie	Oprogramowanie określone w OPZ
6.	OPZ	Opis przedmiotu zamówienia, stanowiący Załącznik nr 2 do Umowy Ramowej wraz z wyjaśnieniami SWZ opublikowanymi na stronie internetowej prowadzonego Postępowania.
7.	Platforma	Elektroniczna platforma zakupowa dostępna za pośrednictwem strony internetowej wskazanej przez COI
8.	Postępowanie	Postępowanie o udzielenie zamówienia publicznego poprzedzające zawarcie Umowy Ramowej.

9.	Postępowanie wykonawcze	Postępowanie o zawarcie umowy wykonawczej, prowadzone na podstawie umowy ramowej.
10.	Siła Wyższa	Zdarzenie nadzwyczajne, zewnętrzne, pozostające poza kontrolą Strony powołującej się na wypadek Siły Wyższej, niemożliwe do przewidzenia i niemożliwe do zapobieżenia. Pojęcie Siły Wyższej nie obejmuje żadnych zdarzeń, które wynikają z niedołożenia przez Stronę należytej staranności ani zdarzeń, które były publicznie znane w dniu zawarcia Umowy Ramowej, oraz ich skutków.
11.	Umowa Ramowa	Niniejsza Umowa wraz z Załącznikami.
12.	Umowa Wykonawcza	Umowa zawarta pomiędzy jedną z Jednostek a jednym z Wykonawców na podstawie Umowy ramowej mająca za przedmiot dostawę Oprogramowania, projektowane postanowienia Umowy wykonawczej (wzór umowy Wykonawczej) stanowią Załącznik nr 3 do Umowy Ramowej .
13.	Zamówienie Wykonawcze	Zamówienie, o którym mowa w art. 314 ust. 1 pkt 3 Pzp, udzielone Wykonawcy w wyniku przeprowadzonego postępowania w ramach Umowy Ramowej obejmujące dostawę Oprogramowania zgodnie z Zaproszeniem do złożenia oferty.
14.	Zaproszenie	Zaproszenie do udziału w postępowaniu wykonawczym, kierowane do wszystkich Wykonawców (za pośrednictwem Platformy wszczynające postępowanie wykonawcze).

§ 2**PRZEDMIOT UMOWY**

1. Przedmiotem Umowy Ramowej (dalej: „**Przedmiot Umowy Ramowej**”) jest określenie warunków udzielania i realizacji Zamówień Wykonawczych na dostawę przez Wykonawcę Oprogramowania do siedziby Jednostek.
2. Wykonawca zobowiązuje się wykonać Przedmiot Umowy Ramowej zgodnie z Umową Ramową, w szczególności OPZ i Ofertą Wykonawcy. Szczegółowy opis przedmiotu zamówienia zawiera OPZ oraz Oferta Wykonawcy.
3. Umowa Ramowa jest umową w rozumieniu art. 7 pkt 26 Pzp oraz została zawarta po przeprowadzeniu postępowania na podstawie art. 311 ust. 1 pkt 1 Pzp i określa warunki udzielania poszczególnych Zamówień Wykonawczych udzielanych w postaci Umów Wykonawczych zawieranych z Wykonawcą.
4. W celu uniknięcia wątpliwości przyjmuje się, że jeżeli Strony nie zdefiniowały danego działania niezbędnego do prawidłowej realizacji Umowy Ramowej jako obowiązku Centralnego Zamawiającego lub Jednostki, a zobowiązanie takie nie wynika z obowiązujących przepisów prawa lub nie jest w sposób oczywisty zobowiązaniem Centralnego Zamawiającego lub Jednostki, Stroną zobowiązaną do wykonania takiego działania jest Wykonawca.
5. Kwota wskazana w §5 ust. 1 stanowi maksymalne zobowiązanie wynikające z Umowy, Wykonawcom nie przysługuje roszczenie o nabycie przez Jednostki w okresie obowiązywania Umowy Ramowej Oprogramowania wskazanego w OPZ.

§ 3**TERMINY REALIZACJI UMOWY RAMOWEJ**

1. Umowa Ramowa zostaje zawarta na okres 12 miesięcy od dnia jej zawarcia lub do wyczerpania kwoty określonej w § 5 ust. 1 Umowy Ramowej – w zależności od tego, które zdarzenie wystąpi wcześniej.
2. W przypadku wskazanym w ust. 1. Umowa Ramowa wygasa bez konieczności składania dodatkowych oświadczeń Stron.

3. Jednostki będą uprawnione do zaproszenia Wykonawców do złożenia Ofert Wykonawczych w okresie wskazanym w ust. 1, przy czym wybór najkorzystniejszej Oferty Wykonawczej, a także zawarcie Umowy Wykonawczej może nastąpić po upływie okresu wskazanego w ust. 1.
4. Termin dostawy Oprogramowania w ramach Umowy Wykonawczej wyniesie **nie więcej niż 5 Dni Roboczych** od dnia zawarcia Umowy Wykonawczej. Termin dostawy zostanie ustalony w Umowie Wykonawczej. W szczególności w tym terminie Wykonawca będący stroną danej Umowy Wykonawczej zapewnia Jednostce możliwość pobierania przez Internet odpowiednich dla przedmiotu Umowy Wykonawczej kluczy licencyjnych do Oprogramowania.

§ 4

OŚWIADCZENIA I ZOBOWIĄZANIA STRON

1. Wykonawca oświadcza, że:
 - 1) nie są mu znane przeszkody prawne do realizacji Umowy Ramowej;
 - 2) posiada zasoby, kwalifikacje, uprawnienia, doświadczenie, urządzenia i narzędzia, niezbędne do prawidłowego wykonania Umowy Ramowej oraz będzie nimi dysponował przez cały okres obowiązywania Umowy Ramowej;
 - 3) zapoznał się z wymaganiami Zamawiającego określonymi w Umowie Ramowej, w tym w Umowie Wykonawczej i potwierdza techniczną możliwość i organizacyjną gotowość do wykonania przedmiotu Umowy Ramowej.
2. Wykonawca zobowiązuje się w szczególności:
 - 1) działać jedynie w zakresie swoich uprawnień i przestrzegać wskazówek Centralnego Zamawiającego;
 - 2) udostępniać na każde żądanie Zamawiającego dokumentację związaną z realizacją przedmiotu Umowy Ramowej;

- 3) przekazywać na żądanie Centralnego Zamawiającego informacje związane z realizacją Umowy Ramowej, w tym dotyczące przyczyn opóźnień lub przyczyn nienależytego wykonywania Umowy Ramowej;
 - 4) poddawać się prowadzonej przez Centralnego Zamawiającego kontroli wykonywania Umowy Ramowej. Wykonawca ma obowiązek przedstawienia Centralnemu Zamawiającemu szczegółowych informacji i wyjaśnień dotyczących realizacji Umowy Ramowej na każde jego żądanie, w szczególności w razie uzasadnionego przypuszczenia, że doszło do nienależytego wykonania Umowy Ramowej lub, że takie nienależyte wykonanie Umowy Ramowej może nastąpić;
 - 5) wykonywać Umowę Ramową w sposób, który nie będzie prowadził do powstania roszczeń osób trzecich z tytułu naruszenia ich praw, w szczególności praw własności intelektualnej. W przypadku zgłoszenia wobec Centralnego Zamawiającego lub Jednostki roszczeń o naruszenie praw osób trzecich objętych powyższym zapewnieniem, Wykonawca podejmie na swój koszt wszelkie środki obrony Centralnego Zamawiającego lub Jednostki przed takimi roszczeniami lub zarzutami i spowoduje, że Centralny Zamawiający lub Jednostka będą od nich zwolnieni, a także pokryje wszelkie koszty i straty, jakie poniesie Centralny Zamawiający lub Jednostki z tego tytułu;
 - 6) realizować Umowę Ramową przy wykorzystaniu całej posiadanej wiedzy i doświadczenia, zgodnie z obowiązującymi przepisami prawa, treścią i celem Umowy Ramowej, przy zachowaniu należytej staranności, uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami współczesnej wiedzy technicznej, najlepszymi praktykami i zgodnie z obowiązującymi przepisami prawa i stosowanymi normami.
3. Wykonawca poniesie wszelkie koszty, które będzie musiał zapłacić Centralny Zamawiający lub Jednostki oraz pokryje wszelkie straty, jakie poniesie Centralny Zamawiający lub Jednostki, jeżeli powyższe zapewnienia oraz pozostałe określone w Umowie Ramowej nie okażą się prawdziwe – w zakresie zgodnym z przepisami prawa powszechnie obowiązującego.

4. Strony zobowiązują się do rzetelnej współpracy w dobrej wierze oraz z poszanowaniem praw i interesów drugiej Strony, mając na uwadze konieczność należytego i terminowego wykonania przedmiotu Umowy Ramowej.
5. Oprogramowanie objęte Umową Ramową musi pochodzić bezpośrednio od producenta Oprogramowania lub z oficjalnych i autoryzowanych przez producenta kanałów dystrybucyjnych.
6. Wykonawca w okresie obowiązywania Umowy Ramowej zobowiązany jest do przekazywania Centralnemu Zamawiającemu w terminie do ostatniego dnia każdego miesiąca zestawienia zawartych Umów Wykonawczych z poszczególnymi Jednostkami. Zestawienie to zawierać ma następujące informacje:
 - 1) okres na jaki Umowy Wykonawcze zostały zawarte,
 - 2) strony i przedmiot Umów Wykonawczych,
 - 3) wartość Umów wykonawczych.
7. Każda ze Stron zobowiązuje się dołożyć należytej staranności w celu zapewnienia drugiej Stronie informacji oraz danych niezbędnych do wykonania Umowy Ramowej. W szczególności Strony będą się wzajemnie na bieżąco informować o wszelkich okolicznościach, które mogłyby spowodować nienależyte wykonanie lub niewykonanie Umowy Ramowej.

§ 5

CENA PRZEDMIOTU UMOWY RAMOWEJ

1. Łączna maksymalna wartość Umowy Ramowej, stanowiąca górny limit wynagrodzenia z tytułu realizacji Umów Wykonawczych, uwzględniająca wszelkie koszty, związane z realizacją wszystkich Umów Wykonawczych zawartych przez Jednostki w wyniku realizacji Umowy Ramowej oraz wynikające z przepisów prawa, w tym wszystkie koszty związane z realizacją Przedmiotu Umowy Ramowej, w szczególności koszty Oprogramowania, a także wszelkie inne opłaty, koszty i nakłady Wykonawcy, niezbędne do wykonania przedmiotu Umów Wykonawczych,

poniesione przez Wykonawcę w związku z realizacją Umowy Ramowej oraz podatek od towarów i usług wynosi: **31 762 285,00 PLN zł netto tj. 39 067 610,55 PLN brutto**.

2. Kwota wskazana w ust. 1 powyżej określa górną granicę zobowiązań, jaką Jednostki mogą zaciągnąć na podstawie Umowy Ramowej łącznie względem wszystkich Wykonawców. Jednostki nie są zobowiązane do wykorzystania powyższego limitu. Wykonawcy nie przysługują żadne roszczenia o wykorzystanie ww. limitu.
3. Maksymalne wynagrodzenie Wykonawcy z tytułu realizacji Umowy Wykonawczej będzie określone każdorazowo w Umowie Wykonawczej.
4. Centralny Zamawiający jak również Jednostki nie będą ponosić żadnych innych dodatkowych kosztów związanych z realizacją Umowy Wykonawczej, oprócz wynagrodzenia Wykonawcy, o którym mowa w ust. 3.
5. Maksymalne ceny jednostkowe za poszczególne rodzaje Oprogramowania zawiera Oferta Wykonawcy/Oferty Wykonawców. Ceny jednostkowe za poszczególne rodzaje Oprogramowania przedstawione w Ofercie Wykonawcy nie ulegną zwiększeniu w terminie obowiązywania Umowy Ramowej, z zastrzeżeniem postanowień zawartych w § 13 i § 14 Umowy Ramowej.
6. Zgodnie z art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t.j. Dz. U. z 2023 r. poz. 1790) Zamawiający oświadcza, że posiada status dużego przedsiębiorcy, w rozumieniu przepisów tej ustawy.

§ 6

ZASADY UDZIELANIA ZAMÓWIEŃ WYKONAWCZYCH

1. Jednostki samodzielnie przygotowują oraz przeprowadzają, poprzez Platformę, postępowania wykonawcze. Jednostki samodzielnie realizują też wszelkie czynności związane z realizacją i zmianami zawieranych przez nie umów wykonawczych, w tym czynności związane z dochodzeniem ewentualnych roszczeń. Do czynności tych zalicza się również ogłoszenia o wykonaniu zawartych Umów wykonawczych, o którym mowa w art. 448 Pzp, jak i sporządzanie raportów

- z realizacji danego zamówienia, w przypadku ziszczenia się przesłanek, o których mowa w art. 446 Pzp.
2. Jednostki każdorazowo będą zwracały się do Wykonawców z Zaproszeniem tj. do zaoferowania cen jednostkowych Oprogramowania wskazanego w punkcie 6.1, 6.2, 6.3, 6.4 albo 6.5 OPZ.
 3. W zaproszeniu jednostka każdorazowo określi:
 - 1) ilość i rodzaj (oprogramowanie wskazane w punkcie 6.1, 6.2, 6.3, 6.4 albo 6.5 OPZ) zamawianego przedmiotu zamówienia (Oprogramowania) oraz termin odpowiedzi na Zaproszenie, z tym, że nie może on być krótszy niż 2 dni robocze od daty wystania Zaproszenia.
 - 2) okres na jaki dostarczane ma być zamawiane Oprogramowanie (12, 24 albo 36 miesięcy).
 4. Wykonawca w odpowiedzi na zaproszenie poinformuje Jednostkę o ewentualnym powstaniu po stronie Jednostki obowiązku podatkowego (tzw. obciążenie odwrotne).
 5. Jednostka zawrze umowę wykonawczą z wykonawcą, który zaproponuje najkorzystniejsze warunki w odpowiedzi na Zaproszenie tj. najniższą cenę (w postępowaniu wykonawczym stosuje się kryterium oceny - cena 100 %, do ceny), przy czym do ceny wykonawcy, o którym mowa w ustępie poprzednim dolicza się wartość tzw. obciążenia zwrotnego.
 6. Pozostałe warunki zaproponowane przez Wykonawcę w ofercie w celu zawarcia Umowy ramowej pozostają niezmiennie w całym okresie obowiązywania umowy ramowej, z zastrzeżeniem § 13 i § 14 Umowy Ramowej.
 7. Cena jednostkowa za dany przedmiot zamówienia zaoferowany przez Wykonawcę w odpowiedzi na Zaproszenie nie może być mniej korzystna od wskazanej w formularzu oferty złożonym przez tego Wykonawcę w postępowaniu prowadzonym w celu zawarcia Umowy ramowej.
 8. Po dokonaniu oceny ofert Jednostka poinformuje Wykonawców o wybranej ofercie.
 9. Zamówienie wykonawcze uważa się za udzielone w momencie zawarcia przez Jednostkę z wybranym Wykonawcą Umowy Wykonawczej.

10. Umowy wykonawcze zawierane będą w formie elektronicznej, podpisanej kwalifikowanym podpisem elektronicznym lub w formie pisemnej, pod rygorem nieważności, oddzielnie w przypadku każdego Zamówienia Wykonawczego.
11. W przypadku zawierania umowy wykonawczej w formie elektronicznej, formularz umowy zostanie przekazany do Wykonawcy za pośrednictwem platformy w celu uzyskania jego podpisu. Wykonawca zobowiązany jest do złożenia kwalifikowanego podpisu elektronicznego na umowie wykonawczej i zwrócenia dokumentu w terminie 2 dni roboczych od dnia jej otrzymania. Zawarta umowa wykonawcza zostanie przekazana do Wykonawcy przez Jednostkę niezwłocznie po opatrzeniu kwalifikowanym podpisem elektronicznym przez Jednostkę.
12. W przypadku zawierania Umowy wykonawczej w formie pisemnej, formularz umowy zostanie przekazany do Wykonawcy za pośrednictwem Platformy w celu uzyskania jego podpisu. Wykonawca w terminie nie dłuższym niż 3 dni robocze od dnia otrzymania do podpisu Umowy wykonawczej, doręczy Jednostce podpisane przez siebie egzemplarze Umowy wykonawczej, w liczbie wskazanej przez Jednostkę, nie większej niż cztery, na adres siedziby Jednostki. Egzemplarz umowy wykonawczej zostanie przekazany do Wykonawcy przez Jednostkę niezwłocznie po opatrzeniu podpisem przez Jednostkę.
13. W przypadku uchybienia terminom wskazanym w ust. 11 lub 12 Jednostka może uznać, iż Wykonawca uchyła się od zawarcia Umowy wykonawczej i odstąpić od udzielenia zamówienia wykonawczego lub zwrócić się do kolejnego wykonawcy, który zaoferował kolejną najkorzystniejszą cenę, o zawarcie umowy wykonawczej.
14. Korespondencja pomiędzy Jednostką a Wykonawcą następuje za pośrednictwem Platformy lub drogą elektroniczną - zgodnie z danymi teleadresowymi określonymi w umowie Wykonawczej.

§ 7

ZAWIERANIE UMÓW WYKONAWCZYCH I WARUNKI ICH REALIZACJI

1. Umowy Wykonawcze będą zawierane z Wykonawcami oddzielnie do każdego Zamówienia Wykonawczego, na zasadach określonych w Umowie Ramowej.
2. Umowy Wykonawcze zawierane są w formie pisemnej pod rygorem nieważności.

3. Postanowienia Umowy Wykonawczej nie mogą być sprzeczne z postanowieniami Umowy Ramowej. W przypadku zaistnienia niezgodności pomiędzy treścią Umowy Wykonawczej a Umowy Ramowej pierwszeństwo będą miały postanowienia Umowy Ramowej.
4. Szczegółowe zasady realizacji Umów Wykonawczych, w tym odbioru zrealizowanych dostaw, zostaną określone w poszczególnych Umowach Wykonawczych.
5. Wykonawca ponosi odpowiedzialność za szkody wyrządzone Centralnemu Zamawiającemu lub Jednostce przy lub w związku z wykonywaniem Umowy Ramowej lub Umowy Wykonawczej.

§ 8

POUFNOŚĆ

1. Wykonawca zobowiązuje się traktować wszelkie informacje lub dane dotyczące działalności Centralnego Zamawiającego, w szczególności informacje techniczne, technologiczne, organizacyjne, finansowe, prawne lub inne informacje posiadające wartość gospodarczą, a także informacje uzyskane w wyniku analizy lub przetworzenia dostarczonych informacji, uzyskane od Centralnego Zamawiającego w formie ustnej, pisemnej lub elektronicznej (w szczególności informacje ujawnione podczas rozmów oraz w treści przekazywanych przez Strony dokumentów) jako informacje poufne (zwane dalej: „**Informacjami Poufnymi**”).
2. W przypadku jakichkolwiek wątpliwości co do charakteru danej informacji lub danych przed ich ujawnieniem lub uczynieniem dostępną Wykonawca zwróci się do Centralnego Zamawiającego lub o wskazanie, czy informacje te ma traktować jako Informacje Poufne.
3. Informacje Poufne uzyskane przez Wykonawcę od Centralnego Zamawiającego w związku z realizacją przedmiotu Umowy Ramowej mogą być wykorzystane tylko w celu jej realizacji.
4. Wykonawca zabezpieczy Informacje Poufne przed dostępem osób trzecich oraz będzie zachowywać zasady poufności w stosunku do wszystkich ww. Informacji i nie będzie ich publikować ani udostępniać osobom trzecim w jakikolwiek sposób

w okresie realizacji Umowy Ramowej oraz w terminie 10 lat po jej wygaśnięciu, bez względu na podstawę wygaśnięcia. Dostęp do Informacji Poufnych będą miały tylko te osoby, które z uwagi na wykonywaną pracę lub pełnioną funkcję potrzebują uzyskać dostęp do Informacji Poufnych – i tylko w takim zakresie, w jakim jest to wymagane do prawidłowego wykonania tej pracy czy pełnienia funkcji.

5. Zobowiązanie do zachowania poufności Informacji Poufnych nie dotyczy:
 - 1) informacji publicznie dostępnych lub stanowiących informację publiczną;
 - 2) informacji, które były znane Stronie przed otrzymaniem od drugiej Strony,
 - 3) informacji, które muszą zostać udostępnione zgodnie z obowiązkiem wynikającym z przepisów powszechnie obowiązującego prawa, orzeczenia sądu lub uprawnionego organu administracji państwowej; w takim przypadku Wykonawca będzie zobowiązany zapewnić, by udostępnienie Informacji Poufnych tylko i wyłącznie w zakresie koniecznym dla zadośćuczynienia powyższemu obowiązkowi.
6. Wykonawca niezwłocznie zawiadomi Centralnego Zamawiającego o każdym przypadku zaistnienia obowiązku udostępnienia Informacji Poufnych osobom trzecim, chyba, że przepisy prawa lub decyzja uprawnionego podmiotu wykluczy możliwość takiego zawiadomienia. Wykonawca podejmie też wszelkie działania konieczne do zapewnienia, by udostępnienie informacji dokonało się w sposób chroniący przed ujawnieniem ich osobom niepowołanym.
7. Strony są zobowiązane do szyfrowania ogólnodostępnymi mechanizmami kryptograficznymi (np. GPG, PGP) korespondencji elektronicznej zawierającej informacje mogące mieć istotny wpływ na bezpieczeństwo lub poufność informacji Stron.
8. W razie wystąpienia przez osobę trzecią z jakimikolwiek roszczeniami skierowanymi do Centralnego Zamawiającego z tytułu naruszenia poufności przekazanych Wykonawcy informacji, jak również dóbr osobistych, Wykonawca zobowiązuje się do pokrycia wszelkich kosztów związanych z dochodzeniem roszczeń przez osoby

trzecie, w tym zasądzonych kwot odszkodowania oraz kosztów obsługi prawnej, w terminie 14 dni od daty doręczenia Wykonawcy wezwania do zapłaty.

§ 9

OCHRONA DANYCH OSOBOWYCH

1. W ramach realizacji Umowy Ramowej nie następuje powierzenie przetwarzania danych osobowych, których administratorem danych, w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „RODO”, jest Centralny Zamawiający.
2. Wykonawca nie będzie miał dostępu do danych osobowych ani nie będzie ich przetwarzał, ponad przetwarzanie danych osobowych udostępnionych sobie wzajemnie przez Strony dotyczących w szczególności osób reprezentujących Strony oraz pracowników i współpracowników Stron wyznaczonych do kontaktów w celu zawarcia i wykonania Umowy Ramowej.
3. W związku z wzajemnym udostępnieniem danych osobowych, o którym jest mowa w ust. 2 powyżej, Strony stają się niezależnymi administratorami udostępnionych im danych osobowych.
4. Niezwłocznie po zawarciu Umowy Ramowej, Strony zobowiązują się do wzajemnego poinformowania osób, których dane zostały udostępnione pomiędzy Stronami zgodnie z ust. 2 powyżej:
 - 1) o zakresie danych osobowych dotyczących tych osób, a przekazanych danej Stronie;
 - 2) o tym, że Strona której dane udostępniono jest administratorem ich danych osobowych oraz że przetwarza ich dane osobowe na zasadach określonych powyżej;
 - 3) o tym, że Strona która dane udostępniła jest źródłem, od którego Strona której dane udostępniono pozyskała ich dane;

- 4) o treści odpowiedniej klauzuli informacyjnej, stanowiącej Załącznik nr 4 do Umowy Ramowej (w przypadku klauzuli informacyjnej Centralnego Zamawiającego) oraz Załącznik nr 5 do Umowy Ramowej (w przypadku klauzuli informacyjnej Wykonawcy).
5. Na żądanie jednej ze Stron złożone w formie elektronicznej lub pisemnej, druga Stronałoży w formie elektronicznej lub pisemnej oświadczenie, potwierdzające, że osobom, o których jest mowa w ust. 2 powyżej, została przekazana klauzula informacyjna zgodnie z treścią ust. 4 powyżej.
6. W przypadku, jeśli Wykonawca lub podwykonawca miałby uzyskać dostęp do innych danych osobowych niż wskazane w ust. 2 powyżej, strony Umowy Ramowej zobowiązują się do niezwłocznego zawarcia stosownej umowy w sprawie powierzenia przetwarzania danych osobowych, zgodnej z obowiązującym u Centralnego Zamawiającego wzorem.

§ 10

PODWYKONAWCY

1. Wykonawca jest uprawniony do powierzenia wykonania części przedmiotu Umowy Ramowej podwykonawcom, z zastrzeżeniem poniższych postanowień.
2. Wykonawcy wykonają Umowę Ramową siłami własnymi.
3. Wykonawca zobowiązany jest do poinformowania Centralnego Zamawiającego w formie pisemnej o każdej zmianie danych dotyczących podwykonawców, jak również o ewentualnych nowych podwykonawcach, którym zamierza powierzyć prace w ramach realizacji Umowy Ramowej.
4. Informacja o zmianie danych dotyczących podwykonawców powinna zostać przekazana Centralnemu Zamawiającemu w terminie 5 Dni Roboczych od zmiany danych.
5. Informacja o zamiarze powierzenia prac nowemu podwykonawcy powinna zostać przekazana Centralnemu Zamawiającemu nie później niż na 5 Dni Roboczych przed planowanym powierzeniem mu realizacji prac.

6. Centralny Zamawiający jest uprawniony do odmowy współdziałania z podwykonawcą, o udziale którego nie uzyskał informacji, do czasu przekazania przez Wykonawcę niezbędnych danych, a opóźnienie powstałe wskutek braku współdziałania z takim podwykonawcą stanowi zwłokę Wykonawcy.
7. Jeżeli Wykonawca dokonuje zmiany podwykonawcy, na zasoby którego powoływał się w toku postępowania poprzedzającego zawarcie Umowy Ramowej, zobowiązany jest do wykazania Centralnemu Zamawiającemu, że nowy podwykonawca spełnia warunki udziału w Postępowaniu w stopniu nie mniejszym, niż podwykonawca dotychczasowy. Jednostki są uprawnione do odmowy współdziałania z podwykonawcą, co do którego Wykonawca nie wykazał spełnienia warunków udziału w Postępowaniu, do czasu wykazania przez Wykonawcę ich spełnienia, a opóźnienie powstałe wskutek braku współdziałania z takim podwykonawcą, stanowi zwłokę Wykonawcy.
8. Jeżeli Wykonawca rezygnuje z posługiwania się podwykonawcą, na zasoby którego powoływał się w toku postępowania poprzedzającego zawarcie Umowy Ramowej, zobowiązany jest do wykazania Centralnemu Zamawiającemu, że Wykonawca samodzielnie spełnia warunki udziału w Postępowaniu w stopniu nie mniejszym, niż podwykonawca, z którego Wykonawca rezygnuje. Jednostki są uprawnione do odmowy współdziałania z Wykonawcą, który nie wykazał samodzielnego spełnienia warunków, do czasu wykazania przez Wykonawcę ich spełnienia lub wskazania innego podwykonawcy i wykazania spełnienia przez niego tych warunków, a opóźnienie w wykonaniu Umowy Ramowej, powstałe wskutek braku współdziałania z Wykonawcą, stanowi zwłokę Wykonawcy.
9. W przypadku powierzenia wykonania części Umowy Ramowej podwykonawcom, Wykonawca odpowiada za działania i zaniechania podwykonawców oraz ich personelu, jak za działania i zaniechania własne.
10. Niewykonanie lub nienależyte wykonanie przez podwykonawcę części przedmiotu Umowy Ramowej upoważnia Zamawiającego do żądania od Wykonawcy odsunięcia podwykonawcy od realizacji przedmiotu Umowy Ramowej.

11. Za zapłatę wynagrodzenia podwykonawcom wyłączną odpowiedzialność ponosi Wykonawca.
12. Umowa Ramowa z podwykonawcą powinna zapewniać realizację powierzonych zobowiązań Wykonawcy w zakresie wynikającym z Umowy Ramowej.
13. Umowa o podwykonawstwo nie może zawierać postanowień kształtujących prawa i obowiązki podwykonawcy, w zakresie kar umownych oraz postanowień dotyczących warunków wypłaty wynagrodzenia, w sposób dla niego mniej korzystny niż prawa i obowiązki Wykonawcy, ukształtowane postanowieniami Umowy Ramowej.
14. Wykonawca o zmianie podwykonawcy zobowiązany jest także powiadomić Jednostki, z którymi ma zawarte Umowy Wykonawcze.
15. Zmiana podwykonawcy nie wymaga zawarcia aneksu.

§ 11

KARY UMOWNE I ODPOWIEDZIALNOŚĆ

1. Wykonawca zapłaci Centralnemu Zamawiającemu kary umowne w okolicznościach i wysokościach ustalonych poniżej:
 - 1) w przypadku odstąpienia od Umowy Ramowej lub jej wypowiedzenia przez jedną ze Stron z winy Wykonawcy w wysokości 5 % maksymalnego wynagrodzenia wskazanego w § ust.1, który ma zostać obciążony karą umowną;
 - 2) w przypadku naruszenia przez Wykonawcę zobowiązań zawartych w § 8 Umowy Ramowej, w wysokości 10 000,00 zł za każde naruszenie;
 - 3) odmowy zawarcia przez Wykonawcę Umowy Wykonawczej zgodnie z § 6 Umowy Ramowej – w wysokości 20 % maksymalnego wynagrodzenia netto Wykonawcy, które ustalone zostałyby w Umowie Wykonawczej, której zawarcia Wykonawca odmówił;
 - 4) w przypadku gdy mimo zmiany wynagrodzenia Wykonawcy zgodnie z § 14 Umowy Ramowej Wykonawca nie dokona zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom

cen materiałów lub kosztów dotyczących zobowiązana podwykonawcy – w wysokości 5 000,00 zł za każdy przypadek.

2. Wykonawca ponosi pełną i nieograniczoną odpowiedzialność za szkody wyrządzone Centralnemu Zamawiającemu przy wykonywaniu lub w związku z wykonywaniem postanowień Umowy Ramowej.
3. Kary umowne są od siebie niezależne i mogą zostać nałożone przez Centralnego Zamawiającego za każdy przypadek naruszenia Umowy Ramowej odrębnie. Kary umowne podlegają sumowaniu, co oznacza, że naliczenie kary umownej z jednego tytułu nie wyłącza możliwości naliczenia kary umownej z innego tytułu, jeżeli istnieją ku temu podstawy.
4. Wysokość kar umownych naliczanych Wykonawcy w toku realizacji Umowy Ramowej nie przekroczy 20 % całkowitej kwoty wynagrodzenia za realizację przedmiotu Umowy Ramowej, określonej w stawce netto w § 5 ust. 1 Umowy Ramowej.
5. Jeżeli szkoda przewyższy wysokość kary umownej, Centralnemu Zamawiającemu przysługiwać będzie roszczenie o zapłatę odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.
6. Kara umowna będzie płatna na podstawie stosownej noty obciążeniowej wystawionej przez Zamawiającego w terminie w niej wskazanym.
7. Strony są zwolnione od odpowiedzialności za szkody powstałe w związku z niewykonaniem lub nienależytym wykonaniem Umowy Ramowej, w przypadku, gdy to niewykonanie lub nienależyte wykonanie jest następstwem zdarzeń określanych jako Siła Wyższa.

§ 12

ZAKOŃCZENIE UMOWY RAMOWEJ

1. Centralny Zamawiający może wypowiedzieć Umowę Ramową lub odstąpić od Umowy Ramowej w przypadkach określonych w przepisach obowiązującego prawa,

w szczególności Pzp, Kodeksu cywilnego oraz w przypadkach określonych w Umowie Ramowej.

2. Centralny Zamawiający może wypowiedzieć Umowę Ramową w całości lub w części ze skutkiem natychmiastowym lub odstąpić od części lub całości Umowy Ramowej ze skutkiem natychmiastowym z przyczyn leżących po stronie Wykonawcy, w przypadku:
 - 1) gdy Wykonawca zostanie trzykrotnie obciążony karą umowną z tytułu nienależytej realizacji Umowy Wykonawczej zgodnie z warunkami Umowy Wykonawczej,
 - 2) dwukrotnego rozwiązania, wypowiedzenia lub odstąpienia od Umowy Wykonawczej przez którąkolwiek ze Stron z winy Wykonawcy;
 - 3) gdy suma kar umownych naliczonych Wykonawcy na podstawie Umowy Ramowej wyniesie 20 % całkowitej kwoty netto wskazanej w § 5 ust. 1 Umowy Ramowej;
 - 4) naruszenia postanowień dotyczących zachowania poufności, o których mowa w § 8 Umowy Ramowej lub ochrony danych osobowych, o których mowa w § 9 Umowy Ramowej, przez Wykonawcę, w tym jakąkolwiek osobę, którą Wykonawca posługuje się w celu wykonania Umowy Ramowej lub Umowy Wykonawczej na szkodę Centralnego Zamawiającego lub Jednostek;
 - 5) niewykonania lub nienależytego wykonania innego zobowiązania umownego przez Wykonawcę niż te określone w pkt 1 – 5 powyżej. W takim przypadku Zamawiający wezwie Wykonawcę do wykonania lub należytego wykonania Umowy Ramowej wyznaczając mu termin co najmniej 7 (słownie: siedmiu) dni.
3. W odniesieniu do wszelkich przypadków, gdy Umowa Ramowa przewiduje uprawnienie Centralnego Zamawiającego do odstąpienia od Umowy Ramowej,

Centralny Zamawiający ma prawo odstąpić od Umowy Ramowej w terminie 90 dni od dnia, gdy powziął wiadomość o przyczynie uzasadniającej odstąpienie.

4. Postanowienia niniejszego paragrafu nie ograniczają możliwości Centralnego Zamawiającego do zakończenia Umowy Ramowej w przypadku okoliczności, o których mowa w obowiązujących przepisach prawa, w tym na podstawie art. 456 Ustawy PZP.
5. Oświadczenie o odstąpieniu od Umowy Ramowej lub jej wypowiedzeniu zostanie złożone w formie pisemnej pod rygorem nieważności i będzie zawierało zwięzłe uzasadnienie. Centralny Zamawiający jest uprawniony do złożenia oświadczenia o wypowiedzeniu Umowy Ramowej lub odstąpieniu od Umowy Ramowej zarówno w całości jak i w części. Centralny Zamawiający w oświadczeniu o odstąpieniu od Umowy Ramowej wskaże w jakim zakresie odstępuje od Umowy Ramowej, tj. czy odstępuje od Umowy Ramowej z mocą wsteczną lub ze skutkiem na przyszłość.
6. Wykonawca niezwłocznie z chwilą złożenia przez Centralnego Zamawiającego oświadczenia o wypowiedzeniu Umowy Ramowej zobowiązuje się do powstrzymania się od dalszego wykonywania przedmiotu Umowy Ramowej z zastrzeżeniem dalszej realizacji zawartych już Umów Wykonawczych.
7. W przypadkach wskazanych w ust. 2 oraz ust. 4 Zamawiający odstąpi od Umowy Ramowej lub ją wypowie w stosunku do Wykonawcy, który dokonał naruszeń będących podstawą odstąpienia lub wypowiedzenia Umowy Ramowej.
8. Skorzystanie przez Centralnego Zamawiającego z uprawnienia do wypowiedzenia Umowy Ramowej lub odstąpienia od niej nie rodzi po stronie Wykonawcy jakichkolwiek roszczeń wobec Centralnego Zamawiającego, w szczególności z tytułu niewykonania lub nienależytego wykonania Umowy Ramowej lub jakichkolwiek

roszczeń odszkodowawczych z tego tytułu – z wyjątkiem wynagrodzenia z tytułu wykonania części Umów Wykonawczych do dnia wygaśnięcia Umowy Ramowej.

9. Odstąpienie od Umowy Ramowej lub jej wypowiedzenie nie wpływa na obowiązek zachowania poufności informacji.

§ 13

ZMIANY POSTANOWIEŃ UMOWY

1. W każdym czasie obowiązywania Umowy Ramowej Strony są uprawnione do dokonania nieistotnych zmian Umowy Ramowej, za które Strony traktują zmianę inną, niż zmiana istotna zdefiniowana w art. 454 ust. 2 Ustawy PZP.
2. Niezależnie od postanowienia ust. 1 powyżej, Strony są uprawnione do dokonania zmiany Umowy Ramowej w razie zaistnienia następujących okoliczności:
 - 1) w przypadku niewykorzystania środków wynikających z Umowy Ramowej w terminie wskazanym w § 3 ust. 1 przewiduje się zmianę terminu obowiązywania Umowy Ramowej, lecz o okres nie dłuższy niż 12 miesięcy, przy zastrzeżeniu, że maksymalna wartość Umowy Ramowej określona w § 5 ust. 1 nie ulegnie zmianie;
 - 2) w przypadku zmiany przepisów prawa lub wydania przez odpowiednie organy nowych wytycznych lub interpretacji dotyczących stosowania przepisów prawa, opublikowanych w Dzienniku Urzędowym Unii Europejskiej, Dzienniku Ustaw, Monitorze Polskim, Dzienniku Urzędowym odpowiedniego ministra lub innych oficjalnych publikatorach, w zakresie w jakim zmiana przepisów prawa lub wydane wytyczne lub interpretacje wymagają zmiany sposobu realizacji Umowy Ramowej, w tym mogą wymagać zmiany zakresu świadczeń Wykonawcy określonych w Umowie Ramowej;
 - 3) w przypadku wystąpienia przyczyn niezależnych od Wykonawcy związanych z równolegle prowadzonymi przez Centralnego Zamawiającego projektami mającymi wpływ na realizację Umowy Ramowej lub w związku ze zmianami okoliczności wynikającymi ze specyfiki działalności Centralnego Zamawiającego albo w związku z podjęciem przez Centralnego Zamawiającego decyzji o

przeprowadzeniu przez osobę trzecią kontroli jakości i sposobu prowadzenia prac, Centralny Zamawiający dopuszcza zmiany terminu realizacji Umowy Ramowej oraz przewiduje możliwość zwiększenia wynagrodzenia Wykonawcy pod warunkiem, że Wykonawca wykaże, że w celu uwzględnienia powyżej opisanych uwarunkowań leżących po stronie Centralnego Zamawiającego musi ponieść koszty, których zawarcie w cenie Oferty Wykonawcy nie było możliwe w dniu jej składania. Zmiana wysokości wynagrodzenia Wykonawcy dopuszczalna jest w oparciu o niniejsze postanowienie wyłącznie do wysokości niezbędnej do pokrycia kosztów, o których mowa w zdaniu poprzedzającym;

- 4) w przypadku uzasadnionych przyczyn technicznych lub funkcjonalnych powodujących konieczność zmiany sposobu wykonania Umowy Ramowej lub terminu realizacji Umowy Ramowej;
- 5) w przypadku zaistnienia Siły Wyższej w zakresie sposobu realizacji Umowy Ramowej lub terminu realizacji Umowy Ramowej;
- 6) w przypadku uzasadnionej przyczynami technicznymi konieczności zmiany zakresu przedmiotu Umowy Ramowej w obszarze wymagań funkcjonalnych lub niefunkcjonalnych, jeżeli zmiana ta skutkować będzie zoptymalizowaniem przedmiotu Umowy Ramowej do potrzeb Jednostek. Centralny Zamawiający dopuszcza wprowadzenie zmian w powyższym zakresie poprzez modyfikację wymagań Centralnego Zamawiającego lub zmianę sposobu ich realizacji;
- 7) w przypadku ograniczenia dostępności Oprogramowania, o ile Oprogramowanie zastępcze spełniają wszystkie wymagania określone w dokumentach zamówienia i Ofercie Wykonawcy, z zastrzeżeniem, że Wykonawca, pomimo zachowania należytej staranności, nie mógł temu zapobiec;
- 8) w przypadku opóźnień powstałych z przyczyn, za które Wykonawca i Jednostki nie odpowiadają dopuszczalna jest zmiana terminów wykonania przedmiotu Umowy Ramowej;
- 9) w przypadku gdy w toku realizacji Umowy Ramowej wdrożenie funkcjonalności określonych w OPZ okaże się zbędne dla Jednostek albo uzyskanie możliwości

objętych daną funkcjonalnością będzie możliwe przy zastosowaniu innych rozwiązań, dopuszczalna jest zmiana przedmiotu Umowy Ramowej;

- 10) w przypadku gdy z przyczyn od Wykonawcy niezależnych, w tym w szczególności z przyczyn leżących po stronie Centralnego Zamawiającego, nie jest możliwe dotrzymanie pierwotnego terminu wykonania przedmiotu Umowy Ramowej dopuszczalna jest zmiana terminu wykonania przedmiotu Umowy Ramowej, z zastrzeżeniem, że termin wykonania przedmiotu Umowy Ramowej może ulec zmianie o czas, o jaki wyżej wskazane okoliczności wpłynęły na termin wykonania przedmiotu Umowy Ramowej, to jest uniemożliwiły Wykonawcy terminową realizację przedmiotu Umowy Ramowej;
- 11) w przypadku zmian w sposobie funkcjonowania Centralnego Zamawiającego, w tym w przypadku zmian w zakresie sprawowania nadzoru nad działalnością Centralnego Zamawiającego, w związku ze zmianą organu sprawującego nadzór na działalnością Zamawiającego lub sposobu funkcjonowania tego organu, w zakresie sposobu realizacji Umowy Ramowej (np. sposobu licencjonowania) lub terminu realizacji Umowy Ramowej;
- 12) w przypadku wycofania z produkcji/sprzedaży jakiegokolwiek Oprogramowania wskazanego w OPZ lub wprowadzenia nowszego Oprogramowania niż wskazane w OPZ, Wykonawca dostarczy obecnie produkowaną/sprzedawaną wersję Oprogramowania o parametrach nie gorszych niż wymagane opisane w OPZ, w ramach cen jednostkowych netto określonych w Ofercie Wykonawcy. W takim przypadku Wykonawca zobowiązany jest do poinformowania Zamawiającego o tych okolicznościach oraz przedstawienia konfiguracji Oprogramowania aktualnie produkowanego celem akceptacji przez Centralnego Zamawiającego;
- 13) w przypadku obiektywnych trudności Wykonawcy w uzyskaniu pierwotnie oferowanego Oprogramowania wskazanego w OPZ dopuszczalna jest zmiana Oprogramowania na inny pod warunkiem, że cena jednostkowa produktu nie przewyższy ceny jednostkowej netto określonej w Ofercie Wykonawcy i zostaną zachowane wszelkie istotne wymagane parametry techniczne i jakościowe określone przez Centralnego Zamawiającego w OPZ oraz w Ofercie Wykonawcy.

W takim przypadku Wykonawca zobowiązany jest do poinformowania Centralnego Zamawiającego o tych okolicznościach oraz przedstawienia konfiguracji Oprogramowania aktualnie oferowanego celem akceptacji przez Centralnego Zamawiającego;

- 14) w przypadku wprowadzenia nowej wersji Oprogramowania przez producenta, która to wersja lub elementy nie były dostępne na rynku w chwili upływu terminu składania ofert, z zastrzeżeniem, że wskutek zmiany wszystkie istotne wymagania określone w dokumentach zamówienia zostaną zachowane, a wynagrodzenie Wykonawcy nie ulegnie podwyższeniu;
- 15) w przypadku ujawnienia się powszechnie występujących wad Oprogramowania Centralny Zamawiający dopuszcza zmianę w zakresie przedmiotu Umowy Ramowej polegającą na zastąpieniu danego Oprogramowania produktem zastępczym, spełniającym wszelkie wymagania przewidziane w OPZ dla Oprogramowania;
- 16) w przypadku wykrycia omyłek, rozbieżności lub niejasności w Umowie Ramowej, których nie można usunąć w inny sposób, a zmiana będzie umożliwiać ich usunięcie i doprecyzowanie Umowy Ramowej zgodnie z jej celem lub w celu jednoznacznej interpretacji jej zapisów przez Wykonawcę i Centralnego Zamawiającego; w przypadku, konieczności zmiany sposobu realizacji umów wykonawczych zawieranych w ramach niniejszej Umowy, polegającej na zastąpieniu Platformy innym narzędziem informatycznym lub innym sposobem realizacji tych czynności, w tym z wykorzystaniem poczty elektronicznej. Zmiana, o której mowa powyżej, może zostać wprowadzona w szczególności przypadku: braku dostępu do Platformy, utraty dostępu do Platformy, wystąpienia problemów technicznych uniemożliwiających prawidłowe korzystanie z Platformy, wdrożenia przez Centralnego Zamawiającego innego narzędzia zapewniającego funkcjonalność równoważną lub szerszą w zakresie obsługi umów wykonawczych, konieczności zapewnienia ciągłości realizacji Umowy w sytuacjach awaryjnych, zmian organizacyjnych po stronie Centralnego Zamawiającego wpływających na sposób realizacji zamówień wykonawczych.

3. Strony przewidują możliwość zmiany wysokości cen jednostkowych netto za poszczególne rodzaje Oprogramowania podane w Ofercie Wykonawcy i wynagrodzenia należnego Wykonawcy, o którym mowa w § 5 ust. 1 Umowy Ramowej, poprzez zawarcie aneksu do Umowy Ramowej, każdorazowo w przypadku wystąpienia jednej z następujących okoliczności:
- 1) zmiany stawki podatku od towarów i usług oraz podatku akcyzowego,
 - 2) zmiany wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 roku o minimalnym wynagrodzeniu za pracę,
 - 3) zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne,
 - 4) zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych
- na zasadach i w sposób określony w ust. 4 – 15 poniżej, jeżeli wskazane okoliczności będą miały wpływ na koszty wykonania Umowy Ramowej przez Wykonawcę.
4. Zmiana wysokości wynagrodzenia należnego Wykonawcy w przypadku zaistnienia przesłanki, o której mowa w ust. 3 pkt 1 powyżej, będzie odnosić się wyłącznie do części przedmiotu Umowy Ramowej, do której zastosowanie znajdzie zmiana stawki podatku od towarów i usług lub podatku akcyzowego po dniu wejścia w życie przepisów zmieniających stawkę podatku.
5. W przypadku zmiany, o której mowa w ust. 3 pkt 1 powyżej, wartość wynagrodzenia netto nie zmieni się, a wartość wynagrodzenia brutto zostanie wyliczona na podstawie nowych przepisów.
6. Zmiana wysokości wynagrodzenia w przypadku zaistnienia przesłanki, o której mowa w ust. 3 pkt 2 lub pkt 3 lub pkt 4 powyżej, będzie obejmować wyłącznie część wynagrodzenia należnego Wykonawcy, w odniesieniu do której nastąpiła zmiana

wysokości kosztów wykonania Umowy Ramowej przez Wykonawcę w związku z wejściem w życie przepisów odpowiednio zmieniających wysokość minimalnego wynagrodzenia za pracę albo wysokość minimalnej stawki godzinowej lub dokonujących zmian w zakresie zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub w zakresie wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne albo wysokość kosztów realizacji przedmiotu Umowy Ramowej w związku z wprowadzeniem pracowniczych planów kapitałowych.

7. W przypadku zmiany, o której mowa w ust. 3 pkt 2 powyżej, wynagrodzenie Wykonawcy ulegnie zmianie o kwotę odpowiadającą wzrostowi kosztu Wykonawcy w związku ze zwiększeniem wysokości wynagrodzeń pracowników świadczących usługi na podstawie Umowy Ramowej do wysokości aktualnie obowiązującego minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, z uwzględnieniem wszystkich obciążeń publicznoprawnych od kwoty wzrostu minimalnego wynagrodzenia.
8. W przypadku zmiany, o której mowa w ust. 3 pkt 3 oraz pkt 4 powyżej, wynagrodzenie Wykonawcy ulegnie zmianie o kwotę odpowiadającą zmianie kosztu Wykonawcy ponoszonego w związku z wypłatą wynagrodzenia pracownikom świadczącym usługi na podstawie Umowy Ramowej lub w związku z ponoszeniem przez Wykonawcę kosztów wynikających z wprowadzenia pracowniczych planów kapitałowych. Kwota odpowiadająca zmianie kosztu Wykonawcy będzie odnosić się wyłącznie do części wynagrodzenia pracowników świadczących usługi, o których mowa w zdaniu poprzedzającym, odpowiadającej zakresowi, w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy Ramowej.
9. W celu zawarcia aneksu, o którym mowa w ust. 3 powyżej, każda ze Stron może wystąpić do drugiej Strony z wnioskiem o dokonanie zmiany wysokości wynagrodzenia należnego Wykonawcy wraz z uzasadnieniem zawierającym w szczególności szczegółowe wyliczenie całkowitej kwoty, o jaką wynagrodzenie Wykonawcy powinno ulec zmianie, oraz wskazaniem daty, od której nastąpiła bądź

nastąpi zmiana wysokości kosztów wykonania Umowy Ramowej, uzasadniająca zmianę wysokości wynagrodzenia należnego Wykonawcy.

10. W przypadku zmian, o których mowa w ust. 3 pkt 2 lub pkt 3 lub pkt 4 powyżej, jeżeli z wnioskiem występuje Wykonawca, jest on zobowiązany dołączyć do wniosku dokumenty, z których będzie wynikać, w jakim zakresie zmiany te mają wpływ na koszty wykonania Umowy Ramowej, w szczególności:

- 1) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie) pracowników świadczących usługi (bez ujawniania tzw. „danych wrażliwych”), wraz z określeniem zakresu, w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy Ramowej oraz części wynagrodzenia odpowiadającej temu zakresowi – w przypadku zmiany, o której mowa w ust. 3 pkt 2 powyżej, lub
- 2) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie) pracowników świadczących usługi (bez ujawniania tzw. „danych wrażliwych”), wraz z kwotami składek uiszczanych do Zakładu Ubezpieczeń Społecznych/Kasy Rolniczego Ubezpieczenia Społecznego w części finansowanej przez Wykonawcę, z określeniem zakresu (części etatu), w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy Ramowej oraz części wynagrodzenia odpowiadającej temu zakresowi – w przypadku zmiany, o której mowa w ust. 3 pkt 3 powyżej, lub
- 3) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie) pracowników świadczących usługi (bez ujawniania tzn. danych wrażliwych) wraz z kwotami składek uiszczanych w ramach pracowniczych planów kapitałowych w części finansowanej przez Wykonawcę, z określeniem zakresu (części etatu), w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy Ramowej oraz części wynagrodzenia odpowiadającej temu zakresowi – w przypadku zmiany, o której mowa w ust. 3 pkt 4 powyżej.

11. W przypadku zmiany, o której mowa w ust. 3 pkt 3 lub pkt 4 powyżej, jeżeli z wnioskiem występuje Centralny Zamawiający, jest on uprawniony do zobowiązania Wykonawcy do przedstawienia w wyznaczonym terminie, nie krótszym niż 10 Dni

- Roboczych, dokumentów, z których będzie wynikać, w jakim zakresie zmiana ta ma wpływ na koszty wykonania Umowy Ramowej, w tym pisemnego zestawienia wynagrodzeń, o którym mowa w ust. 10 pkt 2 i 3 powyżej.
12. W terminie do 30 Dni Roboczych od dnia przekazania wniosku, o którym mowa w ust. 10 powyżej, Strona, która otrzymała wniosek, przekaże drugiej Stronie informację o zakresie, w jakim zatwierdza wniosek oraz wskaże kwotę, o którą wynagrodzenie należne Wykonawcy powinno ulec zmianie, albo informację o niezatwierdzeniu wniosku wraz z uzasadnieniem.
 13. W przypadku otrzymania przez Stronę informacji o niezatwierdzeniu wniosku lub częściowym zatwierdzeniu wniosku, Strona ta może ponownie wystąpić z wnioskiem, o którym mowa w ust. 9 powyżej. W takim przypadku przepisy ust. 10 - 12 powyżej stosuje się odpowiednio.
 14. Zawarcie aneksu nastąpi nie później niż w terminie 14 Dni Roboczych od dnia zatwierdzenia wniosku o dokonanie zmiany wysokości wynagrodzenia należnego Wykonawcy.

§ 14

WALORYZACJA W TRYBIE ART. 439 PZP

1. Zgodnie z przepisem art. 439 Pzp Umowa Ramowa reguluje zasady wprowadzania zmian wysokości wynagrodzenia należnego Wykonawcy w przypadku zmiany ceny materiałów lub kosztów związanych z realizacją Umowy Ramowej.
2. Strony dopuszczają możliwość zmiany wynagrodzenia Wykonawcy w przypadku zmiany cennika producenta Oprogramowania (dalej: „**Cennik**”).
3. Wykonawca zobowiązuje się do dostarczenia pierwszego Cennika w terminie 7 dni od dnia zawarcia Umowy. Brak dostarczenia Cennika przez Wykonawcę uniemożliwia dokonanie waloryzacji wynagrodzenia.
4. Dostarczony Cennik musi być wiarygodny przez co należy rozumieć:

- 1) oficjalny cennik producenta Oprogramowania upubliczniony na oficjalnych stronach internetowych producenta, które zostaną wskazane przez Wykonawcę lub,
 - 2) dokument opracowany przez Wykonawcę i złożony wraz z oświadczeniem producenta w zakresie wysokości cen Oprogramowania.
5. Waloryzacja wynagrodzenia może nastąpić wyłącznie w odniesieniu do cen jednostkowych wskazanych w Ofercie.
 6. Zmiana cen jednostkowych wskazanych w Ofercie następuje proporcjonalnie do procentowej zmiany ceny Oprogramowania w aktualnym Cenniku producenta, w stosunku do Cennika, o którym mowa w ust. 3 powyżej.
 7. Wniosek o podwyższenie wynagrodzenia Wykonawcy może zostać złożony jednokrotnie w okresie każdych kolejnych 6 miesięcy wykonywania Umowy Ramowej, licząc od dnia zawarcia Umowy Ramowej. W celu uniknięcia wątpliwości, Strony uzgadniają, że zmiana wynagrodzenia, zgodnie z postanowieniami niniejszego §14 Umowy, nie może być dokonana częściej niż raz na każde 6 miesięcy wykonywania Umowy Ramowej.
 8. Zwaloryzowana cena przedmiotu Umowy Ramowej będzie wykorzystywana do rozliczenia pomiędzy Stronami wyłącznie dla ceny Oprogramowania które nie było dotychczas objęte Zamówieniem Wykonawczym i co do którego nie została zawarta Umowa Wykonawcza. Wynagrodzenie za Oprogramowanie należne Wykonawcy, wynikające z różnicy pomiędzy wynagrodzeniem wynikającym z Oferty Wykonawcy a ustaloną zgodnie z ust. 7 waloryzacją, będzie podstawą do ustalenia przez Wykonawcę cen w Ofercie Wykonawczej i dokonywanych na jej podstawie rozliczeń w ramach Umów Wykonawczych.
 9. Zamawiający dopuszcza maksymalne podwyższenie każdej z cen jednostkowych wskazanych w Ofercie maksymalnie o **10 %** w efekcie zastosowania postanowień niniejszego paragrafu.
 10. Wykonawca, którego wynagrodzenie zostało zmienione zgodnie z niniejszym paragrafem, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom Cennika, dotyczących zobowiązania podwykonawcy, jeżeli przedmiotem umowy są dostawy lub usługi oraz okres obowiązywania umowy przekracza 6 miesięcy.

11. Występując o zmianę wynagrodzenia zgodnie z postanowieniami niniejszego paragrafu, Strona zobowiązana jest do złożenia pisemnego pod rygorem nieważności wniosku. We wniosku należy wykazać, że zaistniały wskazane w niniejszym paragrafie przesłanki do dokonania zmiany wynagrodzenia w szczególności, że doszło do zmiany Cennika uprawniającej do dokonania zmiany wynagrodzenia oraz załączyć Cennik w formie, o której mowa w ust. 4 powyżej. Strony zastrzegają sobie prawo do żądania dokumentów lub wyjaśnień w celu rozpatrzenia wniosku wymienionego w zdaniu poprzedzającym.

§ 15

PRZEDSTAWICIELE STRON

1. Przedstawicielem ze strony Centralnego Zamawiającego w zakresie realizacji obowiązków umownych jest:

[REDACTED]

[REDACTED]

2. Przedstawicielem ze strony Wykonawców w zakresie realizacji obowiązków umownych jest:

Servcomp sp. z o.o.:

[REDACTED]

Ikaria sp. z o.o. sp.k.:

[REDACTED]

Perceptus sp. z o.o. :

[REDACTED]

[REDACTED]

- 
3. Osoby wymienione w ust. 1 i ust. 2 powyżej odpowiedzialne są merytorycznie za nadzór nad prawidłowością i terminowością realizacji Umowy Ramowej, w szczególności upoważnione są do monitorowania należytego wykonania Umowy Ramowej i prowadzenia bieżącej korespondencji. Wykonawca zobowiązuje się zapewnić, że przez cały okres wykonywania Umowy Ramowej, Wykonawca będzie reprezentowany przez co najmniej dwie osoby, wskazane w ust. 2 i każda z tych osób będzie uprawniona do samodzielnej reprezentacji Wykonawcy w zakresie, o którym mowa w zd. 1.
 4. Wszelka korespondencja prowadzona pomiędzy Stronami w związku z realizacją Umowy Ramowej będzie przekazywana, z zastrzeżeniem ust. 5 poniżej lub innych postanowień Umowy Ramowej, w formie dokumentowej na wskazane powyżej adresy e-mail przedstawicieli Stron.
 5. Wszelka korespondencja prowadzona pomiędzy Stronami w związku z Umową Ramowej, co do której zastrzeżono formę pisemną, będzie przesyłana zgodnie z § 17 ust. 4 Umowy Ramowej.
 6. Zmiana wskazanych w Umowie Ramowej danych adresowych lub numerów telefonów lub adresów e-mail nie stanowi zmiany Umowy Ramowej i może być dokonywana przez Stronę, której dotyczy oraz staje się skuteczna wobec drugiej Strony z chwilą otrzymania przez nią zawiadomienia w formie pisemnej, z zastrzeżeniem ust. 7 poniżej.
 7. Zmiana osoby wskazanej w ust. 1 lub ust. 2 powyżej lub jej danych kontaktowych nie wymaga zmiany Umowy Ramowej, ale wymaga dla swej skuteczności uprzedniego powiadomienia drugiej Strony, co najmniej w formie dokumentowej, przez osobę uprawnioną do reprezentacji danej Strony.

§ 16

SIŁA WYŻSZA

1. Żadna ze Stron nie będzie odpowiedzialna za niewykonanie swoich zobowiązań w

ramach Umowy Ramowej w przypadku, jeśli zostało ono spowodowane zaistnieniem Siły Wyższej.

2. Strona powołująca się na Siłę Wyższą przekaze drugiej Stronie powiadomienie o zaistnieniu lub możliwości zaistnienia Siły Wyższej w możliwie najszybszym czasie, nie później jednak niż terminie 3 Dni Roboczych od:
 - 1) wystąpienia Siły Wyższej, w tym rozpoczęcia działania Siły Wyższej,
 - 2) powzięcia wiedzy o możliwości zaistnienia Siły Wyższej.
3. Strona powołująca się na Siłę Wyższą przekaze drugiej Stronie wraz z powiadomieniem o zaistnieniu lub możliwości zaistnienia Siły Wyższej informację o:
 - 1) spodziewanych skutkach działania Siły Wyższej dla możliwości prawidłowego wykonywania Umowy Ramowej,
 - 2) czasie rozpoczęcia i spodziewanym czasie zakończenia Siły Wyższej,
 - 3) proponowanych działaniach, które mogą zminimalizować wpływ Siły Wyższej na wykonywanie Umowy Ramowej.
4. Strona otrzymująca powiadomienie o zaistnieniu lub możliwości zaistnienia Siły Wyższej jest zobowiązana do niezwłocznego, nie później niż w terminie 3 Dni Roboczych, ustosunkowania się do proponowanych działań, o których mowa w ust. 3 pkt 3 powyżej, jeżeli te działania wymagają interakcji z tą Stroną, tj. do wskazania terminu w którym zostaną one podjęte lub przedstawienia uzasadnienia, dlaczego ich podjęcie nie jest możliwe.
5. Strony zobowiązują się do współpracy w celu zminimalizowania wpływu Siły Wyższej dla wykonywania Umowy Ramowej.

§ 17

PRAWA WŁASNOŚCI INTELEKTUALNEJ

1. Na podstawie każdej poszczegółnej Umowy Wykonawczej Wykonawca zapewni udzielenie licencji na będące przedmiotem tej Umowy Wykonawczej Oprogramowanie. Celem umowy ramowej jest zapewnienie Jednostkom

możliwości korzystania z całości Oprogramowania dostarczanego w ramach danej Umowy Wykonawczej, jak i wszystkich jego elementów i aktualizacji, w sposób i w celu opisanym w umowie ramowej i umowie wykonawczej, w pełnym zakresie i bez dodatkowych kosztów. Wszystkie postanowienia Umowy i złożone oświadczenia Wykonawcy interpretuje się w myśl tego postanowienia Umowy.

2. Do licencji zapewnianej w ramach Umów Wykonawczych zastosowanie mają tzw. standardowe warunki licencyjne producenta. warunki te jednak nie mogą być sprzeczne z postanowieniami Umowy Ramowej a odpowiedzialność za ich zgodność z Umową Ramową ponosi wykonawca.
3. Wykonawca zapewnia, że warunki korzystania z Oprogramowania w ramach Umów Wykonawczych nie będą wymagać od Jednostek ponoszenia jakichkolwiek opłat lub kosztów na rzecz Wykonawcy ani innych podmiotów, które nie zostały wprost wskazane w Umowie Ramowej lub Umowie Wykonawczej. Wynagrodzenie określone przez Umowę Wykonawczą obejmować będzie każdorazowo całość wynagrodzenia za korzystanie z Oprogramowania objętego Umową Wykonawczą.
4. Bez uszczerbku dla OPZ Wykonawca zapewnia, że Oprogramowanie dostarczane w oparciu o Umowę Wykonawczą nie będzie zawierało ograniczeń polegających na tym, że Oprogramowanie może być używane wyłącznie z innym oprogramowaniem lub może być wdrażane, serwisowane itp. wyłącznie przez określony podmiot lub grupę podmiotów.
5. Wykonawca zobowiązany jest w ramach realizacji Umowy Wykonawczej zapewnić udzielenie Jednostce licencji na Oprogramowanie będące przedmiotem Umowy Wykonawczej, obejmującej prawo do korzystania z tego Oprogramowania na następujących polach eksploatacji:
 - 1) prawo do korzystania z Oprogramowania, w tym ze wszystkich funkcjonalności tego Oprogramowania w dowolny sposób w liczbie kopii/ stanowisk/ serwerów/ użytkowników zgodnej z tym co wynika z Umowy Ramowej i Wykonawczej.
 - 2) prawo do instalowania Oprogramowania, na które udzielana jest licencja w liczbie kopii/ stanowisk/ serwerów/ użytkowników zgodnej z tym co wynika z Umowy Ramowej i Wykonawczej.

- 3) prawo do aktualizowania Oprogramowania, w tym instalowania i korzystania z aktualizacji Oprogramowania, na które udzielana jest licencja lub aktualizacja licencji poprzez zażądania i zainstalowanie nowszych wersji Oprogramowania z zachowaniem wszystkich pól eksploatacji wymienionych w niniejszej umowie,
 - 4) prawo do instalowania i korzystania z wszelkich poprawek i uzupełnień opublikowanych na stronach producenta Oprogramowania na polach eksploatacji określonych w opublikowanych przez producenta oprogramowania warunkach licencyjnych,
 - 5) prawo do trwałego lub czasowego zwielokrotniania Oprogramowania w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, w tym zwielokrotniania dokonywanego podczas wprowadzania, wyświetlania, stosowania, przekazywania lub przechowywania oprogramowania,
 - 6) prawo do utrwalania i zwielokrotniania dowolną techniką, w tym techniką zapisu magnetycznego lub techniką cyfrową, taką jak zapis na płycie CD, DVD, Blu-ray, urządzeniu z pamięcią flash lub jakimkolwiek innym nośniku pamięci,
 - 7) prawo do rozpowszechniania Oprogramowania, jeżeli jest to potrzebne dla wykorzystania funkcjonalności Oprogramowania oraz do korzystania z Oprogramowania w celu wynikającym z OPZ.
6. Licencje, o których mowa w ust. 6, będą niewyłączne, nieograniczone terytorialnie i udzielone na czas określony, tj. czas obowiązywania danej Umowy Wykonawczej.
 7. Licencje, o których mowa w ust. 6, będą pozwalają na swobodne przenoszenie korzystania z Oprogramowania pomiędzy stacjami roboczymi i serwerami (np. w przypadku wymiany sprzętu) oraz na udzielanie dalszych licencji (sublicencji) na korzystanie z oprogramowania przez Jednostki.
 8. Wykonawca zapewnia, że Jednostkom w ramach udzielonych im licencji, o których mowa w ust. 6, przysługiwać będzie możliwość nieograniczonej ilości zastosowania Oprogramowania, uprawniającą jednostki co najmniej do:
 - 1) wykorzystywania wszystkich przewidzianych dla danego zamówionego Oprogramowania jego funkcjonalności,
 - 2) przenoszenia licencji lub aktualizacji licencji pomiędzy Jednostkami,

- 3) uruchamiania Oprogramowania przez użytkownika na którymkolwiek z urządzeń po autoryzacji użytkownika,
 - 4) korzystania z wytworów powstałych w wyniku eksploatacji Oprogramowania oraz modyfikowania tych wytworów i dalszego z nich korzystania, w tym publikowania i wyświetlania w całości i w części w Internecie i innych mediach bez ograniczeń.
9. W ramach pozyskanego oprogramowania Jednostka będąca licencjobiorcą będzie uprawniona do udzielenia sublicencji innym Jednostkom, na warunkach, zasadach, polach eksploatacji i w zakresie, w jakim jednostce zostaną udzielone licencje na podstawie niniejszej Umowy Ramowej i poszczególnych Umów wykonawczych.
10. Wraz z dostarczonym Oprogramowaniem Wykonawca dostarczy lub udostępni za pośrednictwem witryny producenta dokumenty określające zasady licencjonowania – warunki korzystania z oprogramowania.
11. Jeżeli wraz z Oprogramowaniem Wykonawca dostarczył Zamawiającemu dokumentację dotyczącą tego oprogramowania, Wykonawca zobowiązany jest wraz z udzieleniem licencji na to Oprogramowanie udzielić lub zapewnić udzielenie licencji na tę dokumentację, obejmującą pola eksploatacji:
- 1) w zakresie utrwalania i zwielokrotniania: wytwarzanie dowolną techniką egzemplarzy utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową,
 - 2) w zakresie obrotu oryginałem albo egzemplarzami, na których ją utrwalono: wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarza,
 - 3) w zakresie rozpowszechniania utworów w sposób inny niż określony powyżej: publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie tej dokumentacji w taki sposób, aby każdy mógł mieć do niej dostęp w miejscu i w czasie przez siebie wybranym.
12. Licencja na dokumentację, o której mowa w ust. 11 powyżej obejmuje także zezwolenie na wykonywanie zależnych praw autorskich do wszelkich opracowań tej dokumentacji, to jest rozporządzanie i korzystanie z takich opracowań w zakresie wszystkich uprawnień nabytych przez jednostkę stosownie do postanowień

niniejszego paragrafu, w szczególności na polach eksploatacji wskazanych powyżej.

13. Licencja na dokumentację, o której mowa w ust. 12 powyżej dotyczy tylko dokumentacji standardowo dołączanej do danego oprogramowania przez producenta, która nie została wytworzona wyłącznie w celu i w związku z realizacją umowy ramowej lub umowy wykonawczej.
14. Aktualizacja lub zmiana wersji oprogramowania dostarczonego w ramach umowy wykonawczej nie może powodować ograniczenia zakresu uprawnień jednostek, o wynikających z umowy ramowej ani umowy wykonawczej. W takim przypadku do aktualizacji lub zmienionej wersji oprogramowania stosuje się postanowienia tych umów dotyczące licencji.

§ 18

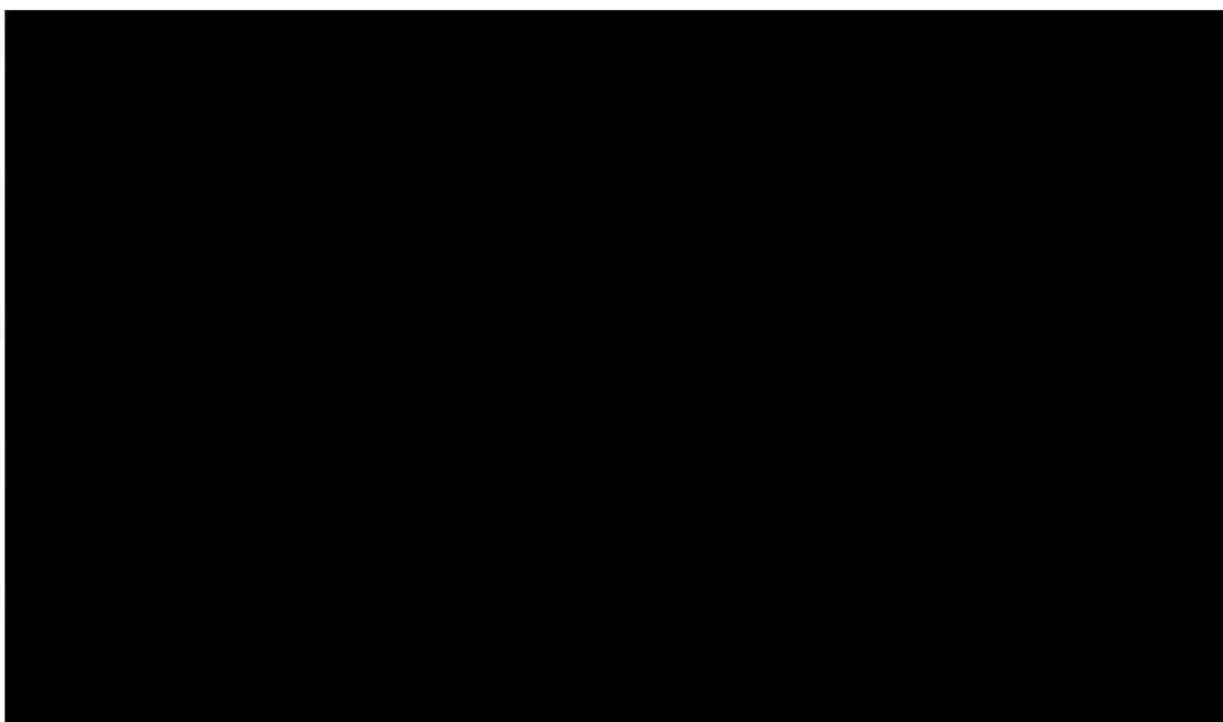
POSTANOWIENIA KOŃCOWE

1. Wykonawca nie ma prawa dokonywać przeniesienia bądź obciążenia swoich praw lub obowiązków wynikających z Umowy Ramowej bez uzyskania uprzedniej zgody Centralnego Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności.
2. W przypadku gdy jakiegokolwiek postanowienia Umowy Ramowej są nieważne lub bezskuteczne, pozostałe postanowienia Umowy Ramowej pozostają w mocy i są wiążące we wzajemnych stosunkach Stron. W przypadku nieważności lub bezskuteczności jednego lub więcej postanowień Umowy Ramowej, Strony zobowiązują się zgodnie dążyć do ustalenia takiej treści Umowy Ramowej, która będzie optymalnie odpowiadała zgodnym intencjom Stron, celowi i przeznaczeniu Umowy Ramowej oraz zaistniałym okolicznościom.
3. Centralny Zamawiający jest instytucją gospodarki budżetowej. Funkcję organu założycielskiego w stosunku do Zamawiającego w rozumieniu przepisów ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych wykonuje MC. Zważywszy na powyższe Wykonawca wyraża zgodę na przeniesienie wszystkich praw i obowiązków Centralnego Zamawiającego wynikających z Umowy Ramowej na jednostkę nadzorującą, MC, bądź inną jednostkę rządową, która sprawować będzie funkcję jednostki nadzorującej wobec Centralnego Zamawiającego, bez konieczności

uzyskania odrębnej zgody Wykonawcy, producenta lub podmiotu przez niego autoryzowanego.

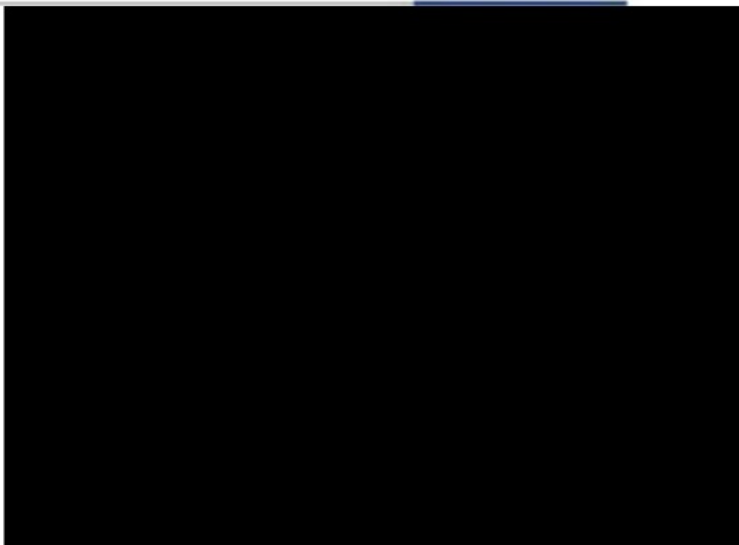
4. Z zastrzeżeniem pozostałych postanowień Umowy Ramowej, wszelkie oświadczenia związane z Umową Ramową dla których zastrzeżono formę pisemną, składane będą przez Stronę za pokwitowaniem odbioru lub listem poleconym na adres korespondencyjny Wykonawcy lub Zamawiającego, pod rygorem uznania za niedoręczoną. Strony zgodnie potwierdzają, że w przypadku złożenia oświadczenia, o którym mowa w zdaniu poprzednim, przez którąkolwiek ze Stron, w postaci elektronicznej i opatrzenia go kwalifikowanym podpisem elektronicznym oraz przesłania za pomocą poczty elektronicznej na adres przedstawiciela Strony, o którym mowa w postanowieniach § 15 ust. 1 i ust. 2 Umowy Ramowej, a w przypadku Wykonawcy również na adres e-mail Centralnego Zamawiającego: coi@cyfra.gov.pl (łącznie), takie oświadczenie jest tożsame z oświadczeniem złożonym w formie pisemnej i dostarczeniem go do siedziby Strony. W takiej sytuacji Strona, która otrzymała oświadczenia, zobowiązana jest niezwłocznie potwierdzić drugiej Stronie otrzymanie oświadczenia w formie elektronicznej. Wszelkie zmiany adresów Strony będą komunikować sobie niezwłocznie pod rygorem uznania korespondencji za doręczoną. Strony oświadczają, że ich aktualne adresy korespondencyjne są następujące:

- 1)
- 2)
- 3)
- 4)
- 5)



5. W przypadku zaistnienia pomiędzy Stronami sporu wynikającego z Umowy Ramowej lub pozostającego w związku z Umową Ramową, każda ze Stron jest uprawniona do podjęcia próby jego rozwiązania w drodze mediacji. Mediacja prowadzona będzie przez Mediatorów Stałych Sądu Polubownego przy Prokuraturii Generalnej Rzeczypospolitej Polskiej zgodnie z Regulaminem tego Sądu. W przypadku niepowodzenia w rozwiązaniu sporu w drodze mediacji spory wynikłe na tle wykonywania Umowy Ramowej będą rozstrzygane przez sąd właściwy dla siedziby Centralnego Zamawiającego.
6. Wszelkie zmiany postanowień zawartej Umowy Ramowej wymagają zachowania formy pisemnej pod rygorem nieważności takiej zmiany, z zastrzeżeniem wyraźnie odmiennych postanowień Umowy Ramowej oraz z uwzględnieniem postanowień ust. 7 poniżej.
7. Zgodnie z art. 78¹ § 2 Kodeksu cywilnego Strony zgodnie potwierdzają, że złożenie oświadczenia, przez którąkolwiek ze Stron, w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym jest tożsame z oświadczeniem złożonym w formie pisemnej i stanowi zachowanie wymogu co do formy określonego w Umowie Ramowej.
8. W przypadku rozbieżności interpretacyjnych pomiędzy postanowieniami Umowy Ramowej /Umowy Wykonawczej a treścią załączników i innych dokumentów stanowiących integralną część Umowy Ramowej /Umowy Wykonawczej lub wytworzonych przez Strony, pierwszeństwo mają postanowienia umowne.
9. Umowa Ramowa podlega prawu polskiemu.
10. Umowę Ramową zawarto w formie elektronicznej.
11. Poniższe Załączniki do Umowy Ramowej stanowią jej integralną część:
- 1) Załącznik nr 1 - Oferty Wykonawców;
 - 2) Załącznik nr 2 - Opis Przedmiotu Zamówienia;
 - 3) Załącznik nr 3 - Wzór Umowy Wykonawczej;

- 4) Załącznik nr 4 - Klauzula informacyjna Zamawiającego;
- 5) Załącznik nr 5 - Klauzula informacyjna Wykonawcy;
- 6) Załącznik nr 6 - informacja odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców Centralnego Zamawiającego;
- 7) Załącznik nr 7 - informacja odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców Wykonawcy Servcomp sp. z o.o.;
- 8) Załącznik nr 8 - informacja odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców Wykonawcy Ikaria sp. z o.o. sp.k.;
- 9) Załącznik nr 9 - informacja odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców Wykonawcy Perceptus sp. z o.o.;
- 10) Załącznik nr 10 – wydruk z CEiDG ;
- 11) Załącznik nr 11 - informacja odpowiadającą odpisowi pełnemu z rejestru przedsiębiorców Wykonawcy Seven sp. z o.o.;



ROZDZIAŁ IV – FORMULARZ OFERTY WRAZ Z ZAŁĄCZNIKAMI

OFERTA

na Umowa ramowa na dostawę oprogramowania antywirusowego.

nr referencyjny: COI-ZAK.262.71.2025

Centralny Zamawiający:

Centralny Ośrodek Informatyki

Al. Jerozolimskie 132-136

02-305 Warszawa

1. WYKONAWCA:

Niniejsza oferta zostaje złożona przez¹:

Lp.	Nazwa(y) Wykonawcy(ów)	Adres(y) Wykonawcy(ów)	NIP /KRS / REGON / kapitał zakładowy
	Servcomp sp. z o.o.	Ul. Oleska 11, 42-700 Lubliniec	NIP PL5751906703 KRS 0000993464 REGON 52319177100000 Kapitał zakładowy: 20 000 PLN

2. DANE KONTAKTOWE WYKONAWCY²:

[wszelka korespondencja prowadzona będzie wyłącznie na nw. adres / e-mail]:

¹ Wykonawca modeluje tabelę powyżej w zależności od swego składu;

² Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wskazują dane pełnomocnika (lidera), z którym prowadzona będzie wszelka korespondencja;



3. OŚWIADCZENIA

Ja(my) niżej podpisany(i) oświadczam(y), że:

- 4.1.do przedmiotowych dokumentów, w tym zwłaszcza do opisu przedmiotu zamówienia i projektowanych postanowień umowy, nie wnoszę żadnych zastrzeżeń i akceptuję je w pełni,
- 4.2.uzyskał(śmy) wszelkie niezbędne informacje do przygotowania oferty i wykonania zamówienia,
- 4.3.w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia,
- 4.4.w przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy ramowej w miejscu i terminie określonym przez Centralny Ośrodek Informatyki,
- 4.5.uważamy się za związanych niniejszą ofertą przez okres wskazany w SWZ,
- 4.6.oferujemy realizację niniejszego zamówienia, zgodnie z opisem przedmiotu zamówienia, zawartym w rozdziale II SWZ,
- 4.7.akceptuję/emy termin płatności za realizację przedmiotu umowy w ciągu 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT,
- 4.8.w kryterium: Deklarowany poziom cyberbezpieczeństwa usługi chmurowej [D] jest zgodny z:

SCCO 2	☒ nie ☐ tak
--------	--

** W przypadku braku wskazania w Formularzu oferty „Deklarowanego poziomu cyberbezpieczeństwa usługi chmurowej” Zamawiający uzna, że Wykonawcy deklaruje poziom SCCO 1 i przyzna 0 pkt w ramach kryterium „Deklarowany poziom cyberbezpieczeństwa usługi chmurowej”.*

4.9. wybór niniejszej oferty³:

- ☒ **NIE** prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego, zgodnie z przepisami o podatku od towarów i usług,
- ☐ prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług i wskazujemy poniżej nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazujemy ich wartość bez kwoty podatku:

Lp.	Nazwa (rodzaj)	Stawka podatku VAT	Wartość bez kwoty podatku
1.	_____		_____ zł
...	_____		_____ zł

4.10. jestem/ nie jestem⁴ czynnym podatnikiem podatku VAT,

4.11. wadium wpłacone w pieniądzu należy zwrócić na rachunek bankowy prowadzony w banku⁵:



4.12. niniejsze zamówienie⁶:

- ☒ w całości wykonam siłami własnymi,
- ☐ zaangażuję podwykonawców do realizacji przedmiotu zamówienia:
- i wskazuję części zamówienia, którą zamierzam powierzyć podwykonawcy:

4.13. dane rejestrowe podwykonawców, którym zamierzam powierzyć realizację

³ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy; w przypadku, gdy wybór oferty prowadzi do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług należy wskazać w tabeli nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazać ich wartość bez kwoty podatku;

⁴ niepotrzebne skreślić;

⁵ uzupełnić odpowiednio miejsca podając nazwę banku i numer konta – dotyczy wadium wnoszonego w pieniądzu;

⁶ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy, w przypadku zaangażowania podwykonawców do realizacji przedmiotu zamówienia należy wskazać części zamówienia, które Wykonawca zamierza powierzyć podwykonawcy;

części zamówienia, o których mowa w pkt. 4.13⁷:

Lp.	Nazwa(y) podwykonawcy(ów)	Adres(y) siedziby podwykonawcy(ów)	Numer wpisu do odpowiedniego rejestru – KRS lub datę rozpoczęcia działalności z CEIDG	NIP oraz Regon

- 4.14. Oświadczam/y, że zastrzegamy/nie zastrzegamy⁸ części oferty jako tajemnica przedsiębiorstwa, w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity: Dz.U. z 2022 r., poz. 11233, z późn. zm.) i w związku z tym informacje zawarte w plikach..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ww. przepisów. Pozostałe części oferty oraz załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa.
- 4.15. Oświadczam/y, że zapoznaliśmy się z Klauzulą Informacyjną Centralnego Ośrodka Informatyki dotyczącą RODO⁹ zamieszczoną w Rozdziale I SWZ – Instrukcja dla Wykonawców.
- 4.16. Oświadczam/y, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/liśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu, w tym również wykonałem/liśmy obowiązek, który ciąży na mnie/nas zgodnie z „Informacją o przetwarzaniu danych osobowych osób fizycznych, których dane są przekazywane Centralnemu Ośrodkowi Informatyki przez Wykonawcę w toku postępowania o udzielenie zamówienia publicznego oraz w toku wykonywania

⁷ uzupełnić odpowiednio – o ile są znane;

⁸ Niepotrzebne skreślić; wypełnić tylko, gdy dotyczy; przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności; w takim przypadku należy wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

umowy”¹⁰

4. CENA OFERTY

- 5.1. oświadczam, że cena zawiera wszelkie koszty jakie Wykonawca poniesie w związku z realizacją zamówienia,
- 5.2. gwarantuję wykonanie niniejszego zamówienia zgodnie z treścią SWZ,
- 5.3. oferujemy wykonanie zamówienia zgodnie z cenami zaoferowanymi w Tabeli cenowej poniżej:

¹⁰ W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Tabela cenowa:

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia <u>tylko</u> w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 12 miesięcy subskrypcji		Netto: 79,14 zł Kwota VAT: 18,20 zł Brutto: 97,34 zł	Netto: 67,36 zł Kwota VAT: 15,49 zł Brutto: 82,85 zł	Netto: 59,46 zł Kwota VAT: 13,68 zł Brutto: 73,14 zł	Netto: 55,39 zł Kwota VAT: 12,74 zł Brutto: 68,13 zł	Netto: 70,31 zł Kwota VAT: 16,17 zł Brutto: 86,48 zł	Netto: 64,76 zł Kwota VAT: 14,89 zł Brutto: 79,65 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 24 miesiące		Netto: 158,28 zł Kwota VAT: 36,40 zł Brutto: 194,68 zł	Netto: 134,72 zł Kwota VAT: 30,99 zł Brutto: 165,71 zł	Netto: 118,92 zł Kwota VAT: 27,35 zł Brutto: 146,27 zł	Netto: 110,77 zł Kwota VAT: 25,48 zł Brutto: 136,25 zł	Netto: 140,62 zł Kwota VAT: 32,34 zł Brutto: 172,96 zł	Netto: 129,53 zł Kwota VAT: 29,79 zł Brutto: 159,32 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 36 miesięcy subskrypcji		Netto: 237,42 zł Kwota VAT: 54,61 zł Brutto: 292,03 zł	Netto: 202,08 zł Kwota VAT: 46,48 zł Brutto: 248,56 zł	Netto: 178,38 zł Kwota VAT: 41,03 zł Brutto: 219,41 zł	Netto: 166,16 zł Kwota VAT: 38,22 zł Brutto: 204,38 zł	Netto: 210,92 zł Kwota VAT: 48,51 zł Brutto: 259,43 zł	Netto: 194,29 zł Kwota VAT: 44,69 zł Brutto: 238,98 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Advanced – 12 miesięcy subskrypcji		Netto: 102,89 zł Kwota VAT: 23,66 zł Brutto: 126,55 zł	Netto: 87,64 zł Kwota VAT: 20,16 zł Brutto: 107,80 zł	Netto: 77,29 zł Kwota VAT: 17,78 zł Brutto: 95,07 zł	Netto: 72,03 zł Kwota VAT: 16,57 zł Brutto: 88,60 zł	Netto: 91,29 zł Kwota VAT: 21,00 zł Brutto: 112,29 zł	Netto: 84,11 zł Kwota VAT: 19,35 zł Brutto: 103,46 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Advanced – 24 miesiące subskrypcji		Netto: 205,77 zł Kwota VAT: 47,33 zł Brutto: 253,10 zł	Netto: 175,28 zł Kwota VAT: 40,31 zł Brutto: 215,59 zł	Netto: 154,59 zł Kwota VAT: 35,56 zł Brutto: 190,15 zł	Netto: 144,05 zł Kwota VAT: 33,13 zł Brutto: 177,18 zł	Netto: 182,57 zł Kwota VAT: 41,99 zł Brutto: 224,56 zł	Netto: 168,21 zł Kwota VAT: 38,69 zł Brutto: 206,90 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Advanced – 36 miesięcy subskrypcji		Netto: 308,66 zł Kwota VAT: 70,99 zł Brutto: 379,65 zł	Netto: 262,92 zł Kwota VAT: 60,47 zł Brutto: 323,39 zł	Netto: 231,88 zł Kwota VAT: 53,33 zł Brutto: 285,21 zł	Netto: 216,08 zł Kwota VAT: 49,70 zł Brutto: 265,78 zł	Netto: 273,86 zł Kwota VAT: 62,99 zł Brutto: 336,85 zł	Netto: 252,32 zł Kwota VAT: 58,03 zł Brutto: 310,35 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Complete – 12 miesięcy subskrypcji		Netto: 126,63 zł Kwota VAT: 29,12 zł Brutto: 155,75 zł	Netto: 107,74 zł Kwota VAT: 24,78 zł Brutto: 132,52 zł	Netto: 95,17 zł Kwota VAT: 21,89 zł Brutto: 117,06 zł	Netto: 88,66 zł Kwota VAT: 20,39 zł Brutto: 109,05 zł	Netto: 112,33 zł Kwota VAT: 25,84 zł Brutto: 138,17 zł	Netto: 103,51 zł Kwota VAT: 23,81 zł Brutto: 127,32 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Complete – 24 miesiące subskrypcji		Netto: 253,27 zł Kwota VAT: 58,25 zł Brutto: 311,52 zł	Netto: 215,48 zł Kwota VAT: 49,56 zł Brutto: 265,04 zł	Netto: 190,34 zł Kwota VAT: 43,78 zł Brutto: 234,12 zł	Netto: 177,32 zł Kwota VAT: 40,78 zł Brutto: 218,10 zł	Netto: 224,66 zł Kwota VAT: 51,67 zł Brutto: 276,33 zł	Netto: 207,02 zł Kwota VAT: 47,61 zł Brutto: 254,63 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Complete – 36 miesięcy subskrypcji		Netto: 379,90 zł Kwota VAT: 87,38 zł Brutto: 467,28 zł	Netto: 323,22 zł Kwota VAT: 74,34 zł Brutto: 397,56 zł	Netto: 285,52 zł Kwota VAT: 65,67 zł Brutto: 351,19 zł	Netto: 265,97 zł Kwota VAT: 61,17 zł Brutto: 327,14 zł	Netto: 336,99 zł Kwota VAT: 77,51 zł Brutto: 414,50 zł	Netto: 310,53 zł Kwota VAT: 71,42 zł Brutto: 381,95 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 12 miesięcy subskrypcji		Netto: 136,75 zł Kwota VAT: 31,45 zł Brutto: 168,20 zł	Netto: 127,42 zł Kwota VAT: 29,31 zł Brutto: 156,73 zł	Netto: 161,60 zł Kwota VAT: 37,17 zł Brutto: 198,77 zł	Netto: 148,87 zł Kwota VAT: 34,24 zł Brutto: 183,11 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 24 miesiące subskrypcji		Netto: 273,50 zł Kwota VAT: 62,91 zł Brutto: 336,41 zł	Netto: 254,84 zł Kwota VAT: 58,61 zł Brutto: 313,45 zł	Netto: 323,19 zł Kwota VAT: 74,33 zł Brutto: 397,52 zł	Netto: 297,74 zł Kwota VAT: 68,48 zł Brutto: 366,22 zł
ESET PROTECT Enterprise – 36 miesięcy subskrypcji		Netto: 410,26 zł Kwota VAT: 94,36 zł	Netto: 382,26 zł Kwota VAT: 87,92 zł	Netto: 484,79 zł Kwota VAT: 111,50 zł	Netto: 446,61 zł Kwota VAT: 102,72 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
		Brutto: 504,62 zł	Brutto: 470,18 zł	Brutto: 596,29 zł	Brutto: 549,33 zł
ESET PROTECT Elite – 12 miesięcy subskrypcji		Netto: 178,33 zł Kwota VAT: 41,02 zł Brutto: 219,35 zł	Netto: 166,18 zł Kwota VAT: 38,22 zł Brutto: 204,40 zł	Netto: 210,86 zł Kwota VAT: 48,50 zł Brutto: 259,36 zł	Netto: 194,23 zł Kwota VAT: 44,67 zł Brutto: 238,90 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Elite – 24 miesięcy subskrypcji		Netto: 356,66 zł Kwota VAT: 82,03 zł Brutto: 438,69 zł	Netto: 332,36 zł Kwota VAT: 76,44 zł Brutto: 408,80 zł	Netto: 421,72 zł Kwota VAT: 97,00 zł Brutto: 518,72 zł	Netto: 388,46 zł Kwota VAT: 89,35 zł Brutto: 477,81 zł
ESET PROTECT Elite – 36 miesięcy subskrypcji		Netto: 535,00zł Kwota VAT: 123,05 zł	Netto: 498,54 zł Kwota VAT: 114,66 zł	Netto: 632,58 zł Kwota VAT: 145,49 zł	Netto: 582,69 zł Kwota VAT: 134,02 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk	50-99 stanowisk	100-249 stanowisk	250+ stanowisk
		(należy podać cenę na jedno stanowisko)	(należy podać cenę na jedno stanowisko)	(należy podać cenę na jedno stanowisko)	(należy podać cenę na jedno stanowisko)
		Brutto: 658,05 zł	Brutto: 613,20 zł	Brutto: 778,07 zł	Brutto: 716,71 zł

* W przypadku zaoferowania oprogramowania równoważnego, Wykonawca powinien wpisać w kolumnie „Oprogramowanie równoważne” nazwę producenta zgodną z oferowanym oprogramowaniem.

5. Oświadczam(y), że¹¹:

- 1) jesteśmy mikroprzedsiębiorstwem:,
- 2) jesteśmy małym przedsiębiorstwem: Tak,
- 3) jesteśmy średnim przedsiębiorstwem:,
- 4) prowadzę jednoosobową działalnością gospodarczą:,
- 5) jestem osobą fizyczną nieprowadzącą działalności gospodarczej:,
- 6) jestem innym rodzajem wykonawcy:

6. Wykaz załączników i dokumentów przedstawianych w ofercie przez Wykonawcę(ów):

7. Załącznik nr 5 do Formularza oferty

- 1) Załącznik nr 5 do Formularza oferty
- 2)
- 3)¹²

.....
.....

Miejscowość / Data

Podpis(y) osoby(osób) upoważnionej(ych) do
reprezentowania Wykonawcy(ów)

¹¹ Odpowiednio wypełnić TAK jeśli dotyczy;

¹² odpowiednio uzupełnić;

ROZDZIAŁ IV – FORMULARZ OFERTY WRAZ Z ZAŁĄCZNIKAMI

OFERTA

na Umowa ramowa na dostawę oprogramowania antywirusowego.

nr referencyjny: COI-ZAK.262.71.2025

Centralny Zamawiający:

Centralny Ośrodek Informatyki

Al. Jerozolimskie 132-136

02-305 Warszawa

1. WYKONAWCA:

Niniejsza oferta zostaje złożona przez¹:

Lp.	Nazwa(y) Wykonawcy(ów)	Adres(y) Wykonawcy(ów)	NIP /KRS / REGON / kapitał zakładowy
1.	IKARIA Sp. z o.o. Sp. k.	Żeligowskiego 3/5, 90-752 Łódź	7272746817 / 0000332204 / 100703365 / nie dotyczy

2. DANE KONTAKTOWE WYKONAWCY²:

[wszelka korespondencja prowadzona będzie wyłącznie na nw. adres / e-mail]:

¹ Wykonawca modeluje tabelę powyżej w zależności od swego składu;

² Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wskazują dane pełnomocnika (lidera), z którym prowadzona będzie wszelka korespondencja;

3. OŚWIADCZENIA

Ja(my) niżej podpisany(i) oświadczam(y), że:

- 4.1. do przedmiotowych dokumentów, w tym zwłaszcza do opisu przedmiotu zamówienia i projektowanych postanowień umowy, nie wnoszę żadnych zastrzeżeń i akceptuję je w pełni,
- 4.2. uzyskaliśmy wszelkie niezbędne informacje do przygotowania oferty i wykonania zamówienia,
- 4.3. w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia,
- 4.4. w przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy ramowej w miejscu i terminie określonym przez Centralny Ośrodek Informatyki,
- 4.5. uważamy się za związanych niniejszą ofertą przez okres wskazany w SWZ,
- 4.6. oferujemy realizację niniejszego zamówienia, zgodnie z opisem przedmiotu zamówienia, zawartym w rozdziale II SWZ,
- 4.7. akceptuję/emy termin płatności za realizację przedmiotu umowy w ciągu 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT,
- 4.8. w kryterium: Deklarowany poziom cyberbezpieczeństwa usługi chmurowej [D] jest zgodny z:

SCCO 2	☒ nie ☐ tak
--------	---

** W przypadku braku wskazania w Formularzu oferty „Deklarowanego poziomu cyberbezpieczeństwa usługi chmurowej” Zamawiający uzna, że Wykonawcy deklaruje poziom SCCO 1 i przyzna 0 pkt w ramach kryterium „Deklarowany poziom cyberbezpieczeństwa usługi chmurowej”.*

4.9. wybór niniejszej oferty³:

- ☒ **NIE** prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego, zgodnie z przepisami o podatku od towarów i usług,
- ☐ prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług i wskazujemy poniżej nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazujemy ich wartość bez kwoty podatku:

Lp.	Nazwa (rodzaj)	Stawka podatku VAT	Wartość bez kwoty podatku
1.	_____		_____ zł
...	_____		_____ zł

4.10. jestem/ nie jestem⁴ czynnym podatnikiem podatku VAT,

4.11. wadium wpłacone w pieniądzu należy zwrócić na rachunek bankowy prowadzony w banku⁵:

4.12. niniejsze zamówienie⁶:

- ☒ w całości wykonam siłami własnymi,
- ☐ zaangażuję podwykonawców do realizacji przedmiotu zamówienia:
- i wskazuję części zamówienia, którą zamierzam powierzyć podwykonawcy:

³ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy; w przypadku, gdy wybór oferty prowadzi do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług należy wskazać w tabeli nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazać ich wartość bez kwoty podatku;

⁴ niepotrzebne skreślić;

⁵ uzupełnić odpowiednio miejsca podając nazwę banku i numer konta – dotyczy wadium wnoszonego w pieniądzu;

⁶ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy, w przypadku zaangażowania podwykonawców do realizacji przedmiotu zamówienia należy wskazać części zamówienia, które Wykonawca zamierza powierzyć podwykonawcy;

4.13. dane rejestrowe podwykonawców, którym zamierzam powierzyć realizację części zamówienia, o których mowa w pkt. 4.13⁷:

Lp.	Nazwa(y) podwykonawcy(ów)	Adres(y) siedziby PODWYKONAWCY(ÓW)	Numer wpisu do odpowiedniego rejestru – KRS lub datę rozpoczęcia działalności z CEIDG	NIP oraz Regon
1.				
2.				

4.14. Oświadczam/y, że **zastrzegamy/nie zastrzegamy**⁸ części oferty jako tajemnica przedsiębiorstwa, w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity: Dz.U. z 2022 r., poz. 1123, z późn. zm.) i w związku z tym informacje zawarte w plikach:..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ww. przepisów. Pozostałe części oferty oraz załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa.

4.15. Oświadczam/y, że zapoznaliśmy się z Klauzulą Informacyjną Centralnego Ośrodka Informatyki dotyczącą RODO⁹ zamieszczoną w Rozdziale I SWZ – Instrukcja dla Wykonawców.

4.16. Oświadczam/y, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/liśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu, w tym również wykonałem/liśmy obowiązek, który ciąży na mnie/nas zgodnie z „Informacją o przetwarzaniu danych osobowych osób fizycznych, których dane są przekazywane Centralnemu

⁷ uzupełnić odpowiednio – o ile są znane;

⁸ Niepotrzebne skreślić; wypełnić tylko, gdy dotyczy; przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom, zwykle zajmującym się tym; rodzajem: informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności; w takim przypadku należy wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Ośrodkowi Informatyki przez Wykonawcę w toku postępowania o udzielenie zamówienia publicznego oraz w toku wykonywania umowy”¹⁰

4. CENA OFERTY

- 5.1. oświadczam, że cena zawiera wszelkie koszty jakie Wykonawca poniesie w związku z realizacją zamówienia,
- 5.2. gwarantuję wykonanie niniejszego zamówienia zgodnie z treścią SWZ,
- 5.3. oferujemy wykonanie zamówienia zgodnie z cenami zaoferowanymi w Tabeli cenowej poniżej:

¹⁰ W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Tabela cenowa:

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 12 miesięcy subskrypcji		Netto: 77,94 zł Kwota VAT: 17,93 zł Brutto: 95,87 zł	Netto: 66,34 zł Kwota VAT: 15,26 zł Brutto: 81,60 zł	Netto: 63,06 zł Kwota VAT: 14,50 zł Brutto: 77,56 zł	Netto: 82,25 zł Kwota VAT: 18,92 zł Brutto: 101,17 zł	Netto: 76,56 zł Kwota VAT: 17,61 zł Brutto: 94,17 zł	Netto: 70,52 zł Kwota VAT: 16,22 zł Brutto: 86,74 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 24 miesiące		Netto: 155,88 zł Kwota VAT: 35,85 zł Brutto: 191,73 zł	Netto: 132,68 zł Kwota VAT: 30,52 zł Brutto: 163,20 zł	Netto: 126,13 zł Kwota VAT: 29,01 zł Brutto: 155,14 zł	Netto: 159,47 zł Kwota VAT: 36,68 zł Brutto: 196,15 zł	Netto: 153,12 zł Kwota VAT: 35,22 zł Brutto: 188,34 zł	Netto: 141,04 zł Kwota VAT: 32,44 zł Brutto: 173,48 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 36 miesięcy subskrypcji		Netto: 233,82 zł Kwota VAT: 53,78 zł Brutto: 287,60 zł	Netto: 199,02 zł Kwota VAT: 45,77 zł Brutto: 244,79 zł	Netto: 186,49 zł Kwota VAT: 42,89 zł Brutto: 229,38 zł	Netto: 246,75 zł Kwota VAT: 56,75 zł Brutto: 303,50 zł	Netto: 229,67 zł Kwota VAT: 52,82 zł Brutto: 282,49 zł	Netto: 211,56 zł Kwota VAT: 48,66 zł Brutto: 260,22 zł
ESET PROTECT Advanced –		Netto: 101,33 zł Kwota VAT: 23,31 zł	Netto: 86,31 zł Kwota VAT: 19,85 zł	Netto: 81,98 zł Kwota VAT: 18,86 zł	Netto: 106,95 zł Kwota VAT: 24,60 zł	Netto: 99,40 zł Kwota VAT: 22,86 zł	Netto: 91,58 zł Kwota VAT: 21,06 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
12 miesięcy subskrypcji		Brutto: 124,64 zł	Brutto: 106,16 zł	Brutto: 100,84 zł	Brutto: 131,55 zł	Brutto: 122,26 zł	Brutto: 112,64 zł
ESET PROTECT Advanced – 24 miesiące subskrypcji		Netto: 202,66 zł Kwota VAT: 46,61 zł Brutto: 249,27 zł	Netto: 172,63 zł Kwota VAT: 39,70 zł Brutto: 212,33 zł	Netto: 163,95 zł Kwota VAT: 37,71 zł Brutto: 201,66 zł	Netto: 207,35 zł Kwota VAT: 47,69 zł Brutto: 255,04 zł	Netto: 198,80 zł Kwota VAT: 45,72 zł Brutto: 244,52 zł	Netto: 183,16 zł Kwota VAT: 42,13 zł Brutto: 225,29 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET		Netto: 303,99 zł	Netto: 258,94 zł	Netto: 242,42 zł	Netto: 320,84 zł	Netto: 298,20 zł	Netto: 274,74 zł
PROTECT		Kwota VAT: 69,92 zł	Kwota VAT: 59,56 zł	Kwota VAT: 55,76 zł	Kwota VAT: 73,79 zł	Kwota VAT: 68,59 zł	Kwota VAT: 63,19 zł
Advanced – 36 miesięcy subskrypcji		Brutto: 373,91 zł	Brutto: 318,50 zł	Brutto: 298,18 zł	Brutto: 394,63 zł	Brutto: 366,79 zł	Brutto: 337,93 zł
ESET		Netto: 124,72 zł	Netto: 106,11 zł	Netto: 100,94 zł	Netto: 131,64 zł	Netto: 122,31 zł	Netto: 112,71 zł
PROTECT		Kwota VAT: 28,69 zł	Kwota VAT: 24,41 zł	Kwota VAT: 23,22 zł	Kwota VAT: 30,28 zł	Kwota VAT: 28,13 zł	Kwota VAT: 25,92 zł
Complete –							

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
12 miesięcy subskrypcji		Brutto: 153,41 zł	Brutto: 130,52 zł	Brutto: 124,16 zł	Brutto: 161,92 zł	Brutto: 150,44 zł	Brutto: 138,63 zł
ESET PROTECT Complete – 24 miesiące subskrypcji		Netto: 249,43 zł Kwota VAT: 57,37 zł Brutto: 306,80 zł	Netto: 212,21 zł Kwota VAT: 48,81 zł Brutto: 261,02 zł	Netto: 201,88 zł Kwota VAT: 46,43 zł Brutto: 248,31 zł	Netto: 255,23 zł Kwota VAT: 58,70 zł Brutto: 313,93 zł	Netto: 244,63 zł Kwota VAT: 56,26 zł Brutto: 300,89 zł	Netto: 225,42 zł Kwota VAT: 51,85 zł Brutto: 277,27 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET		Netto: 374,15 zł	Netto: 318,32 zł	Netto: 298,49 zł	Netto: 394,93 zł	Netto: 366,94 zł	Netto: 338,13 zł
PROTECT		Kwota VAT: 86,05 zł	Kwota VAT: 73,21 zł	Kwota VAT: 68,65 zł	Kwota VAT: 90,83 zł	Kwota VAT: 84,40 zł	Kwota VAT: 77,77 zł
Complete – 36 miesięcy subskrypcji		Brutto: 460,20 zł	Brutto: 391,53 zł	Brutto: 367,14 zł	Brutto: 485,76 zł	Brutto: 451,34 zł	Brutto: 415,90 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 12 miesięcy subskrypcji		Netto: 145,04 zł Kwota VAT: 33,36 zł Brutto: 178,40 zł	Netto: 189,20 zł Kwota VAT: 43,52 zł Brutto: 232,72 zł	Netto: 175,96 zł Kwota VAT: 40,47 zł Brutto: 216,43 zł	Netto: 162,10 zł Kwota VAT: 37,28 zł Brutto: 199,38 zł
ESET PROTECT Enterprise – 24 miesiące subskrypcji		Netto: 290,08 zł Kwota VAT: 66,72 zł Brutto: 356,80 zł	Netto: 366,81 zł Kwota VAT: 84,37 zł Brutto: 451,18 zł	Netto: 351,92 zł Kwota VAT: 80,94 zł Brutto: 432,86 zł	Netto: 324,20 zł Kwota VAT: 74,57 zł Brutto: 398,77 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 36 miesięcy subskrypcji		Netto: 428,90 zł Kwota VAT: 98,65 zł Brutto: 527,55 zł	Netto: 567,60 zł Kwota VAT: 130,55 zł Brutto: 698,15 zł	Netto: 527,88 zł Kwota VAT: 121,41 zł Brutto: 649,29 zł	Netto: 486,31 zł Kwota VAT: 111,85 zł Brutto: 598,16 zł
ESET PROTECT Elite – 12 miesięcy subskrypcji		Netto: 243,18 zł Kwota VAT: 55,93 zł Brutto: 299,11 zł	Netto: 251,79 zł Kwota VAT: 57,91 zł Brutto: 309,70 zł	Netto: 234,29 zł Kwota VAT: 53,89 zł Brutto: 288,18 zł	Netto: 211,49 zł Kwota VAT: 48,64 zł Brutto: 260,13 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Elite – 24 miesiące subskrypcji		Netto: 378,28 zł Kwota VAT: 87,00 zł Brutto: 465,28 zł	Netto: 493,51 zł Kwota VAT: 113,51 zł Brutto: 607,02 zł	Netto: 459,21 zł Kwota VAT: 105,62 zł Brutto: 564,83 zł	Netto: 422,99 zł Kwota VAT: 97,29 zł Brutto: 520,28 zł
ESET PROTECT Elite – 36 miesiące subskrypcji		Netto: 567,42 zł Kwota VAT: 130,51 zł Brutto: 697,93 zł	Netto: 740,26 zł Kwota VAT: 170,26 zł Brutto: 910,52 zł	Netto: 688,81 zł Kwota VAT: 158,43 zł Brutto: 847,24 zł	Netto: 634,48 zł Kwota VAT: 145,93 zł Brutto: 780,41 zł

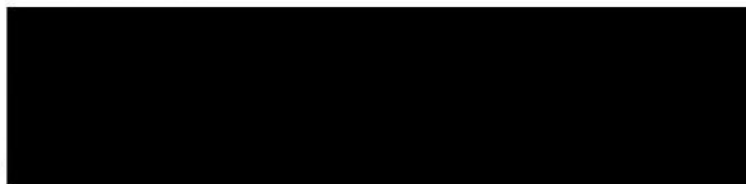
* W przypadku zaoferowania oprogramowania równoważnego, Wykonawca powinien wpisać w kolumnie „Oprogramowanie równoważne” nazwę producenta zgodną z oferowanym oprogramowaniem.

5. Oświadczam(y), że¹¹:

- 1)–jesteśmy mikroprzedsiębiorstwem:,
- 2) jesteśmy małym przedsiębiorstwem: TAK
- 3)–jesteśmy średnim przedsiębiorstwem:,
- 4)–prowadzę jednoosobową działalnością gospodarczą:,
- 5)–jestem osobą fizyczną nieprowadzącą działalności gospodarczej:,
- 6)–jestem innym rodzajem wykonawcy:

6. Wykaz załączników i dokumentów przedstawianych w ofercie przez Wykonawcę(ów):

- 1) Potwierdzenie wpłaty - wadium
- 2) Załącznik nr 5
- 3)¹²



.....
Łódź, 14/01/2026

Miejscowość / Data

Podpis(y) osoby(osób) upoważnionej(ych) do
reprezentowania Wykonawcy(ów)

¹¹ Odpowiednio wypełnić TAK jeśli dotyczy;

¹² odpowiednio uzupełnić;

Oferta na**„Umowa ramowa na dostawę oprogramowania antywirusowego”****Znak Sprawy:****COI-ZAK.262.71.2025****Wykonawca**

Perceptus sp. z o. o.
ul. Nowy Kisielin – Wysockiego 10
66-002 Zielona Góra

Perceptus sp. z o. o.

ul. Nowy Kisielin – A. Wysockiego 10

66-002 Zielona Góra

+48 68 470 07 70**perceptus@perceptus.pl**

NIP: 929 180 85 78

REGON: 080307093

KRS: 0000320099

Kapitał zakładowy 50 000,00 zł wpłacony w całości

BANK PEKAO S.A. (SWIFT: PKOPPLPW)

PLN: 10 1240 6843 1111 0011 0564 4328

EUR: 31 1240 6843 1978 0011 0564 4735

ROZDZIAŁ IV – FORMULARZ OFERTY WRAZ Z ZAŁĄCZNIKAMI

OFERTA

na Umowa ramowa na dostawę oprogramowania antywirusowego.

nr referencyjny: COI-ZAK.262.71.2025

Centralny Zamawiający:

Centralny Ośrodek Informatyki

Al. Jerozolimskie 132-136

02-305 Warszawa

1. WYKONAWCA:

Niniejsza oferta zostaje złożona przez¹:

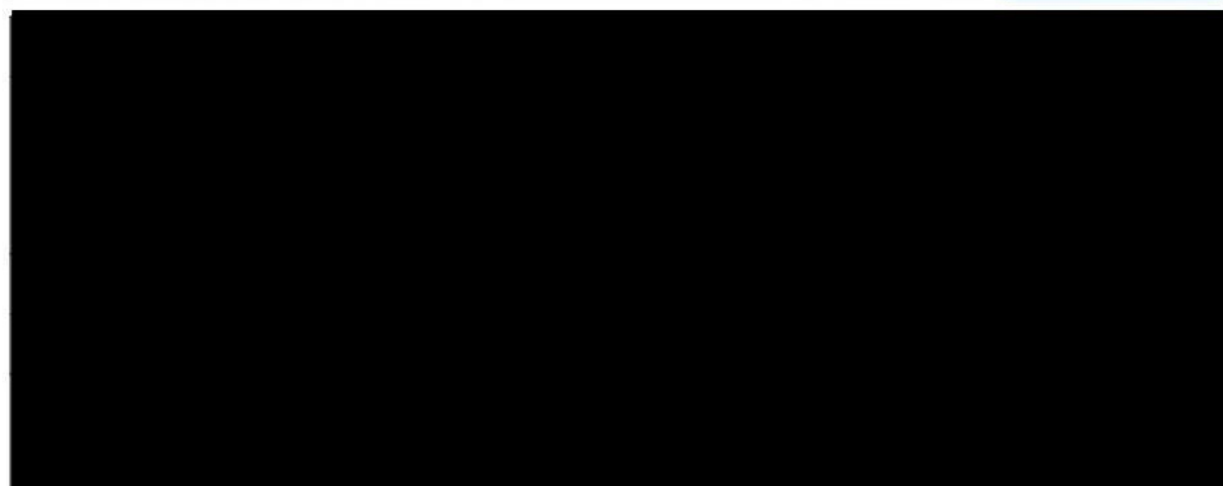
Lp.	Nazwa(y) Wykonawcy(ów)	Adres(y) Wykonawcy(ów)	NIP /KRS / REGON / kapitał zakładowy
	Perceptus Sp. z o.o.	ul. Nowy Kisielin – Antoniego Wysockiego 10 66-002 Zielona Góra	NIP 929-180-85-78 REGON 080307093 KRS 0000320099 Kapitał zakładowy 50 000,00 wpłacony w całości.

2. DANE KONTAKTOWE WYKONAWCY²:

[wszelka korespondencja prowadzona będzie wyłącznie na nw. adres / e-mail]:

¹ Wykonawca modeluje tabelę powyżej w zależności od swego składu;

² Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wskazują dane pełnomocnika (lidera), z którym prowadzona będzie wszelka korespondencja;



3. OŚWIADCZENIA

Ja(my) niżej podpisany(i) oświadczam(y), że:

- 4.1. do przedmiotowych dokumentów, w tym zwłaszcza do opisu przedmiotu zamówienia i projektowanych postanowień umowy, nie wnoszę żadnych zastrzeżeń i akceptuję je w pełni,
- 4.2. uzyskaliśmy wszelkie niezbędne informacje do przygotowania oferty i wykonania zamówienia,
- 4.3. w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia,
- 4.4. w przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy ramowej w miejscu i terminie określonym przez Centralny Ośrodek Informatyki,
- 4.5. uważamy się za związanych niniejszą ofertą przez okres wskazany w SWZ,
- 4.6. oferujemy realizację niniejszego zamówienia, zgodnie z opisem przedmiotu zamówienia, zawartym w rozdziale II SWZ,
- 4.7. akceptuję/emy termin płatności za realizację przedmiotu umowy w ciągu 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT,
- 4.8. w kryterium: Deklarowany poziom cyberbezpieczeństwa usługi chmurowej [D] jest zgodny z:

SCCO 2	☐ nie ☒ tak
--------	---

** W przypadku braku wskazania w Formularzu oferty „Deklarowanego poziomu cyberbezpieczeństwa usługi chmurowej” Zamawiający uzna, że Wykonawcy deklaruje poziom SCCO 1 i przyzna 0 pkt w ramach kryterium „Deklarowany poziom cyberbezpieczeństwa usługi chmurowej”.*

4.9. wybór niniejszej oferty³:

- ☒ **NIE** prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego, zgodnie z przepisami o podatku od towarów i usług,
- ☐ prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług i wskazujemy poniżej nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazujemy ich wartość bez kwoty podatku:

Lp.	Nazwa (rodzaj)	Stawka podatku VAT	Wartość bez kwoty podatku
1.	_____		_____ zł
...	_____		_____ zł

4.10. jestem/ ~~nie jestem~~⁴ czynnym podatnikiem podatku VAT,

4.11. wadium wpłacone w pieniądzu należy zwrócić na rachunek bankowy prowadzony w banku⁵:

Nr rachunku: _____

4.12. niniejsze zamówienie⁶:

- ☒ w całości wykonam siłami własnymi,

³ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy; w przypadku, gdy wybór oferty prowadzi do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług należy wskazać w tabeli nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazać ich wartość bez kwoty podatku;

⁴ niepotrzebne skreślić;

⁵ uzupełnić odpowiednio miejsca podając nazwę banku i numer konta – dotyczy wadium wnoszonego w pieniądzu;

⁶ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy, w przypadku zaangażowania podwykonawców do realizacji przedmiotu zamówienia należy wskazać części zamówienia, które Wykonawca zamierza powierzyć podwykonawcy;

☐ zaangażuję podwykonawców do realizacji przedmiotu zamówienia:
i wskazuję części zamówienia, którą zamierzam powierzyć podwykonawcy:

4.13. dane rejestrowe podwykonawców, którym zamierzam powierzyć realizację części zamówienia, o których mowa w pkt. 4.13⁷:

Lp.	Nazwa(y) podwykonawcy(ów)	Adres(y) siedziby PODWYKONAWCY(ów)	Numer wpisu do odpowiedniego rejestru – KRS lub datę rozpoczęcia działalności z CEIDG	NIP oraz Regon
1.				
2.				

4.14. Oświadczam/y, że ~~zastrzegamy~~/nie zastrzegamy⁸ części oferty jako tajemnica przedsiębiorstwa, w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity: Dz.U. z 2022 r., poz. 1123, z późn. zm.) i w związku z tym informacje zawarte w plikach..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ww. przepisów. Pozostałe części oferty oraz załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa.

4.15. Oświadczam/y, że zapoznaliśmy się z Klauzulą Informacyjną Centralnego Ośrodka Informatyki dotyczącą RODO⁹ zamieszczoną w Rozdziale I SWZ – Instrukcja dla Wykonawców.

4.16. Oświadczam/y, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub

⁷ uzupełnić odpowiednio – o ile są znane;

⁸ Niepotrzebne skreślić; wypełnić tylko, gdy dotyczy; przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności; w takim przypadku należy wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

pośrednio pozyskałem/liśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu, w tym również wykonałem/liśmy obowiązek, który ciąży na mnie/nas zgodnie z „Informacją o przetwarzaniu danych osobowych osób fizycznych, których dane są przekazywane Centralnemu Ośrodkowi Informatyki przez Wykonawcę w toku postępowania o udzielenie zamówienia publicznego oraz w toku wykonywania umowy”¹⁰

4. CENA OFERTY

- 5.1. oświadczam, że cena zawiera wszelkie koszty jakie Wykonawca poniesie w związku z realizacją zamówienia,
- 5.2. gwarantuję wykonanie niniejszego zamówienia zgodnie z treścią SWZ,
- 5.3. oferujemy wykonanie zamówienia zgodnie z cenami zaoferowanymi w Tabeli cenowej poniżej:

¹⁰ W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Tabela cenowa:

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 12 miesięcy subskrypcji		Netto: 83,94 zł Kwota VAT: 19,31 zł Brutto: 103,25 zł	Netto: 80,63 zł Kwota VAT: 18,54 zł Brutto: 99,17 zł	Netto: 79,28 zł Kwota VAT: 18,23 zł Brutto: 97,51 zł	Netto: 78,89 zł Kwota VAT: 18,14 zł Brutto: 97,03 zł	Netto: 78,12 zł Kwota VAT: 17,97 zł Brutto: 96,09 zł	Netto: 71,96 zł Kwota VAT: 16,55 zł Brutto: 88,51 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 24 miesiące		Netto: 167,87 zł Kwota VAT: 38,61 zł Brutto: 206,48 zł	Netto: 161,25 zł Kwota VAT: 37,09 zł Brutto: 198,34 zł	Netto: 158,56 zł Kwota VAT: 36,47 zł Brutto: 195,03 zł	Netto: 157,79 zł Kwota VAT: 36,29 zł Brutto: 194,08 zł	Netto: 156,24 zł Kwota VAT: 35,94 zł Brutto: 192,18 zł	Netto: 143,92 zł Kwota VAT: 33,10 zł Brutto: 177,02 zł
ESET PROTECT Entry – 36		Netto: 251,81 zł Kwota VAT: 57,92 zł Brutto: 309,73 zł	Netto: 238,82 zł Kwota VAT: 54,93 zł Brutto: 293,75 zł	Netto: 237,84 zł Kwota VAT: 54,70 zł Brutto: 292,54 zł	Netto: 236,68 zł Kwota VAT: 54,44 zł Brutto: 291,12 zł	Netto: 234,36 zł Kwota VAT: 53,90 zł Brutto: 288,26 zł	Netto: 215,88 zł Kwota VAT: 49,65 zł Brutto: 265,53 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
miesiące subskrypcji							
ESET PROTECT Advanced – 12 miesięcy subskrypcji		Netto: 109,12 zł Kwota VAT: 25,10 zł Brutto: 134,22 zł	Netto: 104,90 zł Kwota VAT: 24,13 zł Brutto: 129,03 zł	Netto: 103,06 zł Kwota VAT: 23,70 zł Brutto: 126,76 zł	Netto: 102,58 zł Kwota VAT: 23,59 zł Brutto: 126,17 zł	Netto: 101,43 zł Kwota VAT: 23,33 zł Brutto: 124,76 zł	Netto: 93,45 zł Kwota VAT: 21,49 zł Brutto: 114,94 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Advanced – 24 miesiące subskrypcji		Netto: 218,25 zł Kwota VAT: 50,20 zł Brutto: 268,45 zł	Netto: 209,81 zł Kwota VAT: 48,26 zł Brutto: 258,07 zł	Netto: 206,11 zł Kwota VAT: 47,41 zł Brutto: 253,52 zł	Netto: 205,16 zł Kwota VAT: 47,19 zł Brutto: 252,35 zł	Netto: 202,86 zł Kwota VAT: 46,66 zł Brutto: 249,52 zł	Netto: 186,90 zł Kwota VAT: 42,99 zł Brutto: 229,89 zł
ESET PROTECT Advanced – 36 miesięcy subskrypcji		Netto: 327,37 zł Kwota VAT: 75,30 zł Brutto: 402,67 zł	Netto: 314,71 zł Kwota VAT: 72,38 zł Brutto: 387,09 zł	Netto: 309,17 zł Kwota VAT: 71,11 zł Brutto: 380,28 zł	Netto: 307,75 zł Kwota VAT: 70,78 zł Brutto: 378,53 zł	Netto: 304,29 zł Kwota VAT: 69,99 zł Brutto: 374,28 zł	Netto: 280,35 zł Kwota VAT: 64,48 zł Brutto: 344,83 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Complete – 12 miesięcy subskrypcji		Netto: 134,31 zł Kwota VAT: 30,89 zł Brutto: 165,20 zł	Netto: 128,96 zł Kwota VAT: 29,66 zł Brutto: 158,62 zł	Netto: 126,90 zł Kwota VAT: 29,19 zł Brutto: 156,09 zł	Netto: 126,27 zł Kwota VAT: 29,04 zł Brutto: 155,31 zł	Netto: 124,81 zł Kwota VAT: 28,71 zł Brutto: 153,52 zł	Netto: 115,01 zł Kwota VAT: 26,45 zł Brutto: 141,46 zł
ESET PROTECT Complete – 24 miesiące subskrypcji		Netto: 268,62 zł Kwota VAT: 61,78 zł Brutto: 330,40 zł	Netto: 257,92 zł Kwota VAT: 59,32 zł Brutto: 317,24 zł	Netto: 253,79 zł Kwota VAT: 58,37 zł Brutto: 312,16 zł	Netto: 252,54 zł Kwota VAT: 58,08 zł Brutto: 310,62 zł	Netto: 249,62 zł Kwota VAT: 57,41 zł Brutto: 307,03 zł	Netto: 230,02 zł Kwota VAT: 52,90 zł Brutto: 282,92 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Complete – 36 miesięcy subskrypcji		Netto: 402,93 zł Kwota VAT: 92,67 zł Brutto: 495,60 zł	Netto: 386,88 zł Kwota VAT: 88,98 zł Brutto: 475,86 zł	Netto: 380,69 zł Kwota VAT: 87,56 zł Brutto: 468,25 zł	Netto: 378,81 zł Kwota VAT: 87,13 zł Brutto: 465,94 zł	Netto: 374,43 zł Kwota VAT: 86,12 zł Brutto: 460,55 zł	Netto: 345,03 zł Kwota VAT: 79,36 zł Brutto: 424,39 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 12 miesięcy subskrypcji		Netto: 186,48 zł Kwota VAT: 42,89 zł Brutto: 229,37 zł	Netto: 183,41 zł Kwota VAT: 42,18 zł Brutto: 225,59 zł	Netto: 179,55 zł Kwota VAT: 41,30 zł Brutto: 220,85 zł	Netto: 165,41 zł Kwota VAT: 38,04 zł Brutto: 203,45 zł
ESET PROTECT Enterprise – 24 miesiące subskrypcji		Netto: 372,96 zł Kwota VAT: 85,78 zł Brutto: 458,74 zł	Netto: 366,81 zł Kwota VAT: 84,37 zł Brutto: 451,18 zł	Netto: 359,10 zł Kwota VAT: 82,59 zł Brutto: 441,69 zł	Netto: 330,82 zł Kwota VAT: 76,09 zł Brutto: 406,91 zł
ESET PROTECT Enterprise –		Netto: 559,44 zł Kwota VAT: 128,67 zł	Netto: 550,22 zł Kwota VAT: 126,55 zł	Netto: 538,65 zł Kwota VAT: 123,89 zł	Netto: 496,23 zł Kwota VAT: 114,13 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
36 miesięcy subskrypcji		Brutto: 688,11 zł	Brutto: 676,77 zł	Brutto: 662,54 zł	Brutto: 610,36 zł
ESET PROTECT Elite – 12 miesięcy subskrypcji		Netto: 243,18 zł Kwota VAT: 55,93 zł Brutto: 299,11 zł	Netto: 239,20 zł Kwota VAT: 55,02 zł Brutto: 294,22 zł	Netto: 234,29 zł Kwota VAT: 53,89 zł Brutto: 288,18 zł	Netto: 215,81 zł Kwota VAT: 49,64 zł Brutto: 265,45 zł
ESET PROTECT Elite – 24 miesiące subskrypcji		Netto: 486,36 zł Kwota VAT: 111,86 zł Brutto: 598,22 zł	Netto: 478,40 zł Kwota VAT: 110,03 zł Brutto: 588,43 zł	Netto: 468,58 zł Kwota VAT: 107,77 zł Brutto: 576,35 zł	Netto: 431,62 zł Kwota VAT: 99,27 zł Brutto: 530,89 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Elite – 36 miesięcy subskrypcji		Netto: 729,54 zł Kwota VAT: 167,79 zł Brutto: 897,33 zł	Netto: 717,60 zł Kwota VAT: 165,05 zł Brutto: 882,65 zł	Netto: 702,87 zł Kwota VAT: 161,66 zł Brutto: 864,53 zł	Netto: 647,43 zł Kwota VAT: 148,91 zł Brutto: 796,34 zł

* W przypadku zaoferowania oprogramowania równoważnego, Wykonawca powinien wpisać w kolumnie „Oprogramowanie równoważne” nazwę producenta zgodną z oferowanym oprogramowaniem.

5. Oświadczam(y), że¹¹:

- 1) jesteśmy mikroprzedsiębiorstwem:,
- 2) jesteśmy małym przedsiębiorstwem: TAK
- 3) jesteśmy średnim przedsiębiorstwem:,
- 4) prowadzę jednoosobową działalnością gospodarczą:,
- 5) jestem osobą fizyczną nieprowadzącą działalności gospodarczej:,
- 6) jestem innym rodzajem wykonawcy:

6. Wykaz załączników i dokumentów przedstawianych w ofercie przez
Wykonawcę(ów):

- 1) KRS
- 2)
- 3)¹²

Zielona Góra,

15.01.2026

Miejscowość / Podpis(y) osoby(osób) upoważnio

Data Wykonawcy(ów)

¹¹ Odpowiednio wypełnić TAK jeśli dotyczy;

¹² odpowiednio uzupełnić;

ROZDZIAŁ IV – FORMULARZ OFERTY WRAZ Z ZAŁĄCZNIKAMI

OFERTA

na Umowa ramowa na dostawę oprogramowania antywirusowego.

nr referencyjny: COI-ZAK.262.71.2025

Centralny Zamawiający:

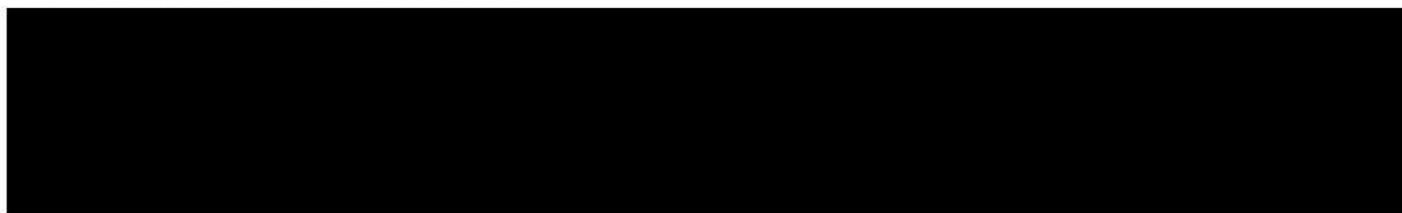
Centralny Ośrodek Informatyki

Al. Jerozolimskie 132-136

02-305 Warszawa

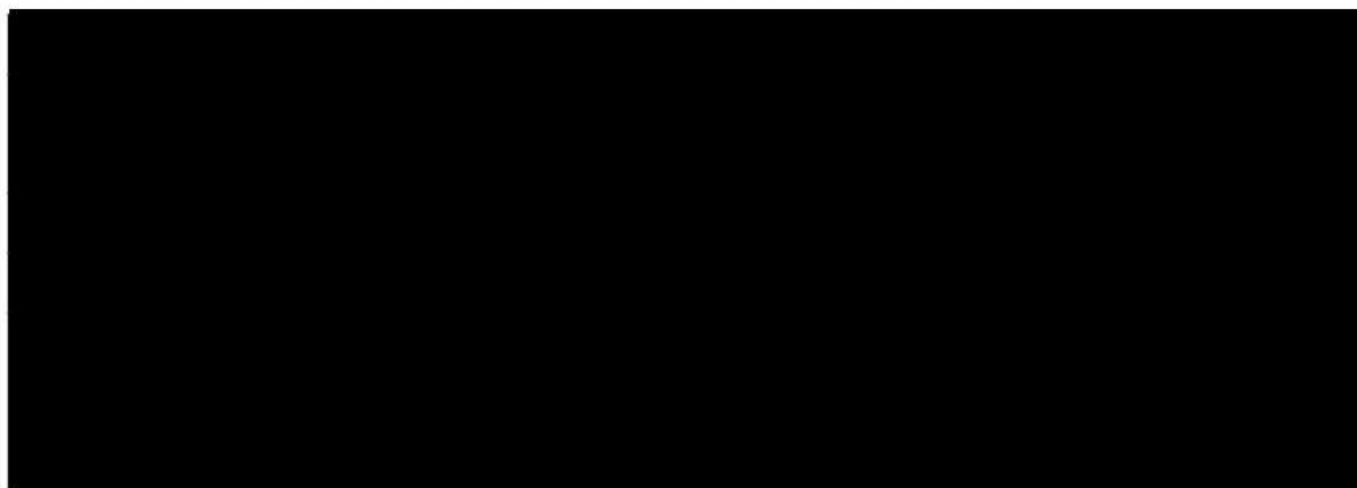
1. WYKONAWCA:

Niniejsza oferta zostaje złożona przez¹:



2. DANE KONTAKTOWE WYKONAWCY²:

[wszelka korespondencja prowadzona będzie wyłącznie na nw. adres / e-mail]:



¹ Wykonawca modeluje tabelę powyżej w zależności od swego składu;

² Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wskazują dane pełnomocnika (lidera), z którym prowadzona będzie wszelka korespondencja;

3. OŚWIADCZENIA

Ja~~(my)~~ niżej podpisany~~(i)~~ oświadczam~~(y)~~, że:

- 4.1. do przedmiotowych dokumentów, w tym zwłaszcza do opisu przedmiotu zamówienia i projektowanych postanowień umowy, nie wnoszę żadnych zastrzeżeń i akceptuję je w pełni,
- 4.2. uzyskaliśmy wszelkie niezbędne informacje do przygotowania oferty i wykonania zamówienia,
- 4.3. w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia,
- 4.4. w przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy ramowej w miejscu i terminie określonym przez Centralny Ośrodek Informatyki,
- 4.5. uważamy się za związanych niniejszą ofertą przez okres wskazany w SWZ,
- 4.6. oferujemy realizację niniejszego zamówienia, zgodnie z opisem przedmiotu zamówienia, zawartym w rozdziale II SWZ,
- 4.7. akceptuję~~emy~~ termin płatności za realizację przedmiotu umowy w ciągu 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT,
- 4.8. w kryterium: Deklarowany poziom cyberbezpieczeństwa usługi chmurowej [D] jest zgodny z:

SCCO 2	☒ nie ☐ tak
--------	---

** W przypadku braku wskazania w Formularzu oferty „Deklarowanego poziomu cyberbezpieczeństwa usługi chmurowej” Zamawiający uzna, że Wykonawcy deklaruje poziom SCCO 1 i przyzna 0 pkt w ramach kryterium „Deklarowany poziom cyberbezpieczeństwa usługi chmurowej”.*

4.9. wybór niniejszej oferty³:

- ☒ **NIE** prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego, zgodnie z przepisami o podatku od towarów i usług,
- ☐ ~~prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług i wskazujemy poniżej nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazujemy ich wartość bez kwoty podatku:~~

³ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy; w przypadku, gdy wybór oferty prowadzi do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług należy wskazać w tabeli nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazać ich wartość bez kwoty podatku;

Lp.	Nazwa (rodzaj)	Stawka podatku VAT	Wartość bez kwoty podatku
1.	_____		_____ zł
...	_____		_____ zł

4.10. jestem/~~nie jestem~~⁴ czynnym podatnikiem podatku VAT,

4.11. ~~wadium wpłacone w pieniądzu należy zwrócić na rachunek bankowy prowadzony w banku~~⁵:

Nr rachunku: _____

Wadium zostało wniesione w formie gwarancji ubezpieczeniowej.

4.12. niniejsze zamówienie⁶:

☐ **w całości wykonam siłami własnymi,**

☐ **zaangażuję podwykonawców do realizacji przedmiotu zamówienia:**

i wskazuję części zamówienia, którą zamierzam powierzyć podwykonawcy: _____

4.13. dane rejestrowe podwykonawców, którym zamierzam powierzyć realizację części zamówienia, o których mowa w pkt. 4.13⁷:

Lp.	Nazwa(y) podwykonawcy(ów)	Adres(y) siedziby PODWYKONAWCY(ÓW)	Numer wpisu do odpowiedniego rejestru – KRS lub datę rozpoczęcia działalności z CEIDG	NIP oraz Regon
1.				
2.				

⁴ niepotrzebne skreślić;

⁵ uzupełnić odpowiednio miejsca podając nazwę banku i numer konta – dotyczy wadium wnoszonego w pieniądzu;

⁶ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy, w przypadku zaangażowania podwykonawców do realizacji przedmiotu zamówienia należy wskazać części zamówienia, które Wykonawca zamierza powierzyć podwykonawcy;

⁷ uzupełnić odpowiednio – o ile są znane;

- 4.14. Oświadczam/~~ę~~, że ~~zastrzegamy/nie zastrzegamy~~⁸ części oferty jako tajemnica przedsiębiorstwa, w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity: Dz.U. z 2022 r., poz. 1123, z późn. zm.) i w związku z tym informacje zawarte w plikach..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ww. przepisów. Pozostałe części oferty oraz załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa.
- 4.15. Oświadczam/~~ę~~, że zapoznaliśmy się z Klauzulą Informacyjną Centralnego Ośrodka Informatyki dotyczącą RODO⁹ zamieszczoną w Rozdziale I SWZ – Instrukcja dla Wykonawców.
- 4.16. Oświadczam/~~ę~~, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/liśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu, w tym również wykonałem/liśmy obowiązek, który ciąży na mnie/nas zgodnie z „Informacją o przetwarzaniu danych osobowych osób fizycznych, których dane są przekazywane Centralnemu Ośrodkowi Informatyki przez Wykonawcę w toku postępowania o udzielenie zamówienia publicznego oraz w toku wykonywania umowy”¹⁰

4. CENA OFERTY

- 5.1. oświadczam, że cena zawiera wszelkie koszty jakie Wykonawca poniesie w związku z realizacją zamówienia,
- 5.2. gwarantuję wykonanie niniejszego zamówienia zgodnie z treścią SWZ,
- 5.3. oferujemy wykonanie zamówienia zgodnie z cenami zaoferowanymi w Tabeli cenowej poniżej:

⁸ Niepotrzebne skreślić; wypełnić tylko, gdy dotyczy; przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności; **w takim przypadku należy wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.**

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

¹⁰ W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Tabela cenowa:

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia <u>tylko</u> w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 12 miesięcy subskrypcji		Netto: 89,00 zł Kwota VAT: 20,47 zł Brutto: 109,47 zł	Netto: 76,00 zł Kwota VAT: 17,48 zł Brutto: 93,48 zł	Netto: 67,00 zł Kwota VAT: 15,41 zł Brutto: 82,41 zł	Netto: 83,00 zł Kwota VAT: 19,09 zł Brutto: 102,09 zł	Netto: 77,00 zł Kwota VAT: 17,71 zł Brutto: 94,71 zł	Netto: 71,00 zł Kwota VAT: 16,33 zł Brutto: 87,33 zł
ESET PROTECT Entry – 24 miesiące		Netto: 180,00 zł Kwota VAT: 41,40 zł Brutto: 221,40 zł	Netto: 153,00 zł Kwota VAT: 35,19 zł Brutto: 188,19 zł	Netto: 135,00 zł Kwota VAT: 31,05 zł Brutto: 166,05 zł	Netto: 166,00 zł Kwota VAT: 38,18 zł Brutto: 204,18 zł	Netto: 155,00 zł Kwota VAT: 35,65 zł Brutto: 190,65 zł	Netto: 142,00 zł Kwota VAT: 32,66 zł Brutto: 174,66 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia <u>tylko</u> w przypadku oferowania oprogramowania równoważnego)	5–10 stanowisk (należy podać cenę na jedno stanowisko)	11–25 stanowisk (należy podać cenę na jedno stanowisko)	26–49 stanowisk (należy podać cenę na jedno stanowisko)	50–99 stanowisk (należy podać cenę na jedno stanowisko)	100–249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 36 miesięcy subskrypcji		Netto: 269,00 Kwota VAT: 61,87 zł Brutto: 330,87 zł	Netto: 229,00 zł Kwota VAT: 52,67 zł Brutto: 281,67 zł	Netto: 202,00 zł Kwota VAT: 46,46 zł Brutto: 248,46 zł	Netto: 188,00 Kwota VAT: 43,24 zł Brutto: 231,24 zł	Netto: 175,00 zł Kwota VAT: 40,25 zł Brutto: 215,25 zł	Netto: 161,00 zł Kwota VAT: 37,00 zł Brutto: 198,03 zł
ESET PROTECT Advanced – 12 miesięcy subskrypcji		Netto: 116,00 zł Kwota VAT: 26,68 zł Brutto: 142,68 zł	Netto: 99,00 zł Kwota VAT: 22,77 zł Brutto: 121,77 zł	Netto: 87,00 zł Kwota VAT: 20,01 zł Brutto: 107,01 zł	Netto: 108,00 zł Kwota VAT: 24,84 zł Brutto: 132,84 zł	Netto: 100,00 zł Kwota VAT: 23,00 zł Brutto: 123,00 zł	Netto: 93,00 zł Kwota VAT: 21,39 zł Brutto: 114,39 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia <u>tylko</u> w przypadku oferowania oprogramowania równoważnego)	5–10 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	11–25 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	26–49 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	50–99 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	100–249 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	250+ stanowisk (<i>należy podać cenę na jedno stanowisko</i>)
ESET PROTECT Advanced – 24 miesiące subskrypcji		Netto: 233,00 zł Kwota VAT: 53,59 zł Brutto: 286,59 zł	Netto: 199,00 zł Kwota VAT: 45,77 zł Brutto: 244,77 zł	Netto: 175,00 zł Kwota VAT: 40,25 zł Brutto: 215,25 zł	Netto: 217,00 zł Kwota VAT: 49,91 zł Brutto: 266,91 zł	Netto: 201,00 zł Kwota VAT: 46,23 zł Brutto: 247,23 zł	Netto: 186,00 zł Kwota VAT: 42,78 zł Brutto: 228,78 zł
ESET PROTECT Advanced – 36 miesiące subskrypcji		Netto: 350,00 zł Kwota VAT: 80,50 zł Brutto: 403,05 zł	Netto: 298,00 zł Kwota VAT: 68,54 zł Brutto: 366,54 zł	Netto: 263,00 zł Kwota VAT: 60,49 zł Brutto: 323,49 zł	Netto: 326,00 zł Kwota VAT: 77,98 zł Brutto: 400,98 zł	Netto: 303,00 zł Kwota VAT: 69,69 zł Brutto: 372,69 zł	Netto: 279,00 zł Kwota VAT: 64,17 zł Brutto: 343,17 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia <u>tylko</u> w przypadku oferowania oprogramowania równoważnego)	5–10 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	11–25 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	26–49 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	50–99 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	100–249 stanowisk (<i>należy podać cenę na jedno stanowisko</i>)	250+ stanowisk (<i>należy podać cenę na jedno stanowisko</i>)
ESET PROTECT Complete – 12 miesięcy subskrypcji		Netto: 143,00 Kwota VAT: 32,89 zł Brutto: 175,89 zł	Netto: 122,00 zł Kwota VAT: 28,06 zł Brutto: 150,06 zł	Netto: 108,15 zł Kwota VAT: 24,87 zł Brutto: 133,02 zł	Netto: 133,00 zł Kwota VAT: 30,59 zł Brutto: 163,59 zł	Netto: 123,00 zł Kwota VAT: 28,29 zł Brutto: 151,29 zł	Netto: 116,00 zł Kwota VAT: 26,68 zł Brutto: 142,68 zł
ESET PROTECT Complete – 24 miesiące subskrypcji		Netto: 287,00 zł Kwota VAT: 66,01 zł Brutto: 353,01 zł	Netto: 244,00 zł Kwota VAT: 56,12 zł Brutto: 300,12 zł	Netto: 216,00 zł Kwota VAT: 49,68 zł Brutto: 265,68 zł	Netto: 267,00 zł Kwota VAT: 61,41 zł Brutto: 328,41 zł	Netto: 248,00 zł Kwota VAT: 57,04 zł Brutto: 305,04 zł	Netto: 229,00 zł Kwota VAT: 52,67 zł Brutto: 281,67 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia <u>tylko</u> w przypadku oferowania oprogramowania równoważnego)	5–10 stanowisk (należy podać cenę na jedno stanowisko)	11–25 stanowisk (należy podać cenę na jedno stanowisko)	26–49 stanowisk (należy podać cenę na jedno stanowisko)	50–99 stanowisk (należy podać cenę na jedno stanowisko)	100–249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Complete – 36 miesięcy subskrypcji		Netto: 431,00 zł Kwota VAT: 99,13 zł Brutto: 530,13 zł	Netto: 367,00 zł Kwota VAT: 84,41 .zł Brutto: 451,41 zł	Netto: 324,00 zł Kwota VAT: 74,52 zł Brutto: 398,52 zł	Netto: 401,00zł Kwota VAT: 92,23 zł Brutto: 493,23 zł	Netto: 373,00 zł Kwota VAT: 85,79 zł Brutto: 458,79 zł	Netto: 344,00 zł Kwota VAT: 79,12 zł Brutto: 423,12 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 12 miesięcy subskrypcji		Netto: 155,00 zł Kwota VAT: 35,65 zł Brutto: 190,65 zł	Netto: 192,00 zł Kwota VAT: 44,16 zł Brutto: 236,16 zł	Netto: 178,00 zł Kwota VAT: 40,94 zł Brutto: 218,94 zł	Netto: 164,00 zł Kwota VAT: 37,72 zł Brutto: 201,72 zł
ESET PROTECT Enterprise – 24 miesiące subskrypcji		Netto: 310,00 zł Kwota VAT: 71,30 zł Brutto: 381,30 zł	Netto: 385,00 zł Kwota VAT: 88,55 zł Brutto: 473,55 zł	Netto: 358,00 zł Kwota VAT: 82,34 zł Brutto: 440,34 zł	Netto: 329,00 zł Kwota VAT: 75,67 zł Brutto: 404,67 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 36 miesięcy subskrypcji		Netto: 466,00 zł Kwota VAT: 107,18 zł Brutto: 573,18 zł	Netto: 578,00 zł Kwota VAT: 132,94 zł Brutto: 710,94 zł	Netto: 537,00 zł Kwota VAT: 123,51 zł Brutto: 660,51 zł	Netto: 495,00 zł Kwota VAT: 113,85 zł Brutto: 608,85 zł
ESET PROTECT Elite – 12 miesięcy subskrypcji		Netto: 202,00 zł Kwota VAT: 46,46 zł Brutto: 248,46 zł	Netto: 250,00 zł Kwota VAT: 57,50 zł Brutto: 307,50 zł	Netto: 233,00 zł Kwota VAT: 53,59 zł Brutto: 286,59 zł	Netto: 214,00 zł Kwota VAT: 49,22 zł Brutto: 263,22 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Elite – 24 miesiące subskrypcji		Netto: 405,00 zł Kwota VAT: 93,15 zł Brutto: 498,15 zł	Netto: 502,00 zł Kwota VAT: 115,46 zł Brutto: 617,46 zł	Netto: 467,00 zł Kwota VAT: 107,41 zł Brutto: 574,41 zł	Netto: 430,00 zł Kwota VAT: 98,90 zł Brutto: 528,90 zł
ESET PROTECT Elite – 36 miesiące subskrypcji		Netto: 607,00 zł Kwota VAT: 139,61 zł Brutto: 746,61 zł	Netto: 754,00 zł Kwota VAT: 173,42 zł Brutto: 927,42 zł	Netto: 701,00 zł Kwota VAT: 161,23 zł Brutto: 862,23 zł	Netto: 646,00 zł Kwota VAT: 148,58 zł Brutto: 794,58 zł

* W przypadku zaofiarowania oprogramowania równoważnego, Wykonawca powinien wpisać w kolumnie „Oprogramowanie równoważne” nazwę producenta zgodną z oferowanym oprogramowaniem.

5. Oświadczam(y), że¹¹:
- 1) ~~jesteśmy mikroprzedsiębiorstwem~~
 - 2) ~~jesteśmy małym przedsiębiorstwem~~
 - 3) ~~jesteśmy średnim przedsiębiorstwem~~
 - 4) prowadzę jednoosobową działalnością gospodarczą: **TAK**
 - 5) ~~jestem osobą fizyczną nieprowadzącą działalności gospodarczej~~
 - 6) ~~jestem innym rodzajem wykonawcy~~

6. Wykaz załączników i dokumentów przedstawianych w ofercie przez Wykonawcę(ów):

a) Załącznik nr 5 – oświadczenie sankcyjne

/Podpisy elektroniczne zgodnie z zasadami reprezentacji/

¹¹ Odpowiednio wypełnić TAK jeśli dotyczy;

Warszawa, dnia 7 lutego 2026 r.



ZAWIADOMIENIE O POPRAWIENIU OCZYWISTYCH OMYŁEK RACHUNKOWYCH

Dotyczy postępowania pn.: „Umowa ramowa na dostawę oprogramowania antywirusowego” - COI-ZAK.262.71.2025

Zamawiający na podstawie art. 223 ust. 2 pkt 2 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 z późn.zm.) zwanej dalej „ustawą Pzp”, poprawia w treści oferty Wykonawcy oczywiste omyłki rachunkowe w następującym zakresie:

było:

		5-10 stanowisk	11-25 stanowisk	26-49 stanowisk	50-99 stanowisk	100-249 stanowisk	250+ stanowisk
ESET PROTECT Entry – 36 miesięcy subskrypcji	Cena jednostkowa netto	269	229	202	188	175	161
	VAT	61,87	52,67	46,46	43,24	40,25	37
	Cena jednostkowa brutto	330,87	281,67	248,46	231,24	215,25	198,03

		5-10 stanowisk	11-25 stanowisk	26-49 stanowisk	50-99 stanowisk	100-249 stanowisk	250+ stanowisk
ESET PROTECT Advanced– 36 miesięcy subskrypcji	Cena jednostkowa netto	350	298	263	326	303	279
	VAT	80,5	68,54	60,49	77,98	69,69	64,17
	Cena jednostkowa brutto	403,05	366,54	323,49	400,98	372,69	343,17

jest:

		5-10 stanowisk	11-25 stanowisk	26-49 stanowisk	50-99 stanowisk	100-249 stanowisk	250+ stanowisk
ESET PROTECT Entry – 36 miesięcy subskrypcji	Cena jednostkowa netto	269	229	202	188	175	161
	VAT	61,87	52,67	46,46	43,24	40,25	37,03
	Cena jednostkowa brutto	330,87	281,67	248,46	231,24	215,25	198,03

		5-10 stanowisk	11-25 stanowisk	26-49 stanowisk	50-99 stanowisk	100-249 stanowisk	250+ stanowisk
ESET PROTECT Advanced– 36 miesięcy subskrypcji	Cena jednostkowa netto	350	298	263	326	303	279
	VAT	80,5	68,54	60,49	74,98	69,69	64,17
	Cena jednostkowa brutto	430,5	366,54	323,49	400,98	372,69	343,17

W toku badania oferty stwierdzono, iż Wykonawca w formularzu ofertowym zobowiązany był do podania cen jednostkowych, kwot podatku VAT wyrażonych w złotych oraz cen brutto. Z analizy treści oferty wynika, że Wykonawca w przeważającej części pozycji formularza ofertowego zastosował stawkę podatku VAT w wysokości 23%. Jedynie w dwóch pozycjach wskazana kwota podatku VAT w złotych nie odpowiada prawidłowemu przeliczeniu ceny netto przy zastosowaniu stawki 23%.

Zdaniem Zamawiającego, powyższe rozbieżności mają charakter oczywistej omyłki rachunkowej, polegającej na błędnym przeliczeniu kwoty podatku VAT, przy jednoczesnym zachowaniu spójności co do przyjętej stawki podatku VAT oraz cen netto. Z treści oferty jednoznacznie wynika wola Wykonawcy zastosowania stawki VAT w wysokości 23%, a poprawa omyłki nie prowadzi do zmiany treści oferty ani nie skutkuje modyfikacją istotnych elementów zobowiązania.

Omyłki rachunkowe zostały również poprawione w zakresie przeliczenia kwoty brutto wynikające z nieprawidłowego sumowania kwoty netto ze stawką VAT wyrażoną w zł.



Zielona Góra, 15 stycznia 2026 r.

OFERTA DLA:

Centralny Ośrodek Informatyki
Aleje Jerozolimskie 132-136
02-305 Warszawa

- **Nazwa postępowania:** „Umowa ramowa na dostawę oprogramowania antywirusowego”
- **Znak sprawy:** COI-ZAK.262.71.2025

ROZDZIAŁ IV – FORMULARZ OFERTY WRAZ Z ZAŁĄCZNIKAMI

OFERTA

na Umowa ramowa na dostawę oprogramowania antywirusowego.

nr referencyjny: COI-ZAK.262.71.2025

Centralny Zamawiający:

Centralny Ośrodek Informatyki

Al. Jerozolimskie 132-136

02-305 Warszawa

1. WYKONAWCA:

Niniejsza oferta zostaje złożona przez¹:

Lp.	Nazwa(y) Wykonawcy(ów)	Adres(y) Wykonawcy(ów)	NIP /KRS / REGON / kapitał zakładowy
	SEVEN sp. z o.o.	ul. Chopina 14A 65-001 Zielona Góra	KRS: 0000249558 REGON: 080070691 NIP: 9730852602 Kapitał zakładowy 100 000,00

2. DANE KONTAKTOWE WYKONAWCY²:

[wszelka korespondencja prowadzona będzie wyłącznie na nw. adres / e-mail]:



¹ Wykonawca modeluje tabelę powyżej w zależności od swego składu;

² Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wskazują dane pełnomocnika (lidera), z którym prowadzona będzie wszelka korespondencja;

3. OŚWIADCZENIA

Ja(my) niżej podpisany(i) oświadczam(y), że:

- 4.1. do przedmiotowych dokumentów, w tym zwłaszcza do opisu przedmiotu zamówienia i projektowanych postanowień umowy, nie wnoszę żadnych zastrzeżeń i akceptuję je w pełni,
- 4.2. uzyskaliśmy wszelkie niezbędne informacje do przygotowania oferty i wykonania zamówienia,
- 4.3. w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia,
- 4.4. w przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy ramowej w miejscu i terminie określonym przez Centralny Ośrodek Informatyki,
- 4.5. uważamy się za związanych niniejszą ofertą przez okres wskazany w SWZ,
- 4.6. oferujemy realizację niniejszego zamówienia, zgodnie z opisem przedmiotu zamówienia, zawartym w rozdziale II SWZ,
- 4.7. akceptuję/emy termin płatności za realizację przedmiotu umowy w ciągu 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT,
- 4.8. w kryterium: Deklarowany poziom cyberbezpieczeństwa usługi chmurowej [D] jest zgodny z:

SCCO 2	☐ nie ☒ tak
--------	---

** W przypadku braku wskazania w Formularzu oferty „Deklarowanego poziomu cyberbezpieczeństwa usługi chmurowej” Zamawiający uzna, że Wykonawcy deklaruje poziom SCCO 1 i przyzna 0 pkt w ramach kryterium „Deklarowany poziom cyberbezpieczeństwa usługi chmurowej”.*

4.9. wybór niniejszej oferty³:

- ☒ **NIE** prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego, zgodnie z przepisami o podatku od towarów i usług,
- ☐ prowadzi do powstania u Centralnego Ośrodka Informatyki lub Jednostki obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług i wskazujemy poniżej nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazujemy ich wartość bez kwoty podatku:

Lp.	Nazwa (rodzaj)	Stawka podatku VAT	Wartość bez kwoty podatku
1.	_____		_____ zł
...	_____		_____ zł

4.10. jestem/ ~~nie jestem~~⁴ czynnym podatnikiem podatku VAT,

4.11. wadium wpłacone w pieniądzu należy zwrócić na rachunek bankowy prowadzony w banku⁵:

Nr rachunku: _____

4.12. niniejsze zamówienie⁶:

- ☒ w całości wykonam siłami własnymi,
- ☐ zaangażuję podwykonawców do realizacji przedmiotu zamówienia:
- i wskazuję części zamówienia, którą zamierzam powierzyć podwykonawcy:

³ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy; w przypadku, gdy wybór oferty prowadzi do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług należy wskazać w tabeli nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazać ich wartość bez kwoty podatku;

⁴ niepotrzebne skreślić;

⁵ uzupełnić odpowiednio miejsca podając nazwę banku i numer konta – dotyczy wadium wnoszonego w pieniądzu;

⁶ zaznaczyć w sposób wyraźny oświadczenie Wykonawcy, w przypadku zaangażowania podwykonawców do realizacji przedmiotu zamówienia należy wskazać części zamówienia, które Wykonawca zamierza powierzyć podwykonawcy;

4.13. dane rejestrowe podwykonawców, którym zamierzam powierzyć realizację części zamówienia, o których mowa w pkt. 4.13⁷:

Lp.	Nazwa(y) podwykonawcy(ów)	Adres(y) siedziby PODWYKONAWCY(ów)	Numer wpisu do odpowiedniego rejestru – KRS lub datę rozpoczęcia działalności z CEIDG	NIP oraz Regon
1.				
2.				

4.14. Oświadczam/y, że **zastrzegamy/nie zastrzegamy**⁸ części oferty jako tajemnica przedsiębiorstwa, w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity: Dz.U. z 2022 r., poz. 1123, z późn. zm.) i w związku z tym informacje zawarte w plikach..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ww. przepisów. Pozostałe części oferty oraz załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa.

4.15. Oświadczam/y, że zapoznaliśmy się z Klauzulą Informacyjną Centralnego Ośrodka Informatyki dotyczącą RODO⁹ zamieszczoną w Rozdziale I SWZ – Instrukcja dla Wykonawców.

4.16. Oświadczam/y, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/liśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu, w tym również wykonałem/liśmy obowiązek, który ciąży na mnie/nas zgodnie z „Informacją o przetwarzaniu danych osobowych osób fizycznych, których dane są przekazywane Centralnemu

⁷ uzupełnić odpowiednio – o ile są znane;

⁸ Niepotrzebne skreślić; wypełnić tylko, gdy dotyczy; przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności; w takim przypadku należy wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Ośrodkowi Informatyki przez Wykonawcę w toku postępowania o udzielenie zamówienia publicznego oraz w toku wykonywania umowy”¹⁰

4. CENA OFERTY

- 5.1. oświadczam, że cena zawiera wszelkie koszty jakie Wykonawca poniesie w związku z realizacją zamówienia,
- 5.2. gwarantuję wykonanie niniejszego zamówienia zgodnie z treścią SWZ,
- 5.3. oferujemy wykonanie zamówienia zgodnie z cenami zaoferowanymi w Tabeli cenowej poniżej:

¹⁰ W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Tabela cenowa:

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia <u>tylko</u> w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 12 miesięcy subskrypcji		Netto: 83,94 zł Kwota VAT: 19,31 zł Brutto: 103,25 zł	Netto: 81,65 zł Kwota VAT: 18,78 zł Brutto: 100,43 zł	Netto: 79,28 zł Kwota VAT: 18,23 zł Brutto: 97,51 zł	Netto: 78,89 zł Kwota VAT: 18,14 zł Brutto: 97,03 zł	Netto: 78,12 zł Kwota VAT: 17,97 zł Brutto: 96,09 zł	Netto: 71,96 zł Kwota VAT: 16,55 zł Brutto: 88,51 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Entry – 24 miesiące		Netto: 167,87 zł Kwota VAT: 38,61 zł Brutto: 206,48 zł	Netto: 163,30 zł Kwota VAT: 37,56 zł Brutto: 200,86 zł	Netto: 158,56 zł Kwota VAT: 36,47 zł Brutto: 195,03 zł	Netto: 157,79 zł Kwota VAT: 36,29 zł Brutto: 194,08 zł	Netto: 156,24 zł Kwota VAT: 35,94 zł Brutto: 192,18 zł	Netto: 143,92 zł Kwota VAT: 33,10 zł Brutto: 177,02 zł
ESET PROTECT Entry – 36		Netto: 251,81 zł Kwota VAT: 57,92 zł Brutto: 309,73 zł	Netto: 244,94 zł Kwota VAT: 56,34 zł Brutto: 301,28 zł	Netto: 237,84 zł Kwota VAT: 54,70 zł Brutto: 292,54 zł	Netto: 236,68 zł Kwota VAT: 54,44 zł Brutto: 291,12 zł	Netto: 234,36 zł Kwota VAT: 53,90 zł Brutto: 288,26 zł	Netto: 215,88 zł Kwota VAT: 49,65 zł Brutto: 265,53 zł

Pakiet / Okres licencji	Oferowane oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	5-10 stanowisk (należy podać cenę na jedno stanowisko)	11-25 stanowisk (należy podać cenę na jedno stanowisko)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
miesiące subskrypcji							
ESET PROTECT Advanced – 12 miesięcy subskrypcji		Netto: 109,12 zł Kwota VAT: 25,10 zł Brutto: 134,22 zł	Netto: 106,23 zł Kwota VAT: 24,43 zł Brutto: 130,66 zł	Netto: 103,06 zł Kwota VAT: 23,70 zł Brutto: 126,76 zł	Netto: 102,58 zł Kwota VAT: 23,59 zł Brutto: 126,17 zł	Netto: 101,43 zł Kwota VAT: 23,33 zł Brutto: 124,76 zł	Netto: 93,45 zł Kwota VAT: 21,49 zł Brutto: 114,94 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Advanced – 24 miesiące subskrypcji		Netto: 218,25 zł Kwota VAT: 50,20 zł Brutto: 268,45 zł	Netto: 212,46 zł Kwota VAT: 48,87 zł Brutto: 261,33 zł	Netto: 206,11 zł Kwota VAT: 47,41 zł Brutto: 253,52 zł	Netto: 205,16 zł Kwota VAT: 47,19 zł Brutto: 252,35 zł	Netto: 202,86 zł Kwota VAT: 46,66 zł Brutto: 249,52 zł	Netto: 186,90 zł Kwota VAT: 42,99 zł Brutto: 229,89 zł
ESET PROTECT Advanced – 36 miesięcy subskrypcji		Netto: 327,37 zł Kwota VAT: 75,30 zł Brutto: 402,67 zł	Netto: 318,70 zł Kwota VAT: 73,30 zł Brutto: 392,00 zł	Netto: 309,17 zł Kwota VAT: 71,11 zł Brutto: 380,28 zł	Netto: 307,75 zł Kwota VAT: 70,78 zł Brutto: 378,53 zł	Netto: 304,29 zł Kwota VAT: 69,99 zł Brutto: 374,28 zł	Netto: 280,35 zł Kwota VAT: 64,48 zł Brutto: 344,83 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Complete – 12 miesięcy subskrypcji		Netto: 134,31 zł Kwota VAT: 30,89 zł Brutto: 165,20 zł	Netto: 130,59 zł Kwota VAT: 30,04 zł Brutto: 160,63 zł	Netto: 126,90 zł Kwota VAT: 29,19 zł Brutto: 156,09 zł	Netto: 126,27 zł Kwota VAT: 29,04 zł Brutto: 155,31 zł	Netto: 124,81 zł Kwota VAT: 28,71 zł Brutto: 153,52 zł	Netto: 115,01 zł Kwota VAT: 26,45 zł Brutto: 141,46 zł
ESET PROTECT Complete – 24 miesiące subskrypcji		Netto: 268,62 zł Kwota VAT: 61,78 zł Brutto: 330,40 zł	Netto: 261,18 zł Kwota VAT: 60,07 zł Brutto: 321,25 zł	Netto: 253,79 zł Kwota VAT: 58,37 zł Brutto: 312,16 zł	Netto: 252,54 zł Kwota VAT: 58,08 zł Brutto: 310,62 zł	Netto: 249,62 zł Kwota VAT: 57,41 zł Brutto: 307,03 zł	Netto: 230,02 zł Kwota VAT: 52,90 zł Brutto: 282,92 zł

Pakiet / Okres licencji	Oferowane	5-10	11-25	26-49	50-99	100-249	250+
	oprogramowanie równoważne (Wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)	stanowisk (należy podać cenę na jedno stanowisko)
ESET		Netto: 402,93 zł Kwota VAT: 92,67 zł Brutto: 495,60 zł	Netto: 391,78 zł Kwota VAT: 90,11 zł Brutto: 481,89 zł	Netto: 380,69 zł Kwota VAT: 87,56 zł Brutto: 468,25 zł	Netto: 378,81 zł Kwota VAT: 87,13 zł Brutto: 465,94 zł	Netto: 374,43 zł Kwota VAT: 86,12 zł Brutto: 460,55 zł	Netto: 345,03 zł Kwota VAT: 79,36 zł Brutto: 424,39 zł
PROTECT Complete – 36 miesięcy subskrypcji							

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Enterprise – 12 miesięcy subskrypcji		Netto: 207,20 zł Kwota VAT: 47,66 zł Brutto: 254,86 zł	Netto: 193,06 zł Kwota VAT: 44,40 zł Brutto: 237,46 zł	Netto: 179,55 zł Kwota VAT: 41,30 zł Brutto: 220,85 zł	Netto: 165,41 zł Kwota VAT: 38,04 zł Brutto: 203,45 zł
ESET PROTECT Enterprise – 24 miesiące subskrypcji		Netto: 414,40 zł Kwota VAT: 95,31 zł Brutto: 509,71 zł	Netto: 386,12 zł Kwota VAT: 88,81 zł Brutto: 474,93 zł	Netto: 359,10 zł Kwota VAT: 82,59 zł Brutto: 441,69 zł	Netto: 330,82 zł Kwota VAT: 76,09 zł Brutto: 406,91 zł
ESET PROTECT Enterprise –		Netto: 621,60 zł Kwota VAT: 142,97 zł	Netto: 579,18 zł Kwota VAT: 133,21 zł	Netto: 538,65 zł Kwota VAT: 123,89 zł	Netto: 496,23 zł Kwota VAT: 114,13 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
36 miesięcy subskrypcji		Brutto: 764,57 zł	Brutto: 712,39 zł	Brutto: 662,54 zł	Brutto: 610,36 zł
ESET PROTECT Elite – 12 miesięcy subskrypcji		Netto: 270,20 zł Kwota VAT: 62,15 zł Brutto: 332,35 zł	Netto: 251,79 zł Kwota VAT: 57,91 zł Brutto: 309,70 zł	Netto: 234,29 zł Kwota VAT: 53,89 zł Brutto: 288,18 zł	Netto: 215,81 zł Kwota VAT: 49,64 zł Brutto: 265,45 zł
ESET PROTECT Elite – 24 miesiące subskrypcji		Netto: 540,40 zł Kwota VAT: 124,29 zł Brutto: 664,69 zł	Netto: 503,58 zł Kwota VAT: 115,82 zł Brutto: 619,40 zł	Netto: 468,58 zł Kwota VAT: 107,77 zł Brutto: 576,35 zł	Netto: 431,62 zł Kwota VAT: 99,27 zł Brutto: 530,89 zł

Pakiet okres licencji	Oferowane oprogramowanie równoważne (wykonawca wypełnia tylko w przypadku oferowania oprogramowania równoważnego)	26-49 stanowisk (należy podać cenę na jedno stanowisko)	50-99 stanowisk (należy podać cenę na jedno stanowisko)	100-249 stanowisk (należy podać cenę na jedno stanowisko)	250+ stanowisk (należy podać cenę na jedno stanowisko)
ESET PROTECT Elite – 36 miesięcy subskrypcji		Netto: 810,60 zł Kwota VAT: 186,44 zł Brutto: 997,04 zł	Netto: 755,37 zł Kwota VAT: 173,74 zł Brutto: 929,11 zł	Netto: 702,87 zł Kwota VAT: 161,66 zł Brutto: 864,53 zł	Netto: 647,43 zł Kwota VAT: 148,91 zł Brutto: 796,34 zł

* W przypadku zaoferowania oprogramowania równoważnego, Wykonawca powinien wpisać w kolumnie „Oprogramowanie równoważne” nazwę producenta zgodną z oferowanym oprogramowaniem.

5. Oświadczam(y), że¹¹:

- 1) jesteśmy mikroprzedsiębiorstwem: TAK
- 2) ~~jesteśmy małym przedsiębiorstwem:~~
- 3) ~~jesteśmy średnim przedsiębiorstwem:~~
- 4) ~~prowadzę jednoosobową działalność gospodarczą:~~
- 5) ~~jestem osobą fizyczną nieprowadzącą działalności gospodarczej:~~
- 6) ~~jestem innym rodzajem wykonawcy:~~

6. Wykaz załączników i dokumentów przedstawianych w ofercie przez
Wykonawcę(ów):

- 1)
- 2)
- 3)¹²

Zielona Góra,

Miejscowość /	Podpis(y) osoby(osób) upoważnionej(ych) do reprezentowania
Data	Wykonawcy(ów)

¹¹ Odpowiednio wypełnić TAK jeśli dotyczy;

¹² odpowiednio uzupełnić;

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Nazwa zamówienia

Umowa ramowa na dostawę chmurowego oprogramowania antywirusowego.

2. Oznaczenie przedmiotu zamówienia wg CPV

48761000-0 Pakiety oprogramowania antywirusowego

3. Określenie przedmiotu zamówienia

3.1. Przedmiotem zamówienia jest dostawa oprogramowania antywirusowego wymienionego w pkt 6 lub oprogramowania do nich równoważnego dla Jednostek (dalej: Jednostki).

4. Termin wykonania zamówienia

4.1. Umowa ramowa będzie obowiązywać przez 12 miesięcy od dnia jej zawarcia lub do wyczerpania maksymalnej wartości brutto, w zależności od tego, które zdarzenie nastąpi pierwsze.

4.2. Zamówienia wykonawcze zostaną udzielone na poszczególne dostawy w miarę istniejących potrzeb, na podstawie umowy wykonawczej, zgodnie z procedurami określonymi w umowie ramowej. Termin realizacji zamówienia wykonawczego, zawartego na podstawie umowy ramowej, wynosi nie dłużej niż 6 dni kalendarzowych od dnia zawarcia umowy wykonawczej.

4.3. Okres obowiązywania umowy wykonawczej zostanie określony na etapie postępowania wykonawczego przez Jednostki tj. minimum 12 miesięcy.

Dopuszczalne jest zawarcie umowy na 12, 24, 36 miesięcy.

5. Ogólne warunki realizacji przedmiotu zamówienia

5.1. Sposób dostawy Oprogramowania:

5.1.1. Wykonawca zapewni dostęp do oprogramowania zgodnie z zapisami umowy wykonawczej.

5.1.2. Wykonawca dostarczy wszelkie dane niezbędne do prawidłowego uruchomienia i korzystania z Oprogramowania

5.1.3. Zawarte w Opisie przedmiotu zamówienia wymagania i zobowiązania Wykonawcy - o ile nie zastosowano wyłączenia - dotyczą zarówno Wykonawcy, który dostarczy oprogramowanie wymagane, jak i Oprogramowanie równoważne.

- 5.1.4. Wszelkie dane gromadzone, przetwarzane lub przechowywane w związku z funkcjonowaniem systemu antywirusowego (w tym m.in. dane konfiguracyjne, dane o zdarzeniach bezpieczeństwa, logi, informacje o użytkownikach i urządzeniach) muszą być przechowywane i przetwarzane wyłącznie na terytorium Europejskiego Obszaru Gospodarczego (EOG).
- 5.1.5. Wykonawca zobowiązany jest do zapewnienia, że dane te nie będą transferowane poza EOG ani powierzane podmiotom przetwarzającym, które przechowują lub przetwarzają dane poza EOG.
- 5.1.6. Oprogramowanie wymienione w Opisie przedmiotu zamówienia musi pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez producenta kanałów dystrybucyjnych i spełniać standard bezpieczeństwa danych na poziomie co najmniej SCCO1.
- 5.1.7. Zamawiający wymaga, aby Wykonawca dostarczył najnowsze wersje Oprogramowania i umożliwił jego aktualizację w każdym momencie użytkowania.
- 5.1.8. Zamawiający wymaga świadczenia usługi wsparcia technicznego przez cały okres używania Oprogramowania lub Oprogramowania równoważnego. Usługa wsparcia technicznego świadczona będzie przez producenta lub autoryzowany przez niego podmiot.
- 5.1.9. Minimalna miesięczna dostępność Oprogramowania wynosi 99,5%.
- 5.2. Zakres usługi wsparcia to:
- 5.2.1.1. zapewnienie świadczenia obsługi zgłoszeń serwisowych we wszystkie dni tygodnia w formie elektronicznej - poprzez internetowy serwis asysty technicznej lub dedykowaną skrzynkę mailową, a także obsługę telefoniczną, zgodnie z danymi wskazanymi przez Wykonawcę Umowie wykonawczej oraz wyznaczenie koordynatora dla każdego zgłoszenia komunikującego się w języku polskim.
- 5.2.1.2. elektroniczny dostęp do informacji na temat posiadanego Oprogramowania, biuletynów technicznych, poprawek programistycznych oraz bazy danych zgłoszonych problemów technicznych przez 24 godziny na dobę, 7 dni w tygodniu przez internetowy serwis asysty technicznej,

- 5.2.1.3. publikowanie i udostępnianie aktualizacji dokumentacji do Oprogramowania w postaci elektronicznej przez internetowy serwis asysty technicznej producenta, takich jak np.: techniczna dokumentacja, internetowa baza wiedzy lub forum internetowe producenta Oprogramowania oraz informowanie o dostępnych aktualizacjach, np. poprzez newsletter lub dedykowaną stronę www udostępnioną Jednostkom.
- 5.2.1.4. publikowanie i udostępnianie wersji instalacyjnych Oprogramowania (w tym dostęp do aktualizacji wersji, poprawek programistycznych, wydań uzupełniających Oprogramowania objętego usługą wsparcia) do pobrania poprzez internetowy serwis asysty technicznej producenta (nowe wersje Oprogramowania mają być dostępne dla Jednostek, od momentu publikacji w internetowym serwisie asysty technicznej producenta, przez cały okres obowiązywania wsparcia technicznego dla Oprogramowania)
- 5.2.1.5. przyjmowanie, rejestrowanie, monitorowanie i obsługiwanie zgłoszeń serwisowych przez Wykonawcę (w tym także telefonicznych).

6. Wymagania szczegółowe dla Oprogramowania

6.1. ESET PROTECT Entry lub równoważne, które spełnia nw. wymagania:

6.1.1. Administracja zdalna

- 6.1.1.1. Konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS).
- 6.1.1.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
- 6.1.1.3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
- 6.1.1.4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- 6.1.1.5. Rozwiązanie musi posiadać dedykowaną aplikację, umożliwiającą co najmniej:

- 6.1.1.5.1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
- 6.1.1.5.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
- 6.1.1.5.3. Buforowanie ruchu HTTPS.
- 6.1.1.6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- 6.1.1.7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
- 6.1.1.8. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy jednej z następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - 6.1.1.8.1. Google Authenticator,
 - 6.1.1.8.2. Microsoft Authenticator,
 - 6.1.1.8.3. Authy,
 - 6.1.1.8.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
- 6.1.1.9. Rozwiązanie musi posiadać minimum 80 szablonów raportów.
- 6.1.1.10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
 - 6.1.1.10.1. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania oraz ochrony, wersja systemu operacyjnego, podzespoły komputera.
- 6.1.1.11. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
 - 6.1.1.11.1. codziennie,
 - 6.1.1.11.2. cotygodniowo,
 - 6.1.1.11.3. co miesiąc,
 - 6.1.1.11.4. co rok,
 - 6.1.1.11.5. po wystąpieniu nowego zdarzenia,

6.1.1.11.6. po automatycznym umieszczeniu hosta w grupie dynamicznej.

6.1.1.12. Konsola centralnego zarządzania musi być dostępna co najmniej w języku polskim.

6.1.1.13. Rozwiązanie musi mieć możliwość tagowania obiektów.

6.1.1.14. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

6.1.1.15. Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.

6.1.2. Ochrona stacji roboczych - Windows

6.1.2.1. Rozwiązanie musi wspierać systemy operacyjne Windows.

6.1.2.2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

6.1.2.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.

6.1.2.4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6.1.2.5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.

6.1.2.6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.

6.1.2.7. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6.1.2.8. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

6.1.2.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.

6.1.2.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych

procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).

6.1.2.11. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.1.2.11.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

6.1.2.11.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.1.2.11.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.1.2.12. 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).

6.1.2.13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.

6.1.2.14. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6.1.2.15. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

6.1.2.15.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.

6.1.2.15.2. parametry urządzenia: numer seryjny, producent, model.

6.1.2.15.3. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.

- 6.1.2.15.4. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.1.2.16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - 6.1.2.16.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i
 - 6.1.2.16.2. wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - 6.1.2.16.3. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - 6.1.2.16.4. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - 6.1.2.16.5. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i
 - 6.1.2.16.6. 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,
 - 6.1.2.16.7. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 6.1.2.17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 6.1.2.18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów
- 6.1.2.19. filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- 6.1.2.20. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.
- 6.1.2.21. Raport musi posiadać co najmniej:
 - 6.1.2.21.1. listę zainstalowanych aplikacji,
 - 6.1.2.21.2. listę usług systemowych,
 - 6.1.2.21.3. informacje o systemie operacyjnym i sprzęcie,
 - 6.1.2.21.4. listę aktywnych procesów i połączeń sieciowych,

- 6.1.2.21.5.harmonogram systemu operacyjnego,
- 6.1.2.21.6.szczegóły pliku hosts,
- 6.1.2.21.7.Informacje o sterownikach.
- 6.1.2.22. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: antywirus, zaporę osobistą, sandbox, antyspyware, metody heurystyczne.
- 6.1.2.23. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
- 6.1.2.24. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- 6.1.2.25. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
- 6.1.2.26. Ochrona musi być realizowana w oparciu o co najmniej:
 - 6.1.2.26.1.globalna czarna lista RBL,
 - 6.1.2.26.2.czarna lista użytkownika,
 - 6.1.2.26.3.biała lista użytkownika, na którą automatycznie muszą zostać dodane adresy email z książki adresowej klienta Microsoft Outlook.
- 6.1.2.27. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- 6.1.2.28. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
- 6.1.2.29. Skanowanie portów TCP oraz UDP,
- 6.1.2.30. Wykrywanie duplikacji adresu IP,
- 6.1.2.31. Atak zatrutowania ARP,
- 6.1.2.32. Nieprawidłowa długość pakietu TCP oraz UDP.
- 6.1.2.33. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
- 6.1.2.34. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
- 6.1.2.35. Rozwiązanie musi posiadać moduł zapory osobistej.

- 6.1.2.36. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.
- 6.1.2.37. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.1.2.37.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 6.1.2.37.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - 6.1.2.37.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - 6.1.2.37.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- 6.1.2.38. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
- 6.1.2.39. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki.
- 6.1.2.40. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- 6.1.2.41. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- 6.1.2.42. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja
- 6.1.2.43. TeamViewer kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
- 6.1.2.44. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych..
- 6.1.2.45. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
- 6.1.2.46. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: treść komunikatu, obraz.

6.1.3. Ochrona stacji roboczych – MacOS

- 6.1.3.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 oraz nowszych.

- 6.1.3.2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
- 6.1.3.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.1.3.4. 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 mieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 6.1.3.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
- 6.1.3.6. Rozwiązanie musi chronić pliki co najmniej za pomocą: sygnatur wirusów, reputacji chmurowej.
- 6.1.3.7. Rozwiązanie musi umożliwiać 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).
- 6.1.3.8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
- 6.1.3.8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
 - 6.1.3.8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.1.3.8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.1.3.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.1.3.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych

procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).

6.1.3.11. Rozwiązanie musi posiadać moduł zapory osobistej.

6.1.3.12. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł.

6.1.3.13. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

6.1.3.13.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

6.1.3.13.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący.

6.1.4. Ochrona stacji roboczych – Linux

6.1.4.1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:

■ Ubuntu Desktop, Red Hat Enterprise Linux, Linux Mint.

6.1.4.2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:

Cinnamon, GNOME, KDE, MATE, XFCE.

6.1.4.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.

6.1.4.4. 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 mieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6.1.4.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6.1.4.6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.1.4.6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.1.4.6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.1.4.7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.

6.1.4.8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń.

6.1.4.9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

6.1.4.9.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe,

6.1.4.9.2. parametry urządzenia: numer seryjny, producent, model.

6.1.4.9.3. typ dostępu: brak możliwości zapisu, pełen dostęp, brak dostępu.

6.1.5. Ochrona serwera – Windows Server

6.1.5.1. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.

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

6.1.5.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.

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

6.1.5.5. 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.

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

6.1.5.7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

6.1.5.8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze który umożliwia co najmniej:

6.1.5.8.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

6.1.5.8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.1.5.8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.1.5.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.

6.1.5.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).

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

6.1.5.12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

6.1.5.12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i

6.1.5.12.2. wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

6.1.5.12.3. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

- 6.1.5.12.4. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- 6.1.5.12.5. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i
- 6.1.5.12.6. 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,
- 6.1.5.12.7. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 6.1.5.13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 6.1.5.14. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów
- 6.1.5.15. filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- 6.1.5.16. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.
- 6.1.5.17. Raport musi posiadać co najmniej:
 - 6.1.5.17.1. listę zainstalowanych aplikacji,
 - 6.1.5.17.2. listę usług systemowych,
 - 6.1.5.17.3. informacje o systemie operacyjnym i sprzęcie,
 - 6.1.5.17.4. listę aktywnych procesów i połączeń sieciowych,
 - 6.1.5.17.5. harmonogram systemu operacyjnego,
 - 6.1.5.17.6. szczegóły pliku hosts, informacje o sterownikach.
- 6.1.5.18. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:
antywirus, zaporę osobistą sandbox, antyspyware, metody heurystyczne.
- 6.1.5.19. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

- 6.1.5.20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- 6.1.5.21. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - 6.1.5.21.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
 - 6.1.5.21.2. parametry urządzenia: numer seryjny, producent, model.
 - 6.1.5.21.3. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
- 6.1.5.22. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.1.5.23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - 6.1.5.23.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 6.1.5.23.2. Skanowanie portów TCP oraz UDP,
 - 6.1.5.23.3. Wykrywanie duplikacji adresu IP,
 - 6.1.5.23.4. Atak zatrutowania ARP,
 - 6.1.5.23.5. Nieprawidłowa długość pakietu TCP oraz UDP,
 - 6.1.5.23.6. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
- 6.1.5.24. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 6.1.5.25. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.1.5.26. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.
- 6.1.5.27. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.1.5.27.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

- 6.1.5.27.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- 6.1.5.27.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- 6.1.5.27.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- 6.1.5.28. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

6.1.6. Ochrona serwera – Linux

- 6.1.6.1. Rozwiązanie musi wspierać systemy w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.
- 6.1.6.2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.1.6.3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
- 6.1.6.4. 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 mieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 6.1.6.5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- 6.1.6.6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- 6.1.6.7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze który umożliwia co najmniej:
 - 6.1.6.7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.1.6.7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

- 6.1.6.8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.1.6.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń.
- 6.1.6.10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- 6.1.6.11. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- 6.1.6.12. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN.
- 6.1.6.13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach: proces budowania obrazu kontenera, wdrażanie obrazu kontenera.

6.1.7. Mobile Device Management

- 6.1.7.1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- 6.1.7.2. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: Android, iOS, iPadOS.
- 6.1.7.3. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - 6.1.7.3.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
 - 6.1.7.3.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

- 6.1.7.3.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
- 6.1.7.3.4. Apple Business Manager (ABM),
- 6.1.7.3.5. Android Enterprise (co najmniej w zakresie Device Owner).
- 6.1.7.4. MDM musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowanie urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS, resetowanie hasła blokady ekranu.
- 6.1.7.5. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
- 6.1.7.6. MDM musi umożliwiać co najmniej:
 - 6.1.7.6.1. Dla systemów iOS oraz iPadOS: konfigurację kont e-mail, konfigurację połączeń VPN, konfigurację połączeń Wi-Fi, konfigurację listy certyfikatów, możliwość uruchomienia trybu jednej aplikacji.
 - 6.1.7.6.2. Dla systemu Android: blokadę wykonywania połączeń, blokadę konfiguracji sieci Wi-Fi, blokadę konfiguracji tuneli VPN, zarządzanie aktualizacjami systemu operacyjnego, blokadę zmiany tapety urządzenia.
- 6.1.8. Mobile Threat Defense (MTD) dla systemu Android
 - 6.1.8.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
 - 6.1.8.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
 - 6.1.8.2.1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
 - 6.1.8.2.2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
 - 6.1.8.3. Aplikacja kliencka powinna być dostępna do pobrania z oficjalnego repozytorium aplikacji przeznaczonego dla systemu Android.

- 6.1.8.4. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- 6.1.8.5. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
 - 6.1.8.5.1. Złożoność kodu blokady ekranu: Wzór, PIN, Hasło,
- 6.1.8.6. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,
- 6.1.8.7. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
- 6.1.8.8. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.
- 6.1.8.9. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

6.2. ESET PROTECT Enterprise lub równoważne, które spełnia nw. wymagania:

6.2.1. Administracja zdalna

- 6.2.1.1. Konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS).
- 6.2.1.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu [WWW](#).
- 6.2.1.3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
- 6.2.1.4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
 - 6.2.1.4.1. Rozwiązanie musi posiadać dedykowaną aplikację, umożliwiającą co najmniej:
 - 6.2.1.4.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
 - 6.2.1.4.3. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,

- 6.2.1.4.4. Buforowanie ruchu HTTPS.
- 6.2.1.5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- 6.2.1.6. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
- 6.2.1.7. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy jednej z następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - 6.2.1.7.1. Google Authenticator,
 - 6.2.1.7.2. Microsoft Authenticator,
 - 6.2.1.7.3. Authy,
 - 6.2.1.7.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
- 6.2.1.8. Rozwiązanie musi posiadać minimum 80 szablonów raportów.
- 6.2.1.9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- 6.2.1.10. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby zostać umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania oraz ochrony, wersja systemu operacyjnego, podzespoły komputera.
- 6.2.1.11. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem: codziennie, cotygodniowo, co miesiąc, co rok, po wystąpieniu nowego zdarzenia, po automatycznym umieszczeniu hosta w grupie dynamicznej.
- 6.2.1.12. Konsola centralnego zarządzania musi być dostępna co najmniej w języku polskim.
- 6.2.1.13. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
- 6.2.1.14. Rozwiązanie musi mieć możliwość tagowania obiektów.
- 6.2.1.15. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

6.2.1.16. Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.

6.2.2. Ochrona stacji roboczych - Windows

6.2.2.1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

6.2.2.2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

6.2.2.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.

6.2.2.4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6.2.2.5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.

6.2.2.6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.

6.2.2.7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.

6.2.2.8. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.

6.2.2.9. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6.2.2.10. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

6.2.2.11. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.

6.2.2.12. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych

procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).

6.2.2.13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.2.2.13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

6.2.2.13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.2.2.13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.2.2.14. 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).

6.2.2.15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.

6.2.2.16. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6.2.2.17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

6.2.2.17.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.

6.2.2.17.2. parametry urządzenia: numer seryjny, producent, model.

6.2.2.17.3. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.

- 6.2.2.17.4. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.2.2.18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- 6.2.2.18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i
 - 6.2.2.18.2. wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - 6.2.2.18.3. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - 6.2.2.18.4. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - 6.2.2.18.5. 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,
 - 6.2.2.18.6. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 6.2.2.19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 6.2.2.20. 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.
- 6.2.2.21. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.
- 6.2.2.22. Raport musi posiadać co najmniej: listę zainstalowanych aplikacji, listę usług systemowych, informacje o systemie operacyjnym i sprzęcie, listę aktywnych procesów i połączeń sieciowych, harmonogram systemu operacyjnego, szczegóły pliku hosts, informacje o sterownikach.
- 6.2.2.23. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące

funkcje systemu: antywirus, zapora osobista, sandbox, antyspyware, metody heurystyczne.

- 6.2.2.24. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
- 6.2.2.25. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- 6.2.2.26. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
- 6.2.2.27. Ochrona musi być realizowana w oparciu o co najmniej:
 - 6.2.2.27.1. globalna czarna lista RBL,
 - 6.2.2.27.2. czarna lista użytkownika,
 - 6.2.2.27.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
- 6.2.2.28. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - 6.2.2.28.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 6.2.2.28.2. Skanowanie portów TCP oraz UDP,
 - 6.2.2.28.3. Wykrywanie duplikacji adresu IP,
 - 6.2.2.28.4. Atak zatrutowania ARP,
 - 6.2.2.28.5. Nieprawidłowa długość pakietu TCP oraz UDP.
 - 6.2.2.28.6. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
- 6.2.2.29. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 6.2.2.30. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.2.2.31. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
- 6.2.2.32. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.2.2.32.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

- 6.2.2.32.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- 6.2.2.32.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- 6.2.2.32.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- 6.2.2.33. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
- 6.2.2.34. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki.
- 6.2.2.35. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- 6.2.2.36. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- 6.2.2.37. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
- 6.2.2.38. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
- 6.2.2.39. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
- 6.2.2.40. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: treść komunikatu, obraz.

6.2.3. Ochrona stacji roboczych – MacOS

- 6.2.3.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 oraz nowszych.
- 6.2.3.2. Rozwiązanie musi być dostępne co najmniej w języku polskim
- 6.2.3.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.2.3.4. 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 mieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6.2.3.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6.2.3.6. Rozwiązanie musi chronić pliki co najmniej za pomocą: sygnatur wirusów, reputacji chmurowej.

- 6.2.3.7. Rozwiązanie musi umożliwiać 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).
- 6.2.3.8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
 - 6.2.3.8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
 - 6.2.3.8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.2.3.8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.2.3.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.2.3.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).
- 6.2.3.11. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.2.3.12. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł.
- 6.2.3.13. Zapora osobista musi posiadać co najmniej dwa tryby pracy:
 - 6.2.3.13.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 6.2.3.13.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący.

6.2.4. Ochrona stacji roboczych – Linux

- 6.2.4.1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: Ubuntu Desktop, Red Hat Enterprise Linux, Linux Mint.

- 6.2.4.2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu: Cinnamon, GNOME, KDE, MATE, XFCE.
- 6.2.4.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.2.4.4. 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 mieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 6.2.4.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
- 6.2.4.6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze który umożliwia co najmniej:
- 6.2.4.6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.2.4.6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.2.4.7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.2.4.8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń,
- 6.2.4.9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- 6.2.4.9.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe,
 - 6.2.4.9.2. parametry urządzenia: numer seryjny, producent, model.
 - 6.2.4.9.3. typ dostępu: brak możliwości zapisu, pełen dostęp, brak dostępu.

6.2.5. Ochrona serwera – Windows Server

- 6.2.5.1. Rozwiązanie musi wspierać systemy w tym co najmniej:
Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016,
Microsoft Windows Server 2019, Microsoft Windows Server 2022,
Microsoft Windows Server 2025.
- 6.2.5.2. Rozwiązanie musi zapewniać ochronę przed wirusami,
trojanami, robakami i innymi zagrożeniami.
- 6.2.5.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń
co najmniej typu: wirus, trojan, robak, adware, spyware, dialer,
phishing, backdoor.
- 6.2.5.4. Rozwiązanie musi zapewniać możliwość skanowania dysków
sieciowych typu NAS.
- 6.2.5.5. 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.
- 6.2.5.6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną
aktualizację silnika detekcji.
- 6.2.5.7. Rozwiązanie musi posiadać możliwość wykluczania ze
skanowania procesów.
- 6.2.5.8. Rozwiązanie musi posiadać system wczesnego ostrzegania
oparty na chmurze, który umożliwia co najmniej:
 - 6.2.5.8.1. Sprawdzenie reputacji działających procesów i plików co
najmniej z poziomu interfejsu programu oraz menu
kontekstowego.
 - 6.2.5.8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz
dokumentów użytkowników.
 - 6.2.5.8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które
nie mają być wysyłane do analizy.
- 6.2.5.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu
kontekstowego oraz zgodnie z harmonogramem co najmniej: całego
dysku, wybranych katalogów, pojedynczych plików, plików

spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.

- 6.2.5.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).
- 6.2.5.11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- 6.2.5.12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - 6.2.5.12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i
 - 6.2.5.12.2. wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - 6.2.5.12.3. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - 6.2.5.12.4. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - 6.2.5.12.5. 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,
 - 6.2.5.12.6. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 6.2.5.13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 6.2.5.14. 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.
- 6.2.5.15. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.

- 6.2.5.16. Raport musi posiadać co najmniej: listę zainstalowanych aplikacji, listę usług systemowych, informacje o systemie operacyjnym i sprzęcie, listę aktywnych procesów i połączeń sieciowych, harmonogram systemu operacyjnego, szczegóły pliku hosts, informacje o sterownikach.
- 6.2.5.17. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: antywirus, zaporę osobistą, sandbox, antyspyware, metody heurystyczne.
- 6.2.5.18. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
- 6.2.5.19. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- 6.2.5.20. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- 6.2.5.20.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
- 6.2.5.20.2. parametry urządzenia: numer seryjny, producent, model.
- 6.2.5.20.3. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
- 6.2.5.21. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.2.5.22. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- 6.2.5.22.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
- 6.2.5.22.2. Skanowanie portów TCP oraz UDP,
- 6.2.5.22.3. Wykrywanie duplikacji adresu IP,
- 6.2.5.22.4. Atak zatrutowania ARP,
- 6.2.5.22.5. Nieprawidłowa długość pakietu TCP oraz UDP.

6.2.5.22.6. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.

6.2.5.23. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

6.2.5.24. Rozwiązanie musi posiadać moduł zapory osobistej.

6.2.5.25. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.

6.2.5.26. Zapora osobista musi posiadać co najmniej cztery tryby pracy:

6.2.5.26.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

6.2.5.26.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

6.2.5.26.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

6.2.5.26.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

6.2.5.27. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

6.2.6. Ochrona serwera – Linux

6.2.6.1. Rozwiązanie musi wspierać systemy w tym co najmniej:

RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.

6.2.6.2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.

6.2.6.3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.

6.2.6.4. 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 mieć

możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

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

6.2.6.6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

6.2.6.7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.2.6.7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.2.6.7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.2.6.8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.

6.2.6.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń.

6.2.6.10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

6.2.6.11. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

6.2.6.12. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN

6.2.6.13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach: proces budowania obrazu kontenera, wdrażanie obrazu kontenera.

6.2.7. Mobile Device Management

- 6.2.7.1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- 6.2.7.2. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: Android, iOS, iPadOS.
- 6.2.7.3. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - 6.2.7.3.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
 - 6.2.7.3.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - 6.2.7.3.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - 6.2.7.3.4. Apple Business Manager (ABM),
 - 6.2.7.3.5. Android Enterprise (co najmniej w zakresie Device Owner).
- 6.2.7.4. MDM musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowanie urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS, resetowanie hasła blokady ekranu.
- 6.2.7.5. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
- 6.2.7.6. MDM musi umożliwiać co najmniej:
 - 6.2.7.6.1. Dla systemów iOS oraz iPadOS: konfigurację kont e-mail, konfigurację połączeń VPN, Konfigurację połączeń Wi-Fi, Konfigurację listy certyfikatów, możliwość uruchomienia trybu jednej aplikacji.
 - 6.2.7.6.2. Dla systemu Android: blokadę wykonywania połączeń, blokadę konfiguracji sieci Wi-Fi, blokadę konfiguracji tuneli VPN, zarządzanie aktualizacjami systemu operacyjnego, blokadę zmiany tapety urządzenia.

6.2.8. Mobile Threat Defense (MTD) dla systemu Android

6.2.8.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 oraz nowszych.

6.2.8.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:

6.2.8.2.1. inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.

6.2.8.2.2. dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.

6.2.8.3. Aplikacja kliencka powinna być dostępna do pobrania z oficjalnego repozytorium aplikacji przeznaczonego dla systemu Android.

6.2.8.4. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

6.2.8.5. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej: złożoność kodu blokady ekranu, wzór, PIN, hasło, przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu, zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

6.2.8.6. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.

6.2.8.7. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

6.2.9. Sandbox w chmurze

6.2.9.1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.

6.2.9.2. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows 10 oraz 11, Microsoft Windows Server, macOS 11 oraz nowszych, RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu,

Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.

- 6.2.9.3. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 6.2.9.4. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej: archiwa, skrypty, pliki wykonywalne, pliki rejestru systemowego, możliwy spam, dokumenty.
- 6.2.9.5. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
 - 6.2.9.5.1. natychmiast po ich przeanalizowaniu,
 - 6.2.9.5.2. po upływie 30 dni,
 - 6.2.9.5.3. nigdy.
- 6.2.9.6. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- 6.2.9.7. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- 6.2.9.8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzania.
- 6.2.9.9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- 6.2.9.10. Rozwiązanie pozwala na wystanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
- 6.2.9.11. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
- 6.2.9.12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników: czysty, podejrzany, bardzo podejrzany, szkodliwy.
- 6.2.9.13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej: wstrzymania uruchamiania pobieranych

plików z następujących źródeł: przeglądarki internetowe, programy poczty e-mail, nośniki wymienne, pliki wyodrębnione z archiwum.

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

6.2.10. Szyfrowanie

- 6.2.10.1. Rozwiązanie musi wspierać systemy operacyjne Windows.
- 6.2.10.2. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
- 6.2.10.3. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
- 6.2.10.4. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
- 6.2.10.5. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
- 6.2.10.6. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
- 6.2.10.7. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
- 6.2.10.8. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
- 6.2.10.9. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
- 6.2.10.10. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
- 6.2.10.11. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.

6.2.10.12. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania, który umożliwia odszyfrowanie dysku.

6.2.11. Endpoint Detection and Response / eXtended Detection and Response

6.2.11.1. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora.

6.2.11.2. Moduł EDR/XDR powinien umożliwiać stosowanie dwuskładnikowego uwierzytelniania podczas logowania do konsoli administracyjnej oraz innych interfejsów zarządzających.

6.2.11.3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego: tworzenie procesów, uruchamianie, zatrzymanie i modyfikacja usług, utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym, usuwanie oraz zmiana nazw plików, tworzenie i usuwanie kluczy rejestru systemowego, ładowanie bibliotek DLL, zalogowanie użytkowników, elementy sieciowe, w tym co najmniej pobranie plików wykonywalnych, zestawienie połączeń TCP/IP, zapytania HTTP, zapytania DNS.

6.2.11.4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.

6.2.11.5. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:

6.2.11.5.1. blokowanie pliku wykonywalnego,

6.2.11.5.2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,

6.2.11.5.3. blokowanie podejrzanej biblioteki DLL,

6.2.11.5.4. zakończenie procesu,

6.2.11.5.5. skanowanie komputera w poszukiwaniu zagrożeń,

6.2.11.5.6. wyłączenie komputera,

6.2.11.5.7. izolacja sieciowa hosta,

6.2.11.5.8. wylogowanie użytkownika.

- 6.2.11.6. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.
- 6.2.11.7. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
- 6.2.11.8. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
- 6.2.11.9. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej: proces, proces nadrzędny (proces rodzica), nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, SHA-2, użytkownika.
- 6.2.11.10. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
- 6.2.11.11. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
- 6.2.11.12. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
- 6.2.11.13. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące): SHA-1, SHA-256.
 - 6.2.11.13.1. Rozwiązanie musi dawać możliwość weryfikację plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
 - 6.2.11.13.2. hash pliku SHA-1,
 - 6.2.11.13.3. hash pliku SHA-256,
 - 6.2.11.13.4. hash pliku MD5,
 - 6.2.11.13.5. typ sygnatury podpisu cyfrowego,
 - 6.2.11.13.6. wydawcę certyfikatu,
 - 6.2.11.13.7. wersję pliku,
 - 6.2.11.13.8. oryginalną nazwę pliku,
 - 6.2.11.13.9. rozmiar pliku,
 - 6.2.11.13.10. reputację i popularność pliku,
 - 6.2.11.13.11. pierwsze uruchomienie pliku w środowisku,
 - 6.2.11.13.12. ostatnie uruchomienie pliku w środowisku.
- 6.2.11.14. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:

- 6.2.11.14.1. oznaczania ich jako bezpieczne lub niebezpieczne,
- 6.2.11.14.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
- 6.2.11.14.3. zablokowania wykonywania i wykorzystania pliku,
- 6.2.11.14.4. wysyłania do sandbox.
- 6.2.11.15. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
- 6.2.11.16. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny, pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, wysyłania do sandbox.
- 6.2.11.17. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
- 6.2.11.18. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
- 6.2.11.19. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
- 6.2.11.20. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
- 6.2.11.21. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików.

6.3. ESET PROTECT Elite lub równoważne, które spełnia nw. wymagania

6.3.1. Administracja zdalna

- 6.3.1.1. Konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS).
- 6.3.1.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu [WWW](#).
- 6.3.1.3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.

- 6.3.1.4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- 6.3.1.5. Rozwiązanie musi posiadać dedykowaną aplikację, umożliwiającą co najmniej:
 - 6.3.1.5.1. pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
 - 6.3.1.5.2. pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
 - 6.3.1.5.3. buforowanie ruchu HTTPS.
- 6.3.1.6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- 6.3.1.7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
- 6.3.1.8. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy jednej z następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - 6.3.1.8.1. Google Authenticator,
 - 6.3.1.8.2. Microsoft Authenticator,
 - 6.3.1.8.3. Authy,
 - 6.3.1.8.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
- 6.3.1.9. Rozwiązanie musi posiadać minimum 80 szablonów raportów.
- 6.3.1.10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- 6.3.1.11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby zostać umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
 - 6.3.1.11.1. adresy sieciowe IP,
 - 6.3.1.11.2. aktywne zagrożenia,
 - 6.3.1.11.3. stan funkcjonowania oraz ochrony,
 - 6.3.1.11.4. wersja systemu operacyjnego,
 - 6.3.1.11.5. podzespoły komputera.

- 6.3.1.12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem, codziennie, cotygodniowo, co miesiąc, co rok, po wystąpieniu nowego zdarzenia, po automatycznym umieszczeniu hosta w grupie dynamicznej.
- 6.3.1.13. Konsola centralnego zarządzania musi być dostępna co najmniej w języku polskim.
- 6.3.1.14. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
- 6.3.1.15. Rozwiązanie musi mieć możliwość tagowania obiektów.
- 6.3.1.16. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
- 6.3.1.17. Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.
- 6.3.1.18. Rozwiązanie musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w systemie centralnego zarządzania.

6.3.2. Ochrona stacji roboczych - Windows

- 6.3.2.1. Rozwiązanie musi wspierać systemy operacyjne Windows.
- 6.3.2.2. Rozwiązanie musi być dostępne co najmniej w języku polskim.
- 6.3.2.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.3.2.4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 6.3.2.5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
- 6.3.2.6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
- 6.3.2.7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.

- 6.3.2.8. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
- 6.3.2.9. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 6.3.2.10. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- 6.3.2.11. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.3.2.12. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).
 - 6.3.2.12.1. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
 - 6.3.2.12.2. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - 6.3.2.12.3. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.3.2.12.4. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.3.2.13. 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).
- 6.3.2.14. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
- 6.3.2.15. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6.3.2.16. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

6.3.2.16.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne,

6.3.2.16.2. parametry urządzenia: numer seryjny, producent, model. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.

6.3.2.16.3. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.

6.3.2.17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

6.3.2.17.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

6.3.2.17.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

6.3.2.17.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

6.3.2.17.4. 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,

6.3.2.17.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

6.3.2.18. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

- 6.3.2.19. 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.
- 6.3.2.20. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.
- 6.3.2.21. Raport musi posiadać co najmniej: listę zainstalowanych aplikacji, listę usług systemowych, informacje o systemie operacyjnym i sprzęcie, listę aktywnych procesów i połączeń sieciowych, harmonogram systemu operacyjnego, szczegóły pliku hosts, informacje o sterownikach.
- 6.3.2.22. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: antywirus, zapor osobista sandbox, antyspyware, metody heurystyczne.
- 6.3.2.23. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
- 6.3.2.24. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- 6.3.2.25. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
- 6.3.2.26. Ochrona musi być realizowana w oparciu o co najmniej:
- 6.3.2.26.1.globalna czarna lista RBL,
 - 6.3.2.26.2.czarna lista użytkownika,
 - 6.3.2.26.3.biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
- 6.3.2.27. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- 6.3.2.27.1.Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 6.3.2.27.2.Skanowanie portów TCP oraz UDP,
 - 6.3.2.27.3.Wykrywanie duplikacji adresu IP,
 - 6.3.2.27.4.Atak zatrutowania ARP,

- 6.3.2.27.5. Nieprawidłowa długość pakietu TCP oraz UDP.
- 6.3.2.27.6. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
- 6.3.2.28. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 6.3.2.29. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.3.2.30. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.
- 6.3.2.31. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.3.2.31.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 6.3.2.31.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - 6.3.2.31.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- 6.3.2.32. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- 6.3.2.33. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
- 6.3.2.34. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki.
- 6.3.2.35. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- 6.3.2.36. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- 6.3.2.37. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
- 6.3.2.38. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
- 6.3.2.39. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.

6.3.2.40. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: treść komunikatu, obraz.

6.3.3. Ochrona stacji roboczych – MacOS

6.3.3.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 oraz nowszych.

6.3.3.2. Rozwiązanie musi być dostępne co najmniej w języku polskim.

6.3.3.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.

6.3.3.4. 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 mieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6.3.3.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6.3.3.6. Rozwiązanie musi chronić pliki co najmniej za pomocą: sygnatur wirusów, reputacji chmurowej.

6.3.3.7. Rozwiązanie musi umożliwiać 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).

6.3.3.8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.3.3.8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.

6.3.3.8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.3.3.8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.3.3.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.

6.3.3.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).

6.3.3.11. Rozwiązanie musi posiadać moduł zapory osobistej.

6.3.3.12. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł.

6.3.3.13. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

6.3.3.13.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

6.3.3.13.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący.

6.3.4. Ochrona stacji roboczych – Linux

6.3.4.1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: Ubuntu Desktop, Red Hat Enterprise Linux, Linux Mint.

6.3.4.2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu: Cinnamon, GNOME, KDE, MATE, XFCE.

6.3.4.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.

6.3.4.4. 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.

6.3.4.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

- 6.3.4.6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
 - 6.3.4.6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.3.4.6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.3.4.7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.3.4.8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń,
- 6.3.4.9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - 6.3.4.9.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, parametry urządzenia: numer seryjny, producent, model.
 - 6.3.4.9.2. typ dostępu: brak możliwości zapisu, pełen dostęp, brak dostępu.

6.3.5. Ochrona serwera – Windows Server

- 6.3.5.1. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
- 6.3.5.2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
- 6.3.5.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.3.5.4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

- 6.3.5.5. 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.
- 6.3.5.6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- 6.3.5.7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- 6.3.5.8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
- 6.3.5.9. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
- 6.3.5.10. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
- 6.3.5.11. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.3.5.12. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.3.5.13. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).
- 6.3.5.14. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- 6.3.5.15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - 6.3.5.15.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

- 6.3.5.15.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- 6.3.5.15.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- 6.3.5.15.4. 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,
- 6.3.5.15.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 6.3.5.16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 6.3.5.17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- 6.3.5.18. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.
- 6.3.5.19. Raport musi posiadać co najmniej:
 - 6.3.5.19.1. listę zainstalowanych aplikacji,
 - 6.3.5.19.2. listę usług systemowych,
 - 6.3.5.19.3. informacje o systemie operacyjnym i sprzęcie,
 - 6.3.5.19.4. listę aktywnych procesów i połączeń sieciowych,
 - 6.3.5.19.5. harmonogram systemu operacyjnego,
 - 6.3.5.19.6. szczegóły pliku hosts,
 - 6.3.5.19.7. informacje o sterownikach.
- 6.3.5.20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: antywirus, zapora osobista sandbox, antyspyware, metody heurystyczne.
- 6.3.5.21. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

- 6.3.5.22. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- 6.3.5.23. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - 6.3.5.23.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne,
 - 6.3.5.23.2. parametry urządzenia: numer seryjny, producent, model,
 - 6.3.5.23.3. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
 - 6.3.5.23.4. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.3.5.24. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - 6.3.5.24.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 6.3.5.24.2. Skanowanie portów TCP oraz UDP,
 - 6.3.5.24.3. Wykrywanie duplikacji adresu IP,
 - 6.3.5.24.4. Atak zatrutowania ARP,
 - 6.3.5.24.5. Nieprawidłowa długość pakietu TCP oraz UDP.
 - 6.3.5.24.6. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
- 6.3.5.25. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 6.3.5.26. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.3.5.27. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.
- 6.3.5.28. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.3.5.28.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

- 6.3.5.28.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- 6.3.5.28.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- 6.3.5.28.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- 6.3.5.29. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

6.3.6. Ochrona serwera – Linux

- 6.3.6.1. Rozwiązanie musi wspierać systemy w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.
- 6.3.6.2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.3.6.3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
- 6.3.6.4. 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.
- 6.3.6.5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- 6.3.6.6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- 6.3.6.7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
 - 6.3.6.7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.3.6.7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

- 6.3.6.8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- 6.3.6.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń,
- 6.3.6.10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- 6.3.6.11. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- 6.3.6.12. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN.
- 6.3.6.13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach: proces budowania obrazu kontenera, wdrażanie obrazu kontenera.

6.3.7. Mobile Device Management

- 6.3.7.1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- 6.3.7.2. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: Android, iOS, iPadOS.
- 6.3.7.3. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - 6.3.7.3.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
 - 6.3.7.3.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

- 6.3.7.3.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
- 6.3.7.3.4. Apple Business Manager (ABM),
- 6.3.7.3.5. Android Enterprise (co najmniej w zakresie Device Owner).
- 6.3.7.4. MDM musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - 6.3.7.4.1. usunięcie zawartości urządzenia,
 - 6.3.7.4.2. przywrócenie urządzenia do ustawień fabrycznych,
 - 6.3.7.4.3. zablokowanie urządzenia,
 - 6.3.7.4.4. uruchomienie sygnału dźwiękowego,
 - 6.3.7.4.5. lokalizację GPS,
 - 6.3.7.4.6. resetowanie hasła blokady ekranu.
- 6.3.7.5. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
- 6.3.7.6. MDM musi umożliwiać co najmniej:
 - 6.3.7.6.1. Dla systemów iOS oraz iPadOS: konfigurację kont e-mail, konfigurację połączeń VPN, Konfigurację połączeń Wi-Fi, Konfigurację listy certyfikatów, możliwość uruchomienia trybu jednej aplikacji.
 - 6.3.7.6.2. Dla systemu Android: blokadę wykonywania połączeń, blokadę konfiguracji sieci Wi-Fi, blokadę konfiguracji tuneli VPN, zarządzanie aktualizacjami systemu operacyjnego, blokadę zmiany tapety urządzenia
- 6.3.8. Mobile Threat Defense (MTD) dla systemu Android
 - 6.3.8.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 oraz nowszych.
 - 6.3.8.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
 - 6.3.8.2.1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
 - 6.3.8.2.2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.

- 6.3.8.3. Aplikacja kliencka powinna być dostępna do pobrania z oficjalnego repozytorium aplikacji przeznaczonego dla systemu Android.
- 6.3.8.4. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- 6.3.8.5. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej złożoność kodu blokady ekranu: wzór, PIN, hasło, przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu, zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
- 6.3.8.6. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.
- 6.3.8.7. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

6.3.9. Sandbox w chmurze

- 6.3.9.1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
- 6.3.9.2. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows 10 oraz 11, Microsoft Windows Server, macOS 11 (Big Sur) oraz nowszych, RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.
- 6.3.9.3. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 6.3.9.4. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej: archiwa, skrypty, pliki wykonywalne, pliki rejestru systemowego możliwy spam, dokumenty.
- 6.3.9.5. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta

w tym co najmniej: natychmiast po ich przeanalizowaniu, po upływie 30 dni, nigdy.

- 6.3.9.6. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- 6.3.9.7. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- 6.3.9.8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
- 6.3.9.9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- 6.3.9.10. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
- 6.3.9.11. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
- 6.3.9.12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników: czysty, podejrzany, bardzo podejrzany, szkodliwy.
- 6.3.9.13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej: wstrzymania uruchamiania pobieranych plików z następujących źródeł: przeglądarki internetowe, programy poczty e-mail, nośniki wymienne, pliki wyodrębnione z archiwum.
- 6.3.9.14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
- 6.3.9.15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.

6.3.10. Szyfrowanie

6.3.10.1.

- 6.3.10.2. Rozwiązanie musi wspierać systemy operacyjne Windows.
 - 6.3.10.3. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
 - 6.3.10.4. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
 - 6.3.10.5. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
 - 6.3.10.6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
 - 6.3.10.7. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
 - 6.3.10.8. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
 - 6.3.10.9. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
 - 6.3.10.10. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
 - 6.3.10.11. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
 - 6.3.10.12. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
 - 6.3.10.13. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania, który umożliwia odszyfrowanie dysku.
- 6.3.11. Endpoint Detection and Response / eXtended Detection and Response
- 6.3.11.1. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora.
 - 6.3.11.2. Moduł EDR/XDR powinien umożliwiać stosowanie dwuskładnikowego uwierzytelniania podczas logowania do konsoli administracyjnej oraz innych interfejsów zarządzających.
 - 6.3.11.3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego: tworzenie procesów, uruchamianie,

zatrzymanie i modyfikacja usług, utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym, usuwanie oraz zmiana nazw plików, tworzenie i usuwanie kluczy rejestru systemowego, ładowanie bibliotek DLL, zalogowanie użytkowników, elementy sieciowe, w tym co najmniej pobranie plików wykonywalnych, zestawienie połączeń TCP/IP, zapytania HTTP, zapytania DNS.

6.3.11.4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.

6.3.11.5. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:

6.3.11.5.1. blokowanie pliku wykonywalnego,

6.3.11.5.2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,

6.3.11.5.3. blokowanie podejrzanej biblioteki DLL,

6.3.11.5.4. zakończenie procesu,

6.3.11.5.5. skanowanie komputera w poszukiwaniu zagrożeń,

6.3.11.5.6. wyłączenie komputera,

6.3.11.5.7. izolacja sieciowa hosta,

6.3.11.5.8. wylogowanie użytkownika.

6.3.11.5.9. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

6.3.11.6. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

6.3.11.7. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.

6.3.11.8. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej: proces, proces nadrzędny (proces rodzica), nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, SHA-2, użytkownika.

6.3.11.9. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.

- 6.3.11.10. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
- 6.3.11.11. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące): SHA-1, SHA-256.
- 6.3.11.12. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej: hash pliku SHA-1, hash pliku SHA-256, hash pliku MD5, typ sygnatury podpisu cyfrowego, wydawcę certyfikatu, wersję pliku, oryginalną nazwę pliku, rozmiar pliku, reputację i popularność pliku, pierwsze uruchomienie pliku w środowisku, ostatnie uruchomienie pliku w środowisku,
- 6.3.11.13. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
 - 6.3.11.13.1. oznaczania ich jako bezpieczne lub niebezpieczne,
 - 6.3.11.13.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - 6.3.11.13.3. zablokowania wykonywania i wykorzystania pliku,
 - 6.3.11.13.4. wysyłania do sandbox.
- 6.3.11.14. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
- 6.3.11.15. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny, pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, wysyłania do sandbox.
- 6.3.11.16. Administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
- 6.3.11.17. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
- 6.3.11.18. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.

6.3.11.19. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.

6.3.11.20. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.

6.3.12. Ochrona serwera pocztowego MS Exchange

6.3.12.1. Rozwiązanie musi wspierać co najmniej następujące serwery poczty: Microsoft Exchange 2010 SP3, Microsoft Exchange 2013, Microsoft Exchange 2016, Microsoft Exchange 2019.

6.3.12.2. Rozwiązanie musi zapewniać wsparcie co najmniej dla następujących ról Mailbox, Edge, Hub.

6.3.12.3. Rozwiązanie musi być instalowane na maszynie z serwerem pocztowym Exchange

6.3.12.4. Wszystkie komponenty rozwiązania ochrony serwera pocztowego Exchange muszą pracować na tym samym serwerze, na którym zainstalowany jest Microsoft Exchange (Rozwiązanie nie może pracować jako rozwiązanie typu gateway).

6.3.12.5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.

6.3.12.6. Rozwiązanie musi skanować pocztę wewnętrzną (ruch pocztowy w obrębie serwera Microsoft Exchange).

6.3.12.7. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.

6.3.12.8. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.

6.3.12.9. Rozwiązanie musi posiadać co najmniej następujące warunki:

6.3.12.9.1. nadawca,

6.3.12.9.2. odbiorca,

6.3.12.9.3. temacie wiadomości,

6.3.12.9.4. adres IP nadawcy,

6.3.12.9.5. nazwa, rozmiar i typ załącznika,

- 6.3.12.9.6.rozmiar wiadomości,
- 6.3.12.9.7.nagłówek wiadomości,
- 6.3.12.9.8.godzina odbioru,
- 6.3.12.9.9.obecność załącznika chronionego hasłem,
- 6.3.12.9.10. wynik SPF, DKIM i DMARC.
- 6.3.12.9.11. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:
 - 6.3.12.9.12. poddaj wiadomość kwarantannie,
 - 6.3.12.9.13. odrzuć wiadomość,
 - 6.3.12.9.14. porzuć wiadomość w trybie dyskretnym,
 - 6.3.12.9.15. usuń załącznik,
 - 6.3.12.9.16. dodaj prefix tematu,
 - 6.3.12.9.17. wyślij powiadomienie e-mail,
 - 6.3.12.9.18. pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.
- 6.3.12.10. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
- 6.3.12.11. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
- 6.3.12.12. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
- 6.3.12.13. Rozwiązanie musi posiadać mechanizm greylisting (szara lista).
- 6.3.12.14. Rozwiązanie musi umożliwiać podpisywanie wiadomości za pomocą DKIM.
- 6.3.12.15. Ochrona usług chmurowych
- 6.3.12.16. Rozwiązanie musi posiadać odrębną konsolę centralnego zarządzania:
 - 6.3.12.17. konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS),
 - 6.3.12.18. konsola centralnego zarządzania musi być dostępna z poziomu interfejsu WWW,

- 6.3.12.19. Konsola centralnego zarządzania musi być zabezpieczona za pośrednictwem protokołu szyfrowanego SSL/TLS.
- 6.3.12.20. Konsola centralnego zarządzania musi być dostępna co najmniej w języku polskim.
- 6.3.12.21. Rozwiązanie musi obejmować ochronę dla co najmniej następujących usług:
 - 6.3.12.21.1. Microsoft Exchange Online,
 - 6.3.12.21.2. Microsoft OneDrive,
 - 6.3.12.21.3. Microsoft Sharepoint,
 - 6.3.12.21.4. Microsoft Teams,
 - 6.3.12.21.5. Google Workspace, w tym co najmniej
 - 6.3.12.21.6. Gmail,
 - 6.3.12.21.7. Google Drive.
- 6.3.12.22. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace.
- 6.3.12.23. Rozwiązanie musi umożliwiać:
 - 6.3.12.23.1. Wybór ręczny kont użytkowników, które będą objęte ochroną,
 - 6.3.12.23.2. Wybór automatyczny całego tenantu, gdzie nowo utworzone konta będą automatycznie chronione.
 - 6.3.12.23.3. Rozwiązanie musi posiadać możliwość raportowania w tym co najmniej:
 - 6.3.12.23.4. kont użytkowników, otrzymujących najwięcej spamu,
 - 6.3.12.23.5. kont użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
 - 6.3.12.23.6. kont użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
 - 6.3.12.23.7. kont użytkowników, które mogą być podejrzane.
- 6.3.12.24. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty.
- 6.3.12.25. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.
- 6.3.12.26. Rozwiązanie musi posiadać co najmniej następujące warunki:

- 6.3.12.26.1. nadawca,
- 6.3.12.26.2. temacie wiadomości,
- 6.3.12.26.3. adres IP nadawcy,
- 6.3.12.26.4. nazwa, rozszerzenie i typ załącznika,
- 6.3.12.26.5. nagłówek wiadomości,
- 6.3.12.26.6. godzina odbioru,
- 6.3.12.26.7. wynik SPF, DKIM, DMARC i ARC.
- 6.3.12.26.8. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:
 - 6.3.12.26.9. poddaj wiadomość kwarantannie,
 - 6.3.12.26.10. usuń wiadomość,
 - 6.3.12.26.11. usuń załącznik,
 - 6.3.12.26.12. dodaj prefix tematu,
 - 6.3.12.26.13. wyślij powiadomienie e-mail,
 - 6.3.12.26.14. pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.
- 6.3.12.26.15. Rozwiązanie musi umożliwiać pobranie plików z kwarantanny co najmniej
 - 6.3.12.26.16. 8.1. w formie oryginalnego pliku,
 - 6.3.12.26.17. 8.2. w formie pliku zabezpieczonego hasłem.
- 6.3.12.27. Rozwiązanie musi umożliwiać przypisanie polityk co najmniej na poziomie:
 - 6.3.12.27.1. całego tenantu,
 - 6.3.12.27.2. grupy,
 - 6.3.12.27.3. grupy Teams,
 - 6.3.12.27.4. lokacji Sharepoint,
 - 6.3.12.27.5. Pojedynczego użytkownika.
- 6.3.12.28. Rozwiązanie musi korzystać z chmury reputacji plików:
 - 6.3.12.28.1. możliwość automatycznego wystania sumy kontrolnej
 - 6.3.12.28.2. możliwość automatycznego wystania fragmentu pliku.
- 6.3.12.29. Rozwiązanie musi umożliwiać określenie czynności realizowanej po wykryciu zagrożenia, w tym co najmniej następujące czynności:
 - 6.3.12.29.1. brak czynności,

- 6.3.12.29.2. przenieś do spamu,
- 6.3.12.29.3. poddaj wiadomość kwarantannie,
- 6.3.12.29.4. poddaj załącznik kwarantannie,
- 6.3.12.29.5. przenieś do kosza,
- 6.3.12.29.6. usuń załącznik,
- 6.3.12.29.7. zastąp załącznik
- 6.3.12.29.8. usuń wiadomość.
- 6.3.12.30. Rozwiązanie musi umożliwiać dodanie znacznika do tematu wiadomości zaklasyfikowanej co najmniej jako: SPAM, phishing.
- 6.3.12.31. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
 - 6.3.12.31.1. archiwa,
 - 6.3.12.31.2. skrypty,
 - 6.3.12.31.3. pliki wykonywalne,
 - 6.3.12.31.4. pliki rejestru systemowego
 - 6.3.12.31.5. możliwy spam,
 - 6.3.12.31.6. Dokumenty.
- 6.3.12.32. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
 - 6.3.12.32.1. natychmiast po ich przeanalizowaniu,
 - 6.3.12.32.2. po upływie 30 dni,
 - 6.3.12.32.3. nigdy.
- 6.3.12.33. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail.
- 6.3.12.34. Powiadomienia muszą dotyczyć wykryć co najmniej:
 - 6.3.12.34.1. zagrożeń w wiadomościach,
 - 6.3.12.34.2. phishing w wiadomościach,
 - 6.3.12.34.3. zagrożeń w plikach onedrive,
 - 6.3.12.34.4. zagrożeń na dysku Google Drive,
- 6.3.12.35. Powiadomienia muszą być możliwe do wysłania w co najmniej języku polskim.

6.3.13.Vulnerability Assessment and Patch Management

- 6.3.13.1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
- 6.3.13.2. Rozwiązanie musi mieć możliwości wykrywania podatności:
 - 6.3.13.2.1. w tym co najmniej następujących systemach operacyjnych:
Windows, macOS, Linux, w aplikacjach zainstalowanych na zarządzanych stacjach.
- 6.3.13.3. Rozwiązanie musi posiadać bazę podatności zawierającą co najmniej 35000 CVE.
- 6.3.13.4. Rozwiązanie musi umożliwiać utworzenie harmonogramu automatycznego wykrywania podatności.
- 6.3.13.5. Rozwiązanie musi umożliwiać wyświetlanie szczegółów danej podatności zawierające co najmniej:
 - 6.3.13.5.1. nazwę aplikacji lub systemu operacyjnego
 - 6.3.13.5.2. punktację CVSS
 - 6.3.13.5.3. opis wykrytej podatności
 - 6.3.13.5.4. wartość ryzyka ocenioną przez wewnętrzne mechanizmy producenta
- 6.3.13.6. Rozwiązanie musi wykrywać podatności w minimum 700 aplikacjach.
- 6.3.13.7. Rozwiązanie musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 300 popularnych aplikacji.
- 6.3.13.8. Rozwiązanie musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji.
- 6.3.13.9. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście.
- 6.3.13.10. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
- 6.3.13.11. Rozwiązanie musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji.
- 6.3.13.12. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich ponad 300 aplikacji, oprócz aplikacji wskazanych na czarnej liście.
- 6.3.13.13. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

- 6.3.13.14. Rozwiązanie musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
- 6.3.13.15. Rozwiązanie musi być zintegrowane bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
- 6.3.13.16. Rozwiązanie musi umożliwiać wyłączenie powiadomień dla wybranej podatności.

6.3.14. Two-factor authentication / Multi-factor authentication

- 6.3.14.1. Rozwiązanie musi być dostępna w wersji lokalnej w wersji chmurowej (SaaS).
- 6.3.14.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu [WWW](#).
- 6.3.14.3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
- 6.3.14.4. Rozwiązanie musi pozwalać na instalację oprogramowania na co najmniej następujących systemach operacyjnych: Systemy serwerowe: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025, Systemy kliencie: Windows 8.1, Windows 10, Windows 11.
- 6.3.14.5. Rozwiązanie musi posiadać integrację z następującymi rozwiązaniami:
 - 6.3.14.5.1. Microsoft Exchange,
 - 6.3.14.5.2. Microsoft Dynamics CRM,
 - 6.3.14.5.3. Microsoft Sharepoint,
 - 6.3.14.5.4. Microsoft Remote Desktop Web Access,
 - 6.3.14.5.5. Microsoft Terminal Services Web Access,
 - 6.3.14.5.6. Microsoft Remote Web Access,
 - 6.3.14.5.7. Active Directory Federation Services.
- 6.3.14.6. Aplikacja mobilna musi wspierać następujące systemy:
 - 6.3.14.6.1. Android,
 - 6.3.14.6.2. iOS.

- 6.3.14.7. Aplikacja mobilna musi umożliwiać uwierzytelnienie użytkownika przy pomocy co najmniej:
 - 6.3.14.8. Generowanego kodu OTP w tym co najmniej:
 - 6.3.14.8.1.HOTP,
 - 6.3.14.8.2.TOTP.
 - 6.3.14.8.3.Powiadomienia PUSH.
- 6.3.14.9. Aplikacja mobilna musi posiadać możliwość zabezpieczenia jej przy pomocy kodu PIN oraz danych biometrycznych.
- 6.3.14.10. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP musi odbywać się w trybie offline.
- 6.3.14.11. Aplikacja musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.
- 6.3.14.12. Rozwiązanie musi oferować alternatywne możliwości uwierzytelnienie użytkownika w tym co najmniej:
 - 6.3.14.12.1. OTP dostarczonego przy pomocy wiadomości SMS,
 - 6.3.14.12.2. OTP dostarczonego przy pomocy wiadomości e-mail,
 - 6.3.14.12.3. tokenu sprzętowego,
 - 6.3.14.12.4. FIDO,
 - 6.3.14.12.5. klucza odzyskiwania (MRK).

6.4. ESET PROTECT Complete lub równoważne, które spełnia nw. wymagania

6.4.1. Administracja zdalna

- 6.4.1.1. Konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS).
- 6.4.1.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
- 6.4.1.3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
- 6.4.1.4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- 6.4.1.5. Rozwiązanie musi posiadać dedykowaną aplikację umożliwiającą co najmniej:

- 6.4.1.5.1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
- 6.4.1.5.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
- 6.4.1.5.3. Buforowanie ruchu HTTPS.
- 6.4.1.6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- 6.4.1.7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
- 6.4.1.8. 7.1. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy jednej z następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - 6.4.1.8.1. Google Authenticator,
 - 6.4.1.8.2. Microsoft Authenticator,
 - 6.4.1.8.3. Authy,
 - 6.4.1.8.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
- 6.4.1.9. Rozwiązanie musi posiadać minimum 80 szablonów raportów.
- 6.4.1.10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- 6.4.1.11. 9.1. 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:
 - 6.4.1.11.1. adresy sieciowe IP,
 - 6.4.1.11.2. aktywne zagrożenia,
 - 6.4.1.11.3. stan funkcjonowania oraz ochrony,
 - 6.4.1.11.4. wersja systemu operacyjnego,
 - 6.4.1.11.5. podzespoły komputera.
 - 6.4.1.11.6. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
 - 6.4.1.11.7. codziennie,
 - 6.4.1.11.8. cotygodniowo,
 - 6.4.1.11.9. co miesiąc,

- 6.4.1.11.10. co rok,
- 6.4.1.11.11. po wystąpieniu nowego zdarzenia,
- 6.4.1.11.12. po automatycznym umieszczeniu hosta w grupie dynamicznej.
- 6.4.1.12. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim
- 6.4.1.13. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
- 6.4.1.14. Rozwiązanie musi mieć możliwość tagowania obiektów.
- 6.4.1.15. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
- 6.4.1.16. Eksport danych musi być możliwy w co najmniej następujących formatach:
 - 6.4.1.16.1.JSON,
 - 6.4.1.16.2.LEEF,
 - 6.4.1.16.3.CEF.
- 6.4.1.17. Rozwiązanie musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w systemie centralnego zarządzania.

6.4.2. Ochrona stacji roboczych – Windows

- 6.4.2.1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- 6.4.2.2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
- 6.4.2.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.4.2.4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 6.4.2.5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.

- 6.4.2.6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
- 6.4.2.7. 7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
- 6.4.2.8. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
- 6.4.2.9. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 6.4.2.10. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- 6.4.2.11. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
- 6.4.2.11.1. całego dysku,
 - 6.4.2.11.2. wybranych katalogów,
 - 6.4.2.11.3. pojedynczych plików,
 - 6.4.2.11.4. plików spakowanych oraz skompresowanych,
 - 6.4.2.11.5. dysków sieciowych,
 - 6.4.2.11.6. dysków przenośnych.
 - 6.4.2.11.7. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 6.4.2.11.8. wybranych plików,
 - 6.4.2.11.9. wybranych procesów,
 - 6.4.2.11.10. wybranych lokalizacji,
 - 6.4.2.11.11. wybranych rozszerzeń,
 - 6.4.2.11.12. nazwy wykrycia,
 - 6.4.2.11.13. sumy kontrolnej (SHA1).
- 6.4.2.12. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
- 6.4.2.13. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
- 6.4.2.14. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

- 6.4.2.15. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.4.2.16. 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).
- 6.4.2.17. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
- 6.4.2.18. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 6.4.2.19. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- 6.4.2.19.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
- 6.4.2.19.2. parametry urządzenia: numer seryjny, producent, model.
- 6.4.2.19.3. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
- 6.4.2.19.4. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.4.2.20. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- 6.4.2.20.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- 6.4.2.20.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

6.4.2.20.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

6.4.2.20.4. 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,

6.4.2.20.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

6.4.2.21. 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.

6.4.2.22. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.

6.4.2.23. Raport musi posiadać co najmniej: listę zainstalowanych aplikacji, listę usług systemowych, informacje o systemie operacyjnym i sprzęcie, listę aktywnych procesów i połączeń sieciowych, harmonogram systemu operacyjnego, szczegóły pliku hosts, informacje o sterownikach.

6.4.2.24. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:

6.4.2.24.1. antywirus,

6.4.2.24.2. zaporę osobistą

6.4.2.24.3. sandbox,

6.4.2.24.4. antyspyware,

6.4.2.24.5. metody heurystyczne.

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

- 6.4.2.26. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- 6.4.2.27. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
- 6.4.2.28. Ochrona musi być realizowana w oparciu o co najmniej:
 - 6.4.2.28.1. globalna czarna lista RBL,
 - 6.4.2.28.2. czarna lista użytkownika,
 - 6.4.2.28.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
- 6.4.2.29. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - 6.4.2.29.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 6.4.2.29.2. Skanowanie portów TCP oraz UDP,
 - 6.4.2.29.3. Wykrywanie duplikacji adresu IP,
 - 6.4.2.29.4. Atak zatrutowania ARP,
 - 6.4.2.29.5. Nieprawidłowa długość pakietu TCP oraz UDP.
 - 6.4.2.29.6. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
 - 6.4.2.29.7. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 6.4.2.30. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.4.2.31. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.
- 6.4.2.32. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.4.2.32.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 6.4.2.32.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - 6.4.2.32.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - 6.4.2.32.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

- 6.4.2.33. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
- 6.4.2.34. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki.
- 6.4.2.35. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- 6.4.2.36. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- 6.4.2.37. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
- 6.4.2.38. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
- 6.4.2.39. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
- 6.4.2.40. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: treść komunikatu, obraz.

6.4.3. Ochrona stacji roboczych – MacOS

- 6.4.3.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 oraz nowszych.
- 6.4.3.2. Rozwiązanie musi być dostępne co najmniej w języku polskim.
- 6.4.3.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.4.3.4. 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.
- 6.4.3.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

- 6.4.3.6. Rozwiązanie musi chronić pliki co najmniej za pomocą:
sygnatur wirusów, reputacji chmurowej.
- 6.4.3.7. Rozwiązanie musi umożliwiać 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).
- 6.4.3.8. Rozwiązanie musi posiadać system wczesnego ostrzegania
oparty na chmurze, który umożliwia co najmniej:
- 6.4.3.9. Sprawdzenie reputacji działających aplikacji i plików co
najmniej z poziomu interfejsu programu.
- 6.4.3.10. Konfigurację wysyłania wszystkich plików do analizy oprócz
dokumentów użytkowników.
- 6.4.3.11. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które
nie mają być wysyłane do analizy.
- 6.4.3.12. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu
kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 6.4.3.12.1. całego dysku,
 - 6.4.3.12.2. wybranych katalogów,
 - 6.4.3.12.3. pojedynczych plików,
 - 6.4.3.12.4. plików spakowanych oraz skompresowanych,
 - 6.4.3.12.5. dysków sieciowych,
 - 6.4.3.12.6. dysków przenośnych.
- 6.4.3.13. Rozwiązanie musi posiadać opcję umieszczenia na liście
wykluczeń ze skanowania co najmniej:
 - 6.4.3.13.1. wybranych plików,
 - 6.4.3.13.2. wybranych procesów,
 - 6.4.3.13.3. wybranych lokalizacji,
 - 6.4.3.13.4. wybranych rozszerzeń,
 - 6.4.3.13.5. nazwy wykrycia,
 - 6.4.3.13.6. sumy kontrolnej (SHA1).
- 6.4.3.14. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.4.3.15. Zapora osobista musi działać w oparciu o reguły i musi
posiadać co najmniej 30 wbudowanych reguł,
- 6.4.3.16. zapora osobista musi posiadać co najmniej dwa tryby pracy:

- 6.4.3.16.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
- 6.4.3.16.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący.

6.4.4. Ochrona stacji roboczych – Linux

- 6.4.4.1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: Ubuntu Desktop, Red Hat Enterprise Linux, Linux Mint.
- 6.4.4.2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu: Cinnamon, GNOME, KDE, MATE, XFCE.
- 6.4.4.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
- 6.4.4.4. 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.
- 6.4.4.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
- 6.4.4.6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
 - 6.4.4.6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.4.4.6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.4.4.7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 6.4.4.7.1. całego dysku,
 - 6.4.4.7.2. wybranych katalogów,
 - 6.4.4.7.3. pojedynczych plików,
 - 6.4.4.7.4. plików spakowanych oraz skompresowanych,
 - 6.4.4.7.5. dysków sieciowych,

6.4.4.7.6. dysków przenośnych.

6.4.4.8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

6.4.4.8.1. wybranych plików,

6.4.4.8.2. wybranych procesów,

6.4.4.8.3. wybranych lokalizacji,

6.4.4.8.4. wybranych rozszerzeń,

6.4.4.9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

6.4.4.9.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe,

6.4.4.9.2. parametry urządzenia: numer seryjny, producent, model.

6.4.4.9.3. typ dostępu: brak możliwości zapisu, pełen dostęp, brak dostępu.

6.4.5. Ochrona serwera – Windows Server

6.4.5.1. Rozwiązanie musi wspierać systemy w tym co najmniej:

Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.

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

6.4.5.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

6.4.5.3.1. wirus,

6.4.5.3.2. trojan,

6.4.5.3.3. robak,

6.4.5.3.4. adware,

6.4.5.3.5. spyware,

6.4.5.3.6. dialer,

6.4.5.3.7. phishing,

6.4.5.3.8. backdoor.

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

- 6.4.5.5. 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.
- 6.4.5.6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- 6.4.5.7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- 6.4.5.8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
- 6.4.5.9. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
- 6.4.5.10. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
- 6.4.5.11. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.4.5.12. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 6.4.5.12.1. całego dysku,
 - 6.4.5.12.2. wybranych katalogów,
 - 6.4.5.12.3. pojedynczych plików,
 - 6.4.5.12.4. plików spakowanych oraz skompresowanych,
 - 6.4.5.12.5. dysków sieciowych,
 - 6.4.5.12.6. dysków przenośnych.
- 6.4.5.13. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 6.4.5.13.1. wybranych plików,
 - 6.4.5.13.2. wybranych procesów,
 - 6.4.5.13.3. wybranych lokalizacji,
 - 6.4.5.13.4. wybranych rozszerzeń,
 - 6.4.5.13.5. nazwy wykrycia,
 - 6.4.5.13.6. sumy kontrolnej (SHA1).

- 6.4.5.14. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- 6.4.5.15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- 6.4.5.15.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - 6.4.5.15.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - 6.4.5.15.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - 6.4.5.15.4. 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,
 - 6.4.5.15.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 6.4.5.16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 6.4.5.17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- 6.4.5.18. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.
- 6.4.5.19. Raport musi posiadać co najmniej: listę zainstalowanych aplikacji, listę usług systemowych, informacje o systemie operacyjnym i sprzęcie, listę aktywnych procesów i połączeń sieciowych, harmonogram systemu operacyjnego, szczegóły pliku hosts, informacje o sterownikach.
- 6.4.5.20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:

antywirus,

6.4.5.20.1.zapora osobista

6.4.5.20.2.sandbox,

6.4.5.20.3.antyspyware,

6.4.5.20.4.metody heurystyczne.

6.4.5.21. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

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

6.4.5.23. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

6.4.5.23.1.typ urządzenia: pamięci masowe, optyczne pamięci masowe,

6.4.5.23.2.17.1.3.pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.

6.4.5.23.3.parametry urządzenia: numer seryjny, producent, model.

6.4.5.23.4.typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.

6.4.5.23.5.System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.

6.4.5.24. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

6.4.5.25. Ochrona przed anomaliami sieciowymi, w tym co najmniej:

6.4.5.25.1.skanowanie portów TCP oraz UDP,

6.4.5.25.2.Wykrywanie duplikacji adresu IP,

6.4.5.25.3.Atak zatrutowania ARP,

6.4.5.25.4.Nieprawidłowa długość pakietu TCP oraz UDP.

6.4.5.25.5.Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.

6.4.5.25.6.Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

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

6.4.6. Ochrona serwera – Linux

- 6.4.6.1. Rozwiązanie musi wspierać systemy w tym co najmniej:
RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.
- 6.4.6.2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - 6.4.6.2.1. wirus,
 - 6.4.6.2.2. trojan,
 - 6.4.6.2.3. robak,
 - 6.4.6.2.4. adware,
 - 6.4.6.2.5. spyware,
 - 6.4.6.2.6. dialer,
 - 6.4.6.2.7. phishing,
 - 6.4.6.2.8. backdoor.
- 6.4.6.3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
- 6.4.6.4. 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.

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

6.4.6.6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

6.4.6.7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.4.6.7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.4.6.7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.4.6.7.3. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

6.4.6.7.4. całego dysku,

6.4.6.7.5. wybranych katalogów,

6.4.6.7.6. pojedynczych plików,

6.4.6.7.7. plików spakowanych oraz skompresowanych,

6.4.6.7.8. dysków sieciowych,

6.4.6.7.9. dysków przenośnych.

6.4.6.8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

6.4.6.8.1. wybranych plików,

6.4.6.8.2. wybranych procesów,

6.4.6.8.3. wybranych lokalizacji,

6.4.6.8.4. wybranych rozszerzeń,

6.4.6.9. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

6.4.6.10. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

6.4.6.11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN.

6.4.6.12. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:

6.4.6.12.1. proces budowania obrazu kontenera,

6.4.6.12.2. wdrażanie obrazu kontenera.

6.4.7. Mobile Device Management

6.4.7.1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

6.4.7.2. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:

6.4.7.2.1. Android,

6.4.7.2.2. iOS,

6.4.7.2.3. iPadOS.

6.4.7.3. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:

6.4.7.3.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),

6.4.7.3.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

6.4.7.3.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

6.4.7.3.4. Apple Business Manager (ABM),

6.4.7.3.5. Android Enterprise (co najmniej w zakresie Device Owner).

6.4.7.4. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

6.4.7.4.1. usunięcie zawartości urządzenia,

6.4.7.4.2. przywrócenie urządzenia do ustawień fabrycznych,

6.4.7.4.3. zablokowanie urządzenia,

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

6.4.8. Mobile Threat Defense (MTD) dla systemu Android

- 6.4.8.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 oraz nowszych.
- 6.4.8.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
 - 6.4.8.2.1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
 - 6.4.8.2.2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
- 6.4.8.3. Aplikacja kliencka powinna być dostępna do pobrania z oficjalnego repozytorium aplikacji przeznaczonego dla systemu Android,
- 6.4.8.4. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- 6.4.8.5. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:

6.4.8.5.1. Złożoność kodu blokady ekranu: wzór, PIN, hasło, przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu, zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

6.4.8.5.2. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.

6.4.8.6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

6.4.9. Sandbox w chmurze

6.4.9.1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.

6.4.9.2. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows 10 oraz 11, Microsoft Windows Server, macOS 11 (Big Sur) oraz nowszych, RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.

6.4.9.3. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

6.4.9.4. Rozwiązanie musi wykorzystywać do działania chmurę.

6.4.9.5. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:

6.4.9.5.1. archiwa,

6.4.9.5.2. skrypty,

6.4.9.5.3. pliki wykonywalne,

6.4.9.5.4. pliki rejestru systemowego

6.4.9.5.5. możliwy spam,

6.4.9.5.6. dokumenty.

6.4.9.6. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:

- 6.4.9.6.1. natychmiast po ich przeanalizowaniu,
- 6.4.9.6.2. po upływie 30 dni,
- 6.4.9.6.3. nigdy.
- 6.4.9.7. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- 6.4.9.8. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- 6.4.9.9. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
- 6.4.9.10. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- 6.4.9.11. Rozwiązanie pozwala na wystanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
- 6.4.9.12. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
- 6.4.9.13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
 - 6.4.9.13.1. czysty,
 - 6.4.9.13.2. podejrzany,
 - 6.4.9.13.3. bardzo podejrzany,
 - 6.4.9.13.4. szkodliwy.
- 6.4.9.14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
 - 6.4.9.14.1. wstrzymania uruchamiania pobieranych plików z następujących źródeł: przeglądarki internetowe, programy poczty e-mail, nośniki wymienne, pliki wyodrębnione z archiwum.
- 6.4.9.15. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
- 6.4.9.16. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki

poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

6.4.10.Szyfrowanie

- 6.4.10.1. Rozwiązanie musi wspierać systemy operacyjne Windows.
- 6.4.10.2. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
- 6.4.10.3. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
- 6.4.10.4. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
- 6.4.10.5. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
- 6.4.10.6. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
- 6.4.10.7. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
- 6.4.10.8. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
- 6.4.10.9. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
- 6.4.10.10. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
- 6.4.10.11. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
- 6.4.10.12. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania, który umożliwia odszyfrowanie dysku.

6.4.11.Ochrona serwera pocztowego MS Exchange

- 6.4.11.1. Rozwiązanie musi wspierać co najmniej następujące serwery poczty: Microsoft Exchange 2010 SP3, Microsoft Exchange 2013, Microsoft Exchange 2016, Microsoft Exchange 2019,
- 6.4.11.2. Rozwiązanie musi zapewniać wsparcie co najmniej dla następujących ról:
 - 6.4.11.2.1. Mailbox,
 - 6.4.11.2.2. Edge,
 - 6.4.11.2.3. Hub.
- 6.4.11.3. Rozwiązanie musi być instalowane na maszynie z serwerem pocztowym Exchange
- 6.4.11.4. Wszystkie komponenty rozwiązania ochrony serwera pocztowego Exchange muszą pracować na tym samym serwerze, na którym zainstalowany jest Microsoft Exchange (Rozwiązanie nie może pracować jako rozwiązanie typu gateway).
- 6.4.11.5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
- 6.4.11.6. Rozwiązanie musi skanować pocztę wewnętrzną (ruch pocztowy w obrębie serwera Microsoft Exchange).
- 6.4.11.7. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
- 6.4.11.8. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.
- 6.4.11.9. Rozwiązanie musi posiadać co najmniej następujące warunki:
 - 6.4.11.9.1. nadawca,
 - 6.4.11.9.2. odbiorca,
 - 6.4.11.9.3. temacie wiadomości,
 - 6.4.11.9.4. adres IP nadawcy,
 - 6.4.11.9.5. nazwa, rozmiar i typ załącznika,
 - 6.4.11.9.6. rozmiar wiadomości,
 - 6.4.11.9.7. nagłówek wiadomości,
 - 6.4.11.9.8. godzina odbioru,
 - 6.4.11.9.9. obecność załącznika chronionego hasłem,
 - 6.4.11.9.10. wynik SPF, DKIM i DMARC.

6.4.11.10. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:

- 6.4.11.10.1. poddaj wiadomość kwarantannie,
- 6.4.11.10.2. odrzuć wiadomość,
- 6.4.11.10.3. porzuć wiadomość w trybie dyskretnym,
- 6.4.11.10.4. usuń załącznik,
- 6.4.11.10.5. dodaj prefix tematu,
- 6.4.11.10.6. wyślij powiadomienie e-mail,
- 6.4.11.10.7. pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.

6.4.11.11. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.

6.4.11.12. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.

6.4.11.13. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.

6.4.11.14. Rozwiązanie musi posiadać mechanizm greylisting (szara lista).

6.4.11.15. Rozwiązanie musi umożliwiać podpisywanie wiadomości za pomocą DKIM.

6.4.12. Ochrona usług chmurowych

6.4.12.1. Rozwiązanie musi posiadać odrębną konsolę centralnego zarządzania:

6.4.12.1.1. konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS),

6.4.12.1.2. konsola centralnego zarządzania musi być dostępna z poziomu interfejsu WWW,

6.4.12.1.3. konsola centralnego zarządzania musi być zabezpieczona za pośrednictwem protokołu szyfrowanego SSL/TLS.

6.4.12.1.4. Konsola centralnego zarządzania musi być dostępna co najmniej w języku polskim.

- 6.4.12.2. Rozwiązanie musi obejmować ochronę dla co najmniej następujących usług: Microsoft Exchange Online, Microsoft OneDrive, Microsoft Sharepoint, Microsoft Teams, Google Workspace, w tym co najmniej: Gmail, Google Drive.
- 6.4.12.3. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace.
- 6.4.12.4. Rozwiązanie musi umożliwiać:
 - 6.4.12.4.1. Wybór ręczny kont użytkowników, które będą objęte ochroną,
 - 6.4.12.4.2. Wybór automatyczny całego tenantu, gdzie nowo utworzone konta będą automatycznie chronione.
- 6.4.12.5. Rozwiązanie musi posiadać możliwość raportowania w tym co najmniej:
 - 6.4.12.5.1. kont użytkowników, otrzymujących najwięcej spamu,
 - 6.4.12.5.2. kont użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
 - 6.4.12.5.3. kont użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
 - 6.4.12.5.4. kont użytkowników, które mogą być podejrzone.
- 6.4.12.6. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty.
- 6.4.12.7. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.
 - 6.4.12.7.1. Rozwiązanie musi posiadać co najmniej następujące warunki:
 - 6.4.12.7.2. nadawca,
 - 6.4.12.7.3. temacie wiadomości,
 - 6.4.12.7.4. adres IP nadawcy,
 - 6.4.12.7.5. nazwa, rozszerzenie i typ załącznika,
 - 6.4.12.7.6. wiadomości,
 - 6.4.12.7.7. godzina odbioru,
 - 6.4.12.7.8. wynik SPF, DKIM, DMARC i ARC.
- 6.4.12.8. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:
 - 6.4.12.8.1. poddaj wiadomość kwarantannie,

- 6.4.12.8.2.usuń wiadomość,
- 6.4.12.8.3.usuń załącznik,
- 6.4.12.8.4.dodaj prefix tematu,
- 6.4.12.8.5.wyślij powiadomienie e-mail,
- 6.4.12.8.6.skanowanie w poszukiwaniu spamu, wirusów oraz phishing.
- 6.4.12.9. Rozwiązanie musi umożliwiać pobranie plików z kwarantanny co najmniej:
 - 6.4.12.9.1.w formie oryginalnego pliku,
 - 6.4.12.9.2.w formie pliku zabezpieczonego hasłem.
- 6.4.12.10. Rozwiązanie musi umożliwiać przypisanie polityk co najmniej na poziomie:
 - 6.4.12.10.1. całego tenantu,
 - 6.4.12.10.2. grupy,
 - 6.4.12.10.3. grupy Teams,
 - 6.4.12.10.4. lokacji Sharepoint,
 - 6.4.12.10.5. Pojedynczego użytkownika.
- 6.4.12.11. Rozwiązanie musi korzystać z chmury reputacji plików:
 - 6.4.12.11.1. możliwość automatycznego wystania sumy kontrolnej
 - 6.4.12.11.2. możliwość automatycznego wystania fragmentu pliku.
- 6.4.12.12. Rozwiązanie musi umożliwiać określenie czynności realizowanej po wykryciu zagrożenia, w tym co najmniej następujące czynności:
 - 6.4.12.12.1. brak czynności,
 - 6.4.12.12.2. przeniesienie do spamu,
 - 6.4.12.12.3. poddaj wiadomość kwarantannie,
 - 6.4.12.12.4. poddaj załącznik kwarantannie,
 - 6.4.12.12.5. przeniesienie do kosza,
 - 6.4.12.12.6. usuń załącznik,
 - 6.4.12.12.7. zastąp załącznik
 - 6.4.12.12.8. usuń wiadomość.
- 6.4.12.13. Rozwiązanie musi umożliwiać dodanie znacznika do tematu wiadomości zaklasyfikowanej co najmniej jako:
 - 6.4.12.13.1. SPAM,
 - 6.4.12.13.2. phishing.

6.4.12.14. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:

- 6.4.12.14.1. archiwa,
- 6.4.12.14.2. skrypty,
- 6.4.12.14.3. pliki wykonywalne,
- 6.4.12.14.4. pliki rejestru systemowego
- 6.4.12.14.5. możliwy spam,
- 6.4.12.14.6. Dokumenty.

6.4.12.15. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:

- 6.4.12.15.1. natychmiast po ich przeanalizowaniu,
- 6.4.12.15.2. upływie 30 dni,
- 6.4.12.15.3. nigdy.

6.4.12.16. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail.

6.4.12.17. Powiadomienia muszą dotyczyć wykryć co najmniej:

- 6.4.12.17.1. zagrożeń w wiadomościach,
- 6.4.12.17.2. phishing w wiadomościach,
- 6.4.12.17.3. zagrożeń w plikach onedrive,
- 6.4.12.17.4. zagrożeń na dysku Google Drive,

6.4.12.18. Powiadomienia muszą być możliwe do wystania w co najmniej w języku polskim.

6.4.13.Vulnerability Assessment and Patch Management

6.4.13.1. Rozwiązanie musi mieć możliwości wykrywania podatności:

6.4.13.2. w tym co najmniej następujących systemach operacyjnych: Windows, macOS, Linux, w aplikacjach zainstalowanych na zarządzanych stacjach.

6.4.13.3. Rozwiązanie musi posiadać bazę podatności zawierającą co najmniej 35000 CVE.

6.4.13.4. Rozwiązanie musi umożliwiać utworzenie harmonogramu automatycznego wykrywania podatności.

- 6.4.13.5. Rozwiązanie musi umożliwiać wyświetlanie szczegółów danej podatności zawierające co najmniej:
 - 6.4.13.5.1.nazwę aplikacji lub systemu operacyjnego
 - 6.4.13.5.2.punktacje CVSS
 - 6.4.13.5.3.opis wykrytej podatności
 - 6.4.13.5.4.wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.
- 6.4.13.6. Rozwiązanie musi wykrywać podatności w minimum 700 aplikacjach.
- 6.4.13.7. Rozwiązanie musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 300 popularnych aplikacji.
- 6.4.13.8. Rozwiązanie musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji.
- 6.4.13.9. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście.
- 6.4.13.10. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
- 6.4.13.11. Rozwiązanie musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji.
- 6.4.13.12. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich ponad 300 aplikacji, oprócz aplikacji wskazanych na czarnej liście.
- 6.4.13.13. Rozwiązanie musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
- 6.4.13.14. Rozwiązanie musi być zintegrowane bezpośrednio z programem antywirusowym zainstalowanym na zarządzanym komputerze.
- 6.4.13.15. Rozwiązanie musi umożliwiać wyłączenie powiadomień dla wybranej podatności.

6.5. ESET PROTECT Advanced lub równoważne, które spełnia nw. wymagania

6.5.1. Administracja zdalna

- 6.5.1.1. Konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS).

- 6.5.1.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
- 6.5.1.3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
- 6.5.1.4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- 6.5.1.5. Rozwiązanie musi posiadać dedykowaną aplikację, umożliwiającą co najmniej:
 - 6.5.1.5.1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
 - 6.5.1.5.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
 - 6.5.1.5.3. Buforowanie ruchu HTTPS.
- 6.5.1.6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- 6.5.1.7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
- 6.5.1.8. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy co najmniej z następujących aplikacji mobilnych dla systemów iOS oraz Android: Google Authenticator, Microsoft Authenticator, Authy, Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
- 6.5.1.9. Rozwiązanie musi posiadać minimum 80 szablonów raportów.
- 6.5.1.10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- 6.5.1.11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby zostać umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
 - 6.5.1.11.1. adresy sieciowe IP,
 - 6.5.1.11.2. aktywne zagrożenia,
 - 6.5.1.11.3. stan funkcjonowania oraz ochrony,
 - 6.5.1.11.4. wersja systemu operacyjnego,

6.5.1.11.5. podzespoły komputera.

6.5.1.11.6. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:

6.5.1.11.7. codziennie,

6.5.1.11.8. cotygodniowo,

6.5.1.11.9. co miesiąc,

6.5.1.11.10. co rok,

6.5.1.11.11. po wystąpieniu nowego zdarzenia,

6.5.1.11.12. po automatycznym umieszczeniu hosta w grupie dynamicznej.

6.5.1.12. Konsola centralnego zarządzania musi być dostępna co najmniej w języku polskim.

6.5.1.13. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania

6.5.1.14. Rozwiązanie musi mieć możliwość tagowania obiektów.

6.5.1.15. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

6.5.1.16. Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.

6.5.2. Ochrona stacji roboczych - Windows

6.5.2.1. Rozwiązanie musi wspierać systemy operacyjne Windows.

6.5.2.2. Rozwiązanie musi być dostępne co najmniej w języku polskim

6.5.2.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

6.5.2.3.1. wirus,

6.5.2.3.2. trojan,

6.5.2.3.3. robak,

6.5.2.3.4. adware,

6.5.2.3.5. spyware,

6.5.2.3.6. dialer,

6.5.2.3.7. phishing,

6.5.2.3.8. backdoor.

- 6.5.2.4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 6.5.2.5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
- 6.5.2.6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
- 6.5.2.7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
- 6.5.2.8. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.

- 6.5.2.9. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 6.5.2.10. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- 6.5.2.11. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 6.5.2.11.1. całego dysku,
 - 6.5.2.11.2. wybranych katalogów,
 - 6.5.2.11.3. pojedynczych plików,
 - 6.5.2.11.4. plików spakowanych oraz skompresowanych,
 - 6.5.2.11.5. dysków sieciowych,
 - 6.5.2.11.6. dysków przenośnych.
- 6.5.2.12. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 6.5.2.12.1. wybranych plików,
 - 6.5.2.12.2. wybranych procesów,
 - 6.5.2.12.3. wybranych lokalizacji,
 - 6.5.2.12.4. wybranych rozszerzeń,
 - 6.5.2.12.5. nazwy wykrycia,
 - 6.5.2.12.6. sumy kontrolnej (SHA1).
- 6.5.2.13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
 - 6.5.2.13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - 6.5.2.13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.5.2.13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.5.2.14. 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).

- 6.5.2.15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
- 6.5.2.16. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 6.5.2.17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- 6.5.2.17.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
- 6.5.2.17.2. parametry urządzenia: numer seryjny, producent, model.
- 6.5.2.17.3. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
- 6.5.2.17.4. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.5.2.18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- 6.5.2.18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- 6.5.2.18.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- 6.5.2.18.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- 6.5.2.18.4. 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,

6.5.2.18.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

6.5.2.19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

6.5.2.20. 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.

6.5.2.21. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.

6.5.2.22. Raport musi posiadać co najmniej:

6.5.2.22.1. listę zainstalowanych aplikacji,

6.5.2.22.2. listę usług systemowych,

6.5.2.22.3. informacje o systemie operacyjnym i sprzęcie,

6.5.2.22.4. listę aktywnych procesów i połączeń sieciowych,

6.5.2.22.5. harmonogram systemu operacyjnego,

6.5.2.22.6. szczegóły pliku hosts,

6.5.2.22.7. informacje o sterownikach.

6.5.2.23. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:

6.5.2.24. antywirus,

6.5.2.25. zaporę osobistą

6.5.2.26. sandbox,

6.5.2.27. antyspyware,

6.5.2.28. metody heurystyczne.

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

6.5.2.30. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.

- 6.5.2.31. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
- 6.5.2.32. Ochrona musi być realizowana w oparciu o co najmniej:
 - 6.5.2.32.1.globalna czarna lista RBL,
 - 6.5.2.32.2.czarna lista użytkownika,
 - 6.5.2.32.3.biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
- 6.5.2.33. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- 6.5.2.34. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 6.5.2.34.1.Skanowanie portów TCP oraz UDP,
 - 6.5.2.34.2.Wykrywanie duplikacji adresu IP,
 - 6.5.2.34.3.Atak zatrutowania ARP,
 - 6.5.2.34.4.Nieprawidłowa długość pakietu TCP oraz UDP.
- 6.5.2.35. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
- 6.5.2.36. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 6.5.2.37. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.5.2.38. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.
- 6.5.2.39. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.5.2.39.1.tryb automatyczny - rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 6.5.2.39.2.tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - 6.5.2.39.3.tryb oparty na regułach - rozwiązanie blokuje ruch przychodzący i wychodzący,
 - 6.5.2.39.4.tryb uczenia się - rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
 - 6.5.2.39.5. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

- 6.5.2.40. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki.
- 6.5.2.41. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- 6.5.2.42. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- 6.5.2.43. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
- 6.5.2.44. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
- 6.5.2.45. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
- 6.5.2.46. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: treść komunikatu, obraz.

6.5.3. Ochrona stacji roboczych – MacOS

- 6.5.3.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
- 6.5.3.2. Rozwiązanie musi być dostępne co najmniej w języku polskim.
- 6.5.3.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - 6.5.3.3.1. wirus,
 - 6.5.3.3.2. trojan,
 - 6.5.3.3.3. robak,
 - 6.5.3.3.4. adware,
 - 6.5.3.3.5. spyware,
 - 6.5.3.3.6. dialer,
 - 6.5.3.3.7. phishing,
 - 6.5.3.3.8. backdoor.
- 6.5.3.4. 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.

6.5.3.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6.5.3.6. Rozwiązanie musi chronić pliki co najmniej za pomocą:

6.5.3.6.1. Sygnatur wirusów.

6.5.3.6.2. Reputacji chmurowej.

6.5.3.7. Rozwiązanie musi umożliwiać 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).

6.5.3.8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.5.3.8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.

6.5.3.8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.5.3.8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.5.3.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

6.5.3.9.1. całego dysku,

6.5.3.9.2. wybranych katalogów,

6.5.3.9.3. pojedynczych plików,

6.5.3.9.4. plików spakowanych oraz skompresowanych,

6.5.3.9.5. Dysków sieciowych,

6.5.3.9.6. dysków przenośnych.

6.5.3.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

6.5.3.10.1. wybranych plików,

6.5.3.10.2. wybranych procesów,

6.5.3.10.3. wybranych lokalizacji,

6.5.3.10.4. wybranych rozszerzeń,

6.5.3.10.5.nazwy wykrycia,

6.5.3.10.6.sumy kontrolnej (SHA1).

6.5.3.11. Rozwiązanie musi posiadać moduł zapory osobistej.

6.5.3.12. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł..

6.5.3.13. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

6.5.3.13.1.tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

6.5.3.13.2.tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący.

6.5.4. Ochrona stacji roboczych – Linux

6.5.4.1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: Ubuntu Desktop, Red Hat Enterprise Linux, Linux Mint.

6.5.4.2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:

6.5.4.2.1. Cinnamon,

6.5.4.2.2. GNOME,

6.5.4.2.3. KDE,

6.5.4.2.4. MATE,

6.5.4.2.5. XFCE.

6.5.4.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

6.5.4.3.1. wirus,

6.5.4.3.2. trojan,

6.5.4.3.3. robak,

6.5.4.3.4. adware,

6.5.4.3.5. spyware,

6.5.4.3.6. dialer,

6.5.4.3.7. phishing,

6.5.4.3.8. backdoor.

6.5.4.4. 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.

6.5.4.5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6.5.4.6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:

6.5.4.6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.5.4.6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

6.5.4.7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

6.5.4.7.1. całego dysku,

6.5.4.7.2. wybranych katalogów,

6.5.4.7.3. pojedynczych plików,

6.5.4.7.4. plików spakowanych oraz skompresowanych,

6.5.4.7.5. dysków sieciowych,

6.5.4.7.6. dysków przenośnych.

6.5.4.8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

6.5.4.8.1. wybranych plików,

6.5.4.8.2. wybranych procesów,

6.5.4.8.3. wybranych lokalizacji,

6.5.4.8.4. wybranych rozszerzeń,

6.5.4.9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

6.5.4.10. typ urządzenia: pamięci masowe, optyczne pamięci masowe,

6.5.4.11. parametry urządzenia: numer seryjny, producent, model.

6.5.4.12. typ dostępu: brak możliwości zapisu, pełen dostęp, brak dostępu.

6.5.5. Ochrona serwera – Windows Server

- 6.5.5.1. Rozwiązanie musi wspierać systemy w tym co najmniej:
Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016,
Microsoft Windows Server 2019, Microsoft Windows Server 2022,
Microsoft Windows Server 2025.
- 6.5.5.2. Rozwiązanie musi zapewniać ochronę przed wirusami,
trojanami, robakami i innymi zagrożeniami.
- 6.5.5.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń
co najmniej typu:
 - 6.5.5.3.1. wirus,
 - 6.5.5.3.2. trojan,
 - 6.5.5.3.3. robak,
 - 6.5.5.3.4. adware,
 - 6.5.5.3.5. spyware,
 - 6.5.5.3.6. dialer,
 - 6.5.5.3.7. phishing,
 - 6.5.5.3.8. backdoor.
- 6.5.5.4. Rozwiązanie musi zapewniać możliwość skanowania dysków
sieciowych typu NAS.
- 6.5.5.5. 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.
- 6.5.5.6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną
aktualizację silnika detekcji.
- 6.5.5.7. Rozwiązanie musi posiadać możliwość wykluczania ze
skanowania procesów.
- 6.5.5.8. Rozwiązanie musi posiadać system wczesnego ostrzegania
oparty na chmurze, który umożliwia co najmniej:
 - 6.5.5.8.1. sprawdzenie reputacji działających procesów i plików co
najmniej z poziomu interfejsu programu oraz menu
kontekstowego.

- 6.5.5.8.2. konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
- 6.5.5.8.3. konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.5.5.9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

- 6.5.5.9.1. całego dysku,
 - 6.5.5.9.2. wybranych katalogów,
 - 6.5.5.9.3. pojedynczych plików,
 - 6.5.5.9.4. plików spakowanych oraz skompresowanych,
 - 6.5.5.9.5. dysków sieciowych,
 - 6.5.5.9.6. dysków przenośnych.
- 6.5.5.10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
- 6.5.5.10.1. wybranych plików,
 - 6.5.5.10.2. wybranych procesów,
 - 6.5.5.10.3. wybranych lokalizacji,
 - 6.5.5.10.4. wybranych rozszerzeń,
 - 6.5.5.10.5. nazwy wykrycia,
 - 6.5.5.10.6. sumy kontrolnej (SHA1).
- 6.5.5.11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- 6.5.5.12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- 6.5.5.12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - 6.5.5.12.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - 6.5.5.12.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - 6.5.5.12.4. 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,
 - 6.5.5.12.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 6.5.5.13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

- 6.5.5.14. 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.
- 6.5.5.15. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone.
- 6.5.5.16. Raport musi posiadać co najmniej:
- 6.5.5.16.1. listę zainstalowanych aplikacji,
 - 6.5.5.16.2. listę usług systemowych,
 - 6.5.5.16.3. informacje o systemie operacyjnym i sprzęcie,
 - 6.5.5.16.4. listę aktywnych procesów i połączeń sieciowych,
 - 6.5.5.16.5. harmonogram systemu operacyjnego,
 - 6.5.5.16.6. szczegóły pliku hosts,
 - 6.5.5.16.7. informacje o sterownikach.

- 6.5.5.17. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:
- 6.5.5.17.1. antywirus,
 - 6.5.5.17.2. zaporę osobistą
 - 6.5.5.17.3. sandbox,
 - 6.5.5.17.4. antyspyware,
 - 6.5.5.17.5. metody heurystyczne.
- 6.5.5.18. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
- 6.5.5.19. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- 6.5.5.20. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- 6.5.5.20.1. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
- 6.5.5.21. parametry urządzenia: numer seryjny, producent, model.
- 6.5.5.22. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
- 6.5.5.23. System powinien zapewniać możliwość zarządzania blokadami przez administratora, w tym ich zdejmowania.
- 6.5.5.24. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

- 6.5.5.24.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 6.5.5.24.2. Skanowanie portów TCP oraz UDP,
 - 6.5.5.24.3. Wykrywanie duplikacji adresu IP,
 - 6.5.5.24.4. Atak zatrutowania ARP,
 - 6.5.5.24.5. Nieprawidłowa długość pakietu TCP oraz UDP.
 - 6.5.5.24.6. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
- 6.5.5.25. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 6.5.5.26. Rozwiązanie musi posiadać moduł zapory osobistej.
- 6.5.5.27. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł.
- 6.5.5.28. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 6.5.5.28.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 6.5.5.28.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - 6.5.5.28.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - 6.5.5.28.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- 6.5.5.29. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

6.5.6. Ochrona serwera – Linux

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

6.5.6.2. Rozwiązanie musi zapewniać wykrywanie i usuwanie
zagrożeń co najmniej typu:

- 6.5.6.2.1. wirus,
- 6.5.6.2.2. trojan,
- 6.5.6.2.3. robak,
- 6.5.6.2.4. adware,
- 6.5.6.2.5. spyware,
- 6.5.6.2.6. dialer,
- 6.5.6.2.7. phishing,
- 6.5.6.2.8. backdoor.

6.5.6.3. Rozwiązanie musi zapewniać możliwość zdalnego
skanowania przy pomocy protokołu ICAP oraz ICAPS.

6.5.6.4. 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.

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

6.5.6.6. Rozwiązanie musi posiadać możliwość wykluczania ze
skanowania procesów.

- 6.5.6.7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze, który umożliwia co najmniej:
 - 6.5.6.7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.5.6.7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 6.5.6.8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 6.5.6.8.1. całego dysku,
 - 6.5.6.8.2. wybranych katalogów,
 - 6.5.6.8.3. pojedynczych plików,
 - 6.5.6.8.4. plików spakowanych oraz skompresowanych,
 - 6.5.6.8.5. dysków sieciowych,
 - 6.5.6.8.6. dysków przenośnych.
- 6.5.6.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 6.5.6.9.1. wybranych plików,
 - 6.5.6.9.2. wybranych procesów,
 - 6.5.6.9.3. wybranych lokalizacji,
 - 6.5.6.9.4. wybranych rozszerzeń.
- 6.5.6.10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- 6.5.6.11. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- 6.5.6.12. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN.

- 6.5.6.13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
 - 6.5.6.13.1. proces budowania obrazu kontenera,
 - 6.5.6.13.2. wdrażanie obrazu kontenera. Mobile Device Management
- 6.5.6.14. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- 6.5.6.15. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: Android, iOS, iPadOS.
- 6.5.6.16. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - 6.5.6.16.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
 - 6.5.6.16.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - 6.5.6.16.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - 6.5.6.16.4. Apple Business Manager (ABM),
 - 6.5.6.16.5. Android Enterprise (co najmniej w zakresie Device Owner).
- 6.5.6.17. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - 6.5.6.17.1. usunięcie zawartości urządzenia,
 - 6.5.6.17.2. przywrócenie urządzenia do ustawień fabrycznych,
 - 6.5.6.17.3. zablokowanie urządzenia,

6.5.6.17.4.uruchomienie sygnału dźwiękowego,

6.5.6.17.5.lokalizację GPS,

6.5.6.17.6.Resetowanie hasła blokady ekranu.

6.5.6.18. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

6.5.6.19. MDM musi umożliwiać co najmniej:

6.5.6.19.1.Dla systemów iOS oraz iPadOS: konfigurację kont e-mail, konfigurację połączeń VPN, Konfigurację połączeń Wi-Fi, Konfigurację listy certyfikatów, możliwość uruchomienia trybu jednej aplikacji.

6.5.6.20. Dla systemu Android: blokadę wykonywania połączeń, blokadę konfiguracji sieci Wi-Fi, blokadę konfiguracji tuneli VPN, zarządzanie aktualizacjami systemu operacyjnego, blokadę zmiany tapety urządzenia.

6.5.7. Mobile Threat Defense (MTD) dla systemu Android

6.5.7.1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9

6.5.7.2. Inteligentne –skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.

6.5.7.3. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.

6.5.7.4. Aplikacja kliencka powinna być dostępna do pobrania z oficjalnego repozytorium aplikacji przeznaczonego dla systemu Android,

6.5.7.5. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do nowszych.

6.5.7.6. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania.

6.5.7.7. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:

6.5.7.7.1. Złożoność kodu blokady ekranu: Wzór, PIN, hasło, przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu, zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

6.5.7.8. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

6.5.7.8.1. nazwę aplikacji,

6.5.7.8.2. nazwę pakietu,

6.5.7.8.3. kategorię sklepu Google Play,

6.5.7.8.4. uprawnienia aplikacji,

6.5.7.8.5. pochodzenie aplikacji z nieznanego źródła.

6.5.7.9. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

6.5.8. Sandbox w chmurze

6.5.8.1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.

6.5.8.2. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows 10 oraz 11, Microsoft Windows Server, macOS 11 (Big Sur) oraz nowszych RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.

- 6.5.8.3. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 6.5.8.4. Rozwiązanie musi wykorzystywać do działania chmurę.
- 6.5.8.5. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
 - 6.5.8.5.1. archiwa,
 - 6.5.8.5.2. skrypty,
 - 6.5.8.5.3. pliki wykonywalne,
 - 6.5.8.5.4. pliki rejestru systemowego
 - 6.5.8.5.5. możliwy spam,
 - 6.5.8.5.6. dokumenty.
- 6.5.8.6. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
 - 6.5.8.6.1. natychmiast po ich przeanalizowaniu,
 - 6.5.8.6.2. po upływie 30 dni,
 - 6.5.8.6.3. nigdy.
- 6.5.8.7. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- 6.5.8.8. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- 6.5.8.9. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
- 6.5.8.10. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

- 6.5.8.11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
- 6.5.8.12. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
Przeanalizowane pliki muszą zostać odpowiednio oznaczone.
Analiza pliku musi zakończyć się jednym z poniższych wyników:
- 6.5.8.12.1. czysty,
 - 6.5.8.12.2. podejrzany,
 - 6.5.8.12.3. bardzo podejrzany,
 - 6.5.8.12.4. szkodliwy.
- 6.5.8.13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
- 6.5.8.13.1. wstrzymania uruchamiania pobieranych plików z następujących źródeł:
 - 6.5.8.13.2. przeglądarki internetowej,
 - 6.5.8.13.3. programy poczty e-mail,
 - 6.5.8.13.4. nośniki wymienne,
 - 6.5.8.13.5. pliki wyodrębnione z archiwum.
- 6.5.8.14. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

6.5.9. Szyfrowanie

- 6.5.9.1. Rozwiązanie musi wspierać systemy operacyjne Windows.

- 6.5.9.2. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
- 6.5.9.3. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
- 6.5.9.4. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
- 6.5.9.5. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
- 6.5.9.6. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
 - 6.5.9.6.1. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
 - 6.5.9.6.2. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
- 6.5.9.7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
- 6.5.9.8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
- 6.5.9.9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
- 6.5.9.10. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

OPROGRAMOWANIE RÓWNOWAŻNE WYMAGANIA:

1. W przypadku zaoferowania oprogramowania równoważnego względem wyspecyfikowanego przez Centralny Ośrodek Informatyki w SWZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że zaoferowane produkty spełniają wszystkie wymagania i warunki określone w SWZ, w szczególności w zakresie:
 - a. warunków licencji / sublicencji / subskrypcji zaoferowanych produktów równoważnych w każdym aspekcie, które nie mogą być gorsze niż dla produktów wymienionych w SWZ;
 - b. funkcjonalności zaoferowanych produktów równoważnych, które nie mogą być ograniczone i gorsze względem funkcjonalności produktów wymienionych w SWZ;
 - c. zakresu kompatybilności i współdziałania zaoferowanych produktów równoważnych ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego, który nie może być gorszy niż dla produktów wymienionych w SWZ;
 - d. poziomu zakłóceń pracy środowiska systemowo-programowego Zamawiającego spowodowanego wykorzystaniem zaoferowanych produktów równoważnych, który nie może być większy niż w przypadku produktów wymienionych w SWZ;
 - e. poziomu współpracy zaoferowanych produktów równoważnych z systemami Jednostek, który nie może być gorszy od tego jaki zapewniają produkty wymienione w SWZ;
 - f. zapewnienia pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności zaoferowanych produktów równoważnych z produktami wymienionymi w SWZ;
 - g. warunków i zakresu usług gwarancji, asysty technicznej i konserwacji zaoferowanych produktów równoważnych, które nie mogą być gorsze niż dla produktów wymienionych w SWZ;

- h. sposobu zarządzania i odnawiania licencji / sublicencji / subskrypcji poprzez dedykowane przez producenta programy licencyjne;
 - i. obsługi przez zaoferowane produkty równoważne języków interfejsu, w ilości i rodzaju nie mniejszych niż oferują produkty wymienione w SWZ;
 - j. wymagań sprzętowych dla zaoferowanych produktów równoważnych, które nie mogą być wyższe niż dla produktów wymienionych w SWZ;
 - k. dostępności wersji bitowych (32, 64) zaoferowanych produktów równoważnych, która nie może być mniejsza niż dla produktów wymienionych w SWZ;
 - l. dostępności wersji na różne systemy operacyjne zaoferowanych produktów równoważnych, która nie może być mniejsza niż dla produktów wymienionych w SWZ.
2. uwagi na złożoność postępowania, w tym obszerny katalog oprogramowania, Zamawiający zastrzega, że badanie równoważności oprogramowania nie jest ograniczone wyłącznie do badania zgodności funkcjonalnej określonej w OPZ, a także do realnej, przekrojowej analizy wszystkich funkcji oprogramowania (poprzez analizę chociażby zmieniającej się specyfikacji technicznej producenta). W przypadku, gdy oprogramowanie będzie zgodne z zapisami OPZ, ale wystąpi jego niezgodność w innym zakresie Centralny Ośrodek Informatyki będzie uprawniony do wezwania Wykonawcy w tym zakresie do wyjaśnień. Potwierdzenie wątpliwości, co do zgodności oprogramowania będzie uprawniać Centralny Ośrodek Informatyki do nieuznania oprogramowania za równoważne. W tym wypadku Centralny Ośrodek Informatyki uzasadni swoją decyzję szczegółowo, wskazując jakie funkcje powinno spełniać oprogramowanie, a ich nie spełnia.

3. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty.
4. W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Jednostek lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Jednostek, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Jednostek oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Jednostek również po usunięciu produktu równoważnego.
5. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.
6. W przypadku, gdy wdrożenie oprogramowania równoważnego wymaga migracji danych, Wykonawca przeprowadzi migrację danych na własny koszt.
7. Za produkt równoważny uznany może zostać ten sam produkt jednego producenta zaoferowany w różnych programach licencyjnych, o ile różnica w programach może wpłynąć na wdrożenie produktu, zarządzanie nim, cenę jego późniejszego odnowienia, czy samą ilość opcji odnowienia.
8. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego

producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

Warszawa, dnia 29 grudnia 2025 r.

Strona WWW**WYJAŚNIENIA I ZMIANY SWZ NR 1****Dotyczy postępowania: „Umowa ramowa na dostawę oprogramowania antywirusowego - COI-ZAK.262.71.2025”**

Zamawiający, działając na podstawie art. 135 ust. 2, art. 137 ust. 1 oraz art. 137 ust. 4 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz.U. z 2024 r., poz. 1320 z późn. zm.) – dalej: ustawa Pzp, przedstawia poniżej treść wyjaśnień oraz zmianę SWZ:

Pytanie nr 1:

W SWZ (pkt.7.1.1) Zamawiający wskazał, że wymagania odnośnie zdolności technicznej będą spełnione jeżeli Wykonawca wykaże, że „wykonał należycie, co najmniej 2 (słownie: dwie) dostawy Oprogramowania antywirusowego o wartości co najmniej 500 000,00 zł brutto każda. Przez jedną dostawę Centralny Ośrodek Informatyki rozumie dostawę zrealizowaną w ramach jednej umowy.” Warunek udziału stawiany w SWZ nie może być bardziej restrykcyjny niż jest to konieczne dla oceny zdolności wykonawcy do należytego wykonania przyszłej umowy (wyrok KIO z dnia 3 grudnia 2018 r. sygn. KIO 2381/18). Warunek musi być też „proporcjonalny do przedmiotu zamówienia oraz umożliwiający ocenę zdolności wykonawcy do należytego wykonania zamówienia” (art. 22 ust. 1a ustawy PZP). Zamawiający stawiając swoje wymagania, nie może dyskryminować wykonawców, a zatem eliminować z postępowania wykonawców, którzy są w stanie wykonać należycie zamówienie. Przedmiotem postępowania jest umowa ramowa, w ramach której udzielanych będzie wiele zamówień wykonawczych. Zgodnie z formularzem ofertowym, najdroższą pozycją w formularzu jest Eset Protect Elite 250+ stanowisk na 36 miesięcy. Zgodnie z cennikiem ESET, wartość Eset Protect Elite 250 stanowisk na 36 miesięcy wynosi 178896,43 zł brutto, a zatem znacznie mniej, niż wynosi wymagane przez Zamawiającego doświadczenie w pojedynczej dostawie oprogramowania antywirusowego. Większość pozostałych pozycji w formularzu oferty jest znacznie tańsza. Tym samym wymóg należytego wykonania dwóch dostaw o wartości

co najmniej 500 000 zł brutto każda jest niewspółmierny do przedmiotu zamówienia i w sposób sztuczny ogranicza konkurencję w tym postępowaniu. W związku z powyższym wnoszę o zmianę zapisów SWZ na: „7. Warunki udziału w postępowaniu 7.1. O udzielenie zamówienia publicznego może ubiegać się Wykonawca, który spełnia warunek udziału w postępowaniu dotyczący zdolności technicznej lub zawodowej, tj.: 7.1.1. w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie, co najmniej 2 (słownie: dwie) dostawy Oprogramowania antywirusowego o wartości co najmniej 175 000,00 zł brutto każda.”

ODPOWIEDŹ:

Zamawiający, zmienia brzmienie pkt 7.1.1 Rozdziału I SWZ:

7. Warunki udziału w postępowaniu

7.1. O udzielenie zamówienia publicznego może ubiegać się Wykonawca, który spełnia warunek udziału w postępowaniu dotyczący zdolności technicznej lub zawodowej, tj.:

7.1.1. w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie co najmniej 2 (słownie: dwie) dostawy oprogramowania antywirusowego o wartości co najmniej 150 000,00 zł brutto każda, przy czym przez jedną dostawę Zamawiający rozumie dostawę zrealizowaną w ramach jednej umowy.”

Zmianie w powyższym zakresie ulega również ogłoszenie o zamówieniu, które to stanowić będzie Załącznik nr 1 do niniejszych Wyjaśnień i Zmian SWZ nr 1

Pytanie nr 2:

Proszę o potwierdzenie, że w Tabeli Cenowej (ROZDZIAŁ IV – FORMULARZ OFERTY WRAZ Z ZAŁĄCZNIKAMI), należy podać ceny jednostkowe (za stanowisko).

ODPOWIEDŹ:

Zamawiający potwierdza, że w Tabeli Cenowej (ROZDZIAŁ IV – Formularz Oferty wraz z załącznikami) należy podać ceny jednostkowe, tj. cenę za jedno stanowisko.

Pytanie nr 3:

Zgodnie z polityką i cennikiem producenta, minimalne zamówienie dla większości produktów ESET Protect to 5 szt, a w przypadku najwyższych pakietów Enterprise i Elite to 26 szt. Wnoszę o modyfikację Tabeli Cenowej, tak aby była zgodna z polityką producenta.

ODPOWIEDŹ:

Zamawiający zmienia brzmienie Rozdziału IV SWZ w powyższym zakresie.

Zmieniony Formularz Oferty stanowić będzie Załącznik nr 2 do niniejszych Wyjaśnień i Zmian SWZ nr 1

Pytanie nr 4:

Zwracamy się z uprzejmą prośbą o rozważenie uzupełnienia kryteriów oceny ofert o dodatkowe punkty za posiadanie przez Wykonawcę certyfikatów ISO 27001 oraz ISO 9001.

Uzasadnienie:

Certyfikat ISO 27001 potwierdza wdrożenie systemu zarządzania bezpieczeństwem informacji i stanowi obiektywny dowód, że Wykonawca realizuje usługi z najwyższymi standardami ochrony danych, co w przypadku dostaw oprogramowania antywirusowego ma szczególne znaczenie.

Certyfikat ISO 9001 potwierdza wysoką jakość procesów zarządzania organizacją oraz obsługą klienta, co przekłada się na stabilną i przewidywaną realizację zamówienia oraz wsparcie powdrożeniowe.

Uwzględnienie wskazanych certyfikatów w kryteriach oceny ofert nie ogranicza konkurencji – są to standardy powszechnie stosowane w IT – natomiast może przyczynić się do wyboru Wykonawcy gwarantującego wysoki poziom bezpieczeństwa oraz jakości realizacji zamówienia.

ODPOWIEDŹ:

Zamawiający pozostawia brzmienie SWZ w zakresie kryteriów oceny ofert bez zmian.

Pytanie nr 5:

W pkt 7.1.1. SWZ Zamawiający wymaga wykazania co najmniej dwóch dostaw oprogramowania antywirusowego o wartości minimum 500 000,00 zł brutto każda. Mając

na uwadze charakter przedmiotu zamówienia, czyli sprzedaż mniejszych paczek rozwiązań Antywirusowych w podanych przedziałach, zwracamy się z uprzejmą prośbą o obniżenie wymaganej wartości pojedynczej dostawy z 500 000,00 zł brutto do 400 000,00 zł brutto.

Uzasadnienie:

Aktualny warunek może ograniczyć konkurencję, ponieważ zamawiający będzie realizował zamówienia w dużo mniejszych paczkach, które nie przekroczą 500 000 PLN brutto.

Obniżenie progu 400 000 zł brutto nadal zapewni wybór wykonawców posiadających niezbędne doświadczenie, a jednocześnie zwiększy konkurencyjność postępowania, co jest zgodne z zasadą uczciwej konkurencji wyrażoną w PZP.

ODPOWIEDŹ:

Zamawiający, zmienia brzmienie pkt 7.1.1 Rozdziału I SWZ:

7. Warunki udziału w postępowaniu

7.1. O udzielenie zamówienia publicznego może ubiegać się Wykonawca, który spełnia warunek udziału w postępowaniu dotyczący zdolności technicznej lub zawodowej, tj.:

7.1.1. w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie co najmniej 2 (słownie: dwie) dostawy oprogramowania antywirusowego o wartości co najmniej 150 000,00 zł brutto każda, przy czym przez jedną dostawę Zamawiający rozumie dostawę zrealizowaną w ramach jednej umowy.”

Pytanie nr 6:

W związku ze zmianą cennika przez producenta oprogramowania firmę ESET w dniu 01-02-2026, zwracamy się z prośbą o przesunięcie terminu składania ofert na minimum dzień 02-02-2026, co pozwoliłoby wykonawcom uzupełnienie cen w formularzu ofertowym wynikających z nowego cennika, wg którego w ramach umowy ramowej dostarczane byłyby pakiety firmy ESET.

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na przesunięcie terminu składania ofert zgodnie z

wnioskiem Wykonawcy.

Według najlepszej wiedzy Zamawiającego, Wykonawcy będący dostawcami oprogramowania ESET posiadają dostęp do odpowiednich narzędzi kalkulacyjnych (kalkulatorów wycen), umożliwiających przygotowanie oferty w oparciu o nowy cennik producenta, obowiązujący od dnia 1 lutego 2026 r. W związku z powyższym Zamawiający oczekuje, że ceny wskazane w formularzu ofertowym będą uwzględniały nowy cennik producenta, gdyż zamówienia wykonawcze będą realizowane po 1.02.2026 r.

Pytanie nr 7:

W formularzu oferty należy wpisać ceny jednostkowe poszczególnych pakietów oferowanych przez producenta firmę ESET w odpowiednich przedziałach jak również okresach ważności licencji (1 rok, 2 lata lub 3 lata). W związku z tym mamy pytania w kwestii zmiany cen przez producenta, które planowane są na dzień 1 lutego 2026, czyli po terminie składania ofert. Czy zamawiający dopuszcza możliwość złożenia ceny powyżej deklarowanej w formularzu ofertowym do tego postępowania podczas konkursu ofert, do którego będą mogli przystąpić wykonawcy wybrani w tym postępowaniu?

ODPOWIEDŹ:

Zamawiający wyjaśnia, że ceny jednostkowe wskazane w formularzu ofertowym w niniejszym postępowaniu i przeniesione do umowy ramowej stanowią maksymalne ceny, jakie mogą zostać zaoferowane w postępowaniach wykonawczych prowadzonych na podstawie umowy ramowej.

W związku z powyższym złożenie w postępowaniu wykonawczym oferty zawierającej ceny wyższe niż określone w umowie ramowej będzie skutkowało odrzuceniem takiej oferty w postępowaniu wykonawczym jako niezgodnej z postanowieniami umowy ramowej.

Pytanie nr 8:

W formularzu oferty należy wpisać ceny jednostkowe poszczególnych pakietów

oferowanych przez producenta firmę ESET w odpowiednich przedziałach jak również okresach ważności licencji (1 rok, 2 lata lub 3 lata). W związku z tym mamy pytania w kwestii zmiany cen przez producenta, które planowane są na dzień 1 lutego 2026, czyli po terminie składania ofert.

Czy złożenie w konkursie ofert, do którego będą mogli przystąpić wykonawcy wybrani w tym postępowaniu oferty z ceną powyżej deklarowanej w formularzu ofertowym nie poniesiemy, żadnych konsekwencji związanych z umową ramową (wykluczenie z jej postanowień).

ODPOWIEDŹ:

Zamawiający udzielił odpowiedzi już w tym zakresie w pytaniu nr 7.

Pytanie 9:

W pkt 7.1.1. SWZ Zamawiający wymaga wykazania co najmniej dwóch dostaw oprogramowania antywirusowego o wartości minimum 500 000,00 zł brutto każda. Mając na uwadze charakter przedmiotu zamówienia oraz obecną praktykę rynkową w zakresie dystrybucji oprogramowania ESET i innych rozwiązań antywirusowych, zwracamy się z uprzejmą prośbą o obniżenie wymaganej wartości pojedynczej dostawy z 500 000,00 zł brutto do 400 000,00 zł brutto. Uzasadnienie: Aktualny warunek może niepotrzebnie ograniczać konkurencję, ponieważ duże dostawy oprogramowania antywirusowego coraz częściej realizowane są indywidualnymi warunkami – w zależności od faktycznych potrzeb klientów. W praktyce rynkowej rzadziej obserwuje się pojedyncze zamówienia przekraczające wartość 500 000 zł brutto, natomiast dostawy o wartości około 400 000 zł brutto są powszechne i w pełni porównywalne pod względem zakresu, złożoności oraz wymagań realizacyjnych. Obniżenie progu do 400 000 zł brutto nadal zapewni wybór wykonawców posiadających niezbędne doświadczenie, a jednocześnie zwiększy konkurencyjność postępowania, co jest zgodne z zasadą uczciwej konkurencji wyrażoną w Pzp. Pytanie II: W pkt 7.1.1. SWZ Zamawiający wymaga wykazania co najmniej dwóch dostaw oprogramowania antywirusowego o wartości minimum 500 000,00 zł brutto każda. Mając na uwadze charakter przedmiotu zamówienia oraz obecną praktykę rynkową w zakresie dystrybucji oprogramowania ESET i innych rozwiązań

antywirusowych, zwracamy się z uprzejmą prośbą o zamienne kryterium dostawy w postaci dwóch dostaw przynajmniej 10 000 licencji każda. Uzasadnienie: Aktualny warunek może niepotrzebnie ograniczać konkurencję, ponieważ duże dostawy oprogramowania antywirusowego coraz częściej realizowane są indywidualnymi warunkami. Dodanie zamiennie kryterium dostawy w postaci dwóch dostaw przynajmniej 10 000lic każda nadal zapewni wybór wykonawców posiadających niezbędne doświadczenie, a jednocześnie zwiększy konkurencyjność postępowania, co jest zgodne z zasadą uczciwej konkurencji wyrażoną w Pzp.

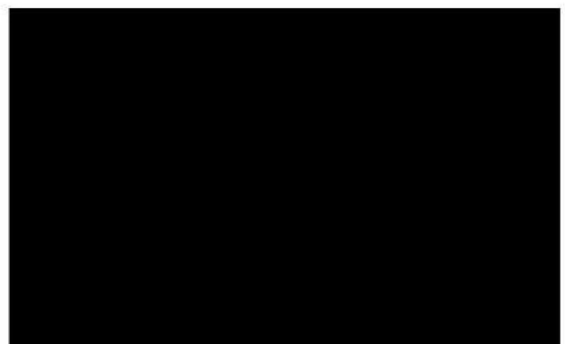
ODPOWIEDŹ:

Zamawiający zmienił treść warunku udziału zgodnie z odpowiedzią na pytanie nr 1.

Zamawiający zmienia treść nw. Rozdziałów SWZ, przekazując w załączeniu załączniki zawierające tekst jednolity:

1. *Ogłoszenie o zmianie ogłoszenia o zamówieniu nr 1.*
2. *Rozdział_IV_SWZ_FO-COI-ZAK.262.71.2025_po_zmianach_nr_1*
3. *Rozdział_I_SWZ_COI-ZAK.262.71.2025_zmiana_nr1*

Niniejsze zmiany treści SWZ stanowią integralną część SWZ i powinny być uwzględnione przez Wykonawców przy składaniu ofert w postępowaniu.



Warszawa, dnia 29.12.2025 r.

Strona WWW**WYJAŚNIENIA SWZ NR 2****Dotyczy postępowania: „Umowa ramowa na dostawę oprogramowania antywirusowego - COI-ZAK.262.71.2025”**

Zamawiający, działając na podstawie art. 135 ust. 2 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz.U. z 2024 r., poz. 1320 z późn. zm.) – dalej: ustawa Pzp, przedstawia poniżej treść wyjaśnień:

Pytanie nr 10

Pytanie dotyczy kryteriów oceny oferty dla ESET PROTECT Enterprise oraz ESET PROTECT Elite w których oceniana ma być średnia arytmetyczna cen jednostkowych pakietów (1-10, 11-25, 26-49, 50 -99, 100 - 249, 250+) czy zamawiający zgodzi się by w przypadku ESET PROTECT Enterprise oraz ESET PROTECT Elite oceniana była średnia arytmetyczna cen jednostkowych pakietów (26-49, 50 -99, 100 - 249, 250+)

Uzasadnienie:

Pakiety ESET PROTECT Enterprise oraz ESET PROTECT Elite są sprzedawane w minimalnej ilości wynoszącej 26 licencji, co nie pozwala wyliczyć ceny dla pakietów od 1-10 oraz 11-25.

ODPOWIEDŹ: Zamawiający odsyła do odpowiedzi na pytanie numer 3 i modyfikacji treści SWZ opublikowanej w piśmie „Wyjaśnienia i zmiany SWZ nr 1” z dnia 29.12.2025

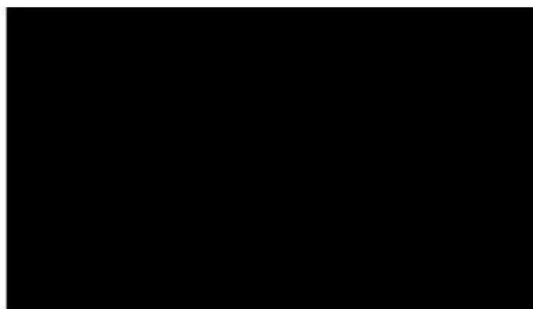
Pytanie nr 11

Pytanie dotyczy kryteriów oceny oferty dla ESET PROTECT Entry, ESET PROTECT Advanced oraz ESET PROTECT Complete w których oceniana ma być średnia arytmetyczna cen jednostkowych pakietów (1-10, 11-25, 26-49, 50 -99, 100 - 249, 250+) czy zamawiający zgodzi się by w przypadku ESET PROTECT Enterprise oraz ESET PROTECT Elite oceniana była średnia arytmetyczna cen jednostkowych pakietów (5-10, 11-25, 26-49, 50 -99, 100 - 249, 250+)

Uzasadnienie:

Pakiety ESET PROTECT Entry, ESET PROTECT Advanced oraz ESET PROTECT Complete są sprzedawane w minimalnej ilości wynoszącej 5 licencji.

ODPOWIEDŹ: Zamawiający odsyła do odpowiedzi na pytanie numer 3 oraz modyfikacji treści SWZ opublikowanej w piśmie „Wyjaśnienia i zmiany SWZ nr 1” z dnia 29.12.2025



Załącznik nr 3 do Umowy Ramowej nr COI/U/PZP/262/13/2026 (COI-ZAK.262.71.2025)

UMOWA WYKONAWCZA NR

na dostawę chmurowego oprogramowania antywirusowego

zawarta w _____ dniu złożenia podpisu przez ostatnią ze Stron, zwana dalej „**Umową Wykonawczą**”, pomiędzy:

..... z siedzibą w, przy ul.wpisanym/ą do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd, Wydział Gospodarczy pod numerem KRS, NIP, REGON, zwanym/ą dalej „**Zamawiającym**”, reprezentowanym/ą przez:

a

..... z siedzibą w, przy ul.wpisanym/ą do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd, Wydział Gospodarczy pod numerem KRS, NIP, REGON, zwanym/ą dalej „**Wykonawcą**”, reprezentowanym/ą przez:

§ 1

DEFINICJE

Lp.	Termin	Definicja
1.	Dni Robocze	Dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.
2.	Oferta Wykonawcza	Oferta złożona przez Wykonawcę w wyniku Zaprośzenia do składania ofert, stanowiąca Załącznik nr 1 do Umowy Wykonawczej.

3.	Oprogramowanie	Oprogramowanie określone w OPZ
4.	OPZ	Opis przedmiotu zamówienia, stanowiący Załącznik nr 2 do Umowy Ramowej wraz z wyjaśnieniami SWZ opublikowanymi na stronie internetowej prowadzonego Postępowania.
5.	Platforma	Elektroniczna platforma zakupowa dostępna za pośrednictwem strony internetowej wskazanej przez COI
6.	Postępowanie wykonawcze	postępowanie o zawarcie umowy wykonawczej, prowadzone na podstawie umowy ramowej w wyniku którego zawarta została niniejsza umowa wykonawcza
7.	Protokół Odbioru	Protokół potwierdzający wykonanie Umowy Wykonawczej w zakresie dostawy Oprogramowaniu. Wzór Protokołu Odbioru Dostawy stanowi Załącznik nr 3 do Umowy Wykonawczej.
8.	Umowa Ramowa	Umowa ramowa nr..... zawarta..... 202... r. pomiędzy Centralnym Ośrodkiem Informatyki a Wykonawcą / Wykonawcami.
9.	Umowa Wykonawcza	Niniejsza Umowa wraz z załącznikami.
10	Zaproszenie	Zaproszenie do udziału w postępowaniu wykonawczym, kierowane do wszystkich wykonawców (za pośrednictwem Platformy wszczynające postępowanie wykonawcze).

§ 2**PRZEDMIOT UMOWY WYKONAWCZEJ**

1. Przedmiotem Umowy wykonawczej jest dostawa Oprogramowania wraz ze wsparciem, o którym mowa w pkt 5.1.9 OPZ, w zakresie określonym w Zaproszeniu. Szczegółowy opis przedmiotu zamówienia oraz sposób i warunki jego realizacji określa OPZ oraz Oferta Wykonawcza.
2. Bez uszczerbku dla stosowania słowniczka Umowy Wykonawczej na gruncie tejże umowy do realizacji Umowy Wykonawczej stosuje się postanowienia Umowy Ramowej.
3. Wykonawca oświadcza, że posiada prawo do udzielenia lub zapewnienia udzielenia na rzecz Zamawiającego licencji na Oprogramowanie, zgodnie z Umową Ramową i Wykonawczą.
4. W przypadku, gdy zaoferowane przez Wykonawcę Oprogramowanie nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po odinstalowaniu Oprogramowania.
5. Wykonawca zapewni świadczenia sposób zapewniający Zamawiającemu korzystanie z oprogramowania w sposób zgodny z obowiązującymi go wymogami prawnymi wynikającymi z powszechnie obowiązującego prawa publicznego, w tym z wymogami zawartymi w rozporządzeniu wydanym na podstawie delegacji zawartej w art.18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne zgodnie z jego każdorazowym brzmieniem.
6. Za dzień dostarczenia przedmiotu Umowy Wykonawczej uznaje się dzień przestania przez Wykonawcę do Zamawiającego informacji e-mail, zawierającej jako załącznik zrzut ekranu z potwierdzeniem zrealizowania zamówienia wykonawczego - zgodnie z danymi teleadresowymi, wskazanymi w § 3, przedmiotowa informacja umożliwi elektroniczne podpisanie Protokołu Odbioru.

7. W wypadku, gdy Zamawiający poweźmie wątpliwość co do należytego wykonywania przez Wykonawcę Umowy Wykonawczej, może wezwać Wykonawcę do udzielenia wyjaśnień lub do usunięcia uchybień, wyznaczając stosowny termin.

§ 3

NADZÓR NAD UMOWĄ WYKONAWCZĄ

1. Osoby sprawujące nadzór nad realizacją umowy wykonawczej:
 - 1) ze strony Zamawiającego:, e-mail:, tel.
 - 2) ze strony Wykonawcy....., e-mail:, tel.
2. Dopuszczalna jest możliwość zmiany danych wskazanych w ust. 1 bez aneksowania umowy wykonawczej. Zmiana taka, aby była skuteczna, wymaga jedynie zawiadomienia przez stronę drugiej strony umowy wykonawczej. Zawiadomienie ma formę jednostronnego pisemnego oświadczenia o zmianie danych dotyczących osoby nadzorującej umowę wykonawczą. Oświadczenie może być przesłane kanałami komunikacji elektronicznej.

§ 4

WYNAGRODZENIE

1. Wykonawca z tytułu należytego wykonania przedmiotu umowy wykonawczej otrzyma łączne wynagrodzenie stanowiące zapłatę ceny w kwocie _____ zł netto, tj. w łączna kwota _____ zł brutto.
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty jakie powstaną w związku z wykonaniem Umowy wykonawczej. Wykonawcy nie przysługuje zwrot od Zamawiającego jakichkolwiek dodatkowych kosztów, opłat i podatków poniesionych przez Wykonawcę w związku z realizacją przedmiotu Umowy wykonawczej.
3. Wynagrodzenie zostanie wypłacone przelewem na rachunek bankowy, na podstawie prawidłowo wystawionej faktury, na której zostanie wyszczególniony

- numer rachunku bankowego Wykonawcy, w terminie do 30 dni od daty jej dostarczenia Zamawiającemu.
4. Fakturę należy doręczyć na adres siedziby Zamawiającego lub przestać w formie elektronicznej z adresu e-mailowego Wykonawcy: _____ na adres e-mailowy Zamawiającego: _____ lub za pomocą platformy, o której mowa w ustawie z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym. Zmiana adresu e-mail, o którym mowa w zdaniu pierwszym, następuje poprzez powiadomienie drugiej strony poprzez przesłanie odpowiedniej informacji na adres e-mail Wykonawcy lub Zamawiającego i nie stanowi zmiany Umowy wykonawczej.
 5. W przypadku dostarczenia przez Wykonawcę faktury w formie elektronicznej inaczej niż wskazano w ust. 4 adresu e-mail, bez uprzedniego powiadomienia Zamawiającego, taką fakturę uznaje się za nieskutecznie dostarczoną.
 6. Wykonawca nie może wpisać do wystawionych zgodnie z Umową faktur innego terminu płatności niż określony w ust. 3.
 7. Zamawiający jest płatnikiem faktur wystawionych przez Wykonawcę.
 8. Za datę zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.
 9. Podstawą do wystawienia faktury jest podpisanie bez zastrzeżeń Protokołu Odbioru.
 10. W przypadku faktury wystawionej niezgodnie z obowiązującymi przepisami lub postanowieniami Umowy wykonawczej lub negatywnie zweryfikowanym rachunkiem bankowym w wykazie podmiotów, o którym mowa w art. 96b ustawy o podatku od towarów i usług, zapłata wynagrodzenia nastąpi dopiero po otrzymaniu przez Zamawiającego prawidłowo wystawionej faktury korygującej lub podpisanej przez Wykonawcę noty korygującej. Z tego tytułu Wykonawcy nie przysługują roszczenia z tytułu niedotrzymania terminu płatności, o których mowa w ust. 11.
 11. Za niedotrzymanie terminu płatności faktury Wykonawca może naliczyć ustawowe odsetki za opóźnienie.
 12. Wykonawca oświadcza, że rachunek, który będzie wskazany na fakturze został otwarty w związku z prowadzoną przez Wykonawcę działalnością gospodarczą,

zgłoszony i ujawniony w wykazie prowadzonym przez Szefa Krajowej Administracji Skarbowej (tzw. „biała lista”) na podstawie art. 96b ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług. W przypadku, gdy wskazany rachunek bankowy nie będzie znajdował się w ww. wykazie, Zamawiający uprawniony będzie do dokonania zapłaty na inny rachunek bankowy Wykonawcy wskazany w ww. wykazie.

13. Cesja wierzytelności wynikająca z realizacji Umowy wykonawczej, jak też dokonanie jakiejkolwiek innej czynności prawnej skutkującej zmianą wierzyciela wymaga pisemnej zgody Zamawiającego. Dokonanie cesji bez zgody Zamawiającego stanowić będzie istotne naruszenie Umowy wykonawczej i może skutkować odstąpieniem Zamawiającego od Umowy wykonawczej.
14. W przypadkach określonych w przepisach prawa powszechnie obowiązującego Zamawiający dokona płatności z zastosowaniem mechanizmu podzielonej płatności („split payment”). Celem uniknięcia wątpliwości strony potwierdzają, że w przypadkach kiedy przepisy prawa powszechnie obowiązującego nie przewidują obowiązku zastosowania mechanizmu podzielonej płatności, Zamawiający jest uprawniony do skorzystania z jego zastosowania.

§ 5

KARY UMOWNE

1. Zamawiający naliczy kary umowne w następujących przypadkach:
 - 1) za zwłokę w realizacji dostawy, w terminie określonym § 3 ust. 4 Umowy Ramowej - w wysokości 0,5% wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy Wykonawczej, za każdy rozpoczęty dzień zwłoki, nie mniej niż 50 zł za każdy dzień;
 - 2) za odstąpienie od Umowy Wykonawczej z winy wykonawcy - w wysokości 20% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 Umowy Wykonawczej, w przypadku odstąpienia od tej umowy wykonawczej w części, podstawą naliczania kary umownej jest wartość Umowy Wykonawczej w części objętej odstąpieniem;

- 3) w przypadku niedotrzymania poziomu oferowanej dostępności miesięcznej oferowanego Oprogramowania - w wysokości 0,2% wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy Wykonawczej za każdy przypadek;
 - 4) w przypadku niespełnienia przez Wykonawcę wskaźnika SCCO 2 , o którym mowa w dokumentacji postępowania, w sytuacji gdy jego spełnienie zostało zadeklarowane w Ofercie, Zamawiający ma prawo naliczyć Wykonawcy karę umowną w wysokości 5% maksymalnego wynagrodzenia, o którym mowa w § 4 ust. 1 Umowy. Kara umowna zostanie naliczona każdorazowo po stwierdzeniu niespełnienia wskaźnika SCCO 2 w okresie obowiązywania Umowy.
 - 5) w przypadku naruszenia klauzuli poufności, o której mowa w § 7 - w kwocie 3 000,00 zł za każdy przypadek naruszenia;
2. Łączna suma kar umownych nie może przekroczyć 30% wartości wynagrodzenia brutto określonego w § 3 ust. 1 Umowy Wykonawczej.
 3. Kary umowne, o których mowa w ust. 1, są wymagalne do zapłaty przez Wykonawcę w terminie 7 dni od dnia doręczenia oświadczenia - noty obciążeniowej wystawionej przez Zamawiającego. Zamawiający może potrącić naliczone kary umowne z przysługującego Wykonawcy wynagrodzenia, bez odrębnego oświadczenia, na co Wykonawca wyraża zgodę.
 4. Zapłata kar umownych wynikających ze zwłoki w realizacji Umowy wykonawczej, nie zwalnia Wykonawcy od wykonywania przedmiotu Umowy wykonawczej zgodnie z warunkami określonymi w niniejszej Umowie wykonawczej.
 5. Jeżeli kara umowna nie pokrywa poniesionej szkody, Zamawiający może dochodzić odszkodowania uzupełniającego do wysokości rzeczywiście poniesionej straty i utraconych korzyści na zasadach ogólnych określonych w Kodeksie cywilnym.

§ 6

ODSTĄPIENIE OD UMOWY WYKONAWCZEJ

1. Zamawiający ma prawo w terminie nie dłuższym niż 30 dni od powzięcia informacji o zdarzeniu, odstąpić od Umowy Wykonawczej w razie rażącego naruszenia przez Wykonawcę postanowień Umowy Wykonawczej, w szczególności:
 - 1) w przypadku co najmniej dwukrotnych zastrzeżeń wniesionych na piśmie lub elektronicznie w zakresie realizacji Umowy wykonawczej, przede wszystkim co do poprawności, terminowości dostaw, jakości dostarczonego oprogramowania;
 - 2) gdy zwłoka w rozpoczęciu realizacji przedmiotu Umowy Wykonawczej przekroczy 10 dni;
 - 3) w przypadku gdy Wykonawca dostarczył Oprogramowanie z wadami lub Oprogramowanie niezgodne z Umową oraz pomimo zobowiązania do uzupełnienia dostawy do poziomu zgodnego z Umową, Wykonawca w ciągu 10 dni od dnia pisemnego lub elektronicznego wezwania Zamawiającego nie dostarczył wymaganego Oprogramowania;
 - 4) gdy Wykonawca, bez uprzedniej zgody Zamawiającego, zleci wykonanie całości lub części przedmiotu Umowy wykonawczej osobie trzeciej lub gdy Wykonawca wykonuje przedmiot Umowy wykonawczej przy udziale podmiotów, które nie uzyskały pisemnej akceptacji Zamawiającego;
 - 5) gdy suma kar umownych naliczonych przez Zamawiającego przekroczy 30% wartości wynagrodzenia brutto określonego w § 3 ust. 1 Umowy Wykonawczej.
 - 6) dwukrotnego naliczenia przez Zamawiającego kary umownej, o której mowa w § 5 ust. 1 pkt. 4, z tytułu niespełnienia przez Wykonawcę wskaźnika SCCO 2,
 - 7) Zamawiającemu przysługuje prawo odstąpienia od Umowy wykonawczej w terminie do 30 dni w całości lub części niewykonanej, jeżeli wykonanie przedmiotu umowy wykonawczej stanie się niemożliwe wskutek okoliczności leżących po stronie Wykonawcy.
2. Wykonawca może odstąpić od Umowy Wykonawczej w terminie 30 dni, gdy zamówienie nie może być realizowane w sposób należyty z powodu siły wyższej, tj. zdarzeń o charakterze nadzwyczajnym, której czas trwania przekracza 90 dni. Ciężar wskazania zaistniałych okoliczności spoczywa na Wykonawcy.

- 1) W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy wykonawczej nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy wykonawczej lub dalsze wykonywanie Umowy wykonawczej może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od umowy wykonawczej w terminie 30 dni od dnia powzięcia wiadomości o powyższych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego z tytułu wykonanej części Umowy wykonawczej. 5.
- 2) Bez uszczerbku dla innych terminów przewidzianych przepisami prawa powszechnie obowiązującego Zamawiający może odstąpić od części lub całości Umowy wykonawczej w terminie do 30 dni od dnia powzięcia informacji o okolicznościach uzasadniających odstąpienie, w przypadkach określonych w przepisach obowiązującego prawa, w szczególności ustawy Pzp, Kodeksu cywilnego oraz w przypadkach określonych w Umowie wykonawczej.
- 3) Odstąpienie od Umowy wykonawczej winno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia.
- 4) Roszczenie o zapłatę kary umownej z tytułu odstąpienia od Umowy wykonawczej przez Zamawiającego staje się wymagalne od dnia doręczenia Wykonawcy pisemnego oświadczenia o odstąpieniu.
- 5) W przypadku odstąpienia od umowy wykonawczej przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Zamawiający zobowiązany jest do zapłaty jedynie za należycie wykonane dostawy.
- 6) Odstąpienie od Umowy wykonawczej nie zwalnia wykonawcy z obowiązku zapłaty naliczonych kar umownych.

§ 7

INFORMACJE POUFNE

1. Wykonawca zobowiązuje się do zachowania w poufności wszelkich informacji, jakie uzyskał w związku z wykonywaniem Umowy wykonawczej, które są informacjami poufnymi dla każdej ze stron Umowy wykonawczej

2. Nie stanowią tajemnicy prawnie chronionej i nie są poufne informacje, których obowiązek udostępnienia wynika z ustawy Pzp lub ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.
3. Wykonawca zobowiązuje się w toku realizacji umowy wykonawczej przestrzegać obowiązujących u Zamawiającego zasad bezpieczeństwa i ochrony informacji. W zależności od przyjętych zasad u Zamawiającego, Wykonawca zobowiązany będzie do podpisania obowiązujących u Zamawiającego dokumentów (umów, oświadczeń itp.) w powyższym zakresie oraz przestrzegania zasad dotyczących wstępu i wjazdu na teren Zamawiającego. Sposób zapoznania z ww. zasadami ustala się w trybie roboczym z osobą sprawującą nadzór nad realizacją Umowy wykonawczej.
4. Wykonawca zobowiązuje się do nieograniczonego w czasie zachowania w tajemnicy wszelkich informacji związanych z wykonywaniem zadań na rzecz Zamawiającego oraz odpowiada w tym zakresie za pracowników, którzy w jego imieniu wykonują zadania na rzecz Zamawiającego.
5. Informacje niezbędne do realizacji Umowy wykonawczej wykonawca udostępnia wyłącznie tym swoim pracownikom, którym są one niezbędne do wykonywania powierzonych zadań.
6. Wykonawca, na żądanie Zamawiającego, zobowiązany jest do złożenia wymaganych oświadczeń dotyczących zasad bezpieczeństwa i ochrony informacji dla osób, które będą wykonywały prace na terenie Zamawiającego. Wykonawca przed planowanym rozpoczęciem prac w lokalizacjach Zamawiającego jest zobowiązany do przedstawienia, na żądanie listy osób, które będą wykonywały prace na rzecz Zamawiającego.
7. Powielanie oraz kopiowanie dokumentów, zawierających informacje związane z realizacją Umowy wykonawczej, wymaga zgody Zamawiającego.
8. Wykonawca jest zobowiązany do ustalenia z Zamawiającym sposobu przekazywania korespondencji zawierającej informacje mogące mieć wpływ na bezpieczeństwo informacji u Zamawiającego.
9. Po zakończeniu realizacji Umowy wykonawczej wykonawca zobowiązuje się do niezwłocznego zwrotu wszystkich informacji, uzyskanych i wytworzonych w trakcie realizacji Umowy wykonawczej, utrwalonych w formie pisemnej, elektronicznej i ich

kopii oraz do trwałego usunięcia informacji przetwarzanych w formie elektronicznej.

§ 8

OCHRONA DANYCH OSOBOWYCH

7. W ramach realizacji Umowy Wykonawczej nie następuje powierzenie przetwarzania danych osobowych, których administratorem danych, w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „RODO”, jest Zamawiający.
8. Wykonawca nie będzie miał dostępu do danych osobowych ani nie będzie ich przetwarzał, ponad przetwarzanie danych osobowych udostępnionych sobie wzajemnie przez Strony dotyczących w szczególności osób reprezentujących Strony oraz pracowników i współpracowników Stron wyznaczonych do kontaktów w celu zawarcia i wykonania Umowy Wykonawczej.
9. W związku z wzajemnym udostępnieniem danych osobowych, o którym jest mowa w ust. 2 powyżej, Strony stają się niezależnymi administratorami udostępnionych im danych osobowych.
10. Niezwłocznie po zawarciu Umowy Wykonawczej, Strony zobowiązują się do wzajemnego poinformowania osób, których dane zostały udostępnione pomiędzy Stronami zgodnie z ust. 2 powyżej:
 - 1) o zakresie danych osobowych dotyczących tych osób, a przekazanych danej Stronie;
 - 2) o tym, że Strona której dane udostępniono jest administratorem ich danych osobowych oraz że przetwarza ich dane osobowe na zasadach określonych powyżej;
 - 3) o tym, że Strona która dane udostępniła jest źródłem, od którego Strona której dane udostępniono pozyskała ich dane;

- 4) o treści odpowiedniej klauzuli informacyjnej, stanowiącej Załącznik nr 4 do Umowy Wykonawczej (w przypadku klauzuli informacyjnej Zamawiającego) oraz Załącznik nr 5 do Umowy Wykonawczej (w przypadku klauzuli informacyjnej Wykonawcy).
11. Na żądanie jednej ze Stron złożone w formie elektronicznej lub pisemnej, druga Stronałoży w formie elektronicznej lub pisemnej oświadczenie, potwierdzające, że osobom, o których jest mowa w ust. 2 powyżej, została przekazana klauzula informacyjna zgodnie z treścią ust. 4 powyżej.
12. W przypadku, jeśli Wykonawca lub podwykonawca miałby uzyskać dostęp do innych danych osobowych niż wskazane w ust. 2 powyżej, Strony Umowy Wykonawczej zobowiązują się do niezwłocznego zawarcia stosownej umowy w sprawie powierzenia

§ 9

SIŁA WYŻSZA

1. Żadna ze Stron nie będzie odpowiedzialna za niewykonanie swoich zobowiązań w ramach Umowy Wykonawczej w przypadku, jeśli zostało ono spowodowane zaistnieniem Siły Wyższej.
2. Strona powołująca się na Siłę Wyższą przekaże drugiej Stronie powiadomienie o zaistnieniu lub możliwości zaistnienia Siły Wyższej w możliwie najszybszym czasie, nie później jednak niż terminie 3 Dni Roboczych od:
 - 1) wystąpienia Siły Wyższej, w tym rozpoczęcia działania Siły Wyższej,
 - 2) powzięcia wiedzy o możliwości zaistnienia Siły Wyższej.
3. Strona powołująca się na Siłę Wyższą przekaże drugiej Stronie wraz z powiadomieniem o zaistnieniu lub możliwości zaistnienia Siły Wyższej informację o:
 - 1) spodziewanych skutkach działania Siły Wyższej dla możliwości prawidłowego wykonywania Umowy Wykonawczej,
 - 2) czasie rozpoczęcia i spodziewanym czasie zakończenia Siły Wyższej,
 - 3) proponowanych działaniach, które mogą zminimalizować wpływ Siły Wyższej

na wykonywanie Umowy Wykonawczej.

4. Strona otrzymująca powiadomienie o zaistnieniu lub możliwości zaistnienia Siły Wyższej jest zobowiązana do niezwłocznego, nie później niż w terminie 3 Dni Roboczych, ustosunkowania się do proponowanych działań, o których mowa w ust. 3 pkt 3 powyżej, jeżeli te działania wymagają interakcji z tą Stroną, tj. do wskazania terminu w którym zostaną one podjęte lub przedstawienia uzasadnienia, dlaczego ich podjęcie nie jest możliwe.
5. Strony zobowiązują się do współpracy w celu zminimalizowania wpływu Siły Wyższej dla wykonywania Umowy Wykonawczej.

§ 10

POSTANOWIENIA KOŃCOWE

1. Wykonawca nie ma prawa dokonywać przeniesienia bądź obciążenia swoich praw lub obowiązków wynikających z Umowy Wykonawczej bez uzyskania uprzedniej zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności.
2. W przypadku gdy jakiegokolwiek postanowienia Umowy Wykonawczej są nieważne lub bezskuteczne, pozostałe postanowienia Umowy Wykonawczej pozostają w mocy i są wiążące we wzajemnych stosunkach Stron. W przypadku nieważności lub bezskuteczności jednego lub więcej postanowień Umowy Wykonawczej, Strony zobowiązują się zgodnie dążyć do ustalenia takiej treści Umowy Wykonawczej, która będzie optymalnie odpowiadała zgodnym intencjom Stron, celowi i przeznaczeniu Umowy Wykonawczej oraz zaistniałym okolicznościom.
3. Z zastrzeżeniem pozostałych postanowień Umowy Wykonawczej, wszelkie oświadczenia związane z Umową Wykonawczą dla których zastrzeżono formę pisemną, składane będą przez Stronę za pokwitowaniem odbioru lub listem poleconym na adres korespondencyjny Wykonawcy lub Zamawiającego, pod rygorem uznania za nedoręczoną. Strony zgodnie potwierdzają, że w przypadku złożenia oświadczenia, o którym mowa w zdaniu poprzednim, przez którąkolwiek ze

Stron, w postaci elektronicznej i opatrzenia go kwalifikowanym podpisem elektronicznym oraz przesłania za pomocą poczty elektronicznej na adres przedstawiciela Strony, o którym mowa w postanowieniach § 3 ust. 1 i ust. 2 Umowy Wykonawczej, a w przypadku Wykonawcy również na adres e-mail Zamawiającego: _____, takie oświadczenie jest tożsame z oświadczeniem złożonym w formie pisemnej i dostarczeniem go do siedziby Strony. W takiej sytuacji Strona, która otrzymała oświadczenia, zobowiązana jest niezwłocznie potwierdzić drugiej Stronie otrzymanie oświadczenia w formie elektronicznej. Wszelkie zmiany adresów Strony będą komunikować sobie niezwłocznie pod rygorem uznania korespondencji za doręczoną. Strony oświadczają, że ich aktualne adresy korespondencyjne są następujące:

- 1) Zamawiający: ..., [nazwa], ... [adres], ... [e-mail].
- 2) Wykonawca: ..., [nazwa], ... [adres], ... [e-mail].
4. W przypadku zaistnienia pomiędzy Stronami sporu wynikającego z Umowy Wykonawczej lub pozostającego w związku z Umową Wykonawczą, każda ze Stron jest uprawniona do podjęcia próby jego rozwiązania w drodze mediacji. Mediacja prowadzona będzie przez Mediatorów Stałych Sądu Polubownego przy Prokuraturii Generalnej Rzeczypospolitej Polskiej zgodnie z Regulaminem tego Sądu. W przypadku niepowodzenia w rozwiązaniu sporu w drodze mediacji spory wynikłe na tle wykonywania Umowy Wykonawczej będą rozstrzygane przez sąd właściwy dla siedziby Zamawiającego.
5. Wszelkie zmiany postanowień zawartej Umowy Wykonawczej wymagają zachowania formy pisemnej pod rygorem nieważności takiej zmiany, z zastrzeżeniem wyraźnie odmiennych postanowień Umowy Wykonawczej oraz z uwzględnieniem postanowień ust. 7 poniżej.
6. Umowa Wykonawcza może zostać zmieniona przez Zamawiającego oraz Wykonawcę na zasadach określonych w § 13 Umowy Ramowej.
7. Zgodnie z art. 78¹ § 2 Kodeksu cywilnego Strony zgodnie potwierdzają, że złożenie oświadczenia, przez którąkolwiek ze Stron, w postaci elektronicznej i opatrzenie go

kwalifikowanym podpisem elektronicznym jest tożsame z oświadczeniem złożonym w formie pisemnej i stanowi zachowanie wymogu co do formy określonego w Umowie Wykonawczej.

8. Umowa Wykonawcza podlega prawu polskiemu.
9. Umowę Wykonawczą zawarto w formie elektronicznej.
10. Poniższe Załączniki do Umowy Wykonawczej stanowią jej integralną część:

Załącznik nr 1 – Oferta Wykonawcza;

Załącznik nr 2 – Wzór - Protokół Odbioru;

Załącznik nr 3 – Klauzula informacyjna Zamawiającego;

Załącznik nr 4 – Klauzula informacyjna Wykonawcy.

do Umowy Wykonawczej nr

Wzór

Protokół Odbioru

sporządzony w dnia

Wykonawca
...

Zamawiający

1. Wyszczególnienie:

Zamawiający potwierdza prawidłową dostawę i dokonuje odbioru jakościowego niżej wymienionych:

Lp	Przedmiot odbioru	Uwagi	PKWIU ¹

2. Decyzja o odbiorze

Zamawiający stwierdza, że przedmiot odbioru:

- 1) wyszczególniony w poz. zostaje odebrany*,
- 2) wyszczególniony w poz. NIE zostaje odebrany*,

3. Przyczyny odrzucenia (w przypadku odrzucenia odbioru)

4. Dotrzymanie terminu

- Przedmiot odbioru został dostarczony w terminie*
- Przedmiot odbioru **NIE** został dostarczony w terminie*

5. Uwagi i postanowienia dodatkowe

¹ Uzupełnia Wykonawca jeśli dana pozycja obejmuje towar lub usługę wymienioną w Załączniku nr 15 pn. Wykaz towarów i usług, o których mowa w art. 105a ust. 1, art. 106e ust. 1 pkt 18a, art. 108a ust. 1a oraz art. 108e ustawy, do ustawy z dnia 11 marca 2004 t. o podatku od towarów i usług.

Załączniki:

1. _____

2. _____

Wykonawca

Data	Podpis

Zamawiający

Data	Podpis

** Niepotrzebne skreślić*